AVG Anti-Virus 2012

Kullanıcı Kılavuzu

Belge revizyonu 2012.20 (3/29/2012)

İçindekiler

1. Giriş

Bu kullanıcı el kitabı, **AVG Anti-Virus** için kapsamlı dokümantasyon sağlar.

AVG Anti-Virus günümüzün en gelişmiş tehditlerine karşı gerçek zamanlı koruma sağlar. Güven içinde sohbet edin, dosya indirin ve alıp verin. Endişe ve kesinti olmaksızın oyunlar oynayıp videolar seyredin:

- AVG Online Shield™ ile güvenle dosya indirin, paylaşın ve iletiler gönderin
- AVG Social Networking Protection ile sosyal ağlarda güvenli kalın
- LinkScanner'ın gerçek zamanlı koruması ile güven içinde gezinin ve arama yapın

2. AVG Yükleme Gereksinimleri

2.1. Desteklenen İşletim Sistemleri

AVG Anti-Virus aşağıdaki işletim sistemlerine sahip iş istasyonlarını koruma amaçlıdır:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86ve x64, tüm sürümleri)
- Windows 7 (x86 ve x64, tüm sürümler)

(ve belirli işletim sistemleri için daha yeni hizmet paketleri)

***Not**: Kimlik Koruma bileşeni Windows XP x64'te desteklenmez. Bu işletim sisteminde, AVG Anti-Virus yazılımını yalnızca Kimlik Koruma (IDP) bileşeni olmaksızın yükleyebilirsiniz.*

2.2. Minimum ve Önerilen Donanım Gereksinimleri

AVG Anti-Virus için minimum donanım gereksinimleri:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM bellek
- 950 MB boş sabit disk alanı (yükleme için)

AVG Anti-Virus için önerilen donanım gereksinimleri:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM bellek
- 1350 MB boş sabit disk alanı (yükleme için)

3. AVG Yükleme Süreci

Yükleme dosyasını nerede bulabilirim?

Bilgisayarınıza **AVG Anti-Virus** programını yüklemek için, en güncel yükleme dosyasını edinmeniz gerekir. **AVG Anti-Virus** uygulamasının doğru sürümünü yüklediğinizden emin olabilmek için yükleme dosyasını AVG web sitesinden (http://www.avg.com/) indirmeniz önerilir. ***Destek Merkezi / İndirme*** bölümü her AVG sürümü için yükleme dosyalarına ayrıntılı bir genel bakış sunar.

Hangi dosyaları indirip yüklemeniz gerektiğinden emin değilseniz, web sayfasının altındaki ***Ürün seç*** hizmetini kullanmak isteyebilirsiniz. Hizmet, üç basit soruya verilen yanıtların ardından tam olarak ihtiyacınız olan dosyaları tanımlar. Kişisel ihtiyaçlarınız için özelleştirilmiş, indirilebilir dosyaların tam listesine yönlendirilmek için ***Devam*** düğmesine basın.

Yükleme nasıl bir süreçtir?

Yükleme dosyasını sabit diskinize indirme ve kaydetme işlemini tamamladıktan sonra yükleme işlemini başlatabilirsiniz. Yükleme, bir dizi kolay ve anlaşılır iletişim kutusundan oluşur. Her iletişim kutusunda yükleme sürecinin her adımında ne yapılması gerektiği kısaca açıklanır. Devamında, her iletişim penceresi için ayrıntılı bir açıklama sunulur:

3.1. Hoşgeldiniz: Dil Seçimi

Yükleme süreci ***AVG Yükleyiciye hoş geldiniz*** iletişim kutusu ile başlar:

Bu iletişim kutusunda yükleme süreci için kullanılan dili seçebilirsiniz. Dil menüsü açmak için iletişim kutusunun sağ köşesindeki açılır kutuyu tıklatın. İstediğiniz dili seçtiğinizde yükleme süreci bu dille devam eder.

Dikkat: Şu anda yalnızca yükleme süreci dilini seçmektesiniz. AVG Anti-Virus uygulaması

seçilen dilde yüklenir ve İngilizce her zaman otomatik olarak yüklenir. Ancak, daha fazla dil yüklemek ve AVG Anti-Virus uygulamasında bu dillerden biriyle çalışmak mümkündür. Özel Seçenekler adlı kurulum iletişim kutularından birinde alternatif dil seçimlerinizi onaylamanız istenir.

3.2. Hoşgeldiniz: Lisans Sözleşmesi

Sonraki adımda, ***AVG Yükleyici hoş geldiniz*** iletişim kutusu AVG lisans sözleşmesinin tam metnini içerir:

Lütfen tüm metni dikkatlice okuyun. Okuduğunuzu, anladığınızı ve sözleşmeyi kabul ettiğinizi onaylamak için, ***Kabul Et*** düğmesine basın. Lisans sözleşmesini kabul etmiyorsanız ***Kabul Etmiyorum*** düğmesine basın, böylece yükleme süreci anında iptal edilecektir.

AVG Gizlilik Politikası

Bu kurulum iletişim kutusu, lisans sözleşmesinin yanı sıra AVG gizlilik politikası hakkında da daha fazla bilgi seçeneği sunar. İletişim kutusunun sol alt köşesinde ***AVG Gizlilik Politikası*** bağlantısını görebilirsiniz. AVG Technologies gizlilik politikası ilkelerinin tam metnini bulabileceğiniz AVG web sitesine (http://www.avg.com/) yönlendirilmek için bu bağlantıyı tıklatın.

Kontrol düğmeleri

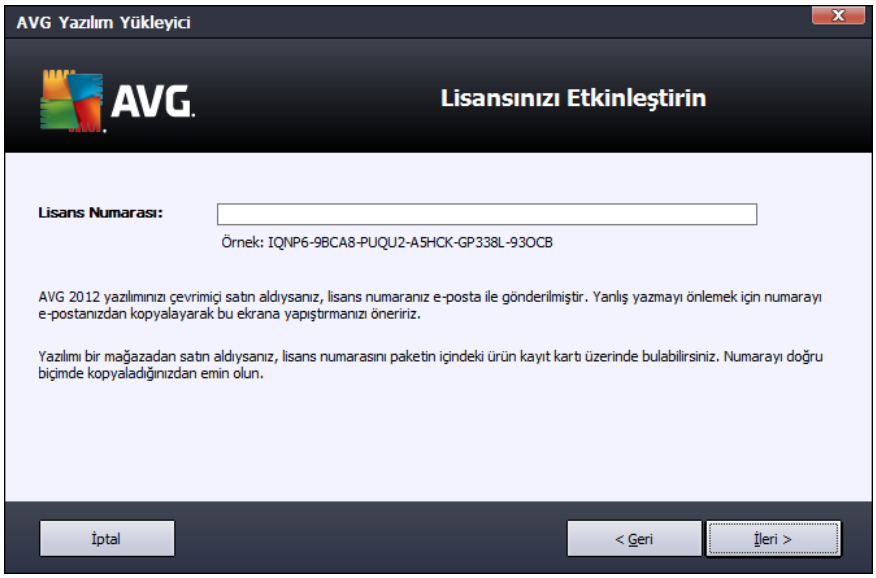
İlk kurulum iletişim kutusunda yalnızca iki kontrol düğmesi mevcuttur:

- ***Yazdırılabilir sürüm*** – AVG lisans sözleşmesinin tüm metnini yazdırmak için tıklatın.
- ***Reddet*** – Lisans sözleşmesini reddetmek için tıklatın. Kurulum süreci derhal sonlandırılır. **AVG Anti-Virus** yüklenmez!

- ***Geri*** – Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatın.
- ***Kabul Et*** - Lisans sözleşmesini okuduğunuzu, anladığınızı ve kabul ettiğinizi onaylamak için tıklatın. Yükleme devam eder ve bir sonraki kurulum iletişim kutusuna geçersiniz.

3.3. Lisansınızı etkinleştirme

Lisansınızı Etkinleştirin iletişim kutusunda, lisans numaranızı verilen metin alanına yazmanız istenir:



Lisans numarası nereden bulunabilir

Satış numarası, **AVG Anti-Virus** kutusundaki CD paketinde bulunabilir. Lisans numarası **AVG Anti-Virus** programını çevrimiçi satın aldıktan sonra alacağınız onay e-postasında olacaktır. Sayıları gösterildiği gibi gitmelisiniz. Lisans numarasının dijital formu mevcut ise (*e-postada*) girmek için kopyala ve yapıştır yönteminin kullanılması önerilmektedir.

Kopyala ve Yapıştır yöntemi nasıl kullanılır

Kopyala ve Yapıştır yöntemini kullanarak **AVG Anti-Virus** lisans numarasını programa girmek, numaranın doğru biçimde girilmesini garanti altına alır. Lütfen şu adımları takip edin:

- Lisans numaranızın bulunduğu e-postayı açın.
- Lisans numarasının başında sol fare düğmesine tıklatın, düğmeyi tutup numaranın sonuna kadar sürükleyin ve düğmeyi bırakın. Numaranın vurgulanması gerekir.
- ***Ctrl*** tuşunu basılı tutun ve ***C*** tuşuna basın. Bu işlem numarayı kopyalar.

- Kopyalanan numarayı yapıştırmak istediğiniz konumu tıklatın.
- ***Ctrl*** tuşunu basılı tutun ve ***V*** tuşuna basın. Bu işlem numarayı seçilen konuma yapıştırır.

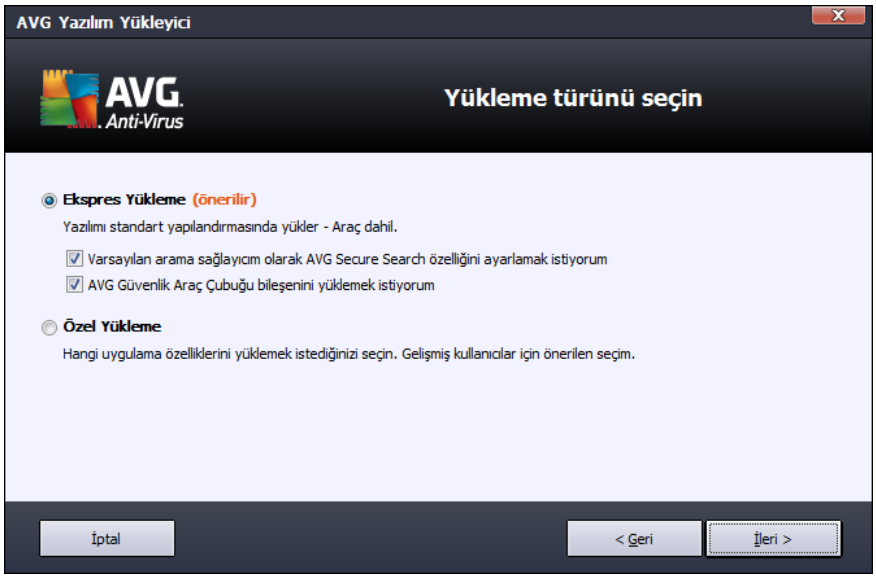
Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- ***İptal*** – Kurulum işleminden hemen çıkmak için tıklatın; **AVG Anti-Virus** kurulmaz!
- ***Geri*** – Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatın.
- ***İleri*** – Kuruluma devam etmek ve bir adım ilerlemek için tıklatın.

3.4. Yükleme türünü seçin

Yükleme türünü seçin iletişim kutusu iki yükleme seçeneği sunar: ***Ekspres Yükleme*** ve ***Özel Yükleme***:



Ekspres yükleme

Kullanıcıların çoğu için **AVG Anti-Virus** uygulamasını program geliştiricisi tarafından önceden tanımlanmış ayarlarla tam otomatik modda AVG Gadget'ı da dahil ederek yükleyen ***Ekspres*** yükleme seçeneği önerilir. Bu yapılandırma, minimum kaynak kullanımı ile maksimum güvenliği bir araya getirir. Gelecekte söz konusu yapılandırmayı değiştirme ihtiyacı duyarsanız söz konusu işlemi doğrudan **AVG Anti-Virus** uygulamasından yapabileceksiniz.

Bu seçenek içinde önceden onaylanmış iki onay kutusu görebilirsiniz ve iki seçeneği de işaretli

tutmanız kesinlikle önerilir:

- ***AVG Secure Search ürününü varsayılan arama sağlayıcım olarak ayarlamak istiyorum*** – çevrimiçi maksimum güvenlik için Link Scanner bileşeni ile sıkı bir işbirliği içinde çalışan AVG Secure Search motorunu kullanmak istediğinizi onaylamak için işaretleyin.
- ***AVG Security Toolbar'ı yüklemek istiyorum*** – AVG Security Toolbar yükleyerek internet taraması sırasında maksimum güvenlik sağlamak için işaretleyin.

Bir sonraki AVG Security Toolbar'ı yükle iletişim kutusuna geçmek için ***İleri*** düğmesine basın.

Özel yükleme

Özel Yükleme **AVG Anti-Virus** uygulamasını standart olmayan ayarlarla kurmak için geçerli bir nedeni olan deneyimli kullanıcılar tarafından kullanılmalıdır. Örn. belirli sistem gereksinimlerini karşılamak için.

Bu seçeneğe karar verirseniz, iletişim kutusunda ***Hedef Klasör*** adında yeni bir iletişim kutusu görüntülenir. Bu iletişim kutusunda **AVG Anti-Virus** uygulamasının yükleneceği yeri belirlemeniz gerekir. Varsayılan olarak, **AVG Anti-Virus**, iletişim kutusundaki metin alanında belirtildiği gibi, C: sürücüsündeki program dosyaları klasörüne yüklenir. Bu konumu değiştirmek istiyorsanız, sürücü yapısını görüntülemek ve ilgili klasörü seçmek için ***Gözat*** düğmesini kullanın. Yazılım satıcısı tarafından önceden ayarlanmış varsayılan hedefi geri getirmek için, ***Varsayılan*** düğmesini kullanın.

Ardından, ***Özel Seçenekler*** iletişim kutusuna gitmek için İleri düğmesine basın.

Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- ***İptal*** – Kurulum işleminden hemen çıkmak için tıklatın; **AVG Anti-Virus** kurulmaz!
- ***Geri*** – Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatın.
- ***İleri*** – Kuruluma devam etmek ve bir adım ilerlemek için tıklatın.

3.5. Özel seçenekler

Özel Seçenekler iletişim kutusu yükleme parametrelerinin ayrıntılı parametrelerini ayarlamanıza olanak verir:

Bileşen Seçimi bölümünde, yüklenebilecek tüm **AVG Anti-Virus** bileşenleriyle ilgili genel bir görünüm bulunur. Varsayılan ayarların size uygun olmaması halinde belirli bileşenleri kaldırabilir ya da ekleyebilirsiniz.

Ancak, yalnızca satın aldığınız AVG sürümü dahilinde bulunan bileşenler arasından seçim yapabilirsiniz!

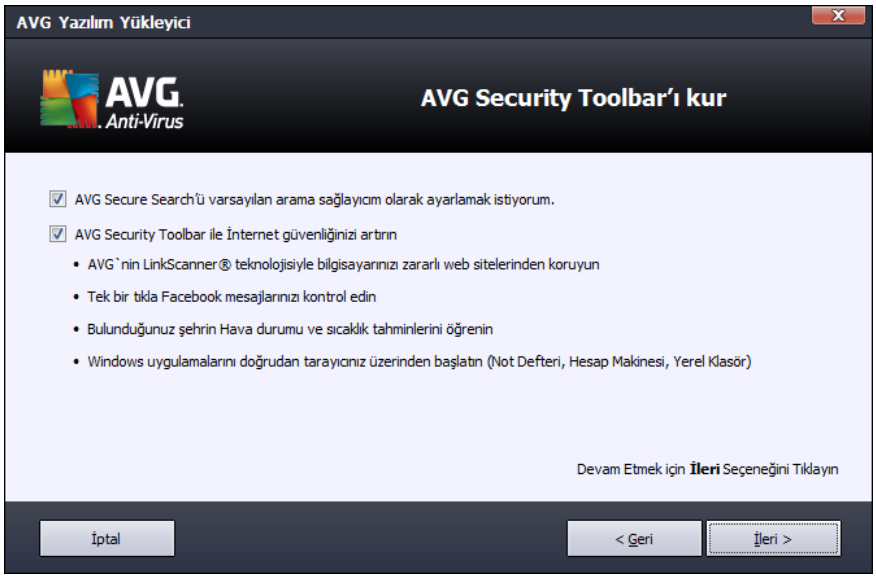
Bileşen Seçimi listesindeki tüm öğeleri vurgulayın, böylece ilgili bileşenin kısa açıklaması bu bölümün sağ tarafından görüntülenir. Her bileşenin işlevleri ile ilgili ayrıntılı bilgiler için, bu belgedeki Bileşen Genel Görünümü bölümüne bakın. Yazılım satıcısı tarafından önceden ayarlanmış varsayılan yapılandırmayı geri getirmek için, ***Varsayılan*** düğmesini kullanın.

Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- ***İptal*** – Kurulum işleminden hemen çıkmak için tıklatın; **AVG Anti-Virus** kurulmaz!
- ***Geri*** – Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatın.
- ***İleri*** – Kuruluma devam etmek ve bir adım ilerlemek için tıklatın.

3.6. AVG Security Toolbar'ı yükle



AVG Security Toolbar'ı yükle iletişim kutusunda, AVG Security Toolbar uygulamasını yüklemek isteyip istemediğinize karar verebilirsiniz. Varsayılan ayarları değiştirmezseniz, internette gezinirken size daha kapsamlı koruma sağlamak için bu bileşen otomatik olarak internet tarayıcınıza yüklenir (*şu anda desteklenen tarayıcılar Microsoft Internet Explorer v. 6.0 ve üstü ve Mozilla Firefox v. 3.0 ya da üstüdür*).

Ayrıca *AVG Secure Search (powered by Google)* arama motorunu varsayılan arama sağlayıcınız olarak atamaya karar verme seçeneğiniz de bulunmaktadır. Öyle istiyorsanız, ilgili onay kutusunu işaretli bırakın.

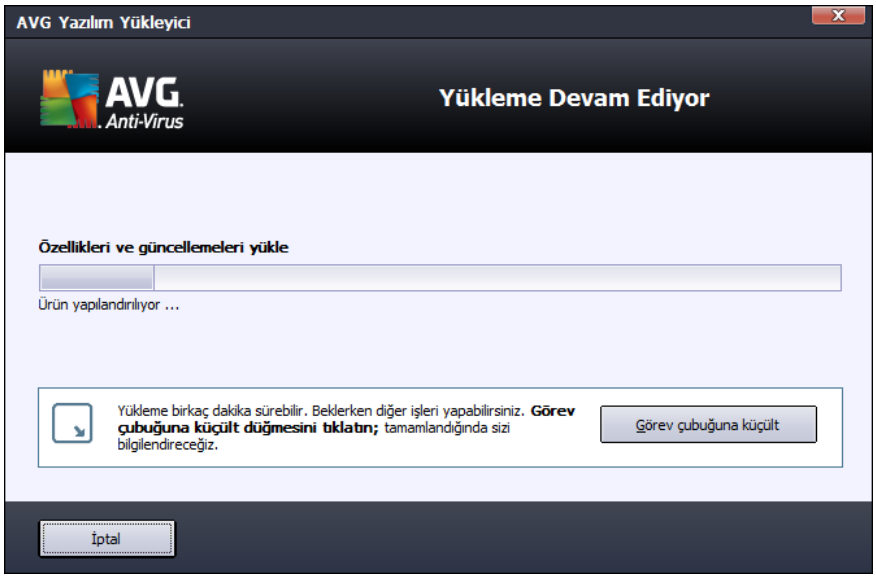
Kontrol düğmeleri

Çoğu kurulum iletişim kutusunda olduğu gibi üç kontrol düğmesi mevcuttur:

- ***İptal*** – Kurulum işleminden hemen çıkmak için tıklatın; **AVG Anti-Virus** kurulmaz!
- ***Geri*** – Önceki kurulum iletişim kutusuna, bir adım geriye gitmek için tıklatın.
- ***İleri*** – Kuruluma devam etmek ve bir adım ilerlemek için tıklatın.

3.7. Yükleme ilerlemesi

Yükleme İlerlemesi iletişim kutusu yükleme sürecinin ilerleme durumu gösterir ve herhangi bir müdahale gerektirmez:



Yükleme işlemi bittiğinde, otomatik olarak bir sonraki iletişim kutusuna yönlendirilirsiniz.

Kontrol düğmeleri

Bu iletişim kutusunda yalnızca bir kontrol düğmesi mevcuttur – ***İptal***. Yalnızca devam eden yükleme sürecini durdurmak istiyorsanız bu düğmeyi kullanmalısınız. Böyle bir durumda **AVG Anti-Virus** uygulamasının yüklenmeyeceğini lütfen unutmayın!

3.8. Yükleme başarılı oldu

Yükleme başarılı oldu iletişim kutusu, **AVG Anti-Virus** yazılımınızın tam olarak yüklendiğini ve yapılandırıldığını onaylar:

Ürün Geliştirme Programı

Burada, genel internet güvenliği seviyesini yükseltmek için anonim olarak bilgi toplayan Ürün Geliştirme Programı'na katılıp katılmamayı seçebilirsiniz (*ayrıntılar için AVG Gelişmiş Ayarları / Ürün Geliştirme Programı* bölümüne bakabilirsiniz). Bu bildirimi kabul ediyorsanız ***AVG 2012 web güvenliği ve Ürün Geliştirme Programı'na katılmayı kabul ediyorum ...*** seçeneğini işaretleyin *(seçenek varsayılan olarak onaylıdır)*.

Yükleme sürecini bitirmek için ***Bitir*** düğmesine basın.

4. Yüklemeden Sonra

4.1. Ürün kaydı

AVG Anti-Virus kurulumunu tamamladıktan sonra, lütfen ürününüzü çevrimiçi olarak AVG web sitesinde (http://www.avg.com/) kaydettirin. Kayıt işleminin ardından AVG Kullanıcı hesabınıza erişebilecek, AVG Güncelleme bültenini alacak ve sadece kayıtlı kullanıcılara sunulan diğer hizmetlerden yararlanacaksınız.

Ürünü kaydettirmenin en kolay yolu doğrudan **AVG Anti-Virus** kullanıcı arayüzünü kullanmaktır. Ana menüde Yardım/Şimdi kaydolun öğesini seçin. AVG web sitesindeki (http://www.avg.com/) ***Kayıt*** sayfasına yönlendirilirsiniz. Lütfen sayfadaki talimatları izleyin.

4.2. Kullanıcı arayüzüne erişim

AVG ana iletişim kutusuna çeşitli yöntemlerle ulaşabilirsiniz:

- AVG sistem tepsisi sembolü
- Masaüstünüzdeki AVG simgesini çift tıklatın
- menüden ***Başlat / Tüm Programlar / AVG 2012***

4.3. Tüm bilgisayarın taranması

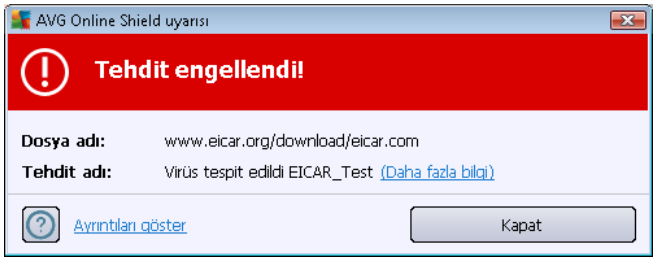
AVG Anti-Virus yüklemesinden önce bilgisayarınıza virüs bulaşmış olması ihtimali bulunmaktadır. Bu nedenle bilgisayarınızda virüs bulunmadığından emin olmak için Tüm bilgisayar taraması yapmanız gerekmektedir. İlk tarama uzun bir süre alabilir *(bir saat civarında)*, ancak bilgisayarınızın herhangi bir tehdit altında olmadığından emin olmak için bu taramayı başlatmanız önerilir. Tüm bilgisayar taraması konusunda talimatlar için AVG Taraması bölümünü inceleyin.

4.4. Eicar testi

AVG Anti-Virus programının düzgün olarak yüklendiğini onaylamak için EICAR testini çalıştırabilirsiniz.

EICAR testi, virüsten koruma sistemin çalıştığından emin olmak üzere kullanılan standart ve kesinlikle güvenli bir yöntemdir. Gerçek bir virüs olmadığı için yayılmasında sakınca yoktur ve herhangi bir virüs kodu içermemektedir. Ürünlerin çoğu sanki bir virüsmüş gibi tepki verir (*ancak "EICAR-AV-Test" adı altında rapor ederler*). EICAR virüsünü www.eicar.com adresinde bulunan EICA'ın web sitesinden indirebilir ve bunun yanı sıra EICAR testi hakkında tüm gerekli bilgileri edinebilirsiniz.

eicar.com dosyasını indirmeye çalışın ve sabit diskinize kaydedin. Siz test dosyasını indirmeyi onaylar onaylamaz Resident Shield (*Link Scanner bileşenin parçasıdır*) bu durum için bir uyarı verir. Bu bildirim, AVG'nin bilgisayarınıza doğru bir şekilde yüklenmiş olduğunu gösterir.



http://www.eicar.com web sitesinden EICAR 'virüs' sıkıştırılmış sürümünü (*örn. eicar_com.zip biçiminde*) de indirebilirsiniz. Online Shield bu dosyayı indirmenizi ve yerel diskinize kaydetmenizi sağlar, ancak Resident Shield (*Virüslerden Koruma bileşeni içinde*) paketi açmaya çalıştığınızda 'virüsü' algılar.

AVG'nin EICAR test dosyasını virüs olarak algılamaması halinde program yapılandırmasını yeniden kontrol etmeniz gerekir!

4.5. AVG varsayılan yapılandırması

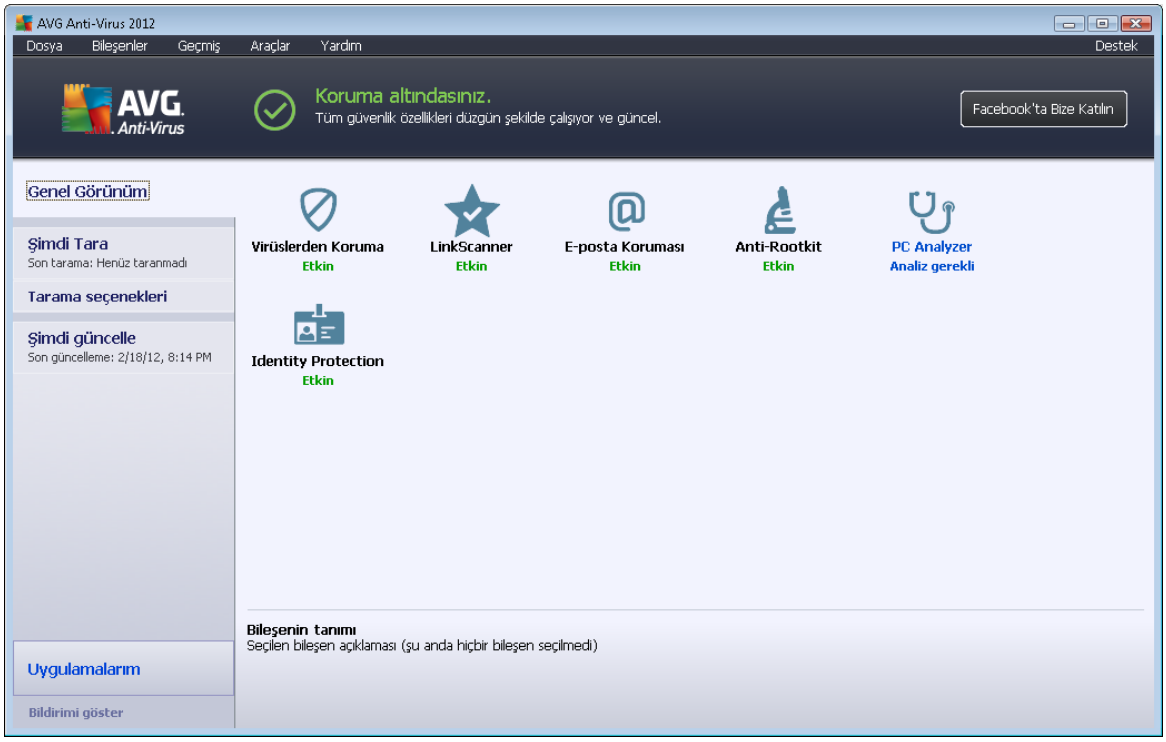
AVG Anti-Virus varsayılan yapılandırması (*yani, uygulamanın yüklemeden sonra doğru şekilde nasıl ayarlanacağı*) yazılım satıcısı tarafından ayarlanabilir, böylece optimum performans elde etmek için tüm bileşenler ve işlevler ayarlanabilir.

Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin! Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.

AVG bileşenlerinde yapılan bazı ufak değişikliklere ilgili bileşenin kullanıcı arayüzünden ulaşabilirsiniz. İhtiyaçlarınızı daha iyi karşılaması açısından AVG yapılandırmasını değiştirme ihtiyacı hissederseniz AVG Gelişmiş Ayarları'na gidin: sistem menüsü öğesini seçin ***Araçlar/Gelişmiş ayarlar*** ve AVG yapılandırmasını yeni açılan AVG Gelişmiş Ayarlar iletişim kutusunda düzenleyin.

5. AVG Kullanıcı Arayüzü

AVG Anti-Virus ana pencerede açılır:



Ana pencere çok sayıda bölüme ayrılır:

- ***Sistem Menüsü*** *(penceredeki en üst sistem çubuğu)*, tüm **AVG Anti-Virus** bileşenlerine, servislerine ve özelliklerine ulaşmanızı sağlayan standart dolaşım yöntemidir – ayrıntılar >>
- ***Güvenlik Durumu Bilgileri*** *(pencerenin üst bölümü)* **AVG Anti-Virus** programınızın mevcut durumu hakkında bilgi sunar – ayrıntılar >>
- ***Facebook'ta bize katılın*** *(pencerenin sağ üst bölümü)* düğmesi Facebook'ta AVG topluluğuna katılmanızı sağlar. Ancak, düğme yalnızca tüm bileşenler tamamen işlevsel olduğunda ve düzgün çalıştığında görünür *(AVG bileşenlerinin durumunu öğrenme hakkında daha fazla bilgi için Güvenlik Durumu Bilgisi bölümüne bakın)*
- ***Hızlı Bağlantılar*** *(pencerenin sol bölümü)* en önemli ve en sık kullanılan **AVG Anti-Virus** görevlerine hızlı bir şekilde erişebilmenizi sağlar – ayrıntılar >>
- ***Uygulamalarım*** *(pencerenin sol alt bölümü)* **AVG Anti-Virus** için mevcut ek uygulamalara bir genel bakış penceresi açar: LiveKive, Family Safety ve PC Tuneup
- ***Bileşenlere Genel Bakış*** *(pencerenin orta kısmı)* yüklü tüm **AVG Anti-Virus bileşenleri hakkında genel bilgi verir** – ayrıntılar >>
- ***Sistem Tepsisi Simgesi*** *(ekranın sağ alt köşesi, sistem tepsisi üzerinde)* mevcut **AVG Anti-Virus durumunu gösterir** - ayrıntılar >>

- ***AVG gadget'ı*** *(Windows kenar çubuğu, Windows Vista/7'de desteklenir)* **AVG Anti-Virus** taramasına ve güncellemesine hızlı biçimde erişmenizi sağlar – ayrıntılar >>

5.1. Sistem Menüsü

Sistem menüsü tüm Windows uygulamalarında kullanılan standart bir dolaşım yöntemidir. **AVG Anti-Virus** ana penceresinin en üstünde yatay olarak konumlandırılmıştır. Belirli AVG bileşenlerine, özelliklerine ve hizmetlerine ulaşmak için sistem menüsünü kullanın.

Sistem menüsü beş ana bölüme ayrılmıştır:

5.1.1. Dosya

- ***Çıkış*** – **AVG Anti-Virus**'nin kullanıcı arayüzünü kapatır. Ancak AVG uygulaması arkaplanda çalışmaya devam edecek ve bilgisayarınız korunmaya devam edecektir.

5.1.2. Bileşenler

Sistem menüsünün Bileşenler öğesi, yüklenen tüm AVG bileşenlerine ilişkin bağlantılar içerir ve kullanıcı arayüzünde bunların varsayılan iletişim kutusu sayfalarını açar:

- ***Sisteme genel bakış*** – yüklü tüm bileşenlerle ve durumlarıyla birlikte varsayılan kullanıcı arayüzü iletişim kutusuna geçer
- ***Virüslerden Koruma*** sisteminizdeki virüs, casus yazılım, solucan, truva atı ve istenmeyen yürütülebilir dosyaları veya kitaplıkları tespit eder ve sizi kötü amaçlı reklam yazılımlarından korur - ayrıntılar >>
- ***LinkScanner*** internette arama ve gezinme sırasında sizi web tabanlı saldırılara karşı korur – ayrıntılar >>
- ***E-posta Koruması*** gelen e-posta mesajlarınızı istenmeyen e-postalara karşı denetler ve virüsleri, kimlik avı saldırılarını veya diğer tehditleri engeller – ayrıntılar >>
- ***Anti-Rootkit*** uygulamalar, sürücüler ve kitaplıklarda gizlenmiş tehlikeli kök dizinler için tarama yapar – ayrıntılar >>
- ***PC Analyzer***, bilgisayarınızın durumu hakkında bilgi verir – ayrıntılar >>
- ***Identity Protection*** dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı korumak üzere sürekli tetiktedir – ayrıntılar >>
- ***Uzaktan Yönetim*** yalnızca yükleme süreci esnasında bu bileşenin yüklenmesini istediğinizi belirtmeniz halinde AVG Business Sürümlerinde görüntülenir

5.1.3. Geçmiş

- Tarama sonuçları – AVG test arayüzüne ve özellikle Tarama Sonuçlarına Genel Bakış penceresine gider
- Resident Shield tespiti – Resident Shield

- E-mail Scanner tespiti – E-posta Koruması bileşeni tarafından tehlikeli olduğu tespit edilen posta eklentileri hakkında genel bilgi veren bir pencere açar

- Online Shield bulguları – LinkScanner bileşeni içindeki Online Shield tarafından tespit edilen tehlikeler hakkında genel bilgi veren bir iletişim kutusu açar

- Virüs Kasası – Belirli bir neden doğrultusunda AVG'nin tespit edilmiş temizlenemeyen tüm bulaşmaları sildiği karantina alanının arayüzünü açar (Virüs Kasası) Karantina altında bulunan bulaşmış dosyalar, yalıtılmıştır, bilgisayarınızın güvenliği garanti altındadır ve aynı anda bulaşmış dosyalar ileride tamir edilebilecekleri göz önünde bulundurularak depolanır

- Etkinlik geçmişi kayıt defteri – kaydedilen tüm **AVG Anti-Virus** eylemler hakkında genel bilgi veren bir geçmiş kayıt defteri arayüzü açar

5.1.4. Araçlar

- Bilgisayarı tara – Tüm bilgisayar taraması başlatır.

- Seçilen klasörü tara... – AVG tarama arayüzüne geçer ve bilgisayarınızın dolaşım ağacından taranmasını istediğiniz dosya ve klasörleri seçmenizi sağlar.

- ***Dosyayı tara...*** – Belirli tek bir dosya üzerinde talebe göre test yapmanızı sağlar. Diskinizin ağaç yapısını içeren yeni bir pencere açmak için bu seçeneği tıklatın. İstediğiniz dosyayı seçin ve tarama başlatmayı onaylayın.

- Güncelle – Otomatik olarak güncellemesi **AVG Anti-Virus** işlemini başlatır.

- ***Dizinden güncelle...*** – Sabit diskinizde bulunan belirli bir dosyanın içinde yer alan güncelleme dosyalarını alarak güncelleme işlemini gerçekleştirir. Diğer bir yandan bu seçim sadece acil durumlarda önerilmektedir. Örn. Internet bağlantısı olmadığı durumlarda (*Örneğin bilgisayarınıza virüs bulaşmış ise ve Internet bağlantınız kesildiyse; bilgisayarınız bir ağa bağlıysa fakat Internet erişimi yok ise vb.*). Yeni açılan pencereden, daha önce güncelleme dosyasını depoladığınız klasörü seçin ve güncelleme işlemini başlatın.

- Gelişmiş ayarlar... – AVG Anti-Virus yapılandırmasını düzenleyebileceğiniz AVG gelişmiş ayarlar iletişim kutusunu açar. Genel olarak uygulamanın yazılım üreticisi tarafından tanımlanan varsayılan ayarlarının muhafaza edilmesi önerilir.

5.1.5. Yardım

- ***İçindekiler*** – AVG yardım dosyalarını açar

- ***Destek Alın*** – Müşteri destek merkezi sayfasında AVG web sitesini (http://www.avg.com/) açar

- ***AVG Web Sayfanız*** – AVG web sitesini (http://www.avg.com/) açar

- ***Virüsler ve Tehditler Hakkında*** – tanımlanan virüs hakkında ayrıntılı bilgi edinebildiğiniz çevrimiçi Virüs Ansiklopedisini açar

- ***Yeniden Etkinleştir*** – ***Yükleme işleminin*** AVG'yi Kişiselleştir iletişim kutusuna girilen verilerle AVG'yi Etkinleştir iletişim kutusunu açar. Bu iletişim kutusunda satış numaranızı (

AVG'yi yüklerken kullandığınız numara), ya da eski lisans numaranızı (*Örn. yeni bir AVG ürününe geçerken*) değiştirmek için lisans numaranızı girebilirsiniz.

- ***Şimdi kaydolun*** - AVG web sitesinin (http://www.avg.com/) kayıt sayfasına bağlanır. Lütfen kayıt bilgilerinizi doldurun; sadece AVG ürünlerini kaydettiren müşterilerimiz ücretsiz teknik destek alabilecektir.

Not: **AVG Anti-Virus** *deneme sürümünü kullanıyorsanız, sonraki iki öğe,* ***Şimdi satın al*** *ve* ***Etkinleştir*** *olarak görünür ve programın tam sürümünü hemen satın almanızı sağlar. Bir satış numarasıyla yüklenmiş* **AVG Anti-Virus** *için, öğeler* ***Kaydet*** *ve* ***Etkinleştir*** *olarak görünür.*

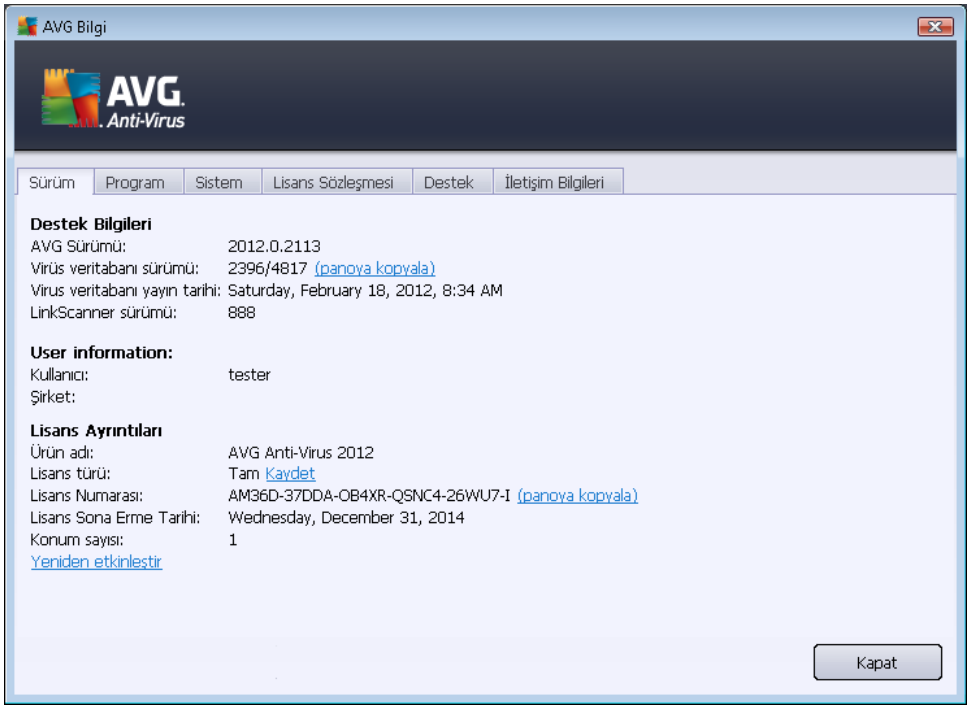
- ***AVG Hakkında*** – ***AVG Technologies CZ***'nin iletişim bilgileri, lisans sözleşmesi, sistem bilgileri, program ve virüs veritabanı versiyonu ve program adı hakkında bilgi veren altı sekmeli ***Bilgi*** iletişim kutusunu açar.

5.1.6. Destek

Destek bağlantısı, yardım ararken ihtiyaç duyabileceğiniz tüm bilgileri içeren yeni bir ***Bilgi*** iletişim kutusu açar. İletişim kutusunda kurulu AVG programınız (*program / veritabanı sürümü*) ile ilgili temel bilgiler, lisans ayrıntıları ve hızlı destek bağlantıları listesi bulunur.

Bilgi iletişim kutusu altı sekmeye ayrılmıştır:

Sürüm sekmesi üç bölüme ayrılmıştır:

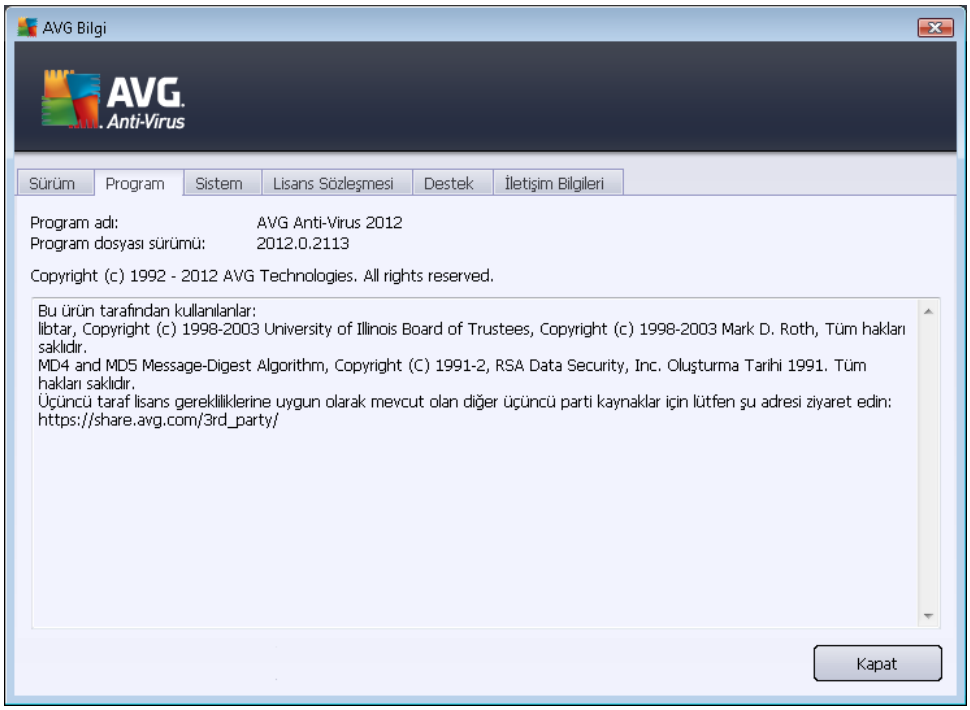


- ***Destek Bilgileri*** - **AVG Anti-Virus** Sürüm, virüs veritabanı, Virüslerden Koruma veritabanı sürümü ve LinkScanner sürümü hakkında bilgi verir.

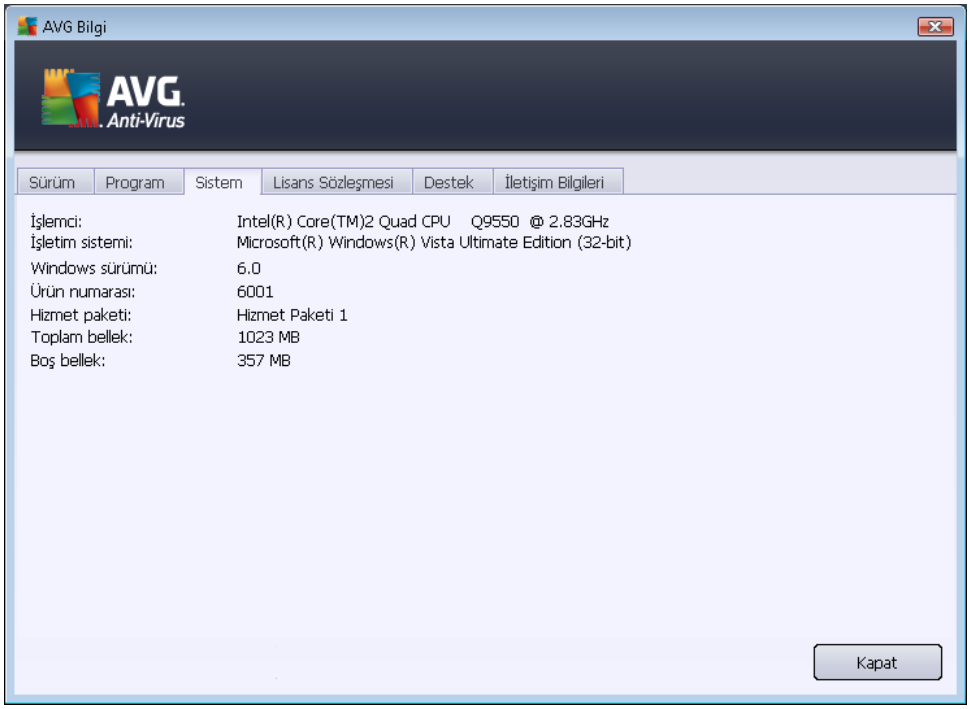
- ***Kullanıcı Bilgileri*** - Lisanslı kullanıcı ve şirket hakkında bilgi verir.

- ***Lisans Ayrıntıları*** - Lisansınız hakkında bilgi verir *(ürün adı, lisans türü, lisans numarası, son kullanma tarihi ve kullanıcı sayısı*). Bu bölümde ***Kaydet*** bağlantısını kullanarak **AVG Anti-Virus** uygulamanızı çevrimiçi kaydettirebilirsiniz; böylece AVG teknik desteği tam kapsamda kullanabilirsiniz. Ayrıca, ***Yeniden etkinleştir*** bağlantısını kullanarak ***AVG'yi etkinleştir*** iletişim kutusunu açabilirsiniz: satış numaranızı *(AVG Anti-Virus kurulumu sırasında kullandığınız)* değiştirmek veya mevcut lisans numaranızı bir başkasıyla değiştirmek *(örn. daha üst bir AVG ürününe yükseltme yaparken) için ilgili alana lisans numaranızı girin.*

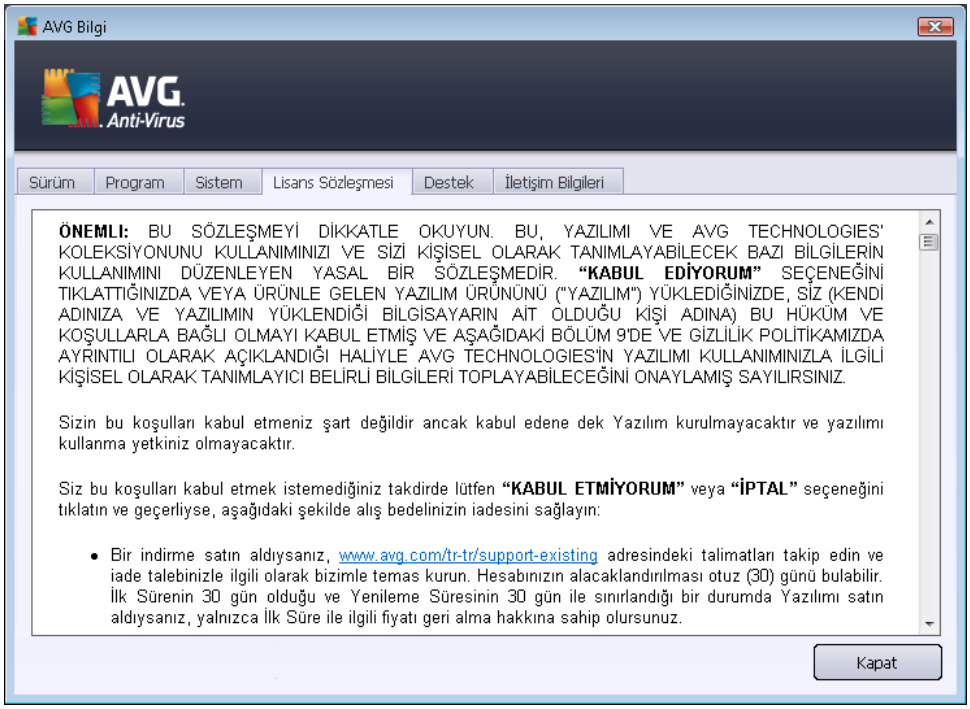
Program sekmesinde **AVG Anti-Virus** program dosyası sürümü ve üründe kullanılan üçüncü partileri kodları hakkında bilgi bulabilirsiniz:



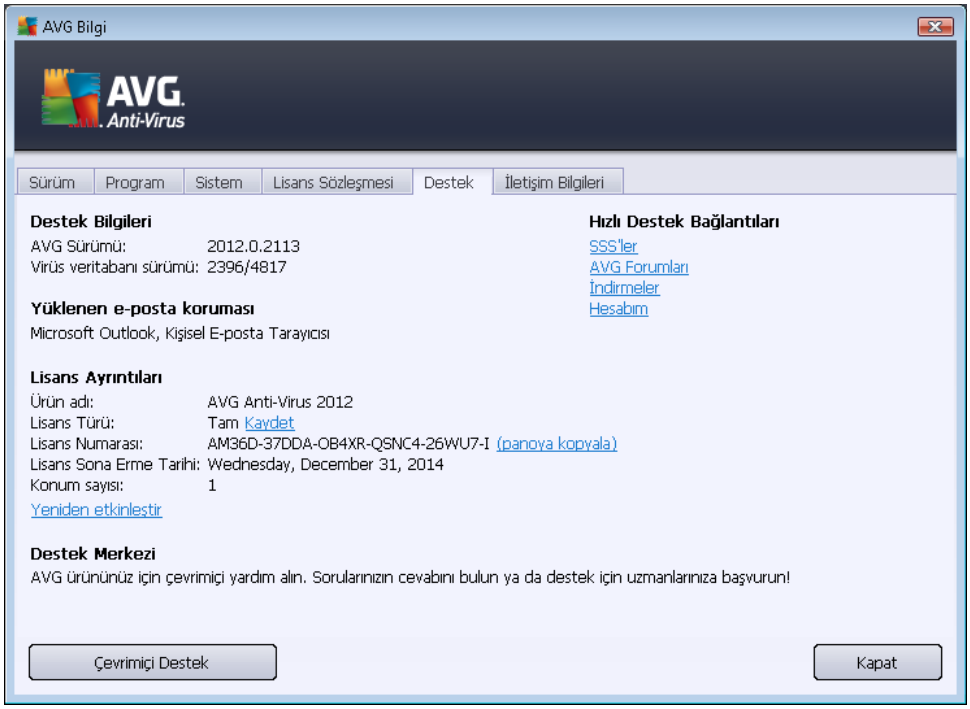
Sistem sekmesi işletim sistemi parametrelerinin listesini sunar *(işlemci türü, işletim sistemi ve sürümü, üretim numarası, kullanılan hizmet paketleri, toplam bellek boyutu ve boş bellek boyutu)*:



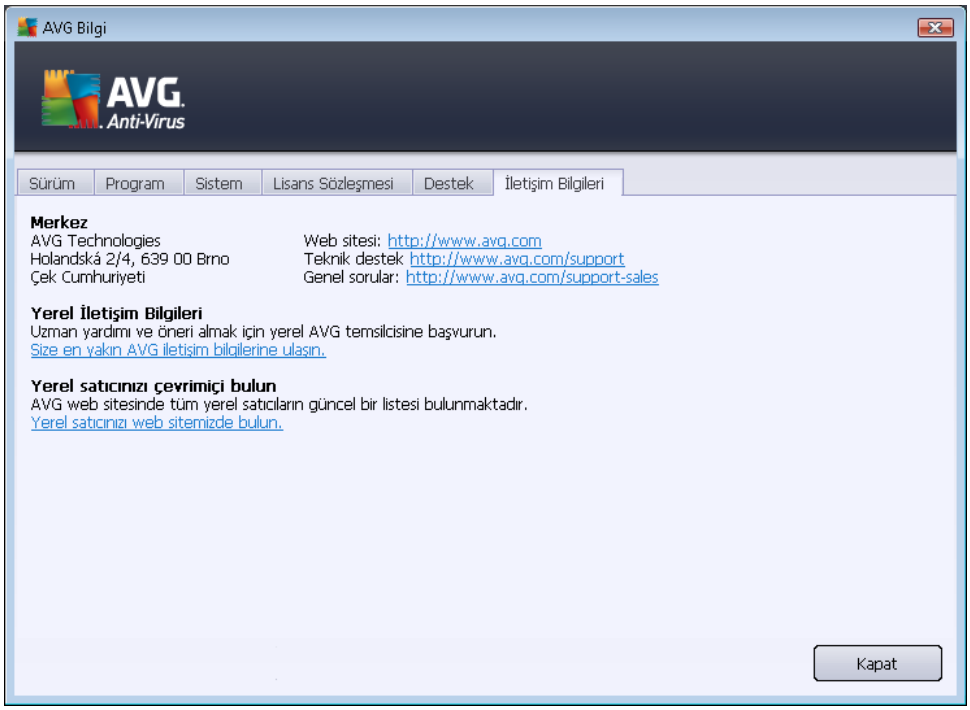
Lisans Sözleşmesi sekmesinde siz ve AVG Technologies arasındaki lisans sözleşmesinin tam metnini okuyabilirsiniz:



Destek sekmesi müşteri desteğiyle iletişim kurma imkanlarının listesini sunar. Ayrıca, AVG web sitesi (http://www.avg.com/), AVG forumları, SSS vb. bölümlerin bağlantılarını sağlar. Müşteri destek ekibiyle iletişim kurduğunuzda kullanabileceğiniz bilgileri de burada bulabilirsiniz:



İletişim sekmesi AVG Technologies ve AVG yerel temsilcileri ve satıcılarında iletişim kurulabilecek kişilerin listesini sunar:



5.2. Güvenlik Durumu Bilgisi

Güvenlik Durumu Bilgisi bölümü **AVG Anti-Virus** ana penceresinin üst kısmında yer alır. Bu bölümde **AVG Anti-Virus** programınızın mevcut güvenlik durumu hakkında her zaman bilgi bulabilirsiniz. Lütfen bu bölümde betimlenmesi muhtemel simgeleri ve anlamlarını inceleyin:

 - Yeşil simge ***AVG Anti-Virus uygulamasının tamamen işlevsel olduğunu belirtir***. Bilgisayarınız tamamen korunmaktadır, günceldir ve yüklü tüm bileşenler doğru çalışmaktadır.

 - Sarı simge, bir ya da birden fazla bileşenin yanlış yapılandırıldığını ve söz konusu bileşenlerin özelliklerine/ayarlarına dikkat etmeniz gerektiğini gösterir. **AVG Anti-Virus** uygulamasında herhangi bir kritik sorun yoktur ve muhtemelen bir nedenden dolayı bileşenlerden bazılarını geçici olarak kapatmayı seçmiş olabilirsiniz. Hala korunuyorsunuz!. Diğer bir yandan lütfen bileşenin ayarlarını inceleyin! Adı ***Güvenlik Durumu Bilgisi*** kısmında sağlanır.

Sarı simge, bir bileşenin hata durumunu herhangi bir nedenle yok saydığınızda da görünür. ***Bileşen durumunu yoksay*** seçeneğine, **AVG Anti-Virus** ana penceresinin bileşen genel görünümü penceresindeki ilgili bileşen simgesi üzerinde bağlam menüsünden (*sağ fare tıklatmasıyla açılır*) erişilebilir. Bileşenin hata durumunun farkında olduğunuzu göstermek için bu seçeneği belirleyin, ancak belirli bir neden doğrultusunda **AVG Anti-Virus** uygulamasının u şekilde çalışmasını istiyorsanız sistem tepsisi simgesi ile uyarılmazsınız. Özel durumlar için bu seçeneği kullanmanız gerekebilir ancak en kısa zamanda ***Bileşen durumunu yoksay*** seçeneğini devre dışı bırakmanız önerilir.

Ya da, sarı simge**AVG Anti-Virus** ürününüz bilgisayar yeniden başlatması gerektirdiğinde de görüntülenir (***Yeniden başlatma gerekiyor***). Lütfen bu uyarıyı dikkate alın ve ***Şimdi yeniden başlat*** düğmesini kullanarak bilgisayarınızı yeniden başlatın.

 – Turuncu simge ***AVG Anti-Virus uygulamasının kritik durumda olduğunu belirtir***! Bir veya daha fazla bileşen düzgün çalışmıyor ve **AVG Anti-Virus** uygulaması bilgisayarınızı koruyamıyordur. Lütfen rapor edilen sorunu çözmek için gerekli ilgiyi gösterin. Hatayı kendi başınıza çözemiyorsanız AVG teknik destek ekibi ile iletişim kurun.

AVG Anti-Virus uygulamasının en verimli performansı ayarlayamaması durumunda, Onar adlı yeni bir düğme (alternatif olarak, sorun birden fazla bileşenle ilgiliyse, Tümünü onar düğmesi) görüntülenir. Program denetimini ve yapılandırmasını otomatik olarak başlatmak için bu düğmeye basın. Bu özellik, AVG Anti-Virus uygulamasını en verimli performansa ayarlamanın ve maksimum güvenlik düzeyine ulaşmanın kolay bir yoludur!

Güvenlik Durumu Bilgisi fonksiyonuna gereken özeni göstermeniz ve herhangi bir sorunun rapor edilmesi halinde anında sorunu çözmeye çalışmanız önerilmektedir. Aksi takdirde bilgisayarınız risk altında olacaktır!

Not: *AVG Anti-Virus durum bilgilerine istediğiniz zaman sistem tepsisi simgesinden de ulaşabilirsiniz.*

5.3. Hızlı Bağlantılar

Hızlı bağlantılar, **AVG Anti-Virus** kullanıcı arayüzünün sol tarafında yer alır. Bu bağlantılar tarama ve güncelleme gibi en önemli ve en sık kullanılan uygulama özelliklerine anında erişebilmenizi sağlar. Hızlı bağlantılara kullanıcı arayüzündeki tüm iletişim kutularından erişilebilir:

Hızlı bağlantılar grafik olarak üç bölüme ayrılmıştır:

- ***Şimdi tara*** - Varsayılan olarak, düğme başlatılan son taramanın bilgilerini sağlar *(tarama türü ve başlatılan son taramanın tarihi gibi)*. Aynı taramayı tekrar başlatmak için ***Şimdi tara*** komutunu tıklatın. Başka bir tarama başlatmak istiyorsanız, ***Tarama seçenekleri*** bağlantısını tıklatın. Bu şekilde taramaları çalıştırabileceğiniz, taramaların zamanını ayarlayabileceğiniz veya bunların parametrelerini düzenleyebileceğiniz AVG tarama arayüzünü açarsınız. *(Ayrıntılar için AVG Tarama bölümüne bakın)*

- ***Tarama seçenekleri*** - açık durumdaki herhangi bir AVG arayüzünden yüklü bileşenlerin tümünün görüntülendiği genel bakış penceresine gitmek için bu bağlantıyı kullanın. *(Ayrıntılar için Bileşen Genel Görünümü bölümüne bakın)*

- ***Şimdi güncelle*** – Bağlantı son başlatılan güncellemenin tarih ve saatini sağlar. Güncelleme işlemini hemen başlatmak ve ilerlemesini izlemek için bu düğmeye basın. *(Ayrıntılar için AVG Güncellemeleri bölümüne bakın)*

Hızlı bağlantılara AVG Kullanıcı Arayüzünden her zaman erişilebilir. Belirli bir işlemi (tarama veya güncelleme) başlatmak üzere hızlı bağlantılardan birini kullandığınızda, uygulama yeni bir iletişim kutusunda açılacaktır fakat söz konusu pencereden de hızlı bağlantılara ulaşabilirsiniz. Ayrıca, çalışan işlem grafik olarak gezinme paneline yansıtılır ve böylece o anda **AVG Anti-Virus** uygulamasında çalışmakta olan tüm başlatılmış işlemler üzerinde tam kontrolünüz olur.

5.4. Bileşen Genel Görünümü

Bileşen Genel Görünümü bölümleri

Bileşen Genel Görünümü bölümü **AVG Anti-Virus** kullanıcı arayüzünün orta kısmında yer alır. Bölüm iki bölüme ayrılır:

- ***Yüklü tüm bileşenlere genel bakış*** yüklü bileşenler için grafik panellerden oluşur. Her panel bileşenin simgesi ile etiketlenir ve ilgili bileşenin o anda aktif olup olmadığına dair bilgi sunar.

- ***Bileşenin açıklaması*** iletişim kutusunun alt kısmında yer alır. Açıklama bileşenin temel işleviyle ilgili kısa bir özettir. Seçilen bileşenin mevcut durumu hakkında bilgi de sağlar.

Yüklü bileşen listesi

AVG Anti-Virus içinde, ***Bileşen Genel Görünümü*** kısmı aşağıdaki bileşenler hakkında bilgiler içerir:

- ***Virüslerden Koruma*** sisteminizdeki virüs, casus yazılım, solucan, truva atı ve istenmeyen yürütülebilir dosyaları veya kitaplıkları tespit eder ve sizi kötü amaçlı reklam yazılımlarından korur - ayrıntılar >>
- ***LinkScanner*** internette arama ve gezinme sırasında sizi web tabanlı saldırılara karşı korur – ayrıntılar >>
- ***E-posta Koruması*** gelen e-posta mesajlarınızı istenmeyen e-postalara karşı denetler ve virüsleri, kimlik avı saldırılarını veya diğer tehditleri engeller – ayrıntılar >>
- ***Anti-Rootkit*** uygulamalar, sürücüler ve kitaplıklarda gizlenmiş tehlikeli kök dizinler için tarama yapar – ayrıntılar >>
- ***PC Analyzer*** analizörü, bilgisayarınızın durumu hakkında bilgi verir – ayrıntılar >>
- ***Identity Protection*** dijital varlıklarınızı yeni ve bilinmeyen tehditlere karşı korumak üzere sürekli tetiktedir – ayrıntılar >>
- ***Uzaktan Yönetim*** yalnızca yükleme süreci esnasında bu bileşenin yüklenmesini istediğinizi belirtmeniz halinde AVG Business Sürümlerinde görüntülenir

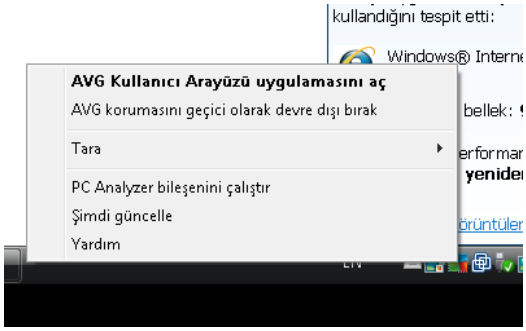
Erişilebilir eylemler

- ***Bileşen genel görünümü ekranında bileşeni seçmek için fareyi ilgili bileşen simgesi üzerinde hareket ettirin***. Aynı anda kullanıcı arayüzünün kısmında bileşenin temel fonksiyonları hakkında açıklamalar görüntülenir.
- ***Bileşenin kendi arayüzünü açmak ve temel istatistiki verileri görüntülemek için bileşen simgesini tek tıklatın***.
- ***Bağlam menüsünü birkaç seçenekle genişletmek için fareyi bileşen simgesi üstünde sağ tıklatın***:
  - ***Aç*** – Bileşenin kendi iletişim kutusunu açmak için bu seçeneği tıklatın *(bileşen simgesi üzerinde tek tıklatma gibi)*.
  - ***Bu bileşenin durumunu yoksay*** – Bileşenin hata durumunun farkında olduğunuzu ancak belirli bir nedenle bu durumu muhafaza etmek istediğinizi ve sistem tepsisi simgesi ile uyarılmak istemediğinizi göstermek için bu seçeneği seçin.

- ***Gelişmiş ayarlarda aç ...*** - Bu seçenek yalnızca, gelişmiş ayarlar olma ihtimali bulunan bazı bileşenlerle kullanılabilir.

5.5. Sistem Tepsisi Simgesi

AVG Sistem Tepsisi Simgesi *(Windows görev çubuğunuzda, ekranınızın sol alt köşesinde)* **AVG Anti-Virus** uygulamanızın mevcut durumunu gösterir. **AVG Anti-Virus** kullanıcı arayüzü ana penceresinin açık ya da kapalı olduğu önemli olmaksızın devamlı olarak sistem tepsinizde bulunur:



AVG Sistem Tepsisi Simgesi görünümü

- Tam renkli ve başka öğe bulunmayan simge tüm **AVG Anti-Virus** bileşenlerinin etkin ve tamamen çalışır durumda olduğunu gösterir. Ancak, simge bileşenlerden biri tam çalışır durumda olmasa da (kullanıcı bileşen durumunu yoksaymaya karar verdiğinde) bu şekilde görünebilir. *(Bileşenin durumunu yoksayma seçeneğini onaylayarak, bileşenin hata durumunun farkında olduğunuzu, ancak kimi nedenlerle durumun böyle kalmasını ve durum hakkında uyarı almak istemediğinizi ifade edersiniz.)*

- Üzerinde ünlem işareti bulunan simge bir bileşenin *(veya daha fazla bileşenin)* hata durumunda olduğunu gösterir. Bu tip uyarılara mutlaka dikkat edin ve düzgün ayarlanmamış bileşenin yapılandırma sorununu gidermeye çalışın. Bileşen yapılandırması değişikliklerini gerçekleştirebilmek için sistem tepsisi simgesini çift tıklatarak uygulamanın kullanıcı arayüzünü açın. Hangi bileşenin hata durumunda olduğuyla ilgili ayrıntılı bilgi için lütfen güvenlik durumu bilgisi bölümüne bakın.

- Sistem tepsisi tam renkli olarak yanıp sönen ve dönen bir ışıkla da görünebilir. Bu grafik gösterim o anda başlatılan bir güncelleme işlemini işaret eder.

- Tam renkli ve ok işaretli simge ise **AVG Anti-Virus** taramasının o anda çalışmakta olduğunu gösterir.

AVG Sistem Tepsisi Simgesi bilgileri

AVG Sistem Tepsisi Simgesi, **AVG Anti-Virus** uygulamanızdaki geçerli etkinlikler ve programdaki olası durum değişiklikleri (*örn. zamanı ayarlanmış bir tarama veya güncellemenin otomatik başlatılması, bir bileşenin durumundaki değişiklik, hata durumu oluşumları...*), sistem tepsi

sembolünde açılır bir pencere yoluyla:

AVG Sistem Tepsisi Simgesi yoluyla erişilebilen işlemler

AVG Sistem Tepsisi Simgesi, **AVG Anti-Virus** kullanıcı arayüzüne erişmek için bir hızlı bağlantı olarak da kullanılabilir; bunun için simgeyi çift tıklatmak yeterlidir. Simgeyi sağ tıklayarak aşağıdaki seçenekleri sunan kısa bir bağlam menüsü açarsınız:

- ***AVG Kullanıcı Arayüzünü Aç*** – **AVG Anti-Virus** kullanıcı arayüzünü açmak için tıklatın.
- ***AVG korumasını geçici olarak devre dışı bırak*** – Bu seçenek **AVG Anti-Virus** tarafından sağlanan tüm korumayı tek seferde kapatmanızı sağlar. Mutlaka gerekli değilse, bu seçeneği kullanmamanız gerektiğini lütfen unutmayın! Çoğu durumda, yeni yazılımı veya sürücüleri yüklemeden önce ve hatta yükleyici veya yazılım sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile **AVG Anti-Virus** uygulamasını devre dışı bırakmak gerekmez. **AVG Anti-Virus** uygulamasını geçici olarak devre dışı bırakmanız gerekirse, işinizi bitirdikten sonra yeniden etkinleştirmeniz gerekir. Virüslerden korunma yazılımınız devre dışı bırakılmışken İnternete veya bir ağa bağlanırsanız, bilgisayarınız saldırılara açık durumda olur.
- ***Taramalar*** – Önceden tanımlanan taramalar (*Tüm Bilgisayar Taraması* ve *Belirli Dosyaları veya Klasörleri Tara*) bağlam menüsünü açmak ve gerekli taramayı seçmek için tıklatın; tarama hemen başlatılacaktır.
- ***Çalışan taramalar ...*** - Bu öğe yalnızca bilgisayarınızda o anda çalışan bir tarama olması durumunda görüntülenir. Bunun ardından, bu tarama için taramanın önceliğini ayarlayabilir, alternatif olarak çalışan taramayı durdurabilir veya duraklatabilirsiniz. Ek olarak, şu işlemlere erişilebilir: *Tüm taramalar için önceliği ayarla, Tüm taramaları duraklat* veya *Tüm taramaları durdur*.
- ***PC Analyzer***'ı çalıştır – PC Analyzer bileşenini başlatmak için tıklayın.
- ***Şimdi güncelle*** – Anında güncelleme işlemini başlatır.
- ***Yardım*** – Başlangıç sayfasında yardım dosyasını açar.

5.6. AVG Advisor

AVG Advisor bilgisayarınızdaki çalışan tüm işlemleri olası sorunlara karşı sürekli izleyen ve sorunları engellemeye yönelik ipuçları öneren bir performans özelliğidir. ***AVG Advisor*** sistem tepsisi üzerinde kayan bir açılır pencere olarak görülebilir.

AVG Advisor'ın görülebileceği durumlar:

- Kullandığınız internet tarayıcısı belleği tüketmekte ve çalışmanızı yavaşlatmaktadır *(AVG Advisor yalnızca Internet Explorer, Chrome, Firefox, Opera ve Safari tarayıcılarını destekler);*
- Bilgisayarınızda çalışan bir işlem çok fazla bellek tüketmekte ve bilgisayar performansını yavaşlatmaktadır;
- Bilgisayarınız bilinmeyen bir WiFi ağına bağlanmak üzeredir.

Bu durumların her birinde, ***AVG Advisor*** gerçekleşebilecek olası sorunlar hakkında sizi uyarır ve çakışan işlem veya uygulamanın adını ve simgesini gösterir. Ayrıca, ***AVG Advisor*** olası sorunları engellemek için yapılması gerekenler hakkında önerilerde bulunur.

5.7. AVG Gadget'ı

AVG gadget'ı Windows masaüstünde görüntülenir (*Windows Kenar Çubuğu*). Bu uygulama yalnızca Windows Vista ve Windows 7 işletim sistemlerinde desteklenir. ***AVG gadget'ı*** en önemli **AVG Anti-Virus** işlevlerine, yani tarama ve güncellemeye hemen erişim sağlar:

Tarama ve güncellemeye hızlı erişim

Gerektiğinde, ***AVG gadget'ı*** hemen bir tarama veya güncelleme başlatabilmenizi sağlar:

- ***Şimdi tara*** – ***Tüm bilgisayarın taranmasını*** doğrudan başlatmak için Şimdi tara bağlantısını tıklatın. Tarama sürecinin ilerlemesini gadget'ın alternatif kullanıcı arayüzünden izleyebilirsiniz. Kısa istatistikler genel görünümü, taranan nesnelerin, tespit edilen tehditlerin ve temizlenen tehditlerin sayısı ile ilgili bilgiler verir. Tarama sırasında, tarama sürecini istediğiniz zaman duraklatabilir veya durdurabilirsiniz. Tarama sonuçlarıyla ilgili

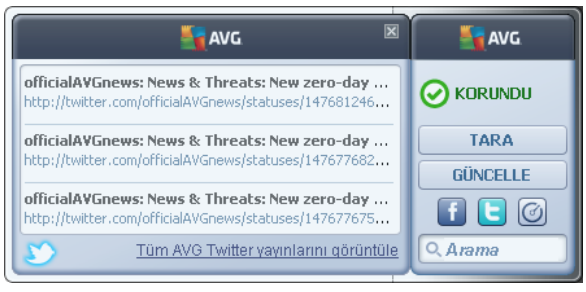
ayrıntılı veriler için lütfen standart Tarama sonuçları genel görünümü iletişim kutusuna başvurun. Bu iletişim kutusu, ***Ayrıntıları göster*** seçeneği aracılığıyla doğrudan araç üzerinden açılabilir *(ilgili tarama sonuçları Kenar çubuğu aracı taraması altında listelenir)*.

- ***Şimdi güncelle*** – Güncellemeyi doğrudan gadget içerisinden başlatmak için ***Şimdi güncelle*****AVG Anti-Virus** bağlantısını tıklatın:

Sosyal ağlara erişim

AVG gadget'ı büyük sosyal ağlara bağlanmanızı sağlayan hızlı bir bağlantı da sunar. Twitter, Facebook veya LinkedIn'deki AVG topluluklarına bağlanmak için ilgili düğmeyi kullanın:

- ***Twitter bağlantısı*** – Twitter'da gönderilen en son AVG yayınlarının genel görünümünü sunan yeni bir ***AVG gadget'ı*** arayüzü açar. İnternet tarayıcınızı yeni bir pencerede açmak için, ***AVG Twitter yayınlarının tümünü görüntüle*** bağlantısını izleyin, böylece doğrudan Twitter web sitesine, özellikle de AVG ile ilgili haberler için atanan sayfaya yönlendirilirsiniz:



- ***Facebook bağlantısı*** - İnternet tarayıcınızı Facebook web sitesinde açar, özellikle de ***AVG topluluğu*** sayfasında açar.

- ***LinkedIn***  - Bu seçenek yalnızca ağ kurulumu içerisinde kullanılabilir (*başka bir deyişle, AVG Business Editions lisanslarından biriyle AVG'yi kurduğunuz anlaşıldıktan sonra*) ve LinkedIn sosyal ağı içerisindeki ***AVG SMB Community*** web sitesinde internet tarayıcınızı açar.

Gadget ile erişilebilen diğer özellikler

- ***PC Analyzer***  - Kullanıcı arayüzünü PC Analyzer bileşeni içinde açar ve analizi hemen başlatır.
- ***Arama kutusu***- Bir anahtar kelime yazın ve varsayılan web tarayıcınızda yeni açılan bir pencerede arama sonuçlarını hemen alın.

6. AVG Bileşenleri

6.1. Virüslerden Koruma

Virüslerden Koruma bileşeni **AVG Anti-Virus** ürününüzün köşe taşlarından biridir ve bir güvenlik programının birçok temel özelliğini bir araya getirir:

- Tarama Motoru
- Yerleşik Koruma
- Casus Yazılımdan Koruma

6.1.1. Tarama Motoru

Virüslerden Koruma bileşenin temel özelliği olan tarama motoru tüm dosyaları ve dosya etkinliklerini bilinen virüslere karşı tarar *(açılan/kapatılan dosyalar, vb.)*. Tespit edilen virüsler, harekete geçmeden engellenecek ve ardından silinecek ya da Virüs Kasasında karantinaya alınacaktır.

AVG Anti-Virus korumasının en önemli özelliği bilinen hiçbir virüsün bilgisayar bulaşamamasıdır!

Tespit yöntemleri

Virüsten koruma yazılımlarının çoğu buluşsal taramayı kullanır. Diğer bir deyişle, dosyalar virüs imzası olarak adlandırılan tipik virüs özelliklerine karşı taranır. Bu, yeni bir virüs mevcut virüslerin tipik özelliklerinden bazılarına sahipse söz konusu virüsten koruma tarayıcısının yeni ve bilinmeyen bir virüsü tespit edebileceği anlamına gelmektedir. ***Virüslerden Koruma*** aşağıdaki tespit yöntemlerini kullanır:

- Tarama – belirli bir virüsün özelliklerine sahip karakter dizeleri aranır
- Buluşsal analiz – sanal bir bilgisayar ortamında taranan nesnenin komutları dinamik bir şekilde canlandırılır
- Jenerik tespit – belirli bir virüs ya da virüs grubunun komut özelliklerinin tespitidir

Tek bir teknoloji bir virüsün tespit edilmesinde ya da tanımlanmasında yetersiz kalabilecekken ***Anti-Virus*** yazılımı, bilgisayarınızın virüslerden korunmasını sağlamak için, çok sayıda teknolojiyi bir araya getirir. **AVG Anti-Virus**, bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kitaplıklarını da inceleyebilmekte ve tespit edebilmektedir. Söz konusu tehlikeleri Potansiyel Olarak İstenmeyen Programlar olarak adlandırırız*(farklı casus yazılım, reklam yazılımı türleri vb)*. Buna ek olarak, **AVG Anti-Virus** sistem kayıt defterinizi şüpheli girdilere, geçici internet dosyalarına ve izleme tanımlama bilgilerine karşı da tarar ve söz konusu potansiyel olarak istenmeyen nesneleri de diğer bulaşmalarla aynı şekilde çözebilmenize olanak tanır.

AVG Anti-Virus bilgisayarınıza kesintisiz koruma sağlar!

6.1.2. Yerleşik Koruma

AVG Anti-Virus, size yerleşik koruma adı altında sürekli koruma sağlar. ***Virüslerden Koruma*** bileşeni açılan, kaydedilen ve kopyalanan her dosyayı tek tek tarar *(belirli uzantılara sahip olanları veya hiç uzantısı olmayanları)*. Bilgisayarın sistem alanlarını ve çıkarılabilir ortamları korur (*flash disk vb.*). Erişilen bir dosyada virüs tespit ederse geçerli işlemi durdurur ve virüsün kendisini etkinleştirmesine izin vermez. Normalde, yerleşik koruma "arkaplanda" çalıştığından işlemin farkına bile varmazsınız. Ancak tehditler bulunduğunda haberdar olursunuz; aynı anda, ***Virüslerden Koruma*** tehdidin etkinliği engeller ve tehdidi kaldırır.

Yerleşik koruma, başlatma sırasında bilgisayarınızın belleğine yüklenir ve bu özelliği daima açık tutmanız çok önemlidir.

6.1.3. Casus Yazılımdan Koruma

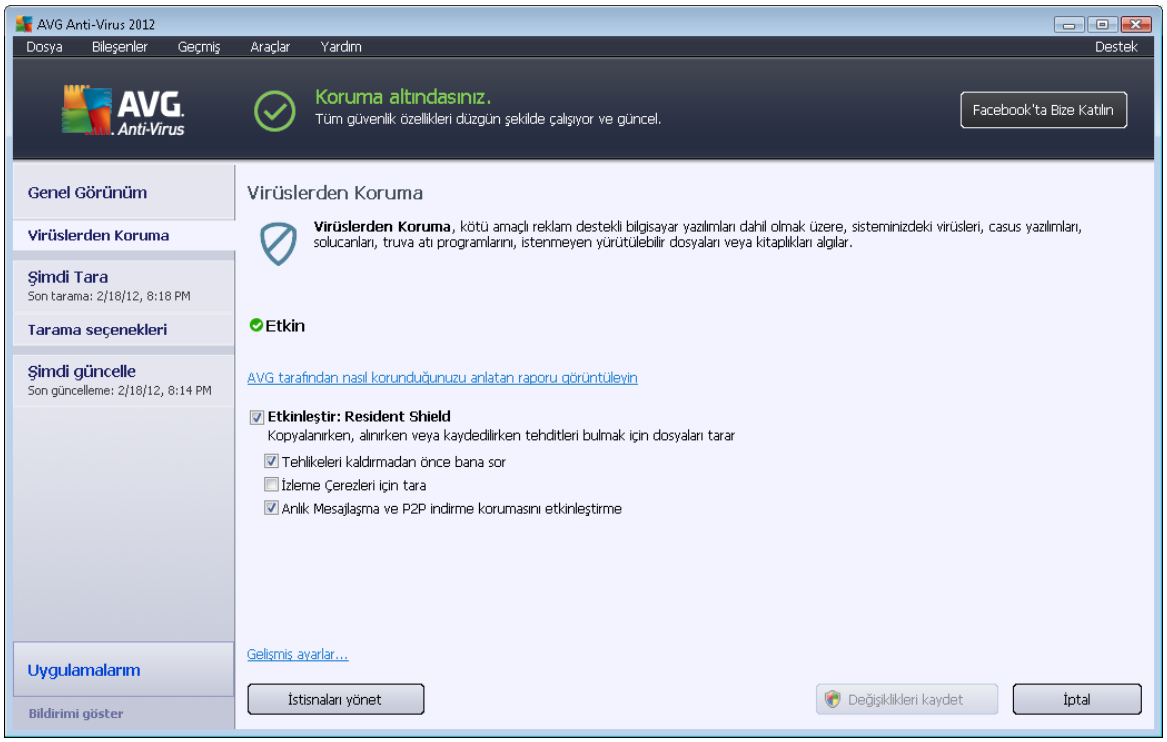
Casus Yazılımdan Koruma bilinen casus yazılım tanımlarını belirlemek için kullanılan bir casus yazılım veritabanı içerir. AVG casus yazılım uzmanları en son casus yazılım şablonlarını ortaya çıktıkları anda tanımlamak ve açıklamak için yoğun şekilde çalışır ve tanımlamaları casus yazılım veritabanına eklerler. Güncelleme işlemi yaptığınızda, bu yeni tanımlamalar bilgisayarınıza indirilir ve en son casus yazılım türlerine karşı daima güvenli şekilde koruma altında olmanız sağlanır. ***Casus Yazılımdan Koruma*** bilgisayarınızı kötü amaçlı yazılım/casus yazılımlara karşı tamamen taramanıza olanak sağlar. Ayrıca, uykuda olan ve etkin olmayan kötü amaçlı yazılımları da (yani, bilgisayara indirilmiş ancak henüz etkinleştirilmemiş olanları) tespit eder.

Casus yazılım nedir?

Casus yazılımlar, genellikle kullanıcının bilgisi ya da izni olmaksızın kullanıcının bilgisayarından bilgi toplayan kötü amaçlı bir yazılım türü olarak tanımlanırlar. Bazı casus yazılım uygulamaları genellikle belirli bir amaç doğrultusunda kurulur ve sıklıkla reklam, açılan pencereler veya farklı istenmeyen yazılım türleri içerirler. Şu anda bilinen en yaygın bulaşma kaynağı, potansiyel anlamda tehlikeli öğeler içeren web siteleridir. E-posta ya da solucan ve virüsler yoluyla aktarım gibi diğer bulaşma yöntemleri de oldukça etkilidir. En önemli korunma, yerleşik bir kalkan olarak çalışan ve siz çalıştırdığınız zaman arka planda uygulamaları tarayan ***Anti-Spyware*** gibi devamlı olarak arka planda çalışan bir tarayıcı kullanmaktır.

6.1.4. Virüslerden Koruma Arayüzü

Virüslerden Koruma bileşeni arayüzü bileşenin işlevselliği, bileşenin mevcut durum bilgisi *(Etkin)* ve bileşenin temel yapılandırma seçenekleri hakkında kısa bilgiler sağlar:



Yapılandırma seçenekleri

İletişim kutusu ***Virüslerden Koruma*** bileşeni özelliklerinin bazı temel yapılandırma seçeneklerini sağlar. Bunların kısa açıklamaları:

- ***AVG tarafından nasıl korunduğunuzu anlatan çevrimiçi raporu görüntüleyin*** – Bağlantı sizi AVG web sitesinde (http://www.avg.com/) belirli bir sayfaya yönlendirir. Bu sayfada belirli bir zaman diliminde ve toplam olarak bilgisayarınızda gerçekleştirilen tüm **AVG Anti-Virus** etkinliklerine ayrıntılı bir istatistiksel genel bakış bulabilirsiniz.

- ***Resident Shield Etkinleştir*** – Bu seçenek yerleşik korumayı kolayca açmanıza/ kapatmanıza olanak sağlar. Resident Shield dosyalar kopyalanırken, açılırken ya da kaydedilirken söz konusu dosyaları tarar. Herhangi bir virüs ya da bir tehlike tespit edildiği zaman anında uyarılırsınız. Varsayılan olarak, bu işlev açıktır ve böyle bırakmanız önerilir! Yerleşik koruma açık durumdayken tespit edilen bulaşmalar hususunda gerçekleştirilecek eylemi belirleyebilirsiniz:

  - ***Tehlikeleri kaldırmadan önce bana sor*** – Tespit edilen herhangi bir tehlikenin Virüs Kasası'na taşınmadan önce size sorulmasını istediğinizi onaylamak için seçeneği işaretli tutun. Bu seçimin güvenlik seviyesi üzerinde herhangi bir etkisi yoktur ve sadece tercihlerinizi yansıtır.

- ***İzleme Çerezleri için tara*** – Önceki seçeneklerde bağımsız olarak, izleme çerezlerini taramak isteyip istemediğinize karar verebilirsiniz. *(Çerezler bir sunucu tarafından web tarayıcısına ve oradan da siteye her ulaşıldığında değiştirilmeksizin tarayıcı tarafından geri gönderilen metin parçalarıdır. HTTP çerezleri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.)*Belirli durumlarda maksimum güvenlik seviyesine ulaşmak için bu seçeneği kullanabilirsiniz fakat varsayılan olarak kapalıdır.

- ***Anlık Mesajlaşma ve P2P indirme korumasını etkinleştir*** - anlık mesajlaşma iletişiminin (*örn. ICQ, MSN Messenger, ...*) virüs içermediğini doğrulamasını istiyorsanız bu öğeyi işaretleyin.

- ***Gelişmiş ayarlar***... – **AVG Anti-Virus** Gelişmiş ayarlar konumunda ilgili iletişim kutusuna yönlendirilmek için bağlantıyı tıklatın. Bu konumda bileşenin yapılandırmasını ayrıntılı biçimde düzenleyebilirsiniz. Ancak, tüm bileşenlerin varsayılan yapılandırmasının **AVG Anti-Virus** uygulaması tarafından en üstün performans ve en yüksek güvenlik sağlayacak biçimde ayarlandığını lütfen unutmayın. Değiştirmek için gerçek bir nedeniniz yoksa, varsayılan yapılandırmayı korumanız önerilir!

Kontrol düğmeleri

İletişim kutusunda kullanabileceğiniz düğmeler:

- ***İstisnaları yönet*** – ***Resident Shield – İstisnalar*** adında yeni bir iletişim kutusu açar. İstisnalar yapılandırmasına Resident Shield taramasından Gelişmiş ayarlar / Virüslerden Koruma / Resident Shield / İstisnalar *yolu izlenerek de ulaşılabilir (ayrıntılı açıklama için lütfen ilgili bölüme bakın)*. İletişim kutusunda Resident Shield taramasının dışında tutulması gereken dosyaları ve klasörleri belirleyebilirsiniz. Bu gerekli değilse, hiçbir öğeyi hariç tutmamanızı önemle öneririz! İletişim kutusundaki kontrol düğmeleri:

  - *Yol Ekle* – Yerel disk menü ağacından teker teker seçerek taramada hariç tutulacak dizini *(veya dizinleri)* belirleyin.

  - *Dosya Ekle* – Yerel disk menü ağacından teker teker seçerek taramada hariç tutulacak dosyaları belirleyin.

  - *Öğeyi Düzenle* – Seçilen dosyaya giden yolu düzenlemenize olanak verir.

  - *Öğeyi Kaldır* – Listeden seçili öğeye götüren yolu silmenize olanak verir.

  - *Listeyi Düzenle* – Tanımlanan istisnaların tüm listesini, standart metin düzenleyici gibi çalışan yeni bir iletişim kutusunda düzenleyebilmenizi sağlar.

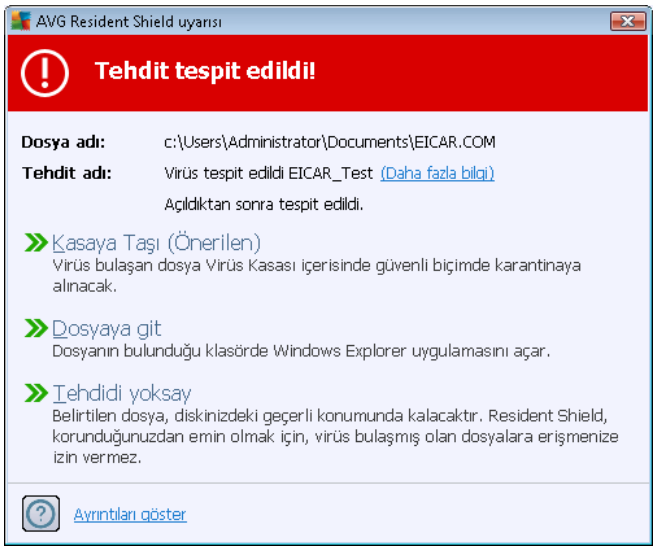
- ***Uygula*** - Bu iletişim kutusunda gerçekleştirilen tüm bileşen ayarları değişikliklerini kaydedin ve ana **AVG Anti-Viruskullanıcı arayüzüne** dönün (*bileşenlere genel bakış*).

- ***İptal*** – Bu iletişim kutusunda gerçekleştirilen tüm bileşen ayarları değişikliklerini iptal edin. Hiçbir değişiklik kaydedilmez. **AVG Anti-Virus** ana kullanıcı arayüzüne geri dönersiniz (*bileşenlere genel bakış*).

6.1.5. Resident Shield Tespitleri

Tehdit tespit edildi!

Resident Shield dosyalar kopyalanırken, açılırken ya da kaydedilirken söz konusu dosyaları tarar. Herhangi bir virüs ya da bir tehlike tespit edildiği zaman aşağıdaki iletişim kutusu ile anında uyarılırsınız:



Bu iletişim kutusunda, tespit edilmiş ve bulaşmış olarak atanan dosya ile ilgili bilgiler (*Dosya adı*), tanınan bulaşmanın adı (*Tehdit adı*) ve bilinen bir tehditse, tespit edilen bulaşma hakkında ayrıntılı bilgiler bulabileceğiniz Virüs ansiklopedisi sayfasına yönlendiren bir bağlantı bulabilirsiniz (*Diğer bilgiler*).

Artık hangi işlemin yapılması gerektiğine karar vermeniz gerekir. Birçok alternatif seçenek mevcuttur. ***Belirli durumlarda (bulaşmış dosyanın türüne ve bulunduğu konuma göre) tüm seçeneklerin her zaman kullanılamayacağını lütfen unutmayın!***

- ***Temizle*** – bu düğme yalnızca tespit edilen bulaşma temizlenebilecekse görüntülenir. Ardından, bulaşma dosyadan silinir ve dosya orijinal durumuna geri getirilir. Dosyanın kendisi virüsse, bunu silmek (*yani Virüs Kasası'na taşımak) için bu işlevi kullanın.*
- ***Kasaya Taşı (Önerilir)*** – Virüs Virüs Kasası
- ***Dosyaya git*** - Bu seçenek sizi şüpheli nesnenin tam konumuna yönlendirir (*yeni Windows Gezgini penceresi açar*)
- ***Tehdidi yoksay*** – çok geçerli bir nedeninizin olmaması halinde KESİNLİKLE bu seçeneği belirlememenizi öneriyoruz!

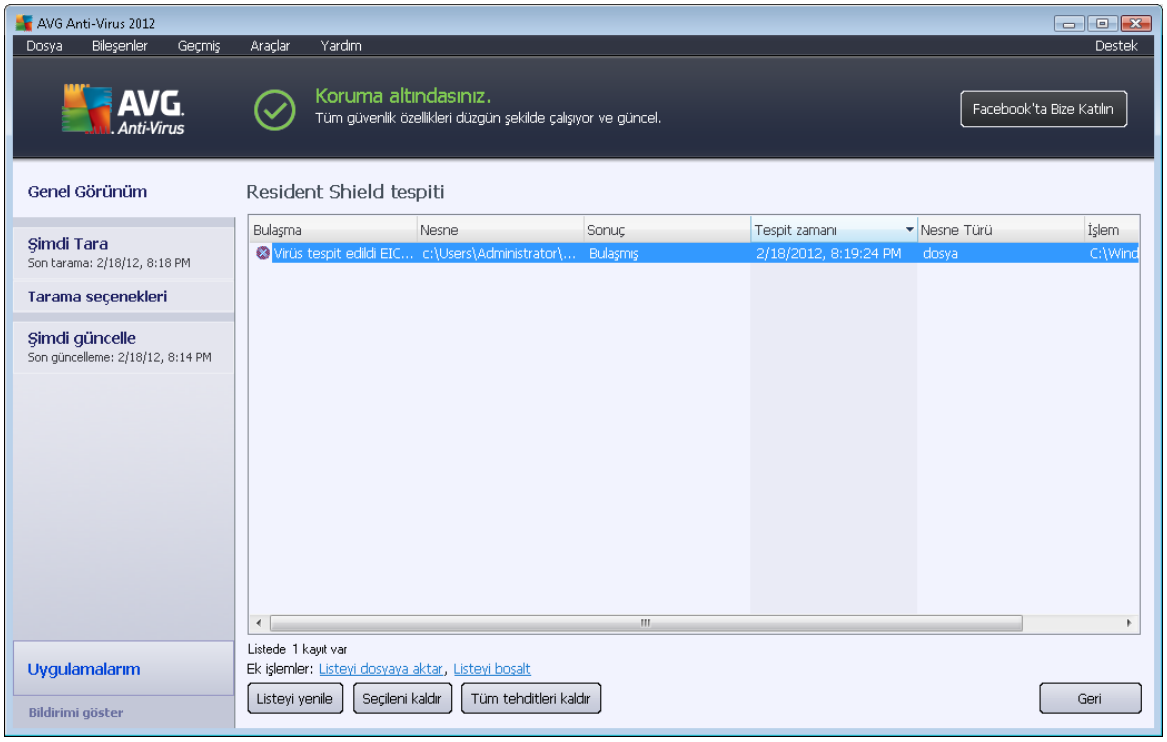
Not: *Tespit edilen objenin büyüklüğü, Virüs Kasası'ndaki boş alan sınırını aşabilir. Bu durumda, bulaşmış nesneyi Virüs Kasasına taşımaya çalıştığınızda size bu sorun hakkında bilgi veren bir uyarı iletisi görüntülenir. Ancak Virüs Kasası boyutu düzenlenebilir. Sabit diskinizin gerçek*

boyutunun uyarlanabilir yüzdesi olarak tanımlanır. Virüs Kasanızın boyutunu arttırmak için, 'Virüs Kasası boyutunu sınırlandır' seçeneği aracılığıyla AVG Gelişmiş Ayarlardaki Virüs Kasası iletişim kutusuna gidin.

İletişim kutusunun alt bölümünde ***Ayrıntıları göster*** bağlantısını bulabilirsiniz – bulaşma tespit edilirken çalışan süreç ve sürecin tanımı hakkında ayrıntılı bilgilerin olduğu açılır pencereyi açmak için bu seçeneği tıklatın.

Resident Shield tespitlerine genel bakış

Resident Shield tarafından tespit edilen tüm tehditlerin tüm genel görünümü, Geçmiş / Resident Shield tespiti sistem menüsü seçeneğinden erişilebilen ***Resident Shield tespiti*** iletişim kutusundan bulunabilir:



Resident Shield tespiti Resident Shield tarafından tespit edilip tehlikeli olduğu görülen ve temizlenen ya da Virüs Kasasına taşınan nesneler hakkında genel bilgi vermektedir. Tespit edilen tüm nesneler için aşağıdaki bilgiler verilir:

- ***Bulaşma*** – Algılanan nesnenin açıklaması (Muhtemelen adı da)
- ***Nesne*** – nesnenin konumu
- ***Sonuç*** – tespit edilen nesne ile gerçekleştirilen eylem
- ***Algılama zamanı*** – Nesnenin algılandığı tarih ve saat

- ***Nesne Türü*** – tespit edilen nesnenin türü
- ***İşlem*** – tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyaran işlem nedir

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelerin toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesneler listesini ayrı bir dosyada dışa aktarabilir (***Listeyi Dosyaya Aktar***) ve tespit edilen nesneler hakkındaki tüm girişleri silebilirsiniz (***Listeyi Temizle***). ***Listeyi Yenile*** düğmesi, ***Resident Shield*** tarafından tespit edilen buluntular listesini günceller. ***Geri*** düğmesi, sizi varsayılan AVG ana iletişim kutusuna (*bileşenlere genel bakış*) geri götürür.

6.2. LinkScanner

LinkScanner sizi web üzerinde "günden güne" artan tehditlere karşı korur. Bu tehditler idari web sitelerinden, tanınmış markaların web sitelerinden tutun, küçük işletmelerin web sitelerine kadar her tür web sitesinde gizlenmiş olabilir. ***LinkScanner*** görüntülemekte olduğunuz web sitesinde bulunan tüm bağlantıların arkasındaki web sayfalarını analiz ederek ve siz söz konusu bağlantıyı tıklamak üzereyken o anda güvenli olup olmadığından emin olarak sizi korur.

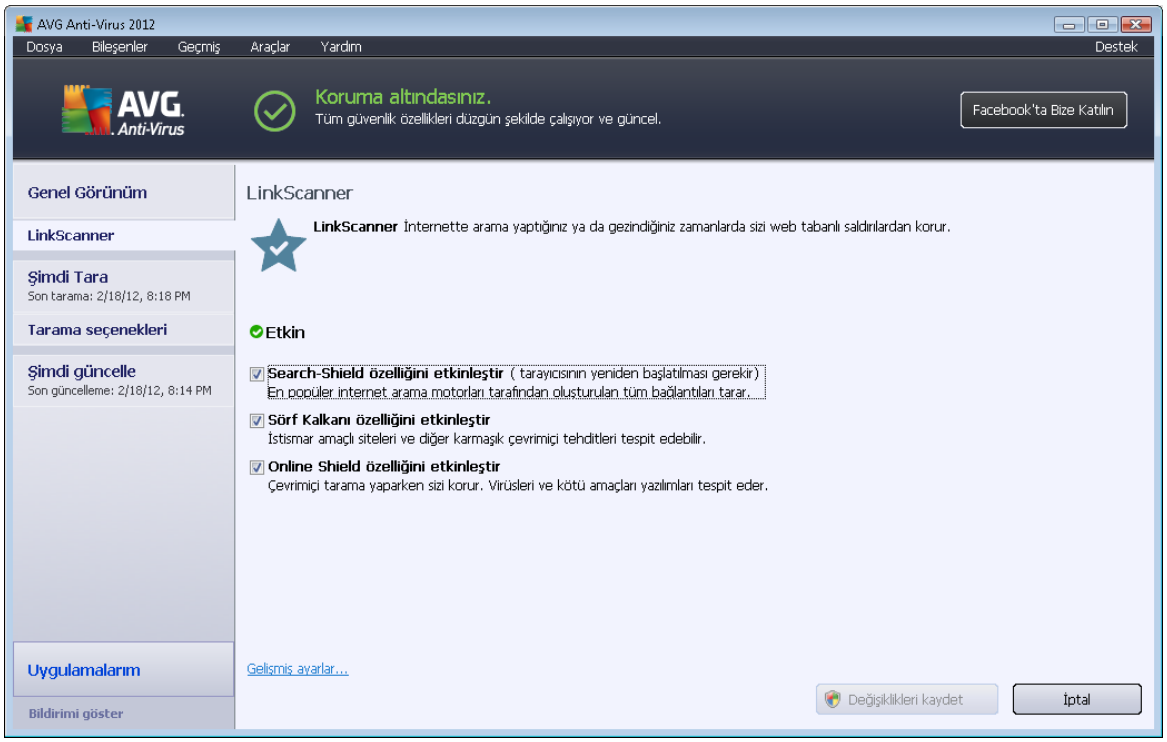
LinkScanner sunucu platformları korumasında kullanılmak için tasarlanmamıştır!

LinkScanner teknolojisi aşağıdaki temel özelliklerden oluşur:

- Search-Shield tehlikeli olduğu bilinen web sitelerinden *(URL adreslerinden)* oluşan bir liste içerir. Google, Yahoo! JP, eBay, Twitter, Digg, SlashDot, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, ve Seznam ile arama yaparken, tüm arama sonuçları bu listeye göre kontrol edilir ve bir karar simgesi gösterilir *(Yahoo! arama sonuçları için yalnızca "yararlanılan web sitesi" karar simgeleri gösterilir)*.
- Surf-Shield ziyaret etmekte olduğunuz web sitelerinin adresi önemli olmaksızın web sitelerinin içeriğini tarar. Bazı web siteleri Search-Shield *tarafından tespit edilmemiş olsa bile (örneğin, yeni ve zararlı bir web sitesi oluşturulduğunda ya da daha önce temiz olan bir web sitesine zararlı yazılım bulaştığında*) tehdit, siz siteyi ziyaret etmeden hemen önce Surf-Shield tarafından tespit edilecek ve engellenecektir.
- Online Shield internette gezinme sırasında gerçek zamanlı koruma gibi çalışır. Ziyaret ettiğiniz web sitelerinin içeriklerini ve sitelerin içindeki muhtemel dosyaları, ilgili web sitesi henüz tarayıcınızda görünmeden ya da bilgisayarınıza indirilmeden tarar. Online Shield ziyaret etmek üzere olduğunuz sayfadaki virüs ve casus yazılımları tespit eder ve indirmeyi derhal durdurur; böylece hiçbir tehdit bilgisayarınıza ulaşamaz.

6.2.1. LinkScanner Arayüzü

LinkScanner bileşeninin arayüzü, bileşenlerin işlevleri hakkında kısa açıklamalar sağlar ve işlevin geçerli durumu *(Etkin)* ile ilgili bilgiler verir:



İletişim kutusunun alt kısmında bileşenin bazı temel yapılandırma seçenekleri bulunur:

- ***Search-Shield'i*** etkinleştir – (*varsayılan olarak açık*): Yalnızca Arama Kalkanı işlevini kapatmak için iyi bir nedeniniz varsa kutunun işaretini kaldırın.
- ***Surf-Shield'i*** etkinleştir – (*varsayılan olarak açık*): Erişim sağlandığı anda güvenlik açığı olan web sitelerine karşı etkin (*gerçek zamanlı*) koruma. Bilinen kötü amaçlı site bağlantıları ve güvenlik açığından yararlanan içerikler, kullanıcı bir web tarayıcısı (*ya da HTTP kullanan diğer bir program*) aracılığıyla erişim sağladığında engellenir.
- ***Online Shield'i*** etkinleştir – (*varsayılan olarak açık*): Olası virüsler ve casus yazılımlara karşı ziyaret etmek üzere olduğunuz web sayfalarının gerçek zamanlı taranması. Bunlar tespit edilirse, indirme derhal durdurulur ve böylece hiçbir tehdit bilgisayarınıza ulaşamaz.

6.2.2. Search-Shield tespitleri

İnternet'te ***Arama Kalkanı*** açıkken arama yaptığınızda, en popüler arama motorlarından (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, ve SlashDot*) döndürülen tüm arama sonuçları tehlikeli veya şüpheli bağlantılar içerip içermedikleri konusunda değerlendirilir. LinkScanner bu bağlantıları kontrol ederek ve zararlı bağlantıları işaretleyerek sizi tehlikeli veya şüpheli bağlantıları tıklatmadan önce uyarır, böylece yalnızca güvenli web sitelerine gittiğinizden emin olursunuz.

Arama sonuçları sayfasında bağlantı değerlendirilirken bağlantının yanında bağlantı teyidi işleminin devam etmekte olduğunu gösteren bir grafik işareti görürsünüz. Değerlendirme işlemi tamamlandığında, ilgili bilgilendirme simgesi görüntülenir:

Bağlantı verilen sayfa güvenli.

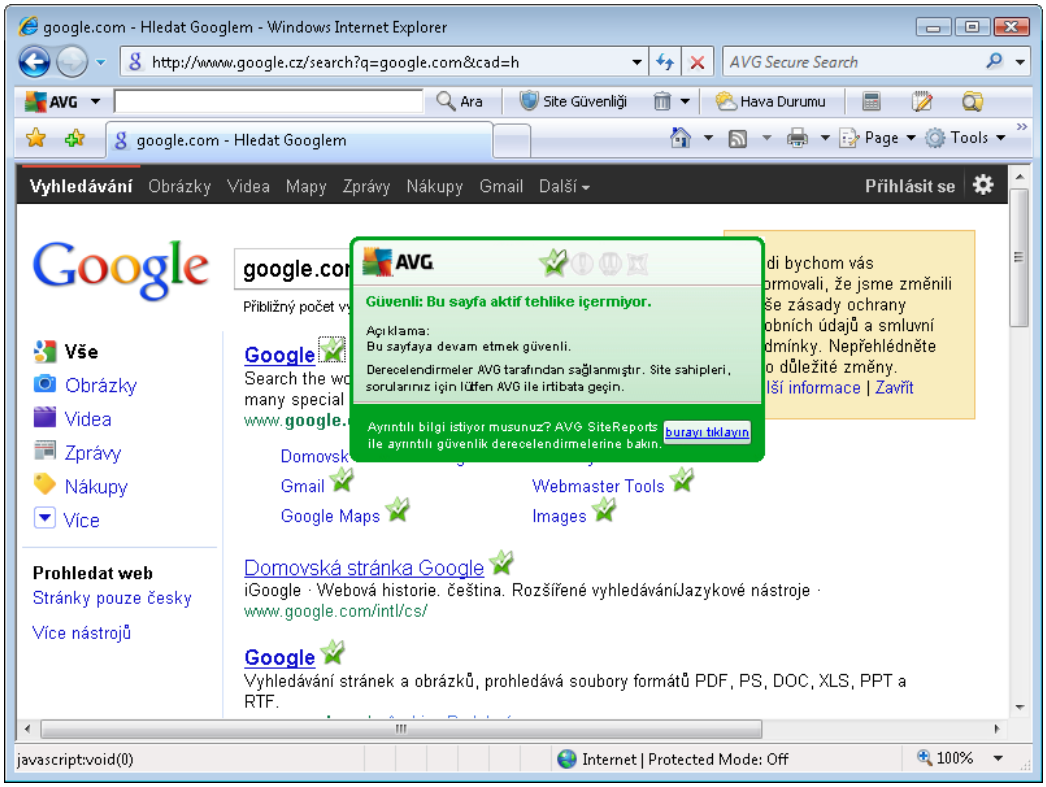
Bağlantılı sayfa tehlike içermiyor, ancak bazı şeyler şüpheli (*orijin ve davranış olarak şüpheli olduğundan e-alışveriş vb. için önerilmez*).

Bağlantılı sayfa güvenli olabilir, ancak şu anda doğrudan herhangi bir tehlike bulunmasa bile tehlikeli ya da kod olarak şüpheli olabilecek sayfalara bağlantılar içermekte.

Bağlantı verilen sayfa etkin tehlike içeriyor! Kendi güvenliğiniz için, bu sayfayı ziyaret etmenize izin verilmeyecek.

Bağlantılı sayfaya erişilemediğinden taranamadı.

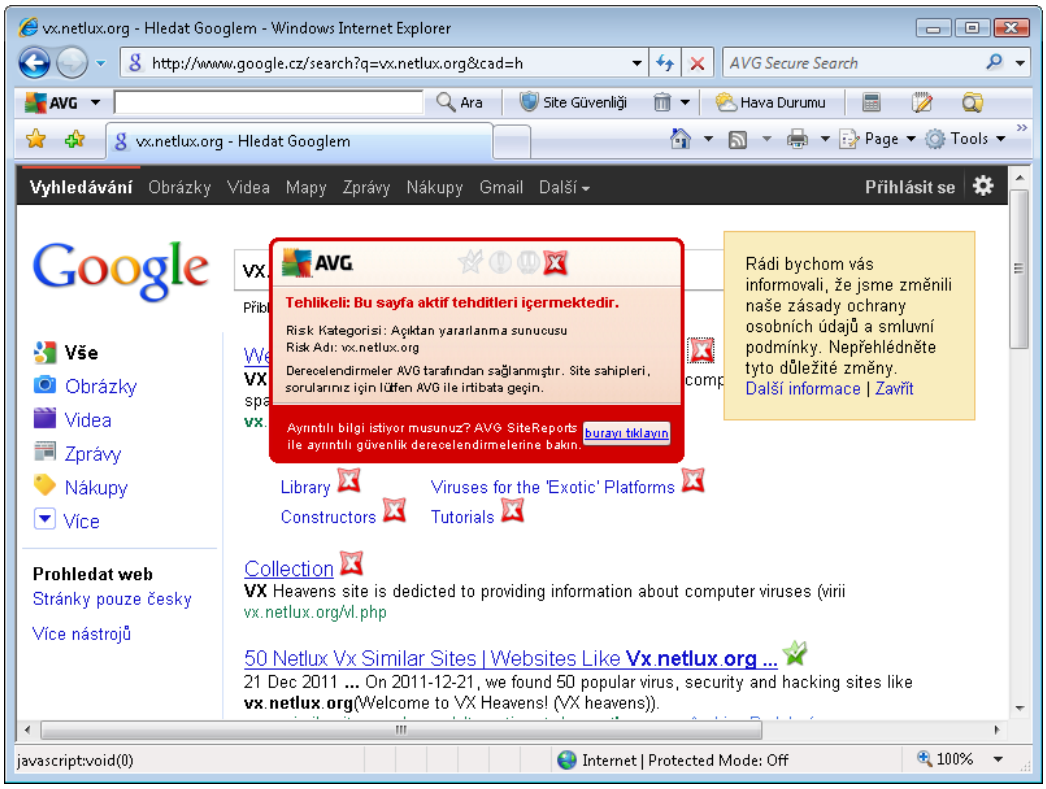
Tek tek değerlendirme simgesinin üzerine gelindiğinde, sorgulanan belirli bağlantıyla ilgili bilgiler gösterilir. Bilgiler, tehditle ilgili ek detayları (*varsa*) içerir:



6.2.3. Surf-Shield tespitleri

Bu güçlü koruma, açmaya çalıştığınız web sayfalarının kötü amaçlı içeriğini engeller ve bilgisayarınıza karşıdan yüklenmesini önler. Bu özellik etkin durumdayken, tehlikeli bir site bağlantısı tıklatıldığında ya da URL'si yazıldığında otomatik olarak web sayfasını açmanız engellenir, bu sayede etkilenmeniz önlenmiş olur. Etkilenen siteyi ziyaret ederek güvenlik açıkları olan web sayfalarının bilgisayarınızı kolaylıkla etkileyebileceğini unutmamak önemlidir, bu nedenle açıklardan yararlanma veya diğer ciddi tehlikeler içeren tehlikeli bir web sayfası isteğinde bulunduğunuzda, LinkScanner tarayıcınızın bu sayfayı göstermesine izin vermez.

Web tarayıcınızda kötü amaçlı bir web sitesiyle karşılaşırsanız, LinkScanner sizi şuna benzer bir ekranla uyaracaktır:



Bu tür bir web sitesine girmek oldukça risklidir ve önerilemez!

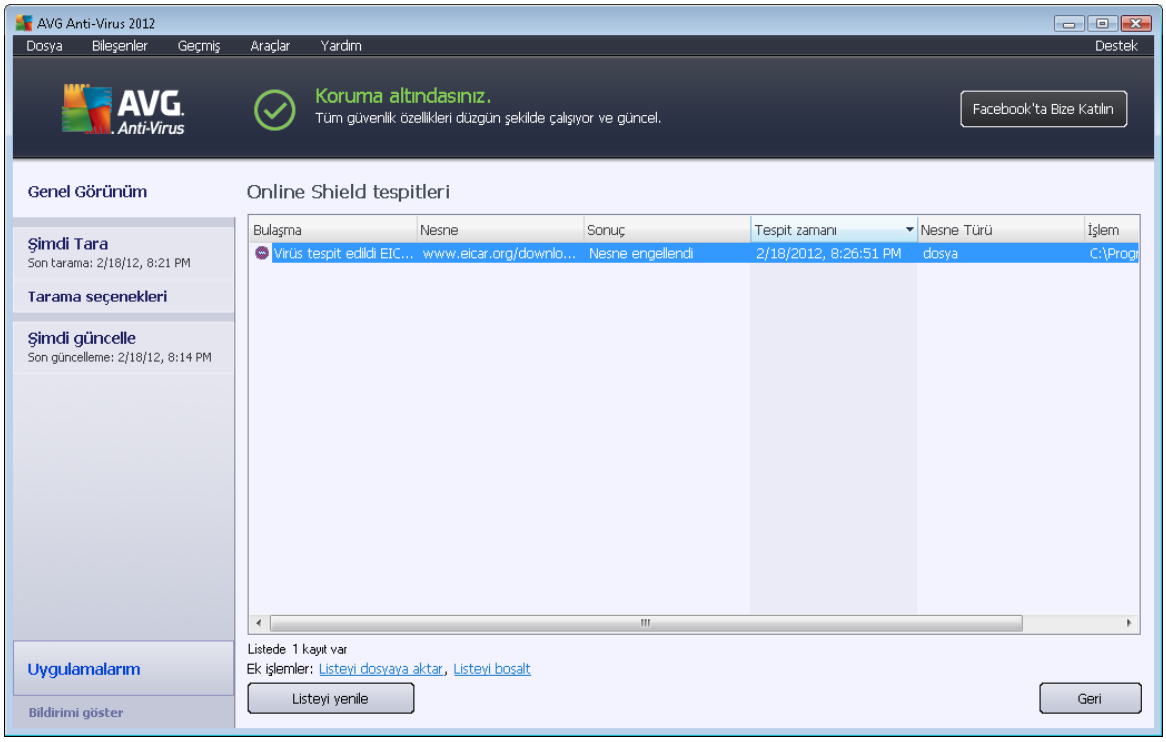
6.2.4. Online Shield tespitleri

Online Shield ziyaret ettiğiniz web sitelerinin içeriklerini ve sitelerin içindeki muhtemel dosyaları, ilgili web sitesi henüz tarayıcınızda görünmeden ya da bilgisayarınıza indirmeden tarar. Bir tehdit tespit edilirse aşağıdaki iletişim kutusu vasıtasıyla hemen uyarılırsınız:

Bu iletişim kutusundan, tespit edilen ve bulaşmış (*Dosya adı*) olarak atanan dosya verilerini, tanınan bulaşmanın adını (*Tehdit adı*) ve (biliniyorsa) tespit edilen bulaşma ile ilgili ayrıntılı bilgiler edinebileceğiniz *Virüs ansiklopedisi*'ne yönlendiren bir bağlantı bulabilirsiniz. Bu iletişim kutusunda aşağıdaki düğmeler bulunur:

- ***Ayrıntıları göster*** - bulaşma tespit edildiğinde çalışan işlem ve işlemin tanımı ile ilgili bilgileri bulabileceğiniz yeni bir açılır pencere açmak için, ***Ayrıntıları göster*** düğmesini tıklatın.
- ***Kapat*** – uyarı iletişim kutusunu kapatmak için bu düğmeyi tıklatın.

Şüpheli web sayfası açılmayacaktır ve tehlike algılama ***Online Shield bulguları*** listesi günlüğüne alınacaktır – algılanan tehlikelere bu genel bakışa sistem menüsünün Geçmiş / Web Shield Tespitleri öğesinden erişilebilir.



Tespit edilen tüm nesneler için aşağıdaki bilgiler verilir:

- ***Bulaşma*** – Algılanan nesnenin açıklaması (*Muhtemelen adı da*)

- ***Nesne*** – Nesne kaynağı (*web sayfası*)
- ***Sonuç*** – tespit edilen nesne ile gerçekleştirilen eylem
- ***Algılama zamanı*** – Tehlikenin algılandığı ve engellendiği tarih ve saat
- ***Nesne Türü*** – tespit edilen nesnenin türü
- ***İşlem*** – tespit edilmesi amacıyla potansiyel tehlike taşıyan nesneyi uyaran işlem nedir

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelerin toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesneler listesini ayrı bir dosyada dışa aktarabilir (***Listeyi Dosyaya Aktar***) ve tespit edilen nesneler hakkındaki tüm girişleri silebilirsiniz (***Listeyi Temizle***).

Kontrol düğmeleri

- ***Listeyi yenile*** – ***Online Shield***
- ***Geri*** – varsayılan AVG ana iletişim kutusuna *(bileşenlere genel bakış) geri döndürür*

6.3. E-posta Koruması

Virüsler ve truva atları yaygın olarak e-postalar aracılığıyla yayılır. Yemleme ve istenmeyen postalar, e-postaları daha büyük risk kaynakları haline getirmektedir. Ücretsiz e-posta hesaplarının zararlı e-postaları alma ihtimali daha yüksek olup (*nadiren istenmeyen posta önleme teknolojisine sahip olmaları nedeniyle*) ev kullanıcıları büyük çoğunlukla söz konusu e-postaları kullanır. Bunun yanı sıra, bilmedikleri sitelerde dolaşan ve çevrimiçi formları kişisel bilgileri ile dolduran (*e-posta adresleri gibi*) ev kullanıcıları, e-posta saldırılarına sıklıkla maruz kalmaktadır. Şirketler genellikle kurumsal e-posta hesapları kullanmakta ve riskleri en aza indirmek için istenmeyen posta önleme filtrelerinden yararlanmaktadır.

E-posta Koruması bileşeni, alınan veya gönderilen her e-posta iletisini taramakla sorumludur. Bir e-postada virüs tespit edildiğinde, hemen Virüs Kasasına kaldırır. Söz konusu bileşen belirli türde e-posta eklerine filtre uygulayabilir ve virüs bulunmayan iletilere bir onay metni ekleyebilir. ***E-posta Koruması*** iki işlevden oluşur:

- E-mail Scanner
- Anti-Spam

6.3.1. E-posta Tarayıcısı

Kişisel E-posta Tarayıcısı bileşeni gelen/giden e-postaları otomatik olarak tarar. AVG'de kendi eklentisi olmayan e-posta istemcileri ile bunu kullanabilirsiniz (*ancak, AVG'nin desteklediği e-posta istemcilerinin, başka bir deyişle Microsoft Outlook, The Bat ve Mozilla Thunderbird* istemcilerinin e-posta iletilerini tarayabilirsiniz). Öncelikli olarak, Outlook Express, Incredimail, vb. gibi e-posta uygulamaları ile kullanılması gerekir.

yüklemesi sırasında, e-posta kontrolü için oluşturulmuş otomatik sunucular bulunur: biri gelen e-

postaları kontrol etmek, ikincisi ise giden e-postaları kontrol etmek içindir. Bu iki sunucu kullanılarak e-postalar otomatik olarak 110 ve 25 bağlantı noktalarında (*e-posta göndermek/almak için standart bağlantı noktaları*) kontrol edilir.

E-Posta Tarayıcısı Internet'te e-posta istemcisi ve e-posta sunucuları arasında arayüz olarak çalışır.

- ***Gelen posta:*** Sunucudan bir ileti alırken, ***E-posta Tarayıcısı*** bileşeni bunun virüs içerip içermediğini kontrol eder, virüslü ekleri kaldırır ve sertifika ekler. Tespit edildikleri zaman virüsler anında Virüs Kasasında karantina altına alınacaktır. Ardından ileti, e-posta istemcisine aktarılır.

- ***Giden posta:*** İleti e-posta istemcisinden E-posta Tarayıcısına gönderilir; o da iletiyi ve eklerinin virüslü olup olmadığını kontrol eder ve sonra mesajı SMTP sunucuna gönderir (*giden e-postaları tarama varsayılan olarak devre dışıdır ve elle ayarlanabilir*).

E-posta Tarayıcısının sunucu platformlarında kullanılması hedeflenmemiştir!

6.3.2. Anti-Spam

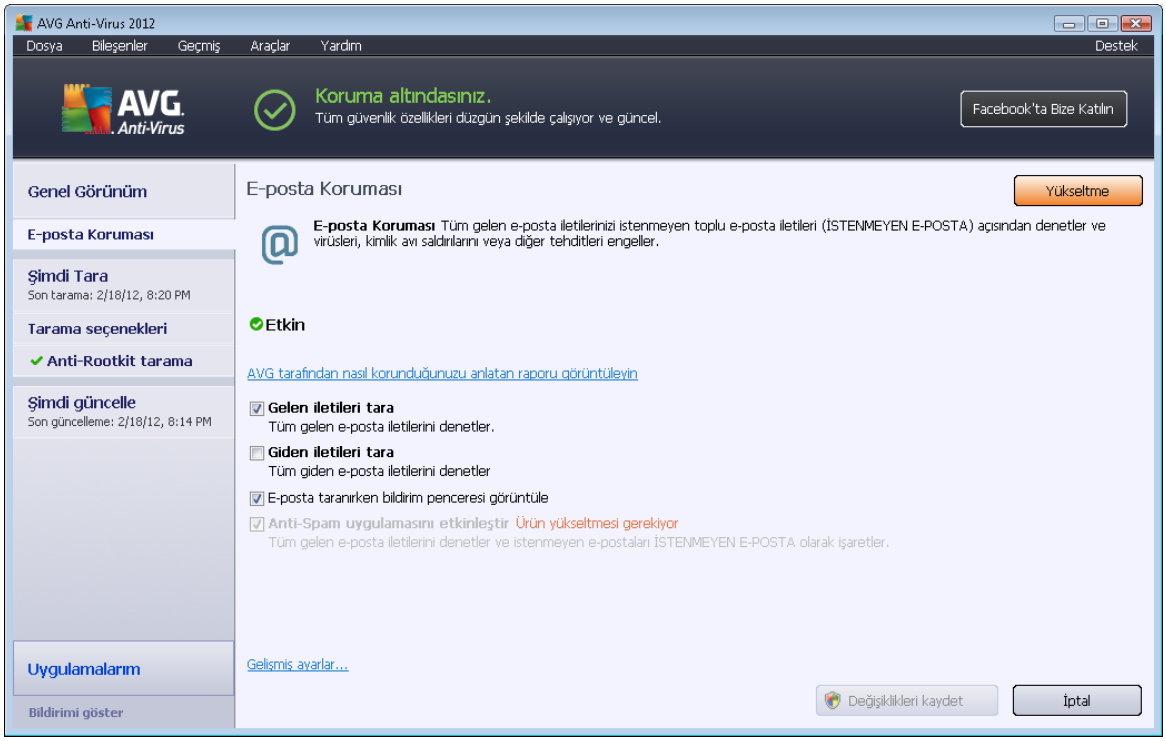
Anti-Spam nasıl çalışır?

Anti-Spam gelen tüm e-posta iletilerini denetler ve istenmeyen e-postaları istenmeyen posta olarak işaretler. ***Anti-Spam*** özel metin dizesi ekleyerek e-postanın konusunu değiştirebilir (*istenmeyen posta olarak tanımlanır*). Böylece, e-posta istemcinize göre e-postalarınızı filtreleyebilirsiniz. ***Anti-Spam*** bileşeni, her e-posta iletisini işlemek için çeşitli inceleme yöntemleri kullanır ve istenmeyen e-postaları karşı mümkün olan en üst seviyede koruma sağlar. ***Anti-Spam*** istenmeyen postayı algılamak için düzenli olarak güncellenen veritabanı kullanır. RBL sunucularını kullanmak (*"bilinen istenmeyen posta göndericisi" e-posta adreslerinden oluşan genel veritabanları*) ve Beyaz listenize (*hiçbir zaman istenmeyen posta olarak işaretleme*) ve Kara listenize (*her zaman istenmeyen posta olarak işaretle*) elle e-posta adresleri eklemek mümkündür.

Spam (istenmeyen e-posta) nedir?

Spam, ürün veya hizmet reklamı yapmak amacıyla bir seferde çok sayıda e-posta adresine toplu olarak gönderilen ve kullanıcılar'ın posta kutularını dolduran istenmeyen e-postalardır. Spam, müşterinin kendi isteğiyle almayı kabul ettiği yasal ticari e-posta anlamına gelmez. Spam kişi için sıkıcı olmanın yanında genellikle aldatma, virüs veya saldırı amaçlı içerik de olabilir.

6.3.3. E-posta Koruması Arayüzü



E-Posta Koruması iletişim kutusunda bileşenlerin fonksiyonları ve mevcut durumu hakkında bilgi bulabilirsiniz *(Etkin).* Özel bir AVG web sitesi sayfasında (http://www.avg.com/), **AVG Anti-Virus** faaliyetleri ve tespitleri hakkında ayrıntılı istatistikleri görmek ***AVG'nin sizi nasıl koruduğuna dair çevrimiçi bir rapor görüntüleyin*** bağlantısını tıklatın.

Temel E-posta Koruması ayarları

E-posta Koruması iletişim kutusunda bileşenin işlevlerinin bazı temel özellikleriyle ilgili başka düzenlemeler yapabilirsiniz:

- ***Gelen iletileri tara*** *(varsayılan olarak açık)* - Hesabınıza teslim edilen tüm e-postalarda virüs taraması yapılması için bu kutuyu işaretleyin.
- ***Giden iletileri tara*** *(varsayılan olarak kapalı)* - Hesabınızdan gönderilen tüm e-postaların virüslere karşı taranmasını onaylamak için kutuyu işaretleyin.
- ***E-posta taranırken bildirim penceresi görüntüle*** *(varsayılan olarak açık)* - E-postanızın taranması sırasında sistem tepsisinde AVG simgesi üzerinde görüntülenen bildirim iletişim kutusu aracılığıyla bilgilendirilmek istediğinizi onaylamak için bu öğeyi işaretleyin..

Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir. AVG yapılandırmasını değiştirmeniz gerekiyorsa sistem menüsü öğesi Araçlar/Gelişmiş

ayarlar'ı seçin ve yeni açılan AVG Gelişmiş Ayarlar iletişim kutusunda AVG yapılandırmasını düzenleyin.

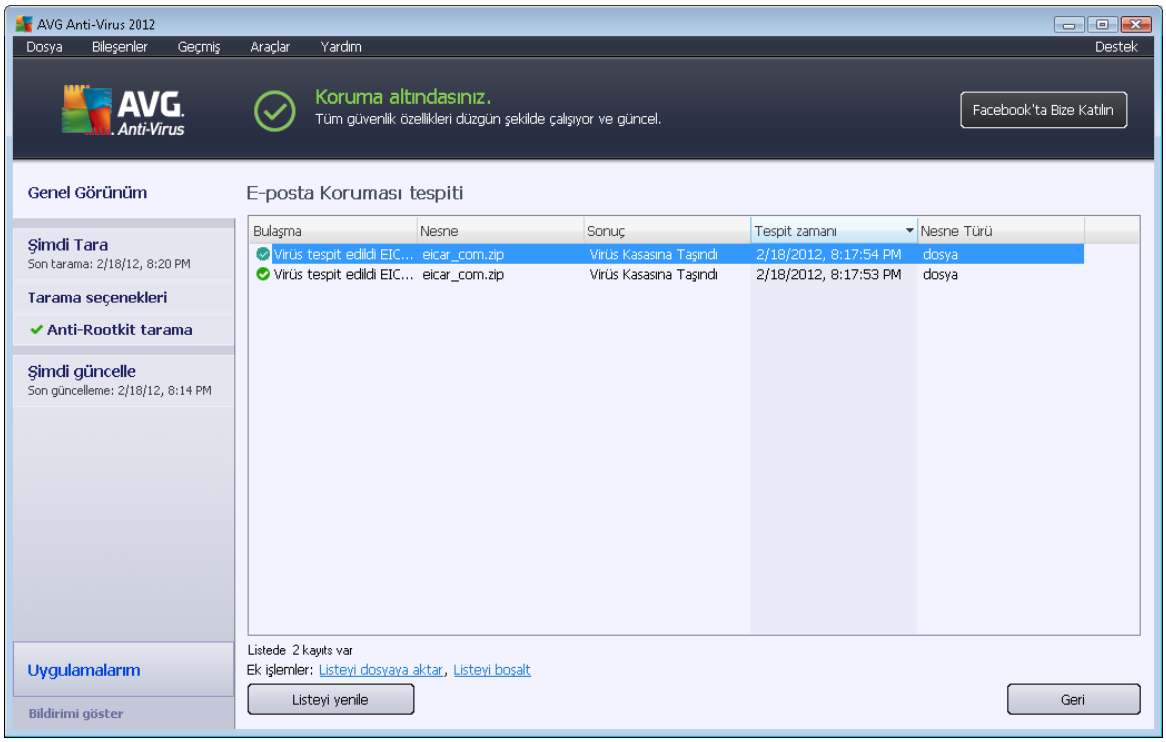
Anti-Spam'ı Etkinleştir öğesi gelen e-postalarınızda istenmeyen e-postaların filtrelenmesini etkinleştirir. Ancak, Anti-Spam hizmeti **AVG Anti-Virus** ürününde mevcut değildir ve yalnızca üst AVG sürümlerinde erişilebilirdir. ***AVG yükseltme bilgileri için lütfen AVG web sitesini (http://www.avg.com/) ziyaret edin.***

Kontrol düğmeleri

E-posta Koruması iletişim kutusunda bulunan kontrol düğmeleri şunlardır:

- ***Değişiklikleri kaydet*** bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- ***İptal*** - varsayılan AVG ana iletişim kutusuna (*bileşenlere genel bakış*) dönmek için bu düğmeye basın

6.3.4. E-Posta Tarayıcısı Tespitleri



E-mail Scanner tespiti iletişim kutusunda (*sistem menüsü seçeneği Geçmiş / E-mail Scanner tespiti üzerinden erişebilirsiniz*) E-Posta Koruması bileşeni tarafından tespit edilen tüm bulguların listesini görebilirsiniz. Tespit edilen tüm nesneler için aşağıdaki bilgiler verilir:

- ***Bulaşma*** – Algılanan nesnenin açıklaması (Muhtemelen adı da)

- ***Nesne*** – nesnenin konumu
- ***Sonuç*** – tespit edilen nesne ile gerçekleştirilen eylem
- ***Algılama zamanı*** – Şüpheli nesnenin algılandığı tarih ve saat
- ***Nesne Türü*** – tespit edilen nesnenin türü

İletişim kutusunun alt kısmında, listenin altında yukarıda listelenen tespit edilen nesnelerin toplam sayısı hakkında bilgi bulabilirsiniz. Buna ek olarak tespit edilen nesneler listesini ayrı bir dosyada dışa aktarabilir (***Listeyi Dosyaya Aktar***) ve tespit edilen nesneler hakkındaki tüm girişleri silebilirsiniz (***Listeyi Temizle***).

Kontrol düğmeleri

E-posta Tarayıcısı algılama arayüzünde bulunan kontrol düğmeleri şunlardır:

- ***Listeyi yenile*** – Algılanan tehlikelerin listesini günceller.
- ***Geri*** – Sizi önce görüntülenen iletişim kutusuna geri döndürür.

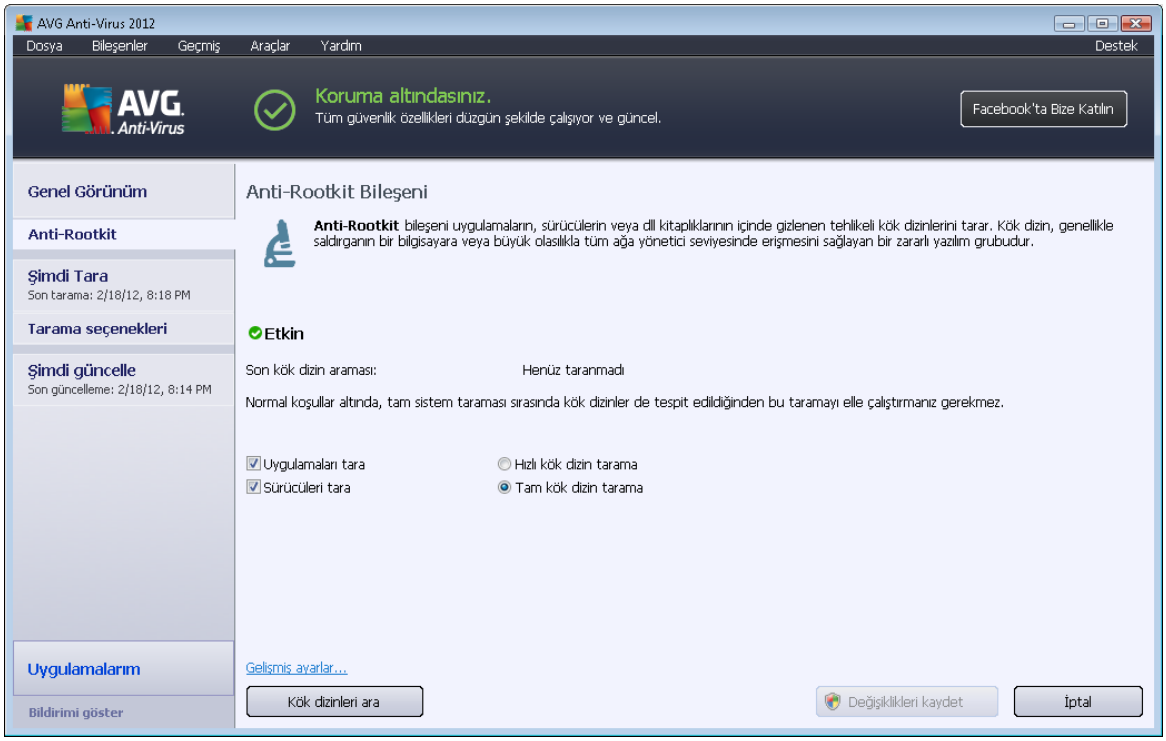
6.4. Anti-Rootkit

Anti-Rootkit tehlikeli kök dizinleri, diğer bir deyişle bilgisayarınızdaki tehlikeli yazılımları gizleyen program ve teknolojileri etkili bir biçimde tespit edip silen özel bir araçtır. ***Anti-Rootkit*** öntanımlı kurallar setine göre rootkit'leri algılayabilir. Lütfen tüm kök dizinlerin tespit edildiğini *(sadece bulaşanlar değil)* unutmayın. ***Anti-Rootkit*** bir kök dizini bulduğunda, bu kök dizinde mutlaka virüs olduğu anlamına gelmez. Bazen kök dizinleri sürücülerde kullanılır ya da doğru uygulamaların bir parçası olabilir.

Kök dizin nedir?

Kök dizin (rootkit), sistem yöneticisinin izni olmaksızın yasal olmayan şekillerde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Kök dizin, donanım üzerinde çalışan işletim sisteminin kontrolünü ele geçirmeyi hedeflediği için donanımsal açıdan erişime gerek duymaz. Kök dizinler genellikle standart işletim sisteminin güvenlik mekanizmalarını dönüştürerek ya da istila ederek sistem üzerindeki varlıklarını gizlerler. Çoğunlukla Truva Atı biçimindedirler, dolayısıyla kullanıcıları sistemleri üzerinden çalışacak kadar güvenli olduklarına inandırırlar. İzleme programlarının çalışan işlemlerini gizlemek ya da işletim sisteminin sistem bilgilerini ya da dosyalarını saklamak, bunu sağlamak için kullanılan teknikler arasında bulunmaktadır.

6.4.1. Anti-Rootkit Arayüzü



Anti-Rootkit iletişim kutusu bileşeninin arayüzü, bileşenlerin işlevleri hakkında kısa açıklamalar sağlar, bileşenin mevcut durumu konusunda bilgilendirir *(Etkin)* ve ***Anti-Rootkit*** testinin en son başlatıldığı zamanla ilgili bilgiler de verir (*Son rootkit araması; rootkit testi*Tüm Bilgisayar Taraması için varsayılan olarak çalışan bir işlemdir). ***Anti-Rootkit*** iletişim kutusu Araçlar/Gelişmiş Ayarlar bağlantısını da sağlar. ***Anti-Rootkit*** bileşeninin gelişmiş yapılandırma ortamına yönlendirilmek için bu bağlantıyı kullanın.

Yazılım satıcısı, en iyi performansın sunulabilmesi için tüm AVG bileşenlerini kurmuştur. Bunun için iyi bir nedeniniz olmadıkça AVG yapılandırmasını değiştirmeyin. Ayarlarda yapılacak her tür değişiklik sadece deneyimli bir kullanıcı tarafından gerçekleştirilmelidir.

Temel Anti-Rootkit ayarları

Kök dizin mevcudiyet taramasının bazı temel işlevlerini iletişim kutusunun en alt kısmında ayarlayabilirsiniz. Öncelikle, taranmasını istediğiniz nesneleri belirlemek üzere ilgili kutuları işaretleyin:

- ***Uygulamaları tara***
- ***Sürücüleri tara***

Bunun ardından kök dizin tarama modunu da seçebilirsiniz:

- ***Hızlı kök dizin tarama*** – Çalışan tüm işlemleri, yüklü sürücüleri ve sistem klasörlerini (

genellikle c:\Windows) tarar.

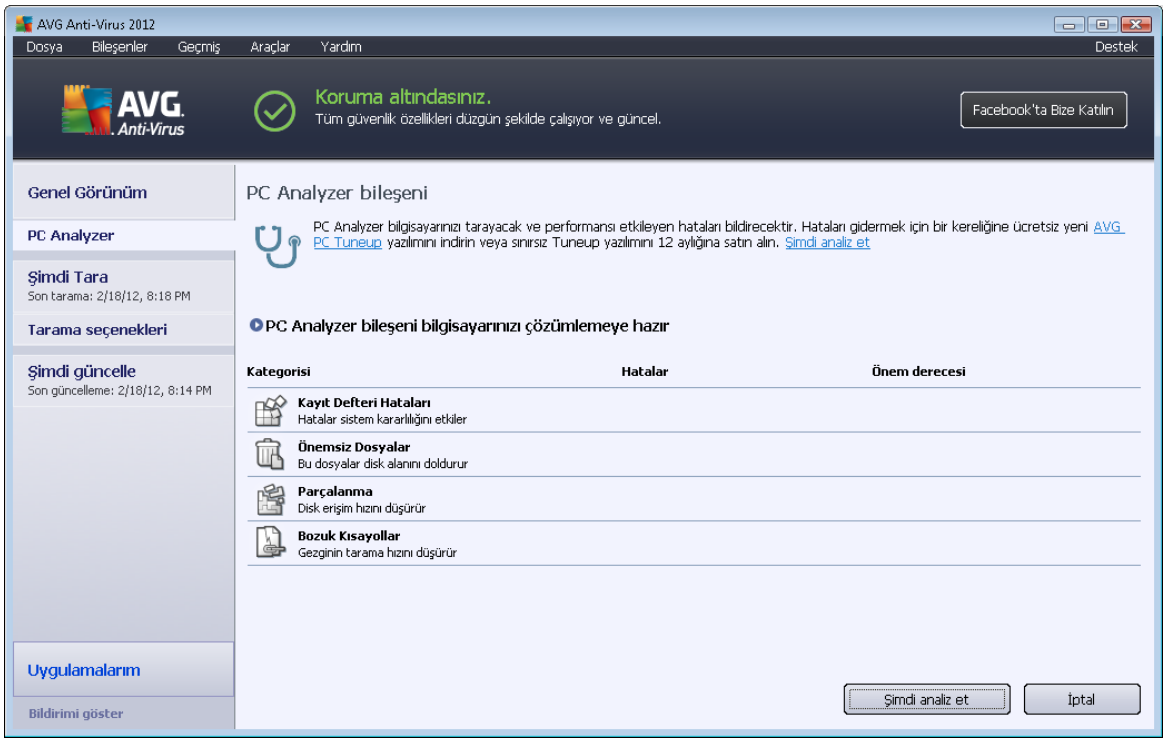
- ***Tam kök dizin tarama*** – Çalışan tüm işlemleri, yüklü sürücüleri, sistem klasörünü (*genellikle c:\Windows*), ayrıca tüm yerel diskleri (*flash disk dahil, ancak disket/CD sürücüleri hariç*) tarar.

Kontrol düğmeleri

- ***Kök dizinleri tara*** – Kök dizin tarama işlemi Tüm bilgisayarın taranması işlevinin temel bir parçası olmadığı için, kök dizin taramasını bu düğmeyi kullanarak doğrudan ***Anti-Rootkit*** arayüzünden başlatabilirsiniz.
- ***Değişiklikleri kaydet*** – Bu arayüzde yapılan tüm değişiklikleri kaydetmek ve varsayılan AVG ana iletişim kutusuna (*bileşenlere genel bakış*) dönmek için bu düğmeye basın.
- ***İptal*** – Yapılan değişiklikleri kaydetmeksizin varsayılan AVG ana iletişim kutusuna (*bileşenlere genel bakış*) dönmek için bu düğmeye basın.

6.5. PC Analyzer

PC Analyzer bileşeni bilgisayarınızı sistem sorunları açısından tarayabilir ve size bilgisayarınızın genel performansını düşürebilecek öğelerin şeffaf bir genel görünümünü verebilir. Bileşenin kullanıcı arayüzünde, ilgili kategorileri (yani kayıt defteri hatalarını, gereksiz dosyaları, bölümlendirmeyi ve bozuk kısayolları) gösteren dört satıra ayrılmış bir tablo görebilirsiniz:



- ***Kayıt Defteri Hataları***, size Windows Kayıt Defterindeki hata sayısını verir. Kayıt Defterini

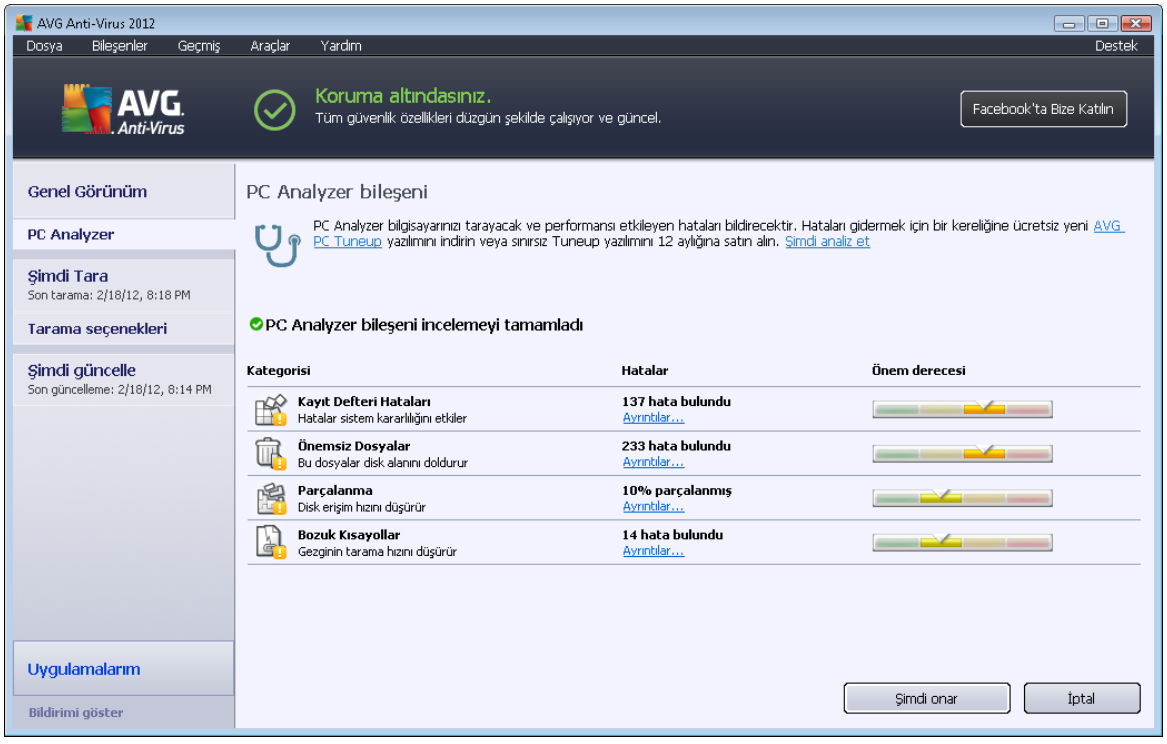
onarmak, oldukça yüksek bilgi gerektirdiğinden, kendi kendinize denemenizi veya onarmanızı önermeyiz.

- ***Gereksiz Dosyalar***, mevcut olmasa da çalışabileceğiniz dosyaların sayısını size verir. Normal olarak, bunlar çeşitli türlerde geçici dosyalar ve Geri Dönüşüm Kutusundaki dosyalar olabilir.

- ***Bölümlendirme***, bölümlendirilmiş sabit disk yüzdesini hesaplar, başka bir deyişle, dosyalar artık fiziksel diskin farklı parçalarına dağıtılmıştır. Bu sorunu gidermek için bazı bölümlendirme araçları kullanabilirsiniz.

- ***Bozuk Kısayollar***, artık çalışmayan, mevcut olmayan konumlara karşılık gelen vb. kısayolları size bildirir.

Sisteminizi analiz etmeye başlamak için, ***Şimdi analiz et*** düğmesine basın. Bundan sonra, analiz sürecini ve sonuçlarını söz konusu tabloda doğrudan izleyebilirsiniz:



Sonuçlar genel görünüm, tespit edilen sistem sorunlarının (***Hatalar***) sayısını, test edilen ilgili kategorilere göre verir. Analiz sonuçları ***Önem Düzeyi*** sütununda bir eksen üzerinde grafiksel olarak da görüntülenecektir.

Kontrol düğmeleri

- ***Şimdi analiz et*** (*analiz başlamadan önce görüntülenir*) - bilgisayarınızın analizini hemen başlatmak için bu düğmeye basın

- ***Şimdi onar*** (*analiz tamamlandıktan sonra görüntülenir*) - AVG web sitesinin (http://www.

avg.com/) sayfaya ***PC Analyzer*** bileşeni ile ilgili ayrıntılı ve güncel bilgiler vermesi için bu düğmeye basın

- ***İptal*** – analizin çalışmasını durdurmak veya analiz tamamlandıktan sonra varsayılan AVG ana iletişim kutusuna (*bileşenler genel görünümüne*) geri dönmek için bu düğmeye basın

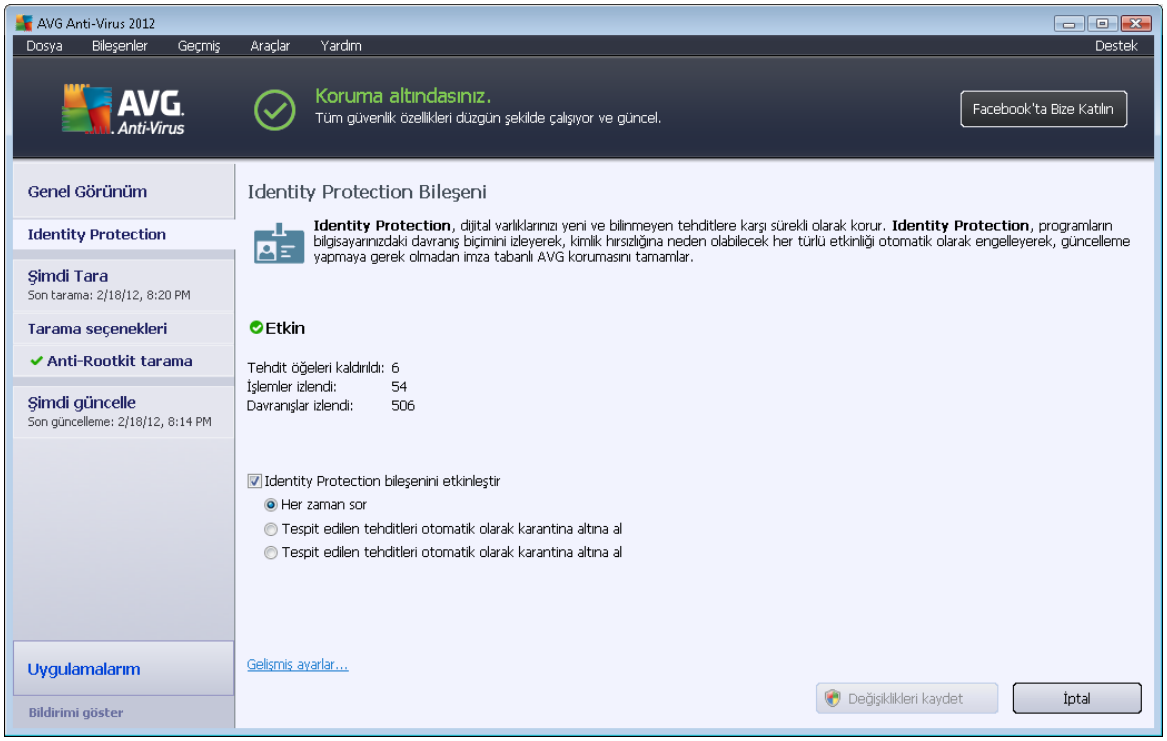
6.6. Kimlik Koruması

Kimlik Koruması kötü amaçlı yazılımlara karşı koruma bileşenidir, davranış teknolojilerini kullanarak ve yeni virüsler için ilk günden koruma sağlayarak sizi her türlü kötü amaçlı yazılımlardan (*casus yazılım, robotlar, kimlik hırsızlığı...*) korur. ***Identity Protection***, PC'nizdeki parolalarınızı, banka hesabı ayrıntılarınızı, kredi kartı numaralarınızı ve diğer kişisel dijital bilgilerinizi tüm kötü amaçlı yazılımlarla (*kötü amaçlı yazılım*) çalan kimlik hırsızlığı üzerine odaklanmıştır. Bilgisayarınızda ve paylaşılan ağınızda çalışan tüm programların düzgün biçimde çalışmasını sağlar. ***Kimlik Koruması***, sürekli olarak şüpheli davranışları belirleyip engeller ve tüm yeni kötü amaçlı yazılımlara karşı bilgisayarınızı korur.

Identity Protection, yeni ve hatta bilinmeyen tehlikelere karşı bilgisayarınıza gerçek zamanlı bir koruma sağlar. Tüm işlemleri *(gizli olanlar da dahil)* ve 285 üzerinde farklı davranış modelini izler ve sisteminizle ilgili kötü amaçlı herhangi bir durum meydana gelip gelmediğini belirleyebilir. Bu nedenle, virüs veritabanında henüz açıklanmamış tehditleri bile açığa çıkarabilir. Bilgisayarınıza bilinmeyen bir kod gelirse söz konusu kod kötü amaçlı davranışlara karşı hemen gözlenir ve izlenir. Dosyanın kötü amaçlı olduğu tespit edilirse, ***Identity Protection*** kodu Virüs Kasasına kaldırır ve sistemde yapılan tüm değişiklikleri *(kod bulaşmaları, kayıt defteri değişiklikleri, bağlantı noktası açma vb.)* geri alır. Korunmak için tarama başlatmanız gerekmez. Bu teknoloji çok öngörülüdür, nadiren güncellemeye gereksinim duyar ve her an korur.

Identity Protection, Virüslerden Koruma'ya ilave bir korumadır. Bilgisayarınız için tam koruma sağlamak üzere her iki bileşenin de bilgisayarınızda yüklenmiş olmasını önemli tavsiye ederiz!

6.6.1. Kimlik Koruması Arayüzü



Identity Protection iletişim kutusu bileşenin temel işlevi, durumu *(Etkin)* ve bazı istatistiksel veriler hakkında kısa açıklamalar sunar:

- ***Kaldırılan kötü amaçlı yazılım öğeleri*** - kötü amaçlı yazılım olarak algılanan ve kaldırılan uygulama sayısını verir
- ***İzlenen işlemler*** – Geçerli olarak çalışan IDP tarafından izlenen uygulama sayısı
- ***İzlenen davranışlar*** – İzlenen uygulamalarda çalışan belirli eylemlerin sayısı

Temel Identity Protection ayarları

İletişim kutusunun alt kısmında bileşenin işlevinin bazı temel özelliklerini düzenleyebilirsiniz:

- ***Kimlik Korumasını Etkinleştir*** - (*varsayılan olarak açıktır*): IDP bileşenini etkinleştirmek ve diğer düzenleme seçeneklerini açmak için işaretleyin.

Bazı durumlarda, ***Kimlik Koruması*** güvenilir bir dosyanın şüpheli veya tehlikeli olduğunu rapor edebilir. ***Kimlik Koruması*** tehditleri davranışlarına göre tespit edeceği için, bu genellikle bazı programlar basılan tuşları izlediğinde, diğer programları yüklediğinde veya yeni bir sürücü bilgisayara yüklendiğinde meydana gelir. Bu yüzden, şüpheli etkinlik algılandığında ***Kimlik Koruması*** bileşeninin nasıl davranacağını belirten şu seçeneklerden birini belirleyin:

  - ***Her zaman sor*** - bir uygulama kötü amaçlı yazılım olarak algılanırsa, engellenmesini

isteyip istemediğiniz sorulacaktır (*bu seçenek, varsayılan olarak açıktır ve geçerli bir nedeniniz yoksa değiştirmemeniz önerilir*)

- ***Algılanan tehlikeleri otomatik olarak karantinaya al*** - Kötü amaçlı yazılım olarak algılanan tüm uygulamalar otomatik olarak engellenecektir
- ***Bilinen tehlikeleri otomatik olarak karantinaya al*** - yalnızca kesin olarak kötü amaçlı yazılım olduğu algılananlar engellenecektir

- ***Gelişmiş ayarlar...*** – Gelişmiş ayarlar**AVG Anti-Virus** konumunda ilgili iletişim kutusuna yönlendirilmek için bağlantıyı tıklatın. Bu konumda bileşenin yapılandırmasını ayrıntılı biçimde düzenleyebilirsiniz. Ancak, tüm bileşenlerin varsayılan yapılandırmasının **AVG Anti-Virus** uygulaması tarafından en üstün performans ve en yüksek güvenlik sağlayacak biçimde ayarlandığını lütfen unutmayın. Değiştirmek için gerçek bir nedeniniz yoksa, varsayılan yapılandırmayı korumanız önerilir!

Kontrol düğmeleri

Identity Protection arayüzünde bulunan kontrol düğmeleri şunlardır:

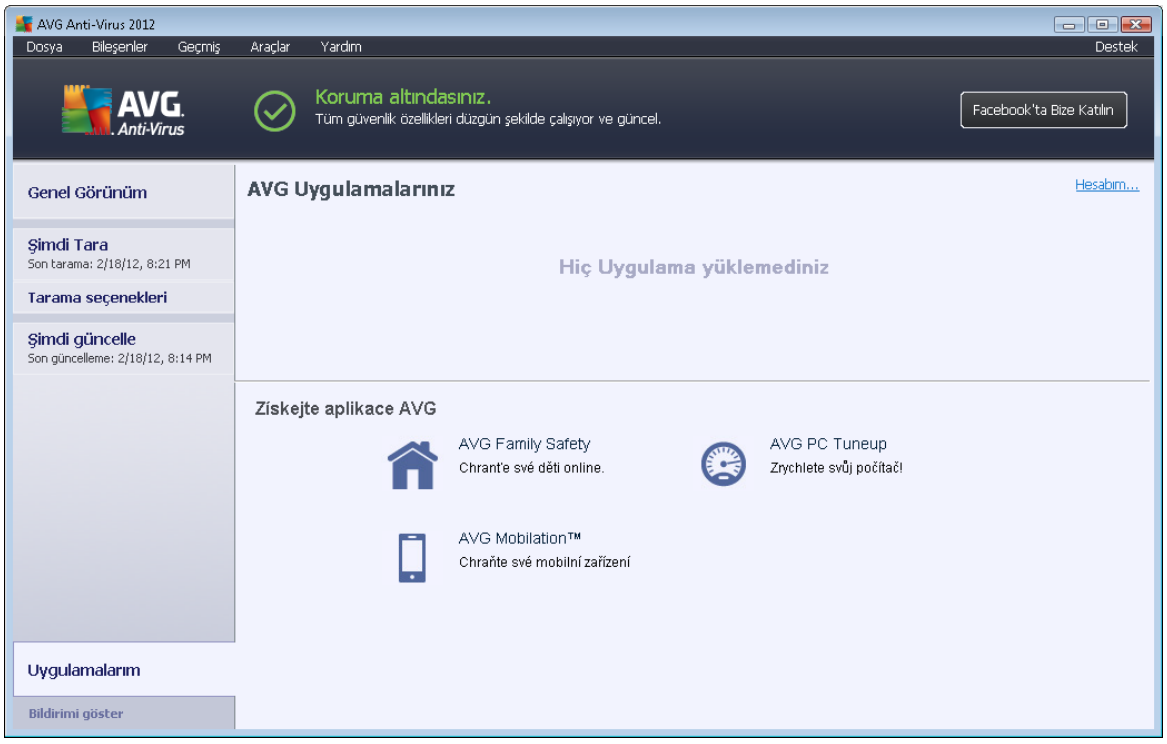
- ***Değişiklikleri kaydet*** bu iletişim kutusunda yapılan her tür değişikliği kaydetmek ve uygulamak için bu düğmeye basın
- ***İptal*** - varsayılan AVG ana iletişim kutusuna (*bileşenlere genel bakış*) dönmek için bu düğmeye basın

6.7. Uzaktan Yönetim

Uzaktan Yönetim bileşeni ancak ürününüzün Business Edition sürümünü kurmuş olmanız durumunda **AVG Anti-Virus** kullanıcı arayüzünde görüntülenir *(kurulum için kullanılan lisans hakkında bilgi için Destek sistem menü öğesinden açılabilen Bilgi iletişim kutusunun Sürüm sekmesine bakın)*. AVG Uzaktan Yönetim sistemindeki bileşen seçenekleri ve işlevselliği ile ilgili ayrıntılı bilgi edinmek için lütfen özel olarak bu başlığa ayrılmış olan ilgili dokümantasyona başvurun. Bu belge AVG web sitesi (http://www.avg.com/), ***Destek merkezi / İndir / Dokümantasyon*** bölümünden indirilebilir.

7. Uygulamalarım

Uygulamalarım iletişim kutusu *(doğrudan AVG ana iletişim kutusundaki Uygulamalarım düğmesinden erişilebilir)* isteğe bağlı olarak hem bilgisayarınızda yüklü hem de yüklemeye hazır AVG bağımsız uygulamalarına bir genel bakış sunar:



İletişim iki bölüme ayrılır:

- ***AVG Uygulamalarınız*** – bilgisayarınızda yüklü olan AVG bağımsız uygulamalarına bir genel bakış sunar;
- ***AVG Uygulamaları Alın*** – ilgilenebileceğiniz AVG bağımsız uygulamalarına bir genel bakış sunar. Bu uygulamalar yüklemeye hazırdır. Öneri lisans, konum ve diğer kriterlerinize bağlı olarak dinamik biçimde değişir. Bu uygulamalar hakkında ayrıntılı bilgi için lütfen AVG web sitesine (http://www.avg.com/) bakın.

Aşağıda kullanılabilir tüm uygulamalara kısa bir genel bakış ve uygulama işlevleri hakkında kısa açıklamalar bulabilirsiniz:

7.1. AVG Family Safety

AVG Family Safety çocuklarınızın uygunsuz web sitelerine, medya içeriklerine ve çevrimiçi aramalara karşı korunmasına yardımcı olur ve çevrimiçi faaliyetleriyle ilgili size rapor sağlar. ***AVG Family Safety çocuklarınızın sohbet odaları ve sosyal paylaşım sitelerindeki etkinliklerini izlemek için tuş vuruşu teknolojisi kullanır.*** Çocukların istismarında kullanıldığı bilinen kelimeler, ifadeler ve cümleler algılarsa, SMS veya e-posta yoluyla sizi anında bilgilendirir. Uygulama aracılığıyla çocuklarınızdan her biri için uygun koruma düzeyi ayarlayabilir ve benzersiz girişler

aracılığıyla onları ayrı ayrı gözlemleyebilirsiniz.

Daha ayrıntılı bilgi için bileşeni de indirebileceğiniz özel AVG web sayfasını ziyaret edin. Bunun için Uygulamalarım iletişim kutusundaki AVG Family Safety bağlantısını kullanabilirsiniz.

7.2. AVG LiveKive

AVG LiveKive güvenlikli sunuculara çevrimiçi veri yedeklemesi yapmak için hazırlanmıştır. ***AVG LiveKive*** tüm dosyalarınızı, fotoğraflarınızı ve müzik dosyalarınızı güvenli bir yerde yedekleyerek bunları ailenizle ve arkadaşlarınızla paylaşmanıza ve iPhone ve Android cihazları da dahil olmak üzere söz konusu dosyalara web etkinliği olan tüm cihazlardan erişmenize olanak sağlar. ***AVG LiveKive*** özellikleri:

- Bilgisayarınızın ve/veya sabit sürücünüzün bozulması durumunda alınacak güvenlik önlemi
- Verilerinize İnternete bağlı herhangi bir cihazdan erişin
- Kolay düzenleme
- Yetkilendirdiğiniz biriyle paylaşma

Daha ayrıntılı bilgi için bileşeni de indirebileceğiniz özel AVG web sayfasını ziyaret edin. Bunun için Uygulamalarım iletişim kutusundaki AVG LiveKive bağlantısını kullanabilirsiniz.

7.3. AVG Mobilation

AVG Mobilation cep telefonunuzu virüs ve kötü amaçlı yazılımlardan korur ve ayrı kalmanız durumunda akıllı telefonunuzu uzaktan izleme imkanı da sunar. ***AVG Mobilation*** özellikleri:

- *Dosya Tarayıcı* farklı saklama konumlarındaki dosyaların güvenlik taramasını sağlar;
- *Görev Sonlandırıcı* cihazın yavaşlaması veya kilitlenmesi durumunda bir uygulamayı durdurmanızı sağlar;
- *Uygulama Kilitleyici* bir veya daha fazla uygulamayı yanlış kullanıma karşı parolayla kilitlemenizi ve korumanızı sağlar;
- *Tuneup* çeşitli sistem parametrelerini *(pil ölçümü, bellek kullanımı, uygulamaların yükleme boyutu ve konumu vb.)* tek bir merkezi görünümde toplayarak sistem performansını kontrol etmenize yardımcı olur;
- *Uygulama Yedekleyici* uygulamaları SD karta yedeklemenizi ve daha sonra geri yüklemenizi sağlar;
- *Spam ve Scam* özelliği SMS mesajlarını spam olarak işaretlemenizi ve web sitelerini sahtekarlık amaçlı olarak rapor etmenizi sağlar;
- *Kişisel bilgileri temizleme* özelliğiyle telefonunuzun çalınması durumunda kişisel bilgilerinizi uzaktan siler;

- *İnternette Güvenli Gezinme* ziyaret ettiğiniz web sayfalarını anlık olarak izler.

Daha ayrıntılı bilgi için bileşeni de indirebileceğiniz özel AVG web sayfasını ziyaret edin. Bunun için Uygulamalarım iletişim kutusundaki AVG Mobilation bağlantısını kullanabilirsiniz.

7.4. AVG PC Tuneup

AVG PC Tuneup uygulaması bilgisayarınızın hızının ve genel performansının nasıl iyileştirilebileceğine yönelik ayrıntılı sistem analizi ve düzeltme işlemi için gelişmiş bir araçtır. ***AVG PC Tuneup*** özellikleri:

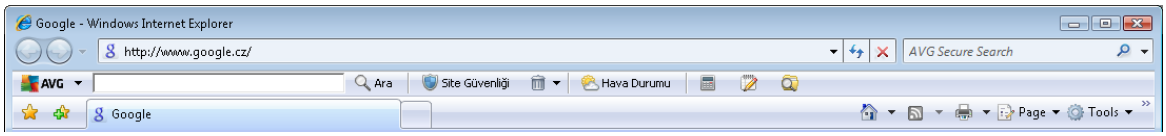
- Disk Temizleyici – Bilgisayarı yavaşlatan gereksiz dosyaları kaldırır.
- Disk Birleştirici – Disk sürücülerini birleştirir ve sistem dosyaları yerleşimini en iyi duruma getirir.
- Kayıt Defteri Temizleyici – Bilgisayarın istikrarını artırmak için kayıt defteri hatalarını onarır.
- Kayıt Defteri Birleştirici – Bellek tüketen boşlukları gidermek için kayıt defterini sıkıştırır.
- Disk Doktoru – Bozuk kesimleri, kayıp kümeleri ve dizin hatalarını tespit eder ve onarır.
- İnternet İyileştirici – "Hepsine uyan tek boyut" ayarlarını belirli bir internet bağlantısına uyarlar.
- İz Temizleyici – Bilgisayar ve internet kullanımı geçmişini temizler.
- Disk Silici – Hassas verilerin kurtarılmasını engellemek için disklerdeki boş alanları temizler.
- Dosya Öğütücü – Disk veya USB çubuğundaki seçilen dosyaları kurtarılamayacak biçimde siler.
- Dosya Kurtarma – Disk, USB çubuk ve kameralardaki yanlışlıkla silinen dosyaları kurtarır.
- Yinelenen Dosya Bulucu – Disk alanını tüketen yenilenen dosyaları bulmaya ve silmeye yardımcı olur.
- Hizmet Yöneticisi – Bilgisayarınızı yavaşlatan gereksiz hizmetleri devre dışı bırakır.
- Başlatma Yöneticisi – Kullanıcıya Windows başlatma sırasında otomatik olarak başlayan programları yönetme olanağı sağlar.
- Kaldırma Yöneticisi – İhtiyacınız olmayan yazılım programlarını tamamen kaldırır.
- Kaldırma Yöneticisi – Kullanıcıya yüzlerce gizli Windows ayarını yapma olanağı sağlar.
- Görev Yöneticisi – Çalışan tüm işlemleri, hizmetleri ve kilitli dosyaları listeler.

- Disk Sihirbazı – Bilgisayarda en çok yeri hangi dosyaların kapladığını gösterir.
- Sistem Bilgileri – Kurulu donanım ve yazılım hakkında ayrıntılı bilgiler sağlar.

Daha ayrıntılı bilgi için bileşeni de indirebileceğiniz özel AVG web sayfasını ziyaret edin. Bunun için Uygulamalarım iletişim kutusundaki AVG PC Tuneup bağlantısını kullanabilirsiniz.

8. AVG Security Toolbar

AVG Security Toolbar, LinkScanner bileşeni ile sıkı bir entegrasyon içinde çalışan bir araçtır ve internet taramaları sırasında güvenliğinizi en üst düzeyde sağlar. **AVG Anti-Virus** içinde ***AVG Security Toolbar*** kurulumu isteğe bağlıdır; kurulum işlemi sırasında bileşenin kurulup kurulmayacağına karar vermeniz istenir. ***AVG Security Toolbar*** internet tarayıcınızdan doğrudan kullanılabilir. Şu anda desteklenen internet tarayıcıları: Internet Explorer (*sürüm 6.0 üstü*), ve/veya Mozilla Firefox (*sürüm 3.0 ve üstü*). Diğer tarayıcılar desteklenmez *(Avant Browser gibi alternatif internet tarayıcıları kullanıyorsanız beklenmeyen davranışlarla karşılaşabilirsiniz)*.



AVG Security Toolbar'ın içerdiği öğeler:

- ***Açılır menülü AVG logosu***:
  - ***AVG Secure Search Kullan***- ***AVG Secure Search*** motorunu kullanarak doğrudan ***AVG Security Toolbar***'dan arama yapabilmenizi sağlar. Tüm arama sonuçları Search-Shield hizmetince denetlenir ve çevrimiçi güvenliğiniz mutlak biçimde sağlanır.
  - ***Geçerli Tehdit Düzeyi*** – Web'de geçerli tehdit seviyesinin grafik görünümünü içeren virüs laboratuarı web sayfasını açar.
  - ***AVG Tehlike Laboratuarları*** – Çeşitli web sitelerinin güvenliği ve geçerli tehlike düzeyi hakkında çevrimiçi bilgi alabileceğiniz ***AVG Tehlike Laboratuarı*** web sitesini açar *(http://www.avgthreatlabs.com)*.
  - ***Araç Çubuğu Yardımı*** - Tüm ***AVG Security Toolbar*** işlevlerini kapsayan çevrimiçi yardımı açar.
  - ***Ürün Geribildirimi Gönder***- ***AVG Security Toolbar*** hakkında görüşlerinizi bildirebileceğiniz bir form içeren bir web sayfası açar.
  - ***Hakkında...*** - Geçerli olarak kurulu ***AVG Security Toolbar*** sürümü hakkında bilgilerin yer aldığı yeni bir pencere açar.
- ***Arama alanı*** - Görüntülenen tüm arama sonuçları yüzde yüz güvenli olduğundan, kesin biçimde güvenli ve rahat olmak için internet aramalarında ***AVG Security Toolbar*** kullanın. Anahtar sözcük veya ifadeyi arama alanına girin ve ***Ara*** düğmesine *(veya Enter)* basın. Tüm arama sonuçları sürekli olarak Search-Shield hizmetince kontrol edilir *(LinkScanner bileşeni içinde)*.

- ***Site Güvenliği*** – Bu düğme ziyaret etmekte olduğunuz sayfanın mevcut güvenlik düzeyi hakkında bilgi sağlayan yeni bir iletişim kutusu açar (*Şu anda güvenli*). Bu kısa açıklama genişletilebilir ve sayfayla ilgili güvenlik aktiviteleri hakkında tüm detaylar doğrudan tarayıcı penceresinde görülebilir (*Raporun tamamını görüntüle*):

- ***Sil*** – 'Çöp kutusu' düğmesi tarama, indirme ve çevrimiçi formlarla ilgili bilgileri seçerek silmek için bir açılır menü sunar; isterseniz tüm arama geçmişinizi tek seferde de silebilirsiniz.

- ***Hava*** – Düğme, yaşadığınız yerin o gün ve sonraki iki günü kapsayan hava durumu hakkında bilgi sağlayan yeni bir iletişim kutusu açar. Bilgiler her 3-6 saatte bir düzenli olarak güncellenir. İletişim kutusunda istediğiniz konumu el ile seçebilir ve sıcaklık değerlerinin Celsius veya Fahrenheit cinsinden gösterilmesini tercih edebilirsiniz.

- ***Facebook*** – Bu düğme doğrudan AVG Security Toolbar içinden ***Facebook*** sosyal paylaşım ağına bağlanabilmenizi sağlar.

- Şu uygulamalara hızlı erişim için kısayol düğmeleri: ***Hesap Makinesi***, ***Not Defteri***, ***Windows Explorer***.

9. AVG Do Not Track

AVG Do Not Track çevrimiçi etkinlikleriniz hakkında bilgi toplayan web siteleri hakkında sizi bilgilendirir. Tarayıcınızdaki bir simge etkinlikleriniz hakkında bilgi toplayan web siteleri ve reklamcıları gösterir ve size bunlara yönelik engelleme veya izin verme seçeneği sunar.

- ***AVG Do Not Track*** her servis için gizlilik politikası hakkında ek bilgilerin yanı sıra varsa ilgili servisin dışında kalmak için doğrudan bir bağlantı da sunar.
- ***AVG Do Not Track*** sizi izlemesini istemediğiniz siteler hakkında otomatik bilgilendirme için W3C DNT protokolünü de destekler. Bu bilgilendirme otomatik olarak etkindir, ancak istenildiğinde değiştirilebilir.
- ***AVG Do Not Track*** uygulaması şu şartlar ve hükümler altında sağlanır.
- ***AVG Do Not Track varsayılan olarak etkindir, ancak istenildiğinde kolayca devre dışı bırakılabilir.*** Talimatları bulabileceğiniz SSS makalesi: AVG Do Not Track özelliğini devre dışı bırakma.
- ***AVG Do Not Track*** hakkında daha fazla bilgi için lütfen web sitemizi ziyaret edin.

Şu anda, ***AVG Do Not Track*** özelliği işlevsel olarak Mozilla Firefox, Chrome ve Internet Explorer tarayıcılarında destekleniyor. *(Internet Explorer'da AVG Do Not Track simgesi komut çubuğunun sağ tarafında yer alır. Tarayıcının varsayılan ayarlarıyla AVG Do Not Track simgesini görmekte sorun yaşıyorsanız, lütfen komut çubuğunu etkinleştirdiğinizden emin olun. Simgeyi hala göremiyorsanız, araç çubuğundaki tüm simgeleri ve düğmeleri görmek için komut çubuğunu sola sürükleyin.)*

9.1. AVG Do Not Track arayüzü

Çevrimiçiyken, ***AVG Do Not Track*** herhangi bir veri toplama faaliyeti tespit edilir edilmez sizi uyarır. Aşağıdaki iletişim kutusunu görürsünüz:

Tespit edilen tüm veri toplama servisleri ***Bu sayfadaki izleyiciler*** bilgi ekranında ada göre listelenir. ***AVG Do Not Track*** tarafından tanınan üç tür bilgi toplama etkinliği vardır:

- ***Web Analytics*** *(varsayılan olarak izin verilir):* İlgili web sitelerinin performans ve deneyimini geliştirmek için kullanılan servisler. Bu kategoride Google Analytics, Omniture veya Yahoo Analytics gibi servisleri bulabilirsiniz. Web sitesi istenildiği şekilde çalışmayabileceğinden web analytics servislerini engellememenizi öneririz.

- ***Social Buttons*** *(varsayılan olarak izin verilir):* Sosyal ağ deneyimini geliştirmek için tasarlanmış öğeler. Social buttons öğeleri ziyaret ettiğiniz siteye sosyal ağlardan sunulur. Oturumunuz açıkken çevrimiçi etkinlikleriniz hakkında bilgi toplayabilirler. Social buttons örnekleri: Facebook Social Eklentileri, Twitter Düğmesi, Google +1.

- ***Ad Networks*** *(bazıları varsayılan olarak engellenir):* İçerik tabanlı reklamlar yerine size özel reklamlar sunmak için birden fazla sitede çevrimiçi etkinlikleriniz hakkında doğrudan veya dolaylı olarak bilgi toplayan ve paylaşan servislerdir. Bu durum ilgili Ad networks öğesinin web sitesindeki gizlilik politikasına göre belirlenir. Bazı ad networks öğeleri varsayılan olarak engellenir.

Not: *Web sitesinin arka planında çalışan servislere bağlı olarak, AVG Do Not Track iletişim kutusunda yukarıda açıklanan bölümlerden bazıları yer almayabilir.*

İletişim kutusunda iki bağlantı da bulunur:

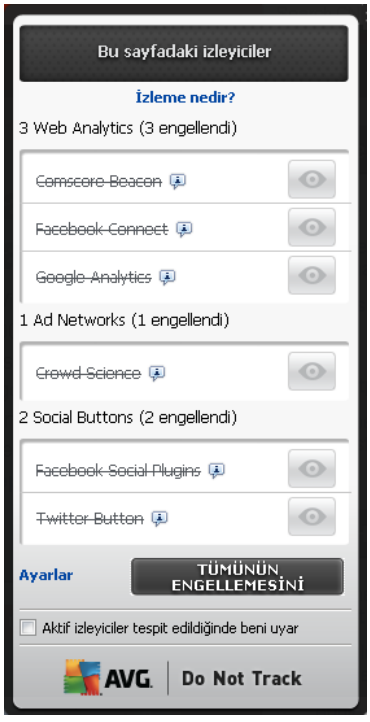
- ***İzleme nedir?*** - izleme prensipleri hakkında ayrıntılı açıklamalar ve belirli izleme türlerinin tarifini içeren bir web sayfasına yönlendirilmek için iletişim kutusunun üst bölümünde yer alan bu bağlantıyı tıklatın.

- ***Ayarlar*** - çeşitli ***AVG Do Not Track*** parametrelerinin yapılandırma ayarlarını yapabileceğiniz bir web sayfasına yönlendirilmek için iletişim kutusunun alt bölümündeki bu bağlantıyı tıklatın *(ayrıntılı bilgi için AVG Do Not Track ayarları bölümüne bakın)*

9.2. İzleme süreçleri hakkında bilgiler

Tespit edilen veri toplama servislerinin listesi yalnızca ilgili servisin adını gösterir. İlgili servise izin verme veya engelleme yönünde bilinçli bir tercih yapmak için daha fazla bilgiye ihtiyacınız vardır. Fare imlecini ilgili liste öğesinin üzerine getirin. Servis hakkında detaylı bilgileri içeren bir bilgi balonu görüntülenir. Servisin kişisel verilerinizi mi yoksa başka verileri mi topladığı, verilerin diğer üçüncü taraflarla paylaşılıp paylaşılmadığı ve toplanan verilerin ileride kullanılmak üzere saklanıp saklanmadığı gibi konular hakkında bilgi sahibi olursunuz.

Bilgi balonunun alt bölümünde, tespit edilen ilgili servisin web sitesinde gizlilik politikasına yönlendiren bir ***Gizlilik Politikası*** bağlantısı bulunur.



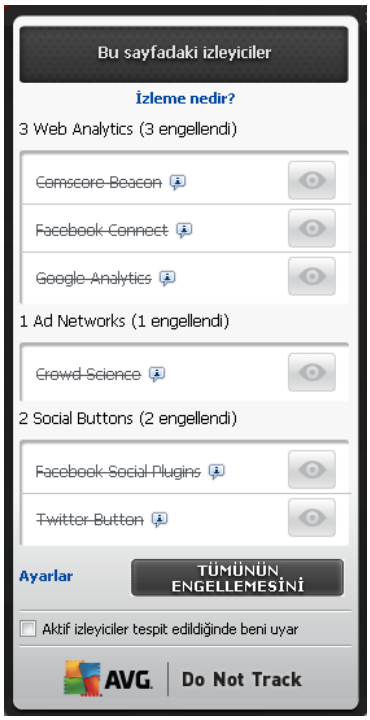
9.3. İzleyici süreçlerini engelleme

Tüm Ad Networks / Social Buttons / Web Analytics listesiyle istediğiniz servislerin engellenmesini kontrol etme seçeneğine sahip olursunuz. İki seçenekten birini tercih edebilirsiniz:

- ***Tümünü Engelle***- Hiçbir veri toplama faaliyeti istemiyorsanız iletişim kutusunun altındaki bu düğmeyi tıklatın. *(Ancak, bu işlemin servisin çalıştığı ilgili web sitesinin işlevlerini*

bozabileceğine dikkat edin!)

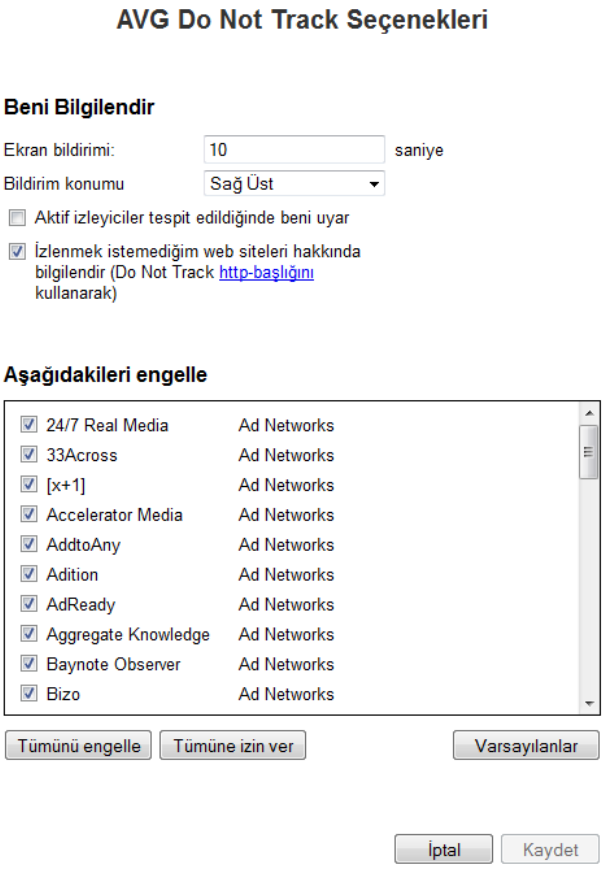
-  - Tespit edilen servislerin tamamını bir seferde engellemek istemiyorsanız, servislerin engellenmesine veya bunlara izin verilmesine tek tek karar verebilirsiniz. Tespit edilen sistemlerden bazılarının çalışmasına izin verebilirsiniz *(örn. Web Analytics):* Bu sistemler toplanan verileri kendi web sitelerinin optimizasyonu için kullanır ve böylece tüm kullanıcılar için internet ortamının geliştirilmesine yardımcı olur. Ancak, aynı zamanda Ad Networks olarak sınıflandırılan tüm veri toplama faaliyetlerini engelleyebilirsiniz. Veri toplamayı engellemek *(servis adı çarpı ile işaretlenir)* veya veri toplamaya yeniden izin vermek için ilgili servisin yanındaki  simgesini tıklatın.



9.4. AVG Do Not Track ayarları

Doğrudan ***AVG Do Not Track*** iletişim kutusunda, yalnızca bir yapılandırma seçeneği mevcuttur: Alt bölümde ***Aktif izleyiciler tespit edildiğinde beni uyar*** onay kutusunu görebilirsiniz. Varsayılan olarak, bu seçenek kapalıdır. Daha önce engellenmemiş yeni bir veri toplama servisi içeren web sitelerine girdiğiniz her seferde bilgilendirilmek istediğinizi onaylamak için onay kutusunu işaretleyin. İşaretlendiğinde, ***AVG Do Not Track*** o anda ziyaret ettiğiniz sayfada yeni bir veri toplama servisi tespit ederse, ekranınızda bildirim iletişim kutusu görünür. İşaretlenmezse, yeni tespit edilen servis hakkında yalnızca rengi yeşilden sarıya dönen***AVG Do Not Track*** simgesi *(tarayıcınızın komut çubuğunda yer alır)* ile haberdar olursunuz.

Ancak, ***AVG Do Not Track*** iletişim kutusunun alt bölümünde ***Ayarlar*** bağlantısını bulabilirsiniz. ***AVG Do Not Track Seçeneklerini*** ayrıntılı olarak düzenleyebileceğiniz web sayfasına yönlendirilmek için bağlantıyı tıklatın:



- ***Bildirim konumu*** *(varsayılan olarak Sağ Üst)* - ***AVG Do Not Track*** iletişim kutusunun monitörünüzde görüneceği konumu belirlemek için açılır menüyü açın.

- ***Ekran bildirimi:*** *(varsayılan olarak 10)* - Bu alanda ekranınızda ne kadar süreyle*(saniye cinsinden)* ***AVG Do Not Track*** bildirimini görmek istediğinizi belirlemeniz gerekir. 0 ila 60 saniye arasında bir değer belirleyebilirsiniz *(0 seçilirse bildirim ekranınızda hiç görünmez)*.

- ***Aktif izleyiciler tespit edildiğinde beni uyar*** *(varsayılan olarak kapalı)* - Daha önce engellenmemiş yeni bir veri toplama servisi içeren web sitelerine girdiğiniz her seferde bilgilendirilmek istediğinizi onaylamak için onay kutusunu işaretleyin. İşaretlendiğinde, AVG Do Not Track o anda ziyaret ettiğiniz sayfada yeni bir veri toplama servisi tespit ederse, ekranınızda bildirim iletişim kutusu görünür. İşaretlenmezse, yeni tespit edilen servis hakkında yalnızca rengi yeşilden sarıya dönen***AVG Do Not Track*** simgesi *(tarayıcınızın komut çubuğunda yer alır)* ile haberdar olursunuz.

- ***İzlenmek istemediğim web siteleri hakkında bilgilendir*** *(varsayılan olarak açık)* - Sizi izlemesini istemediğiniz bir veri toplama servisi tespit edildiğinde bu servisin ***AVG Do Not Track*** tarafından bilgilendirilmesini istediğinizi onaylamak için bu seçeneği işaretli bırakın.

- ***Aşağıdakileri engelle*** *(varsayılan olarak listelenen tüm veri toplama servislerine izin verilir)* – Bu bölümde Ad Networks olarak sınıflandırılan bilinen veri toplama servislerinin listesini

içeren bir kutu görebilirsiniz. Varsayılan olarak, ***AVG Do Not Track*** Ad Network'lerin bir kısmını otomatik olarak engeller ve geri kalanların engellenmesi veya bunlara izin verilmesi sizin seçiminize kalır. Bunun için listenin altındaki ***Tümünü Engelle*** düğmesini tıklatmanız yeterlidir.

AVG Do Not Track Seçenekleri sayfasında kontrol düğmeleri:

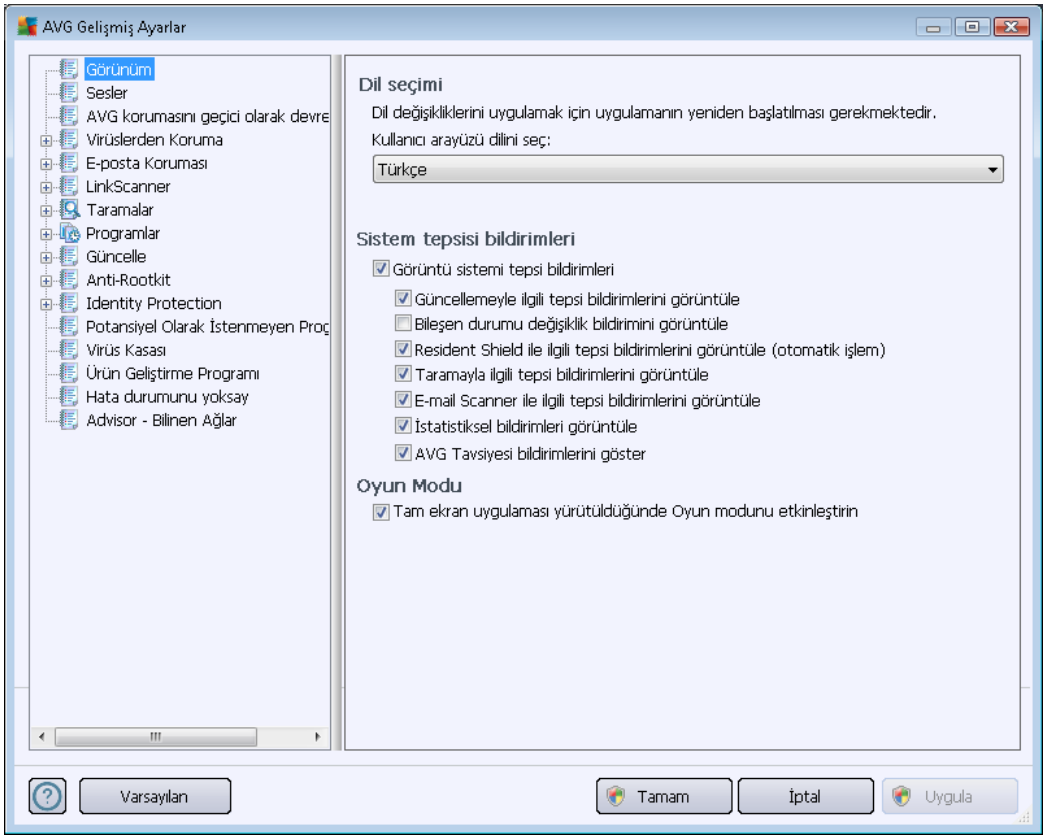
- ***Tümünü Engelle*** – Yukarıdaki kutuda Ad Networks olarak sınıflandırılan servislerin tamamını bir kerede engellemek için tıklatın;
- ***Tümüne İzin Ver*** – Yukarıdaki kutuda Ad Networks olarak sınıflandırılan ve daha önce engellenen servislerin tümüne bir seferde izin vermek için tıklatın;
- ***Varsayılanlar*** – Özelleştirilmiş tüm ayarlarınızı iptal etmek ve varsayılan yapılandırmaya dönmek için tıklatın;
- ***Kaydet*** – belirlediğiniz yapılandırmayı uygulamak ve kaydetmek için tıklatın;
- ***İptal*** – Önceden belirlediğiniz tüm ayarları iptal etmek için tıklatın.

10. AVG Gelişmiş Ayarlar

AVG Anti-Virus Gelişmiş yapılandırma iletişim kutusu ***Gelişmiş AVG Ayarları*** adlı yeni bir pencerede açılır. Pencere iki bölüme ayrılır: sol tarafta program yapılandırma seçeneklerini gösteren ağaç tipli menü bulunmaktadır. İletişim penceresini pencerenin sağ kısmında görüntülemek için (*'nin ya da belirli bir bileşeninin*) yapılandırmasını değiştirmek istediğiniz bileşeni seçin.

10.1. Görünüm

Menü ağacının ilk öğesi olan ***Görünüm***, **AVG Anti-Virus** kullanıcı arayüzünün genel ayarlarına ilişkindir ve uygulama davranışı için bazı temel seçenekleri sağlar:

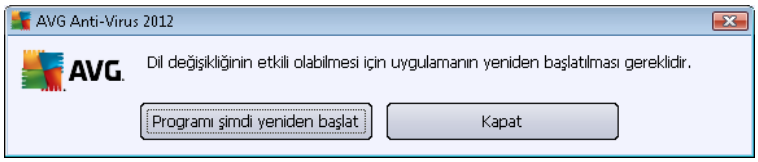


Dil seçimi

Dil seçimi bölümünde açılır menüden istediğiniz dili seçebilirsiniz. Seçilen dil **AVG Anti-Virus** kullanıcı arayüzünün tamamı için kullanılır. Aşağı açılır menü yükleme işlemi sırasında yüklenmesini istediğiniz dilleri (*bkz. Özel seçenekler*) ve İngilizceyi sunar (*İngilizce daima varsayılan olarak yüklenir*). **AVG Anti-Virus** uygulamasını başka bir dile geçirmek için yeniden başlatmanız gerekir. Lütfen şu adımları takip edin:

- Aşağı açılır menüde istediğiniz uygulama dilini seçin
- ***Uygula*** düğmesine *(iletişim kutusunun sağ alt tarafında) basarak seçiminizi onaylayın*

- Onaylamak için ***Tamam*** düğmesine basın
- Uygulamanın dilini değiştirmek için **AVG Anti-Virus**
- Programın yeniden başlatılmasını onaylamak için ***Programı şimdi yeniden başlat*** düğmesine basın ve dil değişikliğinin gerçekleşmesi için bir saniye bekleyin:



Sistem tepsisi bildirimleri

Bu bölümde **AVG Anti-Virus** uygulama durumu hakkında sistem tepsisi üzerinde beliren bildirimleri kaldırabilirsiniz. Varsayılan olarak, sistem bildirimlerinin görüntülenmesine izin verilir. Bu yapılandırmayı korumanız kesinlikle önerilir! Sistem bildirimleri örneğin tarama veya güncelleme işlemi başlatma ya da bir **AVG Anti-Virus** bileşeni durum değişikliği hakkında bilgi verir. Bu duyurulara kesinlikle dikkat etmeniz gerekir!

Ancak, belirli bir neden dolayısıyla bu yolla bilgilendirilmek istemiyorsanız ya da sadece belirli bildirimlerin görüntülenmesini istiyorsanız *(belirli AVG Anti-Virus bileşenlerine ilişkin)* tercihlerinizi aşağıdaki seçenekleri işaretleyerek ya da işaretlemeyerek tanımlayabilir ve belirleyebilirsiniz:

- ***Sistem tepsisi bildirimlerini görüntüle*** *(açık, varsayılan olarak)* - Varsayılan olarak tüm bildirimler görüntülenir. Tüm sistem bildirimleri kapatmak için bu öğenin işaretini kaldırın. Açıldığı zaman hangi bildirimlerin görüntüleneceğini seçebilirsiniz:
  - ***Güncellemeyle*** ilgili tepsi bildirimlerini görüntüle *(açık, varsayılan olarak)* - **AVG Anti-Virus** güncellemesi işleminin başlaması, ilerleyişi ve bitişi hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.
  - ***Bileşen durum değişimi hakkında bildirimleri görüntüle*** *(kapalı, varsayılan olarak)* – Bileşenleri etkin olup olmadığı ya da muhtemel sorunları hakkında bildirimlerin görüntülenmesini isteyip istemediğinize karar verin. Bir bileşenin hata durumu rapor edilirken bu fonksiyon, sistem tepsisi simgesinin herhangi bir. **AVG Anti-Virus** bileşeninde meydana gelen sorunu rapor eden kullandığı bilgilendirici fonksiyonuna eşdeğerdir.
  - ***Resident Shield ile ilgili tepsi bildirimlerini görüntüle (otomatik işlem)*** *(açık, varsayılan olarak)* – Dosya kaydetme, kopyalama ve açma işlemleriyle ilgili bilgilerin görüntülenmesine veya gizlenmesine (*bu yapılandırma yalnızca Resident Shield Otomatik temizleme seçeneği açıksa*gösterilir) karar verin.
  - ***Tarama*** ile ilgili bildirimleri görüntüle *(açık, varsayılan olarak)* - Programlı taramaların otomatik olarak başlaması, ilerleyişi ve sonuçları hakkında bilgilerin görüntülenmesini isteyip istemediğinize karar verin.
  - ***E-mail Scanner ile ilgili tepsi bildirimlerini görüntüle*** *(açık, varsayılan olarak)* –

Gelen ve giden e-posta mesajlarının taranmasına ilişkin bildirimleri görüntülemek isteyip istemediğinize karar verin.

- ***İstatistiksel uyarıları görüntüle*** *(açık, varsayılan olarak)* - Düzenli istatistiksel inceleme uyarılarının sistem tepsisinde görüntülenmesine izin vermek için bu seçeneği işaretli halde bırakın.

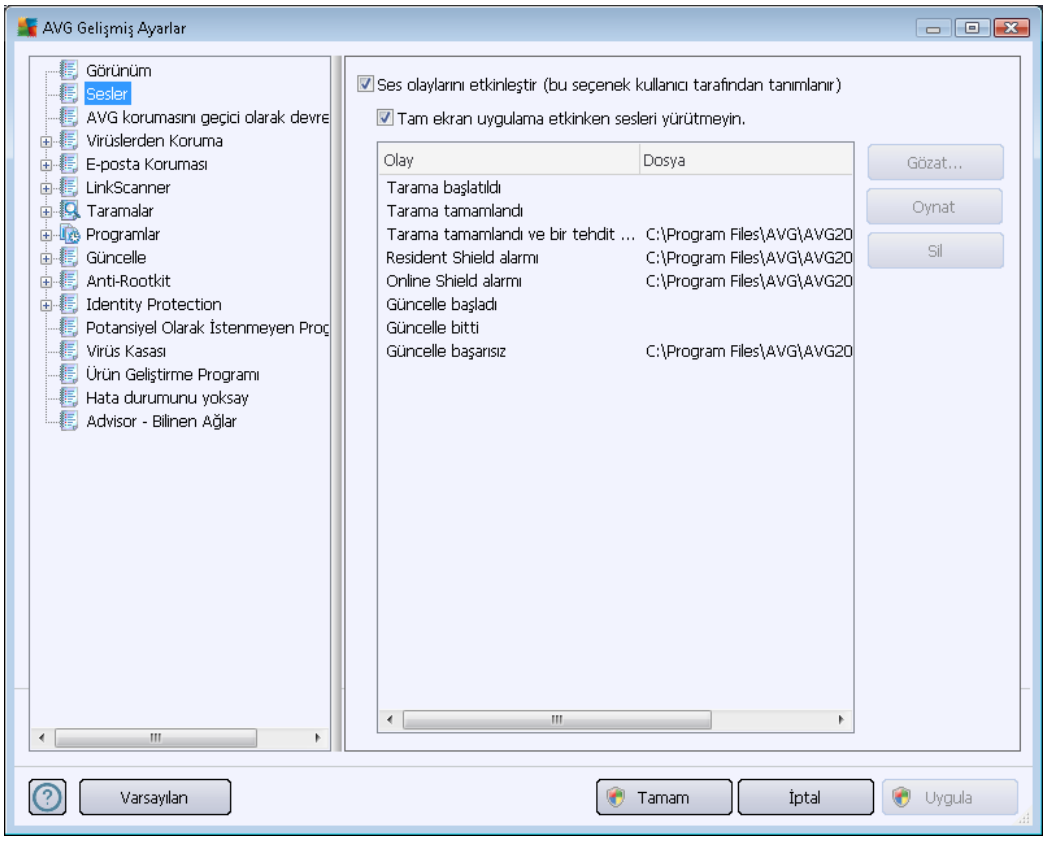
- ***AVG Advice performans bildirimlerini görüntüle*** *(açık, varsayılan olarak)* - ***AVG Advice*** desteklenen internet tarayıcılarının *(Internet Explorer, Chrome, Firefox, Opera ve Safari)* performansını izler ve tarayıcınızın önerilen bellek miktarının fazlasını kullanması durumunda sizi bilgilendirir. Böyle bir durumda bilgisayarınızın performansı ciddi bir düşüş gösterebilir; işlemleri hızlandırmak için internet tarayıcınızı yeniden başlatmanız önerilir. Bilgilenmek için ***AVG Advice performans bildirimlerini görüntüle*** öğesini açık tutun.

Oyun modu

Bu AVG işlevi, olası AVG bilgi balonlarının (*örn. programlı bir tarama başlatıldığında gösterilir*) rahatsız edici olabilen (*uygulamayı küçültebilir veya grafiklerini bozabilir*) tam ekran uygulamaları için tasarlanmıştır. Bu durumu önlemek için, ***Tam ekran uygulaması çalıştırılırken oyun modunu etkinleştir*** seçeneğini işaretli bırakın (*varsayılan ayar*).

10.2. Sesler

Sesler iletişim kutusu içinde, belirli **AVG Anti-Virus** eylemleri hakkında bir ses bildirimiyle bilgilendirilmek isteyip istemediğinizi belirleyebilirsiniz:



Bu ayarlar yalnızca mevcut kullanıcı hesabı için geçerlidir. Bu nedenle bilgisayar üzerindeki kullanıcıların her birine ait ses ayarları vardır. Sesli bildirime izin vermek istiyorsanız, ilgili tüm eylemler listesini etkinleştirmek için ***Sesli uyarıları etkinleştir*** seçeneğini işaretli bırakın (*seçenek varsayılan olarak açıktır*). Ayrıca, rahatsız edici olabilecekleri durumlarda sesli bildirimleri kapatmak için ***tam ekran uygulama etkinken sesleri yürütme*** seçeneğini işaretlemek isteyebilirsiniz *(ayrıca bu belgedeki Gelişmiş Ayarlar/Görünüm bölümünün Oyun modu kısmına bakın)*.

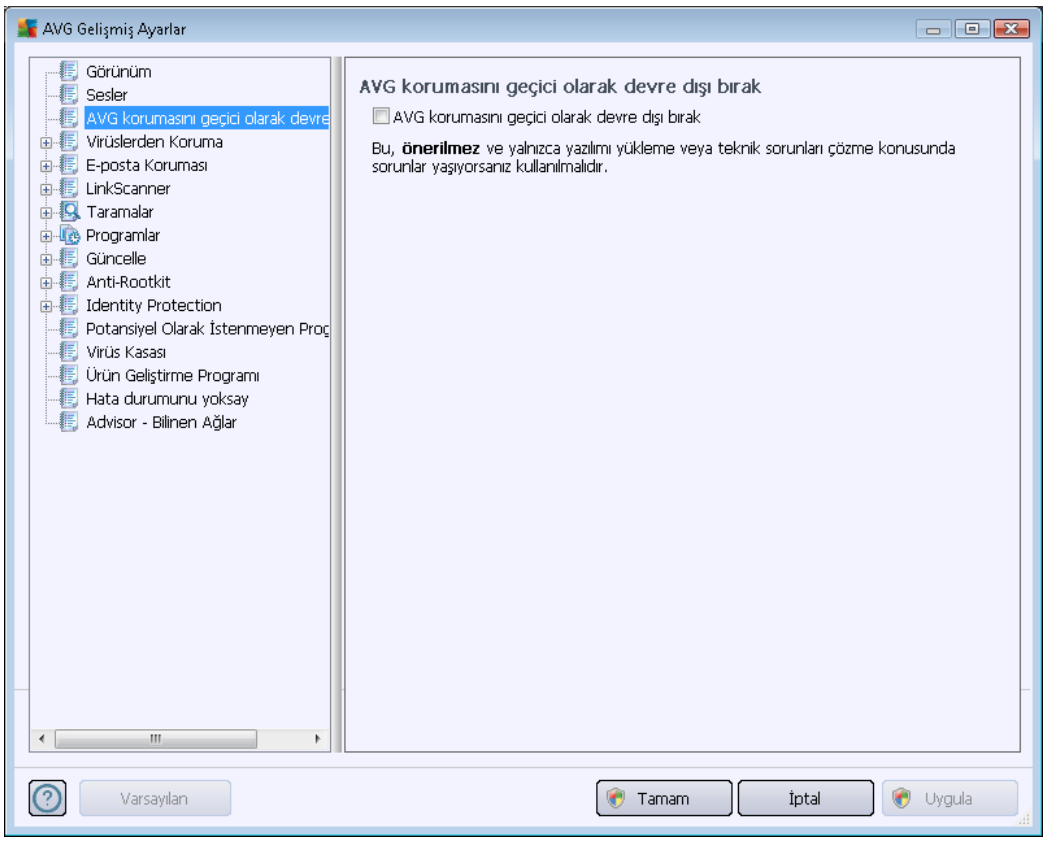
Kontrol düğmeleri

- ***Gözat*** – Diskinizde atamak istediğiniz ilgili ses dosyasını aramak için, listeden ilgili eylem seçilmiş olarak ***Gözat*** düğmesini kullanın. *(Şu anda yalnızca *.wav seslerinin desteklenmekte olduğunu lütfen unutmayın!)*
- ***Çal*** – Seçili sesi dinlemek için, listede olayı vurgulayın ve ***Çal*** düğmesine basın.
- ***Sil*** – Belirli olaya atanan sesi kaldırmak için ***Sil*** düğmesini kullanın.

10.3. AVG korumasını geçici olarak devre dışı bırak

AVG korumasını geçici olarak devre dışı bırak iletişim kutusunda, **AVG Anti-Virus** yazılımınız tarafından güvende tutulan tüm korumayı bir seferde kapatma seçeneğiniz vardır.

Mutlaka gerekli değilse, bu seçeneği kullanmamanız gerektiğini lütfen unutmayın!

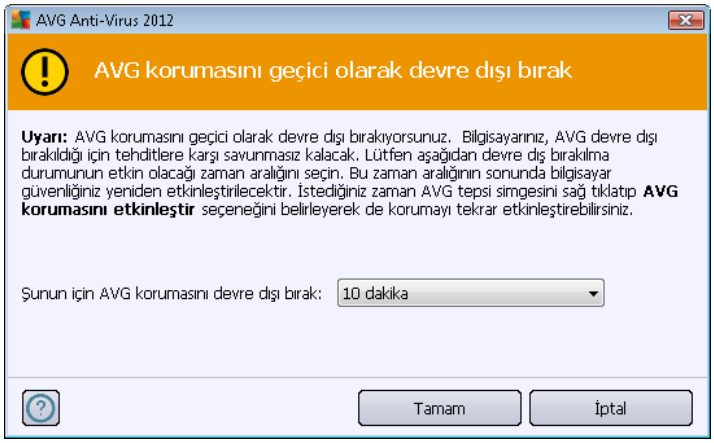


Çoğu durumda, yeni yazılımı veya sürücüleri yüklemeden önce ve hatta yükleyici veya yazılım sihirbazı yükleme işlemi sırasında istenmeyen kesintilerin olmamasını sağlamak için çalışan program ve uygulamaların kapatılmasını önerse bile **AVG Anti-Virus** uygulamasını devre dışı bırakmak ***gerekmez***. Yükleme sırasında gerçekten sorun yaşıyorsanız, öncelikle yerleşik korumayı devre dışı bırakmayı deneyin (*Resident Shield etkinleştir*). **AVG Anti-Virus** uygulamasını geçici olarak devre dışı bırakmanız gerekirse, işinizi bitirdikten sonra yeniden etkinleştirmeniz gerekir. Virüslerden korunma yazılımınız devre dışı bırakılmışken İnternete veya bir ağa bağlanırsanız, bilgisayarınız saldırılara açık durumda olur.

AVG koruması geçici olarak nasıl devre dışı bırakılır

- ***AVG korumasını geçici olarak devre dışı bırak*** onay kutusunu işaretleyin ve ***Uygula*** düğmesine basarak seçiminizi onaylayın
- Yeni açılan ***AVG korumasını geçici olarak devre dışı bırak*** iletişim kutusunda **AVG Anti-Virus** uygulamanızı ne kadar süreyle devre dışı bırakmak istediğinizi belirleyin. Koruma,

varsayılan olarak 10 dakika süreyle kapatılır. Bu süre, yeni bir yazılım yükleme gibi herhangi bir işlem için yeterli olacaktır. İlk baştaki sürenin ancak 15 dakikaya uzatılabileceğini ve güvenlik nedenlerinden ötürü bu sınırın aşılamayacağını unutmayın. Belirlenen zaman aralığından sonra devre dışı bırakılan tüm bileşenler otomatik olarak tekrar etkinleştirilir.

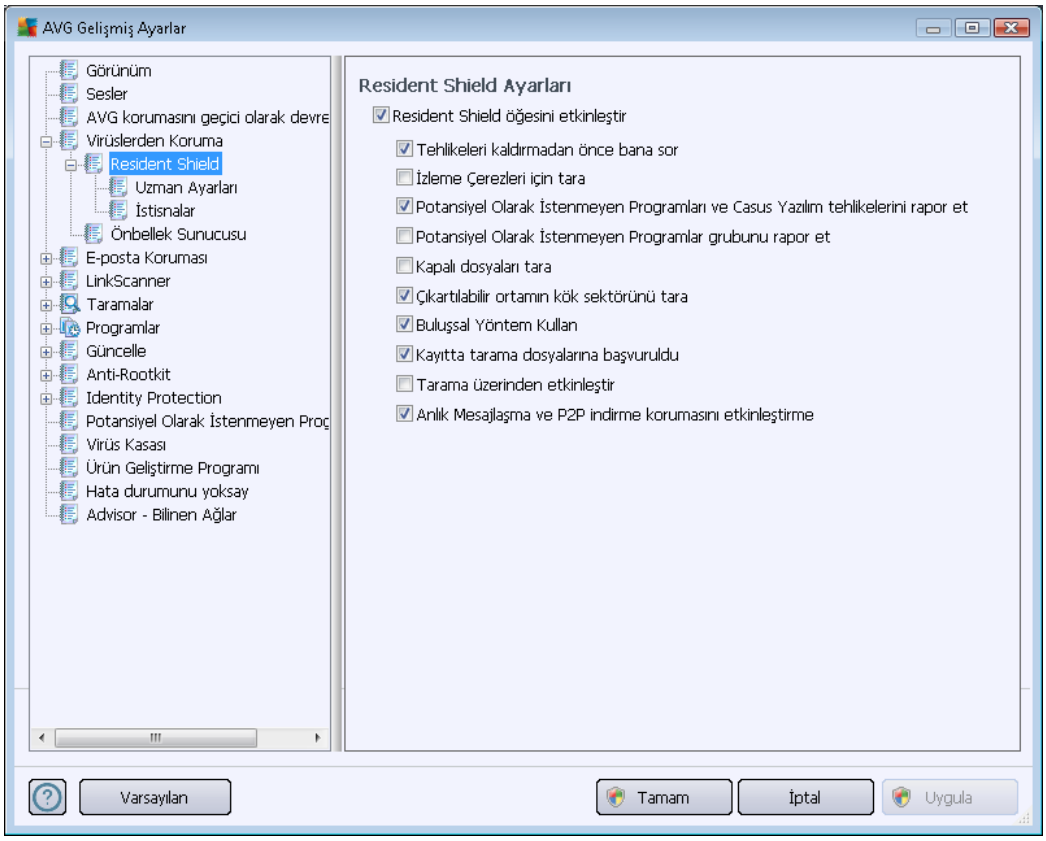


10.4. Virüslerden Koruma

Virüslerden Koruma bileşeni bilinen tüm virüs ve casus yazılım türlerine karşı bilgisayarınızı korur *(indirilen ancak henüz aktif hale geçmeyen kötü amaçlı yazılımlar gibi uyuyan ve aktif olmayan kötü amaçlı yazılım olarak adlandırılan yazılımlar da dahil)*.

10.4.1. Resident Shield

Resident Shield dosya ve klasörlerinizi çevrimiçi ortamda virüslere, casus yazılımlara ve diğer zararlı yazılımlara karşı korur.



Resident Shield Ayarları iletişim kutusunda yerleşik kalkan korumasını ***Resident Shield Etkinleştir*** öğesini işaretleyerek ya da işaretini kaldırarak etkinleştirebilir ya da devre dışı bırakabilirsiniz (*bu seçenek varsayılan olarak açıktır*). Ayrıca yerleşik kalkanın hangi özelliklerinin etkinleştirileceğini seçebilirsiniz:

- ***Tehlikeleri kaldırmadan önce bana sor*** (*varsayılan olarak açık*) – Resident Shield hiçbir işlemi otomatik olarak yapmaması; bunun yerine, tespit edilen tehlikeyi ne yapacağınıza karar vermeniz için göstermesini sağlamak için işaretleyin. Kutuyu işaretlemezseniz, **AVG Anti-Virus** bulaşmayı otomatik olarak temizler ve eğer mümkün değilse nesne Virüs Kasası 'na taşınır.

- ***Tanımlama bilgilerini izlemek için tara*** (*varsayılan olarak kapalı*) – Bu parametre, tanımlama bilgilerinin tarama işlemi sırasında tespit edilmesi gerektiğini belirtir. (*HTTP tanımlama bilgileri, site tercihleri veya elektronik alışveriş sepetlerinin içerikleri gibi kullanıcılar hakkındaki belirli bilgilerin kimliklerinin doğrulanması, takibi ve sürdürülmesi için kullanılır.*)

- ***Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et*** (*varsayılan olarak açık*) – Anti-Spyware motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da denetlemek için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım

kategorisini ifade eder: Genellikle güvenlik riski oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- ***Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et*** (*varsayılan olarak kapalı*) - Casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

- ***Dosyaları kapatılırken tara*** (*varsayılan olarak kapalı*) – İşlem sonunda tarama, AVG'nin etkin nesneleri hem açılırlarken hem da kapatılırlarken taradığından emin olmanızı sağlar. Bunun yanı sıra bu özellik, bilgisayarınızı karmaşık virüslere karşı korumanıza da yardımcı olur.

- ***Çıkarılabilir ortamların önyükleme kesimini tara*** (*varsayılan olarak açıktır*)

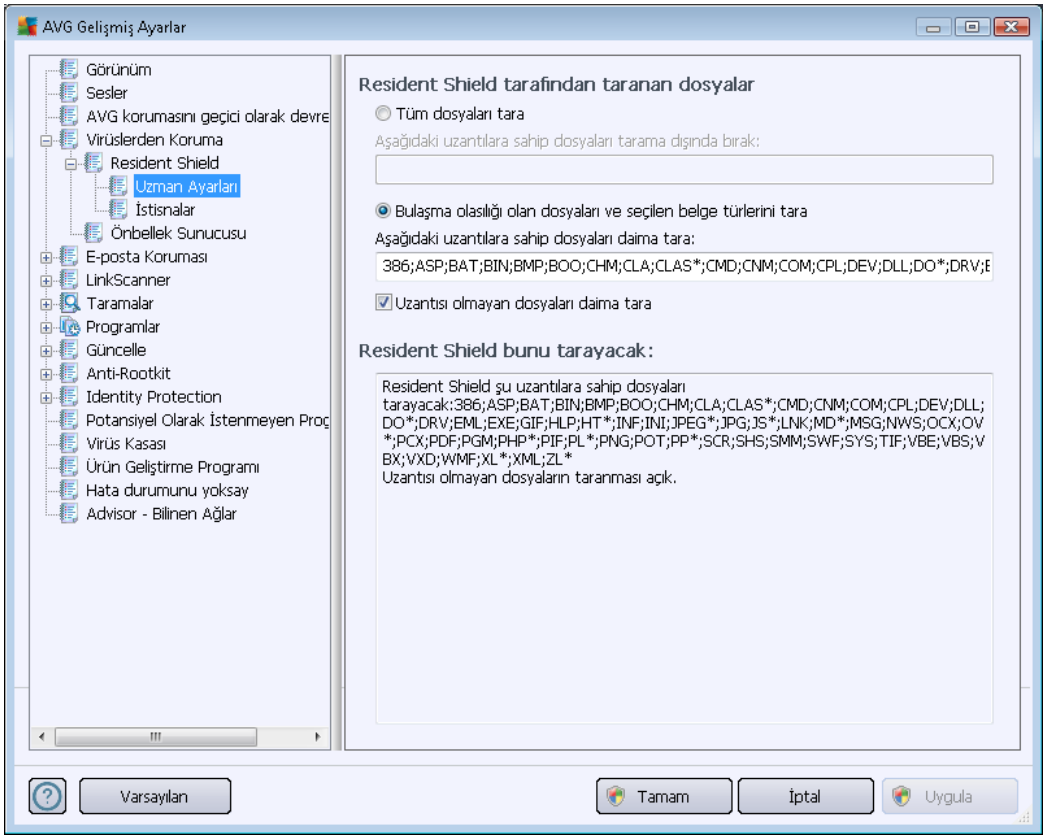
- ***Buluşsal Analiz Kullan*** - (*varsayılan olarak açık*) Buluşsal analiz, tespit etme işlemi sırasında kullanılır (*taranan nesnenin komutlarının sanal bilgisayar ortamında dinamik olarak canlandırılması*).

- ***Kayıt defterindeki dosyaları tara*** (*varsayılan olarak açık*) – Bilinen bulaşmanın sonraki bilgisayar başlangıcında çalıştırılmasını önlemek için, başlangıç kayıt defterine eklenmiş tüm çalıştırılabilir dosyaları AVG tarar.

- ***Kapsamlı taramayı etkinleştir*** (*varsayılan olarak kapalı*) - Belirli durumlarda (*çok acil bir durum olduğunda*) nesnelerin derinlemesine işlenme olasılığını denetleyecek çok hassas algoritmaları etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.

- ***Anlık Mesajlaşma korumasını ve P2P indirme korumasını etkinleştir*** (*varsayılan olarak açık*) - Anlık mesajlaşma iletişimi (*örn. ICQ, MSN Messenger, ...*) ve P2P indirmelerinin virüssüz olduğunu doğrulamak istiyorsanız bu seçeneği işaretleyin.

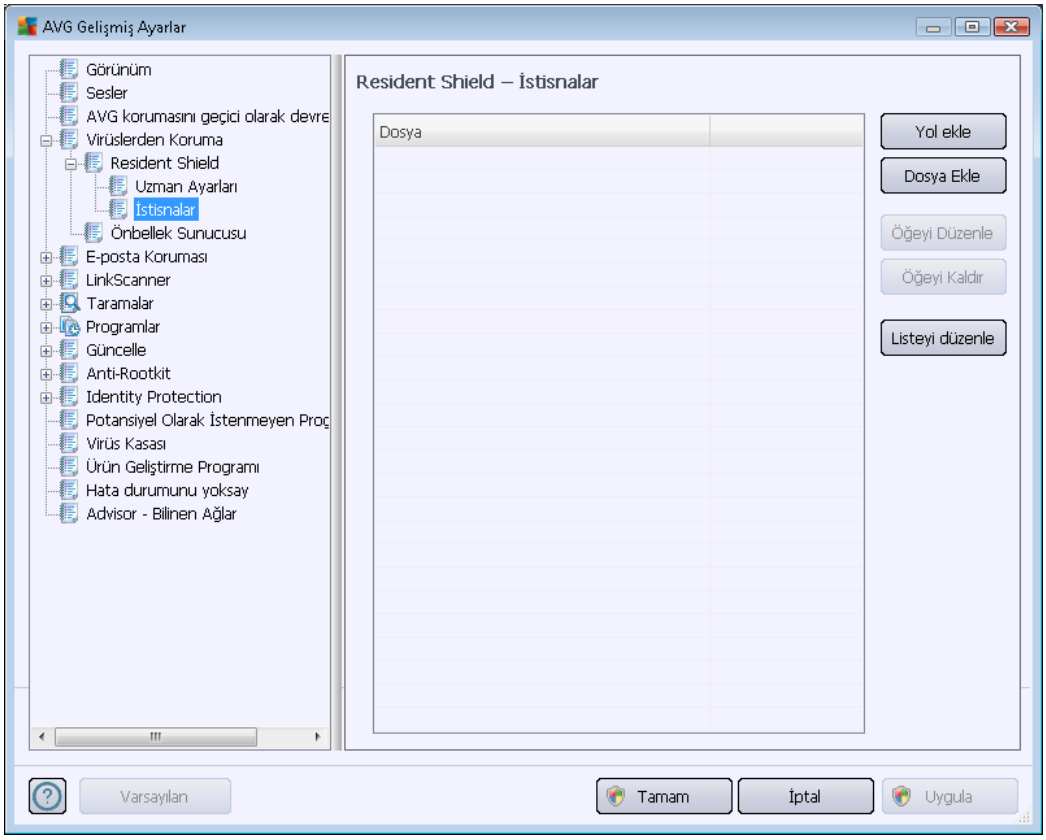
Resident Shield tarafından taranan dosyalar penceresinde taranan dosyaların yapılandırılması mümkündür (*belirli dosya uzantılarına göre*):



Tüm dosyaları tara veya yalnızca ***Bulaşma olasılığı olan dosyaları ve seçilen belge türlerini tara*** seçim yapmak için ilgili onay kutusunu işaretleyin. İkinci seçenekte karar kılarsanız, taramanın dışında tutulması gereken dosyaları tanımlayan bir uzantılar listesi ve her durumda taranması gereken dosyaları tanımlayan bir uzantılar listesinden tarama işlemini daha fazla özelleştirebilirsiniz.

Uzantısı olmayan ve bilinmeyen biçimdeki dosyaların da Resident Shield ile taranmasını sağlamak için ***Uzantısı olmayan dosyaları daima tara*** (*varsayılan olarak açıktır*) seçeneğini işaretleyin. Uzantısı olmayan dosyalar şüpheli dosyalar olduğundan, bu özelliği her zaman açık tutmanızı öneririz.

Aşağıda bahsi geçen ***Resident Shield tarayacak*** bölümü, ***Resident Shield***'ın gerçekte ne taradığı ile ilgili detaylı bilgiler görüntüleyerek geçerli ayarları daha fazla özetler.



Resident Shield – İstisnalar iletişim kutusu ***Resident Shield*** taraması sırasında hariç tutulması gereken klasörleri seçebilmenizi sağlar.

Bu gerekli değilse, hiçbir öğeyi hariç tutmamanızı önemle öneririz!

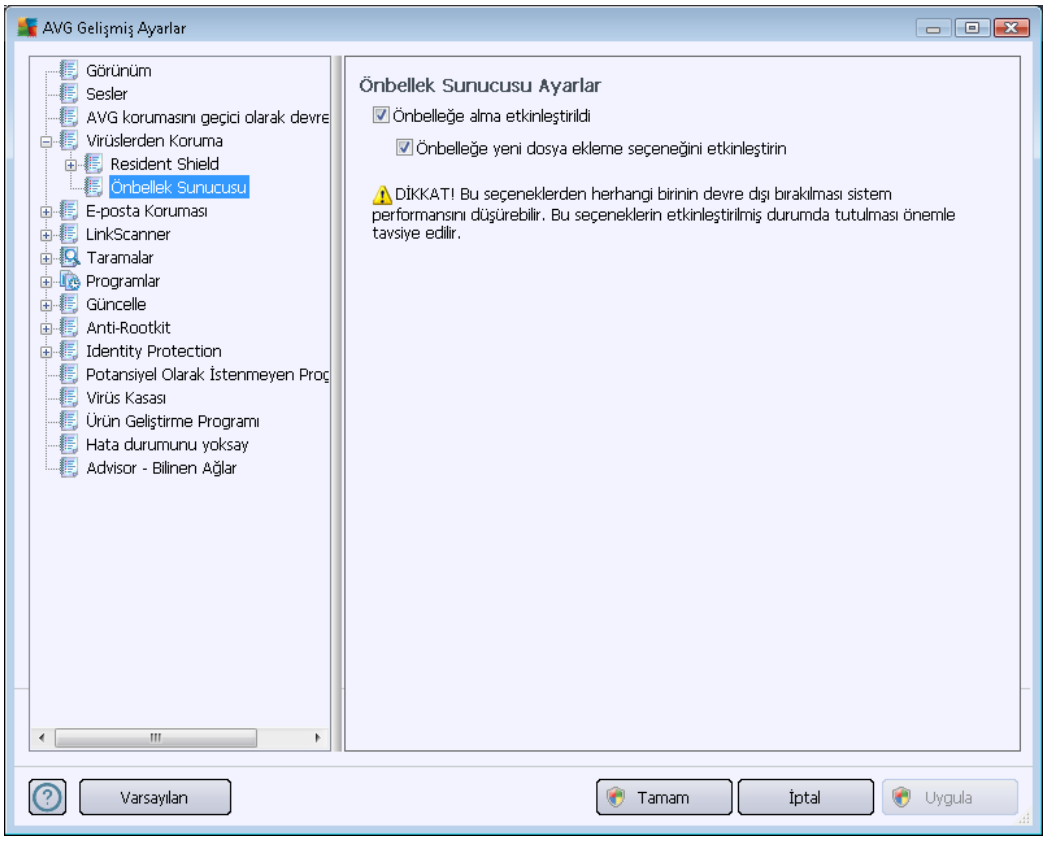
Kontrol düğmeleri

İletişim kutusunda aşağıdaki kontrol düğmeleri bulunur:

- ***Yol Ekle*** – yerel disk menü ağacından teker teker seçerek taramada hariç tutulacak dizini (dizinleri) belirleyin.
- ***Dosya Ekle*** – yerel disk menü ağacından teker teker seçerek taramada hariç tutulacak dosyaları belirleyin.
- ***Öğeyi Düzenle*** – seçilen dosyaya giden yolu düzenlemenize olanak verir
- ***Öğeyi Kaldır*** - listeden seçili öğeye götüren yolu silmenize olanak verir
- ***Listeyi Düzenle*** – tanımlanan istisnaların tüm listesini, standart metin düzenleyici gibi çalışan yeni bir iletişim kutusunda düzenleyebilmenizi sağlar

10.4.2. Önbellek Sunucusu

Önbellek Sunucusu Ayarları iletişim kutusu tüm **AVG Anti-Virus** tarama türlerini hızlandırmak için tasarlanan önbellek sunucusu sürecini işaret eder:



Önbellek sunucusu güvenilir dosyaların bilgilerini toplar ve saklar (*bir dosya güvenilir bir kaynak tarafından dijital imza ile imzalandığında güvenilir sayılır*). Böylece bu dosyalar otomatik olarak güvenli varsayılır ve yeniden taranmalarına gerek duyulmaz; bu nedenle tarama sırasında bu dosyalar atlanır.

Önbellek Sunucusu Ayarları iletişim kutusu aşağıdaki yapılandırma seçeneklerini sunar:

- ***Önbelleğe alma etkin*** (*varsayılan olarak açıktır*) – ***Önbellek Sunucusu***'nu kapatmak için kutunun işareti kaldırın ve önbellek belleğini boşaltın. Lütfen, kullanımdaki her bir dosya virüs ve casus yazılım için ilk kez taranacağından taramanın yavaş olabileceğini ve bilgisayarınızın genel performansının azalacağını unutmayın.

- ***Önbelleğe yeni dosyaların eklenmesini etkinleştir*** (*varsayılan olarak açıktır*) – önbelleğe daha fazla dosya eklenmesini durdurmak için kutunun işaretini kaldırın. Önceden önbelleğe alınmış her dosya korunacak ve önbelleğe alma tamamen kapatılıncaya kadar veya virüs veritabanının bir sonraki güncellenmesine kadar kullanılacaktır.

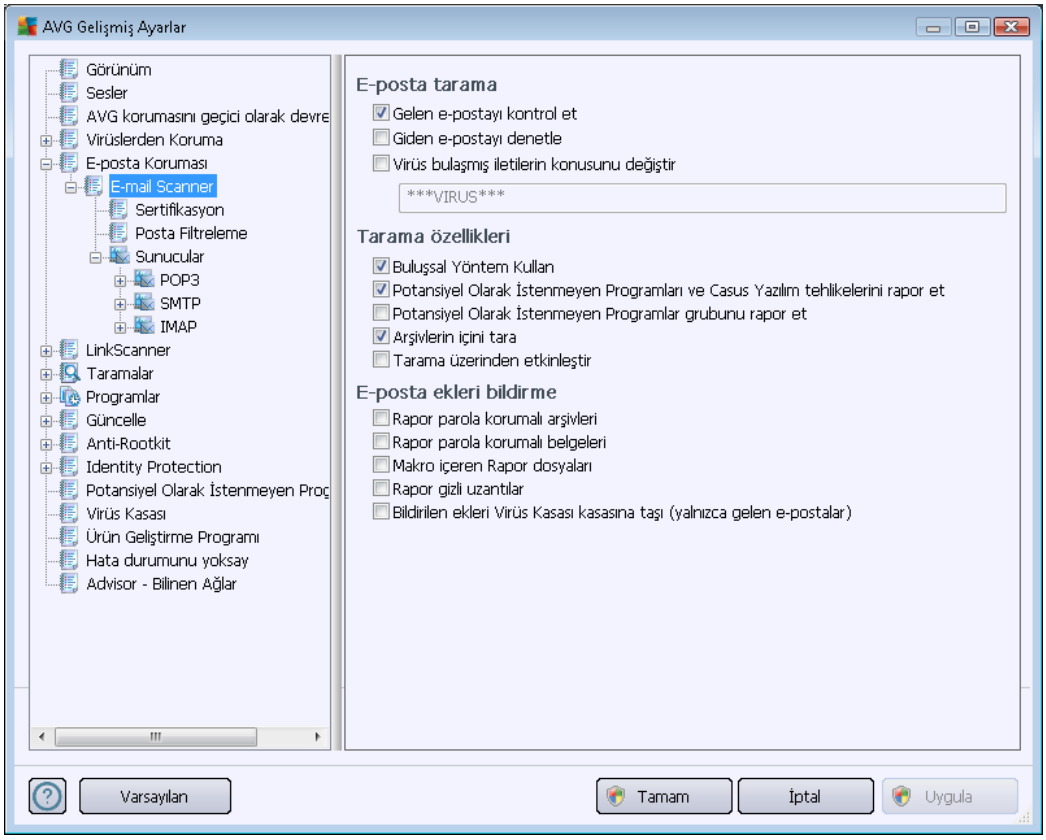
Önbellek sunucusunu kapatmak için iyi bir nedeniniz yoksa, kesinlikle varsayılan ayarları korumanızı ve seçeneğin açık kalmasını öneririz! Aksi durumda, sistem hızı ve performansında ciddi bir düşüş görebilirsiniz.

10.5. E-posta koruması

E-posta koruması bölümünde E-mail Scanner ve Anti-Spam için ayrıntılı yapılandırmalar düzenleyebilirsiniz:

10.5.1. E-Posta Tarayıcısı

E-Posta Tarayıcısı iletişim kutusu üç bölüme ayrılmıştır:



E-posta tarama

Bu bölümde, gelen ve/veya giden e-posta iletileri için bu temel bilgileri ayarlayabilirsiniz:

- ***Gelen e-postayı denetle*** (*varsayılanda açıktır*) – e-posta istemcinize gelen tüm e-postaları tarama seçeneğini açmak/kapatmak için işaretleyin
- ***Giden e-postayı denetle*** (*varsayılanda kapalıdır*) – hesabınızdan gönderilen tüm e-postaları tarama seçeneğini açmak/kapatmak için işaretleyin
- ***Virüs bulaşmış iletilerin konusunu değiştir*** (*varsayılanda kapalıdır*) – taranan e-posta iletisinin bulaşmış olarak tespit edilmesi durumunda size bildirilmesini istiyorsanız, bu öğeyi işaretleyin ve metin alanına istediğiniz metni yazın. Ardından bu metin, daha kolay tanımlanması ve filtrelenmesi için tespit edilen her e-posta iletisinin "Konu" alanına eklenecektir. Varsayılan değer ***VİRÜS*** olarak belirlenmiştir ve bu değeri korumanızı öneririz.

Tarama özellikleri

Bu bölümde, e-posta iletilerinin nasıl taranacağını belirleyebilirsiniz:

- ***Buluşsal Yöntem Kullan*** (*varsayılanda açıktır*) – e-posta iletilerini tararken buluşsal tespit yöntemi kullanmak için işaretleyin. Bu seçenek açık olduğunda, e-posta eklerini yalnızca uzantıya göre filtrelemezsiniz; ekin gerçek içeriği de göz önünde bulundurulur. Filtreleme işlemi Posta Filtreleme iletişim kutusundan ayarlanabilir.

- ***Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et*** (*varsayılanda açıktır*) – Anti-Spyware motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: Genellikle güvenlik riski oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- ***Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et*** (*varsayılanda kapalıdır*) – bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

- ***Arşivlerin içini tara*** (*varsayılanda açıktır*) – e-posta iletilerine eklenen arşivlerin içeriklerini taramak için işaretleyin.

- ***Kapsamlı taramayı etkinleştir*** (*varsayılanda kapalıdır*) – belirli durumlarda (*örneğin, bilgisayarınıza virüs veya kötü amaçlı yazılım bulaştığından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.

E-posta eklerini bildirme

Bu bölümde, potansiyel olarak tehlikeli ve şüpheli olan dosyalar için ek raporlar ayarlayabilirsiniz. Lütfen bir uyarı iletişim kutusu görüntülenmeyeceğini unutmayın. Yalnızca e-posta iletisinin sonuna bir onay metni eklenir ve bu tür tüm raporlar E-posta Tarayıcısı tespiti iletişim kutusunda listelenir:

- ***Parola korumalı arşivleri bildir*** – parolayla korunan arşivler için (*ZIP, RAR vb.*) virüs taraması mümkün değildir. Bunların potansiyel olarak tehlikeli olduklarını bildirmek üzere kutuyu işaretleyin.

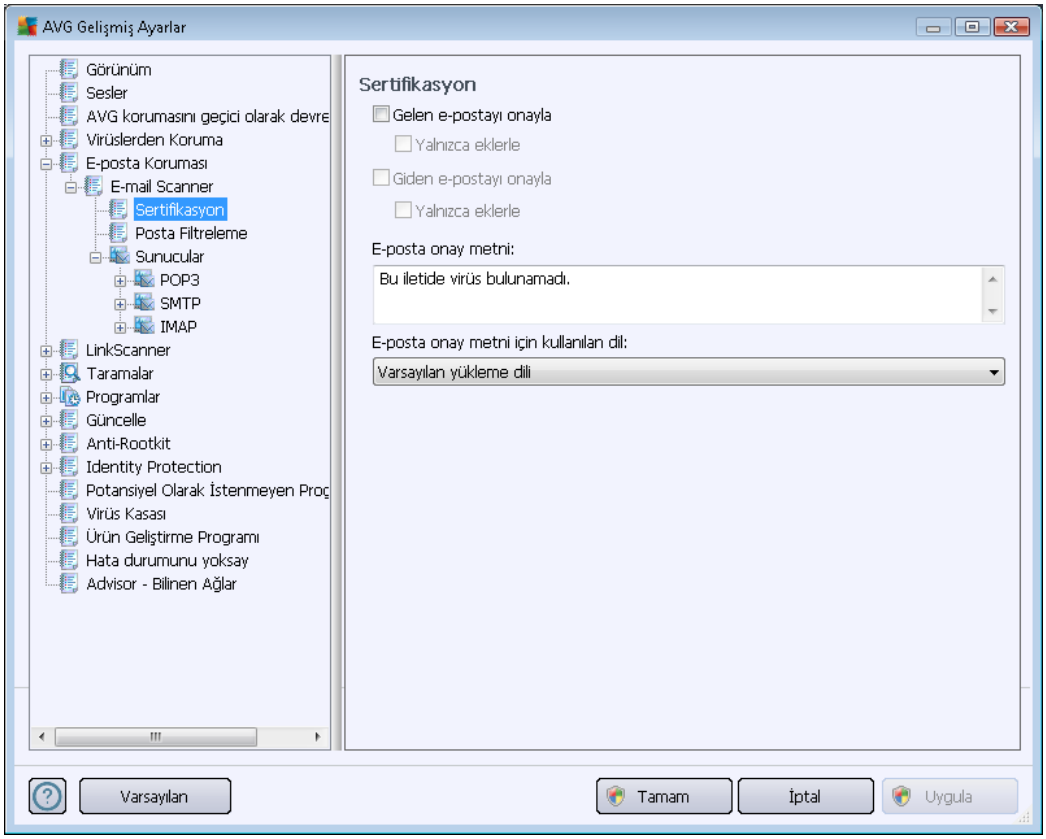
- ***Parola korumalı belgeleri bildir*** – parolayla korunan belgeler için virüs taraması mümkün değildir. Bunların potansiyel olarak tehlikeli olduklarını bildirmek üzere kutuyu işaretleyin.

- ***Makro içeren dosyaları bildir*** – Makro, bazı görevlerin kullanıcı için daha kolay hale getirilmesini amaçlayan önceden tanımlanmış adımlar dizisidir (*MS Word makroları yaygın olarak bilinir*). Makro, potansiyel olarak tehlikeli talimatlar içerebilir. Makro içeren dosyaların şüpheli olarak bildirilmesini sağlamak için kutuyu işaretleyebilirsiniz.

- ***Gizlenen uzantıları bildir*** – gizli uzantılar şüpheli bir çalıştırılabilir dosyayı (örn. "birşey.txt.exe") zararsız bir düz metin dosyası gibi (örn. "birşey.txt") gösterebilir; bunları potansiyel olarak tehlikeli olarak bildirmek için kutuyu işaretleyin.

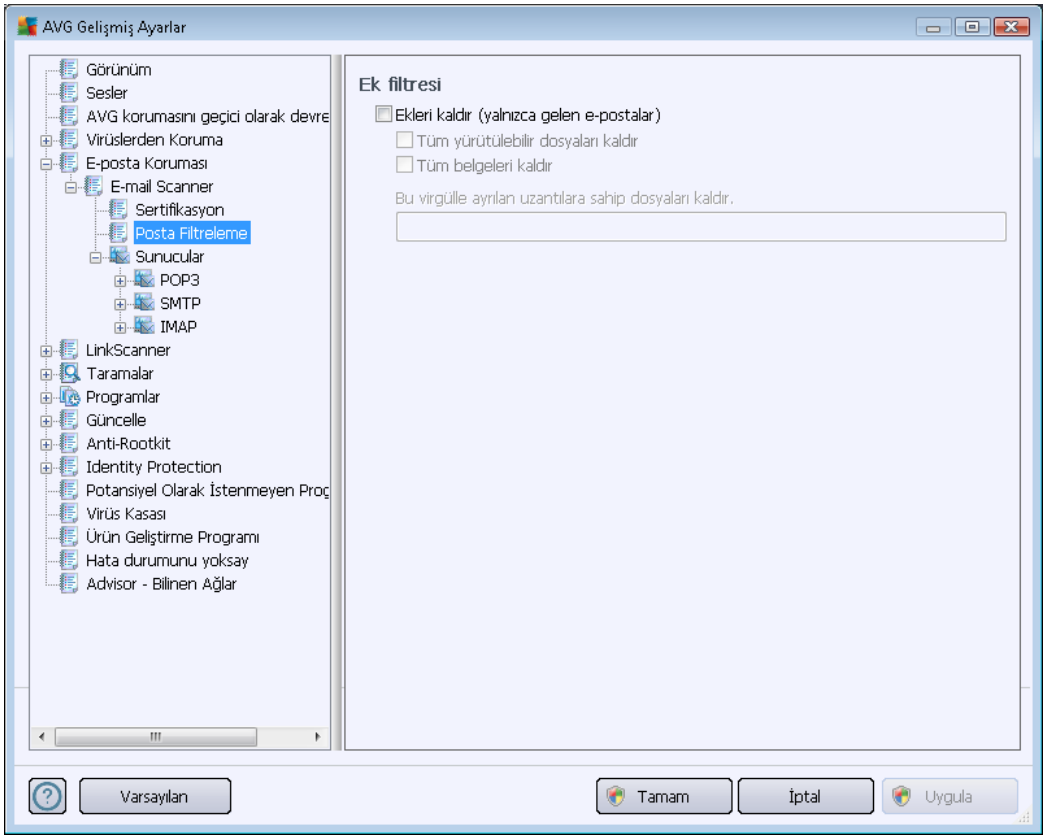
- ***Rapor edilen ekleri Virüs Kasasına taşı*** – taranan e-posta iletisinin ekinde gizli bir eklenti tespit edildiğinde parola korumalı arşivler, parola korumalı belgeler, makro içeren belgeler ve/veya dosyalar hakkında e-posta vasıtasıyla bilgilendirilmek isteyip istemediğinizi belirtin. Tarama işlemi sırasında bu tür bir mesaj tespit edilirse tespit edilen bulaşmış nesnenin Virüs Kasasına taşınmasını isteyip istemediğinizi belirtin.

Sertifika iletişim kutusunda gelen ve/veya giden e-postaları onaylamaya (***Gelen e-postayı onayla***) veya onaylamamaya (***Giden e-postayı onayla***) karar vermek için çeşitli onay kutularını işaretleyebilirsiniz. Bu seçeneklerin her biri için ***Yalnızca ekleri olanlar*** parametresini işaretleyip onayın yalnızca ekleri olan e-postalara eklenmesini sağlayabilirsiniz:



Varsayılan olarak, onay mesajı şunun gibi temel bilgiler içerir:*Bu iletide virüs bulunamadı gibi.* Ancak, bu bilgiler ihtiyaçlarınıza göre artırılabilir veya değiştirilebilir: ***E-posta onay metni*** alanına istediğiniz onay metnini yazın. ***E-posta onay metni için kullanılan dil*** bölümünde onayın otomatik olarak oluşturulan kısmının (*Bu iletide virüs bulunamadı*) hangi dilde görüntüleneceğini de belirleyebilirsiniz.

Not: *İstenen dilde yalnızca varsayılan metnin görüntüleneceğine ve özelleştirilmiş metninizin otomatik olarak çevrilmeyeceğine dikkat edin!*



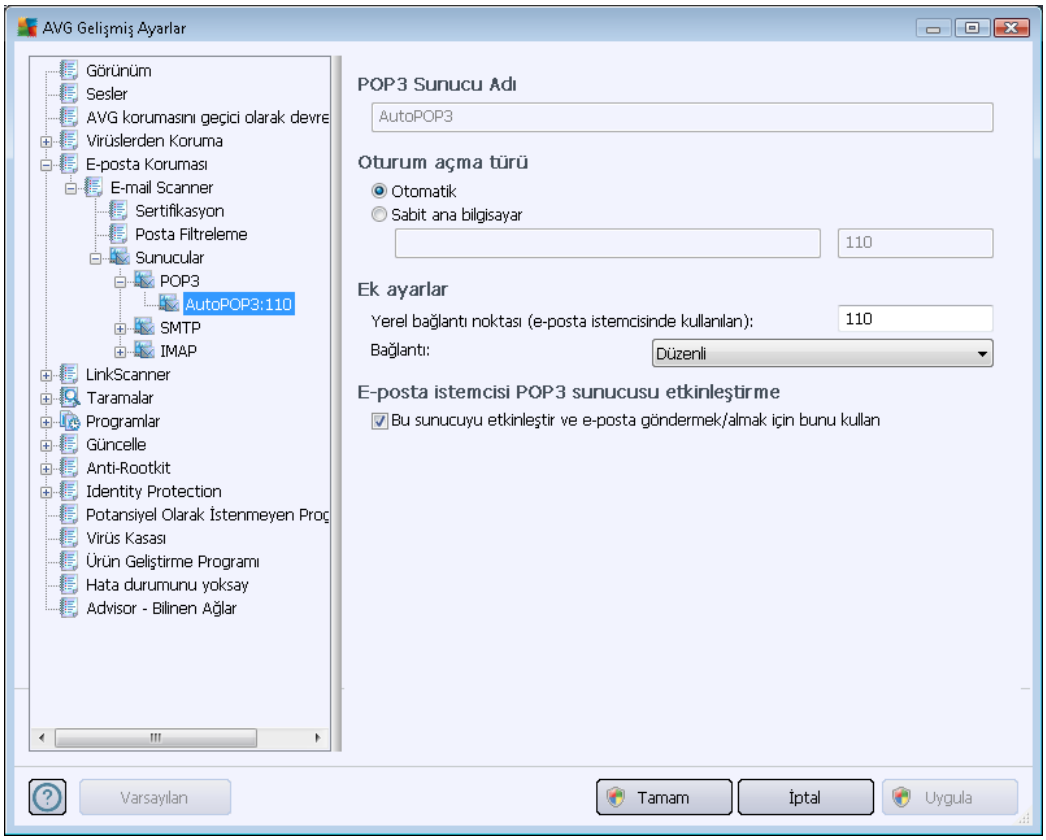
Ek filtresi iletişim kutusu, e-posta mesajlarının eklerinin taranmasına ilişkin parametreleri ayarlayabilmenizi sağlar.Varsayılan olarak ***Eklentileri sil*** seçeneği kapalıdır. Etkinleştirmeye karar verirseniz tüm e-posta mesajlarının eklentileri, bulaşmış nesne ya da potansiyel olarak tehlikeli nesne olarak algılanacak ve silinecektir. Belirli ek türlerinin silinmesini istiyorsanız ilgili seçeneği seçin:

- ***Tüm çalıştırılabilir dosyaları sil*** – tüm *.exe dosyaları silinecektir
- ***Tüm belgeleri kaldır*** - tüm *.doc, *.docx, *.xls, *.xlsx dosyaları silinecektir
- ***Virgülle ayrılmış şu uzantılara sahip dosyaları kaldır*** – Tanımlanan uzantılara sahip tüm dosyalar kaldırılacaktır

Sunucular bölümünde E-posta Tarayıcısı sunucularının parametrelerini düzenleyebilirsiniz:

- POP3 sunucusu
- SMTP sunucusu
- IMAP sunucusu

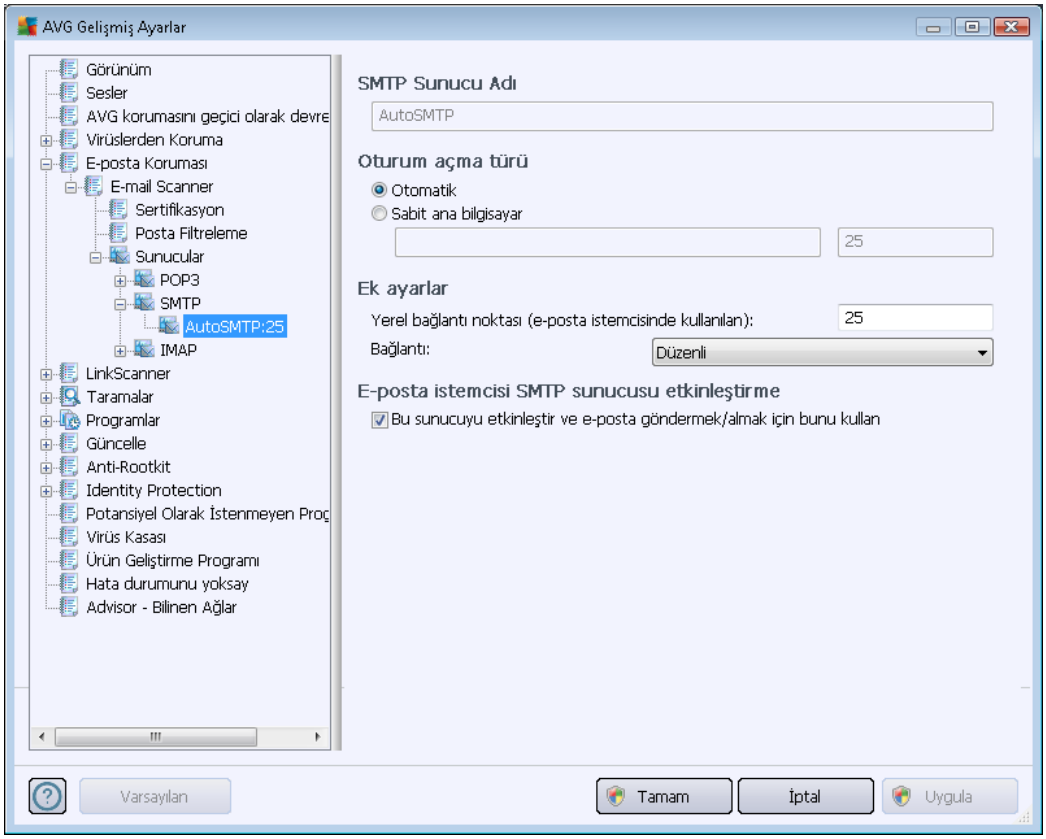
Ayrıca, ***Yeni sunucu ekle*** düğmesiyle gelen ve giden postalar için yeni sunucu tanımlayabilirsiniz.



(***Sunucular / POP3*** ile açılan) bu iletişim kutusunda, gelen postalar için POP3 protokolü kullanarak yeni bir E-posta Tarayıcısı sunucusu kurabilirsiniz:

- ***POP3 Sunucusunun Adı*** – bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir POP3 sunucusu eklemek için, sol menü ağacının POP3 öğesinin üzerinde sağ fare düğmesini tıklatın*). Otomatik olarak oluşturulan "AutoPOP3" sunucusu için bu alan devre dışı bırakılmıştır.
- ***Oturum açma tipi*** – gelen postalar için kullanılan posta sunucularının belirlenmesi sırasında kullanılan yöntemi tanımlar:
  - ***Otomatik*** - Oturum açma işlemi, e-posta istemcinizin ayarlarına göre otomatik olarak gerçekleştirilir.
  - ***Sabit ana bilgisayar*** – Bu durumda, program her zaman burada belirtilen sunucuyu kullanır. Lütfen posta sunucunuzun adresini veya adını belirtin. Oturum açma adı değişmez. Ad için, IP adresinin yanı sıra (*örneğin, 123.45.67.89*) etki alanı adı da (*örneğin, pop.acme.com*) kullanabilirsiniz. Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına yazabilirsiniz (*örn. smtp.acme.com:8200*). POP3 iletişimi için standart bağlantı noktası 110'dur.

- ***Diğer ayarlar*** – daha ayrıntılı parametreleri belirler:
    - ***Yerel bağlantı noktası*** – Posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Posta uygulamanızda, bu bağlantı noktasını POP3 iletişimi bağlantı noktası olarak belirtmeniz gerekir.
    - ***Bağlantı*** - *kullanılacak bağlantı türünü aşağı açılır menüden belirtebilirsiniz (normal/ SSL/SSL varsayılan*). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik de, yalnızca hedef posta sunucusu tarafından desteklendiğinde kullanılabilir.
- ***E-posta istemcisi POP3 sunucusu etkinleştirme*** - belirtilen POP3 sunucusunu etkinleştirmek veya devre dışı bırakmak için bu öğeyi işaretleyin/işaretini kaldırın.



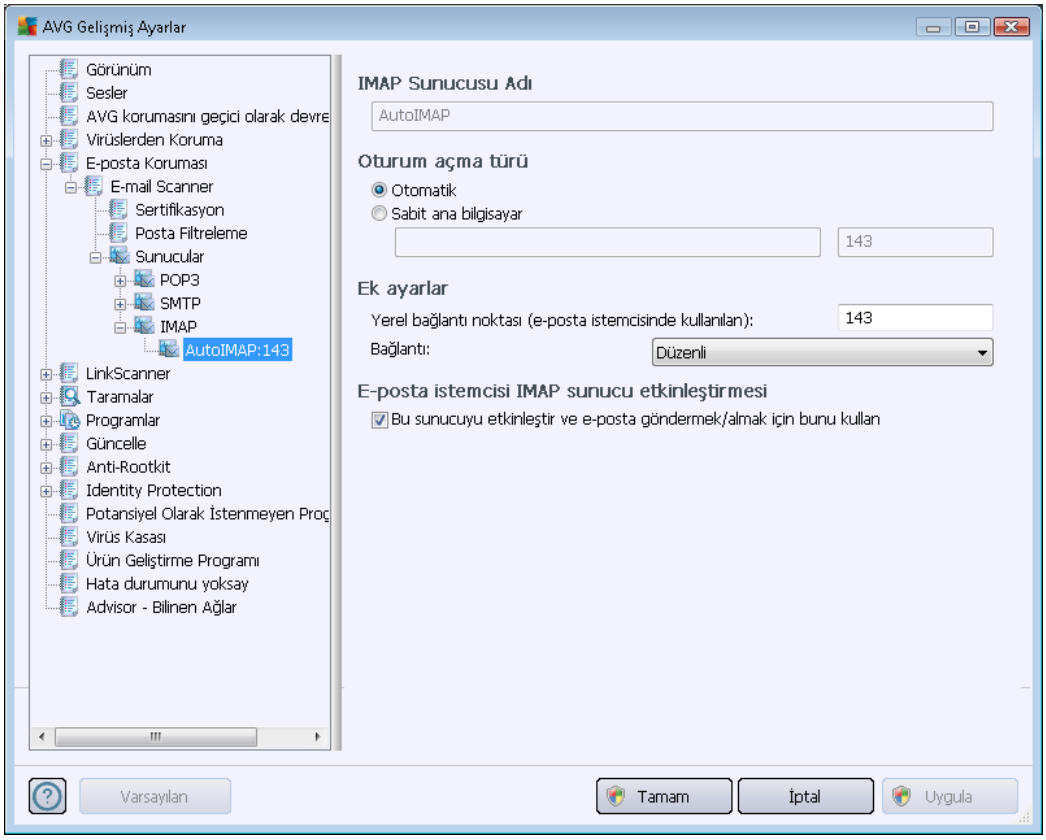
*Bu iletişim kutusunda (**Sunucular /SMTP üzerinden açılır**)* yeni bir E-posta Tarayıcısı sunucusu belirlemek üzere giden postalar için SMTP protokolünü kullanabilirsiniz:

- ***SMTP Sunucusunun Adı*** – bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir SMTP sunucusu eklemek için, sol menü ağacının SMTP öğesinin üzerinde sağ fare düğmesini tıklatın*). Otomatik olarak oluşturulan "AutoSMTP" sunucusu için bu alan devre dışı bırakılmıştır.
- ***Oturum açma tipi*** – giden postalar için kullanılan posta sunucularının tanımlanması

sırasında kullanılan yöntemdir:

- ***Otomatik*** – oturum açma işlemi, e-posta istemcinizin ayarlarına göre otomatik olarak gerçekleştirilir
- ***Sabit ana bilgisayar*** – bu durumda, program her zaman burada belirtilen sunucuyu kullanır. Lütfen posta sunucunuzun adresini veya adını belirtin. Ad için, IP adresinin yanı sıra (*örneğin, 123.45.67.89*) etki alanı adı da (*örneğin, smtp.acme.com*) kullanabilirsiniz. *Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına girebilirsiniz (örn. smtp.acme.com:8200*). SMTP iletişimi için standart bağlantı noktası 25'tir.

- ***Diğer ayarlar*** – daha ayrıntılı parametreleri belirler:
  - ***Yerel bağlantı noktası*** – Posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Posta uygulamanızda, bu bağlantı noktasını SMTP iletişimi bağlantı noktası olarak belirtmeniz gerekir.
  - ***Bağlantı*** – bu açılır aşağı menüden, kullanılacak bağlantı türünü belirtebilirsiniz (*normal/SSL/SSL varsayılan*). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik, yalnızca hedef posta sunucusu tarafından desteklendiğinde kullanılabilir.
- ***E-posta istemcisi SMTP sunucusu aktivasyonu*** – yukarıda belirtilen SMTP sunucusunu etkinleştirmek/devre dışı bırakmak için bu kutuyu işaretleyin/işaretini kaldırın



Bu iletişim kutusunda (***Sunucular /IMAP üzerinden açılır***) yeni bir E-posta Tarayıcısı sunucusu belirlemek üzere giden postalar için SMTP protokolünü kullanabilirsiniz:

- ***IMAP Sunucusunun Adı*** – bu alanda yeni eklenen sunucuların adını belirtebilirsiniz (*bir IMAP sunucusu eklemek için, sol menü ağacının IMAP öğesinin üzerinde sağ fare düğmesini tıklatın*). Otomatik olarak oluşturulan "AutoIMAP" sunucusu için bu alan devre dışı bırakılmıştır.
- ***Oturum açma tipi*** – giden postalar için kullanılan posta sunucularının tanımlanması sırasında kullanılan yöntemdir:
  - ***Otomatik*** – oturum açma işlemi, e-posta istemcinizin ayarlarına göre otomatik olarak gerçekleştirilir
  - ***Sabit ana bilgisayar*** – bu durumda, program her zaman burada belirtilen sunucuyu kullanır. Lütfen posta sunucunuzun adresini veya adını belirtin. Ad için, IP adresinin yanı sıra (*örneğin, 123.45.67.89*) etki alanı adı da (*örneğin, smtp.acme.com*) kullanabilirsiniz. Posta sunucusu standart olmayan bir bağlantı noktası kullanıyorsa, bu bağlantı noktasını ayırıcı olarak iki nokta üst üste kullanarak sunucu adının arkasına yazabilirsiniz (*örneğin, smtp.acme.com:8200*). IMAP iletişiminin standart bağlantı noktası 143'tür.
- ***Diğer ayarlar*** – daha ayrıntılı parametreleri belirler:

- ***Yerel bağlantı noktası*** – posta uygulamanızın iletişim kurması beklenen bağlantı noktasını belirler. Bundan sonra, posta uygulamanızda, bu bağlantı noktasını IMAP iletişimi bağlantı noktası olarak belirtmeniz gerekir.

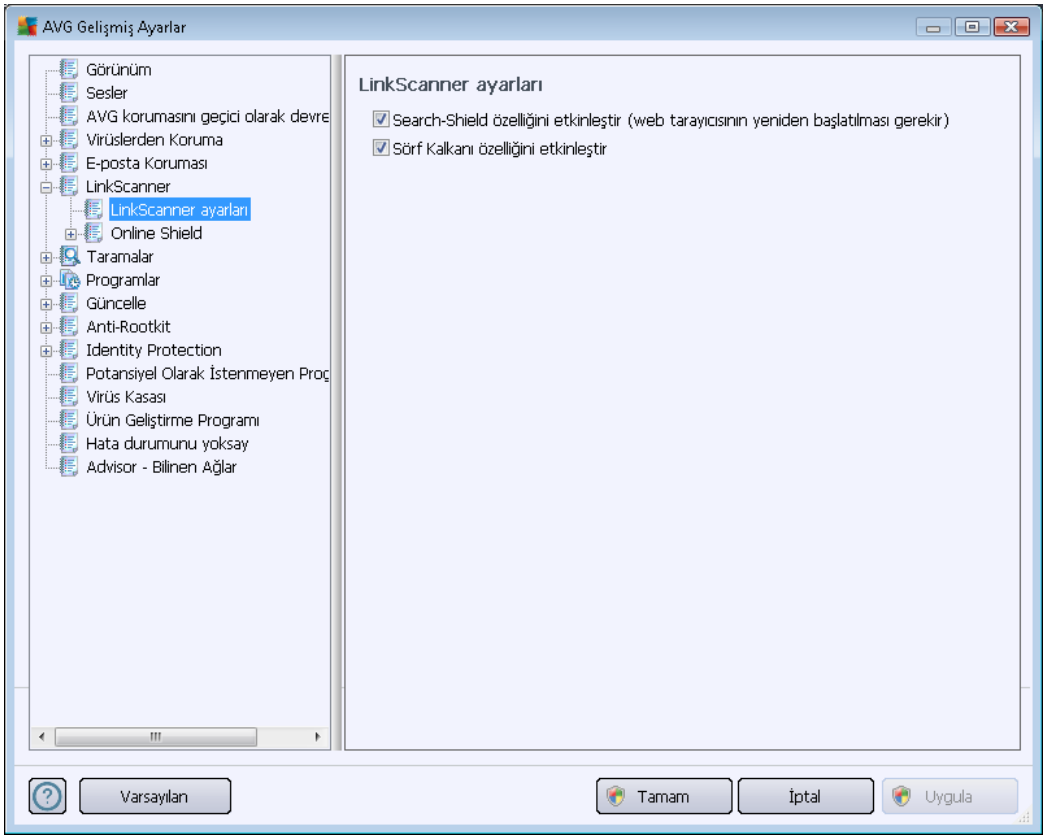
- ***Bağlantı*** – bu açılır aşağı menüden, kullanılacak bağlantı türünü belirtebilirsiniz (*normal/SSL/SSL varsayılan*). SSL bağlantıyı tercih ederseniz, gönderilen veri, üçüncü bir taraf tarafından izlenme riski olmayacak şekilde şifrelenir. Bu özellik, yalnızca hedef posta sunucusu tarafından desteklendiğinde kullanılabilir.

- ***E-posta istemcisi IMAP sunucusu aktivasyonu*** – yukarıda belirtilen IMAP sunucusunu etkinleştirmek/devre dışı bırakmak için bu kutuyu işaretleyin ve kutunun işaretini kaldırın

10.6. LinkScanner

10.6.1. LinkScanner ayarları

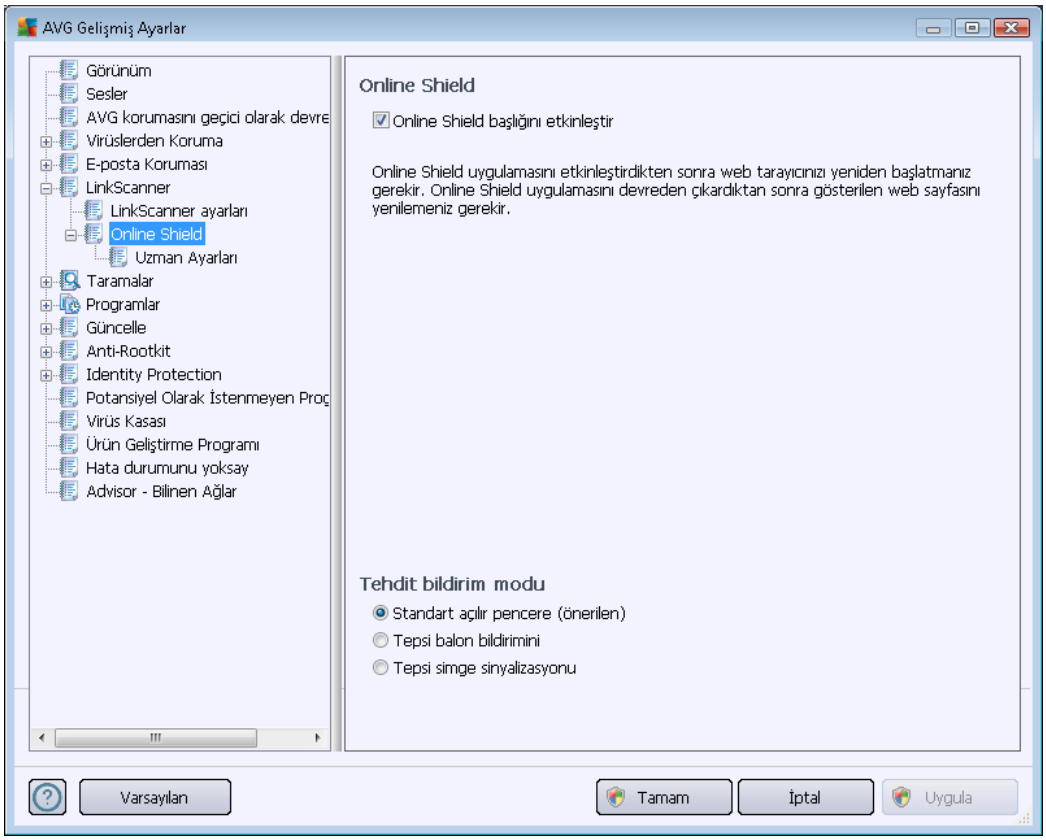
LinkScanner ayarları iletişim kutusu, LinkScanner uygulamasının temel özelliklerini açıp kapatmanızı sağlar:



- ***Arama Kalkanı'nı Etkinleştir*** – (*varsayılan olarak açıktır*): Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg veya SlashDot ile yapılan aramalarda, arama motoru tarafından döndürülen içeriği önceden denetleyerek tavsiye niteliğinde uyarı simgeleri görüntüler.

- ***Surf-Shield'i etkinleştir*** – (*varsayılan olarak açıktır*): erişim sağlandığı anda güvenlik açığı olan web sitelerine karşı (*anlık zamanlı*) koruma sağlamak için etkinleştirin. Bilinen kötü amaçlı site bağlantıları ve güvenlik açığından yararlanan içerikler, kullanıcı bir web tarayıcısı (*ya da HTTP kullanan diğer bir program*) aracılığıyla erişim sağladığında engellenir.

10.6.2. Online Shield



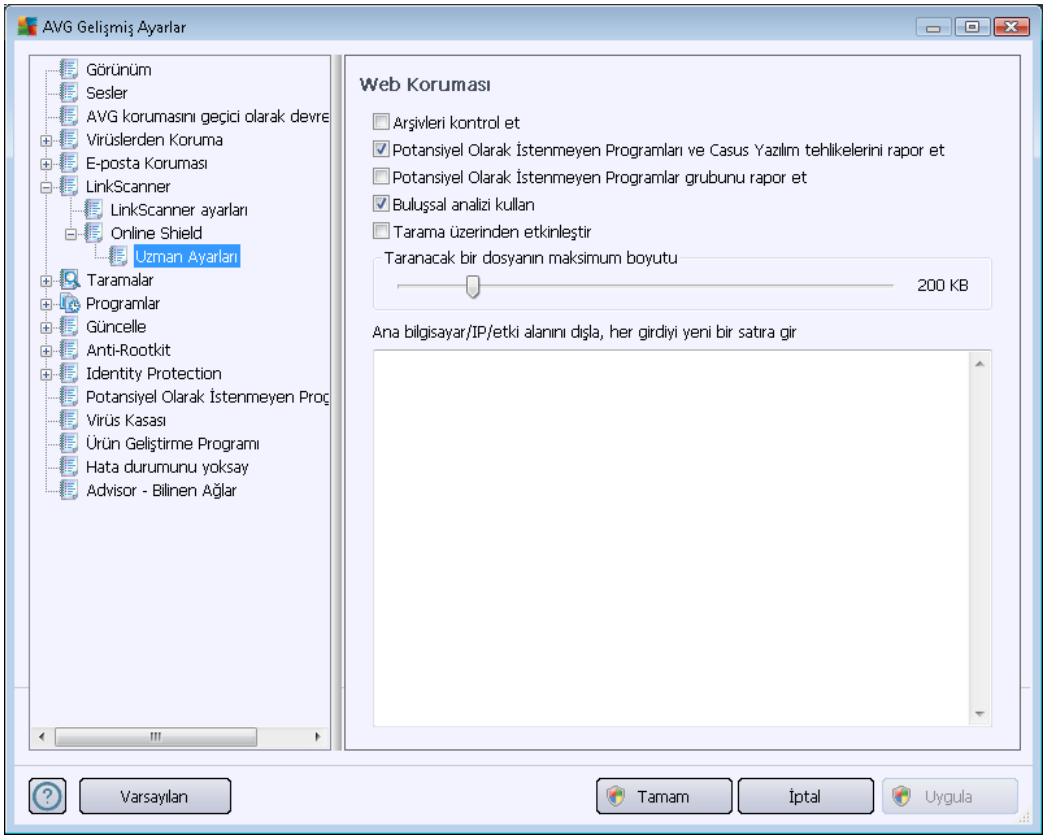
Online Shield iletişim kutusu şu seçenekleri sunar:

- ***Online Shield'ı etkinleştir*** *(varsayılan olarak açık)* – ***Online Shield*** hizmetinin tamamını etkinleştirir/devre dışı bırakır. Diğer ***Online Shield*** gelişmiş ayarları için lütfen Web Koruması adındaki sonraki iletişim kutusuna geçin.

- ***AVG Accelerator'ı etkinleştir*** *(varsayılan olarak açık)* - Daha düzgün çevrimiçi video oynatma ve ilave indirmeleri kolaylaştırma olanağı sağlayan ***AVG Accelerator*** hizmetini etkinleştirir/devre dışı bırakır.

Tehdit bildirim modu

İletişim kutusunun alt kısmında algılanması muhtemel tehdit hakkında ne şekilde bilgilendirilmek istediğinizi seçin: standart açılır iletişim kutusuyla, tepsi balon bildirimiyle ya da tepsi simgesi bilgileriyle.



Web Koruması – web sitelerinin içeriğinin taranmasına ilişkin bileşen yapılandırmasını düzenleyebilirsiniz. Düzenleme arayüzü ile aşağıdaki temel seçenekleri yapılandırabilirsiniz:

- ***Web korumasını etkinleştir*** – bu seçenek ***Online Shield***'in www sayfalarının içeriğinin taranmasını gerçekleşmek gerektiğini onaylar. Bu seçeneğin etkin konumda olmasına rağmen (*varsayılan olarak*) söz konusu öğeleri açıp kapatabilirsiniz:
    - ***Arşivleri denetle*** – (*varsayılanda kapalıdır*): muhtemelen www sayfasında görüntülenecek arşivlerin içeriğini tarayın.
    - ***Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et*** (*varsayılan olarak açık*) – Anti-Spyware motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: Genellikle güvenlik riski oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.
    - ***Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et*** – (*varsayılanda kapalıdır*): casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

- ***Buluşsal analiz yöntemini kulan*** - (*varsayılanda açıktır*): görüntülenecek web sitesinin içeriği buluşsal analiz yöntemi kullanılarak taranır (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*).

- ***Kapsamlı taramayı etkinleştir*** (*varsayılanda kapalıdır*) – belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.

- ***Taranacak maksimum dosya bölümü büyüklüğü*** – Dahil edilen dosyalar görüntülenen sayfada mevcutsa, bunları bilgisayarınıza indirmeden önce de içeriklerini tarayabilirsiniz. Ancak büyük dosyaların taranması zaman alabilir ve web sayfasının indirilmesi de önemli ölçüde yavaşlayabilir. ***Online Shield*** ile taranacak dosyanın maksimum boyutunu belirlemek için kaydırma çubuğunu kullanabilirsiniz. İndirilen dosya belirtilen dosya boyutundan daha büyük olsa ve buna bağlı olarak Online Shield ile taranmasa bile korunmaya devam edersiniz: dosya, bulaşmış olması halinde ***Resident Shield*** tarafından tespit edilecektir.

- ***Barındırma/IP/etki alanını dışla*** – metin alanına *Online Shield* tarafından taranmasını istemediğiniz bir sunucunun tam adını (***barındırma, IP adresi, maskeli IP adresi ya da URL****) ya da etki alanı adını girin.* Bu nedenle, bu işlemi yapmadan önce web sitesinin içeriğinin zararlı olmadığından emin olmanız gerekir.

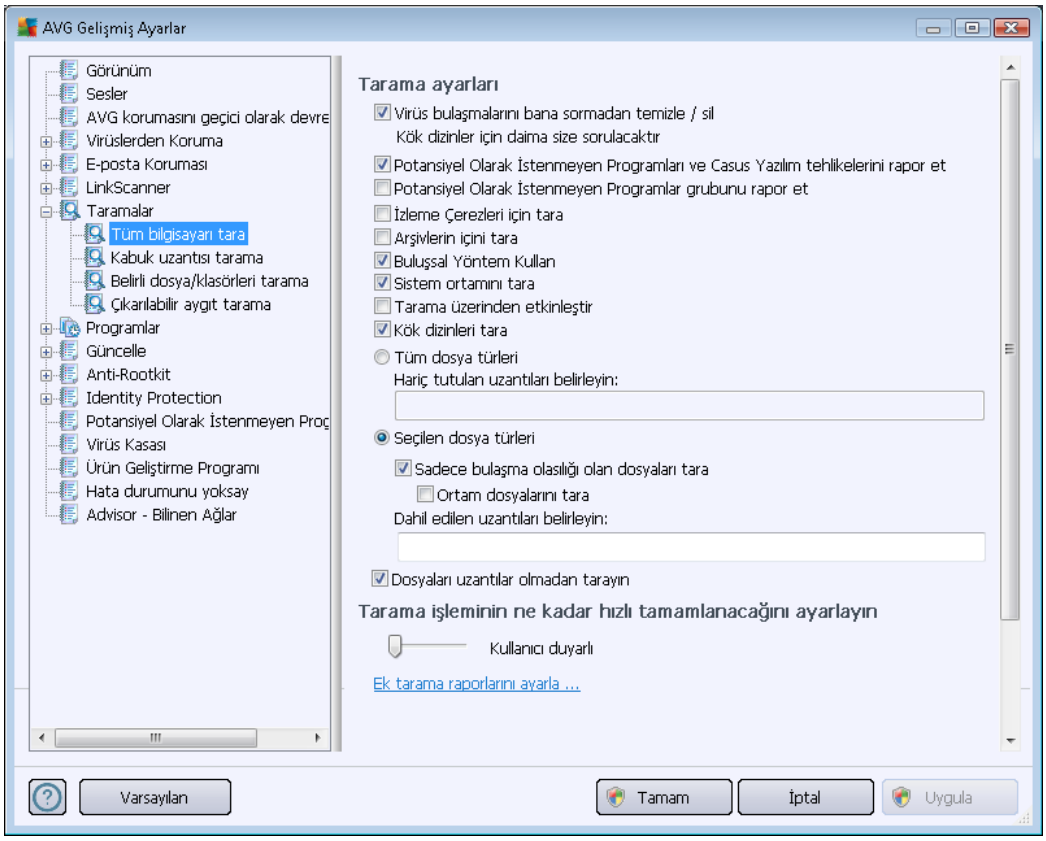
10.7. Taramalar

Gelişmiş tarama ayarları, yazılım geliştiricisi tarafından tanımlanan belirli tarama türlerine ilişkin dört kategoriye bölünmüştür:

- ***Tüm bilgisayarın taranması*** - tüm bilgisayarın standart öntanımlı taramasıdır
- ***Kabuk Uzantı Taraması*** - seçilen nesnenin doğrudan Windows Gezgini ortamında taranması işlemidir
- ***Belirli Dosya veya Klasörleri Tarama*** – bilgisayarınızın seçilen alanlarının tarandığı standart öntanımlı taramadır
- ***Çıkartılabilir Aygıt Taraması*** – bilgisayarınıza bağlanan çıkartılabilir aygıtların taranması işlemidir

10.7.1. Tüm bilgisayar taraması

Tüm Bilgisayarı Tara seçeneği, yazılım satıcısı tarafından belirlenmiş varsayılan tarama yöntemlerinden birinin parametrelerini düzenleyebilmenize olanak tanır, Tüm bilgisayarı tara:



Tarama ayarları

Tarama ayarları bölümünde isteğe bağlı olarak açılıp kapatılabilecek tarama parametreleri listelenmiştir:

- ***Bulaşmayı bana sormadan temizle / kaldır*** (*varsayılan olarak açık*) – Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne Virüs Kasası'na taşınır.

- ***Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et*** (*varsayılanda açıktır*) – Anti-Spyware motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- ***Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et*** (*varsayılanda kapalıdır*) – bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen

zararsız olan, ancak daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

- ***İzleme Tanımlama Bilgilerini Tara*** (*varsayılan olarak kapalıdır*) – Anti-Spyware bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar; (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

- ***Arşivleri tara*** (*varsayılan olarak kapalıdır*) – bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.

- ***Buluşsal Analiz Yöntemlerini Kullan*** (*varsayılan olarak açıktır*) – buluşsal analiz yöntemi (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.

- ***Sistem ortamını tara*** (*varsayılan olarak açıktır*) – tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.

- ***Kapsamlı taramayı etkinleştir*** (*varsayılanda kapalıdır*) – belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.

- ***Rootkit'leri tara*** (*varsayılan olarak açık*) – Anti-Rootkit taraması bilgisayarınızı olası rootkit'lere, örneğin bilgisayarınızda kötü amaçlı etkinlik içerebilecek programlar ve teknolojilere karşı tarar. Bir kök dizin algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri kök dizin olarak yanlış algılanabilir.

Ayrıca, taramak isteyip istemediğinize karar vermelisiniz

- ***Tüm dosya türleri*** , virgülle ayrılmış (*kaydedilirken virgüller noktalı virgüle dönüşür*) dosya uzantıları listesi sağlayarak taramadan hariç tutulacakların taranmaması için tanımlama olasılığı sağlar;

- ***Seçili dosya türleri*** – Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılamayan dosyalar*); ortam dosyaları (*video, ses dosyaları – bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.

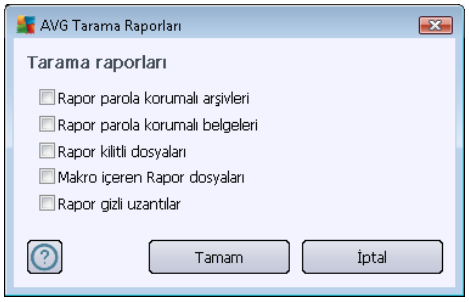
- İsteğe bağlı olarak, ***Uzantıları olmayan dosyaları taramaya*** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

Taramanın ne kadar hızlı tamamlanacağını ayarla

Taramanın ne kadar hızlı tamamlanacağını ayarla bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (*bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir*). Öte yandan tarama süresini uzatarak da sistem kaynaklarının kullanımını azaltabilirsiniz.

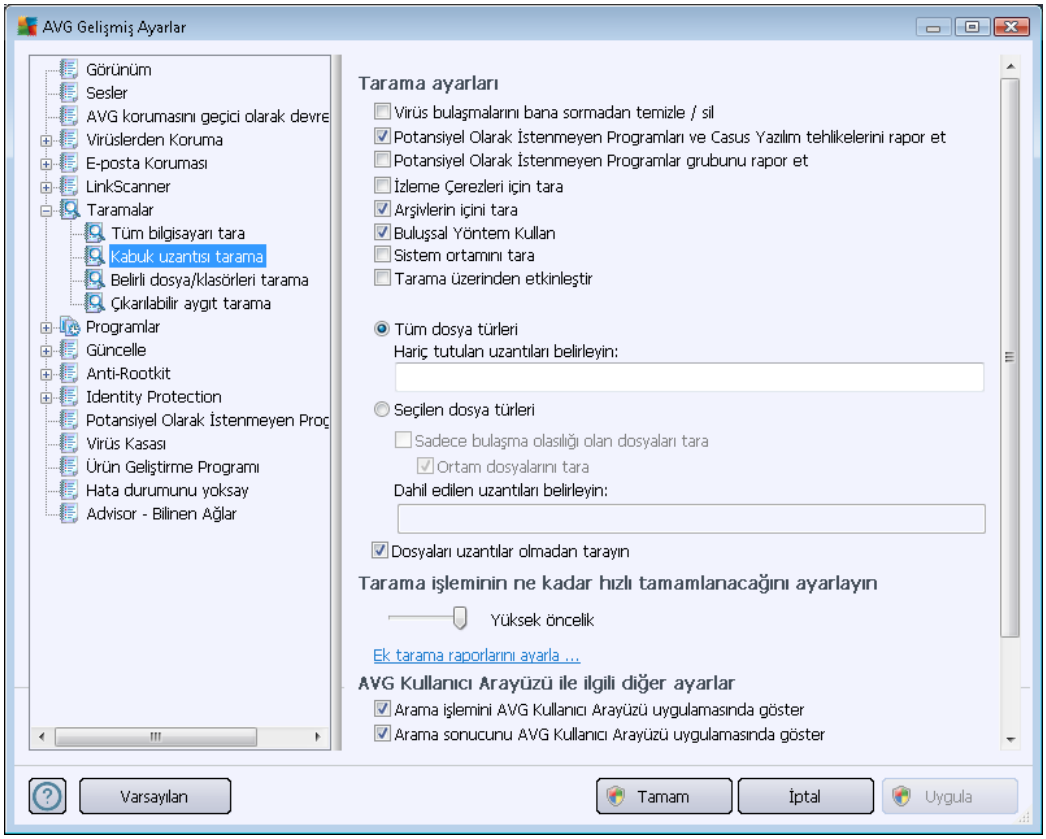
Ek tarama raporlarını ayarla...

Diğer tarama raporlarını belirle... bağlantısına tıklayarak hangi tarama bulgularının rapor edileceğine ilişkin seçimleri yapabileceğiniz ***Tarama raporları*** iletişim kutusu penceresini açabilirsiniz:



10.7.2. Kabuk uzantısı tarama

Daha önce bahsettiğimiz Tüm bilgisayar taraması öğesine benzer olan bu öğe, ***Kabuk uzantı taraması*** olarak adlandırılır, taramayı düzenlemek için yazılım satıcısı tarafından önceden tanımlanmış birkaç seçenek de sunar. Bu sefer, yapılandırma doğrudan Windows Gezgini üzerinden başlatılan belirli nesnelerin taranması esasına dayanmaktadır (*kabuk uzantısı*), Windows Gezgini'nde Tarama bölümüne bakın:



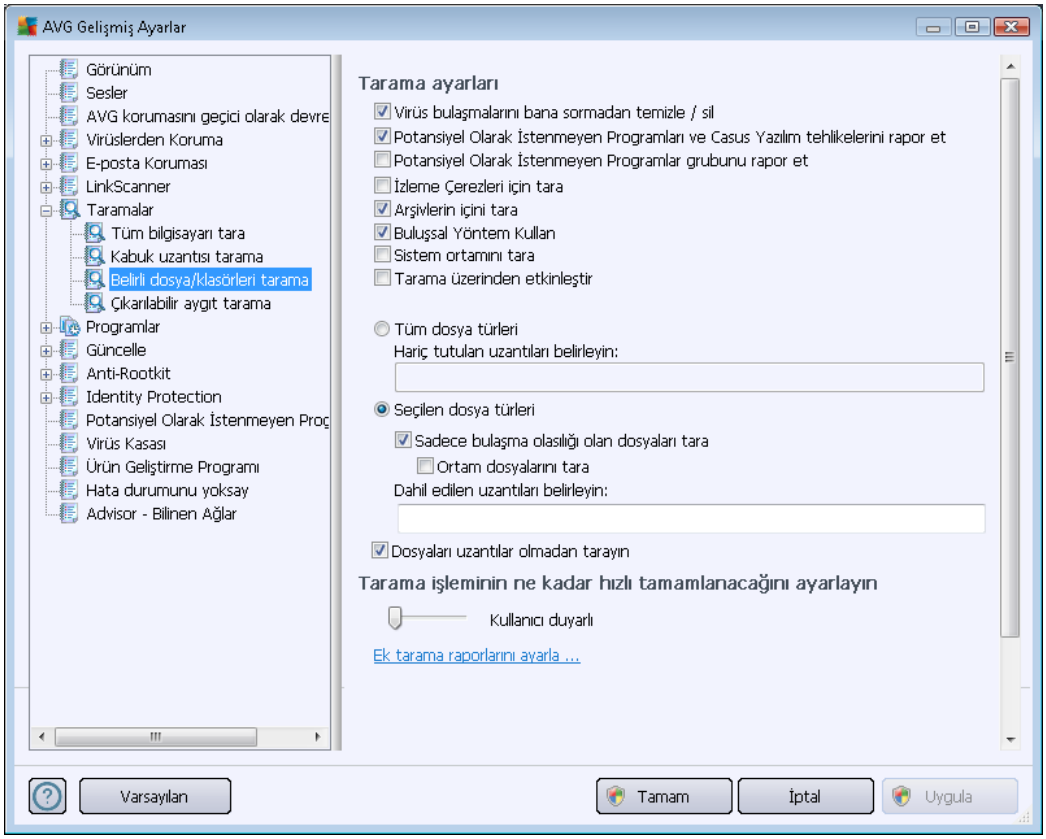
Parametre listesi, Tüm bilgisayarı tarama öğesinin parametre listesi ile aynıdır. Bununla birlikte, varsayılan ayarlar farklılık gösterebilir (*örneğin, Tüm bilgisayarın taranması işlevi arşivleri denetlemez ancak Kabuk Uzantısı Tarama başka bir işlem yaparken sistem ortamını tarar*).

Not: *Belirli parametrelerin açıklaması için, lütfen AVG Gelişmiş Ayarları / Taramalar / Tüm bilgisayarın taranması bölümüne bakın.*

Tüm bilgisayar tarama iletişim kutusuyla karşılaştırıldığında ***Kabuk uzantısı tarama*** iletişim kutusu tarama sürecinde ve tarama sonuçlarında AVG kullanıcı arayüzünden erişilebilir olmasını isteyip istemediğinizi belirleyebileceğiniz ***AVG Kullanıcı Arayüzü ile ilgili diğer ayarlar*** adlı bölümü de içerir. Tarama sırasında bir bulaşma tespit edilmesi durumunda tarama sonucunun görüntülenmesi gerektiğini de tanımlayabilirsiniz.

10.7.3. Belirli dosya/klasörleri tarama

Belirli dosyaları veya klasörleri tara işlevinin düzenleme arayüzü Tüm Bilgisayar Taraması işlevinin düzenleme iletişim kutusu ile aynıdır. Tüm konfigürasyon seçenekleri aynıdır; diğer bir yandan Tüm bilgisayar taraması için varsayılan ayarlar daha kesindir:

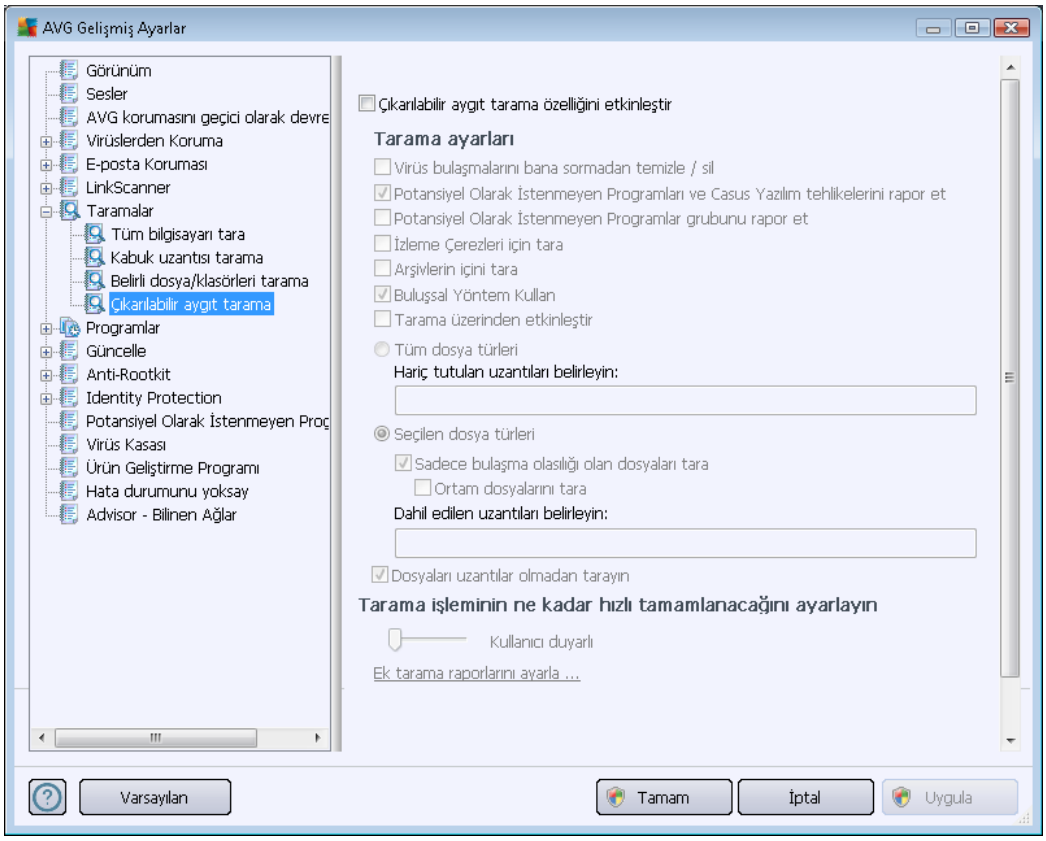


Bu yapılandırma iletişim kutusunda ayarlanan tüm parametreleri Belirli dosya ya da klasörleri tara ile tarama sırasında seçilen alanlar için geçerlidir!

Not: *Belirli parametrelerin açıklaması için, lütfen AVG Gelişmiş Ayarları / Taramalar / Tüm bilgisayarın taranması bölümüne bakın.*

10.7.4. Çıkarılabilir aygıt tarama

Çıkarılabilir aygıt tarama için düzenleme arayüzü de Tüm bilgisayarın taranması düzenleme iletişim kutusu ile aynıdır:



Çıkartılabilir aygıt tarama bilgisayarınıza çıkartılabilir bir aygıt taktığınız anda otomatik olarak başlar. Varsayılan olarak söz konusu tarama işlemi kapalıdır. Diğer bir yandan başlıca bulaşma kaynaklarından biri olduğu için söz konusu çıkartılabilir aygıtların potansiyel tehditlere karşı taranması hayati önem taşımaktadır. Bu tarama özelliğinin istendiği zaman otomatik olarak başlatılacak şekilde hazır bulundurulması için ***Çıkartılabilir aygıt taramayı etkinleştir*** seçeneğini işaretleyin.

Not: *Belirli parametrelerin açıklaması için, lütfen AVG Gelişmiş Ayarları / Taramalar / Tüm bilgisayarın taranması bölümüne bakın.*

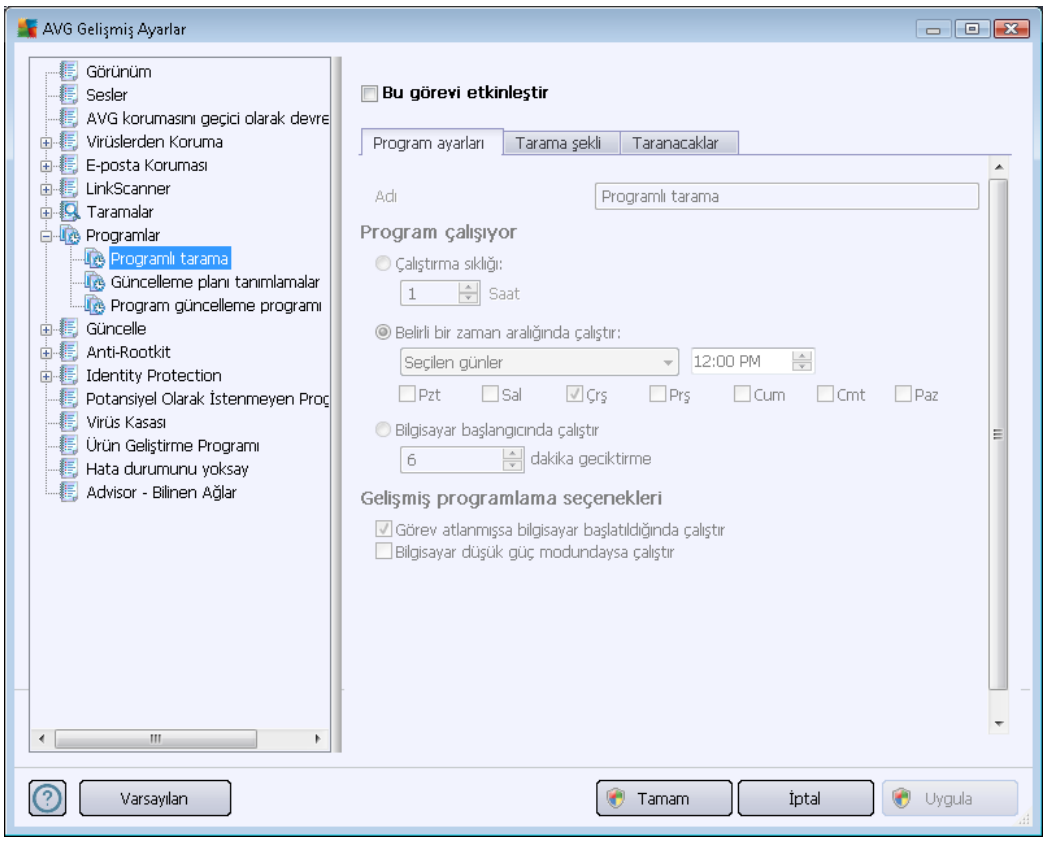
10.8. Programlar

Programlar bölümünde aşağıdaki bileşenlerin öntanımlı ayarlarını düzenleyebilirsiniz:

- Zamanlanan tarama
- Güncelleme planı tanımlamalar
- Program güncelleme programı

10.8.1. Programlı Tarama

Üç sekmede zamanlanan tarama parametreleri düzenlenebilir (*veya yeni bir zamanlama ayarlanabilir*). Her sekmede ***Bu görevi etkinleştir*** öğesini işaretleyerek veya söz konusu öğenin işaretini kaldırarak zamanlanan testi geçici olarak devre dışı bırakabilir ve gerektiğinde yeniden açabilirsiniz:



Daha sonra, ***Ad*** adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcı tarafından atanan ad bulunur. Yeni eklenen zamanlamalar için (*sol gezinti ağacındayken* ***Taramayı programla*** *öğesi üzerinde sağ tıklatarak* yeni bir zamanlama ekleyebilirsiniz) kendi adınızı belirtebilirsiniz ve bu durumda metin alanı düzenleme için açılacaktır. Programladığınız taramaları diğerlerinden kolaylıkla ayırabilmek için her zaman taramalarınıza kısa, açıklayıcı adlar vermeye çalışın.

Örnek: *Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanları taraması" oldukça açıklayıcı bir isim olacaktır. Ayrıca, taramanın adında söz konusu taramanın tam bilgisayar taraması ya da sadece seçilen dosya ya da klasörlerin taranması olup olmadığını belirtmenize gerek yoktur – taramalarınız seçilen dosya ya da klasörleri tara işlevinin farklı şekillerinden ibaret olacaktır.*

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

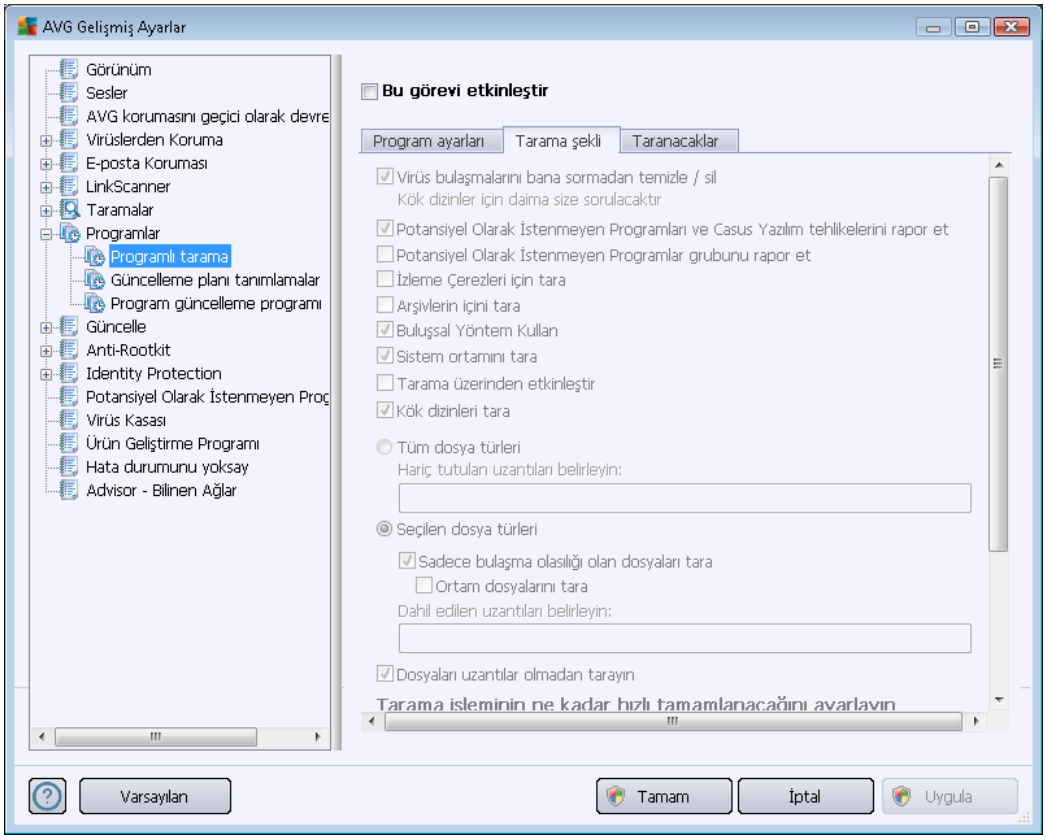
Program çalışıyor

Burada, yeni programlanan tarama başlatması için zaman aralıkları belirtebilirsiniz. Zamanlama belirli bir sürenin ardından tekrarlanan tarama başlatması ile (***Her ...'de bir***) ya da kesin bir tarih ve saat tanımlayarak (***Belirli bir zaman aralığında çalıştır ...***), veya tarama başlangıcıyla ilgili bir olay tanımlanarak (***Bilgisayar başlangıcında çalıştır***) tanımlanabilir.

Gelişmiş zamanlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaysa veya tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/başlatılmaması gerektiğini tanımlamanızı sağlar. Programlanan tarama belirttiğiniz saatte başlatıldığında, AVG sistem tepsisi simgesi üzerinde bir açılır pencere ile bu konuda bilgilendirileceksiniz:

Bunun ardından yeni bir AVG sistem tepsisi simgesi görüntülenir (*üzerinde beyaz bir ok bulunur ve tamamen renklidir*) ve programlanan taramanın başladığını bildirir. Çalışan taramayı duraklatmaya hatta durdurmaya karar verebileceğiniz ve o anda çalışmakta olan taramanın önceliğini değiştirebileceğiniz bağlam menüsü açmak için, çalışan taramayı sağ tıklatın.



Tarama Şekli sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. Varsayılan olarak birçok parametre devreye sokulur ve işlevsellik de tarama sırasında uygulanacaktır. ***Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa öntanımlı konfigürasyonu olduğu gibi muhafaza etmeniz önerilir***:

- ***Bulaşmayı bana sormadan temizle / kaldır*** *(varsayılan olarak açık):* Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne Virüs Kasası'na taşınır.

- ***Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehlikelerini rapor et*** - *(varsayılan olarak açıktır*): Anti-Spyware motorunu etkinleştirmek ve virüslerin yanı sıra birlikte casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- ***Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et*** (*varsayılanda kapalıdır*) – bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

- ***İzleme Tanımlama Bilgilerini Tara*** (*varsayılan olarak kapalıdır*):Anti-Spyware bileşeninin

bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

- ***Arşivleri tara*** - (*varsayılan olarak kapalıdır*): bu parametre, tarama işleminin ZIP, RAR gibi belirli bir arşiv türü ile sıkıştırılmış olsa bile tüm dosyaların taranması gerektiğini tanımlar.

- ***Buluşsal Analiz Yöntemlerini Kullan*** – (*varsayılan olarak açıktır*). Buluşsal analiz yöntemi (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.

- ***Sistem ortamını tara*** - (*varsayılan olarak açıktır*). Tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.

- ***Kapsamlı taramayı etkinleştir*** (*varsayılan olarak kapalı*) belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.

- ***Rootkit'leri tara*** *(varsayılan olarak açık):* Anti-Rootkit taraması bilgisayarınızı olası rootkit'lere, örneğin bilgisayarınızda kötü amaçlı etkinlik içerebilecek programlar ve teknolojilere karşı tarar. Bir kök dizin algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri kök dizin olarak yanlış algılanabilir.

Ayrıca, taramak isteyip istemediğinize karar vermelisiniz

- ***Tüm dosya türleri*** – virgülle ayrılmış (*kaydedilirken virgüller noktalı virgüle dönüşür*) dosya uzantıları listesi sağlayarak taramadan hariç tutulacakların taranmaması için tanımlama olasılığı sağlar;

- ***Seçili dosya türleri*** – Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılamayan dosyalar*); ortam dosyaları (*video, ses dosyaları – bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.

- İsteğe bağlı olarak, ***Uzantıları olmayan dosyaları taramaya*** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

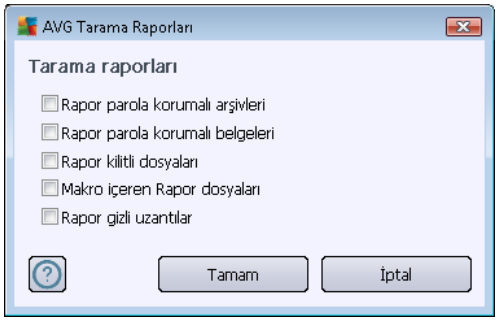
Taramanın ne kadar hızlı tamamlanacağını ayarla

Taramanın ne kadar hızlı tamamlanacağını ayarla bölümünde, sistem kaynakları kullanımına bağlı olarak istediğiniz tarama hızını seçebilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Tarama işleminin daha hızlı ilerlemesini istiyorsanız tarama işlemi daha kısa sürecektir fakat tarama işlemi sırasında sistem kaynakları

oldukça yüklü bir şekilde kullanılacak ve bilgisayar üzerindeki diğer işlemleri yavaşlatacaktır (*bu seçenek bilgisayarınız açıkken kullanılmadığı sırada seçilebilir*). Öte yandan, tarama süresini uzatarak sistem kaynaklarının kullanımını azaltabilirsiniz.

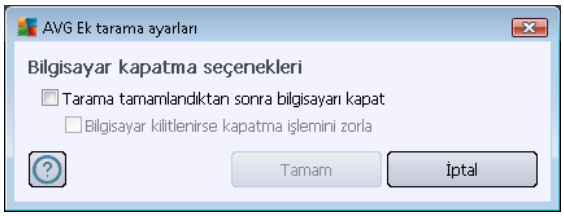
Ek tarama raporlarını ayarla

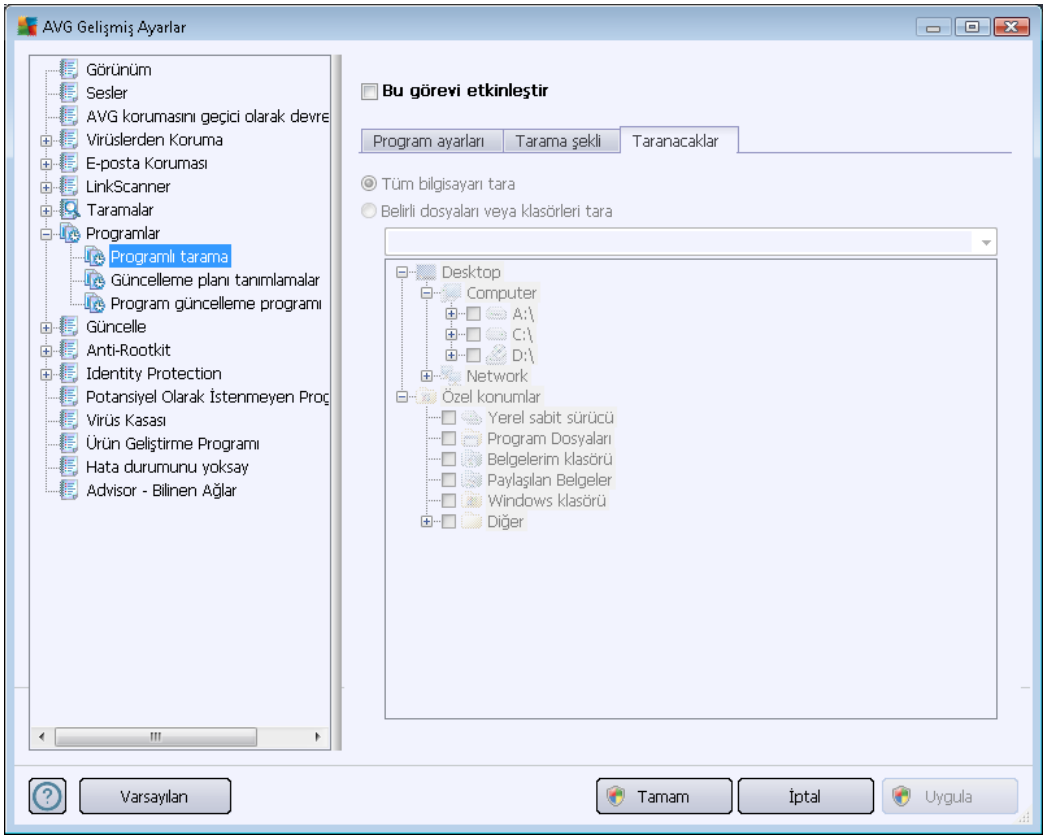
Tarama bulgularının rapor edilmesi gerekip gerekmediğini tanımlamak üzere birden fazla öğeyi ayarlayabileceğiniz ***Tarama raporları*** olarak adlandırılan bağımsız bir iletişim penceresi açmak için ***Ek tarama raporlarını ayarla...*** bağlantısını tıklatın:



Ek tarama ayarları

Ekstra tarama ayarları'na tıklamak yeni bir ***Bilgisayar Kapatma seçenekleri*** iletişim kutusunu açar. Burada tarama işlemi bittikten sonra bilgisayarın otomatik olarak kapanmasını ayarlayabilirsiniz. Bu seçeneği seçerseniz (***Tarama bittikten sonra bilgisayarı kapat***) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (***Bilgisayar kilitliyse bilgisayarı kapanmaya zorla***).

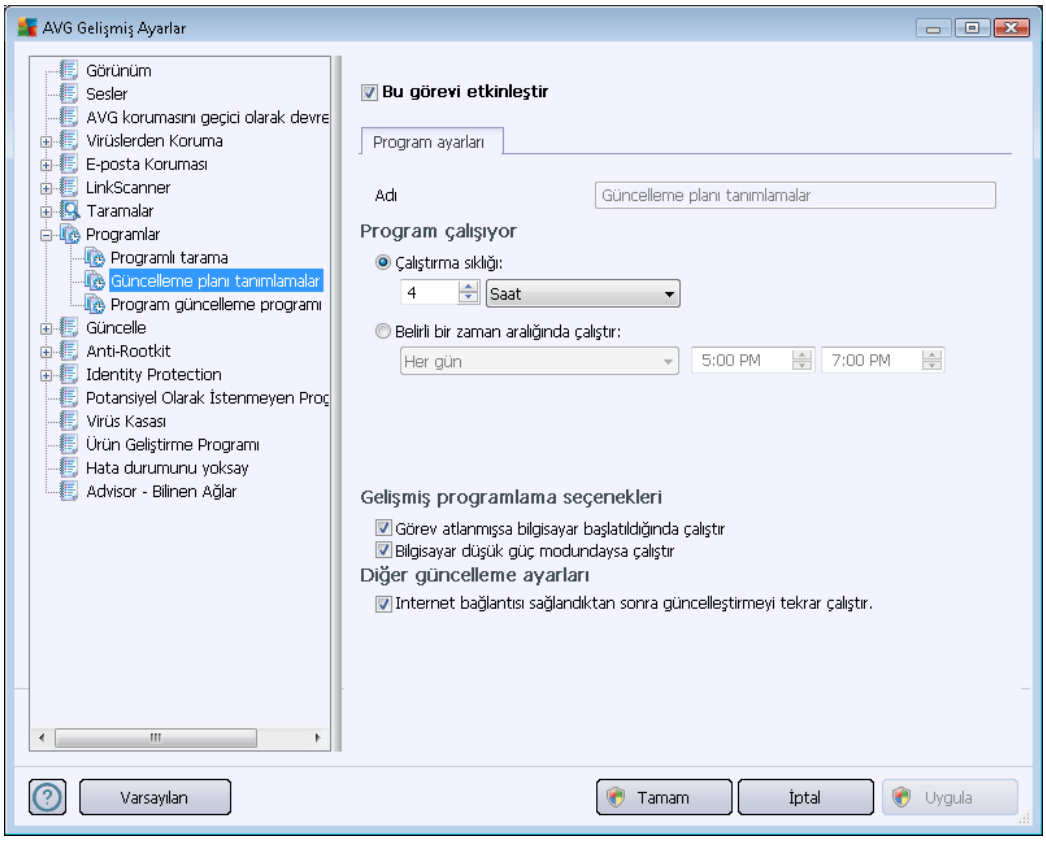




Taranacaklar sekmesinde, tüm bilgisayarı tarama veya belirli dosya veya klasörleri taramayı programlamak isteyip istemediğinizi belirleyebilirsiniz. Belirli dosya ve klasörleri taramayı seçerseniz, bu iletişim penceresinin alt kısmında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri seçebilirsiniz.

10.8.2. Güncelleme Planı Tanımlamalar

Gerçekten gerekliyse Bu görevi etkinleştir öğesinin işaretini kaldırarak zamanlanmış tanımları geçici olarak devre dışı bırakabilir ve daha sonra tekrar açabilirsiniz:



Bu iletişim kutusunda tanımlar güncelleme zamanlaması parametrelerinden bazılarını ayrıntılarıyla yapılandırabilirsiniz. ***Ad*** adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcısı tarafından atanan ad bulunur.

Programlı çalıştırma

Bu bölümde, yeni programlanan tanımlar güncellemesini başlatmak için zaman aralıkları belirtin. Zamanlama, belirli bir süreden sonra (***Çalıştırma sıklığı...***) tekrarlanan güncelleme başlatması olarak veya belirli bir tarih ve saat (***Belirli bir saatte çalıştır...***) tanımlanarak tanımlanabilir.

Gelişmiş programlama seçenekleri

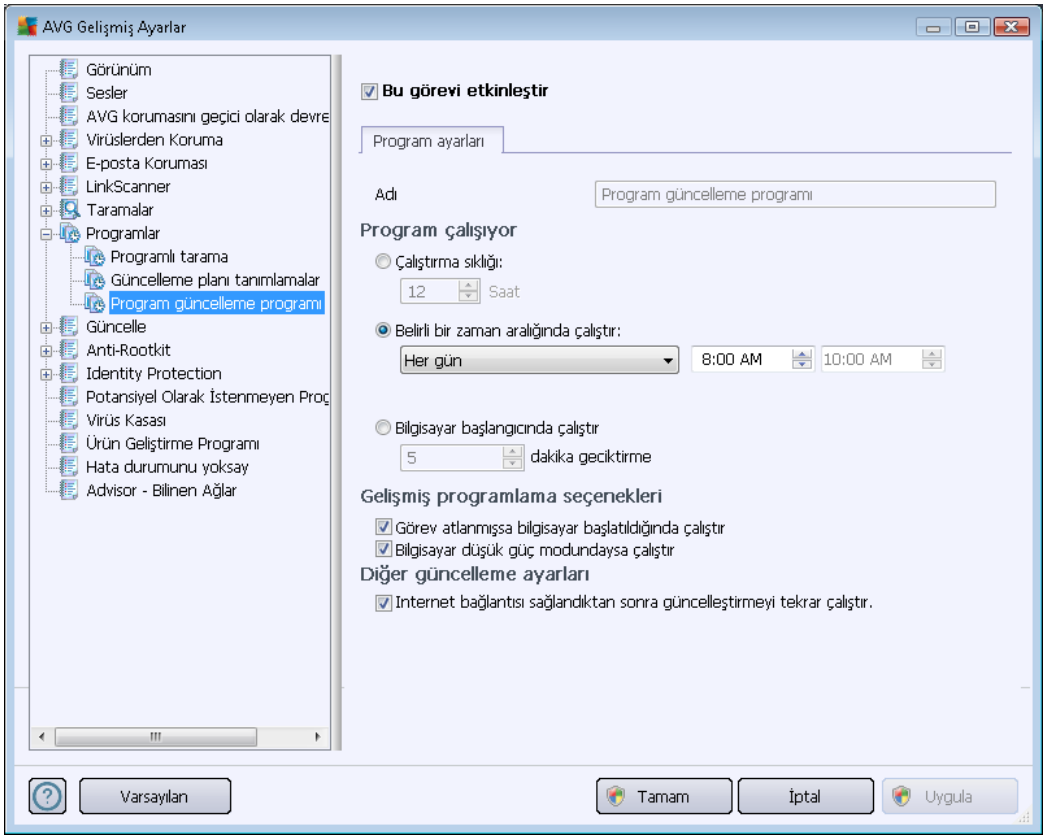
Bu bölümde, bilgisayar düşük güç modundaysa veya tamamen kapatılmışsa hangi koşullar altında tanımlar güncellemesinin başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.

Diğer güncelleme ayarları

Son olarak, ***Internet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır*** seçeneğini işaretleyerek Internet bağlantısı bozulduğunda ve güncelleme işlemi başarısız olduğunda, Internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatıldığından emin olun. Programlı güncelleme işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra AVG sistem tepsisi simgesi üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz (*Gelişmiş Ayarlar/Görünüm iletişim kutusunun varsayılan yapılandırmasını değiştirmemiş olmanız kaydıyla)*.

10.8.3. Program Güncelleme Planı

Gerçekten gerekliyse Bu görevi etkinleştir öğesinin işaretini kaldırarak zamanlanmış programı geçici olarak devre dışı bırakabilir ve daha sonra tekrar açabilirsiniz:



Ad adındaki metin alanında (*tüm varsayılan programlamalar için devre dışı bırakılmış*) bu programlamaya program satıcısı tarafından atanan ad bulunur.

Program çalışıyor

Burada, yeni programlanan program güncellemesinin başlaması için zaman aralıklarını girin. Zamanlama belirli bir sürenin ardından tekrarlanan güncelleme ile (***Her ...'de bir***) ya da kesin bir tarih ve saat tanımlayarak (***Belirli bir saatte çalıştır...***) ya da (***Bilgisayar başlangıcında***) ilgili bir

programın güncellemesiyle tanımlanabilir.

Gelişmiş programlama seçenekleri

Bu bölümde, bilgisayar düşük güç modundaysa veya tamamen kapatılmışsa hangi koşullar altında program güncellemesinin başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.

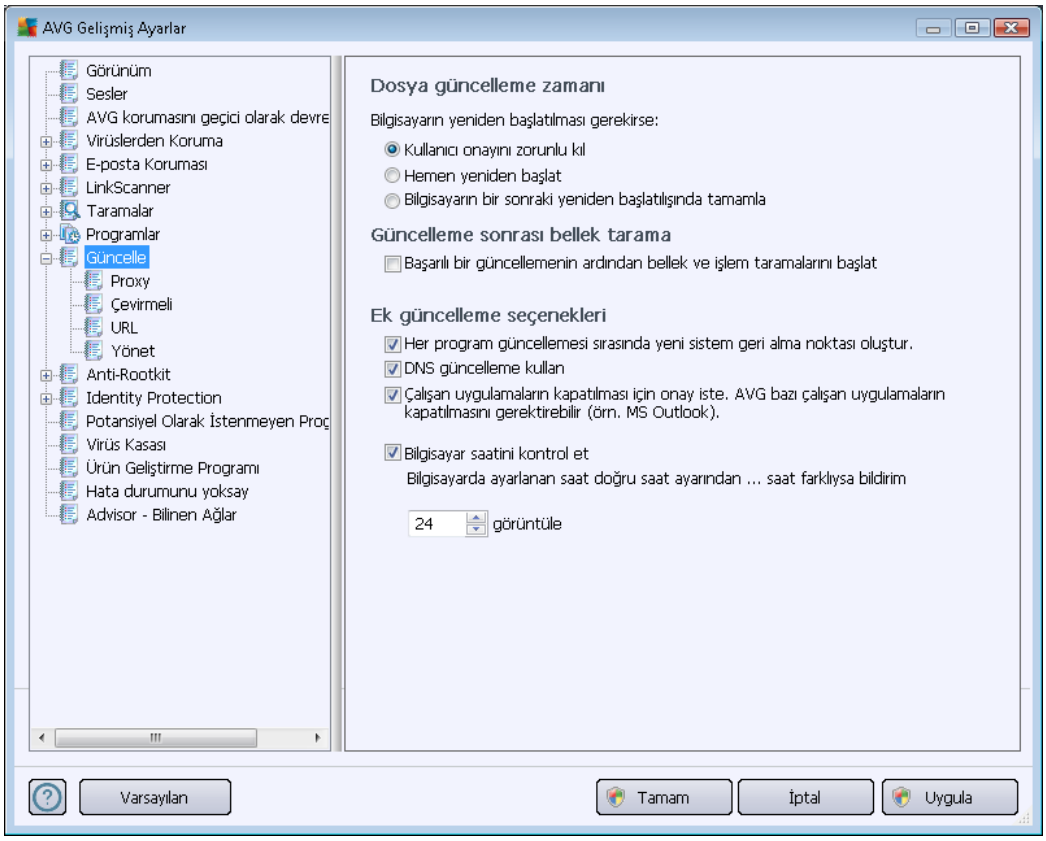
Diğer güncelleme ayarları

Internet bağlantısı kurulduğunda güncellemeyi yeniden çalıştır seçeneğini işaretleyerek Internet bağlantısı bozulduğunda ve güncelleme işlemi başarısız olduğunda, Internet bağlantısı yeniden sağlanır sağlanmaz yeniden başlatıldığından emin olun. Programlı güncelleme işlemi sizin belirlediğiniz tarih ve saatte başladıktan sonra AVG sistem tepsisi simgesi üzerinde açılan bir açılır pencere vasıtasıyla bilgilendirileceksiniz (*Gelişmiş Ayarlar/Görünüm iletişim kutusunun varsayılan yapılandırmasını değiştirmemiş olmanız kaydıyla*).

Not: *Programlanmış bir program güncellemesinin zaman çakışması oluşursa ve programlı tarama gerçekleşirse, güncelleme işlemi daha yüksek önceliğe sahiptir ve tarama kesilir.*

10.9. Güncelleme

Güncelle navigasyonu öğesi, AVG güncellemesine ilişkin genel parametreleri belirleyebileceğiniz yeni bir iletişim kutusu açar:



Dosya güncelleme zamanı

Bu bölümde güncelleme işlemi bilgisayarınızın yeniden başlatılmasını gerektiriyorsa üç seçenek arasından birini belirleyebilirsiniz. Güncellemenin tamamlanması işlemi, bilgisayarınızın bir sonraki yeniden başlatılma sürecine zamanlanabilir veya yeniden başlatma işlemini hemen yapabilirsiniz:

- ***Kullanıcıdan onay iste*** *(varsayılan)* - güncelleme işleminin tamamlanması için gereken bilgisayarın yeniden başlatılması süreci için onayınız istenir
- ***Hemen yeniden başlat*** – güncelleme işlemi tamamlanır tamamlanmaz onayınız istenmeden bilgisayarınız yeniden başlatılacaktır
- ***Bilgisayarın bir sonraki yeniden başlatılmasında tamamla*** – güncelleme işleminin tamamlanması bilgisayarın bir sonraki yeniden başlatılmasına kadar ertelenir. Lütfen bu seçeneğin yalnızca bilgisayarın düzenli olarak (en azından günde bir kez) yeniden başlatıldığını bilmeniz halinde önerildiğini unutmayın!

Güncelleme sonrası bellek tarama

Başarıyla tamamlanan her güncelleme sonrasında yeni bir bellek taraması başlatmak istediğinizi tanımlamak için bu onay kutusunu işaretleyin. En son indirilen güncelleme yeni virüs tanımlarını içerebilir ve bunlar taramaya hemen uygulanır.

Ek güncelleme seçenekleri

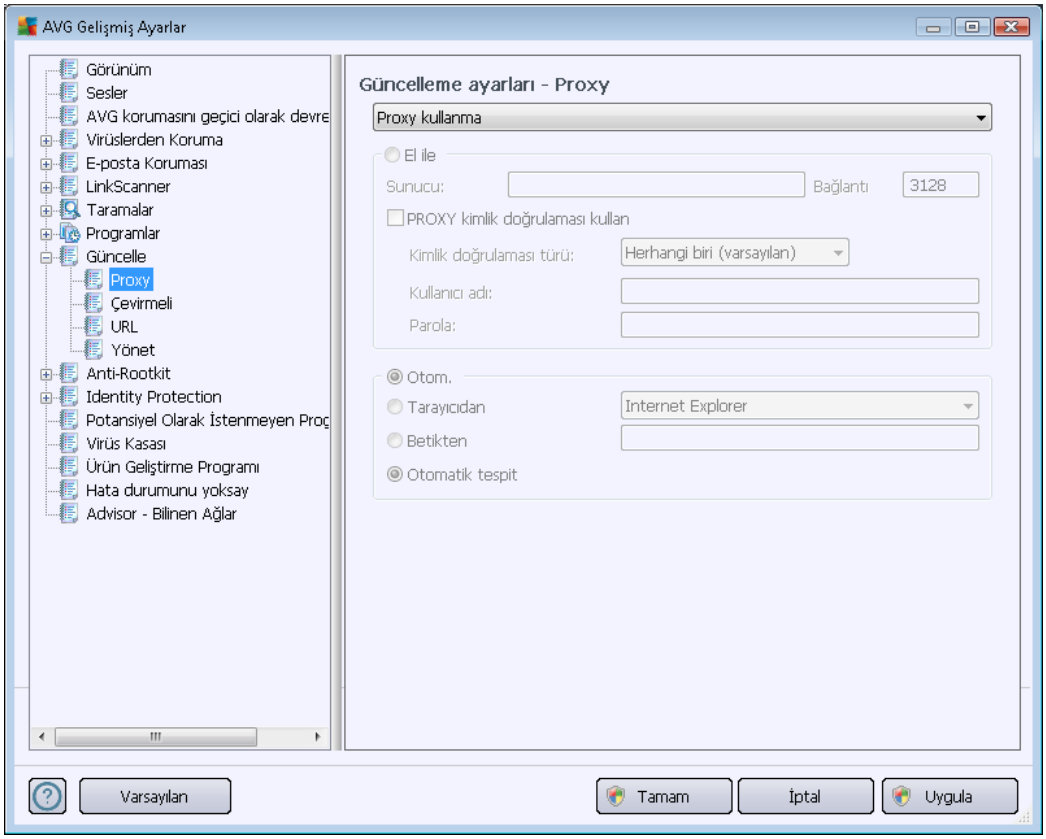
- ***Her program güncellemesinden sonra sistem geri yükleme noktası oluştur*** – AVG programının güncelleme işlemi başlamadan önce her seferinde geri yükleme noktası oluşturulur Güncelleme işleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletme sisteminizi bu noktaya geri döndürebilirsiniz. Bu seçeneğe Başlat/Tüm Programlar bilgisayarınızın günde an az bir kere açıldığından emin olduğunuz durumlarda önerilir/ Donatılar /Sistem Araçları /Sistem Geri Yükleme menüsünden erişebilirsiniz fakat değişikliklerin sadece uzman kullanıcılar tarafından yapılması önerilmektedir. Bu fonksiyonu kullanmak istiyorsanız bu kutucuğu işaretleyin.

- ***DNS güncellemesini kullan*** (*varsayılan olarak açıktır*) – bu öğe işaretlendiğinde güncelleme işlemi başlatıldığında **AVG Anti-Virus** en yeni veritabanı sürümüyle ve DNS sunucusundaki en yeni program sürümüyle ilgili bilgileri arar. Yalnızca en küçük, kesin olarak gerekli güncelleme dosyaları indirilir ve uygulanır. Bu şekilde, indirilen toplam veri miktarı en düşük seviyede tutulur ve güncelleme süreci daha hızlı bir şekilde gerçekleştirilir.

- ***Çalışan uygulamaları kapatmak için onay iste*** (*varsayılan olarak açıktır*) güncelleme işleminin tamamlanması için gerekirse izniniz olmaksızın geçerli olarak çalışan uygulamaların kapatılmamasını sağlayacaktır.

- ***Bilgisayar saatini kontrol et*** – Bilgisayar saati ile doğru saat arasındaki fark belirlenen süreden uzun olduğunda bilgilendirilmek isterseniz bu seçeneği işaretleyin.

10.9.1. Proxy



Proxy sunucusu, İnternet'e daha güvenli bir şekilde bağlanmanızı sağlayan bağımsız bir sunucu ya da bilgisayarınızda çalışan bir hizmet programıdır. Belirlenen ağ kuralları doğrultusunda, İnternet'e doğrudan ya da bir proxy sunucusu üzerinden ulaşabilirsiniz; aynı anda her iki işleme de izin verilir. Bunun ardından ***Güncelleme ayarları – Proxy*** iletişim kutusunun ilk öğesinden aşağıdaki seçimleri yapmanız gerekmektedir:

- ***Proxy kullan***
- ***Proxy kullanma*** – varsayılan ayarlar
- ***Proxy kullanarak bağlanmayı dene; başarısız olursa doğrudan bağlan***

Proxy sunucusunu kullanan herhangi bir seçeneği seçerseniz daha ayrıntılı bilgi girmeniz istenecektir. Sunucu ayarları manüel ya da otomatik olarak yapılandırılabilir.

Manüel yapılandırma

Manüel yapılandırmayı seçerseniz (ilgili iletişim kutusu bölümünü etkinleştirmek için ***Manüel seçeneğini işaretleyin***) aşağıdaki bilgileri girmeniz gerekir:

- ***Sunucu*** – sunucunun IP adresini ya da sunucunun adını girin

- ***Bağlantı Noktası*** – İnternet erişimine açık bağlantı noktasının numarasını girin (*varsayılan olarak bu değer 3128 olarak atanmıştır fakat isteğiniz doğrultusunda değiştirebilirsiniz – emin değilseniz lütfen ağ yöneticiniz ile irtibat kurun*)

Proxy sunucusunda her kullanıcı için farklı kurallar yapılandırılabilir. Proxy sunucunuz bu şekilde yapılandırılmış ise proxy sunucusu üzerinden yapılan İnternet bağlantınıza ilişkin kullanıcı adı ve parolanızı onaylamak için ***PROXY kimlik doğrulamasını kullan*** seçeneğini işaretleyin.

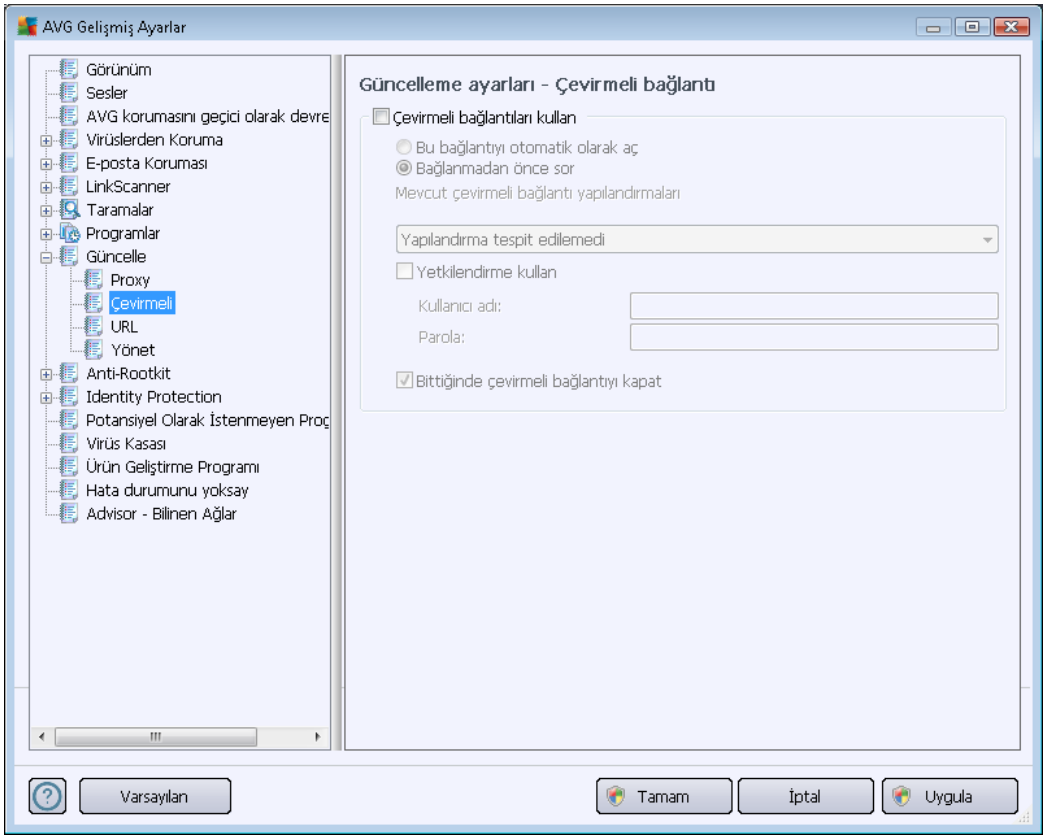
Otomatik yapılandırma

Otomatik yapılandırmayı seçerseniz (*ilgili iletişim kutusunu etkinleştirmek için **Oto** seçeneğini işaretleyin*) ardından proxy yapılandırmasının nereden alınacağını belirleyin:

- ***Tarayıcıdan*** - Yapılandırma varsayılan Internet tarayıcınızdan okunacaktır
- ***Komut satırından*** – yapılandırma, proxy adresine dönme fonksiyonu olan indirilmiş bir komut satırından okunacaktır
- ***Otomatik Tespit Et*** – yapılandırma otomatik olarak doğrudan proxy sunucusundan tespit edilecektir

10.9.2. Çevirmeli

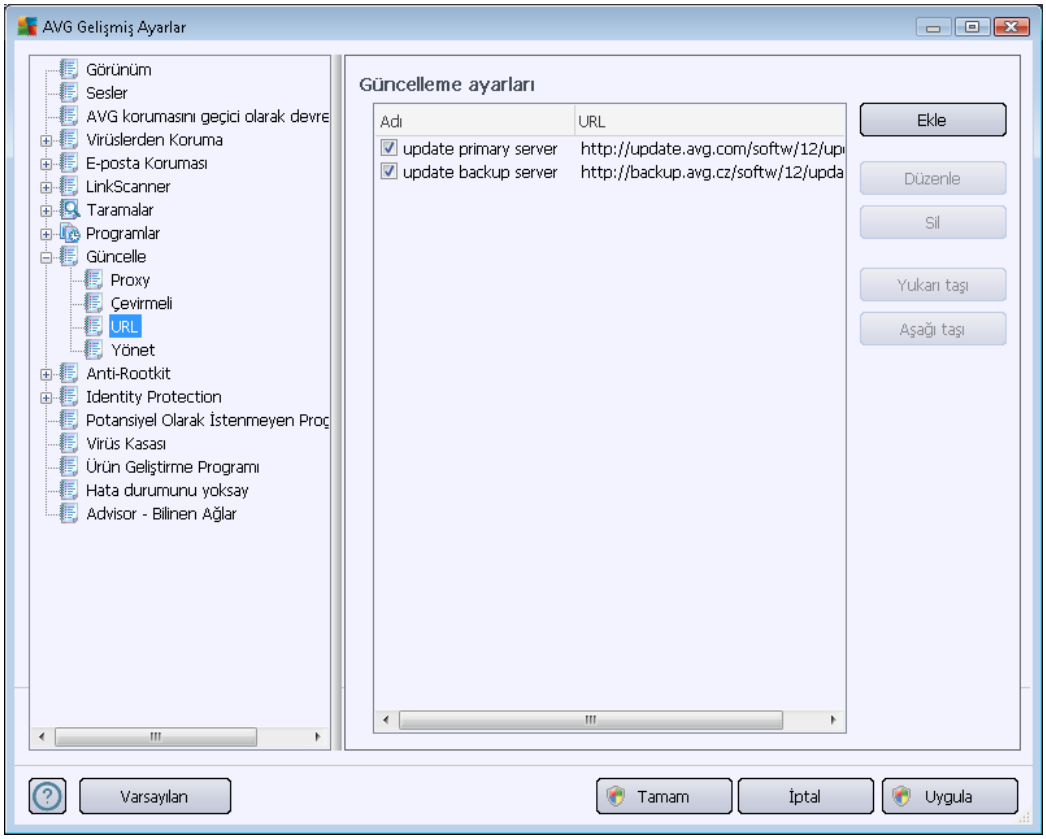
İsteğe bağlı olarak ***Güncelleme ayarlarında tanımlanan tüm parametreler – Çevirmeli Bağlantı*** iletişim kutusu Internet'e çevirmeli bağlantı ile bağlanılmasına ilişkindir. ***Çevirmeli bağlantı kullan*** seçeneği seçilip alanlar etkinleştirilene kadar iletişim kutusunun alanları pasif olacaktır:



İnternet'e otomatik olarak bağlanmak isteyip istemediğinizi (***Bu bağlantıyı otomatik olarak aç***) ya da bağlantıyı her seferinde manüel olarak kurmak isteyip istemediğinizi (***Bağlanmadan önce sor***) seçin. Otomatik bağlantılarda güncellemenin tamamlanmasının ardından bağlantının kesilmesini isteyip istemediğinizi de seçin (***Tamamlandığı zaman çevirmeli bağlantıyı kes***).

10.9.3. URL

URL iletişim kutusunda güncelleme dosyalarının indirilebileceği bir dizi internet adresi bulunur:



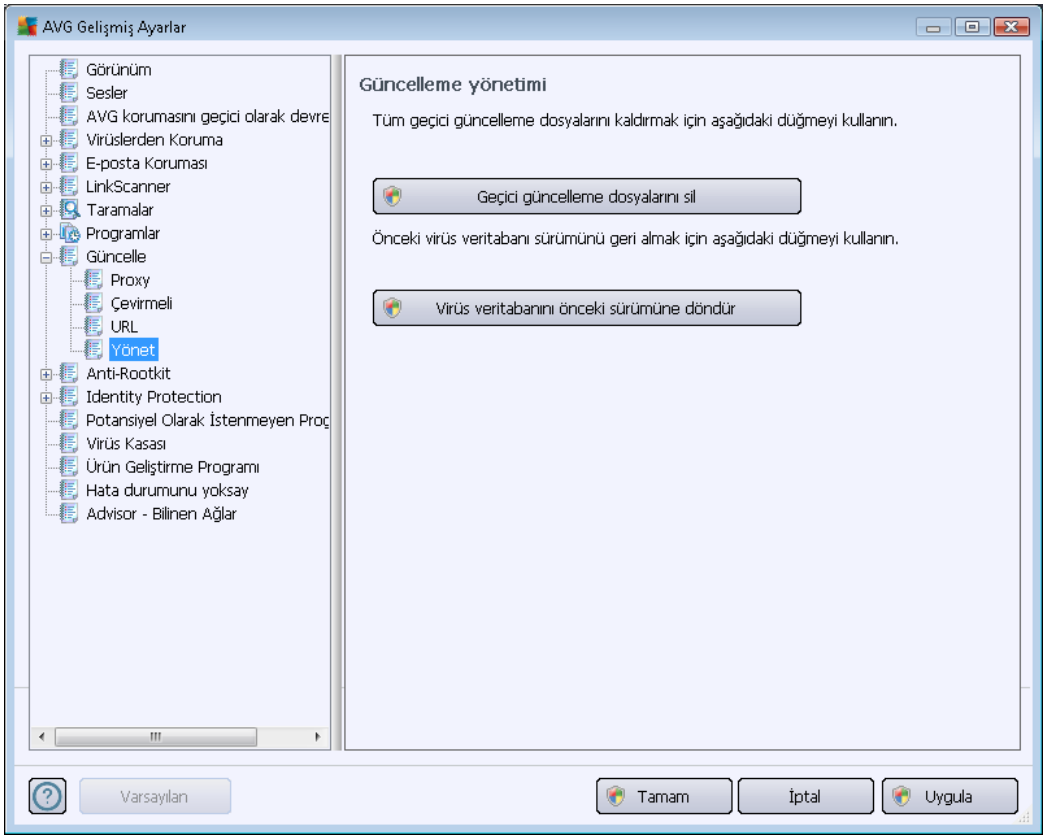
Kontrol düğmeleri

Liste ve liste öğeleri aşağıdaki kontrol düğmeleri kullanılarak düzenlenebilir:

- ***Ekle*** – Listenize yeni bir URL eklemek için kullanacağınız iletişim kutusunu açar
- ***Düzenle*** - seçilen URL parametrelerini düzenleyebileceğiniz iletişim kutusunu açar
- ***Sil*** – seçilen URL'yi listeden seçer
- ***Yukarı Taşı*** – seçilen URL'yi listede bir sıra yukarı taşır
- ***Aşağı Taşı*** – seçilen URL'yi listede bir sıra aşağı taşır

10.9.4. Yönetme

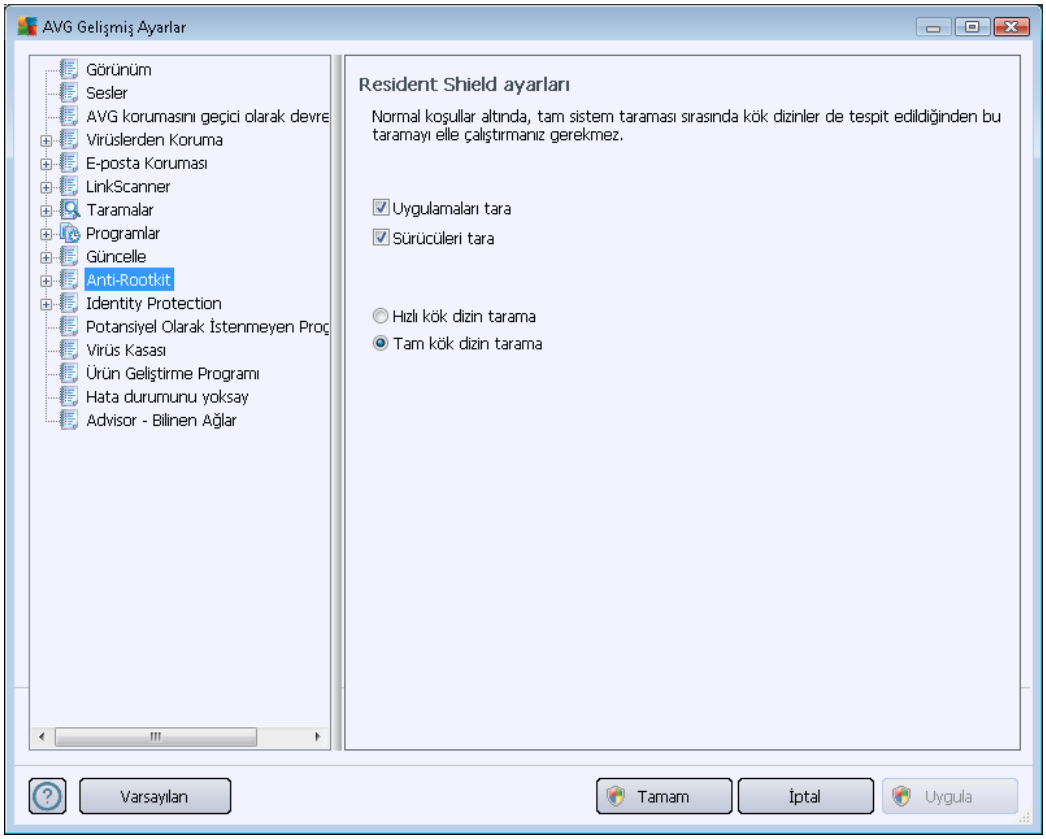
Güncelleme yönetimi iletişim kutusu, iki adet düğme ile ulaşılabilen iki seçenek sunmaktadır:



- ***Geçici güncelleme dosyalarını sil*** - tüm gereksiz güncelleme dosyalarını sabit diskinizden silmek için bu düğmeye basın (*öntanımlı olarak söz konusu dosyalar 30 gün boyunca saklanır*)
- ***Virüs veritabanını bir önceki sürüme döndür*** - En güncel virüs veritabanını sabit diskinizden silmek ve daha önce kaydedilmiş sürüme dönmek için bu düğmeye basın (*yeni virüs tabanı sürümü, bir sonraki güncellemenin bir parçası olacaktır*)

10.10. Anti-Rootkit

Anti-Rootkit ayarları iletişim kutusunda Anti-Rootkit bileşeninin yapılandırmasını ve anti-rootkit taramasının belirli parametrelerini düzenleyebilirsiniz. Anti-rootkit taramasıTüm Bilgisayar Taraması dahilindeki varsayılan bir işlemdir:



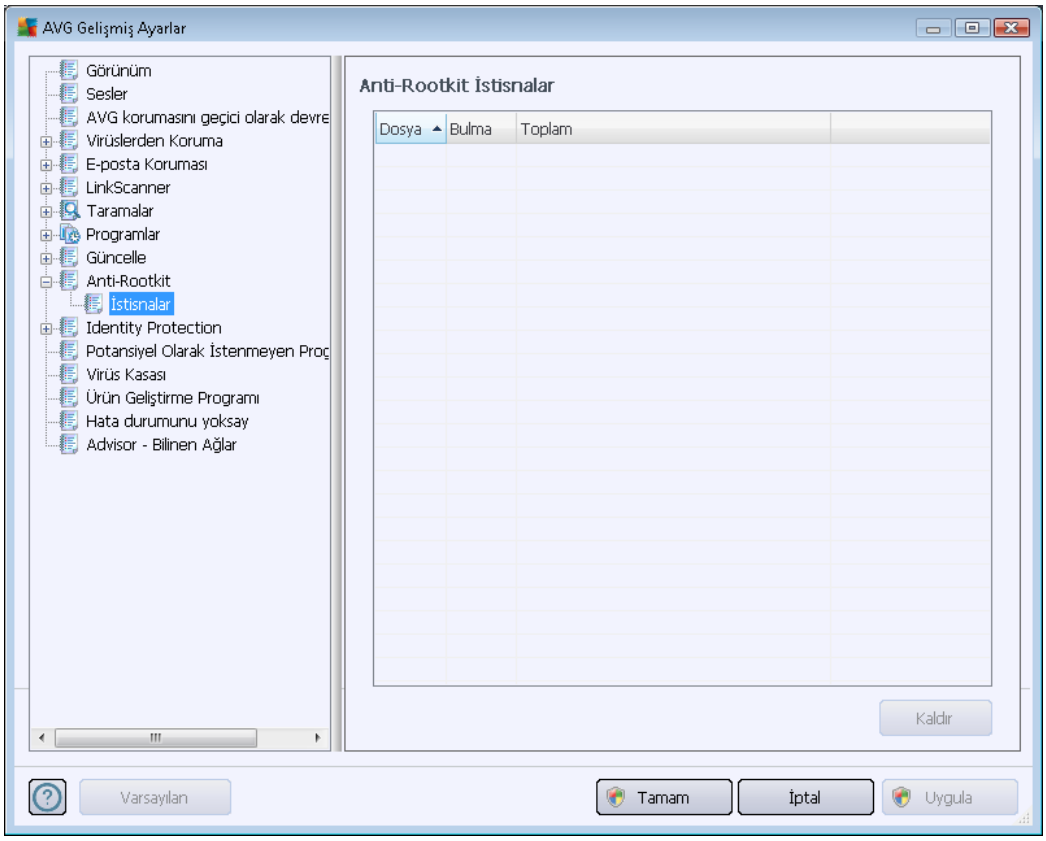
İletişim kutusu içinde sağlanan Anti-Rootkit bileşeninin tüm işlevlerinin düzenlenmesine Anti-Rootkit bileşeninin arayüzünden de ulaşabilirsiniz.

Tarama uygulamaları ve ***Tarama sürücüleri*** anti-rootkit taramasına nelerin dahil edileceğini ayrıntılı şekilde belirlemenize olanak tanır. Bu ayarlar gelişmiş kullanıcılara yöneliktir; tüm seçenekleri açık konumda tutmanızı öneririz. Bunun ardından kök dizin tarama modunu da seçebilirsiniz:

- ***Hızlı kök dizin tarama*** – çalışan tüm işlemleri, yüklü sürücüleri ve sistem klasörlerini (*genellikle c:\Windows*) tarar
- ***Tam kök dizin tarama*** – çalışan tüm işlemleri, yüklü sürücüleri, sistem klasörünü (*genellikle c:\Windows*), ayrıca tüm yerel diskleri (*flash disk dahil, ancak disket/CD sürücüleri hariç*) tarar

10.10.1. İstisnalar

Anti-Rootkit İstisnaları iletişim kutusunda belirli dosyaları bu taramanın dışında tutulması için belirleyebiliriniz *(örneğin yanlışlıkla kök dizin olarak silinebilecek bazı sürücüler)*:

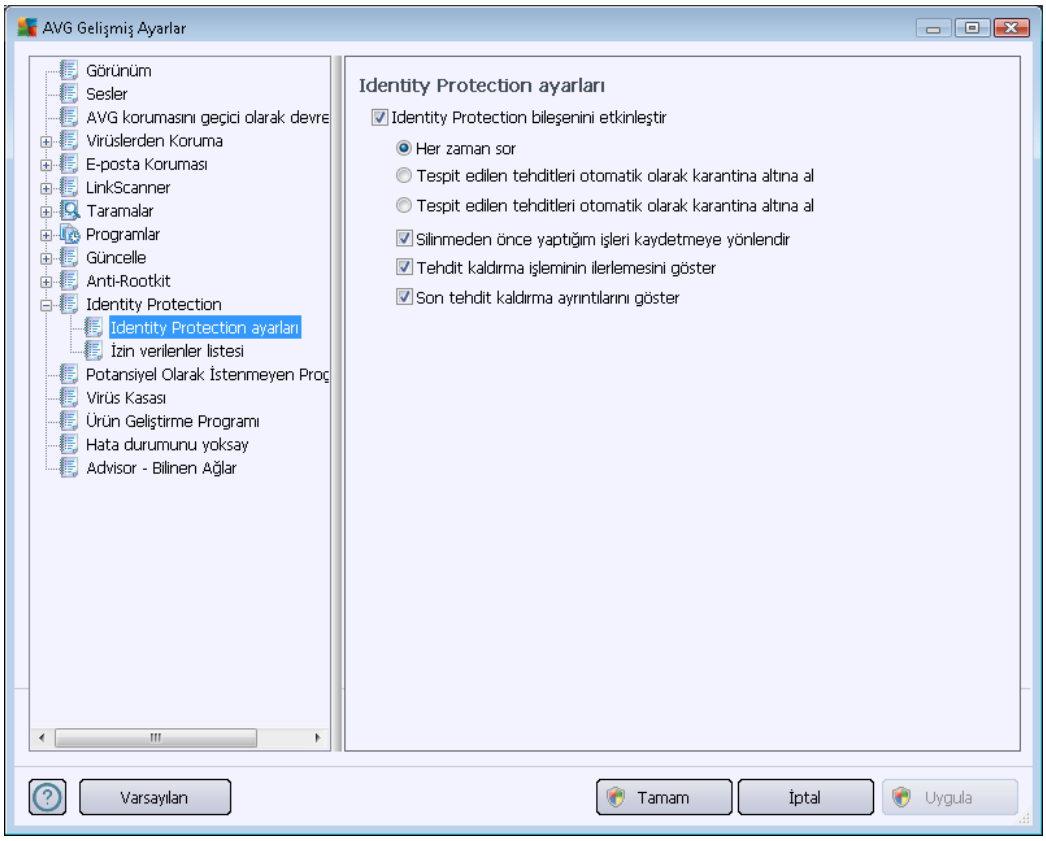


10.11. Identity Protection

Kimlik Koruması davranışsal teknolojiler ve yeni virüslere karşı sıfır gün koruması kullanarak sizi tüm kötü amaçlı yazılımlardan (*casus yazılım, robotlar, kimlik hırsızlığı, ...*) koruyan bir kötü amaçlı yazılımlara karşı koruma bileşenidir *(bileşenlerin işlevleri hakkında ayrıntılı bilgi için lütfen Kimlik Koruması bölümüne bakın*).

10.11.1. Identity Protection Ayarları

Kimlik Koruması ayarları iletişim kutusu Kimlik Koruması bileşeninin temel özelliklerini açmanızı/kapatmanızı sağlar:



Kimlik Korumasını Etkinleştir (*varsayılanda açıktır*) – Kimlik Koruması bileşenini kapatmak için işaretleyin.

Zorunlu olmadıkça, bu işareti kaldırmamanızı önemle tavsiye ederiz!

Identity Protection etkinleştirildiğinde, bir tehlike algılandığında ne yapacağınızı belirtebilirsiniz:

- ***Her zaman sor*** (*varsayılan olarak açıktır*) - bir tehlike algılandığında, çalıştırmak istediğiniz bir uygulamanın kaldırılmamasından emin olmak için karantinaya alınması gerekip gerekmediği size sorulacaktır.
- ***Algılanan tehlikeleri otomatik olarak karantinaya al*** – Algılanan tüm olası tehlikelerin Virüs Kasası güvenilir alanına hemen taşınmasını istediğinizi tanımlamak için bu onay kutusunu işaretleyin. Varsayılan ayarlarda, bir tehlike algılandığında, çalıştırmak istediğiniz hiçbir uygulamanın kaldırılmaması için size uygulamanın karantinaya alınması gerekip gerekmediği sorulacaktır.
- ***Bilinen tehlikeleri otomatik olarak karantinaya al*** – kötü amaçlı yazılım olasılığı algılanan tüm uygulamaların otomatik olarak ve hemen Virüs Kasası'na alınmasını istiyorsanız bu öğeyi işaretli bırakın.

Ayrıca, belirli öğeleri isteğe bağlı olarak etkin daha fazla Identity Protection işlevlerine atayabilirsiniz:

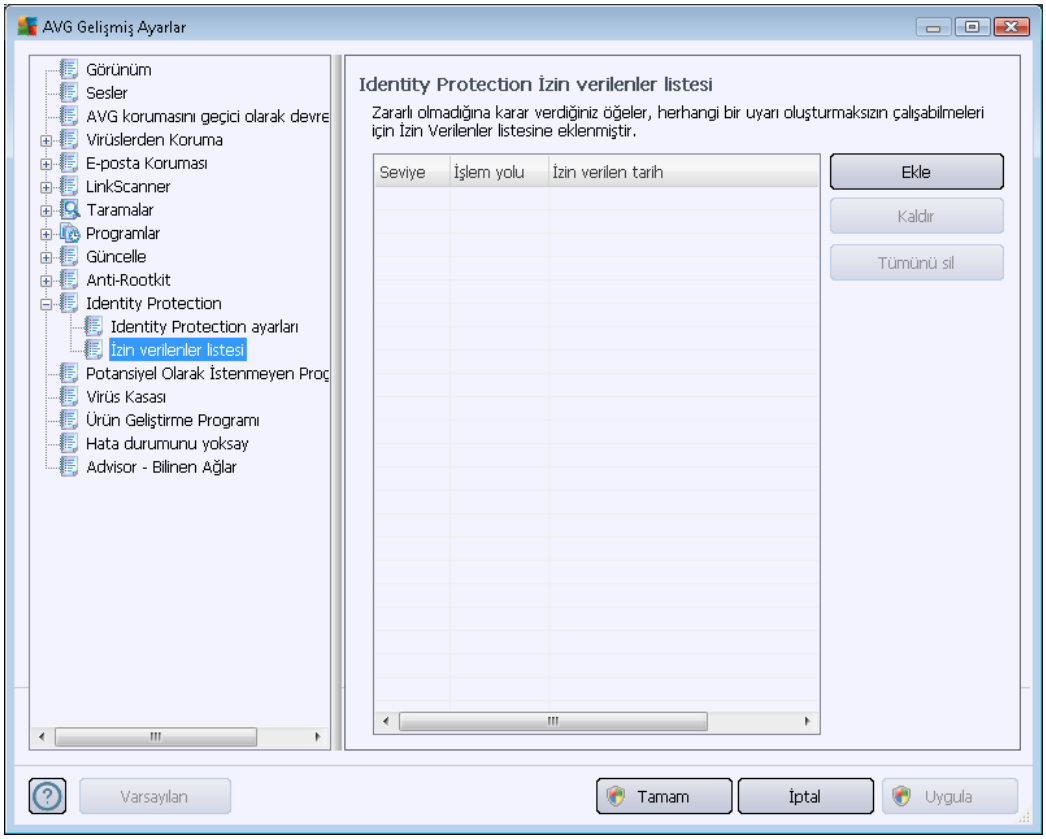
- ***Kaldırmadan önce işi kaydetmek isteyip istemediğimi sor*** - (*varsayılan olarak açık*) – olası kötü amaçlı yazılım olarak algılanan uygulama karantinaya alınmadan önce uyarılmak istiyorsanız bu öğeyi işaretli bırakın. Uygulamayı çalıştırmak istiyorsanız, projeniz kaybolabilir ve önce kaydetmeniz gerekir. Varsayılan olarak, bu öğe açıktır ve böyle kalmasını önemle öneririz.

- ***Tehdidin kaldırılma ilerlemesini göster*** - (*varsayılan olarak açık*) – bu öğe açıkken, kötü amaçlı bir yazılım algılandığında, kötü amaçlı yazılımın karantinaya alınma işlemini gösteren yeni bir iletişim kutusu açılır.

- ***Son tehdit kaldırma ayrıntılarını göster*** - (*varsayılan olarak açık*) – bu öğe açıkken, ***Kimlik Koruması***, karantinaya kaldırılan her nesne hakkında ayrıntılı bilgi görüntüler (*güvenlik seviyesi, konum vb.*).

10.11.2. İzin Verilenler Listesi

Kimlik Koruması ayarları iletişim kutusu içinde ***Algılanan tehlikeleri otomatik olarak karantinaya al*** öğesinin işaretini kaldırmaya karar verirseniz, tehlikeli olabilecek bir kötü amaçlı yazılım her algılandığında, kaldırmak isteyip istemeyeceğiniz sorulacaktır. Şüpheli uygulamayı (*davranışına göre algılandı*) güvenli olarak atarsanız ve bilgisayarınızda kalmasını onaylarsanız, uygulama ***Kimlik Koruması İzin Verilenler listesi*** olarak adlandırılan listeye eklenecek ve bir daha potansiyel olarak tehlikeli şeklinde bildirilmeyecektir:



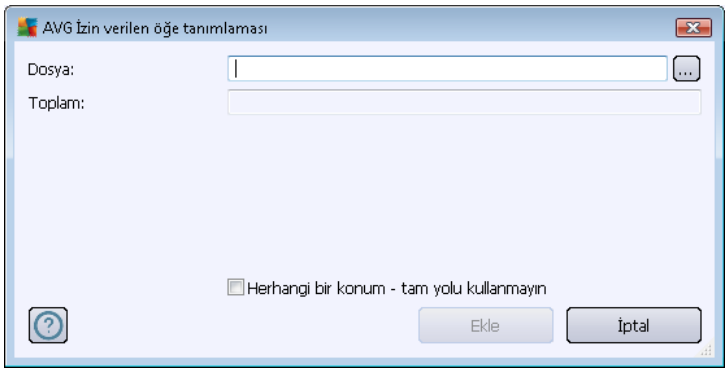
Kimlik Koruması İzin Verilenler listesi her uygulamada aşağıdaki bilgileri sağlar:

- ***Seviye*** – ilgili sürecin önem derecesinin en düşükten (■□□□) en kritiğe (■■■■) dört seviyeli ölçekte grafiksel olarak tanımlanmasıdır
- ***İşlem yolu*** - uygulamanın (*süreç*) çalıştırılabilir dosya konumuna götüren yoldur
- ***İzin tarihi*** – uygulamayı elle güvenli olarak atadığınız tarihtir

Kontrol düğmeleri

Kimlik Koruması İzin Verilenler listesi iletişim kutusu içerisinde bulunan kontrol düğmeleri şunlardır:

- ***Ekle*** - izin verilenler listesine yeni bir uygulama eklemek için bu düğmeye basın. Aşağıdaki iletişim kutusu açılır:

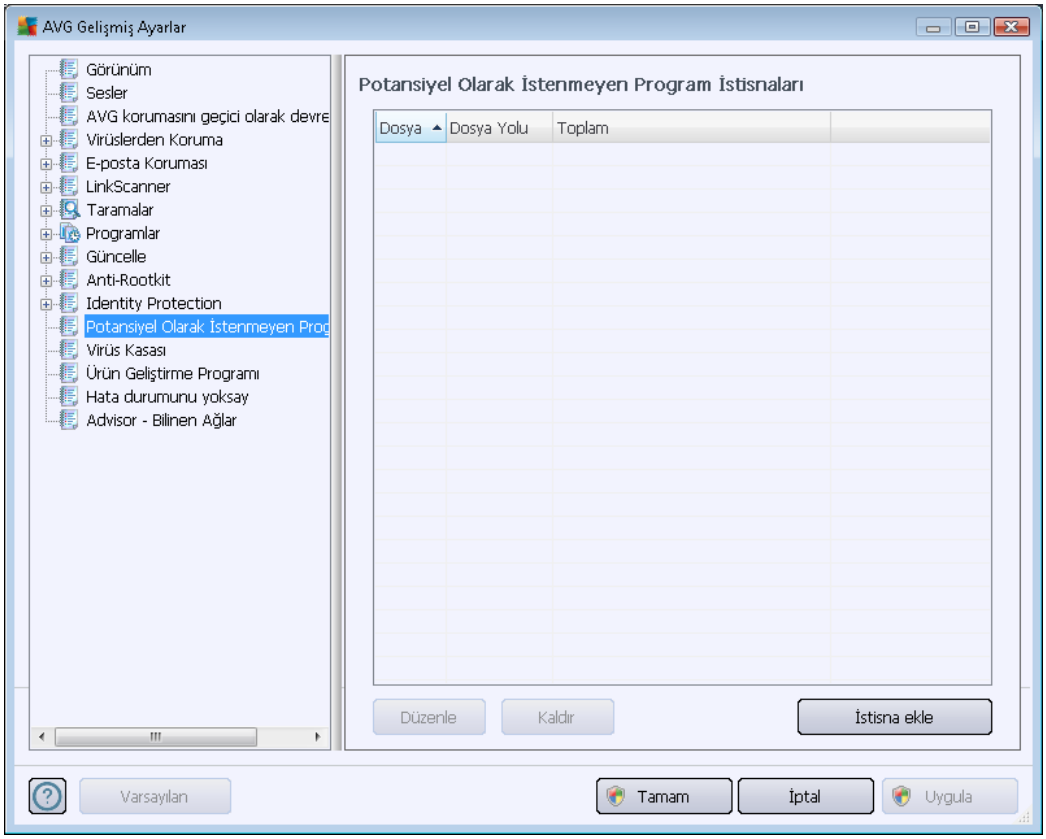


  - ***Dosya*** – istisna olarak işaretlemek istediğiniz dosyanın (*uygulama*) tam yolunu yazın
  - ***İmzayı Kontrol Et*** – seçilen dosyanın benzersiz 'imzasını' görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter dizeleridir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.
  - ***Herhangi bir yerde – tam yolu kullanmayın*** – bu dosyayı sadece belirli bir konumda istisna olarak atamak istiyorsanız bu onay kutusunu işaretlemeden bırakın
- ***Kaldır*** - seçili uygulamayı listeden kaldırmak için basın
- ***Tümünü kaldır*** - listelenen tüm uygulamaları kaldırmak için basın

10.12. Potansiyel Olarak İstenmeyen Programlar

AVG Anti-Virus, bunun yanı sıra sistemde potansiyel anlamda istenmeyen çalıştırılabilir uygulamaları ya da DLL kütüphanelerini de inceleyebilmekte ve tespit edebilmektedir. Bazı durumlarda kullanıcı belirli istenmeyen programların (bilerek yüklenen programlar) bilgisayarında bulunmasını tercih edebilir. Bunlardan bazıları reklam yazılımları ve özellikle ücretsiz yazılımlardır. Bu

tür reklam yazılımları **AVG Anti-Virus** tarafından *potansiyel olarak istenmeyen program* olarak tespit edilip raporlanabilir. Söz konusu programın bilgisayarınızda bulunmasını istiyorsanız ilgili programı, potansiyel olarak istenmeyen program istisnası şeklinde atayabilirsiniz:



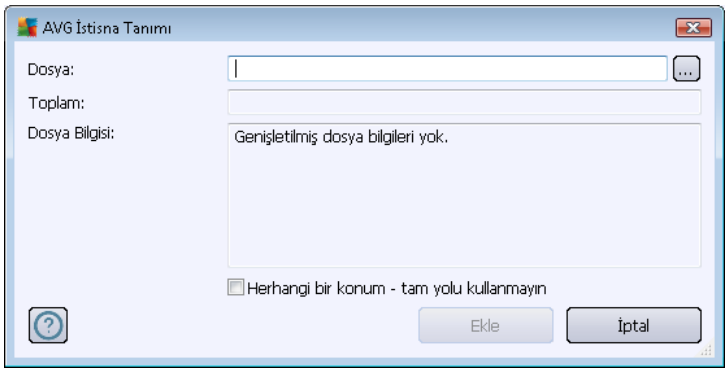
Potansiyel Olarak İstenmeyen Program İstisnaları iletişim kutusunda, potansiyel olarak istenmeyen programlardan tanımlanan ve mevcut durumda geçerli istisnalar bulunmaktadır. Listeyi düzenleyebilir, varolan öğeleri silebilir veya yeni istisnalar ekleyebilirsiniz. Aşağıdaki bilgiler her bir istisna için listede bulunabilir:

- ***Dosya*** - İlgili uygulamanın tam adını sağlar
- ***Dosya Yolu*** - Uygulamanın konumuna olan yolu gösterir
- ***İmzayı Kontrol Et*** – seçilen dosyanın 'imzasını' görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter dizeleridir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.

Kontrol düğmeleri

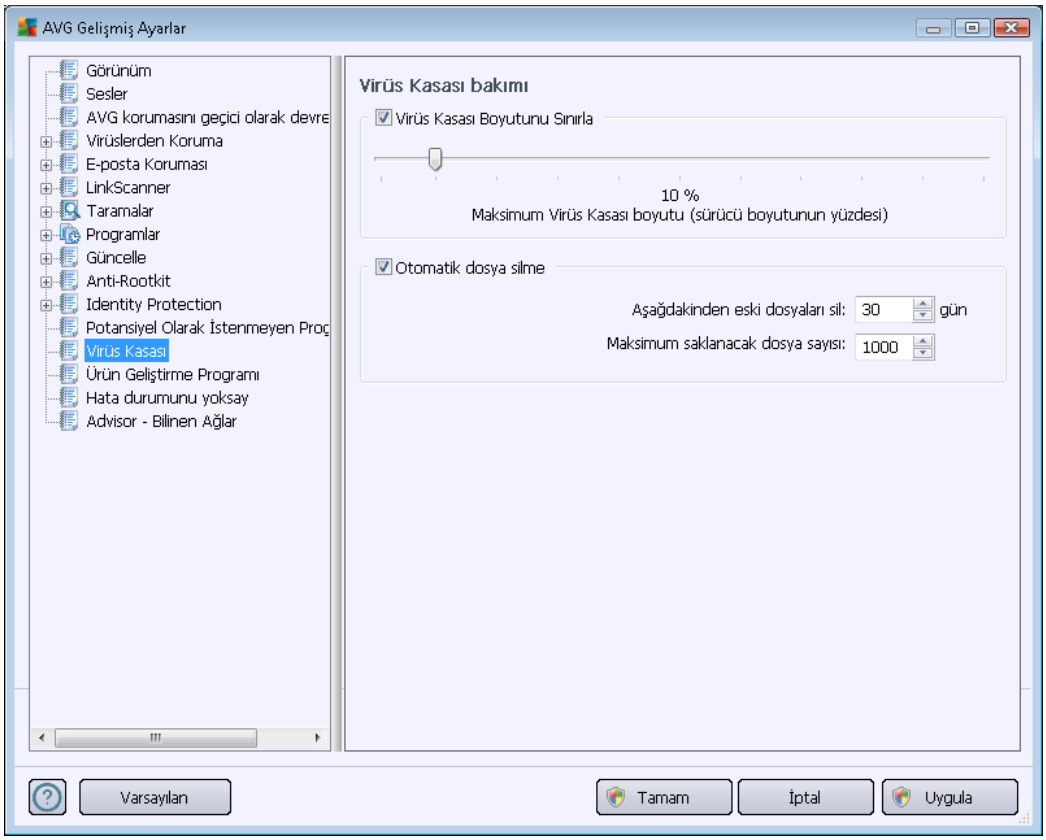
- ***Düzenle*** - önceden tanımlanmış olan bir istisnanın parametrelerini düzenleyebileceğiniz bir düzenleme iletişim kutusu açar (*yeni istisna tanımı iletişim kutusuyla aynı, aşağıya bakın*)
- ***Sil*** - seçilen öğeyi istisnalar listesinden siler

- ***İstisna ekle*** – oluşturulacak yeni istisnanın parametrelerini tanımlayabileceğiniz yeni bir düzenleme iletişim kutusu açar:



  - ***Dosya*** – istisna olarak belirlemek istediğiniz dosyanın tam yolunu girin
  - ***İmzayı Kontrol Et*** – seçilen dosyanın "özel imzasını" görüntüler. Bu sağlama, AVG'nin seçilen dosyayı diğer dosyalardan ayırmasını sağlamak üzere otomatik oluşturulan karakter dizeleridir. Sağlama, dosyanın başarıyla eklenmesinin ardından oluşturulur ve görüntülenir.
  - ***Dosya Bilgisi*** – dosya hakkında *(lisans/sürüm bilgileri vb.) mevcut tüm bilgileri görüntüler.*
  - ***Herhangi bir yerde – tam yolu kullanma*** – söz konusu dosyayı sadece belirli bir konumda istisna olarak atamak istiyorsanız bu kutucuğu işaretlemeden bırakın. Onay kutusu işaretlenirse, belirtilen dosya nerede bulunduğuna bağlı olmaksızın istisna olarak atanır *(ancak, belirli dosya için yine de tam yolu doldurmanız gerekir, bundan sonra dosya aynı ada sahip iki dosyanın sisteminizde görüntülenme olasılığının benzersiz bir örneği olarak kullanılır)*.

10.13. Virüs Kasası



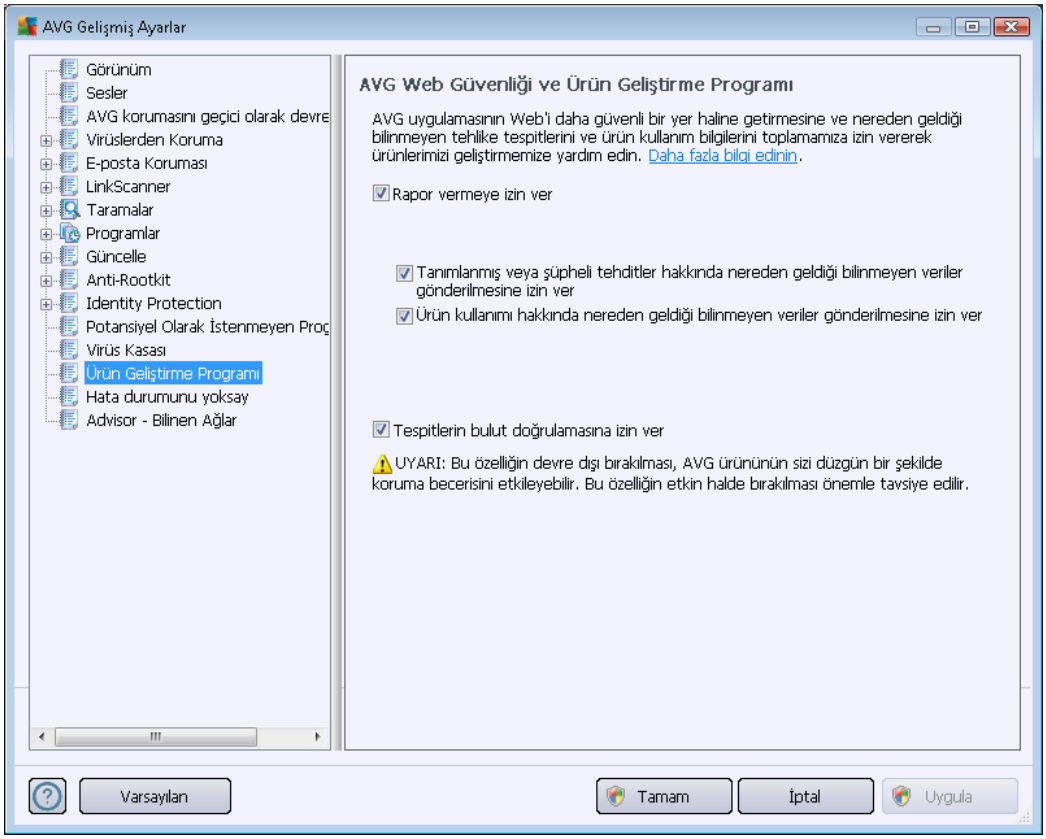
Virüs Kasası bakımı iletişim kutusu, Virüs Kasası'nda depolanan nesnelerin yönetimi hususunda çeşitli parametreleri tanımlayabilmenizi sağlar:

- ***Virüs Kasası boyutunu sınırla*** – Virüs Kasasının maksimum boyutunu ayarlamak için kaydırıcıyı kullanın. Söz konusu boyut, sabit diskinizin boyutu ile doğru orantılı olacaktır.
- ***Otomatik dosya silme*** – Bu bölümde nesnelerin Virüs Kasasında depolanacakları maksimum süreyi (***... Günden eski dosyaları sil***), Virüs Kasasında depolanacak maksimum dosya sayısını (***Depolanacak maksimum dosya sayısı***) belirleyebilirsiniz.

10.14. Ürün Geliştirme Programı

AVG Web Güvenliği ve Ürün Geliştirme Programı iletişim kutusu sizi AVG ürün geliştirme programına katılmaya ve genel İnternet güvenliği düzeyini artırmamıza yardım etmeye davet eder. Tespit edilen tehditlerin AVG'ye bildirilmesini etkinleştirmek için ***Raporlamaya izin ver*** seçeneğini işaretli tutun. Bu, dünyanın her tarafındaki katılımcılardan en son tehditlere ilişkin güncel bilgileri toplamamıza ve koruma özelliklerini herkes için geliştirmemize yardımcı olacaktır.

Raporlama işlemi otomatik olarak gerçekleştirilir; bu nedenle sizi herhangi bir şekilde rahatsız etmez. Raporlar kişisel bilgilerinizi içermez. Tespit edilen tehditlerin rapor edilmesi isteğe bağlıdır, ancak, bu seçeneği açık bırakmanızı rica ediyoruz. Böylece hem siz hem de diğer AVG kullanıcıları için korumayı geliştirmeye devam edebiliriz.



İletişim kutusundaki mevcut ayarlama seçenekleri:

- ***Raporlamaya izin ver*** *(varsayılan olarak açık)* - Daha fazla geliştirme için bize yardımcı olmak isterseniz **AVG Anti-Virus**, onay kutusunu işaretli tutun. Bu şekilde, karşılaşılan tüm tehditler AVG'ye bildirilir ve böylece biz tüm dünyadan kötü amaçlı yazılımlarla ilgili güncel bilgileri toplayarak korumayı herkes için geliştirebiliriz. Raporlama işlemi otomatik olarak gerçekleştirilir; bu nedenle sizi herhangi bir şekilde rahatsız etmez ve raporlar kişisel bilgilerinizi içermez.
    - ***Kullanıcı onayı üzerine yanlış tanımlanan e-posta hakkında veri gönderilmesine izin ver*** *(varsayılan olarak açık)* – yanlış bir şekilde istenmeyen posta olarak tanımlanan e-postalar veya Anti-Spam bileşeni tarafından algılanmayan istenmeyen postalar hakkında bilgi gönderin. Bu tür bilgiler gönderilirken onayınız istenir.
    - ***Algılanan veya şüpheli tehditler hakkında anonim veriler gönderilmesine izin ver*** *(varsayılan olarak açık)* – tüm şüpheli veya olumlu bir şekilde tehlikeli kod veya davranış modeli hakkında bilgi gönderin *(bilgisayarınızda algılanan virüs, casus yazılım veya erişmeye çalıştığınız kötü amaçlı web sitesi olabilir)* .
    - ***Ürün kullanımı hakkında anonim bilgi gönderilmesine izin ver*** *(varsayılan olarak açık)* – algılama sayısı, yapılan taramalar, başarılı veya başarısız güncellemeler gibi uygulama kullanımı hakkında temel istatistikler gönderin.

- ***Algılamaların bulut doğrulamasına izin ver*** *(varsayılan olarak açık)* – hatalı pozitif sonuçları ayıklamak için algılanan tehditler gerçekten virüs bulaşması içerip içermediklerinin belirlenmesi amacıyla denetlenir.

En yaygın tehditler

Günümüzde, normal virüslerin dışında çok fazla tehdit bulunmaktadır. Kötü amaçlı yazılımların ve tehlikeli web sitelerinin yazarları çok yenilikçidir ve yeni tehdit türleri oldukça sık ortaya çıkar, bunların oldukça büyük bir çoğunluğu ise İnternet üzerindedir. Bu tehditlerin en yaygın olanları şunlardır:

- ***Virüs***, kendi kendini kopyalayan ve yayılan zararlı bir koddur ve genellikle zarar oluşana kadar fark edilmez. Bazı virüsler ciddi bir tehdit oluşturur, dosyaları siler veya istediği şekilde değiştirir. Bazı virüsler ise görünüşte zararsız olan müzik çalma gibi işlemler yapar. Ancak, temel olarak sahip oldukları çoğalma özelliği nedeniyle tehlikelidir. En basit virüs bile bilgisayarınızın tüm belleğini bir anda ele geçirebilir ve bilgisayarın çökmesine neden olur.

- ***Solucan***, normal virüsün aksine, "taşıyıcı" nesneye gerek duymayan bir virüs alt kategorisidir; genellikle e-posta yoluyla kendini diğer bilgisayarlara gönderir ve e-posta sunucuları ve ağ sistemlerinde aşırı yüklenmeye neden olur.

- ***Casus yazılım***, genellikle kötü amaçlı kategorisinde (*kötü niyetli yazılım = virüsler de dahil tüm kötü amaçlı yazılımlar*) yer alan programlardır (genellikle Truva atlarıdır). Bu tür yazılımların amacı kişisel bilgileri, şifreleri, kredi kartı numaralarını çalmak veya bir bilgisayarın içine sızarak saldırganın bilgisayarı uzaktan yönetmesini sağlamaktır. Elbette, bunların hepsi bilgisayar sahibinin izni veya bilgisi olmadan yapılır.

- ***Potansiyel olarak istenmeyen programlar***, tehlikeli olabilecek ancak bilgisayarınız için mutlaka tehlikeli olması gerekmeyen bir casus yazılım türüdür. Özel bir PUP örneği reklam yazılımlarıdır. Bu yazılımlar, genellikle açılır pencerelerde reklam görüntülemek üzere tasarlanır. Can sıkıcıdır ancak gerçekte zararlı değildir.

- ***İzleme çerezleri*** de bir casus yazılım türü olarak değerlendirilebilir. Bu küçük dosyalar web tarayıcısında saklandığından ve tekrar ziyaret ettiğinizde "ana" web sitesine otomatik olarak gönderildiğinden, tarama geçmişiniz ve benzer diğer bilgiler gibi verileri içerebilir.

- ***Güvenlik açığı yazılımı***, işletim sistemindeki, İnternet tarayıcısındaki veya gerekli diğer programlardaki bir açıktan faydalanan kötü amaçlı bir koddur.

- ***Kimlik Avı***, kendilerini güvenilir veya tanınmış kuruluş gibi göstererek hassas kişisel verileri elde etme girişimidir. Genel olarak, potansiyel kurbanlara, örneğin banka hesabı bilgilerini güncellemelerini isteyen toplu postalarla ulaşılır. Bunu yapmak için, kişilerden verilen bağlantıyı ziyaret etmeleri istenir. Bu bağlantı sahte bir banka web sitesine yönlendirir.

- ***Aldatmaca (Hoax)*** tehlikeli, uyarıda bulunan veya yalnızca rahatsız edici ve gereksiz bilgiler içeren toplu e-postalardır. Yukarıdaki tehditlerin çoğu, yayılmak için aldatıcı e-posta iletilerini kullanır.

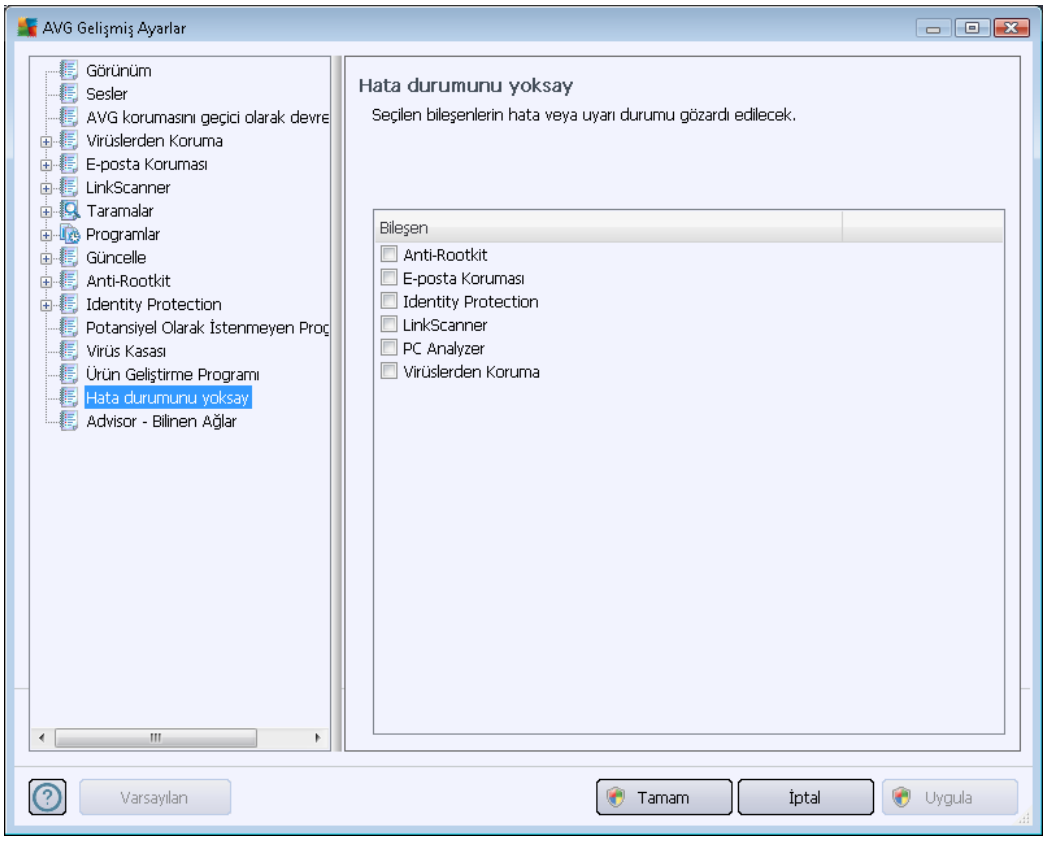
- ***Kötü amaçlı web siteleri***, bilgisayarınıza bilerek kötü amaçlı yazılım yükleyen sitelerdir.

Saldırıya uğrayan siteler de aynısını yapar ancak bunlar kötü amaçlı ziyaretçiler tarafından zarar verilen yasal web siteleridir.

AVG Anti-Virus sizi farklı türlerdeki tüm bu tehditlerden korumak için özel bileşenler içerir. Bu bileşenlerin kısa bir açıklaması için lütfen Bileşen Genel Görünümü bölümüne bakın.

10.15. Hata durumunu yoksay

Hata durumunu yoksay iletişim kutusunda, bilgilendirilmek istemediğiniz bileşenleri seçebilirsiniz:



Varsayılan olarak listede herhangi bir bileşen seçilmemiştir. Bileşenlerden herhangi biri hatalı duruma düşerse aşağıdaki yöntemlerden biri vasıtasıyla uyarılacaksınız demektir:

- sistem tepsisi simgesi – AVG'nin tüm bileşenleri doğru şekilde çalışırken simge, 4 renkli görünecektir ancak herhangi bir aksaklık oluşursa simgenin yanında sarı bir ünlem işareti görülür,
- AVG ana penceresinin Güvenlik Durumu Bilgileri bölümünde mevcut sorun açıklanır

Bileşenlerden birini geçici bir süre kapatmanız gereken bir durum ile karşılaşabilirsiniz (*bileşenlerin geçici süre kapatılması önerilmez. Tüm bileşenleri daima açık durumda tutmanız ve varsayılan yapılandırmayı muhafaza etmeniz gerekir ancak aksi durumlarla karşılaşabilirsiniz*). Bu durumda sistem tepsisi simgesi, bileşenin hata durumunda olduğunu otomatik olarak bildirir. Ancak bu durumda gerçek bir hatadan söz edemeyiz çünkü hatayı siz başlatmışsınızdır ve potansiyel riskin

farkında olmalısınız. Aynı zamanda, simge gri renkli görüntülendikten sonra daha sonra meydana gelecek hataları rapor edemez.

Bu durumda yukarıdaki pencerede hata durumunda olan (*ya da kapatılmış*) bileşenleri seçebilirsiniz ve söz konusu durum hakkında bilgilendirilmek istemeyebilirsiniz. Aynı seçenek *(Bileşen durumunu yoksay)* doğrudan AVG ana ekranının bileşenlere genel bakış penceresinden de kullanılabilir.

10.16. Advisor – Bilinen Ağlar

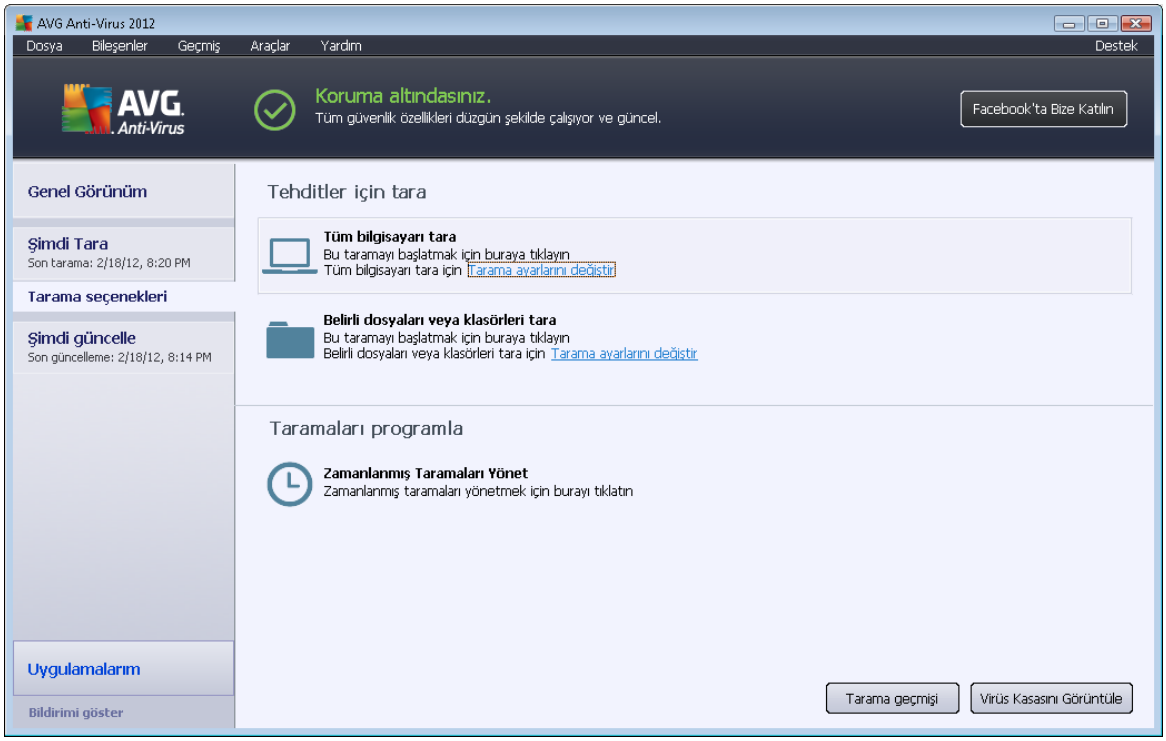
AVG Advisor bağlandığınız ağları izleyen ve yeni bir ağ bulunduğunda *(daha önce kullanılan bir ağ adına sahip olduğundan karışıklığa neden olabilecek bir ağ)* sizi bilgilendiren ve ağın güvenliğini kontrol etmenizi öneren bir özelliğe sahiptir. Yeni ağın bağlanmak için güvenli olduğuna karar verirseniz, ağı bu listeye de kaydedebilirsiniz; bu durumda AVG Advisor ağın benzersiz özelliklerini hatırlayacak *(özellikle de MAC adresini)* bir sonraki seferde bildirim göstermeyecektir.

Bu iletişim penceresinde, önceden hangi ağları bilinen ağ olarak kaydettiğinizi kontrol edebilirsiniz. ***Kaldır*** düğmesine basarak herhangi bir girişi silebilirsiniz; bu durumda ilgili ağ tekrar bilinmeyen ve muhtemelen güvensiz ağ olarak değerlendirilir.

11. AVG Tarama

Varsayılan olarak, **AVG Anti-Virus** ilk taramadan sonra olduğu gibi hiçbir taramayı çalıştırmaz, her zaman korumada olan **AVG Anti-Virus** ürününün yerleşik bileşenleri ile mükemmel olarak korunuyor olmanız ve hiçbir kötü amaçlı yazılımın bilgisayarınıza hiçbir surette girmesine izin vermemeniz gerekir. Elbette belirli aralıklarda çalıştırılacak bir tarama planlayabilir veya bir taramayı gereksinimlerinize göre manuel olarak başlatabilirsiniz.

11.1. Tarama Arayüzü



AVG tarama arayüzüne ***Tarama seçenekleri*** hızlı bağlantısı aracılığıyla erişilebilir. ***Tehditleri tara*** iletişim kutusuna geçmek için bu bağlantıyı tıklatın. Bu iletişim kutusunda aşağıdakiler bulunmaktadır:

- öntanımlı taramalara genel bakış – yazılım satıcısı tarafından tanımlanan üç tarama türü isteğe bağlı olarak hemen veya programlı olarak kullanılmaya hazırdır:
  - Tüm bilgisayarın taranması
  - Belirli dosyaları veya klasörleri tara
- Taramaları programla bölümü – Gerektiğinde yeni testler tanımlayabilir ve yeni programlar oluşturabilirsiniz.

Kontrol düğmeleri

Tarama arayüzünde bulunan genel kontrol düğmeleri şunlardır:

- ***Tarama geçmişi*** - tüm tarama geçmişi ile birlikte Tarama sonuçlarına genel bakış iletişim kutusunu açar
- ***Virüs Kasasını Görüntüle*** - tespit edilen bulaşmaların karantina altına alındığı Virüs Kasasını yeni bir pencerede açar.

11.2. Öntanımlı Taramalar

AVG Anti-Virus programının ana özelliklerinden biri istek üzerine taramadır. İsteğe bağlı taramalar, muhtemel bir virüs hakkında şüpheye düştüğünüz an bilgisayarınızın istediğiniz kısmında istediğiniz zaman yapabileceğiniz taramalardır. Kısacası, bilgisayarınızda virüs olduğunu düşünmeseniz bile söz konusu taramaların düzenli aralıklarla yapılması önerilmektedir.

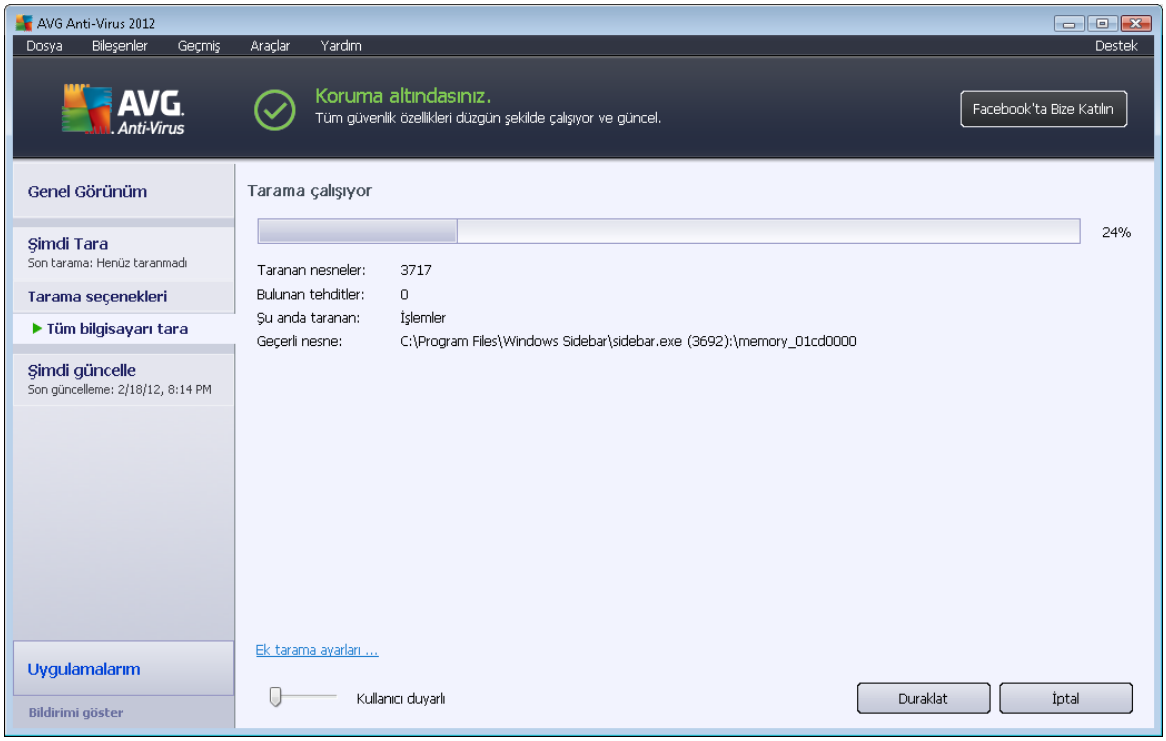
AVG Anti-Virus içinde, yazılım satıcısının önceden tanımladığı aşağıdaki tarama türlerini bulacaksınız:

11.2.1. Tüm Bilgisayarın Taranması

Tüm Bilgisayarın taranması – tüm bilgisayarı muhtemel bulaşmalara ve/veya potansiyel olarak istenmeyen programlara karşı tarar. Bu tarama, bilgisayarınızın tüm sabit disklerini tarayacak, virüsleri tespit edecek ve temizleyecek ya da tespit edilen bulaşmayı Virüs Kasasına taşıyacaktır. Bilgisayarın tümü haftada en az bir defa taranmalıdır.

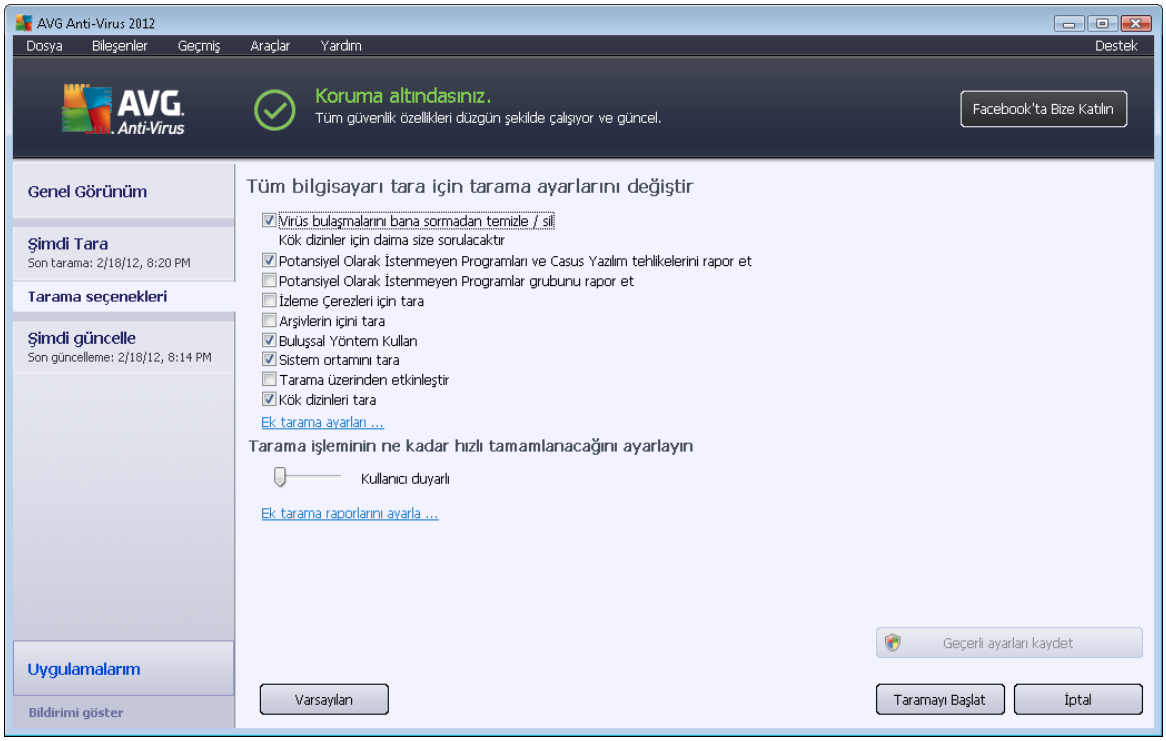
Tarama başlatma

Tüm bilgisayarın taranması, taramanın simgesi tıklatılarak doğrudan tarama arayüzünden başlatılabilir. Bu tarama türü için başka belirli ayarlamaların yapılmasına gerek yoktur, tarama ***Tarama yapılıyor*** iletişim kutusunda anında başlayacaktır (*bkz. ekran görüntüsü*). Tarama işlemi gerekirse geçici olarak kesilebilir (***Duraklat***) ya da iptal edilebilir (***Durdur***).



Tarama yapılandırması düzenleme

Tüm bilgisayarın taranması işlevinin önceden tanımlı varsayılan ayarlarını düzenleme seçeneğiniz vardır. ***Tüm bilgisayarın taranması için tarama ayarlarını değiştir*** iletişim kutusunu açmak için ***Tarama ayarlarını değiştir*** bağlantısına basın *(Tüm bilgisayarın taranması işlevinin Tarama ayarlarını değiştir seçeneği ile tarama arayüzünden erişilebilir.* ***Geçerli bir nedeniniz olmadığı müddetçe varsayılan ayarları değiştirmek için bu ayarları korumanız önerilir!***



- ***Tarama parametreleri*** – tarama parametreleri listesindeki belirli parametreleri gereksinimleriniz doğrultusunda açıp kapatabilirsiniz.

    - ***Bulaşmayı bana sormadan temizle / kaldır*** (*varsayılan olarak açık*) – Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne Virüs Kasası'na taşınır.

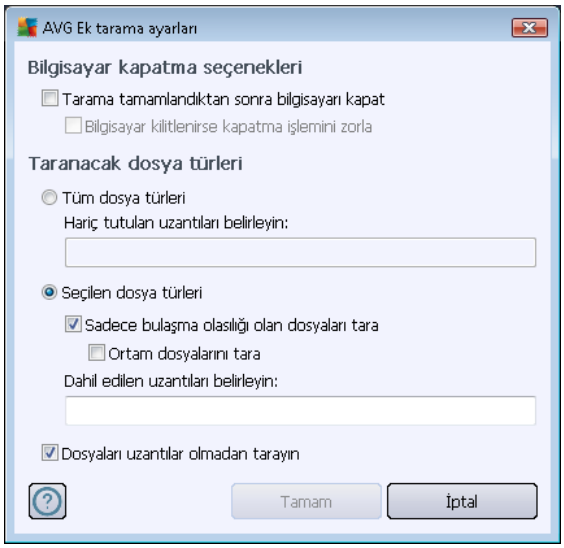
    - ***Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et*** (*varsayılan olarak açık*) – Anti-Spyware motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da denetlemek için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

    - ***Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et*** (*varsayılan olarak kapalı*) – bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

    - ***İzleme Tanımlama Bilgilerini Tara*** (*varsayılan olarak kapalı*): Anti-Spyware bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

- ***Arşivleri tara*** (*varsayılan olarak kapalı*) – Bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.
- ***Buluşsal Analiz Yöntemlerini Kullan*** (*varsayılan olarak açık*) – Buluşsal analiz yöntemi (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.
- ***Sistem ortamını tara*** (*varsayılan olarak açık*) – Tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.
- ***Kapsamlı taramayı etkinleştir*** (*varsayılanda kapalıdır*) – Belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.
- ***Rootkit'leri tara*** (*varsayılan olarak açık*) – Anti-Rootkit taraması bilgisayarınızı olası rootkit'lere, örneğin bilgisayarınızda kötü amaçlı etkinlik içerebilecek programlar ve teknolojilere karşı tarar. Bir kök dizin algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri kök dizin olarak yanlış algılanabilir.

- ***Ek tarama ayarları*** – Bağlantı, şu parametreleri belirtebileceğiniz yeni bir ***Ek tarama ayarları*** iletişim kutusu açar:



- ***Bilgisayar kapatma seçenekleri*** – Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (***Tarama bittikten sonra bilgisayarı kapat***) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (***Bilgisayar kilitliyse bilgisayarı kapanmaya zorla***).
- ***Tarama için dosya türleri*** – Nelerin taranmasını istediğinize de karar vermelisiniz:

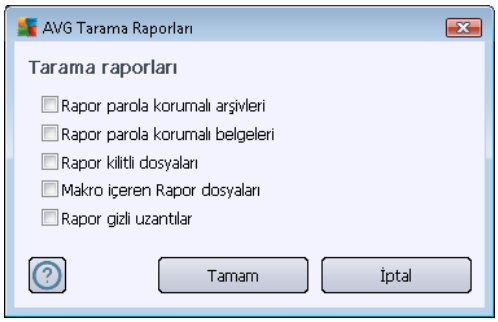
- ***Tüm dosya türleri*** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;

- ***Seçili dosya türleri*** – Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılamayan dosyalar*); ortam dosyaları (*video, ses dosyaları – bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.

- İsteğe bağlı olarak, ***Uzantıları olmayan dosyaları taramaya*** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

- ***Taramanın ne kadar hızlı tamamlanacağını ayarlayın*** – tarama sürecinin önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini yavaşlatabilir (*bilgisayarda çalışmanız gerektiği ancak taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) veya sistem kaynaklarını daha yoğun kullanmak suretiyle daha hızlı bir şekilde (*ör., bilgisayar geçici bir süreyle kullanılmadığında*) çalıştırabilirsiniz.

- ***Tarama raporu oluştur*** – bağlantı üzerinden ***Tarama Raporları*** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğiniz seçebilirsiniz:



Uyarı: *Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır – AVG Taraması / Tarama Planlama/ Tarama Tipi bölümünde açıklandığı doğrultuda.* ***Tüm bilgisayarı tara*** *fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar verirseniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taranması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz.*

11.2.2. Belirli Dosyaları veya Klasörleri Tara

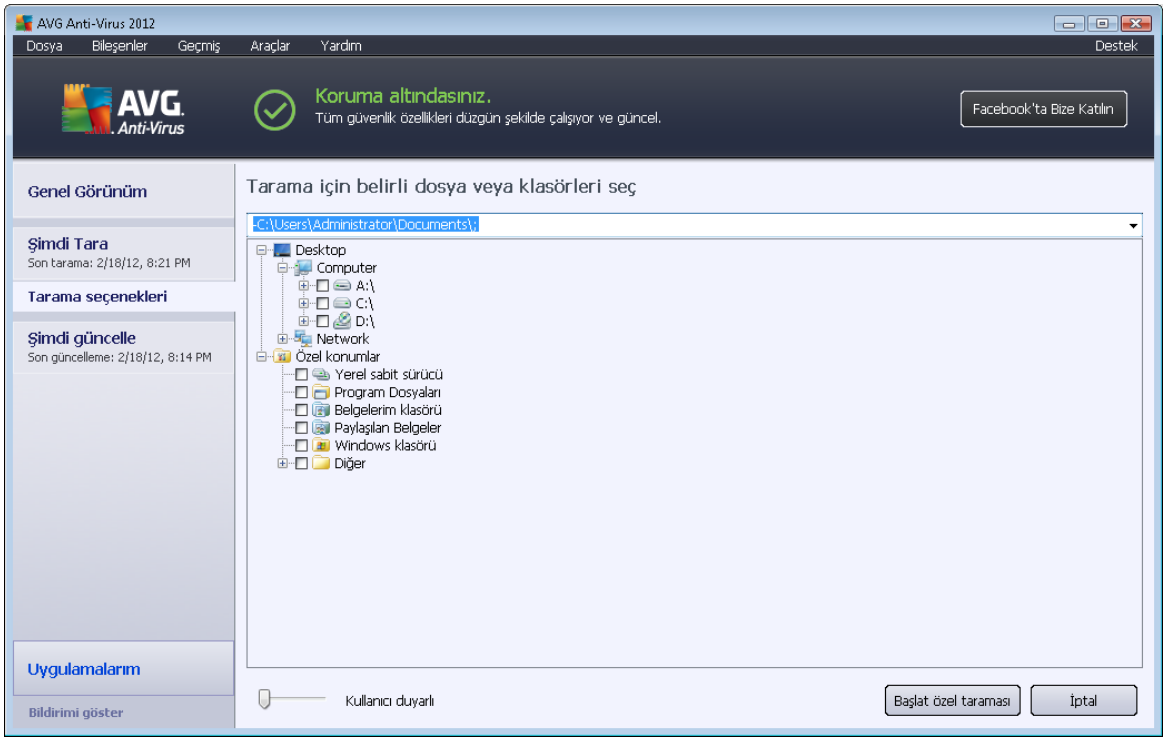
Belirli dosyaları veya klasörleri tara – bilgisayarınızın sadece taranması için seçtiğiniz alanlarını tarar (*seçilen klasörler, sabit diskler, disket sürücüleri, CD'ler vb.*). Virüs tespiti ve temizlenmesi sırasında tarama işlemi, tüm bilgisayar taraması ile aynıdır. Bulunan virüsler temizlenir ya da Virüs Kasası'na taşınır. Belirli dosyaları veya klasörleri tara işlevi, kendi testlerinizi ve gereksinimlerinize bağlı olarak bunların programlamasını ayarlamak için kullanılabilir.

Tarama başlatma

Belirli dosya ve klasörleri tara işlevi, tarama simgesi tıklatılarak doğrudan tarama arayüzünden başlatılabilir. Yeni bir ***Taramak için belirli dosya ve klasörleri seçin*** iletişim kutusu açılır. Bilgisayarınızın ağaç görünümünden taranmasını istediğiniz klasörleri seçin. Seçilen klasörlerin her birine giden yol, otomatik olarak oluşturulacak ve iletişim kutusunun üst kısmındaki metin alanında görüntülenecektir.

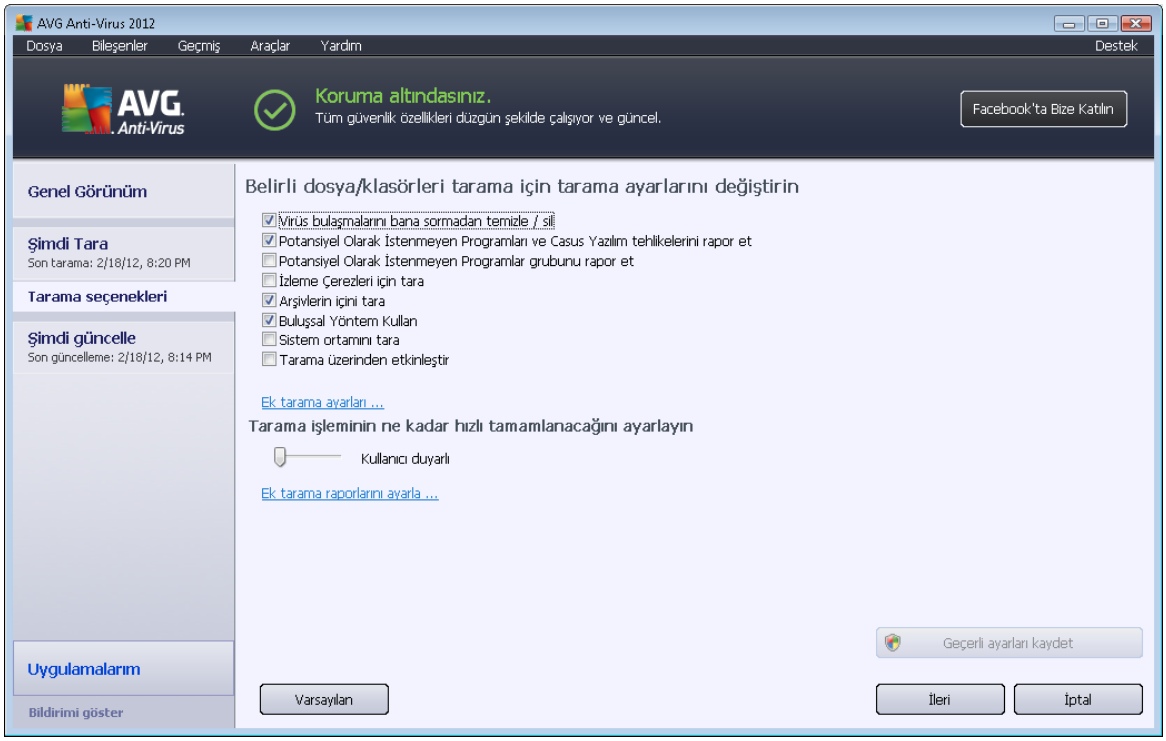
Belirli bir klasör taranırken içinde bulunan klasörlerin taranmaması gibi bir ihtimal de vardır. Bunu yapabilmek için otomatik olarak oluşturulan yolun başına "**-**" işareti koyun (*ekran görüntülerini inceleyin*). Klasörün tümünü tarama dışında tutmak için "!" parametresini kullanın.

Son olarak, taramayı başlatabilmek için ***Taramayı başlat*** düğmesine basın. Tarama işleminin kendisi temel olarak Tüm bilgisayar tarama ile aynıdır.



Tarama yapılandırması düzenleme

Belirli dosya ve klasörleri tara fonksiyonunun varsayılan ayarlarını düzenleme opsiyonunuz da bulunmaktadır. ***Tarama ayarlarını değiştir*** bağlantısına tıklayarak ***Belirli dosya ve klasörlerin taranmasına ilişkin tarama ayarlarını değiştir*** iletişim kutusuna gidin. ***Geçerli bir nedeniniz olmadığı müddetçe varsayılan ayarları değiştirmek için bu ayarları korumanız önerilir!***



- ***Tarama parametreleri*** – tarama parametreleri listesindeki belirli parametreleri gereksinimleriniz doğrultusunda açıp kapatabilirsiniz.

    - ***Bulaşmayı bana sormadan temizle / kaldır*** (*varsayılan olarak açık*) – Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Bulaşmış dosya otomatik olarak temizlenemezse, bulaşmış nesne Virüs Kasası'na taşınır.

    - ***Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et*** (*varsayılanda açıktır*) – Anti-Spyware motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da taramak için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

    - ***Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et*** (*varsayılanda kapalıdır*) – bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

    - ***İzleme Tanımlama Bilgilerini Tara*** (*varsayılan olarak kapalıdır*): Anti-Spyware bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

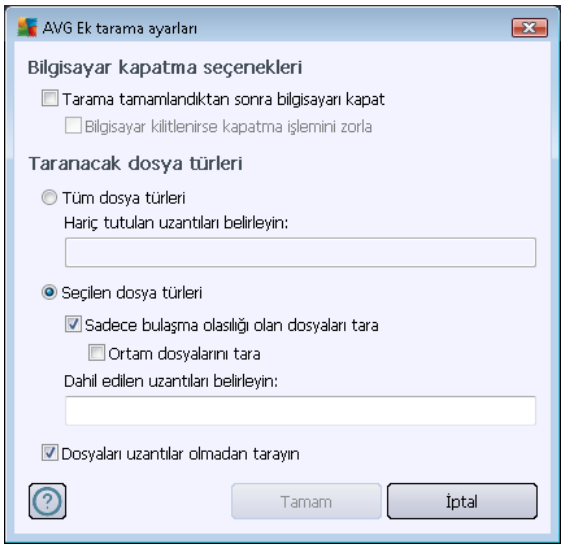
- ***Arşivleri tara*** (*varsayılan olarak açıktır*) – bu parametre, ZIP, RAR vb. arşiv dosyalarının içinde sıkıştırılmış dosyaların bile taranmasını sağlar.

- ***Buluşsal Analiz Yöntemlerini Kullan*** (*varsayılan olarak açıktır*) – buluşsal analiz yöntemi (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.

- ***Sistem ortamını tara*** (*varsayılan olarak kapalıdır*) – tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.

- ***Kapsamlı taramayı etkinleştir*** (*varsayılanda kapalıdır*) – belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.

- ***Ek tarama ayarları*** – bağlantı, şu parametreleri belirtebileceğiniz yeni bir ***Ek tarama ayarları*** iletişim kutusu açar:



  - ***Bilgisayar kapatma seçenekleri*** – Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (***Tarama bittikten sonra bilgisayarı kapat***) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (***Bilgisayar kilitliyse bilgisayarı kapanmaya zorla***).

  - ***Taranacak dosya türleri*** – nelerin taranmasını istediğinize de karar vermelisiniz:

    - ***Tüm dosya türleri*** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;

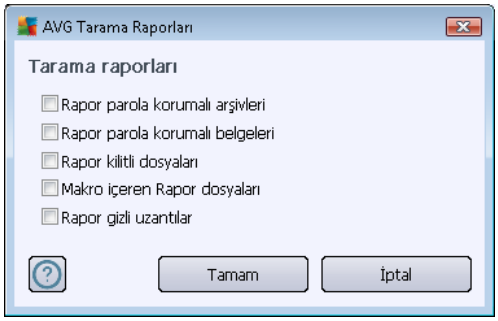
    - ***Seçili dosya türleri*** – yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşamayan dosyalar taranmayacaktır, örneğin,*

bazı düz metin dosyaları veya bazı diğer çalıştırılamayan dosyalar); ortam dosyaları (*video, ses dosyaları – bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.

- İsteğe bağlı olarak, ***Uzantıları olmayan dosyaları taramaya*** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

- ***Tarama işlemi önceliği*** – tarama işlemi önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Bu seçenek değeri, varsayılan olarak, otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini yavaşlatabilir (*bilgisayarda çalışmanız gerektiği ancak taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) veya sistem kaynaklarını daha yoğun kullanmak suretiyle daha hızlı bir şekilde (*ör., bilgisayar geçici bir süreyle kullanılmadığında*) çalıştırabilirsiniz.

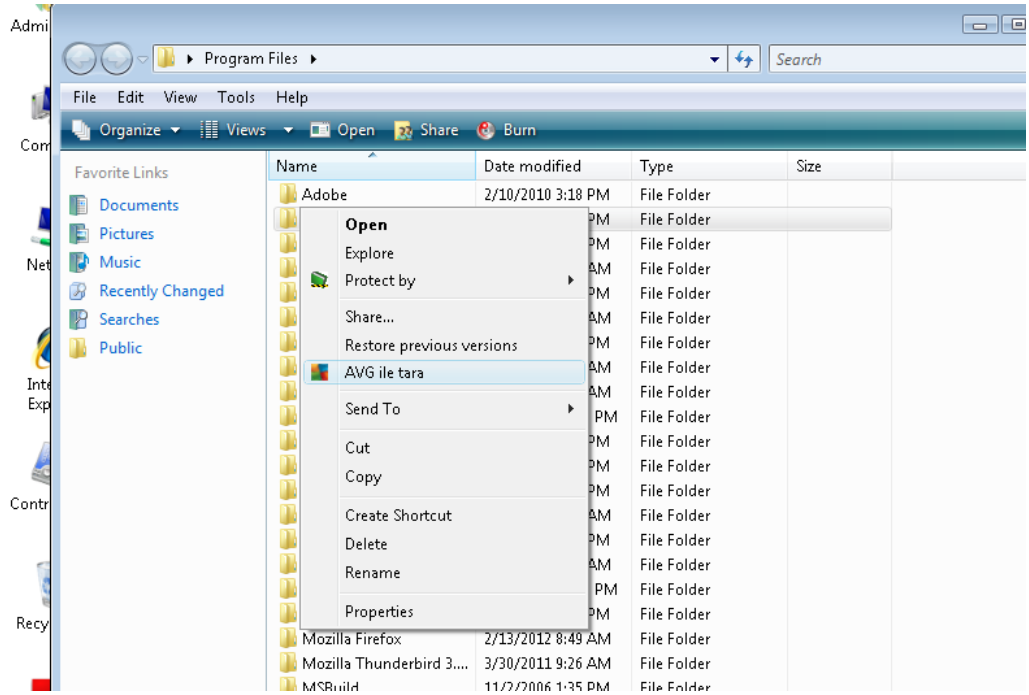
- ***Tarama raporu oluştur*** – bağlantı üzerinden ***Tarama Raporları*** isimli bir iletişim kutusu açılır ve buradan ne tip buluntuların rapor edileceğini seçebilirsiniz:



Uyarı: *Bu tarama parametreleri, yeni tanımlanan taramanın parametreleri ile aynıdır – AVG Taraması / Tarama Planlama/ Tarama Tipi bölümünde açıklandığı doğrultuda.* ***Belirli dosya veya klasörleri tara*** *fonksiyonunun varsayılan yapılandırmasını değiştirmeye karar verirseniz yeni ayarlarınızı, belirli dosya ya da klasörlerin taranması için kullanılacak varsayılan yapılandırma olarak atayabilirsiniz. Buna ek olarak söz konusu yapılandırma tüm yeni programlı taramalarınız için şablon görevi görecektir (tüm özelleştirilmiş taramalar, Seçilen dosya ya da klasörleri tara fonksiyonunun mevcut yapılandırmasına dayanmaktadır).*

11.3. Windows Gezgini'nde Tarama

Bilgisayarın tümünde ya da seçilen bölümlerinde gerçekleştirilen öntanımlı taramaların yanı sıra **AVG Anti-Virus**, doğrudan Windows Gezgini ortamında bulunan belirli nesnelerin hızlı bir şekilde taranmasını da sağlamaktadır. Bilinmeyen bir dosyayı açmak istiyor fakat içeriğinden emin olamıyorsanız isteğe bağlı olarak tarayabilirsiniz. Bu adımları takip edin:



- Windows Gezgini'nde taramak istediğiniz dosyayı *(ya da klasörü)* seçin
- Bağlam menüsünü açmak için nesneye farenizle sağ tıklatın
- ***ile Tara*** seçeneğini seçerek dosyanın AVG tarafından taranmasını sağlayın **AVG Anti-Virus**

11.4. Komut Satırı Tarama

AVG Anti-Virus içinde, taramayı komut satırından çalıştırma seçeneği vardır. Bu seçeneği, sunucularda ya da bilgisayar yeniden başlatıldıktan sonra otomatik olarak çalıştırılacak komut metinlerinin oluşturulması sırasında kullanabilirsiniz. Komut satırında AVG'nin grafik kullanıcı arayüzünde sunulan parametrelerden daha fazlasını kullanarak tarama işlemini gerçekleştirebilirsiniz.

AVG taramasını komut satırından çalıştırmak için AVG'nin yüklendiği klasörde aşağıdaki komutu çalıştırın:

- ***32 bit OS için avgscanx***
- ***64 bit OS için avgscana***

Komut sözdizimi

Komut söz dizimi aşağıdaki gibidir:

- ***Tam bilgisayar taraması yapılırken avgscanx /parametre*** ... Örn. ***avgscanx /comp***

- ***avgscanx /parameter /parameter*** .. Birden fazla parametre kullanıldığı zaman bunlar bir sıra halinde dizilmeli ve bir boşluğun yanı sıra bir de tire işareti ile ayrılmalıdır

- Parametrelerden biri için belirli bir değer verilmesi gerekiyorsa (***/scan*** parametresi taranmak üzere bilgisayarınızın seçilen alanları hakkında bilgi talep eder ve sizin de seçilen bölüme ilişkin veri yolunu tam olarak sağlamanız gerekir). Değerler noktalı virgül ile birbirinden ayrılır. Örn: ***avgscanx /scan=C:\;D:***

Tarama parametreleri

Mevcut parametrelerin tam görünümümü görüntülemek için, /? parametresi ile birlikte ilgili komutu yazın. ya da /HELP (örn. ***avgscanx /?***). Zorunlu olan tek parametre, bilgisayarın hangi alanlarının taranması gerektiğini belirlemek için kullanılan /SCAN parametresidir. Seçenekler hakkında daha ayrıntılı açıklama almak için komut satırı parametrelerine genel bakış bölümüne bakın.

Tarama işlemini başlatmak için ***Enter*** tuşuna basın. Tarama sırasında işlemi ***Ctrl+C*** veya ***Ctrl+Pause*** tuşlarına basarak durdurabilirsiniz.

CMD taraması grafik arayüzünden başlatıldı

Bilgisayarınızı Windows Güvenli Modda çalıştırdığınız zaman komut satırı taramasını grafik kullanıcı arayüzünden başlatma ihtimaliniz de bulunmaktadır. Taramanın kendisi komut satırından başlatılacaktır, ***Komut Satırı Oluşturucu*** iletişim kutusu, en yaygın tarama parametrelerini konforlu grafik arayüzünde görüntüler.

Söz konusu iletişim kutusuna sadece Windows Güvenli Moddan ulaşılabildiği için iletişim kutusu hakkında ayrıntılı bilgi almak için doğrudan iletişim kutusundan açılan yardım dosyasını inceleyin.

11.4.1. CMD Tarama Parametreleri

Komut satırı taramasında kullanılan parametrelerin listesi aşağıda verilmiştir:

- ***/SCAN*** Belirli dosya ya da klasörleri tara */SCAN=yol;yol (örn. /SCAN=C:\;D:\)*
- ***/COMP*** Tüm Bilgisayarın Taranması
- ***/HEUR*** Bulgusal analizi kullan
- ***/EXCLUDE*** Tarama işleminden dizin yolu veya dosyaları hariç tut
- ***/@*** Komut dosyası /dosya adı/
- ***/EXT*** Bu uzantıları tara /örneğin EXT=EXE,DLL/
- ***/NOEXT*** Uzantıları tarama /örneğin NOEXT=JPG/
- ***/ARC*** Arşivleri tara

- ***/CLEAN*** Otomatik olarak temizle
- ***/TRASH*** Bulaşan dosyaları Virüs Kasasına taşı
- ***/QT*** Hızlı test
- ***/LOG*** Bir tarama sonucu dosyası oluştur
- ***/MACROW*** Makroları rapor et
- ***/PWDW*** Parola ile korunan dosyaları rapor et
- ***/ARCBOMBSW*** Arşiv bombalarını raporla*(tekrar tekrar sıkıştırılan arşivler)*
- ***/IGNLOCKED*** Kilitli dosyaları göz ardı et
- ***/REPORT*** /dosya adı/ dosyasına rapor et
- ***/REPAPPEND*** Rapor dosyasına ekle
- ***/REPOK*** Bulaşmamış dosyaları Tamam olarak raporla
- ***/NOBREAK*** CTRL-BREAK ile işlemin kesilmesine izin verme
- ***/BOOT*** MBR/BOOT kontrolünü etkinleştir
- ***/PROC*** Aktif işlemleri tara
- ***/PUP*** Potansiyel olarak istenmeyen programları rapor et
- ***/PUPEXT*** Potansiyel olarak istenmeyen programlar
- ***/REG*** Kayıt defterini tara
- ***/COO*** Tanımlama bilgilerini tara
- ***/?*** Bu konuyla ilgili yardımı görüntüle
- ***/HELP*** Bu konuyla ilgili yardımı görüntüle
- ***/PRIORITY*** Tarama önceliğini belirle /Düşük, Oto, Yüksek/ *(bkz. Gelişmiş ayarlar / Taramalar)*
- ***/SHUTDOWN*** Tarama tamamlandıktan sonra bilgisayarı kapat
- ***/FORCESHUTDOWN*** Tarama tamamlandıktan sonra bilgisayarı kapatmayı zorla
- ***/ADS*** *Alternatif Veri Akışlarını Tara (sadece NTFS)*
- ***/HIDDEN*** Gizli uzantılı dosyaları bildir

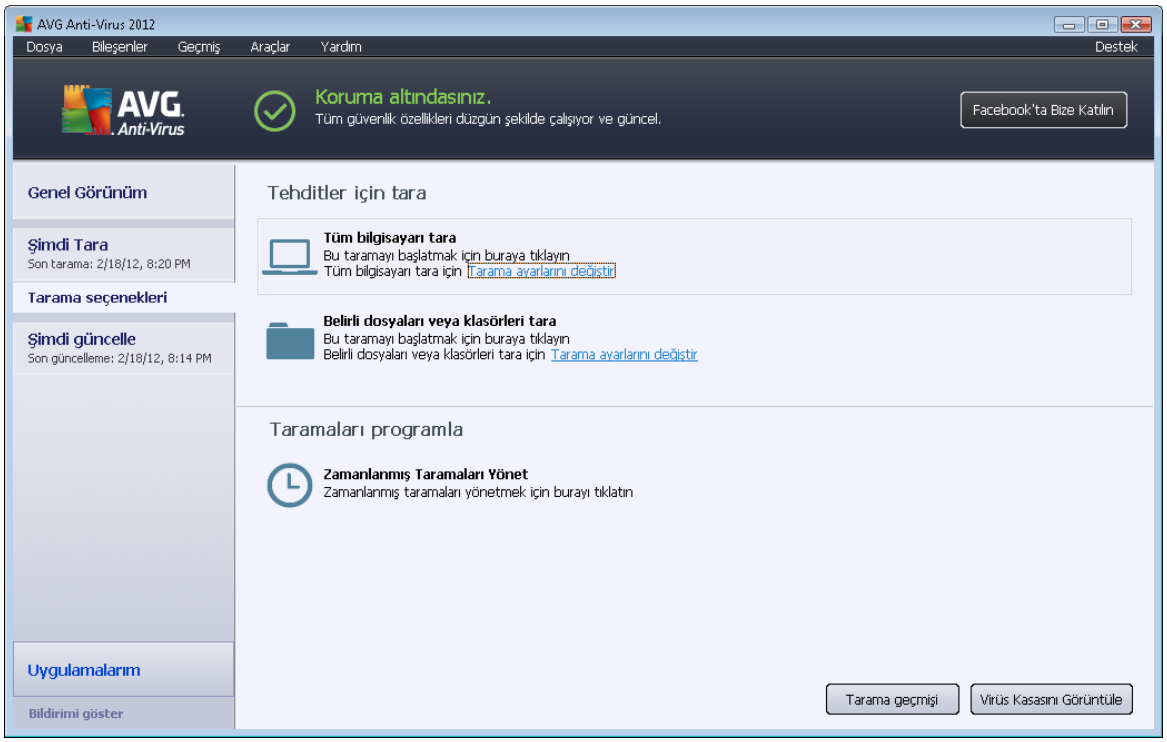
- ***/INFECTABLEONLY*** Yalnızca bulaşabilir uzantıya sahip dosyaları tara
- ***/THOROUGHSCAN*** Kapsamlı taramayı etkinleştir
- ***/CLOUDCHECK*** Hatalı pozitif sonuçlar açısından denetle
- ***/ARCBOMBSW*** Yeniden sıkıştırılmış arşiv dosyalarını bildir

11.5. Tarama Programlama

AVG Anti-Virus ile, taramayı talep üzerine (örneğin bilgisayarınıza virüs bulaştığından şüphelenirseniz) veya programlanan bir plan doğrultusunda başlatabilirsiniz. Taramaların bir program doğrultusunda yapılması önemle önerilir. Bu şekilde, bilgisayarınızın bulaşma ihtimaline karşı korunduğundan emin olursunuz ve ne zaman tarama yapmanız gerektiği konusunda endişelenmenize gerek kalmaz.

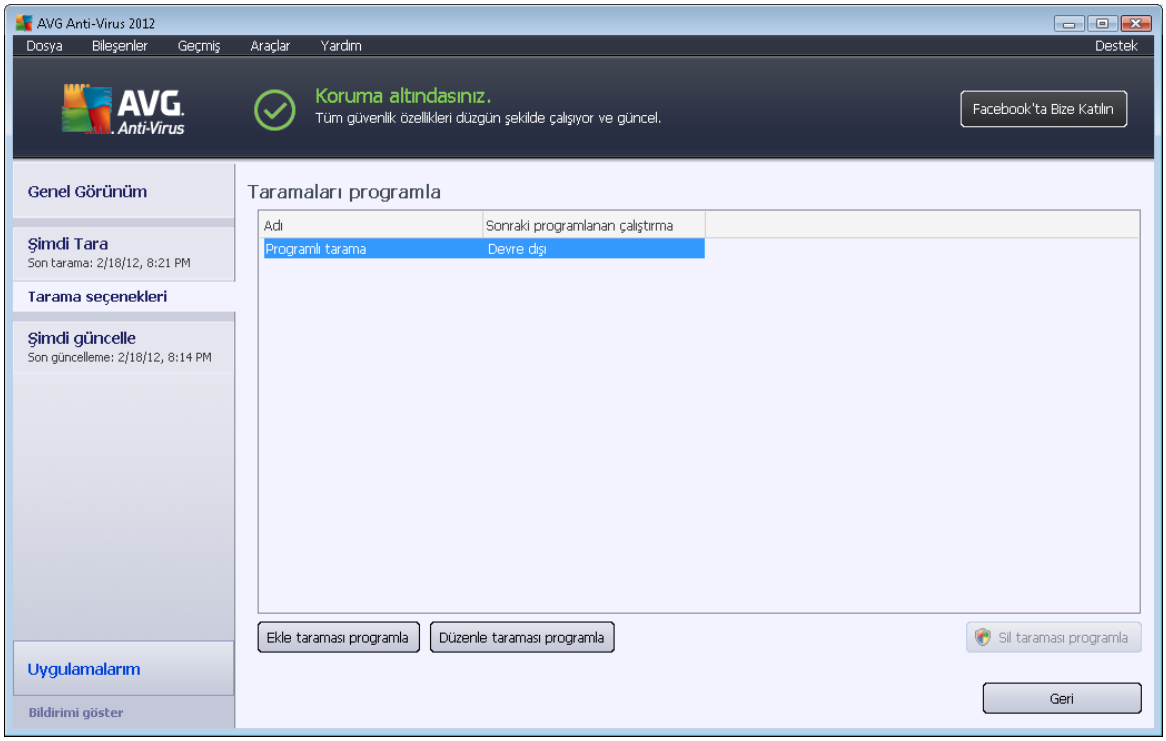
Tüm bilgisayar taraması'nı en az haftada bir kez düzenli olarak başlatmanız gerekir. Diğer bir yandan, mümkün olması halinde programlı taramanın varsayılan yapılandırmasında ayarlandığı gibi tüm bilgisayar taramasını günlük olarak yapın. Bilgisayarınız "daima açık" ise taramaları çalışma saatlerinden sonra gerçekleştirilecek şekilde programlayabilirsiniz. Bilgisayarınızı arada sırada kapatıyorsanız taramayı, taramaları görev yerine getirilemediğinde bilgisayarın başlaması ile başlat şeklinde programlayın.

Yeni tarama programları oluşturmak için AVG tarama arayüzünü inceleyin ve ***Tarama programla*** adı altındaki bölümü bulun:



Taramaları programla

Geçerli olarak zamanlanmış taramaların bir listesini bulabileceğiniz yeni bir ***Taramaları programla*** iletişim kutusunu açmak için ***Taramaları programla*** bölümündeki grafik simgeyi tıklatın:



Şu kontrol düğmelerini kullanarak taramaları düzenleyebilir/ekleyebilirsiniz:

- ***Tarama programı ekle*** – düğme, ***Programlanan tarama ayarları*** iletişim kutusunu ve Programlama Ayarları sekmesini açar. Bu iletişim kutusunda yeni tanımladığınız taramanın parametrelerini belirleyebilirsiniz.

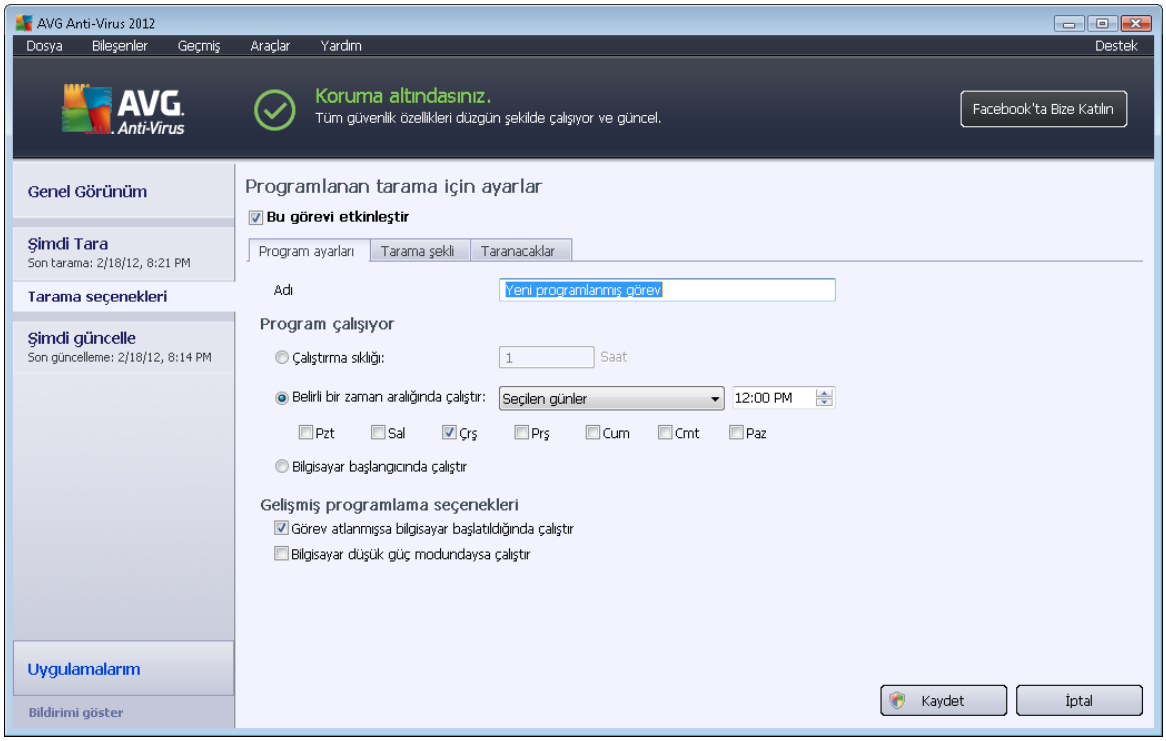
- ***Tarama programını düzenle*** – bu düğme, programlanan taramalar listesinden mevcut bir taramayı seçtiyseniz kullanılabilir. Bu durumda düğme etkinleşir ve ***Programlanan tarama ayarları*** iletişim kutusuna ve Programlama ayarları sekmesine geçmek için düğmeyi kullanabilirsiniz. Seçilen tarama parametreleri, zaten belirlenmiştir ve düzenlenebilir.

- ***Tarama programını sil*** – bu düğme, programlanan taramalar listesinden mevcut bir taramayı seçmeniz halinde etkinleşir. Bu tarama, ilgili kontrol düğmesine basılarak listeden silinebilir. Diğer bir yandan sadece kendi taramalarınızı silebilirsiniz; varsayılan ayarlar içinde ***Tüm bilgisayar taraması programı*** öntanımlıdır ve kesinlikle silinemez.

- ***Geri*** – AVG tarama arayüzüne geri döner

11.5.1. Program Ayarları

Yeni bir test programlamayı ve testin düzenli olarak başlamasını istiyorsanız, ***Programlanan test ayarları*** iletişim kutusuna girin, *(**Taramaları programla** iletişim kutusundaki Tarama programı ekle* düğmesini tıklatın). Bu iletişim kutusu üç sekmeye ayrılmıştır: ***Programlama ayarları*** *(aşağıdaki resme bakın; doğrudan yönlendirileceğiniz varsayılan sekmedir)*, Tarama türü ve Taranacaklar.



Planlama ayarları sekmesinde ***Bu görevi etkinleştir*** öğesini işaretleyerek ya da işareti kaldırarak planlanan taramayı geçici olarak devre dışı bırakabilir ve ihtiyaç duyduğunuzda yeniden açabilirsiniz.

Sonra oluşturmak ve programlamak üzere olduğunuz taramanın adının verir. ***İsim*** öğesini kullanarak metin alanına bir isim girin. Programladığınız taramaları diğerlerinden kolaylıkla ayırabilmek için taramalarınıza kısa, açıklayıcı isimler vermeyi deneyin.

Örnek: *Taramayı "Yeni Tarama" veya "Taramam" adıyla adlandırmanız uygun değildir çünkü bu adlar, taramanın fiilen neyi kontrol ettiğini açıklamaz. Diğer bir yandan "Sistem alanları taraması" oldukça açıklayıcı bir isim olacaktır. Ayrıca, taramanın adında söz konusu taramanın tam bilgisayar taraması ya da sadece seçilen dosya ya da klasörlerin taranması olup olmadığını belirtmenize gerek yoktur – taramalarınız seçilen dosya ya da klasörleri tara işlevinin farklı şekillerinden ibaret olacaktır.*

Bu iletişim kutusunda taramanın aşağıdaki parametrelerini de tanımlayabilirsiniz:

- ***Planlama çalışıyor*** – yeni planlanan taramanın başlaması için zaman aralığı girin. Zamanlama belirli bir sürenin ardından tekrarlanan tarama ile (***Her ...'de bir***) ya da kesin bir tarih ve saat tanımlayarak (***Belirli bir saatte çalıştır ...***), ya da (***Bilgisayar başlangıcında***) ilgili bir programın taranmasıyla tanımlanabilir.

- ***Gelişmiş planlama seçenekleri*** – bu bölümde, bilgisayar düşük güç modundaysa veya tamamen kapatılmışsa hangi koşullar altında taramanın başlatılması/başlatılmaması gerektiğini belirleyebilirsiniz.

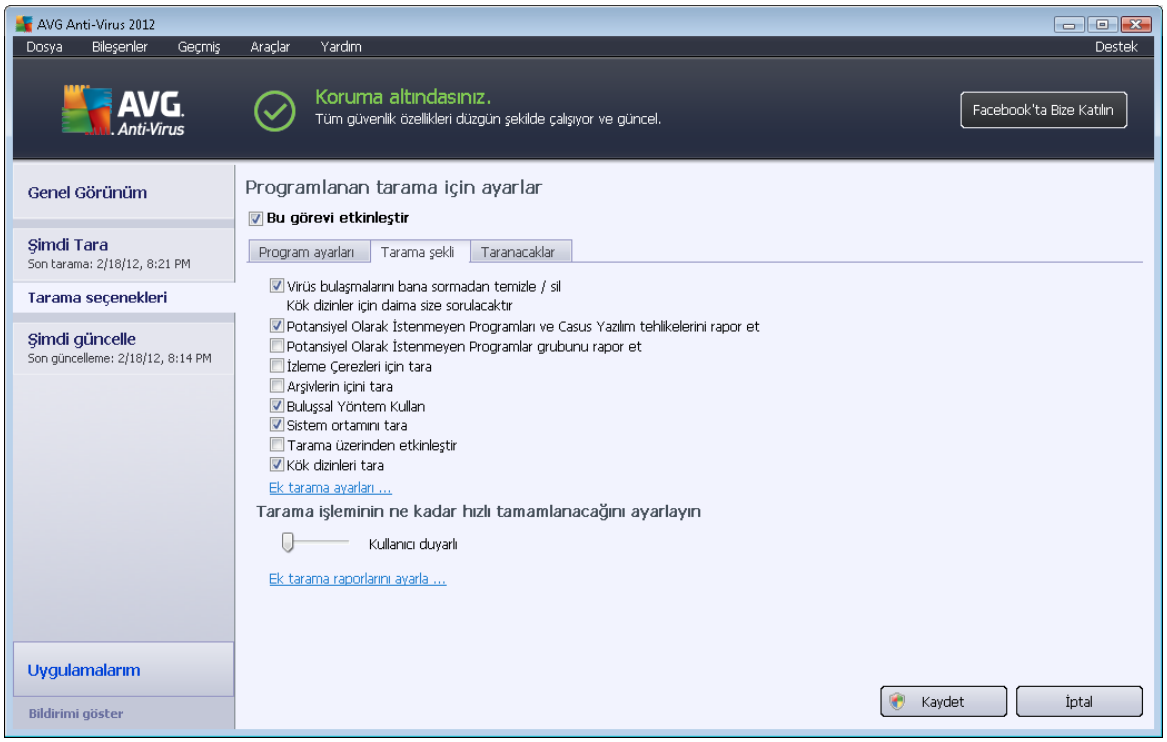
Programlı tarama iletişim kutusuna dair ayarların kontrol düğmeleri

Programlı tarama ayarları iletişim kutusunda üç adet sekme bulunmaktadır (*Programlama ayarları, Tarama şekli ve Taranacaklar*) ve hangi sekmede olduğunuz önemli olmaksızın aşağıdaki düğmelerin fonksiyonları aynıdır:

- ***Kaydet*** – bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve AVG tarama arayüzü varsayılan penceresine geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.

- ***İptal*** – bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve AVG tarama arayüzü varsayılan iletişim kutusuna geri döner.

11.5.2. Tarama Şekli



Tarama Şekli sekmesinde, isteğe bağlı olarak açılıp/kapatılabilen tarama parametrelerine ilişkin bir liste bulabilirsiniz. Varsayılan olarak birçok parametre devreye sokulur ve işlevsellik de tarama sırasında uygulanacaktır. Söz konusu ayarları değiştirmek açısından geçerli bir nedeniniz yoksa varsayılan yapılandırmayı olduğu gibi muhafaza etmeniz önerilir:

- ***Bulaşmayı bana sormadan temizle / kaldır*** (*varsayılan olarak açık*): Tarama sırasında virüs tanımlanırsa, bir giderme yazılımı mevcutsa otomatik olarak temizlenir. Etkilenen dosyanın otomatik olarak silinemiyor olması halinde ya da bu seçeneği kapatmayı seçerseniz bir virüs tespit edildiğinde bilgilendirileceksiniz ve tespit edilen bulaşma hakkında ne yapılacağına karar vermek zorunda kalacaksınız. Önerilen işlem, bulaşmış dosyayı Virüs Kasasına kaldırmaktır.

- ***Potansiyel Olarak İstenmeyen Programları ve Casus Yazılım tehditlerini rapor et*** (*varsayılan olarak açıktır*): Anti-Spyware motorunu etkinleştirmek ve virüslerin yanı sıra casus yazılımları da denetlemek için işaretleyin. Casus yazılım, şüpheli kötü amaçlı yazılım kategorisini ifade eder: genellikle bir güvenlik riskini oluşturmasına rağmen bu programlardan bazıları bilerek yüklenebilir. Bilgisayarınızın güvenliğini artırdığından, bu özelliği etkin durumda tutmanızı öneriyoruz.

- ***Potansiyel Olarak İstenmeyen Programlar gelişmiş grubunu rapor et*** (*varsayılanda kapalıdır*) – bu parametre casus yazılımların, yani doğrudan üreticiden alınan tamamen zararsız olan, ancak daha sonra kötüye kullanılabilecek programların genişletilmiş paketinin tespit edilmesi için işaretleyin. Bu, bilgisayar güvenliğinizi daha da artıran ek bir önlemdir, ancak yasal programları da engelleyebilir ve bu yüzden varsayılan olarak kapalıdır.

- ***İzleme Tanımlama Bilgilerini Tara*** (*varsayılan olarak kapalıdır*): Casus Yazılımdan Korunma bileşeninin bu parametresi, tarama sırasında tespit edilmesi istenen tanımlama bilgilerini tanımlar (*HTTP tanımlama bilgileri kimlik doğrulaması, izleme ve kullanıcılar hakkındaki site tercihleri veya elektronik alışveriş sepetlerinin içeriği gibi belirli bilgilerin korunması için kullanılır*).

- ***Arşivleri Tara*** - (*varsayılan olarak kapalıdır*). Bu parametreler, tarama işleminin ZIP, RAR gibi bazı arşiv türleri ile sıkıştırılmış olsa bile tüm dosyaları denetlemesini tanımlar.

- ***Buluşsal Analiz Yöntemlerini Kullan*** – (*varsayılan olarak açıktır*). Buluşsal analiz yöntemi (*taranan nesnenin komutlarının sanal bir bilgisayar ortamında dinamik olarak canlandırılması*) tarama sırasında kullanılacak virüs tespiti yöntemlerinden biridir.

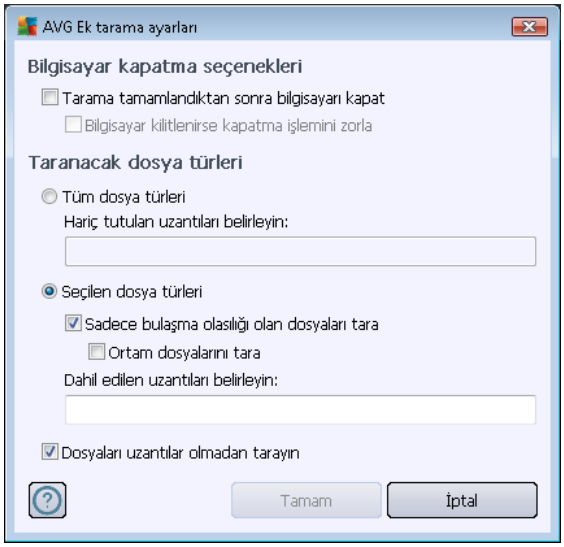
- ***Sistem ortamını tara*** - (*varsayılan olarak açıktır*). Tarama işlemi, bilgisayarınızın sistem alanlarını da kontrol edecektir.

- ***Kapsamlı taramayı etkinleştir*** (*varsayılanda kapalıdır*) – belirli durumlarda (*bilgisayarınıza bulaşma olmasından şüpheleniliyorsa*) yalnızca emin olmak üzere bilgisayarınızın bulaşma olması çok zor olan alanlarını bile tarayan en kapsamlı tarama algoritmalarını etkinleştirmek için bu seçeneği işaretleyebilirsiniz. Ancak, bu yöntemin çok fazla zaman aldığını unutmayın.

- ***Rootkit'leri tara*** (*varsayılan olarak açık*): Anti-Rootkit taraması bilgisayarınızı olası rootkit'lere, örneğin bilgisayarınızda kötü amaçlı etkinlik içerebilecek programlar ve teknolojilere karşı tarar. Bir kök dizin algılanırsa, bu, bilgisayarınızda mutlaka virüs olduğu anlamına gelmez. Bazı durumlarda, belirli sürücüler veya normal uygulamaların bölümleri kök dizin olarak yanlış algılanabilir.

Sonra, tarama yapılandırmasını şu şekilde değiştirebilirsiniz:

- ***Ek tarama ayarları*** – Bağlantı, şu parametreleri belirtebileceğiniz yeni bir ***Ek tarama ayarları*** iletişim kutusu açar:



- ***Bilgisayar kapatma seçenekleri*** – Çalışan tarama işlemi bittiğinde bilgisayarın otomatik olarak kapatılması gerekip gerekmediğine karar verir. Bu seçeneği seçerseniz (***Tarama bittikten sonra bilgisayarı kapat***) bilgisayar mevcut durumda kilitli olsa bile bilgisayarın kapatılmasını sağlayan bir seçeneğin bulunduğu bir pencere açılacaktır (***Bilgisayar kilitliyse bilgisayarı kapanmaya zorla***).

- ***Tarama için dosya türleri*** – Nelerin taranmasını istediğinize de karar vermelisiniz:

  - ***Tüm dosya türleri*** taranmaması gereken virgülle ayrılmış dosya uzantılarının listesini sağlayarak taramada istisnaları tanımlama seçeneğiyle;

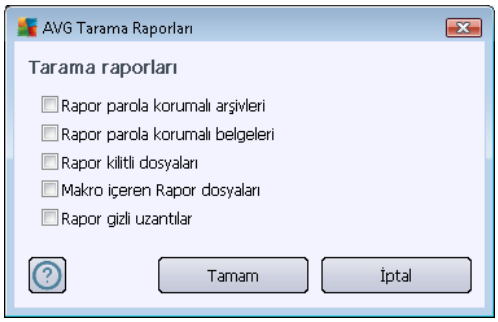
  - ***Seçili dosya türleri*** – Yalnızca virüs bulaşabilme olasılığı olan dosyaları taramayı istediğinizi belirtebilirsiniz (*virüs bulaşamayan dosyalar taranmayacaktır, örneğin, bazı düz metin dosyaları veya bazı diğer çalıştırılamayan dosyalar*); ortam dosyaları (*video, ses dosyaları – bu onay kutusunun işaretini kaldırırsanız, bu dosyalar genellikle çok büyük olduğundan ve virüs bulaşma olasılıkları çok az olduğundan tarama süresini daha da azaltır*). Tekrar, her zaman taranması gereken dosyaları uzantılarına göre belirtebilirsiniz.

  - İsteğe bağlı olarak, ***Uzantıları olmayan dosyaları taramaya*** da karar verebilirsiniz ve bu seçenek varsayılan olarak açıktır ve gerçekten bir nedeniniz yoksa değiştirmemeniz önerilir. Uzantısı olmayan dosyalar şüpheli olabilir ve her zaman taranmalıdır.

- ***Taramanın ne kadar hızlı tamamlanacağını ayarlayın*** – Tarama sürecinin önceliğini değiştirmek için kaydırma çubuğunu kullanabilirsiniz. Bu seçenek varsayılan olarak otomatik kaynak kullanımının *kullanıcıya duyarlı* düzeyine ayarlanmıştır. Alternatif olarak, sistem kaynakları kullanımını minimize etmek için tarama işlemini yavaşlatabilir (*bilgisayarda çalışmanız gerektiği ancak taramanın ne kadar sürdüğünü önemsemediğiniz durumlar için uygundur*) veya sistem kaynaklarını daha yoğun kullanmak suretiyle daha hızlı bir şekilde (*ör., bilgisayar geçici bir süreyle kullanılmadığında*) çalıştırabilirsiniz.

- ***Tarama raporu oluştur*** – bağlantı üzerinden ***Tarama Raporları*** isimli bir iletişim kutusu

açılır ve buradan ne tip buluntuların rapor edileceğiniz seçebilirsiniz:



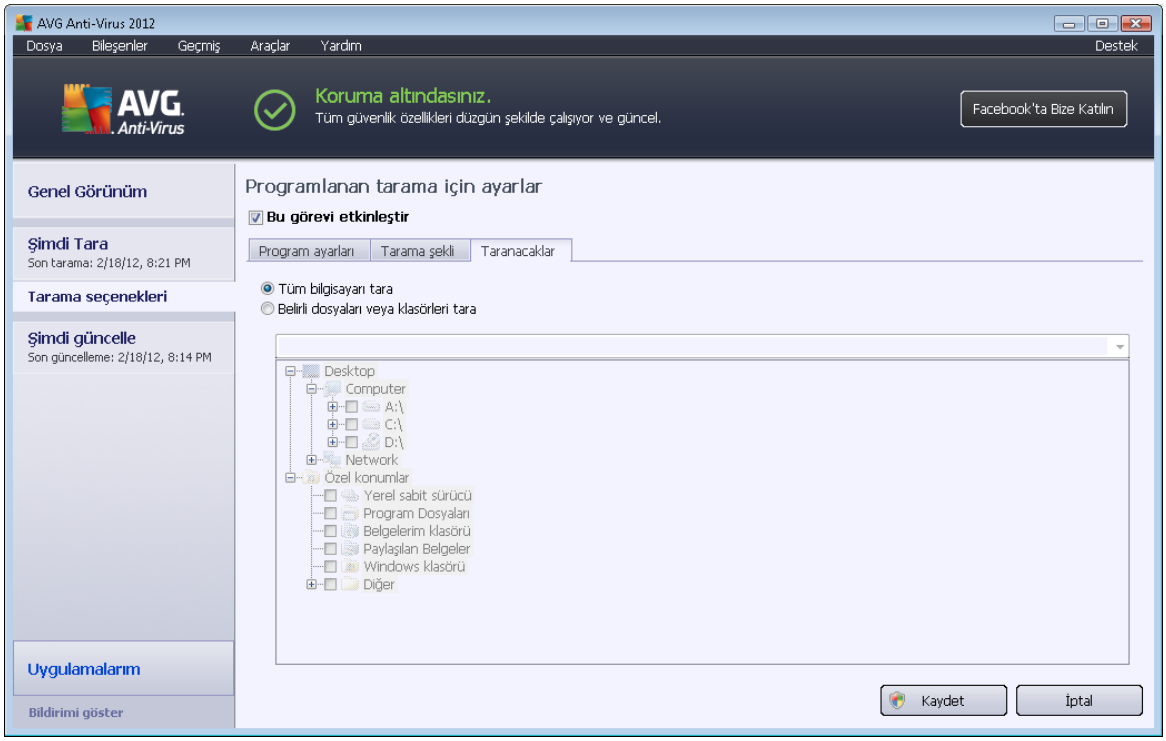
Kontrol düğmeleri

Programlı tarama ayarları iletişim kutusunun her üç sekmesinde *(Programlama ayarları, Tarama şekli ve Taranacaklar)* iki kontrol düğmesi bulunmaktadır ve hangi sekmede olduğunuz önemli olmaksızın bunların fonksiyonları aynıdır:

- ***Kaydet*** – bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve AVG tarama arayüzü varsayılan penceresine geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.

- ***İptal*** – bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve AVG tarama arayüzü varsayılan iletişim kutusuna geri döner.

11.5.3. Taranacaklar



Taranacaklar sekmesinde, tüm bilgisayarı tarama veya belirli dosya veya klasörleri taramayı programlamak isteyip istemediğinizi belirleyebilirsiniz.

Belirli dosya ve klasörlerin taranmasını seçmeniz durumunda, bu iletişim kutusunun alt tarafında görüntülenen ağaç yapısı etkinleşir ve taranacak klasörleri belirleyebilirsiniz (*taramak istediğiniz klasörü buluncaya kadar artı işaretini tıklatarak öğeleri genişletin*). İlgili kutuları işaretleyerek birden fazla klasör seçebilirsiniz. Seçilen klasörler, iletişim kutusunun üstünde bulunan metin alanında görüntülenir; açılır menü seçilen tarama geçmişini daha sonra kullanılmak üzere saklar. Alternatif olarak, istediğiniz klasörün tam yolunu elle girebilirsiniz (*birden fazla yol girerseniz, bunları ekstra boşluk bırakmadan noktalı virgülle ayırmanız gerekir.*

Ağaç yapısı içinde ***Özel konumlar*** adında bir dal da görürsünüz. Aşağıda, ilgili onay kutusu işaretlendiğinde taranacak konumların listesi bulunmaktadır:

- ***Yerel sabit sürücüler*** - bilgisayarınızdaki tüm sabit sürüler
- ***Program dosyaları***
    - C:\Program Files\
    - *64-bit'lik sürümde* C:\Program Files (x86)
- ***Belgelerim klasörü***

- *Win XP için:* C:\Documents and Settings\Default User\Belgelerim\
- *Windows Vista/7 için*: C:\Users\user\Documents\

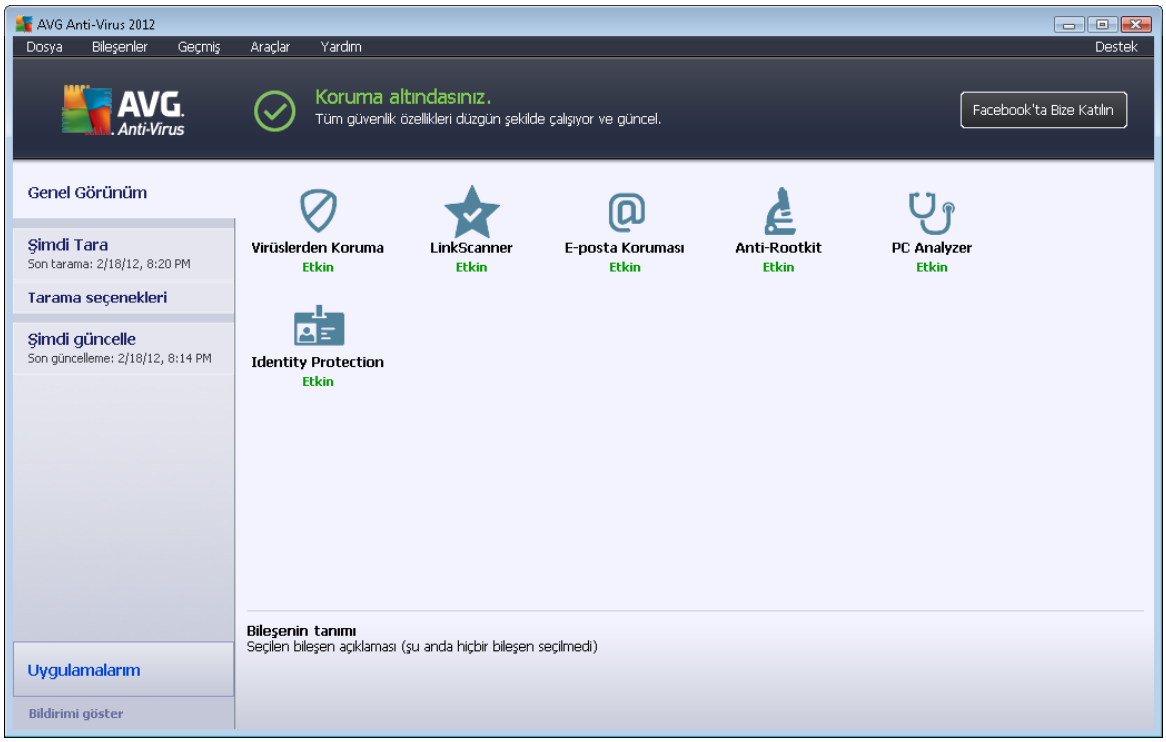
- ***Paylaşılan Belgeler***
  - *Win XP için*: C:\Documents and Settings\All Users\Documents\
  - *Windows Vista/7 için*: C:\Users\Public\Documents\
- ***Windows klasörü*** – C:\Windows\
- ***Diğer***
  - *Sistem sürücüsü* – işletim sisteminin yüklü olduğu sabit sürücü (genellikle C:)
  - *Sistem klasörü* – C:\Windows\System32\
  - *Geçici Dosyalar klasörü* – C:\Documents and Settings\User\Local\ (*Windows XP*) veya C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Geçici İnternet Dosyaları* – C:\Documents and Settings\User\Local Settings\Geçici İnternet Dosyaları\ (*Windows XP*) veya C:\Users\user\AppData\Local\Microsoft\Windows\Geçici İnternet Dosyaları (*Windows Vista/7*)

Kontrol düğmeleri

Aynı iki kontrol düğmesi ***Programlanan tarama için ayarlar*** iletişim kutusunun her üç sekmesinde de mevcuttur *(Program ayarları, Tarama türü ve Taranacaklar)*:

- ***Kaydet*** – bu sekmede veya bu iletişim kutusunun başka herhangi bir sekmesinde gerçekleştirdiğiniz tüm değişiklikleri kaydeder ve AVG tarama arayüzü varsayılan penceresine geri döner. Bu nedenle tüm sekmelerdeki test parametrelerini yapılandırmak istiyorsanız gereksinimlerinizin tamamını belirledikten sonra bunları kaydetmek için düğmeye basın.
- ***İptal*** – bu iletişim kutusunun bu sekmesinde veya başka bir sekmesinde yaptığınız değişiklikleri iptal eder ve AVG tarama arayüzü varsayılan iletişim kutusuna geri döner.

11.6. Tarama Sonuçları Genel Görünümü



Tarama sonuçlarına genel bakış penceresine, AVG tarama arayüzünde ***Tarama geçmişi*** düğmesine basarak ulaşabilirsiniz. İletişim kutusunda, daha önce başlatılan tüm taramalar ve sonuçları hakkında bilgi bulunmaktadır.

- ***Adı*** – taramanın amacı; öntanımlı taramalardan birinin adı ya da programladığınız taramaya verdiğiniz adlardan biri olabilir. Her ismin yanında tarama sonucunu belirten bir simge bulunmaktadır:

  – yeşil simge tarama sırasında herhangi bir bulaşmanın tespit edilemediğini gösterir

  – mavi simge tarama sırasında bir bulaşmanın tespit edildiğini ancak bulaşmış nesnenin otomatik olarak silindiğini gösterir

  – kırmızı simge tarama sırasında bir bulaşmanın tespit edildiğini, ancak bulaşmış nesnenin silinemediğini gösterir!

  Simgeler bütün halinde ya da yarısı kesilmiş olabilir – bütün halindeki simge, tarama işleminin doğru şekilde tamamlandığını ve bitirildiğini gösterirken yarısı kesilmiş simge, taramanın iptal edildiğini ya da kesildiğini gösterir.

  ***Not**: Taramaların her biri hakkında ayrıntılı bilgi almak için lütfen Ayrıntıları Görüntüle düğmesine (bu pencerenin alt kısmındadır) basarak ulaşabileceğiniz Tarama Sonuçları penceresini inceleyin.*

- ***Başlangıç zamanı*** – taramanın başlatıldığı tarih ve saati gösterir.
- ***Bitiş zamanı*** - taramanın bittiği tarih ve saati gösterir.
- ***Taranan nesneler*** – tarama sırasında kontrol edilen nesne sayısıdır
- ***Bulaşmalar*** – tespit edilen / silinenvirüs bulaşması sayısı
- ***Casus yazılım*** - tespit edilen / silinen casus yazılım sayısı
- ***Uyarılar*** – algılanan şüpheli nesnelerin
- ***Kök dizinler*** – algılanan kök dizinlerin
- ***Tarama kaydı bilgileri***- tarama işlemine ve sonucuna ilişkin bilgiler (genellikle işlemin tamamlanmasının ya da kesilmesinin hemen ardından görüntülenir)

Kontrol düğmeleri

Tarama sonuçlarına genel bakış penceresindeki kontrol düğmeleri şunlardır:

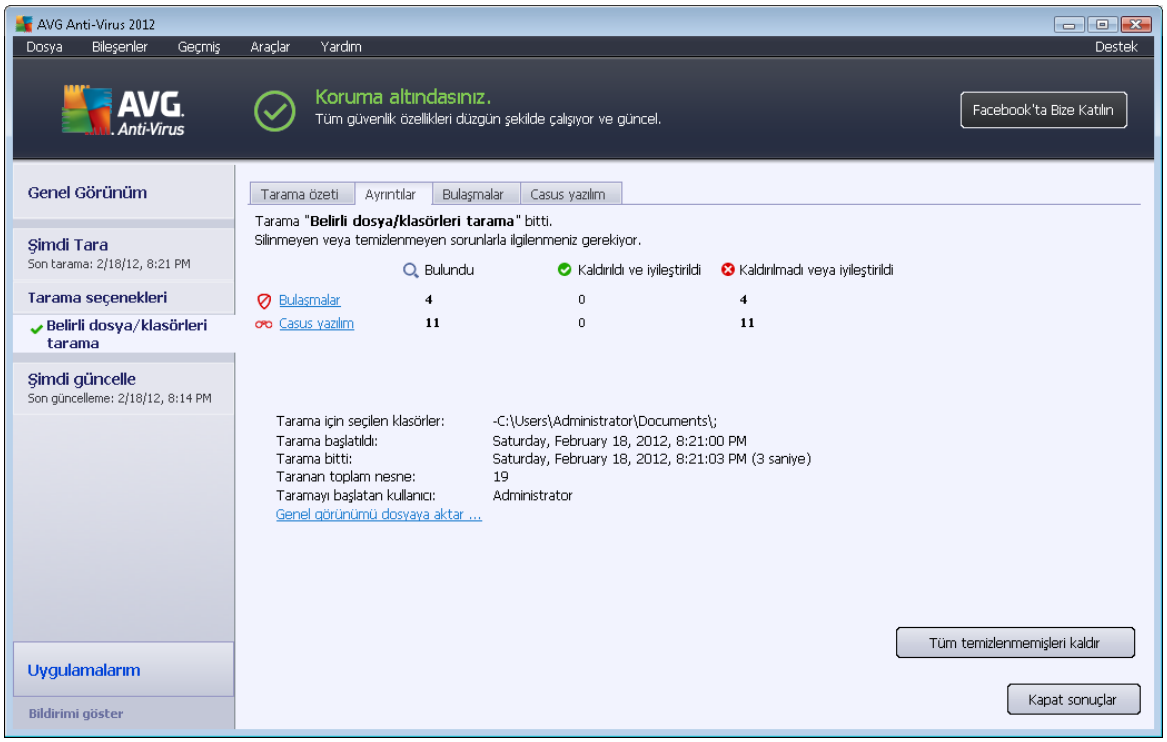
- ***Ayrıntıları görüntüle*** - seçili taramada ayrıntılı verileri görüntülemek için Tarama sonuçları iletişim kutusuna geçmek için basın
- ***Sonucu sil*** - seçili öğeyi tarama sonuçlarına genel bakıştan silmek için basın
- ***Geri*** – AVG tarama arayüzünün öntanımlı iletişim penceresine geri döner

11.7. Tarama Sonuçları Ayrıntıları

Tarama Sonuçlarına Genel Bakış penceresinde belirli bir tarama türü seçildiyse tarama ve seçilen taramanın sonuçları hakkında ayrıntılı bilgi veren ***Tarama Sonuçları*** penceresini açmak için ***Ayrıntıları görüntüle*** düğmesine tıklayabilirsiniz. İletişim penceresi çok sayıda sekmeye ayrılır:

- Sonuçlara Genel Bakış – bu sekme daima görüntülenir ve tarama işlemini tanımayan istatistiki veriler sunar.
- Bulaşmalar – bu sekme tarama sırasında virüs bulaşması tespit edilirse görüntülenir
- Casus yazılım – bu sekme tarama sırasında casus yazılım tespit edilirse görüntülenir
- Uyarılar – bu sekme, örneğin tarama sırasında tanımlama bilgileri algılandıysa görüntülenir
- Kök kullanıcı – bu sekme tarama sırasında kök kullanıcı tespit edilirse görüntülenir
- Bilgi – bu sekme, yukarıdaki kategorilerde sınıflandırılamayan potansiyel tespit edildiğinde görüntülenir; ardından söz konusu sekmede buluntu hakkında bir uyarı mesajı görüntülenir. Ayrıca, burada taranamayan nesneler hakkında bilgi de bulacaksınız *(örn. parola korumalı arşivler)*.

11.7.1. Sonuçlara Genel Bakış Sekmesi



Tarama sonuçları sekmesinde aşağıdaki hususlar hakkında ayrıntılı istatistikler ve bilgi bulabilirsiniz:

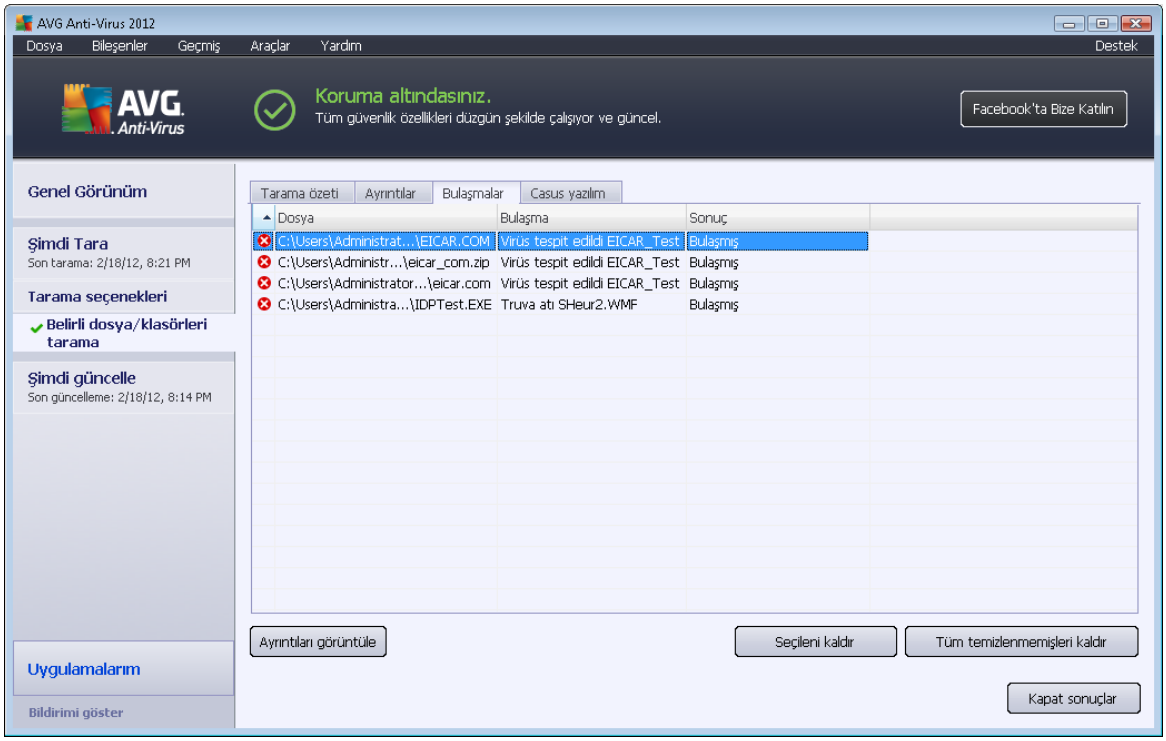
- tespit edilen virüs bulaşmaları / casus yazılım
- silinen virüs bulaşmaları / casus yazılım
- kaldırılamayan ya da temizlenemeyen virüs bulaşması / casus yazılım sayısı

Buna ek olarak, tarama başlangıcı hakkında tarih ve zaman verileri, toplam taranan nesne sayısı, tarama süresi ve tarama sırasında ortaya çıkan hataların sayısı hakkında da bilgi bulabilirsiniz.

Kontrol düğmeleri

Bu iletişim kutusunda sadece bir adet düğme bulunmaktadır. ***Sonuçları kapat*** düğmesi Tarama sonuçlarına genel bakış iletişim kutusuna dönmenizi sağlar.

11.7.2. Bulaşma Sekmesi



Tarama sırasında bir virüs bulaşması tespit edilirse ilgili***Bulaşmalar*** sekmesi sadece ***Tarama Sonuçları*** iletişim kutusunda görüntülenir. Sekme, şu bilgileri sağlayan üç bölüme ayrılmıştır:

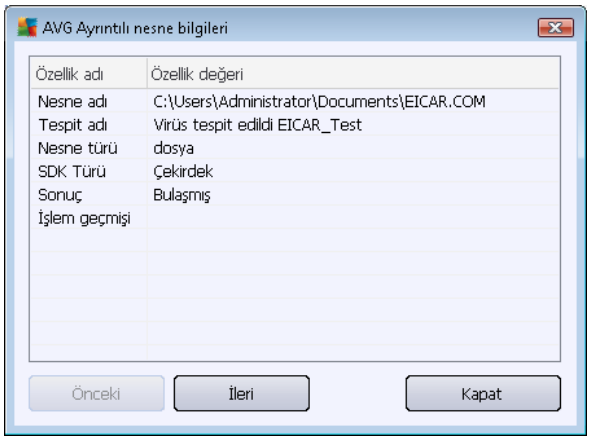
- ***Dosya*** – bulaşmış nesnenin orijinal konumunun tam dizin yolu
- ***Bulaşmalar*** – tespit edilen virüsün adı(*belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi Virüs Ansiklopedisine danışın*)
- ***Sonuç*** – tarama sırasında tespit edilen bulaşmış nesnenin mevcut durumunu tanımlar:
    - ***Bulaşanlar*** – bulaşan nesne tespit edildi ve orijinal konumunda bırakıldı (*örneğin belirli bir tarama işlemi sırasında otomatik temizleme seçeneğini devre dışı bıraktıysanız*)
    - ***Temizlenenler*** – bulaşmış nesne otomatik olarak temizlenmiştir ve orijinal konumunda bırakılmıştır
    - ***Virüs Kasasına Taşınanlar*** – bulaşmış nesne Virüs Kasası karantinasına taşınmıştır
    - ***Silinenler*** – bulaşmış nesne silinmiştir
    - ***PUP istisnalarına eklenenler*** – *bulgu bir istisna olarak değerlendirilmiş ve PUP istisnaları listesine eklenmiştir (gelişmiş ayarların PUP İstisnaları penceresinden yapılandırılır)*

- ***Kilitli dosya – taranmayanlar*** - ilgili nesne kilitlidir ve bu nedenle AVG tarafından taranamamaktadır
- ***Potansiyel olarak tehlikeli nesne*** - nesnenin potansiyel anlamda tehlikeli olduğu tespit edilmiş fakat nesneye herhangi bir virüs bulaşmamıştır (*örneğin makro içeriyor olabilir*); bilgi sadece uyarı amaçlıdır
- ***Eylemi tamamlamak için bilgisayarınızın yeniden başlatılması gerekmektedir*** - bulaşmış nesne silinememektedir ya da nesneyi tamamen silmek için bilgisayarınızın yeniden başlatılması gerekmektedir

Kontrol düğmeleri

Bu iletişim kutusunda kullanılabilir üç kontrol düğmesi var:

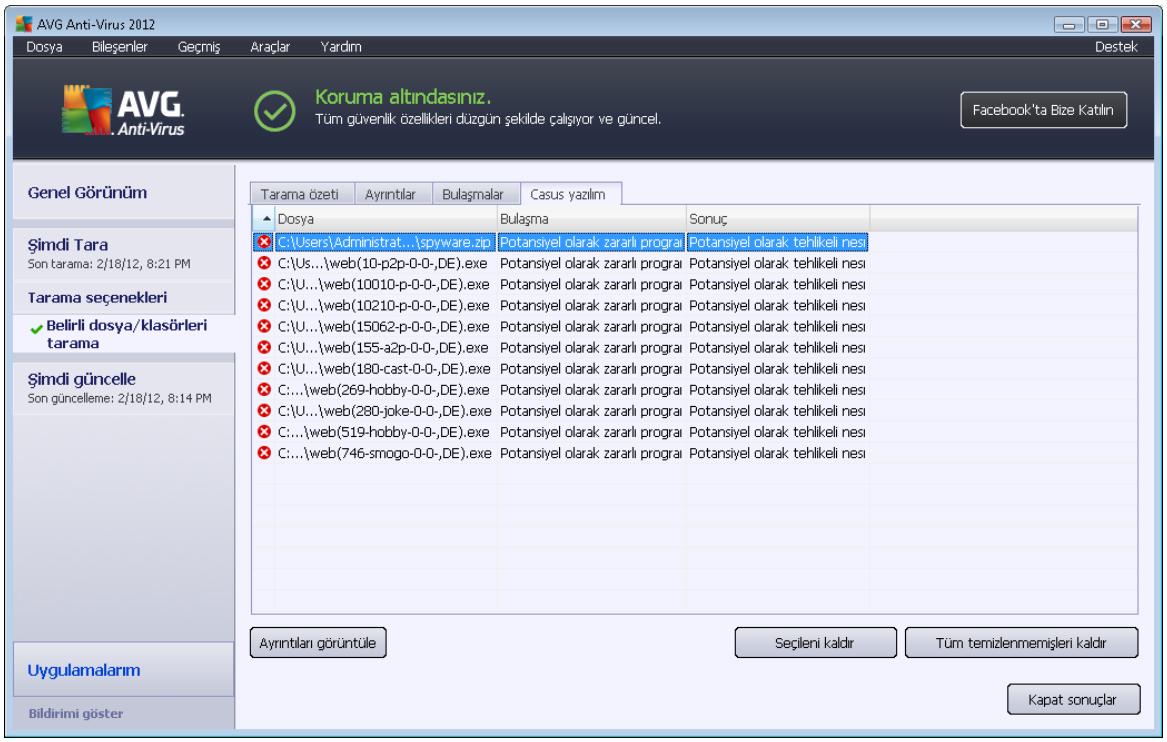
- ***Ayrıntıları görüntüle*** – düğme Ayrıntılı nesne bilgileri adlı yeni bir iletişim kutusu penceresi açar:



  Bu iletişim kutusunda, tespit edilen bulaşıcı nesne ile ilgili ayrıntılı bilgiler bulabilirsiniz (*örn. bulaşmış nesnenin adı ve konumu, nesne tipi, SDK tipi, tespit sonucu ve tespit edilen nesne ile ilgili eylemlerin geçmişi*). ***Geri*** /***İleri*** düğmelerini kullanarak belirli bulgular hakkında ayrıntılı bilgi görüntüleyebilirsiniz. Bu iletişim kutusunu kapatmak için ***Kapat*** düğmesini tıklatın.

- ***Seçileni kaldır*** – seçili nesneyi Virüs Kasası
- ***Temizlenmeyen tüm bulaşmaları sil*** – bu düğme temizlenemeyen ya da Virüs Kasası
- ***Sonuçları kapat*** - ayrıntılı bilgi penceresini kapatır ve Tarama sonuçlarına genel bakış iletişim kutusuna döner

11.7.3. Casus Yazılım Sekmesi



Tarama sırasında bir casus yazılım tespit edilirse ilgili***Casus Yazılım*** sekmesi sadece ***Tarama Sonuçları*** iletişim kutusunda görüntülenir. Sekme, şu bilgileri sağlayan üç bölüme ayrılmıştır:

- ***Dosya*** – bulaşmış nesnenin orijinal konumunun tam dizin yolu
- ***Bulaşmalar*** – tespit edilen casus yazılımınadı *(belirli virüs türleri hakkında ayrıntılı bilgi almak için lütfen çevrimiçi Virüs Ansiklopedisine bakın)*
- ***Sonuç*** – tarama sırasında tespit edilen nesnenin mevcut durumunu tanımlar:
    - ***Bulaşanlar*** - *bulaşan nesne tespit edildi ve orijinal konumunda bırakıldı (örneğin belirli bir tarama işlemi sırasında otomatik temizleme seçeneğini devre dışı bıraktıysanız)*
    - ***Temizlenenler*** - bulaşmış nesne otomatik olarak temizlenmiştir ve orijinal konumunda bırakılmıştır
    - ***Virüs Kasasına Taşınanlar*** - bulaşmış nesne Virüs Kasası karantinasına taşınmıştır
    - ***Silinenler*** – bulaşmış nesne silinmiştir
    - ***PUP istisnalarına eklenenler*** – *bulgu bir istisna olarak değerlendirilmiş ve PUP istisnaları listesine eklenmiştir (gelişmiş ayarların PUP İstisnaları penceresinden yapılandırılır)*
    - ***Kilitli dosya – taranmayanlar*** – ilgili nesne kilitlidir ve bu nedenle AVG tarafından

taranamamaktadır

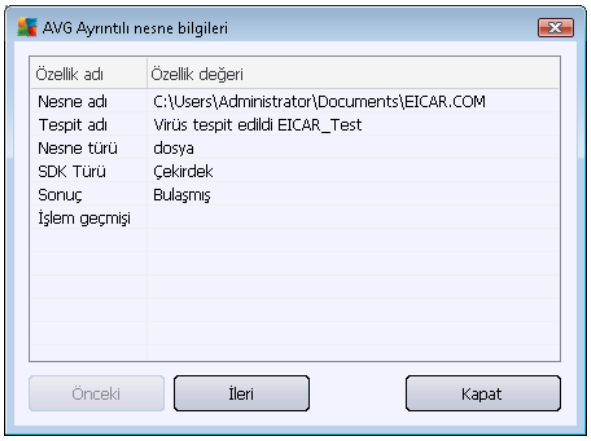
- ***Potansiyel olarak tehlikeli nesne*** - nesnenin potansiyel anlamda tehlikeli olduğu tespit edilmiş fakat nesneye herhangi bir virüs bulaşmamıştır (örneğin makro içeriyor olabilir); bilgi sadece uyarı amaçlıdır

- ***Eylemi tamamlamak için bilgisayarınızın yeniden başlatılması gerekmektedir*** - bulaşmış nesne silinememektedir ya da nesneyi tamamen silmek için bilgisayarınızın yeniden başlatılması gerekmektedir

Kontrol düğmeleri

Bu iletişim kutusunda kullanılabilir üç kontrol düğmesi var:

- ***Ayrıntıları görüntüle*** – düğme Ayrıntılı nesne bilgileri adlı yeni bir iletişim kutusu penceresi açar:



  Bu iletişim kutusunda, tespit edilen bulaşıcı nesne ile ilgili ayrıntılı bilgiler bulabilirsiniz (*örn. bulaşmış nesnenin adı ve konumu, nesne tipi, SDK tipi, tespit sonucu ve tespit edilen nesne ile ilgili eylemlerin geçmişi*). ***Geri*** /***İleri*** düğmelerini kullanarak belirli bulgular hakkında ayrıntılı bilgi görüntüleyebilirsiniz. Bu iletişim kutusunu kapatmak için ***Kapat*** düğmesini tıklatın.

- ***Seçileni kaldır*** – seçili nesneyi Virüs Kasası

- ***Temizlenmeyen tüm bulaşmaları sil*** – bu düğme temizlenemeyen ya da Virüs Kasası

- ***Sonuçları kapat*** - ayrıntılı bilgi penceresini kapatır ve Tarama sonuçlarına genel bakış iletişim kutusuna döner

11.7.4. Uyarılar Sekmesi

Uyarılar sekmesinde, tarama sırasında tespit edilip "şüphe duyulan" nesneler (*tipik olarak dosyalar*) hakkında çeşitli bilgiler görüntülenir. Resident Shield tarafından tespit edildiği zaman tespit edilen dosyalara erişim engellenir. Bu şekilde tespit edilen buluntulardan bazıları gizli dosyalar, tanımlama bilgileri, şüpheli kayıt anahtarları, parola korumalı belgeler ya da arşivlerdir. Bu dosyalar

bilgisayarınıza ya da güvenliğinize karşı doğrudan tehlike teşkil etmez. Bu dosyalar hakkında verilen bilgiler, bilgisayarınızda reklam yazılımı ya da casus yazılım tespit edildiği durumlarda oldukça yararlıdır. Test sonuçlarında yalnızca **AVG Anti-Virus** tarafından tespit edilen Uyarılar varsa, işlem yapmak gerekmez.

Aşağıda bu tür nesnelere ilişkin en yaygın örnekler kısaca açıklanmıştır:

- ***Gizli dosyalar*** - Gizli dosyalar, Windows'da varsayılan olarak görülmez durumdadır ve bazı virüsler ya da diğer tehditler dosyalarını söz konusu gizli dosyalara kaydederek algılanma ihtimallerini ortadan kaldırmaya çalışır. **AVG Anti-Virus** zararlı olabileceğinden şüphelendiğiniz gizli bir dosya rapor ederse, bunu Virüs Kasasına taşıyabilirsiniz.
- ***Tanımlama Bilgileri*** – Tanımlama bilgileri, kullanıcılara ilişkin bilgileri kaydetmek ve daha sonra söz konusu bilgileri web site şablonlarını yükleme ve kullanıcı adını girmek üzere web siteleri tarafından kullanılan düz metin dosyalarıdır.
- ***Şüpheli kayıt anahtarları*** - Bazı kötü amaçlı yazılımlar, sistem başlatıldığında yüklendiğinden emin olmak ya da işletim sistemi üzerindeki etkisini artırmak üzere bilgilerini Windows kayıt defterine kaydeder.

11.7.5. Rootkit'ler Sekmesi

Rootkit'ler sekmesi Tüm Bilgisayar Taraması dahilinde gerçekleşen anti-rootkit taramasında tespit edilen rootkit'ler hakkında bilgileri görüntüler.

Rootkit, sistem yöneticisinin izni olmaksızın yasal olmayan şekillerde bilgisayar sisteminin kontrolünü ele almak için tasarlanmış bir programdır. Kök dizin, donanım üzerinde çalışan işletim sisteminin kontrolünü ele geçirmeyi hedeflediği için donanımsal açıdan erişime gerek duymaz. Kök dizinler genellikle standart işletim sisteminin güvenlik mekanizmalarını dönüştürerek ya da istila ederek sistem üzerindeki varlıklarını gizlerler. Çoğunlukla Truva Atı biçimindedirler, dolayısıyla kullanıcıları sistemleri üzerinden çalışacak kadar güvenli olduklarına inandırırlar. İzleme programlarının çalışan işlemlerini gizlemek ya da işletim sisteminin sistem bilgilerini ya da dosyalarını saklamak, bunu sağlamak için kullanılan teknikler arasında bulunmaktadır.

Bu sekmenin yapısı temel olarak Bulaşmalar sekmesi ya da Casus Yazılım sekmesi ile aynıdır.

11.7.6. Bilgi Sekmesi

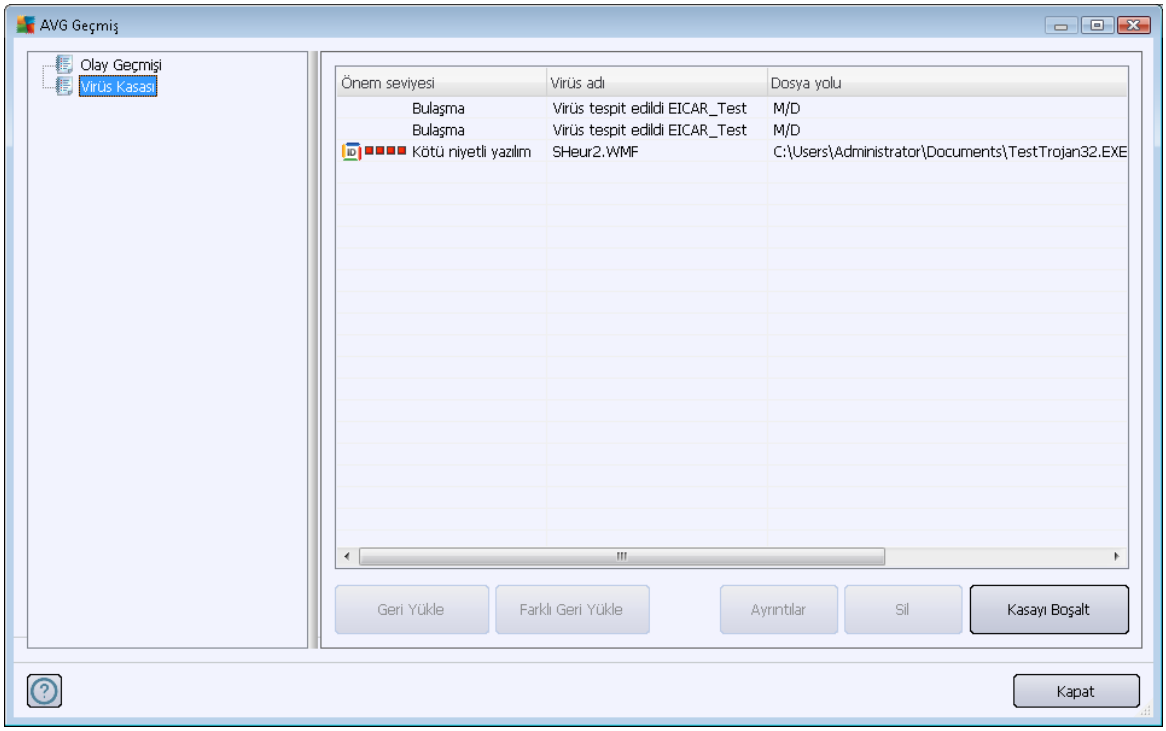
Bilgi sekmesinde, bulaşma ya da casus yazılım şeklinde sınıflandırılamayan "buluntular" hakkında bilgi bulunmaktadır. Bunlar tehlikeli şeklinde etiketlenebilir ancak söz konusu öğeler hususunda dikkatli olmalısınız. **AVG Anti-Virus** taraması, virüs bulaşmamış ancak şüpheli dosyaları tespit edebilir. Bu dosyalar Uyarı veya Bilgi olarak rapor edilir.

Önem derecesi ***Bilgiler*** aşağıdaki nedenlerden birine bağlı olarak rapor edilebilir:

- ***Çalışma zamanı paketli*** - Dosya, dosyanın taranmasını önleme çabası olarak değerlendirilebilecek yaygın olmayan paketleyicilerinden biri kullanılarak paketlenmiştir. Diğer bir yandan bu tür dosyalar her rapor edildiğinde virüs teşkil etmezler.
- ***Çalışma zamanı paketi yinelemeli*** – Yukarıdakine benzerdir, ancak yaygın yazılımlar arasında nispeten daha az sıklıkta kullanılır. Söz konusu dosyalar şüphelidir ve kaldırılmaları ya da incelenmeleri için bize gönderilmeleri göz önünde bulundurulmalıdır.

- ***Parola ile korunan arşiv ya da belge*** - Parola ile korunan dosyalar, **AVG Anti-Virus** (*ya da genellikle diğer kötü amaçlı yazılımlara karşı koruma programları*) tarafından taranamaz.
- ***Makro içeren belge*** – Rapor edilen belge, zararlı olabilecek makrolar içermektedir.
- ***Gizli uzantı*** - Gizli uzantılı dosyalar resimler gibi görünebilir, ancak aslında çalıştırılabilir dosyalar olabilir (*örn resim.jpg.exe*). İkinci uzantı, varsayılan olarak Windows'da görünür değildir ve **AVG Anti-Virus** yanlışlıkla açılmalarını engellemek için bu tür dosyaları rapor eder.
- ***Uygun olmayan dosya yolu*** - Önemli bir sistem dosyası varsayılan yoldan başka bir yerden çalışıyorsa (*örn. winlogon.exe Windows klasöründen başka bir yerde çalışıyorsa*) bu durumu rapor eder.**AVG Anti-Virus** Bazı durumlarda virüsler, sistemde fark edilmemek için standart sistem işlemlerinin adını alır.
- ***Kilitli dosya*** - Rapor edilen dosya kilitli, bu yüzden **AVG Anti-Virus**tarafından taranamıyor. Bu, genellikle bir dosyanın sistem tarafından kullanılmakta olduğu anlamına gelir (*örn. takas dosyası*).

11.8. Virüs Kasası



Virüs Kasası AVG taramaları sırasında tespit edilen şüpheli/bulaşmış nesnelerin yönetilmesi için güvenli bir ortamdır. Tarama sırasında bulaşmış bir nesne tespit edildikten sonra AVG, söz konusu bulaşmayı otomatik olarak temizleyemiyorsa şüpheli nesne hakkında ne yapmak istediğiniz sorulur. Önerilen çözüm, nesneyi daha sonra ilgilenmek üzere ***Virüs Kasasına*** taşımaktır. ***Virüs Kasası***'nı satın almanın ana amacı silinen bir dosyayı belirli bir süre için saklamasıdır, böylece dosyayı orijinal konumunda artık istemediğinizden emin olabilirsiniz. Dosyanın yokluğu sorun oluşturuyorsa, bu

dosyayı analize gönderebilir veya orijinal konumuna geri yükleyebilirsiniz.

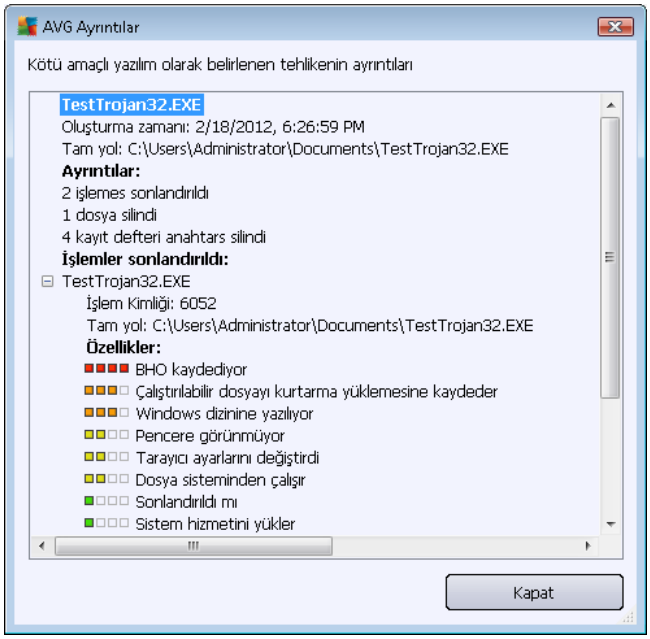
Virüs Kasası arayüzü, yeni bir pencerede açılır ve karantina altındaki bulaşmış nesneler hakkında genel bilgi içerir:

- ***Önem Düzeyi*** – **AVG Anti-Virus** uygulamanızın içine Kimlik Koruma bileşenini yüklemeye karar verdiğinizde, ilgili tehdidinin önem seviyesinin kusursuzdan (■□□□) çok tehlikeliye kadar (■■■■) dört seviyeli bir ölçekte grafik olarak gösterimi ve bulaşma türü hakkındaki bilgiler (*bulaşma seviyesine bağlı olarak – listelenen tüm nesnelere virüs bulaşmıştır veya bulaşma olasılığı vardır*)
- ***Virüs Adı*** – Virüs Ansiklopedisi*'ne göre (çevrimiçi) tespit edilen bulaşmanın adını görüntüler*
- ***Dosya yolu*** – Bulaşmış dosyanın orijinal konumuna giden tam yol
- ***Orijinal nesne adı*** – Tabloda listelenmekte olan tespit edilmiş nesneler, tarama işlemi sırasında AVG tarafından verilen standart isim ile etiketlenmiştir. Nesnenin bilinmeyen farklı bir adı olması halinde (*Örn. bir e-posta ekinin adının ekin mevcut içeriğine yanıt vermemesi halinde*), söz konusu isim bu sütunda gösterilecektir.
- ***Saklama tarihi*** – Şüpheli dosyanın tespit edildiği ve Virüs Kasası'na kaldırıldığı tarih ve saat

Kontrol düğmeleri

Virüs Kasası arayüzünden ulaşabileceğiniz kontrol düğmeleri şunlardır:

- ***Geri Yükle*** - bulaşmış dosyayı sabit diskinizdeki orijinal konumuna geri yükler
- ***Farklı Geri Yükle*** – bulaşmış dosyayı seçili klasöre taşır
- ***Ayrıntılar*** – bu düğme yalnızca Identity Protection tarafından algılanan tehlikeler içindir. Tıklatıldığında, tehlike ayrıntılarının özet genel görünümünü görüntüler (*hangi dosyalar/ işlemler etkilendi, işlemin özellikleri vb.*). IDP'nin algıladığı dışındaki diğer tüm öğeler için, bu düğmenin gri ve devre dışı olduğunu unutmayın!



- ***Sil*** – bulaşmış dosyayı ***Virüs Kasasından*** tamamen ve geri dönüştürülemeyecek şekilde siler

- ***Kasayı Boşalt*** – ***Virüs Kasası*** içeriğini tamamen temizler. Dosyaları ***Virüs Kasası***'ndan kaldırdığınızda, bu dosyalar diskten geri alınmayacak biçimde kaldırılır (*Geri Dönüşüm Kutusu'na taşınmaz*).

12. AVG Güncellemeleri

Güvenlik yazılımlarının hiçbiri, rutin olarak güncellenmediği takdirde sizi çeşitli tehlikelere karşı korumayı garanti edemez! Virüs yazarları, yazılım ve işletim sistemlerinde yararlanabilecekleri güvenlik açıkları aramaktadır. Her gün yeni virüsler, yeni kötü amaçlı yazılımlar ve yeni bilgisayar saldırıları gerçekleştirilmektedir. Bu nedenle yazılım geliştiricileri,tespit edilen güvenlik açıklarını kapatmak üzere devamlı olarak güncellemeler ve güvenlik paketleri yayınlamaktadır.

Yeni ortaya çıkan tehditler ve bunların yayılma hızı dikkate alındığında **AVG Anti-Virus** ürününüzü düzenli olarak güncellemek hayati bir önem kazanır. En iyi çözüm, otomatik güncellemenin yapılandırıldığı program varsayılan ayarlarına güvenmektir. **AVG Anti-Virus** ürününüzün virüs veritabanı güncel değilse, programın en yeni tehditleri tespit edemeyeceğini lütfen unutmayın!

AVG'nizi rutin olarak güncellemeniz çok önemlidir! Gerekli virüs tanımı güncellemelerinin mümkün ise her gün yapılması gerekmektedir. Daha az önem taşıyan program güncellemeleri haftada bir yapılabilir.

12.1. Güncelleme başlatma

Mümkün olan en yüksek güvenliği sağlamak için, **AVG Anti-Virus** varsayılan olarak her dört saatte bir yeni güncellemeleri kontrol etmeye ayarlanmıştır. AVG güncellemeleri belirli bir takvime göre değil yeni tehditlerin miktarı ve ciddiyetine göre yayınlandığından, bu kontrol AVG virüs veritabanınızın sürekli güncel tutulması açısından çok önemlidir.

Güncelleme başlatmalarının sayısını azaltmak istiyorsanız, kendi güncelleme başlatma parametrelerinizi ayarlayabilirsiniz. Ancak, günde en az bir kez güncellemeyi başlatmanız kesinlikle önerilir! Yapılandırma Gelişmiş ayarlar/Programlar bölümünde, aşağıdaki iletişim kutularından düzenlenebilir:

- Güncelleme planı tanımlamalar
- Program güncelleme programı

Yeni güncelleme dosyalarını hemen kontrol etmek istiyorsanız, ana kullanıcı arayüzündeki Şimdi güncelle hızlı bağlantısını kullanın. Bu bağlantıya her zaman herhangi bir kullanıcı arayüzü iletişim kutusundan ulaşabilirsiniz.

12.2. Güncelleme ilerlemesi

Güncellemeye başladıktan sonra AVG, yeni güncelleme dosyasının olup olmadığını aramaya başlayacaktır. Varsa, **AVG Anti-Virus** dosya ve güncellemeleri indirmeye başlar ve güncelleme işlemini kendisi başlatır. Güncelleme işlemi sırasında güncelleme işleminin ilerleyişinin yanı sıra ilgili istatistiki parametreleri de görüntüleyebileceğiniz ***Güncelleme*** arayüzüne yeniden yönlendirileceksiniz (*güncelleme dosyasının boyutu, alınan veriler, indirme hızı, kalan süre...*):

***Not**: Her AVG program güncellemesi başlatılmadan önce sistem geri yükleme noktası oluşturulur. Güncelleme işleminin başarısız olması ve işletim sisteminizin çökmesi halinde işletme sisteminizi bu noktaya geri döndürebilirsiniz. Seçeneğe Windows menüsü yoluyla erişilebilir: Başlat / Tüm Programlar / Aksesuarlar / Sistem araçları / Sistem Geri Yükleme. Yalnızca deneyimli kullanıcılara önerilir!*

12.3. Güncelleme seviyeleri

AVG Anti-Virus seçilebilecek iki güncelleme düzeyi sunar:

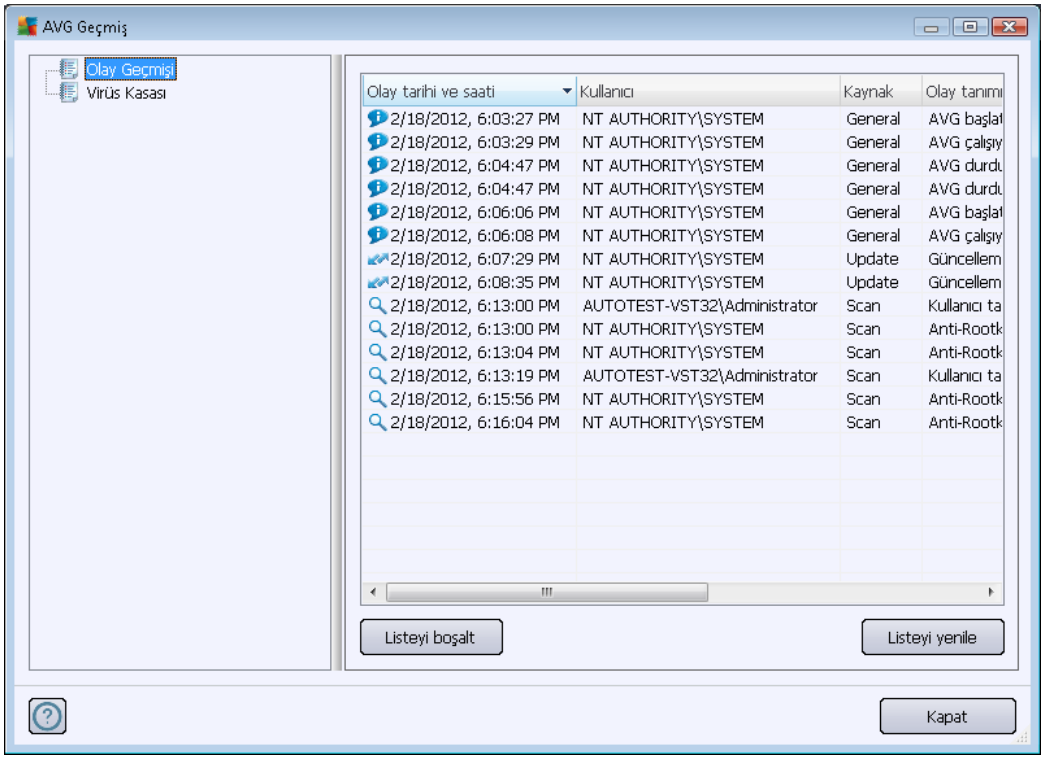
- ***Tanım güncellemeleri*** güvenilir virüsten koruma için gerekli değişiklikleri içerir. Genellikle kodu değiştirmez ve yalnızca tanımlama veritabanını günceller. Bu güncelleme sunulur sunulmaz yüklenmelidir.
- ***Program güncellemeleri*** çeşitli program değişikliklerini, onarımları ve iyileştirmeleri içerir.

Bir güncelleme programlarken, her iki güncelleme düzeyi için de belirli parametreler tanımlamak mümkündür:

- Güncelleme planı tanımlamalar
- Program güncelleme programı

***Not:** Programlanmış bir program güncellemesinin zaman çakışması oluşursa ve programlı tarama gerçekleşirse, güncelleme işlemi daha yüksek önceliğe sahiptir ve tarama kesilir.*

13. Olay Geçmişi



Geçmiş iletişim kutusuna sistem menüsü üzerinden ***Geçmiş/Olay Geçmişi Günlüğü*** öğesi aracılığıyla ulaşabilirsiniz. Bu iletişim kutusunda, **AVG Anti-Virus** uygulamasının çalışması sırasında oluşan önemli olayların bir özetini bulabilirsiniz. ***Geçmiş*** aşağıdaki etkinlik türlerini kaydeder:

- AVG uygulamasının güncellemeleri hakkında bilgi
- Tarama başlangıcı, sonu veya taramanın durdurulması hakkında bilgi (*otomatik olarak gerçekleştirilen taramalar dahil olmak üzere*)
- Olay konumu da dahil olmak üzere virüs tespitine bağlı olaylar hakkında bilgi (*Resident Shield veya tarama* ile)
- Diğer önemli olaylar

Her olay için, şu bilgiler listelenir:

- ***Olay tarihi ve zamanı*** olayın gerçekleştiği kesin tarihi ve zamanı belirtir
- ***Kullanıcı*** olayın gerçekleştiği sırada oturum açmış olan kullanıcının adını gösterir
- ***Kaynak***, kaynak bileşeni veya AVG sisteminin olayı tetikleyen bölümü hakkında bilgi verir
- ***Olay açıklaması***, tam olarak ne olduğu hakkında kısa bir açıklama sağlar

Kontrol düğmeleri

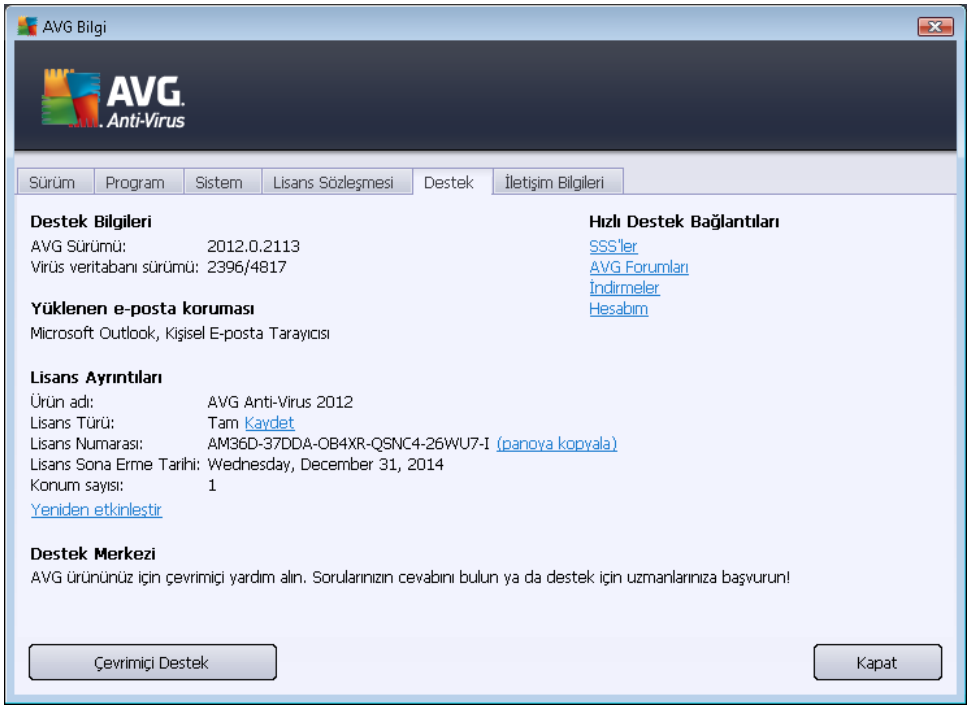
- ***Listeyi boşalt*** - olaylar listesindeki tüm girişleri silmek için bu düğmeye basın
- ***Listeyi yenile*** - olaylar listesindeki tüm girişleri güncellemek için bu düğmeye basın

14. SSS ve Teknik Destek

AVG Anti-Virus uygulamanızın satışıyla ilgili veya teknik sorunlarınız olması durumunda yardım için birçok yol mevcuttur. Lütfen aşağıdaki seçeneklerden birini seçin:

- ***Destek Alın***: Doğrudan AVG uygulaması içinden AVG web sitesindeki (http://www.avg.com/) özel bir müşteri destek sayfasına erişebilirsiniz. AVG web sitesindeki destek seçeneklerine erişmek için ***Yardım / Destek Alın*** ana menü öğesini seçin. Devam etmek için lütfen web sayfasındaki talimatları izleyin.

- ***Destek (ana menü bağlantısı)***: AVG uygulama menüsünde (*ana kullanıcı arayüzünün en üstünde*) yardım bulmaya çalışırken ihtiyacınız olabilecek tüm bilgileri içeren yeni bir iletişim kutusu açan ***Destek*** bağlantısı bulunur. İletişim kutusunda kurulu AVG programınız (*program / veritabanı sürümü*) ile ilgili temel bilgiler, lisans ayrıntıları ve hızlı destek bağlantıları listesi bulunur:



- ***Yardım dosyasında sorun giderme***: Doğrudan **AVG Anti-Virus** *içindeki yardım dosyasından erişilebilen yeni bir* ***Sorun giderme*** bölümü mevcuttur (yardım dosyasını açmak için uygulamadaki herhangi bir pencerede F1 tuşuna basın). Bu bölüm, bir kullanıcı teknik bir sorun hakkında profesyonel yardım aradığında en sık karşılaşılan durumlar hakkında bir liste sunar. Lütfen sizin sorununuzu en iyi açıklayan durumu seçin ve sorunun çözümüne dair ayrıntılı talimatlar almak için tıklatın.

- ***AVG web sitesi Destek Merkezi***: Sorunuzun çözümünü AVG web sitesinde de (http://www.avg.com/) arayabilirsiniz. ***Destek Merkezi*** bölümünde hem satış sorunları hem de teknik sorunlarla ilgili tematik olarak gruplandırılmış konular bulabilirsiniz.

- ***Sık sorulan sorular***: AVG web sitesinde (http://www.avg.com/) ayrı ve çok ayrıntılı bir sık sorulan sorular bölümü de bulabilirsiniz. Bu bölüme ***Destek Merkezi / SSS*** menü

seçeneğinden erişilebilir. Burada da tüm sorular satış, teknik ve virüs kategorileri şeklinde sınıflandırılmıştır.

- ***Virüsler ve tehditler hakkında***: Virüs sorunlarına ayrılmış özel bir AVG web sitesi (http://www.avg.com/) bölümü *(web sayfasına ana menüdeki Yardım / Virüsler ve Tehditler Hakkında seçeneğinden erişilebilir)*. Çevrimiçi tehlikeler hakkında sınıflandırılmış bilgiler sunan bir sayfaya girmek için menüde ***Destek Merkezi / Virüsler ve tehlikeler hakkında*** öğesini tıklatın. Virüs, casus yazılım silme talimatları ve nasıl güvenli kalacağınıza dair öneriler de bulabilirsiniz.

- ***Tartışma forumu***: Ayrıca http://forums.avg.com adresindeki AVG kullanıcıları tartışma forumunu kullanabilirsiniz.