AVAST! antivirus

Professional Edition

Version 4.8

Kullanma klavuzu

İçindekiler

Giriş

Avast! antivirus Professional Edition versiyon 4.8

Bir çok ödle sahip olan avast! antivirus, yüksek teknolojisini mükkemmel bir sinerji ile birleştirerek değerli veri ve programlarınızı çeşitli zararlılardan ve virüslerden korur. Windows tabanlı bilgisayarların korunmasında sınıfında en iyi koruma çözümüdür.

Avast! antivirus anonim şirketi antispyware teknolojisi, West Coast Lab's Checkmark tarafından sertifikalıdır. Yerleşik anti-rootkit ve kendi kendini koruyabilme özelliklerine sahiptir.

ALWIL Software a.s. Hakkında

ALWIL Software, 1988 den beri antivirüs programları üretmekte ve geliştirmektedir. Ürün yelpazesini devamlı geliştirilmesi ve ödüllerine her zaman bir yenisini eklemesiyle avast! ,bugün, piyasasında en ünlü ve en çok test edilen antivirüs ürünü haline gelmiştir.

Çek Cumhuriyeti'nin başkenti Pragta bulunan ALWIL Software, başlıca işletim sistemlerini ve başlıca aygıtları koruyan antivirüs ürünleri üretmekte ve geliştirmektedir. Şirket ve ürünleri hakkında ayrıntılı bilgi için www.avast.com adresini ziyaret edebilirsiniz.

avast!® ABD'de ve diğer ülkelerde ALWIL Software a.s. adı altında bir ticari markadır.

Yardım

Avast! antivürüs programları ile herhangi bir teknik sorun yaşarsanız Yardım Merkezimize http://support.avast.com adresinden ulaşabilirsiniz.

- Knowledgebase seçtiğinizde sıkça sorulan soru ve cevaplarına ulaşabilirsiniz.
- Ayrıca avast! Support forumlarını ziyaret edebilirsiniz. Burada sizinle aynı sorunu yaşamış olan kullanıcılara ulaşabilir, tartışabilir ve yeni şeyler öğrenebilirsiniz. Foruma katılmak için kayıt olamanız gerekmektedir. Kayıt işlemi son derece hızlıdır. Kayıt olmak için lütfen http://forum.avast.com/ adresini ziyaret ediniz.

Sorununuz hala çözülmedi ise "Submit a ticket" butonuna tıklayarak teknik destek servisimize mesaj gönderebilirsiniz. Bunun için kayıt olmanız gerekmektedir. Bunu yanı sıra bize sorun bildirirken ekleyebildiğiniz kadar detay eklemenizi tavsiye ediyoruz.

Tehlikeler

Virüsler, casus yazılımlar (spyware), rootkitler ve zararlı yazılımların her türü kötücül yazılım (malware) olarak bilinir ve bazen kötü niyetli yazılım (badware) olarak da bahsedilir.

Virüs nedir?

Bilgisayar virüsü, genellikle kötü amaç taşıyan, bilgisayardan bilgisayara kendilerini yayan bir tür yazılımdır. Virüsler sisteme zarar verebilir, değerli verileri yok edebilir,casus yazılım, rootkit veya diğer zararlı yazılımları savunmasız sistemlere yüklemek için kullanılabilir.
Hasarı önlemek için en önemli yol, güncellemelerinin sık sık yapıldığı ve işletim sistemi için en son güvenlik önlemlerinin eklendiği bir antivirüs programı kullanmaktır. Bazen yasal görünümlü yazılımın içinde malware gizlenmektedir. Bu nedenle kullanıcılar internetten yükledikleri yazılım kaynağının güvenilirliğinden emin olmalıdırlar.

Spyware nedir?

Spyware/casus yazılım; bilgisayara yüklenmiş, kullanıcının haberi olmaksızın önemli bilgileri ele geçirme amacında olan yazılımlardır. Bu bilgiler banka bilgileri, kimlik bilgileri. şifreler v.s. gibi önemli bilgilerdir.
Bu yazılımlar daha çok organize suç örgütleri tarafından geliştirilmektedir.

Rootkit nedir?

Rootkitler bilgisayara kullanıcının haberi olmaksızın kurulan, kendilerini ve aktivitelerini gizleyen programlardır. Rootkitler hem ev bilgisayrlarında hem de şirket ağlarında bulunması ve kaldırılması oldukça güç olan, belirli güvenlik riski olarak da tanımlanabilir.
Rootkitler genellikle bir virüs tarafından ya da diğer kötücül yazılım tarafından (truva atı gibi) yüklenir. Bu nedenle kullanıcılara önemle devamlı güncellenen antivirüs/spyware yazılım versiyonlarından birini kullanmalarını öneriyoruz ki avast! 4.8 hali hazırda bu versiyonlardan birisidir.

avast! antivirüs'ün ana özellikleri

Avast! ALWIL Software ürün yelpazesinden bir çok ödül kazanmış olup, ICSA LABs ve Checkmark sertifikalarına sahiptir (antivirüs ve antimalware). Avast! antivirüs tehlikeli virüsleri 100% tarayarak, sıklıkla Virüs Bulletin %100 ödüllerini kazanmıştır ve kazanmaya devam edecektir. Bunun yanı sıra Secure Computing Award ödüllerini de sıklıkla almaktadır.

Avast! antivirüs dünya çapında 75 milyonun üzerinde kullanıcı kitlesine sahiptir. Program küçük ve etkili bir sisteme sahip olup, kendini ve virüs tanımlamalarını otomatik olarak günceller.

Avast! yüksek teknolojisi ile size her türlü malware korumasını sağlar. Aşağıdaki tabloda avast! Home Edition ve avast! Professional Editionun karşılaştırmasını yapabilirsiniz.

Anahtar özellikler	Home Edition	Professional Edition
Yüksek teknolojili antivirüs motoru üzerinde Antivirüs Çekirdeği	**evet**	**evet**
Güçlü yerleşik koruma	**evet**	**evet**
Yerleşik anti-spyware	**evet**	**evet**
Yerleşik rootkit taraması	**evet**	**evet**
Kendini savunabilme	**evet**	**evet**
Olağanüstü otomatik güncellemeler	**evet**	**evet**
Şüpheli dosyaların depolanması için Virüs Karantinası	**evet**	**evet**
Sistem uyumu	**evet**	**evet**
Uyumlu virüs temizleyicisi	**evet**	**evet**
Komut satırı tarayıcısı	**hayır**	**evet**
Komut dosyası engelleyici	**hayır**	**evet**
PUSH güncellemeleri	**hayır**	**evet**
Gelişmiş arayüzde görev oluşturma ve programlama	**hayır**	**evet**

Antivirüs Çekirdeği

Antivirüs çekirdeği programın temelini oluşturmaktadır. Avast! antivirüs çekirdeğinin son versiyonu sıradışı tarama kabiliyetive yüksek performansla kombine edilmiştir. Virüsler kullanıcıdan kullanıcıya yayılmakta iken, avast!'tan, bu virüsleri ve Truva atlarını 100% taramasını rahatlıkla bekleyebilirsiniz. Çekirdek ICSA Labs tarafından sertifikalıdır, Virus Bulletin dergisinin testlerinde sıklıkla yer almakta, ve yine sıklıkla VB100 ödüllerini kazanmaktadır.

Yerleşik koruma (ya da "erişimde" koruma)

Yerleşik koruma, bilgisayar sisteminin gerçek zamanlı olarak korunmasıdır ve bu özellik günümüz antivirüs programlarının vazgeçilmez özelliklerinden biridir. Avast!ın yerleşik koruması "yerleşik modüllerin" kombinasyonundan oluşmaktadır ve bu koruma virüsün sisteme henüz zarar veremeden taranmasını sağlar.

Yerleşik anti-spyware teknolojisi

Avast! antivirüs, şimdi, değerli program ve verilerinizi daha iyi koruyabilmek için, West Coast Labs Checkmark sertifikalı yerleşik anti-spyware teknolojisine sahiptir.

Yerleşik anti-rootkit teknolojisi

Sınıfının lideri GMER teknolojisi üzerine kurulu avast! sisteminizi rootkit tehlikelerinden korur. Rootkit bulunduğu taktirde, program öncelikle rootkiti etkisiz hale getirir. Güvenli bir şekilde bilgisayara zarar vermeden rootkiti kaldırabildiği taktirde rootkit artık bilgisayarınızda yoktur. avast! antivirüs bilgisayarınızı rootkitlerden sonsuz korumak için devamlı güncellenen virüs veri tabanına sahiptir.

Kendini koruyabilme özelliği

Bazı virüsler bilgisayarınızda bulunan antivirüs programını kapatıp etkisiz hale getirebilir. Avast! bu son tehlikelere karşı bile bilgisayarınızı korumak için sınıfında en iyi olup (avast! teknolojisi üzerine kurulu) yerleşik kendini koruyabilme özelliğine sahiptir.

Otomatik güncellemeler

Otomatik güncelleme, antivirüs ürünlerinde bir diğer önemli noktadır.Virüs veri tabanı ve programın kendisi otomatik olarak güncellenebilir. Güncellemeler yeni bilgileri eklemek yada kayıp bilgileri yenilemek amacını taşır, böylece veri transferinin ağırlığı en aza indirgenmiş olur. Virüs veri tabanı güncellemeleri yüz KB dan fazla yer kaplamamaktadır.
İnternet bağlantınız sürekli ise (örneğin geniş bağlantı gibi), güncellemeler tamamen otomatik olarak performans gösterecektir.İnternete sürekli bağlanmıyorsanız, avast! bağlandığınız zamanları takip edecek ve bağlantıda olduğunuz durumlarda mutlaka güncellemeleri gerçekleştirecektir. (bknz. 34)

Virüs karantinası

Virüs karantinasını disk sürücünüzdeki bir klasör gibi düşünülebilirsiniz. Virüs karantinasındaki dosyalarla bazı güvenlik kısıtlamalarına rağmen çalışabilirsiniz.
Virüs karantinasının en önemli özelliği işletim sisteminin geri kalan kısmından tamamıyla izole oluşudur. Hiç bir dış etken, virüs gibi, dosyanın içine giremez ve yürütülemez. Virüsleri burada toplamanın hiç bir tehlikesi yoktur. (bknz. 46)

Sistem uyumu

avast! antivirüs tüm özellikleriyle beraber sisteminize mükemel bir şekilde entegre olur. Tarama herhangi bir dosyaya ya da klasöre farenizin yalnızca sağ butonuna tıklayarak ve menüden ilgili seçeneği seçerek Windows Explorer'dan direk olarak başlatılabilir.

Özel ekran koruyucusu virüs taraması gerçekleştirilirken çalışabilmektedir. Yani avast! antivirüs, favori ekran koruyucunuzla birlikte çalışabilmektedir. Bu nedenle kişisel ayarlarınızı programı kullanabilmek için değiştirmenize gerek yoktur. Avast! ekran koruyucusunu ayarlamak için sayfa 68’a bakınız.

Bu sürüme ait bir diğer özellik, boot-time tarama yani açılışta tarama yapmasıdır. (Windows NT/2000/XP/Vista 32bit için). Bu çok önemli özellik, kullanıcıya virüsün aktif hale gelmeden önce taranıp bulunmasını sağlar.

avast! Virüs Temizleyicisi ile uyumlu

Avast antivirüs, bilgisayrınızı diğer kötücül yazılımlardan ya da virüslerden korumak için dizayn edilmilştir. Fonksiyonu, bilgisayarınızı tamir etmekten çok, hasarı önlemeye çalışmaktır. Bunun yanında, özel olarak Virüs Temizleyicisini bazı yaygın virüslerin hasarlı bilgisayarlardan uzaklaştırılması için sunmaktayız. Malesef, virüslerin sayıları hızla artmaktadır. Bilgisayarınız virüslerden hasar gördü ise ve Virüs Temizleyicisi bilgisayarınızı temizleyemiyorsa bu durumda bir uzmana başvurmanız gerekmektedir.

Virüs temizleyicisi hakkında daha fazla bilgi için lütfen sayfa 66’ya bakınız.

Komut satırı tarayıcısı

Deneyimli kullanıcılar için geliştirilmiş olan bir özelliktir. ashCmd programı avast! gibi tamamen aynı tarama çekirdeğini kullanmaktadır, sonuç bu durumda kesinlikle aynıdır. Tarama bir çok parametreler ve anahtarlar kullanan komut satırı tarafından gerşekleştirilir ve özel STDIN/STDOUT modülü vardır. Bu modül BATCH programlarında kullanılması amacını taşır ve çıktısı rapor dosyaları dahil tıpkı Geliştirilmiş kullanıcı arayüzündeki görevlerindeki gibidir. Komut satırı tarayıcısının kullanımı ile bilgiler için sayfa 93’e bakınız.

Betik engelleyici

Yerleşik script blocker (komut dosyası engelleyici) web sitelerdeki betik virüslerine karşı bilgisayarınızı korur. Bazı betikler zararsız olmakla beraber, eğer gezginde bir güvenlik boşluğu varsa, bu boşluk bilgisayarınızın virüslenmesine neden olabilir. avast! herhangi bir betik için gezindiğiniz web sayfalarını kontrol eder.

PUSH Güncellemeleri

Push güncellemeleri avast! Professional Edition'un bir diğer önemli özelliğidir. Bu özellik güncelleme geleneğinde dramatik bir değişimdir. Genellikle, programlar arasıra yeni versiyonları takip eder. Fakat PUSH güncellemeleri sunucumuz tarafından başlatılır, ve gerekli güncellemeler hemen gerçekleştirilir. Sistem SMTP protokolü üzerine kuruludur (e-posta mesajları için kullanılırken). Güncellemenin kendisi avast! yerleşik eposta istemcileri tarafından kontrol edilmektedir (MS outlook ve İnternet Posta). Bütün sistem asimetrik ciphers tarafından korunmaktadır ve izinsiz kullanımlara karşı direnişlidir.

Gelişmiş kullanıcı arayüzü

Bu özellik sayesinde özel "görevler" belirleyebilir çalışmasını günlük, haftalık, aylık vs. programlayıp zamanlayabilirsiniz. Görev başlatıldığı zaman yeni bir "oturum" yaratılır ve tarama sonuçları depolanır. Varsayılan basit arabirimden farklı olarak, gelişmiş arayüzde çalışırken, virüs bulunduğu zaman, ne tür bir tepki verilmesi gerektiğini, ne tür hamle yapılması gerektiğini belirleyebilirsiniz. Örneğin, virüs bulunduğunda, programın, derhal virüslü dosyayı tamir etmesini ayarlayabilirsiniz. Ayrıca, ilk hamle başarısız olursa, alternative bir hamle belirlemeniz de mümkündür. Örneğin, dosya tamir edilemez ise, otomatik olarak virüs karantinasına taşınabilir. Geliştirilmiş arayüzle ilgili özellikler için lütfen buraya tıklayınız.

Sistem gereksinimleri

NOT: Aşağıda tanımlanan donanım yapıları, işletim sistemi için, minimum olarak tavsiye edilen sistem spesifikasyonudur.

Windows® 95/98/Me:
486 Processor, 32MB RAM ve 100MB boş hard disk alanı.

Windows® NT® 4.0:
486 Processor, 24MB RAM ve 100MB boş hard disk alanı ve kurulu Service Pack 3 (ya da daha fazla)

Windows® 2000/XP® Makineleri (Sunucu değil):
Pentium class İşlemci, 64MB RAM (128MB tavsiye edilir) ve 100 MBboş hard disk alanı.

Windows® XP® 64-bit Edition:
An AMD Athlon64, Opteron ya da Intel EM64T-enabled Pentium 4 / Xeon işlemci, 128MB RAM (256MB tavsiye edilir) ve 100 MB boş hard disk.

Windows® Vista:
Pentium 4 işlemci, 512MB RAM ve 100 MB boş hard disk alanı

Programın kendisi yaklaşık 60MB boş hard disk alanına ihtiyacı vardır; Geriye kalan tavsiye edilmiş olan boşluk, virüs veri tabanı dosyası ve indeksi içindir

Fonksiyonel bir MS Internet Explorer 4 yada daha yükseği programın çalışması için gereklidir.

Bu ürün **sunucu işletim sistemine kurulamaz** (Windows NT/2000/2003 Server families).

Not; Birden fazla güvenlik programını aynı bilgisayar üzerine kurmak probleme neden olabilir. Başka bir güvenlik yazılımı daha kullanıyorsanız, avast!ı kurmadan önce diğer program kaldırmanız tavsiye edilir.

avast! antivirüs Professional Edition'ı yükleme

Bu bölümde avast! Professional Edition'u nasıl indireceğiniz ve indirdikten sonra nasıl lisans numaranızı programa gireceğiniz bilgisine ulaşabilrsiniz.

Aşağıdaki gösterilen ekranlar Windows XP içindir. Diğer işletim sistemlerinde daha farklı görülebilmektedir.

avast! antivirus Professional Editionwww.avast.com adresinden indirilebilir.

Yüklemeye başlamadan önce diğer Windows programlarının kapatılması önerilmektedir.

Sitemizde, önce "İndir" daha sonra "programlar" butonuna tıklayınız ve indirilmesi gereken programı seçiniz.

Listeden dil seçiminizi yapınız ve seçtiğiniz dilin yanındaki gri "download" butonuna tıklayınız.

Download avast! 4 Professional Edition

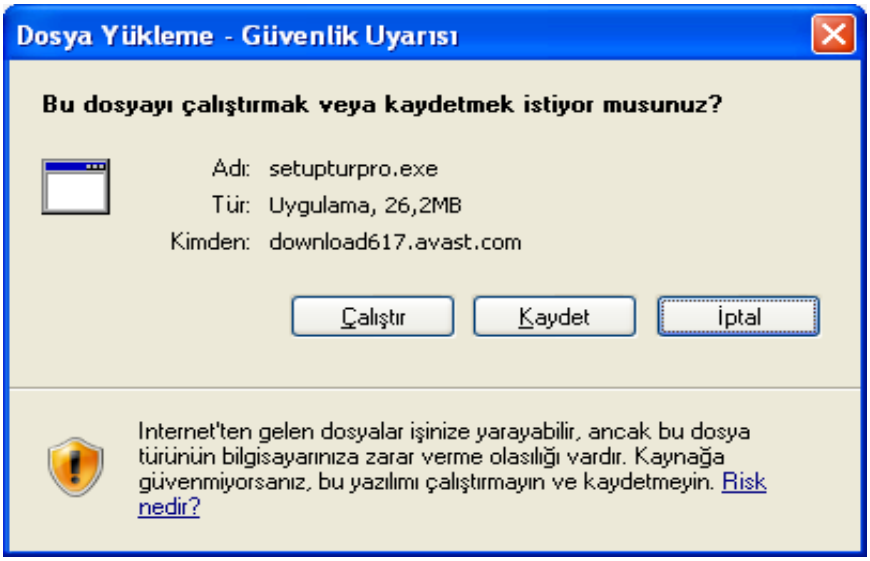
Download avast! 4 Professional - **English** version (length 21.70 MB)

Download avast! 4 Professional - **Arabic** version (length 21.50 MB)

Download avast! 4 Professional - **Bulgarian** version (length 21.54 MB)

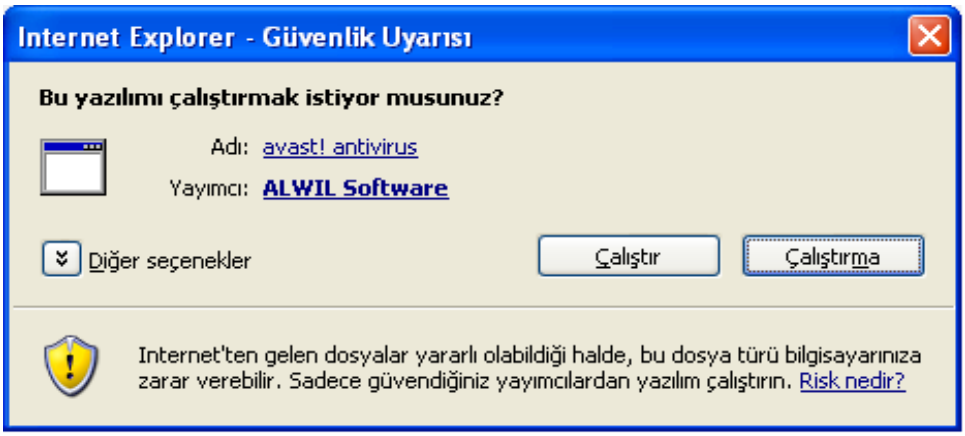
Download avast! 4 Professional - **Catalan** version (length 21.80 MB)

İnternet Explorer kullanıyorsanız, ekranınızda şöyle bir kutucuk göreceksiniz.



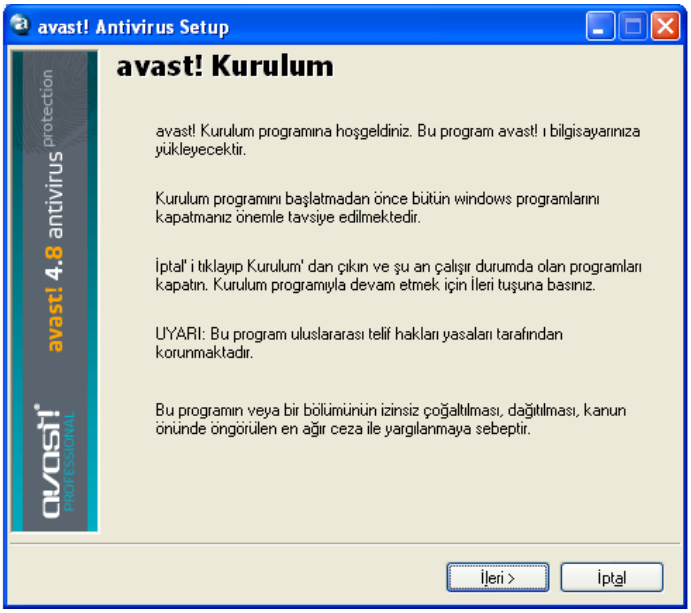
"Çalıştır" ya da "Kaydet"e tıkladığınızda "setupturpro.exe" kur dosyası yüklenmeye başlayacaktır.

Avast! antivirüsün indirme işleminin tamamlanmasının ardından hemen yüklenmesini istiyorsanız "Çalıştır"ı tıklayın. Kur programı indirilir indirilmez karşınıza şöyle bir pencere çıkacaktır.

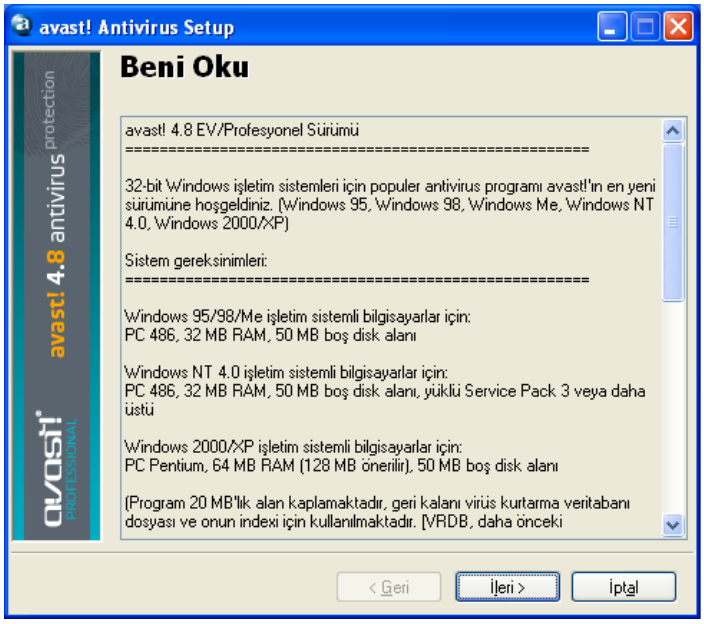


Diğer web tarayıcılarında yalnızca “Kaydet” seçeneği ile karşılaşabilirsiniz. “Kaydet” i seçerseniz program indirilmeye başlayacak fakat bu kez kurulmayacaktır. Kurulum işlemini tamamlamak için “setuptur.exe” kur dosyasını yürütmeniz gerekmektedir. Bu nedenle, nereye yüklediğinizi lütfen unutmayınız! Dosyayı yürütmek için üzerine iki kez tıklayınız.

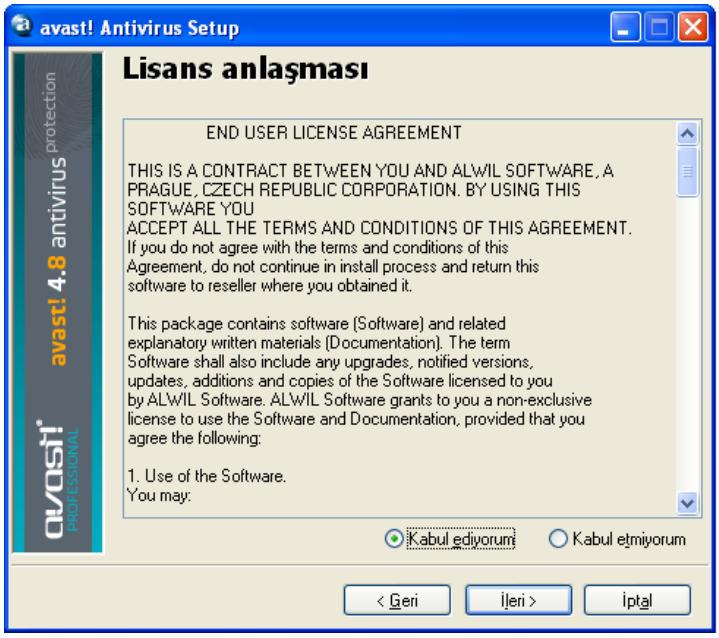
“Çalıştır”a tıkladığınızda avast! Kur dosyası ekranınıza gelecektir.



“İleri” tuşu ile devam edin ve sihirbaz geri kalan kurulum işleminde size rehberlik edecektir.

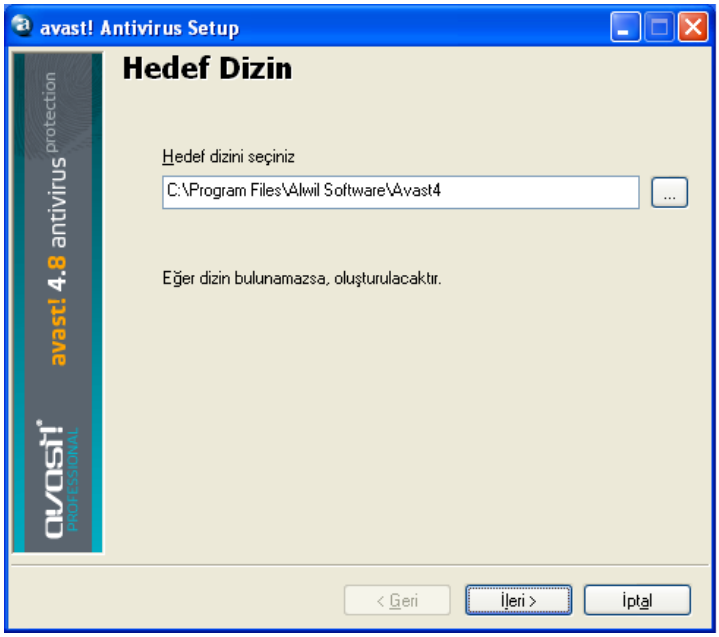


İlk olarak, minimum sistem gereksinimlerini okumanız istenecektir. Daha sonrasında ise -kullanıcı lisansı şartlarını- kabul etmeniz gerekecektir. Aşağıdaki ekran kopyalarını inceleyiniz

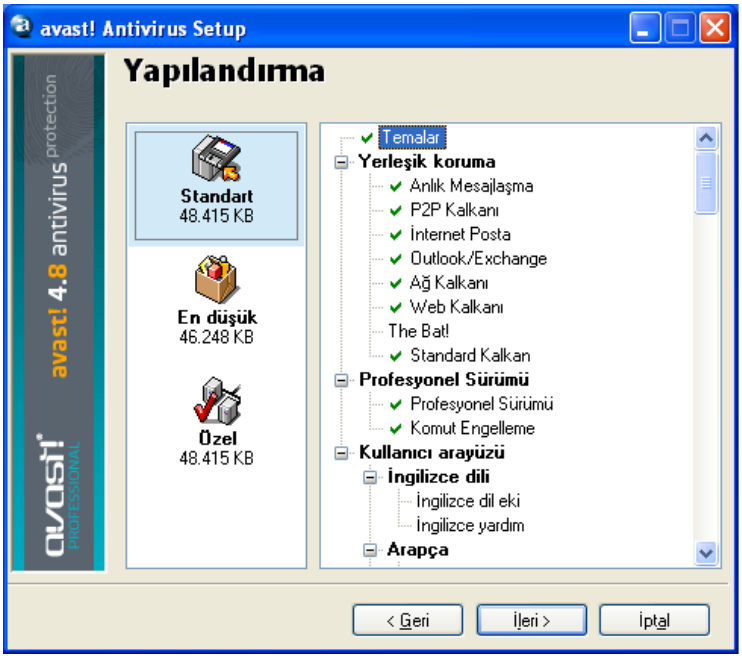


Devam etmek için lütfen “Kabul ediyorum” u seçin ve “ilerle” ile devam edin.

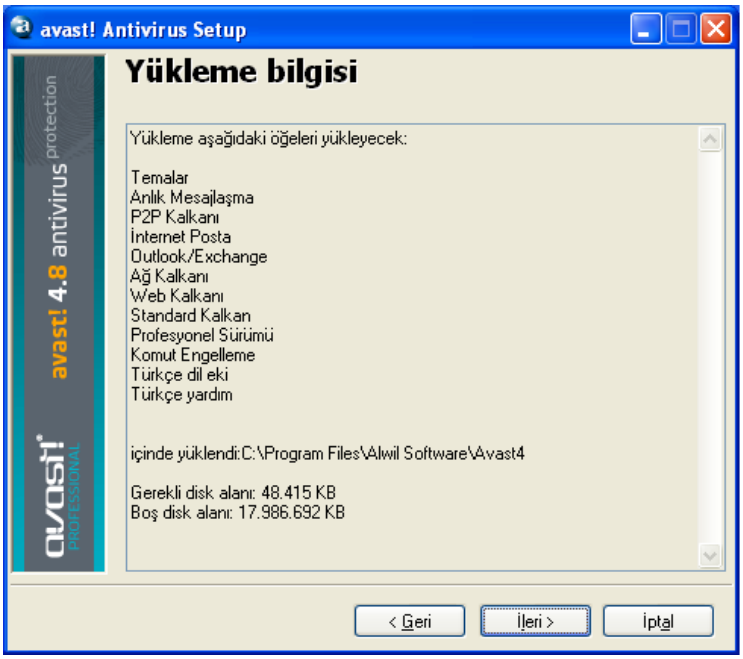
Daha sonra “Hedef Dizin”ini, programın nereye kaydedilieceğini, teyid etmeniz gerekmektedir. Programın kendisi bunu otomatik olarak seçecek ya da yeni bir hedef yaratacaktır. Varsayılan hedef dizininiz kabul edilmesi ve “ilerle” tuşu ile devam edilmesi tavsiye edilmetedir.



Gelecek olan ekranda, yapılandırmayı teyid etmeniz gerekecektir. Seçeneklerin çoğu , varsayılandan farklı bir ayarlama tercih etmediğiniz sürece, örneğin dil seçeneği gibi, otomatik olarak seçili bulunmaktadır. Bu noktadan sonra yapmanız gereken yine “ileri” tuşu ile devam etmek olacaktır.



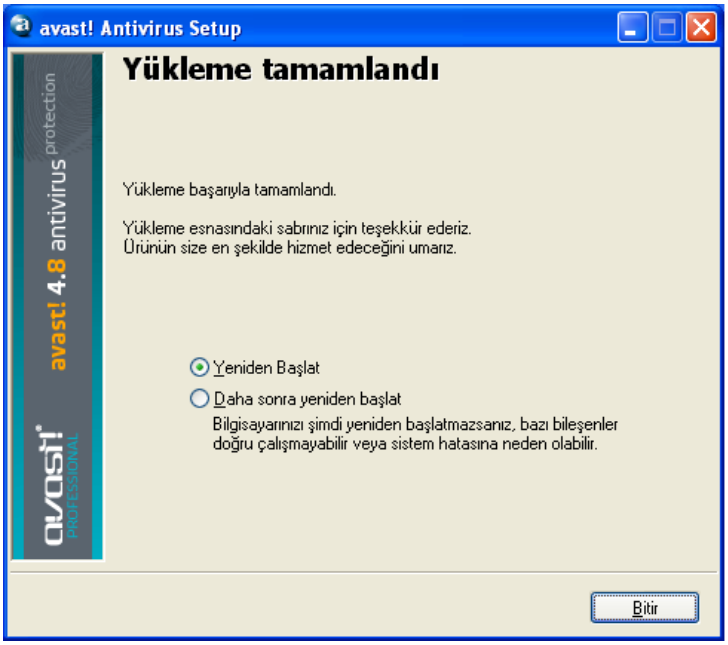
Bundan sonra program, neyin nereye kurulacağını, gerekli ve mümkün olan disk boşluğunu teyid edecektir. “ilerle ” tuşu ile devam ediniz.



Bu noktada yerel sabit disklerinizin açılış anında taranması için belli bir zaman belirlemek isteyip istemediğiniz sorulacaktır. (bknz. Sy. 64)

Son pencere kurulumun tamamlandığını gösterecektir. Yine de kurulum işlemini tam anlamıyla tamamlamak için bilgisayarınızı yeniden başlatmanız gerekmektedir.

“Yeniden Başlat”ı seçin , ve sonrasında “bitir”e tıklayın ve bilgisayarınız otomatik olarak başlatılacaktır.

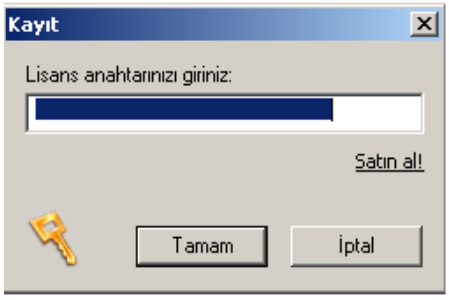


İşte yükleme işlemi tamamlandı!

Başlangıç

Bilgisayarınız yeniden başlatıldığında, ekranınızın sağ alt köşesinde "mavi balon" şeklinde avast! simgesi belirecektir.

avast! Professional Edition 60 gün ücretsiz olarak kullanılabilir. Bu süre sonunda , programı kullanmaya devam etmek isterseniz, lisans satın almanız gerekecektir. Yine de, programı ilk olarak çalıştırdığınızda karşınıza şöyle bir ekran çıkacaktır.

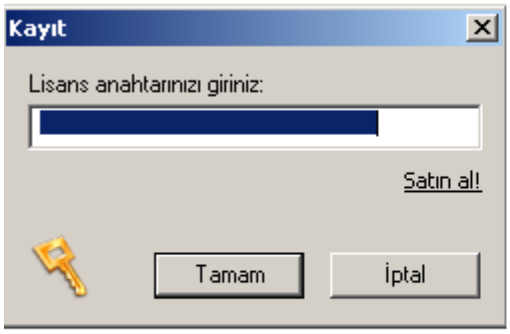


İlk etapta lisans numarasını girmeniz gerekmemektedir. Programı 60 gün süre ile lisans numarası girmeden de kullanabilirsiniz. Bunun için "Demo" üzerine tıklayın. Fakat, hemen lisans almak istiyorsanız "satın al" seçeneğini işaretleyiniz ve takip eden işlemleri gerçekleştiriniz.
Demo versiyonunu seçtiğiniz takdirde, bu kutucuk programı tekrar çalıştırana kadar gözükmeyecektir. Lisans kodunu altmış gün süre içinde herhangi bir zaman girebilirsiniz. İlerleyen bölümde "Lisans anahtarı nasıl alınır" sayfasını okuyunuz.

60 gün sonunda, hala lisans kodunu girmedi iseniz, aşağıdaki uyarı notunu alacaksınız.

Ayrıca programı başlattığınızda her zaman aşağıdaki mesajı alacaksınız.

"Tamam"a tıkladığınızda kayıt mesajı ekrana gelecektir.



Lisans numaranızı nasıl elde edeceğiniz ve nasıl programa gireceğiniz ilerleyen sayfalarda açıklanmıştır.

Şifre ile koruma

Avast mavi ikonuna sağ tıkladığınızda "Şifre oluştur/değiştir" seçerek, yetkili olmayan kişilerce yapılabilecek değişiklikleri önlemek için, yeni şifre oluşturabilirsiniz.

Lisans anahtarı nasıl alınır

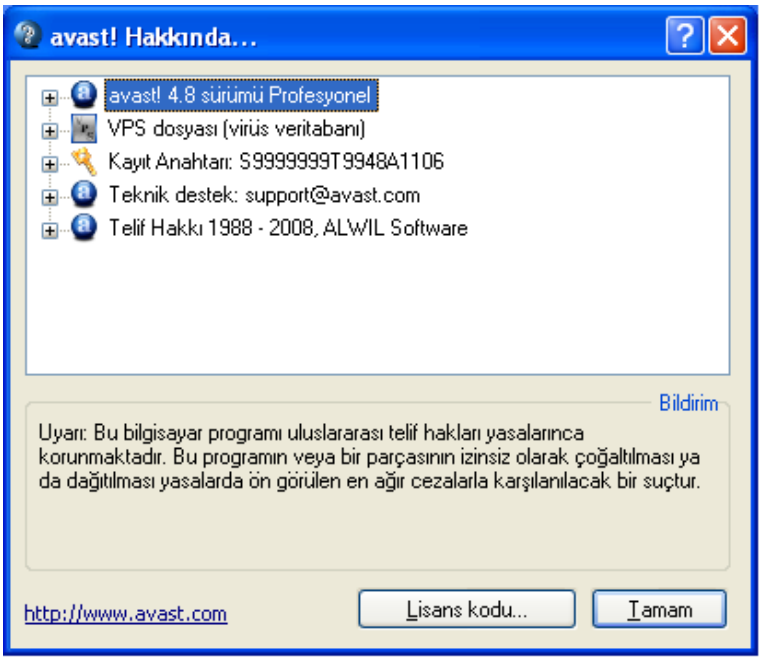
60 günlük deneme süresinin ardından, programı kullanmaya devam etmek için geçerli bir lisans numarası almanız ve bu numarayı programa girmeniz gerekmektedir.

Avast! Professional Edition lisansı 1, 2 ya da 3 yıl için satın alınabilir. Fiyat listesi ve para birimi göstericisi ile beraber ödeme seçenekleri için lütfen http://www.avast.com/index_tur.html adresini ziyaret ediniz.

Lisans numarası satın almak için, önce web sitemizdeki "ürünler" kısmına, daha sonra "masa üstü koruma çözümleri", "Kobilere özel koruma çözümleri" ya da "büyük şirketlere özel koruma çözümleri"ne tıklayın ve "avast! 4 Professional Edition"ı seçin. Gelecek olan sayfada "satın al" butonuna tıklayın ve bir sonraki sayfada 1 yıl, 2 yıl ya da 3 yıl için seçiminizi yapınız.

Bu esnada ihtiyacınız olan lisans sayısını belirlemeniz gerekecektir. Forma, kişisel detaylarınızı ve ödeme şeklinizi giriniz. Ödemeyi gerçekleştirdikten sonra 24 saat içinde girmiş olduğunuz e-posta adresinize lisans kodu gönderilecektir.

Programı daha önceden indirip kurdu iseniz, avast! mavi ikonuna farenizin sağ tuşu ile tıklayınız ve "avast! hakkında"yı seçiniz.



Önce "Lisans kodu"na, sonra açılacak olan kayıt penceresinde "satın al" butonuna tıklayın. Böylece, avast! websitesine yönlendirilip satın alma işlemini gerçekleştirebileceksiniz.

Lisan kodunun programa girilmesi

Epostanıza iletilen lisans kodunu programınıza girmeniz gerekmektedir. Girdikten sonra program otomatik olarak güncellenecek ve lisans süresi bitene kadar lisans anahtarı ile ilgili bir uyarı almayacaksınız.
Not; avast! programını lisans kodunu girmeden önce indirmiş ve kurmuş olmanız gerekmektedir.

Lisan kodunu girme konusunda size rehberlik edecek olan videomuzu izlemek için lütfen buraya tıklayınız. Ya da http://www.avast.com/index_tur.html adresinden "yardım" seçeneğinin altında "Teknik yardım " sayfasına gidiniz ve sayfanın sol alt köşesinde "aktivasyon kodu nasıl girilir" başlığına tıklayınız.

Alternatif olarak aşağıdaki adımları takip edebilirsiniz:

1. Lisans kodunu farenizin sol tuşu ile işaretleyerek koyultun ve sağ tuş ile tıklayarak "Kopyala"yı seçin.
2. Şimdi bilgisayarınızın sağ alt köşesindeki mavi balon şeklindeki avast! simgesine farenizin sağ tuşu ile tıklayın ve "avast! hakkında"yı seçin.
3. "Lisans Kodu" na tıklayın.
4. Karşınıza çıkacak olan lisans kodu kutucuğuna lisans numaranızı farenizin sağ tuşuna tıklayıp "Yapıştır" seçeneği ile girin.
5. Son olarak "Tamam"ı seçin. Şimdi programı sözleşmenizin uzunluğuna bağlı olarak 1, 2, ya da 3 yıl olarak kullanabilirsiniz. Bu süre bittiği zaman ise yeni bir lisans almanız gerekmektedir.

avast! antivirüs'ün kullanımı ile ilgili bazı esaslar

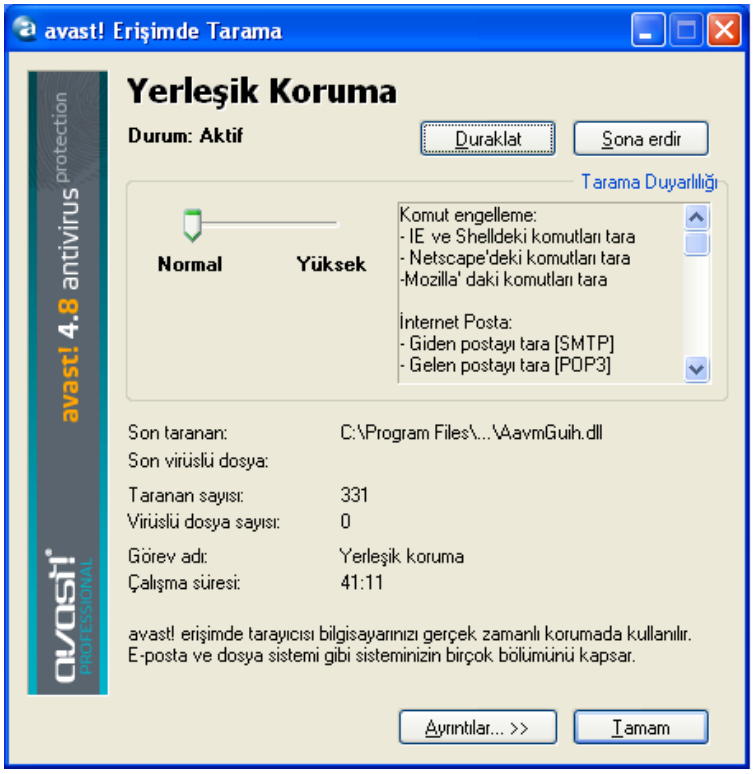
Avast! bütün kötücül yazılımlara karşı "Yerleşik koruması" ile güçlü koruma sağlamaktadır. Genel olarak, program, dosyaları erişimde taradığı için "erişimde tarama" olarak tanımlanır.
Normalde, yerleşik koruma bilgisayarınızın ihtiyacı olan tüm virüs korumasını sağlar. Program yüklenir yüklenmez, yerleşik koruma arka planda çalışmaya başlar ve bilgisayarınızdaki bütün aktiviteleri izler. Fakat, yerleşik koruma, herhangi bir nedenle kapanırsa, ya da her hangi bir zaman diliminde etkisiz hale getirilirse, bilgisayarınızdaki bütün dosyaların geriye dönük elle taraması yapılabilir.

Avast! antivirüs ayrıca özel ekran koruyucusu içerir. Bu ekran koruyucusu, avast! çalışıyor fakat o anda kullanılmıyorken, bilgisayarınızı virüslerden korumak için devamlı tarar.

Yerleşik "erişimde" Koruma

Programın bu bölümü, bilgisayarınızdaki dosyaların herhangi bir hasar görmemesi için, tüm bilgisayarın ve yürütülen bütün programların şüpheli aktivitelerini izler (virüs vs.). Kesinlikle bağımsız çalışır, bilgisayarınız açıldığı anda harekete geçer, ve herşey yolunda ise çalışıp çalışmadığını bile farkettirmez. Ekranınızın sağ alt köşesindeki mavi avast! ikonu yerleşik korumanın durumunu göstermektedir. Mavi ikonun bulunma nedeni programın yüklü olduğunu ve bilgisayarınızın koruma altında olduğunu gösterir. Üzerinde kırmızı çizgi varsa, korumanın geçici olarak aktif olmadığını yani o anda etkisiz olduğunu, bilgisayarınızın korunmadığını gösterir. Gri bir görünüm varsa , programın duraklatıldığını gösterir.

Mavi simgeye farenizin sol tuşu ile tıkladığınızda yerleşik koruma ayarlarına ulaşabilirsiniz. Aşağıdaki pencere ekranınıza gelecektir.



Bu pencereden yerleşik korumayı butonları kullanarak "duraklatabilir "ya da "sona erdirebilirsiniz" . Her iki seçenekte aynı etkiye sahiptir. Yerleşik koruma bilgisayarınız yeniden başlatıldığında tekrar aktif hale gelecektir. Bu özellik bilgisayarınızın yanlışlıkla korunmasız kalmasını önler.

Ayrıca, yerleşik korumanın hassaslığını ekrandaki kursörü (ibreyi) kullanarak "normalden" "yükseğe", ne şekilde istiyorsanız ayarlayabilirsiniz. Yerleşik koruma, bilgisayarınızaın farklı parçalarını, farklı şekilde korumak için farklı modülleri içermektedir. Bu pencere üzerinde yapacağınız herhangi bir değişiklik bütün yerleşik koruma modüllerine uygulanacaktır.

Yerleşik koruma aşağıdaki modülleri yani "sağlayıcıları" içermektedir.

Anında mesajlaşma; anında mesajlaşma yada "chat/sohbet" programları tarafından indirilen dosyaları kontrol eder (MSN ya da ICQ gibi programlar ya da bu türden sohbet programları vs.). Mesajlaşma programlarının kendisi bir risk unsuru oluşturmazken, bu programın sohbetin ötesinde ayrıca dosya paylaşımı olarak da kullanılması, tam olarak kontrol edilmezse, virüs riskini beraberinde getirmektedir.

İntenet E-posta Outlook express, Eudora vs gibi yani MS Outlook ve MS Exchange dışındaki istemciler tarafından işlenen giden ve gelen epostaları kontrol eder.

Ağ kalkanı İnternet solucanlarına karşı koruma sağlar. Blaster, Sasser vs. gibi. Bu özellik yalnızca NT tabanlı sistemlerde mümkündür. (Windows NT/2000/XP/Vista).

Outlook/Exchange Ms Outlook ya da MS Exchange tarafından işletilen gelen ve giden epostaları kontrol eder ve herhangi potansiyel virüs içeren epostayı kabul edilmeden ya da gönderilmeden durdurur.

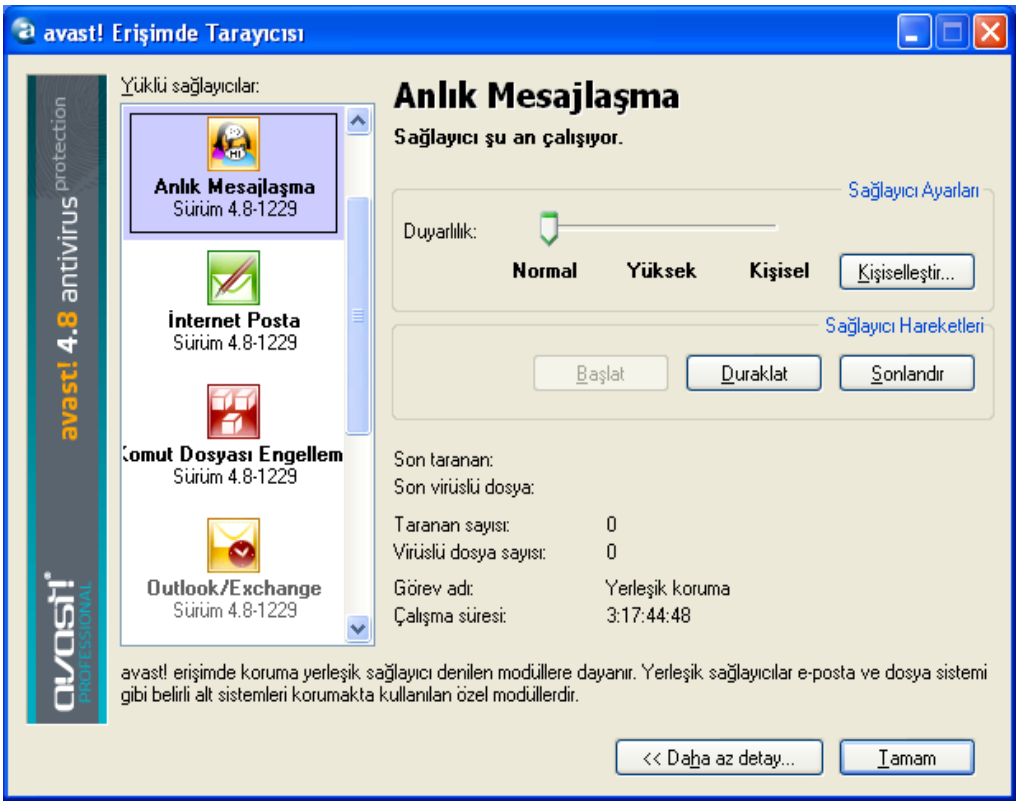
P2P Kalkanı Yaygın dosya paylaşımı programları tarafından indirilen dosyaları kontrol eder. (Kazaa vs.)

Komut dosyası engelleme Web sayfalarındaki komut dosyalarını kontrol eder.

Standart Kalkan Progaramları çalışmaya başlamadan önce ya da dosyaları açılmadan önce kontrol eder. Böylece bilgisayarınız hasar görmeden önlem alınmış olur.

Web kalkanı İnterneti kullanırken bilgisayarınızı virüslerden korur ve bazı belirli web sayfalarını engeller. Virüslü bir dosya indirirseniz, Standart Kalkan, bilgisayarınız herhangi bir hasar görmeden bunu engelleyecektir. Bunu yanında Web Kalkanı siz dosyayı indirmeden kontrol ederek daha güçlü bir koruma sağlar. Web Kalkanı bir çok web tarayıcısı ile uyumludur (Microsoft Internet Explorer, FireFox, Mozilla ve Opera dahil) "Intelligent Stream Scanning" ile indirilen dosyaların hemen hemen gerçek zamanlı taranmasını sağlar. Tarama hızını etkisi çok düşüktür, hatta yok denecek kadar azdır.

Her modüle ayrı bir duyarlılık kazandırmanız mümkündür. Her bir modülü duraklatmak, ya da her bir modülün duyarlılığını değiştirmek için "ayrıntılar"a tıklayın.

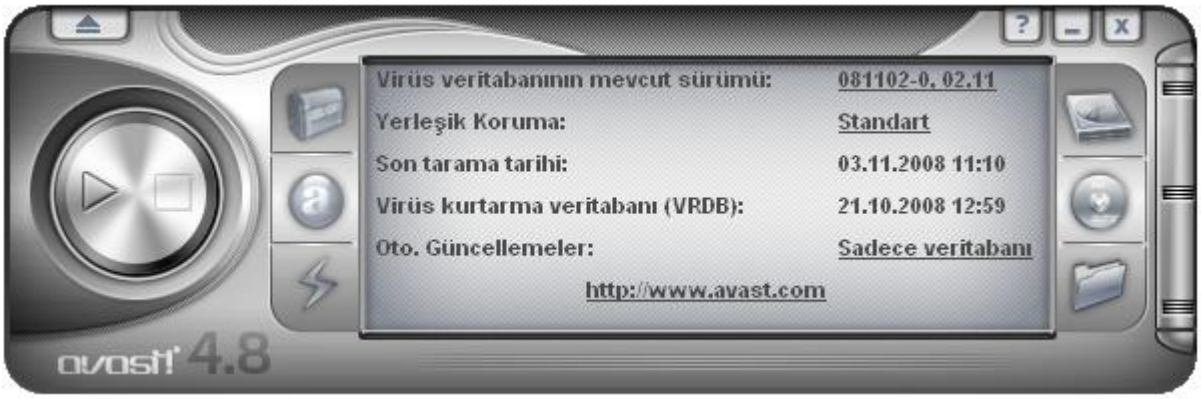


Sol panelde modüller bulunmaktadır. Önce ayarını değiştirmek istediğiniz modülü seçin. Daha sonra seçtiğiniz bu modülü "Duraklat" ya da "sonlandır" seçeneklerini kullanarak duraklatabilir ya da sonlandırabilirsiniz. Duraklattığınız taktirde ilişkili modül, bilgisayarınızı yeniden başlattığınızda güncellenecek, ayarlar aktif hale gelecektir. Sonlandırdığınız takdirde ise program, değişiklikleri tamamen mi yoksa bu seferlik mi kaydetmek istediğinizi soracaktır. (bknz. 86) "Evet"i seçerseniz modül, siz tekrak başlatana kadar etkisiz hale gelecektir.

Her modül için daha bir çok ek özellik mevcuttur. Örneğin taranacak dosyaların türünü belirleyebilirsiniz. Bu ek özelliklere "Kişiselleştir" butonunu kullanarak ulaşabilirsiniz (bknz.sy. 70)

Virüs taramasını başlatma – Basit kullanıcı arabirimi

Programı ilk çalıştırdığınızda gümüş renkli, radyo/Cd çalar şeklinde bir oynatıcı açılacaktır. Bu oynatıcıdan programı çalıştırabilir , virüs taramalarını sonuçlandırabilirsiniz. Bu oynatıcı programın varsayılan arayüzüdür. Değiştirmek için sayfa 27' e bakınız.



Oynatıcının ortasındaki bölümde , durum bilgileri yer almaktadır.

- ***Virüs veritabanının mevcut sürümü;*** Virüs veritabanı bilinen, tanımlanmış olan bütün virüslerin detaylarını içerir ve program tarafından herhangi bir şüpheli dosyayı bulmak için kullanılır.
- ***Yerleşik koruma;*** burada mevcut duyarlılık ayarlarınızı görebilirsiniz.
- ***Son tarama tarihi;*** elle yapılan son taramanın tarihini gösterir.
- ***Virüs kurtarma veritabanı;*** bilgisayarınızda yüklü olan dosyalara ait detayları içerir ve dosyalar virüslü ise tamir eder. Belirtilen tarih ise virüs kurtarma veritabanının, en son ne zaman güncellendiğini gösterir.
- ***Otomatik güncellemeler;*** Virüs veritabanının ve programın kendisinin güncellemelerini gösterir. Güncellemenizin durumunu değiştirmek için pencerenin sağındaki durumun üzerine tıklayınız. (bknz. sy. 34)

- Oynatıcının her iki tarafında da üçer tane kontrol tuşu bulunmaktadır:

- **Sol üst buton:** Bu buton Virüs karantinasını açacaktır. Virüs karantinasında dosyalarla nasıl çalışılacağı hakkında bilgi almak için sayfa 46'ye bakınız..

- **Orta sol:** Bu butona tıkladığınızda Yerleşik Korumanın duyarlılığını değiştirebileceğiniz bir gösterge belirecektir. Göstergenin üzerine tıklayıp, ibreyi sağa ya da sola doğru hareket ettirerek duyarlılığı arttırıp azaltabilirsiniz. Buradaki duyarlılığı değiştirmek, yerleşik korumadaki bütün modülleri etkileyecektir. Modüllerin duyarlılığını ayrı ayrı ayarlamak için sayfa 21'ye bakınız.

- **Alt sol:** Virüs veritabanını güncellemek için bu butona tıklayınız ya da ekranınızın sağ alt köşesindeki mavi avast! "i" simgesine sağ tıklayıp "Şimdi VRDB oluştur" a basınız.

- **Sağdaki üç buton:** Taranacak alanları belirlemek için bu tuşu kullanabilirsiniz. Taşınmaz yerel sürücüler, taşınabilir sürücüler (disket, CD vs.) ve taranacak ek alanları belirleyebilirsiniz.

- **BAŞLAT:** Bu butonu kullanarak başlayabilir ya da seçili alanların taranmasına devam edebilirsiniz. Bu buton daha sonra "duraklat" olarak değişecektir.

- **DURAKLAT:** Taramanın geçici olarak durdurulması için bu butona tıklayınız.

- **DUR:** Taramayı sonlandırmak için bu butona tıklayınız.

MENÜ: Sol üst köşedeki ok işaretinden **SEÇENEKLER menüsüne** ulaşabilirsiniz. Seçeneklere ayrıca oynatıcı ekranın üzerine, herhangi bir yere sağ tıklayarak da ulaşabilirsiniz.

Programı arayüz olmadan kullanırken (bknz. 27), menüye oynatıcı ekranın üzerindeki "Araçlar" ya da "Ayarlar"dan ulaşabilirsiniz.

Bazı seçeneklere ise programı başlatmadan da ulaşabilirsiniz. Bunun için, ekranınızın sağ alt köşesindeki "mavi avast balonuna" sağ tuş ile tıklayınız.

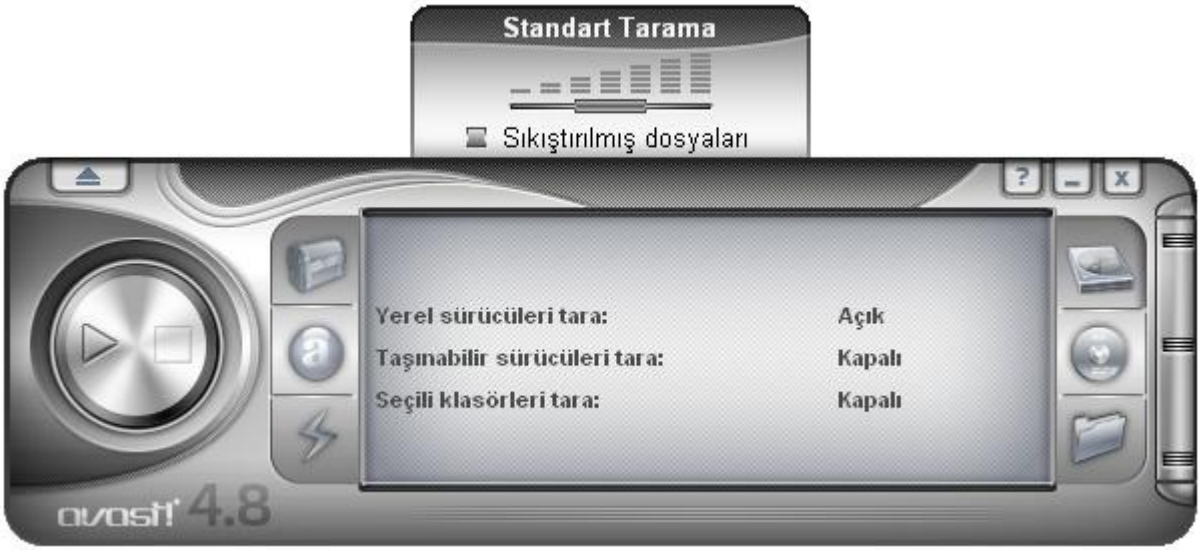
Kullanım klavuzumuzun ilerleyen bölümlerinde seçeneklere(menüye) ayrıntılı yer verilmiştir.

El ile taranacak alanların belirlenmesi

Taramaya başalamadan önce taranacak dosyaları belirlemeniz gerekmektedir.

- ***Yerel sürücülerin taranması***

Bilgisayarınızdaki bütün dosyaları taratmak istiyorsanız oynatıcı ekranın sağ üstündeki butona tıklayınız. Oynatıcının üzerinde küçük bir kutucuk açılacaktır. Durum bilgisine geri dönmek için oynatıcı ekranın üzerine sağ tuş ile tıklayın ve "Durum bilgisi"ni seçin.



Oynatıcı ekranın üzerinde şimdi "Yerel sürücüleri tara" mesajını ve bu seçeneğin "Kapalı"dan "Açık"a dönüştüğünü göreceksiniz.

Taramanın duyarlılığını ayarlamak için oynatıcını üzerinde beliren küçük ekranı kullanabilirsiniz. İbreyi farenizle tutarak sağa yada sola hareket ettirebilirsiniz. Sola doğru kaydırdığınızda duyarlılık azalacak, sağa doğru kaydırdığınızda ise artacaktır. Ayrıca sıkıştırılmış dosyaları bu küçük ekrandan taratabilirsiniz. Bu seçenekler ilerleyen safhalarda ayrıntılı olarak ele alınmıştır.

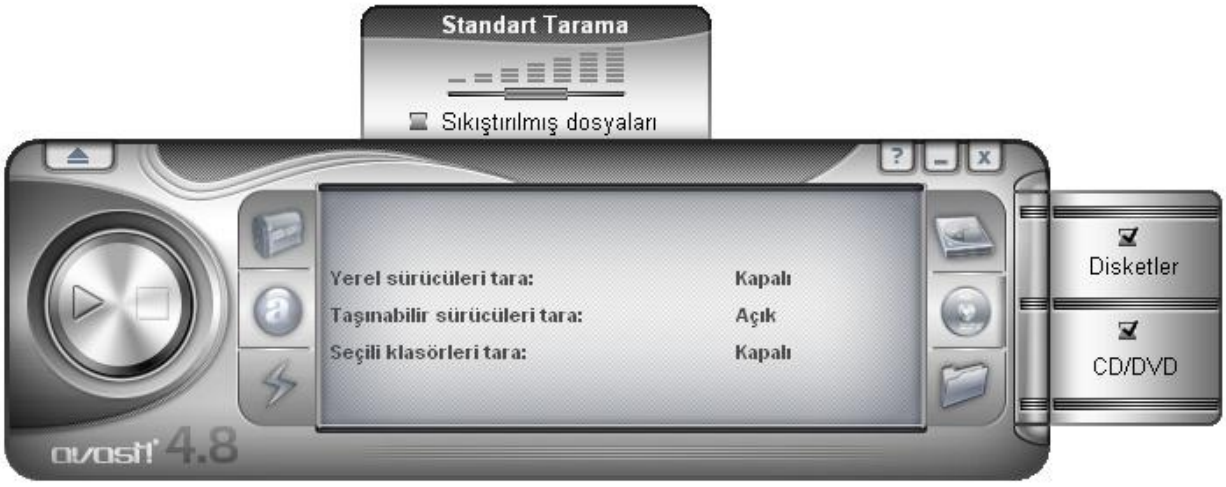
- ***Taşınabilir ortamların taranması***

Taşınabilir sürücüleri CD/DVD vs. taratmak istiyorsanız, sağ orta butona tıklayınız.

Bu butona tıkladığınızda "Taşınabilir sürücüleri tara" seçeneği "Kapalı"dan "Açık"a dönüşecektir.

İki kutucuk "Disketler" ve "CD/DVD" başlıkları altında açılacaktır. Bu kutucuklardan hangisinin taranmasını istiyorsanız seçebilirsiniz. Taranmasını istemediğiniz alandaki işereti kaldırabilirsiniz. Diğer manyetik ve manyetooptik medyalar da, ZIP diskleri gibi disket olarak hesaba katılır.

Üstteki standard tarama kutucuğu açık kalacaktır.



- ***Seçili kalasörlerin taranması***

  Son seçenek sağ alttaki butondur. Bu buton ile taramak istediğiniz klasörleri kesin olarak belirleyebilirsiniz. Bu butonu tıkladıktan sonra, bilgisayarınızdaki bütün klasörlerin listesi ekrana gelecek. Bu listeden taratmak istediğiniz klasörü seçebilirsiniz. Bu seçenek bir çok olanak sunmaktadır, fakat kullanıcının kesin olarak neyin taratılmasını istediğini belirlemesi gerekmektedir.

  Taramanın duyarlılığını ayarlayabilir, sıkıştırılmış dosyaların diğer alanlar gibi taranıp taranmayacağını belirleyebilirsiniz.

  Birden fazla tarama tipini kombine edebilirsiniz. Mesela, yerel taşınamaz sürücüler ve taşınabilir disk butonlarını bereber tıkladığınızda yerel taşınamaz ve taşınabilir diskleriniz, kombine bir şekilde taranacaktır.

Taramanın duyarlılığını ayarlamak ve başlatmak

Taranacak alanları tanımlarken, taramanın duyarlılığını ayarlayabilir ve aynı zamanda programın, sıkıştırılmış dosyaları (dosya isimleri .zip, .rar, ace, .acj vs. ile biten) tarayıp taramayacağını ayarlayabilirsiniz. Bu dosyaların taranmasını istiyorsanız, öncelikle hangi alanın taranacağını belirlemeniz gerekmektedir (yukarıdaki şekli inceleyiniz). Daha sonra oynatıcının üzerinde olan "Sıkıştırılmış dosyaları" kutucuğunu işaretleyiniz. Göstergeyi sağa ya da sola doğru hareket ettirerek taramanın duyarlılığını belirleyebilirsiniz. Önceden tanımlanmış üç tür seviyeden birini seçebilirsiniz.

- **Hızlı tarama;** Bu tarama yöntemi, adından da anlaşılacağı üzere hızlı bir tarama yöntemidir. Dosyalar, dosya adlarına göre incelenir ve yalnızca potansiyel olarak tehlikeli görülenler taranır. Bu tarama yöntemi bazen virüslü dosyaları gözden kaçırabilir, fakat genellikle etkilidir.

- **Standart tarama;** Bu tarama yöntemi ile dosyalar, hızlı taramanın aksine içeriklerine göre taranmaktadır. Hızlı taramada isimlerine göre taranmaktadır. Normal taramada dosyanın yalnızca dosyanın "tehlikeli" kısmı test edilir. Yine bazı durumlarda virüs kaçırabilir, fakat Hızlı Tarama'ya kıyasla çok daha etkilidir.

- **Eksiksiz tarama;** Bu tarama yöntemi ile dosyalar eksiksiz olarak taranır, daha güvenilirdir fakat Hızlı Tarama ve Standart taramaya göre çok daha fazla zaman alır.

Tarama şeklinizi belirledikten sonra, yapmanız gereken tek şey testi başlatmak olacaktır. Bunun için soldaki Başlat butonuna tıklamanız yeterli olacaktır.

Alternatif Metod

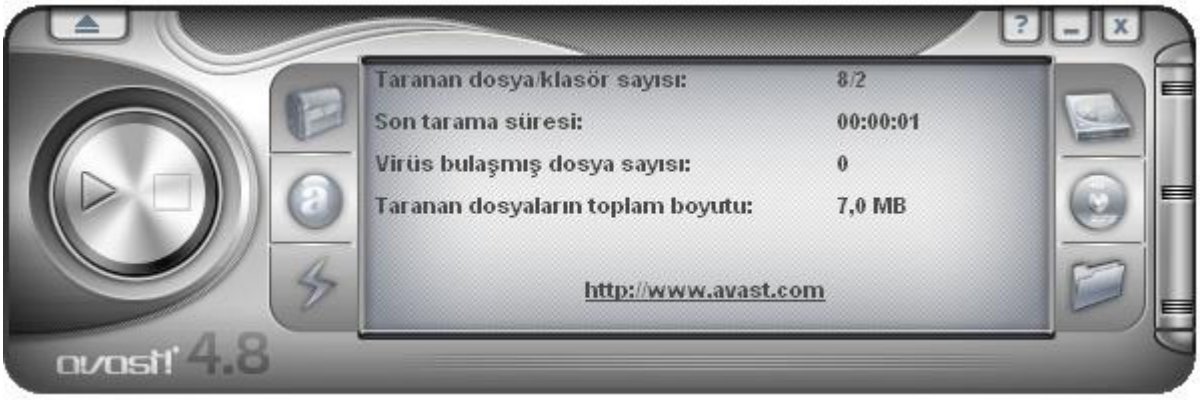
Ayrıca, menüden taranacak alanları tanımlayabilirsiniz. "Başlat" ve daha sonra " Taranacak alanı belirle"ye tıklayın. Taranacak alanı belirleyin, "sıkıştırılmış dosyaları tara"yı seçin, böylece sıkıştırılmış dosyalarınız da taranacaktır.

"Tarama derecesini seçiniz" seçeneğinden ayrıca taramayı Hızlı, Standart yada Eksiksiz Tarama olarak belirleyebilirsiniz.

Taramanın yürütülmesi ve sonuçlandırılması

Başlat butonunu tıkladıktan sonra, ya da menüden "Taramayı başlat" butonuna tıkladığınızda program seçili alanları taramaya başlayacaktır. Bu işlem, bilgisayarınızın hızına, test edilen dosyaların boyutuna ve sayısına bağlı olarak uzun sürebilir. Eksiksiz tarama uzun sürecektir fakat bu yöntemin en etkili yöntem olduğunu hatırlatmak isteriz.
Programı başlattığınızda, tarama esnasında, diğer dosyalarla ya da programlarla çalışabilirsiniz. Bunu yapabilmeniz için, avast!ı küçültmeniz gerekmektedir, böylece avast! arka planda çalışmaya devam edecektir. Küçültmediğiniz taktirde, bilgisayarınız yavaşlayabilir (Virüs tarama oldukça çaba gerektiren bir görevdir). Tarama başladıktan sonra, programı arka planda çalıştırmak için, yalnızca oynatıcının sağ üst köşesindeki (_) küçültme butonunu kullanmanız yeterlidir. Böylece program görünmez hale gelecektir. Geri getirmek için, sadece ekranınızın sağ alt köşesindeki avast! ikonuna tıklayınız.

Tarama sonlandığında hiç bir virüs taranmamışsa, oynatıcı temel tarama bilgisini sunacaktır, örneğin taranan klasör ve dosya sayısı, tarama zamanı vb.

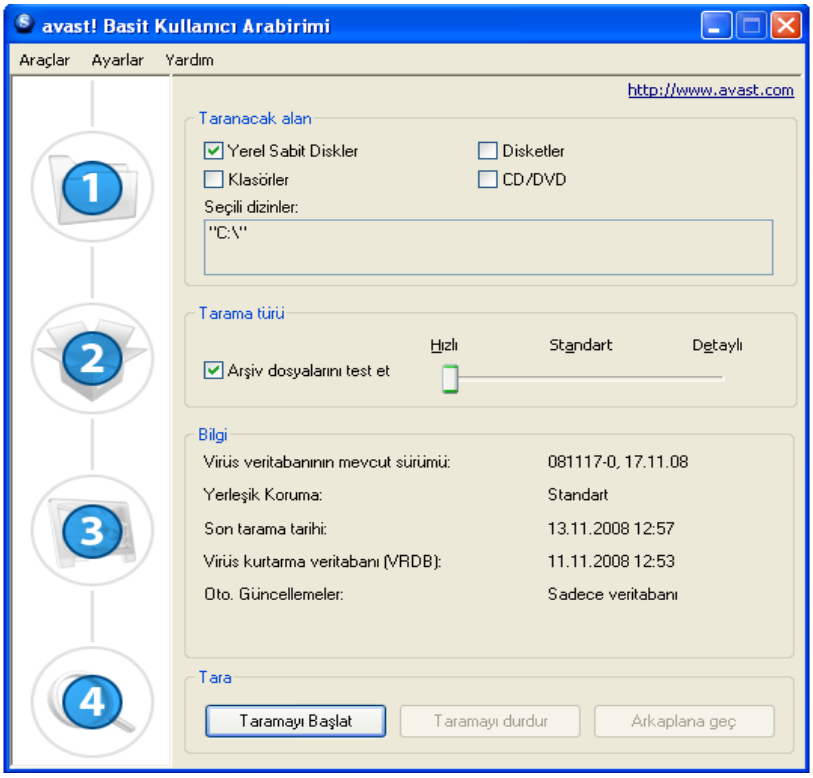


Herhangi bir virüs bulundu ise, program virüslü dosya(lar) ile ne yapacağınızı soracaktır. Bir kaç seçenek sunulacaktır.Virüs karantinasına taşı, **sil**, **yeni ad** ver ya da **taşı**, ve hatta mümkünse **tamir et** seçeneklerini sunacaktır. Ya da dosyayı olduğu gibi eksiksiz saklayabilirsiniz, fakat, bu yöntem virüsün yayılmasına ve hasara yol açmasına neden olabilir. Bu seçenekler ilerleyen bölümlerde "Herhangi bir virüs bulunduğunda yapmanz gerekenler" başlığı altında ayrıntılı olarak anlatılmıştır.

Basit Kullanıcı Arabirimi'nin görünümünün değiştirilmesi

Basit kullanıcı arabirimini kullanıyorsanız, programı farklı görünümlerde kullanabilirsiniz. Arzu ederseniz, standart ve diğerleri olmak üzere üç farklı skin/görünümü İnternetten indirebilirsiniz. Avast! oynatıcısına sağ tıklayarak ya da menüden "Tema seç" i ve daha sonra "uygulama başlangıcında rastgele tema seç" i tıklayınız. Alternatif olarak, programı arayüz olmadan kullanmak istiyorsanız, seçeneklerden "ayarlar"a gidin, "Basit Kullanıcı Arabirimi için temeları etkinleştir" onay kutucuğunu işaretleyin. Programı yeniden başlattığınızda, seçenekler, temel formda görünecektir. Eski haline döndürmek için "Ayarları" seçin daha sonra tekrar "ayarlar"ı seçin ve son olarak , "Basit Kullanıcı Arabirimi için temeları etkinleştir" onay kutucuğundaki işareti kaldırın. Programı yeniden başlattığınızda herşey eski haline dönecektir.

Basit kullanıcı arabiriminin temel görünümü:



Tarama alanını/alanlarını ve tarama türünü ilgili kutucukları işaretleyerek belirleyebilirsiniz. Sadece belirli klasörleri taratmak istiyorsanız, "klasörler" kutucuğunu işaretleyiniz. Bu kutucuğu işaretlediğinizde, klasörlerinizin listesi küçük bir pencerede ekrana gelecektir. Klasör(leri) seçmek için, sadece ilgili kutucukları işaretleyin. Yukarıdaki pencerede "Seçili dizinler" başlığı altında seçtiğiniz klasörleri görebilirsiniz.

Taramanın duyarlılığını, yine göstergedeki ibreyi hareket ettirerek ayarlayabilirsiniz. Arşiv dosyalarını da test etmek istiyorsanız, göstergenin hemen yanındaki "Arşiv dosyalarını test et" kutucuğunu işaretleyiniz.

Taramayı başlattıktan sonra, "arka plana geç"e tıklayarak bilgisayarınızı diğer görevler için kullanmaya devam edebilirsiniz.

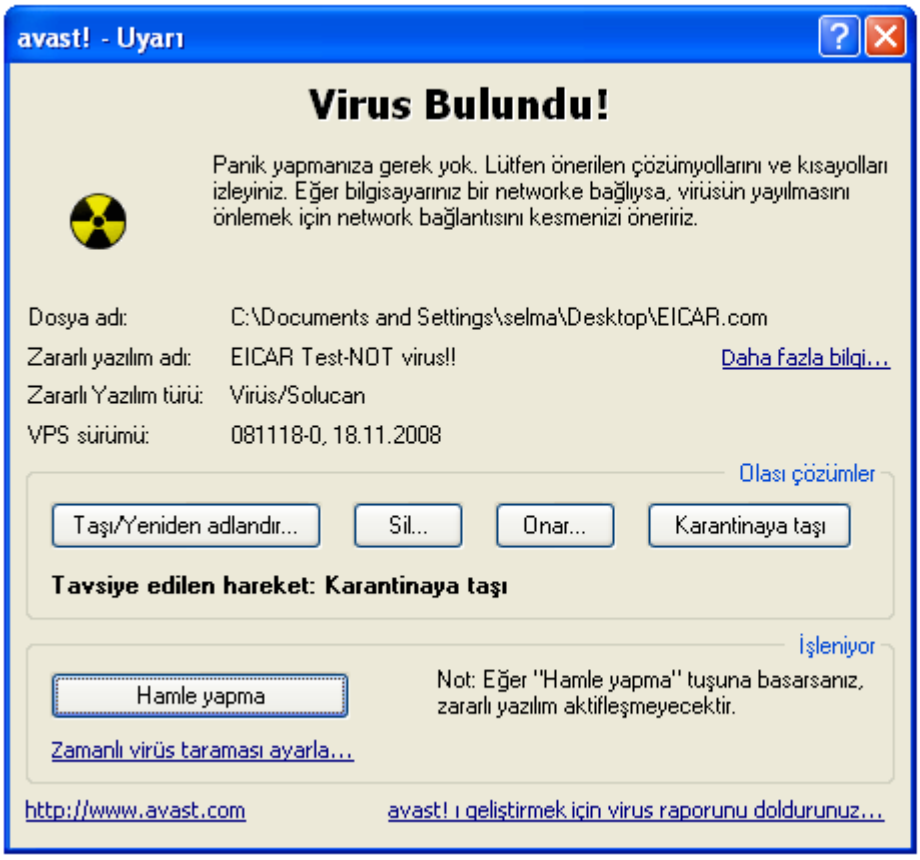
Yerleşik korumanın duyarlılığını ayarlamak için "ayarlar"a gidin, ve "yerleşik koruma"yı seçin. Duyarlılığı standart ya da yüksek olarak ayarlayabilir, veya devre dışı bırakabilirisiniz. Fakat, daha önce de belirttiğimiz gibi burada yapacağınız herhangi bir değişiklik bütün yerleşik koruma modüllerini etkileyecektir. Modüllerin ayrı ayrı duyarlılığını ayarlamak için, sayfa 22'ye bakınız.

Virüs Karantinası ve Virüs Veritabanı gibi diğer özelliklere "Araçlar"dan ulaşabilirsiniz. Bütün bunlar ve diğer özellikler, ilerleyen bölümlerde ele alınmıştır.

Durum bilgisi, ekranın alt kısmında yer almaktadır.

Herhangi bir virüs bulunduğunda yapmanız gerekenler

Program şüpheli bir dosya bulduğunda, taramaya ara verilecek, ve aşağıdaki ekran sizi yönlendirecektir.

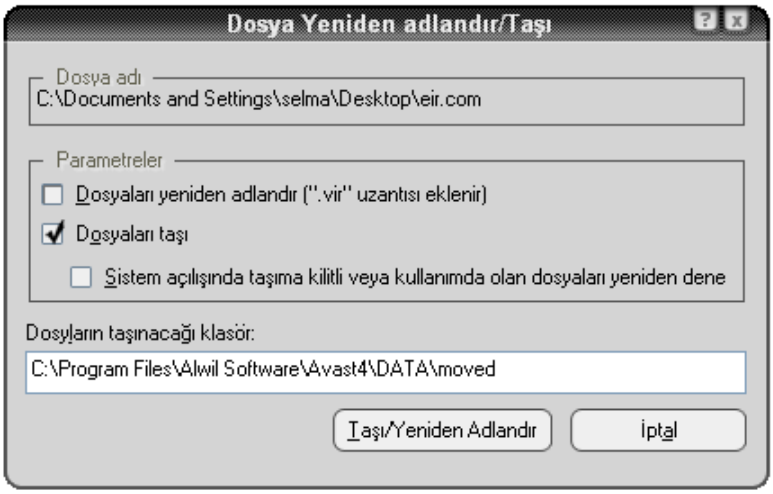


"Devam" tuşuna bastığınızda, hiç bir işlem yapılmayacaktır ve bu tarama sonuçları listesinde yer alacaktır (bknz. 33). "Dur" tuşunu tıkladığınızda ise tarama o anda sonlanacaktır.

Yerleşik koruma modüllerinden herhangi biri tarafından virüs bulunursa, mesela virüslü bir dosya açarken ya da ekran koruyucunuz tarafından, uyarı ekranı farklı görünebilir. "Devam" yada "dur" tuşlarının yerine tek bir seçenek "Hamle yapma" sunulacaktır. Bu butona tıklarsanız hiç bir hamle yapılmayacak, virüslü dosya olduğu yerde kalacak fakat aktif olmayacaktır.

Eğer o nada harekete geçmek istiyorsanız, dört farklı yöntem uygulayabilirsiniz;

Yöntem 1: Virüslü dosyayı bilgisayarınızdaki herhangi bir diğer klasöre taşıyabilirsiniz. Bu noktada , aynı zamanda, dosyayı yeniden adlandırabilirsiniz. "Taşı/Yeniden adlandır" butonunu tıkladığınızda aşağıdaki küçük pencere açılacaktır. "Dosyaları taşı" seçeneği önceden işaretlenmiştir.



Pencerenin beyaz kısmında, şüpheli dosyanın nereye taşınmasını istiyorsanız belirleyebilirsiniz. Program otomatik olarak yerini belirleyecektir, fakat arzu ederseniz farklı bir klasör belirleyebilirsiniz.

"Dosyaları yeniden adlandır" kutucuğunu işaretleyecek olursanız, dosya adının sonuna ".vir" uzantısı eklenecektir. Böylelikle, dosyanın virüslü olduğunu gelecek sefer hatırlayacak ve yanlışlıkla yürütmeyeceksiniz. Dolayısı ile bilgisayarınızın virüslenmesi önlenmiş olacaktır.

Dosya başka bir progarm tarafından kullanılıyorsa, dosyayı taşımak mümkün olmayabilir. Bu durumda, "Sistem açılışında taşıma kilitli veya kullanımda olan dosyaları yeniden dene" onay kutucuğunu işaretlerseniz, dosya, otomatik olarak, bilgisayarınız yeniden başlatıldığında seçilen alana taşınacaktır.

Not: Eğer, ***sistem dosyası*** virüslenirse (örneğin; anahtar programı yürütmek için kullanılan bir dosya olabilir) ve bu dosyayı taşırsanız, bilgisayarınız, bir dahaki sefer, programı yürütmeye çalışırken hata verebilir. Ancak, dosyayı Karantinaya taşırsanız , karantina alanında korunacak ve eski yerine geri taşınmadan önce tamir edilmesi mümkün olabilecektir. (bknz. 8)

Yöntem 2: "Sil" seçeneğini tıkladığınızda ise aşağıdaki pencere ekranınıza gelecektir:

Hangi Windows versiyonunu kullandığınıza bağlı olarak, dosyayı silmenin iki yolu vardır.

- ***Dosyayı çöp kutusuna yolla***

Bu seçenek, dosya yada dosyaları geri dönüşüm kutusuna atacak fakat tamamen silmeyecektir. Böylece bu dosya ya da dosyalar, daha sonra restore edilebilir (geri yüklenebilir). Bu seçenek bazı Windows versiyonlarında kullanılmayabilir.

- ***Dosyayı tamamen sil***

Bu seçenek, dosya ya da dosyaları bir daha geri yükleme olanağı olmaksızın silecektir. Fakat, bu seçenek yalnızca virüslü dosyayı silecektir. Bazı virüsler, bilgisayarınıza yeni dosyalar yükleyebilir. Bu yeni yüklenen dosyaların kendisi virüs içermiyorsa, bu dosyalar şüpheli dosya olarak bulunmayacaktır. Bu dosyalar bilgisayarınızda yer kaplar, fakat güvenlik riski oluşturmazlar.

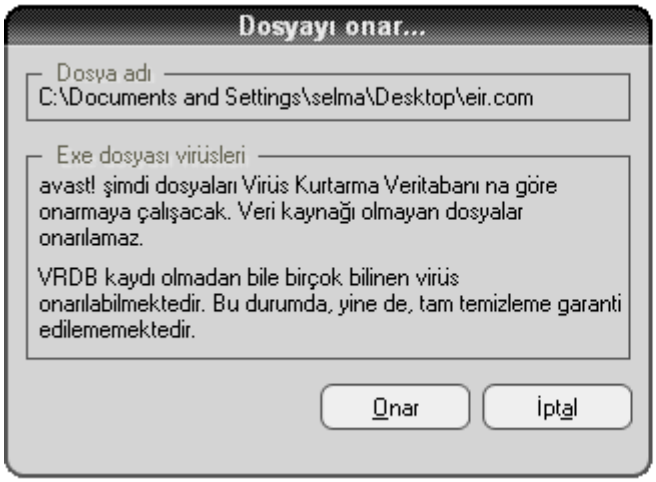
Yerleşik virüs silicisi tarafından, tamamen kaldırılabilir türde (yeni eklenen dosyalar dahil) bir virüs bulunursa, ***" Virüsü sistemden tamamen kaldır***" seçeneği, virüs uyarı kutusunda yer alacaktır. Eğer bu seçenek kullanılabilir durumda ise , bu seçeneği kullanmanızı tavsiye ediyoruz.

Dosya başka bir program tarafından kullanılıyorsa, silmek mümkün olmayabilir. Bu durumda "Gerekli ise sistem yeniden başlatıldığında dosyayı sil" seçeneğini işaretlerseniz, dosya bilgisayarınız yeniden başlatıldığında silinmiş olacaktır. Daha sonra "SİL" butonuna tıklayarak silme işlemini teyid etmeniz gerekecektir.

Not: Eğer, ***sistem dosyası*** virüslenirse (örneğin; anahtar programı yürütmek için kullanılan bir dosya olabilir) ve bu dosyayı silerseniz, bilgisayarınız, bir dahaki sefer, programı yürütmeye çalışırken hata verebilir. Dosyayı tamamen silmeden önce, virüslü dosyanın sistem dosyası olmadığından emin olmalısınız. Ya da dosyayı temiz bir dosya ile (mesela yedeklerinizden) yerine koyabilmeniz gerekmektedir. Emin değilseniz, dosyayı Karantinaya taşımanızı tavsiye ediyoruz . Karantinaya taşınan dosyalar korunacak ve eski yerine geri taşınmadan önce tamir edilmesi mümkün olabilecektir. (bknz. 8)

Yöntem 3: Dosyayı onarabilirsiniz.

"Onar" seçeneğini seçtiğinizde aşağıdaki pencere açılacaktır.



"Onar" butonuna tekrar tıklarsanız, program, dosyayı orjinal haline geri getirmek için tamir etmeye çalışacaktır.

Dosyayı tamir etmek için, program ***Virüs Kurtarma Veritabanına*** sevkedecektir. Veritabanında programla ilgili yeterli bilgi varsa, dosyayı tamir etme şansınız olabilir. Yalnızca virüs tarafından fiziksel olarak değiştirilen dosyalar onarılabilir. Yeni dosyalar yaratılmış ise, bu dosyalar virüs temizleyicisi ile kaldırılmadığı müddetçe yerinde kalacaktır. Yukarıdaki Yöntem 2 kısmına bakınız.

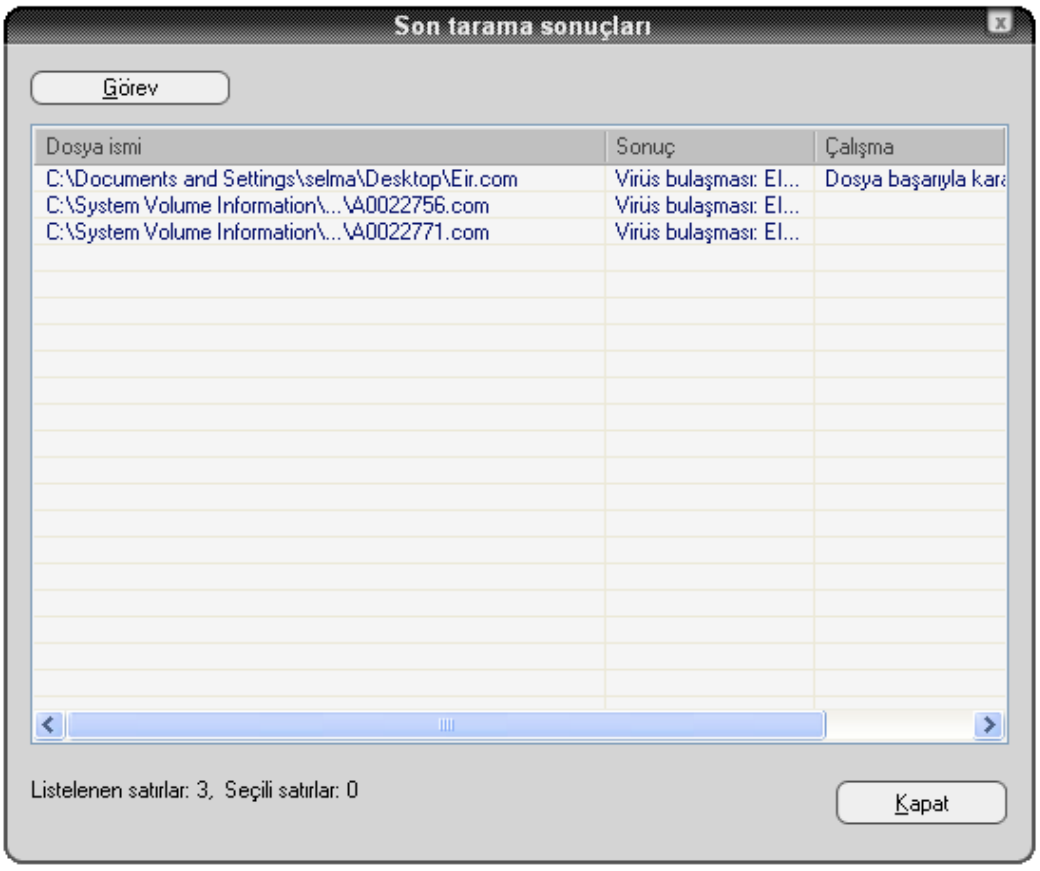
Veritabanında herhangi bir bilgi yoksa, onarmak belki hala mümkün olabilir ancak tam olarak onarılması mümkün olmayabilir. Bu nedenle, Veritabanının devamlı güncellenmesi çok önemlidir, Virüs kurtarma Veritabanını güncellemek için, bilgisayar ekranınızın sağ alt köşesindeki, mavi "i-avast" balonuna sol tuş ile basın ve "Şimdi VRDB oluştura tıklayın". Veritabanı bu durumda, bilgisayarınıza, son güncellemeden itibaren yüklenen, bütün yeni programların detayları ile güncellenecektir.

Yöntem 4: TAVSİYE EDİLEN YÖNTEM Karantinaya Taşı seçeneğidir.

Not: Eğer, ***sistem dosyası*** virüslenirse (örneğin; anahtar programı yürütmek için kullanılan bir dosya olabilir) ve bu dosyayı taşırsanız, bilgisayarınız, bir dahaki sefer, programı yürütmeye çalışırken hata verebilir. Ancak, dosyayı Karantinaya taşırsanız , karantina alanında korunacak ve eski yerine geri taşınmadan önce tamir edilmesi mümkün olabilecektir (bknz. 8)

Tarama sonuçları

Dosya ile ne yapacağınızı belirlediğinizde, tarama otomatik olarak başlayacaktır. Eğer daha fazla şüpheli dosya bulunursa, tarama duraklatılacak (*isteğe bağlı taramada "Hepsini sil" seçeneğini işaretlemedi iseniz*) ve aynı işlem devam edecektir.Tarama tamamlandığında , tarama sonuçları, yapılan hamlelerin tüm detayları ile farklı bir pencerede gösterilecektir. Aşağıdaki pencereyi inceleyiniz.



Tarama sırasında herhangi bir hamlede bulunmaz iseniz, bu da tarama sonuçlarında yer alacaktır. Fakat Çalışma bölümü boş olacaktır.

Dosya ile şimdi ilgilenmek için, önce tablodaki dosyanın adının üzerine tıklayınız. Daha sonra sol üst köşedeki "Görev "butonuna tıklayın. Daha sonra mevcut seçeneklerin listesini göreceksiniz. Bu işlemden sonra yaptığınız hamle "Çalışma" kolonunda görnecektir.

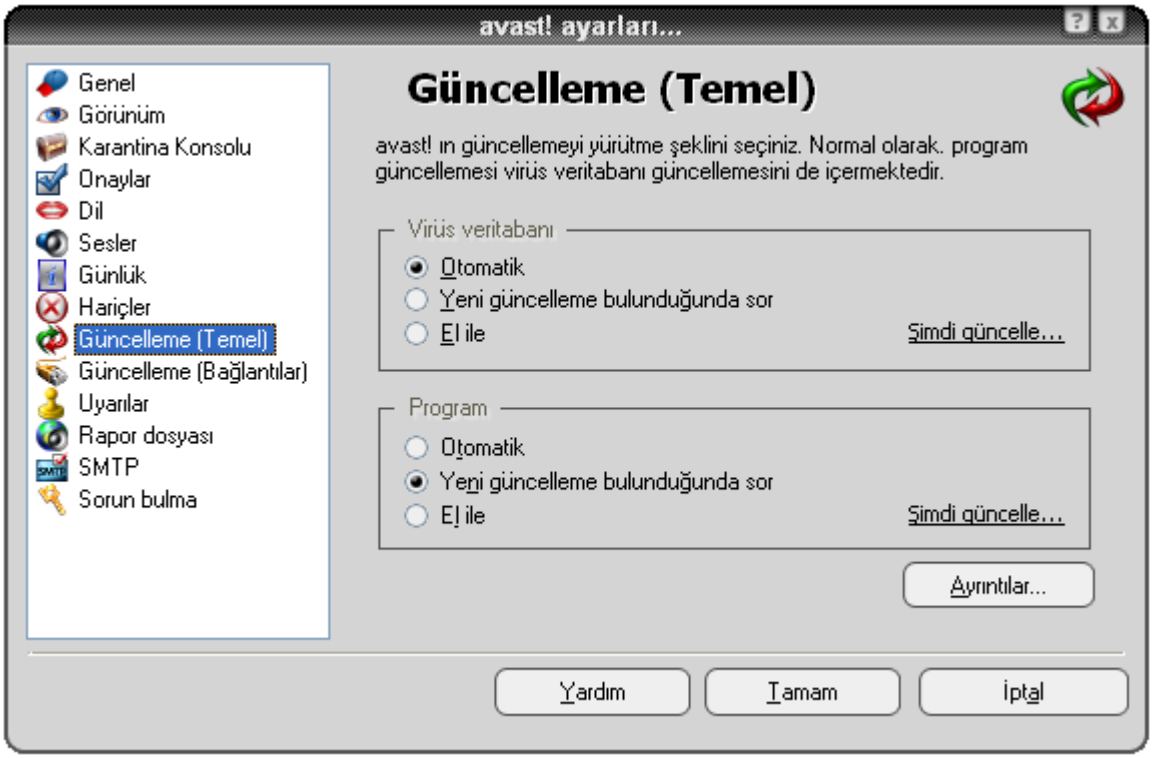
Şüpheli dosyalarla işiniz bittikten sonra, Kapat butonunu tıklayaraktarama işlemini sonlandırmanız gerekmektedir. Tarama sonuçlarını tekrar görmek için menüyü açın ve "Son tarama sonuçlarını" seçin.

Not: Programı kapatırsanız, parogramı yeniden başlattığınızda "Son tarama sonuçları"nı görüntülemeniz mümkün olmayacaktır. Bu seçenek yalnızca yeniden tarama başlattığınızda kullanılabilir. Fakat, kaydedilen virüslerin detayları ya da herhangi bir hata Günlük görüntüleyicisinden bulunabilir. (bknz. 48)

İleri Özellikler

Otomatik güncellemeleri ayarlama

Herhangi bir antivirüs progarmının kendisinin ve kendisine ait virüs veri tabanının, düzenli bir şekilde güncellenmesi çok önemlidir.
Programın elle yada otomatik olarak güncellenmasini sağlayabilirisiniz.Ya da sadece güncelleme notunu takip ederek programı ve veri tabanını güncelleyebilirsiniz. Durumu değiştirmek için, oynatıcının üzerinde ya virüs veri tabanının mevcut sürümü üzerine tıklayın, ya da, menüden açın, "Ayarları" seçin ve daha sonra "Güncelleme (Temel)" e tıklayın. Bu noktada, programın ve virüs veri tabanının hangi yöntemde güncelleneceğini belirleyebilirsiniz. Lütfen aşağıdaki pencereyi inceleyiniz.



"Tamam"a tıklayın ve oynatıcıdaki mevcut durum şu şekilde güncellenecektir:

- **AÇIK:** Hem veri tabanı hem de program için Otomatik güncelleme tercih edildi ise,
- **YALNIZCA PROGRAM:** Sadece program için Otomatik güncelleme seçildi ise,
- **YALNIZCA VERİTABANI:** Sadece Veritabanı için Otomatik güncelleme seçildi ise,
- **KAPALI:** Otomatik güncelleme hem veri tabanı hemde program için seçilmedi ise kapalı olacaktır.

Hem programı hemde virüs veri tabanını elle güncellemek için, menüye (sayfa 22) gidin ve "Güncelleme" seçeneğini seçin.

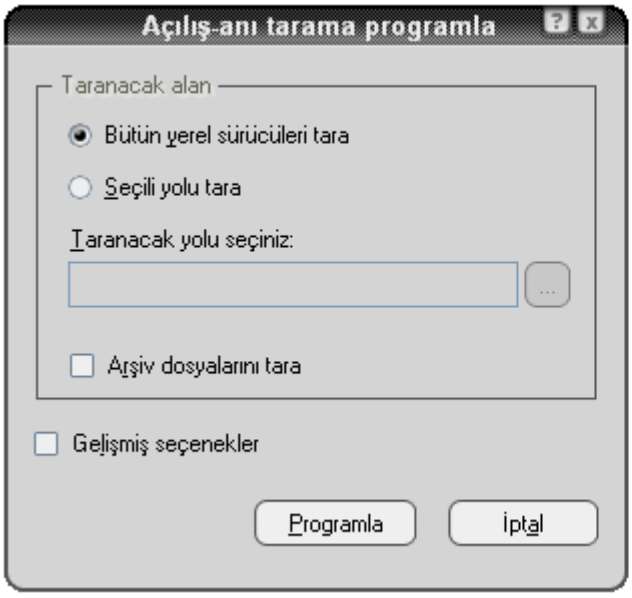
- Virüs veri tabanını güncelleemk için **iAVS Güncelleme**
- avast! programı güncellemek için **Program Güncellemeyi** seçiniz.

Açılışta taramanın programlanması

(Yalnızca Windows NT/2000/XP/Vista 32 bit versiyonları)

Taramanın açılışta, daha işletim sistemi henüz başlamadan, otomatik olarak gerçekleştirilmesini sağlayabilirsiniz. Bilgisayarınızda virüs olduğunu düşünüyorsanız, bu yöntem ile virüsün bilgisayarınıza zarar vermeden etkisiz hale getirilmesini sağlayabilirsiniz.

Açılışta taramayı programlamak için, menüye gidin ve "Açılışta taramayı programla " seçeneğinin üzerine tıklayın. Aşağıdaki pencere ekranınıza gelecektir.



Buradan, ya bütün yerel sürücülerin taranmasını ya da yalnızca seçeceğiniz alanların taranmasını programlayabilirsiniz. Yalnızca seçili yolu taratmak istiyorsanız , "seçili yolu tara" seçeneğini işaretleyiniz, daha sonra taranacak yolun adını metin boşluğuna yazınız ya da metin boşluğunun yanındaki kutucuktan seçilecek yol için göz atınız. Taranacak yolu bulduktan sonra, üzerine tıklayın, böylece taranacak yolun adı otomatik olarak metin boşluğuna kopyalanacaktır. Arşiv dosyalarının da taranmasını istiyorsanız, yalnzıca "Arşiv dosyalarını tara" onay kutucuğunu işaretleyiniz.

"Geşilmiş seçenekleri" işaretleyerek, virüslü dosyalarla ne yapmak istediğinizi belirleyebilirsiniz. Aşağıdaki seçeneklerden herhangi birini seçebilirsiniz.

- Hareket için sor
- Virüslü dosyayı sil
- Virüslü dosyayı taşı
- Virüs bulaşmış dosyaları karantinaya taşı
- Virüslü dosyayı yoksay
- Virüs bulaşmış dosyayı onar.

"Virüslü dosyayı taşı" seçeneğini işaretlerseniz, şüpheli dosya C:/Program Files\Alwil Software\Avast4\DATA\moved klasörüne taşınacaktır. Dosya adının sonuna ".vir" uzantısı eklenecektir. Böylece virüslü dosyayı yanlışlıkla yürütmeniz ve dolayısı ile bilgisayarınızın hasar görmesi engellenmiş olacaktır.

Virüslü dosyayı sil yada taşı seçeneklerinden herhangi birini işaretlerseniz, virüslü ***sistem dosyaları*** ile ne yapmak istediğinizi onaylamanız gerekmektedir.

Sistem dosyaları, bilgisayarınız tarafından, programlarınızı yürütmek için kullanılmaktadır. Bu dosyaları silmek, ya da taşımak ciddi sorunlara neden olabilir. Bu nedenle, ne yapmak istediğinizi teyid etmeniz gerekmektedir.

- Silme veya taşımaya izin ver
- Sistem dosyaları için silme ya da taşımayı yoksay

"Sistem dosyaları için silme ya da taşımayı yoksay" seçeneğini işaretlediğinizde herhangi bir potansiyel işletim problemi meydana gelebilir. Yani, bilgisayarınız, potansiyel problem nedeni ile risk altında olmaya devam edecektir. Önerilen seçenek, şüpheli dosyaların hepsini virüs karantinasına taşımak olacaktır. Virüs karantinasına taşıdığınızda, şüpheli dosyalar artık diğer dosyalarınıza zarar veremeyeceklerdir sayfa 46 de virüslü dosyalarla ne yapılması gerektiği açıklanmıştır. Örneğin, bu dosyalar silinebilir, güvenli olduğundan eminseniz eski alanına geri gönderilebilir, ya da ne yapacağınıza karar verene kadar depolanabilir.

Virüslü dosyalarla ne yapacağınıza karar verdiğinizde ve onayladığınızda, "Programla" seçeneğine tıklayınız.

Bilgisayarınızı yeniden başlatmak ve açılışta taramayı hemen başlatmak için "Evet"e tıklayın. "Hayır"a tıklarsanız, tarama otomatik olarak, bilgisayarınızı yeniden başlattığınızda gerçekleştirilecektir.

Tarama dışı bırakılacak dosyaların belirlenmesi (Hariçler)

Bazı alanları ve hatta bazı dosyaları kendi başına tarama dışı bırakabilirsiniz. Tarama dışı bırakılan alan ya da dosyalar, test edilmeyecektir. Bu uygulama aşağıdaki durumlarda son derece yararlıdır.

- **Yanlış pozitif alarmlarını önlemek:** Program bir dosyada virüs alarmı verirse, ve bu alarmın yanlış alarm olduğundan emin iseniz, dosyayı tarama dışı bırakabilir ve gelecekte meydana gelebilecek yanlış alarmların önüne geçebilirsiniz**.** Lütfen, avast!ı yanlış alarmların önüne geçilmesi için, bu dosyalar hakkında bilgilendiriniz.

- **İşlemi hızlandırmak:** Örneğin, hard diskinizde yer alan yalnızca imgeler içeren klasörleri, hariçler listesine ekleyerek tarama hızını arttırabilirsiniz.

Bu hariçler gelecekte, yerleşik koruma hariç, bütün taramaları etkileyecektir. Belirli dosyaları ve klasörleri taramadan hariç tutmak için, menüye gidin ve ayarlardan "Hariçler" bölümününün üzerine tıklayın. Aşağıdaki pencere ekranınıza gelecektir.

Bir dosyayı yada bir kalasörü tarama dışı bırakmak için, "Gözat" butınuna tıklayın, ve taranmasını istemediğiniz kalsörü yada dosyayı seçin. Aslternatif olarak, "Ekle" butonuna tıklayıp tarama dışı bırakmak istediğiniz dosya ya da klasörü Hariçler kutucuğuna giriniz. Eğer bir klasörü bütün alt klasörleri ile beraber girmek isterseniz "*" bu uzantıyı klasörün adının sonuna eklemeniz gerekmektedir. Örneğin, . C:\Windows*. Herhangi bir kalsörü yada dosyayı hariçler listesinden kaldırmak için, dosyayı ya da klasörü seçin ve "Kaldır" butonuna tıklayın.

Tarama sonuçlarının raporlanması

Bütün tarama sonuçlarını içeren bir rapor oluşturabilirsiniz. Rapor oluşturmak için, menüye gidin, ve "Ayarlar"ı seçin. Daha sonra pencerenin solunda bulunan "Rapor dosyası" nın üzerine tıklayın ve "Rapor dosyası oluştur" onay kutucuğunu aşağıdaki gibi işaretleyin.

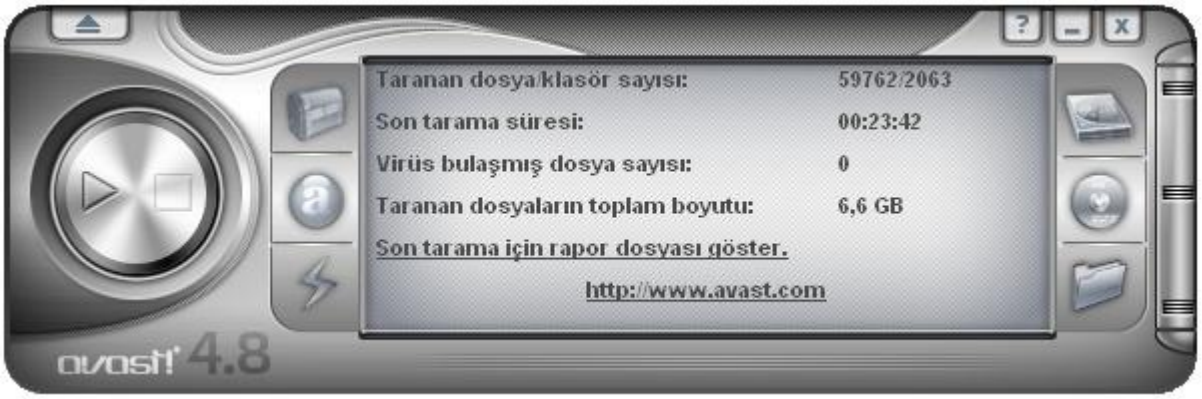
Her taramadan sonra yeni bir rapor dosyası oluşturmak istiyorsanız ve önceki tarama sonuçlarının raporlarını saklamak istemiyorsanız, "Varolanın üzerine yaz " kutucuğunu işaretleyiniz. Bu kutucuk işaretli değilse, her bir tarama sonucu, önceki raporun sonuna eklenecektir.

Ayrıca raporun nerede saklanacağını da seçebilirsiniz. Standart program klasöründe (program bunu otomatik olarak seçmektedir) ya da "özel program klasörü" seçeneğini işaretleyip klasör alanını girerek yeni bir alan belirleyebilirsiniz.

Dahası, raporun hangi bilgileri içereceğini belirleyebilirsiniz.

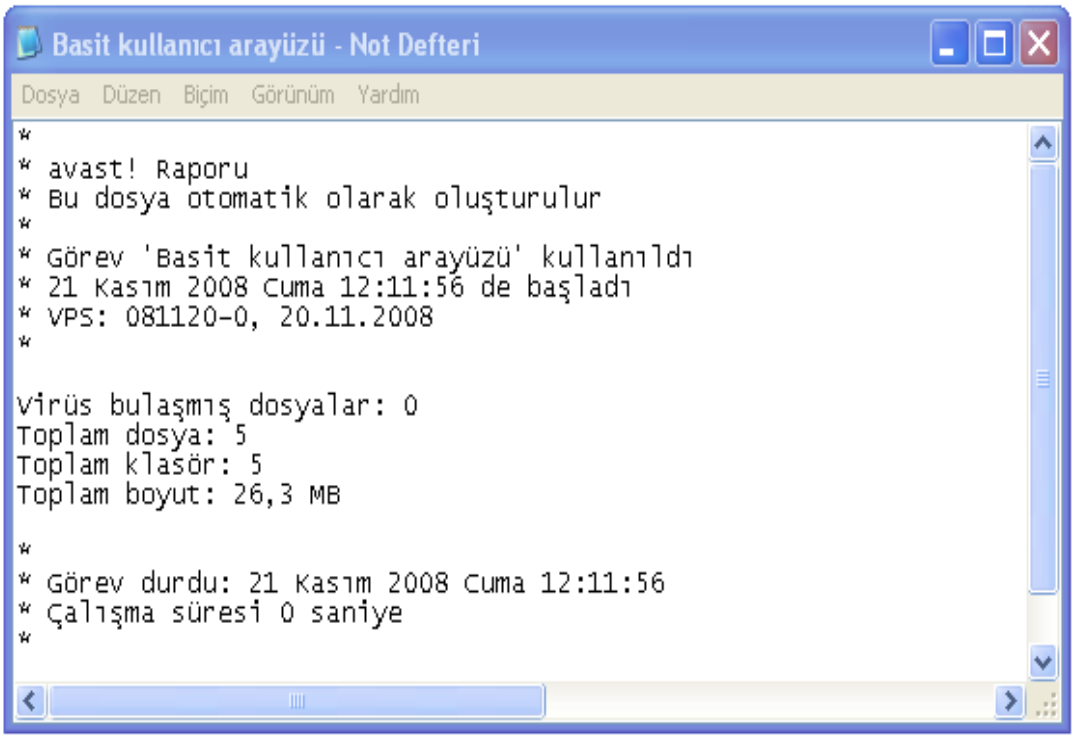
- Görev başlat- Taramanın başlatıldığı tarih ve saat
- Görev durdur- Taramanın tamamlandığı tarih ve saat.
- Hatasız dosyalar- Taranıp, şüpheli herhangi bir şeyin bulunmadığı dosyalar. Bütün yerel sürücüler tarandı ise, bu rapor oldukça uzun olacaktır. Muhtemelen binlerce satır olabilir. Önerimiz, bu seçeneği, yalnızca, sınırlı tarama gerçekleştirmek istiyorsanız ve bütün temiz dosyaların raporlanmasını istiyorsanız işaretlemenizdir.
- Büyük hatalar, normalde beklenmeyen birşey bulduğunda ortaya çıkmaktadır. Bu hataların araştırılması gerekmektedir.
- Küçük hatalar, büyük hatalardan daha az önem arzetmektedir. Genellikle, açık ve başka bir uygulama tarafından kullanıldığı için taranamayan dosyalarla ilişkili bir sorundur.
- Atlanan dosyalar, tarama ayarlarında yer almayan dosyalardır. Örneğin, hızlı taramada dosyalar, dosya uzantılarına göre taranmaktadır. Tehlikeli olmadığı varsayılan uzantılara sahip dosyalar, taranmamaktadır.Tarama dışı bırakılan dosyalar da, ayrıca, atlanan dosya olarak raporlanmaktadır.
- Virüslü dosyalar, ise potansiyel olarak virüs içeren dosyalardır.

Son olarak, raporun metin dosyası fromatında mı yoksa XML dosyası formatında mı olacağını belirleyebilirsiniz. Taramayı başlattıktan sonra, "son tarama için rapor dosya göster" şeklinde, aşağıdaki pencerede olduğu gibi, durum bilgisi penceresine satır eklenmiş olacaktır.



"Son tarama için rapor dosya göster" satırının üzerine tıkladığınızda, seçtiğiniz formatta rapor gösterilecektir. Alternatif olarak, menüye gidebilir ve "Tarama raporlarını Görüntüle" satırını işaretleyerek, raporu görüntüleyebilirsiniz.

Metin dosyası formatında:

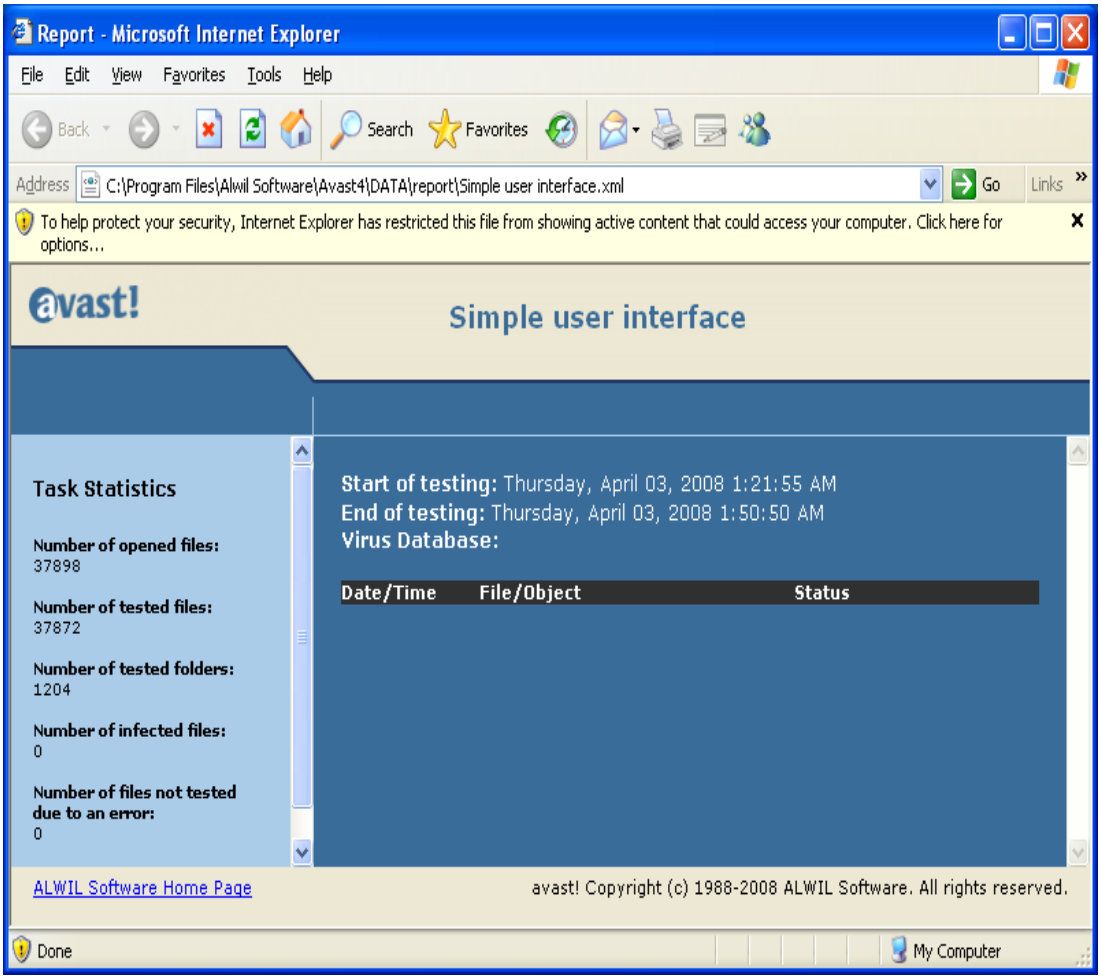


XML formatında :

Bir önceki tarama raporu, yapmış olduğunuz ayarlamaya bağlı olarak, ya standart dosya klasöründe ya da özel dosya klasöründe depolanmaktadır.(bir önceki sayfaya bakınız)

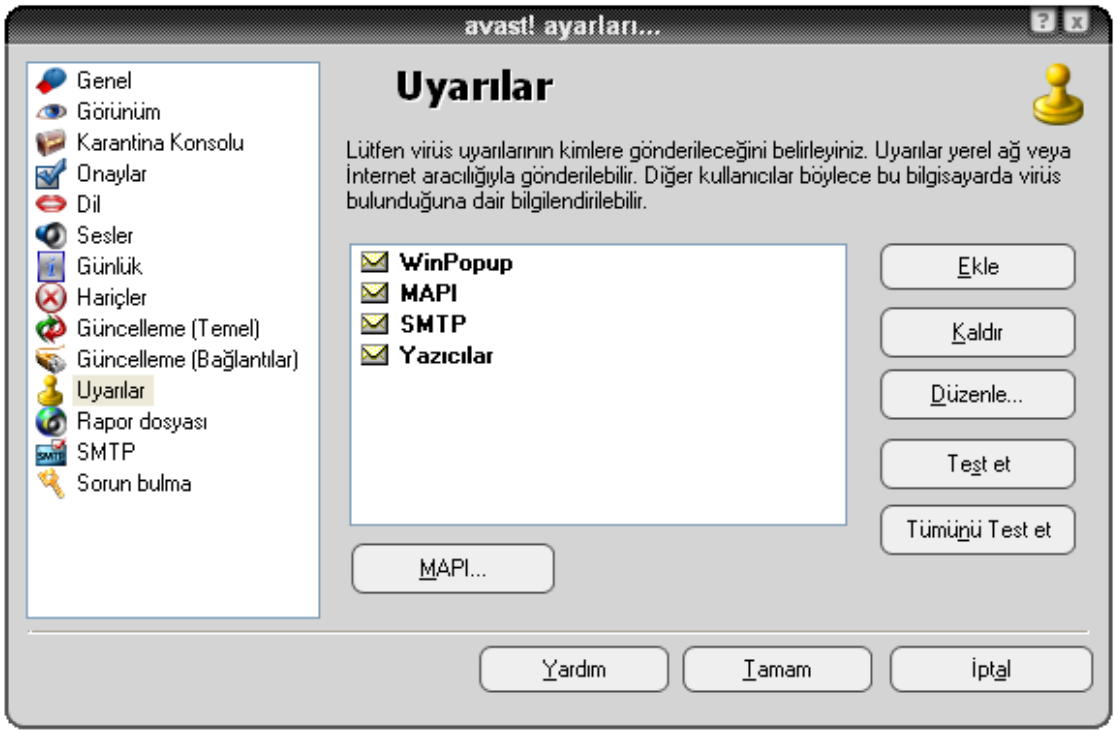
Metin menüsü formatını seçti ve "Varolanın üzerine yaz" kutucuğunu işaretlemedi iseniz, önceki raporları da görebilirsiniz.

Sonraki taramalarınızda rapor istemiyorsanız, menüye gidin "Rapor dosyasına" gidin ve "Rapor dosyası oluştur" onay kutucuğunun yanındaki işareti kaldırın.



Uyarılar

avast! virüs bulduğunda uyarı mesajı göndermektedir. Menüden "ayarlar" ı seçin, "Uyarılar" bölümüne tıklayın. Bu özellik, ağ yöneticileri için çok yararlıdır. Böylece, herhangi bir virüs bulunduğunda, ağ yöneticisi, hemen duruma müdahale
edebilecektir



Uyarı aşağıdaki formlarda gönderilebilmektedir.

- **WinPopup.**
  "Ekle" butonuna tıklayın, ve WinPopup satırını işaretleyin. Daha sonra uyarının gönderileceği IP adresini ya da bilgisayara ait ağ adını girin. Ya da, gözatın ve listeden mümkün olan adresi seçin.

- **MAPI.**
  Uyarı, MAPI protokolü ile, eposta şeklinde gönderilecektir. Epostanın gönderileceği eposta adresinizi girin, daha sonra, ekranın altındaki MAPI butonunun üzerine tıklayın. Bu noktadan sonra, MAPI profil adını ve ilgili şifreyi girin.

- **SMTP.**
  Uyarı, SMTP protokolü ile, eposta şeklinde gönderilecektir. Yeni bir uyarı oluşturmak için, "Ekle" butonuna tıklayın, ve SMTP'yi seçin. Açılan kutuya, uyarının gönderileceği eposta adresini girin. Diğer ayarların da kesin olarak gerçekleştirilmesi gerekmektedir. İlerleyen safhadaki SMTP bölümünü inceleyiniz.

- **Yazıcılar.**
  Uyarı belirlenen yazıcıya gönderilecektir. "Ekle" butonuna ve daha sonra "Yazıcı"ya tıklayın. Gözat butnuna tıklayın ve kullanılabilecek yazıcıyı seçiniz.

Yeni bir uyarı yaratmak için, "Ekle" butonundan uyarının gönderilmesini istediğiniz alıcıyı seçin. Daha sonra istenilen detayları yukarıda belirtildiği gibi girin. Yeni uyarı oluşturulduğunda, bundan böyle artık, ne zaman şüpheli bir dosya bulunursa, uyarı belirtmiş olduğunuz alıcıya gönderilecektir.

Oluşturmuş olduğunuz uyarı alıcısını düzenlemek için, alıcıyı koyultun, daha sonra "Düzenle" butonuna tıklayın yada aynı şekilde kaldırmak için, alıcıyı koyultun ve "Kaldır"a tıklayın.

"Test et"butonuna tıklarsanız, test mesajı seçilen adrese gönderilecektir. "Tümünü test et" butonuna tıklarsanız, test mesajı bütün alıcılara gönderilecektir.

SMTP

Ekranın solundaki listeden SMTP2ye tıklayarak , SMTP parametrelerinizi belirleyebilirsiniz.avast! ayarlarını email mesajları için kullanmaktadır. Özellikle şu durumlarda,

- Virüs bulunduğunda uyarı mesajı göndermek için,
- Dosyaları Virüs Karantinasından ALWIL Software'e göndermek için,
- avast! hata raporlarını ALWIL Software'e göndermek için.

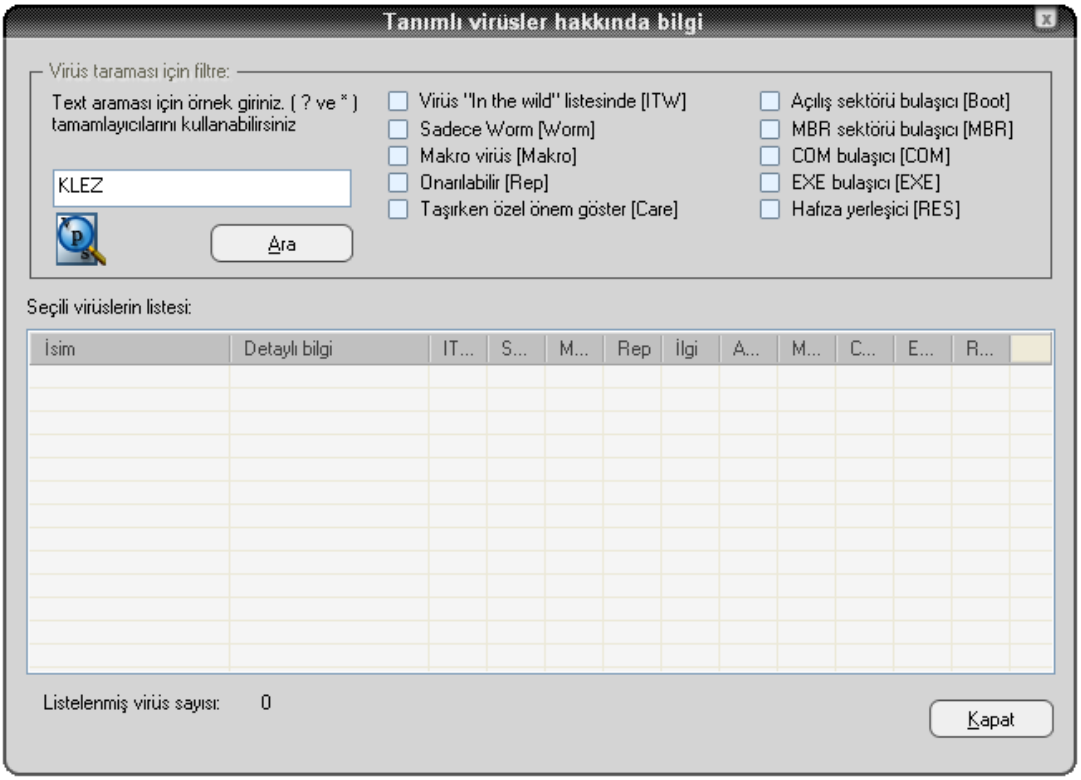
Aşağıdaki bilgileri girmeniz gerekmektedir.

- Sunucu adresi. Yani giden e-posta sunucusunun adresi. (Ör; smtp.server.com ya da 192.168.1.25)
- Port numarası, yani bağlantı noktası numarası. (varsayılan numara 25'tir)
- Gönderen adres yani göndericinin adresi.

SMTP, giriş yaparken kimlik doğrulaması isterse, "SMTP sunucusu kimlik doğrulaması istiyor" kutucuğunu işaretleyip, kullanıcı adı ve şifre kutucuklarını girmeniz gerekmektedir.

Virüs Veritabanında arama yapmak

Virüs veri tabanı, bilinen bütün virüslerle ilgili bilgileri içermektedir ve program tarafından herhangi bir potansiyel tehlikeyi tanımlamak için kullanılır.
Virüs veritabanına ulaşmak için, menüye gidin ve "Virüs veri tabanı" seçeneğinin üzerine tıklayın. Aşağıdaki pencere ekranınıza gelecektir.



Listedeki virüsler, bir çok parametre seçeneği ile araştırılabilir. Virüsün adını biliyorsanız, sadece bu adı kutucuğa giriniz, ve "Ara" butonuna tıklayınız. Eğer yalnızca, virüs adının bir kısmını biliyorsanız, "?" işaretini bilmediğiniz karekter (ya da numara)olarak kullanbilir ya da "*****" işaretini, birden fazla bilimeyen karekterler yerine kullanabilirsiniz.

Örneğin, "Klez" virüsü için arama yaptığınızı varsayalım. Bu virüsün gerçek adı **Win32:Klez-H [Wrm]** dir. Bu durumda virüsün adını *klez*. olarak girebilirsiniz. Bu durumda "klez" kelimesini içeren bütün virüsler bulunacaktır.

Aranacak ögenin daha da belirgin hale getirilmesi için, özelliklerin yer aldığı, onay kutucuklarını kullanabilirsiniz. Belirlenen özellikte arama yapılması için onay kutucuğunun üzerine iki kez tıklayınız.Herhangi bir onay kutucuğunun üzerine bir kere tıklarsanız, kutucuk gri bir renge dönüşecektir. Bunun anlamı programın bu özellikleri araştırmaması gerektiğidir. Hiç bir kutucuğu işaretlemezseniz, gri yada mavi olarak kalabilir, bunun anlamı virüsün o özellikleri içerip içermediği önemli değildir. ,

Aranabilir virüs özellikleri

- ***Virüs "In the wild" listesinder (ITW…)***
  Virüs listesindeki tüm dünyadaki kullanıcılara yayılabilen virüslerdir.

- ***Sadece Worm (Worm)***
  Bu türden olan virüsler dosyaları direk olarak etkilemezler, fakat kötü sonuçlar doğurabilirler. Örneğin kendilerini eposta yolu ile yayabilir, önmeli şifrelerinizi ele geçirebilirler.

- ***Macro virüs (Makro)***
  Bu tür virüsler makro dilini, özellikle Microsoft ürünlerini kullanmaktadır. (Word, Excel gibi…)

- ***Onarılabilir (Rep)***
  Yukarıdaki virüsler tarafından virüslenen dosyalar, avast! programı tarafından tamir edilebilir ve virüslenmeden önceki orjinal şekline dönüştürülebilir, restore edilebilir.

- ***Taşırken özel önem göster (Care)***
  Virüsleri kaldırırken, direktifleri takip etmeniz son derece önemlidir. Çünkü yapacağınız bir hata, virüsün verdiği zarardan daha fazla kötü sonuç doğurabilir.

- ***Açılış sektörü bulaşıcı (Boot)***
  Bu tür virüsler, hard diskin ya da disketin ön yükleme kesimini etkilemektedir.

- ***MBR sektörü bulaşıcı (MBR)***
  Bu tür virüsler, hard diskin ana ön yükleme kesimini etkilemektedir.

- ***COM bulaşıcı (COM)***
  Bu tür virüsler, ".com" uzantısı olan yürütülebilir dosyaları etkilemektedir.

- ***EXE bulaşıcı (EXE)***
  Bu tür virüsler, ".exe" uzantısı olan yürütülebilir dosyaları etkilemektedir.

- ***Hafıza yerleşici (RES)***
  Bu tür virüsler, bilgisayarın RAM hafızasına yerleşir, ve dosyaları başladıklarında virüslerler.

Virüs karantinasındaki dosyalarla neler yapılabilir

Virüs karantinasına menüden direkt olarak ulaşılabilir. Efektif bir "karantina" alanıdır. Aşağıdakileri uygulayabilirsiniz.

- ***Virüsleri depolamak***

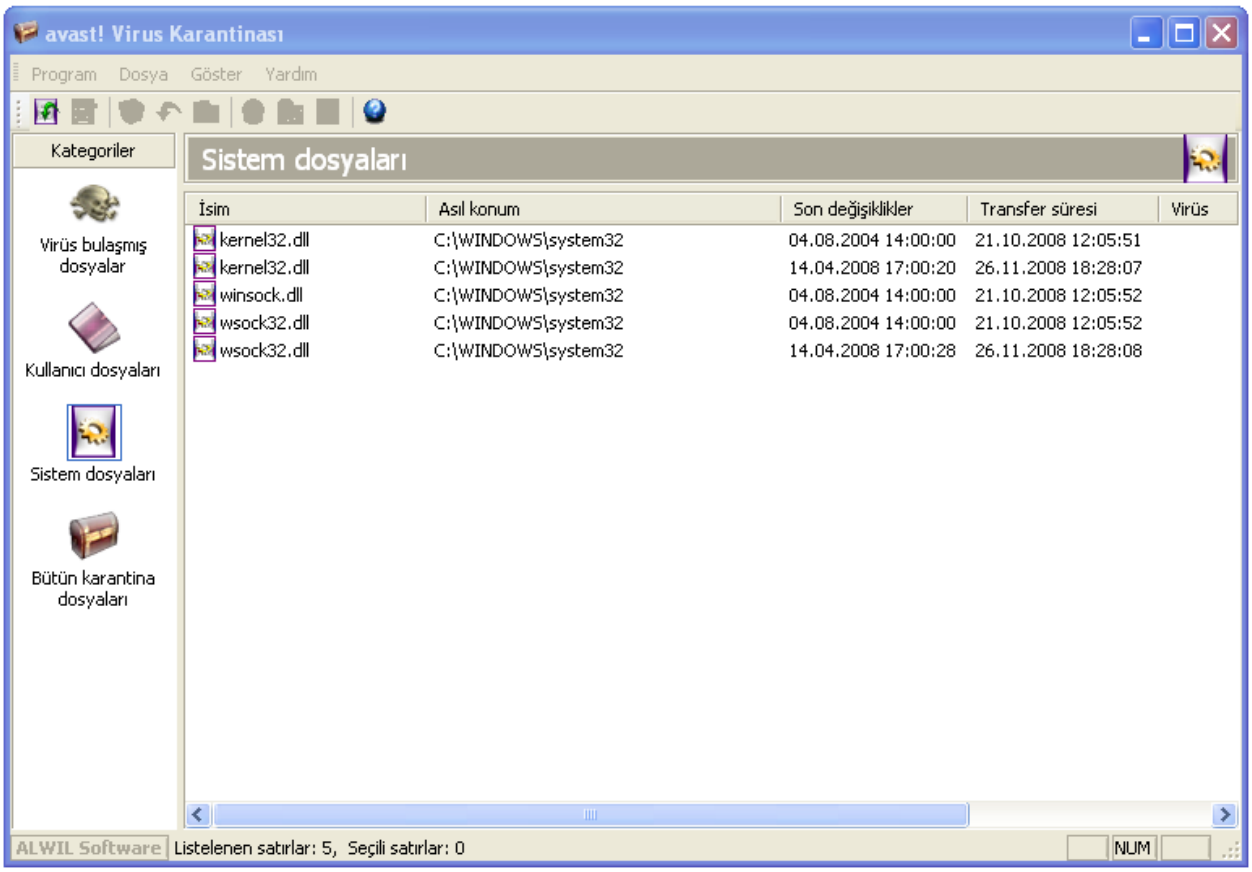
  Avast! virüs blduğunda, virüsü silmemeye karar verirseniz, program virüsü Virüs karantinasına taşımanızı önerecektir. Virüs karantinasındaki virüsün, yanlışlıkla açılması, yürütülmesi engellenmiş olacaktır.

- ***Şüpheli dosyaların depolanması***

  Daha sonra incelemeniz açısından, şüpheli dosyaları Virüs Karantinasına taşıyabilirsiniz.

- ***Sistem dosyalarının yedeklenmesi***

  Yükleme sırasında, bazı kritik sistem dosyalarının kopyaları, Karantinada "Sistem dosyaları" kategorisi altında depolanmaktadır. (aşağıdaki örneği inceleyiniz.) Ana sistem dosyası virüslenirse, yedek dosyalara karantinadan ulaşılıp yerlerine konulabilir.



Herhangi bir dosyanın üzerine sağ tıkladığınızda, aşağıdaki seçenekler sunulacaktır. Alternatif olarak, dosyaya sol tuş ile tıklayarak dosyayı koyultun, daha sonra ekranın üzerindeki ilgili ikonun üzerine tıklayın ya da "Dosya"seçeneğinin altındaki seçeneklerden istediğinizi uygulayınız. *(Not: Dosyaya **iki kez** tıklarsanız, dosyayı yürütemezsiniz, bunun yerine dosyanın özellikleri ekrana gelecektir. Bu bir güvenlik önlemidir. Böylece virüs karantina konsolundan herhangi bir zarar görmeniz engellenmiş olacaktır.):*

- ***Bütün dosyaları yenile***
  Dosyaların tam listesini yenilemek istiyorsanız bu seçeneği seçiniz. Program listeyi otomatik olarak yenilemektedir, fakat yinede, bu seçeneği, beklemek istemiyorsanız kullanabilirsiniz.

- ***Ekle***
  Bu seçenek yalnızca "Kullanıcı dosyaları" kategorisi için kullanılabilmektedir.

- ***Sil***
  Bu seçeneği seçerseniz, dosya tamamıyla silinecektir. Örneğin, dosya geri dönüşüm kutusuna gönderilmeyecektir! Herhangi bir dosyayı silerken, bu dosyanın sistem dosyası olmadığından kesinlikle ve kesinlikle emin olmanız gerekmektedir. Sistem dosyalarını silmek büyük sorunlara yol açabilmektedir.

- ***Geri yükle***
  Bu seçenek ile, dosya Karantinadan kaldırılmasıı ile beraber, orjinal yerine taşınacaktır.

- ***Sıkıştırılmış dosya aç***
  Dosya, seçili klasöre kopyalanacaktır.

- ***Tara***
  Dosya, virüslerin bulunması için taranacaktır.

- ***Özellikler***
  Dosyaya ait özellikler açılacaktır. Ayrıca, açıklama kısmına not da ekleyebilirsiniz.

- ***ALWIL Software'e eposta gönder***
  Seçilen dosya e-posta yolu ile ALWIL Software'e gönderilecektir. Bu seçeneği, lütfen, yalnızca özel durumlarda kullanınız. Örneğin, program, virüssüz olan dosyayı, virüslü olarak algılayıp hata yaptığında, yani yanlış alarm verdiğinde bu seçeneği kullanabilirsiniz. Gönderdiğiniz dosyaya ekleyebildiğiniz kadar bilgi ekleyiniz. Dosyayı gönderme nedeniniz, virüs veritabanınızın versiyonu, vs. Bu tür bilgileri eklemeniz, size vereceğimiz hizmetin kalitesini arttırması açısından son derece önemlidir.

Önce "Programlar"a sonra "Ayarlar"a tıkladığınızda "Karantina Konsolu"nu seçerek, en fazla karantina boyutunu ve gönderilebilecek en büyük dosya boyutunu seçebilirsiniz. Böylece konsolun ne kadar yer kaplayacağına karar verebilirsiniz.

Günlük Görüntüleyicisi

Herhangi bir taramadan sonra, avast! antivirüs, herhangi bir hata yada süpheli dosya hakkında bilgiler içeren birçok kayıt dosyası tutar. Kurulum yada programın güncellemeleriyle ve virüs veritabanı ile ilgili bilgiler de burada bulunur. Bu kayıtları görüntülemek için menüden "avast! Günlük Görüntüleyicisi"ni seçiniz.
Kayıt dosyalarında tutulan bilgiler aşağıdaki tablodaki gibi gruplandırılır.

Bilgi	Sadece bilgi için, herşey yolundadır.
Bildiri	Program ve veri tabanı göncellemeleri hakkında bilgiler içerir.
Uyarı	Bir hata oluşması ya da virüs bulunması, fakat program çalışabilir ya da sorunu tamir edebilir.
Hata	Hata oluştu ve program çalışamaz.
Kritik	Ciddi bir program hatası, program kapatılacaktır.
Uyarı	Bilgisayarın tamamı için bir risk söz konusudur.
Acil	Bilgisayarın tamamı için bir risk söz konusudur (güvenlik, sistem dosyalarının silinmesi)

"Ayarları" ve ardından Günlük Görüntüleyicisini tıklayarak, saklanacak her dosyanın maksimum boyutunu ayarlayabilirsiniz.

Günlük Görüntüleyicisi sayesinde,kayıtları özel kriterlere göre filtrelemek yada kayıtları başka yere taşımak için ,kayıtlarda arama yapmak mümkündür.

Kayıt bul

1. ‘’CTRL’’ ve ‘’F’’ tuşlarına beraber basabilir,
2. Ekranın sol üst köşesindeki ‘’Düzenle’’ butonuna ardından ‘’Bul’’ butonuna tıklayabilir,
3. Sol üst köşedeki büyütece tıklayabilir, ya da
4. Kayıtlar listesini sağ tıklayıp ve sunulan menüde ‘’Filitrele’’ye tıklayabilirsiniz.

Karşınıza bulmak istediğin kaydın adını ya da adının bir kısmını yazabileceğiniz bir kutu çıkacak. Eğer tam ismi biliyorsanız, “Sadece tam sözcükleri eşleştir” kutusunu işaretlemek, tam eşleştirmelerin listesini sunacaktır. Benzer şekilde,eğer büyük yada küçük harf kullanarak kayıtları aramak istiyorsanız ‘Büyük küçük harf eşeleştir ’’ işaretleyin. ‘’Yukarı’’ yada ‘’Aşağı’’ kutularını işaretlemek, kayıtların alafabetik olarak sırasıyla artan sırada yada azalan sırada listelenmesini sağlar.

Ardından “sonrakini bul” a tıklayın.İ lk kayıt görüntülenecektir. Girilen isimle eşleşen diğer kayıtlar başka kayıt bulanamayana kadar ‘’sonrakini bul”a tıklanarak bulunabilir.

Liste için filtre tanımla Bu, uzun bir kayıt listesinini özel kriterlerle uyuşan (mesela özel bir anahtar kelime yada bir kelimenin parçası gibi) ,daha kısa bir liste haline getirmek için kullanılır.

1. ‘’CTRL’’ ve ‘’R’’ tuşlarına beraber basın,yada
2. Ekranın sol üst köşesindeki ‘’Düzenle’’ butonuna ardından ‘’Filitrele’’ butonuna tıklayabilir, veya
3. Ekranın sol üst köşesindeki sarı huniye tıklatın, veya
4. Kayıtlar listesini sağ-tıklayın ve sunulan menude ‘’Bul’’a tıklayın

Filtreleme kriterini belirteceğiniz bir kutu belirecektir.

Kapsanacak

Gösterilmesi için, kayıtlarda olması gereken bir kelime yada kelimenin bir kısmını giriniz. Bilmediğiniz herhangi bir harf yerine * gibi özel simgeler kullanabilirsiniz. Farklı anahtar kelimeler noktalı virgül (;) ile ayrılmalıdır.

Kapsanmayacak

Gösterilmesi için, kayıtlarda olmaması gereken bir kelime yada kelimenin bir kısmını giriniz.

Süre sınırı

Gösterilecek listedeki kayıtlar için arama periyodunun başlangıç ve bitiş zamanlarını belirtebilirsiniz.

Tanımlanmış satırları seçin

Bu seçeneği işaretlerseniz, belirtilen kriterle eşleşen kayıt listede vurgulanacaktır

Sadece Tanımlanmış satırları göster (Kalanı gizle)

Bu seçeneği işaretlerseniz,belirtilen kriterle eşleşen kayıt lar listede gösterilecek,diğerleri görülmeyecektir .Bu orijinal listenin çok uzun olduğu durumlarda faydalıdır.

Kayıtları sınıflandır

Herhangi bir sütun başlığını tıklamak o sütundaki bilgiye göre kayıtların küçükten büyüğe (ya da tersi) sıralanmasını sağlar. Tekrar sütün başlığına tıklamak listeyi orijinal sıraya geri çevirir.

Kayıtları aktar

Bulunmuş yada filterlenmiş kayıtlar ,veya tüm liste dışa aktarılabilir ve yeni bir dosya olarak kaydedilebilir. Bulunmuş yada filtrelenmiş kayıtları dışa aktarmak için , 'Seçili satırları dışa aktar'' seçeneğini seçiniz yada ekranın sol üst köşesindeki sol yeşil oku tıklayın. Mevcut listeyi dışa aktarmak için, "Mevcut listeyi dışa aktar'' ı seçin yada sağ yeşil oku tıklayın. Yeni çıkan pencerede hedef klasörü seçip yeni dosya ismi girin, daha sonra ''Kaydet'' i tıklayın.

Gelişmiş arayüz kullanımı

Programı arayüz olmadan kullanıyorsanız, "Araçlar"dan "Gelişmiş kullanıcı arayüzüne geç" seçeneğini işaretlerseniz aşağıdaki pencere ekranınıza gelecektir. Arayüz (skin) kullanıyorsanız, gelişmiş kullanıcı arayüzüne "Ayarlar"dan "Gelişmiş kullanıcı arayüzüne geç"i tıklayarak geçebilirsiniz. Basit kullanıcı arayüzüne geçmek için, Sol üst köşedeki "Görüntüle" seçeneğinin altından "Basit kullanıcı arayüzü"ne tıklayınız.

Tarama Gelişmiş Kullanıcı Arayüzünde "Görevler" oluşturularak gerçekleştirilir. Bir görev yaratılırken, hangi alanların taranması gerektiğini, duyarlılığını vs. belirlemeniz gerekmektedir. Görev oluşturmanın avantajı, ya da "Programlayıcı" seçeneği ile daha sonra kullanılmak üzere kaydedilebilir oluşudur. Görev bir kere başlatıldığında, sonuçlar daha sonra tekrar görülebilmesi için kaydedilir.

Görevler

Program daha önceden ayarlanmış dört göreve sahiptir. Klasörlerin listesinde "Görevler"e tıkladığınızda pencerenin sağ pencerenin üstünde yürütülmeye başlayacaktır. Herhangi bir göreve tıkladığınızda, sağ pencerenin altında kısa bir özet yer alacaktır.
İlk görev "**yerleşik koruma**" dır. Durmaksızın gerçek zamanlı koruma sağlamaktadır. Bu koruma bilgisayarınız başlar başlamaz otomatik olarak çalışmaktadır.

Diğer üç görev, taranacak alanların belirlenmesi için kullanılmaktadır. Başlatmak için üzerine iki kez tıklayın ya da sağ tıklayıp "çalıştır"ı seçin.

"**Tara: A: Disket sürücüsü**" görevini tıkladığınızda bilgisayarınızın disket sürücüsündeki herhangi bir disk taranmış olacaktır.

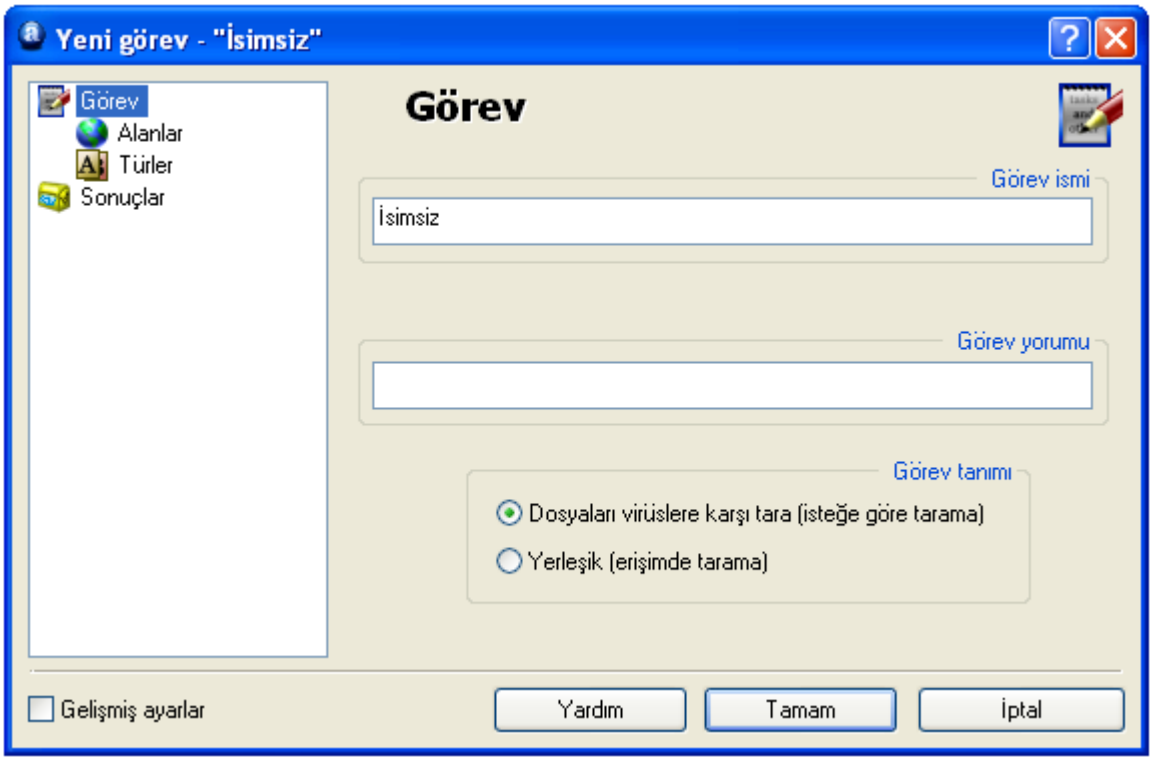
"Tara: Etkileşimli seçim" görevini, bilgisayarınızda belirli alanların taranmasını istediğinizde kullanabilirsiniz. Bu görevi başlatırsanız yeni bir pencere açılacak ve böylece pencerenin içindeki kutucukları işaretleyerek taranacak alanları seçebileceksiniz.

"Tara: yerel sürücüler" görevini başlattığınızda ise taşınamaz sürücülerdeki bütün dosyalar taranacaktır.

Görev oluşturulması ya da düzenlenmesi

Kendi görevlerinizi oluşturup, istediğiniz sıklıkta kullanmanız da mümkündür.
Görev oluşturmak, alanların belirlenmesi, hangi bilgilerin raporlanması, dosyaların nasıl belirleneceği gibi bir çok adımdan oluşmaktadır. Herhangi bir görev oluşturup "Tamam" a tıkladığınızda, aynı zamanda görev kaydedilmiş olacaktır. Herhangi bir ayar yapılmadı ise, görev varsayılan ayarlar ile kaydedilecektir. Herhangi bir görev kaydedildikten sonra , herhangi bir değişiklik yapmak için, ekranın üstündeki "Düzenle " seçeneğini kullanınız. Benzeri şekilde, kaydedilmiş herhangi bir görevi silmek için, görevi koyultun "Sil" seçeneği ile silin.

İlk olarak pencerenin üzerindeki, "Görevler" butonuna tıklayın. Daha sonra "Yeni oluştur" seçeneğini seçin. Ya da yine ekranın üzerindeki "Yeni" seçeneğine tıklayın. Aşağıdaki pencere ekranınıza gelecektir.

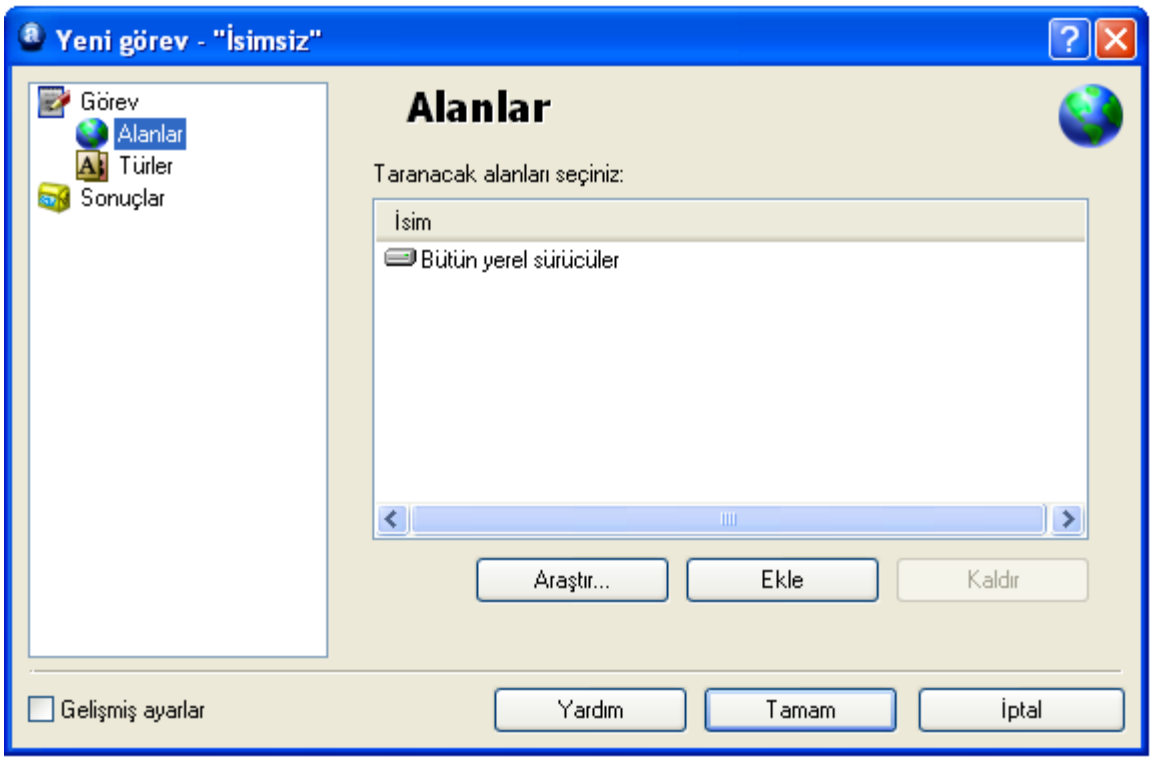


Bu pencerede, göreve isim verebilirsiniz. Verdiğiniz ism ana pencerede listede görünecektir. Verdiğiniz isim anlaşılır olmalıdır. Örneğin "Tara: Belgelerim" gibi. Ayrıca, yararlı olabilecek bir yorum da ekleyebilirisniz. Sonuç olarak bu pencerede, alt kısımdaki seçenekleri kullanarak, oluşturduğunuz görevi" isteğe bağlı" olarak ya ra "erişimde" taramaya ayarlayabilirsiniz. Erişimde taramaya ayarlarsanız, belirtilen dosya ya da klasörleri açmaya çalıştığınızda tarama gerçekleştirilecektir.

“İsteğe bağlı ” görev oluşturma

- ***Alanlar***

“Dosyaları virüslere karşı tara (isteğe bağlı olarak)” seçeneği ile görev oluşturmaya başlayabilirsiniz. Bunu yapabilmek için, görevlerin altındaki “Alanlar” butonuna tıklayınız. Aşağıdaki pencere ekrana gelecektir.



Taranacak alanlar, otomatik olarak “Bütün yerel sürücüler” in içinde yer alacaktır. Bütün yerel sürücülerin taranmasını istemiyorsanız, önce “Bütün yerel sürücüler”e daha sonra “Kaldır” butonuna tıklayınız. Bu noktadan sonra, “Araştır” butonunu kullanarak, taranacak alanları ilgili kutucukları işaretleyerek belirleyebilirsiniz.

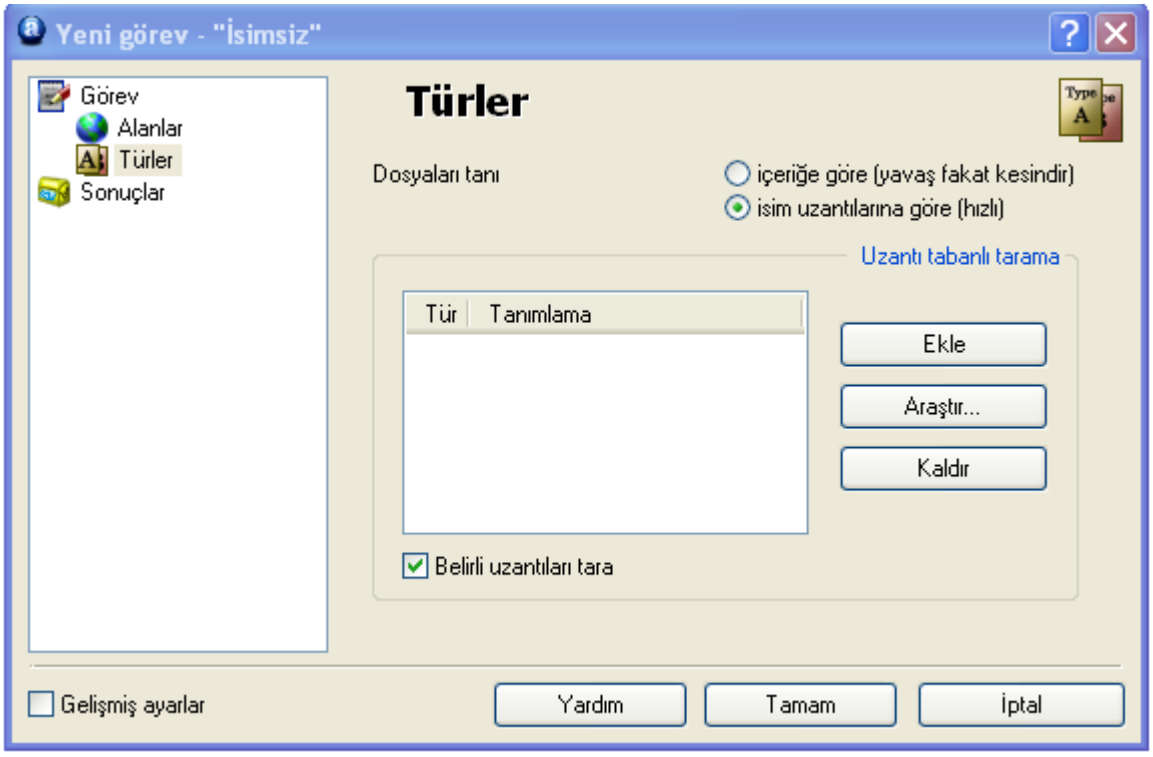
“Ekle” butonu ile, önceden tanımlanmış olan birçok alanı seçebilirsiniz. Fakat, “Tara: Etkileşimli seçim”i seçereseniz, görevi her başlattığınızda, taranacak alanları belirlemeniz gerekmektedir. “Diğer”i seçerseniz, taranacak alanı “<tür alanı>” kısmına yazarak girmeniz gerekecektir.

- ***Türler***

Taranacak alan(lar)I seçtikten sonra, hangi dosyaların taranacağını belirlemek için "Türler"e tıklayın. Dosyalar, içeriklerine göre şüpheli olarak tanımlanabilir, bu daha derin ve yavaş olacaktır. Ya da uzantılarına göre tanımlanabilirler.

İçeriğine göre tarama yapılmasını seçerseniz, "Tüm dosyaları tara" seçeneğini işaretleyebilirsiniz. Bu seçeneği işaretlerseniz, genellikle virüs içermeyen dosyalar dahil, imaj (imge) dosyaları gibi, taranacaktır. İşaretlemezseniz, bu tür dosyalar taranmayacak, ve "atlanmış dosya(lar)" olarak raporlanacaktır.

Uzantısına göre taramayı seçerseniz, hangi uzantıların şüpheli olarak algılanması gerektiğini belirlemeniz gerekecektir. Aşağıdaki ekranı inceleyiniz.



Dosyaların bir ya da birden fazla uzantıya göre taranmasını istiyorsanız, "Araştır" butonuna tıklayın. Dosya uzantıları listesi ekranınıza gelecektir. Eklemek istediğiniz uzantıyı bulduğunuzda, bu uzantının önce üzerine daha sonra, listeye eklemek için "Tamam"a tıklayın. Herhangi bir uzantıyı listenizden kaldırmak için, önce üzerine daha sonra "Kaldır" butonuna tıklayınız.

"Belirli uzantıları tara" seçeneği işaretli ise, bütün bilinen "tehlikeli" virüsler otomatik olarak tarancaktır.

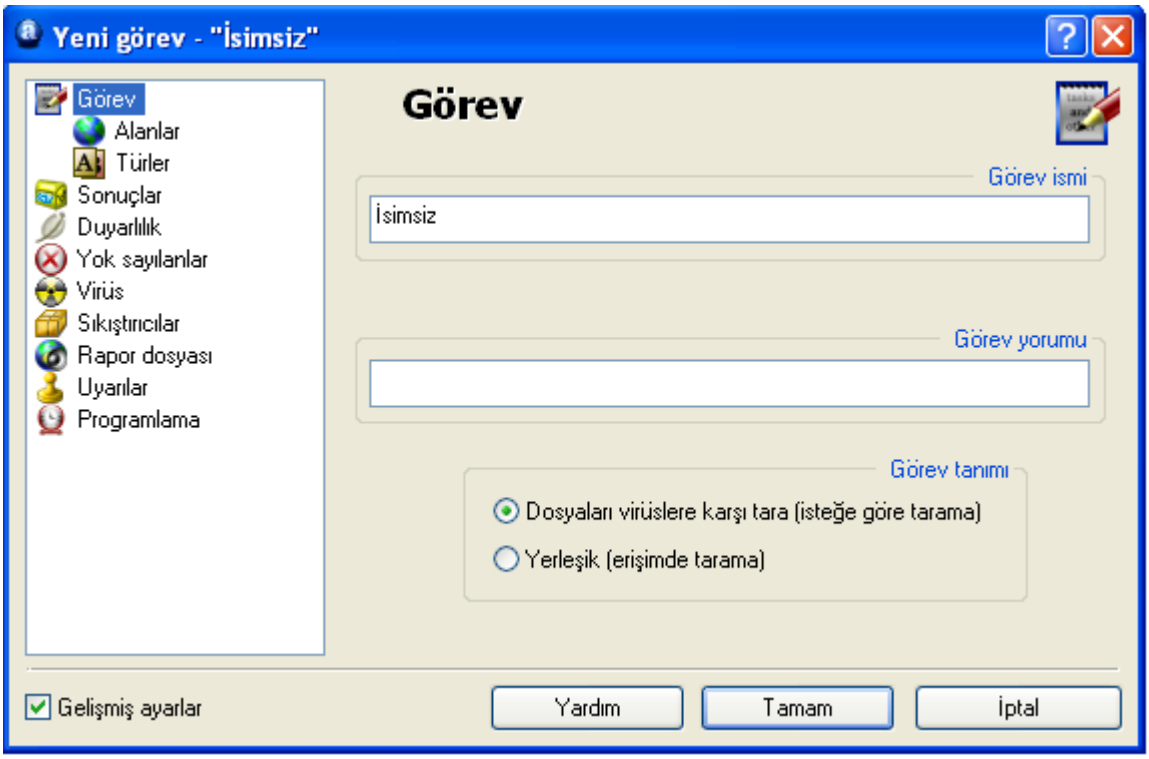
Belirlenen uzantıların dışında uzantıya sahip olan dosyalar taranmayacaktır ve "atlanan dosyalar" olarak rapor edilecektir.

- ***Sonuçlar***

"Sonuçlar" butonuna tıklayarak, taramadan sonra hangi sonuçların depolanacağını belirleyebilirisiniz. Normalde, virüs bulaşmış dosyaları, çok hatalı dosyaları, ve tarama bırakma ayarları nedeniyle test edilmeyen dosyaları depolamak yeterlidir. Fakat diğer sonuçları da ilgili kutucuğu işaretleyerek depolamanız mümkündür. "Hatasız dosyalar"ın depolanması önerilmemektedir. Çünkü, bu dosyalar çok fazla yer kaplayacaktır.

Tarama sonuçlarının depolanmasını istemiyorsanız, sonuçlar ekranın altındaki kutucukta olan işareti kaldırınız.

Ek seçeneklere, sol altta bulunan "Gelişmiş ayarlar"a tıklayarak ulaşabilirsiniz. Tıkladıktan sonra ek seçenekler aşağıdaki gibi ekrana eklenecektir.



- ***Duyarlılık***

Duyarlılık ekranınında bulunan "Bütün dosyaları test et (büyük dosyalarda çok yavaş olabilir)" tıklarsanız, bütün dosyalar, derinlemesine test edilmeye başlayacaktır. Virüslerin çoğu hem dosyaların başlangıcında hem de sonunda bulunabilmektedir. Bu nedenle bu kutucuğu tıklamanız, taramanın daha sağlıklı olmasını sağlayacak fakat aynı zamanda daha yavaş olmasına neden olacaktır.

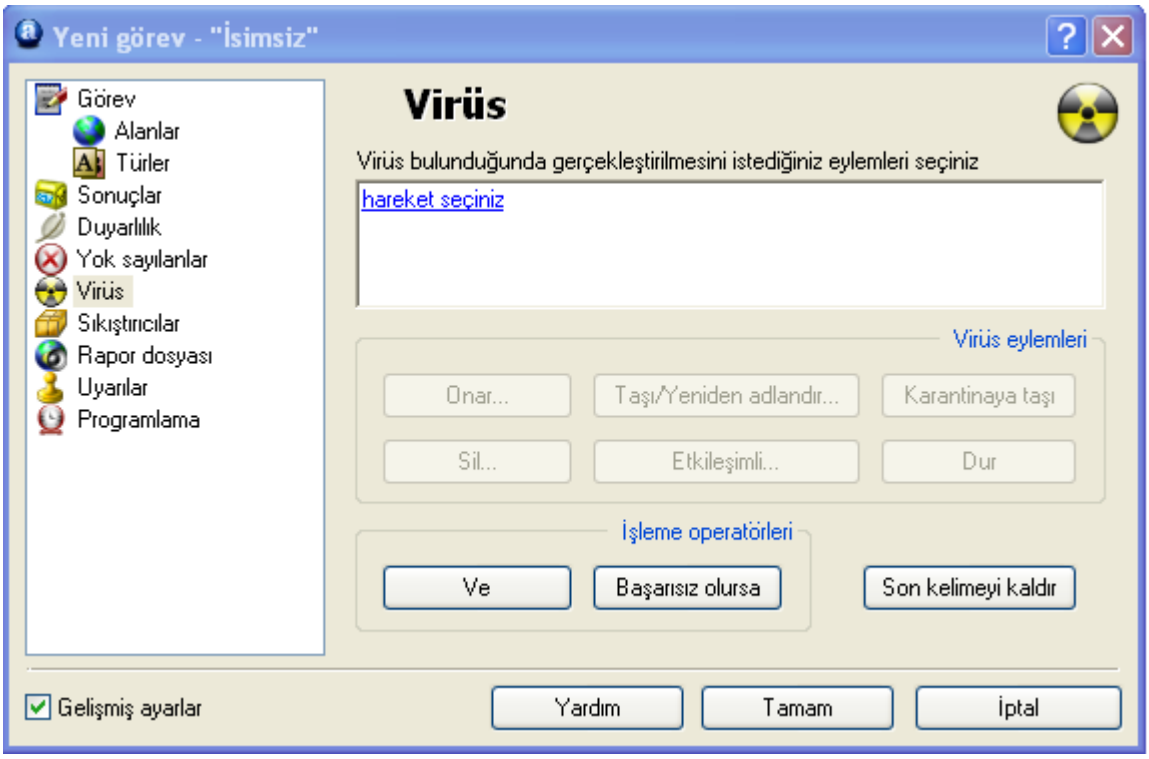
"Virüs hedeflemeyi yoksay" seçeneği ise dosyaların yalnızca virüs veri tabanında bulunan bütün virüslere göre test edilmesini sağlayacaktır. Bu kutucuğu işaretlemezseniz, dosyalar yalnızca verilen dosyanın türünü etkileyebilecek virüslere göre taranacaktır. Mesela, program ".com" uzantılı dosyanın içerisinde bulunan ".exe" uzantılı dosyalara zarar veren virüsleri test etmeyecektir.

- ***Yok sayılanlar***

  Burada bazı dosya ya da klasörleri yok sayabilir, yani tarama dışı bırakabilirsiniz. Bu özellik aynen Hariçler başlığı altında açıklandığı gibi çalışmaktadır. Farklı olarak, yok sayılanlar ayarları, yalnızca belirlenen görevler üzerine uygulanmaktadır. Ayarlar menüsünde, hariç tutulan dosya ya da kalasörler, otomatik olarak, bütün taramalarda yok sayılacaktır. Hariç tutulan dosyalar "atlanan dosyalar" şeklinde sonuç raporunda yer alacaktır.

- ***Virüs***

  "Virüs" butonuna tıkladığınızda aşağıdaki pencere ekranınıza gelecektir:



Bu pencerede virüs bulunduğunda nasıl bir yöntem izlenmesi gerektiğini belirleyebilirsiniz. Varsayılan yöntem "hareket seçiniz" dir. Bu seçenek sizi "etkileşimli eylem ayarları " penceresine götürecektir.

Bu pencereden istediğniz eylemi seçebilirsiniz. Seçtikten sonra, her virüs bulunduğunda seçtiğiniz eylem işleme konulacaktır.

"Hareket seçiniz" butonuna tıkladığınızda, açılan pencerede Sil, Tamir et, Karantinaya taşı, Taşı/yeniden adlandır, Dur düğmeleri yer almktadır. Bu seçeneklerde bulunan tik işaretlerinden birini kaldırırsanız, virüs bulunduğunda kaldırmış olduğunuz hamle, sunulmayacaktır. Bu hamleler "Herhangi bir virüs bulunduğunda yapmanız gerekenler" başlığı altında açıklanmıştır.

Bu özellik, virüs bulduğunda, siz hangi eylemin işleme konulacağını seçene kadar tarama duracaktır. Bu nedenle, görevi bilgisayarınızın başında olmadığınız bir zamana programlıyorsanız, bir yada birden fazla seçimde bulunmalısınız, virüs karantinasına taşı gibi.

Farklı bir eylem seçmek istiyorsanız, "Son kelimeyi kaldır" düğmesine tıklayın. Varsayılan eylem, bu noktada silinecek, altı eylem seçeneği pencerenin üzerinde sıralanacaktır. Herhangi birine tıkladığınızda, tıkladığınız eylem kutucuğa eklenecektir. Daha sonra bu seçtiğiniz eylem, her şüpheli dosya bulunduğunda uygulanacaktır. Bu uygulamayı iptal etmek için "son kelimeyi kaldır" düğmesine tekrar tıklayınız.

İlk dört eylem sayfa 29 den itibaren açıklanmıştır. "Etkileşimli" düğmesine tekrar tıklarsanız, "hareket seçin" seçeneği tekrar kutucuğa eklenecektir. " Dur" butonu ise herhangi bir şüpheli dosya bulunduğunda tarama durdurulacaktır.

"Ve" butonu ile birden fazla eylem belirleyebilirsiniz. Örneğin, herhangi bir virüslü dosyanın, tamir edilmesini ve başka bir alana taşınmasını, önce " Onar" daha sonra "Ve" ve son olarak "Taşı yeniden adlandır" butonlarını kullanarak gerçekleştirebilirsiniz.

Ayrıca, ilk eylemin başarısızlığı sonucunda alternatif olarak farklı bir eylem de ekleyebilirsiniz. Örneğin, ilk olarak "Onar" seçeneğini tercih edebilirsiniz, fakat onarılamayan dosyaların karantinaya taşınmasını garantilemek için önce "Başarısız olursa" ve ardından "Karantinaya taşı" butonuna tıklayınız. (bknz. 46)

Not: "Sil" butonuna tıkladığınızda iki seçenek sunulacaktır. Birincisi dosyanın tamamen mi silineceği ikincisi çöp kutusuna mı gönderileceğidir. Bu seçeneklerden birini seçmeniz gerekmektedir."Dosyaları tamamen sil" seçeneğini işaretlerseniz, bu noktadan sonra ayrıca dosyaların, o an silinememesi durumunda, bilgisayarın yeniden başlatıldığında silinebilmesini belirleyebilirsiniz. Bunun için "eğer gerekliyse, dosyayı birdahaki sistem açılışında sil" kutucuğunu işaretleyiniz.

- ***Sıkıştırıcılar***

Bu bölümde, görev sırasında, hangi arşiv dosyalarının taranıp taranmayacağını belirleyebilirsiniz. Varsayılan ayar, kendi kendini açabilen çalıştırılabilirlerdir. Taramayı yavaşlatacak olsa dahi, buna ekleme yapılabilir. "Bütün arşiv dosyaları"nı seçerseniz tarama sırasında, bütün arşiv dosyaları test edilecektir.

- ***Rapor dosyası***

Bu bölümde ise, tamamlanmış görev ile ilgili anahtar bilgiyi içeren, rapor dosyası oluşturabilirsiniz. Raporun içinde bulunan bilgi esasen, oturum sonucunda bulunan bilgiyle aynıdır.

Rapor dosyasının oluşturulması ile ilgili ayrıntılı bilgiye 38. Sayfadan itibaren ulaşabilirsiniz.

Not: Varsayılan ad task_name.rpt. Rapor dosyası modife edilip acılabilen basit metin dosyalarıdır.

- ***Uyarılar***

  Uyarılar, hem genel olarak hem de yalnızca görevde özellikle belirtilen bir virüs bulunduğunda alınabilir.

  Uyarılar "geçerli uyarılar" kutusuna görev olarak eklenebilir.

  Genel uyarılar "ayarlar" ve "uyarılar" butonları kullanılarak sayfa 42 de açıklandığı gibi oluşturulabilir. Yine de oluşturulan uyarılar bu yol ile göreve bağlanamayabilir.

  Ekelemek istediğiniz uyarı gösteriliyorsa, üzerine tıklayın ve koyultun. Daha sonra "→" butonun atıklayın. Bu hareket ile uyarı "Kullanılmış uyarılar" bölümüne taşınacaktır. Bunun anlamı ise uyarının göreve bağlanmış olduğudur.

  Eklemek istedğiniz uyarı gösterilmiyor ise, yeni bir uyarı oluşturmak için "Yeni" butonuna tıklayınız.

  Uyarıya isim de verebilirsiniz. Örneğin, görevle ilgili olan bir isim. Ayrıca, " yorum " kutusuna bilgi ekleyebilirsiniz. Bu durumda uyarı kesinlikle sayfa 42 da tanımlandığı gibi oluşturulmuş olacaktır.

  Yeni uyarı oluşturduğunuz zaman, "Tamam" butonuna tıklayın. Bu hareket uyarıyı otomatik olarak "Kullanılmış uyarılar" kutusuna taşıyacaktır.

  Uyarıyı "kullanılmış ayarlardan" kaldırmak için, üzerine tıklayıp koyultun ve "←" butonuna tıklayın. Böylece uyarı tekrar "Geçerli uyarı" kutusuna taşınmış olacaktır.

  Uyarıyı değiştirmek için "Düzenle" butonuna, silmek için "Sil" butonuna tıklayınız.

  SMTP uyarısı oluşturmak istiyorsanız, görevi oluşturduktan sonra, "Ayarlar" ve "SMTP" butonlarını kullanarak, SMTP detaylarını da eklemeyi unutmayınız.

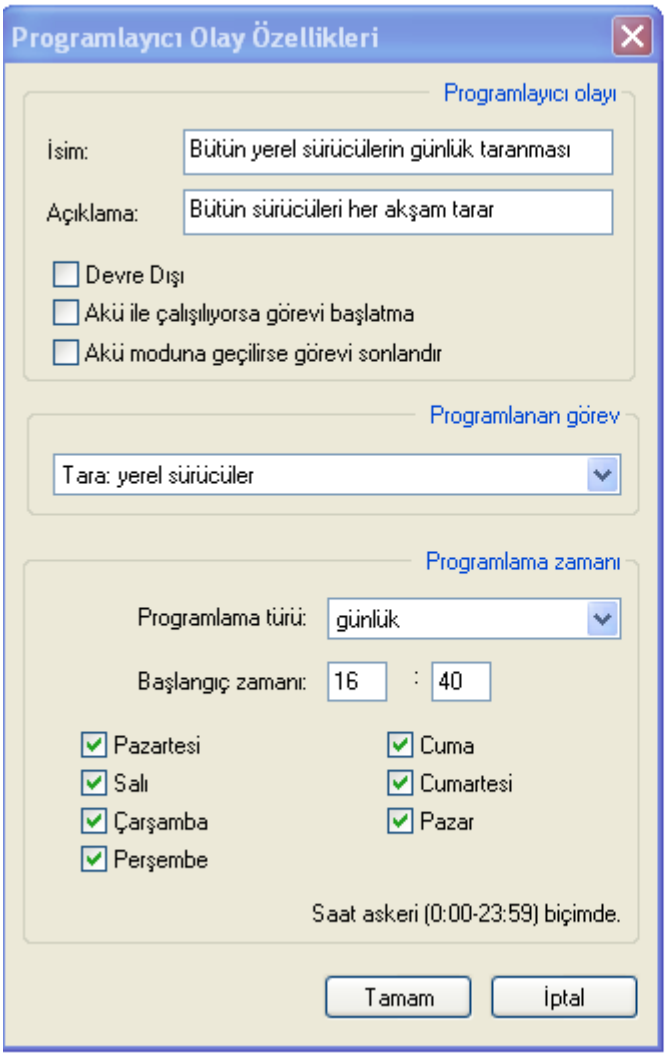
  Göreve bağlı olan uyarılar, yalnızca görev tarafından belirlenen bir virs bulunduğunda verilecektir. Virüs başka bir görev tarafından bulunduysa, program uyarı vermeyecektir. Herhangi bir görev tarafından , her virüs bulunduğunda uyarı almak istiyorsanız sayfa 42 teki gibi, genel bir uyarı oluşturmanız gerekmektedir.

  Bu yolla oluşturulan uyarılar, klasörler listesindeki "Uyarılar"a tıklanarak görülebilir. Burada , yine gelecek görevlerde kullanılmak üzere yeni uyarılar oluşturabilirsiniz. Bunun için, ekranın üzerinde bulunan " Uyarılar"a tıklayınız ya da Uyarılar klasörüne sağ tıklayın ve "Yeni uyarıyı" seçin.

  Bir önce oluşturulmuş olan uyarıyı değiştirmek için, ekranın üzerindeki "Uyarılar"listesine tıklayın ve "Düzenle" seçeneğini seçin, silmek için ise "Kaldır" butonuna tıklayın.

Programlama

Görev oluştururken, görevi istediğiniz zaman ve tarihte otomatik olarak başlamaya programlayabilirsiniz. Ya da belirli zaman dilimlerinde, örneğin günlük, haftalık, aylık olarak programlayabilirsiniz.
"Programlama" penceresinde, "Ekle" butonuna tıklayın. "Programlayıcı olay özellikleri" başlığı altında, yeni bir pencere açılacaktır. Programlanmış olay için bir isim girin, örneğin "Bütün yerel sürücülerin günlük taranması" gibi. Açıklama kutusuna herhangi bir açıklayıcı mesaj (Bütün yerel sürücüleri her akşam tarar gibi)
girebilirsiniz.



Taramanın henüz aktif hale gelmesini istemiyorsanız yada tamamen silmeksizin iptal etmek istiyorsanız "Devre dışı" kutucuğunu işaretleyiniz.

Bu kutucuğun aşağısında ek olarak iki seçenek daha bulunmaktadır."Akü ile çalışıyorsa görevi başlatma" seçeneği notbook kullanan kullanıcılar için son derece yararlı bir özelliktir. Bu kutucuğu işaretleyecek olursanız, programlanmış olay , bilgisayar pil ile çalışıyorsa başlatılmayacaktır.

"Akü moduna geçilirse sonlandır" seçeneği ise, bilgisayar elektirkle çalışmayı sonlandırıp pille çalışmaya başladığı anda programlanmış olayın sonlandırılmasını istiyorsanız kullanabilirsiniz. Yine bu özellik notebook kullanıcıları için son derece faydalı bir özelliktir.

"Programlanan görev" altındaki listeden görevin adını seçin. Son olarak, "Programlama türü" metin kutusunda, görevin ne zaman ve ne kadar sıklıkla gerçekleştirilmesi gerektiğini belirleyebilirsiniz. Bir kere, günlük, haftalık, ya da aylık olarak parogramlayabilirsiniz. Bir kere seçeneğini işaretlerseniz, zaman ve tarih belirtmeniz gerekmektedir. Günlük seçeneğini işaretlerseniz, görevin hangi gün ve zaman diliminde gerçekleştirilmesi gerektiğini belirlemeniz mümkündür. Haftalık ya da aylık seçeneğini seçerseniz, zamana ek olarak tarih belirlemeniz gerekecektir.

Programlanan olayı daha sonradan incelemek için, programlanan olaylar penceresinde, olayın üzerine sağ tıklayın ve "Özellikler"i seçin. Olayı kaldırmak için "Sil" butonuna tıklayın.

"Erişimde" görev oluşturma

Yerleşik koruma görevi çalışıyor olduğu sürece, bilgisayarınızdaki bütün aktiviteleri izliyor olacaktır. Yerleşik korumada herhangi bir değişiklik yapmanız gerekiyorsa, varsayılan görevi duraklatmanız önerilmektedir. Daha sonra yeni bir görev oluşturup yürütmelisiniz. Varsayılan görevi değiştirirseniz, varsayılan ayarları kaybetmeniz sözkonusudur. Görevi duraklatmanız için, üzerine sağ tıklayın ve "Duraklat" seçin. Yerleşik koruma görevini durdurmak yada herhangi bir değişiklik yapmak burada "durdurmak" ya da yerleşik koruma bölümünde anlatıldığı gibidir.
Herhangi bir yerkeşik koruma görevi çalıştırmak diğer yerleşik koruma görevlerinin durmasına neden olacaktır. Yerleşik koruma aktif hale gelir gelmez, ekranın sağ alt köşesindeki mavi "balon" ikonu tarafından gösterilecektir. Hiç bir yerleşik koruma görevi aktif değilse, "balon" ikonu üzerinde kırmızı bir işaret olacaktır.

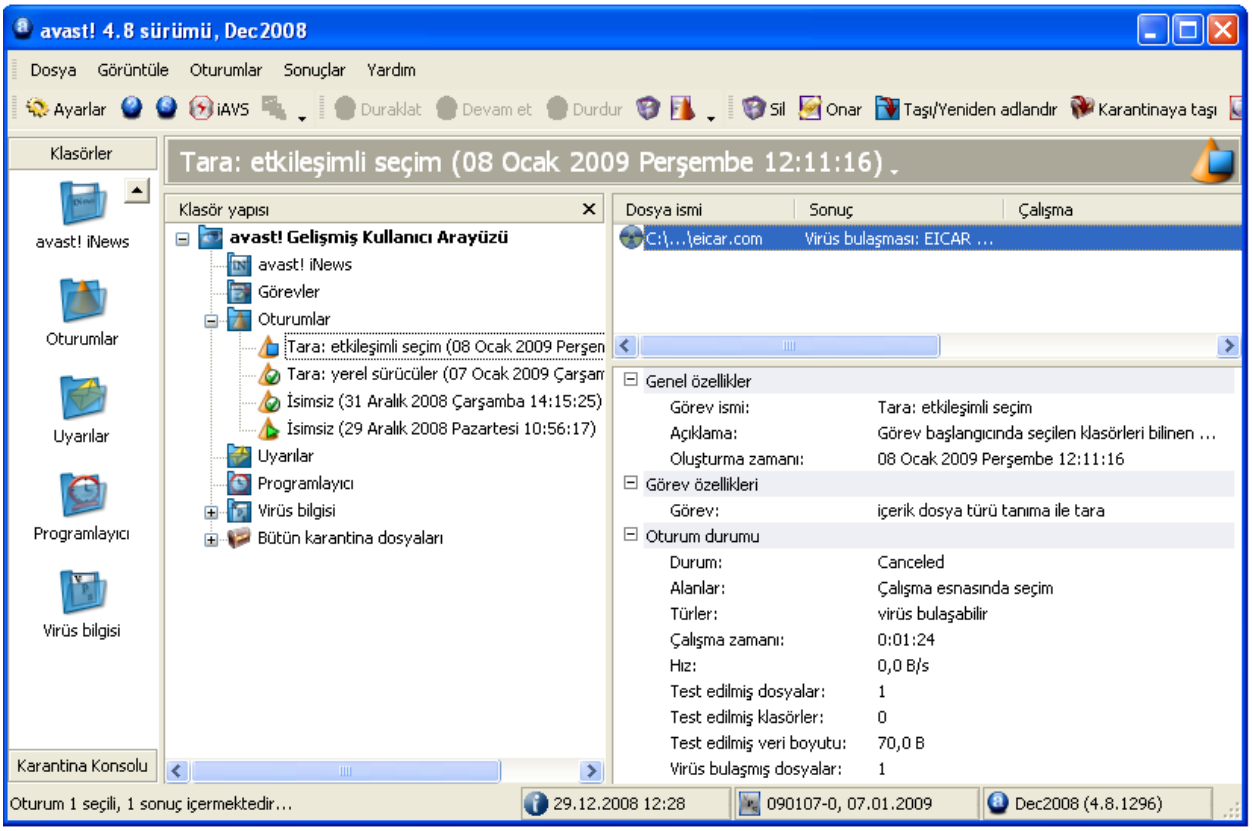
Yeni bir yerleşik koruma görevi oluşturmak için, önce ekranın üzerindeki "Yeni" butonuna daha sonra, ekranın altındaki "Yerleşik" üzerine tıklayın. (bknz. 55)Yerleşik koruma modüllerini gösteren yeni bir pencere açılacaktır. Daha sonra "Sağlayıcılar" seçeneğine tıklayın. İştenmeyen koruma modüllerindeki tik işaretini kaldırın. Aşağıdaki tabloyu inceleyebilirsiniz. Ayrıca soldaki sağlayıcıların üzerine tıklayarak duyarlılığını da "Normal olarak " ya da "Yüksek olarak" ayarlayabilirsiniz.

"Gelişmiş ayarlar"a tıklarsanız, soldaki modüllere ait liste, her sağlayıcı için gereken ek özelliklerle beraber genişleyecektir. Bu seçenekler, yalnızca belirli türde dosyaları taramak, virüslü dosya tespit edildiğinde ne tür bir yol izleneceğini belirlemek içindir (bknz. 70)Yerleşik koruma ayarları önceki bölümlerde anlatılan Rapor ve Uyarı oluşturma seçenekleri gibidir.

Oturumlar : "İsteğe bağlı" görev başlatma

Herhangi bir görevin üzerine tıkladığınızda, pencerenin altında göreve ait açıklayıcı bilgilere ulaşabilirsiniz. Göreve çift ya da sağ tıklayıp "Çalıştır"ı seçerseniz görev başlatılacaktır.
Herhangi bir görev başladığı anda, yeni bir oturum oluşturulur ve sonuçlar "Oturumlar" klasöründe depolanır. Her bir oturumu görmek için, Görüntüle'den Program klasörlerine tıklayın. Ve daha sonra klasör yapısı listesindeki "Oturumlar"ın solundaki "+" işaretine tıklayınız. Her bir görev için bir oturum bulunmaktadır. Oturumlardan birine tıkladığınızda sağ tarafta açıklayıcı bilgilere ulaşabilirsiniz. Tarama esnasında herhangi bir virüs bulunursa pencerenin üst kısmında gösterilecektir. Diğer açıklayıcı bilgiler ise pencerenin alt kısmında yer alacaktır.

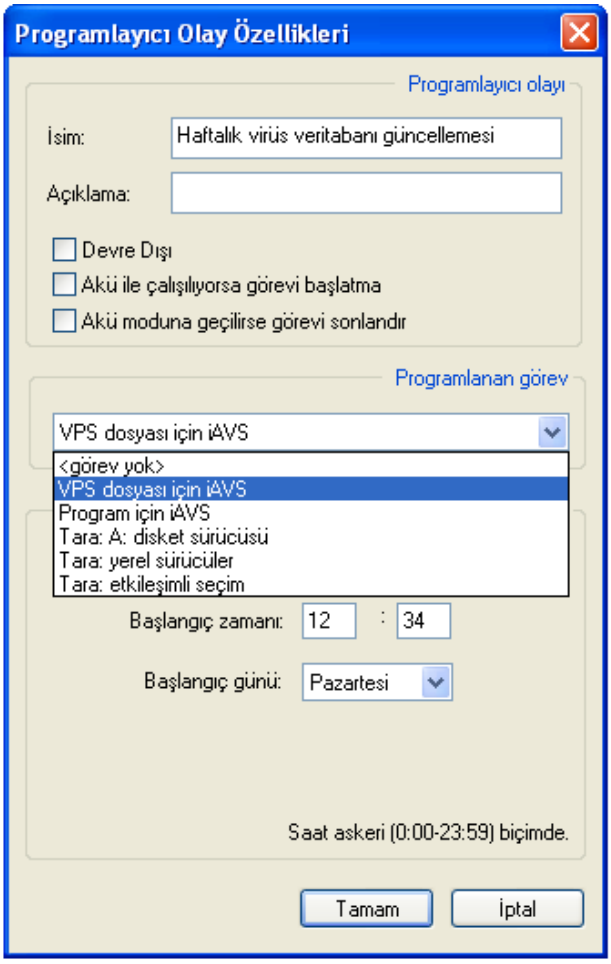
"Çalışma" kısmında ne tür bir yol izlendiği ve izlenen yolun başarılı olup olmadığı yer almaktadır. Eğer "Etkileşimli" seçenek seçilmiş ise, vürüs bulunduğu uyarısı yer alacak ve ne tür bir yol izlemek istediğiniz sorulacaktır. (bknz. 29) Hemen istediğiniz yolu takip edebilirsiniz ya da daha sonraya bırakabilirsiniz. Virüslü dosyanın üzerine tıkladığınızda mümkün olan seçenekler ekranın üzerinde yer alacaktır. İzlediğiniz yol her zaman "Çalışma" kısmında yer alacaktır.



Görevi ayarlarken herhangi bir rapor oluşturuldu ise, raporu görmek için ekranın sağ üst köşesindeki "Oturumlar"a tıklayın ve "Rapor Göster"e tıklayın.

Varolan görevleri ve güncellemeleri programlama

Gelişmiş arayüzdeki programlayıcı, oluşturulan herhangi bir görevi programlamak için kullanılabilir. Bu özellik ayrıca programın ve veritabanı güncellemesinin programlanması için de kullanılabilir. Herhangi bir görev programlamak istiyorsanız (örneğin virüs veri tabanı güncellemesi gibi) öncelikle "Programlayıcı" dosyasına tıklayınız. Daha sonra ekranın üzerinde bulunan "Yeni" tuşuna , ya da yine ekranın üzerinde bulunan "Programlayıcı" seçeneğinin altındaki "Olay oluştur" seçeneğini seçin. Açılacak olan pencerede oluşturulan olay için isim ve gerekli ise açıklama giriniz. Diğer üç kutucuk "İsteğe bağlı görev oluşturma" bölümünde programlama başlığı altında açıklanmıştır. Programlamak istediğiniz görevi "programlanan görev" listesinden seçiniz.



Son olarak, zamanı ayarlayın ve "Tamam" a tıklayın.

Bu noktadan sonra görev programlanmış olacaktır. Klasörler listesinden "Programlayıcı" seçeneğine gittiğinizde, programlanmış bir görev olarak görünecektir. Programlanmış görev başlar başlamaz, yeni bir oturum oluşturulmuş olacak. Daha sonra istediğiniz zaman, "Oturumlar" klasöründen ilgili oturuma tıkladığınızda sonuçlara ulaşabilirsiniz.

Programlanan olayı düzenlemek için, üzerine sağ tıklayın ve "Özellikler"i seçin. Silmek için "Kaldır" seçeneğine tıklayın.

Bilgisayarınızı taramaya programladığınızda, görevi oluştururken "Etkileşimli" seçeneği seçmiş olduğunuzdan emin olunuz. Böylece virüs bulunduğu zaman program, ne tür bir hamale yapacağınıza karar verene kadar, duraklayacaktır (bknz. 56) Bu durumda, virüs bulunduğunda başka bir yolun izlenmesi için (dosyanın virüs karantinasına taşınması gibi) yeni bir görev oluşturmanız ve programlamanız tavsiye edilebilir.

Not: Virüs veritabanı yada programın kendisini istediğiniz zaman güncelleyebilirsiniz. Virüs veritabanını güncellemek için "Dosya" ya da "iAVS güncelleme" ye tıklayınız. Programın güncellenmesi için ise "Program güncelleme" seçeneğini kullanınız. Virüs veritabanı ayrıca ekranın üzerindeki "iAVS" butonuna tıklayarak da güncelleyebilirsiniz.

Açılış anı taramasını programlama

Açılış anı taramayı programlamak için, ilk olarak "Programlayıcı" klasörüne tıklayınız. Daha sonra ekranın üzerinde bulunan "Programlayıcı" butonunun altından "Açılış anı taraması programla" seçeneğine tıklayınız. Ya da, yine ekranın üzerindeki ikonlar arasında yer alan, üzerinde kalem olan küçük yeşil üçgenli ikona tıklayınız. 35. sayfada açıklandığı gibi yeni bir pencere açılacaktır.

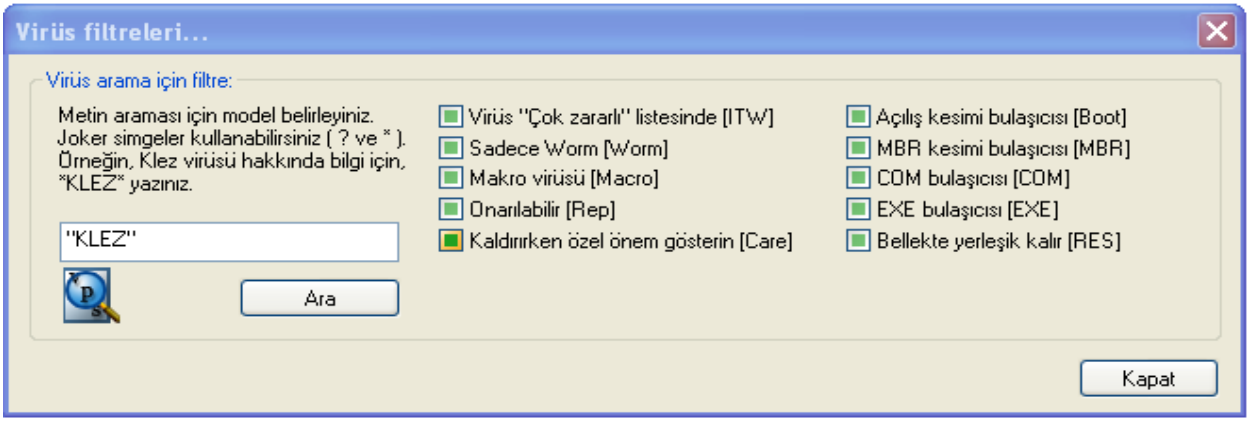
Virüs karantinası

Virüs karantinsında bulunan bütün dosyaları görmek için, klasör listesinde bulunan "Bütün karantina dosyaları" butonuna tıklayınız. Sol alt köşede bulunan "Karantina konsolu" ve ardından dört ikondan birine tıkladığınız takdirde, ayrı ayrı virüslü dosyaları, sistem dosyalarını, ya da kullanıcı dosyalarını görebilirsiniz. Ayrıca "Bütün karantina dosyaları" klasörünün yanında bulunan "+" işaretine tıklayarak bu dosyaları görmeniz mümkündür.
Belirlenen dosyaya yönelik herhangi bir hamlede bulunmak için, üzerine tıklayın. Ekranın üzerindeki gri ikonların rengi değişecektir. Bu ikonlarla istediğiniz hamleyi gerçekleştirebilirsiniz (sy. 47). Alternatif olarak, ekranın üzerindeki "Karantina konsoluna" tıklayarak ya da dosyanın üzerine sağ tıklayarak da mümkün olan hamlelerin listesine ulaşabilirsiniz.
"Bütün dosyaları yenile" ve "Ekle" seçeneklerini kullanmak için, dosyalara ait listenin bulunduğu pencereye tıklamayı unutmaynız.

Virüs veritabanında arama yapmak

Virüs veritabanına, Gelişmiş Arayüzden "virüs bilgisine" tıklanarak ulaşılabilir.
Listelenen her bir virüsün özelliği onaylıdır. Bu özellikler sayfa 44' da açıklanmıştır.

Belirli bir virüsü araştırmak için, ekranın üzerindeki "Virüs bilgisi" üzerine tıklayın ve "Filitrele" butonuna basın. Aşağıdaki ekran karşınıza çıkacaktır.



Listedeki virüsler, bir çok parametreler ile aranabilir. Virüsün adını biliyorsanız, yalnızca virüsün adını kutucuğa girin ve “Ara” butonuna tıklayın. Virüsün adını tam bilmiyor, yalnızca bir kısmını biliyorsanız, bilmediğiniz karekter için “?” işaretini giriniz. Bilmediğiniz karekter sayısı birden fazla ise “*” işaretini kullanınız.

Örneğin “Klez” virüsünü aradığınızı varsayalım. Bu virüsün asıl adı Win32:Klez-H [Wrm] . Bu durumda ismi *klez* şeklinde girmeniz grekmektedir. Böylece “Klez” sözcüğünü içeren bütün virüsler bulunacaktır.

Aramayı hızlandırmak için, aradığınız virüsün özelliklerine göre, ekranda görülen kutucukları kullanabilirsiniz. Belirli bir özelliğe göre ararama yapmak için, özelliklere ait kutucukları iki kez tıklayınız. Bir kere tıklarsanız, kutucuğun rengi griye dönüşecektir. Gri olması, virüsün bu özelliğe sahip olmadığı anlamına gelmektedir. Kutucuklar işaretlenmez ve yeşil olarak bırakılırsa, bu, aradığınız virüsün o özelliğe sahip olup olmamasının farketmemesi anlamına gelmektedir.

Günlük görüntüleyicisi

Günlük görüntüleyicisinin özellikleri ve belirli raporların nasıl araştırılacağı sayfa 48 da açıklanmıştır. Günlük görüntüleyicisine ulaşmak için, önce “Görüntüle” daha sonra “Günlük dosyalarını göster” seçeneğine tıklayınız.

Virüs temizleyicisi

Avast! virüs temizleyicisi, sisteminizdeki bütün virüsleri temizlemek için dizayn edilmiştir. Tamir edilmesi mümkün olan dosyaları tamir eder, virüsleri siler. Böylece sisteminizi yeniden kurmak ya da yedeklerinizden geriye döndürmek zorunda kalmazsınız. Ayrıca virüs ögelerini sistem kaydından kaldırır, yapısı bozuk olan dosyaları temizler, virüs tarafından oluşturulmuş olan geçici dosyaları siler (bazı dosyalar virüs kodu içermeyebilir. Bu nedenle şüpheli dosya olarak algılanmazlar fakat hard diskinizde yer kaplamaktadır).

Virüs Temizleyicisi direk olarak programın içine yerleştirilmiştir. Virüs Temizleyicisi tarafından tamemen kaldırılabilmesi mümkün olan herhangi bir virüs bulunduğunda, virüs uyarı ekranında, ek olarak "Virüsü sistemden tamamen kaldır" butonu yer alacaktır. Virüs bulunduğunda böyle bir ek buton sunuluyorsa, bu seçeneği kullanmanızı tavsiye ediyoruz.

Virüs Temizleyicisi gelişmiş arayüzden direkt olarak ulaşılabilir. Bunun için önce "Dosya" ardından "avast! virüs temizleyiciyi çalıştır" seçeneğine tıklayınız. Başladığı zaman sırasıyla aşağıdaki işlemleri gerçekleştirecektir.

- İşletim siteminin hafızası taranacak ve bilinen herhangi bir virüs bulunduğunda virüsün yayılmasını önlemek için işlem duraklayacaktır. Duraklatmak imkansız ise, yine virüsün yayılmasını önlemek için, virüs hafızada etkisiz hale getirilecektir.
- Yerel sabit diskiniz taranacak.
- Sistem kaydı, Başlangıç klasörleri vs. gibi başlangıç ögeleri taranacak.
- Hafızada ya da diskte bulunan virüslü dosyalar kaldırılacak ya da tamir edilecektir (gerektiğinde)
- Ek olarak, algılanmış virüs tarafından bulunan çalışan/geçici dosyalar kaldırılacaktır.

Virüs temizleme işleminin tamamlanması için bilgisayarınızın yeniden başlatılması gerekiyor ise (*örneğin, dosyanın o anda kullanımda olduğundan kaldırılamaması ya da aktif olmayan virüs temizleme işleminin hala hafızada bulunuyor olması nedeniyle*), bilgisayarınızı derhal yeniden başlatıp başlatmak istemediğiniz sorulacaktır.

Virüs temizleyicisi çalışıyor durumda iken, lütfen başka bir uygulama başlatmayınız. Çünkü bazı virüsler ya da solucanlar başka bir uygulama başlatıldığında otomatik olarak başlayacaktır. Aktif virüs işlemi yalnızca, başka bir uygulama başlattığınızdan ötürü (Notepad, Explorer, vs.) bir virüs bulunursa duraklayacak ya da sonlandırılacaktır ve muhtemelen bilgisayarınızdan kaldırılamayacaktır!

Virüs temizleyicisi Windows NT/2000/XP/2003/Vista/2008 işletim sistemlerinde, Virüs temizleyicisinin tam olarak çalışabilmesi için, bazı yetkili kullanıcı ayrıcalıkları gerekmektedir. Yoksa bazı virüsler bulunamayabilir ve/veya tam olarak kaldırılamayabilir.

Sessiz yükleme

Bu özellik, daha çok ağ yöneticileri için kullanışlıdır. Bu özellik sayesinde, birden çok bilgisayara avast! programını yüklemek (istemcilere tek tek yüklemeye gerek kalmaksızın) mümkün ve de çok kolaydır. Program önceden tanımlanmış ayarlar ve görevler sayesinde yüklenebilir.
Sessiz yükleme oluşturmak için:

- Öncelikle programı bir bilgisayara yükleyiniz.
- Ayarları diğer bilgisayarda olmasını istediğiniz şekilde düzenleyiniz.
- Görevlere ait istenen parametreleri ayarlayınız.
- Gerekli ise, yerleşik koruma ayarlarına ulaşabilmek için parola oluşturunuz.
- Gelişmiş arayüzünde, önce "Dosya" butonuna ardından "Sessiz yükleme oluştur" seçeneğine tıklayın.

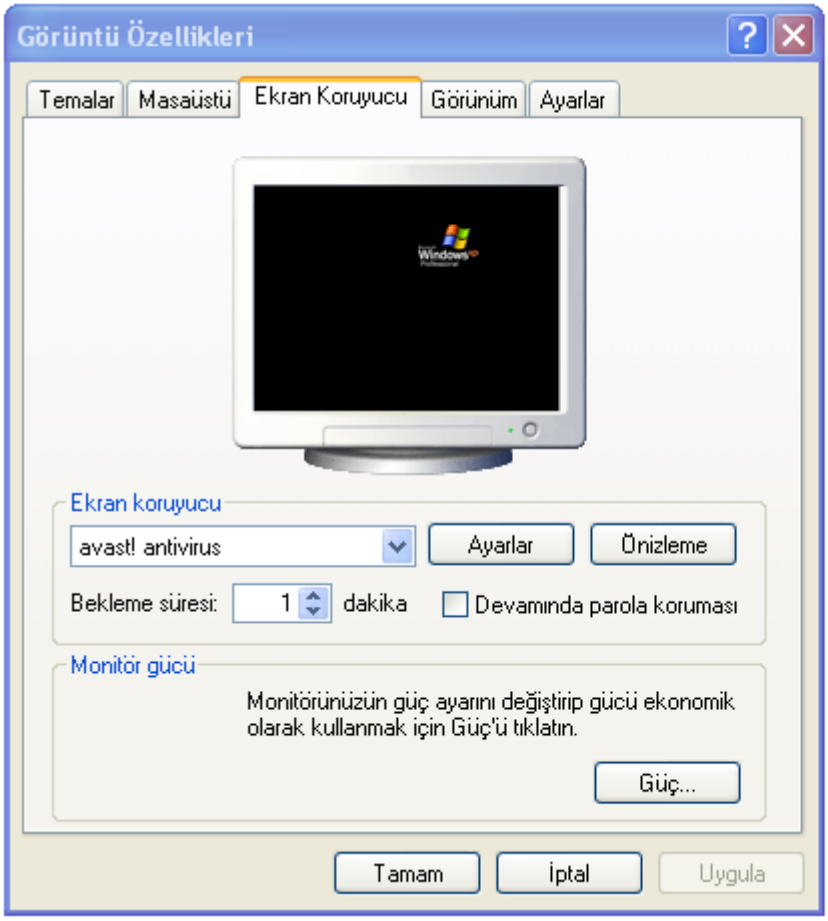
Daha sonra, sessiz yüklemenin parametrelerini oluşturun.

- Sessiz kip: Hedef bilgisayarlara yükleme yapılırken, yalnızca hata kodları kullanıcıya bildirilir.
- En sessiz kip: Hedef bilgisayarlara yükleme yapılırken, hiçbir hata mesajı kullanıcıya bildrilmez.
- Yükleme yolu: Programın yükleneceği klasörü giriniz. Varsayılan klasör Program files\Alwil Software\Avast4
- Yeniden başlatmak yok: Bilgisayarın, yükleme işlemi tamamlandıktan sonra yeniden başlatılması gerekmektedir. Bu seçeneği işaretlerseniz, yeniden başlatma işlemi istenmeyecektir.
- Yeniden başlatmak için sor: Yükleme işlemi tamamlandıktan sonra, kullanıcıya yeniden başlatılması için sorulacaktır.
- "Yeniden başlatmak yok" ya da "Yeniden başlatmak için sor" seçeneklerinden hiç birini işaretlemezseniz, yükleme işlemi tamamlandıktan sonra, sistem otomatik olarak yeniden başlatılacaktır.
- Oluştur butonuna tıklayın.

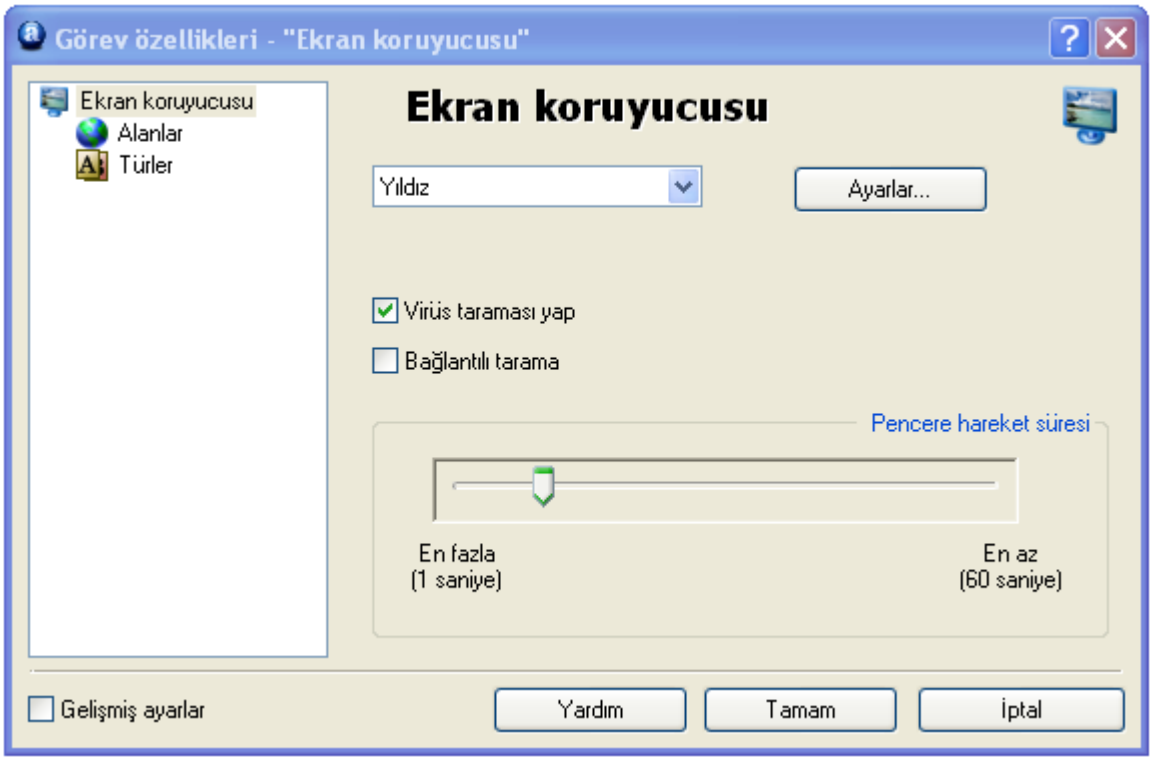
Son olarak, kolay yüklemenin saklanacağı paylaşılan bir klasör seçiniz. Admin.ini ve tasks.xml dosyaları seçtiğiniz dosyada saklanacaktır. Admin.ini dosyası avast! programının ayarlarını içermektedir. Task.xml ise görevlerin ayarlarını içerir. Yerleşik koruma ayarları için şifre oluşturduysanız, hedef klasörün içerisinde aswResp.dat adında üçüncü bir dosya olacaktır. Bu dosyanın içerisinde şifre bulunmaktadır. Avast kurma dosyası, ayrıca, bu klasöre kopyalanacaktır.

avast! antivirüs ekran koruyucusunun aktif hale getirilmesi

Avast! antivirüs, bilgisayarınızı kullanmadığınız zamanlarda, ekran koruyucunuz aktif iken, potensiyel virüsleri bulma yeteneğine sahiptir. Bu esnada, ekran koruyucusunun içinde taramanın gelişimi ile bilgi veren küçük bir kutucuk açılacaktır.
Avast! ekran koruyucuyu açmak için, bilgisayar ekranınızın sol köşesinde bulunan "Başlat" butonuna tıklayın ve "Ayarlar"ı seçin. Daha sonra "Kontrol Paneli/Denetim masası"ne tıklayın. Kutucuklardan "Görüntü"yü seçin ve açılan pencerede "Ekran koruyucusu"na tıklayın ve mavi okla mümkün olan ekran koruyucularına gözatın. Avast! antivirüs'ü seçin. Aşağıdaki kutuda gözüktüğü gibi, zamanı ayarlayabilir ve istiyorsanız, devam etmek için şifre kullanılmasını ayarlayabilirsiniz.



Pencerenin ortasında bulunan "Ayarlar"tıklayıp, avast!ın birlikte çalışacağı, tarama sonuçlarının üzerinde gösterileceği başka bir ekran koruyucusu seçebilirsiniz. Aşağıdaki pencereyi inceleyiniz.



Bilgisayarınızın, ekran koruyucunuzun her aktif oluşunda taranmasını istiyorsanız, yukarıdaki ekranda görünen "Virüs taraması yap" kutucuğunu işaretleyiniz. Bu kutucuğu işaretlemezseniz ekran koruyucu normal bir ekran koruyucusu vazifesi görecektir.
"Bağlantılı tarama" seçeneği, belirlenen alanlar tarandığında, tarama işleminin tekrardan başlatılması içindir.

Pencere hareket süresi ibresini tarama işlemi kutucuğu pozisyonunun ne kadar sıklıkta değişeceğini etkilemektedir.

Tekrar ayarlara tıklarsanız yalnızca normal ekran koruyucusunu aktif hale getirebilirsiniz.

Sayfa 55 te anlatıldığı gibi hangi alanların ve hangi dosyaların taranacağını ayarlamak için "Alanlar" ve "Türler" butonlarını kullanabilirsiniz.

"Gelişmiş ayarlar" kutucuğunu işaretlerseniz İsteğe bağlı görev oluşturma başlığı altında açıklandığı gibi daha bir çok ek ayarlama yapabilirsiniz.

Yerleşik koruma ayarları

1. **Anlık mesajlaşma**

   Programlar

   Burada hangi anlık mesajlaşma programlarının taranacağını belirleyebilirsiniz.Windows 95/98/ME kullanıyorsanız ve Trillian programını korumak istiyorsanız,yapılandırma dosyasına yol yani talk.ini girmeniz gerekmektedir (Gözat butonunu kullanabilirsiniz). Bazı programlar yalnızca Windows NT, 2000, XP,2003, Vista ya da 2008 kullanıyorsanız korunabilir.

   Sıkıştırıcılar

   Bu sayfa yalnızca yerleşik koruma görevleri ayarlarına Gelişmiş Arayüzden giderseniz ulaşabilirsiniz**.** (sayfa 57)

   Virüs

   Bu sayfada virüslü dosyalara karşı ne tür bir hareket izleneceği belirlenebilir. Bu sayfaya yalnızca Gelişmiş arayüzden yerleşik koruma görevleri ayarlarından ulaşılabilir (sayfa 56)

2. **İnternet Mail**

   "POP", "SMTP", "IMAP" ve "NNTP" sayfalarında, gelen ve/veya giden eposta ve haberlerin taranıp taranmayacağını belirleyebilirsiniz. Virüs bulunursa, epostaya uyarı mesajı eklenecektir. Ayrıca virüssüz olduğu teyid edilmiş epostalara, virüssüzdür şeklinde not ekleyebilirsiniz.

   Yönlendir

   Bu sayfada şeffaf eposta tarama ayarlaması yapabilirsiniz. Belirli bir porttan gelen Herhangi belirli bir porttan gelen epoatalar taranacaktır. Bu özellik yalnızca NT tabanlı işletim sistemleri için geçerlidir. (Windows NT/2000/XP/2003/Vista/2008).

   - Yönlendirilmiş portlar

     Varsayılan portlar dört temel e-posta protokolleri için olan standart port numaralarıdır. Farklı bir port kullanıyorsanız bu portun ya da portalların buraya girilmesi gerekmektedir. Birden fazla port girmeniz gerekiyorsa virgül ile ayırınız.

- Yoksayılan adresler

  Burada, taranmasını istemediğiniz, yani hariç tutmak istediğiniz posta sunucularının ya da belirli portların adreslerini girebilirsiniz. Bu özelliği avast!ın yalnızca belirli bir hesaptan gelen ya da giden mesajları taramasını istiyorsanız kullanabilirsiniz. Örneğin, smtp.server.com adresini girerseniz avast! giden (SMTP) hesaba ilişkin mesajları taramayacaktır.

- Yerel haberleşmeyi yoksay

  Bu seçeneğin normalde işaretlenmiş olması lazım. İşaretli değilse avast! yerel haberleşmeyi dahil tarayacaktır. Bunun güvenlik açısından daha güvenli olduğu açıktır fakat bilgisayarınızı yavaşlatabilir. Kesinikle eposta için kullandığınız port numarası dışında numara girmeyiniz. Yoksa, beklenmeyen bir sorun ortaya çıkabilir.

Gelişmiş

- Gerçekleştirilen hareket hakkında detaylı bilgi ver.

  Bu kutucuğu işaretlerseniz, o anda taranan dosyalar hakkında bilgi ekranın sağ köşesinde gösterilecektir.

- Sessiz mod.

  Virüs sayfasında belirlenmiş olan hamle, örneğin, etkileşimli seçimse ve sessiz modu işaretlerseniz, virüslü dosyalarla otomatik olarak aşağıdaki kurallara göre çalışılacaktır.

  - "Genel cevaplarla Evet (Tamam)" seçili ise, bu durumda epostaya eklenmiş herhangi bir virüslü dosya otomatik olarak silinecektir.
  - İkinci seçenek olan "genel cevaplarla hayır (Hayır)" seçili ise, virüslü dosyalar karantinaya taşınacaktır.

Virüs sayfasında varsayılan hareketi seçtiniz ise ve sessiz mod kutucuğunu işaretlemedi iseniz, normal virüs uyarı ekranı virüs ile ne yapmak istediğinizi soracaktır.

Varsayılan hareketten farklı bir hareket seçtiyseniz, bu kutucuğu işaretlemeniz herhangi bir etki yaratmayacaktır.

Ancak varsayılandan farklı olan hareket aynı zamanda Satandart kalkan için de belirlenmiş seçilmişse, bu belirlenmiş olan hareketi İnternet Posta sağlayıcısı için iptal edecektir.

Keşifsel

avast! yalnızca gelen epostaları taramakla kalmaz, ayrıca mesajları keşifsel analiz yöntemi ile kontrol eder ve hatta veritabanında bulunmayan potansiyel virüsleri ortaya çıkarır.

- Duyarlılık – Düşük
  - Temel dosya eki denetimi.

    Ekler isimlerine göre gerçekleştirilir, örneğin, dosyanın iki uzantısı varsa mesela "Patch.jpg.exe" gibi, potansiyel tehlike olarak algılanmaktadır. Avast! ayrıca dosyanın adının dosyanın gerçekten türü ile ilgili olup olmadığını da kontrol eder. Örneğin, "Pamela.jpg" resim dosyası olarak tahmin edebilirsiniz. Fakat yeniden adlandırılmış "COM" dosyası da olabilir.

  - Görünmez karakter dizi denetimi

    Bazı virüsler dosya uzantısının sonuna bir çok boşluk (ya da çalışmayan beyaz karekter) ekler. Ardından tehlikeli olangerçek uzantıyı eklerler. Dosyanın uzantısından dolayı, kullanıcı ikinci uzantıyı görmeyebilir, fakat keşifsel analiz bu hileyi açığa çıkarabilmektedir. Varsayılan görünmez karekter dizi sayısı 5'tir. 5'ten daha fazla boşluk olursa program uyarı verecektir.

- Duyarlılık – Orta (Düşük duyarlılığa ek olarak)

  Temel dosya denetimi gibi, eğer ek dosya basit (EXE, COM, BAT vs.) uzantısına sahipse uyarı mesajı ekrana gelecektir. Bu tür dosyaların hepsi tehlikeli değildir, bu nedenle orta derecedeki duyarlılık daha fazla yanlış alarm verebilmektedir.

- Duyarlılık – Yüksek (Orta duyarlılığa ek olarak)
  - HTML bölüm kontrolü.

    Bazı virüsler bazı mail programlarında özellikle savunmasız MS Outlook ve Outlook Express programlarında hata oluşmasına neden olur. Böylece virüsün başlaması için önizleme kısmında virüsün görülmesi yeterli olmaktadır. Avast! mesajın, HTML kodunun, bir tuzağı yürütebilecek etiketinin var olup olmadığını araştırır. Varsa, uyarı verir.

  - Giden mesajlar - Zaman periyodu denetimi

    Bir çok virüs e-posta yolu ile bulaşır ve Windows adres rehberinde yer alan bütün adreslere kendilerini gönderir. Çok kısa bir sürede, mesajlar aynı konu ve/veya ek ile bir çok adrese gönderilir. Avast! verilen sürede kaç mesaj gönderildiğini izler, ayrıca mesajların konusunu ve/veya ekleri kontrol eder. Bu parametrelerin hepsi Keşifsel (Gelişmiş) sayfasında ayarlanabilir.

- Giden mesajlar - Toplu mesajlar

  Virüsler aynı zamanda yalnızca tek bir mesajda bir çok alıcıya kendilerini göndererek yayılırlar. Avast! bu durumda toplam alıcı sayısını izler. İzin verilebilir toplam alıcı sayısı Keşifsel(Gelişmiş) sayfasında ayarlanabilir.

- Duyarlılık- Özel

"Özelleştir"e tıklayarak, yukarıdaki keşifsel analizlerden hangilerinin kullanılmasını istiyorsanız ayarlayabilirsiniz.

Ek olarak "Konu yapı denetimi"ni seçebilirsiniz. Bu seçeneği işaretlerseniz, e-posta konu başlıkları birçok anlamsız karektere göre taranacaktır. Örneğin, "<?*&$^*(^%#$%*_()", ve tabi uyarı verilecektir.

- İzinli URL'ler

  Bu pencerede "güvenli" URL leri tanımlayabilirsinzi, böylece keşifsel analiz tarafından uyarı almayacaksınız. Url ekelmek için, "Ekle" butonuna tıklayın ve URL'nin adını girin. URL'yi kaldırmak için "Kaldır" butonuna tıklayın.

- Sessiz mod

  Bu sayfada da virüs bulunduğunda ne tür bir yöntem kullanılacağını belirleyebilirsiniz.

Keşifsel (Gelişmiş)

Bu sayfada, giden postaların keşifsel analiz ayarlarını düzenleyebilirsiniz. Ayarlar yalnızca "Keşifsel" duyarlılık yüksek ya da özel olarak ayarlandığında kullanılabilir. (ve yalnızca özelleştirme ayarlarından değiştirilebilir.)

- Denetim süresi.

  avast! verilen süre içerisinde giden epostaları sayar. Varsayılan ayar 30 saniyede 5 mesajdır. Bu, yarım dakikada aynı konu ve/veya dosya eki ile beraber 5den fazla mesaj gönderilirse uyarı alacağınız anlamına gelir.

- Uyarı sayısı.

  Bu sayı, hiç bir uyarı olmaksızın, minimum izin verilen aynı konulu ve/veya aynı dosya ekli mesajların sayısıdır. Bu sayının üzerinde aynı konulu ve/veya aynı dosya ekli mesaj gönderilirse uyarı ekrana gelecektir.

- Konuyu denetle.

  Bu özelliği ayarlarsanız, toplu mesajlar eposta konusuna göre tanımlanacaktır.

- Dosya eklerini denetle.

  Bu özelliği ayarlarsanız, toplu mesajlar dosya eklerine göre tanımlanacaktır.

- Mutlak sayım.

  Bu toplam alıcı sayısıdır. Örneğin, varsayılan ayar, adreslerin girildiği Kime, CC ve BCC alanları için en fazla 10'dur. Alıcı sayısı bu sayının üzerine çıkarsa uyarı ekrana gelecektir.

Sıkıştırıcılar

Bu sayfa yalnızca yerleşik koruma görevi ayarlarına Gelişmiş arayüzden ulaşıldığında gösterilir. (sayfa 57)

Virüs

Bu sayfada virüslü dosyalara karşı ne tür bir hareketin izlenceğini belirleyebilirsiniz. Bu sayfa yalnızca yerleşik koruma görevi ayarlarına Gelişmiş arayüzden ulaşıldığında gösterilir. (sayfa 56)

3. Ağ kalkanı

Ağ kalkanı bilgisayarınızı İnternet worm/solucanı ataklarından korur. Çalışma şekli, tam olarak olmasa da güvenlik duvarına benzer. Bu durumda farklı güvenlik duvarı kullanılması kesinlikle tavsiye edilmektedir.

Ayarlar

- Uyarı mesajlarını göster

  Bu kutucuk işaretli ise, her solucan atağı tespit edildiğinde ekranın sağ alt köşesinde bir mesaj belirecektir.

- Günlük tutma

  Bu seçenek bir sonraki saldırı geçmişinin raporlanması ve ""Son ataklar" sayfasında gösterilmesi için işaretlenmelidir. Bu sayfayı görebilmek için yerleşik koruma ayarlarına direk olarak ulaşılması gerekmektedir. Örneğin ekranınızın sağ alt köşesindeki mavi avast! ikonuna sağ tıkladığınızda ulaşılabilir. Bu ayarlara gelişmiş arayüzde yerleşik koruma görevi ayarlarından ulaşılamaz.

Son saldırılar

Bir önceki sayfada "Günlük tutma" kutucuğu işaretlendi ise, son 10 solucan saldırısı bu sayfada listelenmektedir. Bu listede saldırının tarihi, zamanı, saldırının türü , IP adresi ve hangi porttan geldiği de yer alacaktır.

4. Outlook/Exchange

Tarayıcı
Burada hangi tür mesajların taranacağını ve mesaj gövdesinin eklerle beraber taranıp taranmayacağını belirleyebilirsiniz.

Gelen mesajları tara
Burada , gelen mesajlarda herhangi bir virüslü mesaj tespit edildiğinde ne yapılması gerektiğini belirleyebilirsiniz. Örneğin, vürüslü mesaj, farklı bir eposta klasörüne yönlendirilebilir, şartlı olarak silinebilir ya da gelen kutusuna aktarılmasına izin verilebilir. Ayrıca temiz ya da virüslü dosyalara not eklenip eklenmeyeceğini de belirleyebilir, notun biçimini TXT ya da HTML olarak seçebilirsiniz. Virüslü dosayalara karşı izlenecek yöntem "Virüs depolama" ve "Gelişmiş" sayfalarındaki ayarlara göre belirlencektir.

Giden posta

Burada yukarıdaki gibi temiz mesajlara not eklenip eklenmeyeceğini ve mesajın biçimini belirleyebilirsiniz. Virüslü mesajler zaten gönderilmeyecektir. Ayrıca dosya eklerinin gönderilirken değil de eklenirken taranmasını ayarlayabilirsiniz.

İmzalar
İmza kullanarak taranması gereken mesajların sayısını büyük ölçüde azaltabilirsiniz. İmzalar virüssüz mesajların virüssüz olduklarını teyid etmek için eklenmiş küçük işaretlerdir. Her imza taramanın tarihini ve zamanını içermektedir.

MS Outlook/Exchange sağlayıcıları imzaları tamamıyla örneğin avast! Exchange Server Edition ile uyumludur. Bu nedenle Exchange Server sağlayıcısı tarafından test edilen mesajlar Outlook/Exchange sağlayıcısı tarafından tekrar test edilmeyecektir.

- **Temiz mesajların içine imza(işatet) ekle**.

  Temiz yani virüssüz mesajlara imza eklenmesini istiyorsanız bu kutucuğu işaretleyiniz.

- **Her zaman işaretlenmiş mesajlara güven**

  Bu kutucuk işaretlenirse, imzanın ne kadar eski olduğuna bakılmaksızın imzalanmış mesajlara her zaman güvenilecek ve taranmayacaktır ("Mevcut virüs veritabanından eski işaretleri her zaman yoksay" kutucuğu işaretlenmediği sürece).

- **Sadece bu dereceye kadar imzalara güven**

  Burada güvenilecek maksimum imza derecesini belirleyebilirsiniz. Buradaki değer "Mevcut virüs veritabanından eski işaretleri her zaman yoksay" seçeneği ile maskelenebilir. Aşağıdaki açıklamaları inceleyiniz.

- **Tüm işaretleri (imzaları) yoksay (güvenme)**

  Bu kutucuk işaretlenirse, geçerli bir imzası olup olmadıklarına bakılmaksızın, bütün mesajlar taranacaktır.

- **Mevcut virüs veritabanından eski işaretleri (imzaları) her zaman yoksay**

  Bu kutucuğu işaretlerseniz, o andaki mevcut virüsveritabanından daha eski bir imzası olan mesajlar taranacaktır. Bu özellik, mesaj, orjinal taramadan sonra virüs veritabanına eklenen yeni bir virüs içeriyorsa, oldukça yararlıdır. Mesaj güvenilir olarak ayarlanırsa, tarama gerçekleştirilmeyecek ve bu durumda virüs bulunamayacaktır.

Virüs Depolama

Bu ekranda, virüslü ekin kopyasını sabit diskinizde belirlediğiniz klasöre kaydetmeye ayarlayabilirsiniz. Gözatma butonunu klasörü ve alanı belirlemek için kullanınız. "Varolan dosyaların üzerine yaz" seçeneğini işaretlerseniz, aynı ada sahip herhangi bir dosyanı yerini yeni dosya alacaktır.

Gelişmiş

- Sessiz mod

  Virüs safasında belirlenmiş olan hareket varsayılan hareket ise, örneğin etkileşimli seçim, sessiz mod kutucuğunu işaretlerseniz bulunan virüsler karantinaya taşınacaktır.

  Virüs sayfasında varsayılan hareket seçiliyken sessiz mod kutucuğu işaretlemezseniz, ekrana normal virüs uyarısı gelecek ve size virüsle ne yapmak istediğiniz sorulacaktır.

  Etkileşimli seçenekten başka bir hareket seçili ise, bu kutucuğu işaretlemenizin hiç bir etkisi olmayacaktır.

- Gerçekleştirilen işlem hakkında detaylı bilgi göster

  Bu kutucuk işaretli ise, o andaki test edilen dosyalara ait detaylı bilgi ekranınızın sağ alt köşesinde gösterilecektir.

- Email taranırken alt çubukta simge göster

  Bu kutucuk işaretliyse, ekranınızın sağ alt köşesinde tarama işlemini göstermek için küçük bir ikon olacaktır.

- Sağlanıcı yüklenirken açılış ekranı göster

  Bu kutucuk işaretlenirse her eposta sağlayıcısı çalıştığında avast! açılış sayfası ekranınıza gelecektir.

Son olarak MAPI profili ve şifre girerseniz, bu Gelen email sayfasında Gözat butonuna tıkladığınızda eposta klasörü yapınızı göstermek için kullanılacaktır.

Keşifsel

Bu sayfadaki ayarlar İnternet Posta ayarları ile aynıdır.

Keşifsel (Gelişmiş)

Bu sayfadaki özellikler İnternet posta ayarları ile aynıdır fakat ek olarak iki farklı ayar daha vardır.

- Göreceli sayım (Adres defteri)

  Bu her bir mesaja ait alıcıların izin verilen sayısıdır. Adres defterindeki toplam sayının yüzdesidir. Bu sınır geçilirse program uyarı verecektir.

- Asgari sayım

  Bu minimum mutlak alıcı sayısıdır. Göreceli sayı aşılırsa, ve mutlak alıcı sayısı minimum saynın altında ise, uyarı mesajı verilmeyecektir. Örneğin; Göreceli sayım %20, Asgari sayım=10. Adress sayısı 40 ve bir mesaj 9 alıcıya gönderilmişse, göreceli sayımın sınırı aşılmış olacak, fakat uyarı verilmeyecektir. Çünkü mutlak alıcı sayısı asgari sayımdan düşüktür.

Sıkıştırıcılar

Bu sayfa, yalnızca yerleşik koruma görevi ayarlarına, Gelişmiş arayüzden ulaşıldığında gösterilir (sayfa 57)

Virüs

Bu sayfada, virüslü dosyalara karşı nasıl bir yöntem uygulanacağını belirleyebilirsiniz. Bu sayfa, yalnızca yerleşik koruma görevi ayarlarına, Gelişmiş arayüzden ulaşıldığında gösterilir (sayfa 56).

5. P2P Kalkanı

Programlar

Alınan dosyaların taranması için P2P programlarını girebilirsiniz. Bazı programlar yalnızca Windows NT, 2000, XP, 2003, Vista yada 2008 de korunabilir.,

Sıkıştırıcılar

Bu sayfa, yalnızca yerleşik koruma görevi ayarlarına, Gelişmiş arayüzden ulaşıldığında gösterilir (sayfa 57)

Virüs

Bu sayfada, virüslü dosyalara karşı nasıl bir yöntem uygulanacağını belirleyebilirsiniz. Bu sayfa, yalnızca yerleşik koruma görevi ayarlarına, Gelişmiş arayüzden ulaşıldığında gösterilir (sayfa 56)

6. Komut dosyası engelleme

Korunan programlar

Bu sayfada, komut dosyası engelleme modülü ile korunmasını istediğiniz web tarayıcılarını seçebilirsiniz.

Gelişmiş

- Başlangıçta açılış penceresini göster

  Bu işaretlenirse, her web tarayıcısı başlatıldığında avast! script blocker yazan bir kutucuk ekrana gelecektir.

- Gerçekleştirilen işlem hakkında detaylı bilgi göster

  Bu kutucuğu işaretlerseniz, o anda taranan dosyalarla ilgili bilgi ekranınızın sağ alt köşesinde gösterilecektir.

- Sessiz mod

  Bu kutucuk işaretliyse ve şüpheli bir komut dosyası belirlenirse siteye ulaşım engellenecektir.

Virüs

Bu sayfada, virüslü dosyalara karşı nasıl bir yöntem uygulanacağını belirleyebilirsiniz. Bu sayfa, yalnızca yerleşik koruma görevi ayarlarına, Gelişmiş arayüzden ulaşıldığında gösterilir (sayfa 56)

7. Standart kalkan

Tarayıcı (Temel)

Bu pencerede, bu modül tarafından neyin taranacağını belirleyebilirsiniz. Bu penceredeki bütün kutucukları işaretlemenizi tavsiye ediyoruz. Böylece bir çok virüs tipi için tarama yapılabilecektir.

Tarayıcı (Gelişmiş)

Bu pencerede, diğer dosyaları uzantısına göre, açıldıklarında ve/veya oluşturulduklarında ya da değiştirildiğinde taranmaya ayarlayabilirsiniz.

- Açılırken tara.

  Taranacak olan eklenen dosyaların, virgül ile ayrılması gerekmektedir. "?" işaretini de kullanabilirsiniz. Mesela bütün açık .htm ve .html dosyalarının taranmasını istiyorsanız, "htm" ya da "html" girmeniz gerekmektedir ya da "ht?" olarak da girebilirsiniz. Böylece "ht" ile başlayan bütün uzantılar, "htt" gibi, taranacaktır.

  - WSH komut dosyalarını herzaman tara.

    Bu seçenek ile bütün komut dosyaları (Wşndows Scripting Host) test edilmiş olacaktır.

  - Sistem kütüphanelerini tarama

    Bu seçenek ile güvenilen sistem kütüphaneleri açılırken taranmayacak, yalnızca hızlı tarama gerçekleştirilecektir. Bu seçenek sistemin başlatılmasını az da olsa hızlandırabilir.

- Oluşturulmuş/değiştirilmiş dosyaları tara

  Bu kutucuğu işaretlerseniz, dosyalar oluşturulduğu anda ya da düzenlenirken taranacaktır. Ayrıca bu tarama işleminin :

  - Tüm dosyalara
  - Ya da sadece seçili uzantılara sahip dosyalara uygulanmasını belirleyebilirsiniz.

    "Varsayılan uzantı set"i işaretlenirse, sadece tehlikeli olduğu varsayılan uzantılar taranacaktır. "Göster" butonuna tıklayarak varsayılan uzantıların listesine ulaşabilirsiniz. Ek olarak taranmasını istediğiniz uzantıları kutucuğa girebilirsiniz.

Engelleyici

Bu pencerede, belirli bazı uzantılara sahip dosyaların çalışmaları engellenebilir. Bu varsayılan uzantı seti ne uygulanabilir. "Göster"e tıklayarak varsayılan uzantıların listesini görebilirsiniz, ayrıca kendiniz de çalışmasının engellenmesini istediğiniz uzantıları ilgili bölüme girebilirsiniz.

Bundan sonra belirlediğiniz dosyalar için engellenmesini istediğiniz çalışmaları belirleyebilirsiniz. Diğer iki seçeneği, avast, bir işlemin engellenmesi gerekiyor ve ne yapması gerektiğini soramadığında kullanacaktır, örneğin ekran koruyucu çalışıyorsa.

Gelişmiş

- Gerçekleştirilen hareket hakkında detaylı bilgi göster

  Bu seçeneği işaretlerseniz, o anda taranan dosyalar, ekranınızın sağ alt köşesinde gösterilecektir.

- Sessiz mod

  Virüs sayfasında varsayılan hareketi seçtiniz ise, örneğin etkileşimli seçim, sessiz mod kutucuğunu işaretlerseniz bulunan virüslerle aşağıdaki kurallara göre ilgilenilecektir:

  - "Genel cevaplarla Evet (Tamam)" seçili ise, bu durumda epostaya eklenmiş herhangi bir virüslü dosya otomatik olarak silinecektir.
  - İkinci seçenek olan "genel cevaplarla hayır (Hayır)" seçili ise, virüslü dosyalar karantinaya taşınacaktır.

Virüs sayfasında varsayılan hareketi seçtiniz ise ve sessiz mod kutucuğunu işaretlemedi iseniz, normal virüs uyarı ekranı virüs ile ne yapmak istediğinizi soracaktır.

Varsayılan hareketten farklı bir hareket seçtiyseniz, bu kutucuğu işaretlemeniz herhangi bir etki yaratmayacaktır.

Son olarak bu mod tarafından taranmasını istemediğiniz alanları belirleyebilirsiniz.

Sıkıştırıcılar

Bu sayfa, yalnızca yerleşik koruma görevi ayarlarına, Gelişmiş arayüzden ulaşıldığında gösterilir. (sayfa 57)

Virüs

Bu sayfada, virüslü dosyalara karşı nasıl bir yöntem uygulanacağını belirleyebilirsiniz. Bu sayfa, yalnızca yerleşik koruma görevi ayarlarına, Gelişmiş arayüzden ulaşıldığında gösterilir (sayfa 56)

8. Web kalkanı

Web kalkanı yerel vekil sunucusu gibi çalışır. NT işletim sistemlerinde (Windows NT/2000/XP/2003/Vista/2008) koruma tamamen şeffaftır ve genellikle herhangi bir normal ayarlamaya gerek yoktur. Windows 95/98/ME kullanıyorsanız, İnternet seçeneklerinden ayarları değiştirmeniz gerekir. Yerel vekil adresi ve portu aşağıdaki gibi olmalıdır.

Yerel alan ağı kullanılıyorsa (LAN):	Aramalı bağlantı kullanılıyorsa (modem):
Internet Explorer'ı başaltın	Internet Explorer'ı başaltın
Önce "Araçlar"a daha sonra "İnternet seçenekleri" ne tıklayın.	Önce "Araçlar"a daha sonra "İnternet seçenekleri" ne tıklayın.
Bağlantılar kısmına tıklayın.	Bağlantılar kısmına tıklayın.
Yerel ağ ayarlarına tıklayın.	Listeden aramalı bağlantıyı (dial up) seçin ve ayarlara tıklayın.
"Yerel ağınız için bir Proxy sunucusu kullanın" seçeneğini işaretleyin.	"Bu bağlantı için bir Proxy sunucusu kullanın" seçeneğini işaretleyin.
adres kısmına "yerelsunucu" yazın. (alternatif olarak,yerel sunucuyla aynı olan IP addresi 127.0.0.1 girebilirsiniz,). B.nok. kısmına 12080 numarasını girin.	adres kısmına "yerelsunucu" yazın. (alternatif olarak,yerel sunucuyla aynı olan IP addresi 127.0.0.1 girebilirsiniz,). B.nok. kısmına 12080 numarasını girin.
Tamam a tıklayarak teyid edin.	Tamam a tıklayarak teyid edin.

Not: Birden fazla bağlantınız varsa, adresi ve yerel proxy portunu her bağlantı için ayrı ayrı ayarlamalısınız.

Temel

- Web taramayı etkinleştir

  Bu kutucuktaki işareti kaldırırsanız, web tarayıcı özelliğini URL engellemeyi etkilemeksizin, kapatabilirsiniz.

- Akıllı akış tarama kullan

  Bu kutucuğu işaretlediğiniz takdirde, indirdiğiniz dosyalar neredeyse gerçek zamanlı olarak taranacaktır. Veriler parça parça indirildikçe taranır, hiç bir parça bir önceki parçanın virüssüz olduğu kesinleşene kadar indirilmez. Bu özelliği etkisiz hale getirseniz dosyaların tamamı geçici klasöre indirilip, daha sonra taranacaktır.

  Bu penceredeki diğer özellikler Windows 95, 98, Millennium da bulunmamaktadır:

- HTTP portlarını yönlendir

  Bu özellik İnternet erişimi ve sunucuyla bilgisayarınız arasındaki bağlantı taramak için bir tür proxy sunucusu kullanıyorsanız çok önemlidir. Örneğin, herhangi bir proxy sunucuya port 3128 kullanarak bağlanıyorsanız, bu numarayı kutucuğa girmeniz gerekmektedir. Yoksa avast! bağlantının port 80 de(varsayılan) yer almasını bekleyecek ve diğer bütün bağlantılar yoksayılacaktır. Not: HTTP dışında başka port girmeyiniz (örneğin ICQ, DC++ portu vs. gibi). Port numaraları virgülle ayrılmalıdır.

- Adresleri yoksay.

  Buraya Web Kalkanına yönlendirilmeyecek olan adları ya da IP adreslerini girmeniz gerekmektedir. Adres sayısı birden fazla ise virgülle ayrılmalıdır.

- Yerel bağlantıyı yoksay.

  Bu kutucuk işaretlenirse, bütün yerel bağlantı, örneğin bilgisayarınızdaki çalışan programlar arasındaki bağlantı yoksayılacaktır.

Web tarama

Bu sayfada hangi tür dosyaların internetten indirilirken taranacağını belirleyebilirsiniz. Bu dosyaların tümünün taranmasını ya da sadece seçilen dosya türerinin taranmasını ayarlayabilirsiniz. İkinci seçeneği seçerseniz, taranmasını istediğiniz dosya türlerinin uzantısını girmeniz gerekmektedir. Uzantıları ayırmak için virgül kullanınız. Ayrıca taranması gereken dosyaların MIME türlerini de girebilirsiniz. Her iki durumda da joker karekter kullanabilirsiniz.

İstisnalar

Burada Web Klakanı tarafından taranmayacak nesneleri belirleyebilirsiniz. Bu güvenilir tek bir yerden bir çok dosya indirirken yararlı olabilir.

- URL Engelleme

  Ekle butonunu, engellenmesi gereken URL adreslerini girmek için kullanınız. Yalnızca bir sayfayı engellemek istiyorsanız tüm yolu girmeniz gerekmektedir. Örneğin http://www.yahoo.com/index.html girerseniz, yalnızca, index.html taramadan dışlanacaktır. http://www.yahoo.com/* girerseniz, http://www.yahoo.com ile başlayan hiç bir sayfa taranmayacaktır. Benzer şekilde , tarama dışı bırakılacak herhangi bir dosya için, örneğin ".txt" uzantılı dosya için *.txt yazınız.

- Dışlanan MIME ve türler

  Burada taranmasını istemediğiniz MIME türlerini/alt türlerini girebilirsiniz.

URL Engelleme

Web Kalkan ayrıca belirli web sayfalarına ulaşılmasını engellemek için de kullanılabilir. Bu özellik kapalı olarak ayarlanmıştır, fakat uygun olmayan web sayfalarına ulaşılmasını engellemek için kullanılabilir (örneğin, porno, yasadışı yazılım içeren sayfalar vb.). Engellenmiş bir sayfaya ulaşılmaya çalışırken, bu sayfaya ulaşmanın avast! antivirus tarafından engellendiğine dair uyarı mesajı gösterilecektir.

"URL engellemeyi etkinleştir" kutucuğunu işaretleyip engellenmesini istediğiniz URL adresini giriniz ve Ekle butonunu tıklayınız. Joker karekterleri (örneğin, ? ve *) kullanabilirsiniz. Mesela http://www.penthouse.com/* adresi girerseniz, http://www.penthouse.com ile başlayan hiçbir sayfa açılmayacaktır.

Girilen URL adresleri aşağıdaki kurallara göre tamamlanacaktır:

Adres http:// ya da joker karekteri ile başlamıyorsa (* veya ?), avast! adresin başına http:// takısını sonuna da yıldız koyacaktır. Bu durumda www.yahoo.com girerseniz, adres http://www.yahoo.com* şeklinde düzenlenecektir.

Gelişmiş

- Gerçekleştirilen bilgi hakkında detaylı bilgi ver

  Bu kutucuk işaretlenirse o anda test edilen dosyalarla ilgili detaylı bilgi ekranın sağ alt köşesinde gösterilecektir.
- Sessiz mod

  Bu kutucuğu işaretlerseniz, her virus bulunduğunda bağlantı sonlandırılacaktır.

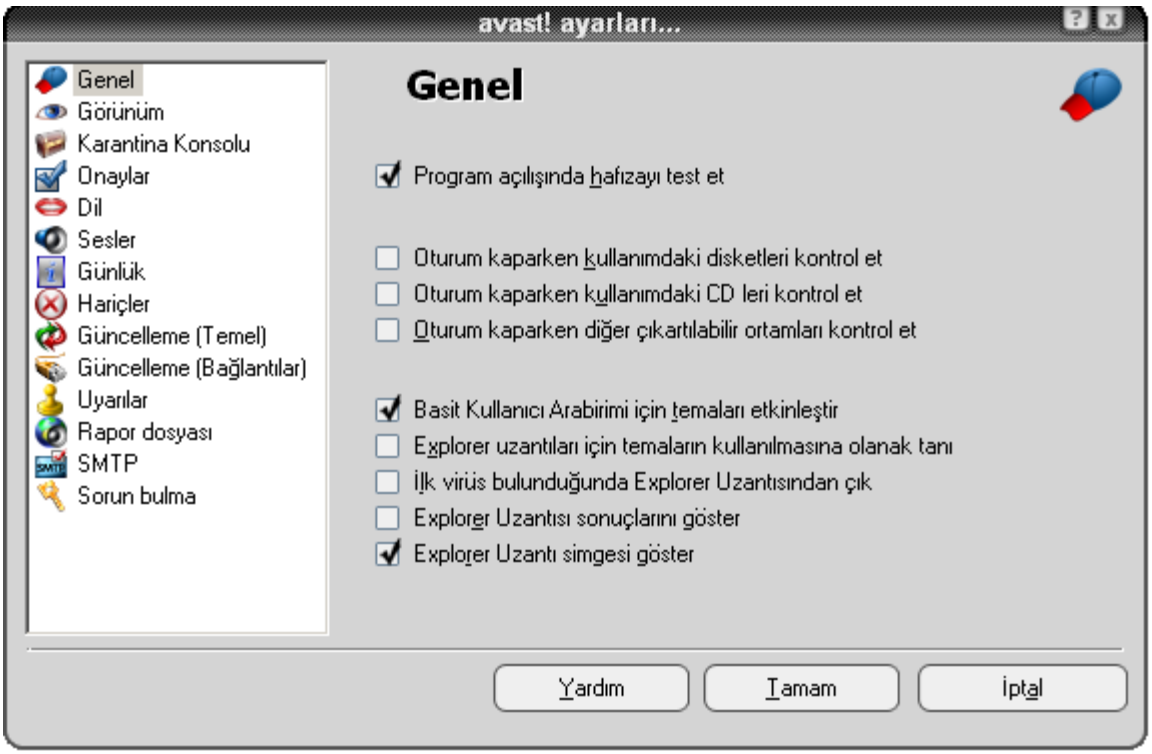
Sıkıştırıcılar

Bu sayfa yalnızca yerleşik koruma görevleri ayarlarına Gelişmiş Arayüzden ulaşıldığında görünebilir (Sayfa 57)

Diğer avast! ayarları

Diğer birçok avast! özelliklerini ihitiyaçlarınıza ve terciklerinize göre ayarlayabilirsiniz. Bu özelliklerin çoğu önceki bölümlerde açıklanmıştır.

Basit kullanıcı arayüzü kullanıyorsanız menüye gidin ve "Program ayarlar"ına tıklayın. Aşağıdaki pencere açılacaktır. Gelişmiş arayüz kullanıyorsanız yalnızca "Ayarlar"a tıklayın ve ek olarak "Gelişmiş arayüz" seçeneğini göreceksiniz. Pencerenin solunda bulunan ilgili ikonlara tıklayarak gerekli ayarlamaları yapabilirsiniz.



Genel ayarlar

Bu ekranda oturumun açılışında ve kapanışında ne tür bir tarama yapılacağını belirleyebilirsiniz. Ayrıca "Basit kullanıcı arabirimi için temaları etkinleştir" kutucuğunu işaretleyerek görünümü değiştirebilirsiniz.

Explorer uzantısı

Son dört kutcuk "Explorer uzantısıyla" alakalıdır. Bu özellik ile her bir dosyayı sağ tıklayıp "tara<dsoya adı>"nı seçerek taratabilirsiniz. Bu kutucuk işaretlenirse yanında mavi balon ikonu gözükecektir.

Görünüm

"Görünüm" ayarlarından avast! ikonunun ekranın sağ köşesinde gösterilip gösterilmeyeceğini ve tarama esnasında simgenin hareket ettirilip ettirilmeyeceğini belirleyebilirsiniz.

Avast! oynatıcısı üzerinde yarı saydam efektler kullanabilirisiniz. Bu ayarlar uygulama yeniden başlatıldıktan sonra devreye girecektir.

Gelişmiş arayüz (yalnızca Gelilmiş arayüz kullanılırken gösterilir)

Bu ekranda özel görevler olan "Explorer uzantısı" (sayfa 68) ve Ekran koruyucusunun gelişmiş arayüzdeki görev listesine eklenip eklenmeyeceğini belirleyebilirsiniz. Bunlar burada gösterilirse, diğer görevler gibi üzerine tıklanıp koyultularak ve "Düzenle" butonunu kullanarak düzenlenebilir.

"Oturum sonuçlarını kaydır" taranmış olan dosyaların listesi devamlı olarak aşağıya doğru hareket ettirilecektir. Bu özellikten tarama işlemini takip etmek istiyorsanız yararlanabilirisniz. Bu kutucuğu işaretlemezseniz, tarama işlemi gerçekleştirilirken listeyi el ile aşağı yönde hareket ettirebilirsiniz.

Son kutucuğu kullanarak, tamamlanmış olan oturumun belli bir süreden sonra silinip silinmeyeceğini belirleyebilirsiniz.

Onaylar

Bu pencerede hamle seçtiğinizde programın onay isteyip istemeyeceğini belirleyebilir ve bu belirli hareketlerden sonra onay mesajı almak isteyip istemediğinizi belirleyebilirsiniz.

Onaylar avast! antivirüsün güvenlik özelliklerinden biridir. Yanlış bir hamle yaptığınızda onaylama özelliği sayesinde hamleyi iptal edebilirsiniz.

Hiç bir onay mesajı almak istemiyorsanız, ilgili kutucuktaki işareti siliniz. Onay isteği ile ilgili herhangi kutucuk işaretlenmemişse, seçilen hamle ya da işlemi iptal edebilme şansınız olmayacaktır.

Aşağıdaki onay istekleri normalde işaretlidir, fakat bu onaylardaki işaretleri kaldırarak bu özellikleri kapatabilirsiniz :

- ***Bir tarama yapma yapılırken basit kullanıcı arabirimini kapatmadan sor.***
  Tarama esnasında program kapanırsa, tarama otomatik olarak sonlandırılacaktır.

- ***Yerleşik sağlayıcı durum değişikliğini kalıcı yapmadan sor***
  Bu mesaj yerleşik koruma modüllerinden herhangi birini sonlandırmak istediğinizde sorulacaktır (sayfa 21). "Evet" butonunu tıkladığınızda, ilgili mod siz tekrar aktif hale getirene kadar durdurulacaktır. "Hayır" olarak cevaplarsanız, bu mod bilgisayarınızı yeniden başlattığınızda tekrar aktif hale gelecektir.

- **Erişimde korumayı durdurmadan önce sor**
  Bu mesaj Erişimde korumayı tamamen "Durdurmak" istediğinizde gösterilecektir. (sayfa 60)"Evet" olarak cevaplarsanız, yerleşik koruma devre dışı kalacaktır. Fakat bilgisayarınızı yeniden başlattığınızda otomatik olarak yeniden aktive edilecektir.

- ***Dosyaları karantinadan silmeden önce sor***
  Bu kutucuk işaretli olduğu sürece program hiçbir dosyayı onay almadan silmeyecektir. Bu özellik sayesinde dosyaları yanlışlıkla silmenizi önleyecektir.

- ***Sonuçlar başarıyla işlenince mesaj gönder***
  Bu özellik sayesinde dosyalarla ilgili seçtiğiniz herhangi bir hamle, örneğin sil ya da karantinaya taşı, başarı ile tamamlanınca program tarafından teyid edilecektir.

- ***Sonuçlar işlenirken hata oluşursa mesaj gönder***
  Bu mesaj size seçtiğiniz hamlenin program tarafından gerçekleştirilemediğini bildirecektir.

- ***Eski VPS dosyası kullanılıyorsa mesaj gönder***
  Bu mesaj size virus veritabanınızın güncel olmadığını haber verecektir.Sisteminizin tamamıyla korunduğundan emin olmak için virus veritabanı düzenli olarak güncellenmelidir.(sayfa 34)

- ***Hata raporları başarıyla işlenince rapor gönder***

- ***Beta program sürümü uyarısı***
  Bu mesaj kullandığınız programın versiyonu hala deneme aşamasında olduğunu gösterir.

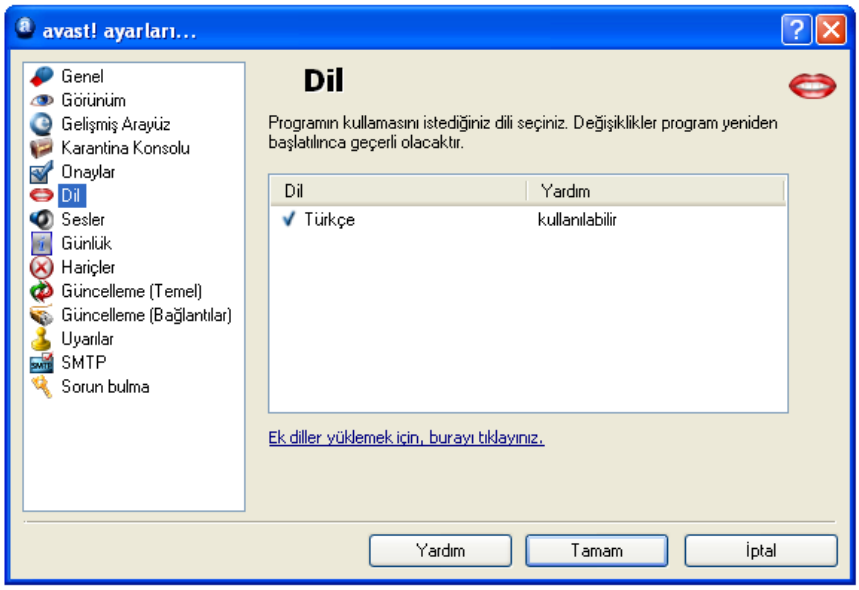
- ***İşlem doğru olarak tamamlansa bile virüs karantina konsolunda durum penceresini göster***
  Seçtiğiniz hamlenin başarıyla tamamlandığını gösterir.

- ***Görev yapılandırması esnasında doğru sonuçlar geçerliyse mesaj gönder***
  Bu kutucuğu işaretlediğinizde, "OK files" tarama sonuçlarına eklenip eklenmeyeceğini belirlerseniz mesaj alacaksınız. Bu uygulama yalnızca Gelişmiş arayüzündeki görev oluşumlarına uygulanmaktadır.

- ***Tehlikeli uzantılara sahip dosyaların silinmesi***
  Önemli bilgileri içeren dosyaların silinmesinin güvenli olmayacağını gösteren bir onay mesajıdır.

Programın dilinin değiştirlmesi

Programın dilini değiştirmek için "Dil" kısmına tıklayınız. Aşağıdaki pencere ekrana gelecektir.



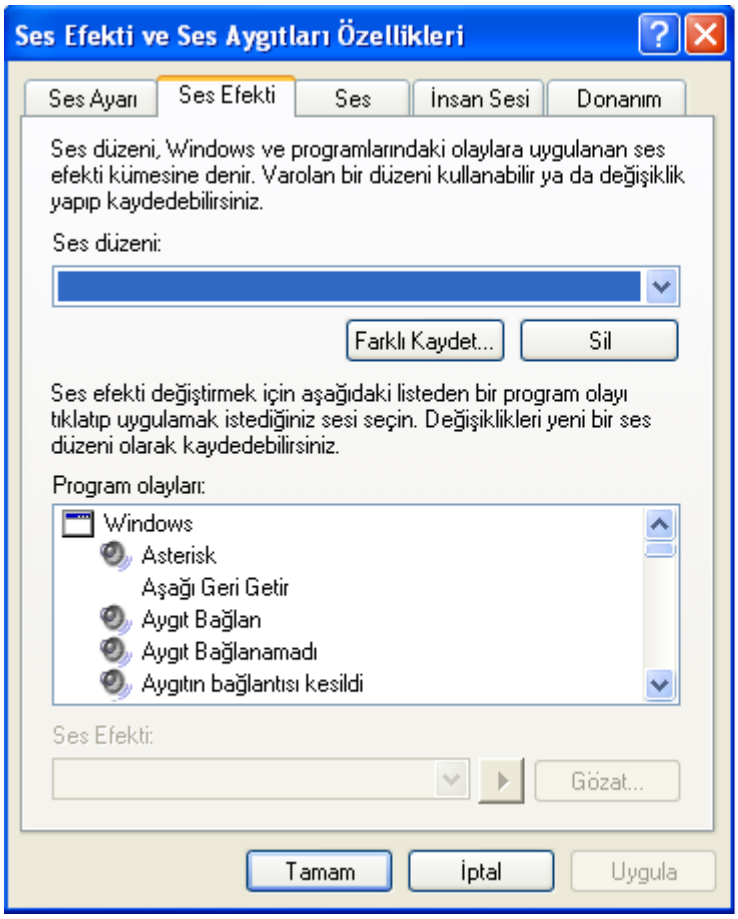
İstenilen dil için pencereniz sağ tarafında "kullanılabilir" yazıyorsa, önce üzerine ve ardından "Tamam" butonuna tıklayın. Bu noktadan sonra programı kapatıp yeniden başlatmalısınız. Yeniden başlattıktan sonra programın dili değişmiş olacaktır.

(Eğer istenilen dil listede yoksa, kutunun altındaki 'Ek diller yüklemek için buraya tıklayınız'' butonuna basın, ardından istediğiniz dilin karşısındaki kutucuğu işaretleyin, İleri'e basın ve yeni program dosyaları yüklenecektir.Tamamlandığında ''Bitir'' e tıklayın. Şimdi artık istediğiniz dili yukarıda anlatıldığı gibi listeden seçebilirsiniz.

Sesler

Bu ekranda, programın ses ayarlarını ayarlayabilir yada tüm sesleri kapatabilirsiniz.

Tekrar ‘’ Ayarlar’’ a tıklarsanız, bu sizi tüm Windows program seslerini ayarlayabileceğiniz bir ekrana götürecektir. Ekranın alt yarısında ‘’Program olayları’’ adında bir kutu vardır. Aşağıdaki pencereye bakınız.



Sağ taraftaki mavi yön oklarıyla listede aşağı doğru yarısına kadar ilerlerseniz avast!antivirus ‘ü ve programa hangi seslerin atandığını görebilirsiniz.Bir olay için başka bir ses atamak isterseniz uygun olayına ve ardından “Gözat”a tıklayın. Mümkün olan seçenekler listesinden istediğinizi seçip Tamam‘a basınız

Daha sonra yukardaki gösterilen kutuya dönüp, Uygula ve ardından Tamam’a tıklayın.

Bu da sizi ana ‘’Sesler’’ ekranına geri götürecektir.Burada işlemleri bitirmek için Tamam’a basın.

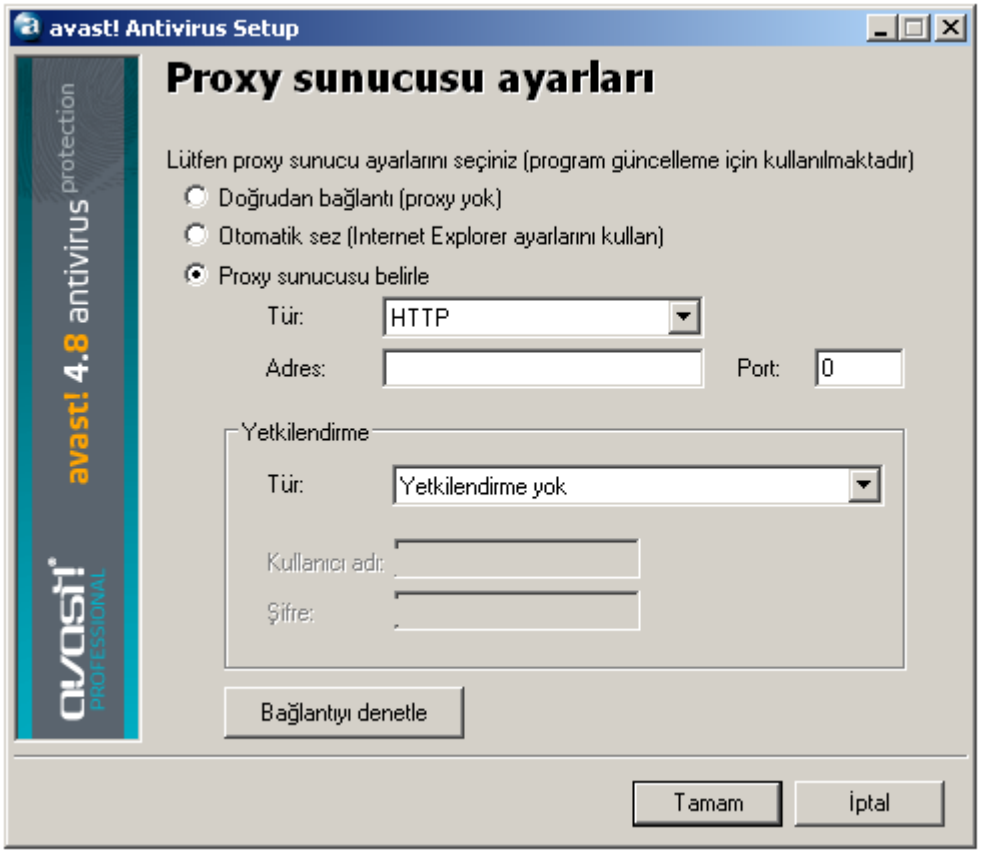
Güncelleme (Bağlantılar)

Ekranda uygun kutucuğu işaretleyerek internet bağlantı türünü belirleyebilirsiniz. Örneğin;

- Sadece dial-up bağlantı ile internet bağlanıyorum, veya
- Bilgisayarım sabit şekilde internete bağlıdır

Bu sayede avast! yeni güncellemeleri araştıracak, ve bu güncellemeleri daha güvenli bir şekilde gerçekleştirecektir.

Bağlantı türünü seçtiğinizde, ‘’Proxy’’ butonuna tıklayın. Karşınıza proxy sunucusu ayarlarına girebileceğiniz yeni bir pencere açılacaktır.Bu ayarlar avast! güncellemeler sırasında internete bağlandığında önem taşır.



Bir proxy üzerinden değilde, direkt olarak internete bağlandığınızda, ‘’Doğrudan bağlantı’’ seçeneğini işaretleyiniz. Bu genellikle dial-up (aramalı) bağlantı kullanıcıları için uygundur

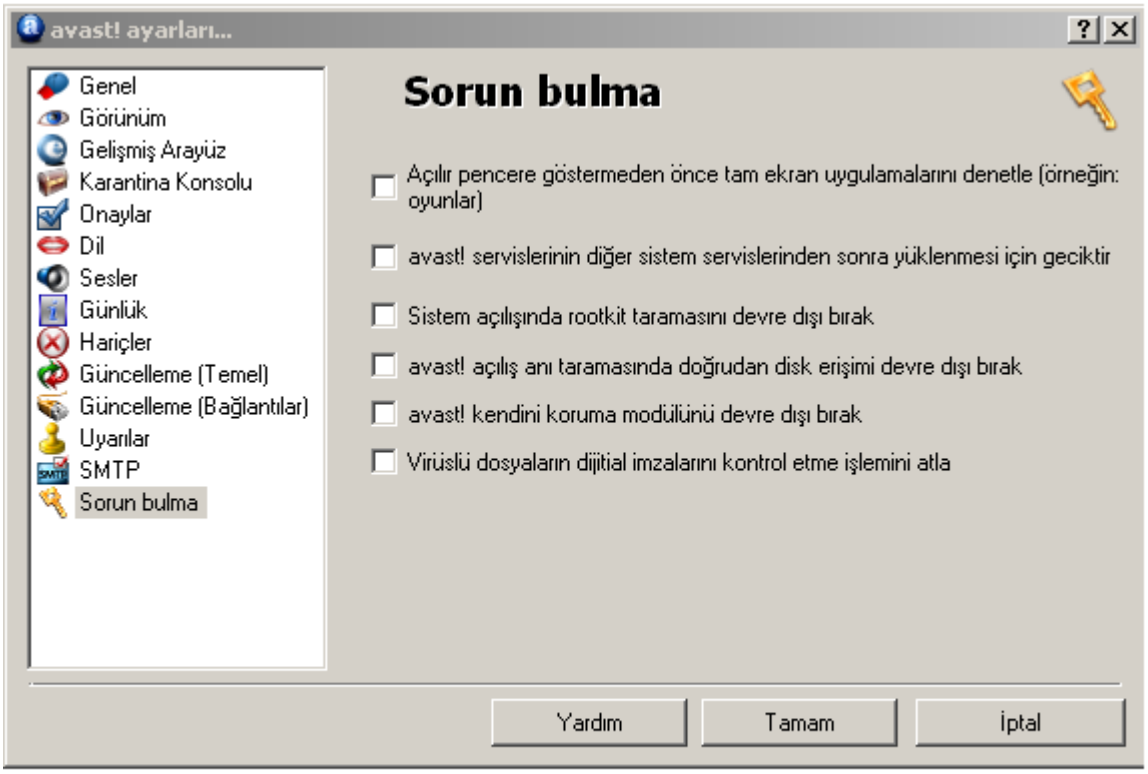
Eğer bir proxy sunucusu yada hangisini kullandığınızdan emin değilseniz ‘’Otomatik Sez’’(İnternet Explorer ayarları) seçeneğini işaretleyin, veya internet servis sağlayıcınıza ya da ağ yöneticinize sorunuz.

Proxy sunucunuzun adresini ve portunu biliyorsanız, "Proxy sunucusu belirle" seçip gerekli proxy det*a*ylarını aşağıdaki gibi giriniz:

- **Tür**. (HTTP yada SOCKS4
- **Adres**. Proxy sunucunuzun adresini girin
- **Port**. Proxy sunucunuzun portunu girin
- **Yetkilendirme türü**. Burada internete bağlanmak için proxy sunusunun bir onaylama isteyip istemediğini, eğer istiyorsa onaylama türünü belirleyin.
- **Kullanıcı adı ve şifre**. Bunlar onaylama için gerekliyse girilmelidir.

  Son olarak, ''Bağlantıyı denetle'' butonuna tıklayın ve yukarıdaki ayarlamalar doğrultusunda, bağlantınızın çalışıp çalışmadığını kontrol edin

Sorun bulma



Bu sayfada ayarları değiştirerek bazı spesifik sorunları çözebilirsiniz. Fakat bu ayarlar gerekmedikçe değiştirilmemelidir. Tereddüt ederseniz ilk olarak avast! ile temasa geçin.

Açılır pencere göstermeden önce tam ekran uygulamalarını denetle (örneğin oyunlar).

Bilgisayarınız çalışırken avast! konfigürasyonuna bağlı olarak virüs veritabanı güncelleştirildiğinde, ya da gelen bir e-posta taranması gibi durumlarda çeşitli mesajlar görüntülenir.Normalde mesajlar bu olayların gerçekleşmesi durumunda gösterilir. Fakat bu,bazı oyunlar gibi tam-ekran uygulamalarında uygulamanın kesintiye uğramasına ve tam ekran görünümünden normal pencere moduna dönmesine sebep olur.Bu seçeneği işaretlerseniz, avast! mesajları göstermeden önce bir tam-ekran uygulamasının o esnada çalışıp çalışmadığını kontrol eder, eğer öyle ise avast! herhangi bir mesaj göstermez.

avast! servislerinin diğer sistem servislerinden sonra yüklenmesi için geciktir.
avast! antivirüs servisi genellikle açılıştan erken başlar. Bu da genellikle bazı sistem servislerinin başlatılmasında, açılışta geçici olarak birkaç saniye yada birkaç dakika donma gibi problemler yaratabilir. Bu seçenek olağan sistem servisleri tamamen yüklenene kadar avast! 'ın başlatılmasını geciktirecektir.

Sistem açılışında rootkit taramasını devre dışı bırak.
İşletim sisteminizi başlattığınızda avast! rootkit taraması yapar. Eğer bu tip taramayı devre dışı bırakmak istiyorsanız bu kutucuğu işaretleyin

avast! açılış anı taramasında doğrudan disk erişimi devre dışı bırak.
Açılış taraması sırasında avast! özel bir disk erişim metodu kullanır. Bu ,kendi dosyalarını gizleyen virüsleri yakalamasını sağlar. Bu özelliği kapatırsanız ve avast! normal disk erişim metodunu kullanacaktır.

Avast! kendini koruma modülünü devre dışı bırak
Bazı virüsler , antivirüs yazılımının çalışmasını önemli dosyalarını silerek yada modifiye ederek durdurabilirler. Avast! bu tehlikeli virüsleri engelleyecek yerleşik bir koruma özelliğine sahiptir. Bu koruma modülünü devre dışı bırkamak için bu kutucuğu işaretleyiniz.

Virüslü dosyaların dijital imzalarını kontrol etme işlemini atla
Yanlış virüs uyarılarını önlemek için avast! virüslü dosyaların dijital imzalarını kontrol eder. Eğer bir dosya virüslü olarak tanımlanırsa, ve fakat Microsoft gibi güvenilir bir otoritenin geçerli bir dijital imzasına sahipse, büyük ihtimal bu yanlış tanımlı bir virüstür. Bu durumda avast! bu virüs tanımlamasını yok sayacaktır. Bu kutucuğu işaretleyerek avast!'ın ek kontorller yapmasını atlatabilirsiniz.

Komut satırı tarayıcısı nasıl kullanılır

Avast! komut satırı tarayıcı ashCmd.exe normalde şu dizine kurulmuştur ; C:\program files\alwil software\avast4.
Bir tarama işlemi, çeşitli anahtarlar ve değişkenler vasıtasıyla komut isteminden çalışır. Değişkenlerin tanımlarını görmek için ashCmd dosyasını bulun ve üzerine çift tıklayın. Bu sayede içinde çeşitli parametretlerin görüntülendiği yeni bir pencere açılacaktır. Tüm değişkenlerin bir listesi aynı zamanda ‘’Yardım’’ bölümünde ‘’ashCmd Program’’ klasörü içinde bulunabilir.
Taramayı gerçekleştirmek için, komut bekleme işaretine gidin ve programın adını ashCmd.exe ve ardından taranacak bölgeyi ve ilgili değişkenleri girin. Örneğin, bütün yerel sabit sürücüleri taratmak için, komut satırı aşağıdakiler gibi olmalıdır:

*C:\Program Files\Alwil Software\Avast4 ashCmd.exe /**

Başka parametreler gerektiğinde eklenebilir. Belirli bir dosyayı taratmak için, istenilen yolu girin ve içinde boşluk olan isimleri tırnak işareti ile yazıldığından emin olun. Örneğin,
C:\Program Files\Alwil Software\Avast4 ashCmd.exe c:\”program files”

Belli bir görevi çalıştırmak için, programın adını /@=<*görevin adı*> şeklinde girin. Örneğin, “Haftalıktarama” adındaki bir görevi çalıştırmak için, komut satırı aşağıdaki gibi olmalıdır:

C:\Program Files\Alwil Software\Avast4 ashCmd.exe /@=haftalıktarama

Görev , bu görev için belirlenmiş parametlerle çalışır. Bu parametrelerin haricinde komut satırına yazılanlar göz ardı edilir.
Eğer görev ismi boşluk içeriyorsa, tırnak içinde yazılmalıdır, mesela; ‘’Dokümanların Haftalık Taraması’’ şeklinde bir görev aşağıdaki gibi çalıştırılır:

C:\Program Files\Alwil Software\Avast4 ashCmd.exe /@=”Dokümanların Haftalık Taraması”

Tarama bittiğinde, sonuç çıktısı şu parametreler ile alınabilir “/_>”. Örneğin komut satırı: ashCmd.exe c:\windows /_> results.txt, c:\windows yolunda sonuçlanır ve tarama sonuçları results.txt adında yeni bir dosyaya kaydedilir.

avast! antivirüsün kaldırması

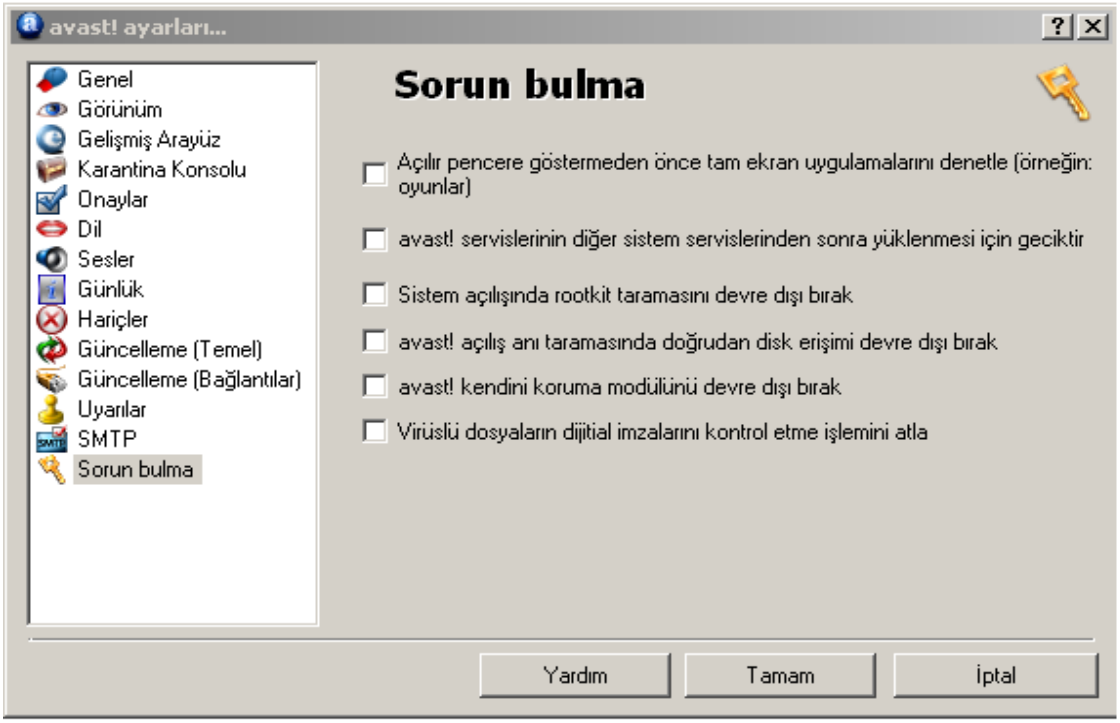
Bazı virüsler bilgisayarın antivirüs yazılımını kapatma özelliğine sahiptir. Bu nedenle avast! antivirüs, kendisinin bir virüs tarafından değiştirilmesinin ya da silinmesinin, çok güçlü kendini koruma modülü ile önler. Fakat, bunun sonucu olarak, diğer programlar avast!ı değiştiririken ya da silerken zorluk çekebilir. avast! antivirüs programını tam olarak kaldırabilmek için, doğru yöntemi uygulamak gerekmektedir.

avast! antivirüsü kaldırmaya çalışmadan önce, diğer yürütmekte olduğunuz programları kapatmanıztavsiye edilmektedir. avast! antivirüs programını kaldırmak için, aşağıdaki önerileri takip ediniz.

1. Kendini koruma modülünü devre dışı bırakın

- Ekranınızın sağ alt köşesinde bulunan mavi avast! ikonuna tıklayın ve "Program ayarlarını" seçin.

- Daha sonra pencerenin solundaki "Sorun giderme"ye tıklayın. Pencere aşağıdaki gibi değişecektir.



- "Avast! kendini koruma modülünü devre dışı bırak" kutucuğunu işaretleyip "Tamam"a tıklayın.

- Şimdi kendini koruma modülü devre dışıdır.

2. Programı kaldırın

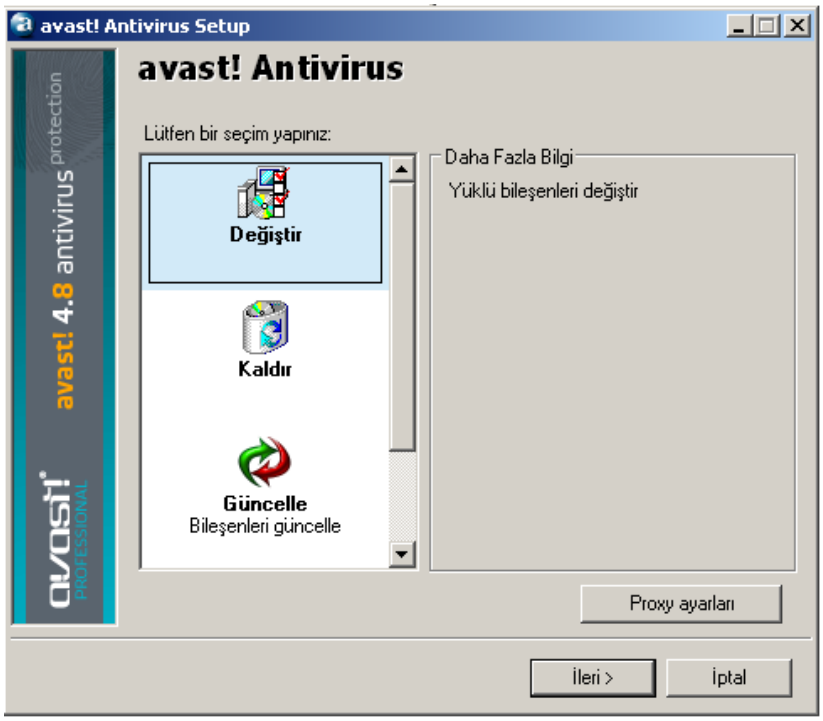
- Ekranınızın sol alt köşesinde bulunan "Başlat" butonuna tıklayın, ve denetim masasını (kontrol panelini) açın. Başalangıç menüsünde bulamıyorsanız, Ayarlara gidin ve listeden bulun.

- Denetim masasında "Program ekle veya kaldır"a tıklayın.

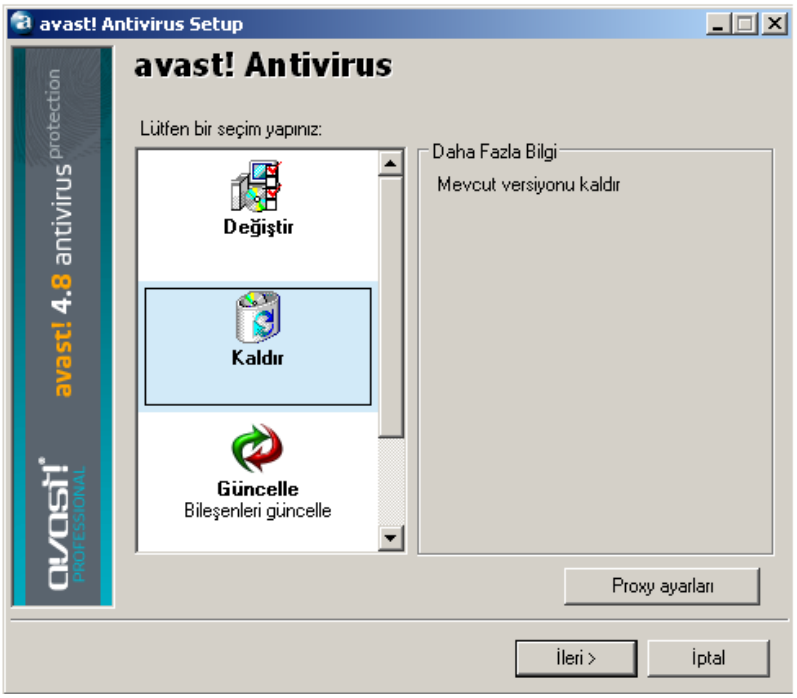
- Yüklü olan programlara ait bir liste ekrana gelecektir.

- "avast! antivirüs" üzerine tıklayarak koyultun ve "Değiştir/Kaldır" butonuna basın.

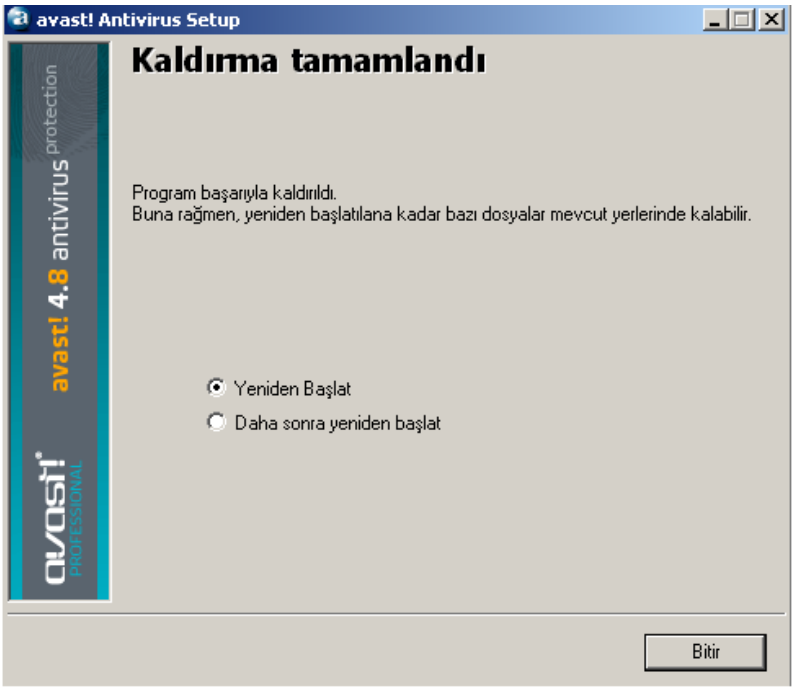
- Aşağıdaki pencere ekranınıza gelecektir:



"Kaldır" butonuna tıklayarak koyultun ve "ileri" tuşuna basın.



Böylece program kaldırılmış olacak ve aşağıdaki pencere ekranınıza gelecektir:



Kaldırma işlemini tamamlamak için bilgisayarınızı yeniden başlatmanız gerekmektedir. "Yeniden başlat" seçeneği işaretli iken, "Bitir" butonuna basın, bilgisayarınız otomatik olarak yeniden başlatılacaktır.