bitdefender

ANTIVIRUS 2008

Kullanıcı Kılavuzu

Telif Hakkı© 2008 BitDefender

BitDefender Antivirus 2008

Kullanıcı Kılavuzu

Yayımlanma 2008.06.20

Telif Hakkı© 2008 BitDefender

Yasal Uyarı

Tüm hakları saklıdır. Bu kitabın hiç bir kısmı, BITDEFENDER yetkili temsilcisinin yazılı izni olmadan fotokopi, kayıt veya herhangi bir bilgi depolama ve alma sistemi de dahil olmak üzere, elektronik veya mekanik olarak, herhangi bir şekilde veya yolla çoğaltılamaz veya aktarılamaz. Çalışmalarda kısa alıntıların yapılması, ancak alıntı kaynağının belirtilmesi şartıyla mümkün olabilir. İçerik hiç bir şekilde değiştirilemez.

Uyarı. Bu ürün ve dökümantasyonu telif hakkı ile korunmaktadır. Bu dökümandaki bilgiler, garanti verilmeden "olduğu gibi" temeline dayanarak sağlanmıştır. Her ne kadar bu dökümanın hazırlanmasında tüm önlemler alınmış olsa da, yazarlar, bu çalışmada ihtiva edilen bilgiler tarafından doğrudan veya dolaylı olarak, neden olunan herhangi bir zarar veya kayıptan dolayı herhangi bir kişi veya kuruma karşı herhangi bir sorumlu olmayacaktır.

Bu kitapta, BitDefender denetimi altında olmayan üçüncü şahıs Web sitelerine linkler bulunmakta olup, bu nedenle , bağlantı kurulan bu link sayfalarının içeriğinden BitDefender sorumlu değildir. Bu dökümanda verilen bir üçüncü şahıs web sitesine erişirseniz, bu kendi sorumluluğunuz altında olacaktır. BitDefender bu linkleri sadece referans amaçlı olarak sağlamaktadır ve bu linklerin dahil edilmiş olması, BitDefender'in, bu üçüncü şahıs web sitelerinin içeriği ile ilgili sorumluluğu kabul ettiği veya onayladığı anlamına gelmemektedir.

Ticari Markalar. Kitapta ticari isimler bulunabilir. Bu dökümandaki tüm tescilli veya tescilsiz ticari markalar tamamen ilgili sahiplerinin mülkiyetindedir ve bu şekilde kabul edilmektedir.

bitdefender

İçindekiler

Lisans ve Garanti ..... **vii**

Önsöz ..... **xi**

1. Bu Kitapta Kabul Edilen Yazım Kolaylıkları xi
   1.1. Tipografik Kurallar xi
   1.2. Uyarılar xii
2. Kitabın Yapısı xii
3. Yorumlarınız xiii

Kurulum Adımları ***1***

1. BitDefender Antivirus 2008 Kurulumu **2**

1.1. Sistem Gereksinimleri 2
1.2. Kurulum Adımları 3
1.3. Başlangıç Kurulum Sihirbazı 5
   1.3.1. Adım 1/6 - BitDefender Antivirus 2008' i Kaydedin 5
   1.3.2. Adım 2/6 BitDefender Hesabının Açılması 6
   1.3.3. Adım 3/6 – RTVR Hakkında Bilgi 8
   1.3.4. Adım 4/6 – Çalıştırılacak Görevlerin Seçilmesi 9
   1.3.5. Adım 5/6 – Görevlerin Tamamlanmasını Bekleyin 10
   1.3.6. Adım 6/6 – Özet 11
1.4. Yükseltme 11
1.5. BitDefender Özelliklerini Düzeltme veya Kaldırma 12

Temel Yönetim ***14***

2. Başlangıç **15**

2.1. Sistem Tepsisindeki Bitdefender İkonu 16
2.2. Tarama Etkinlik Çubuğu 17
2.3. BitDefender Manuel Tarama 17
2.4. Oyun Modu 18
   2.4.1. Oyun Modunu Kullanmak 18
   2.4.2. Oyun Modu kısayol tuşunu değiştir 18

3. Güvenlik Durumu **20**

3.1. Antivirüs Durumu Butonu 21
3.2. Antiphising Durum Butonu 22
3.3. Kimlik Kontrolü Durum Butonu 23
3.4. Güncelleme Durumu Butonu 23

4. Hızlı Görevler **25**

4.1. Güvenlik 25
   4.1.1. BitDefender Güncelleme 25

4.1.2. BitDefender ile taramak 27

5. Geçmiş 32

6. Kayıt 34

6.1. Adım 1/3 - BitDefender Antivirus 2008' i Kaydedin 34
6.2. Adım 2/3 BitDefender Hesabının Açılması 35
6.3. Adım 3/3 - BitDefender Antivirus 2008' i Kaydedin 37

Gelişmiş Güvenlik Yönetimi 38

7. Yönetim Konsolu 39

7.1. Genel Ayarları Yapılandırma 40
7.1.1. Genel Ayarlar 40
7.1.2. Virüs Raporu Ayarları 42
7.1.3. Ayarların Yönetimi 42

8. Antivirus 43

8.1. Erişim anında tarama 43
8.1.1. Koruma Seviyesi Yapılandırma 44
8.1.2. Koruma Seviyesini Özelleştirme 45
8.1.3. Gerçek-zamanlı Korumayı Kapat 49
8.2. İsteğe bağlı tarama 49
8.2.1. Tarama Görevleri 50
8.2.2. Kısayol Menüsünü Kullanmak 52
8.2.3. Tarama Görevleri Yaratmak 53
8.2.4. Tarama Görevlerini Yapılandırmak 53
8.2.5. Taranan Objeler 63
8.2.6. Tarama Kayıtları 70
8.3. Nesne Hariç Tarama 72
8.3.1. Yolları taramadan hariç tutmak 74
8.3.2. Uzantıları Hariç Tutarak Tarama 76
8.4. Karantina Alanı 79
8.4.1. Karantinaya Alınmış Dosyaları Yönetmek 79
8.4.2. Karantina Ayarlarını Yapılandırma 80

9. Gizlilik Kontrolü 82

9.1. Kişisel Gizlilik Durumu 82
9.1.1. Gizlilik Kontrolü 83
9.1.2. Antiphising Koruması 84
9.2. İleri Ayarlar – Kişisel Gizlilik Kontrolü 85
9.2.1. Kimlik Kurallarını Yaratmak 86
9.2.2. İstisnaları Belirleme 89
9.2.3. Kuralların Yönetimi 90
9.3. Gelişmiş Ayarlar – Kayıt Kontrolü 91
9.4. Gelişmiş Ayarlar - Cookie Kontrolü 93
9.4.1. Yapılandırma Sihirbazı 95

9.5. Gelişmiş Ayarlar - Script Kontrolü 97
9.5.1. Yapılandırma Sihirbazı 99
9.6. Sistem Bilgileri 100
9.7. Antiphishing Araç Çubuğu 101

10. Güncelleme 103
10.1. Otomatik Güncelleme 103
10.1.1. Güncelleme İsteği 105
10.1.2. Otomatik Güncellemeyi Kapatma 105
10.2. Güncelleme Ayarları 106
10.2.1. Güncelleme Yeri Ayarları 106
10.2.2. Otomatik Güncelleme Yapılandırma 107
10.2.3. Manuel Güncelleme Yapılandırma 108
10.2.4. Gelişmiş Ayarları Yapılandırma 108
10.2.5. Vekil Sunucuları Yönetmek 109

BitDefender Kurtarma CD'si 111

11. Tanıtma 112
11.1. Sistem Gereksinimleri 112
11.2. Dahil edilen Yazılımlar 113

12. BitDefender Kurtarma CD'si nasıl kullanılır. 116
12.1. BitDefender' ı Başlatmak 116
12.2. BitDefender Kurtarma CD'sini Durdur 117
12.3. Bir virüs koruma taraması nasıl yapabilirim? 118
12.4. BitDefender' ı bir vekil sunucu üzerinden nasıl güncelleştirebilirim? 119
12.5. Verilerimi nasıl kaydedebilirim? 120

Yardım Alma 122

13. Destek 123
13.1. BitDefender Bilgi Üssü 123
13.2. Yardım Almak 124
13.2.1. Web Selfservisine Gidin 124
13.2.2. Bir destek kaydı açın 124
13.3. İletişim Bilgileri 125
13.3.1. Web Adresleri 125
13.3.2. Şubeler 125

Sözlük 128

Lisans ve Garanti

BU ŞART VE KOŞULLARI KABUL ETMİYORSANIZ YAZILIMI YÜKLEMEYİNİZ. “KABUL EDİYORUM”, “TAMAM”, "DEVAM ET", “EVET”’İ SEÇEREK VEYA HERHANGİ BİR ŞEKİLDE YAZILIMI YÜKLEYEREK VEYA KULLANARAK, BU ANLAŞMANIN ŞARTLARINI TAMAMEN ANLADIĞINIZI VE KABUL ETTİĞİNİZİ BELİRTMİŞ OLUYORSUNUZ.

Bu Şartlar, satın alınan lisans veya herhangi bir ilgili hizmet anlaşması altında size teslim edilen ve dökümantasyonda veya bunların herhangi bir kopyasında tanımlanan uygulamaların ilgili dökümantasyonunu ve herhangi bir güncelleme ve yükseltmesini (upgrade) içeren, sizin için lisanslanmış olan, ev kullanıcıları için BitDefender Çözüm ve Hizmetlerini kapsamaktadır.

Bu Lisans Anlaşması, siz (gerçek veya tüzel kişi) ve BITDEFENDER arasında, bilgisayar yazılım ve hizmetlerini içeren, yukarıda tanımlı BITDEFENDER yazılım ürünlerinin kullanımı için yapılan yasal bir anlaşmadır ve tümü, uluslararası telif hakları kanunları ve uluslararası anlaşmalar tarafından korunan ilgili medya, basılı materyaller ve “çevrimiçi” veya elektronik dökümantasyonları (bundan sonra “BitDefender” olarak anılacaktır) içerebilir. BitDefender’ı yükleyerek, kopyalayarak veya kullanarak, bu anlaşma şartları ile bağlı olduğunuzu kabul etmiş oluyorsunuz.

Bu anlaşma şartlarını kabul etmiyorsanız, BitDefender’ı yüklemeyin veya kullanmayın.

BitDefender Lisansı. BitDefender, telif hakları kanunları ve uluslararası telif hakları anlaşmaları ve de diğer fikri mülkiyet hakları ve anlaşmaları ile korunmaktadır. BitDefender satılmamaktadır, sadece lisansı verilmektedir.

LİSANSIN VERİLMESİ. BITDEFENDER, BitDefender’ı kullanmak için, size ve sadece size aşağıdaki münhasır olmayan, sınırlı, devredilemez ve lisans ücretine tabi olan lisansı vermektedir.

UYGULAMA YAZILIMI. BitDefender’ı, toplam lisanslı kullanıcı sayısı sınırı altında kalma koşulu ile, gereken sayıdaki bilgisayara yükleyebilir ve kullanabilirsiniz. Yedekleme amacı ile bir ek kopya alabilirsiniz.

MASAÜSTÜ KULLANICI LİSANSI. Bu lisans, tek bir bilgisayara yüklenebilen ve ağ hizmetleri sağlamayan BitDefender yazılımı için geçerlidir. Her ana kullanıcı bu yazılımı tek bir bilgisayara yükleyebilir ve yedekleme amacıyla başka bir cihazda bir ek kopyasını alabilir. İzin verilen ana kullanıcı sayısı, lisans kullanıcı sayısıdır.

LİSANS SÜRESİ. Burada verilen lisans, BitDefender’ın satın alınma tarihinde başlayacak ve satın alınan lisansın süresinin sonunda sona erecektir.

LİSANS BİTİMİ. Ürün, lisans süresinin dolduğu andan itibaren işlevselliğini yitirecektir

YÜKSELTMELER (UPGRADE). BitDefender yükseltme olarak etiketlenmişse, BitDefender'ı kullanmak amacıyla yükseltilebilir olan ve BITDEFENDER tarafından tanımlanan bir ürünü kullanmak için uygun şekilde lisans almanız gerekmektedir. Yükseltme olarak etiketlenen bir BitDefender, yükseltme yapabilmenizin temelini oluşturan ürünün yerine geçer ve/veya onu tamamlar. Yükseltilmiş ürünü ancak bu Lisans Anlaşması şartlarına göre kullanabilirsiniz. BitDefender, tek bir ürün olarak lisansını aldığınız yazılım programları paketinin bir bileşeninin yükseltmesi ise, BitDefender yalnızca bu tek ürün paketinin bir parçası olarak kullanılabilir ve transfer edilebilir ve toplam lisanslı kullanıcı sayısından daha fazlasına ayrılamaz. Bu lisansın şart ve koşulları siz ve BITDEFENDER arasında asıl ürün veya yükseltme ürünlerle ilgili önceki tüm anlaşmaların yerine geçer.

TELİF HAKKI. BitDefender içindeki ve BitDefender'a ait tüm haklar, isimler ve BitDefender içindeki ve BitDefender'a ait tüm telif hakları (BitDefender içindeki herhangi bir resim, fotoğraf, logo, animasyon, video, ses, müzik, metin, ve "küçük uygulamalar" dahil olmak, fakat bunlarla sınırlı olmamak üzere), birlikte gelen basılı materyaller ve BitDefender kopyaları BITDEFENDER' a aittir. BitDefender telif hakları kanunları ve uluslararası anlaşma hükümleri tarafından korunmaktadır. Bu nedenle, BitDefender'ı herhangi diğer bir tescilli materyal gibi kullanmanız gerekmektedir. BitDefender ile birlkte gelen basılı materyalleri kopyalayamazsınız. BitDefender'ın bulunduğu medya veya yollardan hangisi tarafından yaratılmış olursa olsun, tüm kopyalardaki tüm telif hakkı uyarıları, asıl şekillerinde üretilecek ve dahil edilecektir. BitDefender lisansı kiralanamaz, satılamaz, paylaşılamaz veya alt lisans yoluyla başkasına verilemez. BitDefender kaynak kodunu bulmak için ters mühendislik, yeniden derleme, sökme, derivatif çalışmalar yapma, değiştirme, tercüme veya başka herhangi bir girişimde bulunamazsınız.

SINIRLI SORUMLULUK. BITDEFENDER, BitDefender'ın üzerinde dağıtıldığı medyada, medya'nın size teslim edildiği tarihten itibaren otuz günlük bir süre içinde hiç bir sorun olmayacağını garanti etmektedir. Bu garantinin ihlal edilmesi durumunda, tek çözüm şekli, BITDEFENDER' in, takdiri kendisinde olmak üzere, hasarlı medyanın alınmasından sonra bu medyayı değiştirmek veya BitDefender'a ödediğiniz ücretin size geri ödenmesi olacaktır. BITDEFENDER, BitDefender'ın hiç bozulmayacağını veya hatasız olduğunu veya hataların düzeltileceğini garanti etmemektedir. BITDEFENDER, BitDefender'ın sizin ihtiyaç ve gerekliliklerinizi karşılayacağını garanti etmemektedir.

BU ANLAŞMADA AÇIKÇA BELİRTİLMEDİĞİ SÜRECE, BITDEFENDER, ÜRÜNLER, GELİŞTİRMELER, BAKIM VEYA DESTEK VEYA DİĞER MATERYALLER (MADDİ VEYA MADDİ OLMAYAN) VEYA BITDEFENDER TARAFINDAN SAĞLANAN HİZMET İLE İLGİLİ, AÇIKÇA VEYA İMA YOLUYLA BELİRTİLMİŞ TÜM DİĞER GARANTİLERİ

KABUL ETMEMEKTEDİR. BITDEFENDER BURADA, TİCARİ SATIMA UYGUNLUK GARANTİLERİ, BELİRLİ BİR AMACA UYGUNLUK, TASARRUF HAKKI, MÜDAHALE ETMEME, VERİ DOĞRULUĞU, BİLGİ İÇERİĞİ DOĞRULUĞU, SİSTEM ENTEGRASYONU VE ÜÇÜNCÜ ŞAHIS YAZILIMLARINI, SPYWARE, ADWARE, COOKIE'LER, E-POSTALAR, DOKÜMANLAR, REKLAMLAR VEYA BENZER ÜRÜNLERİNİ FİLTRELEYEREK, ETKİSİZ KILARAK VEYA SİLEREK BU ÜÇÜNCÜ ŞAHISLARIN YASA, KANUN, ANLAŞMA, GELENEK VE UYGULAMA VEYA TİCARİ KULLANIM YOLUYLA KAZANILMIŞ HAKLARININ İHLAL EDİLMEMESİ GİBİ, FAKAT BUNLARLA SINIRLI KALMAMAK ÜZERE İMA EDİLMİŞ HERHANGİ BİR GARANTİYİ AÇIKÇA REDDETMEKTEDİR.

HASARLAR İÇİN YASAL UYARI. BitDefender'ı kullanan, test eden veya değerlendiren herkes, BitDefender kalitesi ve performansı ile ilgili tüm riskleri üzerine almaktadır. Hiç bir durumda, BitDefender'ın kullanımı, performansı veya teslimatı da dahil olmak, fakat bunlarla sınırlı olmamak üzere, doğrudan veya dolaylı olarak meydana gelen hiç bir zarar için, bu zararların varlığı veya ihtimali konusunda BITDEFENDER uyarılmış olsa dahi, BITDEFENDER' in hiç bir yükümlülüğü bulunmamaktadır. BAZI ÜLKELER KAZARA VEYA SONUÇSAL ZARARLAR İÇİN SORUMLULUK SINIRLANDIRILMASI VEYA HARİÇ TUTULMASINA İZİN VERMEMEKTEDİR. BU NEDENLE YUKARIDAKİ SINIRLANDIRMALAR VEYA İSTİSNAİ DURUMLAR SİZİN İÇİN GEÇERLİ OLMAYABİLİR. HİÇ BİR KOŞULDA, BITDEFENDER'IN YÜKÜMLÜLÜĞÜ, BITDEFENDER'IN SİZE SATILDIĞI FİYATI AŞAMAZ. Yukarıda belirtilen yasal uyarılar ve sınırlandırmalar, BitDefender'ı kullanmayı, değerlendirmeyi veya denemeyi kabul edip etmemeniz dikkate alınmaksızın geçerli olacaktır.

KULLANICILAR İÇİN ÖNEMLİ UYARILAR. BU YAZILIM HATA TOLERANSLI DEĞİLDİR VE HATASIZ PERFORMANS VEYA KULLANIM GEREKTİREN HERHANGİ BİR TEHLİKELİ ORTAMDAKİ KULLANIM İÇİN TASARLANMAMIŞ VE AMAÇLANMAMIŞTIR. BU YAZILIM, UÇAK NAVİGASYONU, NÜKLEER TESİSLER VEYA İLETİŞİM SİSTEMLERİ, SİLAH SİSTEMLERİ, DOĞRUDAN VEYA DOLAYLI HAYAT-DESTEK SİSTEMLERİ, HAVA TRAFİĞİ KONTROLÜ İŞLEMLERİNDE VEYA HATALARIN ÖLÜM, CİDDİ FİZİKSEL YARALANMA VEYA MÜLKE ZARAR VERME İLE SONUÇLANABİLECEĞİ UYGULAMA VE KURULUMLARDA KULLANILMAK ÜZERE TASARLANMAMIŞ VE AMAÇLANMAMIŞTIR.

GENEL. Bu Anlaşma Romanya kanunları ve uluslararası yönetmelik ve anlaşmalar tarafından yürütülecektir. Bu Lisans Şartlarından kaynaklanacak herhangi bir ihtilafın çözümünde münhasır yargı yetkisi Romanya mahkemelerine aittir.

BitDefender kullanım ücretleri ve maliyetleri, size önceden bildirimde bulunma şartı olmadan değişmeye tabidir.

Bu Anlaşmanın herhangi bir hükmünün geçersiz olması durumunda, bu geçersizlik, Anlaşmanın diğer hükümlerinin geçerliliğini etkilemeyecektir.

BitDefender ve BitDefender logoları BITDEFENDER'in ticari markalarıdır. Bu üründe ve ürünün ilgili materyallerinde kullanılan tüm diğer ticari markalar ilgili sahiplerinin mülkiyeti altındadır.

Bu şart ve koşulların herhangi birini ihlal etmeniz durumunda, önceden bildirimde bulunulmadan, lisansınız hemen iptal edilecektir. Lisansın iptal edilmesi durumunda BITDEFENDER veya diğer BitDefender satıcılarının hiç birinden herhangi bir geri ödeme alma hakkınız olmayacaktır. Gizlilik ve kullanım kısıtlamaları ile ilgili şart ve koşullar lisansın iptal edilmesinden sonra da geçerli olmaya devam edecektir.

BITDEFENDER bu şartları herhangi bir zamanda yenileyebilir ve yenilenen şartlar otomatik olarak, Yazılımın ilgili versiyonlarına uygulanacaktır. Bu Şartların herhangi bir kısmının geçersiz veya etkisiz olduğu anlaşılırsa, bu durum geri kalan Şartların geçerliliğini etkilemeyecek, bunlar geçerli ve yürülükte olmaya devam edeceklerdir.

Bu Şartların diğer dillere tercüme edilmesinde, tercümeler arasında tutarsızlık veya karşıtlık olması durumunda BITDEFENDER tarafından yayınlanan İngilizce sürümü geçerli olacaktır.

İrtibat: BITDEFENDER, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, veya Tel No: 40-21-2330780 veya Fax:40-21-2330763, e-posta adresi:office@bitdefender.com.

Önsöz

Bu kılavuz, **BitDefender Antivirus 2008**'i kişisel bilgisayarları için bir güvenlik çözümü olarak seçen tüm kullanıcılar için amaçlanmıştır. Bu kitapta sunulan bilgiler, yalnızca bilgisayar eğitimi almış kişiler için değil, aynı zamanda Windows altında çalışabilen herkes için uygundur.

Bu kitap size, **BitDefender Antivirus 2008**'u, bunu yaratan Şirket ve ekibini tanıtacak, kurulum sürecinde size rehberlik edecek ve nasıl yapılandırılacağını öğretecektir. **BitDefender Antivirus 2008**'un nasıl kullanılacağını, nasıl güncelleneceğini, test edileceğini ve kişiselleştirileceğini öğreneceksiniz. BitDefender'dan en iyi şekilde nasıl yararlanabileceğinizi öğreneceksiniz.

Size tatmin edici ve faydalı bir çalışma diliyoruz.

1. Bu Kitapta Kabul Edilen Yazım Kolaylıkları

1.1. Tipografik Kurallar

Kitapta, okumayı kolaylaştırması amacıyla bazı metin stilleri kullanılmıştır. Görünüşleri ve anlamları aşağıdaki tabloda açıklanmıştır.

Görünüş	*Açıklama*
`sample syntax`	Söz dizimi örnekleri `tek boşluklu` karakterler ile yazılmıştır
http://www.bitdefender.com	URL linki, http veya ftp sunucuları üzerindeki bazı dış lokasyonları işaret etmektedir.
support@bitdefender.com	E-posta adresleri, irtibat bilgisi olarak metin içine eklenmiştir.
"Önsöz" (shf. xi)	Bu, doküman içindeki bazı yerleri işaret eden dahili bir linktir.
`filename`	Dosya ve dizinler `tek boşluklu` font kullanılarak yazılmıştır.
option	Tüm ürün opsiyonları **koyu** karakterler ile yazılmıştır.

Görünüş	Açıklama
`sample code listing`	Kod listeleri `tek boşluklu` karakterler ile yazılmıştır.

1.2. Uyarılar

Uyarılar grafiklerle işaretlenmiş, mevcut paragraf ile ilgili ek bilgiye dikkatinizi çeken, metin içindeki notlardır.

Not
Not sadece kısa bir gözlemdir. Her ne kadar bunlar ihmal edilebilir olsa bile, notlar belirli bazı özellikler veya bazı ilgili başlıklara linkler gibi değerli bilgiler sağlayabilirler.

Önemli
Bunlara dikkat edilmesi gerekir ve bunların atlanması tavsye edilmemektedir. Genellikle çok kritik olmayan fakat önemli bilgiler sunmaktadırlar.

Uyarı
Çok dikkatli olarak ele almanız gereken kritik bilgilerdir. Bu uyarılara riayet ettiğinizde hiç bir kötü sonuç ortaya çıkmayacaktır. Bunları okumalı ve anlamalısınız, çünkü oldukça riskli olan şeyleri açıklamaktadırlar.

2. Kitabın Yapısı

Bu kitap birbirinden farklı birkaç ana başlıktan meydana gelmektedir. Ayrıca teknik terimleri anlayabilmek için açıklayıcı bir sözlük bulunmaktadır.

Kurulum Adımları. BitDefender'ın bir çalışma istasyonuna kurulması için gerekli olan talimatları adım adım verir. **BitDefender Antivirus 2008**'nun yüklenmesini anlatan kapsamlı bir derstir. Başarılı bir kurulum için gerekli ön koşullardan başlanarak, tüm kurulum süreci boyunca yönlendirilirsiniz. Son olarak, BitDefender'ı silmenizin gerekmesi halinde uygulamak üzere, silme prosedürü anlatılmaktadır.

Temel Yönetim. BitDefender temel yönetim ve bakım açıklamaları.

Gelişmiş Güvenlik Yönetimi. Güvenlik kapasitesinin detaylı bir sunumu BitDefender tarafından sağlanıyor. Gelişmiş ayarlar konsolunun tüm seçeneklerini ayrıntılı bir şekilde açıklayan bölümler. BitDefender, bilgisayarınızı her türlü kötücül yazılıma karşı korur (virüsler, Truva atları, spywareler, rootkitler gibi)

BitDefender Kurtarma CD'si. BitDefender Kurtarma CD'si anlatımı. Başlangıç CD'si ile sunulan özellikleri anlamanıza ve kullanmanıza yardım eder.

Yardım Alma. Beklenmeyen herhangi bir şey olduğunda nereye bakmanız gerektiği ve nasıl yardım isteyeceğinizi anlatır.

Sözlük. Sözlük, bu döküman sayfalarında rastlayabileceğiniz bazı teknik ve pek olağan olmayan terimleri açıklamaya çalışmaktadır.

3. Yorumlarınız

Bu kitabı daha da geliştirmek için sizden yorumlarınızı bekliyoruz. Tüm bilgileri yapabileceğimizin en iyisi düzeyinde test ettik ve doğruladık. Bu kitapta bulduğunuz herhangi bir sorunu ve bunun nasıl düzeltilebileceği ile ilgili fikrinizi bize iletmek ve mümkün olan en iyi dökümantasyonu size sunabilmek için lütfen bize yazın.

Yorumlarınızı lütfen documentation@bitdefender.com adresine e-posta yoluyla gönderin.

Önemli
Dökümantasyon ile ilgili e-postalarınızı daha etkin ve hızlı olarak değerlendirebilmemiz için lütfen İngilizce dilinde gönderin.

Kurulum Adımları

1. BitDefender Antivirus 2008 Kurulumu

Bu kullanım kılavuzunun **BitDefender Antivirus 2008 Kurulumu** bölümü aşağıdaki bölümlerden oluşmaktadır:

- Sistem Gereksinimleri
- Kurulum Adımları
- Başlangıç Kurulum Sihirbazı
- Yükseltme
- BitDefender'ı Düzeltme veya Kaldırma

1.1. Sistem Gereksinimleri

Ürünün doğru şekilde çalıştığından emin olmak için, kurulumdan önce, aşağıdaki sistem gerekliliklerinin sağlandığını doğrulayın:

- İşletim platformu: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (veya üstü)

Windows 2000

- 800 MHz işlemci veya üzeri
- Minimum 256 MB RAM Bellek (512 MB tavsiye edilmektedir)
- Minimum 60 MB boş sabit disk alanı

Windows XP

- 800 MHz işlemci veya üzeri
- Minimum 256 MB RAM Bellek (1 GB tavsiye edilmektedir)
- Minimum 60 MB boş sabit disk alanı

Microsoft Windows Vista

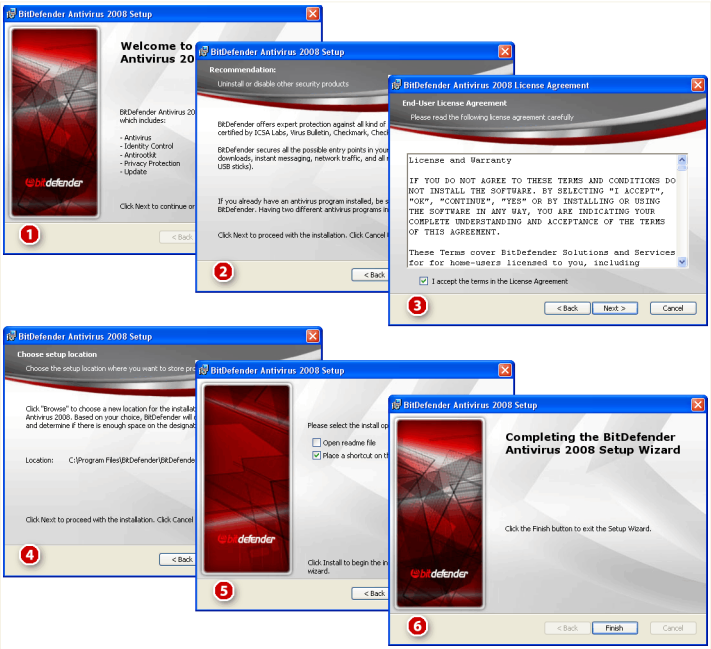
- 800 MHz işlemci veya üzeri
- Minimum 512 MB RAM Bellek (1 GB tavsiye edilmektedir)
- Minimum 60 MB boş sabit disk alanı

BitDefender Antivirus 2008'i değerlendirmek amacıyla, veri güvenliği ile ilgili olarak hazırlanan BitDefender kurumsal web sitesini http://www.bitdefender.com dan ziyaret edebilirsiniz.

1.2. Kurulum Adımları

Kurulum dosyası üzerine çift tıklayın. Bu, sizi kurulum süreci boyunca yönlendirecek olan bir sihirbazı başlatacaktır.

Kurulum sihirbazını çalıştırmadan önce, BitDefender yeni sürümleri kontrol edecek. Daha yeni bir sürüm var ise onu indirmeniz için sizi yönlendirecek. Tıklayın **Evet** yeni versiyonu indirin ya da **Hayır**Yüklemeye devam edin.



Kurulum Adımları

BitDefender Antivirus 2008' i yüklemek için bu adımları takip edin:

1. Devam etmek için **İleri**'yi veya kurulumdan çıkmak için **İptal**'i tıklayın.

2. **İleri**'yi tıklayın.

   BitDefender Antivirus 2008, bilgisayarınızda yüklü olan başka virüs koruma ürünleri olduğunda sizi uyaracaktır. Benzer ürünü kaldırmak için**Kaldır**'ı tıklayın. Bulunan ürünü kaldırmadan devam etmek için **İleri**'yi tıklayınız.

   Uyarı
   BitDefender'ı yüklemeden önce, tespit edilen diğer virüs koruma programlarının kaldırılması önemle tavsiye edilmektedir. Bilgisayar üzerinde aynı zamanda iki veya daha fazla virüs koruma ürününün çalıştırılması genellikle sistemi kullanılamaz hale getirmektedir.

3. Lütfen Lisans Anlaşmasını okuyun, **Lisans Anlaşmasındaki şartları kabul ediyorum**'u seçin ve **İleri**'yi tıklayın. Bu şartları kabul etmiyorsanız **İptal**'i tıklayın. Bu durumda kurulum süreci iptal edilecek ve kurulumdan çıkacaksınız.
4. Ürünü yüklemek istediğiniz klasörü seçebilirsiniz. Varsayılan klasör:`C:\Program Files\BitDefender\BitDefender 2008`. Başka bir klasör seçmek istiyorsanız, **Gözat**'a tıklayın ve açılan pencerede BitDefender Antivirus 2008'i yüklemek istediğiniz klasörü seçin. **İleri**'yi tıklayın.

   İleri'yi tıklayın.
5. Yükleme işleminin seçeneklerini belirleyin. Varsayılan olarak seçili iki seçenek bulunmaktadır:
   - **Beni oku dosyasını aç** – kurulum sonunda beni oku dosyasını açmak için.
   - **Masaüstünde kısayol oluştur** – kurulum sonunda masa üstünüzde BitDefender Antivirus 2008 kısayolunu oluşturmak için.
   - **Kurulum bittiğinde CD'yi çıkart** - Kurulum bitince CD çıkacaktır; bu seçenek CD den kurulum yapıldığında görünür.
   - **Windows Defenderi kapat** - Windows Defenderi kapatmak için; bu seçenek sadece Windows Vista'da ortaya çıkar.

   Ürünün kurulumunu başlatmak için **Yükle**'yi tıklayın.

   Önemli
   Kurulum sürecinde bir sihirbaz ortaya çıkacaktır. Sihirbaz **BitDefender Antivirus 2008**'unuzu kaydettirmenizde,BitDefender hesabı açmanızda ve önemli güvenlik işlemlerini gerçekleştirmek için BitDefender'ı ayarlamanızda size yardım edecektir. Bir sonraki adıma geçmek için sihirbaz destekli süreci tamamlayın.

6. **Bitir** seçeneğini tıklayın. Kurulum sihirbazının kurulum sürecinin tamamlayabilmesi için sistemi yeniden başlatmanız istenebilir. Bu opsiyonu seçili bırakmanızı tavsiye ediyoruz

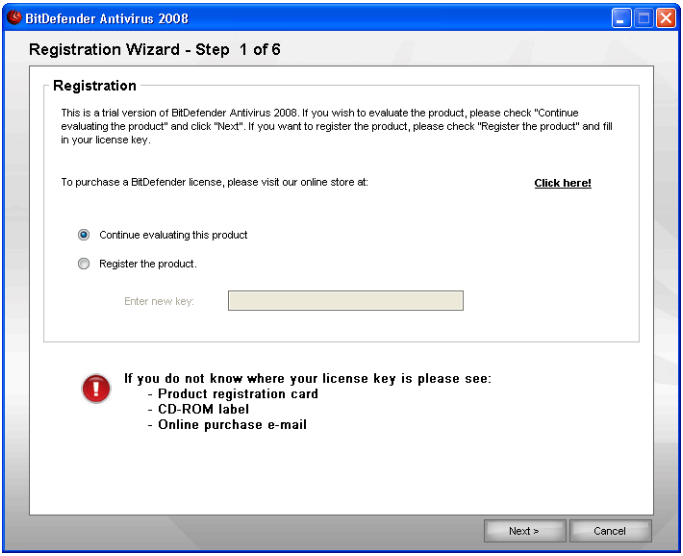
Ürün kurulumunu tamamlamak için **Bitir**'i tıklayın. Kurulumda varsayılan ayarları kabul ettiyseniz, `Program Files`'ta `BitDefender` adında yeni bir klasör yaratılacak ve burada `BitDefender 2008` alt klasörü bulunacaktır.

1.3. Başlangıç Kurulum Sihirbazı

Kurulum sürecinde bir sihirbaz ortaya çıkacaktır. Sihirbaz **BitDefender Antivirus 2008**'inizi kaydettirmenizde, bir BitDefender hesabı açmanızda ve önemli güvenlik işlemlerini gerçekleştirmek için BitDefender'ı ayarlamanızda size yardım edecektir.

Bu sihirbaz işlemini tamamlamak zorunlu değildir; ancak, zaman kazanmak ve BitDefender Antivirus 2008 kurulmadan önce sistemin güvenli olduğundan emin olmak için yapılmasını tavsiye ediyoruz.

1.3.1. Adım 1/6 - BitDefender Antivirus 2008' i Kaydedin



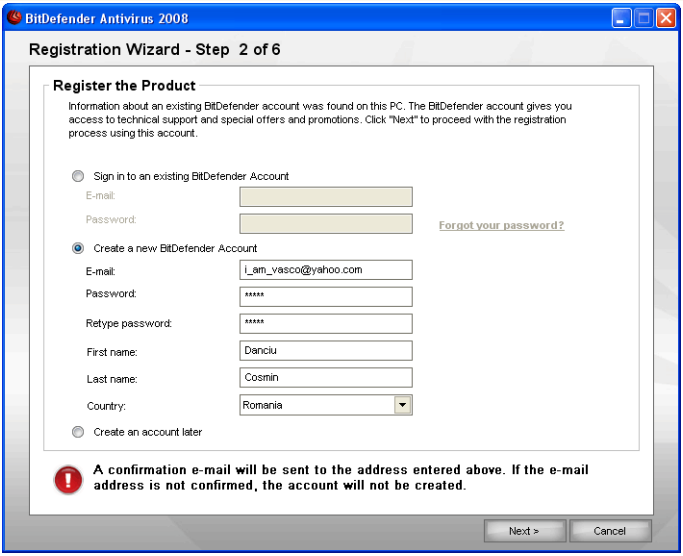
Kayıt

BitDefender Antivirus 2008'i kaydetmek için **Ürünü kaydet** seçeneğini seçin. **Yeni anahtarı gir** alanına lisans anahtarını yazın.

Ürünü denemeye devam etmek için **Ürünü denemeye devam et**'i seçin.

İleri'yi tıklayın.

1.3.2. Adım 2/6 BitDefender Hesabının Açılması



Hesap Yaratma

BitDefender hesabım yok

BitDefender'ın teknik destek ve diğer ücretsiz hizmetlerinden yararlanabilmek için bir hesap açtırmanız gerekmektedir.

Not
BitDefender hesabınızı daha sonra yaratmak istiyorsanız uygun seçeneği seçiniz.

BitDefender hesabı açmak için **BitDefender Hesabı Yarat** seçeneğini seçip, gerekli alanları doldurun. Internet bağlantısı gereklidir. Burada sağlayacağınız bilgiler gizli kalacaktır.

- **E-mail** – Email adresinizi girin.
- **Şifresi** – daha önce tanımlanan kullanıcı için geçerli bir şifre girin.

Not
Şifre en az dört karakter uzunluğunda olmalıdır.

- **Şifreyi Tekrar Gir** – daha önce tanımlanan kullanıcı için geçerli bir şifreyi tekrar girin.
- **Ad** – Adınızı girin.
- **Soyad** – Soyadınızı girin.
- **Ülke** – Ülke adını seçin.

Not
E-mail adresinizi ve şifrenizi kullanarak http://myaccount.bitdefender.com hesabınıza girin.

Hesabınızın açılmasını gerçekleştirmek için önce e-posta adresinizi aktif hale getirmeniz gerekmektedir. e-posta adresinizi kontrol edin ve BitDefender kayıt hizmetleri tarafından size gönderilen e-postadaki talimatları uygulayın.

Devam etmek için **İleri**'yi tıklayın.

BitDefender hesabım var

Eğer daha önceden bilgisayarınızda bir hesabınız varsa, BitDefender bunu otomatik olarak algılayacaktır. Bu pencereyi kapatmak istiyorsanız,**İleri**' ı tıklayınız.

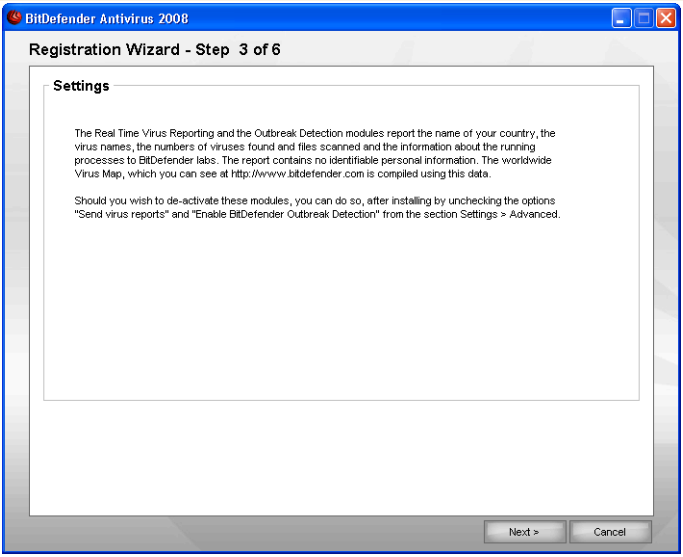
Zaten bir BitDefender hesabınız varsa, **BitDefender Hesabınıza girin** Hesabınız e-posta adresiniz ve hesap şifrenizden oluşur.

Not
Yanlış bir şifre girerseniz, **İleri** tıkladığınızda şifreyi yeniden yazmanız istenecektir. Yeniden şifre girmek için **İleri** seçeneğine tıklayın. Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

Şifrenizi unuttuysanız, **Şifremi unuttum**'u tıklayın ve talimatları uygulayın.

Devam etmek için **İleri**'yi tıklayın.

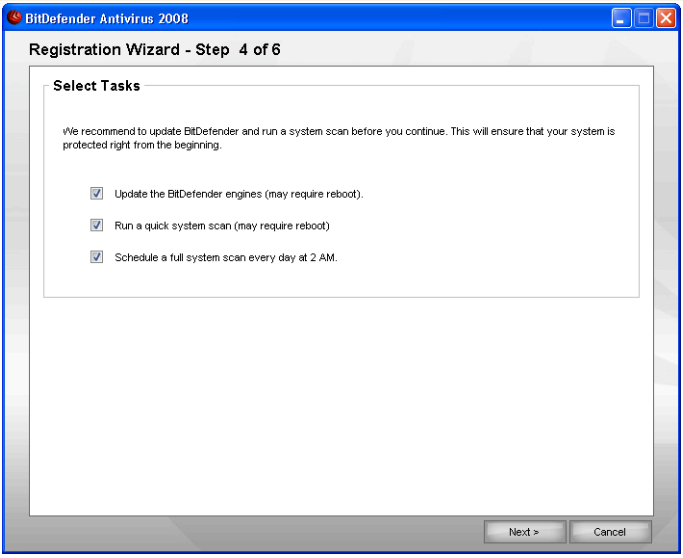
1.3.3. Adım 3/6 – RTVR Hakkında Bilgi



RTVR Bilgisi

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

1.3.4. Adım 4/6 – Çalıştırılacak Görevlerin Seçilmesi



Görev Seçimi

Sisteminizin güvenliği için gerekli olan önemli görevleri gerçekleştirmek üzere BitDefender Antivirus 2008'i ayarlayın.

Aşağıdaki seçenekler mevcuttur:

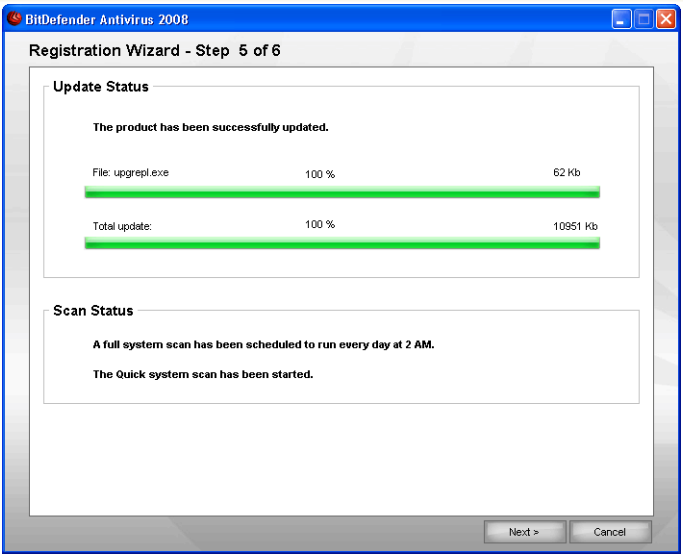
- **BitDefender motorlarını (yeniden başlatma gerekebilir) güncelle** -Bir sonraki adımda, en son tehditlere karşı bilgisayarınızı korumak için BitDefender motorlarının güncellenmesi
- **Hızlı bir sistem tarama gerçekleştirin (yeniden başlatma gerekebilir)** – bir sonraki adımda, BitDefender Antivirus 2008`Windows` ve `Program Files` klasörlerinin etkilenmemesini sağlaması için hızlı bir sistem taraması yapılacaktır.
- **Hergün saat 02:00'de tam sistem taraması gerçekleştir** - hergün saat 02:00'de tam bir sistem taraması gerçekleştirir.

Önemli
Sistemin güvenliğini sağlamanız için bir sonraki adıma geçmeden önce bu seçenekleri etkin kılmanızı tavsiye ediyoruz.

Sadece son seçeneği seçtiyseniz ya da hiç birini seçmediyseniz, bir sonraki adım atlanacaktır.

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

1.3.5. Adım 5/6 – Görevlerin Tamamlanmasını Bekleyin

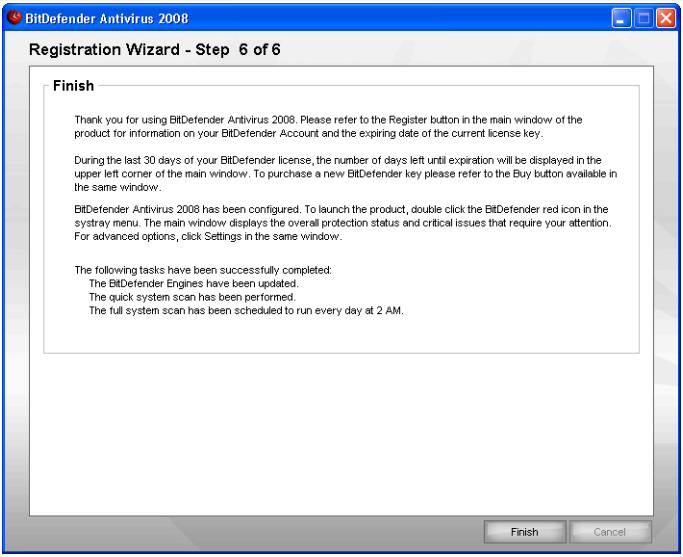


Görev Durumu

Görev(ler)in tamamlanmasını bekleyin. Önceki adımda seçilen görev(ler)in durumunu görebilirsiniz.

Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

1.3.6. Adım 6/6 – Özet



Bitir

Bu, yapılandırma sihirbazının en son adımıdır.

Sihirbazı tamamlamak için **Bitir**'i tıklayarak kurulum sürecine devam edin.

1.4. Yükseltme

Yükseltme işlemi aşağıdaki şekillerde yapılabilir:

- **Önceki sürümü kaldırmadan yüklemek - v8 veya üzeri için, Internet Security hariç**

  Kurulus dosyasına çift tıklayın ve sihirbazı "*Kurulum Adımları*" (shf. 3) bölümündeki gibi takip edin.

Önemli

Kurulum işlemi sırasında `Filespy servisi` tarafından oluşan bir hata görünecektir. **Tamam**'a tıklayarak kuruluma devam edin.

- **Önceki sürümü kaldırın ve yeni sürümü yükleyin – tüm BitDefender sürümleri için**

  Önce eski sürümü kaldırmanız gerekmektedir, daha sonra, bilgisayarı yeniden başlatın ve yeni sürümü "*Kurulum Adımları*" (shf. 3) bölümünde anlatıldığı şekilde yükleyin.

Önemli
BitDefender v8 veya daha üst bir yazılımdan yükseltme yapıyorsanız, BitDefender ayarlarınızı, arkadaşlar listenizi ve Spam'ciler listenizi kaydetmenizi tavsiye ediyoruz. Yükseltme işlemi tamamlandıktan sonra, bunları yükleyebilirsiniz.

1.5. BitDefender Özelliklerini Düzeltme veya Kaldırma

BitDefender Antivirus 2008' i kaldırmak, yenilemek, düzenlemek isterseniz aşağıdaki adımları takip ediniz. **Başlat** → **Programlar** → **BitDefender 2008** → **Düzelt veya Kaldır**.

İleri seçeneğine tıklayarak seçiminizi onaylamanız istenecektir. Seçim yapabileceğiniz yeni bir pencere açılacaktır

- **Onar** - yüklenmiş olan tüm program bileşenlerini yeniden yüklemek için

  BitDefender'ı onarmayı seçtiğinizde, yeni bir pencere açılacaktır. Onarma işlemine başlamak için**Onar'**ı tıklayınız .

  Bilgisayarınız yeniden başladıktan sonra **Yükle**' ye basarak BitDefender Antivirus 2008' i yeniden yükleyebilirsiniz.

  Yükleme işlemi biter bitmez yeni bir pencere açılacak. **Bitir** seçeneğini tıklayın.
- **Kaldır**- tüm yüklü bileşenleri kaldırmak için

Not
Temiz bir yeniden kurulum için öncelikle **Kaldır**' a basarak tüm yüklü bileşenleri kaldırmanızı öneririz.

BitDefender'ı kaldırmayı seçtiğinizde, yeni bir pencere açılacaktır:

Önemli

BitDefender' i kaldırdığınızda virüsler ve spywareler gibi kötücül yazılım tehditlerine karşı bir korumanız kalmayacak. BitDefender' ı kaldırma işleminden sonra Windows

Defender' in aktif olmasını istiyorsanız, uygun kutucuğu işaretleyiniz. Bu seçenek sadece Windows Vista için geçerlidir.

KaldırBitDefender Antivirus 2008' i bilgisayarınızdan kaldırır.

Kaldırma işlemi sırasında bize izlenimlerinizi aktarmanız istenecektir. **Tamam'** a tıklayarak 5 kısa soruya yanıt verin. Sorulara cevap vermek istemiyorsanız, sihirbazdan çıkmak için **Bitir**'i tıklayın.

Kaldırma işlemi tamamlandığında, yeni bir pencere açılacaktır: **Bitir** seçeneğini tıklayın.

Not
Kaldırma işlemi tamamlandıktan sonra,`BitDefender`klasörünü `Program Dosyaları`'ndan silmenizi tavsiye ediyoruz.

BitDefender kaldırma işlemi sırasında bir hata oluştu

BitDefender kaldırma işlemi sırasında bir hata oluşursa, işlem iptal edilecek ve yeni bir pencere açılacak. **Kaldırma Aracı'** nı çalıştırarak BitDefender' in tamamıyla kaldırıldığından emin olabilirsiniz. Kaldırma aracı, otomatik kaldırma işlemi sırasında kaldırılamayan tüm dosyaları ve kayıt defteri kayıtlarını kaldıracaktır.

Temel Yönetim

2. Başlangıç

BitDefender bilgisayarınıza yüklendikten hemen sonra korumaya başlar. BitDefender Güvenli Merkezi' ni açarak sistem güvenlik durumunu kontrol edebilir, önleyici tedbirle alabilir ya da ürünü tam olarak konfigüre edebilirsiniz.

Yönetim konsoluna ulaşmak için Windows Başlat menüsünü kullanarak sırasıyla **Başlat** → **Programlar** → **BitDefender 2008** → **BitDefender Antivirus 2008**'u seçin veya sistem tepsisinden **BitDefender ikonuna** çift tıklayarak daha çabuk bir şekilde erişin.

BitDefender Güvenlik Merkezi

BitDefender Güvenlik Merkezi iki alan içerir:

- **Durum** alanı: Bilgisayarınızdaki güvenlik açıklarını giderme konusunda size yardımcı bilgiler verir. Kırmızı alanlara tıklayarak bilgisayarınızı etkileyen faktörleri kolayca görebilirsiniz. **Tüm Sorunları Düzelt** butonu bilgisayarınızın kırılganlık noktalarını düzeltecektir, ya da size nasıl kolayca çözebileceğiniz konusunda yardımcı olacaktır. Aynı zamanda, 4 ayrı güvenlik kategorisi için 4 ayrı buton bulunur. Yeşil durumdaki

butonlar herhangi bir risk olmadığını gösterirken, Sarı ve Kırmızı durumdaki butonlar, orta ve yüksek güvenlik risklerini gösterir. Bunları düzeltmek için Sarı/Kırmızı butonlara tıkladıktan sonra, **Düzelt'** e tıklayarak birer birer düzeltebilir veya **Hepsini Düzelt'** e tıklayabilirsiniz. Gri olanlar ise henüz konfigüre edilmemiş bileşenleri ifade eder.

- **Hızlı Görevler** alanı: Size sisteminizi güvende tutma ve verilerinizi koruma konusunda yardımcı olur.

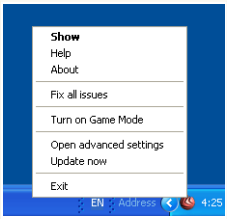
Ayrıca, BitDefender Güvenlik Merkezi bir takım kullanışlı kısayollar içerir.

Link	*Açıklama*
Satın Al	Ürünü satın alabileceğiniz bir sayfa açar
Hesabım	BitDefender hesap sayfanızı açar.
Kayıt	Kayıt Sihirbazını çalıştırır.
Yardım	Yardım dosyalarını açar.
Destek	BitDefender destek web sayfasını açar.
Ayarlar	Gelişmiş ayarlar konsolunu açar.
Geçmiş	Geçmiş ve Olay günlüğü penceresini açar.

2.1. Sistem Tepsisindeki Bitdefender İkonu

Sistem Tepsisindeki Bitdefender İkonu' nu kullanarak tüm ürünleri hızlı bir şekilde yönetebilirsiniz.

Bu ikona çift tıkladığınızda, yönetim konsolu açılacaktır. Ayrıca sağ tıkladığınızda bağlamsal bir menü görülecektir. Bu, BitDefender'ın hızlı yönetimini sağlamaktadır.



Bitdefender İkonu

- **Göster** - BitDefender Güvenlik Merkezi' ni açar.
- **Yardım** - yardım dosyasını açar.
- **Hakkında** - BitDefender web sayfasını açar.
- **Tüm sorunları düzelt** - Güvenlik açıklarını gidermede yardımcı olur
- **Oyun Modu aç / kapat** Oyun Modu aç / kapat.
- **Gelişmiş ayarlar** – Gelişmiş ayarlar konsoluna erişimi sağlar.
- **Şimdi güncelle** – anında güncelleme gerçekleştirir. Güncelleme durumunu görebileceğiniz bir pencere açılacak.

■ **Çıkış** - Uygulamayı kapatır.

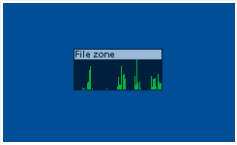
Oyun modu aktifken, BitDefender ikonu'nun üzerinde G harfini görebilirsiniz.

Eğer sistem güvenliğini etkileyen kritik bir durum varsa BitDefender ikonu'nun üzerinde bir ünlem işareti görünür. Sistem güvenliğinizi etkileyen sorunun adedini farenizi ikon'un üzerinde tutarak görebilirsiniz.

2.2. Tarama Etkinlik Çubuğu

Tarama etkinlik çubuğu, sisteminizdeki tarama etkinliğinin grafiksel olarak gösterimidir

Yeşil çubuklar (**Dosya Bölgesi**) 0 ila 50 aralığında, saniyede taranan dosya sayısını gösterir



Etkinlik Çubuğu

Not
Tarama etkinlik çubuğu, **Dosya Bölgesi** üzerinde kırmızı çarpı işareti varsa size gerçek zamanlı korumanın kapalı olduğunu gösterecektir..

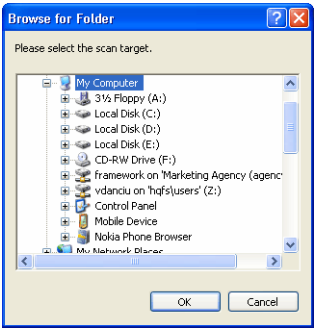
Tarama etkinlik çubuğu' nu objeleri taramak için kullanabilirsiniz. Taramak istediğiniz objeyi çubuk üzerine sürükleyip bıraktığınız taktirde taranmış olacaktır. Daha fazla bilgi için bakınız,"*Sürükle&Bırak Taraması*" (shf. 64)

Grafik gösterimini daha fazla görmek istemiyorsanız, sadece sağ tıklayarak **Gizle** seçeneğini seçin.

2.3. BitDefender Manuel Tarama

Belirli bir klasörü hızlı şekilde taramak istiyorsanız, BitDefender Manuel Tarama' yı kullanabilirsiniz.

BitDefender Manuel Tarama Menüsüne erişmek için Windows Başlat menüsüne giderek takip eden adımları izleyebilirsiniz. **Başlat** → **Programlar** → **BitDefender 2008** → **BitDefender Manuel Tarama** Sıradaki pencere çıkacaktır:



BitDefender Manuel Tarama

Tüm klasörleriniz görüntülenecektir. Taramak istediğiniz klasörü seçip, **Tamam'** a basın. BitDefender Tarayıcısıaçılacak ve size tarama sürecinde rehberlik yapacaktır.

2.4. Oyun Modu

Yeni Oyun Modu geçici olarak koruma ayarlarını değiştirerek, sistem performansının en az düzeyde etkilenmesini sağlar. Oyun Modunu açtığınızda, aşağıdaki ayarlar uygulanır:

- Tüm BitDefender alarmları ve pop-upları kapatılır.
- BitDefender gerçek zamanlı koruma düzeyi **İsteğe Bağlı Düzey**'e iner

Oyun modu aktifken, BitDefender ikonu'nun üzerinde `G` harfini görebilirsiniz.

2.4.1. Oyun Modunu Kullanmak

Oyun Modunu açmak istiyorsanız, aşağıdaki metodlardan birini kullanınız.

- Sistem tepsisinden BitDefender ikonunu sağ-tıklayın ve **Oyun Modunu Aç**'ı seçin.
- `Alt+G` (Kısayol Tuşu) tuşlarına basınız.

Önemli
Oyun Modunu kapatmayı unutmayın. Açtığınız metodlarla kapatabilirsiniz.

2.4.2. Oyun Modu kısayol tuşunu değiştir

Kısayol tuşunu değiştirmek istiyorsanız, adımları takip edin:

1. BitDefender Güvenlik Merkezindeki ayarlar konsolundan**Ayarlar'** ı tıklayın.

Not
Veya Sistem tepsisinden BitDefender ikonunu sağ-tıklayın ve **Gelişmiş ayarları aç**'ı seçin.

2. **Gelişmiş**'i tıklayın.
3. **Oyun modu için kısayol tuşu**seçeneğinden istediğiniz tuşu atayabilirsiniz:
   - Kısayol tuşunu kullanımınıza göre atayabilirsiniz. Control tuşu (`Ctrl`), Shift tuşu (`Shift`) veya Alternatif tuş (`Alt`).
   - Düzenleme sahasında, istediğiniz herhangi bir harfi kısayol olarak atayabilirsiniz.

   Örnek olarak `Ctrl+Alt+D` kutucukları işaretleyin`Ctrl` ve`Alt` ve `D`yazın.

Not
Kutucuklardaki işaretleri kaldırırsanız **Oyun Modu için kısayol tuşu** Kısayol tuşu kapatılacaktır.

3. Güvenlik Durumu

Güvenlik durumu, bilgisayarınızdaki güvenlik açıklarını düzenli ve kolay yönetilebilir bir liste halinde sistematik olarak size gösterir. BitDefender Antivirus 2008 bilgisayar güvenliği etkilendiğinde size haber berecektir.

Dört güvenlik durumu butonu bulunmaktadır:

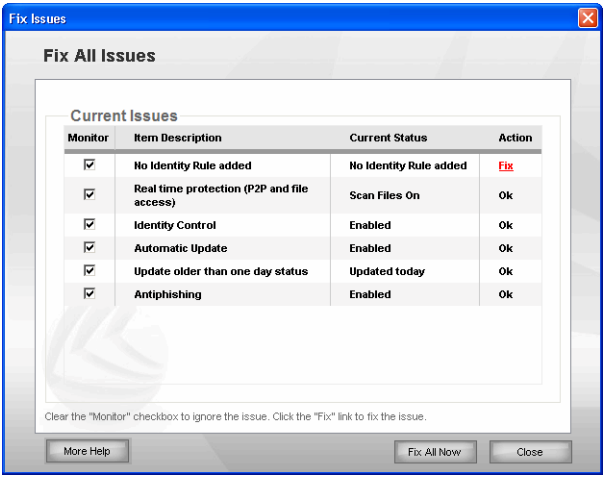
- **ANTIVIRUS**
- **ANTIPHISING**
- **KİMLİK KONTROLÜ**
- **GÜNCELLEME**

Aynı zamanda sol tarafta sisteminizi etkileyen sorunlar ve**Tüm Sorunları Gider**butonunu görebilirsiniz.

Durum butonları o andaki koruma düzeyine bağlı olarak, yeşil, sarı, kırmızı ve gri renkte görünebilirler.

- **Yeşil**Bilgisayarınız için düşük dereceli güvenlik riski.
- **Sarı**Bilgisayarınız için orta dereceli güvenlik riski.
- **Kırmızı**Bilgisayarınız için yüksek dereceli güvenlik riski.
- **Gri**Konfigüre edilmemiş bileşen.

Güvenlik problemlerini çözmeniz için sadece **Tüm Sorunları Gider**butonuna tek dokunuş yapmanız yeterli. Yeni bir pencere çıkacaktır.



Güvenlik Sorunu

Güvenlik sorunlarını ve kısa açıklamalarını bir liste halinde göreceksiniz.

Sadece belirli sorunları düzeltmek için uygun olan **Düzelt**butonuna basın. Eğer sorunların hepsini düzeltmek istiyorsanız, **Tümünü Düzelt** butonuna basabilirsiniz.

Ek yardıma ihtiyacınız varsa**Daha Çok Yardım** linkine tıklayın. Bağlamsal yardım sayfası, bu sorunları nasıl çözeceğiniz hakkında size ayrıntılı bilgileri görüntüler.

Önemli
Her soruna ait kutucuk varsayılan olarak işaretli gelecektir. Eğer belirli sorunların güvenlik risk düzeyi belirlenirken dikkate alınmasını istemiyorsanız, kutucuktaki işareti kaldırabilirsiniz. Lütfen bu seçeneği dikkatli kullanın, bilgisayarınız artan güvenlik risklerine maruz kalabilir.

Sorunları daha sonra düzeltmek istiyorsanız, **Kapat'** a basın.

3.1. Antivirüs Durumu Butonu

Antivirüs durum butonu yeşil ise endişe etmeye gerek yok. Eğer sarı, kırmızı veya gri ise bilgisayarınız orta veya yüksek güvenlik riskleri ile karşı karşıya olabilir.

Durum butonlarının renkleri, sadece siz güvenlik ayarlarını konfigüre ettiğinizde değişmeyebilir. Örnel olarak, son sistem tarama tarihi eski ise sarıya, çok eski ise kırmızıya dönecektir.

Aşağıdaki tablo, güvenlik risk düzeyi belirlenirken hangi elementlerin dikkate alındığı hakkında size bilgi verecektir.

Sorun	Renk
Son sistem tarama tarihi eski	Sarı
Son sistem tarama tarihi çok eski	Kırmızı
Gerçek-zamanlı koruma kapalı	Kırmızı
Antivirüs koruma düzeyi isteğe göre ayarlanmış	Sarı

Sorunları düzeltmek için bu adımları takip edin:

1. Antivirüs durum butonuna basın.
2. Tek tek düzeltmek için**Düzelt** butonuna basın, veya hepsini düzeltmek için **Hepsini Düzelt** butonuna basın.
3. Eğer herhangi bir sorun düzelmiyor ise sihirbazı takip ederek düzeltin.

3.2. Antiphising Durum Butonu

Antiphising durum butonu yeşil ise endişe etmeye gerek yok. Eğer kırmızı ise bilgisayarınız yüksek güvenlik riskleri ile karşı karşıya olabilir.

Aşağıdaki tablo, güvenlik risk düzeyi belirlenirken hangi elementlerin dikkate alındığı hakkında size bilgi verecektir.

Sorun	Renk
Antiphising koruması açık	Yeşil
Antiphising koruması kapalı	Kırmızı

Sorunları düzeltmek için bu adımları takip edin:

1. Antiphising durumu butonuna basın
2. Tek tek düzeltmek için**Düzelt** butonuna basın, veya hepsini düzeltmek için **Hepsini Düzelt** butonuna basın.
3. Eğer herhangi bir sorun düzelmiyor ise sihirbazı takip ederek düzeltin.

3.3. Kimlik Kontrolü Durum Butonu

Kimlik kontrolü durum butonu yeşil ise endişe etmeye gerek yok. Eğer kırmızı veya gri ise bilgisayarınız yüksek güvenlik riskleri ile karşı karşıya olabilir.

Aşağıdaki tablo, güvenlik risk düzeyi belirlenirken hangi elementlerin dikkate alındığı hakkında size bilgi verecektir.

Sorun	Renk
Kişisel Gizlilik koruması açık	Yeşil
Kişisel Gizlilik koruması kapalı	Kırmızı
Kişisel Gizlilik koruması ayarlanmadı	Gri

Sorunları düzeltmek için bu adımları takip edin:

1. Kimlik Durumu butonuna basın.
2. Tek tek düzeltmek için**Düzelt** butonuna basın, veya hepsini düzeltmek için **Hepsini Düzelt** butonuna basın.
3. Eğer herhangi bir sorun düzelmiyor ise sihirbazı takip ederek düzeltin.

3.4. Güncelleme Durumu Butonu

Güncelleme durum butonu yeşil ise endişe etmeye gerek yok. Eğer kırmızı ise bilgisayarınız yüksek güvenlik riskleri ile karşı karşıya olabilir.

Aşağıdaki tablo, güvenlik risk düzeyi belirlenirken hangi elementlerin dikkate alındığı hakkında size bilgi verecektir.

Sorun	Renk
Otomatik Güncelleme Açık	Yeşil
Otomatik Güncelleme Kapalı	Kırmızı
Son güncelleme tarihi eski	Kırmızı

Sorunları düzeltmek için bu adımları takip edin:

1. Güncelleme Durumu butonuna basın.
2. Tek tek düzeltmek için**Düzelt** butonuna basın, veya hepsini düzeltmek için **Hepsini Düzelt** butonuna basın.

3. Eğer herhangi bir sorun düzelmiyor ise sihirbazı takip ederek düzeltin.

4. Hızlı Görevler

Hızlı Görevleralanı altında 4 durum butonu bulunmaktadır.

4.1. Güvenlik

BitDefender, güncel ve bilgisayarınızın virüssüz kalabilmesi amacıyla bir Güvenlik Modülü ile birlikte gelir.

Güvenlik modülüne girmek için, **Güvenlik** sekmesine tıklayın.

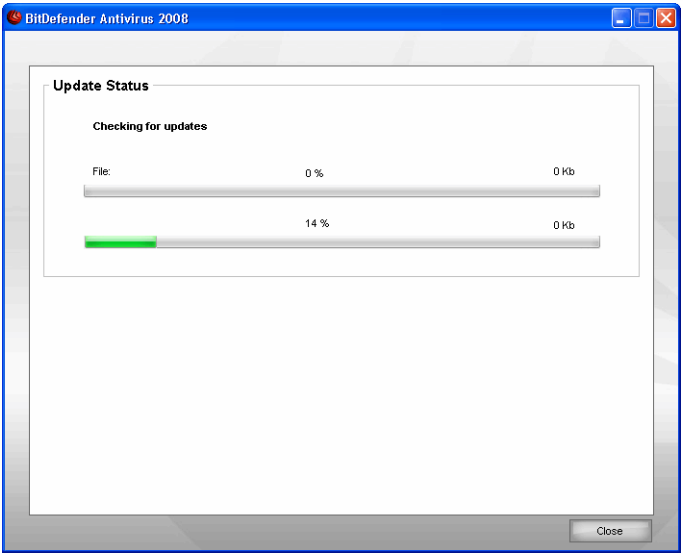
Aşağıdaki butonlar mevcuttur:

- **Şimdi güncelle** – anında güncelleme gerçekleştirir.
- **Belgelerimi Tara** – document and settings klasörünüz için hızlı tarama başlatır.
- **Yoğun sistem tarama** bilgisayarınız için tam tarama başlatır.
- **Tam sistem tarama** bilgisayarınız için tam tarama başlatır.

4.1.1. BitDefender Güncelleme

Hergün yeni bir kötü amaçlı yazılım bulunmakta ve tanımlanmaktadır. Bu nedenle, BitDefender'ın en yeni kötü amaçlı yazılım imzaları ile güncel kılınması çok önemlidir. Fabrika ayarlarında, BitDefender her saatte güncellemeleri kontrol etmek üzere ayarlanmıştır.

BitDefender güncellemeyi kendisi yapar. Bilgisayarınızı açtığınızda ve daha sonra her **saatte bir** güncellemeleri kontrol eder. Bununla beraber, eğer BitDefender' ı anında güncellemek istiyorsanız sadece **Şimdi Güncelle**' ye tıklamanız yeterli. Güncelleme işlemi aşağıdaki pencereyi açacaktır:



BitDefender Güncelleme

Bu pencerede güncelleme işleminin durumunu görebilirsiniz.

Güncelleme işlemi hemen başlayarak, dosyaları kademeli olarak günceller. Güncelleme işlemi devam eden operasyonları etkilemeyecek, tüm kırılganlıkları dışarıda tutacaktır.

Bu pencereyi kapatmak istiyorsanız,**Kapat**' ı tıklayınız. Ancak, bu güncelleme sürecini durdurmayacaktır.

Not
Eğer internete bir çevirmeli bağlantı ile bağlıysanız, bu takdirde BitDefender'ı kullanıcı isteği ile güncellemeyi düzenli bir alışkanlık haline getirmeniz iyi bir fikir olacaktır.

Bilgisayarı yeniden başlatın. Büyük bir güncelleme olduğu taktirde, bilgisayarı yeniden başlatın ibaresi belirecektir. Güncelleme sonrası bilgisayarı yeniden başlatın ibaresini görmek istemiyorsanız, **Bilgisayarı yeniden başlatmadan devam et**seçeneğini işaretleyin. Bu yolla bir sonraki güncelleme sonrası ürün, sistem tekrar başlatılana dek eski dosyalar ile çalışmaya devam edecektir.

Yeniden başlat' a tıklarsanız, sistem yeniden başlatılacaktır.

Eğer sistemi daha sonra yeniden başlatmak istiyorsanız, **Tamam'** a tıklayın Sisteminizi hemen yeniden başlatmanız tavsiye edilir.

4.1.2. BitDefender ile taramak

Bilgisayarınızı kötücül yazılımlara karşı tararken, belirli tarama görevlerini çalıştırmak için uygun butona basınız. Aşağıdaki tabloda, mevcut tarama görevlerini, açıklamaları ile birlikte göreceksiniz.

Görev	Açıklama
Belgelerimi tara	Bu görev geçerli kullanıcının önemli klasörlerini tarar:`Belgelerim`, `Masaüstü` ve `Başlangıç`. Bu belgelerinizin güvenliğini, güvenli bir çalışma alanı ve başlangıçta temiz uygulamaların çalışmasını sağlayacak.
Derin sistem tarama	Tüm sistemi tarar. Varsayılan konfigürasyonda tüm kötücül yazılım tehditleri için tarama yapılır, virüsler, spywareler, adwareler, rootkitler ve diğerleri gibi.
Tam Sistem Tarama	Virüs ve spyware'lere karşı, arşivler hariç olarak, tüm sistemi tarar. Varsayılan konfigürasyonda tüm kötücül yazılım tehditleri için tarama yapılır, virüsler, spywareler, adwareler, rootkitler ve diğerleri gibi.

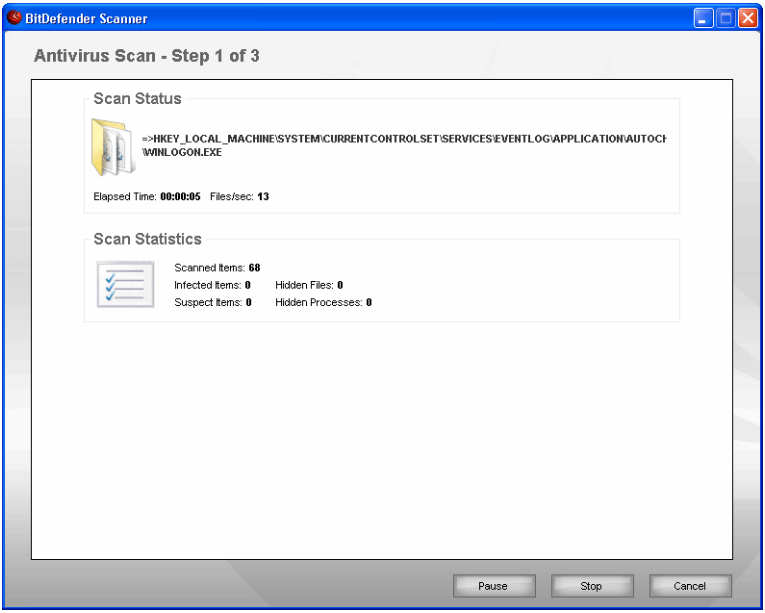
Not
Yoğun sistem tarama ve **Tam sistem tarama** görevleri tüm sistemi analiz edeceği için belirli bir süre almaktadır. Bu nedenle düşük öncelikli seçilmesi ve sistem boşta iken çalışması tavsiye edilir.

İsteğe bağlı tarama işleminde taramanın hızlı veya tam bir tarama olup olmayacağını BitDefender Tarayıcısı bize gösterecektir.

Takip eden üç adımda tarama süreci rehber eşliğinde tamamlanır.

Adım 1/3 – Tarama

BitDefender seçili objeleri taramaya başlayacak.



Tarama

Tarama durumunu ve istatistikleri görebilirsiniz (tarama hızı, geçen süre, taranan sayısı / bulaşmış / şüpheli / gizli objeler ve diğerleri)

Not
Tarama süreci, taramanın karmaşıklığına bağlı olarak, belirli bir zaman alabilir

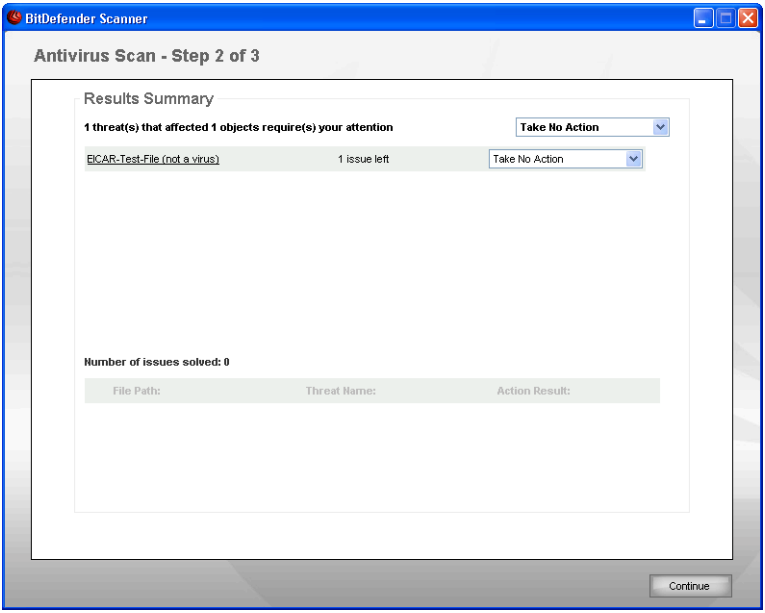
Tarama sürecini geçici olarak duraklatmak için **Duraklat**, devam etmek için **Devam** tuşuna basabilirsiniz.

Herhangi bir anda taramayı durdurmak için, **dur&Evet** tuşuna basıp son adıma geçebilirsiniz.

BitDefender' in taramayı bitirmesini bekleyin.

Adım 2/3 - İşlemi Seçin

Tarama bittiğinde, açılacak yeni pencerede tarama sonuçlarını görebilirsiniz.



İşlem

Sisteminizi etkileyen sorunun adedini görebilirsiniz.

Kötücül yazılımlar temel alınarak etkilenmiş objeler gruplarda görüntülenir. Uygun linke tıklayarak, tehditlerden etkilenmiş objeler hakkında daha fazla bilgi alabilirsiniz.

Her grup için bütün işlemleri seçebilir veya her sorun için ayrılmış işlemi seçebilirsiniz.

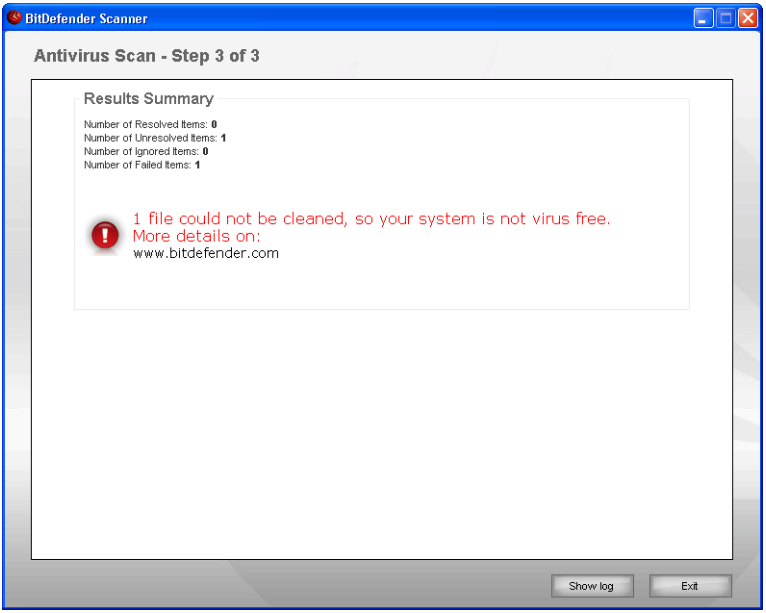
Menüde aşağıdaki seçenekler mevcuttur:

İşlem	*Açıklama*
İşlem Yapma	Virus bulaşmış dosyalar üzerinde hiç bir işlem yapılmaz.
Dosyaları temizle	Virüs bulaşan dosyayı temizler.
Dosyayı Sil	Saptanan dosyayı siler.
Açığa Çıkar	Gizli objeleri görünür yapar.

Devam etmek için **İleri**'yi tıklayın.

Adım 3/3 – Sonuçları Görüntüle

BitDefender sorunları düzeltmeyi bitirdiğinde, tarama sonuçlarının göründüğü yeni bir pencere açılır.



Özet

Sonuçların özetini görebilirsiniz. Rapor dosyası, ilgili görevin **Özellikler** penceresindeki Tarama Kayıtları bölümünde otomatik olarak kaydedilir.

Önemli
Kurulum sihirbazının kurulum sürecinin tamamlayabilmesi için sistemi yeniden başlatmanız istenebilir.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

BitDefender Bazı Sorunları Çözemeyebilir.

BitDefender, birçok durumda enfekte olan dosyaları başarı ile temizler veye enfeksiyondan yalıtır Ancak, çözülemeyen sorunlar var.

Eğer çözümsüz sorunlar varsa bizim tavsiyemiz BitDefender Destek Takımı ile irtibata geçmenizdir www.bitdefender.com. Destek ekibimizbaşınıza gelen sorunları çözmede size yardımcı olacak.

BitDefender Şifre Korumalı Öğeler Algıladı

Şifre koruma kategorisi arşiv ve yükleme dosyaları olmak üzere iki tip içerir. Bunlar, eğer çalışan enfekte olan dosyalar içermiyorlarsa, sistemin güvenliği için gerçek bir tehdit oluşturmazlar.

Bu öğelerin temizliğinden emin olmak için:

- Eğer şifre korumalı öğe bir arşiv ise, dosyayı açıp onu bağımsız olarak taramak gerekir. Taranmasını istediğiniz dosya veya klasöre sağ tıklayıp **BitDefender Antivirus 2008**' i seçin.
- Eğer şifre korumalı öğe bir yükleme dosyası ise, çalıştırmadan önce, gerçek zamanlı koruma ile kontrol ettiğinize emin olun. Eğer yükleme dosyası enfekte olmuş ise, Bitdifender algılar ve enfeksiyonu izole eder.

Eğer BitDefender' ın bu öğeleri tekrar algılamasını istemiyorsanız, onları tarama harici tutulacaklara eklemelisiniz. Tarama harici tutulacaklara eklemek için, Ayarlar konsolundan **Ayarlar**' a ve sonra **Antivirus > Hariç Tut**' a tıklayın. Objeleri dışarıda bırakarak tarama

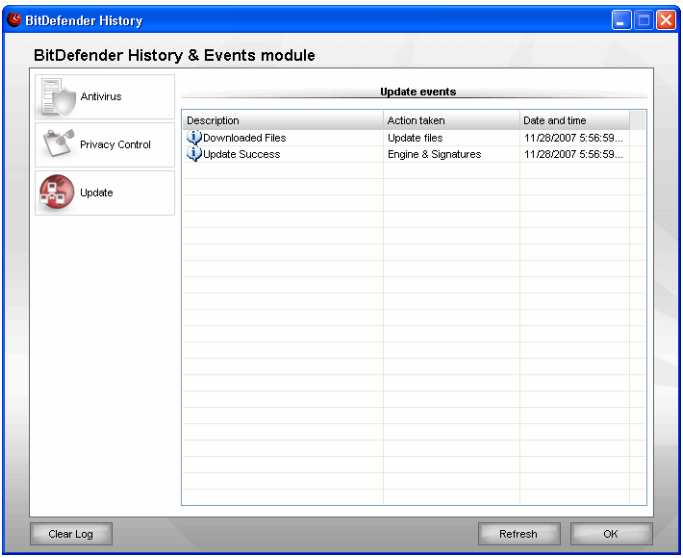
BitDefender şüpheli Dosyalar Algıladı

Sezgisel analiz tarafından saptanan şüpheli dosyalar ve henüz kötücül yazılım adıyla adlandırılmamış dosyalar.

Eğer tarama süresince şüpheli bir dosya tespit edilirse bunların BitDefender Lab.'ına gönderimi için sorulacaktır. **Tamam** tuşuna basarak bu dosyaları daha ileri araştırma için BitDefender Laboratuarlarına gönderebilirsiiniz

5. Geçmiş

BitDefender Güvenli Merkezi penceresinin alt sağ köşesinde bulunan **Geçmiş** linkine tıkladığınızda, geçmiş & olaylar penceresi açılır. Bu pencerede güvenlikle ilgili olaylar yer alır. Örneğin güncellemelerin başarı durumu, varsa bilgisayarınızda bulunan kötücül yazılımlar, başarıyla tamamlanan yedekleme görevleri gibi.



Olaylar

Size yardımcı olmak amacıyla BitDefender geçmiş & olaylar penceresinin sol tarafında, kategoriler tek tek sıralanmıştır.

- **Antivirus**
- **Gizlilik Kontrolü**
- **Güncelle**

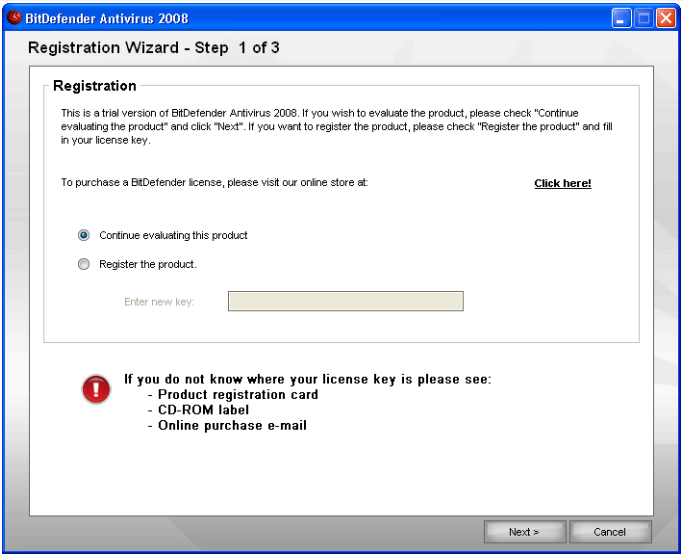
Olaylar listesi her kategori için geçerlidir. Her olay bir bilgi içerir: Kısa bir açıklama, BitDefender' in ne gibi bir işlem yaptığı, hangi tarih ve saatte meydana geldiği gibi. Eğer belirli bir olay hakkında daha fazla bilgi almak istiyorsanız, o olaya çift tıklamanız yeterlidir.

Eğer kayıtları silmek istiyorsanız, **Kayıtları Sil** veya listeyi yenilemek istiyorsanız, **Yenile** tuşuna basınız.

6. Kayıt

BitDefender Antivirus 2008 30 günlük Deneme sürümü ile birlikte gelir. BitDefender Antivirus 2008' i kayıtlı olarak kullanmak için lisans anahtarını değiştirmek veya BitDefender hesabı yaratmak için, BitDefender Güvenlik Merkezi' nin üst tarafındaki**Kayıt** linkine tıklayın. Kayıt sihirbazı 5 adımlı bir prosedürdür.

6.1. Adım 1/3 - BitDefender Antivirus 2008' i Kaydedin



Kayıt

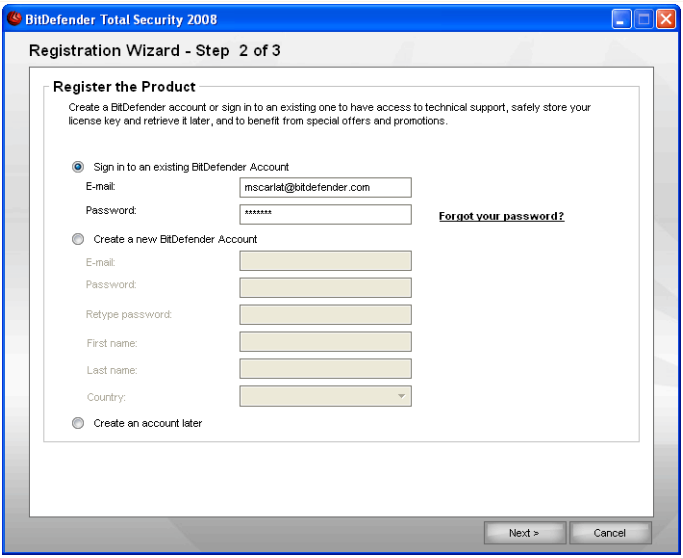
Eğer BitDefender lisansınız yok ise, linke tıklayarak BitDefender online satış mağazasından bir lisans anahtarı alın.

BitDefender Antivirus 2008' i kaydetmek için **Ürünü kaydet** seçeneğini seçin. **Yeni anahtarı gir** alanına lisans anahtarını yazın.

Ürünü denemeye devam etmek için **Ürünü denemeye devam et**'i seçin.

Devam etmek için **İleri**'yi tıklayın.

6.2. Adım 2/3 BitDefender Hesabının Açılması



Hesap Yaratma

BitDefender hesabım yok

BitDefender'ın teknik destek ve diğer ücretsiz hizmetlerinden yararlanabilmek için bir hesap açtırmanız gerekmektedir.

Not
BitDefender hesabınızı daha sonra yaratmak istiyorsanız uygun seçeneği seçiniz.

BitDefender hesabı açmak için **BitDefender Hesabı Yarat** seçeneğini seçip, gerekli alanları doldurun. Internet bağlantısı gereklidir. Burada sağlayacağınız bilgiler gizli kalacaktır.

- **E-mail** – Email adresinizi girin.

- **Şifresi** – daha önce tanımlanan kullanıcı için geçerli bir şifre girin.

Not
Şifre en az dört karakter uzunluğunda olmalıdır.

- **Şifreyi Tekrar Gir** – daha önce tanımlanan kullanıcı için geçerli bir şifreyi tekrar girin.
- **Ad** – Adınızı girin.
- **Soyad** – Soyadınızı girin.
- **Ülke** – Ülke adını seçin.

Not
E-mail adresinizi ve şifrenizi kullanarak http://myaccount.bitdefender.com hesabınıza girin.

Hesabınızın açılmasını gerçekleştirmek için önce e-posta adresinizi aktif hale getirmeniz gerekmektedir. e-posta adresinizi kontrol edin ve BitDefender kayıt hizmetleri tarafından size gönderilen e-postadaki talimatları uygulayın.

Devam etmek için **İleri**'yi tıklayın.

BitDefender hesabım var

Eğer daha önceden bilgisayarınızda bir hesabınız varsa, BitDefender bunu otomatik olarak algılayacaktır. Bu pencereyi kapatmak istiyorsanız,**İleri**' ı tıklayınız.

Zaten bir BitDefender hesabınız varsa, **BitDefender Hesabınıza girin** Hesabınız e-posta adresiniz ve hesap şifrenizden oluşur.

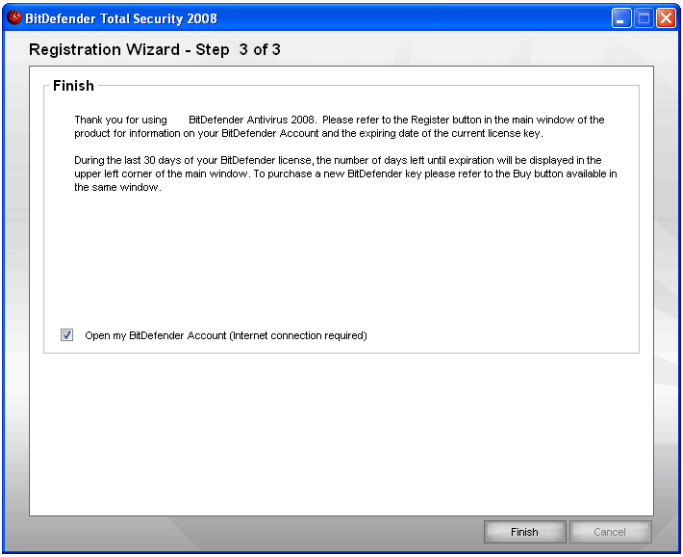
Not

Yanlış bir şifre girerseniz, **İleri** tıkladığınızda şifreyi yeniden yazmanız istenecektir. Yeniden şifre girmek için **İleri** seçeneğine tıklayın. Devam etmek için **İleri** veya sihirbazdan çıkmak için **İptal** seçeneğine tıklayın.

Şifrenizi unuttuysanız, **Şifremi unuttum**'u tıklayın ve talimatları uygulayın.

Devam etmek için **İleri**'yi tıklayın.

6.3. Adım 3/3 - BitDefender Antivirus 2008' i Kaydedin



Özet

BitDefender hesabınıza giriş yapmak için **BitDefender Hesabımı Aç** seçeneğini seçin. Internet bağlantısı gereklidir.

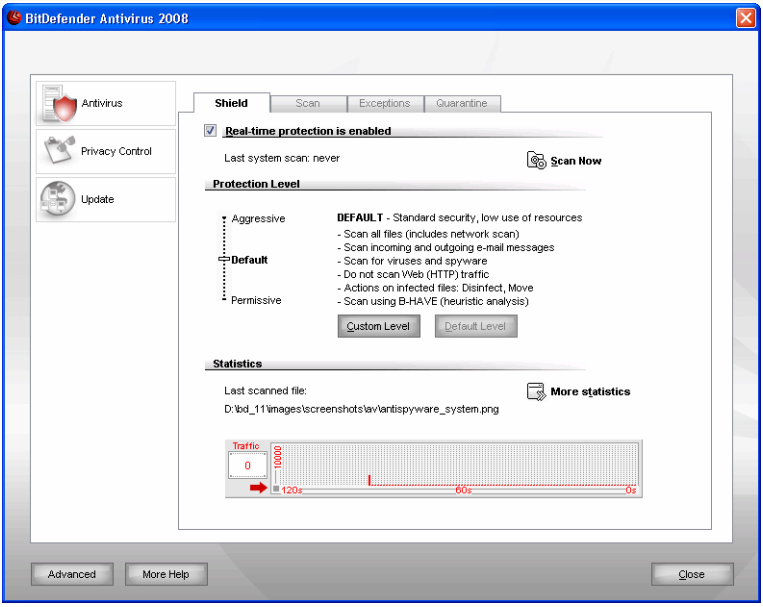
Pencereyi kapatmak için **Bitir** seçeneğini tıklayın.

Gelişmiş Güvenlik Yönetimi

7. Yönetim Konsolu

BitDefender Antivirus 2008, BitDefender' ı gelişmiş olarak ayarlayıp yönetebilmek için bir merkezi yönetim konsolu ile birlikte gelir.

Bu bölüme erişmek için, Güvenlik Merkezini alt tarafındaki**Ayarlar** linkine tıklayın.



Yönetim Konsolu

Yönetim konsolu şu modüllerden oluşur: **Antivirus**, **Gizlilik Kontrolü** ve **Güncelle**. Bu BitDefender' ı, güvenlik sorununun tipine göre kolayca yönetmeye izin verir.

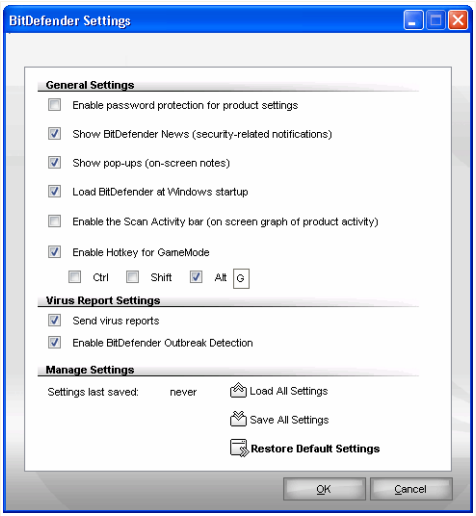
Yönetim konsolunun sol tarafında modül seçicisini göreceksiniz:

- Antivirüs – bu bölümde **Antivirüs** modülünü yapılandırabilirsiniz.
- Gizlilik Kontrolü - bu bölümde **Gizlilik Kontrolü** modülünü yapılandırabilirsiniz.
- Güncelleme – bu bölümde **Güncelleme** modülünü yapılandırabilirsiniz.

Ek yardıma ihtiyacınız varsa**Daha Çok Yardım** linkine tıklayın. Bağlamsal yardım sayfası, bulunduğunuz bölüm hakkında size ayrıntılı bilgileri görüntüler.

7.1. Genel Ayarları Yapılandırma

BitDefender Antivirus 2008' in genel ayarlarını yönetmek için **Gelişmiş**' e basın. Yeni bir pencere çıkacaktır.



Genel Ayarlar

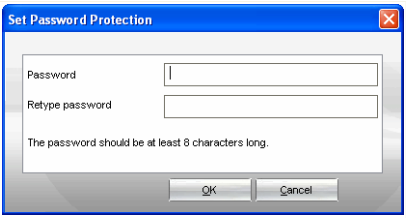
Burada, genel BitDefender davranışlarını ayarlayabilirsiniz. Fabrika ayarları olarak, BitDefender Windows başlangıcında yüklenir ve daha sonra görev çubuğunda küçültülmüş olarak çalışır.

7.1.1. Genel Ayarlar

- **Ürün ayarları için parola korumasını etkin kıl** - BitDefender Yönetim Konsolu konfigürasyonunu korumak için bir parola belirlenmesine imkan verir

Not
Bu bilgisayarı kullanan, yönetim hakları olan tek kişi değilseniz, BitDefender ayarlarınızı bir şifre ile korumanızı tavsiye ediyoruz.

Bu opsiyonu seçtiğinizde, bir sonraki pencere açılacaktır:



Şifre Giriniz

Şifre alanına şifrenizi yazın ve **Şifreyi yeniden yazın** alanında şifrenizi tekrar yazarak **Tamam**'ı tıklayın.

Bir kere şifre girdiğinizde, BitDefender ayarlarını değiştirmek istediğiniz her seferinde size şifre soracaktır. Başka sistem yöneticileri varsa, BitDefender ayarlamaları için bu şifreyi kullanmak zorundadırlar.

Önemli
Şifreyi unuttuğunuzda, BitDefender konfigürasyonunu değiştirmek için ürünü onarmanız gerekecektir.

- **BitDefender Haberlerini Göster (güvenlikle ilgili bildirimler)** - zaman zaman virüs saldırıları ile ilgili BitDefender sunucusu tarafından gönderilen güvenlik bildirimlerini gösterir.
- **Açılır Pencereleri Göster (ekran üzerindeki notlar)** - shows pop-up windows regarding the product status.
- **BitDefender' ı Windows başlangıcında yükle**– BitDefender'ı otomatik olarak sistem başlangıcında başlatır. Bu opsiyonu seçili bırakmanızı tavsiye ediyoruz
- **Tarama Etkinlik Çubuğunu Etkin Kıl (ürün etkinliği ekran grafiğinde)** - Tarama Etkinlik Çubuğunu etkin yapar Tarama Etkinlik Çubuğunun görüntülenmesini istemiyorsanız, kutucuktaki işareti kaldırın.

Not
Bu seçenek sadece geçerli Windows hesabı ile yapılandırılabilir.

- **Oyun Modu için kısayol tuşunu etkin kıl** klavyeyi kullanarak oyun modunu açıp / kapatmayı mümkün kılar. Varsayılan kısayol `Alt+G` olarak belirlenmiştir.

  Kısayolu değiştirmek için aşağıdakileri yapın:

  1. Kısayol tuşunu kullanımınıza göre atamak için. Control tuşu (`Ctrl`), Shift tuşu (`Shift`) veya Alternatif tuş (`Alt`).
  2. Düzenleme sahasında, istediğiniz herhangi bir harfi kısayol olarak atayabilirsiniz.

7.1.2. Virüs Raporu Ayarları

- **Virüs raporları gönder**BitDefender Laboratuarlarına, bilgisayarınızda belirlenen virüsler ile ilgili raporlar gönderir. Bu bizim, virüs saldırılarının kaydını tutmamıza yardım eder.

  Raporlarda, adınız, IP adresiniz veya diğer gizli bilgiler bulunmayacak ve ticari amaçlar için kullanılmayacaklardır. Verilen bilgilerde sadece virüs adı olacak ve sadece istatistiki raporlar oluşturmak için kullanılacaklardır
- **BitDefender Saldırı Tespitini Etkin Kıl** BitDefender Laboratuarlarına, potansiyel virüs saldırıları ile ilgili raporlar gönderir.

  Raporlarda, adınız, IP adresiniz veya diğer gizli bilgiler bulunmayacak ve ticari amaçlar için kullanılmayacaklardır. Verilen bilgilerde sadece potansiyel virüs adı olacak ve sadece yeni virüsleri tespit etmek için kullanılacaklardır

7.1.3. Ayarların Yönetimi

BitDefender için yapmış olduğunuz ayarları, istediğiniz bir yere kaydetmek/yüklemek için **Tüm ayarları kaydet** / **Tüm ayarları yükle** butonlarını kullanın. Bu şekilde, BitDefender ürününü yeniden kurduktan veya onardıktan sonra aynı ayarları kullanabilirsiniz.

Önemli
Sadece yönetim hakları olan kullanıcılar ayarları kaydedebilir ve yükleyebilir

Varsayılan ayarları yüklemek için **Varsayılan Ayarları Geri Yükle** tuşuna basınız

8. Antivirus

BitDefender bilgisayarınızı her türlü kötücül yazılıma karşı korur (virüsler, Truva atları, spywareler, rootkitler gibi)

Dosyaların sezgisel taramasını kullanmak için. Sezgisel taramanın amacı, bir virüs tanımı bulunmadan önce, belirli kalıp ve algoritmalara göre yeni virüslerin tanımlanmasıdır. Yanlış alarm mesajları görünebilir.Böyle bir dosya tespit edildiğinde şüpheli olarak sınıflandırılır. Bu durumlarda, dosyayı analiz edilmesi için BitDefender laboratuarına göndermenizi tavsiye ediyoruz.

BitDefender'ın sunduğu koruma iki kategoriye ayrılmaktadır:

- **Erişim anında tarama** - yeni virüs, spyware ve diğer kötü amaçlı yazılımların sisteminize girmesini engeller. Aynı zamanda gerçek zamanlı koruma olarak da adlandırılır. Kullanıcı, dosyalara eriştikçe dosyalar taranır. Örnek olarak, Bitdefender bir word dökümanı açtığınızda veya bir e-mail aldığınızda onu bilinen tehditlere karşı tarayacaktır.
- **İsteğe bağlı tarama**sisteminizde mevcut olan virüs, spyware ve diğer kötü amaçlı yazılımları tesbit eder. Bu, kullanıcı tarafından başlatılan klasik bir taramadır – BitDefender'ın hangi sürücü, klasör veya dosyayı taraması gerektiğini seçersiniz ve BitDefender bunları talebiniz üzerine tarar. Tarama görevleri isteğe göre düzenlenebilir ve planlama dahilinde düzenli olarak çalıştırılabilir.

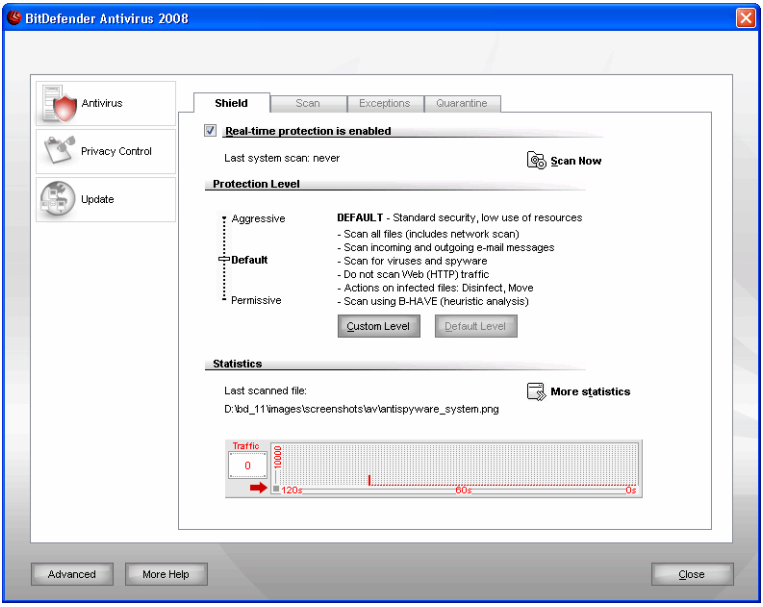
Bu kullanım kılavuzunun **Antivirüs** bölümü aşağıdaki başlıklardan oluşmaktadır.

- Erişim anında tarama
- İsteğe bağlı tarama
- Objeleri dışarıda bırakarak tarama
- Karantina

8.1. Erişim anında tarama

Erişim anında tarama erişilen dosyaları ve Anlık Mesajlaşma Yazılımlarından (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) kurulan iletişimi tüm bilinen kötü amaçlı yazılım tehditlerine karşı tarar.

Gerçek zamanlı koruma ayarlarını konfigüre etmek için yönetim konsolundan**Antivirus>Kalkan**'ı tıklayınız Sıradaki pencere çıkacaktır:



Gerçek-zamanlı Koruma

Önemli
Virüslerin bilgisayarınıza bulaşmasını önlemek için **Gerçek-zamanlı** korumayı etkin kılın.

Bölümün sonunda, taranmış dosya ve e-posta mesajları ile ilgili **Gerçek-zamanlı** koruma istatistiklerini görebilirsiniz. Bu istatistiklerle ilgili daha detaylı bir pencereyi görmek isterseniz **Daha fazla istatistik** seçeneğine tıklayın.

Hızlı sistem taramayı çalıştırmak için, **Şimdi Tara**' ya tıklayınız

8.1.1. Koruma Seviyesi Yapılandırma

Koruma ihtiyaçlarınıza en uygun olan koruma seviyesini seçebilirsiniz. Uygun Koruma seviyesini belirlemek için kaydırma çubuğunu ölçek üzerinde kaydırın

3 koruma seviyesi bulunmaktadır:

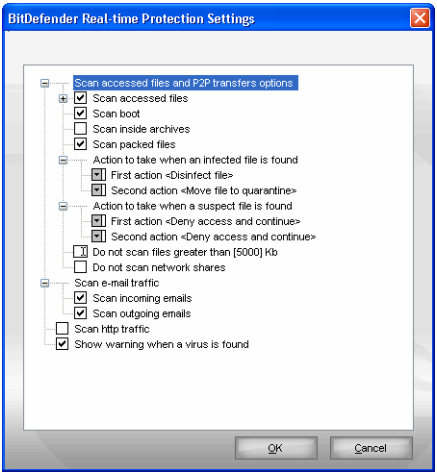
Koruma Seviyesi	Açıklama
Hoşgörülü	Temel güvenlik ihtiyaçlarını karşılar. Kaynak tüketim seviyesi çok düşüktür Yalnızca programlar ve gelen e-postalar virüse karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosya temizleme/erişimi reddetme.
Varsayılan	Standart bir güvenlik sunar. Kaynak tüketim seviyesi düşüktür. Tüm dosyalar, gelen ve giden posta mesajları virüsler ve spyware'lere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosya temizleme/erişimi reddetme.
Agresif	Yüksek düzeyde bir güvenlik sunar. Kaynak tüketim seviyesi ortadır. Tüm dosyalar, gelen ve giden posta mesajları ve web trafiği, virüsler ve spyware'lere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır. Virüs bulaşmış olan dosyalar üzerinde yapılan faaliyetler şunlardır: dosya temizleme/erişimi reddetme.

Varsayılan gerçek zamanlı koruma ayarlarını uygulamak için **Varsayılan Seviye**'yi tıklayınız

8.1.2. Koruma Seviyesini Özelleştirme

İleri düzeydeki kullanıcılar, BitDefender'ın sunduğu tarama ayarlarından yararlanmak isteyebilirler. Tarayıcı, zararsız olduğunu bildiğiniz dosya uzantılarını, dizinleri veya arşivleri atlayacak şekilde ayarlanabilir. Bu şekilde, tarama sürelerini oldukça azaltabilir ve bilgisayarınızın tarama sırasında daha iyi yanıt vermesini sağlayabilirsiniz.

Özel seviye seçeneğini tıklayarak **Gerçek-zamanlı korumayı** ayarlayabilirsiniz. Aşağıdaki pencere görülecektir:



Kalkan Ayarları

Tarama seçenekleri, Windows'taki arama menüleri gibi, genişletilebilir bir menü şeklinde düzenlenmektedir Bir seçeneği açmak için "+" olan kutuyu, seçeneği kapatmak için "-" olan kutuyu tıklayın.

Not

Her ne kadar "+" işareti olsa da bazı tarama seçeneklerinin açılmadığını görebilirsiniz. Bunun nedeni, bu seçeneklerin henüz seçili olmadıklarıdır. Eğer bunları seçerseniz, açılabileceklerini göreceksiniz.

- **Erişilen dosyaları ve P2P aktarım seçenekleri'ni tara** - erişilen dosyaları ve Anlık Mesajlaşma Yazılımlarından (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger) kurulan iletişimi tarar.Taranmasını istediğiniz dosyaların tipini seçiniz.

Seçenek		*Açıklama*
Erişilen dosyaları tara	**Tüm dosyaları tara**	Hangi tipte olursa olsun, tüm erişilen dosyalar taranacaktır
	Sadece program dosyalarını tara	Yalnızca program dosyaları taranacaktır. Bunlar aşağıdaki uzantıları olan dosyalardır: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`;

Seçenek		Açıklama
		.class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws.
	Kullanıcı tanımlı uzantıları tara	Sadece kullanıcı tarafından belirlenmiş uzantıları olan dosyalar taranacaktır. Bu uzantılar ";" ile ayrılmalıdır
	Riskware için tara	Gizli kötü amaçlı yazılımlara karşı hafızayı tarar. Riskware'leri tarar. Bu dosyalar virus bulaşmış dosyalar olarak ele alınır. Bu seçenek etkin kılındığında, adware bileşen içeren yazılımların çalışması durabilir. Bu tür dosyaların taramadan çıkartılmasını istiyorsanız **Tarama'dan arayıcı ve uygulamaları atla**'yı seçin.
Boot sektörü tara		Sistem boot sektörlerini tarar
Dahili arşivleri tara		Erişilen arşivler taranır. Bu seçenek seçildiğinde, bilgisayar yavaşlayacaktır
Paketlenmiş dosyaları tara		Tüm paketlenmiş dosyalar taranır.
İlk işlem		Virus bulaşmış ve şüpheli dosyalara ilk uygulanacak işlemi menüden seçin
	Erişimi reddet ve devam et	Virus bulaşmış bir dosya tespit edildiğinde, bu dosyaya erişim reddedilir.
	Dosyayı temizle	Virüs bulaşan dosyayı temizler.
	Dosyayı Sil	Hiç bir uyarı vermeden virus bulaşan dosyayı siler.
	Dosyayı karantinaya taşı	Virus bulaşan dosyaları karantinaya taşır.

Seçenek		Açıklama
İkinci işlem		Birinci işlemin başarısız olması durumunda, virus bulaşmış dosyalara uygulamak için menüden ikinci işlemi seçin
	Erişimi reddet ve devam et	Virus bulaşmış bir dosya tespit edildiğinde, bu dosyaya erişim reddedilir.
	Dosyayı Sil	Hiç bir uyarı vermeden virus bulaşan dosyayı siler.
	Dosyayı karantinaya taşı	Virus bulaşan dosyaları karantinaya taşır.
[x] Kb'dan büyük dosyaları tarama		Taranacak maksimum dosya boyutunu girin. Eğer boyut 0 Kb ise, boyutu ne olursa olsun tüm dosyalar taranacaktır
Ağ paylaşımlarını tarama		Bu seçenek etkin durumda ise, BitDefender hızlı ağ erişimi için paylaşılmış ağ klasörlerini taramayacaktır Eğer ağınızın bir bölümü antivirüs yazılımları tarafından korunuyorsa, biz bu seçeneğin etkin olmasını tavsiye ediyoruz.

- **E-posta trafiğini tara** - e-posta trafiğini tarar

  Aşağıdaki seçenekler mevcuttur:

Seçenek	Açıklama
Gelen postaları tara	Tüm gelen e-posta mesajlarını tarar
Giden postaları tara	Tüm giden e-posta mesajlarını tarar.

- **Http trafiğini tara** - http traffiğini tarar.
- **Bir virüs bulunduğunda uyarı göster** - dosyada veya e-posta mesajında virüs bulunduğunda bir uyarı penceresi açılır.

  Virüs bulaşmış bir dosya için, uyarı penceresinde virüsün adı, bulunduğu yer, BitDefender tarafından alınan önlem ve bununla ilgili daha fazla bilgi bulabileceğiniz BitDefender sitesine bir link bulunacaktır. Virüs bulaşmış bir dosya için, uyarı penceresinde ayrıca, gönderen ve alan hakkında bilgi olacaktır.

Şüpheli bir dosya tespit edildiğinde, uyarı penceresinden, bu dosyayı analiz etmek üzere BitDefender Laboratuarına göndermenize yardım edecek bir sihirbazı başlatabilirsiniz. Bu raporla ilgili bilgi almak için e-posta adresinizi yazabilirsiniz.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

8.1.3. Gerçek-zamanlı Korumayı Kapat

Gerçek-zamanlı korumayı kapatırsanız, bir uyarı penceresi açılacaktır.

Gerçek-zamanlı Korumayı Kapat

Gerçek zamanlı korumayı ne kadar süre için kapatacağınızı menüden seçerek belirlemelisiniz. Bunu 5, 15, 30, dakika veya 1 saat için, ya da sürekli olarak veya sistem tekrar başlatılana dek kapatabilirsiniz.

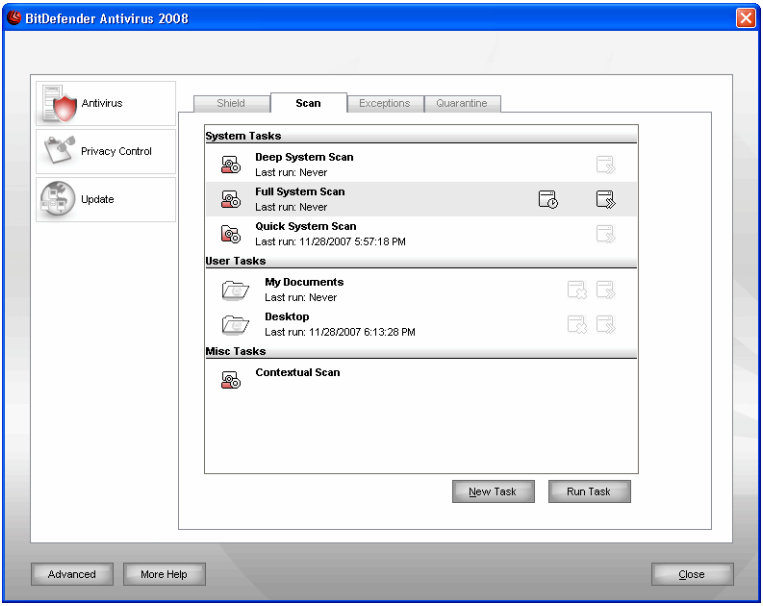
Uyarı
Bu kritik bir güvenlik sorunudur. Eğer gerçek zamanlı koruma kapatılırsa tehditlere karşı korumasız kalırsınız, bu nedenle biz bunu kısa süreler için tavsiye ediyoruz.

8.2. İsteğe bağlı tarama

BitDefender'ın temel amacı, bilgisayarınızı virüslerden uzak tutmaktır. Bunun için yapılacak ilk ve en önemli şey, bilgisayarınızı yeni virüslerden uzak tutmak ve daha sonra e-posta mesajlarınızı ve sisteminize yüklenen veya kopyalanan yeni dosyaları taramaktır.

BitDefender'ı yüklemeden önce, sisteminizde hali hazırda var olan bir virüs olması riski vardır. Bu nedenle BitDefender'ı yükledikten sonra, bilgisayarınızı mevcut virüslere karşı taramanız iyi bir fikir olacaktır. Ve aynı şekilde virüslere karşı bilgisayarınızı sık sık taramanız da çok faydalı olacaktır.

İsteğe bağlı taramayı yapılandırmak için, yönetim konsolundan **Antivirus>Tara**' yı tıklayın. Sıradaki pencere çıkacaktır:



Tarama Görevleri

İsteğe bağlı tarama, tarama gövleri tabanlı olup, belirli tarama seçenekleri ile belirli objeler taranabilir. İstediğinizde bilgisayarınızı varsayılan veya kendinize özgü görevlerle (kullanıcı tanımlı görevler) tarayabilirsiniz. Ayrıca zamanlanmış görevlerle, bilgisayarınız boşta iken ve işlerinizi etkilemeden, düzenli olarak tarayabilirsiniz.

8.2.1. Tarama Görevleri

BitDefender, yaygın güvenlik sorunlarına karşı, varsayılan olarak oluşturulmuş çeşitli görevlerle birlikte gelir. Ayrıca kendi düzenlediğiniz tarama görevlerini de oluşturabilirsiniz.

Her görev, onu düzenleyebileceğiniz ve tarama sonuçlarını görebileceğiniz, **Özellikler** penceresine sahiptir. Daha fazla bilgi için lütfen linke tıklayın. "*Tarama Görevlerini Yapılandırmak*" (shf. 53)

Üç tarama görevi kategorisi bulunmaktadır:

- **Sistem görevleri** – varsayılan sistem görevleri listesini içerir. Aşağıdaki görevler mevcuttur:

Varsayılan Görev	*Açıklama*
Derin sistem tarama	Tüm sistemi tarar. Varsayılan konfigürasyonda tüm kötücül yazılım tehditleri için tarama yapılır, virüsler, spywareler, adwareler, rootkitler ve diğerleri gibi.
Tam Sistem Tarama	Virüs ve spyware'lere karşı, arşivler hariç olarak, tüm sistemi tarar. Varsayılan konfigürasyonda tüm kötücül yazılım tehditleri için tarama yapılır, virüsler, spywareler, adwareler, rootkitler ve diğerleri gibi.
Hızlı Sistem Tarama	`Windows`, `Program Files` and `All Users` klasörleri taranır. Varsayılan konfigürasyon, her tipteki kötücül yazılımı tarar rootkitleri dışarıda tutar, fakat belleği, kayıt defterini ve çerezleri taramaz.

Not
Yoğun sistem tarama ve **Tam sistem tarama** görevleri tüm sistemi analiz edeceği için belirli bir süre almaktadır. Bu nedenle düşük öncelikli seçilmesi ve sistem boşta iken çalışması tavsiye edilir.

- **Kullanıcı görevleri** - kullanıcı tanımlı görevleri içerir

  `Belgelerim` adlı bir görev mevcuttur Bu görev, önemli kullanıcı klasörlerini taramak için kullanılır: `Belgelerim`, `Masaüstü` ve `Başlangıç` Bu, dökümanlarınızın güvenliğini sağlayacak, başlangıçta temiz çalışan uygulamalarla güvenli bir çalışma ortamında çalışmanızı sağlayacak.
- **Çeşitli görevler**– çeşitli tarama görevlerini içermektedir. Bu tarama görevleri, bu pencereden çalıştırılamayan alternatif tarama tipleri ile ilgilidir. Sadece ayarlarını değiştirebilir veya tarama raporlarını görebilirsiniz

Her görevin sağında üç buton vardır:

- **Zamanlanmış Görev**seçilen görevin daha sonra yapılmak üzere seçildiğini gösterir. Bu ayarı değiştirebileceğiniz, **Özellikler** penceresindeki Zamanlayıcı bölümüne gitmek için bu butonu tıklayın.
- **Sil** - seçilen görevi kaldırır.

Not
Sistem görevleri için uygun değildir. Bir sistem görevini silemezsiniz

- **Şimdi Tara** - hemen bir tarama. başlatarak seçilen görevi çalıştırır.

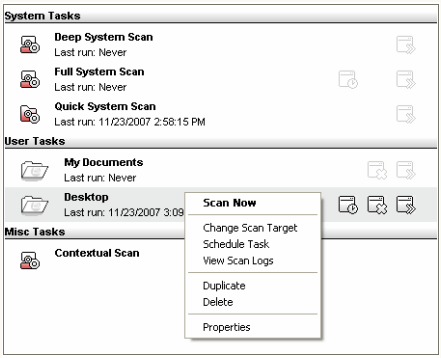
Her görevin solunda görebileceğiniz **Özellikler**butonu, görevi düzenlemeyi ve tarama kayıtlarını görebilmenizi sağlar.

8.2.2. Kısayol Menüsünü Kullanmak

Her bir görev için bir kısayol menüsü bulunmaktadır. Seçilen görevi açmak için üzerine sağ tıklayın.

Kısayol menüsünde aşağıdaki komutlar bulunmaktadır:

- **Şimdi Tara** - hemen bir tarama başlatarak seçilen görevi çalıştırır
- **Tarama Hedefini Değiştir** – seçilen görevin tarama hedefini değiştirebileceğiniz **Özellikler** penceresi, **Tarama Yolu** sekmesini açar.



Kısayol Menüsü

Not
Sistem görevlerinde bu seçenek**Tarama Yolunu Göster** olarak değişir, sadece taranan hedefi görebilirsiniz

- **Görevi Zamanla** - seçilen görevi zamanlayabileceğiniz **Özellikler** penceresi, **Zamanlayıcı** sekmesini açar.
- **Tarama Kayıtlarını Göster** – seçilen görev çalıştırıldıktan sonra üretilen raporları görebileceğiniz **Özellikler** penceresi, **Tarama Kayıtları** sekmesini açar.
- **Çoğalt** - seçilen görevi kopyalar.

Not
Çoğaltılmış görevin ayarlarını değiştirebileceğiniz için, bu özellik yeni görev yarattığınızda yararlı olur.

- **Sil** – seçilen görevi siler.

Not
Sistem görevleri için uygun değildir. Bir sistem görevini silemezsiniz

- **Özellikler** – seçilen görevlerin ayarlarını değiştirebileceğiniz **Özellikler** penceresi, **İnceleme** sekmesini açar.

Not
Farklı özellikleri nedeniyle, sadece **Özellikler** ve **Tarama Kayıtlarını Göster** seçenekleri, **Çeşitli Görevler** kategorisindeki görevler için uygundur.

8.2.3. Tarama Görevleri Yaratmak

Tarama görevi için bu metodlardan birini kullanın:

- Mevcut bir görevi Kopyalayıp, yeni isim verin ve Özellikler penceresinde gerekli değişiklikleri yapın;
- Yeni bir görev yaratmak ve onu yapılandırmak için **Yeni Görev'** e tıklayın.

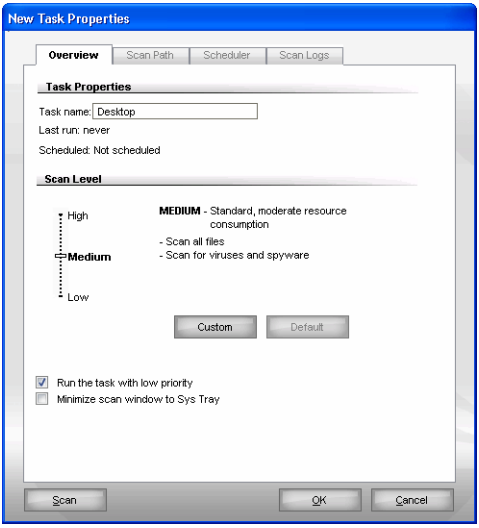
8.2.4. Tarama Görevlerini Yapılandırmak

Her tarama görevinin kendi **Özellikler** penceresi vardır. Burada tarama seçeneklerini yapılandırabilir, tarama hedefini ve görevin zamanını belirleyebilir veya raporları görebilirsiniz. Bu pencereyi açmak için, görevin sağ tarafındaki**Özellikler**butonunu tıklayın (veya görevin üzerine sağ tıklayarak **Özellikler'** i tıklayın).

Not
Daha fazla bilgi için, **Kayıtlar** sekmesine veya "*Tarama Kayıtları*" (shf. 70) bölümüne bakınız.

Tarama Ayarlarını Yapılandırma

Belirli bir tarama görevinin tarama seçeneklerini yapılandırmak için, görevin üzerine sağ tıklayarak **Özellikler'** i seçin. Sıradaki pencere çıkacaktır:



Tanıtma

Burada görev hakkındaki bilgileri görebilir (adı, son çalıştırma ve zaman durumu) ve tarama ayarlarını belirleyebilirsiniz.

Tarama Seviyesini Seçme

Öncelikle tarama seviyesini seçmeniz gerekmektedir. Uygun tarama seviyesini belirlemek için kaydırma çubuğunu ölçek üzerinde kaydırın.

3 tarama seviyesi bulunmaktadır

Koruma Seviyesi	*Açıklama*
Düşük	Makul tespit etkinliği sunar. Kaynak tüketim seviyesi düşüktür Programlar yalnızca virüslere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır.
Orta	İyi tespit etkinliği sunar. Kaynak tüketim seviyesi ortadır. Tüm dosyalar virüsler ve spyware'lere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır.

Koruma Seviyesi	Açıklama
Yüksek	Yüksek tespit etkinliği sunar. Kaynak tüketim seviyesi yüksektir Tüm dosya ve arşivler virüsler ve spyware'lere karşı taranır. Klasik imza tabanlı taramanın yanında sezgisel analiz de kullanılır.

Tarama süreci için bir dizi genel seçenek bulunmaktadır:

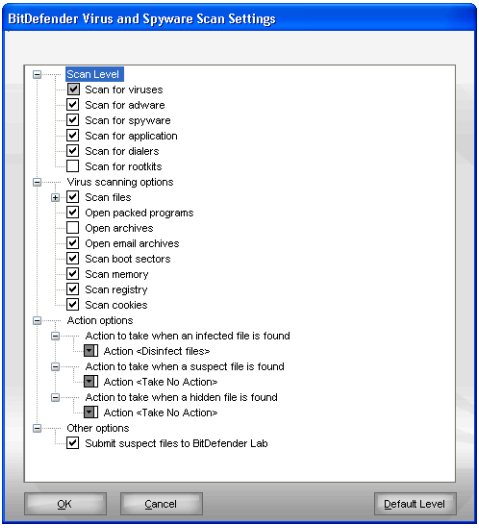
Seçenek	Açıklama
Görevi Düşük öncelikli olarak çalıştır	Tarama sürecinin önceliğini düşürür. Diğer programların daha hızlı çalışmasını ve tarama sürecinin tamamlanması için gerekli zamanı artırmayı sağlayabilirsiniz.
Tarama penceresini başlangıçta sistem tepsisine gönder	Tarama penceresini sistem tepsisi'ne gönderir. Açmak için BitDefender ikonuna çift tıklayın

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın. Görevi başlatmak için sadece **Tara**'ya tıklayın.

Tarama Seviyesini Yapılandırmak

İleri düzeydeki kullanıcılar, BitDefender'ın sunduğu tarama ayarlarından yararlanmak isteyebilirler. Tarayıcı, zararsız olduğunu bildiğiniz dosya uzantılarını, dizinleri veya arşivleri atlayacak şekilde ayarlanabilir. Bu şekilde, tarama sürelerini oldukça azaltabilir ve bilgisayarınızın tarama sırasında daha iyi yanıt vermesini sağlayabilirsiniz.

Kendi tarama seçeneklerinizi belirlemek için **Özel**seçeneğini tıklayın. Yeni bir pencere görünecektir.



Tarama Ayarları

Tarama seçenekleri, Windows'taki arama menüleri gibi, genişletilebilir bir menü şeklinde düzenlenmektedir Bir seçeneği açmak için "+" olan kutuyu, seçeneği kapatmak için "-" olan kutuyu tıklayın.

Tarama seçenekleri dört kategori olarak gruplanmaktadır:

- **Tarama Seviyesi**
- **Virus tarama seçenekleri**
- **İşlem seçenekleri**
- **Diğer seçenekler**

- BitDefender' in belirli tiplerdeki kötü niyetli yazılımlar için tarama yapmasını istiyorsanız, **Tarama Seviyesi** bölümünden uygun opsiyonları seçmelisiniz.

  Aşağıdaki seçenekler mevcuttur:

Seçenek	Açıklama
Virüsler için Tara	Bilinen virüsleri tarar.

Seçenek	Açıklama
	BitDefender tamamlanmamış virüs yapılarını da tespit eder, böylece olası tehditleri silerek sistem güvenliğinizi etkileyebilecek tehditlerden korur.
Adware için tara	Adware' leri tarar. Bu dosyalar virus bulaşmış dosyalar olarak ele alınır. Bu seçenek etkin kılındığında, adware bileşen içeren yazılımların çalışması durabilir.
Spyware için tara	Bilinen spyware tehditleri için taranır. Tespit edilen dosyalar virüs bulaşmış olarak ele alınacaktır.
Uygulama için tara	Uygulamalar taranır (`.exe` ve `.dll` uzantılı dosyalar).
Arayıcılar için tara	Yüksek faturalara neden olan arama uygulamaları için tarama yapılır. Bunlar tespit edildiğinde virüs bulaşmış olarak ele alınır. Bu seçenek etkinken arama bileşeni içeren yazılımların çalışması durdurulur.
Rootkitler için tarama	Gizli objeler için tarama (dosyalar ve işlemler) bunlar genel olarak rootkit olarak bilinirler.

- Taranacak nesnelerin tipini (arşivler, e-posta mesajları ve benzeri) ve diğer seçenekleri belirleyin. Bu, **Virüs tarama seçenekleri** kategorisindeki belirli seçeneklerin seçilmesiyle yapılır.

  Aşağıdaki seçenekler mevcuttur:

Seçenek		Açıklama
Dosyaları tara	**Tüm dosyaları tara**	Hangi tipte olursa olsun, tüm erişilen dosyalar taranacaktır
	Sadece program dosyalarını tara	Sadece program dosyaları taranacaktır. Bunun anlamı sadece aşağıdaki uzantıları olan dosyaların taranacağıdır:`exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`; `prc`; `url`; `smm`; `pdf`; `msi`; `ini`; `csc`; `cmd`; `bas`; `eml` and `nws`.

Seçenek		Açıklama
	Kullanıcı tanımlı uzantıları tara	Sadece kullanıcı tarafından belirlenmiş uzantıları olan dosyalar taranacaktır. Bu uzantılar “;” ile ayrılmalıdır
Paketlenmiş programları aç		Paketlenmiş dosyaları tarar
Arşivleri aç		Dahili arşivleri tarar.
E-posta arşivlerini aç		Dahili posta arşivlerini tarar
Boot sektörlerini tara		Sistem boot sektörlerini tarar
Hafızayı tara		Virüs ve diğer kötü amaçlı yazılımlara karşı hafızayı tarar.
Kaydı tara		Kayıt girişlerini tarar
Çerezleri tara		Çerezleri tarar.

- Virüs bulaşmış veya şüpheli dosyaları belirleyin. Bu dosyalardaki tüm muhtemel işlemleri görmek için **İşlem seçenekleri’ni** açın.
  - Virüs bulaşmış dosya üzerinde aşağıdaki işlemleri yapmayı seçebilirsiniz. Aşağıdaki seçenekler mevcuttur:

İşlem	Açıklama
Hiçbiri (nesneleri kaydet)	Virus bulaşmış dosyalar üzerinde hiç bir işlem yapılmaz. Bu dosyalar rapor dosyasında olacaktır.
Dosyaları temizle	Virüs bulaşan dosyayı temizler.
Dosyaları sil	Hiç bir uyarı vermeden virus bulaşan dosyayı siler.
Dosyaları karantinaya taşı	Virus bulaşan dosyaları karantinaya taşır.

  - Şüpheli dosyalar üzerinde aşağıdaki işlemleri yapmayı seçebilirsiniz. Aşağıdaki seçenekler mevcuttur:

İşlem	Açıklama
Hiçbiri (nesneleri kaydet)	Şüpheli dosyalar üzerinde hiç bir işlem yapılmaz. Bu dosyalar rapor dosyasında olacaktır.
Dosyaları sil	Hiç bir uyarı vermeden şüpheli dosyayı siler.
Dosyaları karantinaya taşı	Şüpheli dosyaları karantinaya taşır.

Not
Eğer sezgisel analiz tarafından şüpheli dosyalar tespit edilirse bunların BitDefender Lab.'ına gönderimi için sorulacaktır.

- Gizli (rootkit) dosyalar üzerinde aşağıdaki işlemleri yapmayı seçebilirsiniz Aşağıdaki seçenekler mevcuttur:

İşlem	*Açıklama*
Hiçbiri (nesneleri kaydet)	Gizli (rootkit) dosyalar üzerinde hiç bir işlem yapılmaz. Bu dosyalar rapor dosyasında olacaktır.
Dosyaları karantinaya taşı	Gizli (rootkit) dosyaları karantinaya taşır.
Görünür yap	Gizli (rootkit) dosyaları görebilmeniz için açığa çıkarır.

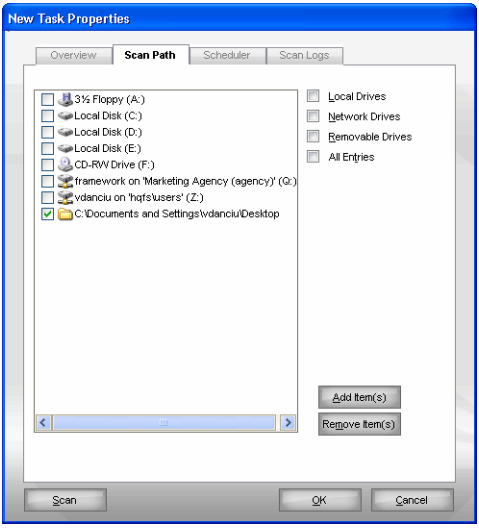
Not
Eğer tespit edilen dosyaları gözardı etmeyi seçtiyseniz ya da seçiminiz başarısızlıkla sonuçlandıysa, tarama sihirbazından bir işlem seçmek zorunda kalacaksınız.

■ Tüm şüpheli dosyaları BitDefender Lab' a bildirmek için, **Diğer seçenekler** bölümündeki **Şüpheli dosyaları BitDefender Lab' a bildir'** i seçin.

Eğer **Varsayılan Seviye**'yi tıklarsanız, varsayılan ayarları yükleyeceksiniz. Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

Tarama Hedefi Ayarı

Belirli bir kullanıcının tarama görevlerinin tarama hedefini ayarlamak için, **Tarama Hedefi Değiştir'** e sağ tıklayıp görevi seçin. Sıradaki pencere çıkacaktır:



Tarama Hedefi

Yerel ağ ve çıkarılabilir cihazların bir listesini, yanısıra önceden eklenmiş dosya ve klasörleri görebilirsiniz. Tüm işaretli nesneler görev çalıştığında taranacaktır.

Bu bölümde aşağıdaki butonlar bulunmaktadır:

- **Dosya(lar)Ekle** - taramak istediğiniz dosya (dosyaları) seçebileceğiniz bir gözatma penceresini açar

Not
Listeye dosya/klasör eklemek için ayrıca sürükle bırak özelliğini de kullanabilirsiniz.

- **Nesne(ler)i Kaldır** önceden seçilmiş dosya/klasör ler listeden kaldırılır.

Not
Sadece daha sonra eklenen dosya/klasörler silinebilir, BitDefender tarafından otomatik olarak görülenler silinmez.

Yukarıda açıklanan butonlar dışında, tarama alanlarının hızlı seçilmesini sağlayan başka seçenekler de bulunmaktadır.

- **Yerel Sürücüler**- yerel sürücüleri taramak için.
- **Ağ Sürücüleri**- ağ sürücülerini taramak için.
- **Çıkarılabilir Sürücüler** - çıkarılabilir sürücüleri (CD-ROM, disket birimi) taramak için.
- **Tüm Girişler** - yerel, ağ veya çıkarılabilen tüm sürücüleri taramak için.

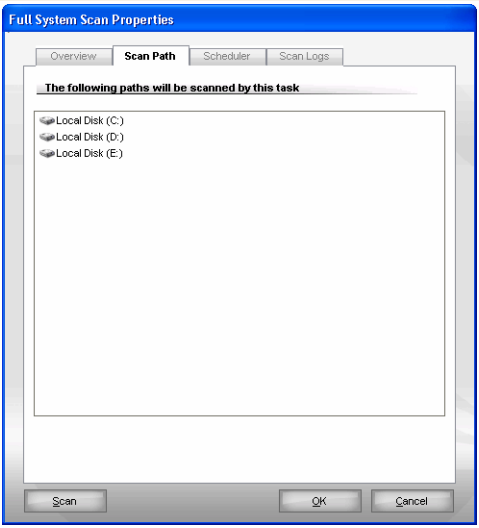
Not
Tüm bilgisayarın virüslere karşı taranmasını isterseniz, **Tüm girişler**. seçeneği yanındaki kutuyu işaretleyin.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın. Görevi başlatmak için sadece **Tara**'ya tıklayın.

Sistem Görevlerinin Tarama Hedefine Bakmak

Sistem görevlerinin tarama hedeflerini **Sistem Görevleri** bölümünden değiştiremezsiniz. Burada tarama hedefini görebilirsiniz.

Belirli bir sistem tarama görevinin hedefini görmek için, **Görev Yolunu Göster** seçeneğini sağ tıklayıp görevi seçin. **Tam Sistem Taraması** için, aşağıdaki pencere açılacaktır:



Tam Sistem Taramasının Tarama Hedefi

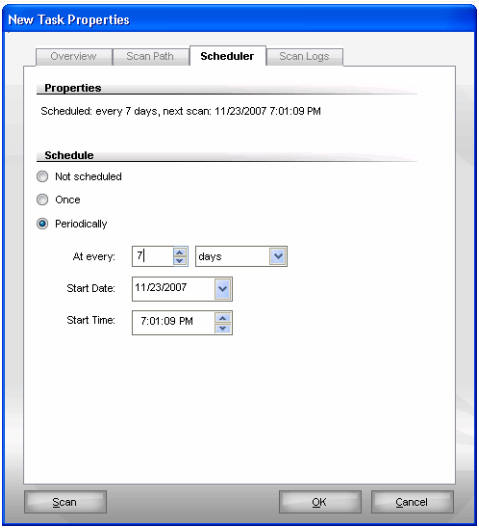
Tam sistem taraması ve **Yoğun sistem taraması** tüm yerel sürücüleri tararken, **Hızlı sistem taraması** sadece `Windows` ve `Program Dosyaları` klasörlerini tarayacaktır.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın. Görevi çalıştırmak için **Tara**'ya basınız.

Tarama Görevlerini Zamanlamak

Karmaşık görevlerde tarama süreci belirli bir zaman alacaktır; tüm diğer programlar kapatıldığında, en etkin şekilde çalışacaktır. Bu nedenle, bilgisayarınızı kullanmadığınızda ve bekleme modunda olduğunda bu görevleri programlamanız en doğru yöntem olacaktır.

Belirli bir görevin zamanlamasını görmek veya değiştirmek için, **Görev Programlayıcı**'ya sağ tıklayıp, görevi seçin. Sıradaki pencere çıkacaktır:



Zamanlayıcı

Herhangi bir görev zamanlayıcıyı görebilirsiniz.

Bir görevi zamanlarken, aşağıdaki seçeneklerden birini seçmeniz gerekecektir:

- **Zamanlanmamış** - yalnızca kullanıcı talep ettiğinde görevi başlatır.

- **Bir Kez** - taramayı sadece bir kez, belirli bir anda başlatır.**Başlatma Tarihi/Zamanı** alanlarına başlatma tarihini ve zamanını girin.
- **Periyodik** - belirli bir tarih ve zamandan başlayarak, taramayı periyodik olarak belirli zaman aralıklarında (saat, gün, hafta, ay, yıl) başlatır.

  Taramanın belirli aralıklarda tekrarlanmasını istiyorsanız, **Periyodik** seçeneğini seçin ve **Her** alanına sürecin sıklığını belirterek dakika/saat/gün/hafta/ay/yıl sayısını girin. Ayrıca **Başlatma Tarihi/Zamanı** alanlarına başlatma tarihini ve zamanını girmelisiniz.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın. Görevi başlatmak için sadece **Tara**'ya tıklayın.

8.2.5. Taranan Objeler

Tarama işlemine başlamadan önce, BitDefender' ın güncellenmiş olduğundan emin olun. Güncellenmemiş bir veritabanı ile tarama yapmak BitDefender' ın yeni kötücül yazılımları bulmasına engel olacaktır. Son güncellemeleri kontrol etmek için ayarlar konsolundaki **Güncelle**' ye basın.

Not
BitDefender'ın tam bir tarama yapabilmesi için tüm diğer açık programları kapatmanız gerekmektedir. Özellikle e-posta istemcinizin (örn.Outlook, Outlook Express veya Eudora) kapatılması önemlidir

Tarama Metodları

BitDefender, dört tip isteğe bağlı tarama tipi sunmaktadır:

- Anında tarama – sistem/kullanıcı görevleri arasından bir tarama görevini çalıştırır.
- Bağlamsal tarama – bir dosya veya klasör üzerine sağ tıklayıp BitDefender Antivirus 2008' i seçin.
- Sürükle&Bırak taraması Tarama Etkinlik Çubuğundaki bir dosya veya klasör sürüklenip bırakılınca tarar.
- Manuel tarama – bir dosya veya klasör üzerine sağ tıklayıp BitDefender Antivirus 2008' i seçin.

Anında Tarama

Bilgisayarınızın tamamını veya bir kısmını taramak için, varsayılan tarama görevlerini kullanabilir veya kendi tarama görevlerinizi yaratabilirsiniz. Anında Tarama

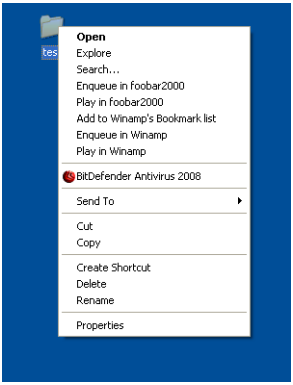
Aşağıdaki işlemlerden birini görebilirsiniz:

- Listeden istenen tarama görevine çift tıklayınız.
- İlişkili görevle ilgili **Şimdi Tara**'ya basınız.
- Görevi seçtikten sonra **Görevi Çalıştır**'a basınız.

BitDefender Tarayıcı penceresi açılacak ve tarama başlatılacaktır. Daha fazla bilgi için "*BitDefender Tarayıcısı*" (shf. 66) bölümüne bakınız.

Bağlamsal Tarama

Dosya veya klasörleri yeni bir tarama görevi yaratmadan taramak için, bağlamsal tarama menüsünü kullanabilirsiniz. Bağlamsal Tarama



Bağlamsal Tarama

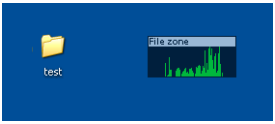
Taranmasını istediğiniz dosya veya klasöre sağ tıklayıp **BitDefender Antivirus 2008**' i seçin.

BitDefender Tarayıcı penceresi açılacak ve tarama başlatılacaktır. Daha fazla bilgi için "*BitDefender Tarayıcısı*" (shf. 66) bölümüne bakınız.

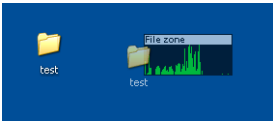
Bağlamsal Menü Tarama görevinin **Özellikler** penceresine girerek tarama seçeneklerini değiştirebilir ve rapor dosyalarını görebilirsiniz.

Sürükle&Bırak Taraması

Taranmasını istediğiniz dosya veya klasörü şekilde gösterildiği gibi sürükleyerek **Tarama Etkinlik Çubuğuna** bırakın.



Dosya Sürükle



Dosya Bırak

BitDefender Tarayıcı penceresi açılacak ve tarama başlatılacaktır. Daha fazla bilgi için "*BitDefender Tarayıcısı*" (shf. 66) bölümüne bakınız.

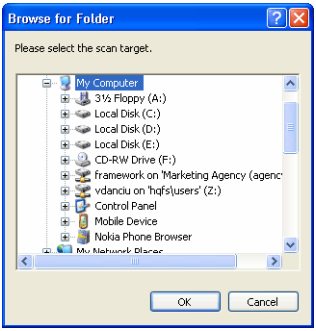
Manuel Tarama

Manuel tarama, Başlat menüsündeki BitDefender program grubundaki BitDefender Manuel Tarama seçeneğini kullanarak seçilen objeleri direk olarak taramaktan ibarettir.

Not
Manuel tarama son derece kullanışlıdır ve Windows Güvenli Mod da çalışırken dahi kullanılabilir.

BitDefender tarafından taranacak olan objeleri Windows Başlat menüsünden seçmek için şu sırayı takip edin; **Başlat** → **Programlar** → **BitDefender 2008** → **BitDefender Manuel Tarama**.

Sıradaki pencere çıkacaktır:



Manuel Tarama

Taramak istediğiniz objenin üzerine tıklayıp, daha sonra**Tamam**' a tıklayın.

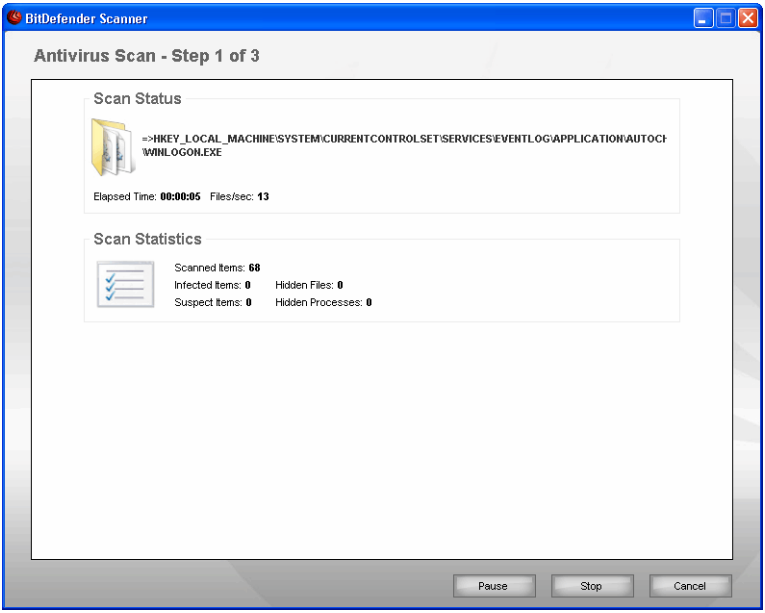
BitDefender Tarayıcı penceresi açılacak ve tarama başlatılacaktır. Daha fazla bilgi için "*BitDefender Tarayıcısı*" (shf. 66) bölümüne bakınız.

BitDefender Tarayıcısı

İsteğe bağlı taramayı başlattığınızda, BitDefender Tarayıcısı açılacaktır. Takip eden üç adımda tarama süreci rehber eşliğinde tamamlanır.

Adım 1/3 – Tarama

BitDefender seçili objeleri taramaya başlayacak.



Tarama

Tarama durumunu ve istatistikleri görebilirsiniz (tarama hızı, geçen süre, taranan sayısı / bulaşmış / şüpheli / gizli objeler ve diğerleri)

Not
Tarama süreci, taramanın karmaşıklığına bağlı olarak, belirli bir zaman alabilir

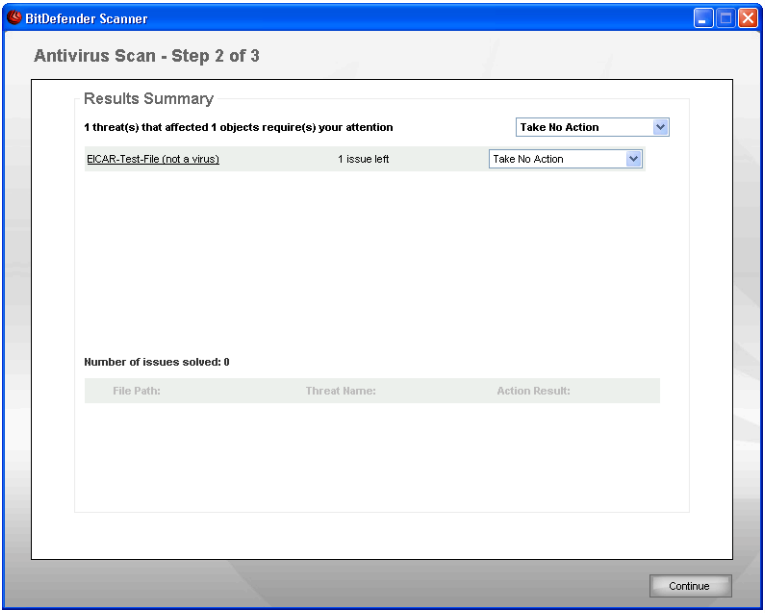
Tarama sürecini geçici olarak duraklatmak için **Duraklat**, devam etmek için **Devam** tuşuna basabilirsiniz.

Herhangi bir anda taramayı durdurmak için, **dur&Evet** tuşuna basıp son adıma geçebilirsiniz.

BitDefender' in taramayı bitirmesini bekleyin.

Adım 2/3 - İşlemi Seçin

Tarama bittiğinde, açılacak yeni pencerede tarama sonuçlarını görebilirsiniz.



İşlem

Sisteminizi etkileyen sorunun adedini görebilirsiniz.

Kötücül yazılımlar temel alınarak etkilenmiş objeler gruplarda görüntülenir. Uygun linke tıklayarak, tehditlerden etkilenmiş objeler hakkında daha fazla bilgi alabilirsiniz.

Her grup için bütün işlemleri seçebilir veya her sorun için ayrılmış işlemi seçebilirsiniz.

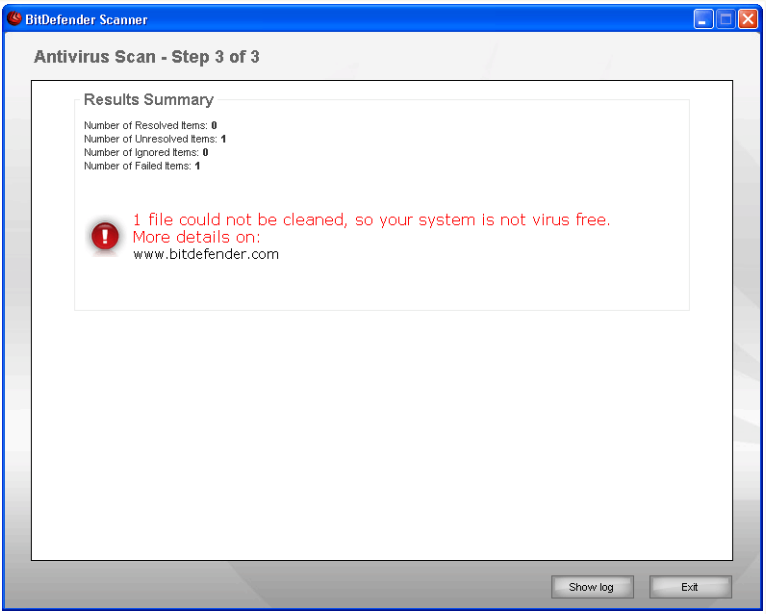
Menüde aşağıdaki seçenekler mevcuttur:

İşlem	*Açıklama*
İşlem Yapma	Virus bulaşmış dosyalar üzerinde hiç bir işlem yapılmaz.
Dosyaları temizle	Virüs bulaşan dosyayı temizler.
Dosyayı Sil	Saptanan dosyayı siler.
Açığa Çıkar	Gizli objeleri görünür yapar.

Devam etmek için **İleri**'yi tıklayın.

Adım 3/3 – Sonuçları Görüntüle

BitDefender sorunları düzeltmeyi bitirdiğinde, tarama sonuçlarının göründüğü yeni bir pencere açılır.



Özet

Sonuçların özetini görebilirsiniz. Rapor dosyası, ilgili görevin **Özellikler** penceresindeki Tarama Kayıtları bölümünde otomatik olarak kaydedilir.

Önemli
Kurulum sihirbazının kurulum sürecinin tamamlayabilmesi için sistemi yeniden başlatmanız istenebilir.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

BitDefender Bazı Sorunları Çözemeyebilir.

BitDefender, birçok durumda enfekte olan dosyaları başarı ile temizler veye enfeksiyondan yalıtır Ancak, çözülemeyen sorunlar var.

Eğer çözümsüz sorunlar varsa bizim tavsiyemiz BitDefender Destek Takımı ile irtibata geçmenizdir www.bitdefender.com. Destek ekibimizbaşınıza gelen sorunları çözmede size yardımcı olacak.

BitDefender Şifre Korumalı Öğeler Algıladı

Şifre koruma kategorisi arşiv ve yükleme dosyaları olmak üzere iki tip içerir. Bunlar, eğer çalışan enfekte olan dosyalar içermiyorlarsa, sistemin güvenliği için gerçek bir tehdit oluşturmazlar.

Bu öğelerin temizliğinden emin olmak için:

- Eğer şifre korumalı öğe bir arşiv ise, dosyayı açıp onu bağımsız olarak taramak gerekir. Taranmasını istediğiniz dosya veya klasöre sağ tıklayıp **BitDefender Antivirus 2008**' i seçin.
- Eğer şifre korumalı öğe bir yükleme dosyası ise, çalıştırmadan önce, gerçek zamanlı koruma ile kontrol ettiğinize emin olun. Eğer yükleme dosyası enfekte olmuş ise, Bitdifender algılar ve enfeksiyonu izole eder.

Eğer BitDefender' ın bu öğeleri tekrar algılamasını istemiyorsanız, onları tarama harici tutulacaklara eklemelisiniz. Tarama harici tutulacaklara eklemek için, Ayarlar konsolundan **Ayarlar'** a ve sonra **Antivirus > Hariç Tut'** a tıklayın. Objeleri dışarıda bırakarak tarama

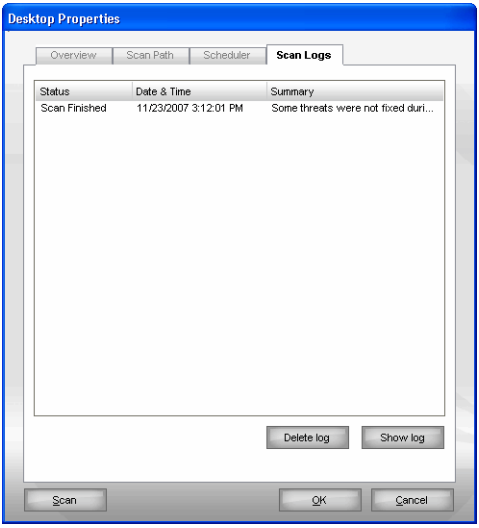
BitDefender şüpheli Dosyalar Algıladı

Sezgisel analiz tarafından saptanan şüpheli dosyalar ve henüz kötücül yazılım adıyla adlandırılmamış dosyalar.

Eğer tarama süresince şüpheli bir dosya tespit edilirse bunların BitDefender Lab.'ına gönderimi için sorulacaktır. **Tamam** tuşuna basarak bu dosyaları daha ileri araştırma için BitDefender Laboratuarlarına gönderebilirsiiniz

8.2.6. Tarama Kayıtları

Tarama kayıtlarını görmek için, görevin üzerinde sağ tıklayıp, **Tarama Kayıtları**seçeneğini seçin. Sıradaki pencere çıkacaktır:



Tarama Kayıtları

Burada, her görevin gerçekleştirildiğinde üretilen raporu görebilirsiniz.

Her dosyada, durumu (temiz/virüslü), taramanın hangi tarih ve zamanda gerçekleştiği hakkında ek bilgiler ve bir özet (tarama tamamlandı) olacaktır.

İki buton vardır:

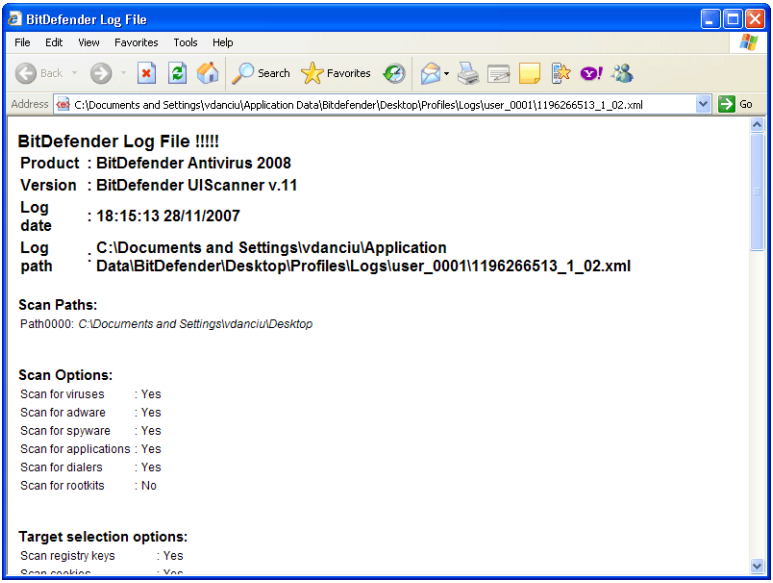
- **Kaydı sil** – seçilen rapor dosyasını silmek için
- **Kaydı göster** – seçilen rapor dosyasını görüntülemek için. Tarama kaydı geçerli web tarayıcınızda açılacaktır.

Not
Bir dosyayı görüntülemek veya silmek için ayrıca, dosyayı sağ tıklayıp kısayol menüsünden ilgili seçeneği seçin.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın. Görevi başlatmak için sadece **Tara**'ya tıklayın.

Tarama Kaydı Örneği

Aşağıdaki şekil tarama kaydına bir örnektir:



Tarama Kaydı Örneği

Tarama kaydı, tarama işlemine ait detaylı bilgi içerir. Tarama seçenekleri, bulunan tehditler ve bunlara uygulanan işlemler gibi.

8.3. Nesne Hariç Tarama

Çeşitli dosyaları tarama dışında tutmak isteyeyeğiniz durumlar olabilir. Örneğin EICAR dosyalarını erişim anında taramada veya `.avi` dosyalarını isteğe bağlı taramada, tarama dışında tutabilirsiniz.

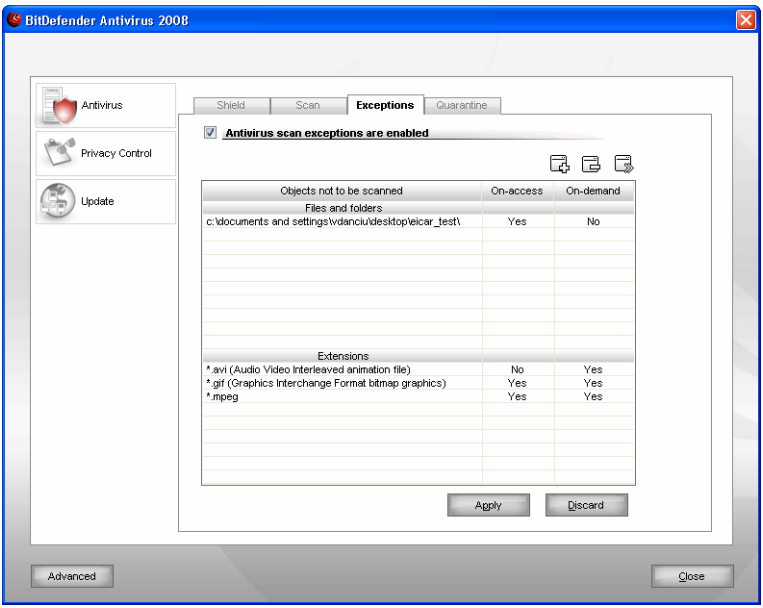
BitDefender erişim anında veya isteğe bağlı taramada yada her ikisinde birden nesneleri hariç tutmaya izin verir. Bu özellik tarama zamanını azaltmak ve işlerinizi engellememek için tasarlanmıştır.

Nesne harici tarama iki şekilde yapılabilir:

- Bir dosya veya bir klasör yolu belirleyip, tarama dışında tutabilirsiniz.
- Dosya uzantılarına göre tarama dışı olacak nesneleri seçebilirsiniz

Not
Erişim anında tarama dışında tutulan nesneler taranmayacaktır, sizin veya bir uygulamanın kullanıyor olması önemli değildir.

Nesne hariç taramayı yönetmek ve görmek için, ayarlar konsolundan **Antivirus>İstisnalar'** ı tıklayın. Sıradaki pencere çıkacaktır:



İstisnalar

Tarama dışında tutulan nesneleri (dosyalar, klasörler, uzantılar) görebilirsiniz.

Not
İstisnalar bağlamsal taramalara uygulanmayacaktır.

Bir girişi kaldırmak için, girişi seçin ve **Sil** seçeneğini tıklayın.

Bir girişi düzenlemek için, girişi seçin ve **Düzenle** seçeneğini tıklayın veya kural üzerine çift tıklayın. Yeni pencere görünecektir. Açılacak olan yeni pencerede tarama

dışı tutmak istediğiniz dosya uzantısını, dosya veya klasörleri değiştirebilirsiniz. Bunun için değişikliği yapıp **Tamam** tuşuna basın.

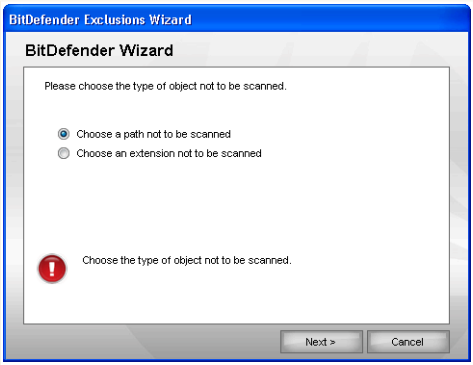
Not
Ayrıca sağ tıklayarak kısayol menüsünden, düzenleme yapabilir ya da silebilirsiniz.

Uygula' ya basarak kaydedilmediyse, **Vazgeç**' e basarak eski hale dönmeyi sağlayabilirsiniz.

8.3.1. Yolları taramadan hariç tutmak

İstediğiniz yolun hariç tutulacağı bir tarama yapmak için, **Ekle** tuşuna basınız. Size tarama boyunca rehberlik edecek yapılandırma sihirbazı görünecektir.

Adım 1/3 - Nesne Tipini Seçin

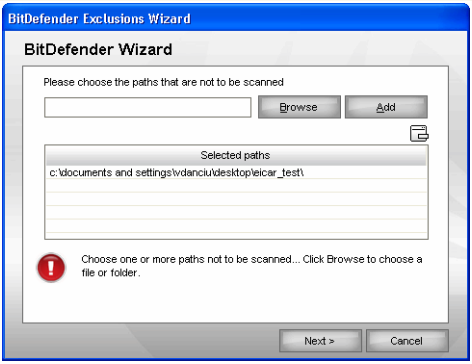


Nesne Tipi

Tarama harici tutacağınız yol tercihlerini seçin.

İleri'yi tıklayın.

Adım 2/3 – Yolu belirleyin



Hariç Tutulan Yollar

Belirlenen yolları tarama harici tutmak için iki metod vardır.

- **Gözat**'a tıklayın, taranmayacak dosya veya klasörü seçin ve **Ekle** seçeneğini tıklayın.
- Düzenleme alanına, hariç tutmak istediğiniz yolu yazmak için, **Ekle**' ye tıklayın.

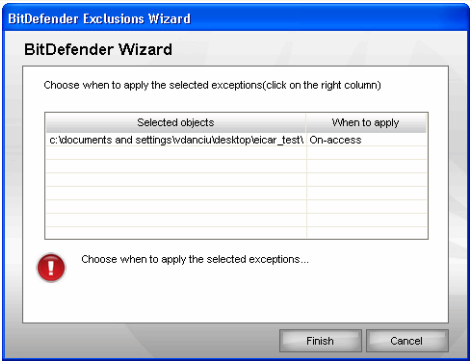
Not
Eğer yol adı yok ise bir hata mesajı alacaksınız. **Tamam**' basıp yolu kontrol edin.

Eklediğiniz yol tabloda görünecektir. İsterseniz bir çok yol daha ekleyebilirsiniz.

Bir girişi kaldırmak için, girişi seçin ve **Sil** seçeneğini tıklayın.

İleri'yi tıklayın.

Adım 3/3 – Tarama Tipini Seçin



Tarama Tipi

Tablo içeriğinde tarama harici tutulacak yolları ve tarama tipini görebilirsiniz.

Varsayılan olarak her iki tarama tipide seçili durumdadır. Değiştirmek isterseniz, sağ kolona tıklayarak arzuladığınız seçeneği seçebilirsiniz.

Bitir seçeneğini tıklayın.

Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

8.3.2. Uzantıları Hariç Tutarak Tarama

Uzantıları hariç tutarak tarama yapmak için, **Ekle**'ye tıklayın. Size tarama boyunca rehberlik edecek yapılandırma sihirbazı görünecektir.

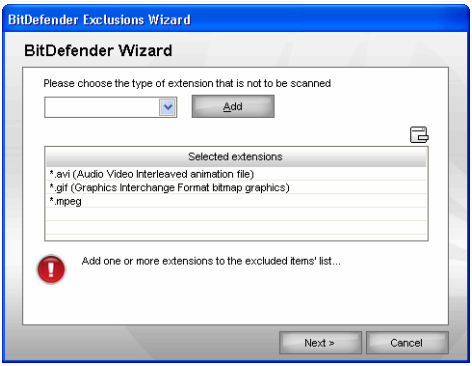
Adım 1/3 - Nesne Tipini Seçin

Nesne Tipi

Tarama harici tutmak istediğiniz uzantı tercihlerini seçin.

İleri'yi tıklayın.

Adım 2/3 - Tarama Harici Uzantıları Belirleyin



Tarama Harici Uzantılar

Tarama harici tutulacak uzantıları belirlemek için, aşağıdaki metodlardan herhangi birini kullanınız.

- Tarama harici tutulacak uzantıları seçmek için, **Ekle'** ye tıklayın.

Not
Menüde sisteminize kayıtlı olan tüm uzantılar listelenecektir. Uzantıyı seçtiğinizde, eğer varsa ona ait açıklamayı görebilirsiniz.

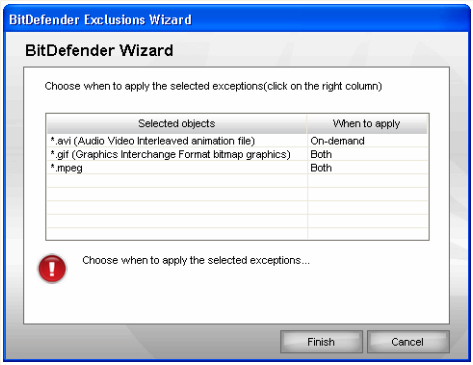
- Düzenleme alanında tarama harici tutmak istediğiniz uzantı tipini **Ekle'** ye tıklayarak seçin.

Eklediğiniz uzantı tabloda görünecektir. İsterseniz bir çok uzantı daha ekleyebilirsiniz.

Bir girişi kaldırmak için, girişi seçin ve **Sil** seçeneğini tıklayın.

İleri'yi tıklayın.

Adım 3/3 – Tarama Tipini Seçin



Tarama Tipi

Tablo içeriğinde tarama harici tutulacak uzantıları ve tarama tipini görebilirsiniz.

Varsayılan olarak her iki tarama tipide seçili durumdadır. Değiştirmek isterseniz, sağ kolona tıklayarak arzuladığınız seçeneği seçebilirsiniz.

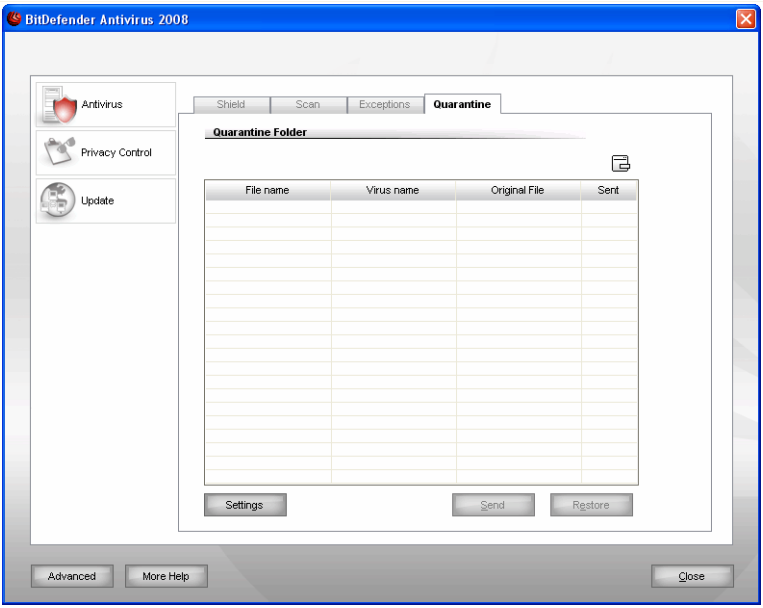
Bitir seçeneğini tıklayın.

Değişiklikleri kaydetmek için **Uygula** tuşuna basınız.

8.4. Karantina Alanı

BitDefender, virüs bulaşmış olan veya şüpheli dosyaların, karantina adı verilen güvenli bir alanda izole edilmelerini sağlar. Bu dosyaları karantinada izole ederek, virüs bulaşma riskini kaldırmış olursunuz ve aynı zamanda daha ileri analizlerin yapılabilmesi için bu dosyaları BitDefender laboratuarına gönderme imkanınız olur.

Karantinaya alınmış dosyaları görmek ve yönetmek ve karantina ayarlarını yapılandırmak için, ayarlar konsolundan**Antivirus>Karantina**' yı tıklayın.



Karantina

8.4.1. Karantinaya Alınmış Dosyaları Yönetmek

Görebileceğiniz gibi, **Karantina** bölümünde, şu ana kadar izole edilmiş dosyaların bir listesi vardır. Her dosyada dosyanın adı, boyutu, izole edilme tarihi ve BitDefender'a gönderildiği tarih bilgileri bulunmaktadır.

Not
Virüs karantinadayken, zarar veremez, çünkü çalıştırılamaz veya okunmayacaktır

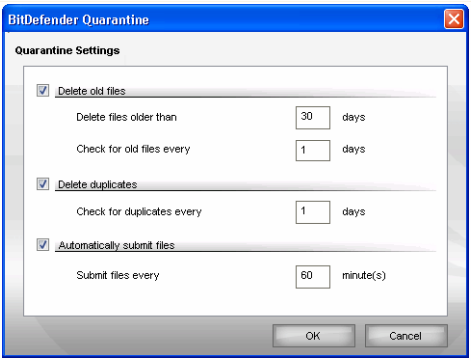
Karantinadan seçilen bir dosyayı silmek için **Kaldır** butonuna tıklayın. Seçilen bir dosyayı orijinal yerine geri yüklemek istiyorsanız, **Geri yükle**'yi tıklayın.

Seçilen bir dosyayı karantinadan BitDefender laboratuarına göndermek için **Gönder**'i tıklayın.

Bağlamsal Menü. Bağlamsal menü, karantinaya alınan dosyaları kolayca yönetmenize imkan verir. Ayrıca **Yenile** tuşuna basarak karantina bölümünü yenileyebilirsiniz.

8.4.2. Karantina Ayarlarını Yapılandırma

Karantina ayarlarını yapılandırmak için, **Ayarlar'** ı tıklayınız. Yeni bir pencere çıkacaktır.



Karantina Ayarları

Karantina ayarlarını kullanarak, BitDefender' ın aşağıdaki işlemleri otomatik olarak yapmasını sağlayabilirsiniz:

Eski dosyaları siler. Eski karantina dosyalarını otomatik olarak silmek için, uygun seçeneği kontrol edin. Karantinadaki dosyaların silinmesi ve BitDefender' ın eski dosyaları belirli frekanslarla kontrol etmesi için gün sayısı belirlemelisiniz.

Not
Varsayılan olarak, BitDefender hergün eski dosyaları kontrol edip 10 günden eski olanları silecektir.

Silme Tekrarı. Karantinadaki dosyaları silme tekrarı otomatik olarak gerçekleşir. Uygun seçeneği kontrol edin. Birbirini takip edecek silme tekrarlarının arası için gün sayısı belirlemelisiniz.

Not
Varsayılan olarak, Bitdefender karantinadaki dosyaları silme tekrarı için hergün kontrol eder.

Otomatik olarak gönderilen dosyalar. Dosyaları karantinaya otomatik olarak göndermek için uygun seçeneği kontrol edin. Gönderilecek dosyalar için bir frekans belirlemelisiniz.

Not
Varsayılan olarak, BitDefender her 60 dakikada bir yapacaktır.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

9. Gizlilik Kontrolü

BitDefender, sisteminizde spyware'lerin saldırabileceği pek çok potansiyel "sıcak noktaları" denetler ve sisteminize ve yazılımınıza yapılan herhangi bir değişikliği kontrol eder. Gizli bilgilerinizi ele geçirmeye çalışan ve kredi kartı bilgileri gibi kişisel bilgileri bilgisayarınızdan korsana göndermeye çalışan korsanlar tarafından yüklenen Trojan Horses (Truva Atı) ve diğer araçların engellenmesinde etkin bir modüldür

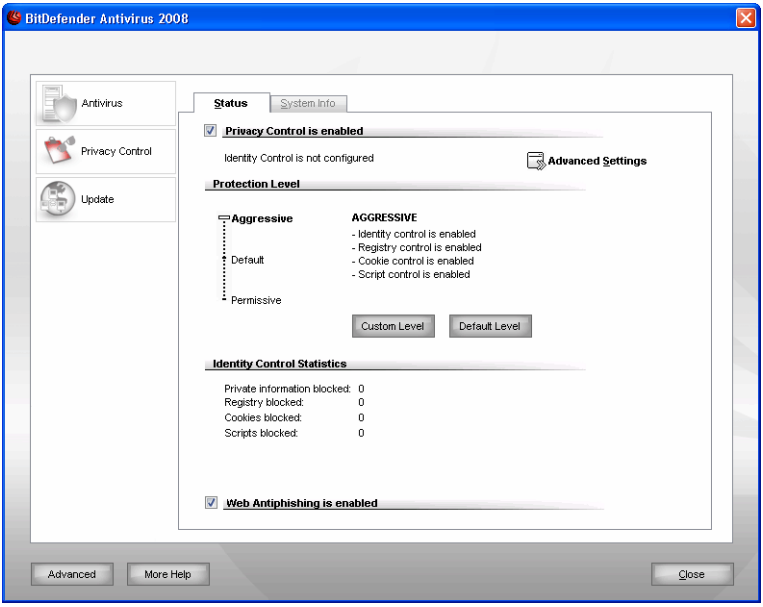
BitDefender ayrıca, gezdiğiniz web sitelerini tarayarak herhangi bir phishing tehdidi algılarsa sizi uyaracaktır.

Bu kullanım kılavuzunun **Gizlilik Kontrolü** bölümü aşağıdaki başlıklardan oluşmaktadır:

- Gizlilik Kontrolü Durumu
- Gelişmiş Ayarlar - Kişisel Gizlilik Kontrolü
- Gelişmiş Ayarlar - Kayıt Kontrolü
- Gelişmiş Ayarlar - Cookie Kontrolü
- Gelişmiş Ayarlar - Script Kontrolü
- Sistem Bilgileri
- Antiphishing Araç Çubuğu

9.1. Kişisel Gizlilik Durumu

Kişisel gizlilik kontrolünü yapılandırmak ve durumu hakkında bilgi almak için ayarlar konsolundan, **Kişisel Gizlilik Kontrolü>Durum** tuşunu tıklayın. Sıradaki pencere çıkacaktır:



Kişisel Gizlilik Durumu

9.1.1. Gizlilik Kontrolü

Önemli
Veri hırsızlığını önlemek ve kişisel bilgilerinizi korumak için, **Kişisel Gizlilik Kontrolü**'nü aktifleştirin.

Kişisel Gizlilik Kontrolü bilgisayarınızı 5 önemli koruma kontrolü Kullanarak korur:

- Kişisel Gizlilik Kontrolü – dışarı giden tüm HTTP ve SMTP trafiğini Kişisel Gizlilik bölümünde oluşturduğunuz kurallara göre filtre ederek, kişiye özel gizli verilerinizi korur.

Not
Bölümün sonunda **Kişisel Gizlilik Kontrolü İstatistikleri**'ni görebilirsiniz

- Kayıt Kontrolü – bir program, Windows başlatıldığında çalıştırılmak için kayıt bilgisini değiştirmeye çalıştığında, izninizi ister.
- Cookie Kontrolü – Yeni bir web sitesi bir cookie kurmaya çalıştığında, izninizi ister.
- Script Kontrolü – Bir web sitesi bir scripti veya başka bir aktif içeriği etkinleştirmek istediğinde, izninizi ister.

Bu kontrollerin ayarlarını yapılandırmak için - Gelişmiş Ayarlar seçeneğini tıklayın.

Koruma Seviyesi Yapılandırma

Koruma ihtiyaçlarınıza en uygun olan koruma seviyesini seçebilirsiniz. Uygun Koruma seviyesini belirlemek için kaydırma çubuğunu ölçek üzerinde kaydırın

3 koruma seviyesi bulunmaktadır:

Koruma Seviyesi	Açıklama
Hoşgörülü	Sadece **Kayıt Kontrolünü** etkinleşir.
Varsayılan	**Kayıt Kontrolü** ve **Kimlik Kontrolü'** nü etkinleşir
Agresif	**Kayıt Kontrolü**, **Kimlik Kontrolü** ve **Script Kontrolü**etkinleşir.

Koruma seviyesini yapılandırmak için, **Kullanıcı Ayarı Seviyesi**' ni tıklayınız. Görüntülenecek olan pencerede etkinleştirmek istediğiniz koruma kontrolünü seçip, **Tamam'** a basın.

Çubuğu varsayılan seviyesine konumlamak için **Varsayılan Seviye** seçeneğini tıklayın.

9.1.2. Antiphising Koruması

Phishing, sosyal mühendislik tekniklerini kullanarak insanları aldatıp, kişisel bilgilerini ele geçirmeye yönelik suç teşkil eden bir aktivitedir.

Çoğu zaman, phishing denemeleri gerçeği gibi görünüp aslında sahte olan yığın e-mailler gönderimi şeklinde gelişir. Bu aldatmaca mesajlar en azından birkaç alıcının bunlara ikna olmasını ümit edip, kişisel bilgileri açığa çıkarmayı amaçlarlar.

Bir phishing mesajı genellikle online hesabınızı ele geçirmeye çalışır. Sahte bir web sitesi tarafından sağlanan özel bilgilerinize ihtiyaç duyan bir linke tıklamanız için sizi ikna etmeye çalışır. Örneğin, hesap bilgilerinizi doğrulayın, banka hesabınızın kullanıcı adını ve şifresini girin gibi. Bazen çok inandırıcı olabilirler, mesajlar sizin halihazırda olan hesaplarınızdan geliyor numarası yapabilir veya linki kullanmazsanız hesabınızın askıya alınacağı gibi korkutma yöntemleri seçebilirler.

Phishingler ayrıca keylogger truva atları gibi spywareleri kullanarak hesap bilgilerinizi direk olarak bilgisayarınızdan çalabilirler.

Phishing mesajlarının ana hedefi eBay, PayPal, bankaların internet şubeleri gibi müşterilerin online ödeme servisleridir Son dönemde sosyalleşme websiteleri kişisel bilgileri kullanarak kimliklerin çalınmasına olanak sağladığı için phishinglerin hedefi haline gelmiştir.

İnternette dolaşırken phishing tehlikelerine karşı korunmak için **Antiphishing**' i etkin halde tutun. Bu yolla, BitDefender siz erişmeden önce her web sitesini taracayak, ve olabilecek phishing tehditlerine karşı sizi uyaracaktır. BitDefender tarafından düzenlenecek Beyaz Liste' deki web siteleri taranmayacaktır.

Antiphishing korumasını ve Beyaz Listeyi kolayca yönetebilmek için Internet Explorer' a entegre edilmiş Antiphishing araç çubuğunu kullanın. Daha fazla bilgi için "*Antiphishing Araç Çubuğu*" (shf. 101) bölümüne bakınız.

9.2. İleri Ayarlar – Kişisel Gizlilik Kontrolü

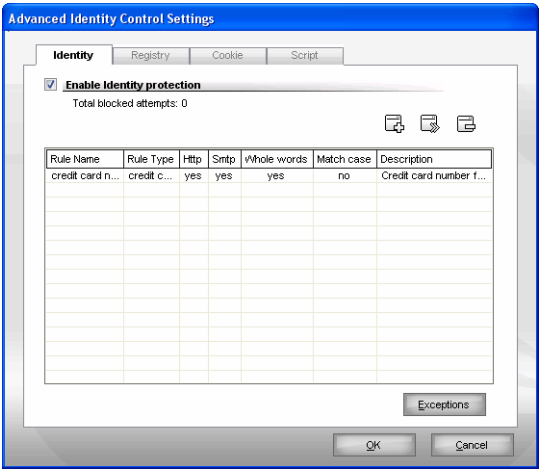
Gizli verileri güvenli tutmak hepimizi endişelendiren önemli bir konudur. Veri hırsızları, İnternet iletişiminin gelişimine ayak uydurarak, insanları aldatıp, özel bilgileri elde edebilmek için yeni yöntemler kullanmaktadır.

Kişisel Gizlilik Kontrolü kişiye özel gizli verilerinizi güvende tutmanıza yardımcı olur. HTTP veya SMTP trafiğini, veya her ikisini de, tanımlamış olduğunuz belirli dizgiler için tarar. Bir eşleşme bulduğunda, ilgili web sayfası veya e-posta engellenir.

Çoklu kullanıcı desteğinin sağlandığı sistemlerde, başka herhangi bir kullanıcı sizin düzenlediğiniz kuralları göremez.

Gizlilik kurallarını **Kişisel Gizlilik** bölümünden düzenleyebilirsiniz. Bu bölüme erişmek için **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden **Kişisel Gizlilik** tabına tıklayınız.

Not
Bu bölüme girmek için, **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden**Gizlilik Kontrolü>Durumu'** nu tıklayın. Sonra ayarlar konsolundan, **Gelişmiş Ayarlar'** ı tıklayın.



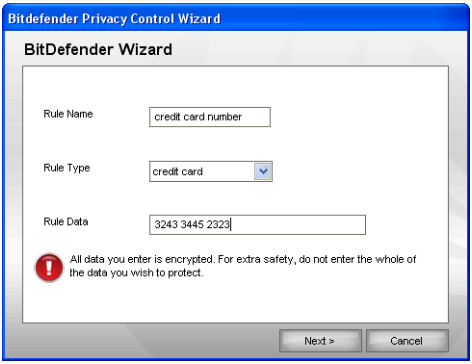
Kimlik Kontrolü

9.2.1. Kimlik Kurallarını Yaratmak

Kurallar manuel olarak girilmelidir (**Ekle** seçeneğini tıklayın ve kural için parametreleri seçin). Yapılandırma sihirbazı ekrana gelecektir

Yapılandırma sihirbazı 3 adımlı bir prosedürden oluşmaktadır.

Adım 1/3 – Kural Tipini ve Veriyi Belirle



Kural Tipini ve Veriyi Belirle

Düzenleme alanına kural ismini girin.

Aşağıda belirtilen parametreleri ayarlamanız gerekmektedir:

- **Kural Tipi** – kural tipini seçin (adres, isim, kredi kartı, PIN, SSN, vs.).
- **Kural Verisi** – Kural verisini girin

Not
Bizim önerimiz kural isminin en az üç karakterden oluşmasıdır. Eğer kural ismi üç karakterden az olursa mesajları ve web sayfalarını engellemede problemler yaşanabilir.

Girdiğiniz bütün veriler şifrelenecektir. Ekstra güvenlik için, korumak istediğiniz verilerin hepsini girmeyin.

İleri'yi tıklayın.

Adım 2/3 – Trafiği Seçin

Trafiği Seç

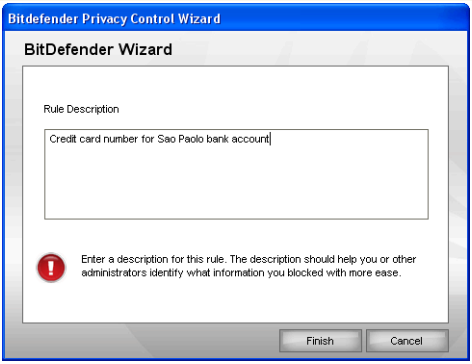
BitDefender'ın taramasını istediğiniz trafiği seçin. Aşağıdaki seçenekler mevcuttur:

- **HTTP'yi Tara**- HTTP (web) trafiğini tarar ve kural verisi ile eşleşen dışarı giden veriyi engeller.
- **SMTP'yi Tara** - SMTP (mail) trafiğini tarar ve kural verisini içeren dışarı giden e-posta mesajlarını engeller.

Kuralı uygulamak için kural verilerinin sadece tüm kelimelerle uymasını yada saptanan dizgi ile uymasını seçebilirsiniz.

İleri'yi tıklayın.

Adım 3/3 – Kuralı Tanımlayın



Kural Tanımla

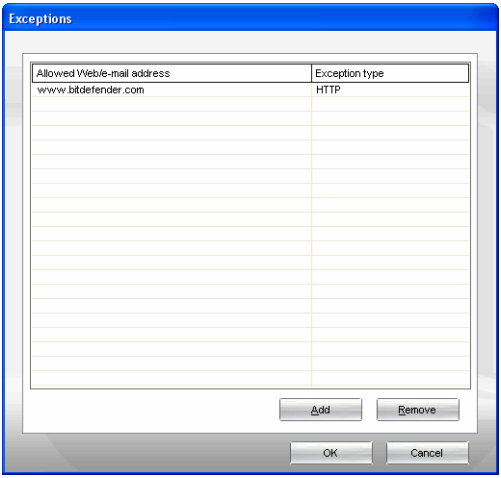
Düzenleme alanına, kuralın kısa bir tanımını girin.

Bitir seçeneğini tıklayın.

9.2.2. İstisnaları Belirleme

Bu bölüme özel kişisel gizlilik kuralları için istisnaları belirlerken ihtiyacınız olacak. Bu bölümü, HTTP (web) üzerinden kredi kartı numarası gönderilmesini engellemek için kural yaratacağımızda göz önüne alalım. Kredi kartı numaranız kullanıcı hesabınızla bir web sitesine gönderildiğinde sayfa bloklanır. Örnek olarak internet üzerinden (güvenli olduğunu bildiğiniz) bir giyim eşyası satın almak istediğinizde, bunu istisna olarak belirlemeniz gerekir.

İstisnaları yönetebileceğiniz pencereyi açmak için, **İstisnalar'** a tıklayın.



İstisnalar

İstisna eklemek için bu adımları takip edin:

1. Tabloya yeni bir giriş yapmak için **Ekle**' ye tıklayın.
2. **İzin verilen adresleri belirle**' ye çift tıklayıp istisna olarak eklemek istediğiniz web veya mail adreslerini yazın.
3. **Tipi Seçin**' ne çift tıklayıp uygun adres tipini seçin.
   - Bir web adresi belirlemek istiyorsanız **HTTP**' yi seçin.
   - Bir web adresi belirlemek istiyorsanız **SMTP**' yi seçin.

Listeden bir istisnayı kaldırmak istiyorsanız, istisnayı seçip **Kaldır**' ı tıklayın.

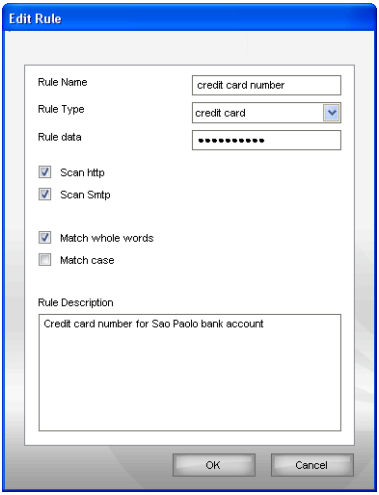
Değişiklikleri kaydetmek için **Tamam** tuşuna basın.

9.2.3. Kuralların Yönetimi

Kuralın tabloda listelendiğini göreceksiniz.

Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralı silmeden, geçici olarak etkisiz kılmak için karşılık gelen onay kutusunu temizleyin.

Bir kuralı düzenlemek için, kuralı seçin ve **Düzenle** seçeneğini tıklayın veya kural üzerine çift tıklayın. Yeni pencere görünecektir.



Kural Düzenle

Bu bölümde, kuralın ismini, tanımını ve parametrelerini (tip, veri ve trafik) değiştirebilirsiniz. Değişiklikleri kaydetmek için **Tamam** seçeneğini tıklayın.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

9.3. Gelişmiş Ayarlar – Kayıt Kontrolü

Windows işletim sisteminin en önemli kısımlarından biri **Kayıt** olarak adlandırılmaktadır. Windows; kendisi ile ilgili ayarları, yüklenmiş programları, kullanıcı bilgilerini ve bunun gibi diğer bilgileri burada tutar.

Kayıt, ayrıca Windows başlatıldığında hangi programların otomatik olarak çalıştırılacağını belirlemek için de kullanılır. Kullanıcı bilgisayarını yeniden çalıştırdığı zaman virüsler otomatik olarak başlatılmak için bunu kullanırlar.

Kayıt Kontrolü Windows'un Kaydını kontrol eder – Bu aynı zamanda Truva atları (Tojan Horses) algılamak içinde faydalıdır. Bir program, Windows başlatıldığında çalıştırılmak için kayıt bilgilerini değiştimeye çalıştığında sizi uyaracaktır.

Kayıt Uyarısı

Bu değişikliği reddetmek için **Hayır**seçeneğini tıklayabilir veya değişiklik yapılmasına izin vermek için **Evet** seçeneğini tıklayabilirsiniz.

BitDefender'ın sizin yanıtınızı hatırlaması için, **Bu yanıtı hatırla** seçeneğine karşılık gelen onay kutusunu işaretlemeniz gerekir Bu yolla, bir kural yaratılacağında ve aynı eylem uygulanacağında bu program Windows başlangıcında uygulamak üzere kayıt girdisini değiştirmeye çalışacaktır.

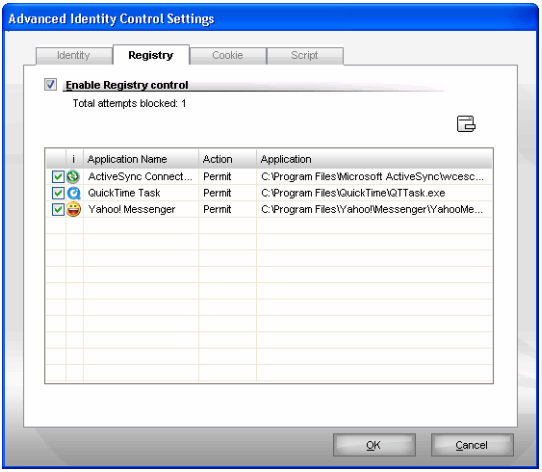
Not

Bilgisayarınızın bir sonraki başlatılmasında çalıştırılması gereken yeni programlar yüklediğinizde, BitDefender genelde sizi uyaracaktır. Çoğu durumda, bu programlar yasal ve güvenilirdir

Hatırlanan her bir kurala daha ileri ayarlar yapmak için **Kayıt** bölümünden erişebilirsiniz. Bu bölüme erişmek için **Gelişmiş Kişisel Gizlilik Ayarları** bölümünden**Kayıt** tabına tıklayınız.

Not

Bu bölüme girmek için, **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden**Gizlilik Kontrolü>Durumu'** nu tıklayın. Sonra ayarlar konsolundan, **Gelişmiş Ayarlar'** ı tıklayın.



Kayıt Kontrolü

Kuralın tabloda listelendiğini göreceksiniz.

Bir kuralı silmek için, kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralı silmeden geçici olarak devredışı bırakmak için uygun kutucuktaki işareti kaldırın.

Bir kuralın eylemini değiştirmek için, eylem sahasını çift tıklayıp menüden uygun seçeneği seçin.

Pencereyi kapatmak için **Tamam** seçeneğini tıklayın.

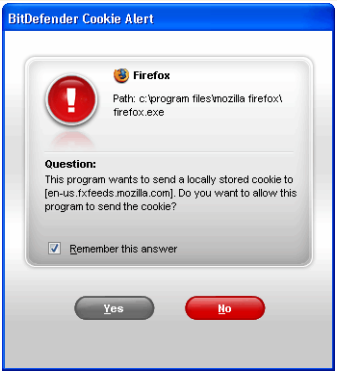
9.4. Gelişmiş Ayarlar - Cookie Kontrolü

Cookie'ler Internette çok yaygın olarak rastlanmaktadır. Bunlar, bilgisayarınıza kaydedilen küçük dosyalardır. Web siteleri, sizin hakkınızda belirli bilgileri izlemek için bu cookie'leri yaratırlar.

Cookie'ler genel olarak hayatınızı kolaylaştırmak için yaratılmışlardır. Örneğin, web sitesinin sizin isminizi ve tercihlerinizi hatırlamasına yardımcı olur ve bu sayede web sitesini her ziyaret ettiğinizde bu bilgileri tekrar girmenize gerek kalmaz.

Fakat cookie'ler aynı zamanda tarama şablonunuzu izleyerek sizin gizliliğinizden ödün vermenize neden olacak şekilde de kullanılabilir.

Cookie Kontrolü işte bu noktada size yardımcı olur. Etkinleştirildiğinde, yeni bir web sitesi bir cookie kurmak istediği zaman, **Cookie Kontrolü** sizin izninizi ister



Cookie Uyarısı

Cookie dosyası göndermeye çalışan uygulamanın ismini görebilirsiniz.

Bu yanıtı hatırla seçeneğini seçin, **Evet** veya **Hayır** seçeneğini tıklayın; kurallar tablosunda bir kural oluşturulacak, uygulanacak ve listelenecektir. Böylece, daha sonra aynı siteye bağlandığınızda artık bilgilendirilmeyeceksiniz.

Bu, hangi web sitelerine güvendiğinizi ve hangilerine güvenmediğinizi seçmeniz konusunda size yardımcı olacaktır.

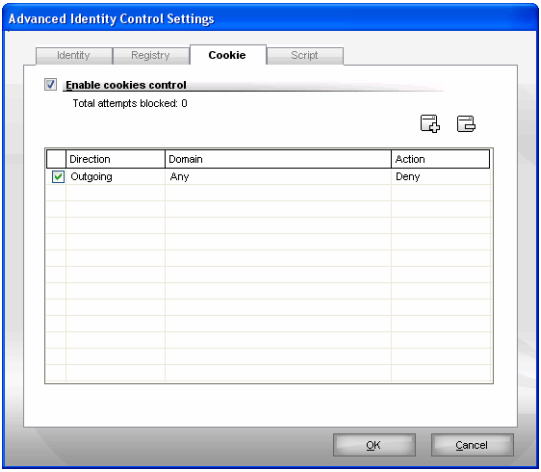
Not

Günümüzde, internette çok sayıda cookie kullanıldığı için, **Cookie Kontrolü** ilk başlangıçta oldukça sıkıcı olabilir. İlk olarak, bilgisayarınıza cookie yerleştimeye çalışan siteler hakkında çok sayıda soru yöneltecektir. Kurallar listesine düzenli olarak taradığınız siteleri ekledikten sonra, internette tarama artık eskisi kadar rahat bir hale gelecektir.

Hatırlanan her kurala, daha sonra ileri ayarlar yapmak için **Cookie** bölümünden erişilebilir. Bu bölüme erişmek için **Gelişmiş Kişisel Gizlilik Kontrolü Ayarları** bölümünden**Cookie** tabına tıklayınız.

Not

Bu bölüme girmek için, **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden**Gizlilik Kontrolü>Durumu'** nu tıklayın. Sonra ayarlar konsolundan, **Gelişmiş Ayarlar'** ı tıklayın.



Cookie Kontrolü

Kuralın tabloda listelendiğini göreceksiniz.

Önemli
Kurallar üstten başlayarak aşağıya doğru önceliklerine göre listelenir, yani listedeki ilk kural en büyük önceliğe sahiptir. Önceliğini değiştirmek için, kuralı listedeki yerinden sürükleyerek istediğiniz yere bırakın.

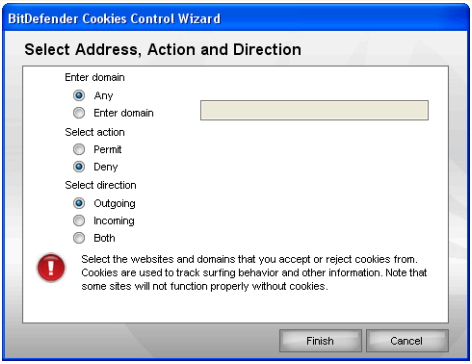
Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralın parametresini değiştirmek için, alanına çift tıklayın ve istediğiniz değişikliği yapın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, buna karşılık gelen onay kutusunu temizleyin.

Kurallar otomatik olarak (uyarı penceresi aracılığıyla) veya elle girilebilirler (**Ekle** seçeneğini tıklayın ve kural için parametreleri seçin). Yapılandırma sihirbazı belirecektir.

9.4.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 1 adımlı bir prosedürden oluşmaktadır.

Adım 1/1 – Adres, İşlem ve Yönü Seçin



Adres, İşlem ve Yönü Seçin

Parametreleri ayarlayabilirsiniz

- **Alan adresi** – Kuralın uygulanacağı Alan adını girin.
- **İşlem** – Kuralın işlemini seçin.

İşlem	*Açıklama*
İzin Ver	Alandaki cookie çalışacak
Reddet	Alandaki cookie'ler çalışmayacak.

- **Yön** – trafik yönünü seçin

Tip	*Açıklama*
Giden	Kurallar sadece bağlanılan sitelere geri gönderilen cookie'ler için geçerli olacaktır.
Gelen	Kurallar sadece bağlanılan sitelerden alınan cookie'ler için geçerli olacaktır.
Her ikisi	Kural her iki yöndede geçerli olacaktır

Bitir seçeneğini tıklayın.

Not
Cookie'leri kabul edebilirsiniz, fakat işlemi **Reddet** ve yönü **Giden** olarak ayarlayarak asla geri gönderemezsiniz.

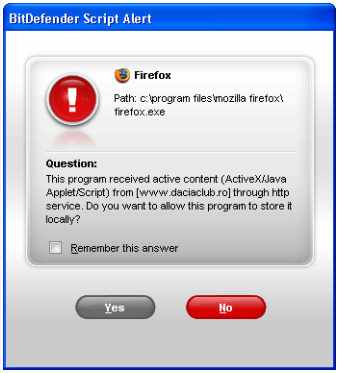
Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

9.5. Gelişmiş Ayarlar - Script Kontrolü

Etkileşimli web sayfaları yaratmak için kullanılan Script ve ActiveX kontrolleri ve Java uygulamaları gibi diğer kodlar zararlı etkiler gösterecek şekilde programlanmış olabilir. Örneğin, ActiveX bileşenleri, çevrimiçi olduğunuzda verilerinize tam erişim sağlayabilir ve bilgisayarınızdaki verileri okuyabilir, bilgileri silebilir, şifreleri elde edebilir ve mesajlarınızı yakalayabilir. Bu yüzden, sadece iyi bildiğiniz ve güvendiğiniz sitelerden gelen aktif içerikleri kabul etmelisiniz.

BitDefender size bu bileşenlerin çalıştırılması veya engellenmesi konusunda seçim yapabilmeniz için olanak sağlamaktadır.

Script Kontrolü ile, hangi sitelere güveneceğiniz hangilerine güvenemeyeceğiniz hakkında karar verme kontrolü sizin elinizde olacaktır. BitDefender, bir web sitesi, script veya diğer aktif içerikleri etkin hale getirmeye çalıştığınızda, sizin izninizi isteyecektir:



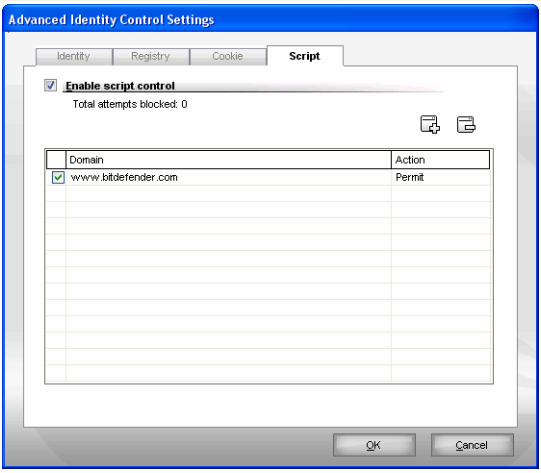
Script Uyarısı

Kaynakların isimlerini görebilirsiniz.

Bu yanıtı hatırla seçeneğini seçip, **Evet** veya **Hayır** seçeneğini tıklayın; kurallar tablosunda bir kural oluşturulacak, uygulanacak ve listelenecektir. Bu site daha sonra size tekrar aktif bir içerik göndermeye çalıştığında artık bilgilendirilmeyeceksiniz

Hatırlanan her bir kurala daha ileri ayarlar yapmak için **Script** bölümünden erişebilirsiniz. Bu bölüme erişmek için **Gelişmiş Kişisel Gizlilik Kontrolü Ayarları** modülünden **Script** tabına tıklayınız.

Not
Bu bölüme girmek için, **Gelişmiş Gizlilik Kontrol Ayarları** bölümünden**Gizlilik Kontrolü>Durumu'** nu tıklayın. Sonra ayarlar konsolundan, **Gelişmiş Ayarlar'** ı tıklayın.



Script Kontrolü

Kuralın tabloda listelendiğini göreceksiniz.

Önemli
Kurallar üstten başlayarak aşağıya doğru önceliklerine göre listelenir, yani listedeki ilk kural en büyük önceliğe sahiptir. Önceliğini değiştirmek için, kuralı listedeki yerinden sürükleyerek istediğiniz yere bırakın.

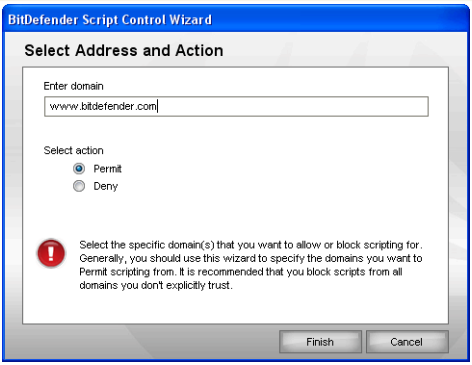
Bir kuralı silmek için, sadece kuralı seçin ve **Sil** seçeneğini tıklayın. Bir kuralın parametresini değiştirmek için, alanına çift tıklayın ve istediğiniz değişikliği yapın. Bir kuralı silmeden sadece geçici olarak etkisiz kılmak için, buna karşılık gelen onay kutusunu temizleyin.

Kurallar otomatik olarak (uyarı penceresi aracılığıyla) veya elle girilebilirler (**Ekle** seçeneğini tıklayın ve kural için parametreleri seçin). Yapılandırma sihirbazı belirecektir.

9.5.1. Yapılandırma Sihirbazı

Yapılandırma sihirbazı 1 adımlı bir prosedürden oluşmaktadır.

Adım 1/1 – Adres ve İşlemi Seçin



Adres ve İşlemi Seçin

Parametreleri ayarlayabilirsiniz

- **Alan adresi** – Kuralın uygulanacağı Alan adını girin.
- **İşlem** – Kuralın işlemini seçin.

İşlem	Açıklama
İzin Ver	Alandaki Scripts çalışacaktır.
Reddet	Alandaki Scripts çalışmayacaktır.

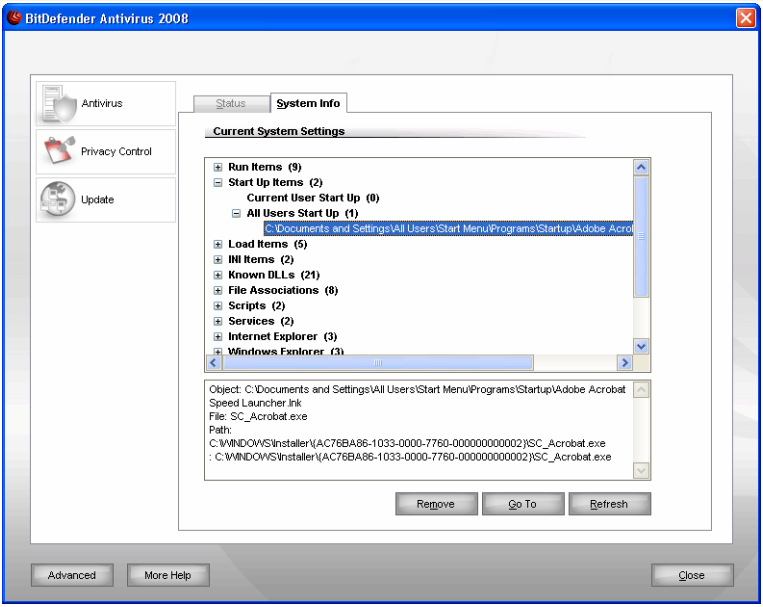
Bitir seçeneğini tıklayın.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

9.6. Sistem Bilgileri

BitDefender, tüm sistem ayarlarını ve başlangıçta çalışan kayıtlı uygulamaları tek bir yerden görmenize izin verir. Bu yolla, sistemdeki aktiviteyi ve yüklenmiş uygulamaları görebileceksiniz, yanısıra sisteme bulaşan enfeksiyonları tanımlayabileceksiniz.

Sistem bilgisine ulaşmak için, ayarlar konsolundan **Kişisel Gizlilik Kontrolü>Sistem Bilgisi'** ni tıklayın. Sıradaki pencere çıkacaktır:



Sistem Bilgileri

Liste, sistem çalıştırıldığında yüklenmiş olan bütün bileşenlerin yanı sıra farklı uygulamalar tarafından yüklenen bileşenleri içermektedir.

Üç buton vardır:

- **Sil** – Seçilen bileşenleri siler. Seçiminizi doğrulamak için, **Evet'** e basmalısınız.

Not
Güncelleme sonrası seçiminizi doğrulayın ibaresini görmek istemiyorsanız, **Bu soruyu tekrar sorma**seçeneğini işaretleyin.

- **Git** – seçilen bileşenlerin bulunduğu bir pencere açar (Örneğin, **Kayıt**).
- **Yenile** – **Sistem Bilgi** bölümünü yeniden açar.

Not
Seçilen öğeye bağlı olarak **Sil** yada **Git** butonlarından biri ya da hepsi görünmeyecektir.

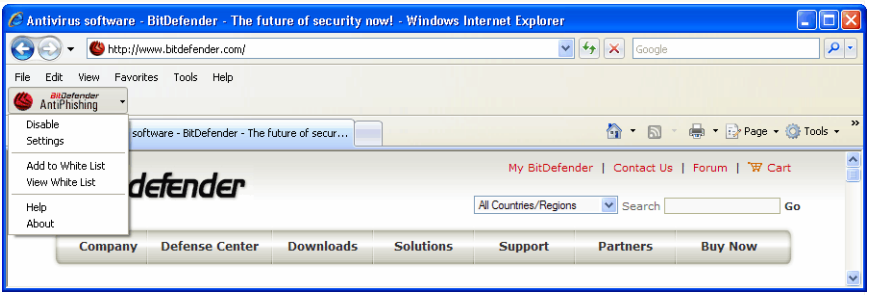
9.7. Antiphishing Araç Çubuğu

BitDefender, sizi, İnternette gezerken phishing denemelerine karşı korur. Erişilen web sitelerini tarayarak herhangi bir phishing tehdidine karşı sizi uyarır. BitDefender tarafından düzenlenecek Beyaz Liste' deki web siteleri taranmayacaktır.

Kolay ve verimli bir şekilde antiphishing korumasını yönetebilirsiniz. Beyaz Liste kullanan BitDefender Antiphishing araç çubuğu Internet Explorer' a entegre edilmiştir.

Antiphishing araç çubuğu, Internet Explorer' ın üst tarafında **BitDefender ikon**' u ile gösterilir. Araç çubuğu menüsünü açmak için üzerine tıklayın.

Not
Eğer araç çubuğunu göremiyorsanız, **Görünüm** menüsünde, **Araç Çubukları** üzerine gelerek **BitDefender Araç Çubuğu**' nu seçin.



Antiphishing Araç Çubuğu

Araç Çubuğu menüsünde aşağıdaki komutlar bulunmaktadır:

- **etkin/etkin değil** - BitDefender Antiphishing araç çubuğu etkin/etkin değil.

Not
Eğer antiphishing araç çubuğunu etkisizleştirirseniz phishing denemelerine karşı etkili bir koruma içinde olmayacaksınız.

- **Ayarlar** - antiphishing araç çubuğu ayarlarını belirleyebileceğiniz bir gözatma penceresini açar.

  Aşağıdaki seçenekler mevcuttur:
  - **Taramayı Etkinleştir** - antiphishing taraması etkinleştirilir.
  - **Beyaz Listeye eklemeden önce sor** - bir web sitesini Beyaz Listeye eklemeden önce sorar.
- **Beyaz Listeye Ekle** - geçerli web sayfasını Beyaz Liste' ye ekler

Not
Beyaz Liste' ye site eklemenin anlamı, BitDefender' ın bu siteyi bir daha taramayacağı demektir. Biz Beyaz Liste' ye sadece tam olarak güvendiğiniz siteleri eklemenizi öneririz.

- **Beyaz Liste** - Beyaz Liste' yi açar.

  BitDefender antiphishing motoru tarafından kontrol edilmeyen tüm web sitelerini görebilirsiniz.

  Bir siteyi, üzerinde var olan phishing tehditlerinden haberdar olabilmek için Beyaz Liste' den kaldırmak istiyorsanız, **Kaldır** tuşuna basın.

  Sadece tamamen güvendiğiniz siteleri Beyaz Liste' ye ekleyiniz, çünkü bu siteler antiphishing motoru tarafından bir daha taranmayacaktır. Beyaz Liste' ye site eklemek için, site adresini uygun alana yazdıktan sonra **Ekle**' ye basın
- **Yardım** - yardım dosyasını açar.
- **Hakkında** - bölümüne tıkladığınızda BitDefender hakkında bilgi alabileceğiniz bir pencere açılır ve acil bir durumda yardım alabileceğiniz yerleri görürsünüz.

10. Güncelleme

Hergün yeni bir kötü amaçlı yazılım bulunmakta ve tanımlanmaktadır. Bu nedenle, BitDefender'ın en yeni kötü amaçlı yazılım imzaları ile güncel kılınması çok önemlidir. Fabrika ayarlarında, BitDefender her saatte güncellemeleri kontrol etmek üzere ayarlanmıştır.

Internete geniş bant veya DSL ile bağlıysanız, BitDefender güncellemeyi kendisi yapar. Bilgisayarınızı açtığınızda ve daha sonra her **saatte bir** güncellemeleri kontrol eder.

Bir güncelleme tespit edildiğinde, Otomatik Güncelleme Seçenekleri bölümündeki seçeneklerin ayarına bağlı olarak, güncellemeyi teyit etmenizi isteyecek veya güncellemeler otomatik olarak yapılacaktır.

Güncelleme işlemi hemen başlayarak, dosyaları kademeli olarak günceller. Güncelleme işlemi devam eden operasyonları etkilemeyecek, tüm kırılganlıkları dışarıda tutacaktır.

Güncellemeler aşağıdaki şekillerde olmaktadır:

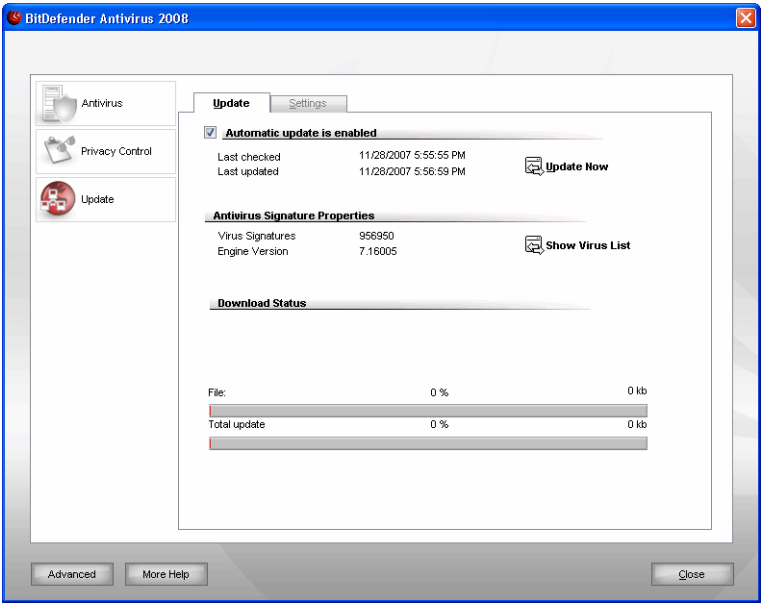
- **Virüs koruma motorları için güncellemeler** – yeni bir tehdit ortaya çıktıkça, bunlara karşı sürekli olarak güncel bir koruma sağlamak amacıyla, virüs imzaları taşıyan dosyaların güncelleştirilmesi gerekmektedir. Bu güncelleme tipi aynı zamanda **Virüs Tanımları Güncellemesi** olarak da bilinmektedir
- **Antispyware motorları güncellemesi** - yeni spyware imzaları veritabanına eklenecektir. Bu güncelleme tipi aynı zamanda **Antispyware Güncellemesi** olarak da bilinmektedir.
- **Ürün yükseltmeleri** - yeni bir ürün sürümü çıkarıldığında, ürün performansını geliştiren yeni özellikler ve tarama teknikleri tanıtılmaktadır.Bu güncelleme tipi aynı zamanda **Ürün Güncellemesi** olarak da bilinmektedir

Bu kullanım kılavuzunun **Güncelleme** modülü aşağıdaki konuları içermektedir:

- Otomatik Güncelleme
- Güncelleme Ayarları

10.1. Otomatik Güncelleme

Güncelleme bilgilerini görmek ve güncellemeleri otomatik yapmak için, ayarlar konsolundan **Güncelle>Güncelle'** yi tıklayın Sıradaki pencere çıkacaktır:



Otomatik Güncelleme

Burada, son güncelleme kontrollerini ve son gerçekleşen güncellemeyi görebilir, ayrıca son güncelleme hakkında bilgi alabilirsiniz (güncelleme başarılı mı, ya da oluşan hatalar). Hem geçerli versiyon numarası hem de imza sayısı görüntülenir.

BitDefender'ınızın kötü amaçlı yazılım imzalarını **Virüs Listesini Göster** seçeneğini tıklayarak görebilirsiniz. Mevcut tüm imzaları içeren bir HTML dosyası oluşturulacaktır. Listeyi görmek için **Virüs Listesini Göster** seçeneğini tekrar tıklayın. Özel bir kötü amaçlı yazılım imzasını veri tabanından arayabilir veya BitDefender imza veri tabanına gitmek için **BitDefender Virüs Listesi** seçeneğini tıklayabilirsiniz.

Eğer bu pencereyi bir güncelleme esnasında açarsanız, yükleme durumunu görebilirsiniz.

Önemli
En son tehlikelere karşı korunmak için **Otomatik Güncelleme**'yi etkin halde tutun.

10.1.1. Güncelleme İsteği

Şimdi Güncelle seçeneği tıklayarak otomatik güncellemeyi istediğiniz herhangi bir zamanda yapabilirsiniz. Bu güncelleme **Kullanıcı isteği** üzerine güncelleme olarak da bilinir.

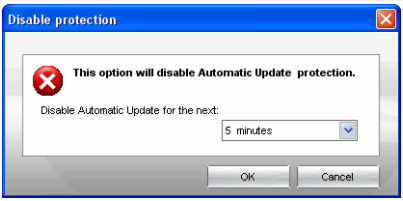
Güncelleme Modülü, BitDefender Güncelleme Sunucusuna bağlanacak ve herhangi bir güncelleme varsa bunu teyit edecektir. Bir güncelleme tespit edildiğinde, Manuel Güncelleme Seçenekleri bölümündeki seçeneklerin ayarlarına bağlı olarak, güncellemeyi teyit etmeniz istenecek veya güncelleme otomatik olarak yapılacaktır.

Önemli
Güncellemeyi tamamladıktan sonra bilgisayarınızı yeniden başlatmanız gerekebilir. Bunu mümkün olan en kısa zamanda yapmanızı öneririz.

Not
Eğer internete bir çevirmeli bağlantı ile bağlıysanız, bu takdirde BitDefender'ı kullanıcı isteği ile güncellemeyi düzenli bir alışkanlık haline getirmeniz iyi bir fikir olacaktır.

10.1.2. Otomatik Güncellemeyi Kapatma

Otomatik güncellemeyi kapatırsanız, bir uyarı penceresi açılacaktır.



Otomatik Güncellemeyi Kapat

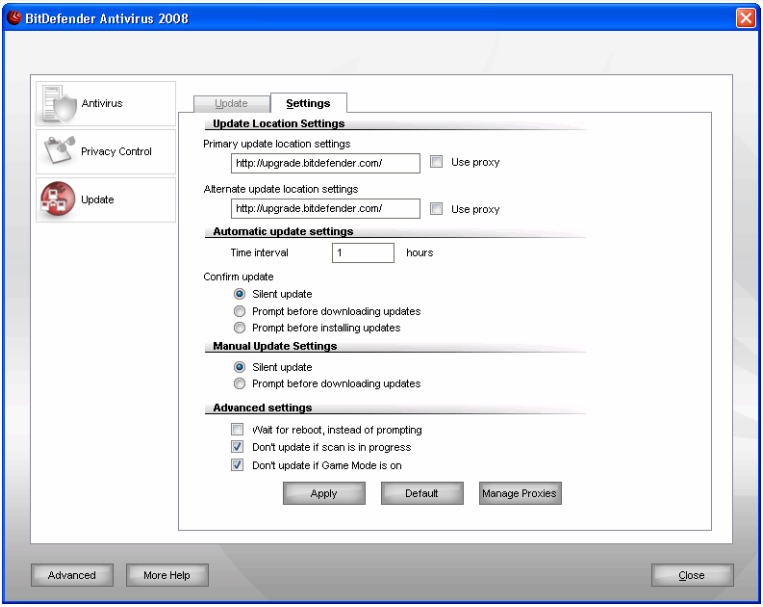
Gerçek zamanlı korumayı ne kadar süre için kapatacağınızı menüden seçerek belirlemelisiniz. Bunu 5, 15, 30, dakika veya 1 saat için, ya da sürekli olarak veya sistem tekrar başlatılana dek kapatabilirsiniz.

Uyarı
Bu kritik bir güvenlik sorunudur. Eğer gerçek zamanlı koruma kapatılırsa tehditlere karşı korumasız kalırsınız, bu nedenle biz bunu kısa süreler için tavsiye ediyoruz.

10.2. Güncelleme Ayarları

Güncellemeler, yerel ağda, internet üzerinden direkt olarak veya Vekil Sunucu üzerinden yapılabilir. Varsayılan olarak, BitDefender, saatbaşı güncelleme yapar, internet üzerinden mevcut güncellemeleri size herhangi bir uyarı yapmadan yükler.

Güncelleme ayarlarını ve vekil sunucuları yapılandırmak için, **Güncelleme>Ayarları**' nı tıklayın. Sıradaki pencere çıkacaktır:



Güncelleme Ayarları

Güncelleme ayarlarının bulunduğu pencere 4 seçenek kategorisi (**Güncelleme Yer Ayarları** , **Otomatik Güncelleme Seçenekleri**, **Manuel Güncelleme Ayarları** ve **Gelişmiş Ayarlar**) içerir. Her kategori ayrı olarak tanımlanacaktır.

10.2.1. Güncelleme Yeri Ayarları

Güncelleme yerini ayarlamak için, **Güncelleme Yeri Ayarları** kategorisindeki seçenekleri kullanın.

Not
Buradaki seçenekleri sadece, bir yerel ağa bağlı iseniz ve bu ağda BitDefender güncellemeleri tutuluyorsa veya internete bir vekil sunucu üzerinden çıkıyorsanız yapılandırabilirsiniz.

Daha güvenilir ve hızlı bir güncelleme için, iki güncelleme yeri yapılandırabilirsiniz: biri **Ana Güncelleme Yeri** ve diğeri **Alternatif Güncelleme Yeri**'dir. Her ikisi için de aşağıdaki seçenekleri yapılandırmalısınız:

Güncelleme yerini değiştirmek için, **URL** alanına yerel ağınızdaki yolu yazabilirsiniz.

Not
Biz, öncelikli güncelleme yerine yerel ağınızdaki yolu gösterdiğinizde, herhangi bir şekilde oraya ulaşılamaması durumuna karşı, alternatif güncelleme yerini değiştirmemenizi öneririz.

İnternete bağlanmak için bir vekil sunucu kullanıldığı durumlarda, **Vekil Sunucu Kullan** kutucuğunu işaretleyip, **Vekil Sunucular** tuşuna basarak ayarları yapınız.

Not
Daha fazla bilgi için bakınız,"*Vekil Sunucuları Yönetmek*" (shf. 109)

10.2.2. Otomatik Güncelleme Yapılandırma

BitDefender' ın güncellemeleri otomatik olarak yapmasını istiyorsanız **Otomatik Güncelleme Ayarları'** nı kullanın.

Güncelleme zamanını **Zaman aralığı** alanından belirleyebilirsiniz. Varsayılan olarak 1 saate ayarlanmıştır.

Otomatik güncellemenin nasıl yapılacağını aşağıdaki seçeneklerden belirleyebilirsiniz.

- **Sessiz Güncelleme** - BitDefender güncellemeyi otomatik olarak indirir ve uygular.
- **İndirmeden önce sor** – güncellemenin her bulunuşunda, indirmeden önce sizi uyaracaktır.

Not
Güvenlik Merkezinin dışında olsanız dahi güncelleme indirmeleri yapılacaktır.

- **Yüklemeden önce sor** – güncellemenin her indirilişinde, yüklemeden önce sizi uyaracaktır.

Not
Güvenlik Merkezinin dışında olsanız dahi güncelleme yapılacaktır.

10.2.3. Manuel Güncelleme Yapılandırma

Manuel güncellemenin (kullanıcı isteği ile güncelleme) nasıl yapılacağını belirlemek için, **Manuel Güncelleme Ayarları** kategorisinden bir seçenek seçmelisiniz.

- **Sessiz Güncelleme**manuel güncelleme arka planda otomatik olarak yapılacaktır.
- **İndirmeden önce sor** – güncellemenin her bulunuşunda, indirmeden önce sizi uyaracaktır.

Not
Güvenlik Merkezinin dışında olsanız dahi güncelleme indirmeleri yapılacaktır.

10.2.4. Gelişmiş Ayarları Yapılandırma

BitDefender güncelleme işleminin sizi engellemesine engel olmak için, **Gelişmiş Ayarlar** kategorisindeki seçenekleri yapılandırın.

- **Uyarı yerine, yeniden başlatma için bekle** - Eğer bir güncelleme bilgisayarın yeniden başlatılmasını gerektiriyorsa, sistem tekrar başlatılana kadar ürün eski dosyalar ile çalışmaya devam edecektir. Kullanıcıya sistemin yeniden başlatılması bilgisi verilmeyecek ve bu nedenle BitDefender güncelleme süreci, kullanıcının çalışmasını engellemeyecektir.
- **Eğer tarama çalıştırılıyorsa, güncelleme yapma** - Eğer bir tarama işlemi çalışıyorsa, BitDefender güncelleme yapmayacaktır. Bu şekilde, BitDefender güncelleme süreci tarama işlemlerini engellemeyecektir

Not
Tarama çalışırken BitDefender güncellenirse, tarama işlemi yarıda kesilecektir.

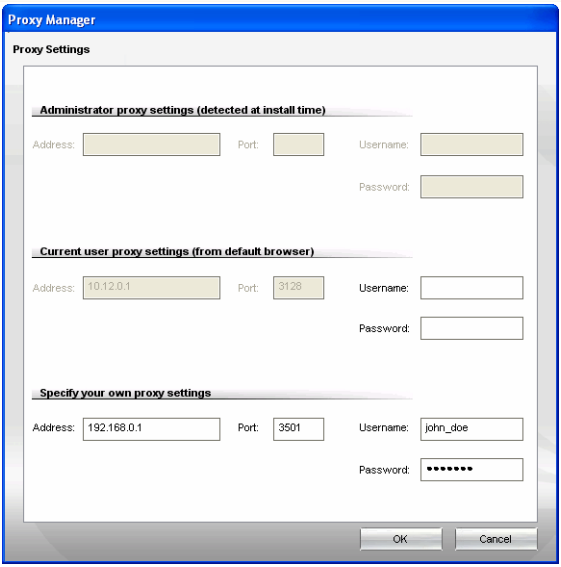
- **Oyun modu açık iken güncelleme yapma** - BitDefender oyun modu açık ise güncelleme yapmayacaktır. Bu yolla, oyun esnasında sistem performansına etkisi en az derecede olur.

10.2.5. Vekil Sunucuları Yönetmek

Eğer internet bağlantısı için vekil sunucu kullanıyorsanız, BitDefender' ın güncellemeleri kendi başına yapabilmesi için vekil sunucu ayarlarını belirlemelisiniz. Aksi taktirde geçerli kullanıcı için yüklü olan tarayıcının, yada yöneticinin ayarlarını kullanacaktır.

Not
Vekil sunucu ayarları sadece yönetici yetkisine sahip kullanıcılar tarafından yapılandırılabilir.

Vekil sunucu ayarlarını yönetmek için, **Vekil Sunucuları Yönet'** i tıklayın. **Vekil Sunucu Yönetimi** diye bir pencere açılacaktır.



Vekil Sunucu Yöneticisi

Vekil sunucu ayarlarında üç adet ayar bulunmaktadır:

- **Yönetici vekil sunucu ayarları (Yükleme esnasında saptanan)** Vekil sunucu ayarları, yükleme sırasında bir yönetici hesabı saptar ve sadece bu hesapla girildiğinde yapılandırılabilir. Eğer vekil sunucunuz için kullanıcı adı ve şifre gerekiyorsa uygun alanlara yazmalısınız.

- **Geçerli kullanıcı vekil sunucu ayarları(from default browser)** - Geçerli kullanıcının vekil sunucu ayarları, varsayılan tarayıcıdan alınır. Eğer vekil sunucunuz için kullanıcı adı ve şifre gerekiyorsa uygun alanlara yazmalısınız.

Not
Dekteklenen web tarayıcılar, Internet Explorer, Mozilla Firefox ve Opera' dır. Eğer varsayılan tarayıcınız başka biri ise, BitDefender geçerli kullanıcının vekil sunucu ayarlarını sağlayamayacaktır.

- **Kendi vekil sunucu ayarlarınız** – yönetici olarak giriş yaptıysanız vekil sunucu ayarlarınızı yapılandırabilirsiniz.

  Aşağıdaki seçenekler mevcuttur:
  - **Adres** – Vekil sunucunun IP adresini yazın.
  - **Port** –BitDefender' ın vekil sunucuya bağlanmak için kullanacağı port numarasını yazın.
  - **Vekil Kullanıcısı** – Vekil tarafından kabul edilen bir kullanıcının ismini girin.
  - **Vekil şifresi** – daha önce tanımlanan kullanıcı için geçerli bir şifre girin.

Internete bağlanmaya çalışıldığında, BitDefender bağlantıyı yönetene kadar her vekil sunucu ayarı çalışacaktır.

İlk önce kendi vekil sunucu ayarlarınız kullanılarak internete bağlanılacaktır. Bağlantı başarısız olursa vekil sunucu ayarları yükleme anında saptadığı ayarlar ile bağlanmayı deneyecektir. Son olarak, bunların hiçbiri çalışmazsa varsayılan tarayıcıdan alınan ayarlar ile internete bağlanılacaktır.

Değişiklikleri kaydetmek ve pencereyi kapatmak için **Tamam**'ı tıklayın.

Değişiklikleri kaydetmek için **Uygula** seçeneğini tıklayın veya varsayılan ayarları yüklemek için **Varsayılan** seçeneğini tıklayın.

BitDefender Kurtarma CD'si

11. Tanıtma

BitDefender Antivirus 2008, işletim sisteminiz başlamadan önce tüm mevcut sabit diskleri tarayacak ve temizleyecek nitelikte bir başlangıç CD'si ile birlikte gelmektedir (BitDefender Kurtarma CDsi).

BitDefender Kurtarma CD'sini, virüs bulaşması nedeniyle işletim sisteminizin düzgün olarak çalışmadığı durumlarda kullanmalısınız. Bu durum, çoğu zaman bir virüs koruma programı kullanılmadığı takdirde ortaya çıkar.

Virüs imzalarının güncellenmesi, BitDefender Kurtarma CD'sini her başlattığınızda kullanıcı müdahelesine gerek kalmadan otomatik olarak yapılır.

BitDefender Kurtarma CD'si, BitDefender ile yeniden yapılandırılmış bir Knoppix dağıtımı olup, Linux güvenlik çözümü için yaratılan en son BitDefender versiyonunu GNU/Linux Knoppix Live CD ile entegre ederek, kullanımı kolay SMTP virüs koruma/antispam koruma sağlayan ve mevcut sabit diskleri (Windows NTFS ana bellek kesimleri dahil), Samba/Windows paylaşımlarını veya NFS yükleme noktalarını tarayan ve temizleyen bir masaüstü virüs koruma yazılım paketi sunmaktadır. BitDefender çözümlerine ulaşmak için Web tabanlı bir yapılandırma arayüzü de pakete dahil edilmiştir.

Not
BitDefender Kurtarma CD' sini indirmek için: http://download.bitdefender.com/rescue_cd/

11.1. Sistem Gereksinimleri

Bilgisayarınızı BitDefender Kurtarma CD'si ile başlatmadan önce, ilk olarak sisteminizin aşağıda belirtilen gereksinimleri karşılayıp karşılamadığını teyit etmeniz gerekmektedir

İşlemci tipi
x86 uyumlu, minimum 166 MHz, fakat bu durumda mükemmel bir performans beklenmemelidir. 800MHz, i686 nesil bir işlemci daha iyi bir seçim olacaktır.

Bellek
Minimum 512 MB RAM Bellek (1 GB tavsiye edilmektedir)

CD-ROM
BitDefender Kurtarma CD'si bir CD-ROM'dan çalıştırılır. Bu nedenle, bir CD-ROM ve başlatılabileceği bir BIOS gerekmektedir.

Internet bağlantısı

BitDefender Kurtarma CD'si internet bağlantısı olmadan da çalışabilmesine rağmen, güncelleme işlemleri için, bir vekil sunucu üzerinden olsa bile faal bir HTTP bağlantısı gerekmektedir. Bu yüzden, güncel bir koruma için internet bağlantısı, bir GEREKLİLİKTİR.

Grafik çözünürlüğü

Standard SVGA-uyumlu grafik kartı.

11.2. Dahil edilen Yazılımlar

BitDefender Kurtarma CD'si aşağıda belirtilen yazılım paketlerini içermektedir.

Xedit

Bu bir text dosyası editörüdür.

Vim

Bu sözdizimi vurgularını, GUI ve daha fazlasını içeren güçlü bir text dosyası editörüdür. Daha fazla bilgi için lütfen, Vim Anasayfası sitesine başvurun.

Xcalc

Bu bir hesaplayıcıdır.

RoxFiler

RoxFiler, hızlı ve güçlü bir grafik dosya yöneticisidir.

Daha fazla bilgi için lütfen, Daha fazla bilgi için lütfen, RoxFiler homepage sitesine başvurun.

MidnightCommander

GNU Midnight Commander (mc) bir text-mode dosya yöneticisidir.

Daha fazla bilgi için lütfen, Daha fazla bilgi için lütfen, MC homepage sitesine başvurun.

Pstree

Pstree çalışan işlemleri görüntüler.

Top

En üstte Linux görevleri görüntülenir.

Xkill

Xkill, müşteri tarafından onun X kaynaklarını öldürür.

Partition Image

Partition Image, EXT2, Reiserfs, NTFS, HPFS, FAT16, and FAT32 dosya sistemi formatlarını bir imaj dosyasına yedeklemenize yardımcı olur. Bu program yedekleme amacı ile kullanılabilir.

Daha fazla bilgi için lütfen, Partimage homepage sitesini ziyaret edin.

GtkRecover

GtkRecover, GTK versiyonlarının konsol program kurtarıcısıdır. Dosya kurtarmanıza yardımcı olur.

Daha fazla bilgi için lütfen, GtkRecover homepage sitesini ziyaret edin.

ChkRootKit

ChkRootKit, bilgisayarınızı rootkitlere karşı taramanıza yardımcı olur.

Daha fazla bilgi için lütfen, ChkRootKit homepage sitesini ziyaret edin.

Nessus Network Scanner

Nessus, Linux, Solaris, FreeBSD, ve Mac OS X için bir uzak güvenlik tarayıcısıdır.

Daha fazla bilgi için lütfen, Nessus homepage sitesini ziyaret edin.

Iptraf

Iptraf bir IP ağ görüntüleme yazılımıdır.

Daha fazla bilgi için lütfen, Iptraf homepage sitesini ziyaret edin.

Iftop

Iftop arayüzün kullandığı bant genişliğini görüntüler.

Daha fazla bilgi için lütfen, Iftop homepage sitesini ziyaret edin.

MTR

MTR bir ağ tanımlama aracıdır.

Daha fazla bilgi için lütfen, MTR homepage sitesini ziyaret edin.

PPPStatus

PPPStatus, gelen ve giden TCP/IP trafiğinin istatistiklerini görüntüler.

Daha fazla bilgi için lütfen, PPPStatus homepage sitesini ziyaret edin.

Wavemon

Wavemon, kablosuz ağ cihazları için bir görüntüleme uygulamasıdır.

Daha fazla bilgi için lütfen, Wavemon homepage sitesini ziyaret edin.

USBView

USBView, USB noktalarında bağlı olan cihazları gösterir.

Daha fazla bilgi için lütfen, USBView homepage sitesini ziyaret edin.

Pppconfig

Pppconfig, otomatik olarak çevirmeli ppp bağlantısını ayarlar.

DSL/PPPoe

DSL/PPPoe, PPPoE (ADSL) bağlantısına göre yapılandırılmıştır.

I810rotate

I810rotate, i810 üzerinde i810switch(1) donanımı kullanan bir video çıkışıdır.

Daha fazla bilgi için lütfen, I810rotate homepage sitesini ziyaret edin.

Mutt

Mutt güçlü text tabanlı bir MIME mail istemcisidir.

Daha fazla bilgi için lütfen, Mutt homepage sitesini ziyaret edin.

Mozilla Firefox

Mozilla Firefox tanınan bir web tarayıcısıdır.

Daha fazla bilgi için lütfen, Mozilla Firefox homepage sitesini ziyaret edin.

Elinks

Elink text mode bir web tarayıcısıdır.

Daha fazla bilgi için lütfen, Elinks homepage sitesini ziyaret edin.

12. BitDefender Kurtarma CD'si nasıl kullanılır.

Bu bölümde bilgisayarınızı kötücül yazılımlara karşı, BitDefender ile taramanın ve Windows PC' nizin yedeklerinin nasıl alınacağını bulacaksınız. Bununla birlikte bu CD ile beraber gelen yazılım uygulamaları ile bu kullanıcı rehberindeki açıklamalar dışında daha bir çok görev yapabilirsiniz.

12.1. BitDefender' ı Başlatmak

CD'yi başlatmak için, bilgisayarınızın BIOS'unu CD'yi yükleyecek şekilde ayarlayın, CD'yi sürücüye yerleştirin ve bilgisayarı yeniden başlatın. Bilgisayarınızın CD'den ön yükleme yapabileceğinden emin olun.

Bir sonraki ekran belirene kadar bekleyin ve BitDefender' ı çalıştırmak için ekrandaki talimatları takip edin.

Boot Splash Ekranı

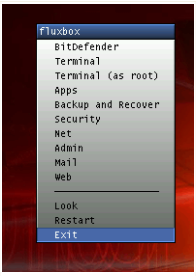
Virüs imzalarının güncellenmesi, yükleme başlangıcında otomatik olarak yapılır. Bu biraz zaman alabilir.

Ön yükleme işlemi tamamlandıktan sonra bir sonraki masaüstünü göreceksiniz. Artık BitDefender' ı kullanmaya başlayabilirsiniz.

Masaüstü

12.2. BitDefender Kurtarma CD'sini Durdur

BitDefender Kurtarma CD'sinden düzgün şekilde çıkmak için, BitDefender menüsünden **Çık** seçeneğini seçerek veya bir terminalde **halt** komutu vererek bilgisayarınızı güvenli bir şekilde kapatabilirsiniz..



"ÇIKIŞ"'ı seçiniz

BitDefender Kurtarma CD'si tüm programları başarılı bir şekilde kapattığında, aşağıdaki gibi bir ekran görünecektir. Bilgisayarınızı sabit diskinizden başlatmak için CD'yi sürücüden çıkartabilirsiniz. Şimdi bilgisayarınızı kapatabilir veya yeniden başlatabilirsiniz

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspe
) (aio/0) Done.
Waiting for processes to finish.....................................
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....................................
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

Kapanırken bu mesaj için bekleyin

12.3. Bir virüs koruma taraması nasıl yapabilirim?

CD' den başlama işlemi bittiğinde, bilgisayarınızı tam olarak tarayabileceğiniz bir sihirbaz görünecektir. **Başla** tuşuna basın.

Not
Eğer ekran çözünürlüğünüz yeterince yüksek değilse, taramaya text modda başlamanız istenecektir.

Takip eden üç adımda tarama süreci rehber eşliğinde tamamlanır.

1. Tarama durumunu ve istatistikleri görebilirsiniz (tarama hızı, geçen süre, taranan sayısı / bulaşmış / şüpheli / gizli objeler ve diğerleri)

Not
Tarama süreci, taramanın karmaşıklığına bağlı olarak, belirli bir zaman alabilir

2. Sisteminizi etkileyen sorunun adedini görebilirsiniz.

   Gruplarda görünen sorunlar. Bir seçeneği açmak için “+” olan kutuyu, seçeneği kapatmak için “-” olan kutuyu tıklayın.

   Her grup için bütün işlemleri seçebilir veya her sorun için ayrılmış işlemi seçebilirsiniz.

3. Sonuçların özetini görebilirsiniz.

Sadece belirli bir dizini taramak istiyorsanız, aşağıdaki adımları takip edin:

Klasörlerinize gözatın, bir dosya veya klasörü sağ-tıklayın ve **Gönder** seçeneğini seçin. Sonra, **BitDefender Tarayıcıyı** seçin.

Veya bir sonraki komutu bir kaynak olarak (root) terminalde verebilirsiniz. **BitDefender Virüs koruma Tarayıcı**, varsayılan tarama yeri olarak seçilen dosya veya klasör ile başlayacaktır.

```
# bdscan /path/to/scan/
```

12.4. BitDefender' ı bir vekil sunucu üzerinden nasıl güncelleştirebilirim?

Eğer internete bağlanmak için bir vekil sunucu kullanıyorsanız, güncelleştirme için bazı yapılandırmalar virüs imzalarına göre olacaktır.

BitDefender' ı vekil sunucu üzerinden güncellemek için aşağıdaki adımları takip edin.

1. Masaüstüne sağ tıklayın. BitDefender Kurtarma CDsi bağlamsal menüsü görünecektir.
2. Kök menüde iken **Terminal**' i seçin.
3. **cd /ramdisk/BitDefender-scanner/etc** komutunu yazın.
4. **mcedit bdscan.conf** komutunu yazın, dosyayı düzenlemek için GNU Midnight Commander (mc) programı kullanılacak.
5. Aşağıdaki satır hakkında yorum yapmadan `#HttpProxy =` sadece `#` işaretini silin) ve etki alanını belirleyin, kullanıcı adı, şifre ve vekil sunucunun portu, takip eden satır buna benzemelidir:

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Değişiklikleri kaydetmek için **F2**' ye basıp kayıt işlemini onaylayın, kapatmak için **F10**' a basın.
7. **bdscan update** komutunu yazın.

12.5. Verilerimi nasıl kaydedebilirim?

Varsayalım ki Windows yüklü bilgisayarınız bilinmeyen bir sorun dolayısı ile açılmıyor. Aynı zamanda bilgisayarınızdaki çok önemli verilere umutsuzca ihtiyacınız var. Bu durumda BitDefender Kurtarma CD' si işinize yarayacak.

Bilgisayarınızdaki verileri çıkarılabilir bir cihaza, örneğin USB hafıza kartı gibi kaydetmek için, aşağıdaki adımları takip edin.

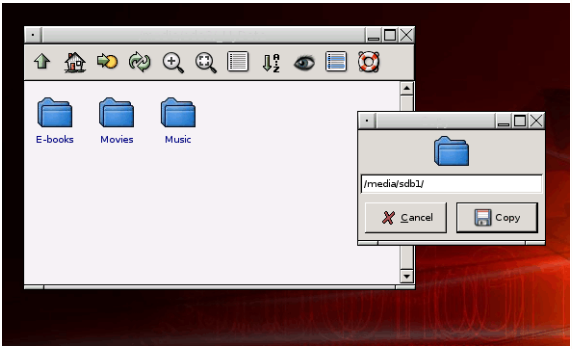
1. BitDefender Kurtarma CD' sini CD sürücüsüne koyun, hafıza kartını USB sürücüye takıp, bilgisayarı yeniden başlatın.
2. Aşağıdaki pencere açılacaktır.

Masaüstü Ekranı

3. Yedeklerini almak istediğiniz verilerin olduğu disk bölümüne çift tıklayın (örneğin `[sda3]` gibi).

> ***Not***
> BitDefender Kurtarma CD' si ile çalışırken, Linux tipindeki disk bölüm isimleri ile çalışacaksınız. Örneğin `[sda1]` Windowstaki `(C:)` yerine, `[sda3]` yine `(F:)` yerine ve `[sdb1]` memory kartı yerine kullanılacaktır.

4. Klasörlerinize göz atarak arzuladığınız dizini açın. Örnek olarak `Belgelerim` içindeki `Videolarım`, `Müziğim` gibi.
5. İstediğiniz dizini sağ tıklayarak **Kopyala** tuşuna basın. Aşağıdaki pencere açılacak.



Verileri Kaydetme

6. Text kutusunda uygun yere `/media/sdb1/` yazarak, **Kopyala** tuşuna basın.

Yardım Alma

13. Destek

Saygın bir tedarikçi olarak, BitDefender müşterilerine eşsiz derecede hızlı ve doğru destek verebilmek için elinden gelen tüm gayreti göstermektedir. Destek Merkezi (aşağıda belirtilen adresten temas kurabilirsiniz) en son tehditleri sürekli olarak takip etmektedir. Burası tüm sorularınızın zamanında cevaplandırıldığı bir yerdir.

İleri teknoloji ürünlerini en makul fiyatlarla sunarak müşterilerine zaman ve para tasarrufu sağlama, BitDefender için her zaman bir öncelik olmuştur. Ayrıca, başarılı bir iş yerinin, iyi iletişime ve müşteriye verilen desteğin mükemmelliğine olan bağlılığa dayalı olduğuna inanıyoruz.

Her zaman bddestek@kavi.com.tr'den destek talep edebilirsiniz. Derhal yanıt alabilmek için, lütfen e-postanızda BitDefender'ınız ve sisteminiz hakkında mümkün olduğu kadar fazla bilgi verin ve karşılaştığınız problemi mümkün olduğu kadar doğru tarif edin.

13.1. BitDefender Bilgi Üssü

BitDefender Bilgi Üssü, BitDefender ürünleri hakkında bilgi alınabilen çevrimiçi bir bilgi bankasıdır. Burada; kolaylıkla erişilebilen bir formatta, BitDefender destek ve geliştirme ekiplerinin süre gelen teknik destek ve arıza giderme faaliyetlerinin sonuçları hakkında raporların yanı sıra, detaylı açıklamalar içeren virüs önleme ve BitDefender çözümlerinin yönetimi hakkında genel makaleler ile çok sayıda diğer makaleler bulunmaktadır.

BitDefender Bilgi Üssü halka açık olup, serbestçe incelenebilmektedir. İçerdiği kapsamlı bilgiler, BitDefender müşterilerine ihtiyaç duydukları teknik bilgi ve anlayışı elde edebilecekleri diğer bir alternatifi oluşturmaktadır. BitDefender müşterilerinden gelen tüm geçerli bilgi talepleri veya arıza raporları, sonunda ürün yardım dosyalarını destekleyici arıza giderme raporları, yararlı broşür kopyaları veya bilgilendirici makaleler olarak BitDefender Bilgi üssünde toplanmaktadır.

BitDefender Bilgi Üssüne http://kb.bitdefender.com adresinden istenildiği zaman erişilebilir.

13.2. Yardım Almak

13.2.1. Web Selfservisine Gidin

Herhangi bir sorununuz olduğunda, destek uzmanlarımız 7/24 telefon, email, veya chat yolu ile hiç bir ek ücret ödemeden yardımcı olacaktır.

Lütfen aşağıdaki linki takip ediniz.

İngilizce

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/

Almanca

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/

Fransızca

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/

Romence

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/

İspanyolca

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2194/

13.2.2. Bir destek kaydı açın

Bir destek kaydı açıp email ile destek almak istiyorsanız, aşağıdaki linkleri takip edin:

İngilizce: http://www.bitdefender.com
Almanca: http://www.bitdefender.com
Fransızca: http://www.bitdefender.com
Romence: http://www.bitdefender.com
İspanyolca: http://www.bitdefender.com

13.3. İletişim Bilgileri

Verimli iletişim, başarılı bir işin anahtarıdır. Son 10 yıl içinde, BITDEFENDER, müşterilerimizin ve ortaklarımızın beklentilerini aşabilmek için sürekli daha iyi iletişim sağlama çabası göstererek tartışmasız saygın bir üne kavuşmuştur. Herhangi bir sorunuz olursa, lütfen bizimle irtibata geçmekten çekinmeyin.

13.3.1. Web Adresleri

Satış Bölümü: bdsatis@kavi.com.tr
Teknik Destek: bddestek@kavi.com.tr
Dokümantasyon: documentation@bitdefender. com
Ortaklık Programı: partners@bitdef ender.com
Pazarlama: marketing@bitdefender. com
Medya İlişkileri: pr@bitdefender.com
İş Olanakları: jobs@bitdefender.com
Virüs Bildirimleri: virus_submission@bitdefender.com
Spam Bildirimleri: spam_submission@bitdefender.com
Suistimal Bildirimleri: abuse@bitdef ender. com
Ürün web sitesi: http://www.kavi.com.tr http://www.bitdefender.com.tr
Ürün ftp arşivler: ftp://ftp.bitdefender.com/pub
Yerel distribütörler: http://www.bitdefender.com/partner_list
BitDefender Bilgi Üssü: http://kb.bitdefender.com

13.3.2. Şubeler

BitDefender şubeleri faaliyet bölgeleri ile ilgili olarak, gerek ticari gerekse genel konularda her türlü sorularınıza yanıt vermeye hazırdır. İlgili adresleri ve irtibat bilgileri aşağıda listelenmiştir.

A.B.D

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Web: http://www.bitdefender.com
Teknik Destek:

- E-mail: support@bitdefender.com
- Telefon:

- 1-888-868-1873 (Sadece kayıtlı kullanıcılar için A.B.D içi erişim numarası)
- 1-954-776-6262 (Sadece kayıtlı kullanıcılar için)

Müşteri Hizmetleri:

- E-mail: customerservice@bitdefender.com
- Telefon:
  - 1-888-868-1873 (Sadece kayıtlı kullanıcılar için A.B.D içi erişim numarası)
  - 1-954-776-6262 (Sadece kayıtlı kullanıcılar için)

Almanya

BitDefender GmbH
Batı Avrupa Merkezi
Karlsdorferstrasse 56
88069 Tettnang
Almanya
Tel: +49 7542 9444 60
Fax: +49 7542 9444 99
Email: info@bitdefender.com
Satış: bdsatis@kavi.com.tr
Web: http://www.bitdefender.com
Teknik Destek: support@bitdefender.com

İngiltere ve İrlanda

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959
Fax: +44 845 130 5069
Email: info@bitdefender.com
Satış: bdsatis@kavi.com.tr
Web: http://www.bitdefender.co.uk
Teknik Destek: bddestek@kavi.com.tr

İspanya

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona

Teknik Destek: soporte@bitdefender-es.com
Satış: comercial@bitdefender-es.com
Tel: +34 932189615
Fax: +34 932179128
Web: http://www.bitdefender-es.com

Romanya

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
Teknik Destek: bddestek@kavi.com.tr
Satış: bdsatis@kavi.com.tr
Tel: +40 21 4085600
Fax: +40 21 2330763
Ürün web sitesi: http://www.kavi.com.tr http://www.bitdefender.com.tr

Sözlük

ActiveX

ActiveX, diğer programların ve işletim sistemlerinin çağırabileceği şekilde bir program yazmak için kullanılan bir modeldir. ActiveX teknolojisi, statik sayfalar yerine bir bilgisayar programı gibi görünen ve davranan etkileşimli web sayfaları hazırlamak için Microsoft Internet Explorer ile birlikte kullanılmaktadır. ActiveX ile, kullanıcılar Web sayfasında sorular sorabilir veya cevap verebilir, basmalı butonları kullanabilir ve diğer şekillerde etkileşim sağlayabilir. ActiveX kontrolleri genelde Visual Basic kullanılarak yazılmıştır.

Active X, güvenlik kontrollerinin bulunmaması konusu dikkate alınmalıdır. Bilgisayar güvenlik uzmanları internet üzerinden kullanılmasını tavsiye etmemektedir.

Adware

Adware, genelde kullanıcının adware' i kabul ettiği taktirde ücretsiz olarak sağlanan bir ana bilgisayar programı ile birlikte gelmektedir. Adware uygulamaları, genelde kullanıcının uygulamanın amacını belirten bir lisans anlaşmasını kabul etmesinden sonra yüklenmesi nedeniyle, yasalara aykırı bir davranış teşkil etmemektedir.

Ancak, açılır pencere reklamları rahatsız edecek bir düzeye gelebilir ve bazen sistem performansını olumsuz yönde etkileyebilir. Ayrıca, bu uygulamalardan bazılarının topladığı bilgiler, lisans anlaşması içinde bulunan şartları tam olarak anlamayan kullanıcılar için gizlilik sorunu yaratabilir.

Arşiv

Yedeklenen dosyaları içeren bir disk, bant veya klasördür.

Şıkıştırılmış formatta bir veya birden fazla dosya içeren bir dosyadır.

Arka Kapı

Tasarımcılar veya bakımcılar tarafından bir sistemin güvenliğinde bilinerek bırakılan bir boşluktur. Bu tür boşlukların bırakılmasındaki neden her zaman kötü amaçlı değildir. Örneğin bazı işletim sistemlerinde, saha servis elemanlarının veya üreticinin bakım zamanlayıcılarının kullanması amacıyla öncelikli kullanıcı hesapları bulunmaktadır.

Ön yükleme sektörü

Her diskin başında bulunan ve diskin mimarisini (kesim boyutu, küme boyutu ve bunun gibi) tanımlayan sektördür. Başlangıç disklerinde, ön yükleme sektörü aynı zaman da işletim sistemini yükleyen bir program içermektedir.

Ön yükleme virüsü

Sabit disk veya disketin ön yükleme sektörüne bulaşan bir virüstür. Ön yükleme sektörü bulaşmış bir disketle sistemin başlatılmaya çalışılması, virüsün bellekte aktif hale gelmesine neden olacaktır. Bu noktadan sonra, sisteminizi her başlattığınızda virüs bellekte aktif halde bulunacaktır

Tarayıcı

Web tarayıcısı teriminin kısaltılmış halidir. Web sayfalarını bulmak ve görüntülemek için kullanılan bir uygulama yazılımıdır. En yaygın iki tarayıcı: Netscape Navigator ve Microsoft Internet Explorer'dır. Bunların her ikisi de grafiksel tarayıcıdır. Bir başka deyişle, her ikisi de, metnin yanı sıra grafikleri de görüntüleyebilmektedir. Ayrıca, en modern tarayıcılar, bazı formatlar için ara programlar gerektirmesine rağmen, ses ve video da dahil olmak üzere çoklu-ortam bilgilerini sunabilirler.

Komut Satırı

Bir komut satırı arayüzünde, kullanıcı ekranda sağlanan boşluğa komut dilini kullanarak komutu direkt olarak girer.

Cookie

Internet endüstrisinde, cookie'ler sizin çevrimiçi ilgi alanlarınızı ve zevklerinizi izlemek için reklamcılar tarafından analiz edilebilen ve kullanılabilen bireysel bilgisayar bilgilerini içeren küçük dosyalar olarak tanımlanmaktadır. Bu alanda, cookie teknolojisi hala geliştirilmekte olup, amaç, reklamları doğrudan söylemiş olduğunuz ilgi alanlarına hedeflemektir. Çoğu insan için, bu iki tarafı da keskin bir bıçaktır. Çünkü, bir taraftan sadece ilgilendiğiniz alanla ilgili reklamları gördüğünüz için verimli ve uygun olmakta, diğer taraftan nereye gittiğiniz ve neyi tıkladığınız gerçekten "izlenmekte" ve takip edilmektedir'. Anlaşılacağı üzere, gizlilik ile ilgili tartışmaların ortaya çıkmasına neden olmakta ve bir çok kişi "SKU numarası" gibi (paketlerin arkasında bulunan ve süpermarket kasalarında taranan bildiğimiz barkod'lar gibi) fark edilme fikrinden rahatsızlık duymaktadır. Bu bakış açısı, biraz abartılı olmasına rağmen, bazı konularda gerçeği yansıtmaktadır.

Disk sürücü

Bir diskten veri okuyan ve disket üzerine veri yazan bir cihazdır.

Bir sabit disk sürücü, sabit diskleri okur ve sabit disk üzerine yazar.

Bir disket sürücü, disket sürücülere erişir.

Disk sürücüler dahili (bilgisayar içinde yer alırlar) veya harici (bilgisayara bağlanan ayrı bir kutu içinde yer alırlar) olabilirler.

İndirme

Bir ana kaynaktan bir çevresel aygıta veri kopyalamadır (genel olarak, bir dosyanın tümü). Terim genelde bir dosyayı bir çevrimiçi servisten kişinin kendi bilgisayarına

kopyalama işlemini tanımlamak için kullanılır. İndirme, aynı zamanda bir dosyanın bir ağ dosya sunucusundan ağdaki bir bilgisayara kopyalanmasını da kapsamaktadır.

E-mail

Elektronik posta. Yerel veya global ağlar üzerinden bilgisayarlara mesajlar gönderilmesini sağlayan bir hizmettir.

Olaylar

Bir program tarafından algılanan bir işlem veya eylemdir. Olaylar, bir fare butonunun tıklanması veya bir tuşa basılması gibi kullanıcı eylemleri veya belleğin yetmemeye başlaması gibi sistem olayları olabilir.

Yanlış Olumlu

Bir tarayıcı, bir dosyayı gerçekten virüs bulaşmamışken, virüs bulaşmış olarak tanımlandığında meydana gelir.

Dosya adı uzantısı

Dosya adından sonraki noktayı takip eden kısmı olup, dosyaya kaydedilen veri türünü belirtir.

Çoğu işletim sistemi dosya adı uzantılarını kullanır. Örneğin, Unix, VMS ve MS-DOS. Genelde bir ile üç harften oluşur (bazı eski işletim sistemleri üçten fazla desteklememektedir). Örnekler arasında; C kaynak kodları için “c”, Dipnotlar için “ps”, gelişigüzel metin için “txt” verilebilir.

Sezgisel

Yeni virüsleri belirlemek için kullanılan kural-tabanlı bir yöntemdir. Bu tarama yöntemi, belirli virüs imzalarına dayanmamaktadır. Sezgisel taramanın avantajı varolan bir virüsün yeni bir versiyonu tarafından aldatılamamasıdır. Ancak, bazen normal programlarda şüpheli kod bildirerek “yanlış olumlu” üretebilir.

IP

Internet Protokolü – TCP/IP protokol takımı içindeki IP adreslemesinden, yönlendirme ve IP paketlerinin bölünmesinden ve yeniden birleştirilmesinden sorumlu olan gönderilebilir bir protokoldür.

Java applet

Sadece bir web sayfasında çalışacak şekilde tasarlanmış bir Java programıdır. Bir web sayfasında bir applet’i kullanmak için, applet’in kullanacağı applet ismini ve boyutunu (uzunluk ve genişlik piksel olarak) belirtmelisiniz. Web sayfasına erişildiğinde, tarayıcı applet’i bir sunucudan indirerek kullanıcının bilgisayarında (istemci) çalıştırır. Applet’ler çok sıkı bir güvenlik protokolü tarafından yönetildikleri için uygulamalardan farklıdır.

Örneğin, applet'ler istemci üzerinde çalışmasına rağmen, istemci makinenin üzerinde veri okuma veya yazma yapamazlar. Ayrıca, applet'ler daha da sınırlandırılmış olup, sunulmuş oldukları aynı alan içinde veri okuyabilir veya yazabilirler.

Makro virüs

Bir döküman içine bir makro olarak saklanmış olan bir bilgisayar virüs tipidir. Microsoft Word ve Excel gibi bir çok uygulama güçlü makro dillerini desteklemektedir.

Bu uygulamalar, bir döküman içine bir makro yerleştirmenize olanak sağlar ve döküman her açıldığında bu makroyu çalıştırır.

Posta İstemcisi

Bir e-posta istemcisi, e-posta almanızı ve göndermenizi sağlayan bir uygulamadır.

Bellek

Bilgisayar içindeki dahili depolama alanlarıdır. Bellek terimi, çip şeklinde gelen veri depolamayı tanımlar. Depolama kelimesi, teyp veya disklerdeki belleği tanımlamak için kullanılır. Tüm bilgisayarlar, genelde ana bellek veya RAM olarak bilinen belirli bir fiziksel belleğe sahiptir.

Sezgisel-olmayan

Bu tarama yöntemi belirli virüs imzalarını esas almaktadır. Sezgisel-olmayan bu taramanın avantajı, virüs gibi görünenler tarafından aldatılamaması ve böylece yanlış alarmlar vermemesidir.

Paket programlar

Sıkıştırılmış formatta olan bir dosyadır. Bir çok işletim sistemi ve uygulamalar bir dosyayı daha az bellek alacak şekilde sıkıştırmanızı sağlayacak komutlar içermektedir. Örneğin, içinde peş peşe on boşluk karakteri bulunan bir metin dosyanız olduğunu varsayın. Normal olarak, bu 10 bayt depolama yeri kullanacaktır.

Ancak, dosyaları sıkıştıran bir program, bu boşluk karakterlerini özel bir boşluk-serisi karakter ve sonuna boşluk adetini belirten bir rakam ekleyerek değiştirebilir. Bu durumda, 10 boşluk sadece iki bayt gerektirecektir. Bu sadece bir sıkıştırma tekniğidir. Çok sayıda başka tekniklerde vardır.

Yol

Bir bilgisayardaki bir dosyaya giden kesin yolu gösterir. Bu yollar, genelde üstten aşağıya doğru olan bir hiyerarşi dosyalama sistemi ile tanımlanırlar.

Herhangi iki nokta arasındaki yön, iki bilgisayar arasındaki iletişim kanalı gibidir.

Phishing

Kimlik hırsızlığında kullanmak üzere özel bilgilerini vermesi için, kullanıcıya, kurulu yasal bir kuruluş olduğunu iddia ederek bir e-posta mesajı gönderme eylemidir. E-posta, kullanıcıyı bir web sitesini ziyaret etmeye yönlendirerek, şifre ve kredi kartı, sosyal sigorta numarası ve banka hesap numarası gibi, yasal organizasyonun halihazırda elinde mevcut olan kişisel bilgileri güncellemesi ister. Web sitesi aslında sahte olup, sadece kullanıcının bilgilerini çalmak için kurulmuştur.

Polimorfik virüs

Bulaştığı her dosyayla şeklini değiştiren virüstür. Düzenli bir ikili formatı olmadığı için, bu tür virüsleri belirlemek oldukça zordur.

Port

Bir cihazı bilgisayara bağlayabileceğiniz bir arayüzdür. Kişisel bilgisayarların çeşitli tipte portları bulunmaktadır. Disk sürücülerini, görüntü ekranlarını ve klavyeyi bağlamak için dahili olarak bir çok port bulunmaktadır. Harici olarak, kişisel bilgisayarların modem, yazıcı, fare ve diğer çevre cihazlarını bağlamak için portları bulunmaktadır.

TCP/IP ve UDP ağlarında, mantıksal bağlantı için uç noktalar bulunmaktadır. Port numarası, ne tür bir port olduğunu tanımlar. Örneğin, port 80 HTTP trafiği için kullanılır.

Rapor Dosyası

Meydana gelen işlemlerin listelendiği bir dosyadır. BitDefender, taranan yolları, klasörleri, taranan arşiv ve dosya sayısını, kaç tanesine virüs bulaştığını ve kaç tane şüpheli dosya bulunduğunu listeleyen bir rapor dosyası tutar.

Rootkit

Bir rootkit, bir sisteme yönetici-seviyesinde erişim sağlayan bir dizi yazılım aracıdır. Terim ilk olarak UNIX işletim sistemi için kullanılmış olup, davetsiz misafirlere yönetimsel haklar sağlayan ve onların sistem yöneticileri tarafından görünmeyecek şekilde varlıklarını saklayan yeniden-derlenmiş araçlar olarak bilinmektedir.

Rootkit'lerin ana görevi işlemleri, dosyaları, girişleri ve kayıtları saklamaktır. Ayrıca, uygun yazılımları dahil ettiklerinde terminallerden, ağ bağlantılarından veya çevre birimlerinden gelen verileri de yakalayabilirler.

Rootkit' ler karakter olarak kötü amaçlı değildir. Örneğin, sistemler hatta bazı uygulamalar rootkit kullanarak kritik dosyaları saklar. Ancak, genelde kötü amaçlı yazılımları saklamak veya sisteme izinsiz olarak giren kişilerin varlığını saklamak için kullanılmaktadır. Kötü amaçlı yazılımlarla birleştirildiğinde, rootkit'ler sistemin bütünlüğü ve güvenliği için büyük tehlike oluştururlar. Trafiği denetleyebilir, sistem

içine arka kapılar yaratabilir, dosyaları ve kayıtları değiştirebilir ve tespit edilmekten kurtulabilirler.

Script

Makro veya toplu dosya için kullanılan diğer bir terimdir. Script, kullanıcı müdahalesi olmadan çalıştırılabilen bir komutlar listesidir.

Spam

Elektronik işe yaramaz posta veya lüzumsuz haber grubu postalarıdır. Yaygın olarak, talep edilmeyen herhangi bir e-posta olarak bilinmektedir.

Spyware

Kullanıcının internet bağlantısını haberi olmadan kullanarak, kullanıcı bilgilerini gizlice ve genelde reklam amaçlı olarak toplayan herhangi bir yazılımdır. Spyware uygulamaları, internetten indirilebilen ücretsiz veya shareware programlarına bunların gizlenmiş bir parçası olarak dahil edilirler. Ancak, shareware ve ücretsiz uygulama yazılımlarının çoğunun spyware ihtiva etmediği unutulmamalıdır. Bir kere yüklendikten sonra, spyware, kullanıcının internet üzerindeki etkinliklerini izler ve bu bilgileri arka planda bir başkasına gönderir.Spyware aynı zamanda e-posta adresleri ve hatta şifreler ve kredi kartı numaralarını da toplayabilir.

Spyware'in bir Truva atına olan benzerliği, kullanıcıların farkında olmadan başka bir şey yüklerken bu ürünleri de yüklemesi gerçeğinde yatmaktadır. Bir spyware kurbanı olmanın en yaygın yolllarından biri, bugün mevcut olan belirli eşler-arası (P2P) dosya alıp verme ürünlerinin internetten indirilmesidir.

Etik ve gizlilik konularını gündeme getirmesinin haricinde, spyware, bilgisayarın bellek kaynaklarını kullanarak ve aynı zamanda kullanıcının internet bağlantısı üzerinden spyware’in ana üssüne bilgi gönderirken bant genişliğini kullanarak kullanıcıdan çalmaktadır. Spyware bellek ve sistem kaynaklarını kullandığı için, arka planda çalışan uygulamalar sistemin çökmesine veya genel sistem dengesizliğine neden olabilirler.

Başlangıç öğeleri

Bu klasöre yerleştirilen herhangi bir dosya bilgisayar başlatıldığında açılacaktır. Örneğin, bir başlangıç ekranı, bilgisayar ilk açıldığında çalınacak olan bir ses dosyası, bir hatırlatma takvimi veya uygulama programları başlangıç öğeleri olabilir. Normal olarak, bu klasöre dosyanın kendisi yerine takma isimli başka bir dosya yerleştirilir.

Sistem Tepsisi

Windows 95 ile ilk kez ortaya çıkan sistem tepsisi, Windows görev çubuğunda (genelde altta, saatin yanında) yer almakta ve faks, modem, ses ayarı ve bir sürü

diğer olanaklar gibi sistem fonksiyonlarına kolay erişim sağlayan minyatür ikonlar içermektedir. Detayları ve kontrollerini görmek için ikonu çift veya sağ-tıklayın.

TCP/IP

Transmission Control Protocol/Internet Protocol (İletim Kontrol Protokolü/ Internet Protokolü) – Farklı donanım mimarileri ve çeşitli işletim sistemlerine sahip birbirine bağlı bilgisayarların oluşturduğu ağlar üzerinden iletişim sağlayan, internet üzerinde yaygın olarak kullanılan bir dizi ağ protokolleridir. TCP/IP, bilgisayarların nasıl iletişim kuracağı ile ilgili standartlar ve bağlantılı ağlar ve yönlendirilen trafik ile ilgili standartları içermektedir.

Trojan (Truva)

İyi huylu bir uygulama gibi rol yapan yıkıcı bir programdır. Virüslerden farklı olarak, Truva atları kendilerini kopyalamazlar, ancak onlar kadar yıkıcı olabilirler. Truva atlarının en sinsi tiplerinden biri, bilgisayarlarınızdan virüsü temizlediğini iddia eden, fakat aslında bilgisayarınıza virüs bulaştırandır.

Terim, Homeros' un İlyada' sındaki bir hikayeden gelmektedir. Bu hikayede, Yunanlılar düşmanlarına devasa bir tahta at hediye ederler. Truvalılar için bu görünüşte bir barış adağıdır. Fakat Truvalılar atı şehir duvarlarının içine çektiklerinde, atın boş karnından gizlice çıkan Yunanlılar şehir kapılarını açar ve diğer askerleri içeri sokarak Truva' nın ele geçirilmesini sağlarlar.

Güncelleme

Aynı ürünün daha eski versiyonunun yerini alması için tasarlanan bir yazılım veya donanım ürününün yeni versiyonudur. Ayrıca, Güncelleme için kurulum rutinleri genellikle daha eski bir versiyonun bilgisayarınızda olup olmadığını kontrol eder. Eğer yoksa, güncellemeyi yükleyemezsiniz.

BitDefender' ın, size güncellemeleri manuel olarak kontrol etmenizi sağlayan veya otomatik olarak ürünü güncelleyen, kendi güncelleme modülü bulunmaktadır.

Virüs

Bilginiz olmadan bilgisayarınıza yüklenen ve iradeniz dışında çalışan bir program veya kod parçasıdır. Virüslerin bir çoğu aynı zaman da kendilerini kopyalayabilirler. Tüm bilgisayar virüsleri insan yapımıdır. Kendini tekrar ve tekrar kopyalayan basit bir virüs yapmak oldukça basittir. Böyle basit bir virüs bile, mevcut tüm belleği kullanacağı ve sistemi kilitlenme noktasına getireceği için tehlikelidir. Daha tehlikeli bir virüs türü, kendini ağ üzerinden yayan ve güvenlik sistemlerini baypas eden virüstür.

Virus tanımı

Virüsü algılamak ve yok etmek için virüs koruma programı tarafından kullanılan, virüsün ikili şablonudur.

Worm

Kendini ağ üzerinden yayan ve yol aldıkça kendini yeniden üreten bir programdır. Kendini diğer programlarla birleştiremez.