Bilgisayar Virüsleri ve Antivirüs Yazılımları

Bilgisayar Virüsleri ve Antivirüs Yazılımları, bilgisayara zarar veren ve onları önleyen zararlı yazılımları ifade eder. Zararlı yazılımlar (malware), bilgisayar sistemlerinin işleyişini olumsuz etkileyen, kullanıcının izni veya bilgisi olmaksızın çeşitli zararlı eylemler gerçekleştiren kötü amaçlı programlardır. Bu tür yazılımların amacı, kullanıcı verilerini silmek, engellemek, kopyalamak, değiştirmek, çalmak veya bilgisayar ile ağ performansını düşürmek olabilir. Siber güvenlik açısından, bilgisayar virüsleri veri güvenliğinin bir numaralı düşmanı olarak kabul edilmektedir. Bilgisayar virüsleri nedeniyle iş dünyasında milyarlarca dolarlık zararlar yaşanmıştır.

Bu makaleyi Spotify'da sesli olarak dinlemek için podcast'ine bu linkten ulaşabilirsiniz.

1.1 Zararlı Yazılımların Bulaşma Yolları

Zararlı yazılımlar, sistemlere çeşitli yollarla bulaşabilir:

- **İnternet üzerinden** (güvenilir olmayan sitelere girme, zararlı bağlantılara tıklama, sahte antivirüs linkleri içeren e-postalar).
- **Harici medya** (harici diskler, USB'ler, CD'ler).
- **E-posta ekleri** ve şüpheli mesajlar.
- **Korsan yazılımlar** ve resmi olmayan kaynaklardan indirilen programlar.
- **Ağ bağlantıları** ve paylaşılan dosyalar.
- **Tarayıcı açıkları**.

1.2 Başlıca Zararlı Yazılım Türleri

Zararlı yazılımlar, işlevlerine ve yayılma biçimlerine göre çeşitli kategorilere ayrılır:

- **Bilgisayar Virüsleri (Computer Viruses):** Kullanıcının izni veya bilgisi olmadan bilgisayarın çalışma şekline müdahale eden, kendini diğer dosyaların içinde gizlemeye veya bir bilgisayardan diğerine yayılmaya çalışan programlardır.
    - **Özellikleri:** Biyolojik virüsler gibi bulaşıcı, gizli, bulaştırıcı, uyuyan, uyarılabilir, dışavurumcu ve yıkıcıdırlar. Hayatta kalmak için bir ana bilgisayara (bilgisayar) ihtiyaç duyarlar. Kendilerini kopyalama ve çoğaltma yetenekleri vardır; normal bir program çalışırken kendilerini de kopyalayabilirler. Virüsler, koşullar olgunlaşana kadar saldırmayarak gizli kalabilir ve bilgisayarı yavaşlatabilirler. Diğer yasal programlar gibi yürütülebilir programlardır, ancak genellikle başka yürütülebilir programlara parazit olarak bulaşırlar.
    - **Türleri:**
        - **Ağ Virüsleri (Network Virus):** Bilgisayar ağı üzerinden yürütülebilir dosyalara bulaşan virüslerdir. Hızlı yayılım gösterirler.
        - **Dosya Virüsleri (File Virus):** Bilgisayardaki dosyalara saldıran virüslerdir.

Genellikle ".exe" ve ".com" uzantılı dosyalara bulaşır ve bu dosyalar çalıştırıldığında aktif hale gelirler.

- **Önyükleme Virüsleri (Boot Virus / Boot Sector Virus):** Genellikle sabit diskin veya sürücünün önyükleme sektörüne bulaşan virüslerdir. Bilgisayar ilk açıldığında çalışmaya başlarlar. Polyboot.B ve AntiEXE bilinen örnekleridir.
- **Makro Virüsleri (Macro Virus):** Microsoft Office yazılımları (Word, Excel, PowerPoint) veya benzeri yazılımlar aracılığıyla bulaşan virüslerdir. Genellikle e-posta ekleriyle yayılırlar.
- **DOS Virüsleri:** DOS işletim sisteminden adını alır ve Windows'un batch özelliğini kullanarak donanımsal zarar verebilirler. Genellikle ".bat" uzantılı metin dosyaları olarak kodlanırlar.
- **Doğrudan Etkili Virüs (Direct Action Virus):** .exe veya .com dosyalarına eklenir ve çalıştırma anında etkinleşir, kalıcı olarak bellekte kalmaz.
- **Yerleşik Virüs (Resident Virus):** Bilgisayarın belleğine yerleşir ve ana program çalışmadığında bile diğer dosya ve programları enfekte edebilir. Tespit edilmesi ve kaldırılması zordur.
- **Çok Parçalı Virüs (Multipartite Virus):** Hem önyükleme sektörünü hem de yürütülebilir dosyaları enfekte edebilir.
- **Üzerine Yazma Virüsü (Overwrite Virus):** Mevcut programları kötü amaçlı kodla değiştirir ve orijinal program kodunu tamamen siler, bu da oldukça yıkıcıdır.
- **Polimorfik Virüs (Polymorphic Virus):** Tespit edilmekten kaçınmak için kendini değiştiren dosya enfektörleridir, ancak orijinal kodunu korur. Spam ve enfekte web siteleri aracılığıyla yayılırlar.
- **Boşluk Doldurucu Virüs (Spacefiller Virus / Cavity Virus):** Dosya boyutunu artırmadan dosyalar içindeki boşlukları doldurur, bu da tespiti zorlaştırır.

◦ **Tehlikeli Virüs Versiyonları ve Tarihsel Örnekler:**

- **Creeper Virüsü (1971):** İlk bilgisayar virüsü olarak kayıtlara geçmiştir. ARPANET'teki bilgisayarlara bulaşmış, ancak doğrudan bir zarar vermemiş, daha çok virüs mantığıyla tanıştırmıştır.
- **Çernobil Virüsü (1998):** Kısa sürede tüm dünyaya yayılmış, dünya genelinde 20 ila 80 milyon dolar zarara yol açmış, Windows işletim sistemindeki hayati dosyalara zarar vermiştir.
- **Melissa Virüsü (1999):** E-posta yoluyla bulaşan bir makro virüsüdür. Ekli .DOC uzantılı bir kelime işlemci dosyasının açılmasıyla yayılmış ve kullanıcıların adres defterindeki kişilere kendini göndermiştir.
- **I Love You (2000):** "Loveletter" olarak da bilinen bu virüs, e-postalara eklenen bir programın çalıştırılmasıyla yayılmış ve e-posta adres defterindeki kişilere kendini göndermiştir. Yaklaşık 10 ila 15 milyar dolar zarara neden olduğu tahmin edilmektedir.
- **Code Red Solucanı (2001):** Ağ sunucuları üzerinde yayılan bir bilgisayar solucanıdır. Web sunucusunun zayıf noktalarını tespit edip zarar verme

amacı taşımıştır. Yaklaşık 400.000 sunucuyu etkilediği ve bir milyondan fazla bilgisayara sızdığı düşünülmektedir.
    - **Bagle Virüsü (2004):** On milyonlarca dolar zarara neden olmuş ve sayısız PC'ye sızmıştır. E-postalardaki dosyaları kullanarak yayılmış ve 60 ila 100 kadar türevi bulunması nedeniyle virüs tarayıcılar tarafından yakalanması zor olmuştur.
    - **Sasser (2004):** E-posta kullanmadan, güncel olmayan işletim sistemlerinin güvenlik açıklarını kullanarak yayılmış ve uçuşların ertelenmesi gibi büyük zararlara neden olmuştur.
    - **MyDoom (2004):** Kimin yazdığı belirlenemeyen bu virüs, çıktığı dönemdeki dünya e-posta trafiğini felç etmiş ve 38 milyar dolarlık zarara yol açmıştır.
    - **Musallat (.exe) Virüsü:** Windows işletim sistemlerinde görev yöneticisine erişimi engelleyen, özellikle USB bellekler üzerinden bulaşan bir Truva atı türüdür (Trojan.Agent/Gen-Malagent).
    - **CryptoLocker (2013):** Fidye yazılımı (ransomware) kategorisinde bir zararlı yazılımdır. Kullanıcıların kişisel dosyalarını şifreleyerek kilitler ve açılması karşılığında fidye ister.
- **Solucan (Worm):** Virüs gibi kendini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır, ancak bunu otomatik olarak yapar. Bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir ve sisteme girdikten sonra kendi başına ilerleyebilir. En büyük tehlikeleri, kendilerini büyük sayılarda çoğaltma becerileridir; bu, yoğun ağ trafiği ve sistem yavaşlamasına neden olabilir. Virüslerden farklı olarak, bir dosyaya bulaşmaya veya insan müdahalesine ihtiyaç duymazlar.
- **Truva Atı (Trojan):** Kendisini zararsız olarak gösteren kötü amaçlı bir yazılımdır. Kullanıcının bilgisi olmadan bilgisayara yerleşir, sistemi diğer bilgisayarlarca internet veya ağ üzerinden kontrol edilebilir hale getirir ve güvenlik açığı oluşturur. Dosyaları görme, değiştirme, etkinlikleri izleme ve kaydetme, başka bilgisayarlara saldırmak için bilgisayarı kullanma gibi eylemlere olanak tanır. Virüslerden farklı olarak kendini çoğaltmaz veya kendi kendine çalışamaz, kullanıcının belirli bir eylemde bulunması gerekir.
- **Casus Yazılım (Spyware):** Kullanıcılara ait önemli ve özel bilgilerin, kullanıcının yaptığı işlemlerin, kullanıcının bilgisi olmadan toplanmasını ve bu bilgilerin kötü niyetli kişilere gönderilmesini sağlayan zararlı yazılımdır. Virüs ve solucanlardan farklı olarak kendi kopyalarını oluşturarak daha fazla yayılmaya ihtiyaç duymazlar; amaçları gizli kalarak bilgi toplamaktır. Şifreler, tarayıcı geçmişi, banka bilgileri gibi birçok bilginin çalınmasına neden olabilir.
- **Reklam Yazılımı (Adware):** Bilgisayarda reklamlar görüntülemek, arama isteklerini reklam web sitelerine yeniden yönlendirmek ve internet kullanıcılarına özel reklamların gösterilmesi için ziyaret edilen web sitelerinin türleri gibi pazarlama verilerini toplamak amacıyla tasarlanmış programlardır. Kullanıcıdan habersiz bilgi topladığında kötü amaçlı yazılım olarak kabul edilir.
- **Botnetler:** "Bot" terimi robotun kısaltmasıdır. Suçlular, bilgisayarınızı bir "bot"a (zombi olarak da bilinir) dönüştürebilen kötü amaçlı yazılımları dağıtırlar. Bu durumda bilgisayarınız, sizin haberiniz olmadan internet üzerinden otomatik görevleri

gerçekleştirebilir.
- **Fidye Yazılımı (Ransomware):** Kötü amaçlı yazılım indirilmesiyle çalışır, dosyaları şifreler ve genellikle kurbanın verilerine erişimini engellemek karşılığında fidye talep eder.
- **Rootkit:** Bir bilgisayar sistemi üzerinde idari düzeyde kontrol elde etmek için kullanılır. Yedek kapıları ve belirli virüs enfeksiyonlarını tespit etmekten kaçınmak için sıklıkla kullanılır.
- **Spam E-postalar:** Kullanıcılara izinleri dışında gönderilen, genellikle reklam, ticari amaçlı bilgilendirme ve bilgi çalma gibi kötü amaçlı iletilerdir.

1.3 Virüs Bulaşma Belirtileri

Bilgisayarınıza zararlı yazılım bulaştığını gösteren çeşitli belirtiler vardır:

- **Sistemin yavaşlaması:** Uygulamaların daha uzun sürede açılması ve genel sistem performansının düşmesi.
- **Veri kaybı veya değişimi:** Bilgilerin kaybolması, dosyaların açılmaması, dosya adlarının, uzantılarının veya tarihlerinin değişmesi.
- **İstenmeyen programlar/web sayfaları:** Bilgisayarın istenmeyen programlar veya internet sayfaları açması, tarayıcı ana sayfasının değişmesi, pop-up reklamların sıkça görünmesi.
- **Kontrol dışı işlemler:** Bilgisayarın verilen komutları yerine getirmemesi veya isteğiniz dışında işlemler yapması, bilgisayarın aniden kapanması.
- **Disk alanının azalması** veya bozuk sektörlerin artması.
- **RAM kullanımının sürekli azalması/artması**.
- **Antivirüs programının çökmesi** veya başlatılamaması.
- **Antivirüs sitelerine erişimin engellenmesi**.

1.4 Korunma Yöntemleri

Zararlı yazılımlardan korunmak için kapsamlı bir güvenlik yaklaşımı benimsemek önemlidir:

- **Güvenlik Duvarı (Firewall) Kullanımı:** Bilgisayarınız ile internet arasına koruyucu bir engel koyan, gelen ve giden ağ trafiğini izleyen ve filtreleyen yazılım veya donanımdır. Çoğu işletim sistemi ve güvenlik yazılımı dahili güvenlik duvarı ile gelir, bunların açık olduğundan emin olunmalıdır.
- **Antivirüs Yazılımı Kullanımı ve Güncel Tutma:** Cihazlarınızı kötü amaçlı yazılımlardan korumak için tasarlanmış yazılımlar yüklenmeli ve düzenli olarak güncellenmelidir.
- **Yazılımları ve İşletim Sistemlerini Güncel Tutma:** Eskimiş yazılımlar güvenlik açıkları yaratır; bu açıklar yazılım güncellemeleriyle kapatılır.
- **Verileri Düzenli Yedekleme:** Dosyaları harici diske veya buluta yedeklemek, fidye yazılımı gibi saldırılara karşı en iyi savunmadır.
- **Şüpheli Bağlantı ve Ekleri Açmaktan Kaçınma:** Bilinmeyen kişilerden gelen e-

postalar açılmamalı, e-posta, metin veya sosyal medya mesajlarındaki bilinmeyen bağlantılara tıklanmamalıdır.
- **Güvenilir Kaynaklardan İndirme:** Yazılımlar sadece resmi web sitelerinden veya doğrulanmış uygulama mağazalarından indirilmelidir.
- **Güçlü Parolalar ve Çok Faktörlü Kimlik Doğrulama:** Sistemlerinizi saldırganlardan daha iyi korumak için güçlü, benzersiz parolalar kullanılmalı ve mümkünse çok faktörlü kimlik doğrulama etkinleştirilmelidir.
- **Bilinmeyen Web Sitelerine Girmeme:** Güvenilir sitelere bağlı kalınmalı ve alan adlarına dikkat edilmelidir.
- **Kablosuz Yönlendirici Güvenliğini Sağlama:** Yönlendiricinin varsayılan şifresi değiştirilmeli, güvenlik ayarları gözden geçirilmeli ve mümkünse misafir ağı kurulmalıdır.
- **Halka açık bilgisayarlarda kişisel parola girmeme**.
- **İnternet tarayıcısının güvenlik ayarlarını üst düzeyde tutma**.
- **Aynı anda birden fazla antivirüs programı kurmaktan kaçınma:** Bu, programların birbiriyle çakışmasına ve bilgisayarın güvenliğini azaltmasına neden olabilir.

1.5 Antivirüs Yazılımları

Tanım ve Amaç: Antivirüs yazılımı, bilgisayar veya mobil cihazları virüsler, solucanlar, Truva atları ve casus yazılımlar gibi kötü amaçlı yazılımlardan korumak için tasarlanmış bir program veya programlar setidir. Temel amacı, tehditlerin bilgisayar sistemine girmesini ve sorunlara yol açmasını önlemek için proaktif bir yaklaşım sağlamaktır. Antivirüs yazılımları, zararlı programları bulup yok etmekle görevlidir, ancak bilgisayar kullanıcılarının tercihlerine göre görevleri de vardır. **Çalışma Prensipleri ve Tespit Teknolojileri:** Antivirüs yazılımları, kötü amaçlı yazılımları tespit etmek için çeşitli yöntemler kullanır:

- **İmza Tabanlı Tarama (Signature/Feature Code Killing Technology):** Bilgisayardaki dosyalarda veya bellek bölgelerinde bilinen kötü amaçlı kodlara ait hash değerleri veya bayt dizileri gibi benzersiz özellik kalıplarını (imzalarını) arar. Bu teknoloji, bilinen virüsleri tespit etmede etkilidir. Virüs veritabanının düzenli olarak güncellenmesi, yeni virüsleri tespit etmek için kritiktir. Ancak, virüslerin sürekli değişen yapıları nedeniyle geleneksel imza tabanlı yöntemler yetersiz kalabilir.
- **Sezgisel Tarama Teknolojisi (Heuristic Scanning Technology):** Bilinmeyen veya değiştirilmiş virüsleri tespit etmek için virüs benzeri davranışları veya kod özelliklerini analiz eder. Bu yöntem, virüs veritabanında henüz bulunmayan yeni virüs varyantlarını yakalamada etkilidir, ancak bazen “yanlış pozitif” (temiz bir dosyayı virüs olarak işaretleme) sonuçlar üretebilir.
- **Davranış Tabanlı Tespit (Behavior-Based Detection):** Bir programın şüpheli davranışlarını (örneğin, korumalı bir dosyaya erişmeye çalışma veya başka bir programı değiştirmeye çalışma) izler. Bu yaklaşım, yeni kötü amaçlı yazılım türlerine karşı koruma sağlar, ancak yine yanlış uyarılar verebilir.
- **Sanal Makine Teknolojisi (Virtual Machine Technology / Sandbox Virtual**

Technology): Virüsü sanal bir ortamda çalıştırarak davranışlarını analiz eder. Bu, şifrelenmiş virüslerin bile imzaları aracılığıyla tespit edilmesine olanak tanır ve hızlı inceleme avantajı sunar.

- **Bütünlük Tespit Teknolojisi (Integrity Detection Technology):** Bilgisayarın içeriğini anlar ve bilgilerde bir değişiklik tespit edildiğinde orijinal bilgilerle karşılaştırır. Bu teknoloji, virüsün türüne, miktarına veya koduna bakılmaksızın tüm virüsleri tespit edebilir.
- **Aktif Savunma Teknolojisi (Active Defense Technology):** İmza teknolojisinin virüsü tanımlayamadığı durumlarda, yani virüs veritabanı eski olduğunda kullanılır. Virüs davranışlarının ortak özelliklerini (örn. kendini çalıştırma, başlangıç öğeleri oluşturma, kayıt defteri değiştirme, kendini kopyalama, sürekli ağ bağlantısı) belirlemek için kullanılır.
- **Gerçek Zamanlı Virüs İzleme Teknolojisi (Real-time Virus Monitoring Technology):** Virüs gerçek zamanlı ve dinamik olduğundan, antivirüs yazılımı gerçek zamanlı izleme işlevlerine sahip olmalıdır. Herhangi bir program çağrıldığında filtrelenmeli ve bir virüs bulunduğunda hemen dezenfekte edilmeli veya sonlandırılmalıdır.
- **“Bulut Güvenliği” Teknolojisi (“Cloud Security” Technology):** Dağıtılmış bilgi işlem, paralel işleme ve bilinmeyen virüs davranış tespiti gibi yeni teknolojileri birleştirir. Truva atları ve kötü amaçlı programlarla ilgili en son bilgiler sunucu tarafına otomatik analiz ve işleme için gönderilir, ardından virüs ve Truva atları için çözümler her istemciye dağıtılır. Bu, antivirüs yazılımının virüsleri daha hızlı ayıklamasını sağlar ve antivirüs verimliliğini büyük ölçüde artırır. Ancak bu teknoloji hala geliştirme aşamasındadır ve bazen yanlış değerlendirmeler yapabilir.

Antivirüs Yazılımlarının Riskleri/Zayıflıkları: Antivirüs programları, bilgisayarınızı korumak için tasarlanmış olsa da, kendileri de saldırılara hedef olabilir ve bazı zayıflıkları bulunur:

- **Karmaşıklık ve Test Süresinin Yetersizliği:** Antivirüs ürünleri çok sayıda tarama ve tespit tekniği içerir, bu da motorlarını son derece karmaşık hale getirir ve kalite kontrolünü zorlaştırır. Sık güncellemeler, geliştiricilerin yeni bileşenleri yeterince test etmesine izin vermez, bu da hatalara yol açar.
- **Kullanıcı Güveni ve Dikkatsizlik:** Kullanıcıların antivirüs programlarına duyduğu aşırı güven, onları daha dikkatsiz hale getirebilir ve enfeksiyon olasılığını artırabilir.
- **Saldırı Yöntemleri:**
  - **Bellekte Kalan Virüsler:** Bellekte kalır ve antivirüs programının önemli işlevlerini felç ederek onu aldatmaya çalışır.
  - **Önyükleme Sektörü Değişimi:** Önyükleme sektörünü değiştirerek veya taklit ederek bütünlük denetleyicilerini yanıltabilirler.
  - **Sıkıştırılmış Dosyalar:** Antivirüsler sıkıştırılmış dosyaları tarayamaz ve açmaları gerekir. Saldırganlar, antivirüsleri sonsuz döngülere sokarak veya disk alanını doldurarak hizmet reddi (DoS) saldırılarına neden olabilecek özel olarak sıkıştırılmış dosyalar oluşturabilirler.
  - **Şifreli ve Parola Korumalı Dosyalar:** Antivirüsler şifreli veya parola korumalı

dosyaların içeriğini tarayamaz. Kötü amaçlı yazılımlar bu tür dosyalara gizlenebilir.
- **Rootkitler:** Sistemin üzerinde yönetici düzeyinde kontrol sağlayan ve arka kapıların veya belirli virüs enfeksiyonlarının tespitini engellemek için kullanılan yazılımlardır.
- **Yerel Ayrıcalık Yükseltme Sorunları:** Antivirüs yazılımı "herkes" grubuna "Tam kontrol" izni verirse, saldırganlar yüklenmiş bir hizmet dosyasını kötü amaçlı bir Truva atı veya rootkit ile değiştirebilir.
- **AV Durum Veritabanı Saldırıları:** Kötü amaçlı yazılımlar, daha önceki tarama verilerini saklayan antivirüs durum veritabanlarına saldırarak dosyaların durumunu "virüssüz" olarak değiştirebilir.
- **Anti-emülasyon ve Anti-sezgisel Teknikler:** Modern virüsler, tespit edilmekten kaçınmak için CPU emülasyonunu ve sezgisel taramayı atlatmak için teknikler kullanır.
- **İmza Taramasına Saldırılar:** Virüsler, virüs tarama yürütülebilir dosyalarını ve virüs imza veritabanlarını değiştirmeye çalışabilir.
- **Bellek Taramasına Saldırılar:** Bazı virüsler birden çok süreçte eşzamanlı olarak çalışabilir veya birden çok solucan kopyası birbirini izleyerek antivirüsün mücadelesini zorlaştırır.
- **Yüksek Ayrıcalıklı Erişim:** Antivirüs yazılımı genellikle işletim sisteminin yüksek güvenilirliğe sahip çekirdek düzeyinde çalıştığı için, herhangi bir güvenlik açığı saldırganlara sistem üzerinde tam kontrol sağlayabilir.

Popüler Antivirüs Programları: Kaynaklarda belirtilen popüler antivirüs programları şunlardır:

- McAfee.
- Norton.
- AVG.
- Avast!.
- Kaspersky.
- Panda.
- BitDefender.
- Trend Micro.
- Avira.
- F-Secure.
- NOD32/ESET End Point Security.
- Sophos.
- Windows Defender (Win10 ile birlikte gelir).

Bir çalışmaya göre Kaspersky, genel performans, özellikler, yardım ve destek açısından en iyi antivirüs yazılımı olarak değerlendirilmiştir. Norton ise özellikleri açısından en iyi olarak belirtilmiştir.

Ücretsiz ve Ücretli Antivirüsler: Antivirüs yazılımları hem ücretsiz hem de ücretli

versiyonlarda mevcuttur. Ücretsiz yazılımlar genellikle temel koruma sağlarken, ticari (ücretli) yazılımlar daha kapsamlı koruma sunar.

Antivirüs Yazılımı Kurulumu: Antivirüs yazılımlarının kurulumu, diğer yazılımların kurulumlarına benzerdir. Kurulum dosyası (setup) temin edildikten sonra başlatılır, bileşenler kurulur ve sonrasında güvenlik ayarları yapılabilir. Genellikle kurulumun tamamlanması için bilgisayarın yeniden başlatılması istenir.

1.6 Virüs Temizleme

Bir bilgisayara virüs bulaştığında, mümkün olan en kısa sürede harekete geçmek daha fazla hasarı veya yayılmayı önlemek için önemlidir. Virüsleri temizlemek için iki ana yöntemden bahsedilmiştir:

1. **Sistem Geri Yükleme:** İşletim sisteminin “sistem geri yükleme” aracını kullanarak, önemli kayıt ve sistem dosyalarını virüsün bulaşmadığı zamandaki bir denetim noktasına geri dönerek virüsten kurtulabilirsiniz.
2. **Antivirüs Programı Kullanımı:** Bilgisayarınıza güncellemelere açık, güvenilir ve lisanslı bir antivirüs programı kurarak veya internet üzerinden tanınmış antivirüs programlarının web sitelerinden çevrimiçi tarama yaparak virüsleri temizleyebilirsiniz.

Bazı durumlarda, bir PC Teknisyeni veya Sistem Yöneticisi, sistemin virüssüz olduğunu onaylayana kadar enfekte olmuş bilgisayar sistemleri ağdan engellenebilir, karantinaya alınabilir veya kaldırılabilir. Okul veya iş ortamlarında ise IT Güvenlik Ekibi veya yardım masası ile iletişime geçilmelidir.

Online Virüs Temizleme Siteleri: Yeterli kapasiteye sahip olmayan veya kurulu antivirüs programı olmayan kullanıcılar için çevrimiçi virüs temizleme siteleri bir çözüm yolu olabilir. Güvenilir birkaç çevrimiçi antivirüs temizleme sitesi örneği verilmiştir:

- Kaspersky: http://www.kaspersky.com/virusscanner
- Trend Micro: http://housecall.trendmicro.com/
- Symantec: http://security.symantec.com
- Panda-Software: http://www.pandasoftware.com/products/ActiveScan.htm ve http://www.pandasecurity.com/activescan/index
- Bitdefender: http://www.bitdefender.com/scan8/ie.html

1.7 Siber Güvenlik Aktörleri

Siber güvenlik dünyasında hem zararlı yazılımları oluşturan hem de bunlara karşı mücadele eden çeşitli aktörler bulunmaktadır:

- **Hacker:** Bilgisayar ve haberleşme teknolojileri konusunda bilgi sahibi olan, bilgisayar programlama alanında standartların üzerinde beceriye sahip bulunan ve ileri düzeyde yazılımlar geliştiren kişilerdir. Sahte antivirüslerin tasarımında ve zararlı amaçlar için

kullanılmasında önemli rol oynarlar. Hackerlar kendi içlerinde Haktivistler, Siyah Şapkalılar (kötü niyetli), Beyaz Şapkalılar (iyi niyetli), Gri Şapkalılar, Yazılım Korsanları, Phreakerlar, Script Kiddieler ve Lamerlar gibi gruplara ayrılır.
- **Cracker:** Ücretli programları kırarak (crack) ücretsiz kullanılmasını sağlayan kişilerdir. Hackerlardan farklı olarak programları kırmaz, sadece program üzerinde ayarlamalar yaparak ücretsiz kullanım, tema veya dil gibi değişiklikler yaparlar. "Yama" sözcüğü de Türkçe'de cracker yerine kullanılabilir. Güvenilir olmayan sitelerden indirilen crackli (yamalı, şifresi kırılmış) yazılımlar, kullanıcıları kandırmak amacıyla tasarlanmış sahte antivirüsler içerebilir.
- **Virüs Yazarları:** Bilgisayar virüslerinin programcılarıdır. Bazıları virüs yazmayı bir meydan okuma olarak görürken, diğerleri yıkıma neden olmak amacıyla yazarlar. Virüs programı yazmak genellikle önemli programlama becerileri gerektirir.
- **Antivirüs Geliştiricileri:** Yeni virüs türleri ortaya çıktığında antivirüs veritabanlarını güncelleyerek antivirüs yazılımlarını güncel tutan uzmanlardır.

Siber güvenliği bir kale savunması gibi düşünebilirsiniz: Zararlı yazılımlar, kaleyi ele geçirmeye çalışan düşman ordusudur. **Antivirüs yazılımları** kalenin kapısındaki bekçiler ve iç duvarlardaki muhafızlar gibidir; gelen tehditleri tanır ve durdurur. **Güvenlik duvarı** ise kalenin dış duvarlarıdır, istenmeyen trafiği baştan engeller. **Düzenli güncellemeler** ise bu bekçilerin ve duvarların en son savunma taktiklerini ve malzemelerini öğrenmeleri demektir, böylece yeni ve daha sinsi düşmanlara karşı hazırlıklı olurlar. Ancak en önemli savunma yine de **kalede yaşayan sizsiniz**, çünkü kötü niyetli bir linke tıklamak ya da şüpheli bir dosyayı indirmek, düşmana kalenin gizli bir kapısını açmak gibidir, en sağlam savunmayı bile etkisiz kılabilir.

1.8 Anahtar Terimler Sözlüğü

- **Adware (Reklam Yazılımı):** Bilgisayarda reklam görüntülemek, arama isteklerini reklam sitelerine yönlendirmek ve pazarlama verileri toplamak amacıyla tasarlanmış programlardır. Kullanıcıdan habersiz bilgi topladığında kötü amaçlı yazılım olarak kabul edilir.
- **Aktif Savunma Teknolojisi:** Antivirüs yazılımlarında, virüs veritabanı eski olduğunda veya virüs imzası tanınmadığında virüs davranışlarının ortak özelliklerini kullanarak kötü amaçlı yazılımları tespit eden tekniktir.
- **Antivirüs (Güvenlik Yazılımı):** Bilgisayarları virüsler, solucanlar, Truva atları, casus yazılımlar ve diğer kötü amaçlı yazılımlardan korumak için tasarlanmış yazılımlardır. Tespit, engelleme, silme veya karantinaya alma işlevlerini yerine getirir.
- **Ağ Virüsü:** Bir ağ üzerinden ağa bağlı tüm cihazlara bulaşabilen virüs türüdür; hızlı yayılım özelliği gösterir.
- **Bilgisayar Virüsü:** Kullanıcının izni veya bilgisi olmadan bilgisayarın çalışma şekline müdahale eden, kendini kopyalayabilen ve diğer dosyalara yayılabilen kötü amaçlı programdır.
- **Botnet:** Bilgisayarı bir "bot" veya "zombi"ye dönüştüren kötü amaçlı yazılım türüdür;

kullanıcının haberi olmadan otomatik görevler gerçekleştirebilir.

- **Bütünlük Algılama Teknolojisi:** Virüs tespitinde, bilgisayar bilgilerinin içeriğini anlayan ve bir değişiklik tespit edildiğinde orijinal bilgilerle karşılaştıran bir teknolojidir.
- **Casus Yazılım (Spyware):** Kullanıcıya ait önemli ve özel bilgilerin, kullanıcının bilgisi olmadan toplanmasını ve kötü niyetli kişilere gönderilmesini sağlayan zararlı yazılımdır.
- **Crack:** Ücretli programları ücretsiz kullanılabilir hale getirme eylemi veya tersine mühendisliğe verilen isimdir.
- **Cracker:** Ücretli programları kırarak ücretsiz kullanılmasını sağlayan kişilerdir.
- **CryptoLocker:** Kullanıcıların kişisel dosyalarını şifreleyerek kilitleyen ve fidye talep eden bir fidye yazılımı (ransomware) türü.
- **Bulut Güvenliği Teknolojisi:** Bilgi güvenliğinde, dağıtılmış hesaplama ve paralel işleme gibi teknolojileri kullanarak virüs ve kötü amaçlı programları otomatik analiz edip çözümlerini istemcilere dağıtan yaklaşımdır.
- **DAT Dosyaları (Virus Definition Files):** Antivirüs yazılımlarına yeni virüsleri nasıl tanıyacaklarını öğreten, bilinen virüslerin imza kalıplarını içeren dosyalardır.
- **DoS Virüsleri:** DOS işletim sisteminden adını alan ve genellikle .bat uzantılı metin dosyaları olarak kodlanıp donanımsal zararlar verebilen virüs türüdür.
- **Dosya Virüsü:** Bilgisayarlardaki dosyalara bulaşan ve bu dosyalar çalıştırıldığında aktif hale gelen virüs türüdür; genellikle .exe ve .com uzantılıdır.
- **Fidye Yazılımı (Ransomware):** Kullanıcının dosyalarını şifreleyerek erişimi engelleyen ve şifreyi çözmek için para (fidye) talep eden kötü amaçlı yazılım.
- **Firewall (Güvenlik Duvarı):** Kullanıcının belirlediği güvenlik ilkelerine göre gelen ve giden ağ trafiğini izleyen ve filtreleyen bir ağ güvenlik cihazı veya yazılımıdır.
- **Hacker:** Bilgisayar ve haberleşme teknolojileri konusunda ileri düzeyde bilgi sahibi olan, bilgisayar programlama alanında becerikli ve gelişmiş yazılımlar geliştiren kişidir.
- **Heuristic Tarama Teknolojisi (Sezgisel Tarama):** Antivirüs yazılımlarında, virüslerin bilinen davranış kalıplarını ve ilgili kodlarını analiz ederek bilinmeyen veya değiştirilmiş virüsleri tespit etmeye çalışan algılama yöntemidir.
- **İmza Tabanlı Algılama (Feature Code Killing Technology):** Bilinen virüslerin benzersiz kod kalıplarını (imzalarını) içeren bir veritabanını kullanarak kötü amaçlı yazılımları tespit eden geleneksel antivirüs yöntemidir.
- **Kumlu Kutu Sanallaştırma Teknolojisi (Sandbox Virtualization):** Bir programı izole edilmiş, sanal bir ortamda çalıştırarak davranışını analiz eden ve virüs olup olmadığını belirleyen bir antivirüs teknolojisidir.
- **Kötü Amaçlı Yazılım (Malware):** Virüsler, solucanlar, Truva atları, casus yazılımlar gibi bilgisayar sistemlerine zarar vermek veya istenmeyen eylemler gerçekleştirmek için tasarlanmış tüm yazılımları kapsayan genel bir terimdir.
- **Makro Virüsü:** Microsoft Office (Word, Excel, PowerPoint) veya benzeri yazılımların makro dilleri aracılığıyla bulaşan ve belgeler açıldığında etkinleşen virüs türüdür.
- **Önyükleme Virüsü (Boot Sector Virus):** Bilgisayar ilk açıldığında çalışan ve sabit diskin önyükleme sektörünü veya sürücü sektörünü enfekte eden virüs türüdür.

- **Pop-up:** İnternet sitelerinde aniden açılan, genellikle reklam veya yanıltıcı bağlantı içeren pencerelerdir.
- **Solucan (Worm):** Kendini otomatik olarak kopyalayabilen ve ağ üzerinden hızla yayılabilen, genellikle ağ trafiğini yavaşlatma gibi zararlar veren zararlı yazılım türüdür.
- **Sanal Makine Teknolojisi:** Virüsü sanal bir ortamda çalıştırarak yürütme davranışını analiz eden ve imza kodu aracılığıyla virüsleri tespit edip imha eden antivirüs algılama tekniğidir.
- **Spam E-postalar:** Kullanıcılara internet ortamında izinleri dışında gönderilen, genellikle reklam, ticari amaçlı veya bilgi çalma gibi kötü amaçlı iletilerdir.
- **Truva Atı (Trojan):** Kendisini zararsız gösteren ancak arka planda kötü amaçlı işlevler (dosya silme, veri çalma, sistemde açık kapı bırakma) gerçekleştiren bir kötü amaçlı yazılım türüdür; kendini kopyalamaz.
- **Virüs Tanımlama Dosyaları (Virus Definition Files):** Bkz. DAT Dosyaları.
- **Zararlı Yazılımlar:** Bkz. Kötü Amaçlı Yazılım.
- **Zombi Bilgisayar:** Bir botnet’e dahil edilmiş ve kötü amaçlı yazılımlar tarafından uzaktan kontrol edilebilen bilgisayar.