KASPERSKY lab

Kaspersky Endpoint Security çözümünün koruma teknolojileri

www.kaspersky.com.tr
#truecybersecurity

Kaspersky Endpoint Security çözümünün koruma teknolojileri

Bu makalede Kaspersky Lab'in kurumsal ağ uç noktalarına yönelik çözümü Kaspersky Endpoint Security'de kullanılan tehdit tespit teknolojilerini inceleyeceğiz.

Uç nokta korumasının gelişim tarihi

Geçmişte yalnızca iş istasyonlarını ve sunucuları kapsayan uç nokta kavramı, günümüzde mobil cihazları ve sanal ortamları kapsayacak şekilde genişletilmiştir. BT altyapıları daha karmaşık hale gelmiş ve sürekli süreçlerin çalışmasını sürdürmede çok daha önemli roller üstlenmeye başlamıştır.

Büyük veri analizi, dağıtılmış veri depoları, süreçlerin otomasyonu gibi teknolojiler, güvenlik için modern yaklaşımlar gerektirir. Aynı zamanda, gizli veri ve finansal varlıklar siber suçluların daha fazla dikkatini çeker. Günümüzdeki tehditlerin çoğu temelde para kazanmaya yönelik araçlardır. Bu tehditler, mağdurlarının ciddi finansal kayıplara ve itibar kayıplarına uğramasına neden olur.

Karmaşık saldırılar, BT güvenlik çözümleri geliştiricileri için yeni bir zorluk oluşturur ve onlara karşı etkili koruma sağlamak yüksek bir uzmanlık düzeyi gerektirir.

Aşağıda, modern uç nokta korumasının sahip olması gereken öznitelikler listelenmiştir:

İş istasyonları, tehditler için ana giriş noktası olmaya devam etmektedir. Bu nedenle kaliteli koruma ihtiyaçları da her geçen gün artmaktadır.

- kullanılan teknolojilerin dengeli çalışması sayesinde hedef sistem üzerinde minimum etki;
- hızlı tespit: uzman bulut hizmetlerinin kullanımı dahil olmak üzere anormal etkinliklerin tespit edilmesi için gelişmiş yöntemler;
- tespit edilen olayların otomatik olarak incelenmesi;
- sistemde kötü amaçlı eylemlerin otomatik olarak geri alınması;
- olaylar hakkındaki bilgilerin SIEM olay ilişkilendirme sistemine ve diğer çözümlere aktarılması;
- kolay yönetim: önceden yapılandırılmış işlevselliğe sahip sezgisel arabirim;
- merkezi yönetim;
- dahili koruma teknolojilerinin bütünlük kontrolü;
- etkin hizmetler: ürün desteği, inceleme araştırması, eğitim vb.

Yukarıdaki listeden modern korumanın artık basit bir imza tabanlı tespit mekanizması olmadığı açıkça görülmektedir. Modern koruma yöntemi, kolay yönetim sağlayan gelişmiş teknolojilerden oluşur.

Güvenlik araçlarını seçerken işlevsel gerekliliklerin yanı sıra dikkate alınması gereken bazı önemli etkenler vardır. Çözümün içinde hangi teknolojilerin uygulandığı ve bu teknolojilerin birbirlerine nasıl bağlandığı açıkça belirtilmelidir. Aynı zamanda üreticinin uzmanlık ve deneyim seviyesini belirlemek ve gelecekte teknoloji geliştirme becerisini değerlendirmek de büyük önem taşır.

Makine öğrenimi yöntemini içeren teknolojiler

Özellik mühendisliği teknikleri, ML algoritmalarında kullanılacak öznitelikleri belirlemek için uzman bilgisi uygulama sürecidir.

Makine öğrenimi (ML) yöntemleri, son zamanlarda büyük dikkat çekmiş ve büyük hacimli verilerde başarılı bir şekilde kullanılmıştır. Ancak ML, tehdit tespiti konusunda etkili bir şekilde kullanılmadan önce özellik mühendisliği tekniklerinin yanı sıra BT güvenliğinde kayda değer miktarda deneyim ve uzmanlık elde edilmesi gereklidir.

ML'nin tehdit tespit görevlerinde ham verilerle kullanılabileceğine dair yaygın bir yanlış inanış vardır. Maalesef ML, tam olarak bu şekilde kullanılamaz. Eski bir programcılık atasözünde söylendiği gibi: "garbage in, garbage out." (kötü girdiler,

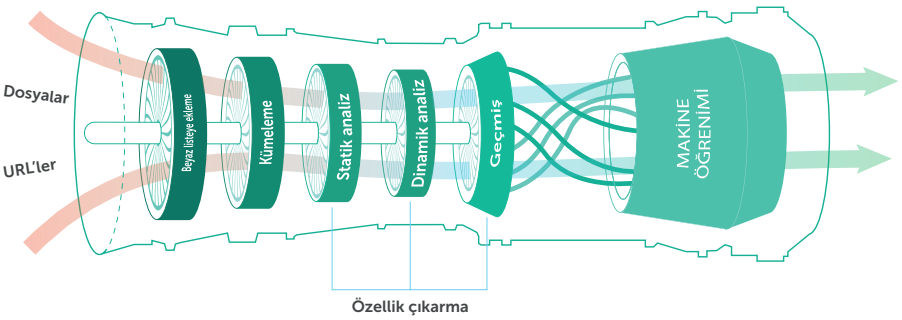
kötü sonuçlar verir) Eğitim süreci düzenlenirken verilerin doğru şekilde önceden işlenmesi ve uzman bilgisi ile desteklenmesi önemlidir (özellik mühendisliği). Kötü amaçlı yazılım analistleri ve onların kapsamlı deneyimleri olmadan etkili algoritmaların oluşturulabileceğini düşünmek naifliktir. Aslında analistler, bu süreçte denetim görevini üstlenir. Algoritmaların çalışmasını kontrol edip ince ayarlamalar yapar ve otomatik analizin her zaman yeterli olmayabileceği karmaşık

tehditleri doğrulama görevlerine dahil olurlar.

Kaspersky Lab, analizlerinin ve biriktirdiği uzman verilerinin yanı sıra kendi araştırma departmanları tarafından gerçekleştirilen yirmi yıllık geliştirme süreci sayesinde makine öğrenimi yöntemlerini kullanarak tehditlerin büyük bir çoğunluğu tespit eder.

Tehdit işleme ve analiz merkezi, nesneleri girdi olarak kabul eden bir "türbine" benzetilebilir. Bu nesneler, ML algoritmaları dahil olmak üzere çeşitli teknolojiler kullanılarak bazı işleme ve analiz aşamalarından geçer. Ortaya çıkan çıktı analizi,

Otomatik tehdit işleme ve analiz merkezi



Kaspersky Security Network aracılığıyla kullanıcılara sunulan tehdit tespit kurallarını formüle etmek için kullanılır.

ML algoritmaları, her gün **310.000'den** fazla benzersiz tehdidi tespit eder ve tanımlar. Kaspersky Security Network'ün çalışması sayesinde bu tehdit bilgilerinin çoğu anında uç nokta güvenlik teknolojilerine sunulur.

Aynı zamanda hatalı pozitif sonuçları önlemeye dikkat edilir. Bu özellik, yeni oluşturulan tespit kurallarının temiz dosyalardan oluşan kapsamlı bir veritabanıyla karşılaştırılarak denetlenmesini içerir.

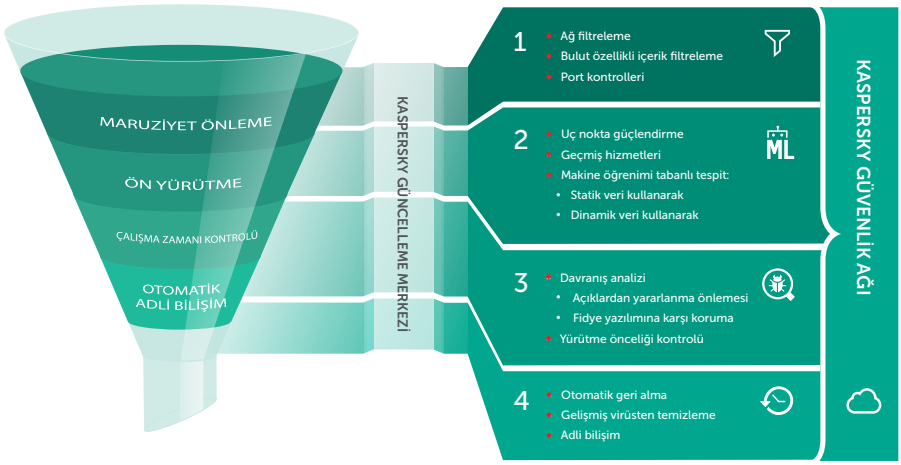
Kaspersky Endpoint Security

İşletmeleri hedef alan tehditlerin gelişimi, yeni nesil uç nokta güvenlik teknolojilerinin ortaya çıkmasına neden olmuştur. Kaspersky Lab, ML yöntemlerini kullananlar dahil olmak üzere çeşitli güvenlik teknolojileri geliştirmiş ve uygulamıştır. Kaspersky Lab, bu teknolojiler sayesinde tehdit tespitini önemli ölçüde hızlandırmış ve aynı zamanda korunan sistem üzerindeki etkiyi azaltmayı başarmıştır. Günümüzde Kaspersky Endpoint Security (KES), kurumsal ağlardaki uç noktaları koruyan son derece etkili bir güvenlik ürünüdür.

Koruma teknolojilerinin aşamaları

KES çalışmasının arkasındaki mantık, genel hatlarıyla dört aşamaya bölünebilir:

Kaspersky Endpoint Security Koruma Teknolojilerinin Sırası

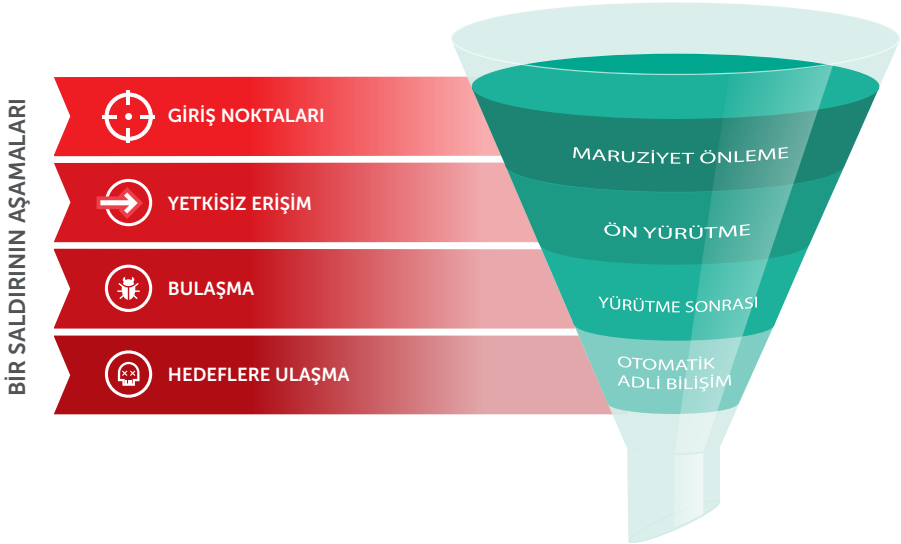


Her aşama, bağımsız bir koruma teknolojileri grubu ile temsil edilir. Yani bu teknolojilerden her biri, kendi uzmanlık alanına denk gelen bir tehdidi tespit edebilir ve engelleyebilir. Yukarıdaki aşama sırası ise çözümün tamamın özelliklerini göstermektedir. Güvenlik teknolojilerinin yanı sıra uzman desteği sağlayan iki bulut hizmeti de bulunmaktadır.

- Güncelleme **merkezi**, yerel uzman veritabanları (imza veritabanı, sezgisel veritabanı, davranış senaryoları veritabanı vb.) dahil olmak üzere koruma bileşenlerinin zamanla kademeli olarak güncellenmesini içerir. Ayrıca güncelleme merkezi, kullanılan tüm ML algoritmalarının parametrelerindeki operasyonel değişiklikleri biriktirerek koruma sağlarken daha fazla esneklik sunar.

- **Kaspersky Security Network**, çeşitli istatistiksel verilere (bilinirlik, içerik, davranış vb. istatistikleri) gerçek zamanlı erişim sağlayan bulut tabanlı bir altyapıdır. Bu teknoloji, tehdit tespit sürelerini azaltır ve korunan düğümün kaynaklarını muhafaza eder.

Yukarıdaki koruma teknolojileri sırası bir saldırının aşamalarına yanıt sırasını



gösterir. Her aşama, tehdidin önlenmesi için gereken kendi güvenlik düzeyini sunar.

Şimdi koruma teknolojilerinin her aşamasını ayrı ayrı ele alacağız.

1. Maruz kalmayı önleme

Günümüzde tehditler, mümkün olan tüm bilgi kanalları aracılığıyla yayılır. Bu nedenle korunan düğümün çevresinin, güvenilir bir şekilde korunması büyük önem taşır.

Birinci aşama, gelen tüm bilgilere yönelik bir filtredir. Önleyici engelleme teknolojileri, korunan düğümün ana etkinliğini izleyerek bilinen tehditlerin erkenden tespit edilmesini ve engellenmesini sağlamak için kullanılır. Birinci aşamadaki engelleme teknolojilerine göz atalım.

1.1 Ağ saldırılarına karşı koruma ve güvenlik duvarı

Ağ bağlantılarının güvenliği, imza tabanlı bir ağ sensörü olan **İzinsiz Giriş Tespit Sistemi (IDS)** tarafından kontrol edilir. Çalışma sırasında IDS, ağ sensörünün geçen trafiğinin tamamını kontrol etmesine olanak tanıyan Derin Paket Denetimi (DPI) teknolojisini uygular. Bu sayede birden çok şüpheli ve tehlikeli ağ olayı anında tespit edilebilir.

Ağ olaylarına örnek olarak aşağıdakiler verilebilir:

- bağlantı noktalarının etkin olarak taranması;
- işletim sisteminin farklı bağlantı noktalarına bağlanma girişimleri;
- anormal ağ iletişiminin tespit edilmesi, ör. uzaktan yönetim araçlarının kullanımı, komuta ve kontrol merkezinden gönderilen komutlar (botnet'leri içeren durumlarda).

Tehlikeli bir ağ olayı tespit edildiğinde sensör güvenlik duvarı işlevini kullanarak bağlantıyı engeller.
Güvenlik duvarı: önceden ayarlanmış kurallara göre korunan düğümün ağ etkinliğini filtreleyen engelleme teknolojisi:

- ağ paketlerinin ve veri akışlarının filtrelenmesi;
- ağ ile etkileşim kurarken yazılım etkinliği.

Parametreler, yönetici tarafından ağ bağlantı ilkesinde belirlenir.

2016 yılında kullanıcı bilgisayarların %31,9'u, interneti kullanırken bir veya daha fazla kötü amaçlı yazılım sınıfı zararlı nesne tarafından saldırıya uğramıştır.

1.2 Web filtreleme

İnternet kaynakları, birer tehdit kaynağıdır. Güvenilir bir web düğümü, ele geçirilebilir ve kötü amaçlı bir komut dosyası veya sıfır (0) gün güvenlik açığı bu düğümde barındırılabilir. Bu durum, günlük işlemleri güvensiz hale getirir. İnternet kaynaklarıyla kolay ve güvenli çalışma sağlamak için web filtreleme teknolojisi iki koruma düzeyinden oluşan KES teknolojisinde uygulanır.

Birinci düzey, bulut tabanlı Kaspersky Security Network (**KSN**) ile ilgilidir ve pasif filtrelemeden sorumludur. Örneğin bu düzey, bir web kaynağının ait olduğu kategori veya sahip olduğu bilinirliğe göre gerçek zamanlı bir referans sağlar. Bu işlem, tarayıcı içeriği indirmeye başlamadan önce gerçekleştirilir.

KSN bilinirlik veritabanı URL'leri aşağıdaki kategorilere ayırır:

- kötü amaçlı URL: bulaşma tehlikesi taşır;
- kimlik avı URL'si: kişisel bilgileri çalmak için kullanılır;
- bilinmeyen URL: mevcut bilinirlik bilgisi yoktur;
- güvenli URL: güvenli kaynak.

2016 yılında 261.774.932 farklı URL, koruma teknolojilerini harekete geçirmiştir.

Web filtreleme, güvenliğe büyük ölçüde katkı sağlar, tehlikeli oldukları bilinen birçok web sitesini engeller ve korunan bir düğümün kaynaklarını muhafaza eder.

İkinci düzey, dinamik analiz teknolojisini temel alır ve bilinmeyen tüm web kaynaklarından indirilen içeriği izler. Aşağıda ikinci aşama koruma teknolojileriyle ilgili bilgi verilirken bu düzey tekrar ele alınacaktır.

1.3 Bağlı çevre birimlerinin kontrolü

Taşınabilir cihazlar da korumalı düğüm için olası bir tehdit oluşturur. Çevre birimleri kontrolü, bağlı cihazın türünü tanımlar ve kullanıcıdan cihazı bağlamanın sorun olmayacağını onaylamasını ister. Onay isteği, kullanıcının gösterilen anahtarı girmesini talep eder. Bu kontrol, yanıltıcı senaryoların belirlenmesine yardımcı olur. Örneğin bazen bir hafıza kartı, tarama işleminden kaçmak için klavye işlevini görebilir. Siber suçlular, güvenlik teknolojilerini yanıltmak ve korunan çevreye sızmak için bu yöntemi kullanır. Çevre birimleri kontrolü, bilinmeyen nesnelerin analiz edildiği yürütme önleme aşamasındaki teknolojilere ayrılmaz bir şekilde bağlıdır.

2. Yürütme önleme aşaması

Siber suçlular için yalnızca ilk filtrelemeyi geçmek değil, aynı zamanda kötü amaçlı yazılımların erken belirlenmesinden sorumlu tespit teknolojilerini kandırmak da önemlidir. Bir saldırının başarılı olması için kötü amaçlı kodun güvenilir ortamda yürütülmesine izin verilmelidir. Siber suçlular, tespit teknolojilerini atlatmak için tekniklerini sürekli değiştirerek amaçlarına ulaşmaya çalışır.
Ana teknikler aşağıda listelenmiştir:

- **paketleyiciler**: kötü amaçlı yapıyı paketlenmiş biçimde saklayarak tespit işlemini zorlaştırır;
- **kod gizleme**: kodu algoritma düzeyinde karmaşık hale getirmek için özel derleyiciler tarafından kullanılır;
- **çok biçimlilik**: zararlı programın kodu, program yürütülürken değiştirilir;
- **sunucu çok biçimliliği**: kötü amaçlı sunucuya her erişim sağlandığında sunucu tarafından yeni bir kötü amaçlı program numunesi üretilir;
- **şifreleme**: kodun bir kısmını tespit mekanizmalarından gizlemek için çok seviyeli şifreleme kullanılır. Bu yöntem genellikle, gizleme ile birlikte uygulanır;
- **0 gün açıkları dahil olmak üzere güvenlik açıkları**: yazılımların güvenlik açıklarını kullanmak, etkili bir saldırı yöntemidir;
- **emülatörleri atlatmak**: kötü amaçlı yazılımlara karşı koruma sağlayan bir emülatör, yürütülebilir bir dosyayı izole bir ortamda çalıştırıp çalışma mantığını analiz ederek kontrol eder. Kötü amaçlı kod, imzalar veya sezgisel algoritmalar kullanılarak tespit edilebilir. Saldırganlar, kodun çalışma mantığının emülatörler tarafından belirlemesini önlemek için farklı kod algoritması değiştirme yöntemlerinden faydalanır.

Yukarıdaki yöntemlerden iki veya daha fazlasının birlikte kullanılması, genellikle siber suçlular tarafından korunan düğüm ortamına sızmak için kullanılan güçlü bir yöntemdir. Bu yöntemle mücadele etmenin tek yolu, yürütülebilir nesneleri kontrol etmek ve analiz etmek için en yeni yöntemleri içeren kapsamlı teknolojik koruma teknolojilerini kullanmaktır.

Yürütme önleme aşaması, sürekli olarak büyük miktarda verinin analiz edildiği yoğun bir aşamadır.

Bu aşamada temel alınan teknolojileri ve gerçekleştirilen görevleri ayrıntılı olarak inceleyelim.

2.1 Güvenilir ortamı güçlendirme

2016 yılı tespit istatistiklerine göre, yazılım güvenlik açıkları, etkin bir şekilde bulaşma noktaları olarak kullanılmaktadır.

Öncelikle, güvenilir ortam için denetim zorunludur. Bu zorunluluk, işletim sistemindeki ve üçüncü taraf yazılımlardaki savunmasız bileşenleri belirleyerek ve ortadan kaldırarak olası tehditleri azaltmak amacıyla uygulanır.

Bunun için global CVE (Common Vulnerabilities and Exposures) veritabanını kullanan bir güvenlik açığı değerlendirmesi gerçekleştirilir. Bu, Kaspersky System Management bileşeni tarafından merkezi olarak yönetilen otomatik bir süreçtir. Yazılımda belirlenen tehditleri anında bildirmeye ve Düzeltme Eki Yönetimi yazılım güncelleme teknolojisiyle tehditleri zamanında ortadan kaldırmaya yardımcı olur.

Kaspersky Lab, tehdit tespit kalitesini artırma ve hatalı pozitif sonuçları en aza indirme çalışmalarının bir parçası olarak Teknoloji Birliği'ni geliştirmektedir. Bu Teknoloji Birliği, bağımsız ücretsiz yazılım geliştiricilerinin yanı sıra EN İYİ İLK 500 yazılım üreticisini de kapsar. Kaspersky Lab, bu sayede proaktif olarak Varsayılan Olarak Reddet teknolojisiyle kullanılabilecek listeler dahil olmak üzere beyaz listeler üretebilir.

Yazılım güncelleme teknolojisi, yüklü yazılımların güncel kalmasını sağlar. İki teknoloji birlikte kullanıldığında korunan ortamı güçlendirir ve güvenlik açıklarından yararlanılması riski önemli ölçüde azaltır.

Ayrıca, ek **Varsayılan Olarak Reddet** engelleme teknolojisi de unutulmamalıdır. Bu teknoloji, yazılım başlatma kontrolüne alternatif bir yaklaşım sağlayarak temelde "yazılıma izin verilmemişse yasaktır" ilkesini benimser.

Bu yaklaşımda yönetici, şirket işlerinin yapılabilmesi için hangi yazılım ürünlerinin gerekli ve yeterli olduğunu belirleyebilir.

"Varsayılan Olarak Reddet" yaklaşımının avantajları şunlardır:

- kötü amaçlı programların yeni sürümleri dahil olmak üzere bilinmeyen uygulamalar engellenebilir;
- iş görevleriyle ilgili olmayan yasa dışı/lisanssız yazılımların kurulumu ve başlatılması engellenebilir.

Bu teknoloji, yöneticinin yazılım programlarına atayabileceği geniş bir kategori yelpazesi sağlar (ör. güvenilir üreticiler, manuel olarak eklenen güvenilir hesaplar, yetkisiz veya lisanssız yazılım vb.). Listeler, tehdit işleme ve analiz merkezi tarafından otomatik olarak oluşturulur ve güncellenir ve insanların işlemlere dahil olmasını gerektirmez.

2.2 Bilinirlik hizmetleri

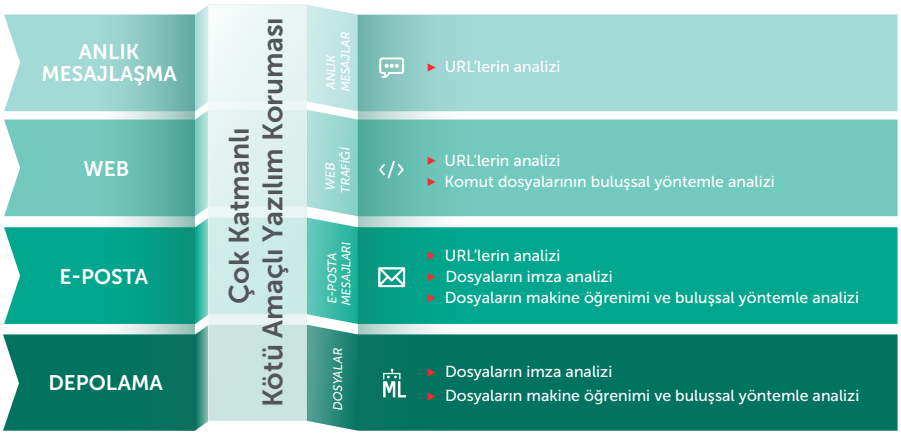
Kaspersky Security Network çözümünün bu parçası, tehditlerin hızla tespit edilmesini sağlar. Bu işlem, nesneler hakkında ayrıntılı bilgiler içeren çevrimiçi bilinirlik veritabanlarının yardımıyla yapılır. Veritabanları sürekli olarak uzman bilgileriyle yenilenir. Bu bilgiler, koruma için uzman bulutunu kullanan diğer KSN altyapı katılımcılarının sahip olduğu tespit teknolojilerinden gelen bilgileri içerir. Bilinirlik hizmetlerinin avantajları aşağıdaki gibidir:

- her nesne için kararlar anında verilir;
- uç noktanın bilgi işlem kaynaklarına bağlı değildir.

Kontrol edildikten sonra her dosya, bir kategoriye atanır:

- **Kötü Amaçlı**: dosya kötü amaçlı kod içerir;
- **Temiz**: dosyanın analizi geçtiğini ve güvenli olarak tanımlandığını belirtir;
- **Bilinmeyen**: daha önce analiz edilmemiş ve potansiyel olarak tehlikeli olan yeni bir dosya.

"Bilinmeyen" olarak sınıflandırılan her dosya, analiz için otomatik olarak makine öğrenimini kullanan tespit teknolojilerine aktarılır.



2.3 Çok aşamalı koruma

İkinci aşamadaki son görev, farklı analiz teknolojileri kullanarak karmaşık tehditleri

belirlemektir. Bu işlem, bilgi giriş noktası türüne göre önceden belirlenen bir dizi senaryodan oluşan çok aşamalı bir koruma bileşeni kullanılarak gerçekleştirilir.

Çok aşamalı koruma aşağıdaki gibi çalışır:

Her senaryo, kendine atanan tespit teknolojilerine sahiptir ancak gerektiğinde tespit teknolojileri, gerekli koruma düzeyini sağlamak için birlikte kullanılabilir.

Web filtreleme – dinamik koruma

Web filtrelemenin (ilk filtreleme aşaması) devamı olarak çalışan bir teknolojiyle başlayalım. İndirilen içerikteki tehdit tespitinin etkin aşamasından sorumludur. İlk aşamada, URL'ler her web kaynağının ait olduğu kategoriyi belirlemek için statik olarak kontrol edilir. İkinci aşamada ise bilinmeyen HTML kodu, kontrollü indirme aşaması başlar başlamaz dinamik analiz işlemine tabi tutulur.

Aktif tespit aşamasında aşağıdaki teknolojiler uygulanır.

- **Sezgisel URL analizi**
  Her URL, korunan düğümdeki tarayıcıda açıldığı anda analiz edilir. HTML kodu bir emülatöre yüklenir ve yürütülmesi sezgisel bir analiz teknolojisi tarafından izlenir. Bu işlem, HTML kodunda gizlenmiş tehditlerin belirlenmesine yardımcı olarak tehlikeli web kaynaklarının açılmasını engeller.

- **Komut dosyalarının sezgisel analizi**
  HTML belgelerindeki komut dosyalarının analizine özellikle dikkat edilir. Bu işlem, farklı betik dillerindeki karmaşık tehditleri tespit edebilen bir emülatörün kullanımını içerir. **Web filtrelemenin** pasif (ilk filtreleme aşaması) ve etkin (izinsiz giriş önleme) düzeyleri birlikte kullanıldığında, kullanıcı için güvenli bir göz atma deneyimi sağlanır.

  Web filtreleme teknolojileri, bir URL adresinin mevcut olabileceği diğer bilgi giriş noktalarında (ör. **e-posta veya mesaj uygulamalarında**) çalışırken de güvenlik kontrollerinde uygulanır.

2016 istatistikleri: web filtreleme teknolojileri komut dosyaları, açıklardan yararlanan yazılımlar ve yürütülebilir dosyalar gibi 69.277.289 adet benzersiz nesne tespit etmiştir.

E-posta

E-postalardaki tehditler analiz edilirken **URL sezgisel analiz** teknolojisinin yanı sıra dosya eklerini analiz etmek için bazı ek teknolojiler kullanılır.

E-posta, siber suçlular tarafından en çok kullanılan saldırı noktalarından biridir. Sosyal mühendislikte hedefli kimlik avı adı verilen bir trend vardır. Bu trend, dikkat bir şekilde hedef alınan etkiyi gerçekleştirmek için tasarlanmış bir yaklaşımdır. Örneğin arşivlenmiş eklerin yanı sıra güvenlik açıklarından yararlanan bir yazılımı içeren özel olarak hazırlanmış bir e-posta, hedef kullanıcıya gönderilebilir. Arşiv parolaları, iletinin gövdesinde veya grafik bir biçimde sağlanabilir. Bu tür e-postalar, koruma araçları için arşivlenmiş dosyaları otomatik olarak açma ve analiz etme gibi bazı özellikler gerektirebilir.

Şimdi dosya analiz teknolojilerini ele alalım.

- **İmza tabanlı dosya analizleri**
  İmza tabanlı analiz teknolojisi, bir nesnede tehdit olup olmadığının belirlenmesi için hızlıca kontrol edilmesi gereken farklı koruma senaryolarında uygulanır. Bu e-posta senaryosunda, ekteki dosyaları kontrol etmek için gereklidir.

  İmza tabanlı yöntem bazı avantajlara sahiptir ve bu nedenle dosya analizi için uygulanan ilk yöntemdir. Başlıca avantajları şunlardır:
  - hızlı tespit;
  minimum düzeyde hatalı pozitif sonuç;
  - korunan düğümün kaynaklarını tüketmez.

  Bu yöntem, doğal olarak veritabanında (sürekli güncellenir) bulunan imza sayısıyla sınırlıdır. Dolayısıyla imza tabanlı analiz, sezgisel analiz ile birlikte çalışır.

İmza, kötü amaçlı bir nesneyi açık bir şekilde tanımlayan kod parçasıdır.

- **Makine öğrenimi yöntemleriyle dosya analizi**
  Aşağıda, makine öğrenimi teknolojisi kullanılarak yapılan dosya analizini ayrıntılı bir şekilde inceleyeceğiz. Bir e-posta koruma senaryosunda makine öğrenimi, parola korumalı arşiv eklerinin açılması için benzersiz bir özellik sağlar. Bu teknoloji, paketi açmak için parolayı (grafik veya metin biçiminde

bulunur) iletinin gövdesinden çıkarır. Parolalar, siber suçluların tespit teknolojilerini atlatmak için kullandığı tekniklerden biridir. İçindekilerin analiz edilemediği korumalı arşiv, "güvenli" bir dosya olarak görünür. Grafik biçiminde sağlanan parolayı tanımak için bir makine öğrenimi algoritması kullanılır. Bundan sonra parola, parola korumalı arşivin içeriğini ayıklamak için kullanılır.

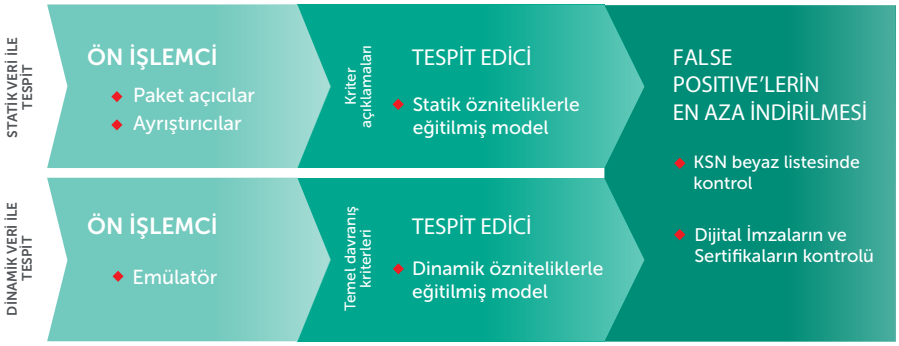
Dosya Depolama

Bilinmeyen her dosya korumalı düğüm için olası bir tehdit oluşturur ve koruma teknolojilerinin özellikle dikkatli olmasını gerektirir.

Bu tür durumlarda çok aşamalı koruma, makine öğrenimi yöntemlerinden faydalanan derin analizin yürütüldüğü gelişmiş bir senaryoya sahiptir.

Birçok dosya analiz teknolojisi vardır.

- **İmza tabanlı dosya analizleri**
  Temel avantajları, yukarıdaki e-posta güvenlik bölümünde listelenmiştir. Bu senaryoda imza tabanlı teknoloji, temel bir filtrenin görevini üstlenir. Bu filtre, tüm bilinen dosyalar için kararları sağlar ve yalnızca bilinmeyen dosyaları makine öğrenimi yöntemleri kullanılarak analiz edilmesi için bırakır.



- **Makine öğrenimi yöntemleriyle dosya analizi**
  Bu, çok aşamalı korumanın en gelişmiş teknolojisidir. Dosyalar üzerinde derin analiz gerçekleştirerek tehditlerin erkenden tespitini sağlar. Bu teknoloji, statik ve dinamik veriler üzerinde dosya analizi gerçekleştiren iki paralel sürecin yürütülmesine dayanır.

  Bu iki süreç, üç aşamaya ayrılır ve her bir aşama, belirli teknoloji gruplarından oluşur. Statik ve dinamik yaklaşımlar, birlikte iyi çalışır ve birbirlerinin olası eksikliklerini tamamlar. Örneğin;
  - model kötü amaçlı programların statik öznitelikleri konusunda eğitildiği zaman bazı dosyalar, temiz dosyalardan çok az farklı gibi görünebilir;
  - model dinamik öznitelikleri konusunda eğitildiği zaman bazı programlar kötü amaçlı davranışlar göstermeyebilir. Bu tür programlar, başlamak için belirli bir ortam veya özel bir komut satırı gerektirebilir.

Statik veriler, yürütmeden toplanan bir nesneyle ilgili bilgilerdir. Bu teknoloji, yüksek genelleme kapasitesine ve performansına sahiptir.

İlerleyen kısımlarda her sürecin nasıl çalıştığına daha yakından bakacağız.

Statik verilere dayalı tespit

Ön işlemci, hazırlık teknolojileri:

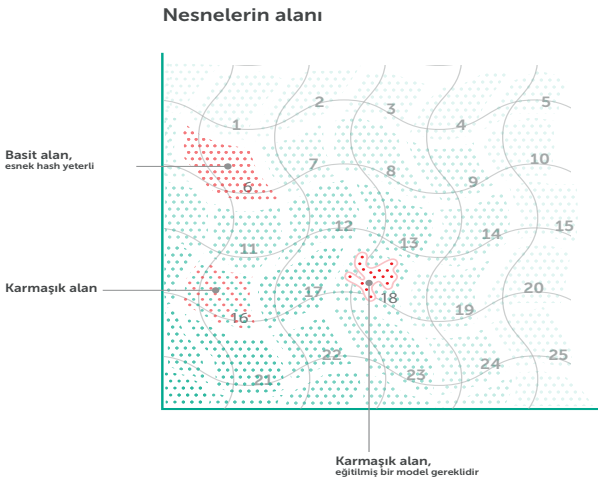
- **paket açıcılar** paketlenmiş kodu ayıklayarak ayrıştırıcıların koddaki meta verileri ayıklamalarını sağlar (paketleyiciler, gizleme ve şifreleme yöntemleri, siber suçlular tarafından kullanılan tipik tespit teknolojilerinden kaçma yöntemleridir);

- **ayrıştırıcılar** çeşitli meta veri kümelerini ayıklamaya yönelik araçlar.

Meta verilerin çeşitliliği, doğrudan tespit kalitesini etkiler. Bu nedenle ön işlemci, farklı ayrıştırıcılardan oluşan geniş bir kitaplık içerir. Ayrıştırıcılar, bilgilendirici öznitelik açıklamaları (yürütülebilir dosyaların yapıları, verilerin ve kodun istatistiksel özellikleri, dizeler vb.) sağlar.

Tespit sistemi, öznitelik açıklamalarını analiz eder ve analiz edilen her nesnenin

kötü amaçlı olup olmadığıyla ilgili bir karar verir. Tespit sisteminin çalışması, iki aşamadan oluşur.



Birinci aşamada esnek bir karma hesaplanır ve analiz edilen nesnenin "kirli" alanda olup olmadığı etkili bir şekilde kontrol edilir. Alan basitse (örn. sadece bir türde nesneler içeriyorsa: tamamı "temiz", tamamı "kirli" gibi) karar bu aşamada verilebilir. Esnek bir karma, çok biçimliliğe ve gizlenmeye karşı dayanıklı olma avantajına sahiptir. Bu özellik sayesinde korunan düğümde gerekli kaynak miktarı önemli ölçüde azalır.

Alan karmaşıksa (örn. hem "kirli" hem de "temiz" nesneleri içeriyorsa) nesne analiz için ikinci aşamaya gönderilir. İkinci aşamada, nesnenin öznitelik açıklamaları sınıflandırıcı tarafından değerlendirilir. Sınıflandırıcının görevi, veritabanında yer alan birçok modelin arasında uygun eğitilmiş modeli (ilgili alanda uzmanlaşan) bulmak ve uygulamaktır. Eğitimli model, nesnenin kötü amaçlı olup olmadığı konusunda son kararı oluşturur.

Esnek karma, bir dosya grubu için aynı olacak şekilde özniteliklere dayalı olarak geliştirilir.

Alan, esnek bir karmanın veya eğitilmiş bir modelin karşılık geldiği nesneler uzayının bir parçasıdır.

Dinamik verilere dayalı nesne analizi

Ön işlemci, nesnenin davranışı ve yürütülebilir kod içeren bellek alanları gibi dinamik bilgileri toplar.

Emülatör, yürütülebilir dosyanın kısmen gerçek sistemi taklit eden kontrollü bir ortamda yürütülebilmesini sağlar. Avantajları, bilgisayar kaynakları ve güvenliği üzerinde minimum etkiye sahip olmasıdır (analiz edilen kod güvenilir ortamı etkileyemez). Dinamik analiz, yürütme sırasında oluşturulan bellek dökümü ve diğer nesnelerin (ör. dosyalar) yanı sıra yürütülebilir dosya eylemlerinin kayıtlı sırasını üretir. Listelenen tüm veriler, temel davranış özniteliklerini oluşturur.

Dinamik veriler, nesne yürütülürken veya yürütme emülasyonu sırasında nesnenin davranışı hakkında toplanan bilgilerdir.

Bellek dökümü, asıl (paketlenmemiş) koda erişim sağlar ve dosyanın kötü amaçlı yapısını ortaya çıkaran verilerin tespitini mümkün kılar.

Tespit sistemi, kötü amaçlı davranış senaryosunu belirler ve analiz edilen her nesnenin kötü amaçlı olup olmadığıyla ilgili bir karar verir.

Tespit sistemi, Kaspersky Lab'in otomatik merkezi tarafından tehdit işleme ve analiz işlemleri için oluşturulan kötü amaçlı senaryolar kitaplığını kullanır.

Merkez, kötü amaçlı ve temiz dosyalardan oluşan geniş koleksiyonlara sahiptir. Bu koleksiyonlar modelleri eğitmek için kullanılan temel davranış özniteliklerini ayıklayarak sürekli işlenir. Modeller, davranış senaryolarına dönüşür ve kademeli güncellemeler biçiminde tespit sistemine iletilir. Bu yaklaşım, gereken süreyi ve güncellemenin boyutunu önemli ölçüde azaltarak tespit sisteminin etkili bir şekilde çalışmasını sağlar.

Kötü amaçlı senaryo, saldırı gerçekleştirilirken uygulanan eylem sırasıdır.

2016 istatistikleri: çok aşamalı koruma 4.071.588 adet benzersiz kötü amaçlı ve olası istenmeyen nesne bildirmiştir.

Hatalı pozitif sonuç, nesne temiz olmasına rağmen tespit sisteminin yanlışlıkla nesnenin kötü amaçlı olduğunu belirten kararı kabul etmesidir.

Hatalı pozitif sonuçların en aza indirilmesi

Tespit sisteminden geçen her karar, hatalı pozitif sonuç için kontrol edilir. Hatalı pozitif sonuç çıkma ihtimali son derece düşüktür. Ancak gerçekleşmesi durumunda ağır sonuçları olabilir.

Bir nesnenin kötü amaçlı olduğu tespit edildiğinde hatalı pozitif sonuç riskini azaltmak için aşağıdaki minimum kontroller yerine getirilir:

- eğitilen modelin sayısı veya belirlenen tehditle ilgili kararın yayınlanmasını sağlayan davranış senaryosu belirtilerek KSN bulut hizmetine bir talep gönderilir (KSN, modelin/senaryonun geri çağrılıp çağrılmadığını kontrol edebilmek için geçerli modeller ve davranış senaryolarıyla ilgili bilgiler içerir).
- Tespit sisteminden gelen tüm hatalı pozitif sonuçların elenmesi için KSN bulut hizmetinin beyaz listelerine bir talep gönderilir (Beyaz listeler, temiz olduğu bilinen dosyalardan oluşan büyük bir koleksiyondur. Bu koleksiyon, Kaspersky Lab'in otomatik merkezi tarafından sürekli olarak güncellenir.)
- dosyayı imzalamak için kullanılan sertifikanın bilinirliğini kontrol etmek için bir sertifika sınıflandırma bulut hizmetine talep gönderilir.

İkinci aşama ile ilgili olarak, önceden kontrol edilen nesnelerle ilgili taleplerin tekrar edilmesini önlemeye yardımcı olan yerel KSN önbelleğinin olduğu unutulmamalıdır. Bu önbellek sayesinde, korumalı düğümün kaynakları korunur.

2016 yılında şifreleyici saldırıları, 1.445.434 adet farklı kullanıcı bilgisayarında engellenmiştir.

Kaspersky Lab, 2016 yılında 54.000'den fazla yeni modifikasyon ve 62 adet yeni şifreleyici ailesi tespit etmiştir.

3. Yürütme kontrolü

İkinci aşama statik ve dinamik analiz teknolojilerini içermesine rağmen bazı tehditler bu aşamayı tespit edilmeden geçebilir. Örneğin yasal bir şifreleme yazılımı kullanan çok bileşenli şifreleyiciler, tespit sistemine takılmadan geçebilir. Çünkü bu tür şifreleyicilerdeki bağımsız bileşenler, herhangi bir tehdit oluşturmaz.

Üçüncü aşamanın amacı, güvenilir ortamda kötü amaçlı davranışı tespit etmektir. Analiz sırasında, tüm etkin bileşenlerin genel davranışı, dikkate alınır. Bunlara sistem bileşenlerinin yanı sıra güvenilir ve güvenilir olmayan uygulamalar da dahildir. Bu tür bir analiz, karmaşık ve çok bileşenli tehditleri belirlemeye yardımcı olur.

0 gün güvenlik açıkları, kodda yer alan henüz düzeltme eki uygulanmamış hatalardır. Bu açıklar, siber suçlunun sistemi ele geçirmek için belgelenmemiş program yürütme özelliklerini kullanmasını sağlar.

Davranış analizi, izinsiz giriş önleme aşamasında analiz edilen varsayılan (emülasyon) eylem görüntüsü yerine gerçek davranışı inceler.

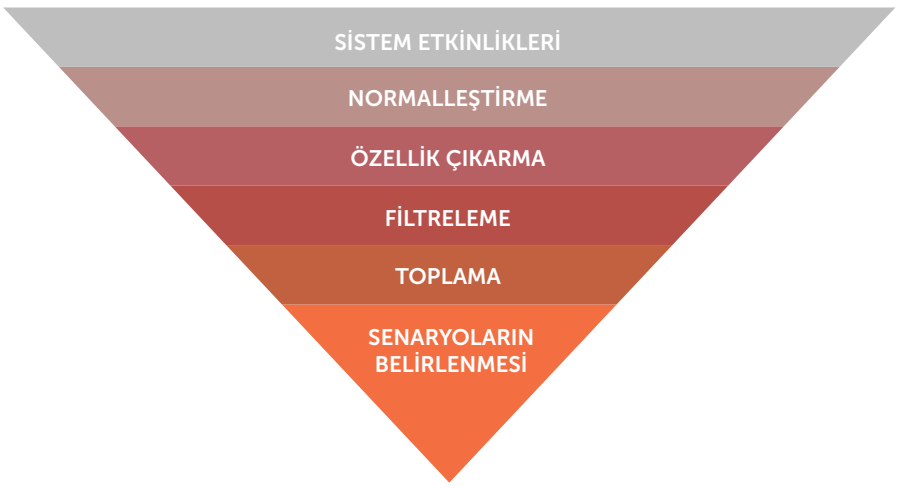
Diğer bir örnek de kötü amaçlı yazılımların önlenmesidir. Bu durumda, güvenilir bir uygulamada kötü amaçlı bir davranış tespit edilir.

Örneğin açıklardan yararlanan bir yazılıma sahip Word belgesi açıldığında Açıklardan Yararlanan Yazılımları Otomatik Önleme (AEP) Teknolojisi, kötü amaçlı davranışı tespit eder ve engeller. Bu teknoloji etkilidir ve 0 gün güvenlik açıklarına yönelik yazılımlar dahil olmak üzere karmaşık tehditleri engelleyebilir.

3.1 Davranış analizi

Bu teknoloji, korumalı düğümün güvenilir ortamındaki tüm etkin bileşenlerin davranışını analiz eder. Aşağıdaki analiz düzeylerinden oluşur:

Davranış analizi



- sistem olayları: süreç oluşturma, kayıt defteri anahtarı değerlerindeki değişiklikler, dosyalarda değişiklikler vb. gibi temel sistem olaylarının izlenmesi;
- normalleştirme: sonraki işleme süreçleri için gelen tüm olayları ortak bir biçimde düzenleme;
- özellik ayıklama: bazı olaylar için ek bilgiler ilave etme, ör. değiştirilmiş bir dosyanın yürütülebilir olup olmadığı;
- senaryoların filtrelenmesi, toplanması ve belirlenmesi: bu aşamalarda önemli olay kombinasyonları ve sıraları tanımlanır ve davranış senaryosu oluşturulur. Kaspersky Lab'in otomatik merkezi, tehdit işleme ve analiz işlemleri için referans olarak kötü amaçlı senaryolar kitaplığını oluşturur.

3.2 Ayrıcalık kontrolü

Ayrıcalık kontrolü, uygulama ilkelerine ve kategorizasyona göre davranış analizine paralel olarak yürütülür.

Kontrol, uygulama etkinliklerinin izlenmesinden ve uygulama özelliklerine göre kısıtlamaların uygulanmasından oluşur. Uygulama özellikleri arasında dünya çapındaki popülerliği, yayıncının güvenilirliği ve tespit işlemini tetiklemesi gibi özellikler bulunur. Bu kontrol nedeniyle program, korumalı ortamda ağ iletişimi kurmak veya benzeri etkinlikler gerçekleştirmek gibi kontrolsüz eylemler yapamaz.

Kaspersky Lab'in otomatik tehdit işleme ve analiz merkezi, farklı uygulama kategorileri için temel kısıtlamalar oluşturur.

Örneğin, Microsoft uygulamaları veya diğer iyi bilinen uygulamalar için zayıf bir kontrol ilkesi atanır. Ancak ayrıcalık kontrol sistemi, az bilinen uygulamalara uygulamanın taşıyabileceği risk ve tehlike düzeyine göre daha sıkı kurallara sahip bir ilke atar.

Ayrıcalık kontrolü, güvenilir yazılım programlarının (etkinse) "Varsayılan Olarak Reddet" listeleriyle birlikte çalışır ve gerçek zamanlı güvenlik sağlar. Kısıtlamalar, şirket ağı seviyesinde merkezi olarak yönetilebilir veya alternatif olarak kişisel verilerin korunması, bireysel olarak yapılandırılabilir.

4. Bulaşmadan sonra onarım

Bulaşma, kötü amaçlı bir kodun güvenilir ortamda yürütülmesidir. Bu durumda yürütülen süreç, siber suçlular tarafından belirlenen hedeflere ulaşmak için çalışmaya başlar ve bir dizi farklı olay oluşturur. Genellikle bu tür durumlar, güvenlik çözümü virüslü olduğu bilinen bir düğüme yüklendiğinde veya davranış çözümleme düzeyinde potansiyel olarak tehlikeli bir etkinlik tespit edildiğinde görülür. Örnek olarak dosya şifrelemenin korumalı düğümün yerel sürücüsündeki yasal bir süreç tarafından başlatılmış olması gösterilebilir.

2016 yılında şifreleyiciler tarafından saldırılan kullanıcıların %22,6'sı, kurumsal firmalardır.

Bu tür durumlarda korumanın dördüncü aşaması başlar. Bu aşama, bir tehdide karşı acil durum yanıtından sorumludur.

Davranış analizi teknolojileri potansiyel olarak tehlikeli bir etkinliği engellediğinde güvenilir ortamı önceki durumuna getiren bir eylem planı uygulanmalıdır.

4.1 Eylemlerin otomatik olarak geri alınması

Eylemlerin otomatik geri alınması, engellenen işlem tarafından gerçekleştirilen adımları izleyerek yapılan değişiklikleri iptal eder. Temelde eylem sırasını çözerek yapıyı önceki durumuna getirir. Her bir süreç tarafından yürütülen eylemler için ayrıntılı bir geçmiş hazırlayan **davranış analizi** aşaması, bu teknolojilere yardımcı olur.

Olay sırası şunları içerebilir:

- işletim sistemi kayıt defterinin dalları;
- süreç tarafından oluşturulan yürütülebilir dosyalar (komut dosyaları veya ikili dosyalar);
- değiştirilmiş dosyalar, örn. şifreleyicinin şifrelediği dosyalar.

4.2 Gelişmiş temizleme

Bazı karmaşık durumlarda (ör. kötü amaçlı bir kod, işletim sisteminin dengesini etkilemeden müdahale etmenin imkansız olduğu bir sistem sürecine sızmışsa) etkin bir bulaşmayı onarma teknolojisi, sürece dahil olur. Bu araç, işletim sisteminin bileşenleri dahil olmak üzere saldırıdan etkilenen dosyaları güvenli bir şekilde geri yükleyebilir. Etkin onarım durumunda, korumalı bilgisayar yeniden başlatılır. Virüslü sistem bileşenleri temiz bileşenlerle değiştirilir. Bu işlemde teknoloji, geri yükleme için gerekli orijinal dosyaları arama becerisini kullanır. Bu şekilde sistem, stabil durumuna geri döner.

2016 yılında toplam 4.071.588 adet kötü amaçlı ve potansiyel olarak tehlikeli program bildirilmiştir. (Benzersiz programların sayısının, benzersiz karar sayısı olduğu varsayılır.)

4.3 Adli Bilişim

Her bilgi güvenliği olayının analizi, kendi kanıt tabanını gerektirir. Koruma teknolojileri geniş bir yelpazede farklı veriler topladığı için olay analiz edilebilir ve önleyici bilgi güvenlik önlemleri alınabilir.

İç güvenlik önlemleri

Çözüm, güvenilir bir şekilde çalışmaya devam etmek için kendi güvenliğini kontrol eden araçlara sahiptir. Bu, kullanıcının devre dışı bırakma girişimlerine karşı koruma dahil olmak üzere koruma bütünlüğü sağlar.

Bu kendini savunma araçları, kullanıcı haklarına ve ayrıcalıklarına bakılmaksızın güvenilir ortamdaki kaynaklarla güvenli olmayan işlemleri durdurur ve engeller. Bu özellik, kötü amaçlı bir programın yönetici ayrıcalıkları kazanmasını sağlayan güvenlik açıkları sorununu giderir.

Yönetim

Kaspersky Security Center bileşeni, esnek güvenlik yönetimi için geliştirilmiştir. Uç nokta güvenliğinin durumu ve merkezi güvenlik ilkesi hakkında ayrıntılı bilgiler sağlar. Kaspersky Security Center, bu özellikleri sayesinde tehditlerle ilgili raporların yanı sıra kurumsal ağ güvenliği yönetimi için de odak noktasıdır.

Ayrıca Kaspersky Systems Management teknolojisinin sunduğu genişletilmiş işlevsellikten de bahsedebiliriz. Aşağıdaki özellikler sayesinde kurumsal ağın güvenliğini artırır:

- güvenlik açığı değerlendirmesi ve düzeltme eki yönetimi;
- donanım ve yazılım envanterleri;
- esnek işletim sistemi ve uygulama sağlama;
- yazılım dağıtımı;
- SIEM entegrasyonu;
- karmaşık kurumsal ağlarda erişim kontrolü.

Kaspersky Lab
Enterprise Cybersecurity:**www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com.tr/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr