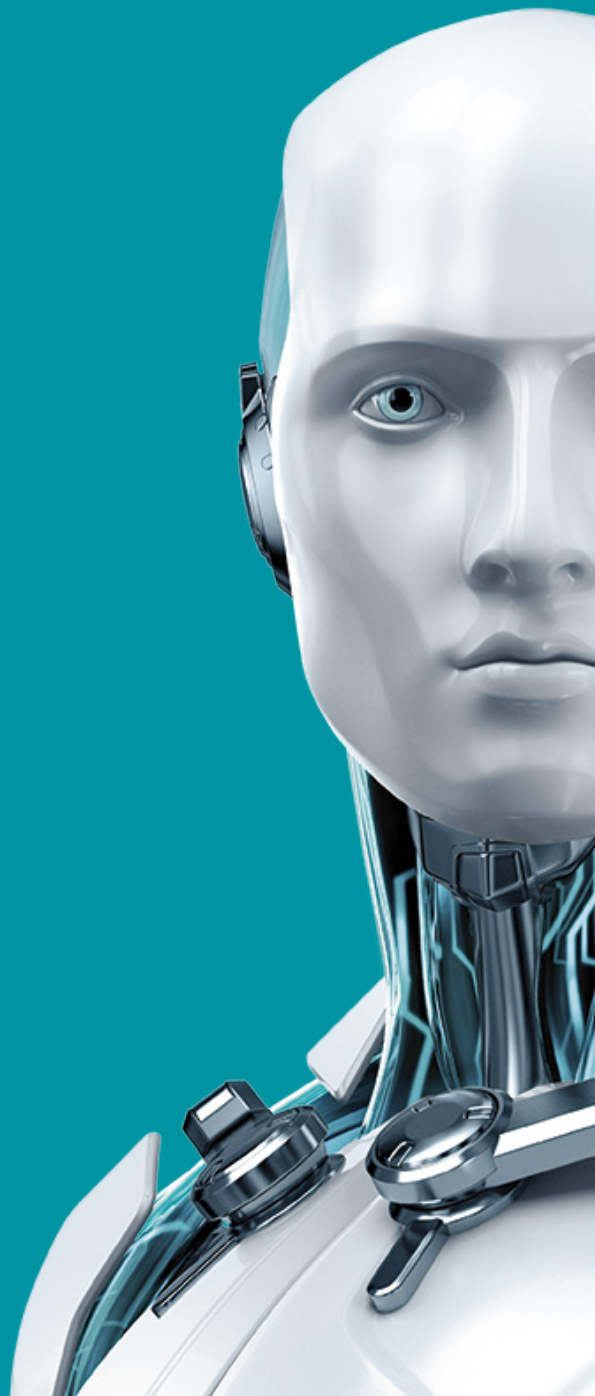
ENJOY SAFER TECHNOLOGY™

ESET TEKNOLOJİSİ

Çok katmanlı yaklaşım ve etkinliği



Belge sürümü:
1.1

Yazarlar:
Jakub Debski, Temel Teknoloji Geliştirme Başkanı
Juraj Malcho, Araştırmadan Sorumlu Başkan
Peter Stancik, Güvenlik Araştırma Görevlisi

ESET TEKNOLOJİSİ

Çok katmanlı yaklaşım ve etkinliği

İçindekiler

Hedefler

Bu belgede ESET'in temel antivirüs program kapasitelerinin çok daha ötesine gidebilmek için kullandığı çok katmanlı teknoloji yöntemlerini özetliyoruz. Bunu, belirli sorunların çözümünde hangi katmanların kullanıldığını ve kullanıcıya ne gibi faydalar sağladıklarını açıklayarak yapıyoruz.

Antivirüs programları miadını neden hem doldurmuştur hem de doldurmamıştır?

Piyasada varlığını kanıtlamış birçok antivirüs şirketi virüslerle veya kötü amaçlı yazılımlarla ilişkili sorunlar yaşayan insanlara yardım etme arzusuyla yola çıkmıştır ve bu şirketlerin kullandığı teknolojiler, güvenlik programı satan firmaların ele almaya başladıkları, gittikçe artan tehdit çeşitliliğine uygun hale gelmek üzere gelişmiştir. Günümüzde, antivirüs bir emtia ticareti olarak ve güvenlik ise, ne anlama geldiği bilinse de bilinmese de herkese hitap eden bir konu olarak algılanır. Son dönemlerde yeni, kendinden menkul "gelecek nesil" şirketlerin yaygınlaştığını görmekteyiz. Bu şirketlerin genel anlamda kötü amaçlı yazılım karşıtı çözüm geliştirmede çok az tecrübesi vardır, ancak piyasadaki şirketleri "dinozor" olarak addedip kendi çözümlerini agresif bir şekilde "yenilikçi" olarak pazarladıkları görülür. Sorunlara şipşak çözüm bulduğunu iddia eden bir çok satıcıda olduğu gibi, bu şirketlerin iddiaları yanıltıcıdır ve işin garip yanı piyasadaki düzinelerce çözüm sağlayıcıdan yalnızca birkaçı kendi temel tehdit algılama teknolojisini geliştirmesini olanaklı kılacak tecrübeye sahip olduğundan, virüs algılama kapasiteleri normal şartlar altında piyasadaki bir şirketten aldıkları üçüncü taraf bir algılama motoruna bağlıdır. Tüm ESET teknolojileri tescillidir ve kurum içinde geliştirilmiştir.

Antivirüs programları miadını doldurmamıştır. Bununla birlikte, piyasaya yeni giren şirketlere göre, uzun zamandır kötü amaçlı yazılım karşıtı ürün ortaya koyan sektörün etkinliğini riske atan, statik taramayla yapılan basit tehdit algılamasının, modern bir güvenlik ürününün modern tehditlere karşı hazırladığı teknoloji cephanesinin, çoktan kaybolup gitmiş olmasa da, yalnızca küçük bir bileşenini oluşturması durumudur.

Çoklu tehditler, çok katmanlı koruma

Bugün piyasada hâlâ iş yapan ve kötü amaçlı yazılım karşıtı ürün ortaya koyan köklü şirketler, mevcut tehditleri ele almak üzere gelişerek pazar paylarını korudular. Bu tehditler statik değildir ve gelişimleri 2000'li yılların başında durmamıştır. Günümüzün tehditleriyle, yalnızca 1990'ların teknolojisi üzerine bir şeyler koyarak etkin bir şekilde başa çıkılamaz. Modern kötü amaçlı yazılımlara karşı savaşmak, yetenekli ve (finansal olarak) motive olmuş kötü adamlardan oluşan ekiplere karşı göğüs gerdiğimiz bir kedi-fare oyunudur. Bu yüzden güvenlik şirketlerinin, modern kötü amaçlı yazılımları algılayabilecek ve/veya engelleyebilecek farklı katmanlar ekleyerek ürünlerini, hem reaktif hem de proaktif olarak etkin çözümler ortaya koyabilmek için sürekli olarak geliştirmeleri gerekmektedir. Basitçe, tek bir koruma noktası veya tek bir savunma yöntemi yeterli değildir. Bu, ESET'in de bir antivirüs programı satıcısından BT güvenliği şirketine dönüşme sebeplerinden birisidir.

Çoklu tehditler, çoklu platformlar

Günümüzde Microsoft işletim sistemleri kötü amaçlı yazılım programlarının çalıştığı tek platform değildir. Saldırganlar daha önceden keşfedilmemiş platformların ve işlemlerin kontrolünü ele geçirmeye çalışırken, mücadele alanı hızlı bir şekilde değişiyor.

- Kötü amaçlı işlemleri yürütmek için kontrol altına alınabilen her şey saldırı için de kullanılabiliyor.
- Harici verileri işlemek için yürütülebilir kodu çalıştıran her şey kötü amaçlı veriler tarafından potansiyel olarak ele geçirilebilir.

Linux sunucuları saldırganlar için büyük bir hedef haline gelmiş durumda (*Operation Windigo, Linux/Mumblehard*), OS X yüklü Mac'ler gelmiş geçmiş en büyük botnet'lerden birine ev sahipliği yaptı (*OSX/Flashback*), cep telefonları yaygın bir hedef (*Hesperbot*) ve yönlendiricilere yönelik saldırılar ciddi bir tehdit haline geliyor (*Linux/Moose*). Rootkit'ler donanımlara yaklaşıyor (aygıt yazılımlarına yönelik saldırılar veya *UEFI rootkit* kullanımı) ve görselleştirme yeni saldırı vektörleri açıyor (Sanal Makine yazılımı Bluepill güvenlik açıklarından kaçabiliyor). Ayrıca web tarayıcıları ve diğer uygulamalar işletim sistemleri kadar karmaşık hale geldiler ve komut dosyası kullanan mekanizmaları sıklıkla kötü amaçlar için kullanılıyor (*Win32/Theola*).

Farklı Dağıtım Vektörleri

Tarihsel olarak, ilk kötü amaçlı yazılımlar kendini kopyalayan işlemler olarak önce sistemlerin içinde, sonra da PC'den PC'ye yayılan, dosyalara ve/veya diske bulaşan virüsler olarak ortaya çıktılar. İnternet kullanımının neredeyse evrenselleşmesiyle beraber, kötü amaçlı yazılımları dağıtma yöntemleri aşırı derecede çoğaldı. Kötü amaçlı nesneler ayrıca e-posta aracılığıyla eklenti veya bağlantı olarak gönderilebiliyor, web sayfalarından indirilebiliyor, bir belge içerisine komut dosyaları tarafından bırakılabiliyor, çıkarılabilir cihazlar üzerinden paylaşılabiliyor, kötü yetkilendirme ve zayıf parolalardan faydalanarak uzaktan dağıtılabiliyor, suistimal yoluyla yürütülebiliyor veya sosyal mühendislik teknikleri tarafından kandırılan son kullanıcılar aracılığıyla yüklenebiliyor.

Kötü Amaçlı Yazılım Tasarımı

Kötü amaçlı yazılımların esas olarak ergenlik çağındaki çocuklar tarafından bir şaka veya gösteriş unsuru olarak yazıldıkları dönem geçip gideli çok oldu. Günümüzde, kötü amaçlı yazılımlar gelir veya bilgi hırsızlığı amacıyla yazılıyor ve geliştirilmeleri için hem suçlular hem de devletler tarafından ciddi miktarda parasal yatırım yapılıyor.

Algılanmalarını güçleştirmek umuduyla kötü amaçlı yazılımlar, farklı derleyicileri ve yorumlanmış dilleri kullanarak, farklı programlama dillerinde yazılıyor. Kod, algılama ve analizi zorlaştırmak için özelleştirilebilir yazılım kullanarak gizleniyor ve korunuyor. Kod, şüpheli etkinlikleri fark etmek için tasarlanmış olan davranışsal izlemeyi atlatma ve silinmeyi engelleme, böylece sistemin içindeki devamlılığını garantiye alma teşebbüsüyle güvenli işlemlerin içine yerleştiriliyor. Komut dosyaları uygulama denetim tekniklerini atlatmak için kullanılıyor ve "yalnızca bellek içi" kötü amaçlı yazılımlar, dosya tabanlı güvenliği atlatabiliyor.

Korumayı gizlice geçebilmek için, kötü adamlar İnternet'i kötü amaçlı yazılımlarının binlerce türüyle dolduruyor. Diğer bir yöntem ise güvenlik şirketlerinin dikkatini çekmekten kaçınmak için kötü amaçlı yazılımı az sayıda hedefe dağıtmak. Algılanmayı önlemek için güvenli yazılım bileşenleri kötüye kullanılıyor veya yetkisiz kodun fark edilmesi daha zor olsun diye kötü amaçlı kod, yasal şirketlerden çalınan sertifikalarla imzalanıyor.

Ayrıca ağ düzeyinde, güvenliği riske atılmış sistemlere talimat gönderebilmek ve bunlardan veri alabilmek için, kötü amaçlı yazılımlar ağ düzeyinde sabit kodlu komuta ve kontrol (C&C) sunucularını daha az kullanıyor. Eşler arası ağ kullanan botnet'lerin merkezi olmayan denetimi yaygın bir şekilde kullanılıyor ve şifrelenmiş iletişim, saldırganların kimliğinin teşhis edilmesini güçleştiriyor. Etki alanı üretme algoritmaları, bilinen URL'lerin engellenmesine dayanarak algılamanın etkinliğini azaltıyor. Saldırganlar iyi itibara sahip, güvenilir web sitelerinin kontrolünü ele geçiriyor ve yasal reklam servisleri bile kötü amaçlı içeriğe hizmet etmek için kullanılıyor.

ÖNEMLİ NOT

Saldırganlar algılamayı pek çok şekilde atlatabilirler; bu yüzden de basit ve tek katmanlı bir çözüm, koruma sağlamak için yeterli değildir. Biz, ESET'te en yüksek seviye güvenliği garantilemek için sürekli, gerçek zamanlı ve çok katmanlı bir korumanın gerekli olduğuna inanıyoruz.

ESET'in temel teknolojisinin avantajları

ESET'in tarama motoru ürünlerimizin merkezinde yer alır ve bunun temelini oluşturan teknoloji "eski usul antivirüs" programlarından devralınmış olmasına karşın, büyük oranda genişletilmiş ve artırılmıştır, ayrıca **modern tehditlere karşı durabilmesi için de sürekli geliştirilmektedir**.

Tarama motorunun amacı muhtemel kötü amaçlı yazılımları tanımlamak ve incelenen kodun kötü amaçlılık olasılığına yönelik otomatikleşmiş kararlar almaktır.

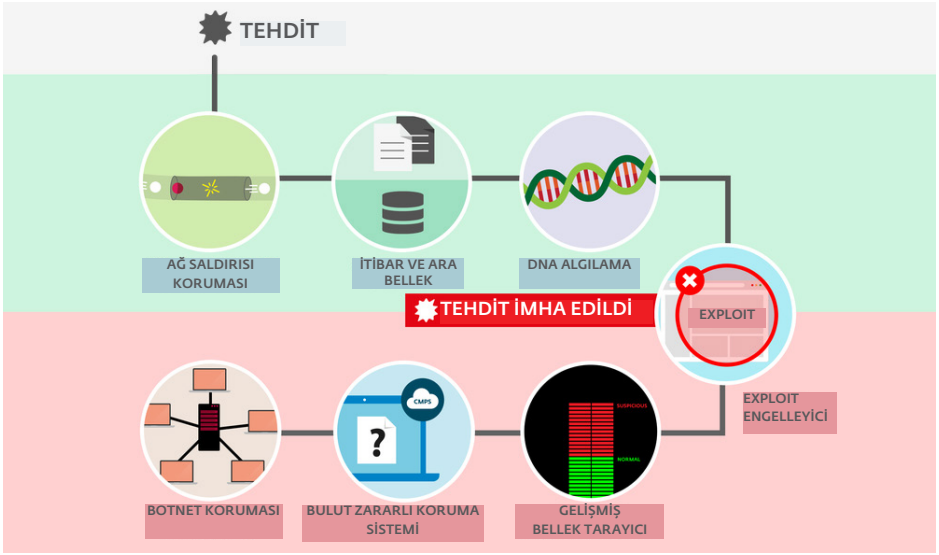
ESET'in performansı yıllardır, ürünle tümleşik sandboxing teknolojisini kullanan derin kod analizinin yol açtığı performans tıkanıklıklarını gidermek için akıllı algoritmalara ve manuel olarak hazırlanmış derleme koduna dayanıyordu. Ancak, bu yaklaşımı geliştirdik. Şimdi, en üst düzey performans için **yorumlu öykünme ile beraber ikili çeviri** kullanıyoruz.

Ürünün sandboxing teknolojisini kullandığınızda, sanallaştırılmış ortamda bir programı yürütmek için bilgisayar donanım ve yazılımının farklı bileşenlerine öykünmeniz gerekir. Bu bileşenler belleği, dosya sistemini, işletim sistemi API'lerini ve CPU'yu (merkezi işlem birimi) kapsarlar.

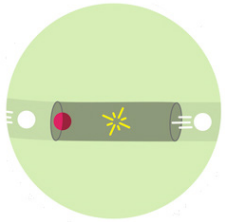
Geçmişte CPU öykünmesi, ısmarlama derleme kullanılarak gerçekleştiriliyordu. Ancak, bu "yorumlanmış bir kod" idi ve bunun anlamı, her bir yönerge öykünmesinin ayrı ayrı gerçekleştirilmesi gerektiğiydi. İkili çeviriyle öykünülen yönergeleri gerçek bir CPU'da yerel bir biçimde yürütürsünüz. Bu, özellikle kod içinde döngülerin olması durumunda çok daha hızlı olur: çoklu döngü, tüm çalıştırılabilir dosyalar için güvenlik ürünleri ve araştırmacılar tarafından analiz edilmelerini engelleyen önlemlerin alındığı durumda koruyucu bir tekniktir.

ESET ürünleri, katıştırılmış kötü amaçlı bileşenleri doğru bir şekilde algılamak amacıyla yüzlerce farklı dosya biçimini (çalıştırılabilir dosyalar, yükleyiciler, komut dosyaları, arşivler, belgeler ve bytecode'lar) analiz eder.

Aşağıdaki şekil, çeşitli temel ESET teknolojilerini ve bu teknolojilerin bir tehdidi, sistem içindeki yaşam döngüsü zarfında ne zaman ve nasıl algılayabileceği ve/veya engelleyebileceğine yönelik bir yaklaşımı gösterir:



Şekil 1: ESET koruma katmanları



Ağ Saldırısı Koruması

Ağ Saldırısı Koruması, **güvenlik duvarı teknolojisinin bir uzantısıdır ve ağ düzeyindeki bilinen güvenlik açıklarının algılanma oranını artırır**. *SMB*, *RPC* ve *RDP* gibi geniş çapta kullanılan protokollerdeki yaygın güvenlik açıklarına yönelik algılamayı uygulamaya koyarak, kötü amaçlı yazılımların yayılmasına, ağ üzerinden yürütülen saldırılara ve henüz piyasaya sürülmüş veya dağıtılmış bir yaması bulunmayan suistimallere karşı **bir önemli koruma katmanı daha oluşturur**.

İtibar ve Ara Bellek

Bir dosya ya da URL gibi bir nesneyi incelerken, herhangi bir tarama işleminin gerçekleşmesinden önce ürünlerimiz yerel ara belleği (ve ESET Endpoint Security varsa **ESET Paylaşımlı Yerel Ara Belleğini**), bilinen kötü amaçlı nesneler veya güvenilenler listesindeki zararsız nesneler için kontrol ederler. Bu, **tarama performansını artırır**. Sonrasında, **ESETLiveGrid® İtibar Sistemimiz nesne itibarını (geçmişini) sorgular** (yani nesnenin daha önce başka bir yerde görülüp görülmediğini ve kötü amaçlı veya başka türlü sınıflandırılıp sınıflandırılmadığını sorgular). Bu, **tarama etkinliğini artırır ve kötü amaçlı yazılım istihbaratının müşterilerimizle daha hızlı şekilde paylaşılmasını olanaklı kılar**. URL kara listelerinin uygulanması ve itibarının kontrol edilmesi, kullanıcıların kötü amaçlı içeriğe sahip ve/veya kimlik hırsızlığı yapan sitelere erişimini engeller.

DNA Algılama

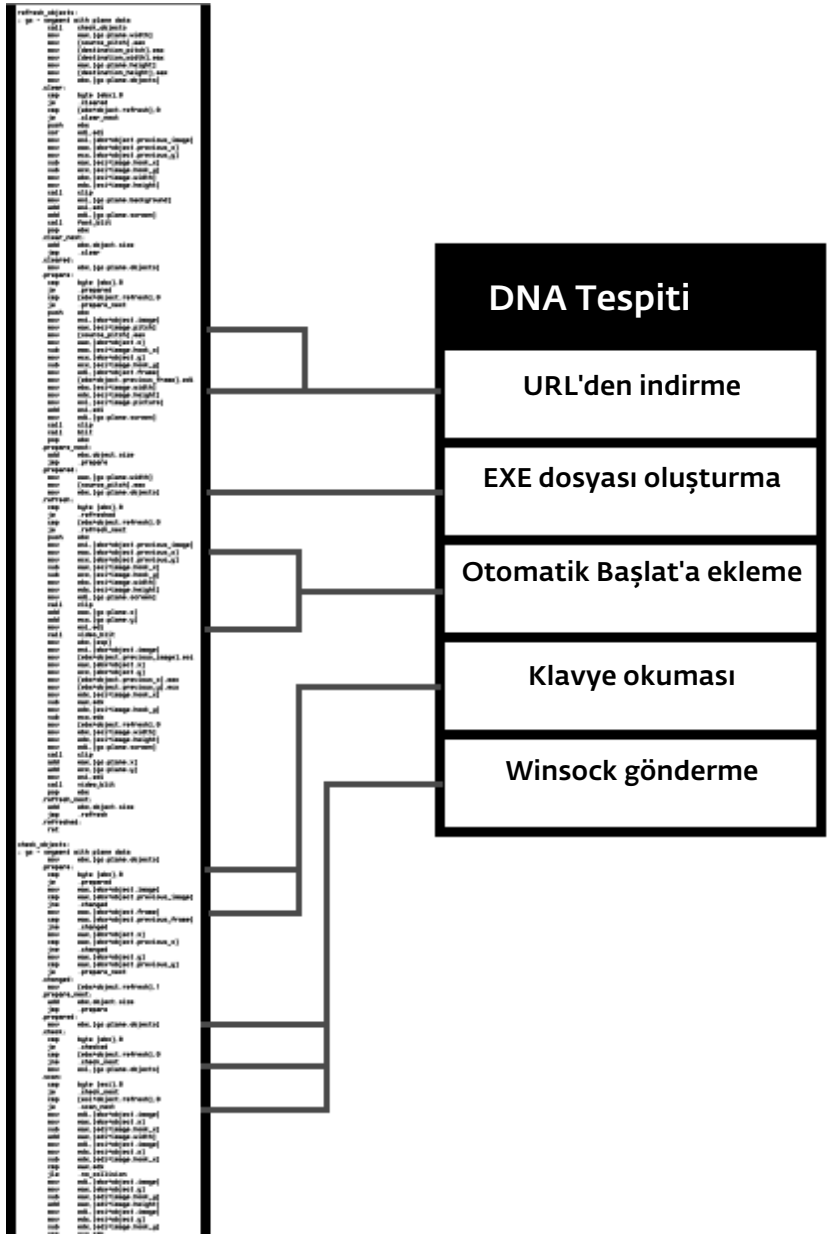
Algılama türleri, (örneğin, istatistiksel amaçlarla veya basitçe, daha önce bulgusal olarak tespit ettiğimiz bir kötü amaçlı yazılıma daha kesin bir algılama adı vermek amacıyla belirli kötü amaçlı ikilikleri veya belirli kötü amaçlı yazılım sürümlerini hedeflemede kullanışlı olan) çok özel karmalardan **kötü amaçlı davranışların**

ve kötü amaçlı yazılım özelliklerinin karmaşık tanımları olan ESET DNA Algılamaya kadar uzanır.

Eski usul antivirüs ürünlerinde kullanılan model eşleşmesi, kodda yapılan basit bir değişiklikle veya gizleme teknikleriyle kolayca atlatılabilir. Ancak, nesnelerin davranışları bu kadar kolay değiştirilemez. ESET DNA Algılamaları tam da bu ilkeden yararlanmak amacıyla tasarlandı. Kodu derinlemesine analiz edip davranışı için sorumlu olan "genleri" çekip çıkartıyoruz. Bazı sözde "gelecek nesil" çözümlerin imza algılamasından "daha iyi bir alternatif" olduğunu iddia edecekleri şekilde, bu tarz **davranışsal genler risk göstergelerinden (IOC'ler) çok daha fazla bilgi içerirler**. ESET davranışsal genleri, ister disk üzerinde ister çalışan işlem belleğinde bulunsunlar, potansiyel olarak şüpheli kodu değerlendirmek için kullanılan DNA Algılamayı oluşturmak için kullanılırlar.

Ek olarak, tarama motorumuz anomali algılaması için kullanılan birçok ayrıştırıcı geni çekip çıkarır: Güvenli görünmeyen her şey potansiyel olarak kötü amaçlıdır.

Ayarlanabilir eşik düzeyine ve eşleşme koşullarına bağlı olarak, DNA Algılamaları belirli ve bilinen kötü amaçlı yazılım örneklerini, bilinen bir kötü amaçlı yazılım ailesinin yeni varyantlarını veya daha önce görülmemiş ya da bilinmeyen, kötü amaçlı davranış gösteren genler içeren kötü amaçlı yazılımları tanımlayabilirler. Diğer bir deyişle, **iyi hazırlanmış tek bir DNA davranışsal tanımlaması, kendisiyle bağlantılı on binlerce kötü amaçlı yazılım varyantını algılayabilir** ve antivirüs yazılımımızın yalnızca halihazırda bildiğimiz veya gördüğümüz kötü amaçlı yazılımları ortaya çıkarmasını sağlamakla kalmaz, **aynı zamanda yeni, daha önceden bilinmeyen varyantları da ortaya çıkarır**. Dahası, otomatikleştirilmiş kümelenme ve kötü amaçlı örnek kümelerimize makine öğrenimi algoritmalarının uygulanması, yeni kötü amaçlı genleri ve davranışsal modelleri tarama motorumuz aracılığıyla tanımlamamızı sağlar. Bu tarz genler, hatalı pozitif üretmemelerini garantiye almak için kolaylıkla devasa bir güvenilenler listesi kümesiyle eşleştirilebilirler.

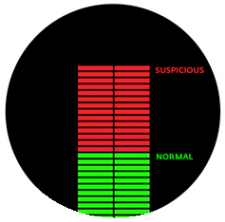


Exploit Engelleyici

ESET teknolojileri farklı düzeylerdeki çeşitli zafiyet türlerine karşı koruma sağlarlar: Tarama motorumuz, kusurlu dosyalarda beliren suistimalleri kapsar; Ağ Saldırısı Koruması, iletişim düzeyini hedef alır ve son olarak Exploit Engelleyici, suistimal işleminin kendisini engeller.

Exploit Engelleyici tipik olarak suistimal edilebilir uygulamaları (tarayıcılar, belge okuyuclar, eposta istemcisi, Flash, Java, ve daha fazlası) **izler ve** yalnızca belirli *CVE belirleyicileri*hedef almak yerine, **suistimal tekniklerine odaklanır**. Her suistimal, işlemin uygulanmasındaki bir anomalidir ve biz, suistimal tekniklerinin varlığını akla getiren anomalileri ararız. Teknoloji sürekli geliştirildiğinden, yeni suistimal tekniklerini kapsamak üzere yeni algılama yöntemleri düzenli olarak eklenir. Tetiklendiğinde, işlemin davranışı analiz edilir ve şüpheli olduğu düşünülüyorsa, diğer saldırı bağlantılı meta verilerin ESET LiveGrid bulut sistemimize gönderilmesiyle beraber, **makinedeki tehdit anında engellenebilir**. Bu bilgi daha fazla işleme tabi tutulur ve diğer bilgilerle ilişkilendirilir; bu da **bizim, daha önceden bilinmeyen tehditleri ve sözde sıfır-gün saldırılarını tespit etmemizi sağlar** ve laboratuvarımız için kıymetli tehdit istihbaratı temin eder.

Exploit Engelleyici, kötü amaçlı kodun kendisini analiz etmeye odaklanan algılama tekniklerinden tamamen farklı bir teknoloji kullanmak yoluyla, saldırganlara bir adım daha yaklaşarak başka bir koruma katmanı daha ekler.



Gelişmiş Bellek Tarayıcı

Gelişmiş Bellek Tarayıcı günümüzün kötü amaçlı yazılımlarının önemli bir sorununa, **gizleme ve/veya şifrelemenin** yoğun bir şekilde kullanılmasına etkin bir şekilde **değinen özgün bir ESET teknolojisidir**.

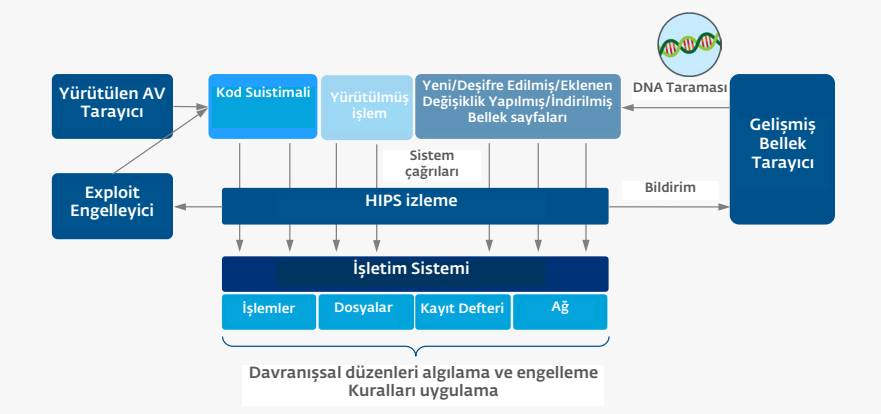
Genellikle çalışma veri paketleyicilerinde ve kod koruyucularında kullanılan bu kötü amaçlı yazılım koruma taktikleri, öykünme ve korumalı alan gibi paket açma tekniklerini uygulayan algılama yaklaşımları için sorunlara neden olmaktadırlar. Üstelik kontrol, ister bir öykünücü ister sanal/fiziksel bir korumalı alan kullanılarak yapılsın, analiz esnasında kötü amaçlı yazılımın, bu şekilde sınıflandırılmasına sebep olacak şekilde kötü amaçlı bir davranış sergileyeceğinin bir garantisi yoktur. Kötü amaçlı yazılım, tüm yürütme yollarının analiz edilemeyeceği şekilde gizlenebilir; kod için koşullu veya zamanlı tetikleyiciler içerebilir ve oldukça sık olarak, ömrü boyunca yeni bileşenler indirebilir. Bu sorunlarla mücadele edebilmek için Gelişmiş Bellek Tarayıcı, kötü amaçlı bir işlemin davranışını izler ve kendini bellekte açığa vurur vurmaz onu tarar. Bu, yürütme öncesindeki veya yürütme esnasındaki proaktif kod analizinin daha geleneksel olan işlevselliğini tamamlar.

Ayrıca güvenli işlemler, suistimal veya kod enjeksiyonu yüzünden bir anda kötü amaçlı işlemler haline dönüşebilirler. Bu sebeplerden ötürü yalnızca bir kez analiz gerçekleştirmek yeterli değildir. Daimi izleme gerekmektedir ve bu, Gelişmiş Bellek Tarayıcının görevidir. **Ne zaman bir işlem, yürütülebilir bir sayfadan sistem araması gerçekleştirse, Gelişmiş Bellek Tarayıcı ESET DNA Algılamalarını kullanarak bir davranışsal kod analizi gerçekleştirir.**

Kod analizi yalnızca standart yürütülebilir bellek için değil, aynı zamanda kötü amaçlı yazılımları yazanlar tarafından dinamik analizi engellemek amacıyla kullanılan .NET MSIL (Microsoft Intermediate Language) kodu için de gerçekleştirilir. Akıllı ara belleğe alma işleminin uygulanmasından ötürü, Gelişmiş Bellek Tarayıcının neredeyse hiçbir ek yükü olmaz ve işlem hızlarında fark edilebilir hiçbir bozulmaya sebep olmaz.

Gelişmiş Bellek Tarayıcı, Exploit Engelleyici ile birlikte iyi çalışır. Gelişmiş Bellek Tarayıcı, Exploit Engelleyici'den farklı olarak yürütme sonrası bir yöntemdir ve bu da bazı kötü amaçlı faaliyetlerin çoktan ortaya çıkmış olması riskinin bulunduğu anlamına gelir. Yine de bir saldırgan, korumanın diğer katmanlarını pas geçebilmeyi başarırsa **son çare olarak koruma zincirine geçer**.

Dahası, gelişmiş kötü amaçlı yazılımlarda yeni bir akım vardır: Günümüzde bazı kötü amaçlı kodlar dosya sisteminde yer alan, geleneksel yöntemlerle algılanabilecek inatçı bileşenlere ihtiyaç duymadan "yalnızca bellek içi" çalışırlar. Başlarda, bu tarz kötü amaçlı programlar, uzun çalışma zamanlarından ötürü (sunucu sistemleri tek seferde aylar veya yıllarca açık kaldıkları için, kötü amaçlı işlemler bellekte, bir yeniden başlatma işlemini atlatmak zorunda kalmadan süresiz olarak kalabilirlerdi) yalnızca sunucularda görülmüştü, ancak son zamanlarda işletmelerin uğradığı saldırılar bu akımda bir değişiklik olduğunu göstermektedir ve bu açıdan uç noktaların da hedef alındığını görürüz. **Yalnızca bellek tarama bu tarz kötü amaçlı saldırıları başarılı bir şekilde keşfedebilir ve ESET bu yeni akım için Gelişmiş Bellek Tarayıcı ile hazır durumdadır.**

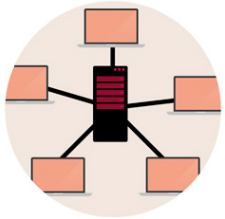


Şekil 2: ESET'in davranışsal algılamasının çalışma şekli

Bulut Zararlı Koruma Sistemi

ESET Bulut Zararlı Koruma Sistemi, ESET'in bulut tabanlı sistemi olan ESET LiveGrid'e dayanan birkaç teknolojiden birisidir. Bilinmeyen, potansiyel olarak kötü amaçlı olabilecek uygulamalar ve diğer muhtemel tehditler ESET LiveGrid Geri Bildirim Sistemi aracılığıyla izlenirler ve ESET bulutuna gönderilirler. **Toplanan örnekler otomatik korumalı alana ve davranışsal analize tabi kılınırlar** -ki bu da, kötü amaçlı karakteristiklerin onaylanması durumunda otomatikleştirilmiş algılamaların oluşturulmasıyla sonuçlanır-. ESET müşterileri, bir sonraki algılama motoru güncelleştirmesini beklemeleri gerekmeden ESET LiveGrid İtibar Sistemi aracılığıyla bu otomatikleştirilmiş algılamalar hakkında bilgi sahibi olurlar. Mekanizmanın devir zamanı genellikle 20 dakikanın altındadır ve bu da, kullanıcıların bilgisayarlarına düzenli algılamaların iletilmesinden bile önce ortaya çıkan tehditlerin etkin bir şekilde algılanmasını sağlar.

Botnet Koruması



Kötü amaçlı yazılımları yazanlar için değiştirilmesi masraflı olan bir unsur varsa, o da C&C sunucularıyla iletişimdir. **ESET'in Botnet Korumasının, botnet'ler tarafından kullanılan kötü amaçlı iletişimleri başarılı bir şekilde algıladığı ve aynı zamanda can sıkıcı işlemleri tanımladığı kanıtlanmıştır.**

ESET'in Ağ Algılamaları, Botnet Koruma teknolojisini ağ trafik analiziyle ilişkili genel sorunları gidermek için genişletmiştir. Algılamalar **kötü amaçlı trafiğin daha hızlı ve daha esnek bir şekilde algılanmasına imkan verirler.** Snort veya Bro gibi sektör standardı imzalar birçok saldırının algılanmasına olanak tanır ancak ESET Ağ Algılamaları özellikle ağ zafiyetlerini, suistimal takımlarını ve gelişmiş kötü amaçlı yazılım iletişimlerini hedef almak üzere özel olarak tasarlanmışlardır.

Uç noktalarda ağ trafik analizini gerçekleştirebilme becerisinin fazladan avantajları vardır. Tam olarak hangi işlem veya modülün kötü amaçlı iletişimden sorumlu olduğunu tanımlamamıza, tanımlanmış nesneye karşı harekete geçmemize ve bazen iletişimin şifrelenmesini bile pas geçmemize imkan verirler.

Günümüzde reaktife karşı proaktif koruma

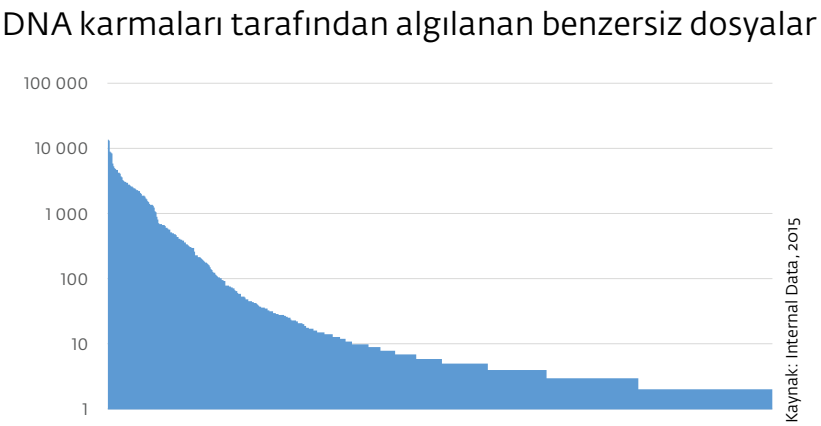
DNA Algılama, bütün bir kötü amaçlı yazılım ailesini algılamada mükemmel olsa da, kullanıcıları koruyabilmeleri için onlara dağıtılmaları gerekmektedir. Aynı durum, tarama motoru, buluşsal yöntemler veya yeni tehditleri hedef alan tüm değişimler için de geçerlidir. Bu günlerde, en yüksek düzeyde korumayı garanti altına almak için ESET'in bulut tabanlı LiveGrid sistemi ile iletişim kurmak birçok sebepten ötürü gereklidir:

- **Çevrimdışı tarama çoğunlukla reaktiftir.** Bu günlerde proaktif olmak, artık sadece ürününüzdeki en iyi buluşsal yöntemlere sahip olmak anlamına gelmez. Koruma araçlarınız bir saldırgan için elde edilebilir oldukları müddetçe; imza, buluşsal yöntemler veya makine öğrenimi sınıflandırıcıları kullanıyor olmanız fark etmez: Kötü amaçlı yazılım yazan biri sizin algılama teknolojinizi kullanarak deney yapabilir, kötü amaçlı yazılımı algılanamayacak hale gelene kadar değiştirebilir ve hemen ardından yayınlayabilir. ESET LiveGrid bu kötü amaçlı yazılım stratejisine karşılık verir.
- **Güncellemeler gerçek zamanlı değildir.** Güncellemeler daha sık piyasaya sürülebilirler ve hatta kullanıcılara birkaç dakikada bir iletilebilirler. Ama bunu daha iyi bir şekilde yapmak mümkün müdür? Evet: ESET LiveGrid, ihtiyaç duyulduğunda bilgi sağlama yoluyla anlık korumayı olanaklı kılar.
- **Kötü amaçlı yazılım radara yakalanmadan uçmaya çalışır.** Kötü amaçlı yazılımları yazanlar, özellikle siber casusluk durumunda olabildiğince uzun süre algılanmaktan kaçınmaya çalışırlar. Hedefli saldırılar (e-posta solucanları gibi kitle dağıtımlarının tersine) az sayıdaki hedefe, bazen yalnızca tek bir hedefe, tek parçalık kötü amaçlı yazılımları konuşlandırırlar. Biz bu olguyu kötü amaçlı yazılımları yazanlara karşı kullanırız: Yaygın olmayan ve iyi bir itibara sahip olmayan nesnelerin potansiyel olarak kötü amaçlı oldukları varsayılır ve bundan sonra ya uç noktada detaylıca analiz edilirler ya da LiveGrid Geri Bildirim sistemimiz aracılığıyla detaylı bir otomatikleştirilmiş analiz için gönderilirler. ESET LiveGrid İtibar Sistemi dosyalar, bunların kaynakları, benzerlikleri, sertifikaları, URL'leri ve IP'leri hakkında bilgiler içerir.

ESET LiveGrid kullanan koruma

Bir bulut sistemi kullanarak koruma sağlamanın en basit yolu karma işlevi kullanarak tam anlamıyla kara listeye almadır. Bu, hem dosyalar hem de URL'ler için işe yarar, ancak yalnızca karmayla tam olarak eşleşen nesneleri engelleyebilir. Bu sınırlama belirsiz karma işlevinin icadına yol açmıştır. Belirsiz karma işlevi, benzer nesnelerin aynı veya benzer karması olduğundan, nesnelerin ikili benzerliklerini hesaba katar.

ESET belirsiz karma işlevini bir sonraki düzeye taşımıştır. Biz veri karması oluşturmayız, DNA Algılamada tanımlanan davranışın karmalarını oluştururuz. DNA karma işlevini kullanarak, kötü amaçlı yazılımın binlerce farklı varyantını anında engelleyebiliriz.



Şekil 3: Bireysel DNA karmaları (x ekseni) tarafından algılanan benzersiz dosyaların sayısı (y ekseni).

Kullanıcılara anlık kara listeleme sağlama, ESET Bulut Zararlı Koruma Sisteminin tek amacı değildir. Bir kullanıcı örnek gönderim sürecine katkıda bulunmak istiyorsa, her ne zaman şüpheli bir itibara sahip yeni bir örnek tanımlansa, bu örnek daha ince bir analiz için ESET'e gönderilir. Bulut Zararlı Koruma Siteminin sahip olduğu potansiyelden tam olarak faydalanabilmek için, kullanıcılar aynı zamanda, incelikli bir analiz yapabilmemiz amacıyla şüpheli itibara sahip tüm şüpheli örnekleri toplamamızı sağlayan ESET LiveGrid Geri Bildirim Sistemini etkinleştirmelidirler.

Örneklerin Otomatik ve Manuel Olarak İşlenmesi

ESET her gün, ön işleme ve kümelemeden sonra otomatik, yarı otomatik ve manuel olarak işlemden geçirdiği yüz binlerce örneği alır. **Otomatikleştirilmiş analiz, bir sanal ve gerçek makine dizisi üzerinde yer alan ve bizim tarafımızdan geliştirilmiş olan araçlar tarafından gerçekleştirilir.** Sınıflandırma, statik ve dinamik kod analizine, işletim sisteminde yapılan değişikliklere, ağ iletişim düzenlerine, başka kötü amaçlı yazılım örneklerine olan benzerliğe, DNA özelliklerine, yapısal bilgiye ve anomali algılamasına göre uygulama sırasında çıkarılmış olan farklı öznitelikler kullanılarak gerçekleştirilir.

Tüm otomatikleştirilmiş sınıflandırıcıların dezavantajları vardır:

- **Sınıflandırma için ayrıştırıcı özelliklerini seçmek önemsiz bir iş değildir** ve kötü amaçlı yazılım alanında uzman olan insanların bilgisini kullanarak gerçekleştirilmelidir.
- **Makine öğrenimi sınıflandırıcıları, öğrenme için kullanılan girdileri doğrulamak üzere insan uzmanların katılımını gerektirirler**. Sistem tarafından sınıflandırılan örneklerin sistem için girdi olarak kullanılacağı, tamamıyla otomatikleştirilmiş işlemlerde, pozitif geri bildirim döngüsünden kaynaklanan bir çığ etkisi olsa, sistem hızla istikrarsızlaşırdı: "Çöp girer, çöp çıkar".
- Makine öğrenimi algoritmaları verileri anlamazlar ve **bilgi istatistiksel olarak doğru dahi olsa, bu onun geçerli olduğu anlamına gelmez**. Örneğin, makine öğrenimi güvenilir yazılımların yeni versiyonlarını kusurlu versiyonlarından ayırt edemez, güvenilir bir uygulamaya bağlı güncelleyiciyi kötü amaçlı yazılım tarafından kullanılan bir indiriciden ayırt edemez ve güvenilir yazılım bileşenleri kötü amaçlar için kullanıldıklarında bunu fark edemez.
- Makine öğrenimiyle, öğrenim sürecine yeni örnekler eklemek hatalı pozitiflere sebep olabilir ve hatalı pozitifleri silmek gerçek pozitif algılamasının etkinliğini azaltabilir.
- Otomatikleştirilmiş işlem, ESET LiveGrid aracılığıyla yeni tehditlere anında tepki vermeyi sağlarken, en yüksek kaliteyi ve algılama oranını ve en düşük miktarda hatalı pozitifi garantilemek için örneklerin algılama mühendisleri tarafından ek işleme tabi tutulması çok önemlidir.

İtibar hizmetleri

ESET LiveGrid nesneler için itibar sağlar. Dosyaları, sertifikaları, URL'leri ve IP'leri içeren çeşitli varlıkların itibarını değerlendiririz. Yukarıda açıkladığımız gibi, itibar yeni kötü amaçlı nesneleri veya bulaşma kaynaklarını tanımlamak için kullanılabilir. Yine de başka kullanım alanları da vardır.

Güvenilenler listesini tarama

Güvenilenler listesini tarama, tarama motorunun bir nesneyi incelemek için ihtiyaç duyduğu tarama sayısını azaltan bir özelliktir. Eğer bir nesnede değişiklik yapılmadığından ve nesnenin güvenilir olduğundan eminsek bir tarama gerçekleştirmenin hiç gereği yoktur. Bunun performans üzerinde çok olumlu bir etkisi olur ve ESET ürünlerinin dikkat çekmemesine yardımcı olur. Her zaman söylediğimiz gibi, "en hızlı kod, hiç yürütülmeyen koddur". Güvenilenler listelerimiz, yazılım dünyasının her daim değişen gerçekliğine sürekli olarak uyum sağlar.

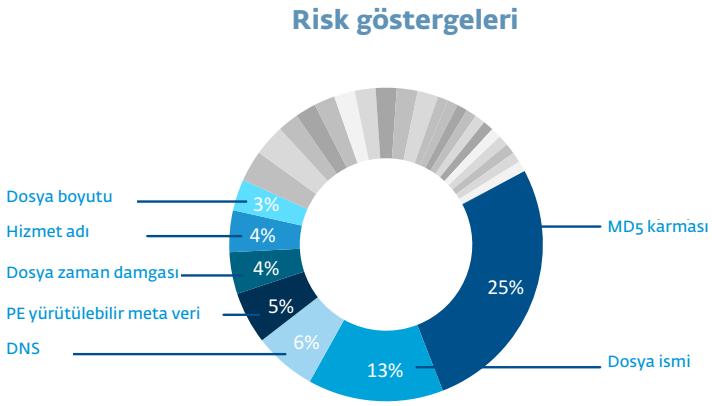
İstihbarat toplama

Eğer bir kullanıcı, ESET LiveGrid'e istatistiksel bilgi gönderimine katkıda bulunmaya karar verirse, biz bu bilgiyi tehditlerin küresel takibi ve izlenmesi için kullanırız. Bu bilgiler bize üzerinde çalışacağımız pek çok araştırma verisi verir ve **en acil ve problemli durumlara odaklanmamızı, kötü amaçlı yazılımlardaki eğilimleri görmemizi ve koruma teknolojilerini planlayıp önem sırasına göre sıralamamızı sağlar**.

FP'ler ve IOC'ler hakkında

Risk göstergelerinin (IOC'ler) çağdaş kurumsal güvenlikte çok önemli bir yeri olduğu düşünülür, ancak bazen "gelecek nesil" güvenlik sağlayıcıları tarafından üzerinde durulsa da, özel veya gelişmiş olmaktan çok uzaktır. Burada en yaygın IOC'lerin bir dökümü ve neye dayandıkları resmedilmiştir.* Görebileceğimiz üzere, ele aldıkları özellikler son derece temel düzeydedir: Vakaların dörtte biri bilindik MD5'le ilgilidir, ardından dosya isimleri vb. gelir. Bu sonuçlar, adli tıp için kullanışlı olabilse de, bu yöntemin koruma ve engelleme için uygun olmadığını netleştirir. "Eski Antivirüs yazılımlarında" kullanılan "modası geçmiş" imza tabanlı algılamaları reddeden bazı "gelecek nesil" satıcıların, kötü amaçlı dosyaları veya olayları algılamak için aslında en zayıf imza tabanlı yöntem olsa da, IOC'leri övmeleri ironiktir.

*Veri kaynağı: IOC Bucket, Nisan 2015. IOC Bucket güvenlik topluluğuna bir tehdit istihbaratı paylaşma yolu sağlamak için oluşturulmuş ve topluluk odaklı ücretsiz bir platformdur.



Şekil 4: IOC Bucket'tan alınan (Nisan 2015 örneği) risk göstergelerinin analizi.

Sonuç

Güvenlik konusunda sihirli bir çözüm yoktur. Günümüzün dinamik olan ve sıklıkla hedef alınan kötü amaçlı yazılımları, deneyimli araştırmacılar tarafından yıllardır toplanan petabaytlarca istihbaratı göz önüne alan proaktif ve akıllı teknoloji temelli çok katmanlı bir yaklaşımı gerektirmektedir. 20 yıl önce ESET, Antivirüs'ün (geleneksel yaklaşımın) yarım kalmış bir çözüm olduğunu fark etti ve bu noktada tarama motorumuzla proaktif teknolojileri birleştirmeye başladık ve yavaş yavaş, siber imha silsilesinin farklı kademelerinde etkimizi göstermek için farklı katmanları uygulamaya koyduk.

ESET, 25 yıldan fazla süredir var olan araştırma birikimine dayanan, yüksek seviye koruma sağlayabilecek birkaç güvenlik satıcısından biridir. Bu, bizim kötü amaçlı yazılımların bir adım önünde olmamızı ve standart, statik imzaların kullanımının ötesine geçebilmek için sürekli teknolojiler geliştirmemizi sağlıyor. Uç nokta temelli ve bulutla zenginleştirilmiş teknolojilerimizin benzersiz birleşimi piyasadaki kötü amaçlı yazılımlara karşı en gelişmiş güvenliği sunuyor.