Kaspersky for Business

KASPERSKY lab

Gerçekler ve Sanrılar: Modern Tehdit Ortamı Kılavuzu

www.kaspersky.com.tr

#truecybersecurity

Gerçekler ve Sanrılar: Modern Tehdit Ortamı Kılavuzu

Yeni nesil tehditler: Gerçekten böyle bir şey var mı?

Bilgisayar korsanları ve siber güvenlik satıcıları arasındaki bitmek bilmeyen savaş, "en güçlü olan hayatta kalır" ilkesine iyi bir örnektir. Saldırganları durdurma konusunda son derece kararlı olan lider savunma çözümü geliştiricileri, yakın zamana kadar bu alanda büyük bir başarı göstermekteydi. Ancak bu baskı, bilgisayar korsanlarını işlerine devam etmek için yeni hileler, teknikler ve iş modelleri geliştirme konusunda teşvik etmiştir.

Darwinizm'e uygun olan bu hızlı evrim, iki yönlü ilginç bir ilerlemeyi başlatmıştır. Bu ilerlemenin bir yönü sadeliğe doğru giderken diğer yönü gelişmişliğe odaklanmıştır. Her iki ilerleme yönü de tehdit ortamındaki karmaşıklığın artmasına neden olmuştur. Bu karmaşıklık karşısında başarılı olmak, piyasada yalnızca birkaç şirketin sahip olduğu düzeyde yenilikçiliği, kaynakları ve deneyimi gerektirir. Bu şirketler gerçekten "yeni nesil güvenlik satıcısı" unvanına lâyıktır.

Bu durum, "yeni nesil tehditlerin" ortaya çıktığını ve işletmelerin yanı sıra özel kullanıcıları da tehdit etmeye başladığını gösterir mi?

Bu sorunun cevabı hem evet hem de hayırdır.

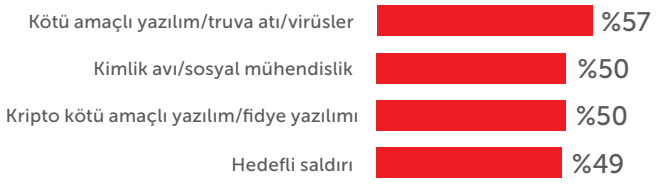
BT güvenlik uzmanları için yanıt doğal olarak **hayırdır**.

Saldırı tekniklerinde, korsanları herhangi bir güvenlik sistemine karşı tanrısal bir güce kavuşturacak sıçramalar yoktur. Bu tür tekniklerin bazıları, yıllar önce denenmiş olmasına rağmen yalnızca kısmen başarıya ulaşabilmişlerdir. Bunun nedeni o dönemdeki global BT ortamının teknolojik kısıtlamalarıdır. Günümüzde BT doğru konuma geldiği için bu teknikler bir anda çoğalarak saldırganların mevcut çözümler karşısında avantaj kazanmasını sağlamıştır.

Yine de bazı savunma sistemleri, saldırılar karşısında pes etmemiştir. Bu dayanıklı sistemlerin satıcıları, sürekli olarak düşmanlarının en yeni hilelerini dikkatle izler ve müşterilerinin haberi bile olmadan cephanelerine yepyeni önlemler ilave eder. Müşteri herhangi bir değişiklik olduğunu hissetmez. Bir teknoloji sessiz ve görünmez bir şekilde müşteri için Mümkün Olan En İyi Sonucu sağlayarak uygulanabiliyorsa hiçbir satıcı, müşterinin kullanım şeklini değiştirmesini gerektiren yeni bir teknolojiyi uygulamanın zorluklarıyla ve masraflarıyla uğraşmak istemez.

Ancak...

Ancak sürekli gelişen BT ortamında kaybedecek daha fazla şeye sahip olan bir son kullanıcı için saldırganlardan gelen ani bir baskıyı hissetmek, aniden ortaya çıkan bir canavarla karşılaşmaya benzer. Yıllardır hiçbir şeyden haberi olmadan mutlu bir şekilde çalışan ve kötü amaçlı yazılım saldırılarıyla nadiren karşılaşan işletmeler, artık son derece etkin siber suç girişimcilerinin kâr kapısı haline geldiklerini fark etmeye başlamıştır ve maalesef bu siber suçluların, işletmelerin peşini bırakmaya niyeti yoktur. Bu nedenle işletmeler, "Yeni Nesil tehditlerin" gerçek olduğunu düşünür.



Dünya genelindeki işletmeler için İLK 4 Güvenlik endişesi doğrudan tehditlerdir[1]

Bu nedenle, "Yeni nesil tehditler diye bir şey var mı?" sorusunun cevabı son derece karmaşıktır. Bu tehditler yeni olmayabilir, ancak güçlü ve engellemesi zordur. Ayrıca koruyucu çözümleri sağlayan satıcıların son derece becerikli, deneyimli ve kararlı olmasını gerektirir. Buradaki en önemli unsur, hem müşterilerin hem de satıcıların tesislerinde kullanılan teknolojilerle kusursuz bir şekilde birleştirilebilen tehdit istihbaratının derinliği ve kapsamıdır.

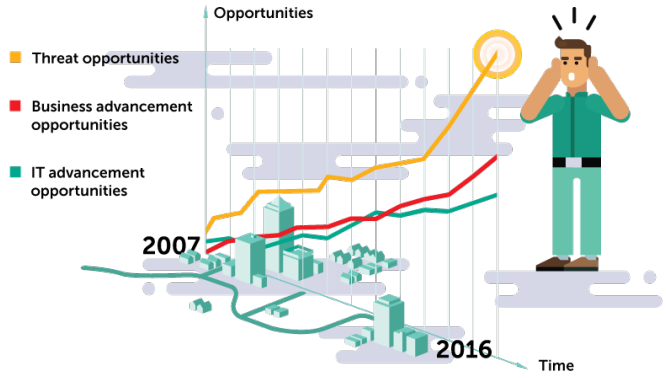
Bazı okuyucular, bu yeni şiddetli saldırılarla mücadele etmek için Yeni Nesil Antivirüsler'in gerekli olduğu sonucuna varabilir. Ancak birçok konuda olduğu gibi bu konuda da çabuk sonuç çıkarmak kötü bir fikirdir. Bunun nedenlerinden biri şudur: Bu "yeni nesil" tehditlerin çeşitliliği göz önüne alındığında koruyucu yaklaşımların da tehditler kadar çeşitli olması gerektiği anlaşılabilir. Dolayısıyla doğru çok katmanlı siber güvenlik, yalnızca en etkin saldırganların sevdiği tehditlere karşı değil her yerden gelen TÜM tehditlere karşı koruma sağlayabilmelidir.

Maalesef ki çok geniş bir yelpazedeki tehditlere karşı koruma ihtiyacı, sadelik ve sistem kaynakları üzerinde daha hafif yük için genellikle "yeni nesil" satıcılar tarafından görmezden gelinir. Bu durum, bağımsız testlerde de kanıtlanmıştır.

Kaspersky Lab gibi pazar liderleri ise bu tehdit

1 Kaynak: B2B International ve Kaspersky Lab tarafından Global Kurumsal BT Güvenlik Riskleri Araştırması 2016

çeşitliliğinin ve gelişmişliğinin farkındadır ve bunlara karşı koruma sağlamak için genellikle *birden çok* teknik sunar. Ayrıca Kaspersky Lab olarak, gerçek hayata en yakın senaryoların kullanıldığı kapsamlı testler gerçekleştirmenin önemini de anlarız. Mümkün olan tüm bağımsız testlere düzenli ve istekli bir şekilde katılmamız, koruyucu katmanlarımızı korumamıza ve iddialarımızın güvenilirliğini kanıtlamamıza yardımcı olur.



Şimdi günümüzün tehditlerinin "yeni nesil" olarak adlandırılmasına neden olan etkenleri inceleyelim.

Tehditlerin İki Yönlü İlerlemesi

Sadeliğe Yönelik Eğilim

Uygun maliyeti en önemli ilke edinen bu eğilim, saldırıların geliştirilmesi ve düzenlenmesi konusunda sadeliğe önem verir. Hazır kötü amaçlı yazılımları alan, bu yazılımları minimum düzeyde özelleştiren ve kurbanlarının doğru güvenlik önlemleri almamasına güvenen geliştiriciler, kayda değer bir başarı oranı yakalamıştır. Dolayısıyla eski yazılımlar da son derece etkili olabileceği için sıfırdan yeni kötü amaçlı yazılımlar geliştirme ihtiyacı ortadan kalkmıştır. Oldukça basit bir çözüm!

Bir diğer sadeleşme alanı ise daha beceriksiz ve sabırsız siber suçluların faydalanabileceği uygun iş modelleri sunan kötü amaçlı yazılımların pazarlanmasıdır. Yalnızca kötü amaçlı uygulama ticaretinin yerine hizmet satmak veya kötü amaçlı yazılımlar için kullanışlı arabirimler hazırlayarak ayrıntılı SSS ve kullanıcı desteği sunmak; "hacker" pazarının genişlemesine neden olmuş ve çok sayıda "deneyimsiz" hacker ve amatörün ilgisini çekmiştir. Sonuç olarak toplam siber saldırı miktarının artmasıyla beraber işletmelerin üzerindeki baskı da artmıştır.

Gelişmişliğe Yönelik Eğilim

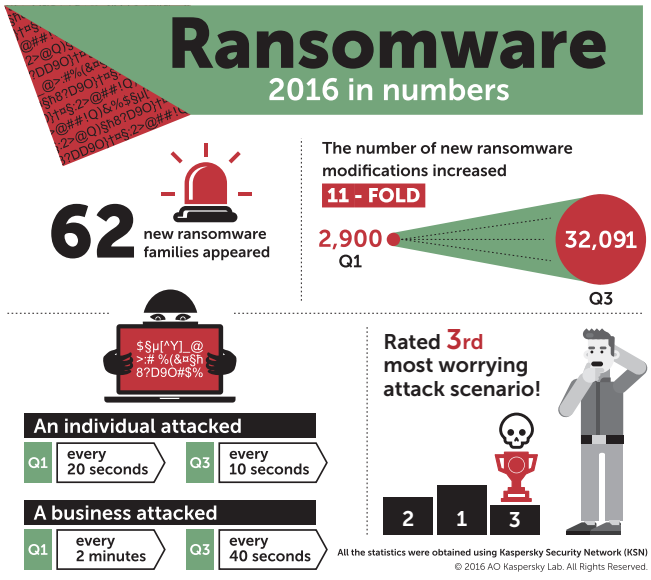
Ancak tüm bu yeni basitleştirilmiş iş modelleri, günümüzde siber saldırganlar tarafından kullanılan araçlar ve tekniklerde teknolojik ilerleme olmadığı anlamına gelmez. Hatta tam tersi geçerlidir. Artık "deneyimsiz saldırganlar" bile daha önce uygulayamayacakları kadar gelişmiş kötü amaçlı yazılımlara erişim sağlayabilir. Ayrıca bu yeni gelişmeler, gerçek uzmanlar tarafından kullanıldığında (siber suçluların arasında bu tür uzmanlara az rastlanır) kesinlikle hafife alınmaması gereken bir silaha dönüşebilir.

Buna ek olarak, daha önce özel veya hedefli saldırılar olarak değerlendirilen bazı teknikler, toplu virüs saldırıları için de kullanılmaya başlanmıştır (bu toplu saldırılar, saldırının herhangi bir aşamasında *hedefli* hale dönüşebilir).

Anonimlik Maskesi

Muhtemelen tehdit ortamında yakın zamanda gerçekleşen büyük değişimin arkasındaki en önemli gelişmelerden biri, anonimliğin artmasıdır. Bitcoin ve diğer kripto para birimlerinin ortaya çıkması, takip edilemeyen ödemeler yapılmasını sağlamıştır. Ayrıca Tor gibi anonim örgüsel ağlar, açığa çıkma riskini azaltarak Siyah Şapkalı saldırganlara iletişim kurmanın yanı sıra bilgi ve teknoloji alışverişi yapma fırsatı sunmuştur. En deneyimli siber suçlular, hâlâ "yalnızca davetiyle giriş" yöntemini kullanarak sıkı topluluklar oluşturmasına rağmen bu yeni teknolojilerin sunduğu ek avantajlardan da faydalanır. Örneğin fidye yazılımı (dünya genelinde en önemli üçüncü BT güvenliği sorunu seçilmiştir[2]) gibi bazı siber suç iş modelleri, son zamanlarda büyük artış göstermiştir.

Fidye yazılımları



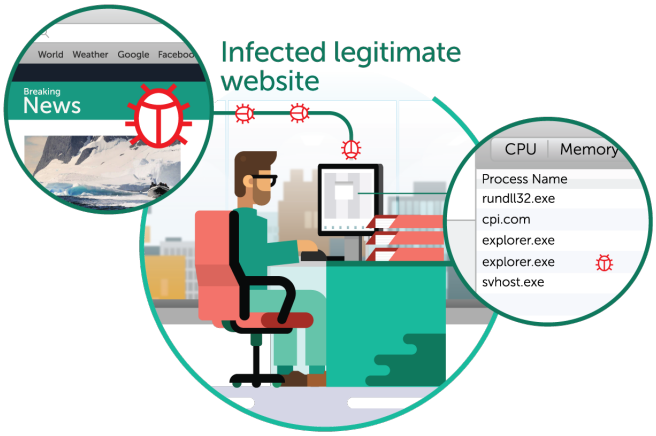
2 B2B International, Mayıs 2016

Fidye yazılımları, belirli bir teknolojiyi temsil etmemesine rağmen günümüzde karşılaştığımız gerçek anlamda "Yeni Nesil" tehditlerden birisidir. Fidye yazılımlarını açıklamak için akla gelen ilk kavramlardan biri "siber suç iş modeli"dir. Bu yazılımlar, teknolojik olarak yalnızca çok çeşitli saldırı araçlarından ve tekniklerinden değil aynı zamanda çok sayıda anonimleştirme önlemlerinden destek alır. Kripto para birimleri ve örgü ağların (Tor, I2P vb.) ortaya çıkışı, dolandırıcıların ödemelerini gizli bir şekilde almalarını sağlar. Bu özellik, şimdiye kadar görülen en büyük fidye yazılımı akımını başlatmıştır. Fidye yazılımları doğru şekilde ele alınmazsa gününüzün doğrudan ve en yıkıcı şekilde mahvolmasına neden olabilir. Ayrıca bu yazılımın etkilerini tersine çevirme şansı da oldukça düşüktür. İstatistiklere göre fidyeyi ödeyen her beş mağdurdan biri, dosyalarının şifresini çözememektedir. Maalesef suçluları bu şekilde finansal olarak desteklemek, bir sonraki fidye yazılımı dalgasını desteklemekten başka bir işe yaramaz.

Farklı fidye yazılımı türleri, farklı saldırı teknolojileri ve bulaşma yöntemleri kullanabilir. Bu nedenle tüm sisteminizi koruyan ve özel fidye yazılımlarından koruma teknolojileriyle donatılmış çok katmanlı çözümlere sahip olmak önemlidir. Örneğin, Kaspersky Endpoint Security for Business çözümümüz, kötü amaçlı yazılımları engelleyebilen ve yazılımın şifrelemeyi başardığı dosyaları eski haline çevirebilen şifreleme yazılımlarına karşı koruma ve geri alma sistemi sunar. Kaspersky Security for File Servers ve Kaspersky Security for Storage çözümleri, şifreleme yazılımlarına karşı tamamlayıcı koruma motoruna sahiptir. Bu motorlar, ağdaki farklı bir ana bilgisayar aracılığıyla başlatılmış şifreleme süreçlerini engeller. Ayrıca başka satıcıların çözümlerini kullanan şirketler için bağımsız (ve ücretsiz) Kaspersky Anti-Ransomware Tool çözümü, ihtiyacınız olan temel korumayı sağlayabilir. Bu ücretsiz aracın temel aldığı teknoloji, Kaspersky Endpoint Security çözümünde kullanılan teknolojiyle aynıdır. Ancak kendi çözümlerimizde bu teknolojiyi destekleyen birçok ek koruma katmanı, bu uygulamaya dahil değildir.

Salt bellek kötü amaçlı yazılımlar

Birçok kötü amaçlı yazılımın normal dosyalar biçiminde gelmesi, dosya tabanlı tespitin önemini doğrular. Ön yürütme tespitinin büyük bir kısmı, bu düzeyde gerçekleşir. Tabii ki bu tespit, yalnızca dar kapsamlı imzalarla sınırlı değildir. Yapı ve kod tabanlı analizler dahil olmak üzere her türlü sezgisel analiz, daha önce bilinmeyen kötü amaçlı yazılımları bile tespit edebilir. Ancak kötü amaçlı yazılımlar dosya sisteminin dışında çalışıyorsa bu kapsamlı özellikler, bir anda kullanışsız hale gelir. Ayrıca dosya yapıları da adli bilişimcilere geniş bir bilgi hazinesi sunar. Tüm bunlar göz önünde bulundurulduğunda, saldırganlar, özellikle hedefli saldırılarda "salt bellek" yaklaşımlarından yararlanmaktadır. Bu saldırı, "watering hole" bulaşma tekniklerinin kullanımı veya dosya eklerinin (erken tespitten kaçınmak için son derece iyi gizlenmiş)



açılması gibi farklı yöntemlerle gerçekleştirilir. Sonuç her durumda aynıdır. Kötü amaçlı yazılım, çalışan bir sürece sızmayı başarır ve bu andan itibaren ek modülleri yükleme ve başlatmanın yanı sıra saldırıdan etkilenen altyapının içinde yatay olarak hareket etme gibi birçok işlemi dosya sistemine hiç dokunmadan gerçekleştirebilir.

Kaspersky Endpoint Security, salt bellek kötü amaçlı yazılımları dahil olmak üzere birçok gelişmiş kötü amaçlı yazılım türünü tespit etmek için Sistem İzleyici özelliğine sahiptir. Bu teknoloji, belirli bir sistemin içindeki etkinlikleri izleyerek şüpheli uygulama davranışlarını tespit eder. Bu yaklaşımda gözetim altındaki sürecin arkasında dosya yapısının olup olmaması önemli değildir. Her türlü kötü amaçlı etkinlik engellenir. Sistem İzleyici'nin tespit ilkeleri, sürekli çalışan Makine Öğrenimi süreçlerine dayanmaktadır. Bu süreçler, Kaspersky Security Network'ün global olarak topladığı istatistiklerin Veri Bilimi destekli işlenmesi aracılığıyla elde edilen kapsamlı tehdit istihbaratlarından faydalanır.

Powershell: yasal yorumlayıcı, yasa dışı etkinlikler

Uzun yıllardır kabuk komut dosyalarının, zararsız olduğu düşünülüyordu. Tabii ki yaratıcı bir şekilde kötü amaçlarla kullanıldığında zararsız diye bir şey yoktur. Powershell komut dosyaları, normal komut dosyalarından farklıdır. Bu dosyalar, son derece güçlü olduğu için saldırganlara çok çeşitli fırsatlar sunar. İnternetten ek modüller indirmek, gövdesiz kötü amaçlı yazılımları çalıştırmak ve ağdaki diğer makinelerde uzaktan rastgele kod yürütmek... Bunlar gibi birçok

zararlı işlemi gerçekleştirebilen Powershell yorumlayıcı, aslında Windows 7'den beri standart Windows ekipmanı olan yararlı bir uygulamadır. Bu tekniğin en ünlü kullanıcıları arasında Carbanak siber suç örgütünün kötü şöhretli banka hırsızları vardır.

Kaspersky Lab, bu Powershell kötü amaçlı yazılım dalgasının ve normal kabuk komut dosyalarının kötü amaçlar için kullanıldığının tam anlamıyla farkındadır. Motorlarımıza aktarılan dizeler, dikkatli bir şekilde analiz edilir ve kötü amaçlı herhangi bir şeyin bulunması halinde engellenir.

Mobil

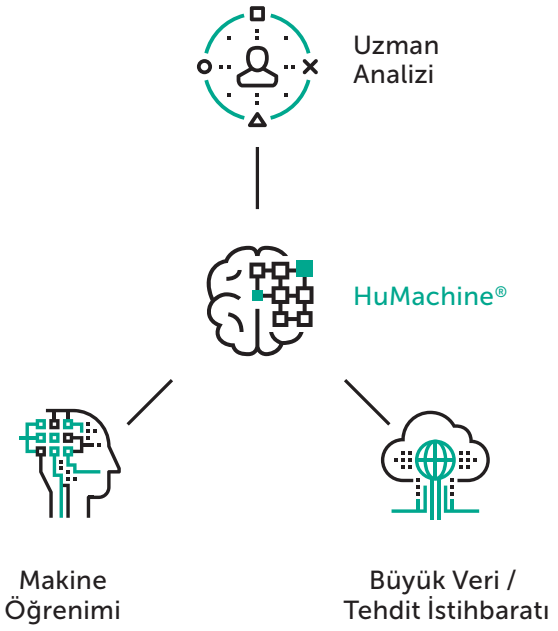
Cep telefonları ve tablet bilgisayarlar, internete erişmenin öncelikli yolu haline gelmiştir. 2016'nın sonuna kadar dünya çapında kullanılan akıllı telefonların sayısı 2,1 milyara ulaşacaktır. Bu sayı, siber suçlular için bereketli bir hasat dönemi anlamına gelir. Mobil cihazlar, kurumsal iş süreçlerine ve veri akışlarına sıkıca entegre edilmelerine rağmen maalesef her zaman kurumsal siber güvenlik altyapılarına entegre edilmezler. Artan jeopolitik gerginlikler, mobil finansal yönetimin artan popülerliği ve şu anda bu cihazlarda tutulan hassas veri sayısının miktarı gibi birçok etken, mobil cihazlara yönelik bir saldırı patlaması için beklentiyi artırmaktadır. Günümüzde mobil sıfır gün açıklarının siber casusluk için kullanıldığı bir gerçektir. Ancak bundan daha az gelişmiş yöntemler bile beklenmedik olduklarında son derece başarılı sonuçlar verebilir. Buna iyi bir örnek olarak kötü amaçlı reklam saldırıları verilebilir. Bu saldırılarda, kötü amaçlı bir JavaScript içeren belirli bir reklam ağı bloğuna sahip popüler siteler, yüklendikten sonra cihazlara bir bankacılık Truva Atı indirilmiştir. Android akıllı telefonların büyük bir kısmında, kısıtlamaların kaldırılmasının (rooting) zahmetsiz olması (sahte/kötü amaçlı yazılımlar tarafından) ve bazı cihazların önceden yüklenmiş kötü amaçlı yazılımlarla temin edilmesi, kullanıcının kontrol edebildiği işletim sistemi katmanın altında yer alan sistem düzeyindeki kötü amaçlı yazılımların yaygın olduğunu gösterir.

Kaspersky Mobile Security for Business, birçok masaüstü çözümle kıyaslanabilir çok çeşitli tespit katmanları sunar. Ayrıca bu katmanların bir kısmının, HuMachine zekamızın tüm gücünden faydalanan Makine Öğrenimi teknolojisiyle desteklendiğini belirtmekte fayda vardır. Bu çözüm, aynı zamanda Cihaz Kontrolü gibi ek güçlü güvenlik katmanlarına sahiptir. Mobil Güvenliğin, Mobil Cihaz Yönetimi ve Mobil Uygulama Yönetimi teknolojileriyle bir bütün olarak hareket etmesi önemlidir. Bu tür bir yaklaşım, işletmelerin sağlam ve özellikle güvenli bir mobilite stratejisi oluşturmasına yardımcı olur.

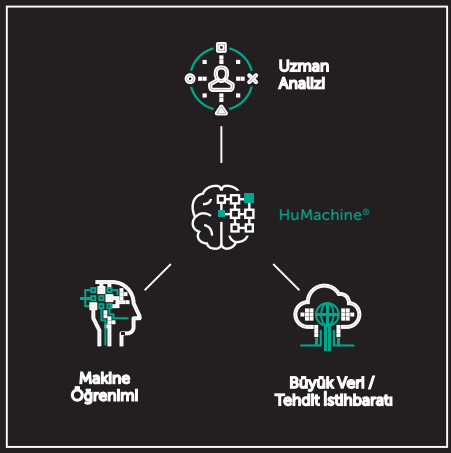
Sonuç

Yukarıda açıklanan teknikler listesi, yeterince kapsamlı olmamasına rağmen yalnızca deneyimli ve profesyonel suçluların başarabileceği bir yaratıcılık seviyesini gösterir. Sevgili okurumuz, belki de bu saldırı teknikleri içinize Korku, Belirsizlik ve Endişe tohumları saçmış olabilir. Dolayısıyla bu korkulardan kurtulmanız için size bazı şeyleri hatırlatmak isteriz.

Öncelikle bu tehditlerde olağanüstü yenilikler kullanılmaz. Hatta "Yeni Nesil" olarak adlandırabileceğimiz en önemli gelişmelerden biri, Bitcoin ve Tor benzeri ağlarla takip edilemeyen iletişim ve ödeme yöntemlerinin kullanılmasıdır. Bu teknolojilerin bile uzun bir geçmişi vardır ve aslında yapısal olarak kötü amaçlı değillerdir. Bunlar da diğer birçok yasal araç gibi siber suçlular tarafından kötü amaçlarla kullanılan hem yararlı hem de zararlı araçlardır.
Yani bu teknikler, çoktan çözülmüştür ve bunlara karşı koruma yöntemleri şu anda Kaspersky Lab gibi lider satıcılar tarafından sunulmaktadır. Tehdit istihbaratı toplama, makine öğrenimi süreçleriyle desteklenen veri bilimi ve dünyaca ünlü uzman ekibimizin birleşiminden oluşan HuMachine yaklaşımımız sayesinde müşterilerimiz Mümkün Olan En İyi Sonucu elde edeceklerinden emin olabilir. Geleceğin "yeni nesil" tehditleri nasıl gelirse gelsin, karşılarında aynı ölçüde etkili "yeni nesil" koruma teknolojilerini bulacaktır. Bu, Gerçek Siber Güvenlik vizyonumuzun önemli bir parçasıdır.



Kaspersky Lab, Moskova, Rusya**www.kaspersky.com.tr**
İnternet güvenliği hakkında her şey için:**www.securelist.com**
Size en yakın iş ortağımızı bulun: **www.kaspersky.com.tr/buyoffline**

www.kaspersky.com.tr

© 2018 Kaspersky Lab. Tüm hakları saklıdır. Tescilli ticari markalar ve hizmet markaları ilgili sahiplerinin mülkiyetindedir.