COMODO
Creating Trust Online®

COMODO zararlı yazılımlara geçit vermiyor!

COMODO Araştırma Laboratuvarı tarafından yapılan incelemelere göre, COMODO'nun kendi geliştirdiği Tehdit Önleme Teknolojisi tüm dünyada milyarlarca dolar zarara yol açan Cryptolocker, SpyEye ve Shylock gibi zarar yazılımları bilgisayara sızmadan engelledi.

Cryptolocker, SpyEye… Bunlar, rutin bir mesai günümüzün en tatlı(!) yerinde ekranımızın orta yerinde belirerek bizden para isteyen ya da masum bir e-mail olarak kendini gösterip internetten ulaşabildiğimiz tüm malvarlığımıza gözünü diken zararlı yazılımların isimleri... Bu isimlere artık en sevdiğimiz televizyon dizisinin oyuncularının isimleri kadar aşinayız; hatta Shylock'u Shakespeare'in ünlü oyunu Venedik Taciri'ndeki gözü açık tüccar karakteri olarak hatırlayanların sayısı gitgide azalıyor… Shylock artık gelen mailleri okuma "naifliğimizi" istismar eden bir virüsün adı.

FBI'ın verilerine göre, 2015'in Haziran ayı sonu itibariyle sadece CryptoWall tarafından bilgisayarı esir alınan kişilerin ödemek zorunda kaldığı toplam fidye 18 milyon doları geçti. Sadece 2014'te zararlı yazılımların tüm dünyada verdiği zararın 500 milyar dolara ulaştığı tahmin ediliyor. Ülkeler bu suçlarla mücadele etmek için birimler oluşturdu. Büyük uluslararası operasyonlarla SpyEye'ın yaratıcısı Aleksandr Andreevich Panin ve Hamza Bendelladj 2013'te tutuklandı. **Sonuç? SpyEye'ı bitti mi? Hayır...** Bugün SpyEye'in tüm dünyada en az yaklaşık 1,5 milyon bilgisayarı enfekte ettiği belirtiliyor.

Araştırmalara göre, zararlı yazılımlar sisteme bir kez girdikten sonra kişilerin veya işletmelerin bunu bulma ve yok etme ihtimali **yüzde 33**'e kadar düşüyor. Bu nedenle asıl mesele bu yazılımları sisteme hiç sokmamakta. Dünyanın önde gelen siber güvenlik firmalarından biri olan COMODO kendi geliştirdiği patent bekleyen teknolojisi *Containment (Tehdit Önleme Teknolojisi)* ile zararlı yazılımları cihazınıza hiç yaklaştırmadan tespit etme ve yok etme imkanı sunuyor. Daha önceden hiç bilinmeyen, sıfırıncı gündeki bir zararlı yazılımı bile Containment, "olağan şüpheli" olarak kabul ediyor ve bilgisayarınıza zarar vermeyecek şekilde korunaklı bir ortamda açarak bakıyor; zararlı yazılım olduğunu anladığı anda yok ediyor. **Sonuç? %100 koruma!**

Geçtiğimiz haftalarda; COMODO Think Tank mühendisleri günümüzde en korkulan zararlı yazılımlar ve fidye yazılımlarını inceleyerek, Comodo Tehdit Önleme Teknolojisi ile karşılaştırdı. **Sonuç? Cryptolocker, Shylock ve SpyEye zararlı yazılımları Comodo Tehdit Önleme Teknolojisi karşısında başarısızlığa uğradı.**

Firmaların CIO ve CISO'lar için, IT yöneticileri ve mühendisleri için *Comodo Uç Nokta Güvenlik* ve *Tehdit Önleme*, cihaz bünyesinde, gerçek zamanlı tehdit önleme imkanı sunan tek çözüm. Kara listeye veya Sandbox'a alma gibi alışılmış yaklaşımlardan farklı olarak; Containment (Comodo Tehdit

Önleme), akıllı filtreleme kullanarak bilinmeyen dosyaları, sistem performansı ya da kullanıcı üretkenliğine zarar vermeden, otomatik olarak hapsederek yürütüyor.

Comodo Teknoloji Direktörü ve COMODO Think Tank üyesi Fatih Orhan'a göre; "*COMODO'nun tehdit önleme teknolojisi günümüzde pazardaki diğer tüm yazılımlardan tümüyle farklı. Tespit etmeye değil, önlemeye odaklı uç nokta koruma teknolojimiz ile müşterimizi güvende tutuyoruz. Müşterilerimizin karşı karşıya kaldığı siber tehditten bağımsız olarak; bilgileri güvenli durumda; çünkü tehdit önleme teknolojimiz bilgiyi korurken zararlı yazılımları engelliyor*."

Comodo Think Tank'in zararlı yazılımlarla savaşına daha ayrıntılı bakalım:

Comodo Containment SpyEye'ya karşı:

SpyEye, siber suçluların çevrimiçi bankacılık detayları, kredi kartı verileri, şifreler ve diğer kişisel bilgileri çalmak için kullandığı bir çeşit zararlı yazılımdır. SpyEye dünya çapında 1,5 milyon bilgisayara bulaşmıştır ve sessiz saldırısı, gizli bilgilerin doğrudan suçlulara iletildiğinin göstergesidir.

SpyEye zararlı yazılımı şöyle çalışır:

1. SpyEye; bilgisayar süreçleri içinde izinsiz bir kodun yürütülmesinde kullanılan bir teknik olan hafıza içi enjeksiyona başvurur.
2. SpyEye'ın enjekte edilen kodu, daha sonra metin kutularına "kanca atarak" kişinin bu kutulara yazdığı tüm bilgileri toplar: giriş detayları, kredi kartı bilgileri ve diğer tüm gizli bilgiler
3. Bu zararlı yazılım, söz konusu hassas bilgileri doğrudan siber suçlulara iletir.

Ancak SpyEye; Comodo'nun patent bekleyen tehdit önleme teknolojisi ile donanmış olan bir bilgisayara ulaştığında; sonuçlar SpyEye için felaket olur:

1. SpyEye zararlı kodunu enjekte etmeye çalışır.
2. SpyEye BAŞARISIZ OLUR – hem de acı bir şekilde. Comodo'nun tehdit önleme teknolojisi ile zararlı yazılımlar, açıkça, diğer süreçlere kod enjekte edemez.
3. **Sonuç: Comodo 1 – SpyEye: 0**

Sonuç: Güvenli Comodo kullanıcısı

Comodo Containment Shylock'a Karşı:

Shylock, bankacılık oturum açma ve hesap detaylarınızı siber dolandırıcılara vermeniz konusunda sizi kandırmaya çalışmak üzere tasarlanmış, kötü şöhrete sahip bir bankacılık kötücül yazılımıdır.

Shylock şöyle çalışır:

1. Shylock kodunu web tarayıcınıza yerleştirir ve bankacılık sitenizin görünümünü taklit eder.
2. Oturum açma bilgilerinizi, şifrelerinizi, kredi kartı bilgilerinizi ve diğer özel bilgilerinizi toplar.

3. Özel bilgilerinizi doğrudan siber dolandıcılara gönderir.

Buna karşılık, Shylock Comodo'nun, bilinmeyen tüm dosyaların önleme işlemine tabi tutulduğu Önleme (Containment) Teknolojisiyle karşılaştığında, sonuç Shylock açısından hüsran olur.

1. Shylock kodunu yerleştirmek için çaba gösterir.
2. Shylock başarısızlığa uğrar. Comodo Önleme teknolojisinde, kötücül yazılımların kodlarını başka süreçlere yerleştirmeleri mümkün değildir.
3. **Sonuç: Comodo: 2 – Shylock: 0**

   Sonuç: Mutlu bir Comodo kullanıcısı

COMODO Containment Cryptolocker'a karşı:

Cryptolocker, fidye yazılımı şu şekilde çalışır:

1. Dosyayı okur

2. Dosyayı şifreler

3. Şifrelenmiş dosyayı orjinal dosyanın üzerine yazar

4. Fidye talep eder

Ancak uzmanlık alanı tanımlanmamış her türlü yeni dosya olan Comodo'nun önleme teknolojisi ile karşılaşınca :

1. Dosyayı okur
2. Dosyayı şifreler
3. Comodo önleme teknolojisi sayesinde başarısız olur, çünkü sabit diskteki veriyi değişteremez. Sadece Comodo'nun önleme teknolojisinde yer alan sanal sunucudaki veriyi değiştirebilir
4. **Sonuç: Comodo: 3 – Cryptolocker: 0**

   Sonuç: Parası güvende bir Comodo kullanıcısı

COMODO, sektörde, etkisi kanıtlanmış ve pratikte ispat edilmiş önleme (containment) teknolojisi sunan yegane antivirüs şirketidir.

Dünyanın İlk Otomatik Önleme Teknolojisi hakkında daha fazla bilgi alabilirsiniz.

Comodo Tehdit Önleme hakkında ayrıntılı bilgiye ulaşmak için "İyi, Kötü ve Çirkin" başlıklı bu kısa videoyu izleyin. https://youtu.be/Uq31kqKiQ4I

En son Comodo haberlerini öğrenmek için ise, Twitter'da @ComodoNews hesabını takip edin.

COMODO Hakkında

Türk girişimci *Melih Abdulhayoğlu* tarafından 1998 yılında kurulan COMODO, bugün dijital sertifika alanında dünyanın en önemli markası durumundadır. Her bir sayısal işlemin özel bir güven ve güvenlik katmanı hak ettiği ve gerektirdiği inancından hareket eden COMODO siber güvenlik çözümleri geliştirme konusunda dünya çapında öncü bir kuruluştur. COMODO'nun SSL sertifikaları, antivirüs ve uç nokta güvenlik liderliğinin yanı sıra gerçek koruma teknolojisi alanındaki uzun geçmişine güvenen bireyler ve kurumlar, en kritik bilgilerinin kimlik denetimi, doğrulanması ve güvenliğinin sağlanması için firmanın kendini kanıtlamış çözümlerini tercih ediyor. Uç nokta, ağ ve mobil güvenliğinin yanı sıra kimlik ve erişim yönetimini de kapsayan veri koruması sunan COMODO'nun kendisine ait teknolojileri günümüzdeki kötü niyetli yazılım ve siber saldırı sorunlarının çözülmesini sağlıyor. Binlerce kurumsal müşterinin online işlemlerinin güvenliğini sağlayan ve 85 milyon üzerinde masaüstü güvenlik yazılım yüklemesine sahip COMODO "Creating Trust Online®" (COMODO Online Güven Sağlar) mottosu ile hareket ediyor.

Merkezi ABD Clifton, New Jersey'de bulunan COMODO'nun Çin, Hindistan, Filipinler, Romanya, Türkiye, Ukrayna ve Birleşik Krallık'ta ofisleri bulunuyor. Türkiye'de teknoloji ekosistemi kurmak üzere girişimlerde bulunan COMODO, bu kapsamda ilk Ar-Ge merkezini ODTÜ Teknokent'te açtı. COMODO, ODTÜ Enformatik Enstitüsü işbirliği ile Türkiye'nin ilk Siber Güvenlik ve Savunma AR-GE Merkezi'ni kurarak, yerli siber savunma teknolojilerinin üretimini sağlıyor.

COMODO'nun müşterileri arasında **NASA, IBM, New York Borsası, Sony, Chase, Michigan Üniversitesi** gibi seçkin bankacılık, finans, eğitim ve devlet kurumları ve ABD Başkanı **Barack Obama** ve Cumhuriyetçi Parti adayı **Mitt Romney** gibi siyasetçiler yer alıyor.

İletişim:

Banu Buyurgan
GTC İletişim Danışmanlığı
+90 312 447 00 20

banu.buyurgan@gtc.com