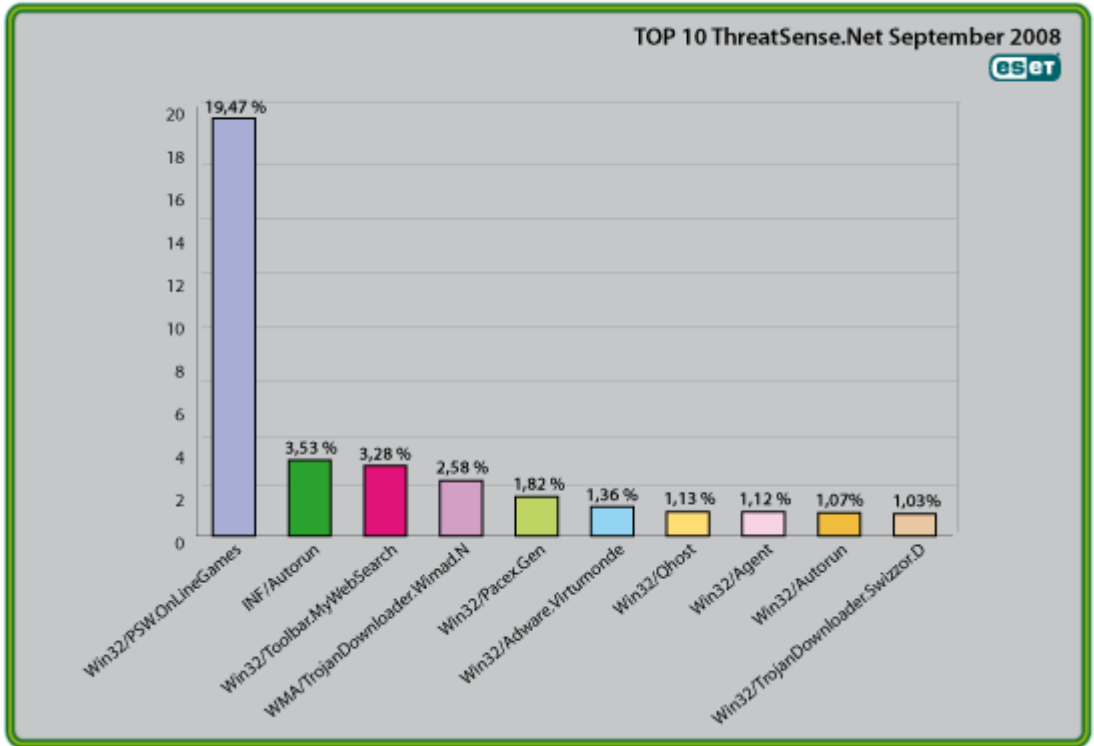




Dünya Tehdit Eğilimleri – Eylül 2008

Şekil 1: Bir Bakışta 2008 Eylül Ayının İlk On Tehdidi



ESET'in gelişmiş bir Malware (zararlı yazılım) raporlama ve takip sistemi olan ThreatSense.Net® analizlerine göre, bu ayın en yüksek sayıdaki tespiti %19,47 ile yine, bizim "Win32/PSW.OnLineGames" ismi ile kategorize ettiğimiz zararlı yazılıma ait.

ThreatSense.Net® tarafından tespit edilen en yaygın tehditler hakkında, ilk on sıralamasındaki önceki yerleri ve diğer tüm tehditlere oranları gibi tüm bilgiler aşağıda verilmiştir.

Raporlama sistemi hakkında daha detaylı bilgi edinmek için sayfanın sonundaki ESET'in ThreatSense.Net® Teknolojisi Dünyayı Kapsıyor başlıklı bölüme bakabilirsiniz.

1. Win32/PSW.OnLineGames

Önceki Sıralaması: 1

Tespit Yüzdesi: 19.47%

2008 Ağustos ayı itibarı ile tüm tespitlerin %19,47 ye yakın bir oranı Win32/PSW.OnLineGames olarak etiketlenmiştir, geçen ayki %16,13 e göre önemli bir artış. Bu yazılım çevrim içi oyunlar ve bu oyunlara katılımlar hakkında bilgi toplama amaçlı ve rootkit, keylogging yeteneklerine sahip bir Truva atı ailesine mensuptur. Genel olarak bilgiler davetsiz misafirin bilgisayarına gönderilir.

Son Kullanıcı Açısından Anlamı;

Lineage, World of Warcraft ve sanal dünya Secondlife gibi MMORPG (masif, çok eşli, çevrim içi oyunlar) katılımcılarının, sadece tacizler ve rahatsız etmeler dış nda phishing (ortalama) ve diğer dolandırıcı ilk yöntemleri gibi gerçek dünyada finansal kayıplarla sonuçlanabilecek kendilerine yönelik tehditlerin farkında olmaları çok önemlidir. Bu gibi olaylarda amaç hesap bilgilerine ya da oyun elemanlarına erişmek ve bunları karaborsa da ya da e-bay'de tekrar satmaktır. ESET Malware Beyin Takım bu olayı daha geniş bir biçimde yine bu sıralar yayınlanacak olan ESET Yıl Ortası Raporunda ele aldı.

2. INF/Autorun

Önceki Sıralaması: 2

Tespit Yüzdesi: 3.53%

Bu tespit etiketi autorun.inf dosyasını kullanarak bilgisayarı risk altında bırakan birçok, çeşitli malware'i tanımlamak için kullanılır. Bu dosya bilgisayara takılan çıkarılabilir aygıtlar (USB Flash Disk gibi) üzerindeki kendi kendine çalışması gereken programlar hakkında bilgiler içerir. ESET'in güvenlik yazılım bu malwareleri başka bir tanım altında bulunmadığı zamanlarda INF/Autorun etiketi ile sezgisel olarak tespit eder. Bu durum rakamlar karşılaştığında az bir düşüşe işaret eder fakat özellikle başka imzalar ile tespit edilenler olduğu da dikkate alındığında trendin azaldığı anlamına gelecek kadar büyük bir düşüş değildir.

Son Kullanıcı Açısından Anlamı;

Çıkarılabilir aletler çok revaçtalar: Malware kodlayıcıları bu durumun farkındalar ve bilgisayar kullanıcıları için oldukça büyük tehlikeler mevcut. Windows İşletim Sistemindeki varsayılan Autorun ayarı çıkarılabilir medya'ları taktığınızda autorun.inf listesindeki programları otomatik olarak başlatma görevi üstlenir. Programın birincil dağıtım mekanizması bu olmasa bile kendilerini çıkarılabilir aygıtlara kopyalayan birçok malware vardır, malware kodlayıcıları her zaman ekstra bir şeyler katarlar. Bu

mekanizmayı kullanan malwarelerin her olayda Antivirus tarafından tespit edilmesindense ki ESET bunu da yapabiliyor ☺ Randy Abrams'ın blog'umuz da (<http://www.eset.com/threat-center/blog/?p=94>) önerdiği gibi sezgisel olarak bulunması daha yerindedir. Bu olay Yıl Ortası Raporunda daha detaylı olarak ele alınmış tır. <http://www.eset.com/threat-center/>.

3. Win32/Toolbar.MywebSearch

Önceki Sıralaması: 4

Tespit Yüzdesi: 3.28%

Yazılım PUA "Potentially Unwanted Applications" (istenmeyen uygulama) kapsamına giriyor. Bu uygulama sorguları MyWebSearch.com üzerine aktaran bir arama çubuğudur.

Son Kullanıcı Açısından Anlamı;

Bu küçük, baş belası aylardır ilk on listemizin ısrarcı bir ziyaretçisi. Anti-Malware firmaları bu tip yazılımları varsayılan olarak standart taramanın yerine "istenmeyen uygulama" olarak imzalıyorlar. Çünkü bazı adware ve spyware uygulamaları son kullanıcı lisans sözleşmesinde (EULA) küçük puntolarla da olsa yazıldıklarından yasal yazılım olabiliyorlar. Küçük puntoları okumaktan zarar gelmez...

4. WMA/TrojanDownloader.Wimad.N

Önceki Sıralaması: 7

Tespit Yüzdesi: 2.58%

Bu tehdit, web tarayıcıların adware de içeren zararlı yazılımları indirebilecekleri başka bir URL'e yönlendiren bir Windows Medya dosyası olarak geliyor. Tehdit kullanıcıları indirmeye teşvik etmek amacı ile peer-to-peer ağlarda popüler bir MP3 dosyası gibi yayınlanıyor.

Son Kullanıcı Açısından Anlamı;

Zararlı dosyaları MP3, Flash Film'ler, Video Codec'ler şeklinde yutturmak kodlayıcılar tarafından sıkılıkla kullanılan bir sosyal mühendislik yöntemidir. Görünüşte masum olan dosyalar çalıştırdıklarında krallığın anahtarını kötü adamlara teslim edebilmektedirler. Kendisi çalıştırılabilir olmayan bir dosyanın yine de zararlı bir kodu içeri alabileceği olması unutulmamalıdır ve ekranda pop-up lar belirmeye başladığında dikkatli olunmalıdır.

Bu tip sosyal mühendislik örnekleri malware yazarları tarafından son kullanıcıyı kandırmak ve zararlı kodu çalıştırmasını sağlamak amacı ile sıklıkla kullanılan bir yöntemdir.

5. Win32/Pacex.Gen

Önceki Sıralaması: 6
Tespit Yüzdesi: 1.82%

Pacex.gen etiketi çok geniş bir yelpazede ki özel bir gizlenme metodu kullanan malwareleri tanımlar. .gen son eki "generic" (genel) anlamındadır. Etiketinin birçok değişik kenisi kapsadığı ve aynı zamanda aynı karakteristiği taşıyan bilinmeyen değişik kenilerinde aynı imza ile tanımlanabileceği anlamındadır.

Son Kullanıcı Açısından Anlamı;

Bu malwarede kullanılan gizlenme metodu daha çok parola çalmakta kullanılan Truva Atlarında görülmüştür. Çevrimiçi oyun kullanıcılarını hedef alan bazı tehditler PSW.OnLineGames 'den daha ziyade bu iki tehdit arasındaki benzerlikten dolayı Pacex olarak tanımlanır. Bu da PSW.OnLineGames kategorisinin zaten yüksek olan tespit yüzdesinin daha da yukarılarda olabileceği anlamına gelir. Buna rağmen, birden çok proaktif tespit algoritması sayesinde yükselen koruma gözlemlenen bu tehdidin maskesini indiriyor.

6. Win32/Adware.Virtumonde

Önceki Sıralaması: 3
Tespit Yüzdesi: 1.3%

Bu tanımlama kullanıcı bilgisayarlarına reklam gönderen Truva Atı ailesindedir. Çalışırken diğer eylemlerinin dışında istenmeyen reklam materyali içeren birçok pencere açar ve tamamen temizliğin otomatize edilmesi güç olabilir. Virtumonde'nin varlığının ilk anda sürmesinden anlaşılacağı üzere malware üreticileri için halen büyük bir gelir kapısıdır.

Son Kullanıcı Açısından Anlamı;

Virtumonde, "adware" olarak tanımlanmasından öte kullanıcılar için olduğu gibi üreticiler içinde başlı başına zor bir problem haline geldi. Bu konu hakkında daha fazla bilgi geçtiğimiz ayın raporunda ki (Temmuz) "Virtumonde: Hoş karşılanmayan ve ısrarcı misafir" başlığında verilmiştir.

Bu konu ayrıca "Adware, Spyware and Possibly Unwanted Applications", başlıklı bloğumuzda da yayınlanmaktadır. <http://www.eset.com/threat-center/blog/?p=138>

7. Win32/Qhost

Önceki Sıralaması: 10

Tespit Yüzdesi: 1.13%

Bu tehdit çalışmaya başlamadan önce kendisini Windows'un %system32% dizinine kopyalar. Daha sonra komuta ve yönetim merkezi ile DNS üzerinden iletişime geçer. Win32/Qhost e-posta yolu ile bile yayılabilir ve bulaştığı bilgisayarın yönetimini saldırgana teslim eder.

Son Kullanıcı Açısından Anlamı;

Tehdit, alan adları ile IP adreslerinin ilişkilerini değiştirmek amacı ile DNS ayarlarını manipüle etmeye çalışan bir Truva atı örneğidir. Genellikle etkilenen makinedeki güvenlik yazılım ım internete üzerinden güncellemeleri indirmesini engellemeye çalışır ya da yasal bir siteye yapılan bağlantı denemelerini başka zararlı bir adrese yönlendirir. Onun için nereden internete bağlandığınızın bir önemi yoktur.

8. Win32/Agent

Önceki Sıralaması: 9

Tespit Yüzdesi: 1.12%

ESET NOD32 Antivirus bu tehdidi; bulaştıkları bilgisayarlardan kullanıcı bilgilerini çalan malware ailesine dâhil olduğundan generic olarak tanımlar.

Bu malware genellikle kendini temporary (geçici) dizinlere kopyalar ve kayıt defterine, gizlice yerleştirdiği ve rastgele başka dizinlere kopyaladığı dosyalar ile ilgili kayıtlar ekler. Bu da dosya tespit edilip silinse dahi sistem her başladığında zararlı işlem tekrar yürütülecek anlamına gelir.

9. Win32/Autorun

Önceki Sıralaması: 8

Tespit Yüzdesi: 1.07%

ESET NOD32 Antivirus bu tehdidi; bulaştıkları bilgisayarlardan kullanıcı bilgilerini çalan malware ailesine dâhil olduğundan generic olarak tanımlar.

Son Kullanıcı Açısından Anlamı;

Bu malware genellikle kendini temporary (geçici) dizinlere kopyalar ve kayıt defterine, gizlice yerleştirdiği ve rastgele başka dizinlere kopyaladığı dosyalar ile ilgili kayıtlar ekler. Bu da dosya tespit edilip silinse dahi sistem her başladığında zararlı işlem tekrar yürütülecek anlamına gelir. Tespit generic olduğu için her meydana gelen tespit de detay verebilmek mümkün değildir.

10. Win32/TrojanDownloader.Swizzor.D

Önceki Sıralaması: 5

Tespit Yüzdesi: 1.03%

TrojanDownloader.Swizzor.D malware'i saldırgan tarafından bulaştığı bilgisayara yeni zararlı bileşenler indirmek için kullanılır

Swizzor.D çoğu zaman Adware indirip kurmak için kullanılır. BitTorrent gibi peer-to-peer ağları için optimizasyon aracı taklidi yapan Swizzor.D kopyalarına bilinen zararlı yazılım sitelerinde rastlanmıştır.

Son Kullanıcı Açısından Anlamı;

Swizzor etkilenen makinedeki birincil tehdit olmak zorunda değildir. Var olan bir zararlı yazılıma özel güncellenmiş bileşenleri genellikle lops.com altındaki bir adresten indirmek için kullanılır. Swizzor genellikle "server-side polymorph" (sunucu-tarafı çok şekillisi) çeşidine örnek gösterilir ve sadece birkaç gün içerisinde rastgele paketlenmiş on binlerce örneğini gördük

Güncel Olaylar

Bu ay boyunca birkaç ilginç bilişim toplantısı düzenlendi, örneğin Estonia da Pierre-Marc Bureau ve David Harley'in botnet ve anti-malware testi sunumu yaptığı (Estonia CERT ve ISOI 5), Messaging Anti-Abuse Working Group, Anti-Spyware Coalition ve daha birçok toplantı. Ne yazık ki bu toplantılar Chatham House Kuralları çerçevesinde ve Las Vegas tarzı (Las Vegas'ta olan Las Vegas'ta kalır!) yapıldığı için ayrıntılar ile ilgili detay veremiyoruz. Buna rağmen, çok önemli işler yapıldığından dolayı bu tip kapalı toplantılara özel ilgi gösterdiğimizizi bilmenizi isteriz. Biz bu toplantılara katılmaya ve sadece geleneksel antivirüs/anti-malware toplulukları hakkında değil aynı zamanda geniş anlamda güvenlik konularında da bilgi toplamaya devam edeceğiz. Geleneksel tespit sağlayan üreticilerin dünyanın geri kalanından izole kendi kafeslerinde yaşadıkları zamanların bittiğine inanıyoruz. Biz çözümün önemli bir bölümünü sizlere sunmaya devam ederken, çoklu çözümlerin ve topluluk içerisindeki ortaklığın önemini de vurgulamak isteriz.

Şu anda birkaçım z Ottawa’da, Randy Abrams, Pierre-Marc Bureau, David Harley gibi birçok konuşmacının yer aldığı ve paylaş ılmış sistemlerde data-mining, anti-malware testleri ve malware isimlendirmesi konularını içeren yıllık Virus Bulletin konferansında (1st-3rd Ekim), bulunuyor. Daha fazla bilgiye <http://www.eset.com/download/whitepapers.php> adresinden ulaşabilirsiniz.

VB konferansı anti-malware takviminde yer alan çok önemli bir olaydır ve ESET konferansın platin sponsoru olmaktan gurur duyar.

Ayrıca Virus Bulletin tarafından yapılan ve dergide yayınlanan testlerde 52. VB100 ödülünü aldığım z için mütevazı olamayacak kadar çok gururluyuz. Bu test (Windows Server 2008 platformunda gerçekleştirildi) Ekim sayısında yayınlandı. Rekabet ettiğimiz birkaç üreticinin performanslarını yüksek göstermek amacı ile VB100 istatistiklerinde birtakım sevimli tahrifler yaptıkları da gözümüzden kaçmadı ama bu bizim halen diğer tüm firmalardan daha fazla ödüle sahip olduğumuz basit gerçeğini gölgeleyemiyor. VB’nin test sürecini geliştirmesine rağmen bizim yerimizi koruyor olmamız da ayrıca gurur veriyor. Virus Bulletin testi, halen yaygın listelere odaklanmasına rağmen titiz bir test süreci olma özelliğini koruyor ve bazı üreticilerin ürünlerini teste sokmayı durdurması artık avantajlı olmamalarından kaynaklanıyor. VB testinin var olan en iyi test olduğunu iddia etmememize rağmen yine de dikkate alabileceğiniz tek sertifikasyon ve bazı çevrelere göre yarış labilecek tek alandır.

Ne yazık ki bu kadar iyi yönetilen başka bir test yok. VirusTotal sonuçlarını temel alan başka resmi ya da gayri resmi testler de var. Bahsettiğimiz bu gizli konferanslardan birinde karşı laş tğ ımız başka bir olayda ise güvenlik endüstrisinin diğer sektörlerinin de üreticinin tepki hızını ölçmek için VT sonuçlarını kullanıyor olduğunu gördük. Ne yazık ki doğrulama amacı ile VT sonuçlarının kullanılmasının çok ciddi mantıksal açıkları var. VT’ye yapılan sunuşlar on-demand tarayıcı lara ulaş ır lara kadar site tarafından doğrulanmazlar ve VT’nin kendi sonuçlarına göre sunulan dosyaların büyük bir bölümü zararlı yazılı m içermiyor. Bu dosyaların false positive ya da temiz dosya oldukları anlamına gelmez, aynı zamanda dosyaların tek başlarına tehdit olmadıkları, çalış ır lamayan bozuk exe ler oldukları gibi birçok anlama gelebilir. Bu dosyalar tüm üreticiler tarafından zararlı olarak tespit edilmezler. VirusTotal’ın bazen komut satırı tarayıcı ları ya da dar çerçeveli masaüstü ürünleri kullanması durumu iyice karış k hale getirir. Gelişmiş Davranış Analizi kullanan ürünler sitenin bu tutumu karş ısında dezavantajlı konuma düşebilirler. Aynı ürünün deęş ik sürümleri içeriğe göre deęş ik sonuçlar verebilir, VirusTotal servisini saęlayan Hispasec bu durumun farkında ve birçok kez test için uygun olmadığını belirtti. Ayrıntılı bilgi için <http://blog.hispasec.com/virustotal/22>.

ESET'in ThreatSense.Net® Teknolojisi Dünyayı Kapsıyor.

Şu sıralar hızla yaygınlaşmakta olan (In the Wild) Malware'ler (zararlı yazılım) çok geniş bir çeşitlilik ve yetenekler, üstelik kategorilere ayırabileceğimiz bu Malware'lerin bir familyaya mensup her birinin değişik varyantları dahi mevcut. Bu durum da Antivirus programınızın sürekli olarak güncellenmesinin yanı sıra her gün ortaya çıkan yeni ve bilinmeyen tehditlere karşı koruyabilmesi için, ESET Nod32 ve ESET Smart Security'de olduğu üzere gelişmiş bir sezgisel tarama özelliği gibi proaktif tehdit algılama yeteneğinin de olması gerekiyor.

Aslına bakarsanız, bu raporda yer vermemiş olmamıza rağmen ThreatSense.Net® tarafından listelenen tüm sonuçlar içerisinde, sezgisel tarama ile algılananlar tek tek algılamalara göre oldukça yüksek bir oran teşkil ediyor.

ThreatSense.Net® gelişmiş bir tehdit takip sistemi olup dünya üzerine yayılmış olan milyonlarca değişik bilgisayardan gelen yakalama sonuçlarını listeler ve gelmiş geçmiş en gelişmiş malware raporlama sistemi olduğuna inanılır. ESET iştiraki olarak hayatına başladı ve VIRUS RADAR ismini aldı (<http://www.virusradar.com>). Raporlama sistemi ve toparlanan istatistiklerin kalitesi çok geliştirildi. VIRUSRADAR'ın e-posta kökenli tehditleri takip ettiği her yerde ThreatSense.Net sisteme saldıran diğer tüm tehditler hakkında bilgiler. Bu bilgi ayarlardan raporlamayı aktifleştirmiş olan tüm ESET güvenlik ürünü kullanıcılarından (anonim olarak) toplanır ve bize malware'in tüm dünya üzerindeki yayılma hızı ve davranışı hakkında genel bir görünüm sunar. Veriler şu an için 10 milyonun üzerinde bilgisayardan toplanmaktadır ve sistem kısa zaman içerisinde 10,000 den fazla değişik tehdit ve malware ailesi hakkında bilgi topladı.