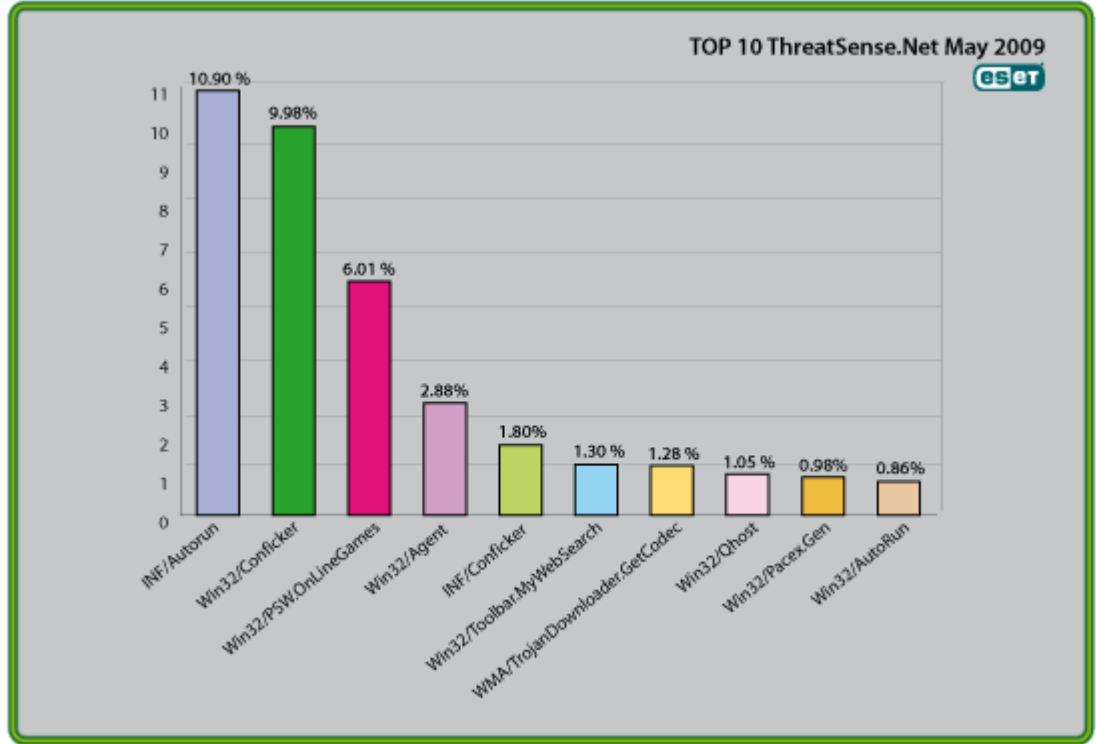




Dünya Tehdit Eğilimleri – Mayıs 2009

Bir Bakışta 2009 Mayıs Ayının ilk On Tehdidi



ESET'in gelişmiş bir Malware (zararlı yazılım) raporlama ve takip sistemi olan ThreatSense.Net® analizlerine göre bu ayın en yüksek karşılaşılan tehdidi % 10.90 ile INF/Autorun sınıfına ait.

İlk on içerisinde yaygın olarak rastlanan tehditlerle ilgili önceki durumları gibi detaylı bilgiler aşağıda verilmiştir.

1. INF/Autorun

Önceki Sıralaması: 2

Tespit Yüzdesi: 10. 90%

Bu tespit etiketi autorun. inf dosyasını kullanarak bilgisayarı risk altında bırakan birçok, çeşitli malware türünü 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 yazılımı bu malwareleri başka bir tanım altında bulunmadığı zamanlarda INF/Autorun etiketi ile sezgisel olarak tespit eder.

Son kullanıcı açısından önemi;

Çıkarılabilir aletler çok revaçtalar, INF/Autorun türünün birinci sırayı almasından da anlaşılacağı gibi malware kodlayıcıları bu durumun farkındalar ve bilgisayar kullanıcıları için büyük tehlike arz ediyor. Problemin sebebi ise şöyle;

Windows İşletim Sistemindeki varsayılan Autorun ayarı çıkarılabilir medya'ları taktığınızda autorun. inf listesindeki programları otomatik olarak başlatma görevi üstlenir. Kendilerini çıkarılabilir aygıtlara kopyalayan birçok malware vardır, programın birincil dağıtım mekanizması bu olmasa bile malware kodlayıcıları bulaşma riskini arttırabilmek için her zaman ekstra bir şeyler katarlar.

Bu mekanizmayı kullanan malware türlerinin sezgisel tarama kullanan bir güvenlik yazılımı tarafından tespit edilmesi daha kolaydır. Randy Abrams'ın bloğumuzda bahsettiği gibi (<http://www.eset.com/threat-center/blog/?p=94>) tehdidin antivirus tarafından tespit edileceğine güvenmektense Windows Autorun özelliğini kapatmak daha yerinde ve güvenli bir davranıştır.

2. Win32/Conficker

Önceki Sıralaması: 1

Tespit Yüzdesi: 9.98%

Win32/Conficker; Windows işletim sistemlerindeki bir açığı kullanarak ağ üzerinde yayılan bir solucan türüdür. RPC alt sisteminde yer alan bu açık sayesinde saldırgan geçerli kullanıcı bilgilerine ihtiyaç duymadan sisteme girebilmektedir. Sürümüne bağlı olarak güvenli olmayan paylaşımlar ve çıkarılabilir medyalar aracılığı ile de Windows'un Autorun özelliğini kullanarak yayılabilir.

Win32/Conficker svchost hizmetine bir DLL ekler. Bu tehdit önceden ayarlanmış domain isimlerine bağlanarak diğer parçalarını da indirmeye çalışır. Conficker hakkında daha

detaylı bilgiye aşağıdaki linkten ulaşabilirsiniz.

http://www.eset.eu/buxus/generate_page.php?page_id=279&lng=en.

Son kullanıcı açısından önemi;

Conficker türevlerine karşı ESET'in etkili bir tespit yöntemi bulunmasına rağmen son kullanıcıların bilgisayarlarında Kasım ayından bu yana indirilebilir durumda olan Microsoft yamasının kurulu olduğundan emin olmaları çok önemli, böylece aynı açığı kullanan diğer tehditlere karşıda önlem almış olurlar. Bu açık ile ilgili detaylı bilgiye <http://www.microsoft.com/technet/security/Bulletin/ms08-067.msp> adresinden ulaşabilirsiniz.

San Diego araştırma birimimiz Conficker sorunları hakkında <http://www.eset.com/threat-center/blog/?cat=203> adresindeki blogda detaylı bilgi vermiştir.

3. Win32/PSW.OnLineGames

Önceki Sıralaması: 3

Tespit Yüzdesi: 6.01%

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 önemi;

Bu tehdidin piyasadaki payı 2008 Eylül ayındaki büyük artışı göz önüne alındığında azalmıştır fakat halen sık rastlanmaktadır ve oyuncuların dikkatli olmaları önemlidir.

Lineage, World of Warcraft ve sanal dünya Secondlife gibi MMORPG (masif, çok eşli, çevrim içi oyunlar) katılımcılarının, sadece tacizler ve rahatsız etmeler dışında phishing (olta) ve diğer dolandırıcılık yöntemleri gibi gerçek dünyada finansal kayıplarla sonuçlanabilecek kendilerine yönelik tehditlerin farkında olmaları çok önemlidir.

ESET Malware beyin takımı bu duruma ESET Yıl-sonu Dünya Tehdit raporunda daha detaylı olarak değinmiştir. http://www.eset.com/threat-center/threat_trends/EsetGlobalThreatReport.

4. Win32/Agent

Önceki Sıralaması: 4

Tespit Yüzdesi: 2.88%

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 yerleştiği 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.

Son kullanıcı açısından önemi;

Rastgele dosya isimleri yaratmak malware türlerinin dosya ismi ile tespitini zorlaştırmak için uygulanan başka bir yöntemdir ve örnekleri yıl içerisinde birçok kez görülmüştür. Dosya ismi ile tespit bazı durumlarda işe yarayabilir fakat güvenilir bir yöntem değildir. Birincil tespit yöntemi olarak dosya isimlerini kullanan bazı anti-malware yazılımlarından uzak durmanızı tavsiye ederiz, özellikle de "Bizim ürün zararlı.dll dosyasını temizleyen ilk ve tek ürün" gibi reklam aldatmacası kullananlardan.

5. INF/Conficker

Önceki Sıralaması: 6

Tespit Yüzdesi: 1.80%

INF/Conficker, INF/Autorun tespiti ile ilintilidir: autorun.inf dosyasını Conficker'ın sonraki sürümlerini indirebilmesi amacı ile etkiler.

Son kullanıcı açısından önemi;

Son kullanıcıyı ilgilendiren yönü ise bu zararlı yazılımın daha önce anlatıldığı gibi INF/Autorun özelliğini devre dışı bırakmak için bir sebep daha olmasıdır.

6. Win32/Toolbar.MywebSearch

Önceki Sıralaması: 9

Tespit Yüzdesi: 1.30%

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

Son kullanıcı açısından önemi;

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...

7. WMA/TrojanDownloader.GetCodec

Önceki Sıralaması: 7

Tespit Yüzdesi: 1.28%

Win32/GetCodec.A ortam dosyalarını kurcalayan bir malware çeşididir. Bu Truva atı bilgisayarda bulunduğu tüm audio dosyalarını WMA türüne çevirir ve dosya başına dosyanın çalınabilmesi için “Codec” indirilmesi gerektiğini belirten ve tabii ki zararlı bir URL içeren bir başlık ekler.

WMA/TrojanDownloader.GetCodec.Gen, Win32/GetCodec.A türevleri gibi malwarelerin bulaşmasını kolaylaştıran, Wimad.N e yakın bir indirme yazılımıdır.

Son kullanıcı açısından önemi;

Zararlı dosyayı yeni bir Video Codec’miş gibi yaymak birçok malware yazarı ve dağıtıcısı tarafından uzun yıllardır kullanıla gelen bir sosyal mühendislik türüdür. Kurban yararlı ya da ilginç bir şey yaptığını zannederek zararlı kodu çalıştırması için ayartılır. Yeni çıkan bir Codec’in gerçek, resmi ya da Truva Atı olup olmadığını anlamak için uygulanan basit ve evrensel bir test olmadığından sizin talep etmediğiniz davetler ile bir şeyler indirme konusunda tedbirli ve seçici davranmanızı tavsiye ederiz. Araç güvenilir bir siteden geliyor gibi görünse de gerçek olup olmadığını elinizden geldiğince sorgulayın. (<http://www.eset.com/threat-center/blog/?p=170>)

8. Win32/Qhost

Önceki Sıralaması: 8

Tespit Yüzdesi: 1.05%

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 önemi;

Tehdit, alan adları ile IP adreslerinin ilişkilerini değiştirmek amacı ile DNS ayarlarını manipüle etmeye çalışan bir Truva atı örneğidir. Genellikle etkilenen makinedeki güvenlik yazılımının internete üzerinden güncellemeleri indirmesini engellemeye çalışır ya da yasal bir siteye yapılan bağlantı denemelerini başka zararlı bir adrese yönlendirir. Qhost'un amacı genellikle MITM (Man In The Middle) saldırısı gerçekleştirmektir. Bu tip saldırılarda, saldırgan iki taraf arasındaki iletiyi tarafların haberi olmadan okuyabilir, ekleme yapabilir ve değiştirebilir, nereden internete bağlandığının bir önemi yoktur.

9. Win32/Pacex.Gen

Önceki Sıralaması: 16

Tespit Yüzdesi: 0. 98%

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

Son kullanıcı açısından önemi;

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 oranımız, gözlemlenen bu tehdidin maskesini indiriyor.

10. Win32/Autorun

Önceki Sıralaması: 10

Tespit Yüzdesi: 0. 86%

'AutoRun' etiketi ile tanımlanan tehditler Autorun.INF dosyasını kullanmaları ile bilinirler. Bu dosya çıkarılabilir medyanın bilgisayara takılması ile otomatik olarak çalıştırılabilmesini sağlar.

Son kullanıcı açısından önemi;

Çıkarılabilir aletler çok revaçtalar, INF/Autorun türünün birinci sırayı almasından da anlaşılacağı gibi malware kodlayıcıları bu durumun farkındalar ve bilgisayar kullanıcıları için büyük tehlike arz ediyor. Problemin sebebi ise şöyle;

Windows İşletim Sistemindeki varsayılan Autorun ayarı çıkarılabilir medya'ları taktığınızda autorun. inf listesindeki programları otomatik olarak başlatma görevi üstlenir. Kendilerini çıkarılabilir aygıtlara kopyalayan birçok malware vardır, programın birincil dağıtım mekanizması bu olmasa bile malware kodlayıcıları bulaşma riskini arttırabilmek için her zaman ekstra bir şeyler katarlar.

Bu mekanizmayı kullanan malware türlerinin sezgisel tarama kullanan bir güvenlik yazılımı tarafından tespit edilmesi daha kolaydır. Randy Abrams'ın bloğumuzda bahsettiği gibi (<http://www.eset.com/threat-center/blog/?p=94>) tehdidin antivirus tarafından tespit edileceğine güvenmektense Windows Autorun özelliğini kapatmak daha yerinde ve güvenli bir davranıştır.