

Zero-day

Birçok üründe karşılaştığımız bir özellik Zero-day Protection. Defalarca yanlış anlaşıldığını gördüğüm Zero-day ve Zero-day protection terimlerinin anlamlarını kapsamlıca anlatmaya çalışacağım. Terimin zihinlere yerleşmesi için "Sıfır Gün" ya da "Sıfırıncı Gün" gibi Türkçe tercüme yerine terimi olduğu gibi kullanacağım.

Zero-day atakları

Güvenlik açıkları bilgi güvenliği uzmanları tarafından bulunur. Bu noktada güvenlik açığının bulan kişinin rengi önemlidir.

Beyaz şapkalılar genellikle kurumsal şirketlerde çalışır. Özellikle güvenlik ürünü geliştiren şirketler, güvenlik açığı tespit etme konusunda yarış halindedirler. Ne kadar çok açık bulurlarsa, satış potansiyeli o kadar artar. Bu şirketlerde çalışan araştırmacı teknik uzmanlar beyaz şapkalıdır (istisnalar kaideyi bozmaz). Bir beyaz şapkalı, bulduğu açığın detaylarını ürün üreticisine gönderir. Üretici açığı testlerden sonra doğrular ve çözüm için yama geliştirir. Yama geliştirme bazen 5-10 gün bazen 250-300 gün sürebilir. Bu tamamı ile açığın teknik altyapısıyla ilgili bir durumdur. www.eeye.com sitesinden bazı açıklar için yama geliştirme sürelerini görebilirsiniz.

Siyah şapkalılar pek de iyi niyetli sayılmazlar. Buldukları açıkları hiçbir kuruma bildirmez, kendileri kullanırlar. Black Community diye tabir edilen gruplar arasında bu zaaflara ait bilgilerin elden ele dolaştığı bilinmektedir. Özellikle FBI ve CERT gibi kurumlar "Black Community" elinde bulunan güvenlik açıklarını tespit etmek için hemen hemen dünyanın her yerinde internet trafiğini gerçek zamanlı olarak dinlemektedir.

SQL Injection, Directory Traversal ya da Authentication Bypass gibi açıklar ek bir uygulama geliştirmeye gerek duyulmaksızın kolayca kullanılabilir. Ancak birçok açık türünde, açığı kullanarak sistemlere saldıran küçük programlar geliştirmek gerekir. Bu yazılımlara "exploit" denir.

Pattern-Matching teknolojisiyle çalışan güvenlik ürünleri (Antivirus, IDS/IPS, Secure Content Management vs.) atakları tespit edebilmek için imza güncellemesine ihtiyaç duyar. Bu nedenle açığın bir beyaz şapkalı tarafından bulunması ve üreticilerin güvenlik güncellemesi yapması zorunludur. Güncelleme yapılan kadar sistemler risk altındadır. Hatta birçok internet korsanı hedef seçtiği sisteme ait bir güvenlik açığının duyurulması için pusuya yatar. Açık duyurulduktan hemen sonra ilgili exploit'i bulmaya ya da geliştirmeye çalışırlar.

Zero-day, açığın bulunduğu ilk günü ifade eder. Açık her kim tarafından bulunursa bulunsun, dünyadaki tüm sistemler bu açık karşısında teorik olarak korumasızdır. Kısaca sistemi koruma altına almak için ya üreticinin yama geliştirmesini bekleyeceğiz ya da güvenlik ürünü üreticisinin ilgili imza

güncellemesini bekleyeceğiz. Her iki durumda da Zero-day atak riski altındayız demektir. Özellikle 2000-2003 yılları arasında Slammer, Code Red ve Nachi gibi internet solucanlarına dünyanın en büyük sistemleri bile karşı koyamadı. McAfee AVERT laboratuvarı raporlarına göre sadece Slammer'ın yayılmaya başladığı ilk saat içerisinde 100.000 sunucuya bulaştığı tahmin ediliyor.

Konumuzun temel sorusu şudur;

Şu an dünyanın diğer ucunda 15 yaşındaki bir çocuğun geliştirdiği internet solucanı ya da bir exploit'e karşı sistemimi nasıl koruyabilirim?

Cevap: Zero-day Protection.

Zero-day protection

Zero-day Protection terimi aslen sunucu tabanlı atak engelleme sistemi (HIPS) geliştiren bir şirket tarafından ortaya çıkarılmıştır. Şirketin söylemi kendi ürünlerinin bilinen atakların yanı sıra bilinmeyen ataklara karşı da güvenlik sağladığıdır. Bu terim günümüzde neredeyse tüm ağ tabanlı (NIPS) ve sunucu tabanlı (HIPS) atak engelleme sistemi geliştiren şirketlerce kullanılıyor. Şimdi, her iki ürün grubu açısından da Zero-day Protection koruma tekniklerini açıklayalım.

Network Intrusion Prevention System (NIPS)

NIPS ürünleri temelde 3 konuda güvenlik sağlar. Bilinen ataklar, bilinmeyen ataklar ve DoS/DDoS atakları. Konumuz Zero-day olduğuna göre sadece bilinmeyen ataklara bakacağız.

Zero-day Protection için NIPS ürünlerinde kullanılan temel teknolojinin adı Protocol Anomaly'dir. Aslında bu teknik Protocol Anomaly, Application Payload Anomaly ve Statistical Anomaly adında 3 önemli ve birbirinden bağımsız özelliğe sahiptir. Statistical Anomaly daha ziyade DoS/DDoS ataklarına karşı geliştirilmiş bir çözüm olduğu için hiç üzerinde durmuyorum. Gelelim diğerlerine...

Bir NIPS ürünüde bulunan Protocol Anomaly özelliği yüzlerce protokolü çözer ve analiz eder. Çünkü atakların büyük kısmı protokol bozukluklarına neden olur. Böylece Pattern-Matching tekniğinin gereksinimi olan imza güncellemesine ihtiyaç duymadan birçok bilinmeyen atak engellenebilir. Örnek vermek gerekirse Protocol Anomaly ile donatılmış birçok NIPS ürünü Slammer ve Code Red gibi bilinmeyen ataklara karşı sistemleri korumayı başarmışlardır. Application Payload Anomaly özelliği ise özellikle Shellcode bazlı atakla-



ra karşı koymak için geliştirilmiştir. Oldukça başarılı örnekleri bulunan bu özelliklerle birçok atak, ağ seviyesinde durdurulabilir. Shellcode atakları sisteme ciddi zararlar verebilecek atak tipleridir, bu sebeple Application Payload Anomaly tekniğinin başarısı oldukça önemlidir.

Bu arada özel bir not düşmek istiyorum. Çoğu yerde Polymorphic türev ataklarında NIPS ürünlerinin yetersiz olduğu söylenir. ADMutate yazıp Google'da aratırsanız bazı makaleler bulabilirsiniz (Bulacağınız makalelerin büyük kısmı 2002 yılına ait olacaktır). Varsayım, özel yöntemlerle şifrelenmiş veya değiştirilmiş exploit'lerin NIPS tarafından tespit edilmeden sisteme gönderilebileceğidir. İşte bu konuda Application Payload Anomaly özelliği bize koruma sağlar. NSS NIPS raporlarını incerseniz IPS Evasion (IPS atlama) testlerinde ADMutate gibi bilinen polymorphic ataklara karşı hemen hemen tüm NIPS ürünlerinin koruma sağladığını görebilirsiniz (www.nss.co.uk). Gerçi açıkça söylemek gerekir ki bu testlerin sonuçlarında dikkat edilmesi gereken ADMutate ataklarının engellenip engellenmediği değil, "decode" edilip edilmediğidir. Nitekim "mutated" dediğimiz değiştirilmiş yapıda olan atakların tespit edilebilmesi için NIPS üreticileri yoğun mesai harcamaktalar. Decode edilemeyen bir trafiğin içinde atak aramak mümkün değil. Bazı ürünler decode edemediği trafiği otomatik olarak engileyebilir ancak bu da False Positive dediğimiz hatalı atak tespiti oranını arttıracaktır. Profesyonel bilgi güvenliği uzmanları için bu hayati bir konudur. Yazı içeriği ile direkt ilgisi olmadığından daha fazla detay veremeyeceğim, ilgilenenler benimle temasa geçebilir.

Host Intrusion Prevention System (HIPS)

Hiç şüphe yok ki Zero-day ataklarına karşı NIPS'in koruma kalkanı HIPS'e göre daha zayıftır.

HIPS ürünlerinin kullandığı teknikleri tek tek açıklamaya kalksam Beyaz Şapka'da 10 sayfa yazı yazmam gerekir. Burada birkaç önemli noktaya değinmekle yetinmek zorunda kalacağım.

HIPS ürünlerinden bazıları Pattern-Matching tekniğine de sahiptir ancak onları değerli kılan Zero-day Protection özellikleridir. Bunlardan en önemlisi de hiç şüphesiz Buffer Overrun Protection özelliğidir.

Buffer Overrun açıkları sistemlerin tüm işlevlerini uzaktan ele geçirmeye neden olur. Çünkü bu ataklar işletim sisteminin adreslemediği hafıza bölümlerinde çalışır, bu sayede işletim sistemi üzerinde bulunan güvenlik tanımlarına tabi tutulamaz. HIPS ürünlerinin büyük kısmı Buffer taşmalarını otomatik olarak algılar ve engeller. Atanın bilinip bilinmemesinin önemi olmadığı gibi kaynağının lokal ya da remote olması da önemli değildir. HIPS her koşulda koruma sağlayacaktır.

Diğer önemli bir koruma tekniği de hafızaya ya da işletim sistemine yapılacak Injection ataklarına karşıdır. Burada sözü edilen Injection atağının "SQL Injection" ile hiçbir ilgisi yoktur. Sanırım bu konuda verebileceğim en basit örnek metasploit

tarafından kullanılan "VNC Injection" örneği olacak. Sistemde bulunan bir açığı kullanarak kurban sisteme VNC Server yazılımına ait DLL'i gönderip bize geri bağlantı yapmasını sağlayabiliyoruz. Kısaca hack ettiğimiz sistemin ekran görüntüsünü olduğu gibi hem de yönetici yetkileriyle alabiliyoruz. Çoğu durumda DLL Injection gibi teknikler Buffer Overrun gibi başka zaafarla tetiklenmek zorundadır. Temel olarak HIPS ürünleri dışarıdan işletim sistemine ya da direkt sistem hafızasına çalıştırılabilir bir uygulama sokulmasını engelleyebilir. Bu sayede sisteminizde bir güvenlik açığı bulunsa bile 'hack' girişimi başarısız olacaktır.

HIPS ürünlerinin anlatılmadan geçilemeyecek diğer bir özelliği de Resource Protection özelliğidir. Kritik dosyalar, dizinler ve Windows Registry kayıtları kesin olarak koruma altına alınabilir. Aslında işletim sisteminin de kendi içerisinde erişim denetimi özelliği vardır. Ancak yukarıda anlattığımız gibi bazı ataklarda işletim sistemi erişim denetimi özellikleri kolayca atlanabilir.

HIPS ürünleri atak olsun olmasın, belirtilen kaynakları kesin koruma altına alır. Örneğin yeni yayılmaya başlamış bir internet solucanı bütün sistemlere sızabilir (Slammer, Code Red vs..) ancak HIPS tarafından korunan sistemler bu ataklardan zarar görmeyecektir. Hatta HIPS yöneticisi izin vermezse, sistem yöneticisi bile koruma altındaki kayıtları değiştiremez.

Sonuç

NIPS ve HIPS ürünleri %100 koruma sağlar mı?

Bu soruya ne güvenlik uzmanları ne de ürün üreticileri evet cevabını veremez. Hiç şüphe yok ki, NIPS konusunda kısaca bahsettiğim polymorphic atak tipleri gibi, her geçen gün yeni atak metotları türeyecektir ve bunların bir bölümü NIPS ve HIPS ürünleri kullanılıyor olmasına rağmen etkili olacaktır. Ancak NIPS ve HIPS üreticileri bu gelişmeler karşısında uyumuyorlar, ürünlerini ve teknolojilerini sürekli geliştiriyorlar.

Öyleyse NIPS/HIPS projesi yaparken üzerinde durmamız gereken en önemli konu ürün seçimi. Ürünü seçerken çok küçük ayrıntılara dikkat etmemiz ve üreticinin IPS teknikleri üzerindeki vizyonunu anlamamız gerekiyor. Bunun yanı sıra ürünlerin doğru yapılandırılması da çok önemli. Bu noktada atak tiplerini iyi tanıyan uzmanlardan fikir veya destek alınması son derece önemli. Nitekim bahsettiğim koruma tekniklerinin bazıları varsayılan olarak aktif durumda gelmiyor. Teknik özelliklerin iyice incelenerek, adım adım devreye alınması ve test edilmesi gerekiyor. Bu aşamada yapılacak yapılandırma hataları pahalıya mal olabilir.

Kaynaklar:

http://www.mcafee.com/us/local_content/white_papers/wp_ddt_anomaly.pdf

<http://www.nss.co.uk/grouptests/ips/edition3/pdf/IPSED3-0601-MA.pdf>

<http://www.metasploit.org/projects/Framework/screenshots.html>

<http://www.securityfocus.com/infocus/1670>