Babana Bile Güvenme

written by Mert SARICA | 11 July 2012
For English, click here.

Günümüzün imza tabanlı teknolojilerinden biri olan Antivirüs yazılımlarına körü körüne güvenmekte, onların da birer yazılım olduğunu ve her yazılım gibi onların da hataları, zafiyetleri olabileceğini çoğunlukla göz ardı etmekteyiz. Halbuki Antivirüs dediğimiz yazılımlar aslında belli bir imza setine göre (sezgisel tarama hariç) hedef dosyaları incelemekte ve doğası gereği hedef dosya üzerinde yapılan basit değişikliklerden (misal kodlama/encode, paketleme) sistem üzerinde yapılan daha karmaşık değişikliklere (misal tasarımsal hataları istismar etme) kadar çeşitli yöntemler ile çoğu zaman kolaylıkla atlatılmaktadırlar. Çoğunlukla kodlama ile atlatma yöntemlerine sıkça rastladığımız bu günlerde tasarımsal veya mimari hatalardan, zayıflıklardan faydalanarak atlatma yöntemlerine çok sık rastlanmamaktadır.

Geçtiğimiz günlerde zararlı bir yazılım analizi gerçekleştirirken Mcafee VirusScan Enterprise Antivirus yazılımında raporlamadan zararlı yazılım tespitine kadar iki önemli noktada tutarsız sonuçlar üretmesine neden olan bir hata,zafiyet keşfettim. Yaptığım incelemeler neticesinde bu hatanın/zafiyetin, antivirus yazılımında bulunan ayrıştırıcının (parser) dosyaları incelerken özel bir satırı dikkate almasından kaynaklandığını düşünüyorum.

Hataya neden olan bu gizemli satır nedir diye soracak olursanız, HTTP protokülüne ait bir başlık (content-disposition ve filename) ile ZIP dosyasının başlığının (header) birleşiminden oluşan bir satır olduğunu söyleyebilirim;
Content-Disposition: inline; filename=setup.exe….PK……..

Normalde web ile ilişkili dosyaları (misal html) bu şekilde ayrıştırmasını beklediğimiz Antivirus yazılımı her ne hikmetse incelediği tüm dosyalarda da bu gizemli satırı dikkate alarak dosya üzerinde inceleme gerçekleştirmektedir. Durum böyle olunca da bu gizemli satırı kullanarak zararlı bir yazılımı bu antivirüs yazılımından kaçırmak, hatalı aksiyon raporu üretmesini (sildim dediği bir zararlı yazılımı aslında silememesi) sağlamak ve durum raporunda sahte dosya ismi göstermesini sağlamak mümkün olmaktadır.

Bu hatanın, zafiyetin istismar edilebileceği senaryolardan bazılarının üzerinden kısaca geçecek olursak;

- Örneğin internetten temin ettiğimiz o meşhur Aurora istismar kodunun başına bu sihirli satırı ekleyip taratacak olursak antivirus yazılımı tarafından tespit edilemediğini görebiliyoruz.

1. Bunun dışında iki adet zararlı yazılım ile gerçekleştirebileceğimiz başka bir senaryoda ise zararlı yazılımlardan bir tanesi Contagio Malware Dump sitesinden temin ettiğimiz APT_1104statment.pdf zararlı PDF dosyası diğeri ise Honeypot sistemi üzerinden temin ettiğimiz ve Blackhole istismar kiti tarafından kullanılan 55993.jar zararlı JAR (CVE-2012-0507) dosyası olsun. Her iki dosyayı da ayrı ayrı bu antivirus yazılımı ile taratacak olursak antivirus yazılımın başarıyla bu zararlı yazılımları tespit ettiğini görebiliyoruz ancak sihirli satırı JAR dosyasının başına ekledikten ve iki dosyayı tek bir zip dosyası haline çevirdikten sonra taratacak olursak sadece 55993.jar dosyasının tespit edildiğini diğer dosyanın ise tespit edilemediğini görebiliyoruz. Ayrıca her ne kadar antivirüs yazılımı bize 55993.jar dosyasının silinmiş olduğunu söylemiş olsa da zip dosyasının içine baktığımızda aslında dosyanın birebir orada olduğunu görebiliyoruz.

    - Son olarak Contagio Malware Dump sitesinden temin ettiğimiz APT_1104statment.pdf zararlı PDF dosyasının başına sihirli satırımızı koyacak ve filename kısmına istediğimiz değeri belirtecek olursak tarama sonucunda zararlı yazılımın adının dosya adından farklı olarak görüntülendiğini ve raporlandığını görebiliyoruz.

Özellikle istismar kitlerinin (exploit kits) sıfırıncı gün zafiyetlerini istismar ettiği, güçlü gizleme (obfuscation) yöntemlerine başvurarak kendilerini imza tabanlı saldırı tespit ve zararlı yazılım tespit teknolojilerden başarıyla gizleyebildiği şu günlerde, yazılımlarda yapılan bu tür basit hatalar da, kullanıcıların kolaylıkla kandırılmasına ve zararlı yazılımların sistemlere daha kolay bulaşmasına imkan tanıyabilmektedir. Tavsiyem sadece ve sadece istemci sistemlerinde çalışan imza tabanlı teknolojilere güvenmek yerine ilave olarak ağ trafiğinin gözlenmesine yönelik modern teknolojilerden de (kum havuzu analizi gerçekleştirebilen ağ güvenlik izleme cihazları) faydalanılması olacaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…