Bellek Analizi ile Zararlı Yazılım Analizi

written by Mert SARICA | 26 Aralık, 2011

Yine bir gün twitter.com/hack4career hesabından duyurulan hack edilmiş ve/veya zararlı yazılım barındıran web sitelerine göz atarken gün aşırı tespit edilen, çoğunlukla iki harften oluşan zararlı yazılımlar (aa.exe, bb.exe vb.) ve bunları barındıran IP adresleri dikkatimi çekti. IP adreslerinden güncel olanını Google arama motoru üzerinde arattığımda malc0de.com isimli bir web sitesi ile karşılaştım. Benim de ilk defa karşılaştığım bu sitenin kuruluş amacının, aynı zararlı yazılımları barındıran ve yayan farklı web sitelerini birbirleriyle ilişkilendiren bir veritabanı olduğunu öğrendim.

> Bu veritabanı, üzerinde ülke bazlı ve ASN bazlı (Autonomous System Name) arama yapılabiliyor olması sayesinde zararlı yazılım analistlerinden güvenli barındırma hizmeti arayanlara kadar birçok kişi tarafından kullanılabilir.

ggg.exe uzantılı dosyayı barındıran ASN'e yönelik arama yaptığımda benzer isimli zararlı yazılımların 2011 yılının Ocak ayından bu yana aynı ASN üzerinde tespit ediliyor olması ve tespit edilen zararlı yazılımların sayısının 300'ü aşkın olması merakımı cezbetti ve deneme yanılma ile hhh.exe adı altında tespit ettiğim zararlı yazılımı kısaca incelemeye karar verdim.

Bu defa daha önce gerçekleştirmiş olduğum alışılagelmiş analizlerin aksine zararlı yazılımın çalıştığı sistemin belleğini diske kaydederek bellek (memory) analizi gerçekleştirmeye karar verdim.

> Adli bilişimde bellek analizi (memory forensic) denilince akla gelen ilk araç Volatility'dir. Aslında araç dersek haksızlık etmiş olabiliriz çünkü işin aslı Volatility, Python ile yazılmış birçok araçtan oluşan bir çatıdır (framework). Volatility ile diske kayıt edilmiş (dump) olan bellek dosyasını analiz ederek sistem üzerinde çalışan programlardan, ağ bağlantılarına, yüklü olan DLL'lerden, kayıt defterinde (registry) yer alan anahtarlara göz atmaya kadar hedef sistem ile ilgili olan birçok işlem gerçekleştirebilirsiniz.
>
> Volatility 2.0 sürümü ile Windows XP SP2/SP3, Windows 2003 SP0/SP1/SP2, Vista SP0/SP1/SP2, Windows 2008 SP1/SP2 ve Windows 7 SP0/SP1 sistem görüntülerini (image) analiz edilebilmektedir.
>
> Volatility ile analiz edeceğimiz bellek dosyasını oluşturmak için

öncelikle hedef sistem üzerinde MoonSols firması tarafından geliştirilen DumpIt programının çalıştırılması gerekmektedir.

İlk iş olarak hhh.exe dosyasını Windows 7 üzerinde çalışan Windows XP SP3 sistemine kopyaladıktan sonra Windows 7 üzerinde Wireshark aracını çalıştırarak zararlı yazılım tarafından hedef sistem üzerinde üretilmesi muhtemel olan trafiği kayıt altına almasını sağladım. hhh.exe dosyası üzerinde yer alan üstveriye (metadata) baktığımda Logitech firması tarafından geliştirilmiş bir araçmış gibi kendini tanımladığını gördüm. Ardından hhh.exe isimli zararlı yazılımı hedef sistem üzerinde çalıştırdıktan sonra daha önce hedef sisteme kopyalamış olduğumu DumpIt aracını çalıştırarak sistemin belleğini diske kayıt etmesini sağladım.

Zararlı yazılımı çalıştırır çalıştırmaz Wireshark aracı üzerinde HTTP ve IRC trafiği oluştuğunu gördüm ve bir IRC istemci yazılımı ile tespit edilen bu IRC sunucusuna bağlandım. Sunucuya bağlandığımda kanalın boş olması, botların ifşa olmasını engelleme adına özel olarak geliştirilmiş/modifiye edilmiş bir irc sunucusu olduğuna işaret ediyordu. Botun IRC kanalına giriş yapar yapmaz, internete çıkış yaptığı ip adres bloğunun 445. bağlantı noktasını otomatik olarak taramaya (port scan) başlaması da gözümden kaçmadı. Wireshark üzerindeki HTTP paketlerini incelediğimde ise botun NAT'lanmış IP adresini öğrenebilmek için bir kaç sayfaya bağlanmaya çalıştığını farkettim.

Zararlı yazılım ile ilgili daha fazla bilgi almak için Volatility ile bellek dosyasını incelemeye başladım.

İlk olarak PSLIST komutu ile sistem üzerinde çalışan işlemleri (process) listeledim ve çalıştırılma zamanına göre zararlı yazılımın sistem üzerinde 2888 PID'sine sahip indek.exe adı altında çalıştığını gördüm.

DLLLIST komutu ile zararlı yazılım tarafından yüklenen DLL dosyalarını listelediğimde ise urlmon.dll ve cryptdll.dll dosyaları şüpheli duruyordu.

CONNSCAN komutu ile sistem üzerindeki aktif ağ bağlantılarını listelediğimde ise 2888 PID'si ile çok sayıda bağlantı kurulduğunu gördüm.

PROCEXEDUMP komutu ile indek.exe yazılımına ait olan belleği diske kaydettikten sonra strings ve IDA PRO programları ile incelediğimde ise bu zararlı yazılımın SDBOT'ın bir varyantı olduğunu kolayca anladım.

Son olarak zararlı yazılım üzerinde yer alan zaman damgasına baktığımda ise SDBOT varyantının hemen hemen hergün güncellenip derlendiği sonucu ortaya çıkıyordu.

Görüldüğü üzere bellek analizi ile zararlı yazılımlar, dinamik analiz kadar olmasa da rahatlıkla analiz edilebilir ve yeterli bir elde edilebilinir. Özellikle bu yazıda değinmediğim diğer Volatility komutlarına (malfind, gdt, apihooks, idt, vb.) göz atacak olursanız bellek analizi ile rootkit yazılımlarını dahi tespit etmeniz mümkün olabilir.

Bir sonraki yazıda görüşmek dileğiyle yeni yılın herkese sağlık, mutluluk ve bol kazanç getirmesini dilerim.