Siber Takip

written by Mert SARICA | 9 Haziran, 2010

Aslında bu haftaki yazım için Linux işletim sistemi üzerinde zararlı kod analizi ile ilgili birşeyler karalamaya karar vermiştim. İncelemek için örnek rootkit benzeri zararlı bir kod arıyordum fakat daha sonra rootkit yerine zombi bot amacıyla kullanılan zararlı bir kod incelemenin daha faydalı olacağını düşünerek aramaya koyuldum. Google arama motorunda bir kaç anahtar kelime kullanarak arama gerçekleştirirken rotayı Türkçe sitelere çevirdim ve bir kaç sorgu sonrasında "botnet paylaşım portalı" anahtarı kelimesi ile arama yaptığımda, içerik olarak dikkatimi çeken ve bir foruma sahip olan web adresi ile karşılaştım. Foruma Firefox internet tarayıcısı ile bağlandığımda 404 hata mesajı ile karşılaştım. Ana sayfayı ziyaret ettiğimde ise karşıma pornografik görsel içeriğe sahip bir sayfa çıktı ve akabinde Java'nın güvenlik uyarısı ile karşılaştım. Java uyarısı bana dijital imzası doğrulanamayan bir java kodunu çalıştırmak isteyip istemediğimi soruyordu ve işin ilginç yanı sitedeki direktifler kodu çalıştırmam yönündeydi. Ana sayfaya Internet Explorer internet tarayıcısı ile bağlandığımda ise bu defa karşıma öncelikle ActiveX eklenti yükleme uyarısı daha sonra ise Java güvenlik uyarısı çıktı.

Sayfanın kaynak kodunu incelediğimde ilk olarak unicode karakterlerden oluşan karakter dizisi daha sonra ise Java class dosyası ve image.exe dosyasını içeren web adresi dikkatimi çekmişti.

İlk iş olarak unicode karakterleri kaldırarak tüm hex değerleri hex editöre kopyalarak stringleri incelemeye başladım ve yüklenmesi önerilen Activex'in bir downloader olduğunu ve indirilecek uygulama olarakta image.exe dosyasının parametre olarak belirtildiğini farkettim. Ardından Inico.class dosyasını decompile ederek içeriğine bakmaya karar verdim ve yine aynı şekilde url parametresinde yer alan image.exe dosyasının indirilip çalıştırılmak üzere kodlandığını gördüm.

Madem image.exe dosyasının bu kadar indirilmesi isteniyor, art niyetli kişi veya kişileri kırmayarak image.exe dosyasını indirip göz atmaya karar verdim. Dosya iner inmez ikonun sahte olduğu dikkatimi çekti.

Dosyanın özelliklerine baktığımda yazar bilgisinde sn0x yazdığını gördüm. Hex

editör ile dosyaya göz attığımda ise winini.exe stringi dikkatimi çekti. Snox ve winini.exe anahtar kelimelerini Google arama motorunda arattığımda ise dosyanın şifreleme programı ile şifrelendiği ve trojan olma ihtimalinin yüksek olduğu anlaşılıyordu.

Dosyayı Immunity Debugger ile çalıştırdığımda geçerli bir PE dosyası olmadığı hatasını aldım. Dosyanın bozuk olma ihtimali olduğu gibi sanal makinada çalışmamak üzere tasarlanmış olma ihtimalide mevcuttu fakat bu yazımdaki amaç programı hazırlayan korsan hakkında bilgi edinmek olduğu için bu konunun üzerine eğilmedim.

Bunun yerine bu şekilde tasarlanmış benzer başka bir site olup olmadığı konusunda Google arama moturunda arama yapmaya karar verdim fakat öncelikle arama için güzel bir anahtar kelimeye ihtiyacım vardı. Sayfanın kaynak kodunda yer alan başlık (title) bilgisi bunun için yeterliydi. Başlık (title) bilgisinde yer alan web sitesi ve “Forra” kelimesi, programı hazırlayan kişinin rumuzu hakkında az çok bilgi veriyordu. Bu başlık bilgisi ile arama yaptığımda karşıma benzer bir şekilde tasarlanmış başka bir sayfa hemen çıkıverdi.

Bu sayfayı Internet exporer internet tarayıcısı ile ziyaret ettiğimde ise sadece Java güvenlik uyarısı ile karşılaştım, ActiveX eklentisi sayfanın kaynak kodunda yer almıyordu. Muhtemelen bu sayfa ilk ziyaret ettiğim sayfadan daha önce hazırlanmıştı.

Bu sayfanın kaynak koduna baktığımda ise bu defa svchost.exe dosyasının yer aldığı bir adres olduğunu gördüm. Bu dosyanın PE başlık bilgisini incelediğimde dosyanın 10 Nisan 2010 tarih damgasına sahip olduğunu gördüm. Image.exe dosyasının tarih damgası ise 29 Mayıs 2010 tarihini gösteriyordu. Bu bilgiler doğrultusunda ilk ziyaret ettiğim sayfanın daha güncel olduğunu teyit etmiş oldum. Svchost.exe dosyasını hex editör ile incelediğimde son satırda yer alan e-posta adresi ve potansiyel e-posta şifresi dikkatimi çekti.

Bu e-posta adresine belirtilen şifre ile giriş yapmayı denediğimde başarılı olamadım fakat kullanıcı adının sonunda yer alan 0045 bilgisi bu zamana dek bu kişinin 45 tane kullanıcı adı kayıt etmiş ve her dosya için yeni bir e-posta adresi kullanmış olma ihtimalini ortaya çıkartmıştı. Rastgele gerçekleştirdiğim bir kaç giriş denemesi sonrasında 0030 ile giriş yapabildim ve bu kişinin Facebook üzerinde hesap yarattığını ve muhtemelen bu hesap ile Facebook üzerinden insanları kandırarak bu iki sayfadan birini ziyaret etmelerini ve zararlı programı çalıştırmalarını sağlamıştı.

Sonuç olarak amacınız size zarar veren birinin izini sürmek ve kanıt toplamak ise sizde bu veya benzer şekillerde biraz gayret ile bunu başarabilirsiniz.

Bunun dışında uyarı olarak doğruluğundan emin olmadığınız bir Activex eklentisini veya Java kodunu çalıştırmadan önce çok çok iyi düşünmenizi öneririm aksi durumda art niyetli kişilere ait bot ağının bir parçası olabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle…