Zararlı Yazılım Analisti Olmak…

written by Mert SARICA | 5 October 2011

Son yıllarda Windows işletim sistemini hedef alan Zeus, SpyEye, TDL gibi hatrı sayılır zararlı yazılımlara manşetlerde sıkça rastlıyorduk. Daha sonra o çok güvenli Mac OS X işletim sisteminin kullanım oranının artış göstermesi ile (bunun en büyük nedenlerinden biri de Mac OS X'e zararlı yazılım bulaşmaz yanılgısı olsa gerek) bu sisteme yönelik geliştirilen zararlı yazılımlar da manşetlerde yerini birer birer almaya başladı. Gün geldi tweet atmaktan internette sörf yapmaya, e-posta okumaktan bankacılık işlemleri gerçekleştirmeye kadar bir çok alanda ihtiyaçlarımızı karşılayabilen, modern işletim sistemleri ile güçlendirilmiş olan akıllı mobil cihazlar için geliştirilen zararlı yazılımlar manşetleri süslemeye başladı. Peki bilgi hırsızlığı için geliştirilen zararlı yazılımlar neden bu kadar revaçta ?

Ünlü bir banka soyguncusu olan Willie Sutton'e "Neden banka soyuyorsunuz ?" diye bir soru yönelten muhabirin aldığı "Çünkü para orada" yanıtını günümüze uyarlar ve "Neden zararlı yazılım geliştiriyorsunuz?" diye bir soru soracak olsaydık alacağımız yanıt şüphesiz "Çünkü finansal getirisi çok yüksek" olurdu ve ilk sorduğumuz sorunun da yanıtını almış olurduk.

Öyle bir dünyada yaşıyoruz ki hiç bir zaman kansere, aidse ve diğer ölümcül hastalıklara çare bulunmayacağına sadece bu hastalıkların ilerlemesini engelleyen, kontrol altında tutan pahalı ilaçların piyasada olacağına inanıyorum. Bilgi/Bilişim güvenliği sektörünü de aynı şekilde düşünüyorum. Hiç bir zaman çok güvenli bir işletim sistemi tasarlanmayacak veya bir antivirüs yazılımı tüm zararlı yazılımları tespit ediyor veya sisteme bulaşmasını engelliyor olmayacak. Durum böyle olunca da nasıl hastalıkların bulaşmasını engellemek, tedavi etmekten daha kolay ise aynı şekilde zararlı yazılımların da sistemlere bulaşmasını engellemek, sistemlerden kaldırmaktan daha kolay olmaya devam edecek. Zararlı yazılımlar ha bulaştı ha bulaşacak derken kurumlar daha fazla zararlı yazılım analistine veya bu beceriye sahip çalışanları istihdam etmeye başlayacak ve bu sayede bu alanda uzmanlaşmak isteyenler, bu işten keyif alanlar için zararlı yazılım analizi hobi olmaktan çıkarak mesleklerinin bir parçası haline dönüşecektir. Özellikle APT'lerin dev kurumları hedef aldığı son aylarda kendi personeli ile zararlı yazılım

analizi yapabilen bir kurum olmanın getirisi (3. partilere güven kaygısı, kapalı kapılar ardında çözüm üretme ihtiyacı) paha biçilmez olsa gerek.

Peki zararlı yazılım analisti olmak için ne tür bilgi/becerilere sahip olmanız gerekiyor ?

Programlama becerisi: Bilişim güvenliği uzmanı olupta programlama dili bilmiyorum demek kulağa ne kadar garip geliyorsa (gelmiyorsa da ben çok yadırgıyorum, her zaman araçlar işinizi görmeyebilir) zararlı yazılım analistiyim ancak Assembly'den, Java'dan, C'den, C#'den anlamıyorum demek kulağa bir o kadar garip gelebilir. Örneğin Java ile yazılmış bir zararlı yazılımı decompile ettikten sonra kodu analiz etmeniz gerekecek bu durumda ne yapacaksınız ? Veya zararlı bir yazılımı assembly seviyesinde çalışan bir debugger ile (Ollydbg veya Immnunity Debugger) analiz ediyorsunuz, Assembly bilmeden programın akışına nasıl müdahale edecek veya şifreleme anahtarlarını nasıl ele geçireceksiniz ? Gereksinimler böyle olunca bir zararlı yazılım analistinin C ve Assembly programlama dillerine yabancı olmaması buna ilaveten diğer programlama dilleri ile yazılmış (C++, Java, .Net) programların kaynak kodlarına az çok göz gezdirmiş olması gerekmektedir. Bunlara ilaveten Python veya Ruby gibi programlama dillerinden faydalanarak hızlı bir şekilde kendi programınızı yazmanız gerekebilir. Örneğin hafızadan diske kayıt ettiğiniz (dump) zararlı bir yazılımdan otomatik olarak şifreleme anahtarlarını toplayan ve şifrelemeyi çözen bir program yazmak istiyorsunuz. Şayet Python biliyorsanız IDAPython ile ufak betikler (script) yazmanız işinizi oldukça hızlandıracaktır. Anlayacağınız üzere zararlı yazılım analisti olma konusunda ısrarcı iseniz birden fazla programlama dili bilmeniz (uzman seviyesinde olmasa da) şart!

Sistem, ağ ve uygulama yöneticisi becerisi: En basitinden elinizde analiz etmeniz gereken bir zararlı yazılım var ve bunu kendi sisteminizde analiz etmemeniz gerektiğini az çok tahmin edebiliyorsunuzdur. Bu durumda yapmanız gereken izole bir ortamda kontrollü bir şekilde bu yazılımı çalıştırmaktır. Bunun için sanal ortamlardan (VMWare veya Virtual Box iyi bir seçim olacaktır) oluşan zararlı yazılım analiz laboratuvarı kurmanız gerektiği için işletim sistemi kurulumundan konfigürasyonuna, sanal ağ yapılandırmaları oluşturmaya kadar bir çok konuda bilgi sahibi olmanız gerekmektedir. Örneğin Android işletim sistemini hedef alan zararlı bir yazılımı analiz etmeniz gerekiyor. Bu durumda mutlaka Android OS yüklü bir cihaza mı ihtiyacınız var ? Tabii ki hayır, sanal sistem üzerine kuracağınız ve yapılandıracağınız bir emülatör işinizi görecektir. Veya ağ üzerinden yayılmaya çalışan zararlı bir

yazılımın oluşturduğu trafiği izlemeniz ve analiz etmeniz gerekecek bu durumda ağ bilgisine ihtiyaç duyacaksınız misal hangi port üzerinden hangi protokolü kullanıyor, şifreli mi haberleşiyor. Veya analiz ettiğiniz zararlı yazılım internette bulunan bir web sunucusu üzerindeki 0. gün zafiyetini istismar etmeye çalışıyor ancak analizi tamamlamak için bunu gerçekleştirmesine izin veremezsiniz bu nedenle sanal sisteminizin DNS kayıtlarını, aradığı alan adını sanal sisteminize yönlendirecek şekilde yapılandırarak ve kuracağınız aynı sürüm web sunucusuna yönlendirerek istismar etmesini sağlamanız ve analiz etmeniz gerekecektir. Kısacası yeri gelecek sistem, ağ ve uygulama yöneticisinin sahip olduğu hünerleri sergileyeceğiniz bir ortam oluşturarak zararlı yazılımın başarıyla çalışmasını sağlayacak alt yapıyı oluşturmanız gerekecektir.

Her zamanki gibi zararlı yazılım analizi ile ilgili kitaplar okumak (misal Malware Analyst’s Cookbook ve bu listede yer alan kitaplar), blogları ve haber kaynaklarını takip etmek (misal MNIN Security Blog), eğitimlere katılmak (misal SANS’ın Reverse-Engineering Malware: Malware Analysis Tools and Techniques eğitimi) ve tabii ki bol bol pratik yapmak (bunun için üzerinde zararlı yazılım tespit edilen sitelerin duyurulduğu twitter.com/hack4career twitter sayfasına göz atmak ve zararlı yazılımları indirerek incelemek iyi bir başlangıç olabilir) zaman içinde sizi başarıya ulaştıracaktır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim…