Antivirus Nasıl Atlatılır ?

written by Mert SARICA | 24 December 2010

Yıllar önce sistemlere nasıl sızılacağı konusunda bilgi sahibi olmaya çalışırken arka kapıları pek önemsemiyordum çünkü art niyetli kişilerin asıl amaçlarının hedef sistemlere sızmak, önemli bilgileri çalmak ve zarar vermek olduğunu düşünüyordum. Sistemlerde uzun süre kalarak verebilecekleri zararın boyutunun ne kadar yüksek olabileceğini aklımın ucundan bile geçirmiyordum. Ancak yıllar geçtikçe arka kapıların art niyetli kişiler için ne kadar değerli olduğunu öğrenmiş oldum. (TJX vakası buna en güzel örnektir.)

Örneğin art niyetli bir kişi, sızdığı sistemde yönetici yetkisine sahip değil ise yetki yükseltmesine imkan tanıyan bir zafiyet keşfedilene kadar bekleyebiliyor ve ardından yetkisini yükselterek kurumsal bir ağda, iç sistemlere doğru ilerlemek için bu arka kapıyı kullanabiliyor veya hedef sistem finansal bir sistemin parçası ise uzun süre bu sistem üzerinden geçen paketleri izleyerek kendisi için karlı, sistem sahibi için ise zararlı sonuçlara yol açabiliyor. Tabii arka kapıların kullanımını sadece kurumsal ağlar ve sunucular ile sınırlı tutmamak gerekiyor özellikle DDOS saldırılarına sıkça rastladığımız şu günlerde, bu işten gelir elde eden art niyetli kişiler için sıradan bir kullanıcının sistemi bile oldukça değerli olabiliyor.

Her gün ziyaret ettiğiniz masum bir site, başka bir gün internet tarayıcınızdaki bir güvenlik zafiyetini istismar ederek sisteminizin zombi sisteme dönüşmesine ve art niyetli kişilerin kontrolüne geçmesine neden olabiliyor. Sisteminizde sadece antivirüs yazılımı kullanıyor olmanız ne yazıkki bu sonucun ortaya çıkmasına engel olamayabiliyor çünkü antivirüs yazılımları ağırlıklı olarak imza tabanlı çalıştıkları için rahatlıkla atlatılabiliyor.

Art niyetli kişiler hazırladıkları istismar kodu ile çoğunlukla hedef sistemleri istismar ederek kendi sistemlerine (reverse tcp shell) bağlanmasını sağlayarak sistemlere izin erişebilirler. Son kullanıcı olarak art niyetli kişilerin bu girişimlerini engelleyemesinizde zorlaştırabilmek için sisteminizi yönetici (administrator) yerine kullanıcı yetkisi ile kullanmak ve antivirüs yazılımına ilave olarak kişisel güvenlik duvarı

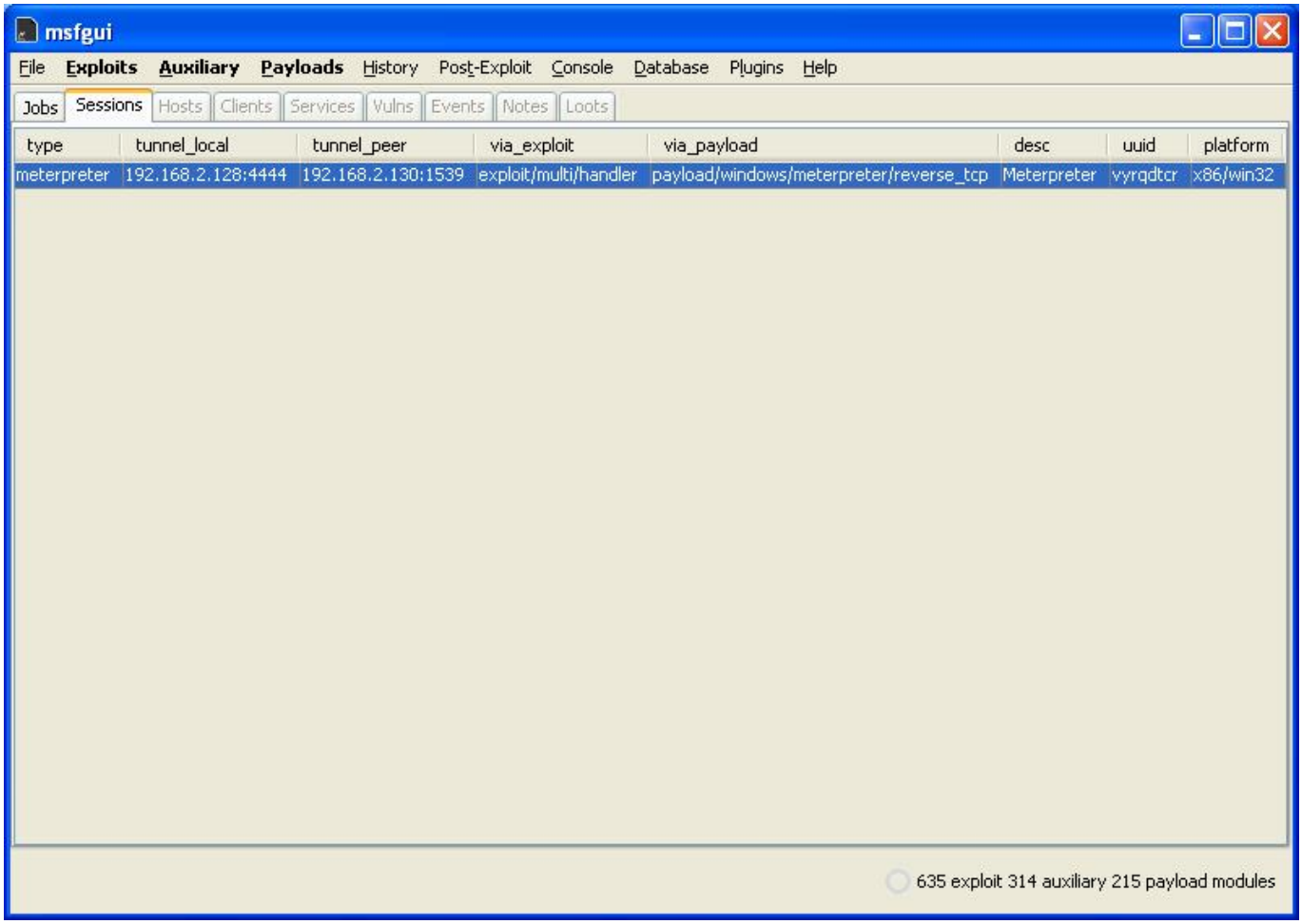
kullanmak iyi bir tercih olabilir. Güvenlik duvarı sayesinde sisteminiz üzerinde çalışan bir uygulama/program uzaktaki bir sisteme bağlanmaya çalıştığı zaman uyarılır ve izin vermeniz durumunda iletişimin gerçekleşmesini sağlarsınız. Kullanıcı yetkisi ile kullandığınız sistem sayesinde ise art niyetli kişi tarafından istismar edilen sisteminiz üzerindeki güvenlik kontrollerinin devre dışı bırakılmasını bir hayli zorlaştırabilirsiniz.

Bu konuya dikkat çekmek için yönetici yetkisi ile çalışan ve sadece antivirüs yazılımı yüklü olan bir sistemin art niyetli kişiler tarafından nasıl ele geçirilebileceğini göstermenin faydalı olacağını düşünerek hemen bir antivirüs yazılımı aramaya karar verdim ve çok fazla vakit kaybetmeden yıllarca severek ve beğenerek kullandığım Mcafee Virusscan yazılımında karar kıldım.

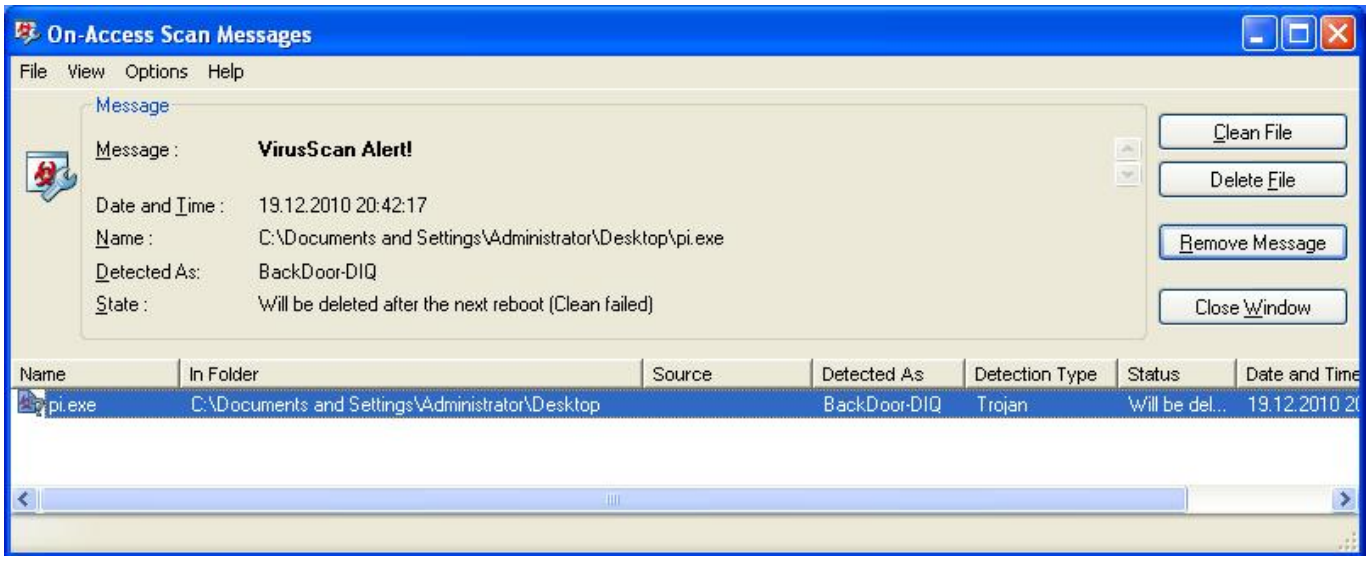
Senaryoma göre yönetici yetkisi ile çalışan ve üzerinde Mcafee Virusscan yazılımı çalışan bir sistem istismar ediliyor ve ardından sisteme Metasploit ile bağlanan art niyetli kişi güvenlik kontrolleri devre dışı bırakarak sisteme arka kapı/truva atı yüklemeye ve sistemin her açılışında bu arka kapı/truva atının yüklenmesini sağlıyor.

Senaryoyu gerçekleştirmek için iki tane sanal sistem hazırladım. Birincisinin adı Kuzu ve üzerinde Virusscan çalışıyor ikincisi ise Hain-Kuzu ve üzerinde Metasploit çalışıyor.

Hain-Kuzu’nun sisteminde Metasploit ile Meterpreter‘i oluşturduktan sonra bunu Kuzu’nun sisteminde çalıştırarak istismar sonrasını simüle etmeye çalıştım. Meterpreter çalışır çalışmaz Kuzu’nun sistemi Hain-Kuzu’nun sistemine bağlanarak konsol için erişime hazır hale geldi. (Meterpreter’i çoğunlukla antivirüs yazılımları zararlı yazılım olarak tespit ederler ve silerler fakat Virusscan’de ne yazıkki böyle bir uyarı ile karşılaşmadım).



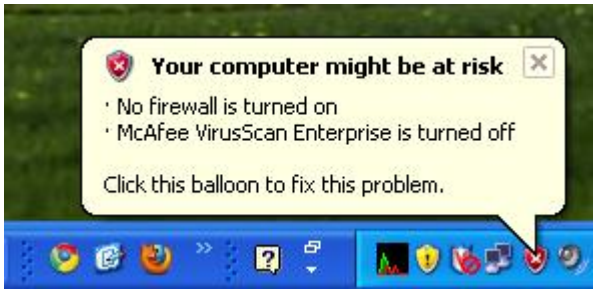
Tuş kayıt özelliğine sahip arka kapı/truva atı niyetine Poison Ivy yazılımını kullanmaya karar verdim ve Kuzu'nun sistemine yüklenecek ve çalıştırıldığı anda sisteme bağlanmaya imkan tanıyacak programı (pi.exe) Poison Ivy ile oluşturdum. Konsol üzerinden "upload pi.exe" komutunu çalıştırdığımda Kuzu'nun sistemine yüklenen pi.exe programı Virusscan tarafından hemen tespit edildi ve silindi.



Öncelikle Virusscan'i devre dışı bırakmam gerekiyordu ancak Virusscan

işlemleri sistem (system) yetkisi ile çalıştığı ve yönetici yetkisi ile bunları sonlandırmak mümkün olmadığı için konsol üzerinde “ps” komutunu çalıştırarak Mcafee işlemlerinden (processes) bir tanesini gözüme kestirdim ve “migrate PID” komutu ile mfevtps.exe işlemine geçiş yaptım. Artık sistem yetkisine sahip olduğum için Virusscan’e ait olan tüm servisleri ve işlemleri kapatabilirdim.

Meterpreter ile gelen ve sistem üzerinde çalışan tüm antivirus işlemlerini sonlandırmak için kullanılan killav betiğini (script) kullansaydım Virusscan’in sistem tepsisinde (system tray) yer alan simgesi (icon) değişecek (park yasağı şeklini alıyor :p) ve Kuzu’nun dikkatini çekecektim.

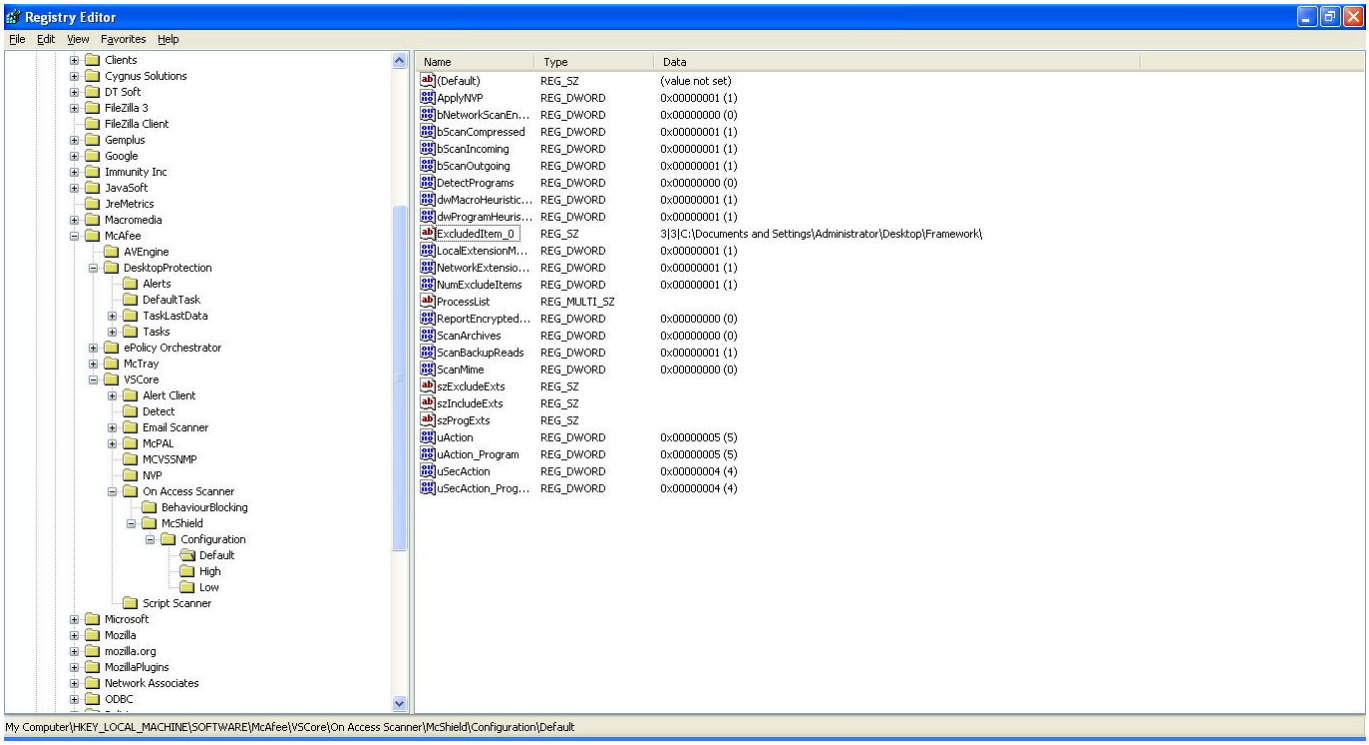


Şüphe çekmek art niyetli kişilerin istemeyeceği bir durum olduğu için bende onlar gibi düşünerek buna bir çözüm aramaya karar verdim ve işlemleri belli bir sırada (shstat, EngineServer, FrameworkService, naprdmgr, mctray, mfeann, vstskmgr, Mcshield, bunun adına sihirli sıra dedim :)) sonlandırarak simgenin değişmemesini sağladım.

Antivirus devre dışı kaldıktan sonra konsol üzerinden “upload” komutu ile pi.exe programını sisteme yükleyebildim. Bundan sonraki amacım pi.exe programının sistem her yeniden başladığında çalışmasını ve Virusscan tarafından tespit edilmesini önlemek olduğu için öncelikle pi.exe programını sistem başlangıcında çalışması için kayıt defterindeki (registry) “HKLM\Software\Microsoft\Windows\CurrentVersion\Run” anahtarına ekledim.

Virusscan, tarama dışında bırakılacak olan program listesini, diske yazma ve diskten okuma esnasında tarama gerçekleştirilmesi ve istenmeyen program (casus yazılımlar, tuş kayıt yazılımları vs) taraması ile ilgili ayarları kayıt defterinde tuttuğu için ilk olarak sisteme yüklediğim pi.exe programının tarama dışında tutulması için ilgili anahtardaki değere ekledim. Ardından işimi garantiye almak için diskten okuma esnasında tarama, diske yazma esnasında tarama ve istenmeyen program taramasını kayıt defteri üzerinden devre dışı bıraktım ve bu sayede sisteme tuş kaydı yapabilen arka kapı yerleştirilmesini ve sistem başlangıcında çalıştırılmasını sağlamış

oldum.



Bu arada bu işlemleri otomatize etmek için virusscan_bypass adında ufak bir Meterpreter betiği hazırladım.

Güncelleme (25/12/2010): Hazırlamış olduğum betik Metasploit projesine dahil olmuştur, ilerleyen sürümlerinde yüklü geleceği için indirmenize gerek kalmayacaktır.

Teyit etmek için bilgisayarı yeniden başlattığımda sistemin açılır açılmaz arka kapıyı/truva atını çalıştırarak Hain-Kuzu sistemine bağlandığını gördüm ve art niyetli kişi açısından görev başarıyla tamamlanmış, madur kişi içinse yönetici yetkisinden kurtulma ve sisteme kişisel güvenlik duvarı yüklenmesi için çok geçerli bir neden ortaya çıkmış oldu.

Daha net anlaşılabilmesi için her zamanki gibi kısa metrajlı bir film çektim :)
Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler ve iyi seyirler dilerim.