Sanal Kuşatma

written by Mert SARICA | 14 April 2010

Hatırlarsanız penetrasyon testi için firma seçiminde honeypot kullandığımdan bahsetmiştim. Honeypot'u hazırlarken zaman zaman internet üzerinden erişime açıyordum. Dikkatimi çeken bir nokta, erişime açar açmaz yaklaşık 3 saat içerisinde Çin ve Rusya kaynaklı IP adreslerinden önce SSH bağlantı noktası taranıyor ve ardından deneme yanılma (brute-force/dictionary attack) saldırıları gerçekleşiyordu. Bir kaç defa IP adresini değiştirsemde değişen birşey olmuyordu yine aynı süreler içerisinde saldırılar başlıyordu. O günlerde bu konunun üzerine eğilme fırsatım olmamıştı ta ki geçtiğimiz Pazar gününe kadar.

Geçtiğimiz Pazar günü yine can sıkıntısından tüm yamaları yüklenmiş olan Windows XP SP3 işletim sistemini internete açmaya ve sonuçları analiz etmeye karar verdim.

Öncelikle bir honeypot kurmam gerekiyordu. Ne kursam ne kursam diye araştırırken sonunda birden fazla servisi taklit etme yeteneğine sahip HoneyBOT adındaki düşük etkileşimli (low interaction) honeypotu kurmaya karar verdim. Devam etmeden önce muhtemelen düşük etkileşimde neyin nesi diye aklınızda bir soru oluşacak bu nedenle öncelikle bunu yanıtlayayım.

Honeypotlar temel olarak 3'e ayrılırlar;

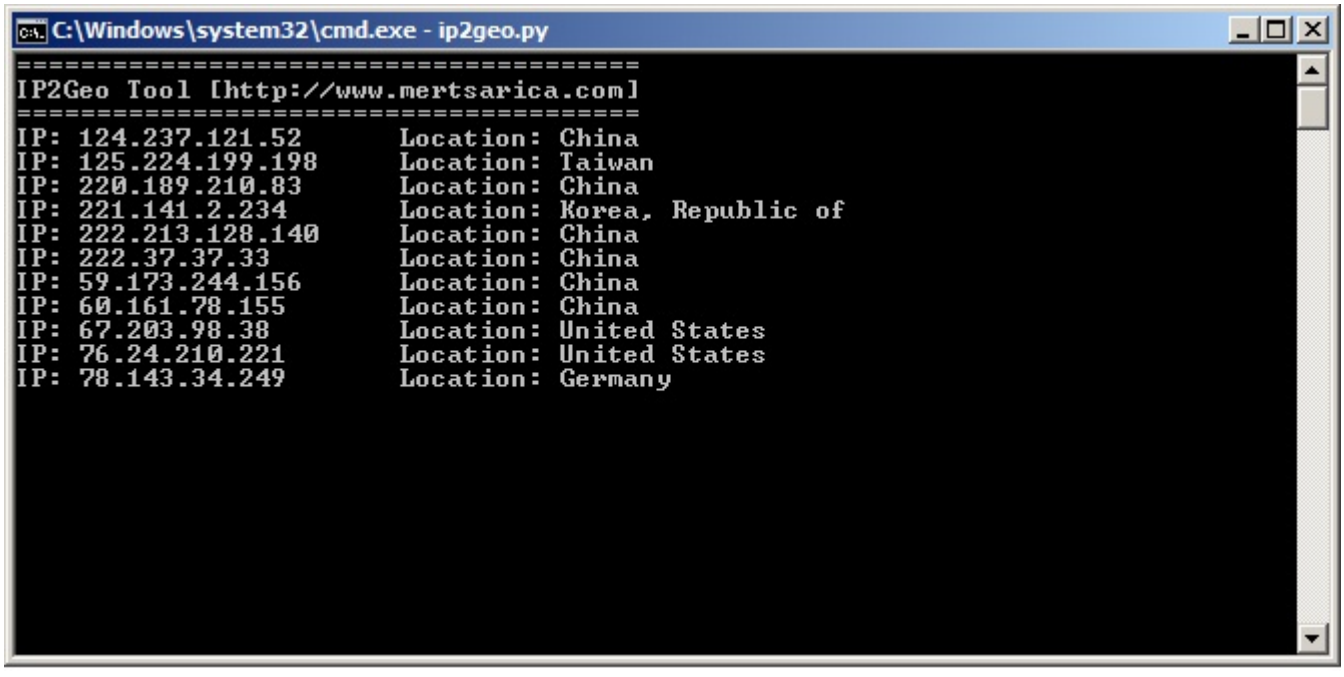
- Düşük etkileşimli: Sadece zafiyet barındıran servisleri taklit ederler, ele geçirilmeleri mümkün değildir.
- Orta etkileşimli: Zafiyet barındıran servisleri taklit ederek zararlı yazılıma ait kod parçacıklarını (payload) temin etmek için kullanılırlar.
- Yüksek etkileşimli: Zafiyet barındıran işletim sisteminden oluşurlar ve en sonunda ele geçirilirler.

Kısa bir bilgilendirmeden sonra kaldığım yerden devam edeyim. HoneyBOT'u kurup çalıştırdığımda 1328 adet soket açtığını gördüm fakat 1328 tane servisten rastgele bir kaç tanesini kontrol ettiğimde o servisi bire bir taklit etmediğini gördüm. Anladığım kadarıyla HoneyBOT sadece bilinen servisleri (örnek http) taklit edebilirken geri kalanlar için sadece gelen bağlantıları dinlemekle yetiniyor.

Pazar günü, akşam üstüne doğru evden çıkmam gerekiyordu. Evden çıkmadan önce honeypotu dinamik ip adresine sahip olan adsl modemimin DMZ segmentine saat 15:47 itibariyle yerleştirdim.

Eve döndüğümde aradan tam tamına 5 saat geçmişti ve ilk işim honeypotun kayıtlarına göz atmak oldu. Kayıtlarda honeypot ile iletişim kuran 14 tane farklı ip adresi olduğu gözüküyordu ve ilk kayıt saat 15:55'de oluşan 220.189.210.83 (port 1433) IP adresine aitti. Honeypot'u internete açalı 12 dakika geçmesine rağmen ilk kaydın oluşması için aradan çok fazla vakit geçmemişti. 6. hissim bana bu ip adresinin çekik gözlülere ait olduğunu söylüyordu ve kontrol ettikten sonra yanılmadığımı anladım, ip adresi Çin'e aitti. Kayıtlarda yer alan bağlantı noktalarına göz attığımda ise toplamda 11 tane bağlantı noktası ile
(1080, 1433, 1434, 22, 23, 3128, 6588, 6881, 80, 8080, 9000) iletişim kurulmuştu. Bu arada geri kalan 13 IP adresinin lokasyonlarını manuel olarak belirlemeye üşendiğim için Python ile IP2Geo adında ufak bir program yazdım.

IP2Geo kısaca ip.txt içerisinde belirtmiş olduğunuz ip adreslerini alarak sırasıyla lokasyonunu belirliyor ve location.txt dosyası adı altında kayıt ediyor.



IP adresleri ile ilişkili lokasyonları sırasıyla listeleyecek olursam;
124.237.121.52:China
125.224.199.198:Taiwan
220.189.210.83:China
221.141.2.234:Korea, Republic of

222.213.128.140:China
222.37.37.33:China
59.173.244.156:China
60.161.78.155:China
67.203.98.38:United States
76.24.210.221:United States
78.143.34.249:Germany
82.38.92.106:United Kingdom
82.73.23.186:Netherlands
94.51.72.75:Russian Federation

Honeypot kayıtlarından edindiğim bilgileri kısaca özetleyecek olursam honeypot üzerinde yer alan 11 bağlantı noktasından bir tanesine internete açıldıktan 12 dakika sonra ilk bağlantı gerçekleşmiş ve 5 saat içinde toplamda honeypota 8 farklı ülkeden, 14 farklı ip adresinden iletişim kurulmuştur.

Bu bilgilerden çıkartılacak sonuç, adsl modemlerimizin, sunucularımızın, bilgisayarlarımızın sanal kuşatma altında olduğudur. Internette onlarca belkide yüzlerce botun, ip bloklarımızı tarayarak güvenlik zafiyeti barındıran sistem, sunucu, uygulama, cihaz aramaktadır. Bu nedenle adsl modemlerinizin ateş duvarında (firewall) yapacağınız bir konfigürasyon hatası, işletim sisteminizdeki eksik bir yama, zayıf yönetici parolası, güncel olmayan bir antivirüs zincirleme olarak size pahalıya mal olabilir, tedbiri elden bırakmamanızı tavsiye ederim.

Unutmadan IP2Geo programına buradan ulaşabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle…