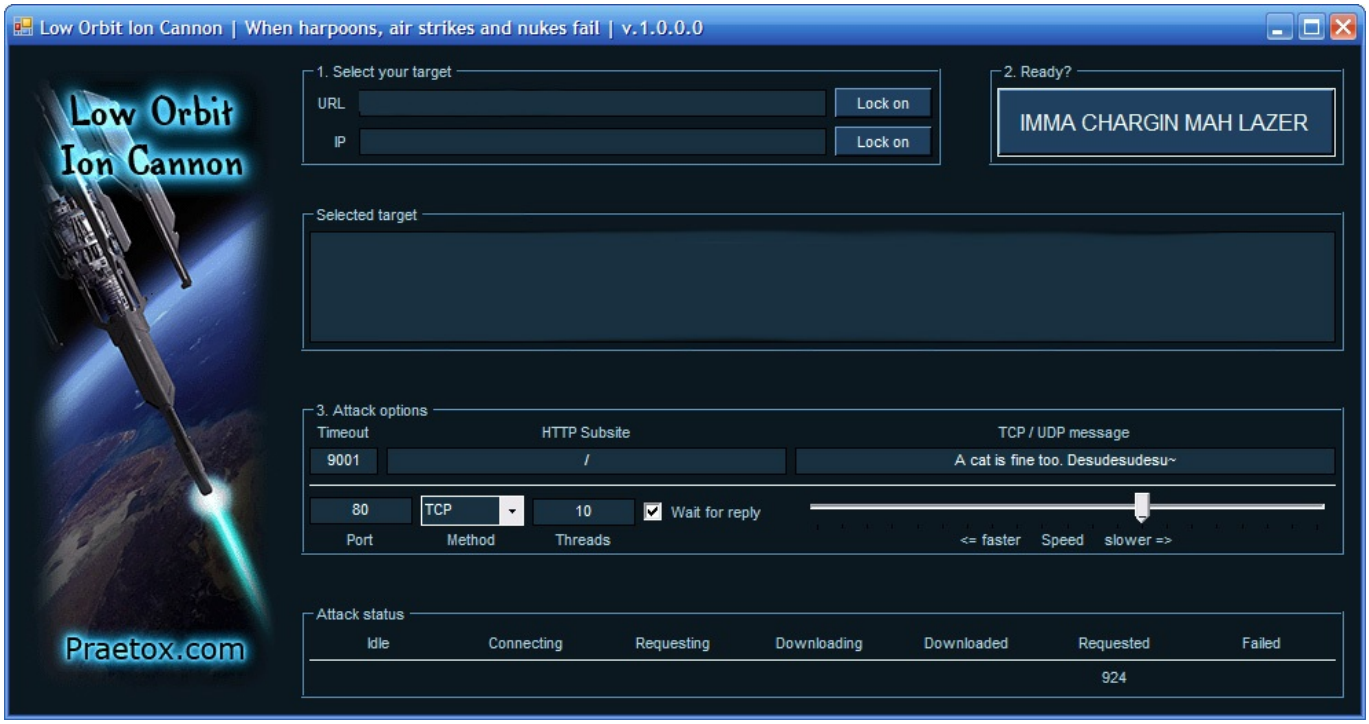
RedBot Analizi

written by Mert SARICA | 2 September 2012

Anonymous grubu, 2010 yılından bu yana gerçekleştirmiş olduğu DDOS (dağıtık hizmet dışı bırakma saldırısı) saldırılarında açık kaynak kodlu Low Orbit Ion Cannon (LOIC) aracından ve 2012 yılından bu yana gerçekleştirdiği saldırılarda ise High Orbit Ion Cannon (HOIC) aracından faydalanmaktadır. Tek başına DOS (hizmet dışı bırakma saldırısı) saldırısı gerçekleştirebilen bu araçlar birden fazla kişinin aynı anda aynı hedefe saldırı gerçekleştirmesi ile DDOS saldırısı gerçekleştirebilmektedir.

Basından sıkça duymuş olduğunuz bilgisayar korsanları X sitesini hackledi şeklinde yapılan haberlerin çoğu yanlış olarak ifade edilmektedir çünkü gerçekleştirilen siber saldırıların büyük bir oranı DDOS saldırıları ile gerçekleştirilmekte, hedef siteye/sisteme erişimler engellenmektedir. X sitesi hacklendi diyebilmek için siteye/sisteme ve sitede/sistemde yer alan verilere yetkisiz erişimin sağlanması gerekmektedir. (Basın mensuplarına duyurulur!)

Bu grubun saldırılarına destek vermek amacıyla dağıtılan ve destekçiler tarafından sistemlerinde çalıştırılan bu araçlardan LOIC ve türevleri, araç ile tanımlı gelen IRC sunuculara bağlanarak saldırıyı gerçekleştiren gruplar tarafından yönetilen kanallara/odalara giriş yapmakta ve uzaktan saldırı komutu almasını sağlamaktadır. HOIC ve türevleri ise saldırı öncesinde dağıtılan booster denilen betiklerin (script) araca yüklenmesi ve saldır komutunun kullanıcı tarafından verilmesi ile gerçekleştirilebilmektedir. LOIC aracı ile UDP, TCP ve HTTP protokollerine yönelik DDOS saldırıları gerçekleştirilebilirken HOIC ile sadece HTTP protokolüne yönelik saldırılar gerçekleştirilmektedir. HOIC aracı ile gerçekleştirilen HTTP protokolüne yönelik saldırılar, LOIC aracına kıyasla imza tabanlı sistemleri atlatmaya yönelik özellikleri olması (rastgele üretilen HTTP başlıkları gibi) nedeniyle daha etkilidir.

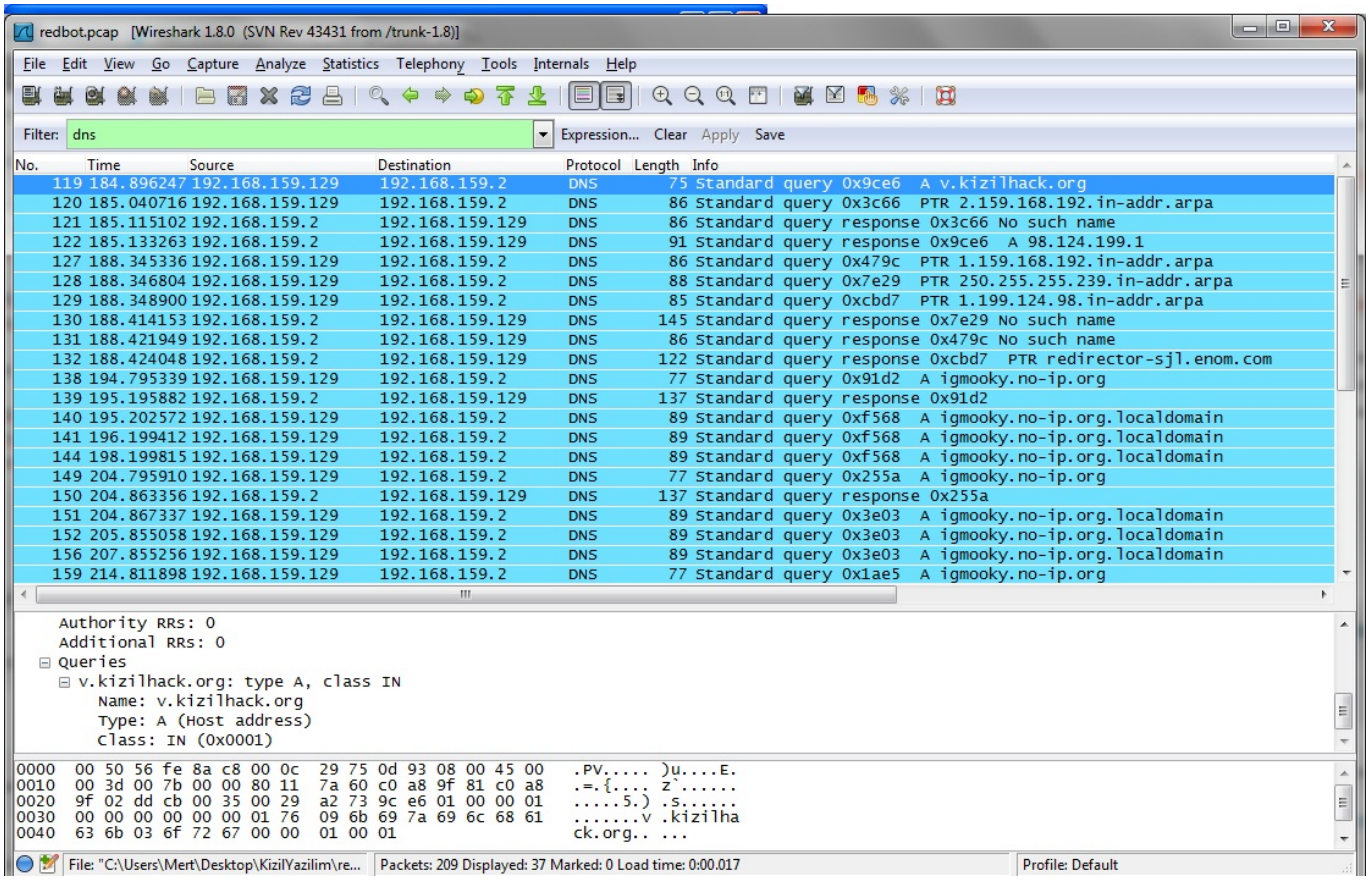


Geçtiğimiz günlerde bir arkadaşım, Twitter hesapları üzerinden son aylarda gerçekleştirdiği siber saldırılar ile adından sıkça söz ettiren RedHack grubunun DDOS saldırılarına destek vermek amacıyla RedBot adında benzer bir aracın yayınlandığını ileterek analiz etmemi rica etti ve ben de vakit kaybetmeden işe koyuldum.

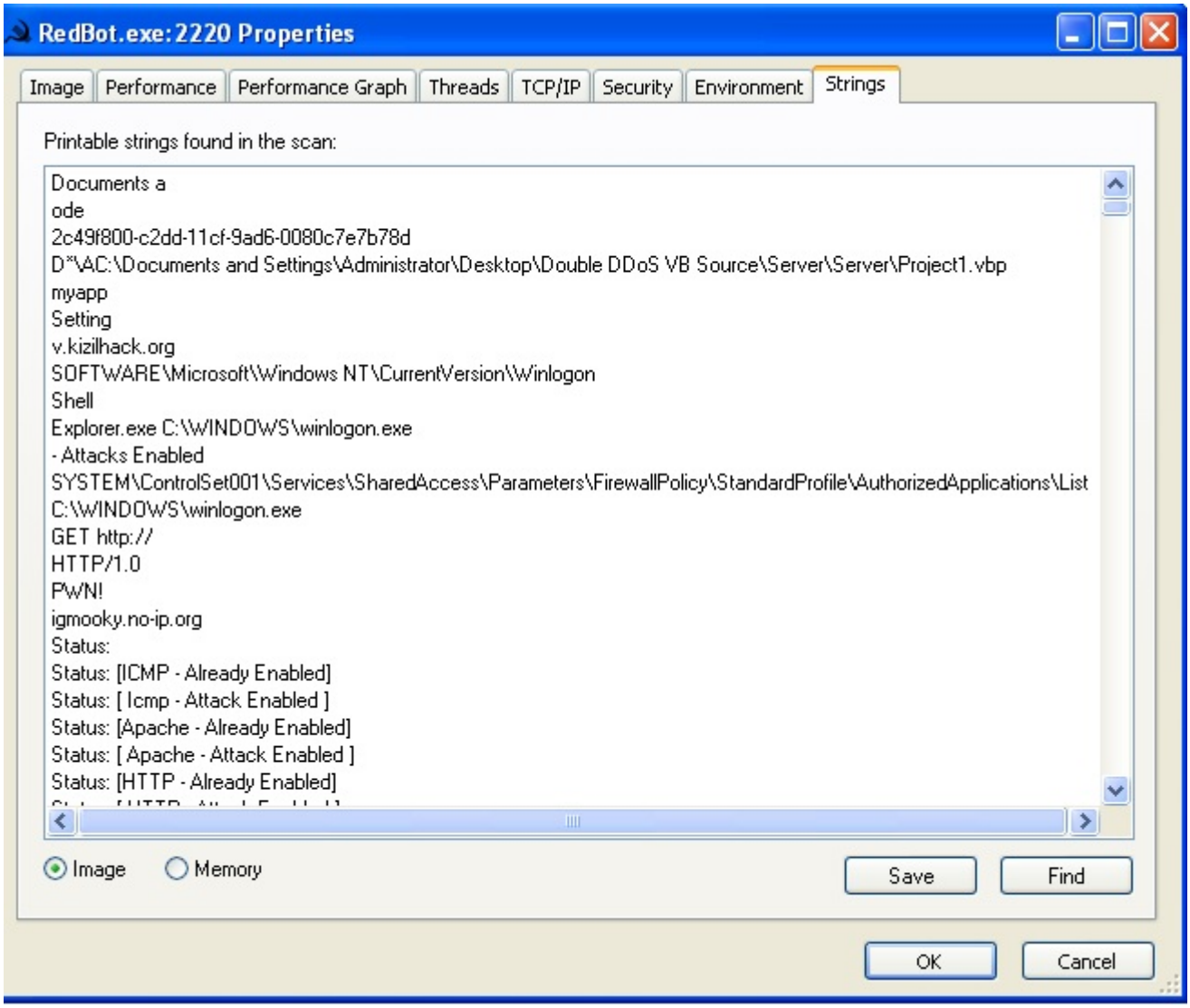
RedBot.rar dosyası içinde yer alan metin dosyasına göz attığımda aracın yukarıda bahsettiğim diğer araçlar ile aynı amaca hizmet ettiği anlaşılıyordu.

```
RedBot Redhack grubunun Saldırılarını Bilgisayarınız Üzerinden Yönlendiren Bir aracı yazılımdır.
Bilgisayarınız için Virus vb. Yazılımlar Taşımaz Bilgisayarınız Sanal bir Saldırı Ağına dahil Eder.
Amacı Daha Fazla Bilgisayarı Kullanarak Etkili Saldırılar Gerçekleştirmektir.
Birkez Çalıştırmanız yeterlidir.
Daha Sonra Saldırı olduğunda Kendiliğinden Çalışacaktır.
```

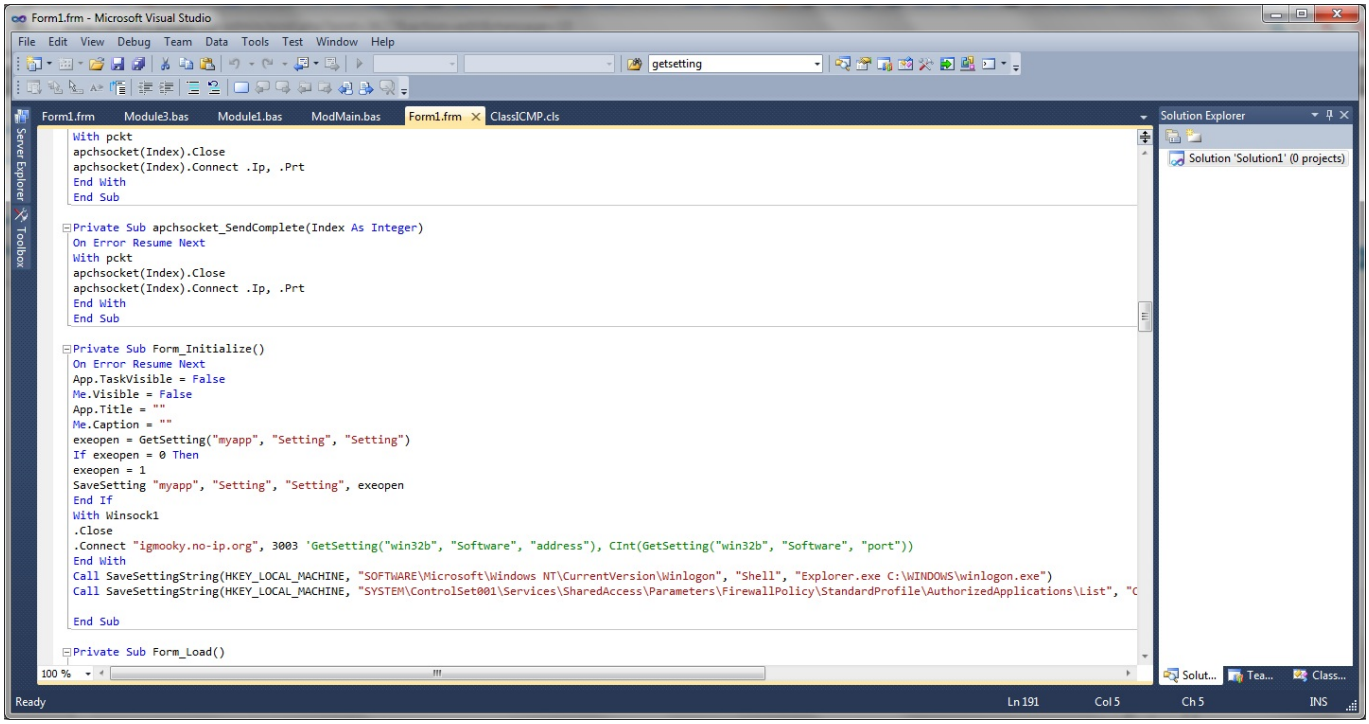
RedBot aracını (RedBot.exe – SHA256: c30240d550d2c86b0f0b71dcc0eed36ad5134c9ce630ca94d2137bfb38f2ec2d) çalıştırdığımda mswinsck.ocx dosyasının sistemde bulunmamasından ötürü hata vererek çalışmayı reddeti. Ardından ilgili dosyayı sisteme kopyalayıp çalıştırdıktan sonra arka planda RedBot.exe adı altında çalışmaya başladığını ve Wireshark aracı ile yarattığı trafiği izlediğimde ise iki farklı DNS sorgusuna ait kayıt yaratması dikkatimi çekti, v.kizilhack.org (bir sorgu) ve igmooky.no-ip.org (onlarca sorgu)



Microsoft Sysinternals'ın Process Explorer aracı ile RedBot aracında tespit edilen dizileri (string) incelediğim zaman aracın geliştirildiği klasör bilgisinden aslında bu aracın Visual Basic ile 2007 yılında geliştirilmiş olan Double DDOS aracının modifiye edilmiş hali olduğunu gördüm.



Double DDOS aracının kaynak kodunu incelediğimde ise RedBot ile bu aracın hemen hemen aynı olduğunu sadece kaynak kodununun iki farklı yerinde bulunan igmooky.no-ip.org adresinden sadece bir tanesinin v.kizilhack.org olarak değiştirildiğini, diğerinin unutulduğunu bu nedenle belirli zaman aralıklarında saldırı komutu almak için v.kizilhack.org adresine 3003. bağlantı noktasından (port) bağlanması gerekirken ön tanımlı olan ve geçerli olmayan igmooky.no-ip.org adresine 3003. bağlantı noktasından bağlanmaya çalıştığını gördüm.



Buna ilave olarak aracın çalıştırıldıktan sonra kayıt defteri (registry) üzerinde değişiklikler yaparak kendisini Windows Güvenlik Duvarı'nın (Firewall) istisna (exception) listesine ekleyerek ilgili adreslere bağlanmasını, sistem yeniden başlatıldıktan sonra tekrar çalışabilmesi için C:\WINDOWS\winlogon.exe satırını HKEY_LOCAL_MACHINE, "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon anahtarına eklediğini ve aracın kendisini winlogon.exe adı altında Windows klasörü altına kopyalamadığı için sistem yeniden başlatıldıktan sonra çalışamadığını gördüm.

```
Call SaveSettingString(HKEY_LOCAL_MACHINE, "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon", "Shell", "Explorer.exe C:\WINDOWS\winlogon.exe")
Call SaveSettingString(HKEY_LOCAL_MACHINE, "SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List", "C:\WINDOWS\winlogon.exe", "C:\WINDOWS\winlogon.exe")
```

Kaynak kodu sayesinde ileri seviye analize ihtiyaç duymadan elde ettiğim bilgiler sonucunda aracın eski, düzgün yapılandırılmamış olması ve temel düzeyde tek tip UDP, TCP, ICMP ve HTTP saldırıları gerçekleştirmesi nedeniyle tespit edilmesinin ve engellenmesinin Anonymous grubu tarafından kullanılan LOIC ve HOIC araçlarına kıyasla daha kolay olduğunu ve aracın saldırı komutu almak dışında başka bir amaca (dosya sistemine erişim, başka zararlı dosyalar indirme gibi) hizmet etmediğini söyleyebilirim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: An itibariyle RedBot aracını 42 Antivirüs yazılımından sadece 16 tanesi tanıyabilmektedir. VirusTotal raporuna buradan ulaşabilirsiniz.