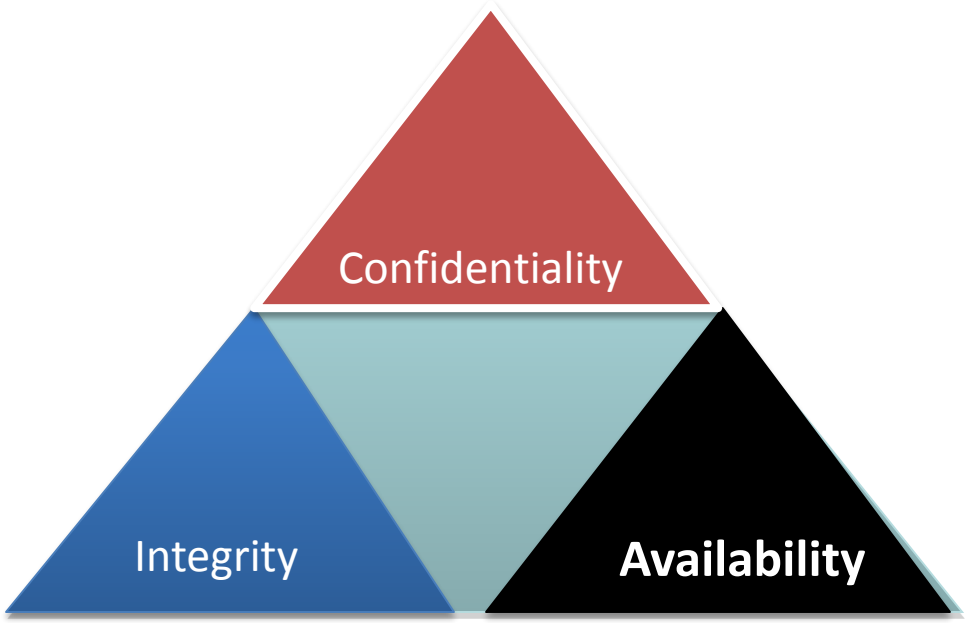
Temel Kavramlar, DoS/DDoS Saldırıları ve Çeşitleri

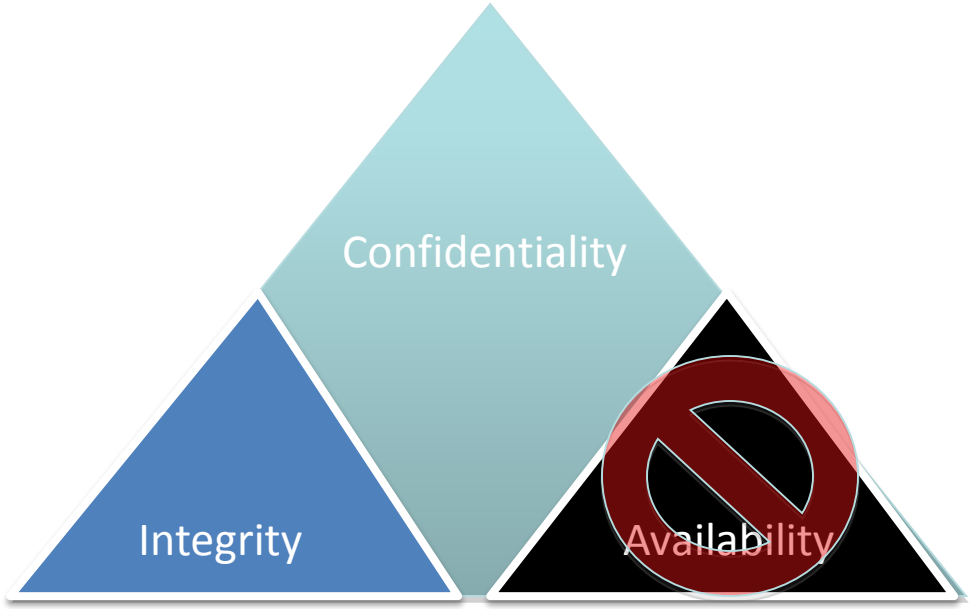
Standart Güvenlik Bileşenleri

- **Herşey gaz ve toz bulutuyken...**
- **(C.I.A)**



En Önemli Bileşen:Availability

- Erişilebilirlik olmadan güvenlikten söz edilemez!



Bilinmesi Gerekenler...

- Gelen DDOS saldırısı sizin sahip olduğunuz bantgenişliğinden fazlaysa yapılabilecek çok şey yok!
- DDOS saldırılarının büyük çoğunluğu bantgenişliği taşırma şeklinde gerçekleşmez!
- Bazı saldırı tiplerinde karşı tarafın gönderim hızı düşürülebilir

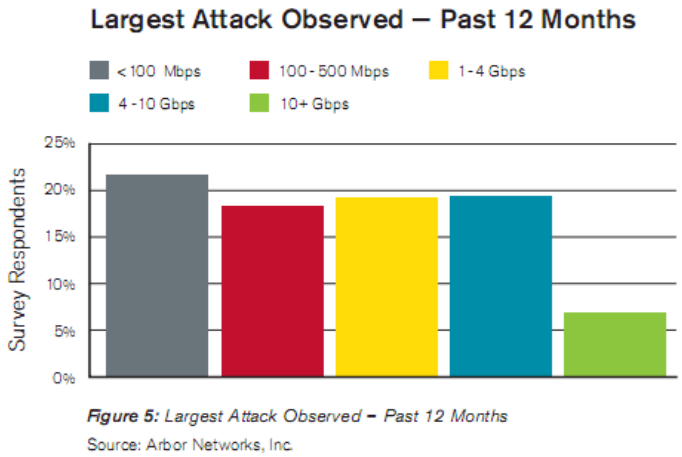


Figure 5: Largest Attack Observed – Past 12 Months

Source: Arbor Networks, Inc.

Gürcistan DDOS saldırısı 200-800 Mbps arası

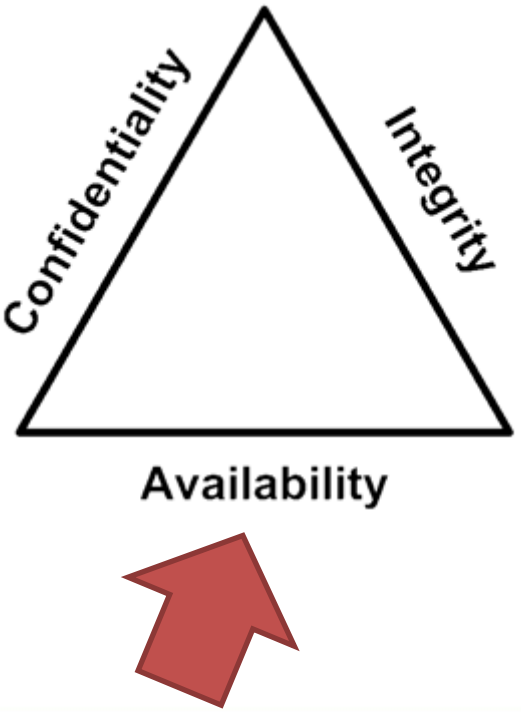
DOS/DDoS Hakkında Yanlış Bilgiler

- Bizim Firewall DOS'u engelliyor
- Bizim IPS DOS/DDOS'u engelliyor...
- Linux DOS'a karşı dayanıklıdır
- Biz de DDOS engelleme ürünü var
- Donanım tabanlı firewallar DOS'u engeller
- Bizde antivirüs programı var

- DOS/DDOS Engellenemez

Genel Kavramlar

- DOS(Denial Of Service)
- DDOS(Distributed Denial Of Service)
- Zombi
- BotNet(Robot Networks)
- IP Spoofing
- FastFlux networks
- SYN, FIN, ACK, PUSH ...
- Flood
- RBN(Russian Business Network)

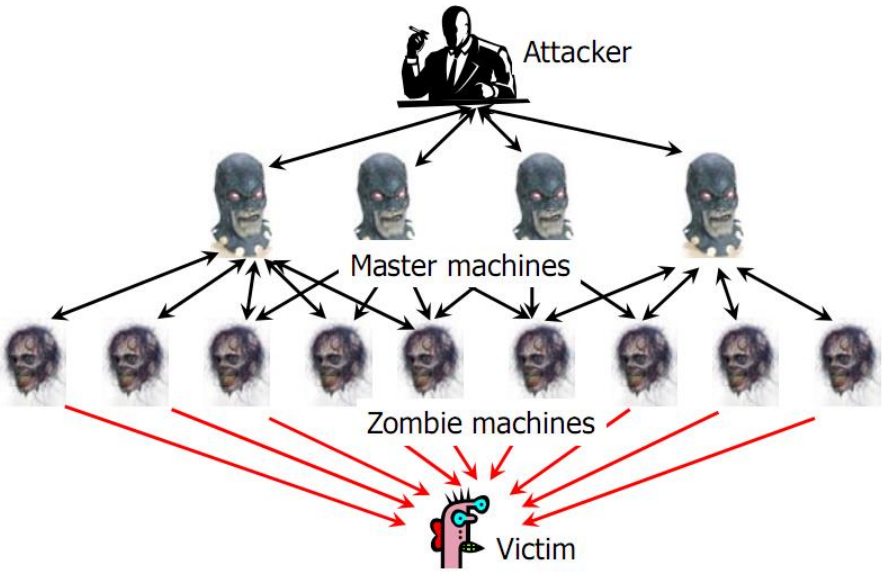


DOS

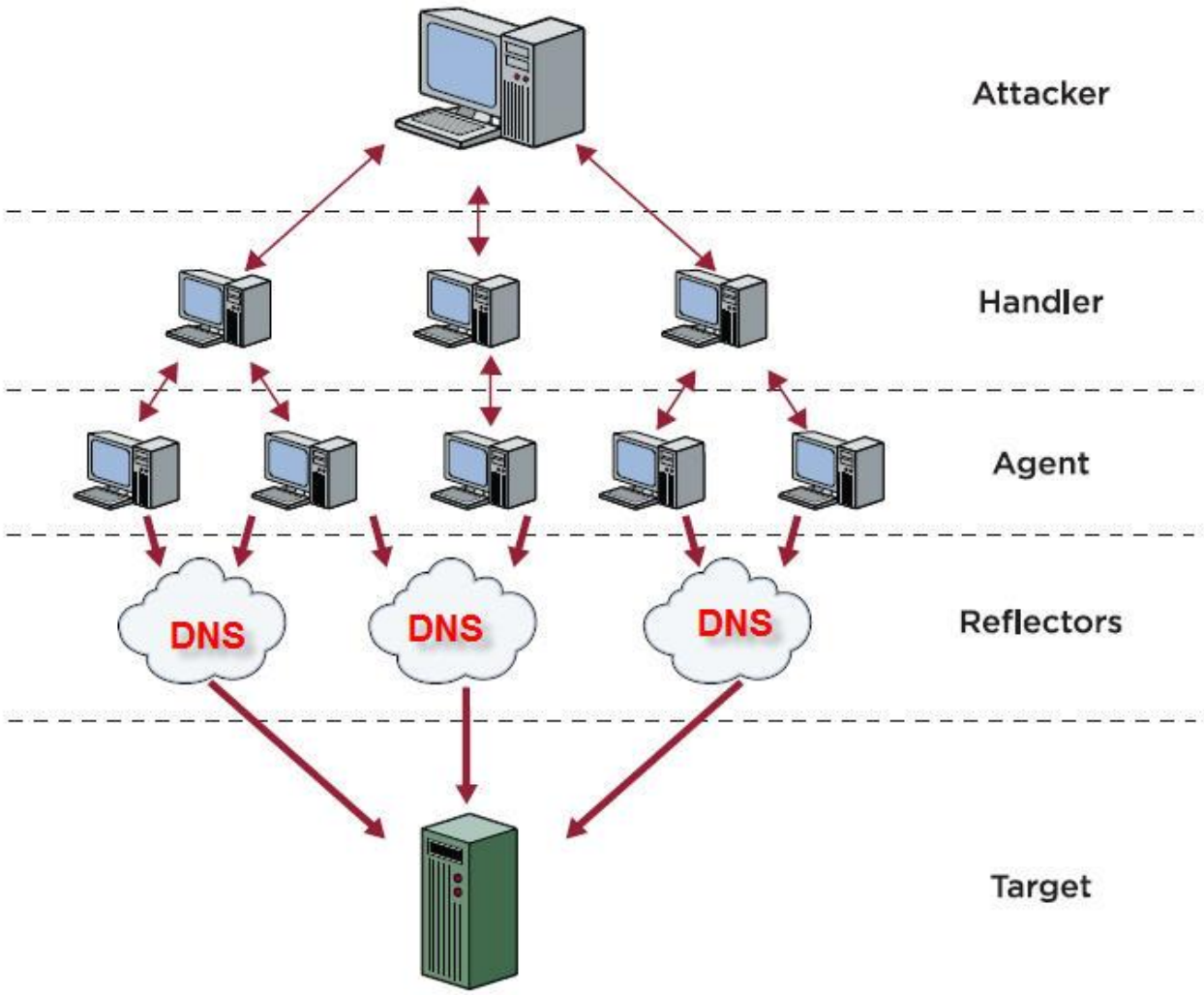
- DOS(Denial Of Service) = sistemleri çalışamaz hale getirmek için yapılan saldırı tipi
- DOS saldırısının yüzlerce, binlerce farklı sistemden yapılmaz
- Bazı saldırılar özünde DoS, sonuçlarına göre DDoS'tur
  - Tek bir sistemden yapılan spoof edilmiş IP kullanılan SYN flood saldırıları gibi
- DoS saldırılarını engelleme kolaydır

DDoS

- DDOS(Distrubuted Denial of Service) =Dağıtık Servis Engelleme
- Binlerce, yüzbünlerce sistemden yapılabilir
- Genellikle sahte IP adresleri kullanılır
- BotNet'ler kullanılır
- Saldırgan kendini gizler



DrDoS

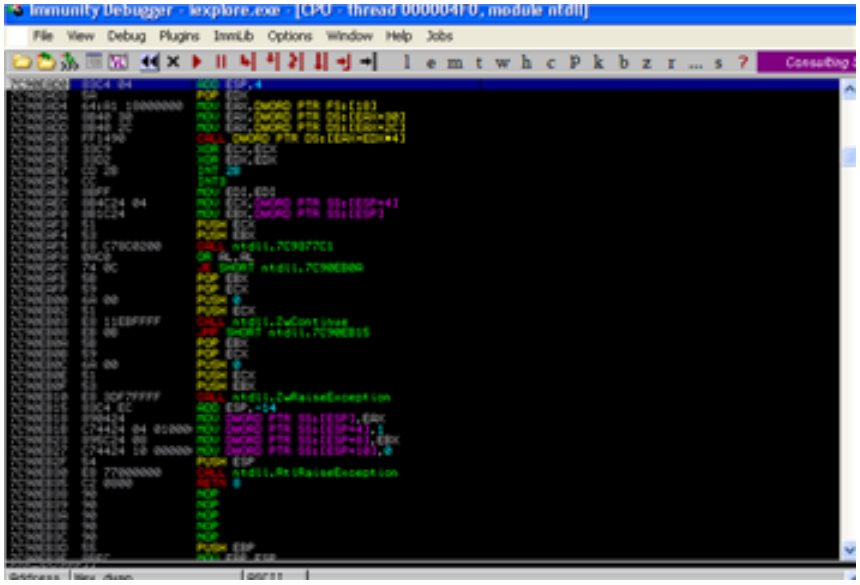


Malware

- Kötücül yazılım
- Bilişim sistemlerine yüklenerek sistemi kötü amaçlı kullanımını sağlayan yazılım türü

Exploit

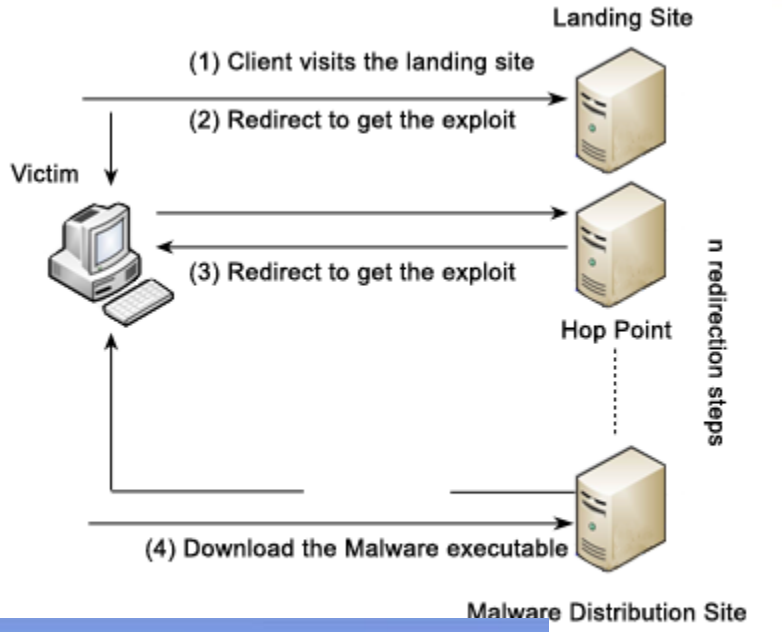
- Bir zaafiyeti kötüye kullanarak sisteme izinsiz erişim yetkisi veren program/scriptlerdir
- Sistemlerdeki zaafiyetler exploit edilerek zararlı yazılımlar yüklenebilir
- Sistemlerdeki zaafiyetler exploit edilerek DoS yapılabilir

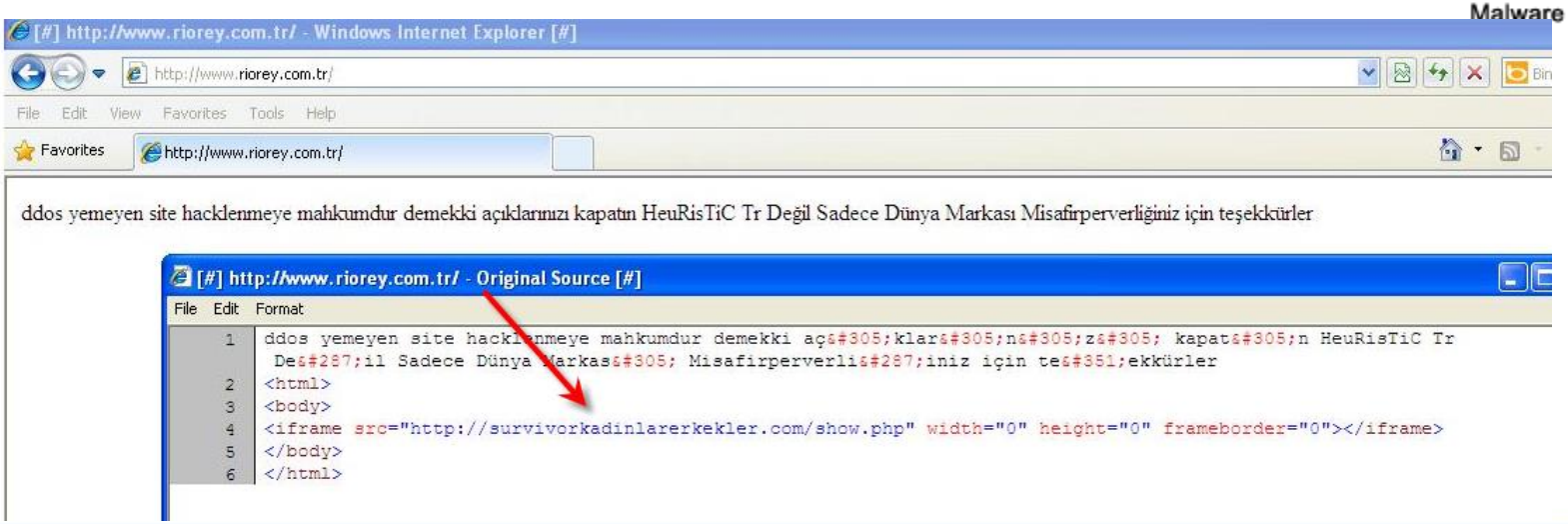


Drive By Download

- Kullanıcının haberi olmadan s

Sistemine zararlı yazılım yükleme





Kaspersky Lab

Zombi/(ro)BOT

- Zombi: Emir kulu
  - Çeşitli açıklıklardan faydalanılarak sistemlerine sızılmış ve arka kapı yerleştirilmiş sistemler
  - Temel sebebi: Windows yamalarının eksikliği
- roBOT = Uzaktan yönlendirilebilir sistemler
  - Zombi
- Dünyada milyonlarca vardır

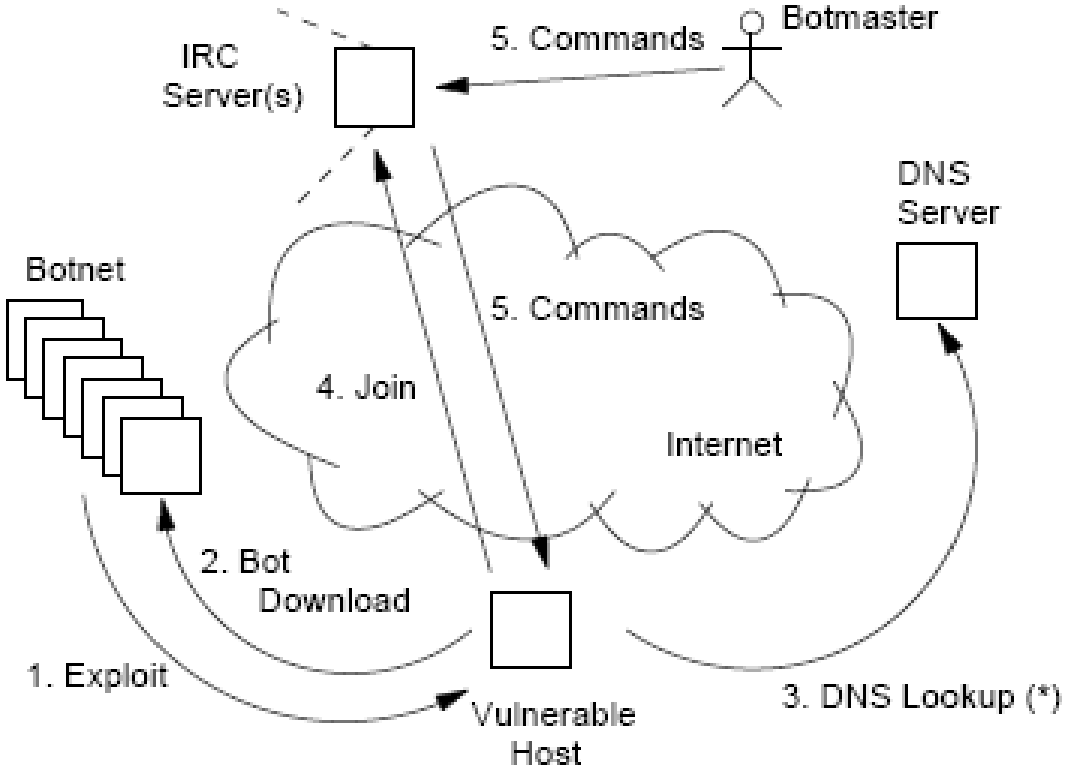
Zombi Olmamak İçin Antivirüs Yeterli midir?

a-squared	4.0.0.101	2009.05.15	-
AhnLab-V3	5.0.0.2	2009.05.15	-
AntiVir	7.9.0.168	2009.05.15	TR/Crypt.XPACK.Gen
Antiy-AVL	2.0.3.1	2009.05.15	-
Authentium	5.1.2.4	2009.05.15	-
Avast	4.8.1335.0	2009.05.15	Win32:MDrop-A
AVG	8.5.0.336	2009.05.15	Dropper.Mdrop.N
BitDefender	7.2	2009.05.15	-
CAT-QuickHeal	10.00	2009.05.15	-
ClamAV	0.94.1	2009.05.15	-
Comodo	1157	2009.05.08	-
DrWeb	5.0.0.12182	2009.05.15	-
eSafe	7.0.17.0	2009.05.14	-
eTrust-Vet	31.6.6507	2009.05.15	-
F-Prot	4.4.4.56	2009.05.15	-
F-Secure	8.0.14470.0	2009.05.15	-
Fortinet	3.117.0.0	2009.05.15	-
GData	19	2009.05.15	Win32:MDrop-A
Ikarus	T3.1.1.49.0	2009.05.15	-
K7AntiVirus	7.10.735	2009.05.14	-
Kaspersky	7.0.0.125	2009.05.15	-
McAfee	5616	2009.05.15	-
McAfee+Artemis	5616	2009.05.15	-
McAfee-GW-Edition	6.7.6	2009.05.15	Trojan.Crypt.XPACK.Gen
Microsoft	1.4602	2009.05.15	-
NOD32	4080	2009.05.15	-
Norman	6.01.05	2009.05.14	-

(ro)BOTNET(works)

- Zombi ve roBOTlardan oluşan yıkım orduları!
- Uzaktan yönetilebilirler

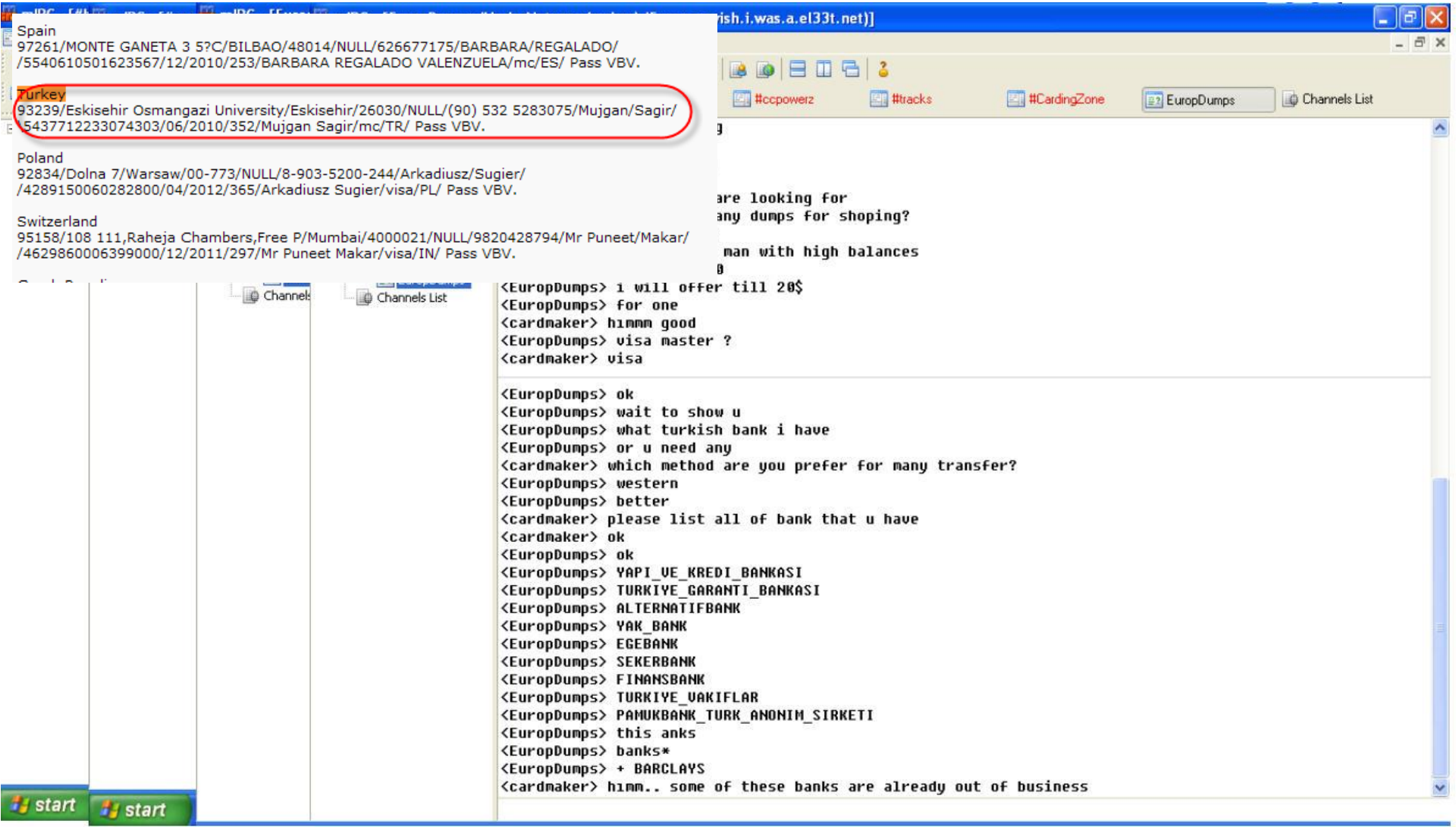
Nasıl Çalışır?



Ne Amaçla Kullanılır

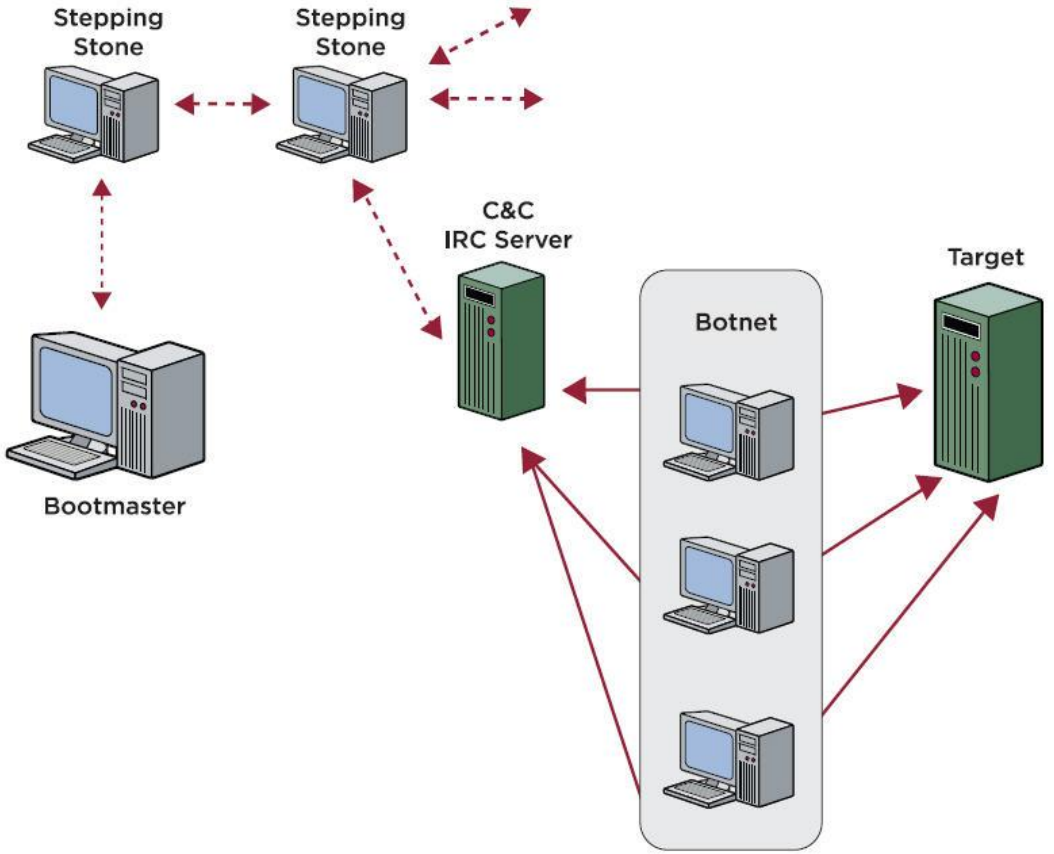
- Yeraltı siber ekonomisinin en güçlü kazanç kapısı
- SPAM maçlı kullanılabilir
- Google reklamlarından para kazanma amaçlı
- Google Adword'de öne çıkma veya bir firmayı geri düşürme amaçlı kullanılabilir
- DdoS yapmak için kullanılabilir
- Bilgi çalma amaçlı kullanılabilir

BotNet'ler Üzerinden Toplanan Kredi Kartları



Nasıl Yönetilir?

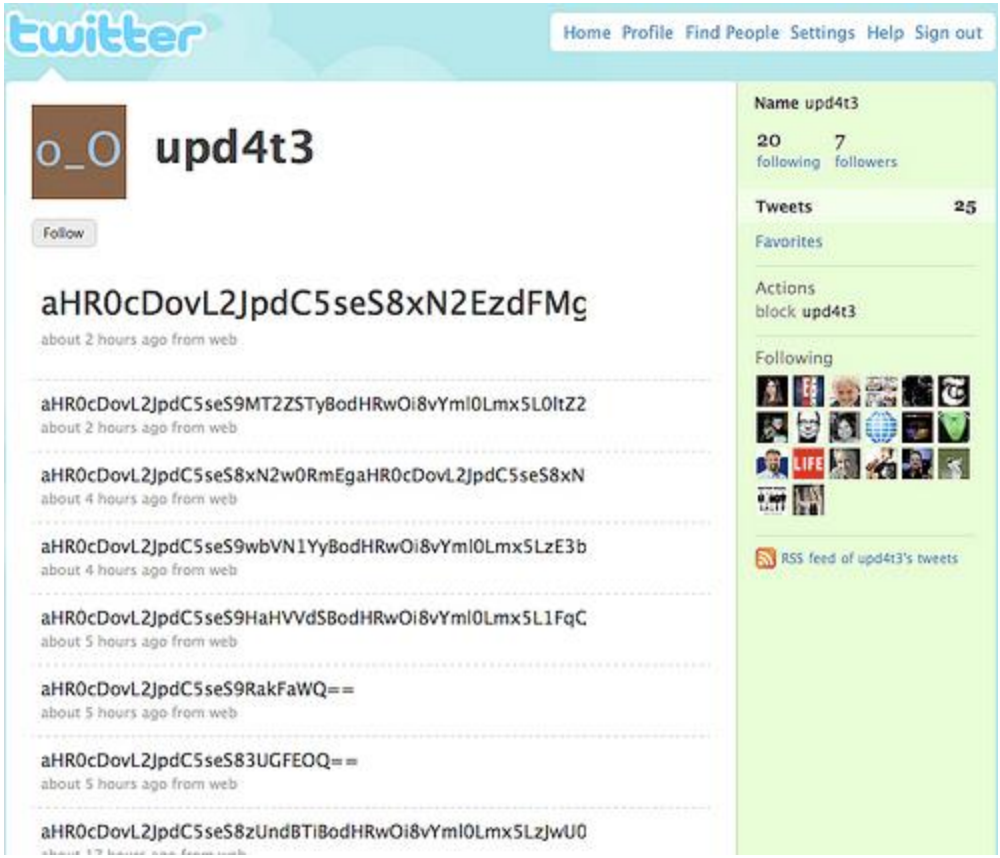
- P2P
- IRC
- WEB
  - HTTPS
- Twitter



Nasıl Farkedilir?

- Garip trafik davranışları
  - SPAM
  - DDoS
- Belirli DNS adreslerine gönderilen istekler
  - Zeus Tracker
- Suç amaçlı kullanılan botnet yönetim IP adreslerine yapılan bağlantılar
  - Russian Business Network

BotNet Yazılımları



FastFlux Nedir?

- Bir atlatma tekniğidir
- Genellikle zararlı içerik yayan sitelerin ip tabanlı kapatılmasını/engellenmesini önlemek için kullanılır
- Teknik açıklama: Domain isimlerinin düşük TTL kullanılarak binlerce farklı IP adresi üzerinden sunulması
  - www.zararlicerik.com = 5000 farklı IP adresi TTL değeri 30 dakika

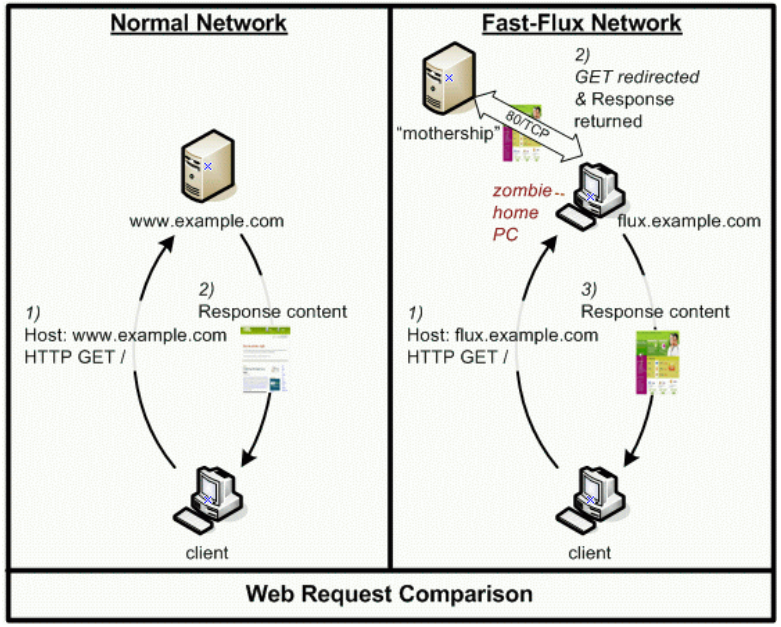
FastFlux Örneği

- Saldırgan zararlı içerikli bir sayfa yapar
- Bunu düşük TTL değeriyle onbinlerce farklı sisteme yönlendirir(botnet)
- Phishing vs için mail gönderir
- Maili alan herkes farklı sunucuya bağlantı kurmaya çalışır
- IP adresi belirlenip engellense

bile birkaç dakika sonra farklı

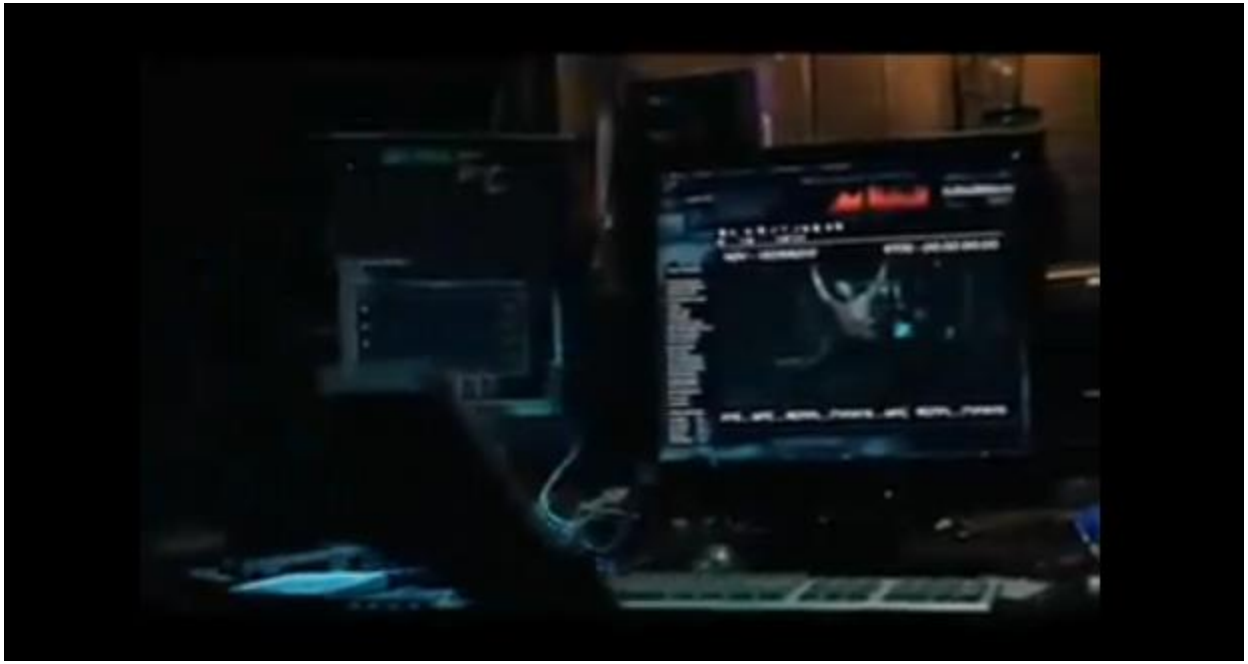
bir IP adresinden tekrar yayın

yapılır...



FastFlux Networks

Untraceable Filmi



FastFlux Networks-Örnek

```
[root@seclabs ~]# dig fastflux.bga.com.tr
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.6.1-P1 <<>> fastflux.bga.com.tr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13652
;; flags: qr rd ra; QUERY: 1, ANSWER: 60, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;fastflux.bga.com.tr.           IN      A

;; ANSWER SECTION:
fastflux.bga.com.tr.    15      IN      A       34.2.3.4
fastflux.bga.com.tr.    15      IN      A       45.2.3.4
fastflux.bga.com.tr.    15      IN      A       65.2.3.4
fastflux.bga.com.tr.    15      IN      A       78.2.3.4
fastflux.bga.com.tr.    15      IN      A       81.2.3.4
fastflux.bga.com.tr.    15      IN      A       88.2.3.4
fastflux.bga.com.tr.    15      IN      A       90.2.3.4
fastflux.bga.com.tr.    15      IN      A       91.2.3.4
fastflux.bga.com.tr.    15      IN      A       111.2.3.4
fastflux.bga.com.tr.    15      IN      A       112.2.3.4
fastflux.bga.com.tr.    15      IN      A       113.2.3.4
fastflux.bga.com.tr.    15      IN      A       114.2.3.4
fastflux.bga.com.tr.    15      IN      A       115.2.3.4
fastflux.bga.com.tr.    15      IN      A       122.2.3.4
fastflux.bga.com.tr.    15      IN      A       152.3.0.4
fastflux.bga.com.tr.    15      IN      A       1.2.3.3
fastflux.bga.com.tr.    15      IN      A       1.2.3.4
fastflux.bga.com.tr.    15      IN      A       1.2.3.24
fastflux.bga.com.tr.    15      IN      A       1.2.3.40
fastflux.bga.com.tr.    15      IN      A       1.2.3.44
fastflux.bga.com.tr.    15      IN      A       1.2.3.45
fastflux.bga.com.tr.    15      IN      A       1.2.3.46
fastflux.bga.com.tr.    15      IN      A       1.2.3.47
fastflux.bga.com.tr.    15      IN      A       1.2.3.48
fastflux.bga.com.tr.    15      IN      A       1.2.3.49
fastflux.bga.com.tr.    15      IN      A       1.2.3.99
fastflux.bga.com.tr.    15      IN      A       1.2.23.4
fastflux.bga.com.tr.    15      IN      A       1.2.30.4
fastflux.bga.com.tr.    15      IN      A       1.2.31.4
fastflux.bga.com.tr.    15      IN      A       1.2.32.4
fastflux.bga.com.tr.    15      IN      A       1.2.33.4
fastflux.bga.com.tr.    15      IN      A       1.2.34.4
fastflux.bga.com.tr.    15      IN      A       1.2.35.4
fastflux.bga.com.tr.    15      IN      A       1.2.36.4
fastflux.bga.com.tr.    15      IN      A       1.2.37.4
```

FastFlux Çeşitleri

- Basit fast flux
  - İllegal web sitesi farklı IP adreslerinde host edilir
- Name Server (NS) fluxing
  - DNS sunucular farklı IP adreslerinde host edilir
  - Böylece Ip yerine domain adından engelleme yapılması da zorlaşır
- Double flux
  - Hep web sayfalarının IP adresleri hem de DNS sunucu IP adresleri farklı IP adreslerinde host edilir

Fast Flux Engelleme

- Fast flux amaçlı kullanılan botların bulunması ve kapatılması
- Fast flux için kullanılan domain isimlerinin kayıtlarının tüm dünyadan silinmesi

DDoS Saldırılarında Amaç

- Sistemlere sızma girişimi değildir!!
- Bilgisayar sistemlerini ve bunlara ulaşım yollarını işlevsiz kılmak
- Web sitelerinin ,

E-postaların, telefon

sistemlerinin çalışmaması

- Para kazancı

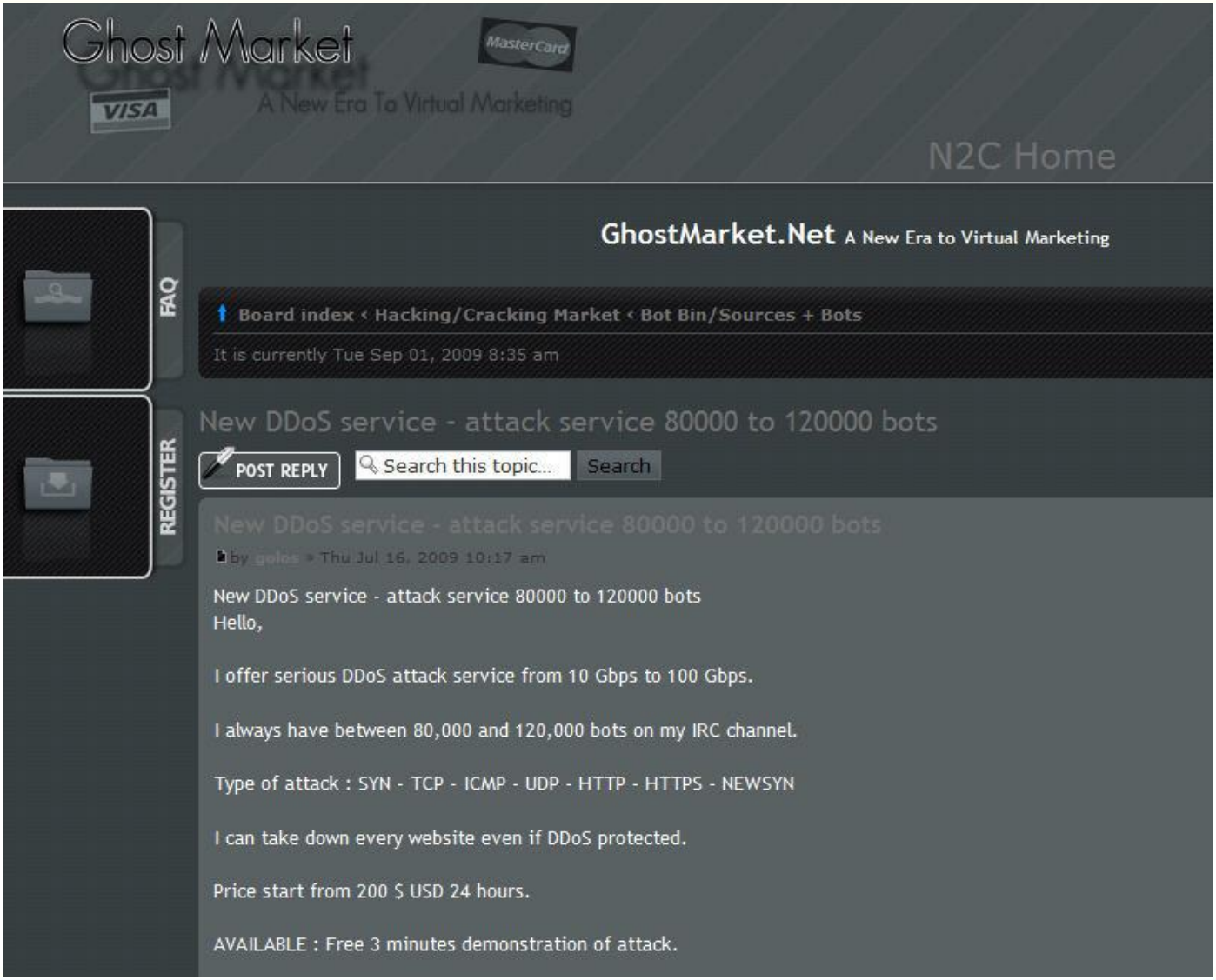
Kim/Kimler yapar?

- Hacker grupları
- Devletler
- Sıradan kullanıcılar
- Ticari şirketler
- Canı sıkılan bilgisayar kurtları

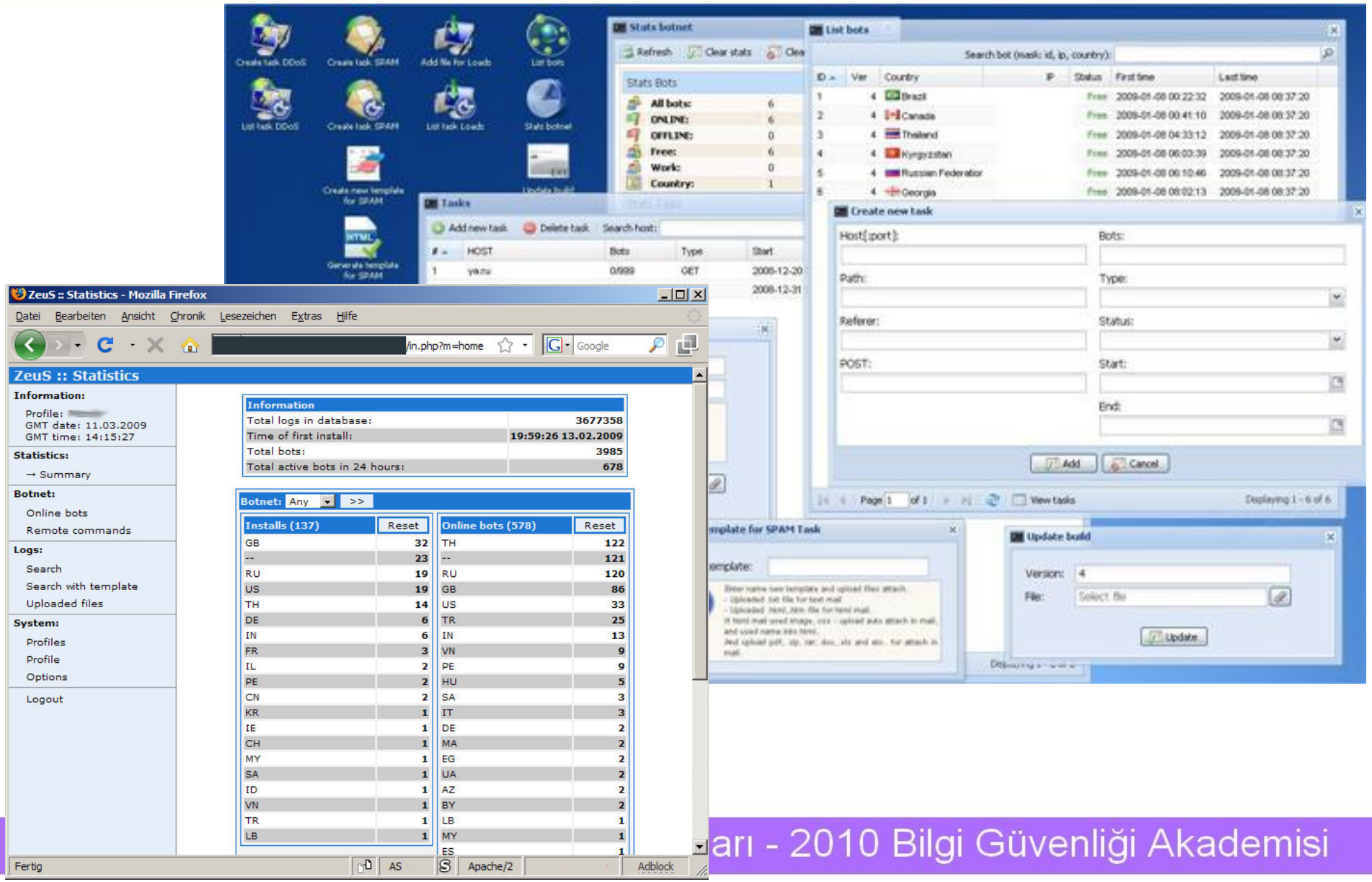
Kimler Neden Yapar?

- Ev kullanıcıları (ADSL vs)
  - Küçük sitelere HTTP GET Flood şeklinde
  - Genelde tehlikesizdirler
- Hackerlar/Profesyoneller
  - Botnet oluştururken sadece son kullanıcılardan değil, sunucu sistemlerden faydalanırlar
  - Bir sunucu ~1000 istemci gücünde trafik üretebilir
  - Özellikle Linux sunuculardaki güvenlik açıklıkları çok kullanılır
- Ellerinde sağlam kaynaklar vardır
  - Bazıları bu kaynakları satar(RBN)
  - Günlük 10 Gb atak 300 $ vs

BotNet Satın Alma



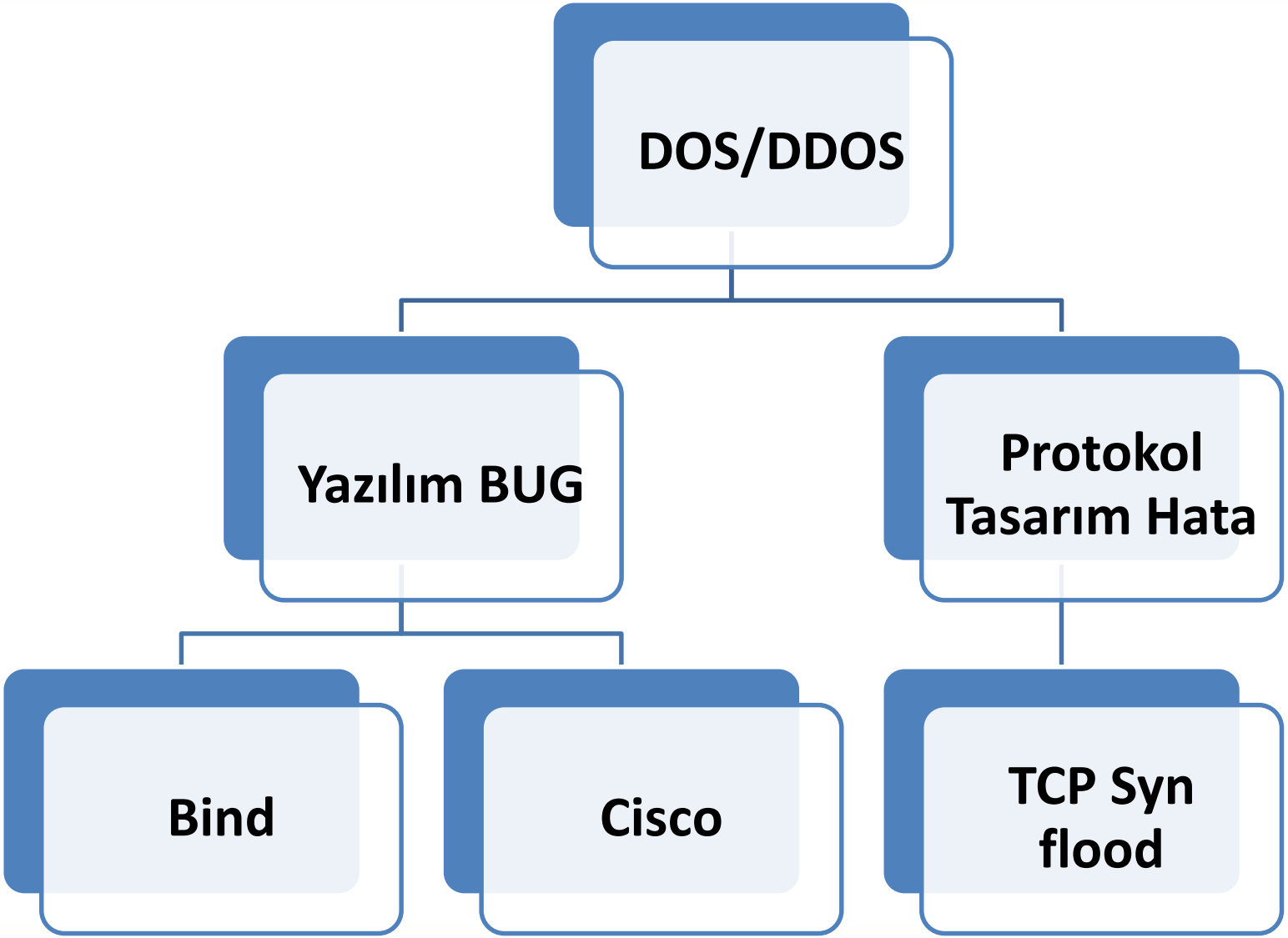
Ne kadar zordur?



Niye Yapılır?

- Sistemde güvenlik açığı bulunamazsa zarar verme amaçlı yapılabilir
  - Ya benimsin ya ...
- Politik sebeplerden
- Ticari sebeplerle
- Can sıkıntısı & karizma amaçlı
  - Bahis amaçlı(forumlarda)

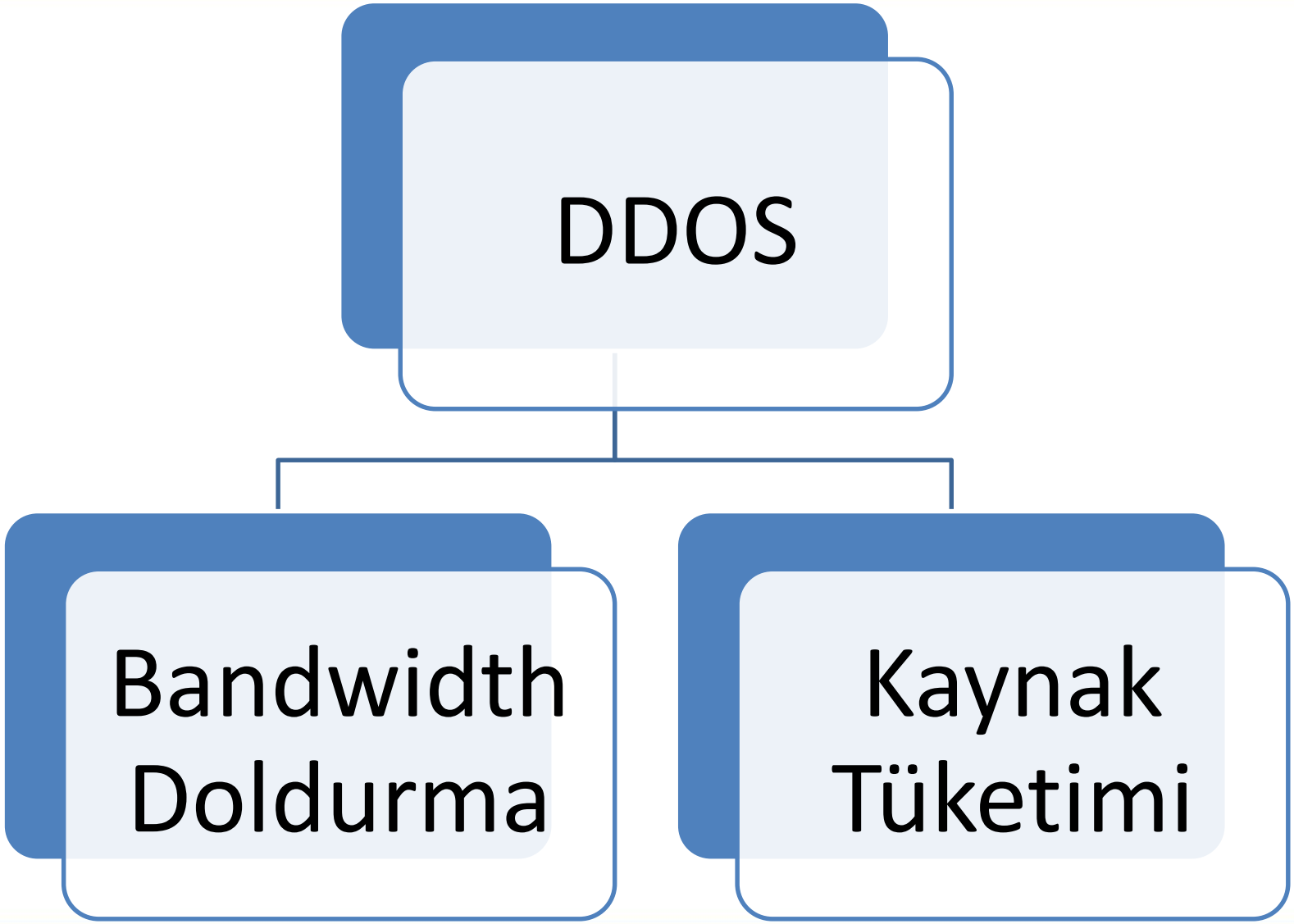
Neden Kaynaklanır?



DDOS Sonuçları

- Finansal kayıplar
- Prestij kaybı
- Zaman kaybı ☺

DDoS Çeşitleri



DOS/DDOS Çeşitleri

- Bandwidth şişirme
  - Udp flood, icmp flood (diğer tüm tipler)
- Kaynak tüketimi(Firewall, server)
  - Synflood, ACK/FIN flood, GET/POST Flood, udp flood
- Programsal hata
  - Bind DOS
- Protokol istismarı
  - DNS amplification DOS
- Sahte IP kullanarak/ Gerçek IP kullanarak

DOS/DDOS Çeşitleri-II

- Her protokole özel DoS/DDoS saldırı yöntemi vardır
  - ARP, Wireless
  - IP
    - İp flooding
  - ICMP
    - İcmp flooding, smurf
  - TCP
    - Syn flood, tcp null flood
  - UDP
    - Udp flood
  - DHCP/SMTP/HTTP/HTTPS/DNS

DDOS-1:Bandwidth Şişirme

- Önlemenin yolu yoktur
  - Sürahi bardak ilişkisi
- ISP seviyesinde engellenebilir...
- L7 protokolleri kullanılarak yapılan DDOS'larda saldırı trafiği çeşitli yöntemlerle ~6'da birine düşürülebilir
  - HTTP GET flood 400 Byte
  - IP Engelleme sonrası sadece syn 60 byte

DDOS-II:Ağ/güvenlik cihazlarını yorma

- Amaç ağ-güvenlik sistemlerinin kapasitesini zorlama ve kaldıramayacakları kadar yük bindirme
- Session bilgisi tutan ağ/güvenlik

Cihazlarının kapasitesi sınırlıdır

Uygulamaya Özel DoS

- Uygulamaya özel DoS saldırıları
- Programlama hatalarından kaynaklanır
- Güncelleme yaparak korunulabilir

Secunia Advisory SA26636

Apache mod_proxy "date" Denial of Service Vulnerability

Secunia Advisory	SA26636
Release Date	2007-08-30
Last Update	2007-09-10
Popularity	19,878 views
Comments	0 comments
Criticality level	Less critical
Impact	DoS
Where	From remote
Authentication level	*Available in Customer Area*
Report reliability	*Available in Customer Area*
Solution Status	Vendor Patch

Eski yöntemler

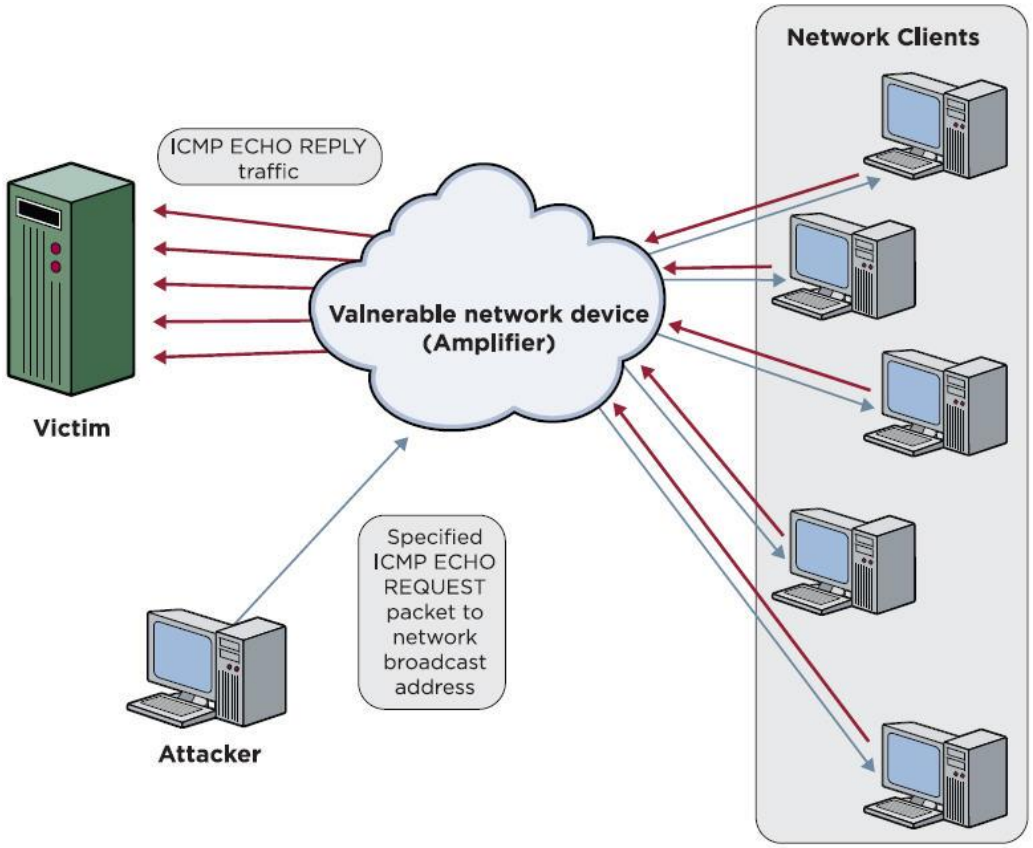
- DDoS saldırıları en çok 2000'li yıllarda medyanın dikkatini çekmiştir
  - Amazon
  - Ebay
  - Yahoo
  - Root Dns saldırıları
- Günümüzdeki DDoS kaynaklarının çoğu eski tip DDoS ataklarını ve araçlarını anlatır
- Günümüzde eski tip yöntem, araç kullanan DDoS saldırılarına rastlamak çok zor

Eski Yöntem DDoS Saldırıları

- Smurf
- Teardrop
- Ping Of Death
- Land Attack

Smurf atağı

ICMP ve UDP Paketleri Broadcast olarak gönderilebilir



Tek bir paket gönderilerek milyonlarca cevap dönülmesi sağlanabilir(di)

Smurf Atağı Artık Çalışmaz. Neden ?

- Tüm router ve işletim sistemleri default olarak broadcaste gelen ICMP paketlerine cevap vermez!

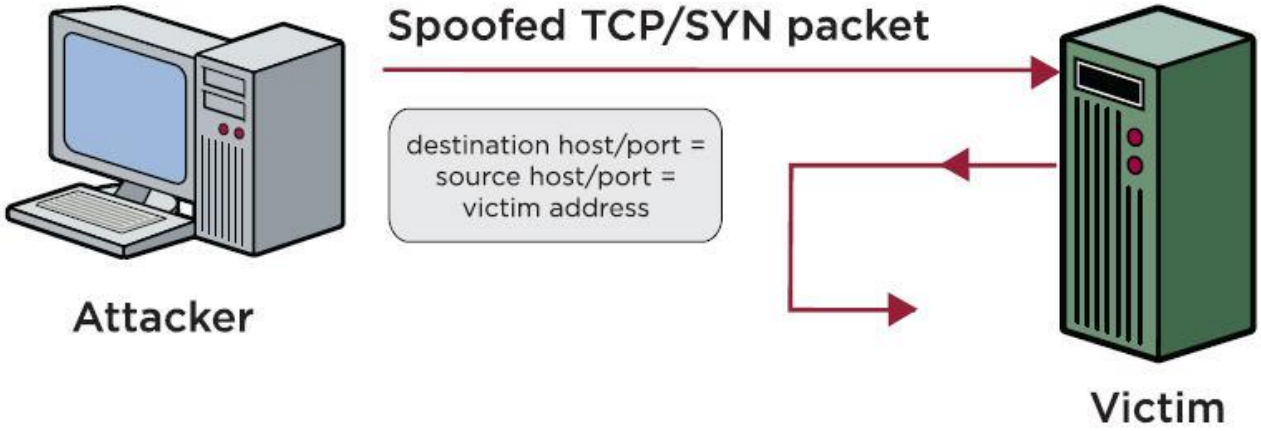
```
root@seclabs:~# sysctl
net.ipv4.icmp_echo_ignore_broadcasts
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

Tear Drop

- Saldırgan parçalanmış paket gönderir ve paketlerin offset değerleriyle oynar
- Paketi alan hedef sistem birleştirme işlemini düzgün yapamadığı için reboot eder
- Günümüzde işlemez bir yöntemdir!
- Tüm işletim sistemleri gerekli yamaları çıkarmıştır

Land

- Hedef sisteme kaynak IP ve hedef IP adresi aynı olan paketler(hedef sistemin IP adresi kayna, hedef sistemin IP adresi hedef) gönderilerek sistemin çakılması sağlanır
- Günümüzde çalışmaz!
- Tüm işletim sistemleri gerekli yamaları geçmiştir.



Eski Araçlar...

Table 3-1 DDoS tools and attack methods

Tools	Flooding or Attack Methods
Trin00	UDP
Tribe flood network	UDP, ICMP, SYN smurf
Stacheldracht and variants	UDP, ICMP, SYN smurf
TFN 2K	UDP, ICMP, SYN smurf
Shaft	UDP, ICMP, SYN combo
Mstream	Stream (ACK)
Trinity, Trinity v3	UDP, SYN, RST, Random Flag, ACK, Fragment

'Zombiler'

DDoS ataklarını gerçekleştirirken yakalanmamak için "zombi" denilen küçük programcıkların kullanıldığından s
bilgisayarın hedeflere yönlendirilmesi sağlanarak, saldırıyı yapan kişinin IP adresininde gizlenmesi sağlanır. Zom
yerleştirilen zombiler kendi bünyesindeki daemonlar vasıtasıyla belirli bir porttan (1524 tcp, 27665 tcp, 2744 u
çok Unix ve Linux tabanlı sistemlerde zombiler kullanılsada Windows tabanlı sistemlerde de zombiler kullanılma

DDoS için kullanılan araçlar:

_ Trinoo(Trin00)
_ The Tribe Flood Network (TFN)
_ Stacheldraht
_ Trinity
_ Shaft
_ Tribe Flood Network 2K (TFN2K)
_ MStream

Günümüzde tercih edilen yöntemler

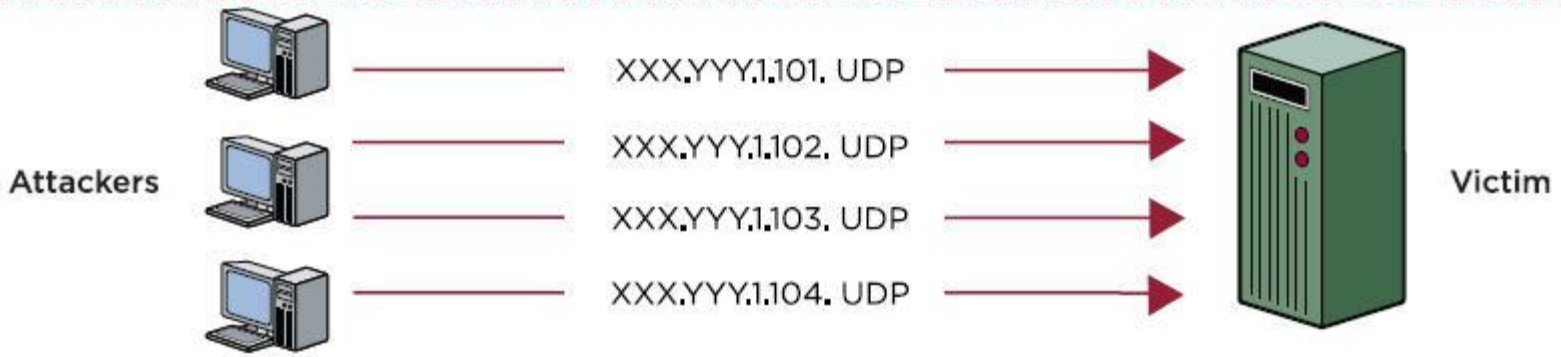
- Eski araçlar, eski yöntemler günümüzde çalışmaz!
- Yeni Yöntemler
  - SYN Flood *
  - HTTP Get / Flood *
  - UDP Flood *
  - DNS DOS
  - Amplification DOS saldırıları
  - BGP Protokolü kullanarak DOS
  - Şifreleme-Deşifreleme DOS saldırıları
- * ‘lı saldırılar eskiden de yapılırdı

Syn Flood

- Hedef sisteme milyonlarca sahte IP adresinden geliyormuş gibi SYN bayraklı TCP paketleri gönderilir
- Günümüzde de en sık tercih edilen DDoS saldırı tipidir
- Yapanı bulmak imkansıza yakındır

UDP Flood

- UDP kullanılarak gerçekleştirilir
- Genellikle sahte IP adresleri tercih edilir
- Ciddi risk barındırmaz
- Kolay engellebilir(!)
- Standart bir engelleme yöntemi yoktur
  - Port kapama
  - Rastgele oturum kapama

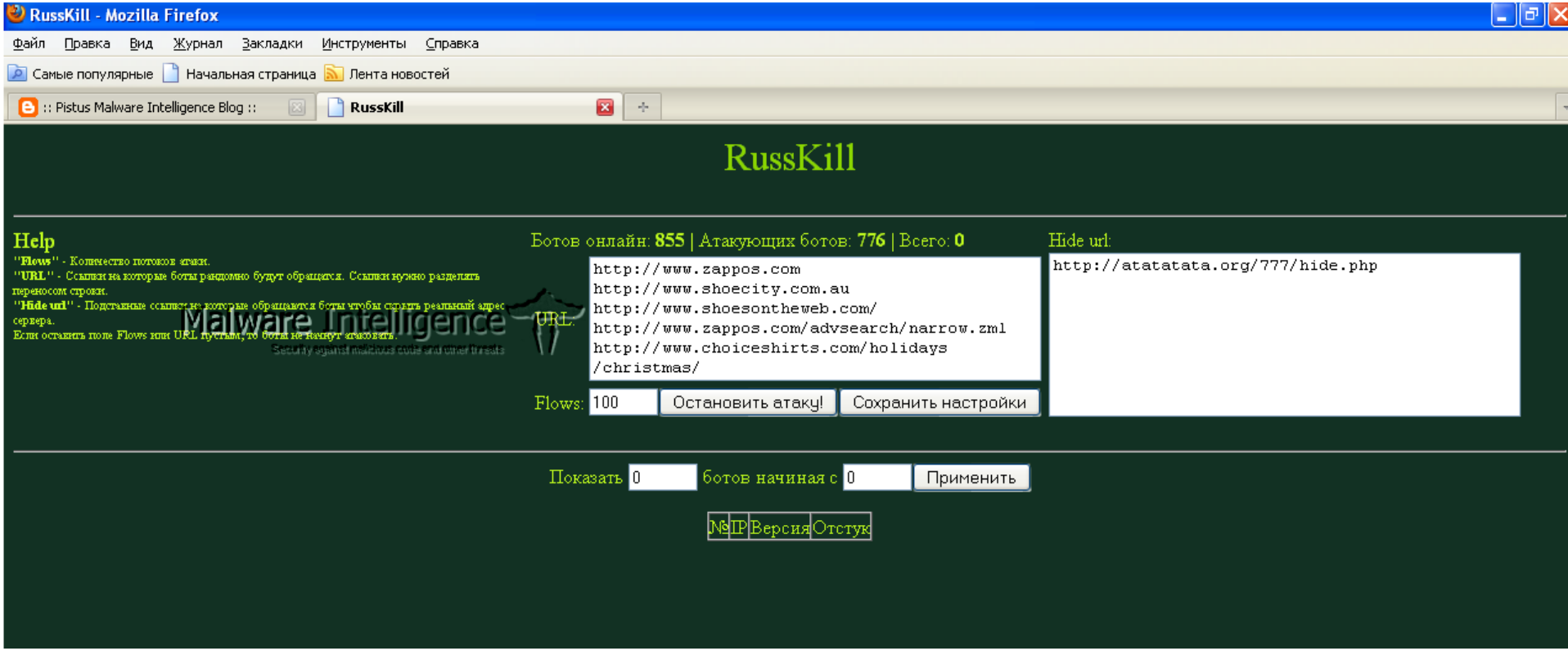


Yeni Araçlar

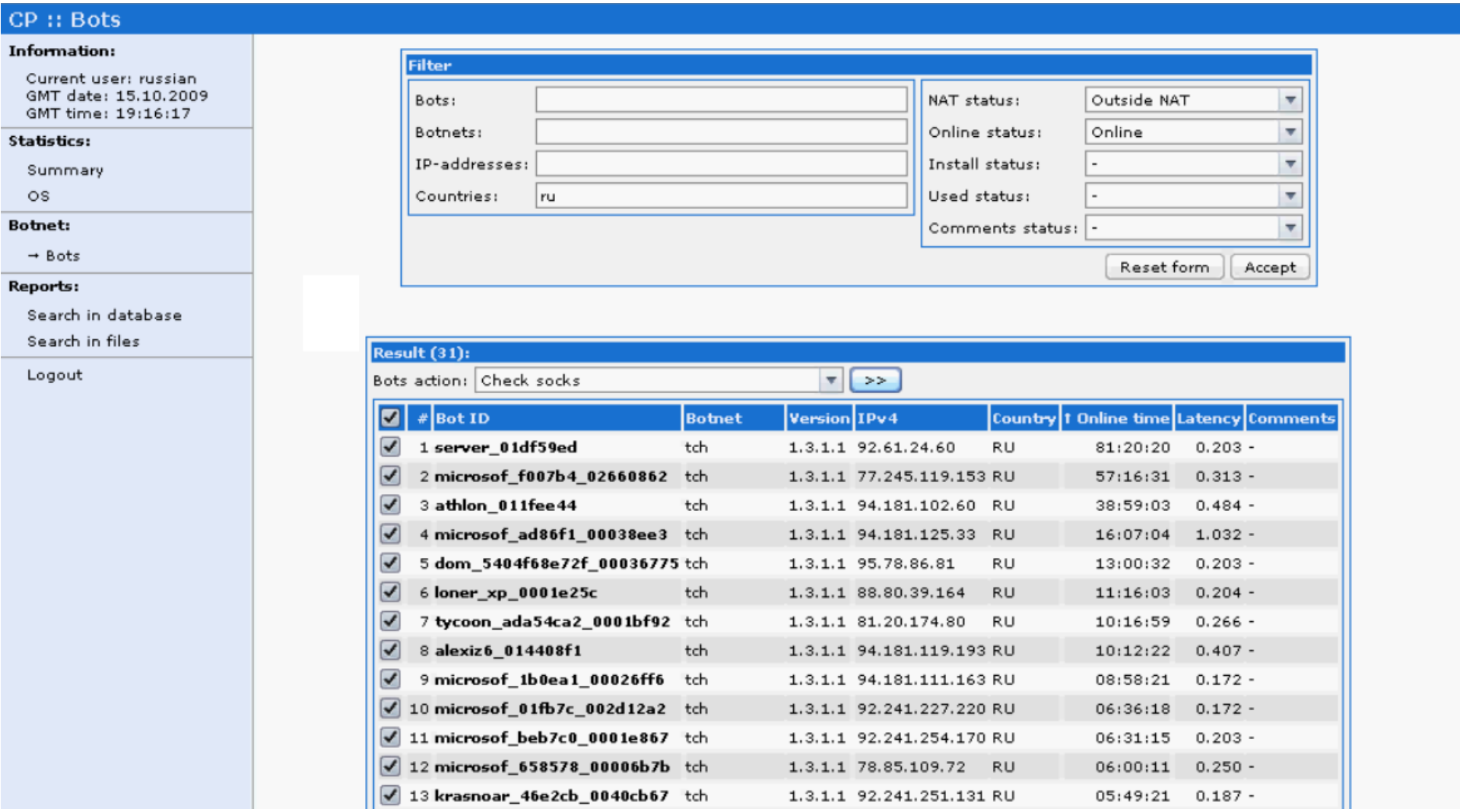
- Hping
- Juno (eskiden de kullanılırdı)
- Netstress ☺
- Daha çok BotNet yazılımları kullanılır
  - Zeus Botnet
  - Yes Exploit System
  - Russ Kill

Kolay Kullanımlı BotNet

RussKill


RussKill - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
Самые популярные Начальная страница Лента новостей
:: Pistus Malware Intelligence Blog ::
RussKill
RussKill
Help
"Flows" - Количество потоков атаки.
"URL" - Ссылки на которые боты рандомно будут обращатся. Ссылки нужно разделять переносом строки.
"Hide url" - Подставные ссылки на которые обращаются боты чтобы скрыть реальный адрес сервера.
Если оставить поле Flows или URL пустым, то боты не начнут атаковать.
Malware Intelligence
Security against malicious code and other threats
Ботов онлайн: 855 | Атакующих ботов: 776 | Всего: 0
URL:
http://www.zappos.com
http://www.shoecity.com.au
http://www.shoesontheweb.com/
http://www.zappos.com/advsearch/narrow.zml
http://www.choiceshirts.com/holidays
/christmas/
Flows: 100
Остановить атаку!
Сохранить настройки
Hide url:
http://atatatata.org/777/hide.php
Показать 0 ботов начиная с 0 Применить
№ IP Версия Отстук

Zeus


CP :: Bots
Information:
Current user: russian
GMT date: 15.10.2009
GMT time: 19:16:17
Statistics:
Summary
OS
Botnet:
→ Bots
Reports:
Search in database
Search in files
Logout
Filter
Bots:
Botnets:
IP-addresses:
Countries: ru
NAT status: Outside NAT
Online status: Online
Install status: -
Used status: -
Comments status: -
Reset form
Accept
Result (31):
Bots action: Check socks
>>
Bot ID Botnet Version IPv4 Country ↑ Online time Latency Comments
1 server_01df59ed tch 1.3.1.1 92.61.24.60 RU 81:20:20 0.203 -
2 microsof_f007b4_02660862 tch 1.3.1.1 77.245.119.153 RU 57:16:31 0.313 -
3 athlon_011fee44 tch 1.3.1.1 94.181.102.60 RU 38:59:03 0.484 -
4 microsof_ad86f1_00038ee3 tch 1.3.1.1 94.181.125.33 RU 16:07:04 1.032 -
5 dom_5404f68e72f_00036775 tch 1.3.1.1 95.78.86.81 RU 13:00:32 0.203 -
6 loner_xp_0001e25c tch 1.3.1.1 88.80.39.164 RU 11:16:03 0.204 -
7 tycoon_ada54ca2_0001bf92 tch 1.3.1.1 81.20.174.80 RU 10:16:59 0.266 -
8 alexiz6_014408f1 tch 1.3.1.1 94.181.119.193 RU 10:12:22 0.407 -
9 microsof_1b0ea1_00026ff6 tch 1.3.1.1 94.181.111.163 RU 08:58:21 0.172 -
10 microsof_01fb7c_002d12a2 tch 1.3.1.1 92.241.227.220 RU 06:36:18 0.172 -
11 microsof_beb7c0_0001e867 tch 1.3.1.1 92.241.254.170 RU 06:31:15 0.203 -
12 microsof_658578_00006b7b tch 1.3.1.1 78.85.109.72 RU 06:00:11 0.250 -
13 krasnoar_46e2cb_0040cb67 tch 1.3.1.1 92.241.251.131 RU 05:49:21 0.187 -