ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/temel-kavramlar-dosddos-saldirilari-ve-cesitleri/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Temel%20Kavramlar,%20Dos,%20Ddos%20Sald%C4%B1r%C4%B1lar%C4%B1%20ve%20%C3%87e%C5%9Fitleri.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Standart Güvenlik Bileşenleri
- Gizlilik
- Bütünlük
- Erişilebilirlik

Bunlardan biri olmadan güvenlikten söz edilemez.

(Page 2)

2)

Gelen DDOS saldırısı sizin sahip olduğunuz bant genişliğinden şayet fazlaysa yapılacak çok şey yok esasında. Fakat DDOS saldırılarının büyük çoğunluğu bant genişliğini taşırma şeklinde gerçekleşmez.

(Page 4)

3)

DOS ve DDOS Hakkında Bilinen Yanlış Bilgiler
- Firewall DOS'u engeller.
- IPS DOS'u engeller.
- Linux DOS'a karşı dayanıklıdır.
- DDOS engelleme ürünleri vardır.
- Donanım tabanlı Firewall DOS'u engeller.
- Antivirus DOS'u engeller.

DOS/DDOS engellenemez!

(Page 5)

4)

Genel Kavramlar
- DOS
- DDOS
- Zombi
- BotNet
- IP Spoofing
- FastFlux Networks
- SYN, FIN, ACK, PUSH
- Flood
- RBN (Russian Business Network)

Bu kavramlardan sırayla bahsedilecektir.

(Page 6)

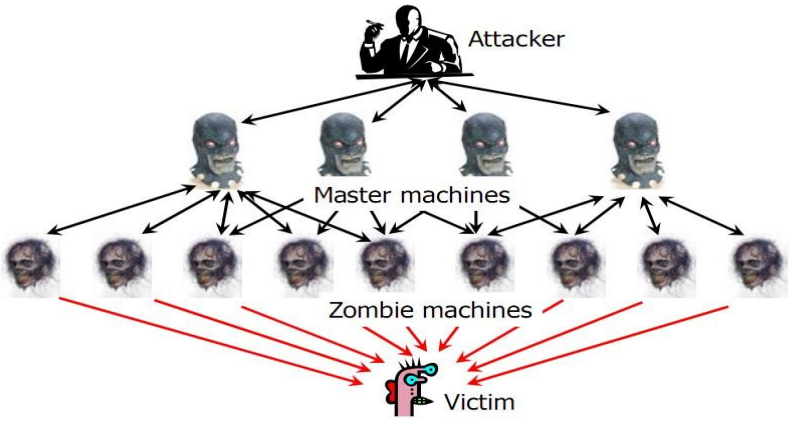
5)

DOS
Sistemleri çalışamaz hale getirmeye yarayan bir saldırı türüdür. DOS saldırılarını engellemek kolaydır.

(Page 7)

6)

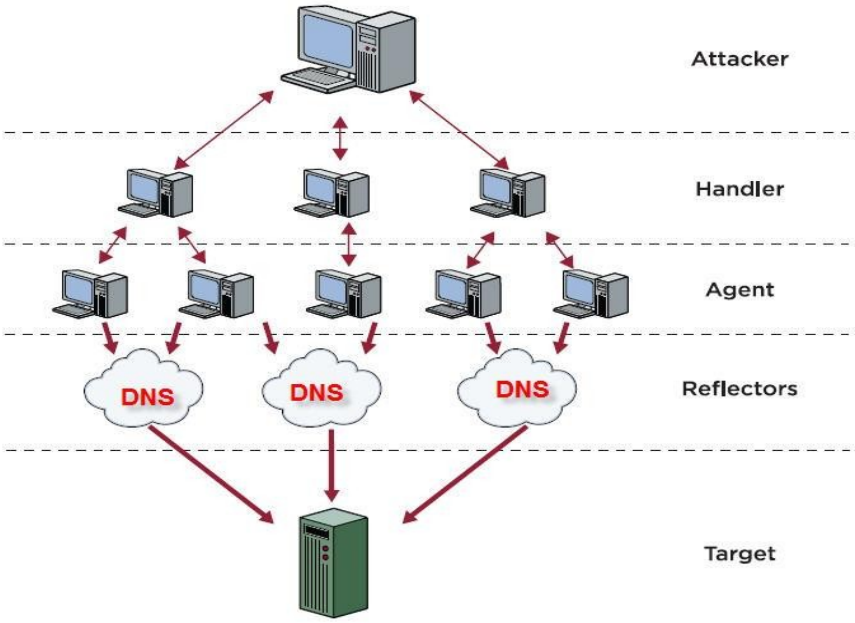
DDOS
Binlerce, yüzbinlerce sistemden organize bir şekilde hedef sisteme yapılan ve sistemin çalışamaz hale getirilmesini sağlayan saldırı türüne denir. Bu saldırı için BotNet'ler kullanılır. Böylece saldırgan kendini gizler.



(Page 8)

7)

DrDOS (Distributed Reflection Denial of Service)
Saldırganın 3. parti cihazlarla saldırdığı ve kendini gizlediği DDOS saldırısına denir.



Fark ettiysen DDOS kavramının bahsedildiği resimde saldırganın önünde bir Master Machines vardı, onun önünde de zombi makinalar vardı ve bu zombi makinalar saldırıyı düzenliyordu. DrDOS'da ise master machines ve zombi machines gibi iki katman var, fakat bir üçüncü katman daha var. O da yukarıdaki resimde görebileceğiniz üzere reflectors diye adlandırılmaktadır.

(Page 9)

8)

Malware
Kötücül bir yazılımdır. Malicious Software kelimelerinin baş harflerinden oluşturulmuştur. Bilişim sistemlerine bu yazılım yüklenerek sistemin kötü amaçlı kullanımı sağlanır.

(Page 10)

9)

Exploit
Hedef sistemin bir zafiyetinden faydalanarak sisteme izinsiz erişimeye exploit etme denir. Aynı zamanda hedef sistemin zafiyetinden faydalanarak sisteme sızma yetkisi veren programlara da (script'lere de) exploit denir. Sistemlerdeki zafiyetler exploit edilerek DOS saldırısı yapılabilir.

(Page 11)

10)

Zombi
Çeşitli açıklıklardan faydalanılarak sistemlerine sızılmış ve arka kapı yerleştirilmiş sistemlere denir. Bir bilgisayarın zombi oluşunun temel sebebi Windows güncellemelerinin yapılmayışıdır.

(page 13)

11)

Botnet
Saldırgan uzaktan herhangi bir hedef sistemi devre dışı bırakmak için yönettiği zombi ordusuna botnet denir.

(Page 15)

12)

Botnet yeraltı siber dünya ekonomisinin en güçlü kazanç kapısıdır. Botnet'ler SPAM yapmak maksadıyla kullanılabilir. Google reklamlarından para kazanma amacıyla kullanılabilir. Google Adword'de öne çıkma veya bir firmayı geri düşürme amacıyla kullanılabilir. DDOS yapmak için kullanılabilir. Saldırganın kimliğini saklayarak bilgi çalabilmesine imkan sağlayabilir.

(Page 17)

13)

IRC Server
MSN'in biraz daha ilkel halini sunan bir iletişim platformudur (protokolüdür). Sesli ve görüntülü iletişim yerine sadece metin tabanlı iletişim imkanı sunar. Hacker'ların sıklıkla kullandığı iletişim ağıdır.

(Page 19)

14)

FastFlux
Fastflux proxy görevi gören ele geçirilmiş sistemlerden oluşan botnet’lerin sürekli değişen ağdaki phishing ve malware sunan siteleri gizlemek için kullandığı bir DNS tekniğidir. Genellikle zararlı içerik yayan siteler IP tabanlı olarak erişime engellenirler. Fakat FastFlux yazılımları ile engellenen sunucunun önündeki botnet'ler kullanılarak tek bir domain için çok sayıda IP adresi çoklaması yapılır ve bu IP adreslerinin ilgili DNS kayıtları sıklıkla değiştirilerek erişimi engellemesi aşılır.

https://www.cyber-warrior.org/Forum/fast-flux-nedir-_426477,0.cwx

(Page 23)

15)

Basit FastFlux
- Engellenen web sitesi farklı farklı IP adreslerinde host edilerek engelleme işlemez olur.

Name Server Fluxing
- Bu sefer DNS sunucu farklı farklı IP adreslerinde host edilir. Böylece IP tabanlı engellenen web sitesi domain tabanlı da engellense bile bu aşılmış olur.

Double Flux
- Hem engellenen web sitesi hem de DNS sunucusu farklı farklı IP adreslerinde host edilir.

(Page 26)

16)

FastFlux Engelleme Yolları
- FastFlux amaçlı kullanılan botların bulunması ve erişime engellenmesi
- FastFlux amaçlı kullanılan domain isim kayıtlarının tüm dünyadan silinmesi

(Page 27)

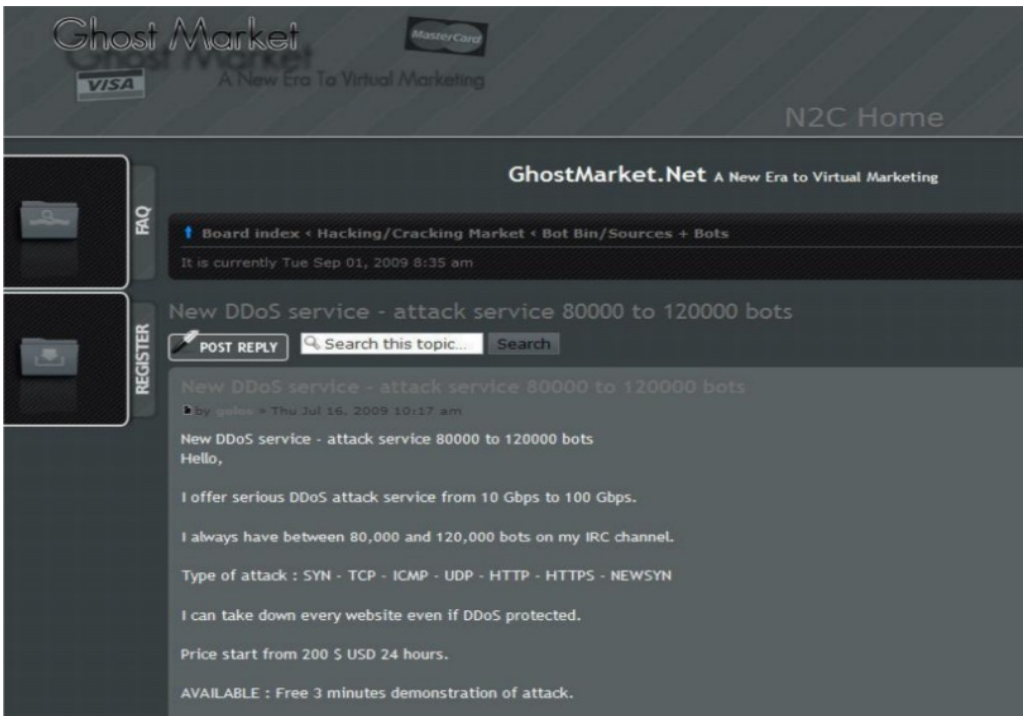
17)

DDOS saldırılarında amaç sisteme sızmak değildir. Sistemleri işlevsiz kılmak, erişilemez kılmaktır. Örneğin epostaların, telefon sistemlerinin çalışamaması gibi. DDOS'u hacker gruplar, devletler, sıradan kullanıcılar, ticari şirketler ve bilgisayar kurtları yapabilir. DDOS'u ev kullanıcıları ADSL vs ile küçük sitelere HTTP GET Flood tekniği ile yapabilirler. Bu genellikle tehlikesizdir. Hacker'lar (Profesyoneller) ise botnet oluştururlar (bu botnet son kullanıcı içerdiği gibi sunucu da içerir) ve botnet'i hedef sisteme musallat ederek DDOS yaparlar.

(Page 28 - 29)

18)

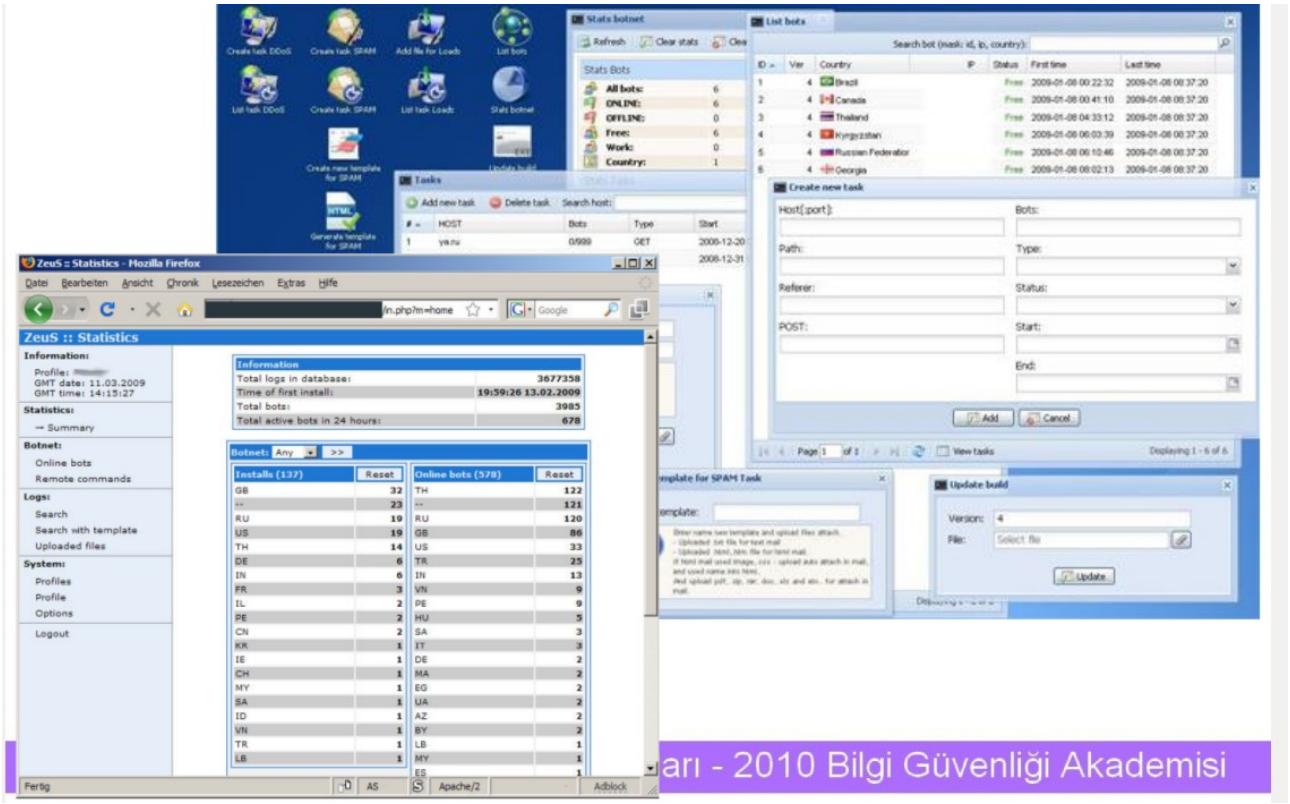
Botnet Satın Alma Sayfası Örneği



(Page 31)

19)

Botnet'leri Kullanmaya Dair Bir Görüntü



Sol alt köşeye bakacak olursak oradaki pencerede botnet ağı ile ilgili istatistikler verilmiş. Örneğin online bot'ları ülke ülke sıralanmış ve bir ülkeden kaç bot var gibi bir bilgi sunulmuş.

(Page 32)

20)

Botnet ile DDOS politik, ticari, keyfi sebeplerden dolayı yapılabilir. Örneğin hedef sistemde açık bulunamadığı takdirde botnet ile DOS yoluna başvurulabilir.

(Page 33)

21)

DDOS Saldırısı Sonuçları
- Finansal kayba neden olur.
- Prestij kaybına neden olur.
- Zaman kaybına neden olur.

(Pag 35)

22)

İki tane DDOS çeşidi vardır:
- Bant genişliğini doldurmaya yönelik DDOS
- Kaynakları tüketmeye yönelik DDOS

(Page 36)

23)

Bant genişliğini şişiren DDOS türlerine örnek olarak UDP Flood ve ICMP flood verilebilir. Kaynak tüketen (Firewall ya da server'ı tüketen) DDOS saldırılarına örnek olarak da Syn Flood, ACK/FIN Flood, GET/POST Flood, UDP Flood verilebilir.

(Page 37)

24)

Her protokole özgü bir DOS/DDOS saldırı yöntemi mevcuttur. Mesela

- IP protokolü : IP Flooding
- ICMP protokolü : ICMP Flooding, Smurf
- TCP protokolü : Syn Flood, TCP Null Flood
- UDP protokolü : UDP Flood

gibi...

(Page 38)

25)

Bant genişliğini şişirmeye yönelik DDOS saldırılarını önlemenin bir yolu yoktur. Yani düşünün: Bir sürahiyi bardağa boşaltmaya kalkarsanız her türlü o taşma olacaktır. Lakin L7 protokolleri kullanılarak yapılan DDOS trafiği altıda birine düşürülebilir. Ayrıca bant genişliğine yönelik bu DDOS saldırıları her ne kadar hedef sistem tarafından önlenemiyor olsa da ISP tarafından önlenmesi mümkündür. Bu yüzden DDOS saldırısı olduğunda kritik bir server'ı yöneten kurban hemen ISP'deki yetkililerle iletişime geçer.

(page 39)

26)

DDOS saldırıları bazen yazılımların kendinden kaynaklanan kusurlardan faydalanılaraktan da yapılabilmektedir. Bu sorun güncelleme yapılarak aşılır.

(Page 41)

27)

Günümüzdeki DDOS kaynaklarının çoğu eski tip DDOS saldırılarını ve araçlarını anlatır. Eski yöntem DDOS saldırıları şunlardır:

- Smurf
- Teardrop
- Ping of Death
- Land Attack

(page 43)

28)

Smurf
Smurf saldırısında saldırgan örneğin bir router'ın broadcast adresine kurban gönderiyormuş gibi bir ICMP paketi gönderir. Bu gönderilen paket broadcast adresine gittiği için router'a bağlı tüm host'lara gidecektir. Router'a bağlı tüm host'lar aldıkları bu ICMP paketine karşılık echo paketi göndermek isteyeceklerdir ve paketi gönderen kısmında kurbanın IP'sini görecekleri için tüm host'lar kurbana paket yollayacaktır. Böylece saldırgan gönderdiği bir paketle kurbana bir sürü host'un paket göndermesini sağlamış olacaktır. Bu paketler kurbanın makinasının taşıyamacağı fazlalıkta olunca da saldırı başarıya ulaşmış olacaktır.

Smurf saldırısı artık kullanılamamaktadır, çünkü tüm router ve işletim sistemleri günümüzde default olarak broadcast'e gelen ICMP paketlerine cevap vermeyecek şekilde yapılandırılmışlardır.

(Page 45)

29)

Tear Drop
Saldırgan paketleri parçalayarak gönderir ve paketlerin sıra numaralarıyla oynar. Paketi alan hedef sistem ise paketleri sıra numaraları manipule edildiğinden düzgün birleştiremeyeceği için sistemi reboot etmek durumunda kalır. Günümüzde bu saldırı yöntemi işe yaramamaktadır. Çünkü tüm işletim sistemleri bu saldırıya karşı bir yama çıkarmışlardır.

(page 46)

30)

Land Attack
A LAND (Local Area Network Denial) attack is a DoS (Denial of Service) attack that consists of sending a special poison spoofed packet to a computer, causing it to lock up. The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address to an open port as both source and destination. This causes the machine to reply to itself continuously.

(https://en.wikipedia.org/wiki/LAND)

31)

Land Attack (cont.)
Hedef sisteme kaynak IP ve hedef IP olarak hedef sistemin IP adresinin olduğu paket gönderilir. Bu paketi yanıtlayan hedef sistem hedef IP kısmında kendi IP'si olacağında kendine paketi yollamış olur. Aldığı pakete tekrar yanıt vermek isteyeceğinden hedef IP kısmında kendi IP'si olacağından yine kendine paketi yollar. Bu böyle devam eder ve kısır döngü sonucu sistem dolar, çalışmaz hale gelir. Günümüzde bu saldırı çalışmamaktadır, çünkü tüm işletim sistemleri bu konuda gerekli yamayı çıkarmışlardır.

(page 47)

32)

Günümüzde Tercih Edilen DOS Saldırı Yöntemleri
- SYN Flood *
- HTTP Get/Flood *
- UDP Flood *
- DNS DOS
- Amplification DOS Attack
- BGP Protokolünü Kullanarak DOS Attack
- Şifreleme-Deşifreleme DOS Attack

NOT: *'lı saldırılar eskiden de yapılırdı.

(page 49)

33)

Syn Flood
Hedef sisteme milyonlarca sahte IP adresinden geliyormuş gibi SYN bayraklı TCP paketleri gönderilir. Hedef sistem bunları belleğinde depolar, fakat gönderdiği paketlere karşılık alamadığından belleğindeki o verileri silmez. Bu yüzden bellek bir süre sonra dolar ve taşar. Günümüzde en sık tercih edilen DOS saldırı yöntemidir. Yapanı bulmak imkansıza yakındır.

(Page 50)

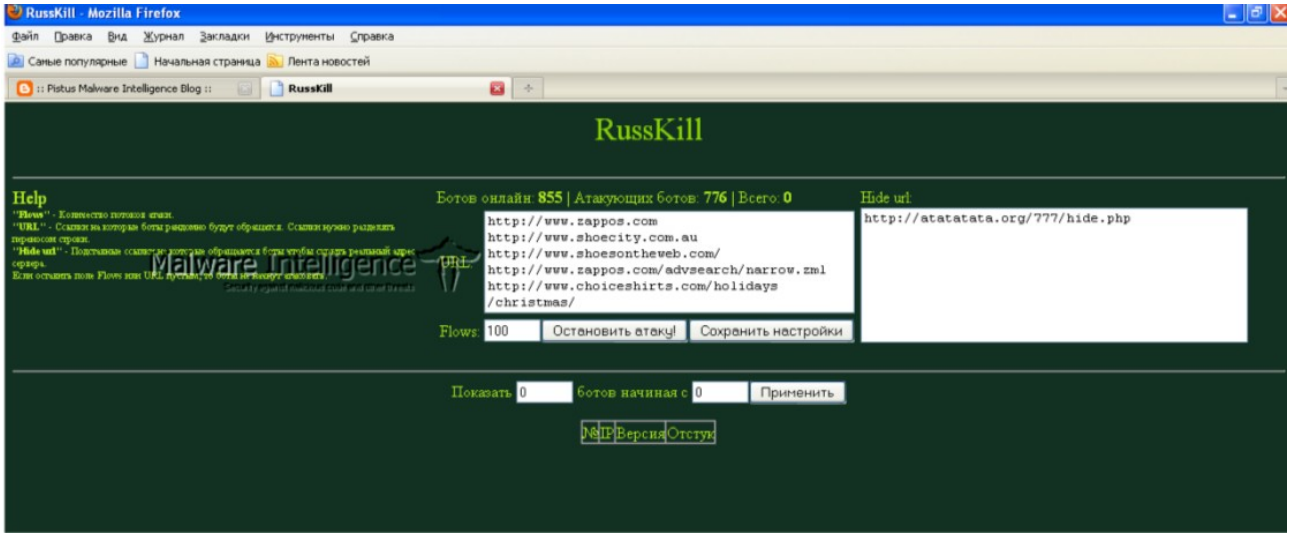
34)

Günümüz DOS Saldırılarını Yapan Araçlar
- Hping
- Juno (eskiden de kullanılırdı)
- Netstress
- BotNet Yazılımları
    - → Zeus Botnet
    - → Yes Exploit System
    - → Russ Kill

(Page 52)

35)

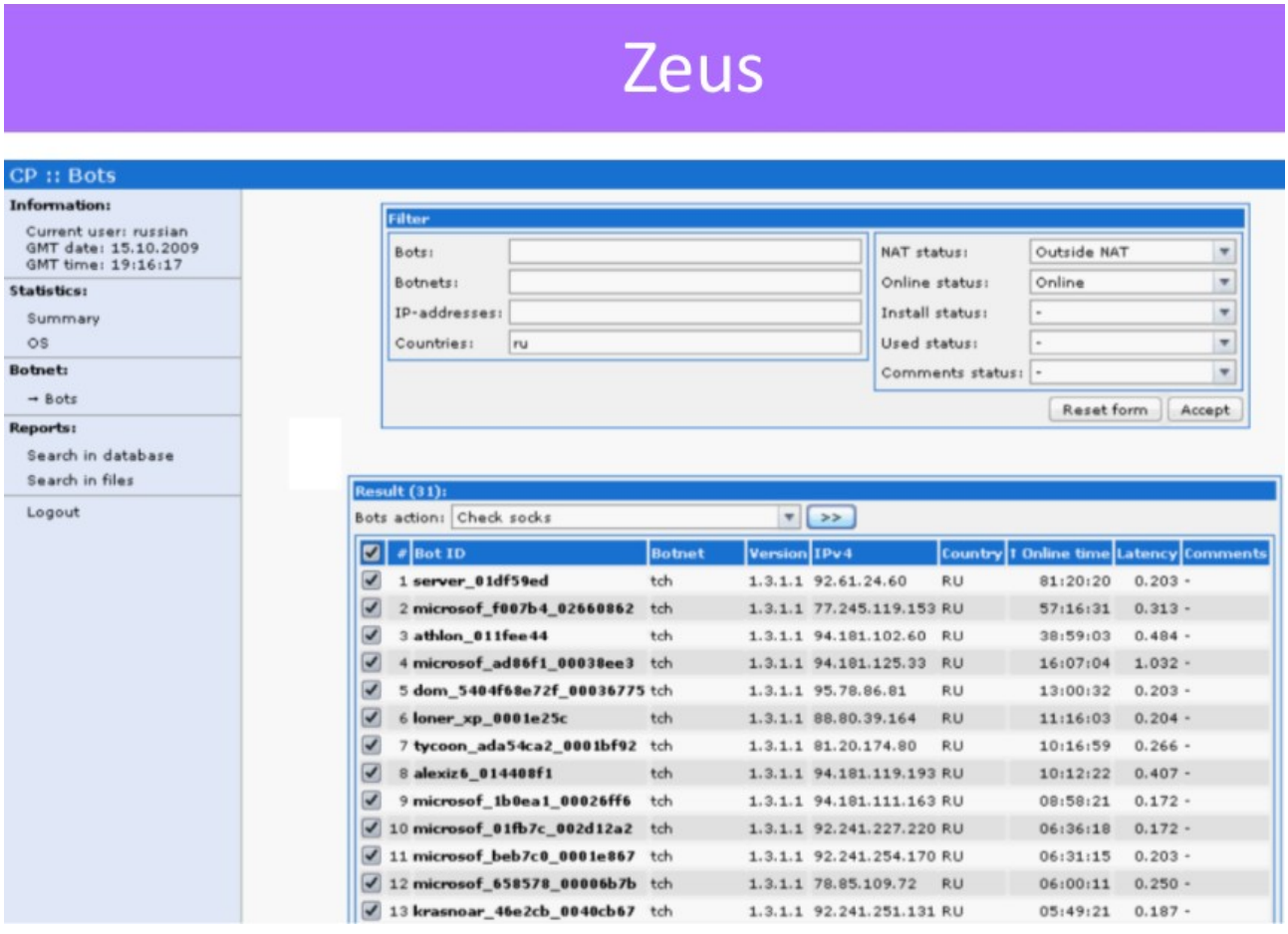
Russ Kill



(Page 54)

36)

Zeus Botnet



(Page 55)