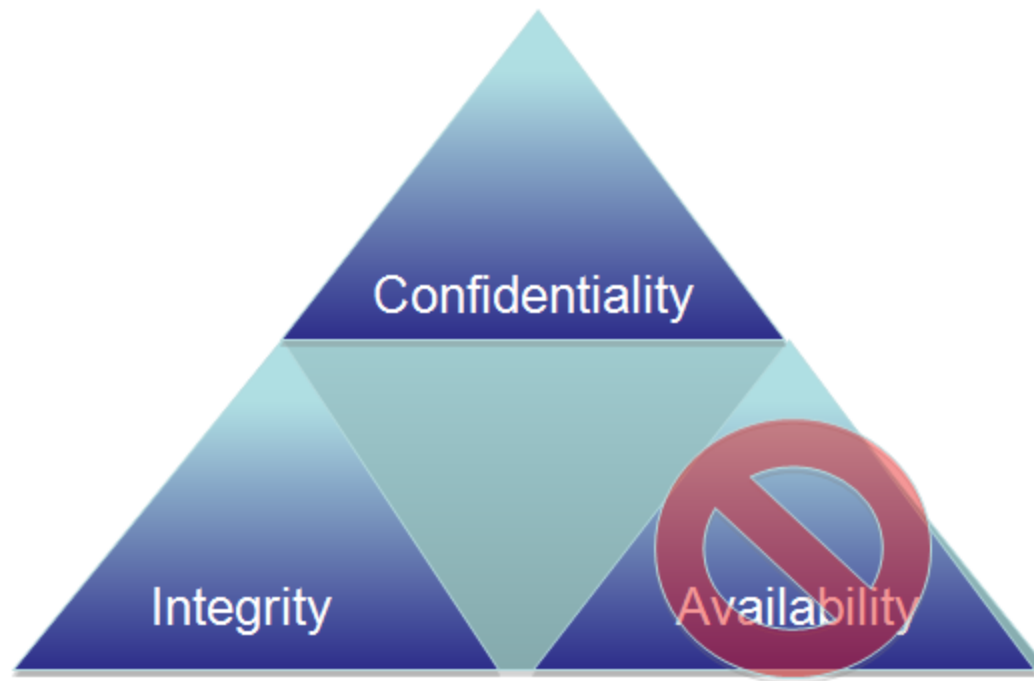


DOS-DDOS-BotNet

Bilgi Güvenliği AKADEMİSİ

Güvenlik ve DOS



Genel Kavramlar

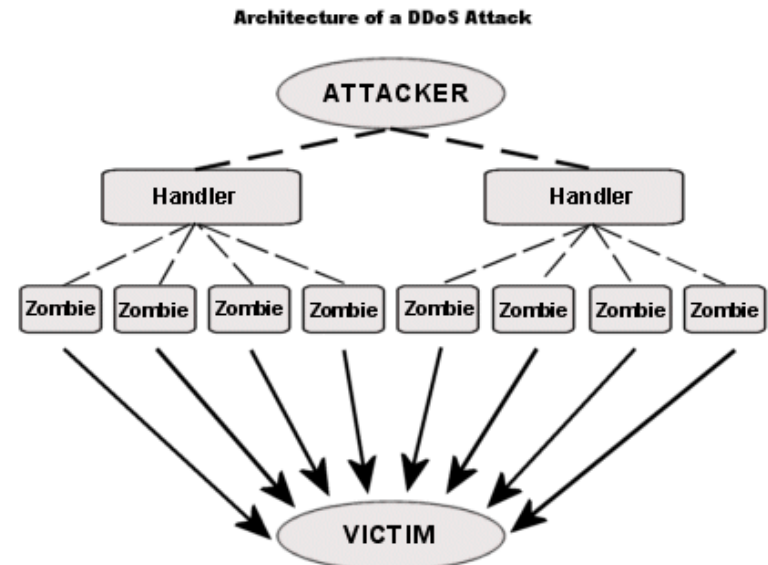
- DOS(Denial Of Service)
- DDOS(Distributed Denial Of Service)
- Zombi
- BotNet(Robot Networks)
- IP Spoofing
- FastFlux networks

DOS Kavramı

- DOS: Sistemi kullanılamaz ya da ulaşılamaz hale getirme çalışmaları.
- Amaç Zarar vermekten çok servis/Hizmet Durdurma.
 - Sisteme sızma değildir!
- Network üzerinden olabileceği gibi yerel sistemlerde de olabilir.
- 2000 yılı Ebay, Yahoo, Amazon gibi büyük firmalar DOS saldırısına maruz kaldı
- 2003 : Microsoft'un web sitesi DOS'a maruz kaldı ve saatlerce ulaşılamaz duruma düştü
- 2007 Türkiye ...
- 2010 DOS kullanarak sanal şantaj...

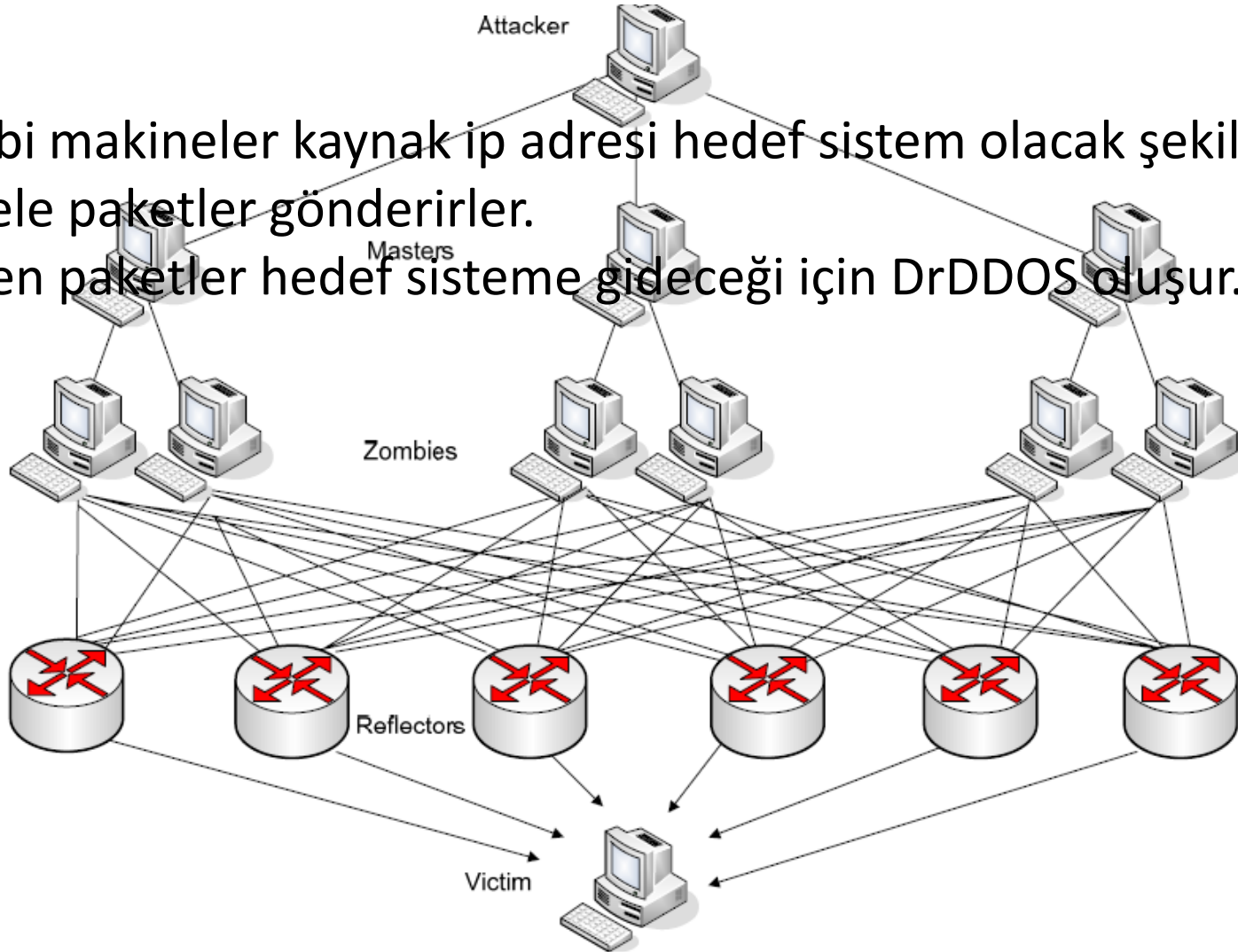
DDOS

- Dağıtık DOS
- DOS'tan Temel farkı iki aşamalı olmasıdır.
 - Saldırgan ilk aşamada Ajan ve zombi olarak kullanacağı sistemleri ele geçirir.
 - Son aşamada Master sistemleri kullanarak zombileri tetikler.
- İstemci – sunucu mimarisi



DrDOS

- Zombi makineler kaynak ip adresi hedef sistem olacak şekilde rastgele paketler gönderirler.
- Dönen paketler hedef sisteme gideceği için DrDDOS oluşur.



Zombi & Botnet

- Zombi: Emir kulu
 - Çeşitli açıklıklardan faydalanılarak sistemlerine sızılmış ve arka kapı yerleştirilmiş sistemler
 - Temel sebebi: Windows yamalarının eksikliği
- BotNet – roBOTNETworks
- Zombilerden oluşan sanal yıkım orduları
- Internette satışı yapılmakta

Master & CC

- Zombileri yöneten sistemler
- CC=Command Center
- Büyük Botnetlerde birden fazla ve dağıtık yapıda olabilir

Amaç?

- Sistemlere sızma girişimi değildir!!
- Bilgisayar sistemlerini ve bunlara ulaşım yollarını işlevsiz kılmak
- Web sitelerinin ,
E-postaların, telefon
sistemlerinin çalışmaması



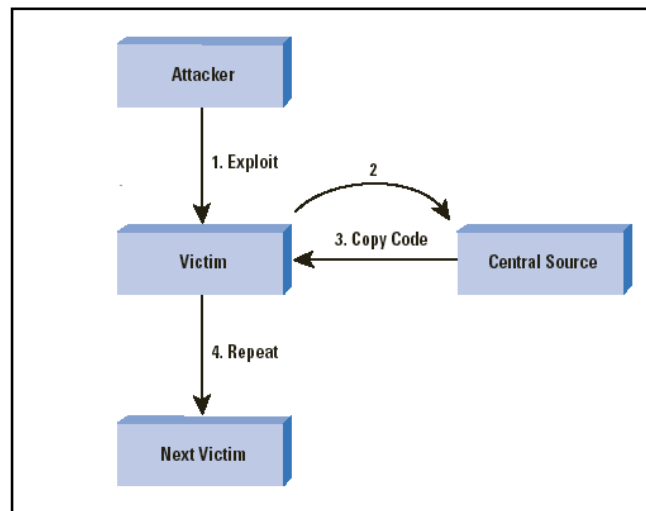
Kim/kimler yapar?

- Hacker grupları
- Devletler
- Sıradan kullanıcılar



DDOS Kaynakları

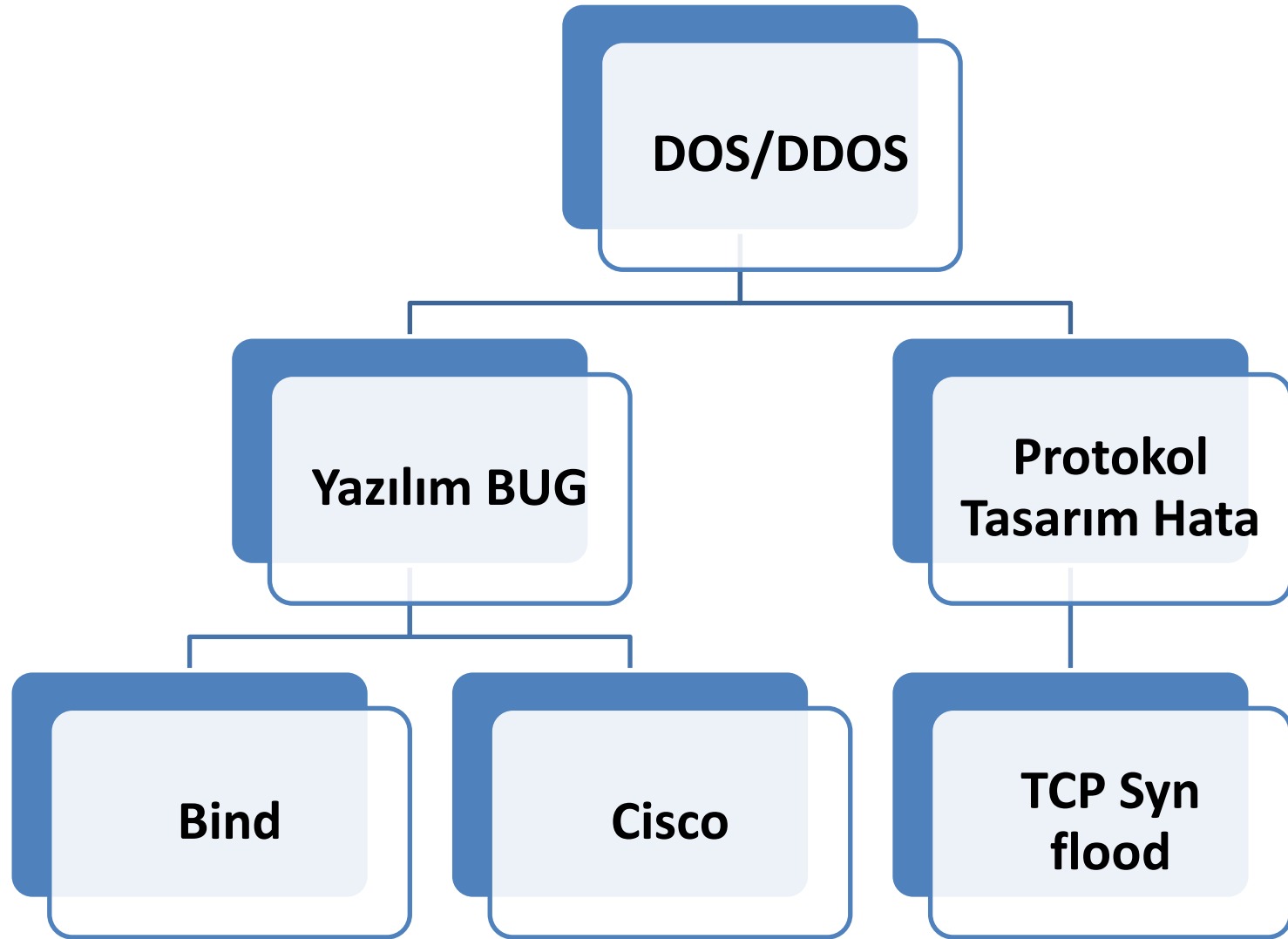
- DDOS için kaynak gerekli
- Kaynaklar
 - Wormlar aracılığı ile elde edilir
 - Bulaşan her makine zombi durumuna düşer ve başka makinelere yaymaya çalışır.



Niye yapılır?

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

Neden kaynaklanır?



DOS'un Sonuçları

- Sisteme erişim yetkisi olan kullanıcıların erişimlerini engellenir.
- Finansal kayıplar
 - Amazon bir saat kapalı kalması
 - KnightOnline login sunucuları 4 saat kapalı
 - Prestij kaybı
- Bandwith yorma



Dünyadan DOS/DDOS Örnekleri

Distributed denial of service attacks on root nameservers

From Wikipedia, the free encyclopedia

Distributed denial of service attacks on root nameservers are several significant [Internet](#) events in which distributed [denial-of-service attacks](#) have targeted one or more of the thirteen [Domain Name System root nameservers](#). The root nameservers are a [critical infrastructure](#) components of the Internet, mapping [domain names](#) to [Internet Protocol](#) (IP) addresses and other information. Attacks against the root nameservers can impact operation of the entire Internet, rather than specific websites.

Contents [hide]

1 Attacks

1.1 October 21, 2002

1.2 February 6, 2007

2 References

3 External links

Attacks

[[edit](#)]

October 21, 2002

[[edit](#)]

On [October 21, 2002](#) an attack, lasting for approximately one hour, was targeted at all 13 DNS root name servers.^[1]

This event was the first significant attack directed at trying to disable the Internet itself, instead of specific websites.^{[[citation needed](#)]} This was the second significant failure of the root nameservers; the first large malfunction of them caused the failure of seven machines in April 1997, due to a technical problem.^[2]

February 6, 2007

[[edit](#)]

On [February 6, 2007](#), an attack began at 10:00 UTC and lasted twenty-four hours. At least two of the root servers reportedly *suffered badly* (G-ROOT and L-ROOT), while two others experienced *heavy traffic* (F-ROOT and M-ROOT). The latter two largely contained the damage by distributing requests to other root server instances with [anycast](#) addressing. ICANN published a formal analysis shortly after the event.^[3] Due to some lack of detail, speculation about the incident proliferated in the press until details were released.^[4]

On [February 8, 2007](#) it was announced by Network World that *"If the United States found itself under a major cyberattack aimed at undermining the nation's critical information infrastructure, the Department of Defense is prepared, based on the authority of the president, to launch an actual bombing of an attack source or a cyber counterattack."*^[5]

Dünyadan DDOS Örnekleri

Georgia DDoS Attacks – A Quick Summary of Observations by Jose Nazario

The clashes between Russia and Georgia over the region of South Ossetia have been shadowed by [attacks on the Internet](#). As we noted in July, the [Georgia presidential website fell victim to attack](#) during a [war of words](#). A number of DDoS attacks have occurred in the region, and [often do when tensions flare](#). We have been observing the attacks, making measurements, and sharing data with a select group of others to trace the origins of the attacks and monitor the situation.

While some are speculating about cyber-warfare and state sponsorship, we have no data to indicate anything of the sort at this time. We are seeing some botnets, some well known and some not so well known, take aim at Georgia websites. Note that [RIA Novosti](#), a Russian news outlet, was apparently targeted during this fighting. Georgian hackers are accused of this event.

Compared to the May 2007 [Estonian attacks](#), these are more intense but have lasted (so far) for less time. This could be due to a number of factors, including more sizable botnets with more bandwidth, better bandwidth at the victims, changes in our observations, or other factors.

Below are some observations of the attacks based on our [Internet statistics collection](#). These are observed attacks, ones that triggered alarms. We know that not all attacks are accounted for here, only many of the major ones. These attacks were mostly TCP SYN floods with one TCP RST flood in the mix. No ICMP or UDP floods detected here. These attacks were all globally sourced, suggesting a botnet (or multiple botnets) were behind them.

Number of attacks	Destination
5	213.131.44.138
3	213.157.196.25
10	213.157.198.33
1	www.gazeti.ge

Raw statistics of the attack traffic paint a pretty intense picture. We can discern that the attacks would cause injury to almost any common website.

Average peak bits per second per attack	211.66 Mbps
Largest attack, peak bits per second	814.33 Mbps
Average attack duration	2 hours 15 minutes
Longest attack duration	6 hour

Dünyadan DOS Örnekleri

Web Attacks Expand in Iran's Cyber Battle (Updated Again)

By Noah Shachtman  June 16, 2009 | 4:06 pm | Categories: [Info War](#), [Rogue States](#)

More and more of Iran's pro-government websites are under assault, as opposition forces launch web attacks on the Tehran regime's online propaganda arms.

What started out as [an attempt to overload a small set of official sites](#) has now [expanded](#), network security consultant Dancho Danchev notes. News outlets like [Raja News](#) are being attacked, too. The semi-official [Fars News](#) site is currently unavailable.



"We turned our collective power and outrage into a serious weapon that we could use at our will, without ever having to feel the consequences. [We practiced distributed, citizen-based warfare](#)," writes Matthew Burton, a former U.S. intelligence analyst who joined in the online assaults, thanks to a "push-button tool that would, upon your click, immediately start bombarding 10 Web sites with requests."

Dünyadan DDoS Örnekleri

Estonian DDoS Attacks – A summary to date

by Jose Nazario

Time sure flies. I looked up from working and noticed I hadn't blogged in a while. And I noticed that I hadn't been analyzing the Estonian DDoS attacks in a week or two.

ATLAS gives us an amazing view into the Internet's activities. ATLAS collects DoS attack data from around the world through sharing arrangements and even from some of our [Peakflow SP](#) deployments. As such, the recent DDoS attacks on Estonia are visible, in part, from within ATLAS. I've always had a soft spot in my heart for [Estonia](#). Since the fall of the Iron Curtain, it's become technically advanced, society has done wonders to improve itself and it's jumped, quite successfully, into the modern world. It has a nearly model economy, based in large part on the teachings of [Milton Friedman](#) who favored free markets unfettered by state control.

As you can imagine, having development access to the ATLAS data repository allows me to build new reports and crunch the data in new and exciting ways. I analyzed about 2 weeks of DDoS attacks on Estonia this morning using internal tools and reporting systems, and here's what I found.

We've seen 128 unique DDoS attacks on Estonian websites in the past two weeks through ATLAS. Of these, 115 were ICMP floods, 4 were TCP SYN floods, and 9 were generic traffic floods. Attacks were not distributed uniformly, with some sites seeing more attacks than others:

Attacks	Destination	Address or owner
35	"195.80.105.107/32"	pol.ee
7	"195.80.106.72/32"	www.riigikogu.ee
36	"195.80.109.158/32"	www.riik.ee, www.peaminister.ee, www.valitsus.ee
2	"195.80.124.53/32"	m53.envir.ee
2	"213.184.49.171/32"	www.sm.ee
6	"213.184.49.194/32"	www.agri.ee
4	"213.184.50.6/32"	
35	"213.184.50.69/32"	www.fin.ee (Ministry of Finance)
1	"62.65.192.24/32"	

The attacks themselves haven't been steady, at least from the perspective given by ATLAS. If we look at how many attacks occurred on every day, we can see that they peaked a week or so ago, but they haven't necessarily stopped.

Türkiye'den DDOS Örnekleri

Teklan ile Siberalem Arasında dDOS Tartışması

EBI firması, kendisine dDOS saldırısı yapıldığı suçlamasıyla Teklan aleyhine beyoğlu Cumhuriyet Savcılığına şikayette bulundu. Şirketin itiraf.com, siberalem benzeri sitelerinin host edildiği firma olan Teklan'dan ayrılmak istemesi üzerine saldırıların başladığı iddiası, sektörü karıştırdı. Teklan konuyla ilgili bir açıklama yaparak, olayı yalanladı.

İnternet kullanımı geliştikçe, internetle ilgili yeni kavramlar ve olaylarla karşılaşılıyor. İşte bunlardan birisi de dDos saldırıları. Saldırı yapılan sunucuları, o sunucunun ya da kullandığı bant genişliğinin kapasitesinin üstünde talep yaparak, çöktürmek anlamına gelen Ddos saldırıları, ilk olarak Microsoft'a ve daha sonra San Fransisco'daki internet kök sunuculara yapılan büyük saldırılarla gündemimize girmişti.

İşte bu konuda ilginç bir olay İstanbul'da meydana geldi. İnternet'in popüler arkadaşlık (sosyal network)portallerinden SiberAlem'in temmuz ayı içinde uğradığı Ddos saldırıları sonucunda, sistemin 5-6 gün gibi uzun süreler boyu kullanılamaz hale gelmesi sonucu adli makamlara şikayette bulunduğu ve yapılan tespitler sonucu da Teklan'ın birlikte çalıştığı, dakikhost firmasından bir kişinin gözaltına alındığı ve sonra tutuksuz yargılanmak üzere hakkında dava açıldığı, ayrıca Teklan yöneticilerinin de ifadelerinin alınacağı bilgisini aldık.

Konuyla ilgili iddia, Teklan ile SiberAlem sitesinin sahibi olan EBI arasında bir iş anlaşmazlığı olduğu şeklinde. Sitenin host edildiği Teklan firmasının dönem sonunda, büyük bir hosting ücreti istemesi üzerine, EBI'nin hosting firmasını değiştirmeye karar vermesinin, Teklan tarafından hoş karşılanmadığı ve bunun üzerine de saldırıların yapılmaya başlandığı iddiası ile yapılan şikayet dün internet camiasına bomba gibi düştü.

Gerçi konu, internet camiasında bir süredir zaten konuşuluyordu. Çünkü dDOS saldırısının, portalin daha sonra taşındığı Netone firmasının da rahatsız ettiği biliniyor. Ayrıca geçtiğimiz günlerde yayına başlayan ve futbol maçlarını video ile veren portal gibi bir kaç sitenin de saldırıya uğradığı konuşuluyor.

Türkiye'den DDOS Örnekleri

Yedik Dos'u Oturduk Mu Hayır Cisco'ya Geçiyoruz (Absürd Deneyim Yazısı)

1 haftadır öyle böyle değil Türkiye'nin bütün ip aralıklarından ağır syn saldırısı geliyordu. 10 numara httpd.conf, mysql.conf ayarı; iyi yapılandırılmış bir csf, arka planda yazdığım kabuk scriptleri ... 1000 civarı direk gelen zombieyi öldürebiliyordu. Ancak bu sabah azmeden arkadaş sayabildiğim 7000 civarı zombie ile sisteme girdi. 2-3 saat kadar dayanabildim. Ama arkası gelmedi. Bu da şunu bir kez daha gösterdi ki ne kadar iyi ayarlanırsa ayarlansın, 4 işlemcili 8 gb ramli, iyi dc konumlu bir yerde olsanız da donanımsal firewall şart.

İlk başlarda beni uğraştırdığı için eleman(lar)a çok kızdım. Saldırgan iplerin bazılarının modemine bazılarının pcsine girip bağlantılarını kestim küfür ettim. Ancak son saldırıda işin lamer işi olmadığını anladım. Profesyonelce yapılan bir saldırıydı. Zarar görüyor olsam da takdir ettim. Pekala oyunu kurallarına göre oynayalım o halde deyip dcy'e talimat verdim. 500 mbps gücünde dünyanın parası bir donanımsal firewall sipariş ettim. Kanada saatiyle 9 gibi hazır olacaktı (TR 16-17:00). -firewall kurulduğunda test edip (zaten saldırı devam ettiği, edeceği için doğal test de olacak) onayladıktan sonra *burası çok absürd oldu sildim*

Akla hayale gelen gelmeyen her tür yazılım önlemine karşı (kalkıp adam akıllı perl de öğrendim) üşenmeyip 7-8 bin botneti toplayan, sonra kalkıp benim gibi acı patlıcana klima açan elemanı buradan tebrik ederim. Serzeniş değil cidden tebrik ederim.

Ne demisim ben: hıyar tarlasında donsuz dolasmamak lazım. Donumuzu nivelim. Ciscomuzu eksik etmevelim.

Bölüm-B: BOTNET

BOT()

- roBOT kavramından türetilmiştir.
- **Genel çalışma mantığı:** Bot olarak yerleştirilen programcıklar sahibinin belirlediği bir IRC kanalına girerek oradan gelecek komutları çalıştırır. Binlerce bot bir araya gelerek botnet'leri oluşturur.
- **BotNet Nasıl Oluşur?**
- Örnek: Windows Acrobat Reader, Internet Explorer açıklıkları, Ms08-067 açıklığı
- Bir sayfaya girersiniz birden java script ile size exploit çalıştırır

Antivirüsler ve Botlar

- Çoğu bot bulaştığı sistemden virüs yazılımı sitelerine erişimi engeller
- Virüs yazılımlarını kapatır
- Virustotal.org
- Evasion teknikleri
 - Metasploit evasion

Zararlı Sayfaların İncelenmesi

Wepawet » JavaScript Report for http://erotic-adventure.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://wepawet.lisecslab.org/view.php?hash=41a0ef86e5b3f342ac336bab0ae9c432&t=1234806209&type=js

Most Visited Getting Started Latest Headlines

Wepawet » JavaScript Report for ht...

Sample Overview

URL	http://erotic-adventure.com
MD5	41a0ef86e5b3f342ac336bab0ae9c432
Analysis Started	2009-02-16 09:43:29
Report Generated	2009-05-17 00:33:12
JsAND version	1.03.02

See the report for domain erotic-adventure.com.

Detection results

Detector	Result
JSAND 1.03.02	malicious

Exploits

Name	Description	Reference
SuperBuddy LinkSBIcons	The LinkSBIcons method in the AOL's SuperBuddy ActiveX control (Sb.SuperBuddy.1) dereferences an arbitrary function pointer	CVE-2006-5820
Office Snapshot Viewer	The Microsoft Office Snapshot Viewer ActiveX control allows remote attackers to download arbitrary files to a client machine	CVE-2008-2463
WksPictureInterface	An ActiveX control in WkImgSrv.dll allows remote attackers to execute arbitrary code or cause a denial of service (browser crash) via an invalid WksPictureInterface property value	CVE-2008-1898
OurGame various errors	Errors in the GLIEDown2.dll ActiveX control via methods and properties IESStart, IESStartNative, ServerList, GameInfo, GroupName	SA30469
GomPlayer OpenURL	Buffer overflow in the GomManager via a long argument to the OpenUrl method	CVE-2007-5779
QuickTime RTSP	Stack-based buffer overflow in Apple QuickTime via an RTSP response with a long Content-Type header	CVE-2007-0015
NCTAudioFile2 SetFormatLikeSample	Stack-based buffer overflow in the NCTAudioFile2.AudioFile ActiveX control via a long argument to the SetFormatLikeSample function	CVE-2007-0018
Creative CacheFolder	Stack-based buffer overflow in the Creative Software AutoUpdate Engine ActiveX control via a long CacheFolder property value	CVE-2008-0955
Windows Media Encoder	Windows Media Encoder buffer overflow	CVE-2008-3008
Yahoo! Webcam Uploader	Yahoo! Webcam Uploader buffer overflow via long 'server' property followed by an invocation of the 'receive' method	CVE-2007-3147
Aurigma Photo Uploader	Aurigma Photo Uploader overflow in the ExtractIptc and ExtractExif properties	CVE-2008-0660
Yahoo! Webcam Viewer	Yahoo! Webcam Viewer buffer overflow via long server property followed by an invocation of the send method	CVE-2007-3148
Adobe Collab overflow	Multiple Adobe Reader and Acrobat buffer overflows	CVE-2007-5659
Adobe util.printf overflow	Stack-based buffer overflow in Adobe Acrobat and Reader via crafted format string argument in util.printf	CVE-2008-2992

Deobfuscation results

Evals

Done

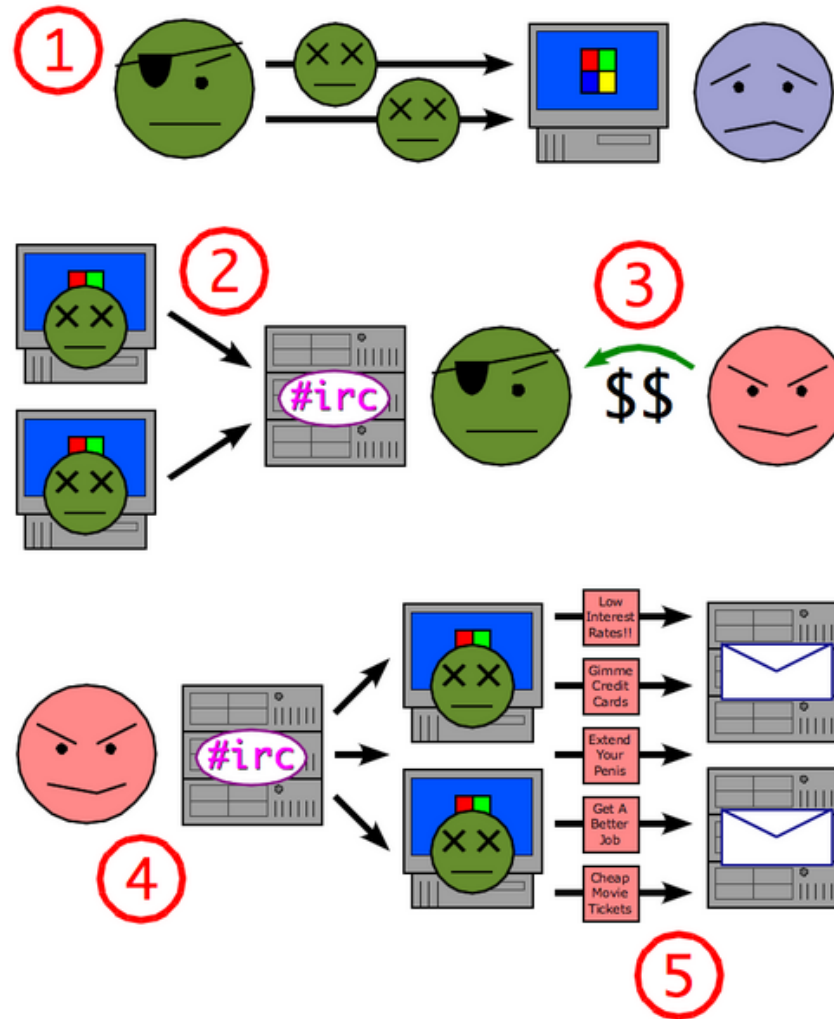
Antivirüs Programları korur mu?

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)

- Bot'ların bir araya gelerek oluşturduğu topluluk
- Genellikle DDOS atakları için kullanılır.
- En tehlikeli DDOS kaynakları.
 - Örnek:1000 tane ADSL kullanıcısının bot olarak kullanıldığını düşünelim:
 - $256 \times 1000 = 256 \text{ Mbps}$ throughput

BotNet

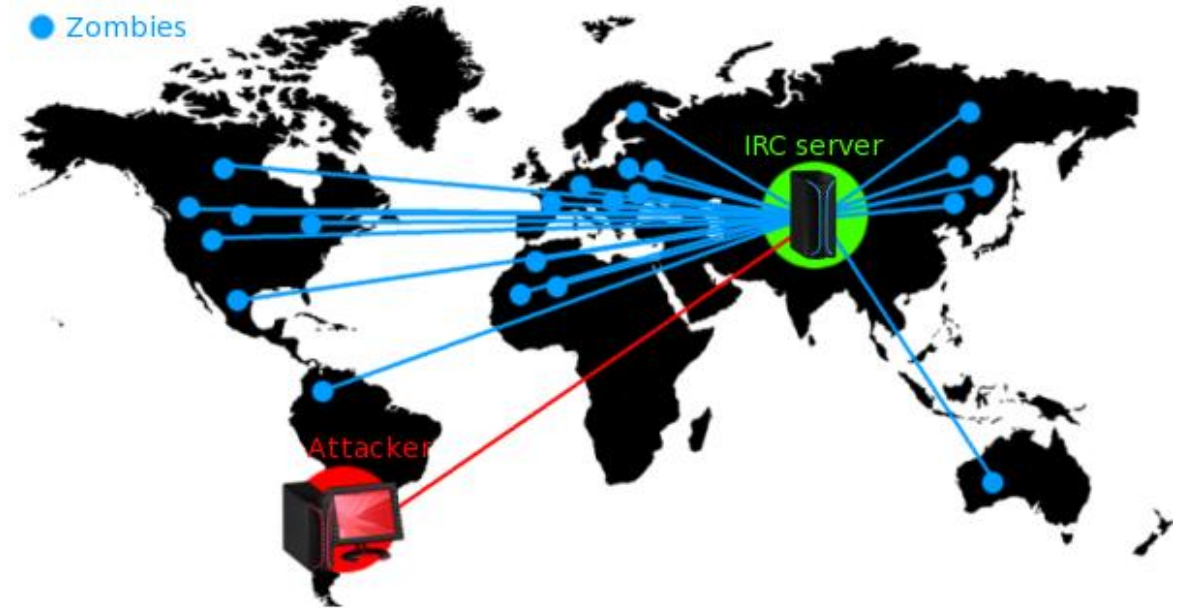


BotNet Kullanım Alanları

- DDOS Saldırılarında araç olarak
- Spam aracı olarak
- Veri çalma işlemlerinde(Sniffing)
- Yeni Malware vs yayma amaçlı
- Paralı reklam firmalarını yanıltmak için
- IRC Chat odalarını saldırmak için
- Online yapılan anket/oylamaları yanıltmak için.

Zombi-Master Haberleşmesi

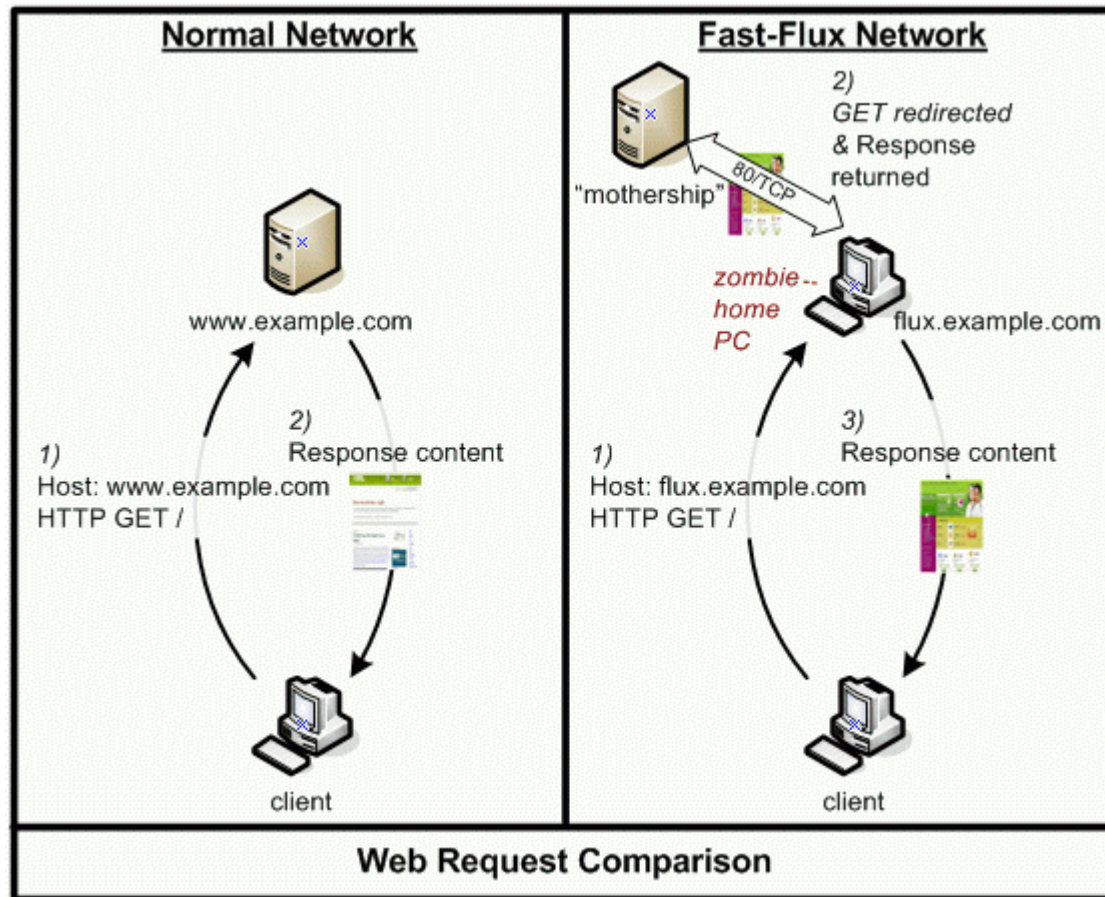
- Bot ile Master nasıl haberleşir?
 - IRC
 - HTTP
 - HTTPS
 - Twitter?




Fast Flux Hosting ve DNS

- Bir domain için anlık değişen binlerce kaydın olması
- Siber suçlarda takip edilmeme amaçlı kullanılır
- Günümüzde spam, phishing ve worm dağıtma amaçlı yaygın kullanılmakta.

Fast-Flux



Güncel Örnek



ONLINE CASINO
Real Money


- Home
- About Black Jack
- About Poker
- About Slots
- About Roulette

Welcome to the internet's leading resource for finding the finest and fairest casinos in the market today. Whether a beginner, novice, or professional, we will make sure that you arrive at the casino that is right for you.






We keep our visitors updated with the latest promotions and bonuses, as well as provide inside tips and techniques for the most popular casino games

Feel free to browse through some of the most beautifully designed and reliable online gaming sites on the internet today.

thebestcasinosonly.org



ALL STARS CASINO
U.S. Players Are Welcome!
Play in your own language! Click your flag to Play



ALL Stars Casino is a rewarding, classy gaming site that delivers a solid and exciting gaming experience. ALL Stars Casino relies on the strength of its fantastic

Güncel Örnek dns çıktısı

```
$ dig thebestcasinosonly.org
; <<>> DiG 9.3.1 <<>> thebestcasinosonly.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34670
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;thebestcasinosonly.org.                IN      A

;; ANSWER SECTION:
thebestcasinosonly.org. 180      IN      A      24.131.245.17
thebestcasinosonly.org. 180      IN      A      24.196.99.141
thebestcasinosonly.org. 180      IN      A      61.33.123.33
thebestcasinosonly.org. 180      IN      A      67.14.250.74
thebestcasinosonly.org. 180      IN      A      67.165.248.201
thebestcasinosonly.org. 180      IN      A      68.118.88.8
thebestcasinosonly.org. 180      IN      A      69.145.50.205
thebestcasinosonly.org. 180      IN      A      72.24.66.110
thebestcasinosonly.org. 180      IN      A      75.35.119.75
thebestcasinosonly.org. 180      IN      A      75.64.184.207

;; AUTHORITY SECTION:
thebestcasinosonly.org. 86398    IN      NS      ns2.c0fbfef6e372ca34a.com.
thebestcasinosonly.org. 86398    IN      NS      ns1.c0fbfef6e372ca34a.com.

;; ADDITIONAL SECTION:
ns1.c0fbfef6e372ca34a.com. 172800 IN      A      76.83.111.64
```

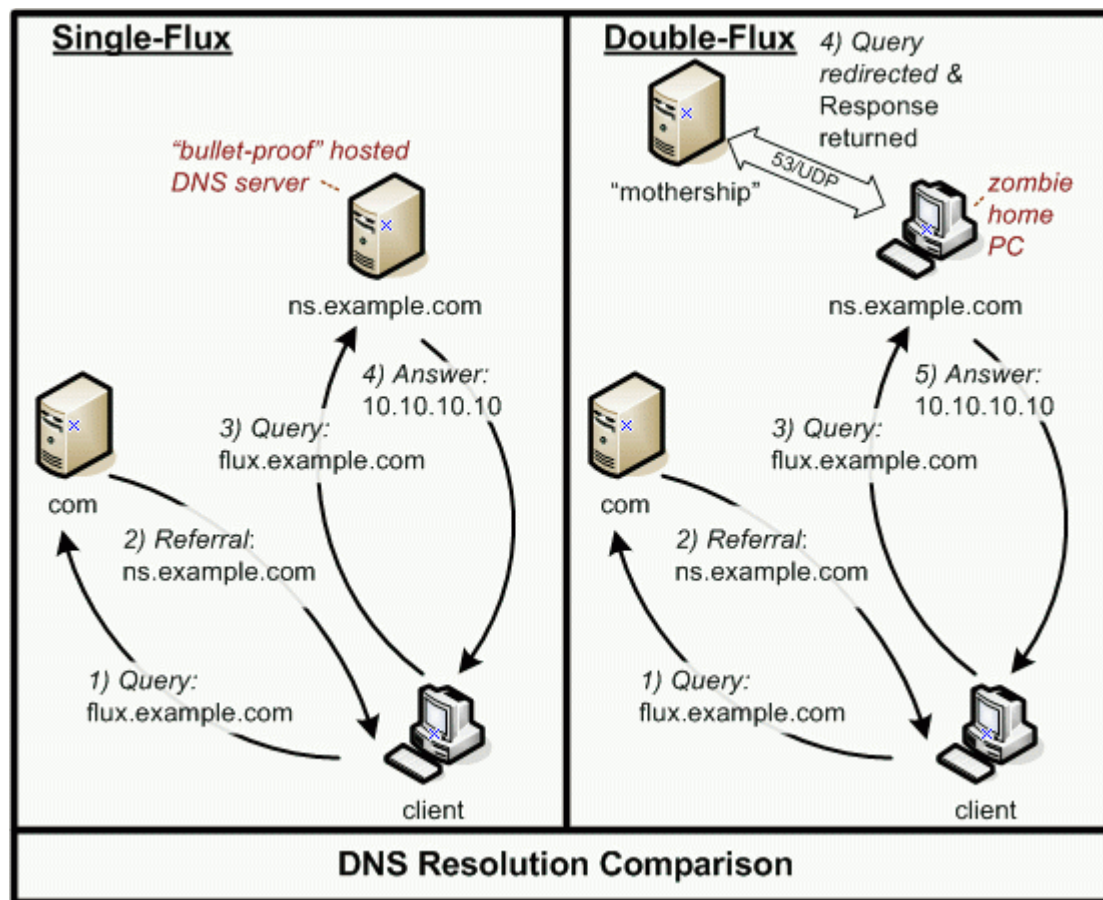
24.62.54.140

287 IP Addresses
60 Different AS #'s

US (USA)	262
KR (Korea)	6
Unresolved	4
IT (Italy)	3
CO (Columbia)	3
CA (Canada)	2
GB (Britain)	2
ES (Spain)	1
HR (Croatia)	1
MA (Morocco)	1
AR (Argentina)	1
IN (India)	1

12.206.40.180	24.170.47.176	67.10.209.213	69.0.73.84	70.240.228.214	75.0.40.101	75.68.235.7
12.206.54.141	24.178.108.58	67.11.53.229	69.104.17.202	70.240.76.64	75.132.196.148	76.105.73.135
12.207.68.178	24.178.70.101	67.122.209.32	69.104.79.110	70.242.226.137	75.132.221.72	76.105.94.93
12.216.56.160	24.192.190.232	67.14.250.74	69.105.29.239	70.247.72.253	75.15.177.242	76.160.14.167
165.247.3.62	24.192.229.71	67.163.9.207	69.105.53.104	70.247.73.240	75.15.246.201	76.160.18.66
172.166.156.216	24.196.99.141	67.165.248.201	69.111.195.192	70.247.75.152	75.15.252.175	76.160.23.48
172.168.162.140	24.197.105.54	67.175.219.231	69.111.195.23	70.249.187.167	75.16.105.1	76.167.164.252
172.190.186.191	24.2.123.87	67.181.91.202	69.139.115.247	70.250.217.237	75.16.110.30	76.18.15.226
172.190.51.251	24.240.70.148	67.182.11.96	69.139.31.14	70.251.246.111	75.176.40.117	76.188.22.61
172.192.138.83	24.27.203.131	67.188.91.127	69.143.2.111	70.255.250.189	75.21.184.230	76.193.35.241
172.192.6.73	24.62.54.140	67.64.114.126	69.145.50.205	70.78.11.19	75.21.191.180	76.195.181.88
172.193.41.102	24.94.62.190	68.116.214.113	69.146.142.65	71.12.14.160	75.21.226.71	76.195.183.56
190.84.147.136	24.98.156.181	68.118.88.8	69.151.200.212	71.135.45.74	75.21.242.103	76.195.9.80
196.217.101.105	4.131.83.22	68.121.85.57	69.151.200.241	71.135.71.54	75.22.20.182	76.197.59.104
200.114.214.92	4.180.60.136	68.126.254.99	69.177.90.100	71.136.13.167	75.26.49.34	76.198.93.93
201.244.248.187	4.180.60.159	68.126.255.178	69.182.21.234	71.136.14.44	75.31.160.172	76.202.254.102
201.245.252.74	4.227.241.192	68.185.180.87	69.183.12.223	71.137.136.140	75.31.163.161	76.203.17.200
203.170.111.16	4.245.120.173	68.204.134.168	69.208.138.101	71.138.48.230	75.31.27.32	76.215.129.131
203.170.115.64	61.33.123.33	68.205.108.135	69.208.138.23	71.140.115.153	75.32.50.25	76.216.115.188
204.13.181.145	65.184.237.226	68.248.1.10	69.209.136.66	71.141.91.134	75.36.125.248	76.22.239.167
204.13.181.171	65.205.65.83	68.250.211.151	69.215.135.107	71.198.93.144	75.37.161.145	76.227.0.122
204.13.181.183	65.24.108.223	68.251.185.64	69.215.136.146	71.205.219.86	75.4.141.137	76.23.121.71
204.13.181.211	65.24.109.83	68.33.3.123	69.215.140.43	71.225.137.78	75.4.61.10	76.24.146.172
207.255.83.226	65.25.6.83	68.37.193.126	69.215.173.148	71.232.66.87	75.4.70.107	76.27.116.145
208.104.21.244	65.33.192.199	68.37.220.199	69.221.7.14	71.238.40.7	75.414.178	76.83.85.235
208.104.84.227	66.139.11.139	68.37.91.78	69.221.92.49	71.74.239.158	75.45.238.22	76.98.91.185
208.104.88.123	66.142.170.139	68.44.187.232	69.232.65.116	71.76.219.163	75.46.10.146	76.99.113.84
208.188.16.15	66.142.185.118	68.45.116.157	69.232.68.109	71.76.56.14	75.46.37.253	76.99.254.64
208.188.17.164	66.16.189.26	68.46.93.192	69.246.178.123	71.79.201.101	75.46.80.126	82.3.234.196
208.188.17.239	66.177.221.151	68.57.63.155	69.251.167.240	71.79.247.170	75.46.95.208	84.125.43.159
208.191.144.174	66.177.24.253	68.73.87.136	69.251.44.158	71.79.252.196	75.47.107.97	84.222.244.186
210.57.250.102	66.188.122.229	68.75.6.70	70.128.42.114	71.81.244.187	75.49.116.215	84.223.131.250
210.57.252.229	66.190.101.125	68.88.13.108	70.129.135.238	72.181.75.188	75.5.2.164	84.223.134.181
210.57.252.80	66.190.102.134	68.88.143.59	70.131.147.172	72.186.86.145	75.51.92.217	86.31.118.11
216.255.60.248	66.214.56.40	68.88.254.147	70.131.153.35	72.187.156.200	75.54.135.226	89.172.26.164
219.91.185.247	66.215.208.135	68.89.175.186	70.226.14.253	72.234.104.254	75.6.138.195	96.2.169.94
24.131.245.17	66.215.91.66	68.89.176.169	70.226.224.180	74.138.21.51	75.6.180.189	98.194.20.186
24.131.245.44	66.229.173.145	68.89.177.5	70.226.23.230	74.140.246.17	75.63.63.97	98.194.66.50
24.14.72.252	66.234.209.142	68.89.189.67	70.233.250.4	75.0.235.83	75.64.184.207	98.199.193.16
24.15.131.102	66.56.26.35	68.90.218.145	70.236.18.72	75.0.36.19	75.65.189.26	98.202.2.4
24.15.179.161	66.65.217.252	68.91.122.22	70.236.29.243	75.0.37.193	75.65.33.136	99.244.112.14

Double Flux



BotNet Satın Alma

The screenshot shows the GhostMarket website interface. At the top, there's a header with the 'Ghost Market' logo, 'A New Era To Virtual Marketing' tagline, and logos for Visa and MasterCard. A 'N2C Home' link is visible on the right. Below the header, a sidebar on the left contains links for 'FAQ' and 'REGISTER'. The main content area displays a forum thread titled 'New DDoS service - attack service 80000 to 120000 bots'. The thread includes a 'POST REPLY' button, a search bar, and the post content which describes a DDoS attack service with details on bot count, attack types, and pricing.

Ghost Market
A New Era To Virtual Marketing
VISA MasterCard
N2C Home

GhostMarket.Net A New Era to Virtual Marketing

Board index < Hacking/Cracking Market < Bot Bin/Sources + Bots
It is currently Tue Sep 01, 2009 8:35 am

New DDoS service - attack service 80000 to 120000 bots

POST REPLY Search this topic... Search

New DDoS service - attack service 80000 to 120000 bots
by golos » Thu Jul 16, 2009 10:17 am

New DDoS service - attack service 80000 to 120000 bots
Hello,

I offer serious DDoS attack service from 10 Gbps to 100 Gbps.

I always have between 80,000 and 120,000 bots on my IRC channel.

Type of attack : SYN - TCP - ICMP - UDP - HTTP - HTTPS - NEWSYN

I can take down every website even if DDoS protected.

Price start from 200 \$ USD 24 hours.

AVAILABLE : Free 3 minutes demonstration of attack.

Snort BotNet imzaları

- Snort imzaları/BleedingThreats

```
alert tcp $HOME_NET 1024: -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET  
TROJAN Zbot/Zeus Download Request"; content:"GET "; depth:4;  
content:"Win32)|0d 0a|";  
pcre:"/\\"(rec\.php|ip\.php|config\.bin|cfg\.bin|cfg2\.bin)"/";  
classification:trojan-activity; reference:url,  
www.blog.malc0de.com/2009/12/16/list-of-zeusbot-command-and-control-  
servers/; sid:2010xxx; rev:2;)
```

DOS/DDOS Çeşitleri

- Amaca göre DDOS Çeşitleri
 - Bandwith tüketimi
 - Kaynak tüketimi(CPU, RAM, disk vs)
- Yapılış şekline göre DOS/DDOS çeşitleri
- ARP, Wireless
- IP
- ICMP
- TCP
- UDP
- DHCP/SMTP/HTTP/HTTPS/DNS

Yerel Ağlarda DOS/DDOS

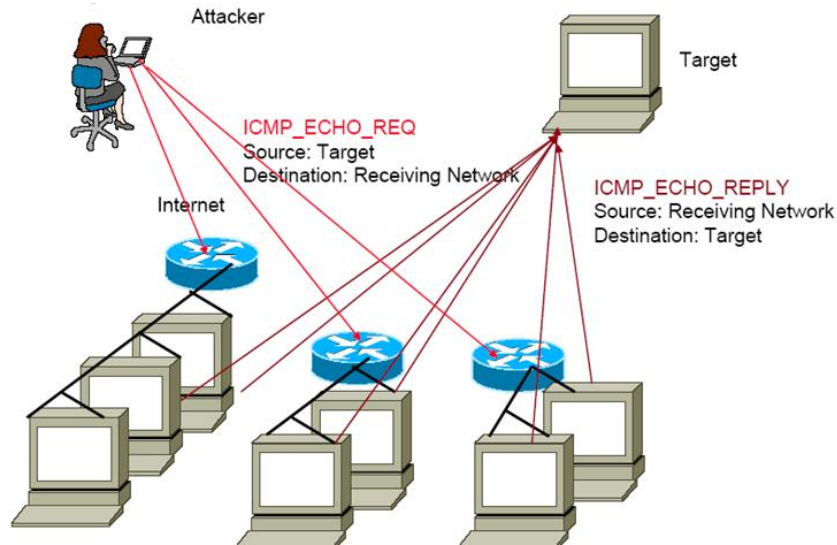
- Yerel Ağlarda Kullanılan TCP/IP Protokolü:ARP
- ARP Stateless bir protokol
- Zararlı birisi tüm ağa gatewayin mac adresi olarak yanlış bir kayıt gönderir
 - Tüm ağın erişimi durur

Kablosuz Ağlarda DOS/DDOS

- Kablosuz Ağlar Fiziksel korumadan yoksun
- Şifresiz Ağlar için DOS Tehlikesi
 - Ağa dahil olan birileri LAN'daki saldırıları gerçekleştirebilir
 - Tüm ağın gateway'ini yanlış mac adresi ile zehirlemek...
- Şifreli Ağlar için DOS Tehlikesi
 - Saldıran ağ şifresini bilmediği için giremez
 - Kismet vs ile havayı dinleyerek ağa bağlı sistemleri bulabilir
 - Ağa bağlı sistemlere AP'den geliyormuşcasına Deauth paketleri gönderir.
 - Ağa bağlı sistemler bağlantı kurmakta zorlanır
 - 802.1x kullanılıyorsa hesap kitleme saldırıları yapılabilir

Eski yöntemler:Smurf atağı

ICMP ve UDP Paketleri Broadcast olarak gönderilebilir



Tek bir paket gönderilerek milyonlarca cevap dönülmesi sağlanabilir(di)

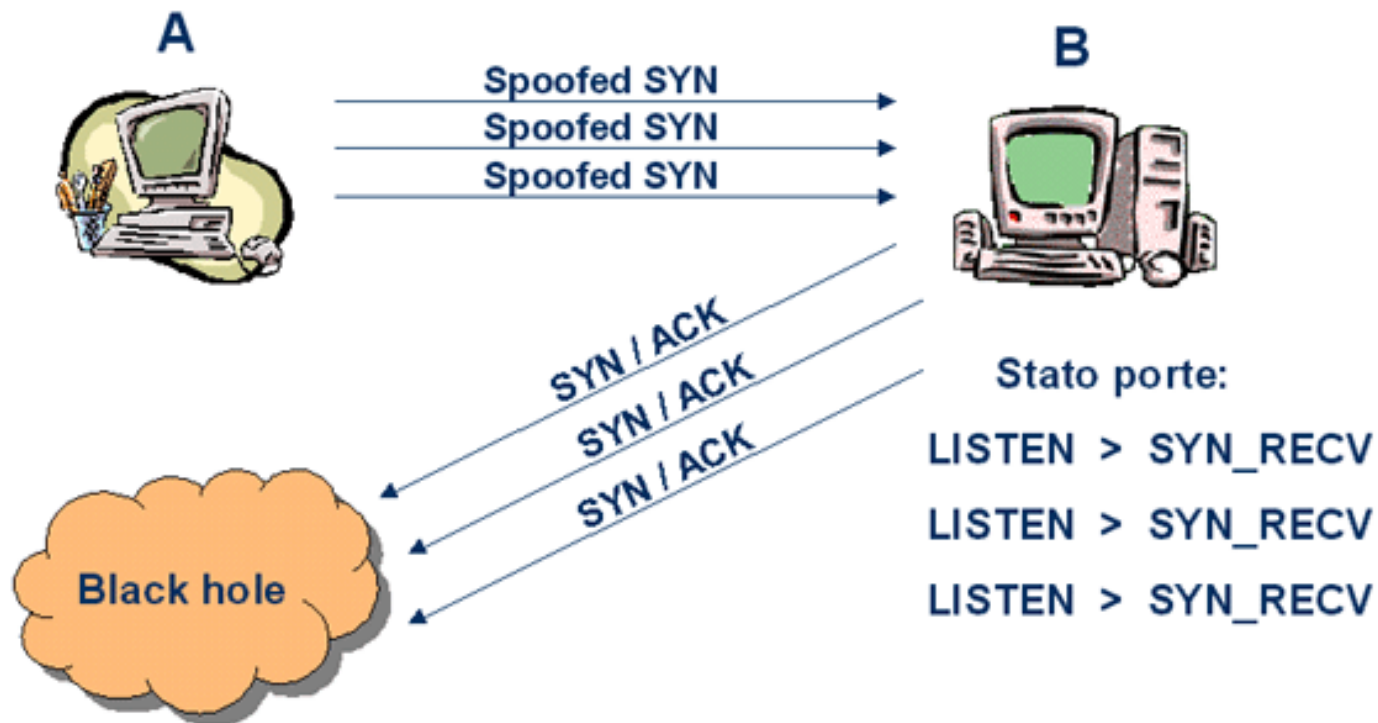
Eski Yöntemler: Ping Of Death

- Bir IP paketinin max boyutu: 65536
- Parçalama yaparak bundan daha büyük bir paket gönderilir
- Hedef sistemin beklemediği bu paket sistemi zora sokar.

Günümüzde tercih edilen yöntemler

- SYN Flood
- HTTP Get / Flood
- UDP Flood
- DNS DOS
- Amplification DOS saldırıları
- BGP Protokolü kullanarak DOS
- Şifreleme-Deşifreleme DOS saldırıları
- Mail bombing(?)

Bölüm-B:SYN Flood Saldırıları

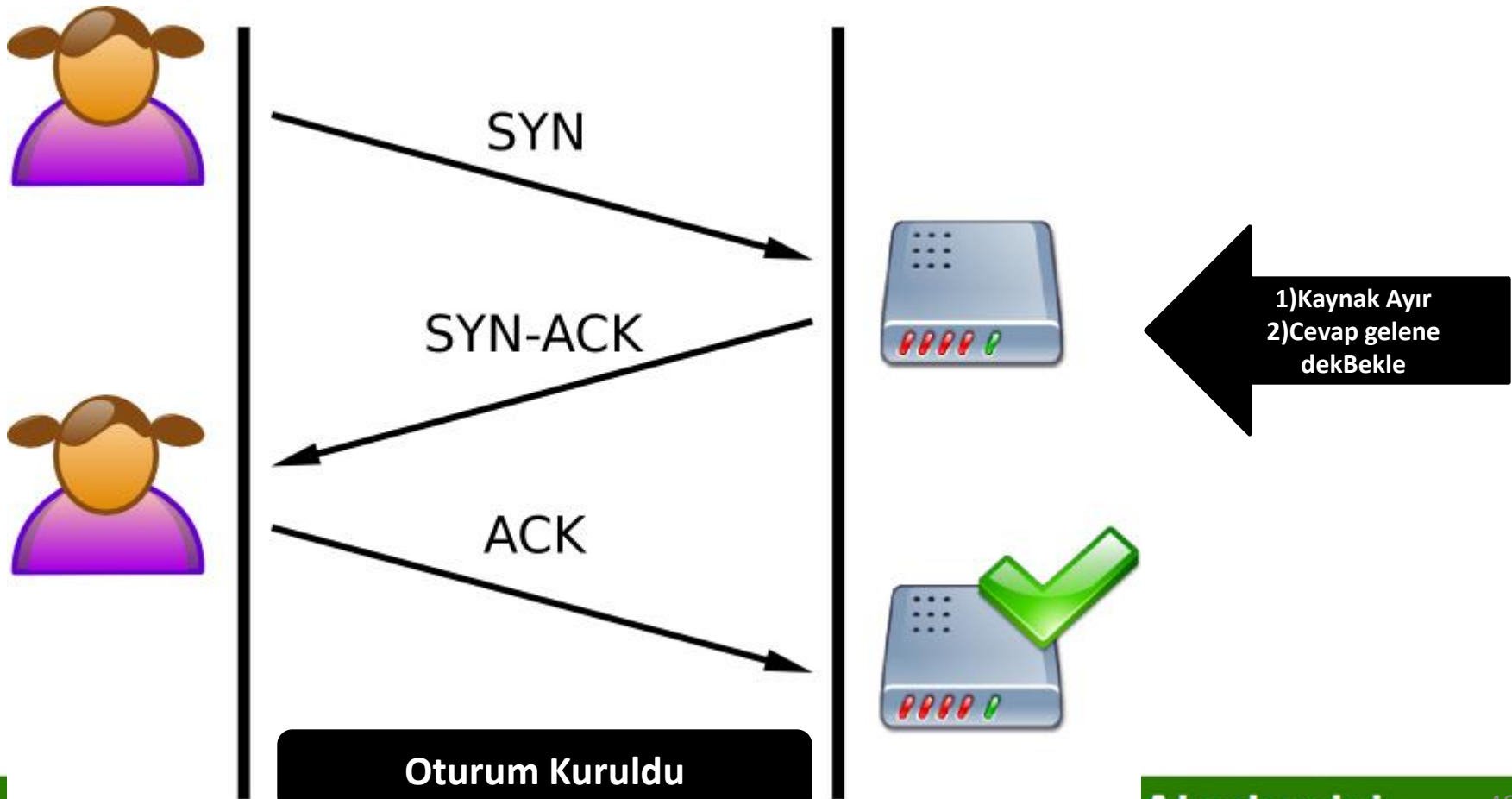


Syn Flood

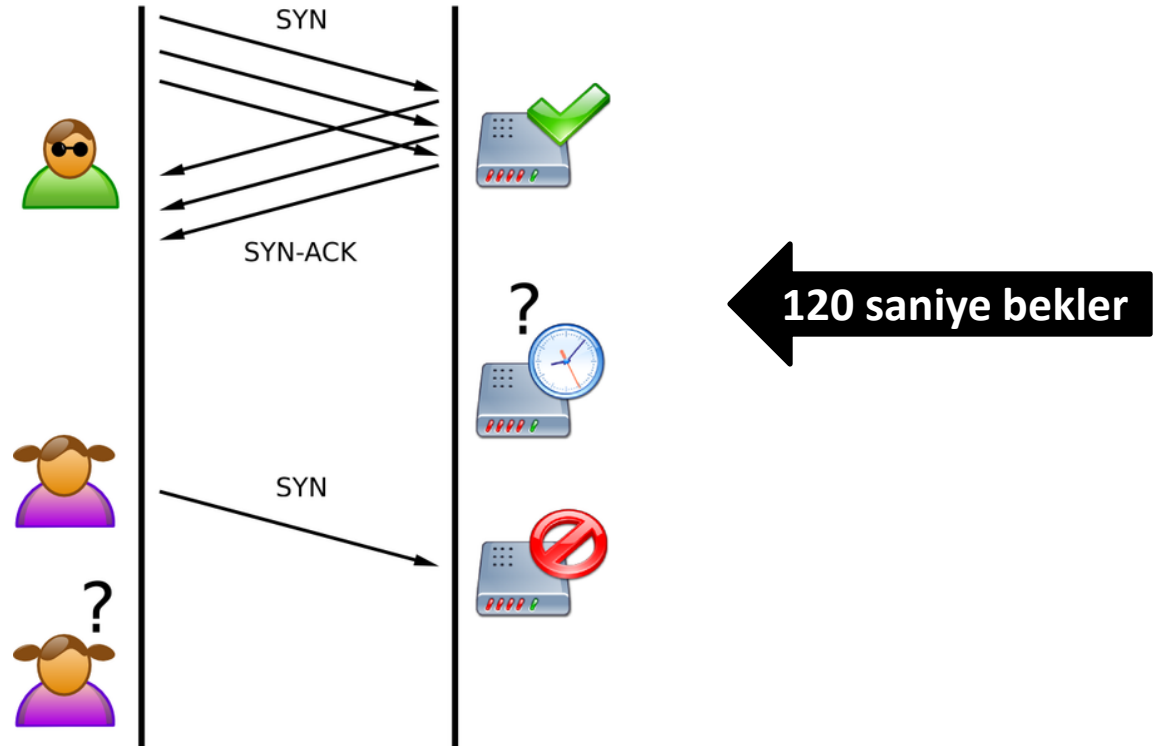
- TCP – Bayraklar -Oturum Kurulması
 - 3 way handshaking SYN- SYN/ACK – ACK
- Rastgele spoof edilmiş iplerden SYN istekleri gönderilir
- Cevaplar spoof edilmiş iplere döner(Açık olanlar RST gönderir kapalı olanlar için bir süre beklenir)
- Büyük boyutlu paketler göndererek sistemin ağ trafiği boğulur.
- Sistem bu paketlerle uğraşırken gerçek isteklere cevap veremez

SYN Flood Saldırıları

- Normal TCP İşleyişi



SYN Flood



- Bir SYN paketi ortalama 65 Byte
- 8Mb ADSL sahibi bir kullanıcı saniyede 4.000 SYN paketi üretebilir, 100 ADSL kullanıcısı?

SynFlood ve güvenlik Duvarları

Juniper Screens Administration Tools (ns5gt) - Mozilla Firefox 3.0 beta 3

File Edit View History Bookmarks Tools Help

http://192.168.2.36/nswebui.html

Smart Bookmarks Customize Links Free Hotmail Windows Marketplace Windows Media Windows

Home

Up time: 0 day 05:22:06, System time: 2008-05-18 00:12:48 GMT Time Zone 00:00

Juniper
NETWORKS

Juniper-NS5GT

- Home
- Configuration
- Network
- Screening
- Policies
- MCast Policies
- VPNs
- Objects
- Reports
- Wizards
- Help
- Logout

[Toggle Menu](#)

Device Information

Hardware Version:	1010(0)
Firmware Version:	5.3.0r1.0 (Firewall+VPN)
Serial Number:	0064062004004075
Host Name:	ns5gt
Operational Mode:	trust-untrust

System Status (Root)

Administrator:	erhan
Current Logins:	3 Details

Resources Status

CPU:	<div><div></div></div>
Memory:	<div><div></div></div>
Sessions:	<div><div></div></div>
Policies:	<div><div></div></div>

[Start from here...](#)

Interface link status:

Name	Zone
trust	Trust
untrust	Untrust

The most recent alarms:

Date/Time	Level	Description
2008-05-18 00:12:45	crit	Session utilization has reached 1857, wh...
2008-05-18 00:12:43	crit	Session utilization has reached 1857, wh...
2008-05-18 00:12:41	crit	Session utilization has reached 1857, wh...
2008-05-18 00:12:39	crit	Session utilization has reached 1857, wh...
2008-05-18 00:12:37	crit	Session utilization has reached 1857, wh...

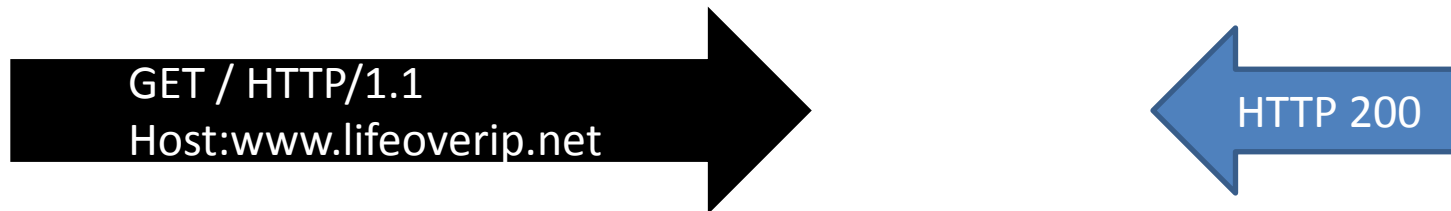
The most recent events:

Date/Time	Level	Description
2008-05-18 00:12:46	warn	Admin user "erhan" logged in for Web(htt...
2008-05-18 00:06:25	notif	All logged events or alarms were cleared...

Bölüm-H:HTTP Flood Saldırıları

HTTP Üzerinden Yapılan DOS/DDOS

- HTTP(Hypertext Transfer Protocol)
 - Web sayfalarını ziyaret ederken kullanılan protokol
- HTTP istek ve cevaplarıyla çalışır



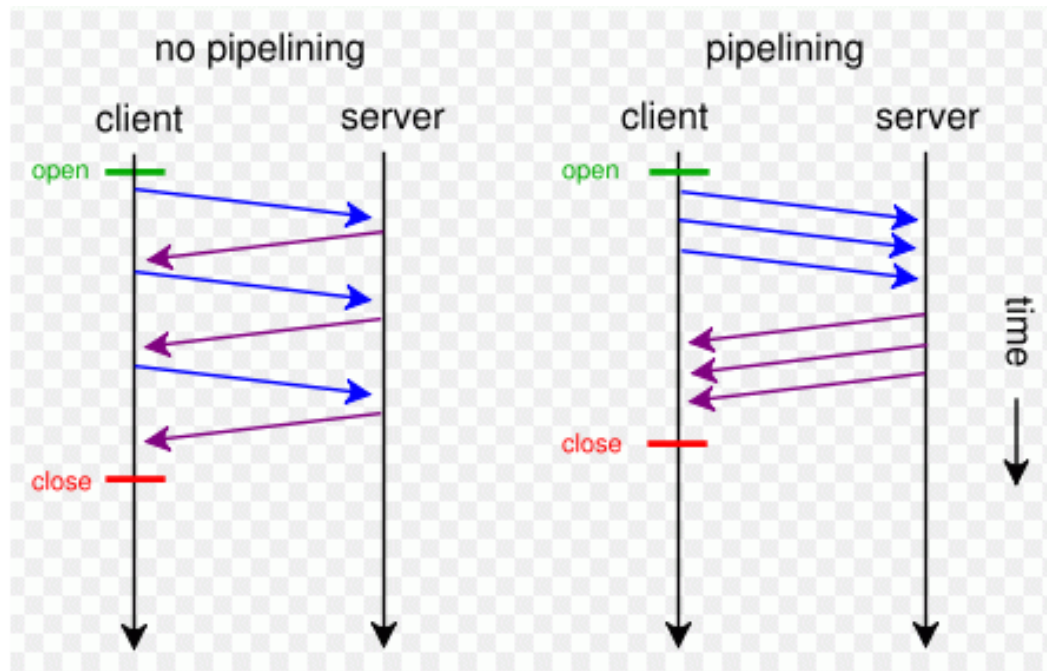
- Web sunucuların belirli kapasitesi vardır
 - Eş zamanlı 500 istek kabul et gibi
- Bir kullanıcı tek bilgisayardan eş zamanlı 500 istek yapabilir

HTTP Çalışma Yapısı

- Garip bir protokol
 - Bir sayfaya girmek için ortalama 50-60 istek gönderilir. Her istek ortalama 6 pakettir(syn, ack, fin)
 - Bu istekler birbirinden bağımsızdır.
 - 100 kişi aynı anda ana sayfaya girse toplamda 30.000 istek oluşur bu da sunucu tarafında performans sıkıntısı demektir.
- Performans sıkıntısına önlem: Keep Alive mekanizması

HTTP KeepAlive

Sunucudan istenecek her isteğin ayrı bir TCP bağlantısı yerine tek bir TCP bağlantısı üzerinden gönderilmesi sağlanabilir.



HTTP Üzerinden DOS

[illegible]

Snort ile HTTP Flood saldırıları Engelleme

- Mantık basit: HTTP sunucuya gelebilecek HTTP isteklerini ip bazında sınırlama(TCP seviyesinde değil)
- Her ip den anlık gelebilecek max HTTP GET/HEAD/POST isteği=100

```
alert tcp any any -> any 80 (msg:"HTTP GET Flood Attack Attempt"; content:"GET";  
nocase; depth:10; detection_filter: track by_src, count 90, seconds 3; sid:1000001;  
rev:1;)
```

Bölüm-A:UDP Flood Saldırıları

UDP Flood Saldırıları

- UDP=Connectionless bir protokol
 - IP spoofing yapılabilir
 - hping –udp www.lifeoverip.net -p 53 -a www.microsoft.com
 - Paket boyutu ~ 30 byte
 - 20Mb hat ile saniyede 90.000 pps üretilebilir.
 - $20 \times 1024 \times 1024 / 8 / 30$
 - UDP bağlantısının kapatılması için gerekli ortalama süre 60 saniye...

UDP Flood saldırıları

- Rastgele üretilmiş sahte ip adreslerinden saniyede 90.000 paket. Her paket için 60 saniye bekleme süresi
- Piyasadaki çoğu Firewall/IPS ürününün kapasitesinin üzerinde
- Eğer firewall kapalı portlar için ICMP Dest. Port Unreachable paketi gönderiyorsa saldırı şiddeti iki katına çıkmış olur.

Bölüm-D:DNS'e Yönelik DOS Saldırıları

DNS Servisine yönelik DDOS Saldırıları

- DNS UDP üzerinden çalışır= kandırılmaya müsait servis
- DNS = Internet'in en zayıf halkası
 - E-posta hizmetleri
 - Web sayfalarının çalışması
 - İnternetim çalışmıyor şikayetinin baş kaynağı ☺
- DNS sunuculara yönelik DDOS saldırıları
 - DNS yazılımında çıkan buglar
 - ENDS kullanımı ile amplification saldırıları
 - DNS sunucuların kapasitelerini zorlama

DNS Sunucularda çıkan buglar ve DOS

İnternetin %80 ISC Bind yazılımı kullanıyor

Yıl 2009 ...

File Name:	solinger.c
Description:	"solinger" Denial Of Service - BIND 8.1.*, 8.2, 8.2.1 - causes a BIND8 server to stop responding to requests for up to 120 seconds. Quick proof of concept of the bug pointed out by ISC.
Author:	Mixer
Homepage:	http://mixter.void.ru
MD5 Checksum:	0969c6c7e46e8710f57450bca51ed6af

File Name:	CSSA-1999-034.0.txt
Description:	Caldera Advisory - Several vulnerabilities have been discovered involves a buffer overflow that can possibly be used by a skilled
MD5 Checksum:	f372b37e400da08fae2dd765c7d715ce

File Name:	bind.nxt.txt
Description:	A bug in the processing of NXT records allows attackers remot detailed information about the bug and the handling of NXT rec
MD5 Checksum:	6f9bfe05817ae7378fd260502ace3530

File Name:	named_dump.sh
Description:	ISC BIND 4.9.7-T1B local exploit - The named daemon will dun any file in the system.
Homepage:	http://www.hack.co.za
MD5 Checksum:	9e3322da75b9792e0a877bdaabb9a82f

File Name:	bind8x.c
Description:	BIND prior to 8.2.3-REL remote root exploit - exploits the name
Author:	lxLucysoft
MD5 Checksum:	c4f9cc6d4b7bc657ff22984adf7d206c

File Name:	sms.203.ypbind
Description:	Sun Microsystems Security Bulletin #203 - The yp.BIND daemon remote attacker to gain root access. Vulnerable systems includ
Homepage:	http://sunsolve.sun.com/security
MD5 Checksum:	46e0491127139c68520874f9000b1129

BIND Dynamic Update DoS

CVE:	CVE-2009-0696
CERT:	VU#725188
Posting date:	2009-07-28
Program Impacted:	BIND
Versions affected:	BIND 9 (all versions)
Severity:	High
Exploitable:	remotely
Summary:	BIND denial of service (server crash) caused by receipt of a specific remote dynamic update message.

Description:

Urgent: this exploit is public. Please upgrade immediately.

Receipt of a specially-crafted dynamic update message to a zone for which the server is the master may cause BIND 9 servers to exit. Testing indicates that the attack packet has to be formulated against a zone for which that machine is a master. Launching the attack against slave zones does not trigger the assert.

This vulnerability affects all servers that are masters for one or more zones - it is not limited to those that are configured to allow dynamic updates. Access controls will not provide an effective workaround.

dns_db_findrrdataset() fails when the prerequisite section of the dynamic update message contains a record of type "ANY" and where at least one RRset for this FQDN exists on the server.

```
db.c:659: REQUIRE(type != ((dns_rdatatype_t)dns_rdatatype_any)) failed  
exiting (due to assertion failure).
```

Workarounds:

BIND Dynamic Update DoS

- ISC bind 2009 Temmuz
- Bu tarihe kadarki tüm bind sürümlerini etkileyen “basit” ama etkili bir araç
- Tek bir paketle Türkiye’nin internetini durdurma(!)
 - Tüm büyük isp’ler bind kullanıyor
 - Dns=udp=src.ip.spoof+bind bug
- %78 dns sunucu bu zaafiyete açık
 - Sistem odalarında nazar boncuğu takılı☺



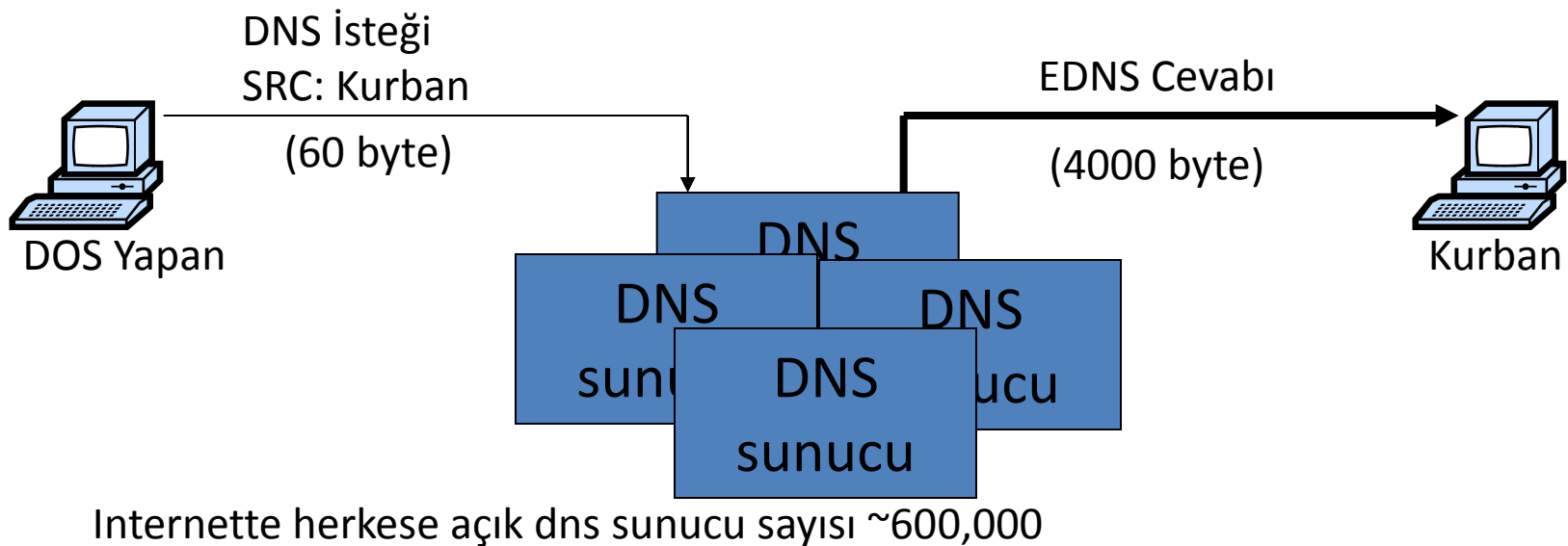
DNS Amplification Saldırısı

- UDP üzerinden taşınan dns paketleri 512 byten büyük olamaz
- EDNS(RFC 2671) dns sorgularının cevapları 512 bytedan daha büyük olabilir
- 60 byte(dns isteği) gönderip cevap olarak 56X byte alınabilir(cevap=56X istek)
- 10Mb bağlantıdan $10 \times 65 = 650$ Mbit t üretilebilir.
- Koruma: recursive dns sorguları ve edns desteği iyi ayarlanmalı



DNS Amplification DOS

DNS Amplification Saldırısı: ($\times 65$ amplification)



```

root@guvenlikod: ~
root@guvenlikod:~# dig . @gezginler.net

;<<>> DiG 9.5.0-P2 <<>> . @gezginler.net
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54348
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
.                IN      A

;; AUTHORITY SECTION:
.                347143 IN      NS      h.root-servers.net.
.                347143 IN      NS      i.root-servers.net.
.                347143 IN      NS      j.root-servers.net.
.                347143 IN      NS      k.root-servers.net.
.                347143 IN      NS      l.root-servers.net.
.                347143 IN      NS      m.root-servers.net.
.                347143 IN      NS      a.root-servers.net.
.                347143 IN      NS      b.root-servers.net.
.                347143 IN      NS      c.root-servers.net.
.                347143 IN      NS      d.root-servers.net.
.                347143 IN      NS      e.root-servers.net.
.                347143 IN      NS      f.root-servers.net.
.                347143 IN      NS      g.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 347143 IN      A      198.41.0.4
a.root-servers.net. 347143 IN      AAAA   2001:503:ba3e::2:30
b.root-servers.net. 347143 IN      A      192.228.79.201
c.root-servers.net. 347143 IN      A      192.33.4.12
d.root-servers.net. 347143 IN      A      128.8.10.90
e.root-servers.net. 347143 IN      A      192.203.230.10
f.root-servers.net. 347143 IN      A      192.5.5.241
f.root-servers.net. 347143 IN      AAAA   2001:500:2f::f
g.root-servers.net. 347143 IN      A      192.112.36.4
h.root-servers.net. 347143 IN      A      128.63.2.53
h.root-servers.net. 347143 IN      AAAA   2001:500:1::803f:235
i.root-servers.net. 347143 IN      A      192.36.148.17
j.root-servers.net. 347143 IN      A      192.58.128.30
j.root-servers.net. 347143 IN      AAAA   2001:503:c27::2:30

;; Query time: 176 msec
;; SERVER: 208.43.98.30#53 (208.43.98.30)
;; WHEN: Fri Mar 12 05:58:09 2010
; MSG SIZE rcvd: 500

```

**Istek 45 byte
Cevap 528 byte**

**10Mb hat ile 120 Mb
UDP trafigi
olusturulabilir.
(10*1024*1024/45)***

DNS sunuculara kaba kuvvet paket saldırısı

- Bir dosya içerisine 1 milyon farklı domain ismi yazılır.
- Paket üreticiler kullanılarak bu domainler hızlıca dns sunucuya spoofed edilmiş ip adreslerinden sorgu olarak gönderilir
- DNS sunucu iyi ayarlanmamışsa gerçek isteklere zaman ayıramaz

Dns Flood Örnek

```
[root@depdep ~]# perl maraveDNSv2.pl -S 5.5.5.5 -t 50.22.202.132
Attacking : 50.22.202.132
Asking A records
Spoofing from 5.5.5.5
Flooding to death :)
```

<Press ENTER to start>

Flood started <CTRL-C> to stop

Stopping the flood ... please wait
Done, have a nice day

You have mail in /var/spool/mail/
[root@depdep ~]# █

```
IP 5.5.5.5.domain > 50.22.202.132.domain: 30767+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 57382+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 18737+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 56926+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 40502+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 47026+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 30047+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 2625+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 4619+[[domain]
IP 5.5.5.5.domain > 50.22.202.132.domain: 15587+ A? d.com. (23)
IP 5.5.5.5.domain > 50.22.202.132.domain: 52013+ A? db.org. (24)
IP 5.5.5.5.domain > 50.22.202.132.domain: 16768+ A? dba.com. (25)
IP 5.5.5.5.domain > 50.22.202.132.domain: 64560+ A? dbam.com. (26)
IP 5.5.5.5.domain > 50.22.202.132.domain: 15564+ A? dbamu.org. (27)
IP 5.5.5.5.domain > 50.22.202.132.domain: 17749+ A? dbamus.org. (28)
IP 5.5.5.5.domain > 50.22.202.132.domain: 10300+ A? dbamusd.org. (29)
IP 5.5.5.5.domain > 50.22.202.132.domain: 15936+ A? dbamusdf.org. (30)
IP 5.5.5.5.domain > 50.22.202.132.domain: 37538+ A? dbamusdfb.org. (31)
IP 5.5.5.5.domain > 50.22.202.132.domain: 55660+ A? dbamusdfbg.com. (32)
IP 5.5.5.5.domain > 50.22.202.132.domain: 55624+ A? dbamusdfbglf.org. (33)
IP 5.5.5.5.domain > 50.22.202.132.domain: 13331+ A? dbamusdfbglf.com. (34)
IP 5.5.5.5.domain > 50.22.202.132.domain: 40351+ A? dbamusdfbglfp.com. (35)
IP 5.5.5.5.domain > 50.22.202.132.domain: 61221+ A? dbamusdfbglfpa.com. (36)
IP 5.5.5.5.domain > 50.22.202.132.domain: 597+ A? dbamusdfbglfpaem.com. (37)
IP 5.5.5.5.domain > 50.22.202.132.domain: 1775+ A? dbamusdfbglfpaem.org. (38)
IP 5.5.5.5.domain > 50.22.202.132.domain: 21790+ A? dbamusdfbglfpaemo.com. (39)
IP 5.5.5.5.domain > 50.22.202.132.domain: 15724+ A? dbamusdfbglfpaemow.com. (40)
IP 5.5.5.5.domain > 50.22.202.132.domain: 7829+ A? dbamusdfbglfpaemowrc.org. (41)
IP 5.5.5.5.domain > 50.22.202.132.domain: 3914+ A? dbamusdfbglfpaemowrc.org. (42)
IP 5.5.5.5.domain > 50.22.202.132.domain: 14663+ A? dbamusdfbglfpaemowrcb.org. (43)
IP 5.5.5.5.domain > 50.22.202.132.domain: 26636+ A? dbamusdfbglfpaemowrcbj.com. (44)
IP 5.5.5.5.domain > 50.22.202.132.domain: 6321+ A? dbamusdfbglfpaemowrcbjx.com. (45)
IP 5.5.5.5.domain > 50.22.202.132.domain: 28727+ A? dbamusdfbglfpaemowrcbjxg.com. (46)
IP 5.5.5.5.domain > 50.22.202.132.domain: 13806+ A? dbamusdfbglfpaemowrcbjxga.com. (47)
IP 5.5.5.5.domain > 50.22.202.132.domain: 44910+ A? dbamusdfbglfpaemowrcbjxgag.org. (48)
IP 5.5.5.5.domain > 50.22.202.132.domain: 15374+ A? dbamusdfbglfpaemowrcbjxgagh.com. (49)
IP 5.5.5.5.domain > 50.22.202.132.domain: 16333+ A? dbamusdfbglfpaemowrcbjxgaghv.org. (50)
IP 5.5.5.5.domain > 50.22.202.132.domain: 41679+ A? dbamusdfbglfpaemowrcbjxgaghvv.com. (51)
IP 5.5.5.5.domain > 50.22.202.132.domain: 33333+ A? dbamusdfbglfpaemowrcbjxgaghvvd.com. (52)
IP 5.5.5.5.domain > 50.22.202.132.domain: 43179+ A? dbamusdfbglfpaemowrcbjxgaghvvdvdo.org. (53)
IP 5.5.5.5.domain > 50.22.202.132.domain: 59203+ A? dbamusdfbglfpaemowrcbjxgaghvvdvdom.com. (54)
```

BGP Anonslarıyla DOS

- YouTube IP= 208.65.152.0/**22** (2^{10} IP adresi)
www.youtube.com -> 208.65.153.238, 239..
- Şubat 2008'de:
 - Pakistan telekom youtube yasaklamak için 208.65.153.0/**24** aralığını anons etmeye başladı
 - Spesifik prefixler daha önceliklidir(Routing karar mekanizmasında)
 - Anons sonrası Internet youtube.com'u Pakistan Telekomda sanıyordu
 - 2 saatliğine kesinti
- Önlemi?

Mail Bombing

Received : victim@dudul.com



Reply to : victim@dudul.com

Sender : anonymous@fvck.com

To : xxx@multiple server



Mail Server C



Mail Server B



Mail Server A

Mail Bomb Örnek

```
[root@depdep ~]# perl mailbomb.pl

mailbomb v1.0 - mass e-mail tool to aid sysadmins in tweaking spam filters - written by Mike Jackson

usage: mailbomb.pl <victim@victimhost.com> <mail relay> <amount> [-s] ["subject here"] [-b] ["body text here"]
    ex: ./mailbomb.pl bill@microsoft.com maila.microsoft.com 100 -s "Windows Sucks!" -b "Hi Bill, Windows should
n Doors!"
    note: if you don't specify the subject/bodytext on the command line, it'll use the static defaults.

[root@depdep ~]# perl mailbomb.pl huzeyfe@lifeoverip.net localhost 100 -s "Mailbomb" -b "Selam olsun"
>
[root@depdep ~]# perl mailbomb.pl huzeyfe@lifeoverip.net localhost 100 -s "Mailbomb" -b "Selam olsun"

mailbomb v1.0 - mass e-mail tool to aid sysadmins in tweaking spam filters - written by Mike Jackson

note: if you don't specify the subject/bodytext on the command line, it'll use the static defaults.

mail flooding [huzeyfe@lifeoverip.net] 100 times.

sending [1/100] from: [ident1@a.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [2/100] from: [etc4@d.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [3/100] from: [ident1@b.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [4/100] from: [etc4@e.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [5/100] from: [ident2@c.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [6/100] from: [ident3@a.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [7/100] from: [ident3@b.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [8/100] from: [etc4@a.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [9/100] from: [etc4@d.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [10/100] from: [ident2@b.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [11/100] from: [ident3@a.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [12/100] from: [ident3@c.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [13/100] from: [etc4@e.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [14/100] from: [ident1@etc.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [15/100] from: [ident2@c.com] subject: [Mailbomb] and body text: [Selam olsun]
sending [16/100] from: [etc4@etc.com] subject: [Mailbomb] and body text: [Selam olsun]
```

relay host önemli

Mailbomb Örnek

Gmail Search Documents Notes Recent View More



Search Mail

Search the Web

Show search options
Create a filter

Click here to enable desktop noti

Mail

Contacts

Tasks

Compose mail

Inbox (83)

Priority Inbox (18)

Starred

Archive Report spam Delete Move to Labels More actions Refresh

Put Your [SPAM OLABILIR] Mailbomb - Selam olsun

Names Here [SPAM OLABILIR] Mailbomb - Selam olsun

Random Real [SPAM OLABILIR] Mailbomb - Selam olsun

Random Real Mailbomb - Selam olsun

Put Your [SPAM OLABILIR] Mailbomb - Selam olsun

Random Real [SPAM OLABILIR] Mailbomb - Selam olsun

Names Here [SPAM OLABILIR] Mailbomb - Selam olsun

Put Your [SPAM OLABILIR] Mailbomb - Selam olsun

Put Your [SPAM OLABILIR] Mailbomb - Selam olsun

Put Your Mailbomb - Selam olsun

Put Your [SPAM OLABILIR] Mailbomb - Selam olsun

Random Real [SPAM OLABILIR] Mailbomb

Names Here [SPAM OLABILIR] Mailbomb

Random Real [SPAM OLABILIR] Mailbomb

Names Here [SPAM OLABILIR] Mailbomb

Names Here [SPAM OLABILIR] Mailbomb

Random Real [SPAM OLABILIR] Mailbomb

Names Here [SPAM OLABILIR] Mailbomb

Random Real [SPAM OLABILIR] Mailbomb

Put Your [SPAM OLABILIR] Mailbomb

Put Your (2) [SPAM OLABILIR] Mailbomb

Put Your Mailbomb - Selam olsun

Random Real [SPAM OLABILIR] Mailbomb

Random Real [SPAM OLABILIR] Mailbomb

Names Here [SPAM OLABILIR] Mailbomb

Put Your Mailbomb - Selam olsun

* 1.1 INVALID_DATE Invalid Date: header (not RFC 2822)
* 1.0 DATE_IN_PAST_12_24 Date: is 12 to 24 hours before Received: date
* 0.9 DKIM_ADSP_NXDOMAIN No valid author signature and domain not in DNS
* 3.0 BAYES_50 BODY: Bayes spam probability is 40 to 60%
[score: 0.5879]
* 0.8 RDNS_NONE Delivered to internal network by a host with no rDNS
X-Spam-Status: Yes, score=6.8 required=6.0 tests=BAYES_50=3,
DATE_IN_PAST_12_24=1.049,DKIM_ADSP_NXDOMAIN=0.9,INVALID_DATE=1.096,
RDNS_NONE=0.793 seclabs.bga.com.tr 1215; Body=0 Reported 0 times.
autolearn=no version=3.3.1
Received: from unknown (HELO depdep.siberguvenlik.org) (178.18.197.18)
by seclabs.bga.com.tr with SMTP; 9 Feb 2011 17:26:31 -0000
Received: from localhost.localdomain (depdep.siberguvenlik.org [127.0.0.1])
by depdep.siberguvenlik.org (Postfix) with ESMTP id A3CA0D0008E
for <huzeyfe@lifeoverip.net>; Wed, 9 Feb 2011 19:25:08 +0200 (EET)
Date: Wed Feb 9 19:25:03 2011
From: Put Your <ident2@c.com>
To: huzeyfe@lifeoverip.net
Subject: [SPAM OLABILIR] Mailbomb
Message-Id: <20110209172508.A3CA0D0008E@depdep.siberguvenlik.org>
X-Spam-Prev-Subject: Mailbomb

Selam olsun

Mail bomb
yapan IP
adresi

Yerel Kaynak Tüketimi

The image shows two PuTTY terminal windows. The top window, titled '192.168.2.23 - PuTTY', displays the output of the 'top' command. It shows system statistics and a table of running processes. The process 'localdos' (PID 3304) is highlighted with a red box. A red arrow points from this box to the bottom window. The bottom window, also titled '192.168.2.23 - PuTTY', shows a C program being edited in a text editor. The program includes `<stdio.h>` and has a `main()` function with an infinite `while(1)` loop that prints the value of `x` and increments it.

```
top - 17:10:56 up 9 min,  3 users,  load average: 1.03, 0.52, 0.22
Tasks:  64 total,   2 running, 62 sleeping,   0 stopped,   0 zombie
Cpu(s):  2.7%us, 97.3%sy,  0.0%ni,  0.0%id,  0.0%wa,  0.0%hi,  0.0%si,  0.0%st
Mem:    449824k total,   55116k used,  394708k free,   1540k buffers
Swap:      0k total,      0k used,      0k free,  28928k cached

  PID USER      PR  NI  VIRT  RES  SHR  S %CPU  %MEM    TIME+  COMMAND
 3304 root        25   0  1512   344  288  S 98.7   0.1   1:15.78 localdos
 3308 root        17   0  6764  2892  2140 S   1.0   0.6   0:00.03 vi
    1 root        15   0   764   292  248  S   0.0   0.1   0:01.47 init
```

```
#include<stdio.h>
main()
{
    while(1)
    {
        int x;
        x=0;
        printf("%d\n",++x);
    }
}
```


Bölüm-X:DOS/DDOS Test Araçları

- Jolt2
 - Windows/Cisco sistemlere karşı etkili(eski)
 - Nessus plugini vardır(jolt2.nasl)
- Juno
- ISIC
 - Ip stack integrity checker
- Hping ?
 - --flood –spoof seçenekleri ile
- Hyenae
- Ab
- HTTPDOS

Bölüm-E:DDOS Saldırılarını Engelleme

DOS Saldırılarını Engelleme

- İlk şart: Sağlam TCP/IP bilgisi
- ISP ile yakın iletişim
- Sınır güvenliğinin ilk halkası routerlar üzerinde
 - Src.port, src ip adresleri belirliyse
- Güvenlik duvarları/IPS'lerin özelliklerini bilme
- Bilinen ddos toollarının default özelliklerini öğrenip doğrudan bloklama
 - Src.port=2043 gibi.
- Kendi sistemlerinizi test edin/ettirin.

UDP Flood Saldırılarından korunma

- Daha güçlü güvenlik duvarları
- Belirli ip adresinden gelecek istekleri sınırlama
- Timeout değerlerini düşürme
 - 60 saniyeden 10 saniyeye düşürülebilir(saldırı anında)

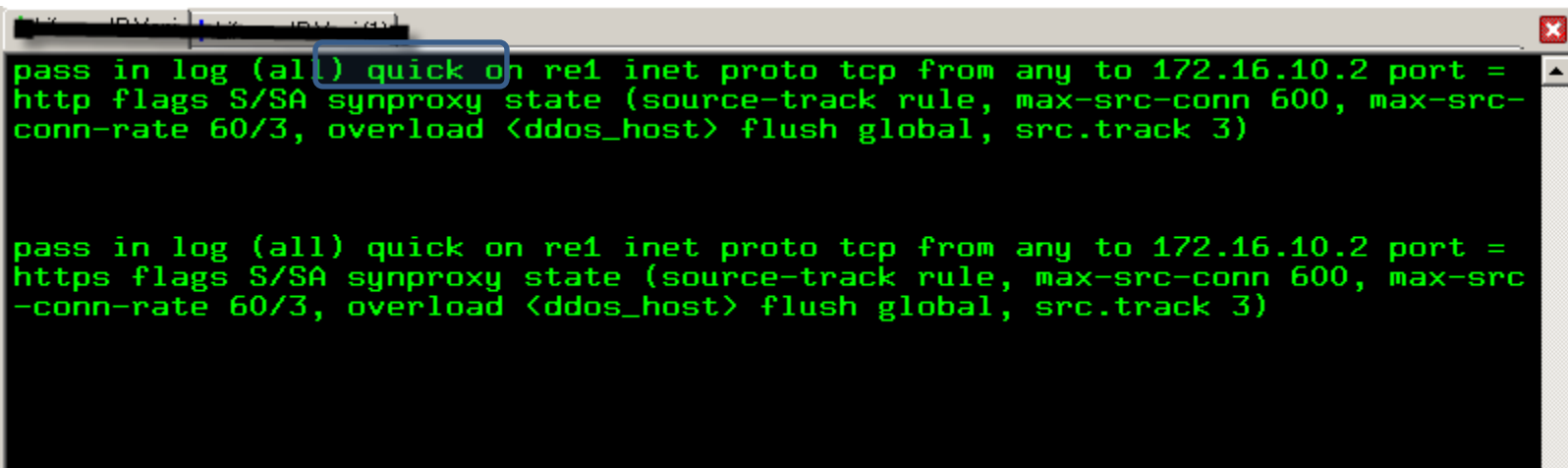
SYN Flood Koruma-1

- Tcp timeout değerlerini düşürme

```
TIMEOUTS:
tcp.first          120s
tcp.opening        30s
tcp.established    86400s
tcp.closing        900s
tcp.finwait        45s
tcp.closed         90s
tcp.tsdiff         30s
udp.first          60s
udp.single         30s
udp.multiple       60s
icmp.first         20s
icmp.error         10s
other.first        60s
other.single       30s
other.multiple     60s
frag              30s
interval          10s
adaptive.start     60000 states
adaptive.end       120000 states
src.track          0s
```

Syn Flood Koruma-II

- TCP servisleri önüne güvenlik duvarı koyma
- Syn cookies özelliği kullanma
- Syncache mekanizması
- Syn proxy mekanizması



```
pass in log (all) quick on re1 inet proto tcp from any to 172.16.10.2 port =  
http flags S/SA synproxy state (source-track rule, max-src-conn 600, max-src-  
conn-rate 60/3, overload <ddos_host> flush global, src.track 3)  
  
pass in log (all) quick on re1 inet proto tcp from any to 172.16.10.2 port =  
https flags S/SA synproxy state (source-track rule, max-src-conn 600, max-src-  
conn-rate 60/3, overload <ddos_host> flush global, src.track 3)
```

SynCookie Mantığı

- Amaç: Kandırılmış ip adreslerinden gelen SYN paketleri için kaynak harcamamak
- Bunun için belirli zaman geçerli olacak cookiler üretilerek SQN olarak gönderilir.
- Dönen ACK cevapları(dönerse) tekrar cookie mantığıyla kontrol edilip kabul edilir.
- Dezavantajı:Yüklü SYN flood saldırılarında kriptografik işlemlerden dolayı CPU performans problemi.

SYN Cookie Alt etme

- Sunucu tarafında kullanılan syncookie özelliği istemci tarafında da kullanılarak sunucudaki syncookie özelliği işe yaramaz hale getirilebilir.
- Böylece istemci kendi tarafında state tutmaz, sunucu tarafında da 3'lü el sıkışma tamamlandığı için bağlantı açık kalır(uzunun süre)
- Sockstress, scanrand araçları

Sonuç

- DOS/DDOS saldırıları internetin en temel sorunlarındanandır
- TCP/IP protokolü yapısı iyi bilinirse saldırılar büyük oranda engellenebilir.
- Sadece protokollerin yapısı değil, DDOS'a karşı korunmak istenen network yapısının bilinmesi ve DDOS saldırıları düşünülerek tasarlanması gerekir

DOS/DDOS Kaynakları

- <http://www.lifeoverip.net/ddos>

DDOS Eğitimleri

DDOS Saldırı Tipleri

DDOS saldırıları İnternet dünyasının en eski ve en etkili saldırılarından. DDOS saldırılarına karşı kesin bir reçete olamayacağı için bu tip saldırılarla karşı karşıya kalmadan konu hakkında detaylı bilgi sahibi olmak en büyük silahtır. Konu hakkında bilgi sahibi olmadan alınacak DDOS koruma ürünleri ayrı bir DOS'a(servis kesintisi) sebep olabilmektedir.

Bu eğitimle birlikte sık kullanılan ve etkili olan DDOS yöntemleri, çalışma mantıkları, uygulamaları ve korunma yöntemlerini hem teorik olarak öğrenme hem de pratik olarak görme fırsatı yakalayacaksınız. Eğitimciler Türkiye ve yurt dışında çeşitli firmaların DDOS Testlerini yapmış uzman kişilerden oluşmaktadır.

DDOS Saldırı Tipleri ve Engelleme Yöntemleri Eğitim İçeriği

1.Temel TCP/IP Bilgisi

1. İnternetin Altyapısı TCP/IP Protokol Ailesi
2. TCP/IP Ailesi Protokolleri Çalışma Yöntemleri
3. ARP, IP, ICMP, TCP, UDP, DNS, HTTP,SMTP Protokolleri

2.Çözülemeyen Problem DDOS