Advanced Network Security

DoS

Dr. Yaeghoobi

PhD. Computer Science & Engineering, Networking, India

dr.yaeghoobi@gmail.com

00 Denial of Service (DoS)

01 Targets (OSI layer)

02 DoS Attack Classification

03 Botnet

04 DDoS Case Study

05 Dos/DDoS Tools

06 DDoS Countermeasures

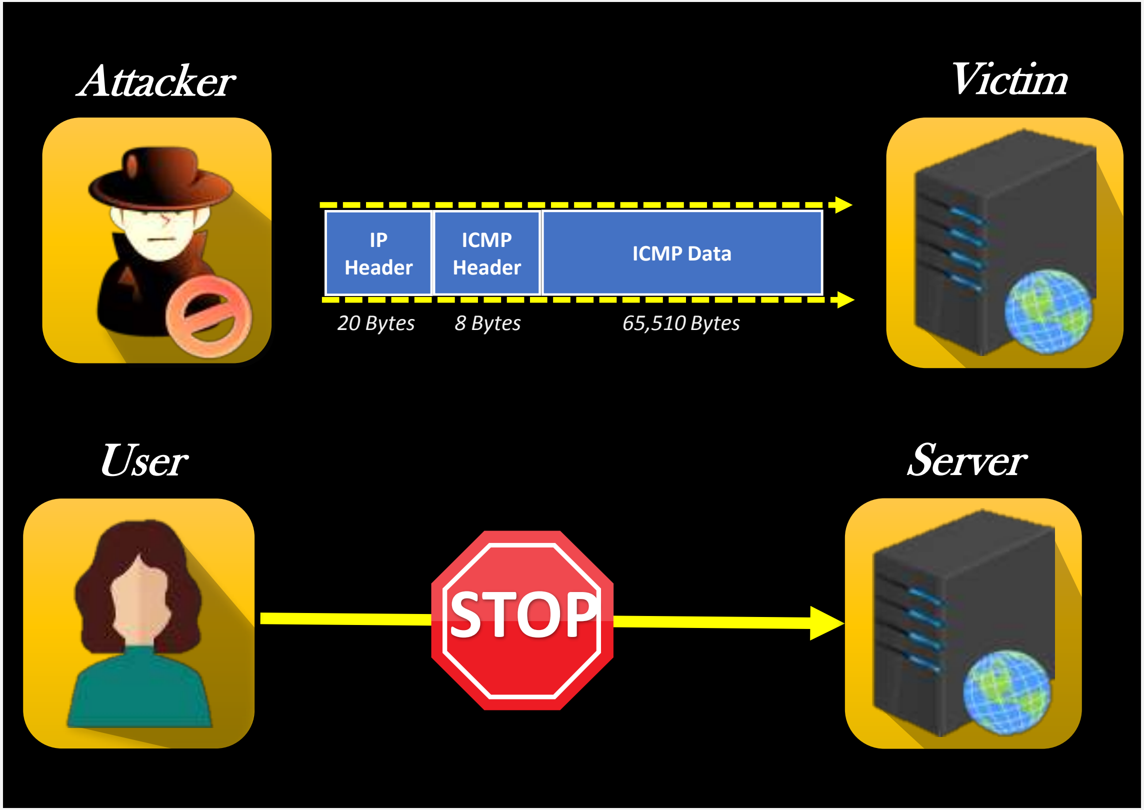
Denial of Service (DoS)

00

Denial of Service Attack

- Denial of Service (DoS) is an **Attack** on a **Computer** or **Network** that **Reduces, Restricts** or **Prevent** Legitimate use of its Resources.

- **DoS** : when a single host attacks
- **DDoS** : when multiple hosts attack simultaneously


Attacker
Victim
IP Header
ICMP Header
ICMP Data
20 Bytes
8 Bytes
65,510 Bytes
User
Server
STOP

Denial of Service Attack …

- In DoS Attack, Attackers **Flood** a Victim System with **Non-Legitimate Service Requests** or **Traffic** to **overload its Resources**.
- در حمله DoS مهاجمان با درخواست خدمات غیر قانونی یا ترافیک، بار اضافی بر روی سیستم و منابع قربانیان ایجاد می‌کنند.
- DoS is an attack through which a person can render a system **unusable**, or **significantly slow** it down for legitimate users, by overloading its resources.
- **If an attacker is unable** to gain access to a machine, the attacker will most likely **crash the machine** to accomplish a denial of service attack.

Denial of Service Attack …

- DoS is an attack through which a person can render a system **unusable**, or **significantly slow** it down for legitimate users, by overloading its resources.
- **If an attacker is unable** to gain access to a machine, the attacker will most likely **crash the machine** to accomplish a denial of service attack.
- اگر مهاجمی نتواند به ماشین دسترسی پیدا کند، مهاجم به احتمال زیاد دستگاه را خراب می کند تا حمله انکار ناپذیر بر روی سرویس انجام دهد.

Goal of DoS

- The goal of DoS is **not to gain unauthorized access to machines or data**, but to **prevent legitimate users of a service from using it.**

- هدف، DoS دستیابی غیرمجاز به ماشینها یا داده ها نیست، بلکه جلوگیری از استفاده قانونی کاربران از یک سرویس است.

Goal of DoS ...

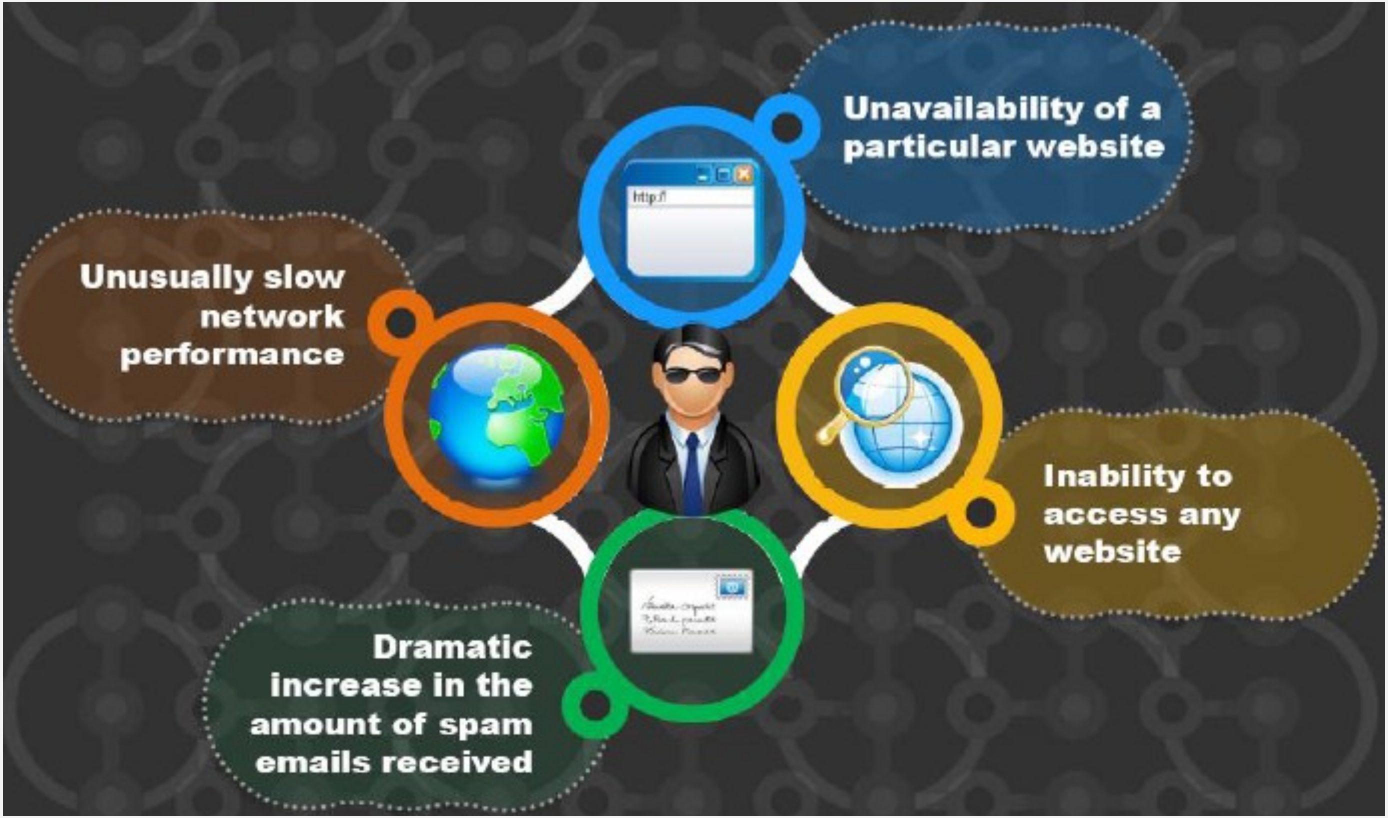
- Purpose is to shut down a site, not penetrate it.
- هدف این است که یک سایت را پایین بیاورید، نه در آن نفوذ کنید.
- Purpose may be vandalism, extortion or social action (including terrorism) (Sports betting sites often extorted)
- هدف ممکن است خرابکاری، اخاذی یا اقدام اجتماعی (از جمله تروریسم) باشد (سایتهای شرط بندی ورزشی)
- • Modification of internal data, change of programs (Includes defacement of web sites)
- اصلاح داده های داخلی، تغییر برنامه ها (شامل جابجایي وب سایت ها)

Attackers may:

- Attempt to **flood a network**, thereby **preventing legitimate network traffic**
- Attempt to **disrupt connections** between two machines, thereby **preventing access to a service**
- Attempt to **prevent** a particular **individual from accessing a service**
- Attempt to **disrupt** service to a **specific system or person**

SERVER IS UP!
AAAAND IT'S GONE

DoS Symptoms



Unavailability of a particular website

Unusually slow network performance

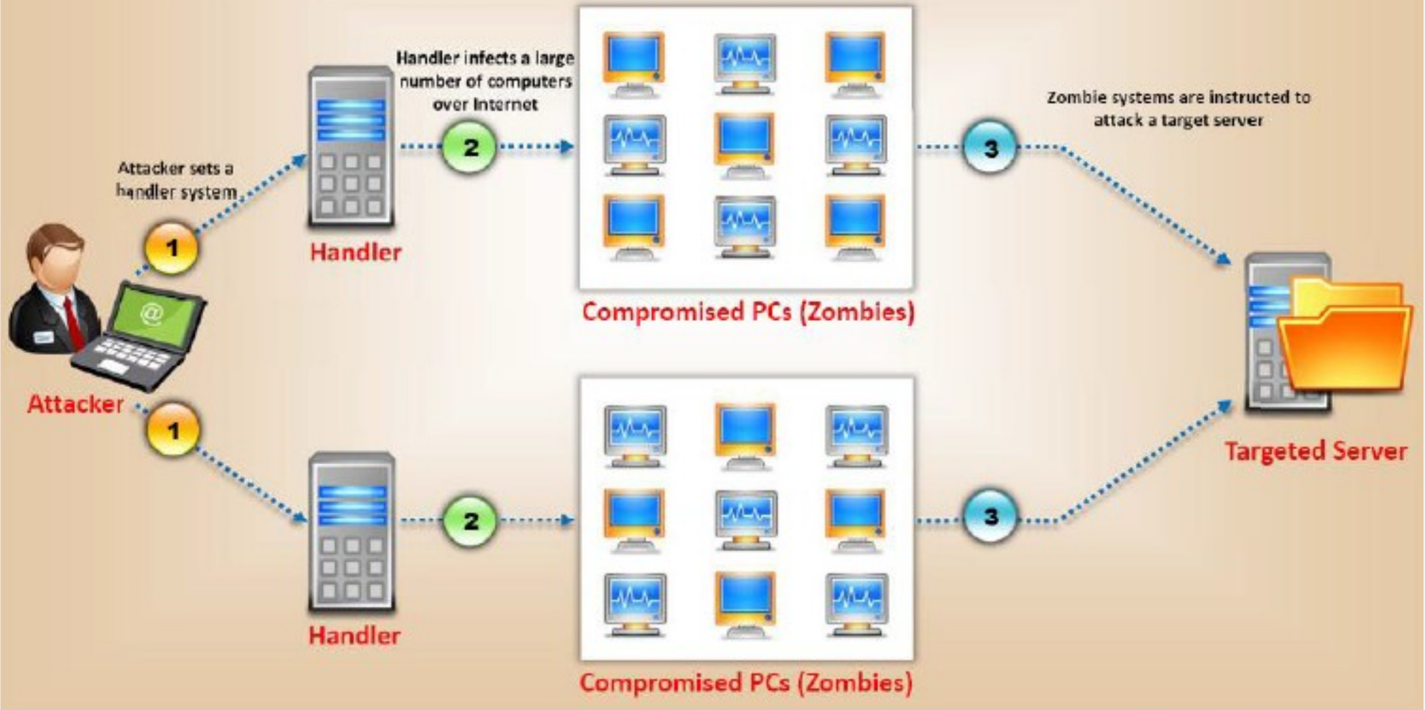
Inability to access any website

Dramatic increase in the amount of spam emails received

DDoS Attack

- A distributed denial of service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system.
- انکار توزیع خدمات توزیع شده از جمله مواردی است که در آن تعداد زیادی از سیستمهای به خطر افتاده به یک هدف واحد حمله می کنند و در نتیجه باعث عدم دسترسی به سرویس برای کاربران می شود.
- The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.
- سیل پیام های دریافتی در سیستم هدف اساساً آن را مجبور به خاموش شدن می‌کند و از این طریق خدمات به کاربران تکذیب می شود.

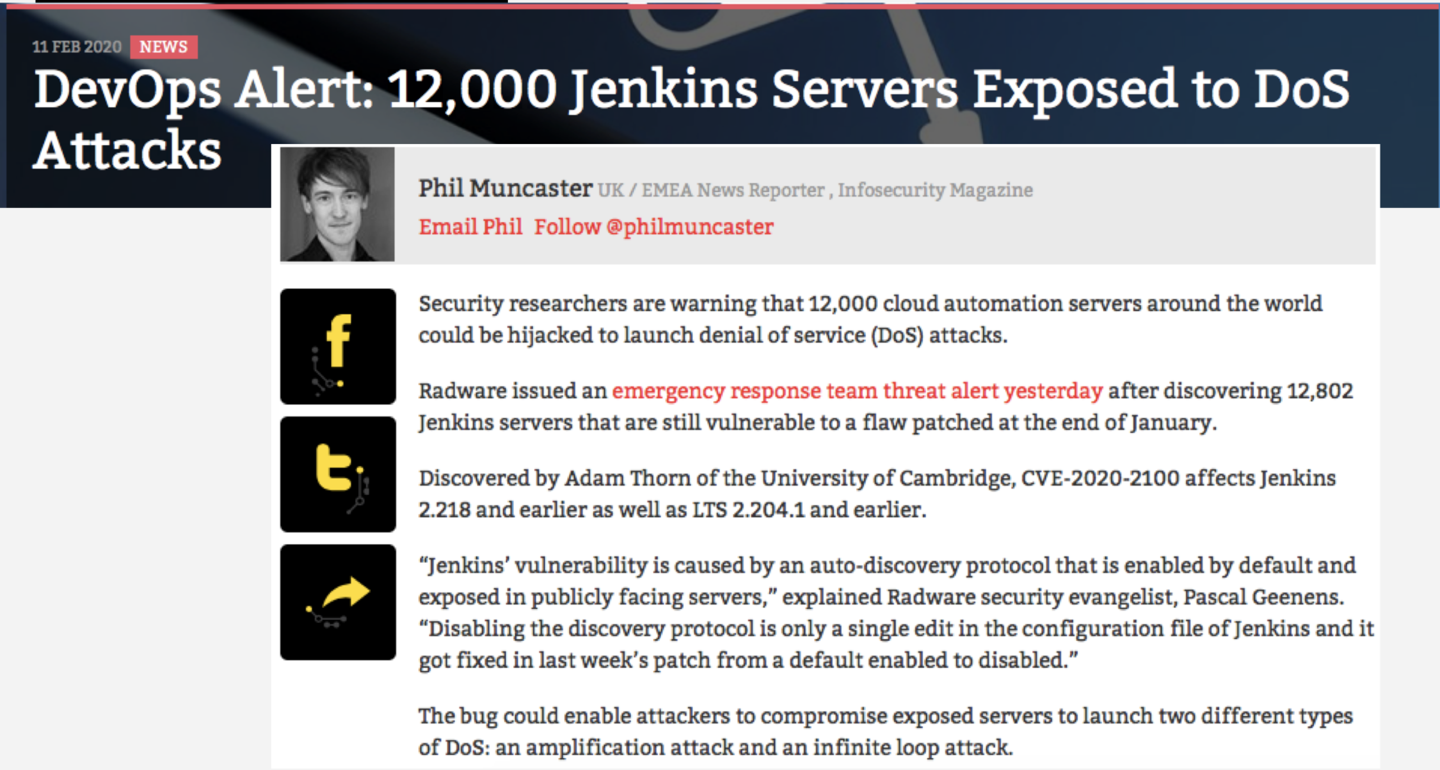
How DDoS Work?



Handler infects a large number of computers over Internet
Zombie systems are instructed to attack a target server
Attacker sets a handler system
1
2
3
Handler
Compromised PCs (Zombies)
Attacker
Targeted Server
1
2
3
Handler
Compromised PCs (Zombies)

Recent Cases

info security
STRATEGY | INSIGHT | TECHNOLOGY



11 FEB 2020 NEWS

DevOps Alert: 12,000 Jenkins Servers Exposed to DoS Attacks

Phil Muncaster UK / EMEA News Reporter , Infosecurity Magazine
Email Phil Follow @philmuncaster

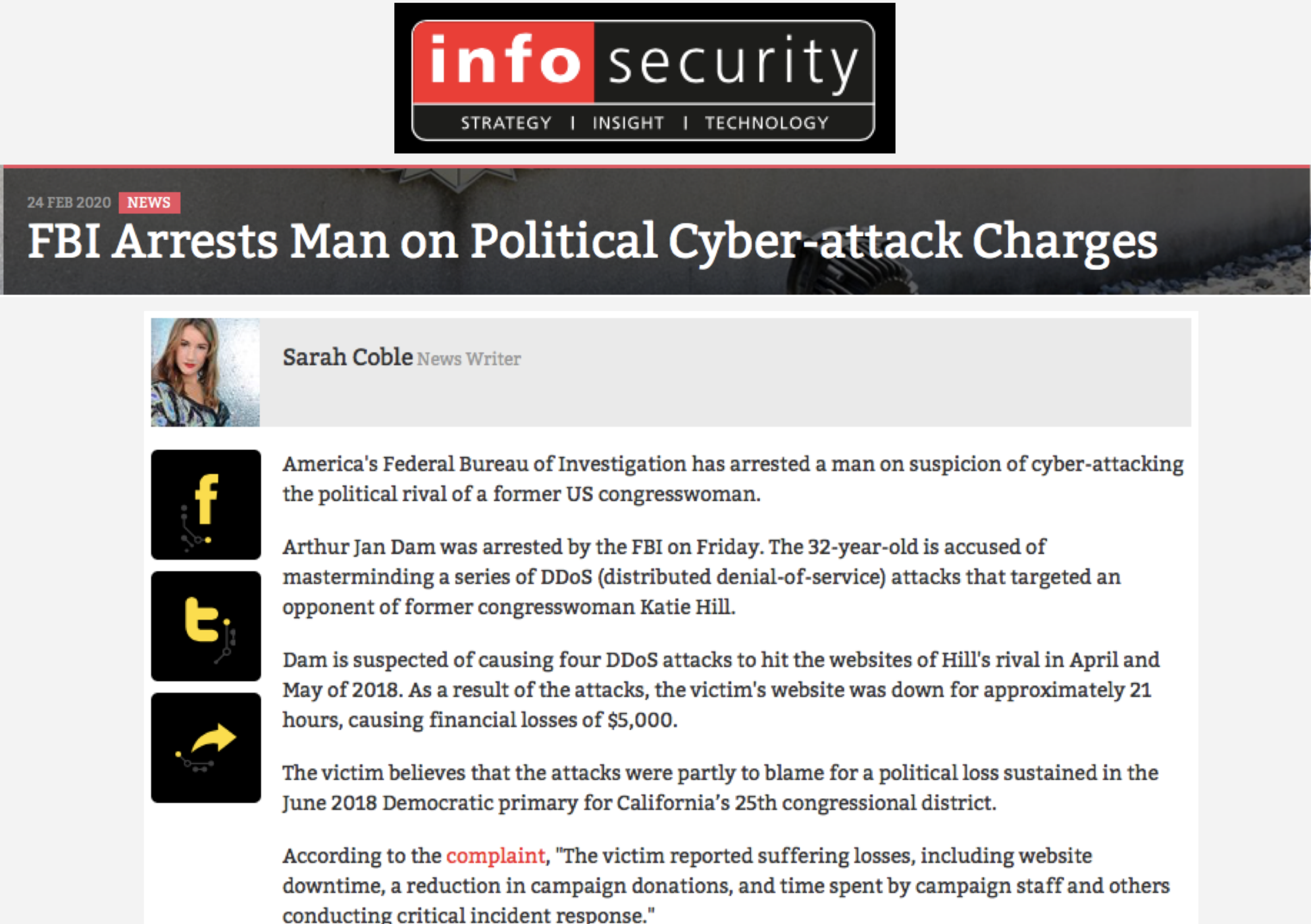
Security researchers are warning that 12,000 cloud automation servers around the world could be hijacked to launch denial of service (DoS) attacks.

Radware issued an emergency response team threat alert yesterday after discovering 12,802 Jenkins servers that are still vulnerable to a flaw patched at the end of January.

Discovered by Adam Thorn of the University of Cambridge, CVE-2020-2100 affects Jenkins 2.218 and earlier as well as LTS 2.204.1 and earlier.

"Jenkins' vulnerability is caused by an auto-discovery protocol that is enabled by default and exposed in publicly facing servers," explained Radware security evangelist, Pascal Geenens. "Disabling the discovery protocol is only a single edit in the configuration file of Jenkins and it got fixed in last week's patch from a default enabled to disabled."

The bug could enable attackers to compromise exposed servers to launch two different types of DoS: an amplification attack and an infinite loop attack.



info security
STRATEGY | INSIGHT | TECHNOLOGY

24 FEB 2020 NEWS

FBI Arrests Man on Political Cyber-attack Charges

Sarah Coble News Writer

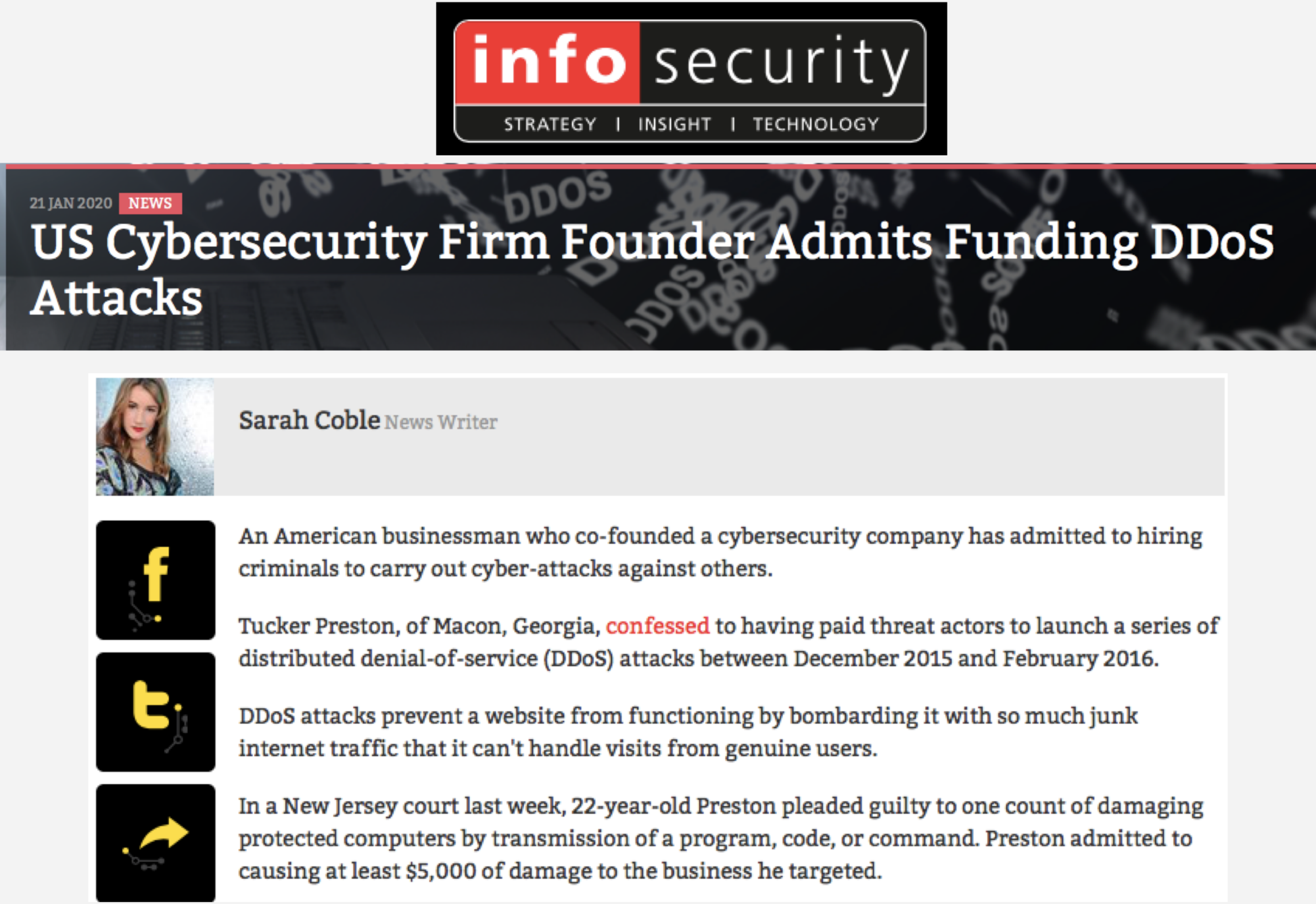
America's Federal Bureau of Investigation has arrested a man on suspicion of cyber-attacking the political rival of a former US congresswoman.

Arthur Jan Dam was arrested by the FBI on Friday. The 32-year-old is accused of masterminding a series of DDoS (distributed denial-of-service) attacks that targeted an opponent of former congresswoman Katie Hill.

Dam is suspected of causing four DDoS attacks to hit the websites of Hill's rival in April and May of 2018. As a result of the attacks, the victim's website was down for approximately 21 hours, causing financial losses of $5,000.

The victim believes that the attacks were partly to blame for a political loss sustained in the June 2018 Democratic primary for California's 25th congressional district.

According to the complaint, "The victim reported suffering losses, including website downtime, a reduction in campaign donations, and time spent by campaign staff and others conducting critical incident response."



info security
STRATEGY | INSIGHT | TECHNOLOGY

21 JAN 2020 NEWS

US Cybersecurity Firm Founder Admits Funding DDoS Attacks

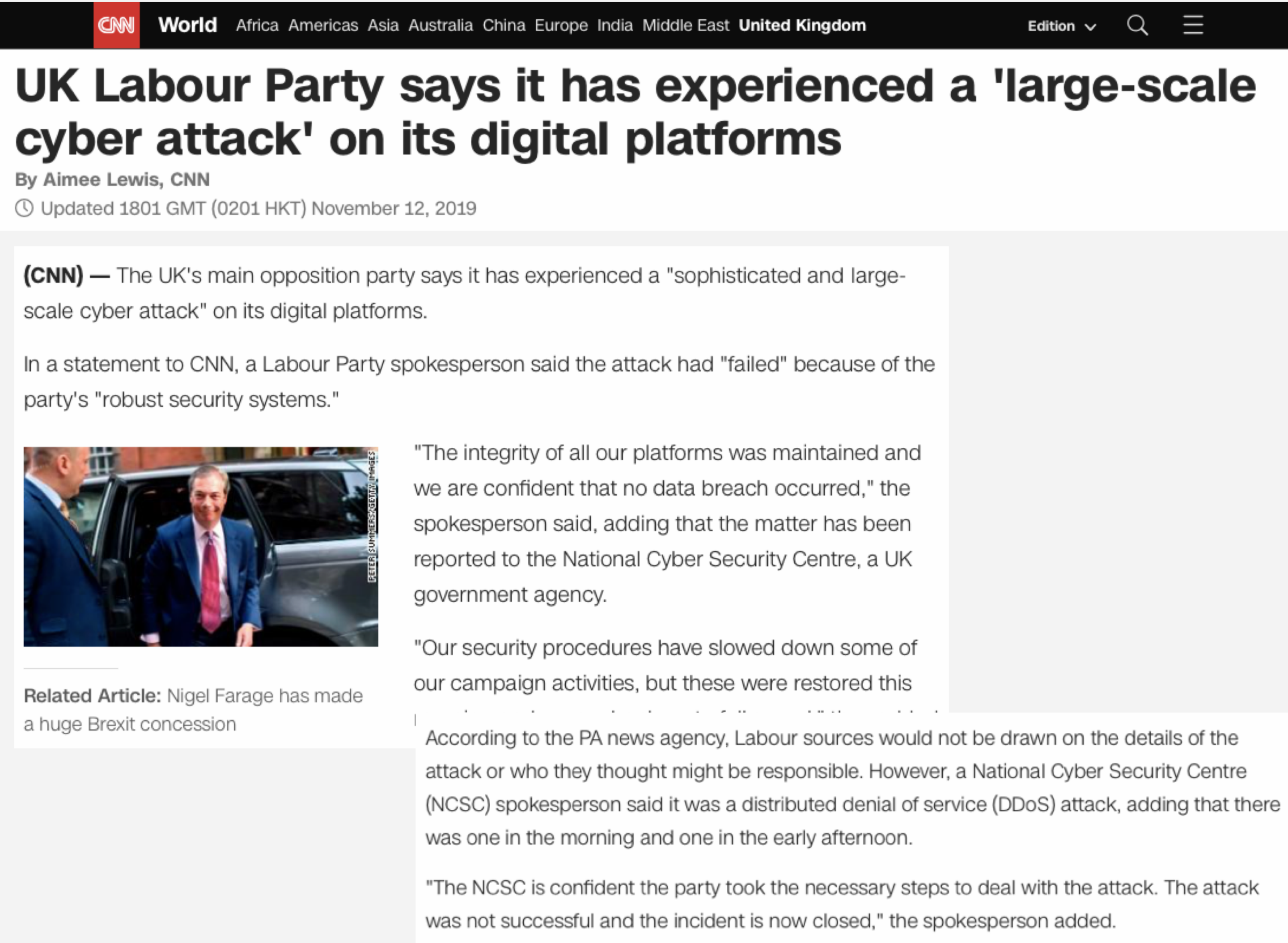
Sarah Coble News Writer

An American businessman who co-founded a cybersecurity company has admitted to hiring criminals to carry out cyber-attacks against others.

Tucker Preston, of Macon, Georgia, confessed to having paid threat actors to launch a series of distributed denial-of-service (DDoS) attacks between December 2015 and February 2016.

DDoS attacks prevent a website from functioning by bombarding it with so much junk internet traffic that it can't handle visits from genuine users.

In a New Jersey court last week, 22-year-old Preston pleaded guilty to one count of damaging protected computers by transmission of a program, code, or command. Preston admitted to causing at least $5,000 of damage to the business he targeted.



UK Labour Party says it has experienced a 'large-scale cyber attack' on its digital platforms

By Aimee Lewis, CNN

Updated 1801 GMT (0201 HKT) November 12, 2019

(CNN) — The UK's main opposition party says it has experienced a "sophisticated and large-scale cyber attack" on its digital platforms.

In a statement to CNN, a Labour Party spokesperson said the attack had "failed" because of the party's "robust security systems."

PETER SUMMERS/GETTY IMAGES

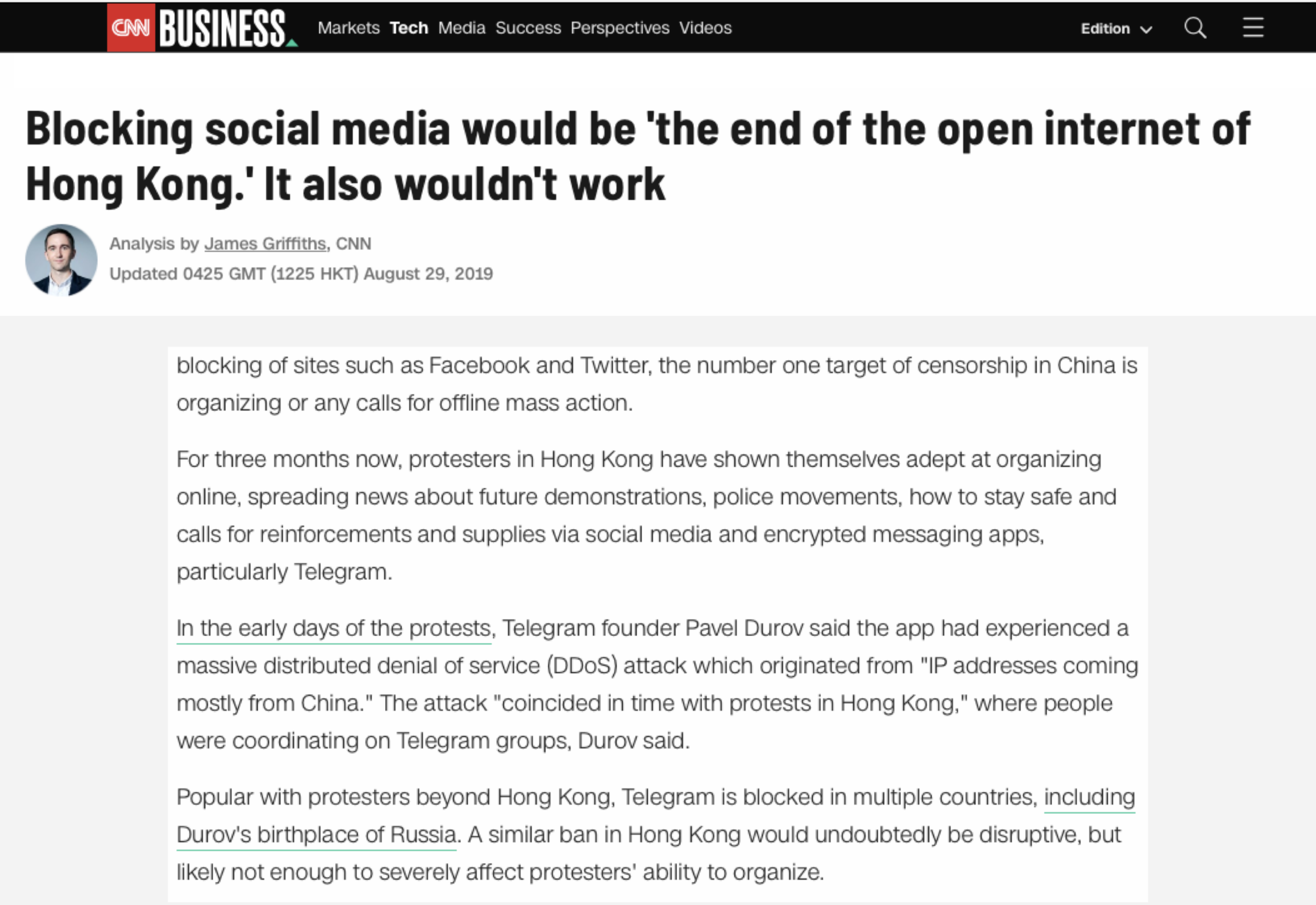
Related Article: Nigel Farage has made a huge Brexit concession

"The integrity of all our platforms was maintained and we are confident that no data breach occurred," the spokesperson said, adding that the matter has been reported to the National Cyber Security Centre, a UK government agency.

"Our security procedures have slowed down some of our campaign activities, but these were restored this

According to the PA news agency, Labour sources would not be drawn on the details of the attack or who they thought might be responsible. However, a National Cyber Security Centre (NCSC) spokesperson said it was a distributed denial of service (DDoS) attack, adding that there was one in the morning and one in the early afternoon.

"The NCSC is confident the party took the necessary steps to deal with the attack. The attack was not successful and the incident is now closed," the spokesperson added.



Blocking social media would be 'the end of the open internet of Hong Kong.' It also wouldn't work

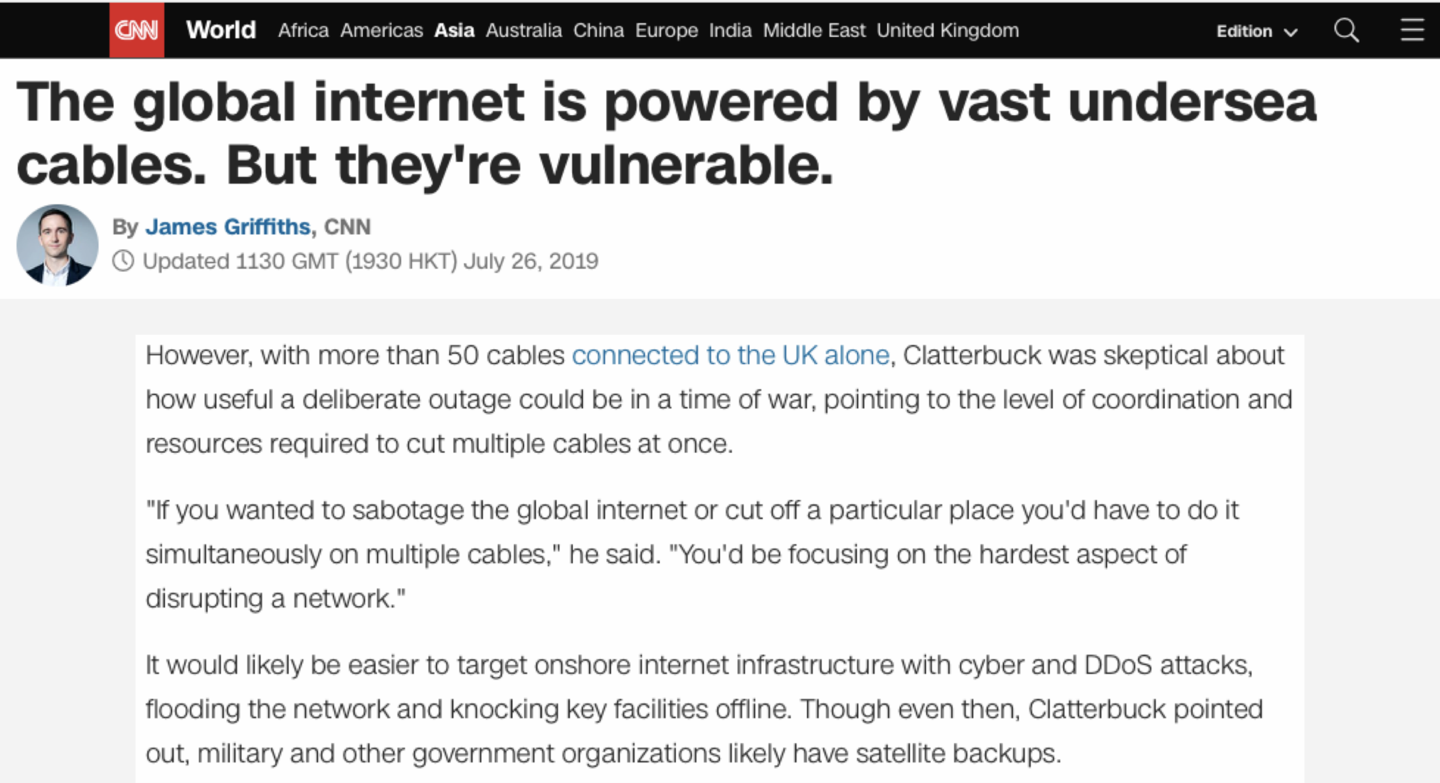
Analysis by James Griffiths, CNN
Updated 0425 GMT (1225 HKT) August 29, 2019

blocking of sites such as Facebook and Twitter, the number one target of censorship in China is organizing or any calls for offline mass action.

For three months now, protesters in Hong Kong have shown themselves adept at organizing online, spreading news about future demonstrations, police movements, how to stay safe and calls for reinforcements and supplies via social media and encrypted messaging apps, particularly Telegram.

In the early days of the protests, Telegram founder Pavel Durov said the app had experienced a massive distributed denial of service (DDoS) attack which originated from "IP addresses coming mostly from China." The attack "coincided in time with protests in Hong Kong," where people were coordinating on Telegram groups, Durov said.

Popular with protesters beyond Hong Kong, Telegram is blocked in multiple countries, including Durov's birthplace of Russia. A similar ban in Hong Kong would undoubtedly be disruptive, but likely not enough to severely affect protesters' ability to organize.



The global internet is powered by vast undersea cables. But they're vulnerable.

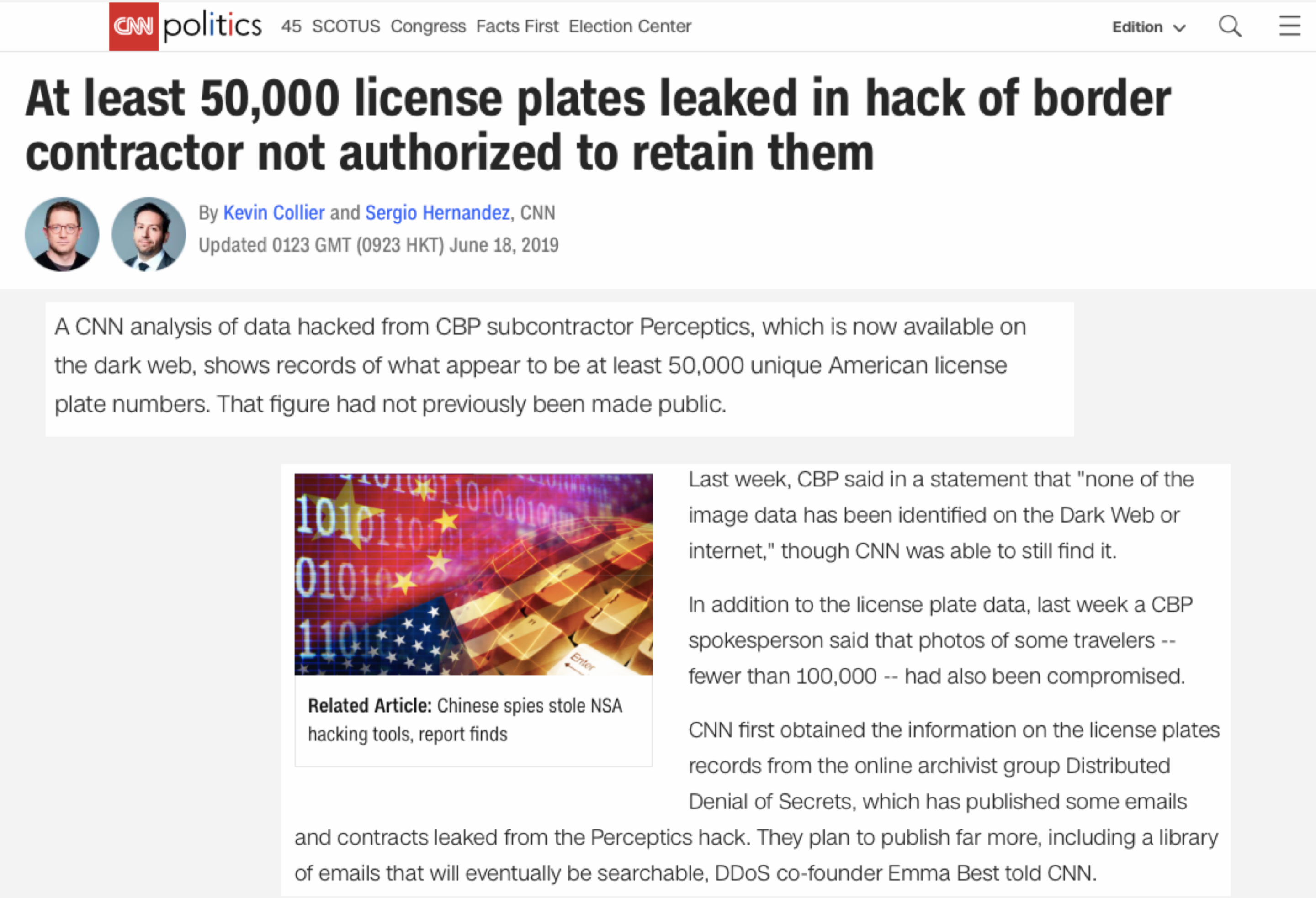
By James Griffiths, CNN

Updated 1130 GMT (1930 HKT) July 26, 2019

However, with more than 50 cables connected to the UK alone, Clatterbuck was skeptical about how useful a deliberate outage could be in a time of war, pointing to the level of coordination and resources required to cut multiple cables at once.

"If you wanted to sabotage the global internet or cut off a particular place you'd have to do it simultaneously on multiple cables," he said. "You'd be focusing on the hardest aspect of disrupting a network."

It would likely be easier to target onshore internet infrastructure with cyber and DDoS attacks, flooding the network and knocking key facilities offline. Though even then, Clatterbuck pointed out, military and other government organizations likely have satellite backups.



At least 50,000 license plates leaked in hack of border contractor not authorized to retain them

By Kevin Collier and Sergio Hernandez, CNN
Updated 0123 GMT (0923 HKT) June 18, 2019

A CNN analysis of data hacked from CBP subcontractor Perceptics, which is now available on the dark web, shows records of what appear to be at least 50,000 unique American license plate numbers. That figure had not previously been made public.

Related Article: Chinese spies stole NSA hacking tools, report finds

Last week, CBP said in a statement that "none of the image data has been identified on the Dark Web or internet," though CNN was able to still find it.

In addition to the license plate data, last week a CBP spokesperson said that photos of some travelers -- fewer than 100,000 -- had also been compromised.

CNN first obtained the information on the license plates records from the online archivist group Distributed Denial of Secrets, which has published some emails and contracts leaked from the Perceptics hack. They plan to publish far more, including a library of emails that will eventually be searchable, DDoS co-founder Emma Best told CNN.

Targets (OSI layer)

01

Targets (OSI layer)

Network (Layer 3)

Bandwidth consumption

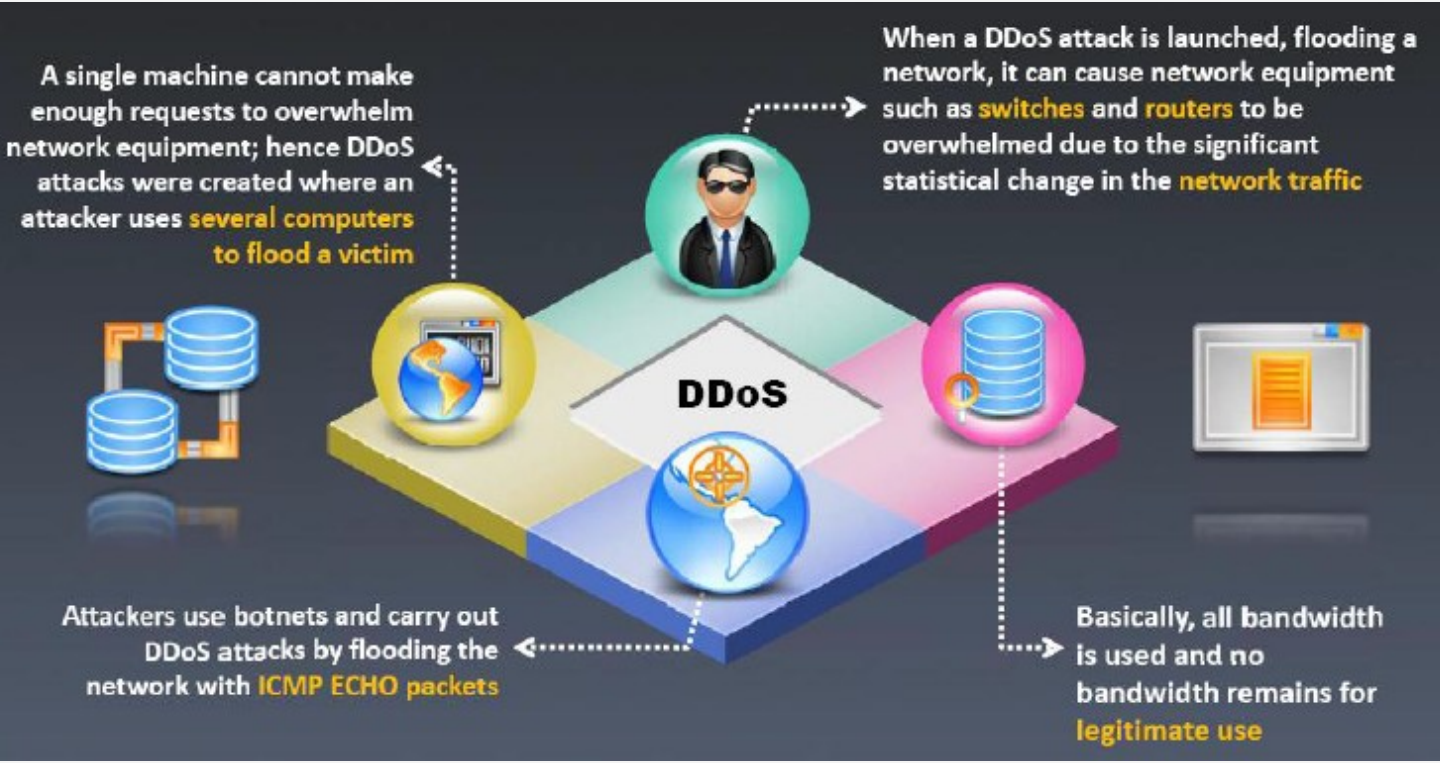
Layer 4 (Transport Protocol)

TCP attacks on server sockets

Application (Layer 7)

Application or operating system resources consumption

Bandwidth Attack



A single machine cannot make enough requests to overwhelm network equipment; hence DDoS attacks were created where an attacker uses several computers to flood a victim

When a DDoS attack is launched, flooding a network, it can cause network equipment such as switches and routers to be overwhelmed due to the significant statistical change in the network traffic

Attackers use botnets and carry out DDoS attacks by flooding the network with ICMP ECHO packets

Basically, all bandwidth is used and no bandwidth remains for legitimate use

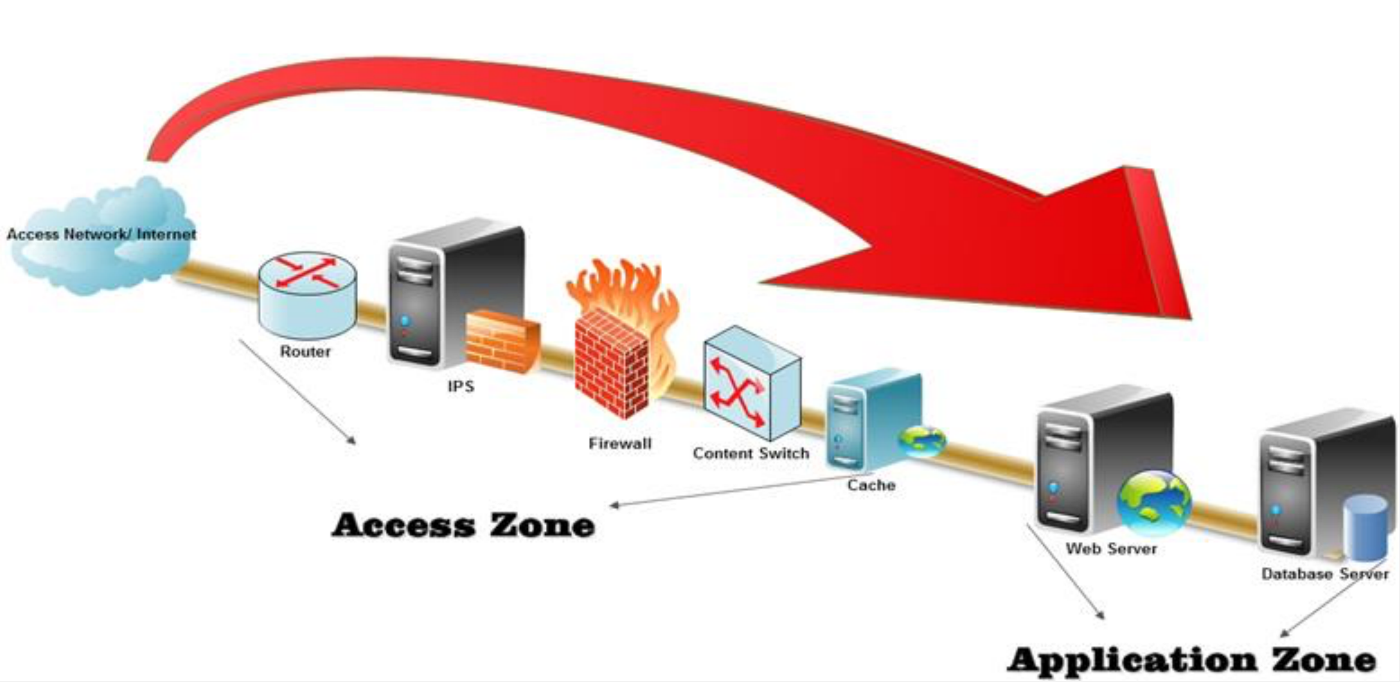
Layer 4 DoS Attack

- A **TCP connection** is established in what is known as a **3-way handshake**.
- The client sends a SYN packet, the server responds with a SYN ACK, and the client responds to *that* with an ACK. After the "three-way handshake" is complete, the TCP connection is considered established.
- Overwhelm a server by sending a **flood of SYN** packets and **then ignoring the SYN ACKs** returned by the server.
- This causes the **server to use up resources** waiting a configured amount of time for the anticipated ACK that *should* come from a legitimate client.

Layer 7 Attack

- HTTP attacks on Web server threads
- Web application attacks on CPU resources

Layer 7 DDoS Attacks

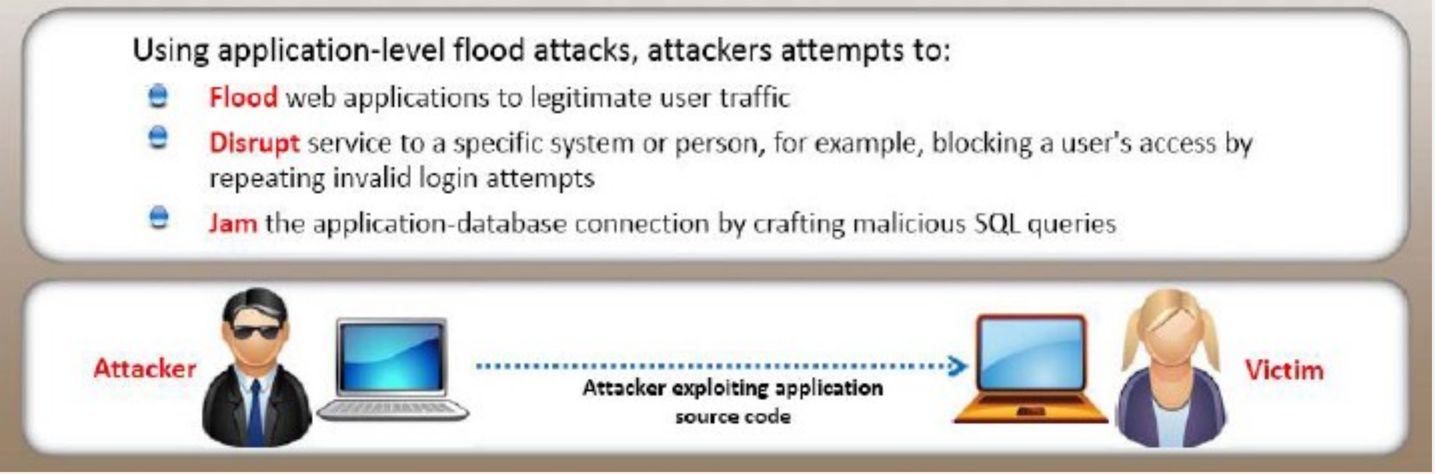


Layer 7 DoS Attacks

- A Network DoS attack operates in the logical “Access Zone”, an **application DoS attack** targets the “Application Zone”.
- That consists of the **web front-end** and the **data storage** for it.
- In order for an application DoS attack to be successful, it has to go around the entire set of “Access Zone” devices and mechanisms in place, **take advantage of a security gap on the “Application Zone”.**
- and then finally inject a payload that goes on to **establish a direct communication line with the web server**, to strike either the server itself or application.

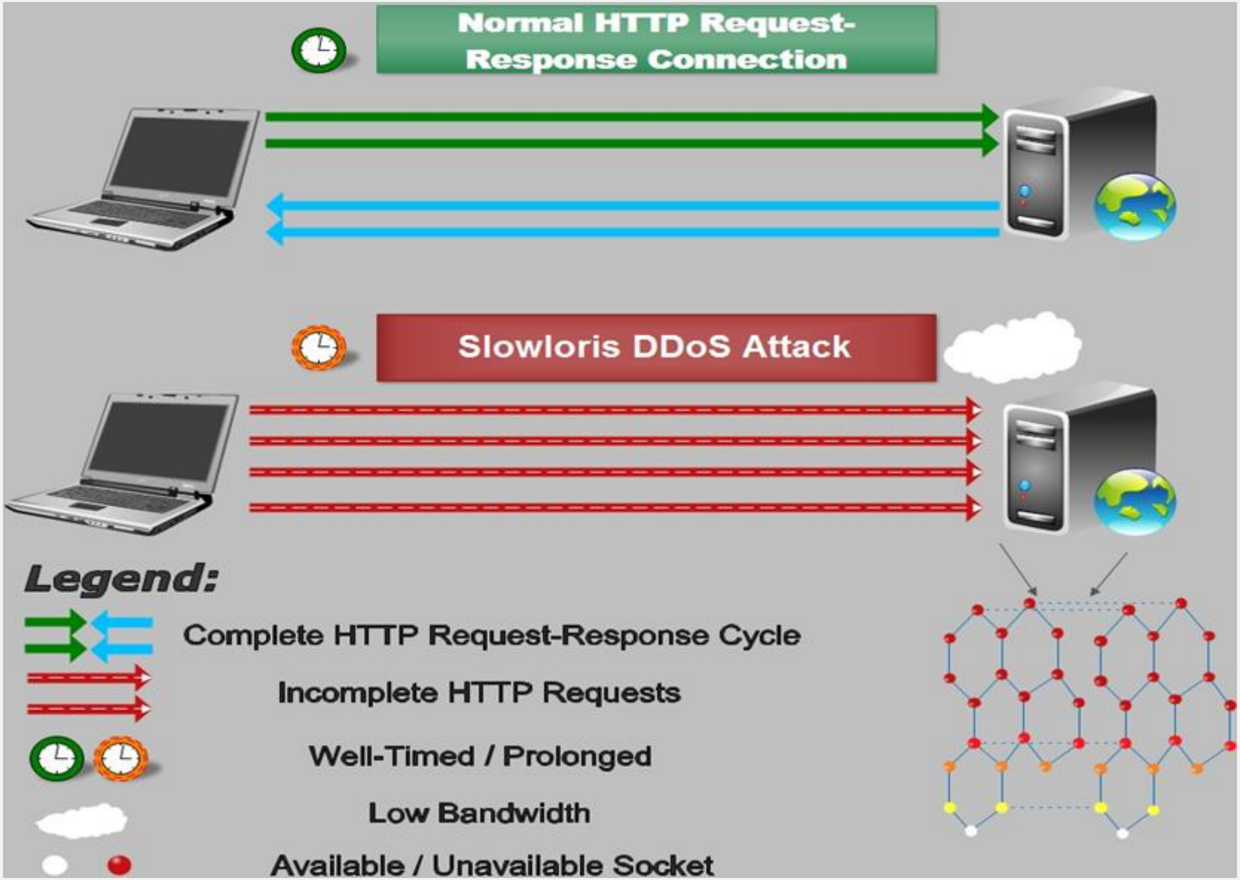
Layer 7 DoS Attacks

- Loss of Services
- Destroy programming source code and files



Using application-level flood attacks, attackers attempts to:

- **Flood** web applications to legitimate user traffic
- **Disrupt** service to a specific system or person, for example, blocking a user's access by repeating invalid login attempts
- **Jam** the application-database connection by crafting malicious SQL queries



Normal HTTP Request-Response Connection

Slowloris DDoS Attack

Legend:

Complete HTTP Request-Response Cycle

Incomplete HTTP Requests

Well-Timed / Prolonged

Low Bandwidth

○ ● Available / Unavailable Socket

Attack Possibilities by OSI Layer

OSI Layer	Protocol Data Unit (PDU)	Examples of Denial of Service Techniques at Each Level	Potential Impact of DoS Attack	Mitigation Options for Attack Type
Application Layer (7)	Data	PDF GET requests, HTTP GET, HTTP POST, = website forms (login, uploading photo/video, submitting feedback)	Reach resource limits of services Resource starvation	Application monitoring is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source more easily than other types of DDoS attacks
Presentation Layer (6)	Data	Malformed SSL Requests -- Inspecting SSL encryption packets is resource intensive. Attackers use SSL to tunnel HTTP attacks to target the server	The affected systems could stop accepting SSL connections or automatically restart	To mitigate, consider options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re- encrypted and forwarded back to the origin infrastructure with unencrypted content only ever residing in protected memory on a secure bastion host
Session (5)	Data	Telnet DDoS-attacker exploits a flaw in a Telnet server software running on the switch, rendering Telnet services unavailable	Prevents administrator from performing switch management functions	Check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability
Transport (4)	Segment	SYN Flood, Smurf Attack	Reach bandwidth or connection limits of hosts or networking equipment	DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its customers. This approach to block DDoS attacks makes the site in question completely inaccessible to all traffic, both malicious attack traffic and legitimate user traffic. Black holding is typically deployed by the ISP to protect other customers on its network from the adverse effects of DDoS attacks such as slow network performance and disrupted service
Network (3)	Packet	ICMP Flooding - A Layer 3 infrastructure DDoS attack method that uses ICMP messages to overload the targeted network's bandwidth	Can affect available network bandwidth and impose extra load on the firewall	Rate-limit ICMP traffic and prevent the attack from impacting bandwidth and firewall performance
Data Link (2)	Frame	MAC flooding -- inundates the network switch with data packets	Disrupts the usual sender to recipient flow of data -- blasting across all ports	Many advances switches can be configured to limit the number of MAC addresses that can be learned on ports connected to end stations; allow discovered MAC addresses to be authenticated against an authentication, authorization and accounting (AAA) server and subsequently filtered
Physical (1)	Bits	Physical destruction, obstruction, manipulation, or malfunction of physical assets	Physical assets will become unresponsive and may need to be repaired to increase availability	Practice defense in-depth tactics, use access controls, accountability, and auditing to track and control physical assets

DoS Attack Classification

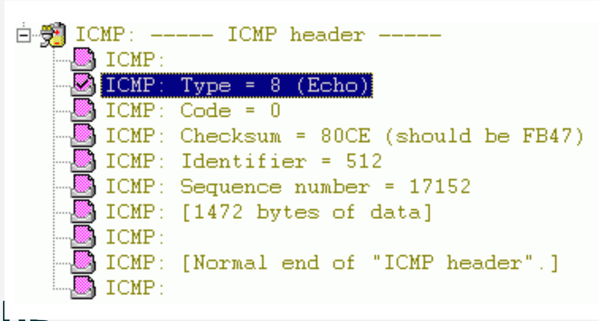
02

DoS Attack Classification

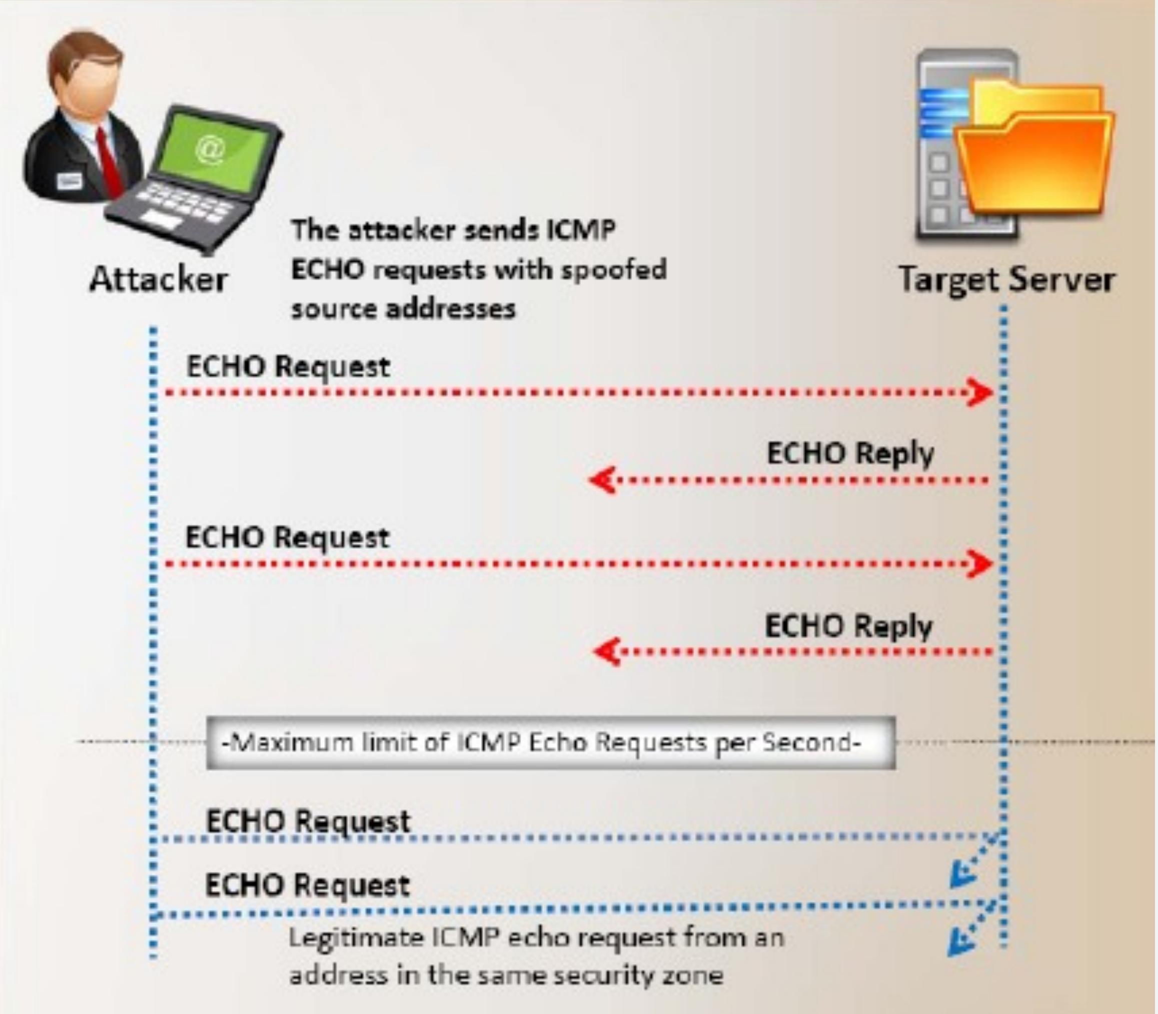
- Smurf
- Buffer Overflow Attack
- Ping of death
- Teardrop
- SYN Attack
- SYN Flooding
- Peer-to-Peer Attack
- Permanent DoS Attack (PDoS)

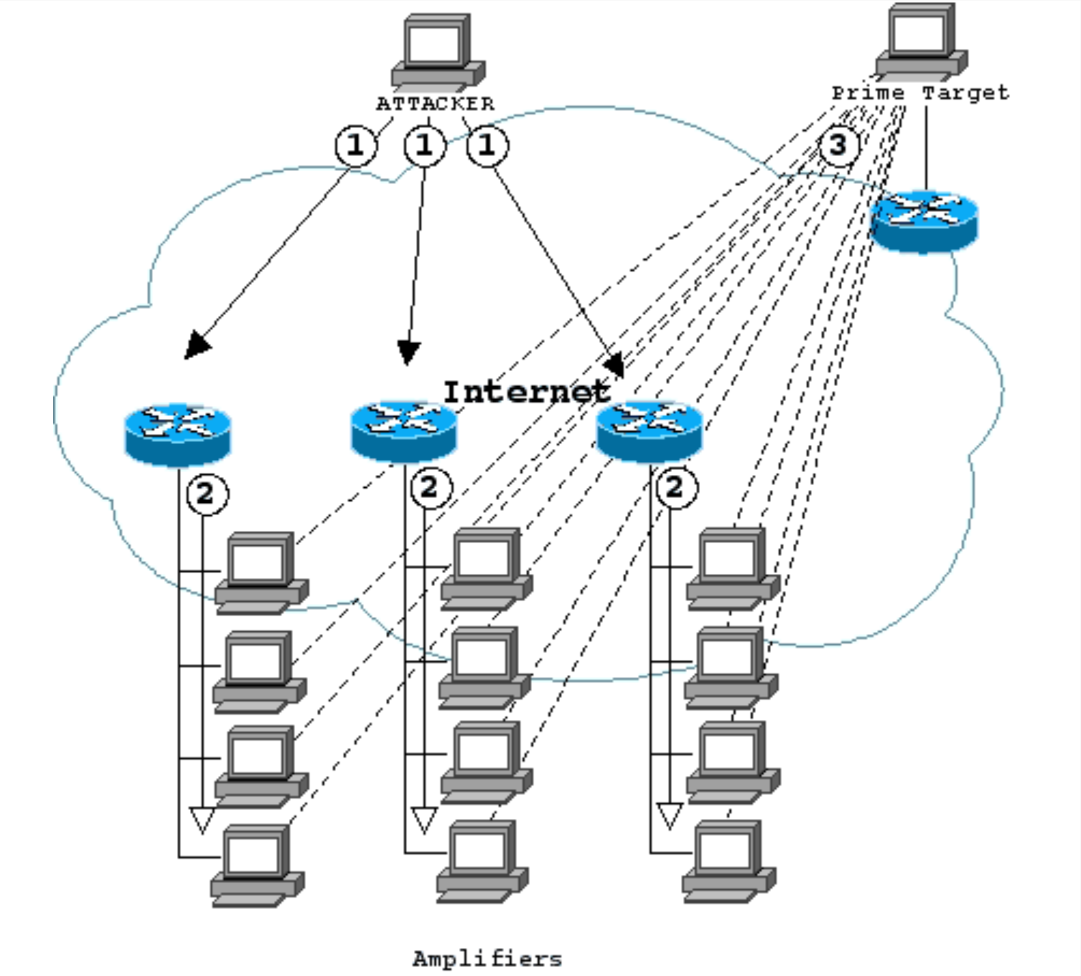
Smurf Attack

- The **perpetrator** generates a large amount of ICMP echo (ping) traffic to a network broadcast address with a spoofed source IP set to a victim host
- The **result will be lots of ping replies (ICMP Echo Reply) flooding the spoofed host**
- Amplified ping reply stream can overwhelm the victim’s network connection
- Fraggle attack, which uses UDP echo is similar to the smurf attack



```
ICMP: ------ ICMP header ------
   ICMP:
   ICMP: Type = 8 (Echo)
   ICMP: Code = 0
   ICMP: Checksum = 80CE (should be FB47)
   ICMP: Identifier = 512
   ICMP: Sequence number = 17152
   ICMP: [1472 bytes of data]
   ICMP:
   ICMP: [Normal end of "ICMP header".]
   ICMP:
```

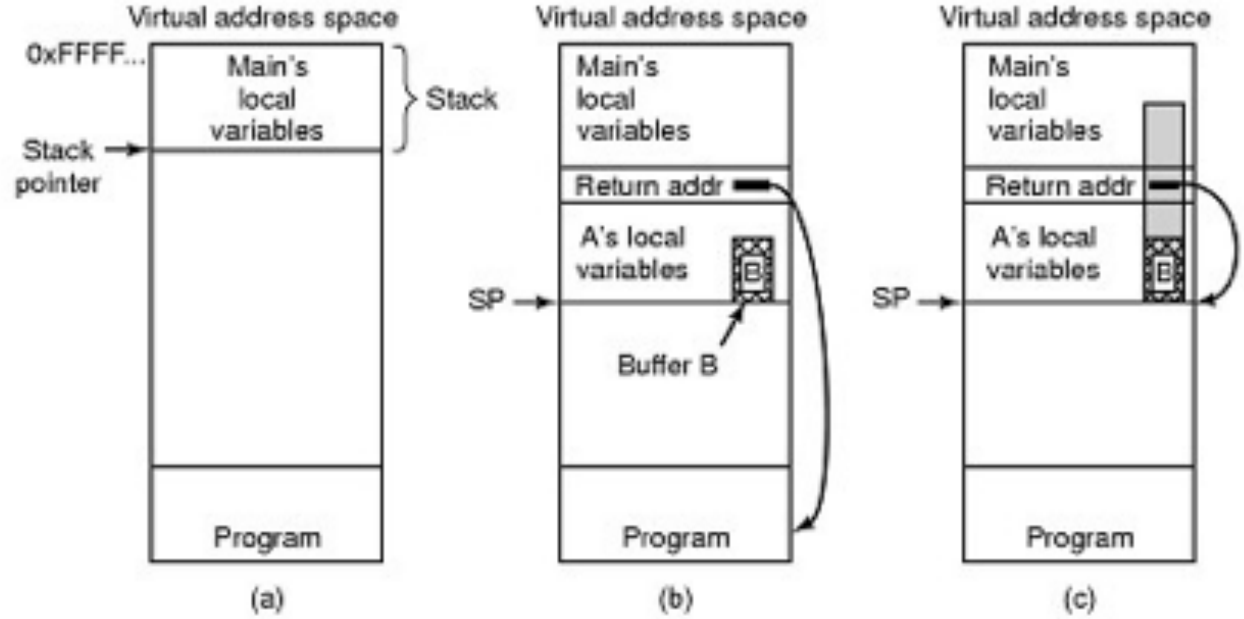

Attacker
The attacker sends ICMP ECHO requests with spoofed source addresses
Target Server
ECHO Request
ECHO Reply
ECHO Request
ECHO Reply
-Maximum limit of ICMP Echo Requests per Second-
ECHO Request
ECHO Request
Legitimate ICMP echo request from an address in the same security zone

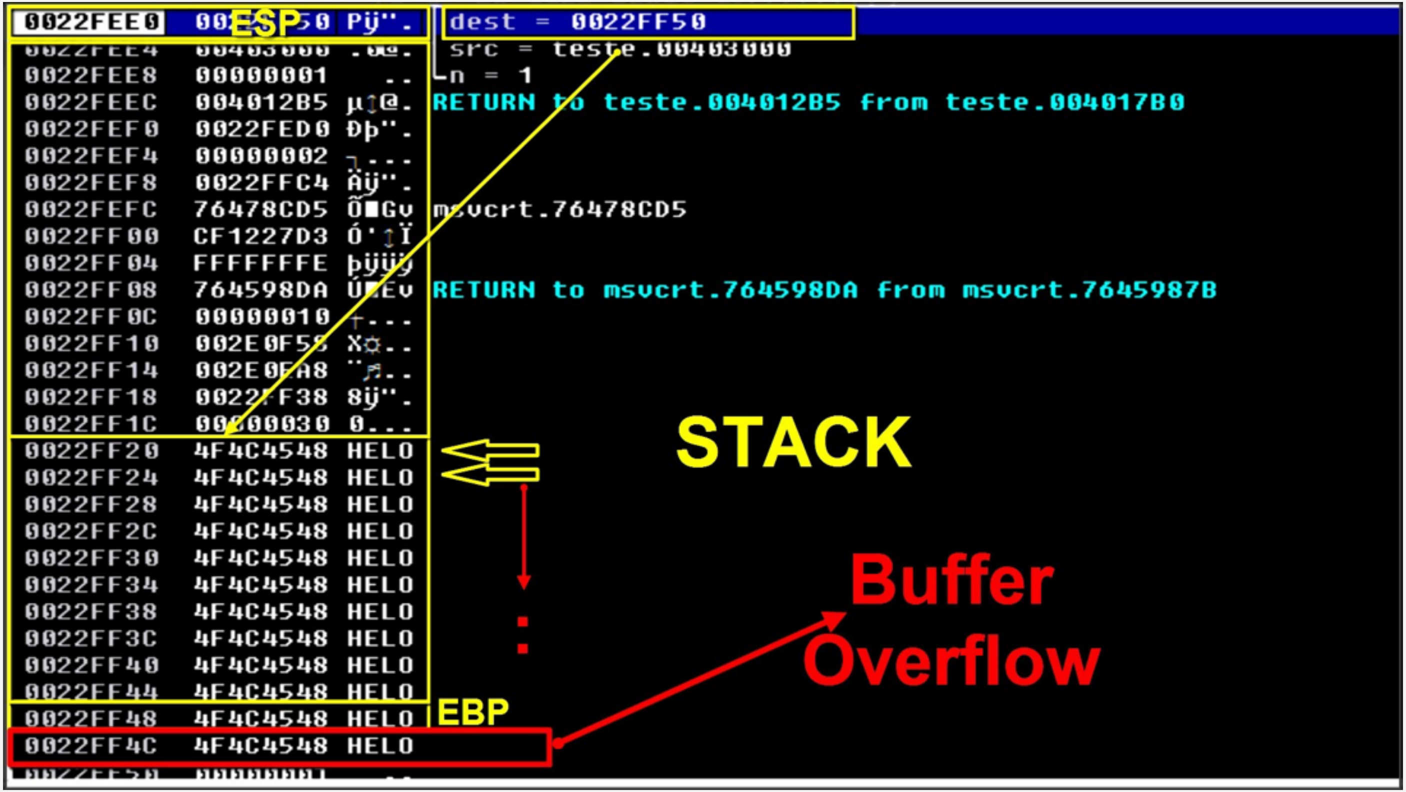

ATTACKER
Prime Target
1
1
1
3
Internet
2
2
2
Amplifiers

Buffer Overflow Attack

- Buffer overflow occurs any time the **program writes more information into the buffer than the space it has allocated in the memory**
- The **attacker can overwrite data** that **controls the program execution path** and **hijack the control** of the program to execute the attacker's code instead of the process code
- Sending email messages that have attachments with 256-character file names can cause buffer overflow

Buffer Overflow Attack …





```
0022FEE0  0022FF50  Pÿ".  dest = 0022FF50
0022FEE4  00403000  .0@.  src = teste.00403000
0022FEE8  00000001  ...   └n = 1
0022FEEC  004012B5  µ↕@. RETURN to teste.004012B5 from teste.004017B0
0022FEF0  0022FED0  Ðþ".
0022FEF4  00000002  ┐...
0022FEF8  0022FFC4  Äÿ".
0022FEFC  76478CD5  Õ■Gv msvcrt.76478CD5
0022FF00  CF1227D3  Ó'↕Ï
0022FF04  FFFFFFFE  þÿÿÿ
0022FF08  764598DA  Ú■Ev RETURN to msvcrt.764598DA from msvcrt.7645987B
0022FF0C  00000010  ┼...
0022FF10  002E0F58  X☼..
0022FF14  002E0EA8  ¨♬..
0022FF18  0022FF38  8ÿ".
0022FF1C  00000030  0...
0022FF20  4F4C4548  HELO
0022FF24  4F4C4548  HELO
0022FF28  4F4C4548  HELO
0022FF2C  4F4C4548  HELO
0022FF30  4F4C4548  HELO
0022FF34  4F4C4548  HELO
0022FF38  4F4C4548  HELO
0022FF3C  4F4C4548  HELO
0022FF40  4F4C4548  HELO
0022FF44  4F4C4548  HELO
0022FF48  4F4C4548  HELO
0022FF4C  4F4C4548  HELO
0022FF50  00000001  ...
```

Ping of Death Attack

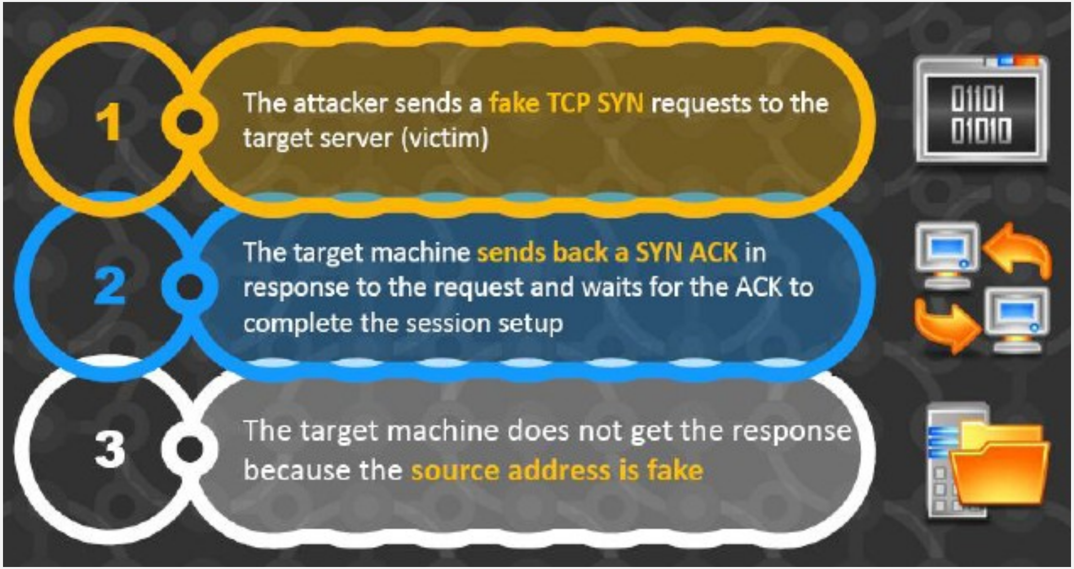
- The attacker deliberately **sends an IP packet larger than** the 65,536 bytes allowed by the IP protocol
- Fragmentation allows a single IP packet to be broken down into smaller segments
- The fragments can add up to more than the allowed 65,536 bytes. **The operating system, unable to handle oversized packets freezes, reboots, or simply crashes**

Teardrop Attack

- IP requires that a packet that is too large for the next router to handle be divided into fragments
- The **attacker's IP puts a confusing offset value in the second or later fragment**
- If the **receiving operating system** is not able to aggregate the packets accordingly, it can **crash the system**
- It is a **UDP attack**, which **uses overlapping offset** fields to bring down hosts.
- The Unnamed Attack
  - Variation of the Teardrop attack
  - Fragments are not overlapping but there are gaps incorporated

SYN Attack

- The attacker **sends bogus TCP SYN requests** to a victim server (Malicious flooding). The **host allocates resources** (memory sockets) to the connection.
- This attack exploits the three-way handshake



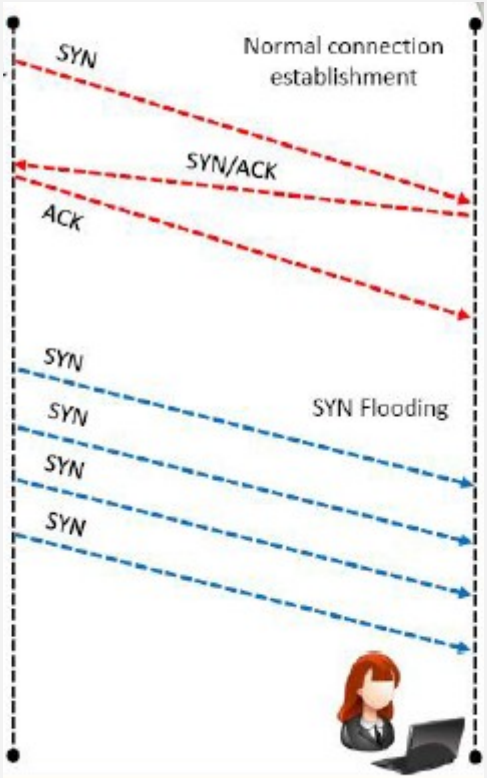
1 The attacker sends a fake TCP SYN requests to the target server (victim)

2 The target machine sends back a SYN ACK in response to the request and waits for the ACK to complete the session setup

3 The target machine does not get the response because the source address is fake

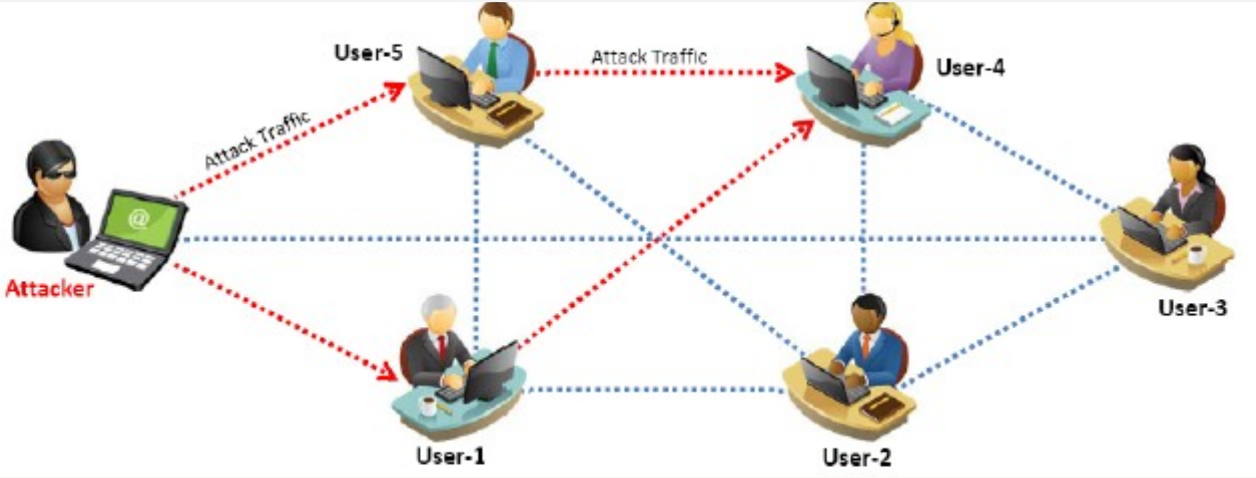
SYN Flooding

1. SYN Flooding takes advantages of a flaw in how most hosts implement the TCP 3-Way Handshake.
2. When Host B Receives the SYN request from A, it must keep track of the partially-opened connection in “listen queue "for at least 75s.
3. A malicious host can exploit the small size of the listen queue by sending multiple SYN request to the host, but Never Replying to SYN/ACK.
4. The victim's listen queue is quickly filled up.
5. This ability of removing a host from the network for at least 75s can be used as DOS Attack.

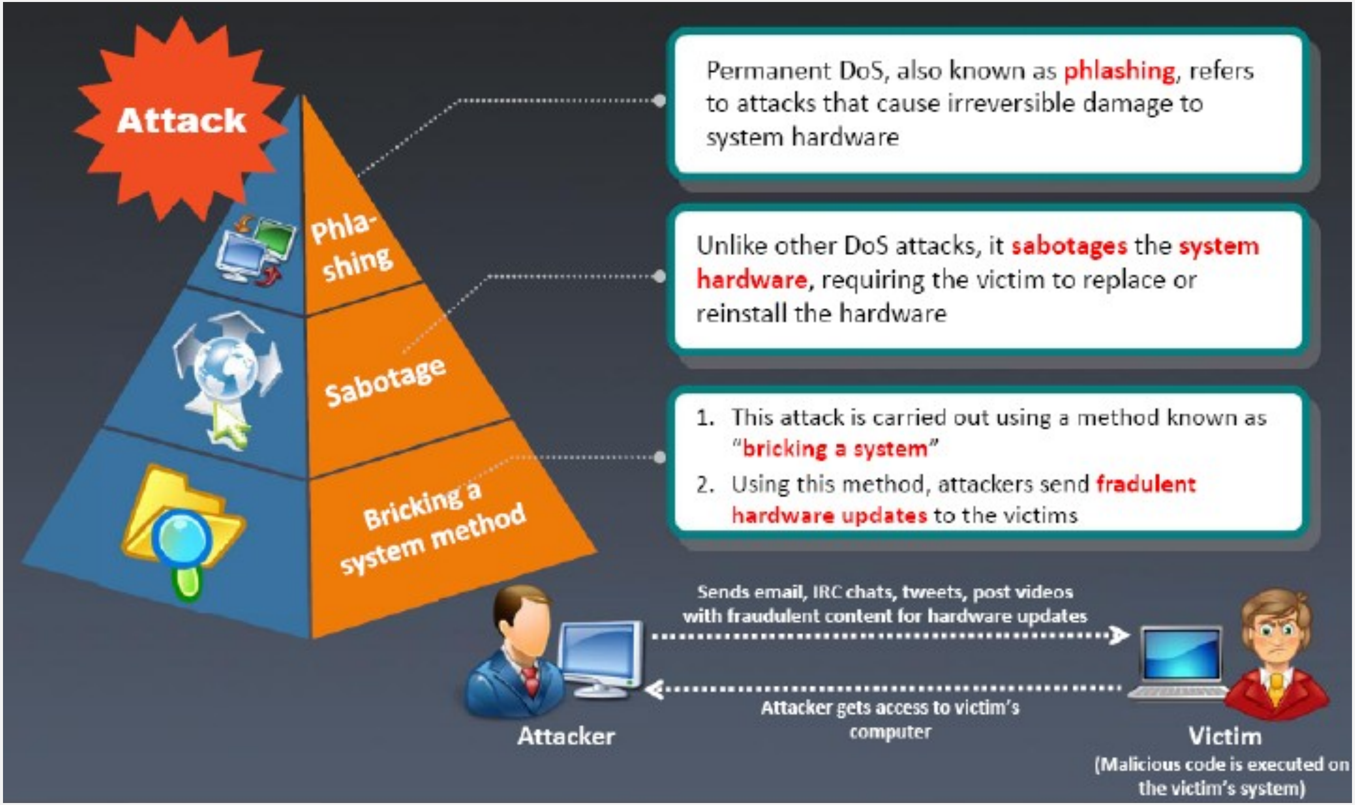


Peer-to-Peer Attack

- Using peer-to-peer attacks, attackers **instruct clients of peer-to-peer file sharing hubs** to disconnect from their network and to connect to the victim's fake website
- Attackers **exploit flaws** found in the network that uses DC++ (Direct Connect) protocol, which allows the exchange of files between instant messaging clients
- Using this method, attackers launch **massive denial-of-service attacks** and compromise websites



Permanent DoS Attack


Attack
Phla-shing
Sabotage
Bricking a system method
Sends email, IRC chats, tweets, post videos with fraudulent content for hardware updates
Attacker gets access to victim's computer
Attacker
Victim
(Malicious code is executed on the victim's system)

Permanent DoS, also known as **phlashing**, refers to attacks that cause irreversible damage to system hardware

Unlike other DoS attacks, it **sabotages** the **system hardware**, requiring the victim to replace or reinstall the hardware

1. This attack is carried out using a method known as "**bricking a system**"
2. Using this method, attackers send **fradulent hardware updates** to the victims

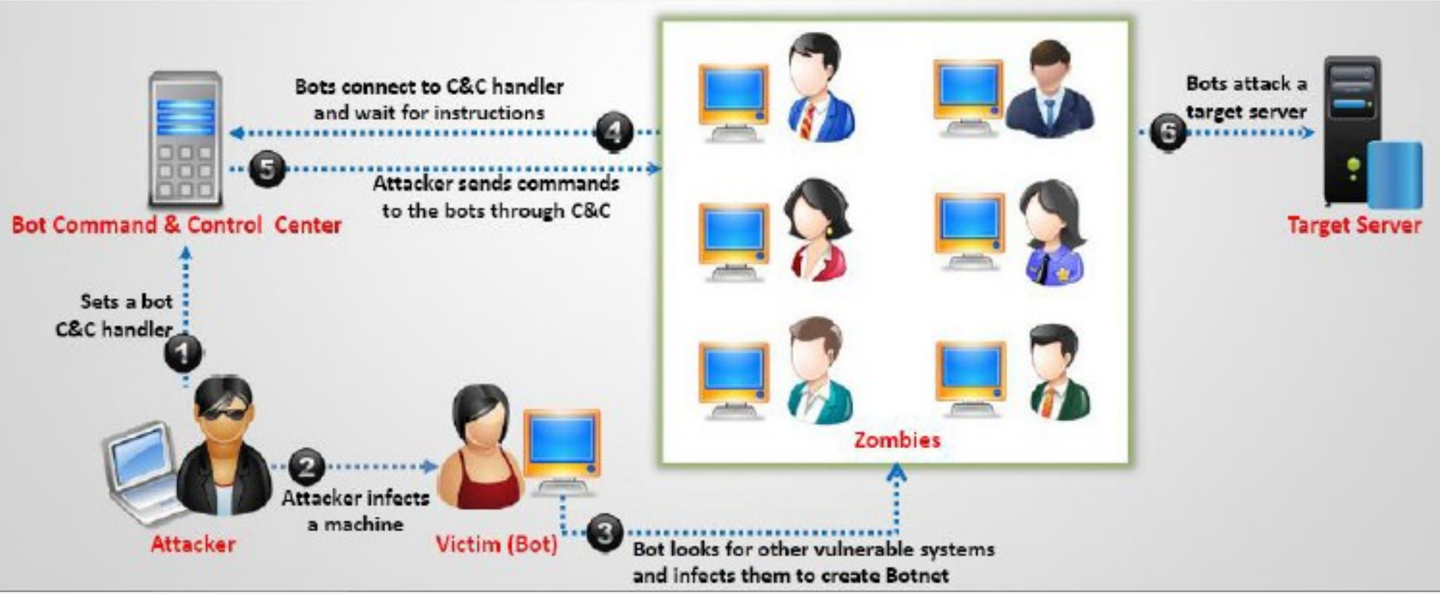
Botnet

03

Botnet

- Bots are software applications that **run automated task over the Internet** and perform simple repetitive tasks, such as web spidering and search engine indexing.
- A botnet is a **huge network of the compromised systems** and can be used by an intruder to create DoS attacks.
- رباتها برنامه‌های نرم افزاری هستند که بصورت خودکار از طریق اینترنت عمل می‌نمایند و کارهای تکراری ساده مانند عنکبوت وب و نمایه سازی موتور جستجو را انجام می دهند.
- یک بات نت شبکه بزرگی از سیستم های دستکاری شده است و می‌تواند توسط یک متجاوز برای ایجاد حملات DoS استفاده شود.

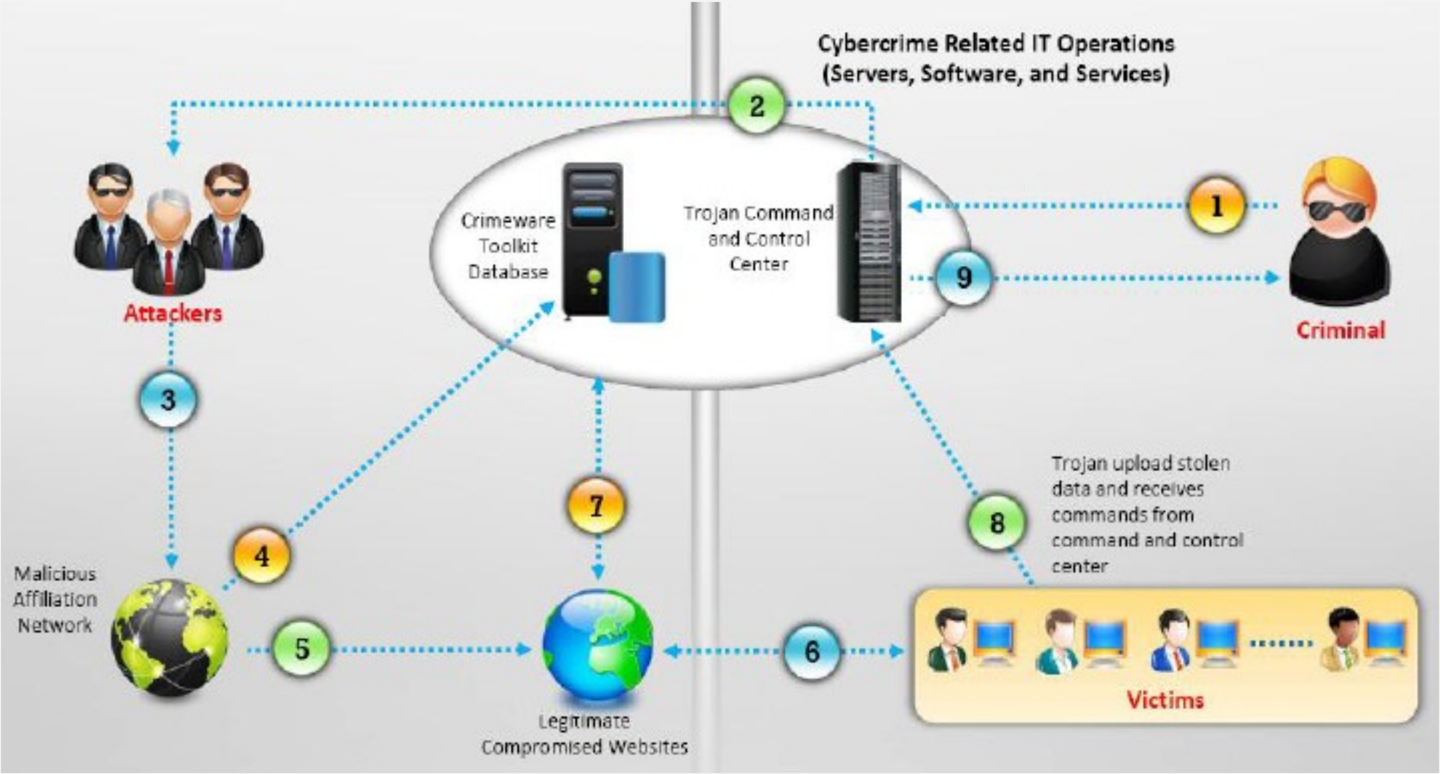
Botnet


Bots connect to C&C handler and wait for instructions
4
5
Attacker sends commands to the bots through C&C
Bot Command & Control Center
Bots attack a target server
6
Target Server
Sets a bot C&C handler
1
Zombies
2
Attacker infects a machine
Attacker
Victim (Bot)
3
Bot looks for other vulnerable systems and infects them to create Botnet

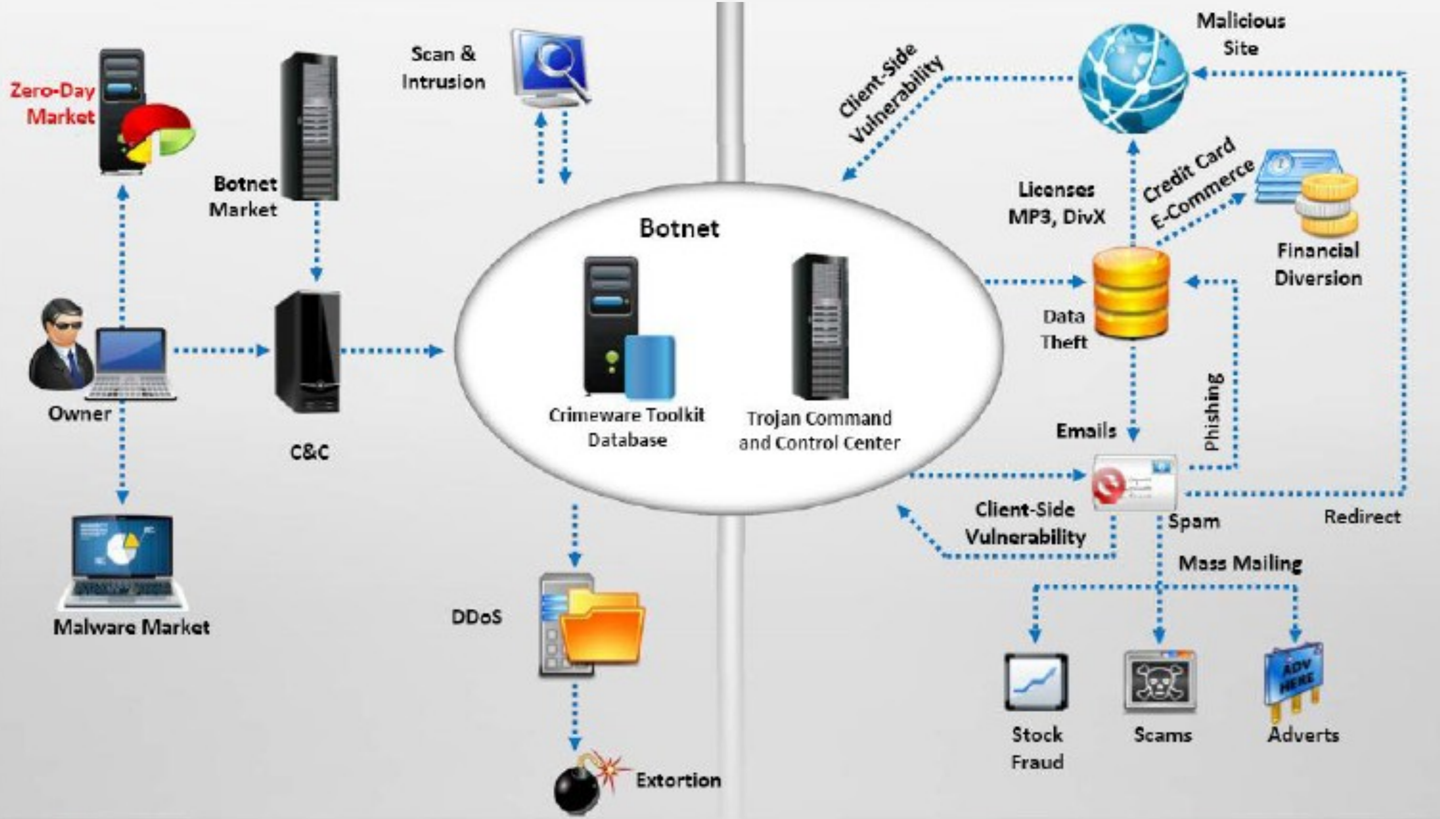
Uses of botnets

- **Distributed Denial-of-Service (DDoS) Attacks**
- **Spamming** هرزنامه
  - Opens a SOCKS v4/v5 proxy server for spamming
- **Sniffing Traffic** خرابکاری ترافیک
  - Bots can also use a packet sniffer to watch interesting clear-text data passing by a compromised machine
- **Keylogging**
  - With the help of a keylogger it is easy for an attacker to retrieve sensitive information such as online banking passwords
- **Spreading new malware** پخش نرم افزارهای مخرب جدید
  - Botnets are used to spread new bots
- **Installing Advertisement Add-ons** نصب تبلیغات
  - Automated advertisement “clicks”
- **Google AdSense abuse**
  - AdSense offers companies the possibility to display Google advertisements on their own website and earn money this way. Botnet is used to click on these advertisements
- **Attacking IRC Chat Networks** حمله به شبکه های چت
  - These are called “clone” attacks
- **Manipulating online polls** دستکاری نظرسنجی های آنلاین
  - Since every bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person
- **Mass identity theft** سرقت هویت جمعی
  - phishing mails

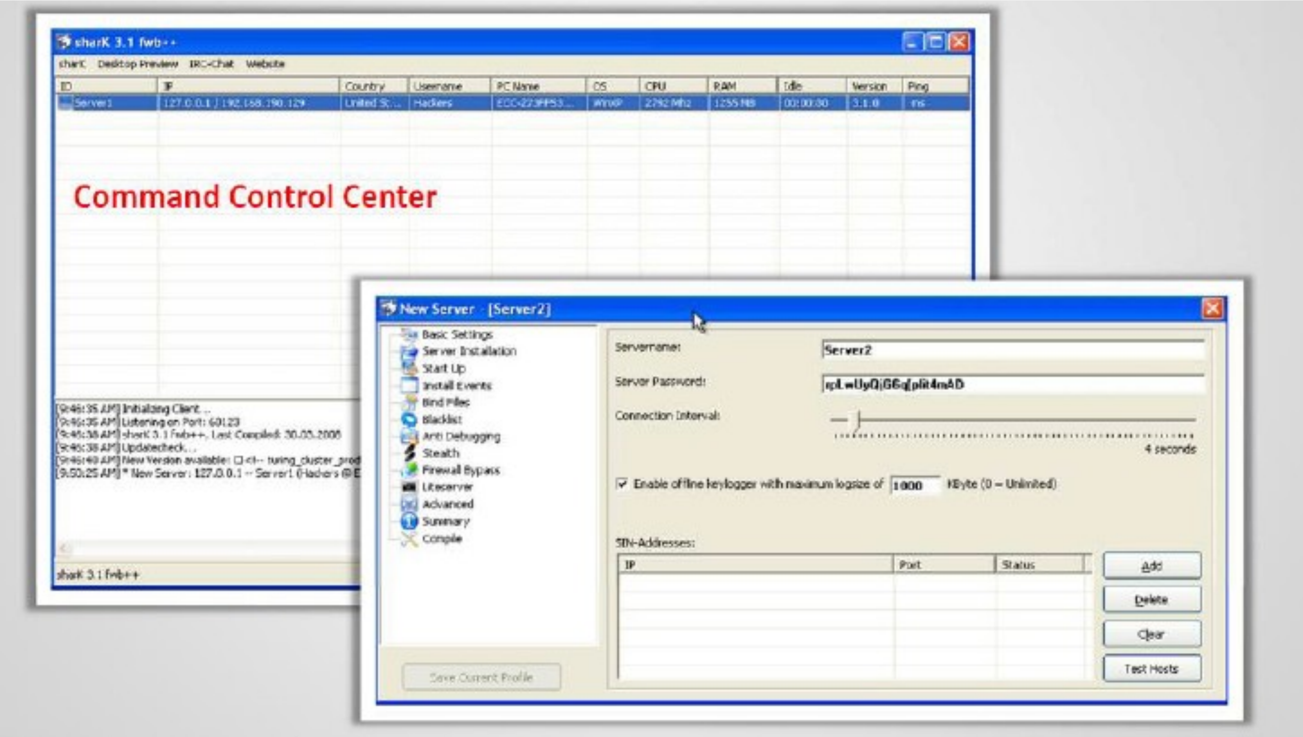
Botnet Propagation Techniques


Cybercrime Related IT Operations
(Servers, Software, and Services)
2
Crimeware Toolkit Database
Trojan Command and Control Center
1
9
Attackers
Criminal
3
Trojan upload stolen data and receives commands from command and control center
7
8
4
Malicious Affiliation Network
5
6
Victims
Legitimate Compromised Websites

Botnet Ecosystem



Botnet Trojan: Shark



ID	IP	Country	Username	PC Name	OS	CPU	RAM	Idle	Version	Ping
Server1	127.0.0.1 / 192.168.190.129	United St...	Hackers	ECC-223FF53...	WinXP	2792 Mhz	1255 MB	00:00:00	3.1.0	ms

Command Control Center

```
[9:46:35 AM] Initializing Client ...
[9:46:35 AM] Listening on Port: 60123
[9:46:38 AM] sharK 3.1 fwb++, Last Compiled: 30.05.2008
[9:46:38 AM] Updatecheck...
[9:46:40 AM] New Version available: □<!-- turing_cluster_prod
[9:50:25 AM] * New Server: 127.0.0.1 -- Server1 (Hackers @ E
```

Servername: Server2

Server Password: rpLwUyQjG6q[plit4mAD

Connection Interval: 4 seconds

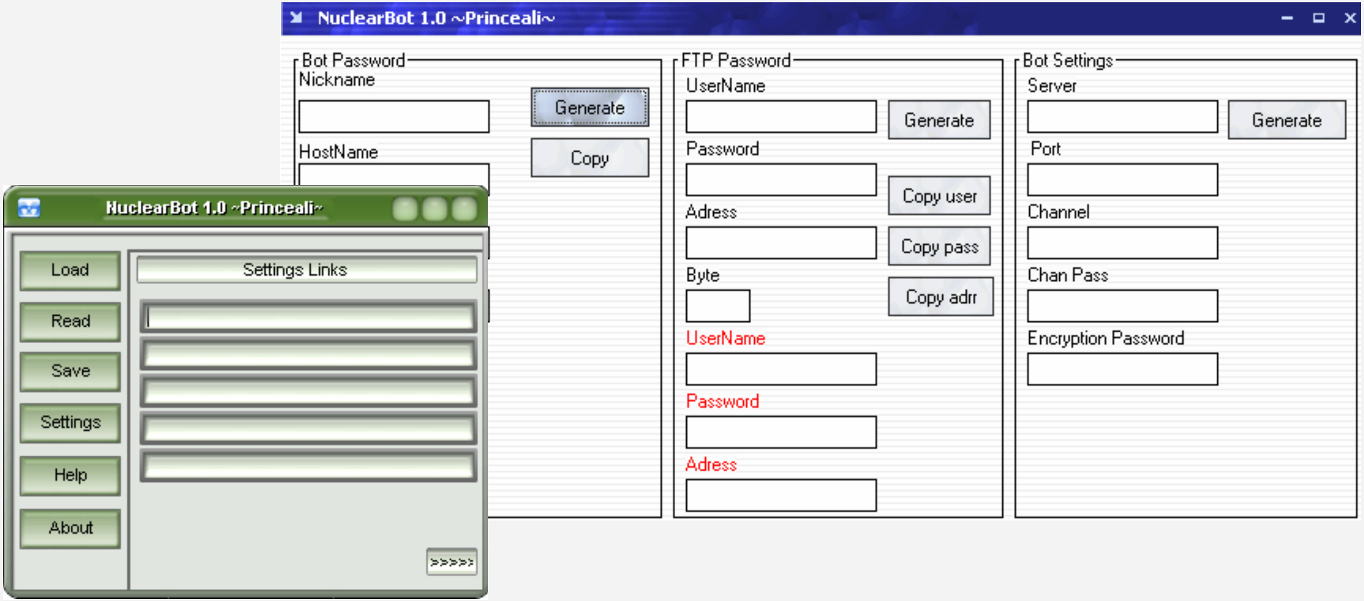
☑ Enable offline keylogger with maximum logsize of 1000 KByte (0 = Unlimited)

SIN-Addresses:

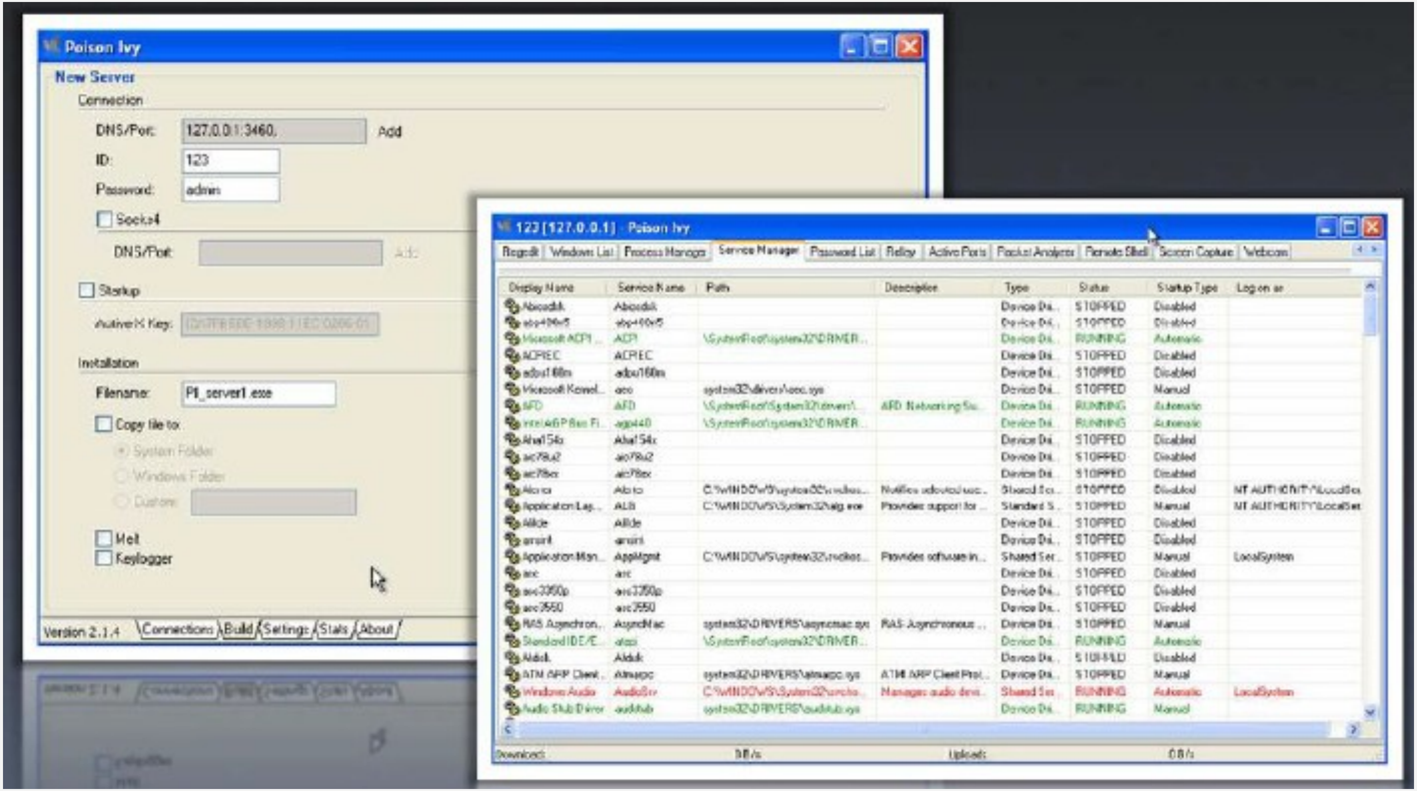
IP	Port	Status

Nuclear Bot

- Nuclear Bot is a **Multi Advanced IRC BOT** that can be used for Floods, Managing, Utilities, Spread, IRC Related, DDOS Attacks, …



Botnet Command Control Centre: Poison Ivy



New Server

Connection

DNS/Port: 127.0.0.1:3460, Add

ID: 123

Password: admin

□ Socks4

DNS/Port: Add

□ Startup

ActiveX Key: [illegible]

Installation

Filename: PI_server1.exe

□ Copy file to:

● System Folder

○ Windows Folder

○ Custom:

□ Melt

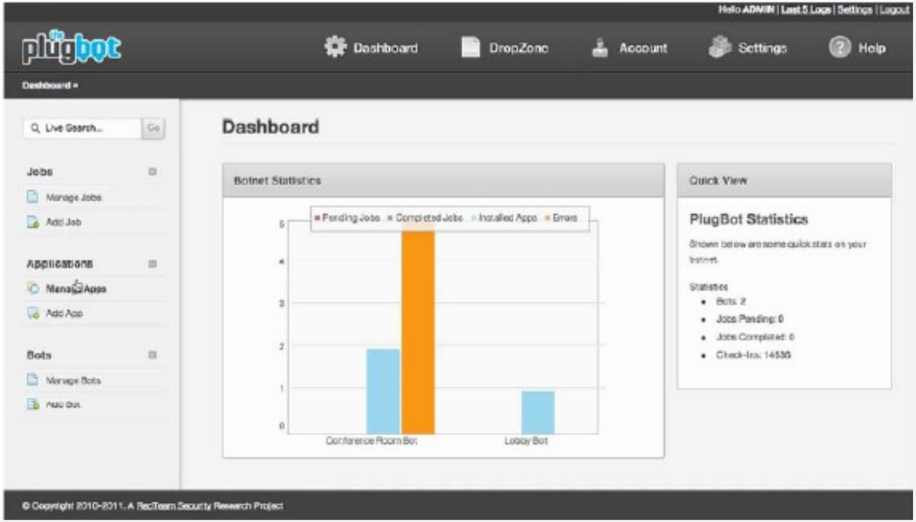
□ Keylogger

Display Name	Service Name	Path	Description	Type	Status	Startup Type	Log on as
Abiosdsk	Abiosdsk			Device Dri...	STOPPED	Disabled	
abp480n5	abp480n5			Device Dri...	STOPPED	Disabled	
Microsoft ACPI ...	ACPI	\SystemRoot\system32\DRIVER...		Device Dri...	RUNNING	Automatic	
ACPIEC	ACPIEC			Device Dri...	STOPPED	Disabled	
adpu160m	adpu160m			Device Dri...	STOPPED	Disabled	
Microsoft Kernel...	aec	system32\drivers\aec.sys		Device Dri...	STOPPED	Manual	
AFD	AFD	\SystemRoot\System32\drivers\...	AFD Networking Su...	Device Dri...	RUNNING	Automatic	
Intel AGP Bus Fi...	agp440	\SystemRoot\system32\DRIVER...		Device Dri...	RUNNING	Automatic	
Aha154x	Aha154x			Device Dri...	STOPPED	Disabled	
aic78u2	aic78u2			Device Dri...	STOPPED	Disabled	
aic78xx	aic78xx			Device Dri...	STOPPED	Disabled	
Alerter	Alerter	C:\WINDOWS\system32\svchos...	Notifies selected use...	Shared Se...	STOPPED	Disabled	NT AUTHORITY\LocalSe...
Application Lay...	ALG	C:\WINDOWS\System32\alg.exe	Provides support for ...	Standard S...	STOPPED	Manual	NT AUTHORITY\LocalSer
AliIde	AliIde			Device Dri...	STOPPED	Disabled	
amsint	amsint			Device Dri...	STOPPED	Disabled	
Application Man...	AppMgmt	C:\WINDOWS\system32\svchos...	Provides software in...	Shared Ser...	STOPPED	Manual	LocalSystem
asc	asc			Device Dri...	STOPPED	Disabled	
asc3350p	asc3350p			Device Dri...	STOPPED	Disabled	
asc3550	asc3550			Device Dri...	STOPPED	Disabled	
RAS Asynchron...	AsyncMac	system32\DRIVERS\asyncmac.sys	RAS Asynchronous ...	Device Dri...	STOPPED	Manual	
Standard IDE/E...	atapi	\SystemRoot\system32\DRIVER...		Device Dri...	RUNNING	Automatic	
Atdisk	Atdisk			Device Dri...	STOPPED	Disabled	
ATM ARP Client ...	Atmarpc	system32\DRIVERS\atmarpc.sys	ATM ARP Client Prot...	Device Dri...	STOPPED	Manual	
Windows Audio	AudioSrv	C:\WINDOWS\System32\svcho...	Manages audio devi...	Shared Se...	RUNNING	Automatic	LocalSystem
Audio Stub Driver	audstub	system32\DRIVERS\audstub.sys		Device Dri...	RUNNING	Manual	

Download: 0 B/s Upload: 0 B/s

Botnet Trojan: PlugBot

- PlugBot is a **hardware botnet** project
- It is a cover Penetration testing device (bot) designed for **covert use during physical penetration test.**



PlugBot Statistics

Shown below are some quick stats on your botnet.

Statistics

- Bots: 2
- Jobs Pending: 0
- Jobs Completed: 0
- Check-Ins: 14536

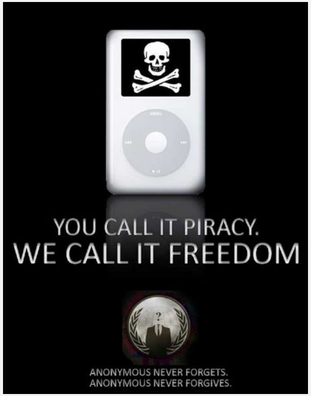
© Copyright 2010-2011. A RedTeam Security Research Project

DDoS Case Study

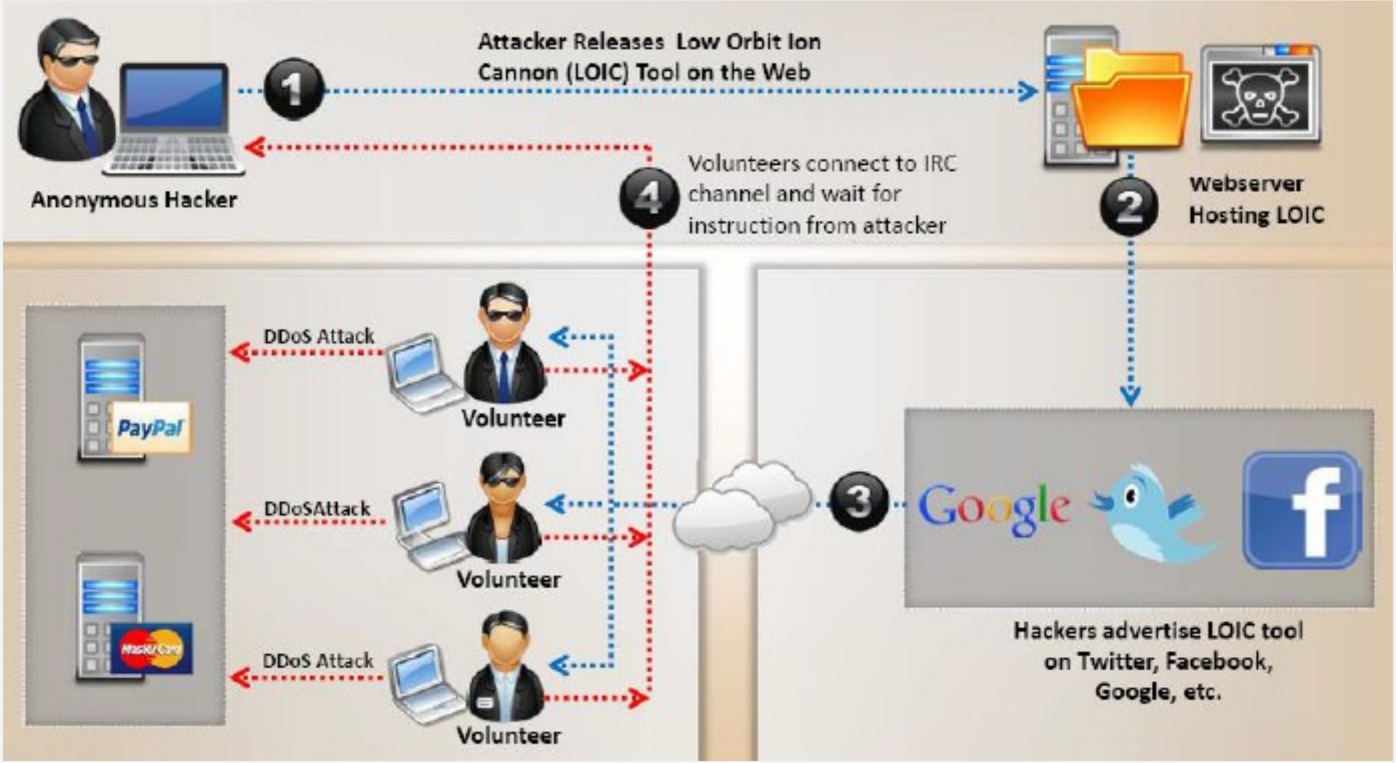
04

Anonymous’ Operation Payback

- **Operation Payback** was a coordinated, decentralized group of attacks on high-profile opponents of Internet piracy by Internet activists using the "Anonymous" moniker.
- The series of DDoS attacks organized by users of **4chan**’s /b/ (random) board that started on 2010 against major entertainment industry websites.



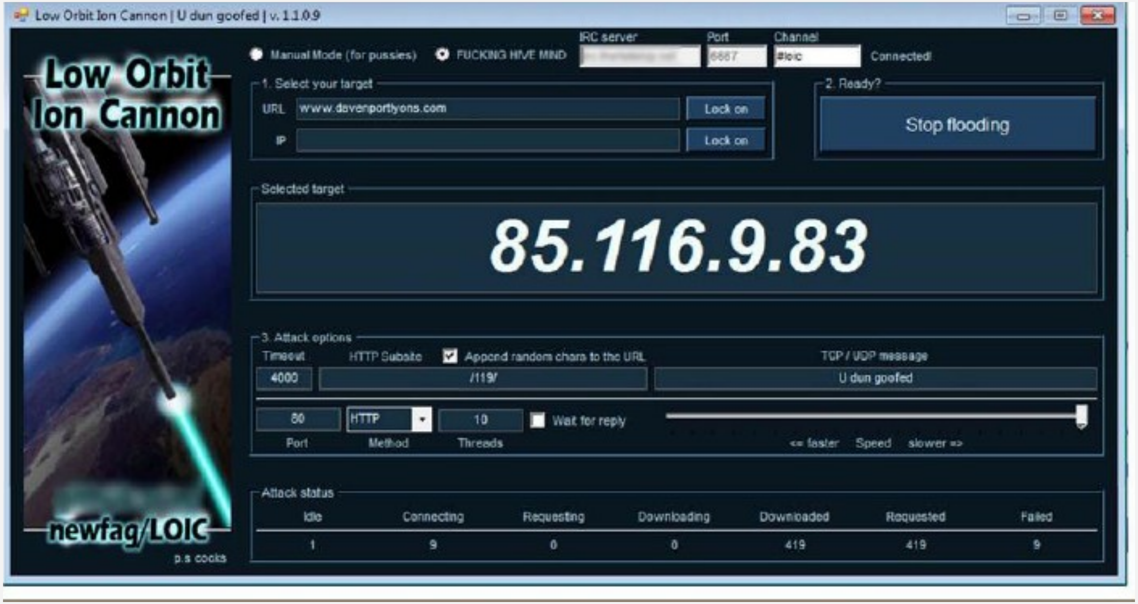
DDoS Attack



Attacker Releases Low Orbit Ion Cannon (LOIC) Tool on the Web
1
Anonymous Hacker
Volunteers connect to IRC channel and wait for instruction from attacker
4
2
Webserver Hosting LOIC
DDoS Attack
Volunteer
DDoSAttack
Volunteer
DDoS Attack
Volunteer
PayPal
MasterCard
3
Google
f
Hackers advertise LOIC tool on Twitter, Facebook, Google, etc.

DDoS Attack Tool: LOIC

- Used to bring down Paypal and Mastercard websites.



Low Orbit Ion Cannon | U dun goofed | v. 1.1.0.9

○ Manual Mode (for pussies) ● FUCKING HIVE MIND

IRC server: [redacted]

Port: 6667

Channel: #loic

Connected!

1. Select your target

URL: www.davenportlyons.com

IP:

Selected target: 85.116.9.83

3. Attack options

Timeout: 4000

HTTP Subsite: /119/

☑ Append random chars to the URL

TCP / UDP message: U dun goofed

Port: 80

Method: HTTP

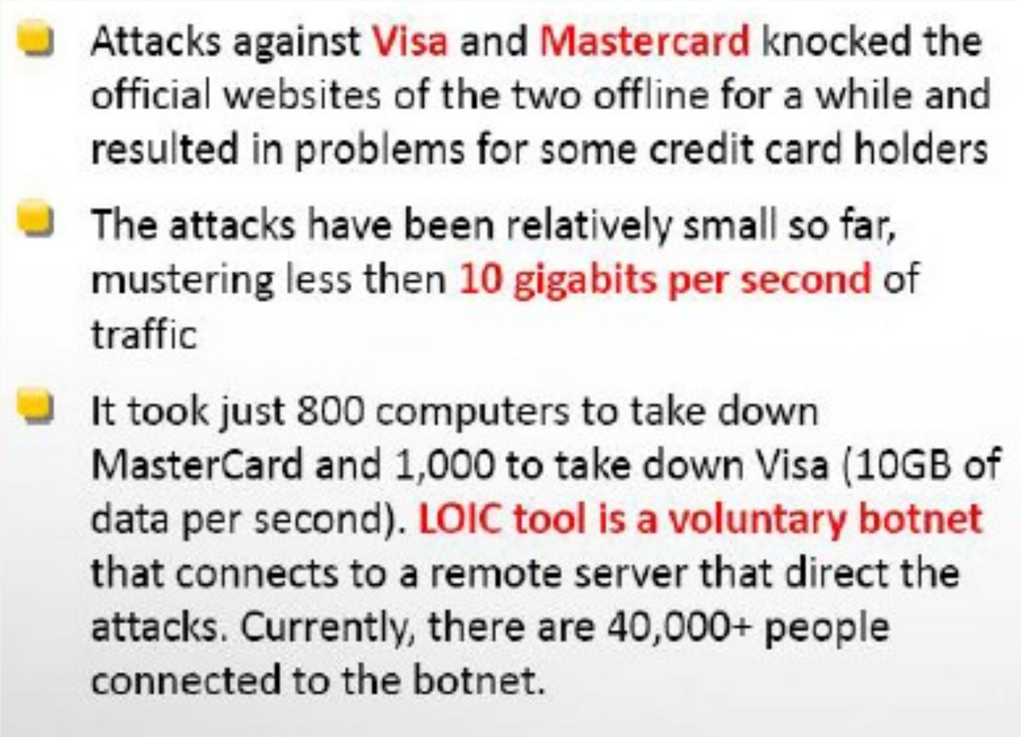
Threads: 10

□ Wait for reply

Attack status

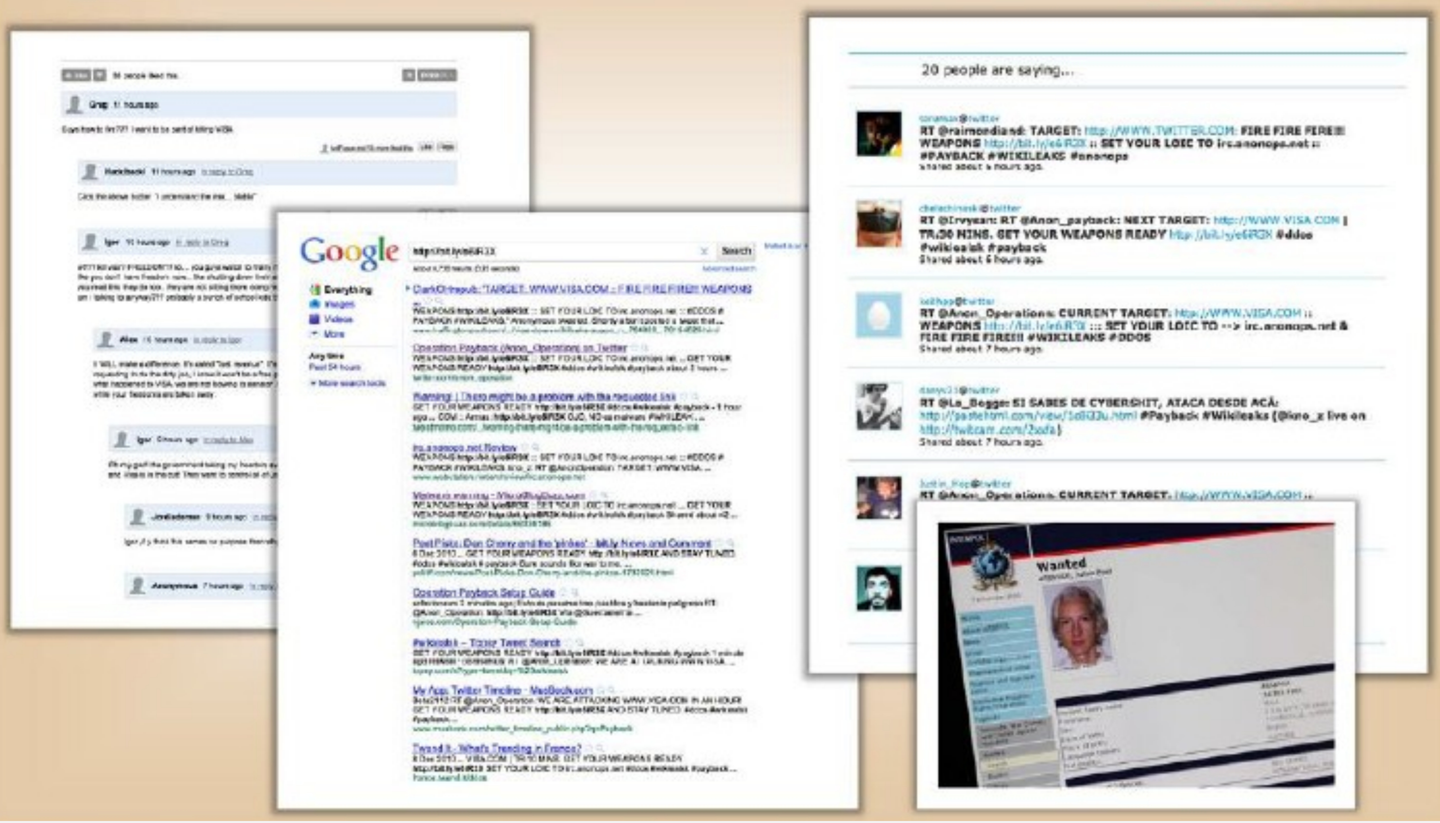
Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
1	9	0	0	419	419	9

DoS Attack Against Mastercard, Visa and Swiss Bank



- Attacks against Visa and Mastercard knocked the official websites of the two offline for a while and resulted in problems for some credit card holders
- The attacks have been relatively small so far, mustering less then 10 gigabits per second of traffic
- It took just 800 computers to take down MasterCard and 1,000 to take down Visa (10GB of data per second). LOIC tool is a voluntary botnet that connects to a remote server that direct the attacks. Currently, there are 40,000+ people connected to the botnet.

Hackers Advertise Links to Download



Greg 11 hours ago

Guys how to do this??? I want to be part of killing VISA

Hackback 11 hours ago in reply to Greg

Click the above button "I understand the risk... stable"

Google

Everything

Images

Videos

More

Any time

Past 24 hours

More search tools

DarkOhrepub: "TARGET: WWW.VISA.COM :: FIRE FIRE FIRE!!! WEAPONS ...

Operation Payback (Anon_Operations) on Twitter

Warning! | There might be a problem with the requested link

irc.anonops.net Review

PostPlate: Don Cherry and the 'pinkos' - billy News and Comment

Operation Payback Setup Guide

#wikileaks – Topsy Tweet Search

My App: Twitter Timeline - MacGeekworm

Tweet It - What's Trending in France?

20 people are saying...

RT @raimondiand: TARGET: http://WWW.TWITTER.COM: FIRE FIRE FIRE!!! WEAPONS http://bit.ly/e6iRGX :: SET YOUR LOIC TO irc.anonops.net :: #PAYBACK #WIKILEAKS #anonops
Shared about 6 hours ago.

RT @Irvyean: RT @Anon_payback: NEXT TARGET: http://WWW.VISA.COM | TR:30 MINS. SET YOUR WEAPONS READY http://bit.ly/e6iRGX #ddos #wikieaiek #payback
Shared about 6 hours ago.

RT @Anon_Operations: CURRENT TARGET: http://WWW.VISA.COM :: WEAPONS http://bit.ly/e6iRGX ::: SET YOUR LOIC TO --> irc.anonops.net & FIRE FIRE FIRE!!! #WIKILEAKS #DDOS
Shared about 7 hours ago.

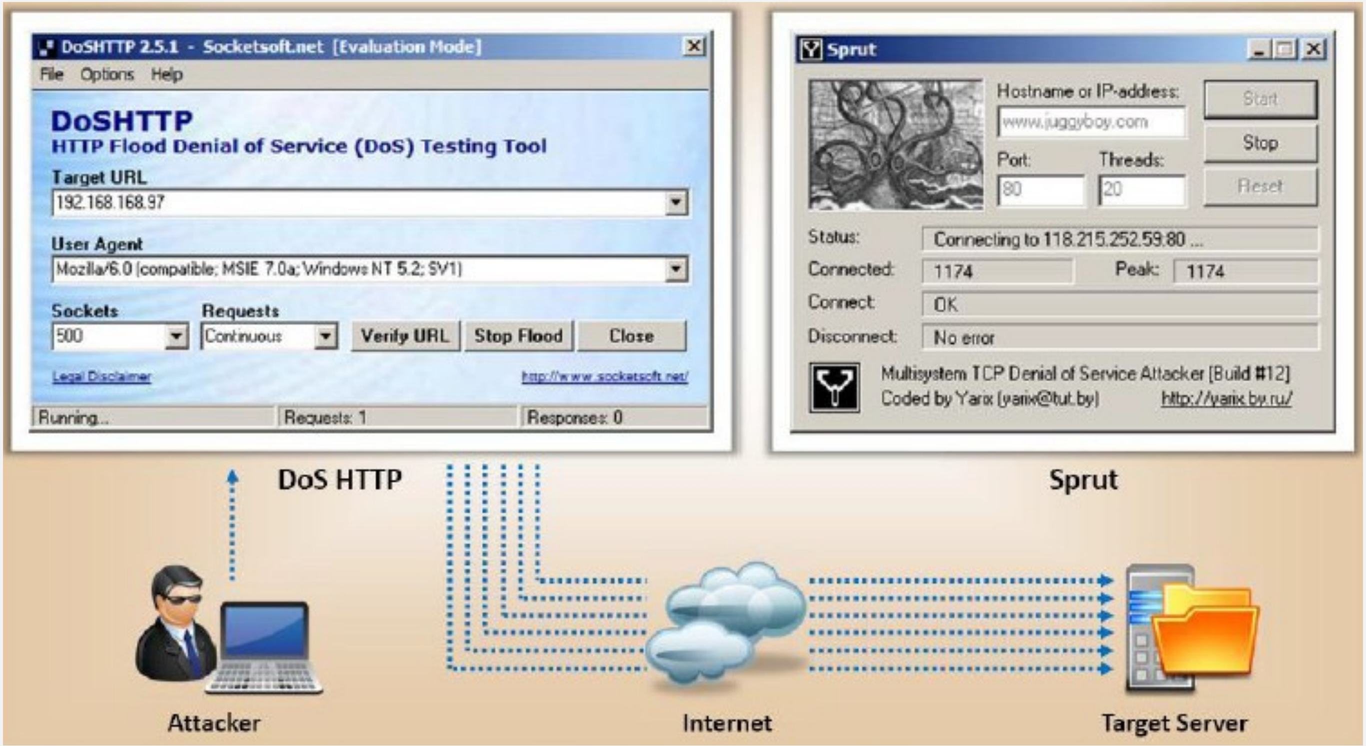
RT @La_Bogga: SI SABES DE CYBERSHIT, ATACA DESDE ACÁ: http://pastehtml.com/view/1o8l33u.html #Payback #Wikileaks (@lino_z live on http://twitcam.com/2soda)
Shared about 7 hours ago.

RT @Anon_Operations: CURRENT TARGET: http://WWW.VISA.COM ::

Dos/DDoS Tools

05

DoSHTTP



DoSHTTP 2.5.1 - Socketsoft.net [Evaluation Mode]

DoSHTTP

HTTP Flood Denial of Service (DoS) Testing Tool

Target URL: 192.168.168.97

User Agent: Mozilla/6.0 (compatible; MSIE 7.0a; Windows NT 5.2; SV1)

Sockets: 500

Requests: Continuous

Running... | Requests: 1 | Responses: 0

Sprut

Hostname or IP-address: www.juggyboy.com

Port: 80

Threads: 20

Status: Connecting to 118.215.252.59:80 ...

Connected: 1174

Peak: 1174

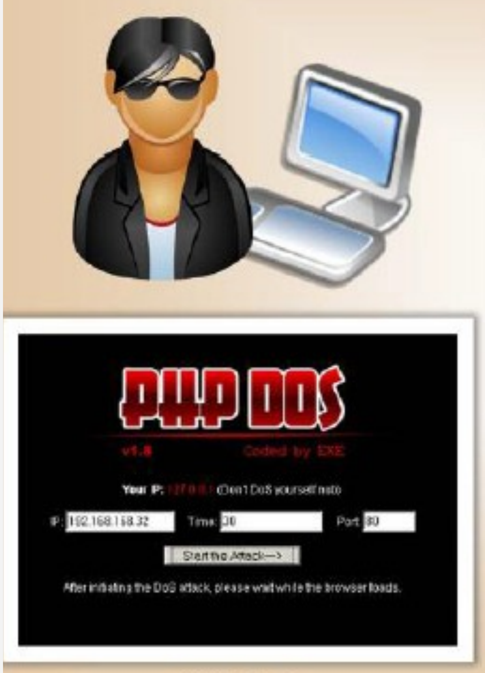
Connect: OK

Disconnect: No error

Multisystem TCP Denial of Service Attacker [Build #12]

Coded by Yarix (yarix@tut.by) http://yarix.by.ru/

PHP DoS

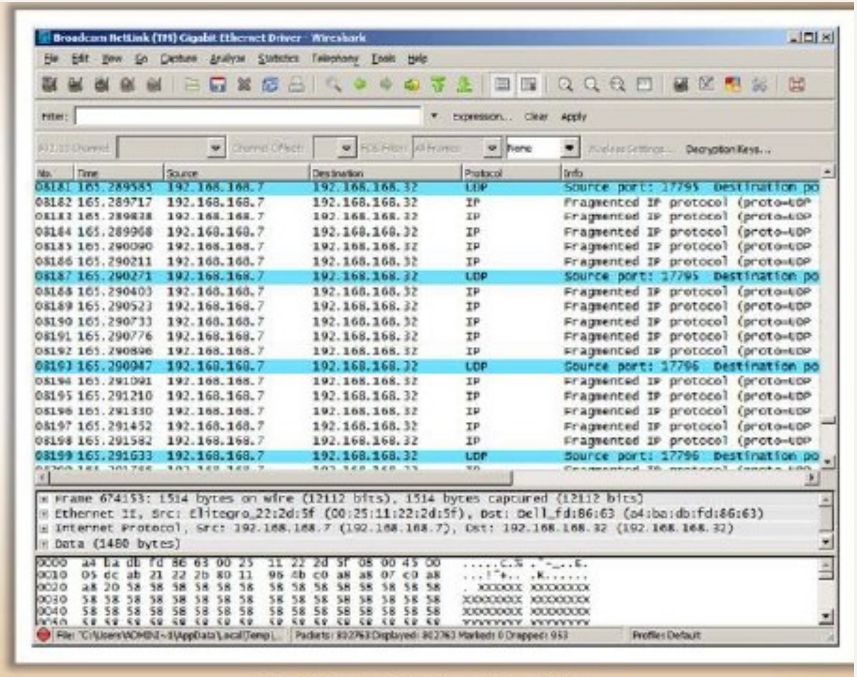


Your IP: 127.0.0.1 (Don't DoS yourself noob)

IP: 192.168.168.32 Time: 30 Port: 80

After initiating the DoS attack, please wait while the browser loads.

PHP DoS


Broadcom NetLink (TM) Gigabit Ethernet Driver - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
802.11 Channel:
Channel Offset:
FCS Filter:
All Frames
None
Wireless Settings...
Decryption Keys...

```
No.   Time       Source         Destination     Protocol  Info
08181 165.289585 192.168.168.7  192.168.168.32  UDP       Source port: 17795  Destination po
08182 165.289717 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08183 165.289838 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08184 165.289968 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08185 165.290090 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08186 165.290211 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08187 165.290271 192.168.168.7  192.168.168.32  UDP       Source port: 17795  Destination po
08188 165.290403 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08189 165.290523 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08190 165.290733 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08191 165.290776 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08192 165.290896 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08193 165.290947 192.168.168.7  192.168.168.32  UDP       Source port: 17796  Destination po
08194 165.291091 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08195 165.291210 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08196 165.291330 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08197 165.291452 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08198 165.291582 192.168.168.7  192.168.168.32  IP        Fragmented IP protocol (proto=UDP
08199 165.291633 192.168.168.7  192.168.168.32  UDP       Source port: 17796  Destination po
```

```
⊞ Frame 674153: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
⊞ Ethernet II, Src: Elitegro_22:2d:5f (00:25:11:22:2d:5f), Dst: Dell_fd:86:63 (a4:ba:db:fd:86:63)
⊞ Internet Protocol, Src: 192.168.168.7 (192.168.168.7), Dst: 192.168.168.32 (192.168.168.32)
⊞ Data (1480 bytes)
```

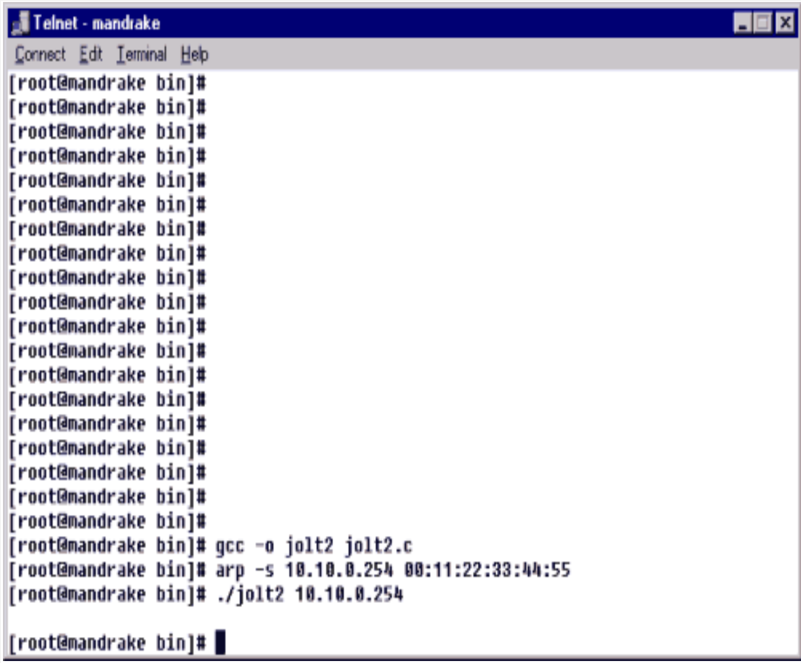
```
0000  a4 ba db fd 86 63 00 25  11 22 2d 5f 08 00 45 00   .....c.% ."-_..E.
0010  05 dc ab 21 22 2b 80 11  96 4b c0 a8 a8 07 c0 a8   ...!"+.. .K......
0020  a8 20 58 58 58 58 58 58  58 58 58 58 58 58 58 58   . XXXXXX XXXXXXXX
0030  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
0050  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58   XXXXXXXX XXXXXXXX
```

File: "C:\Users\ADMINI~1\AppData\Local\Temp\... Packets: 802763 Displayed: 802763 Marked: 0 Dropped: 953 Profile: Default

Traffic at Victim Machine

Jolt2

- Causes the target machines to consume 100% of the CPU time on processing the illegal packets
- Not Windows-specific. **Cisco routers and other gateways may be vulnerable**



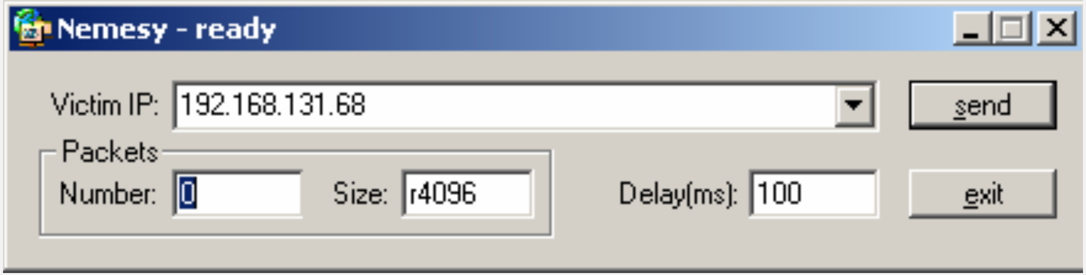
```
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]#
[root@mandrake bin]# gcc -o jolt2 jolt2.c
[root@mandrake bin]# arp -s 10.10.0.254 00:11:22:33:44:55
[root@mandrake bin]# ./jolt2 10.10.0.254

[root@mandrake bin]# 
```

Land and LaTierra

- IP spoofing in combination with the opening of a TCP connection
- Both IP addresses, source and destination, are modified to be the same—the address of the destination host
- This results in sending the packet back to itself, because the addresses are the same

Nemesys

- This application generate random packets (protocol, port, etc)
- It's presense means that your computer is infected with malicious software and is insecure



Nemesy - ready

Victim IP: 192.168.131.68

Packets

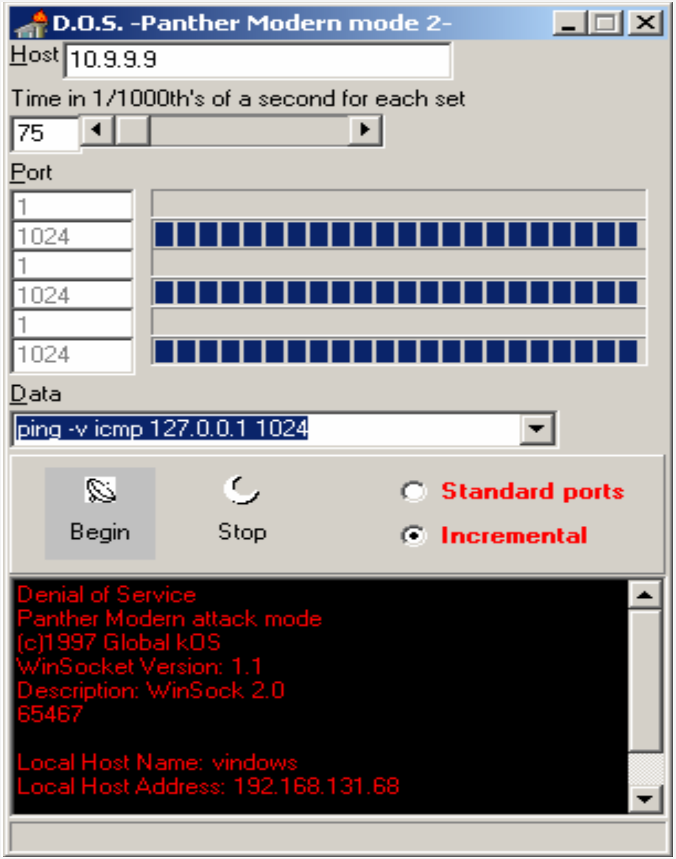
Number: 0

Size: r4096

Delay(ms): 100

Panther2

- Denial of service **UDP-based** attack designed for a 28.8-56k connection
- It comes under Flooder category
- Flooder:
  - A program that overloads a connection by any mechanism, such as fast pinging, causing a DoS attack



D.O.S. -Panther Modern mode 2-

Host 10.9.9.9

Time in 1/1000th's of a second for each set

75

Port

1
1024
1
1024
1
1024

Data

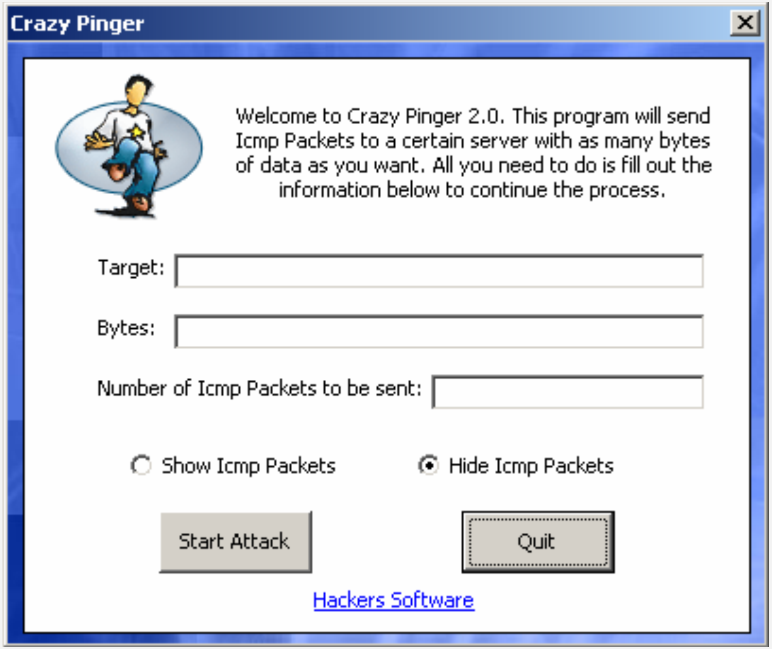
ping -v icmp 127.0.0.1 1024

○ Standard ports
● Incremental

```
Denial of Service
Panther Modern attack mode
(c)1997 Global kOS
WinSocket Version: 1.1
Description: WinSock 2.0
65467

Local Host Name: vindows
Local Host Address: 192.168.131.68
```

Crazy Pinger

- This tool could send large packets of ICMP to a remote target network



Welcome to Crazy Pinger 2.0. This program will send Icmp Packets to a certain server with as many bytes of data as you want. All you need to do is fill out the information below to continue the process.

Target:

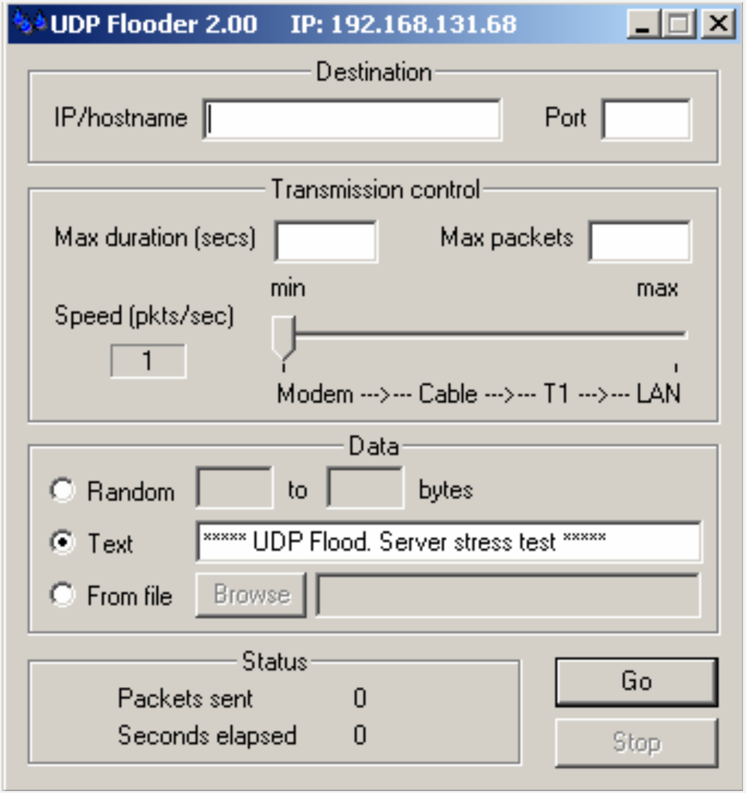
Bytes:

Number of Icmp Packets to be sent:

○ Show Icmp Packets ● Hide Icmp Packets

UDP Flood

- UDPFlood is UDP packet sender
- It sends out UDP packets to the specified IP and port at a controllable rate
- Packets can be made from a typed text string, a given number of random bytes or data from a file
- Useful for server testing



UDP Flooder 2.00 IP: 192.168.131.68

Destination

IP/hostname

Port

Transmission control

Max duration (secs)

Max packets

Speed (pkts/sec) 1

min max

Modem --->--- Cable --->--- T1 --->--- LAN

Data

○ Random to bytes

● Text ***** UDP Flood. Server stress test *****

○ From file Browse

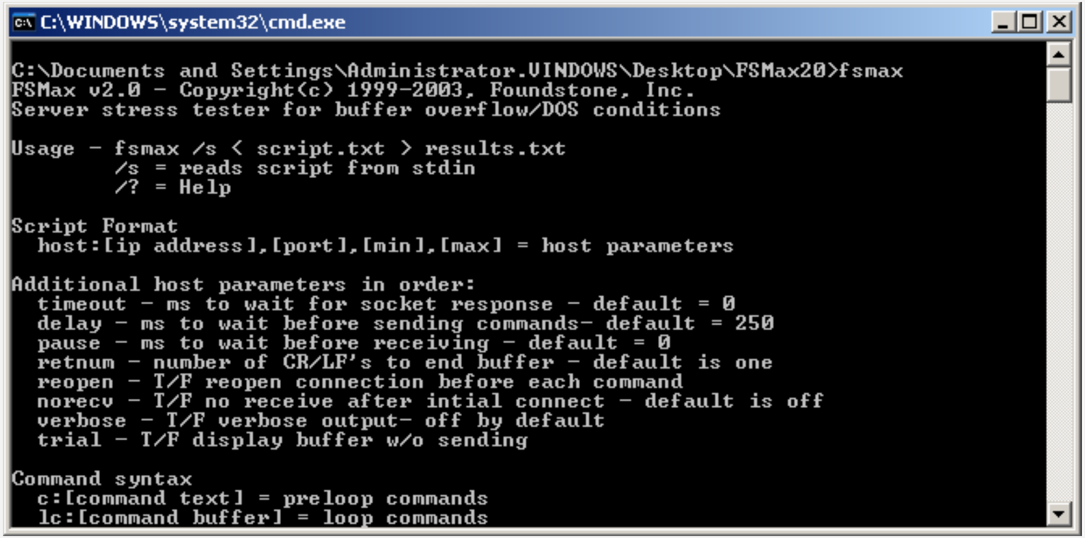
Status

Packets sent 0

Seconds elapsed 0

FSMax

- A scriptable, **server stress testing** tool
- It takes a **text file as input** and runs a server through a series of tests based on the input
- The purpose of this tool is **to find buffer overflows of DOS points in a server**

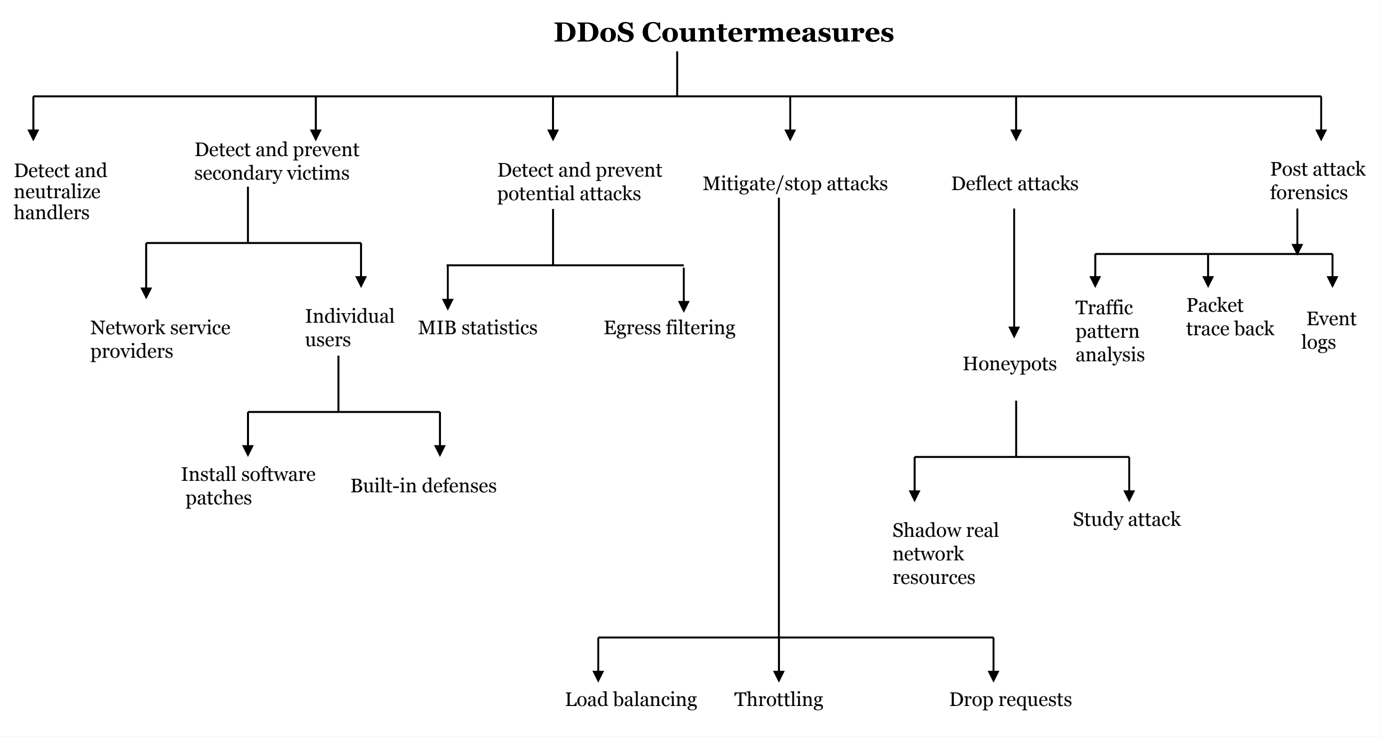


```
C:\Documents and Settings\Administrator.WINDOWS\Desktop\FSMax20>fsmax
FSMax v2.0 - Copyright(c) 1999-2003, Foundstone, Inc.
Server stress tester for buffer overflow/DOS conditions

Usage - fsmax /s < script.txt > results.txt
        /s  = reads script from stdin
        /?  = Help

Script Format
  host:[ip address],[port],[min],[max] = host parameters

Additional host parameters in order:
  timeout - ms to wait for socket response - default = 0
  delay - ms to wait before sending commands- default = 250
  pause - ms to wait before receiving - default = 0
  retnum - number of CR/LF's to end buffer - default is one
  reopen - T/F reopen connection before each command
  norecv - T/F no receive after intial connect - default is off
  verbose - T/F verbose output- off by default
  trial - T/F display buffer w/o sending

Command syntax
  c:[command text] = preloop commands
  lc:[command buffer] = loop commands
```

DDoS Counterme asures

06

DDoS Countermeasures



Taxonomy of DDoS Countermeasures

- Three essential components:
  - **Preventing secondary victims**, and **detecting** and **neutralizing handlers**
  - **Detecting or preventing the attack, mitigating or stopping the attack**, and **deflecting the attack**
  - The **post-attack component** which involves **network forensics**
    - جلوگیری از قربانی ثانویه بودن و کشف و خنثی کردن حمله
    - تشخیص یا جلوگیری از حمله، کاهش یا توقف حمله و خنثی کردن حمله
    - مؤلفه پس از حمله، که شامل پی‌جویی شبکه است

Preventing Secondary Victims

- A heightened awareness of security issues and prevention techniques from **all Internet users**
- **افزایش آگاهی از مسائل امنیتی و تکنیک های پیشگیری از سوی همه کاربران اینترنت**
- **Agent programs** should be scanned for in the systems
- اسکن برنامه های عامل در سیستم ها

Preventing Secondary Victims ...

- Installing anti-virus and anti-Trojan software, and keeping these up-to-date can prevent installation of the agent programs
- نصب نرم افزارهای ضد ویروس و ضد تروجان و به روز بودن این موارد
- Daunting for the average “web-surfer,” recent work has proposed built-in defensive mechanisms in the core hardware and software of computing systems
- پیشنهاد نصب مکانیسم‌های دفاعی داخلی در سخت افزار اصلی و نرم افزار سیستم‌های محاسباتی

Detect and Neutralize Handlers

- **Study of communication protocols** and traffic patterns between handlers and clients or handlers and agents in order to identify network nodes that **might be infected** with a handler

- بررسی پروتکل‌های ارتباطی و الگوهای ترافیکی بین کارفرمایان و مشتری‌ها یا فروشندگان و نمایندگان به منظور شناسایی گره های شبکه ای که ممکن است به یک کنترل کننده آلوده شود

- There are usually **few DDoS handlers deployed as compared to number of agents**. So neutralizing a few handlers can possibly render multiple agents useless, thus thwarting DDoS attacks.

- معمولا تعداد راه‌اندازها کمتر از عامل‌ها می‌باشد. در نتیجه خنثی کردن راه‌اندازها باعث از بین رفتن تعداد بیشتر عامل‌ها می‌شود.

Detect Potential Attacks

- **Egress filtering**
  - Scanning the packet headers of IP packets leaving a network
  - اسکن هدر بسته‌های IP که از شبکه خارج می شوند
- There is a good probability that the spoofed source address of DDoS attack packets **will not represent a valid source address** of the specific sub-network
- Placing a **firewall** or **packet sniffer** in the sub-network that **filters out any traffic** without an originating IP address.
- قرار دادن فایروال یا گیرنده بسته در شبکه فرعی که هرگونه ترافیکی را بدون داشتن آدرس IPمنشاء فیلتر می کند

Mitigate or Stop the Effects of DDoS Attacks

1. Load Balancing تعادل بار

- Providers can **increase bandwidth** on critical connections to prevent them from going down in the event of an attack
  - افزایش پهنای باند
- **Replicating servers** can help provide additional failsafe protection
  - داشتن کپی از سرور
- **Balancing the load to each server** in a multiple-server architecture can **improve** both **normal performances** as well as **mitigate the effect** of a DDoS attack
  - تعادل بار با هر سرور

Mitigate or Stop the Effects of DDoS Attacks …

2. Throttling جلوگیری/ کنترل کردن

- ○ This method sets up routers that access a server with logic to adjust (throttle) incoming traffic to levels that will be safe for the server to process

- ○ این روش روترهايي را تنظیم می کند که ه یک سرور دسترسی داشته باشند تا بتوانند ترافیک ورودی را به سطح‌هايي تنظیم کنند که پردازش سرور بی خطر باشد.

Deflect Attacks

- **Honeypots**
  - Systems that are **set up** with **limited security** act as an enticement for an attacker
  - Serve as a means for **gaining information** about **attackers by storing a record of their activities** and **learning** what types of attacks and software tools the attackers used

Post-attack Forensics

- **Traffic pattern analysis تحلیل الگوی ترافیک**
  - Data can be analyzed—post-attack—to look for specific characteristics within the attacking traffic
  - داده ها را می توان (پس از حمله) مورد تجزیه و تحلیل قرار داد تا به دنبال ویژگی های خاص در ترافیک مهاجمان باشید
- This characteristic data can be used for **updating load balancing** and **throttling** countermeasures
- DDoS attack traffic patterns can help network **administrators develop new filtering techniques** for preventing it from entering or leaving their networks

Packet Traceback

- This allows back tracing the attacker’s traffic and **possibly identifying the attacker**
- Additionally, when the attacker sends vastly different types of attacking traffic, this method assists in providing the victim system with information that might help develop **filters to block the attack**
- **Event Logs**
  - It **keeps logs** of the DDoS attack information in order to **do a forensic analysis**, and to **assist law enforcement** in the event the attacker does severe financial damage

Thanks for your Attention.