

Three Generations of DoS Attacks

(with Audience Participation, as
Victims)

Defcon, 2011

Bio

 User Profile ✕



Sam Bowne
@sambowne

I teach Ethical Hacking,
networking, and security at City
College San Francisco

 San Francisco

<http://samsclass.info>

Summary

- The DoS Circus
- Layer 4 DDoS: Thousands of attackers bring down one site
- Layer 7 DoS: One attacker brings down one site
- Link-Local DoS: IPv6 RA Attack: One attacker brings down a whole network

The DoS Circus

Characters

Wikileaks



- Published <1000 US Gov't diplomatic cables from a leak of 250,000
- Distributed an encrypted "Insurance" file by BitTorrent
 - Widely assumed to contain the complete, uncensored leaked data
 - Encrypted with AES-256--no one is ever getting in there without the key
 - Key to be released if Assange is jailed or killed, but he is in UK now resisting extradition to Sweden and the key has not been released

Anonymous



Operation Payback



- 4chan's Anonymous group
 - Attacked Scientology websites in 2008
 - Attacked the RIAA and other copyright defenders
 - Using the Low Orbit Ion Cannon with HiveMind (DDoS)
 - "Opt-in Botnet"

HB Gary Federal

- Aaron Barr
 - Developed a questionable way to track people down online
 - By correlating Twitter, Facebook, and other postings
 - Announced in Financial Times that he had located the “leaders” of Anonymous and would reveal them in a few days



Aaron Barr

Anonymous speaks: the inside story of the HBGary hack

By Peter Bright | Last updated 20 days ago



It has been an embarrassing week for security firm HBGary and its HBGary Federal offshoot. HBGary Federal CEO Aaron Barr thought he had **unmasked the hacker hordes of Anonymous** and was preparing to name and shame those responsible for co-ordinating the group's actions, including the denial-of-service attacks that hit MasterCard, Visa, and other perceived enemies of WikiLeaks late last year.

Social Engineering & SQLi



```
From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up
firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to
88Scr3am3r88 ?
thanks
```

```
From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed
```

```
From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
no i dont have the public ip with me at the moment because im ready
for a small meeting and im in a rush.
if anything just reset my password to changemel23 and give me public
ip and ill ssh in and reset my pw.
```

- <http://tinyurl.com/4gesrcj>

Leaked HB Gary Emails



- For Bank of America
 - Discredit Wikileaks
 - Intimidate Journalist Glenn Greenwald
- For the Chamber of Commerce
 - Discredit the watchdog group US Chamber Watch
 - Using fake social media accounts
- For the US Air Force
- Spread propaganda with fake accounts
- <http://tinyurl.com/4anofw8>

Drupal Exploit

Anonymous Takes Down U.S. Chamber Of Commerce And Supporter Websites

POSTED BY [ARMTHEHOMELESS](#) · 05/27/2011 · 5 COMMENTS

FILED UNDER [ANONYMOUS](#), [CHAMBER OF COMMERCE](#), [HBGARY](#)



Last Monday, the online activist group [Anonymous](#) launched a DDOS attack on the [U.S. Chamber of Commerce](#) website in retaliation against the [PROTECT IP Bill](#), which will give the U.S. federal government the sweeping power of forcing ISPs and search engines to block websites they believe to be infringing on copyright and intellectual property laws. Many are saying, compared to their previous attacks on Mastercard, Visa, and HBGary Federal, that the campaign on Monday was a failure. However, Anonymous is back and doing some damage.

Late Thursday evening, the collective identified and used exploits on the site to take down the main page of the U.S. CoC and their web-based mail service. They used a Drupal exploit to gain access to the site's content manager.

The U.S. Chamber of Commerce wasn't the only website targeted. [Several Senator and organization websites](#) were also taken offline from 6PM – 10PM EST via DOS. Senators targeted include [Chuck Grassley](#), [Lindsey Graham](#), and organizations such as the [National Association of Theater Owners](#); all of which had shown their support for the Protect IP Bill.

Th3j35t3r



- "Hacktivist for Good"
- Claims to be ex-military
- Originally performed DoS attacks on Jihadist sites
 - Bringing them down for brief periods, such as 30 minutes
 - Announces his attacks on Twitter, discusses them on a blog and live on irc.2600.net

Jester's Tweets from Dec 2010



th3j35t3r Jester

www.almedad.net - TANGO DOWN. Temporarily. For the online radicalization of young muslims in US and Europe.

12 Dec



th3j35t3r Jester

www.ansar1.info - TANGO DOWN. Temporarily. For online incitement to cause young muslims to carry out acts of violent jihad.

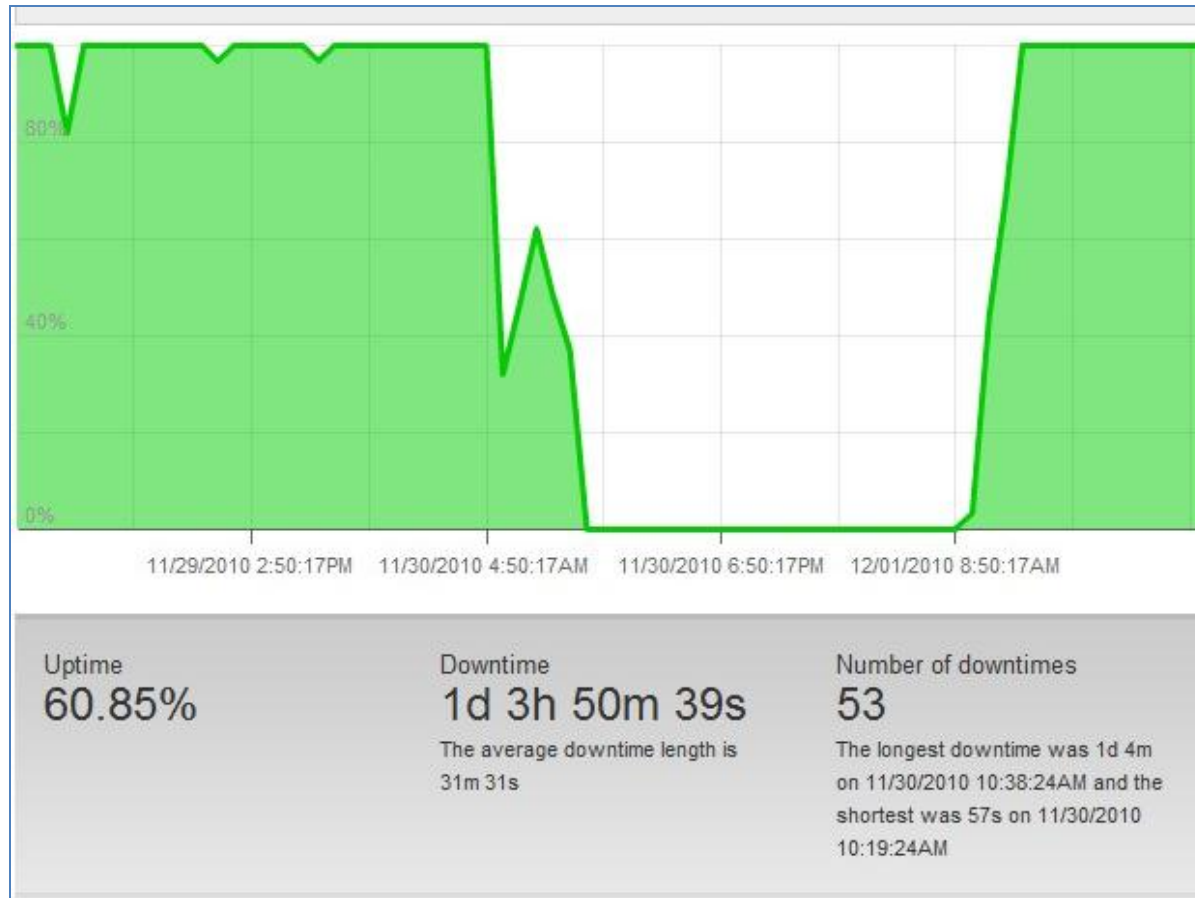
12 Dec

Th3j35t3r v. Wikileaks



- He brought down Wikileaks single-handed for more than a day
 - I was chatting with him in IRC while he did it, and he proved it was him by briefly pausing the attack

Wikileaks Outage



- One attacker, no botnet

Th3j35t3r




- After his Wikileaks attack
 - He battled Anonymous
 - He claims to have trojaned a tool the Anons downloaded
 - He claims to pwn Anon insiders now

Jester's Tweets

stDeck

User Profile ✕



Harley Quinn
@th3j35t3r


Hactivist for good. Obstructing the lines of communication for terrorists, sympathizers, fixers, facilitators, and other general bad guys... living the dream?

✓ Friend

📍 Behind you.


<http://th3j35t3r.wordpress.com>
[Twitter page](#)

9229 Followers 99 Following **566** Tweets 330 Listed




"There's unequal amount of good & bad in most things, trick is to figure out the ratio, act accordingly" <http://bit.ly/fLcDeC> - DAY 15 #wbc

● th3j35t3r, [+] Tue 08 Mar 14:04 via web



www.majahden.com - TANGO DOWN. Temporarily. For facilitating jihadi recruitment of young muslims & spreading propaganda.

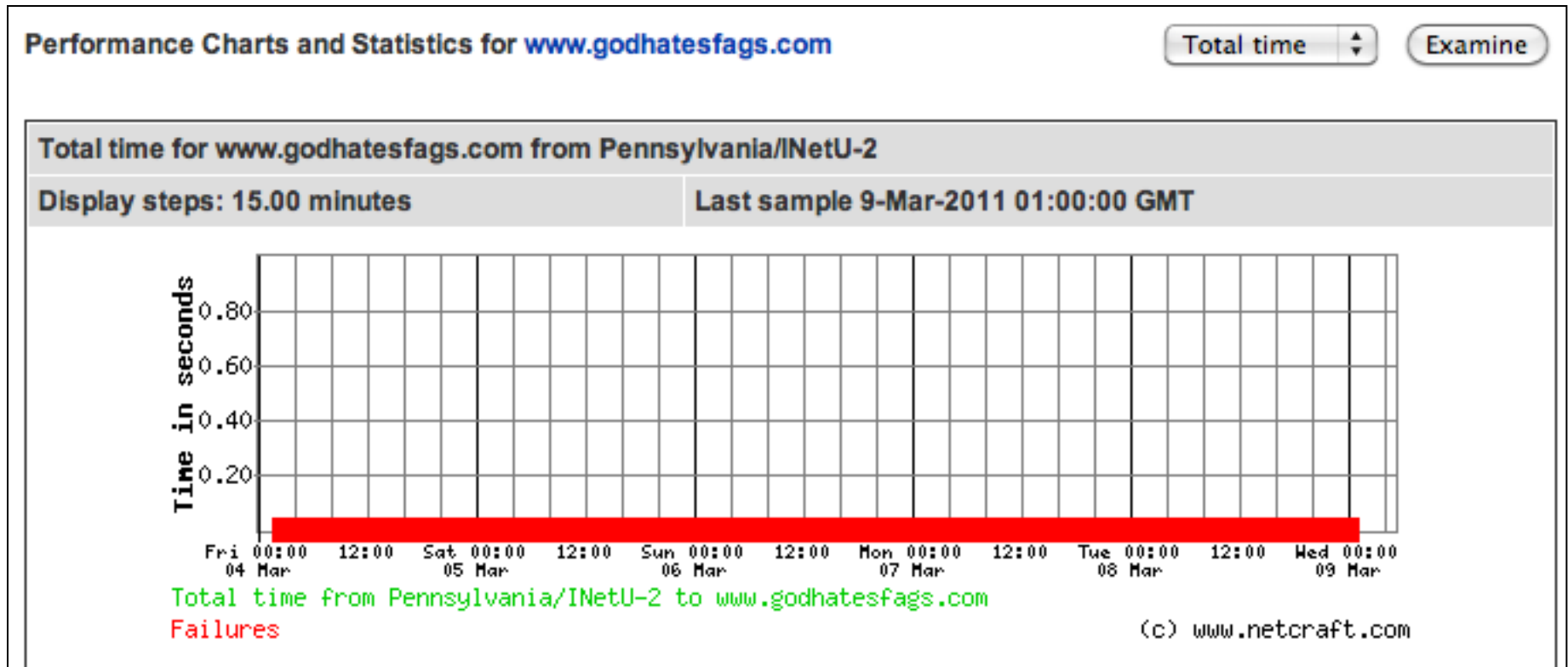
● th3j35t3r, [+] Tue 08 Mar 13:36 via XerXeS Attack Platform \



<http://bit.ly/gDxga5> << worth full watch if you wanna know why I am still #TANGODOWN on #WBC 13 days into no holds barred assault. #nointel

● th3j35t3r, [+] Sun 06 Mar 14:10 via web

Westboro Baptist Outage

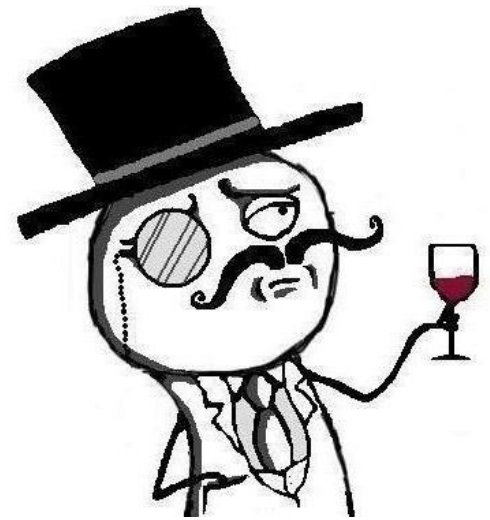


- 4 sites held down for 8 weeks
- From a single 3G cell phone
 - <http://tinyurl.com/4vggluu>



LulzSec

- The skilled group of Anons who hacked H B Gary Federal
- Hacked
 - US Senate
 - Pron.com
 - Sony
 - FBI
 - PBS
 - Fox News



Lulz Security® (LulzSec) rele. x

lulzsecurity.com/releases/

Releases

13/06/11

- Senate.gov internal data | [http](#)
- Bethesda internal data press release | [http](#) | [torrent](#)
- Bethesda internal data | [http](#) | [torrent](#)

10/06/11

- Pron.com user database | [http](#)

06/06/11

- Sownage™ 2 press release | [http](#) | [torrent](#)
- Scedev.net source code | [http](#) | [torrent](#)
- Sony BMG internal network maps | [http](#) | [torrent](#)

03/06/11

- Fuck FBI Friday™ press release | [http](#) | [torrent](#)
- Infragard Atlanta users database | [http](#) | [torrent](#)
- Karim dox | [http](#) | [torrent](#)
- Karim IRC log | [http](#) | [torrent](#)
- Karim emails | [torrent](#)
- Nintendo.com webserver configuration | [http](#)
- Unveillance secret conference | [http](#)

02/06/11

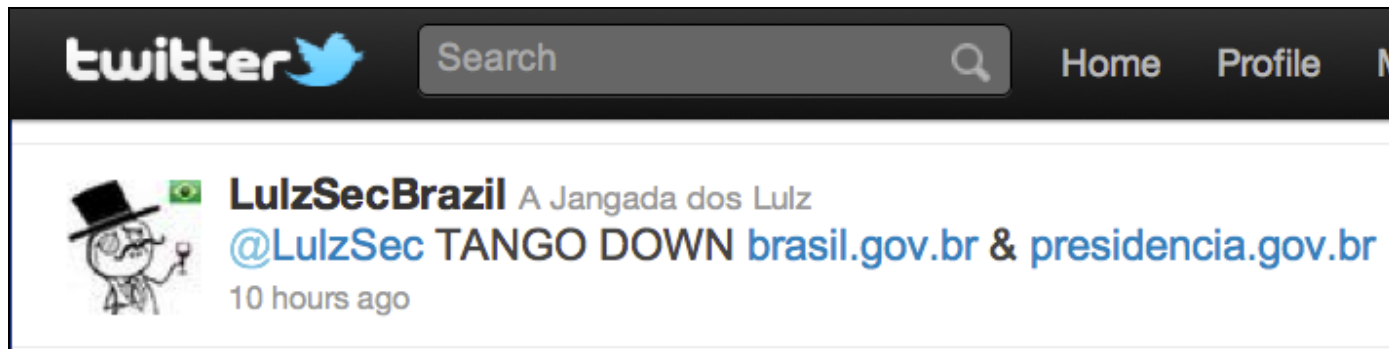


twitter.com/LulzSec

Hey Anonymous, we heard you were having trouble!

LulzSec Attacks on Government Sites

- FBI, CIA, US Senate
- UK's National Health Service
- SOCA, the UK's Serious Organised Crime Agency taken down 6-20-2011



THE Sun

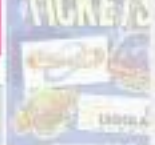
JAIL U-TURN
KNIFE BLITZ

SWOOP ON STUDENT

HACK THE LAD

Essex geek, 19, arrested for being 'global cyber-villain'

1/2 PRICE TICKETS



How Gormless are you?

DAILY Mirror

BLUE ARE YA?
DAWN FRENCH
Now I'm ready to love again

WORLD'S No1 HACKER SUSPECT IS ESSEX BOY

Computer geek arrested

CAMERON AT V WITH TOP BRA



THE TIMES

What next for Britain?
The CEO Summit report



Essex teenager linked to wave of global hacking

Message after attack on CIA and NHS

Daily Mail Money Mail

As it's revealed that half of Brits have German blood
TIME TO EMBRACE YOUR INNER JERRY!

Prosecutors will be able to fight off England's without fear of prosecution

THE LEGAL RIGHT TO PROTECT YOUR HOME



Exclusive: Face of the teenage 'cyber terrorist'

Britain's best-loved concise quality newspaper



Police swoop on teen cyber mastermind

Essex 19-year-old held in dawn raid over CIA and NHS web attacks



FINANCIAL TIMES

Britain
May the course? Analysis, Page 12



Police arrest suspected CIA hacker

Message after attack on CIA and NHS

Two Factor Authentication

- First factor: what user knows
- Second factor: what user *has*
 - Password token
 - USB key
 - Digital certificate
 - Smart card
- Without the second factor, user cannot log in
 - Defeats password guessing / cracking



RSA SecurID SD600



RSA SecurID SID700



RSA SecurID SD200



RSA SecurID SID800



RSA SecurID SD520



BlackBerry with
RSA SecurID software token

RSA was Hacked, and their Customers Too

Stolen Data Is Tracked to Hacking at Lockheed

By CHRISTOPHER DREW
Published: June 3, 2011

[Lockheed Martin](#) said Friday that it had proof that hackers breached its network two weeks ago partly by using data stolen from a vendor that supplies coded security tokens to tens of millions of computer users.



Lockheed's finding confirmed the fears of security experts about the safety of the SecurID tokens and heightened concerns that other companies or government agencies could be vulnerable to hacking attacks.

The tokens, which are used to protect remote access to computer networks, are sold by the RSA Security Division of the EMC Corporation. RSA officials said Friday that they accepted Lockheed's findings and were working with customers to offset the risks through other measures.

RSA disclosed in March that [hackers had stolen data](#) that could compromise a company's SecurID system in a broader attack, and the breach of Lockheed, the nation's largest defense contractor, is the first time that is known to have occurred.

Harry Sverdlow, of Bit9, said RSA might need to reprogram many of its security tokens.

RECOMMEND
TWITTER
SIGN IN TO E-MAIL
PRINT
REPRINTS
SHARE

SNOW FLOWER
and the SECRET FAN
WATCH THE TRAILER

- <http://samsclass.info/RSA-alternatives.html>



FOR TEH LULZ

The only reason anyone does anything

Layer 4 DDoS

Many Attackers – One Target
Bandwidth Consumption

Companies that Refused Service to Wikileaks

- Amazon
- Paypal
- Mastercard
- Visa
- Many others

Low Orbit Ion Cannon



- Primitive DDoS Attack, controlled via IRC
- Sends thousands of packets per second from the attacker directly to the target
- Like throwing a brick through a window
- Takes thousands of participants to bring down a large site
 - They tried but failed to bring down Amazon

Low Orbit Ion Cannon



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.3.0

Low Orbit Ion Cannon

1. Select your target

URL

IP

2. Ready?

Selected target

216.119.208.50

3. Attack options

Timeout HTTP Subsite TCP / UDP message

Wait for reply

Port Method Threads

<= faster Speed slower =>

Attack status

Idle Connecting Requesting Downloading Downloaded Requested Failed

Praetox.com

Operation Payback v. Mastercard

- Brought down Visa, Mastercard, and many other sites
 - Easily tracked, and easily blocked
 - High bandwidth, cannot be run through anonymizer
 - Dutch police have already arrested two participants



Mastercard Outage



3,000 to 30,000 attackers working together

Cybercrime can ruin entire economies

May 21, 2011 1:32 PM | By GREG GORDON

Russian anti-virus guru Eugene Kaspersky does a quick calculation in his head as he blinks at the ceiling.

Satisfied, he announces: "About 200000."

That's the number of virus-infected computers in a targeted attack on SA's internet infrastructure that would shut it off from the rest of the world. No e-mail. No electronic transactions. No web searches. No e-government. No Skype, Twitter or Facebook. Nothing.

He's not being alarmist - it happened in Estonia in 2007.

And 200000 rogue computers is not a huge number. Organised syndicates or loners with modest technical know-how and resources can harness millions of virus-infected machines they effectively control to add muscle to their efforts - from stealing money and identities to managing online corporate espionage or collapsing the infrastructure and function of a country's economy and government.

Kaspersky is CEO and founder of Kaspersky Lab, one of the world's top four anti-virus software companies and Europe's biggest. Worldwide, the

[Tweet](#) 68 [Share](#) 20



Layer 7 DoS

One Attacker – One Target
Exhausts Server Resources

Layer 7 DoS

- Subtle, concealable attack
- Can be routed through proxies
- Low bandwidth
- Can be very difficult to distinguish from normal traffic

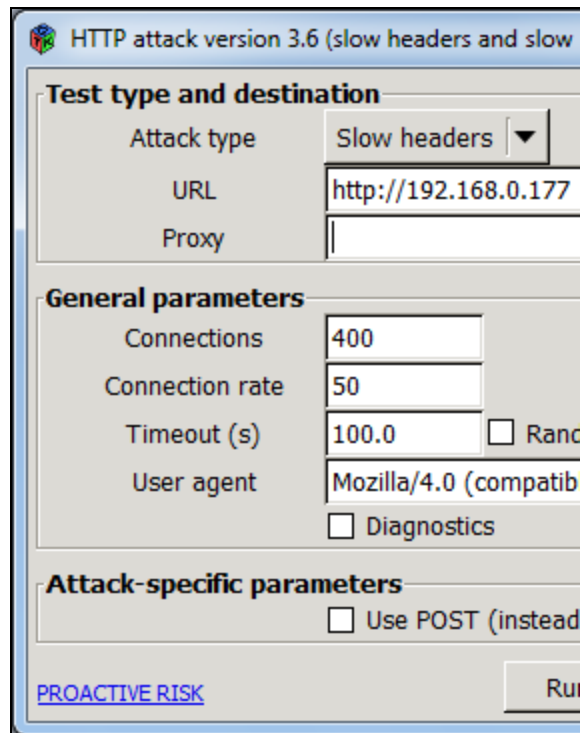
HTTP GET

No.	Time	Source	Destination	Protocol	Info
86	30.002700	192.168.19.52	74.208.84.186	HTTP	GET / HTTP/1.0

▶	Frame 86: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits)
▶	Ethernet II, Src: Vmware_24:3b:c0 (00:50:56:24:3b:c0), Dst: 06:90:4b:e6:06:10 (06:90:4b:e6:06:10)
▶	Internet Protocol, Src: 192.168.19.52 (192.168.19.52), Dst: 74.208.84.186 (74.208.84.186)
▶	Transmission Control Protocol, Src Port: 53395 (53395), Dst Port: 80 (80), Seq: 4231253285, Ack
▼	Hypertext Transfer Protocol
▶	GET / HTTP/1.0\r\n
	User-Agent: Wget/1.11.4\r\n
	Accept: */*\r\n
	Host: samsclass.info\r\n
	Connection: Keep-Alive\r\n
	\r\n

SlowLoris

- Send incomplete GET requests
- Freezes Apache with one packet per second



R-U-Dead-Yet

- Incomplete HTTP POSTs
- Stops IIS, but requires thousands of packets per second

The image displays three overlapping 'HTTP Attack Information' windows from a security tool. Each window shows the following data:

Attack	
Type	Slow POST
Protocol	http
Host	192.168.0.175
Path	/

Connections	
Target	20000
Active	1497
Connected	1496
Error/disconnected	4801
Create error	0

Diagnostics	
Diagnostics not enabled.	

The bottom-most window also includes a 'Run attack' button and a 'PROACTIVE RISK' indicator.

Overlaid on the bottom window is a browser window titled 'Service Unavailable' with the URL '192.168.0.175'. The page content reads:

Service Unavailable

HTTP Error 503. The service is unavailable.

Keep-Alive DoS

- HTTP Keep-Alive allows 100 requests in a single connection
- HEAD method saves resources on the attacker
- Target a page that is expensive for the server to create, like a search
 - <http://www.esrun.co.uk/blog/keep-alive-dos-script/>
- A php script
 - `pkp keep-dead.php`

Ubuntu test 2

Suspend Take Snapshot Rollback Settings

Unity Full Screen

Applications Places System Fri May 27, 8:21 AM student

```
student@ubuntu: /etc/init.d
File Edit View Terminal Help
top - 08:21:24 up 11:59, 2 users, load average: 0.17, 0.12, 0.16
Tasks: 147 total, 1 running, 145 sleeping, 1 stopped, 0 zombie
Cpu(s): 8.0%us, 3.0%sy, 0.0%ni, 75.3%id, 0.0%wa, 0.7%hi, 13.0%si, 0.0%st
Mem: 509244k total, 480916k used, 28328k free, 21352k buffers
Swap: 916472k total, 17084k used, 899388k free, 296460k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
  6531 www-data  20   0   223m 3732 1500  S  12.6   0.7   0:13.39 apache2
  6532 www-data  20   0   223m 4060 1824  S  11.6   0.8   0:13.07 apache2
```

BT4R2

root@bt: /var/www - Shell No. 3 - Konsole

Session Edit View Bookmarks Settings Help

```
Opening connection [438] to 192.168.198.167..success
Sending requests: |.....|
Closed connection
Opening connection [439] to 192.168.198.167..success
Sending requests: |.....|
Closed connection
Opening connection [440] to 192.168.198.167..success
Sending requests: |.....|
Closed connection
Opening connection [441] to 192.168.198.167..success
Sending requests: |.....|
Closed connection
Opening connection [442] to 192.168.198.167..success
Sending requests: |.....|
Closed connection
Opening connection [443] to 192.168.198.167..success
Sending requests: |.....|
```

Shell Shell No. 2 Shell No. 3

root@bt: /var/www eth0 - Wiresha Mozilla Firefox Downloads 1 2 11:21

XerXes



- Th3j35t3r's DoS Tool
 - Routed through proxies like Tor to hide the attacker's origin
 - No one knows exactly what it does
 - Layer 7 DoS?

XerXes



The screenshot shows the XerXes Attack HUD Console interface. At the top, there is a browser address bar with "WWW." and a page number "2 / 20". Below this is the "XerXes Attack HUD Console" window, which contains a log of attack progress:

- Attack in progress....
- Target Server Acquired: <http://alemarah.info>
- Weapons Free @09:18:04
- I'll notify you when target is down (Normally within 2 mins).
- Ramped this attack up a notch!
- Launched parallel drones

Below the log is a "Target Heartbeat" graph showing a green waveform, with the status "Status: TARGET UP".

The main interface features a network diagram with the following components:

- localhost**: 127.0.0.1
- Entry Node**: XX.XX.XX.XX
- Exit Node**: XX.XX.XX.XX
- Target**: alemarah.info

Additional information includes "140 Characters Remaining" and a "HOOKO" label. At the bottom, there are buttons for "Einger", "Start Attack", and "Halt Attack", along with a copyright notice: "By jester: <http://www.twitter.com/th3j35t3r>".

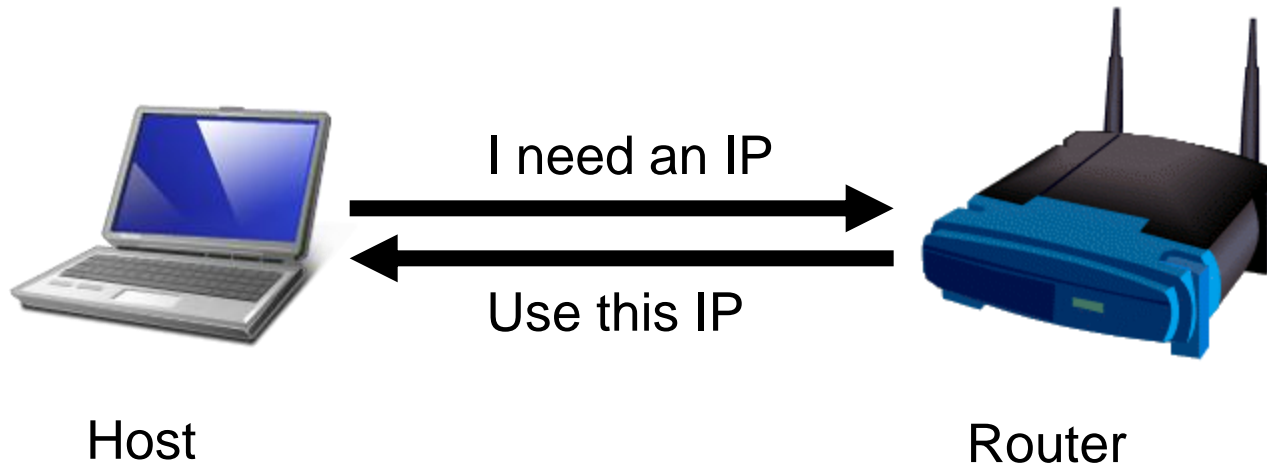
Link-Local DoS

IPv6 Router Advertisements

IPv4: DHCP

PULL process

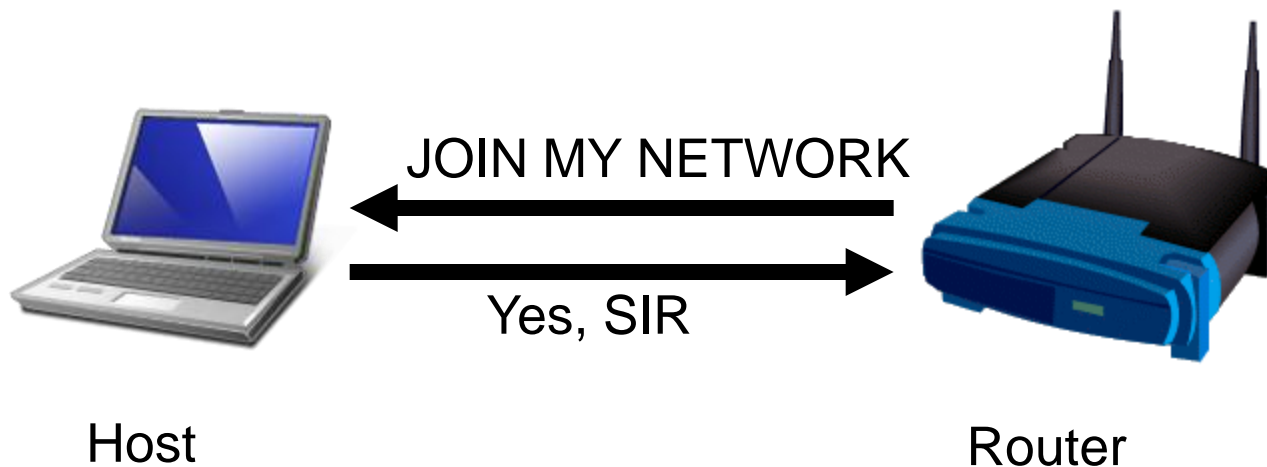
- Client requests an IP
- Router provides one



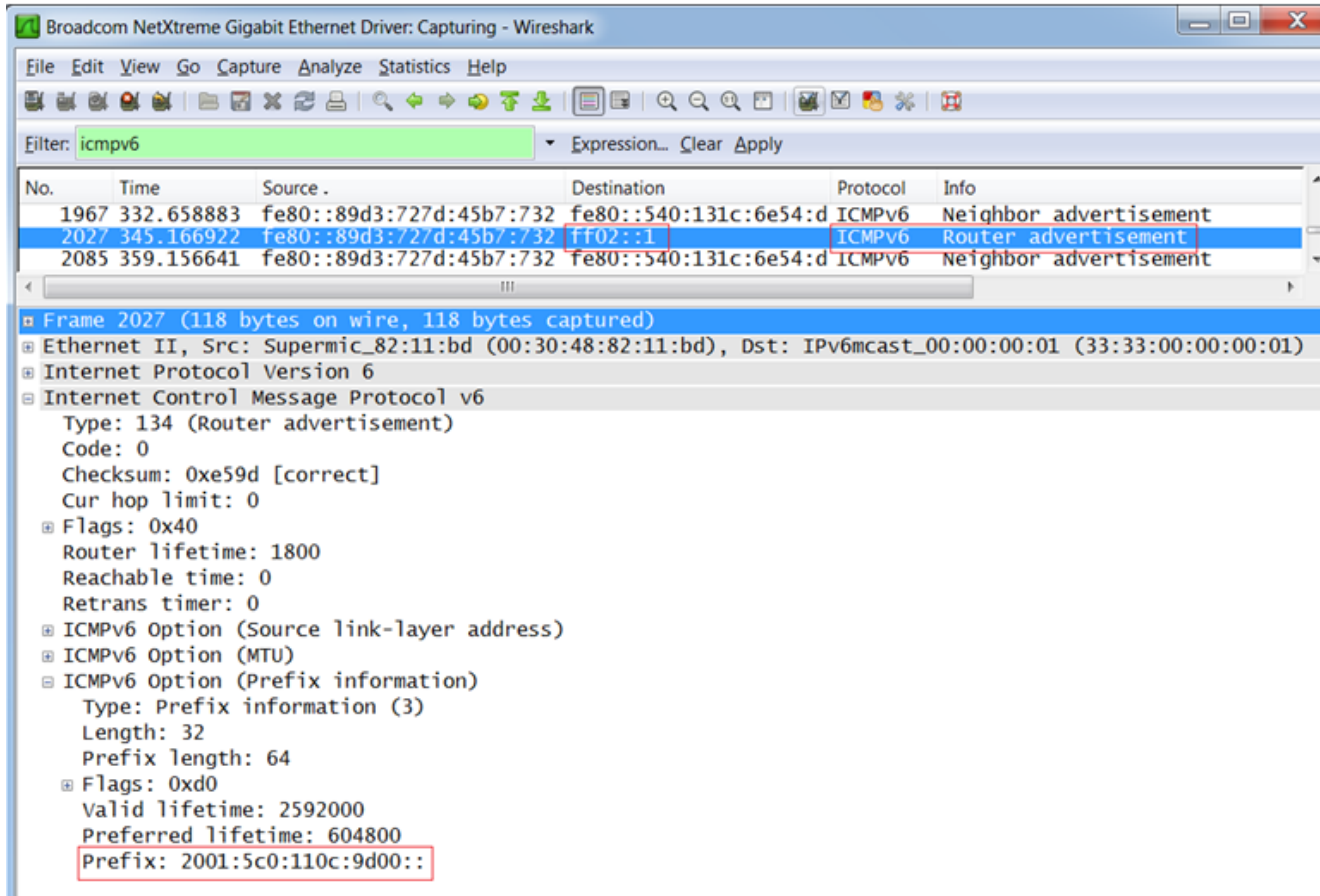
IPv6: Router Advertisements

PUSH process

- Router announces its presence
- Every client on the LAN creates an address and joins the network



Router Advertisement Packet



Broadcom NetXtreme Gigabit Ethernet Driver: Capturing - Wireshark

Filter: icmpv6

No.	Time	Source	Destination	Protocol	Info
1967	332.658883	fe80::89d3:727d:45b7:732	fe80::540:131c:6e54:d	ICMPv6	Neighbor advertisement
2027	345.166922	fe80::89d3:727d:45b7:732	ff02::1	ICMPv6	Router advertisement
2085	359.156641	fe80::89d3:727d:45b7:732	fe80::540:131c:6e54:d	ICMPv6	Neighbor advertisement

Frame 2027 (118 bytes on wire, 118 bytes captured)

- Ethernet II, Src: Supermic_82:11:bd (00:30:48:82:11:bd), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
- Internet Protocol Version 6
- Internet Control Message Protocol v6
 - Type: 134 (Router advertisement)
 - Code: 0
 - Checksum: 0xe59d [correct]
 - Cur hop limit: 0
 - Flags: 0x40
 - Router lifetime: 1800
 - Reachable time: 0
 - Retrans timer: 0
 - ICMPv6 Option (Source link-layer address)
 - ICMPv6 Option (MTU)
 - ICMPv6 Option (Prefix information)
 - Type: Prefix information (3)
 - Length: 32
 - Prefix length: 64
 - Flags: 0xd0
 - Valid lifetime: 2592000
 - Preferred lifetime: 604800
 - Prefix: 2001:5c0:110c:9d00::

RA Flood

```
Administrator: cmd - Shortcut
C:\Windows\system32>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IPv6 Address. . . . .             : 4:1:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:2:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:3:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:4:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:5:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:6:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:7:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:8:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:9:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .             : 4:10:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:11:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:12:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:13:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:14:1:0:156d:9e7e:48d3:704e
    IPv6 Address. . . . .            : 4:15:1:0:156d:9e7e:48d3:704e
```


Windows Vulnerability

- It takes a LOT of CPU for Windows to process those Router Advertisements
- 5 packets per second drives the CPU to 100%
- And they are sent to every machine in the LAN (ff02::1 is Link-Local All Nodes Multicast)
- One attacker kills all the Windows machines on a LAN
- FreeBSD is also vulnerable!
 - But not OpenBSD, of course

Responsible Disclosure

- Microsoft was alerted by Marc Heuse on July 10, 2010
- Microsoft does not plan to patch this
- Juniper and Cisco devices are also vulnerable
- Cisco has released a patch, Juniper has not

Defenses from RA Floods

- Disable IPv6
- Turn off Router Discovery
- Block rogue RAs with a firewall
- Get a switch with RA Guard

RA Guard Evasion

- Add "Fragmentation Headers" to the RA Packets
 - <http://samsclass.info/ipv6/proj/RA-evasion.html>

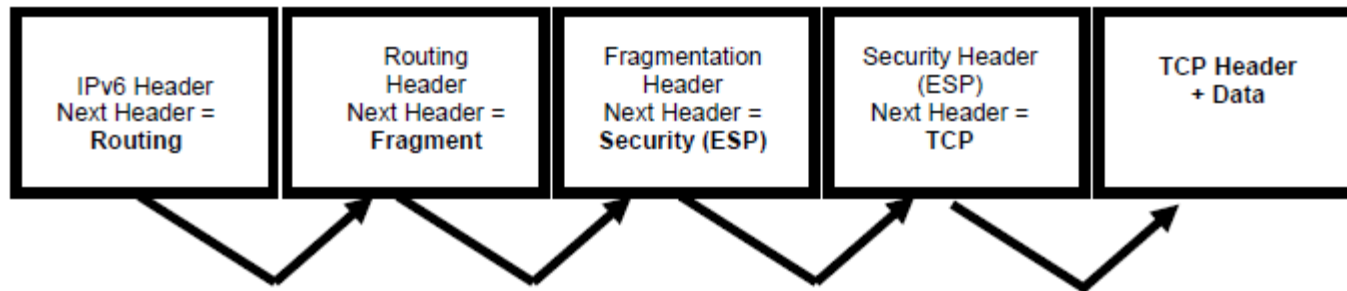


Figure 3-8. Next Header Fields in IPv6 and Extension Headers

Fragmentation Headers

Filter: icmpv6 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
3	1.41260	fe80::218:f4ff:fe78:26e4	ff02::1	ICMPv6	Router advertisement from 00:18:06:2d:3c:f4

Internet Protocol Version 6, Src: fe80::218:f4ff:fe78:26e4 (fe80::218:f4ff:fe78:26e4), Dst: ff02::1 (ff02::1)

- 0110 = Version: 6
- 0000 0000 = Traffic class: 0x00000000
- 0000 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
- Payload length: 80
- Next header: IPv6 fragment (0x2c)
- Hop limit: 255
- Source: fe80::218:f4ff:fe78:26e4 (fe80::218:f4ff:fe78:26e4)
[Source SA MAC: EoTechni_78:26:e4 (00:18:f4:78:26:e4)]
- Destination: ff02::1 (ff02::1)

Fragmentation Header

- Next header: IPv6 fragment (0x2c)
- 0000 0000 0000 0... = Offset: 0 (0x0000)
- 0 = More Fragment: No
- Identification: 0x4743b00b

Fragmentation Header

- Next header: ICMPv6 (0x3a)
- 0000 0000 0000 0... = Offset: 0 (0x0000)
- 0 = More Fragment: No
- Identification: 0x01000000

Internet Control Message Protocol v6

```
0000 33 33 00 00 00 01 00 18 f4 78 26 e4 86 dd 60 00 33.....x&...`
0010 00 00 00 50 2c ff fe 80 00 00 00 00 00 00 02 18 ...P,.....
0020 f4 ff fe 78 26 e4 ff 02 00 00 00 00 00 00 00 00 ...x&.....
```

Defending Websites

Attack > Defense

- Right now, your website is only up because
 - Not even one person hates you, or
 - All the people that hate you are ignorant about network security

Defense

- Mod Security--free open-source defense tool
 - Latest version has some protections against Layer 7 DoS
- Akamai has good defense solutions
 - Caching
 - DNS Redirection
 - Javascript second-request trick

Load Balancer

The image shows a network tool interface on the left and a web browser window on the right. The network tool displays an active 'Slow headers' attack on the target IP 192.168.11.143. The browser window shows the target server's response, which is a simple HTML page with the text 'Apache on the target Ubuntu VM'.

HTTP Attack Information

Attack

Type	Slow headers
Protocol	http
Host	192.168.11.143
Path	/

Connections

Target	400
Active	400
Connected	400
Error/disconnected	0
Create error	0

Diagnostics

Diagnostics not enabled.

Browser Window: http://192.168.11.143/ ... x
192.168.11.143
Other bookmarks

Page Content:

Apache on the target Ubuntu VM



CLOUDFLARE

- Proxy servers
- Conceals your server's IP address
- Blocks attacks using information from other attacks
- Free version
- Effective against th3j35t3r in real combat

Counterattacks

- Reflecting attacks back to the command & control server
- Effective against dumb attackers like Anonymous' LOIC
 - Will lose effect if they ever learn about Layer 7 DoS, which is happening now

References

References

Anonymous Takes Down U.S. Chamber Of Commerce And
Supporter Websites

<http://goo.gl/Mue9k>

Slowloris HTTP DoS

<http://ha.ckers.org/slowloris/>

OWASP HTTP DoS Tool

<http://code.google.com/p/owasp-dos-http-post/>

Mitigating Slow HTTP DoS Attacks

<http://blog.spiderlabs.com/2010/11/advanced-topic-of-the-week-mitigating-slow-http-dos-attacks.html>

'Tis the Season of DDoS – WikiLeaks Edition (Outage charts)

<http://goo.gl/V5jZc>

References

ModSecurity

<http://goo.gl/56hbl>

Akamai DDoS Report

http://baythreat.org/MichaelSmith_DDoS.pdf

How Secure Is Julian Assange's "Thermonuclear"
Insurance File?

<http://goo.gl/sY6Nn>

Overview of Anonymous and their attack on MasterCard:

<http://goo.gl/IVsCD>

Operation Payback Toolkit: LOIC and HiveMind

<http://pastehtml.com/view/1c8i33u.html>

References

r-u-dead-yet

<http://code.google.com/p/r-u-dead-yet/>

Keep-Alive DoS Script

<http://www.esrun.co.uk/blog/keep-alive-dos-script/>

Router Advertisement DoS in Windows

<http://samsclass.info/ipv6/proj/flood-router6a.htm>

RA Guard Evasion

<http://samsclass.info/ipv6/proj/RA-evasion.html>

XerXes Attack Video

<http://goo.gl/j8NQE>