DNS Security

Ch 1: The Importance of DNS Security

Updated 8-21-17

DNS is Essential

- Without DNS, no one can use domain names like *ccsf.edu*
- Almost every Internet communication begins with a DNS resolution

Topics

- DNS Under Attack
- DNS Assisting Attacks
- DNS Traffic as a Gauge of Malicious Activity
- Lack of DNS Authentication and Privacy

DNS Under Attack

Microsoft (2001)

- In 2001, Microsoft's DNS servers were attacked
  - Link Ch 1a

January 25, 2001 5:25 PM PST

Attack knocks out Microsoft Web sites

By Robert Lemos
Staff Writer, CNET News

Related Stories

Microsoft customers

Network attackers overwhelmed Microsoft's connection to the Internet on Thursday, causing traffic to the company's major Web sites to slow to a crawl.

Single Point of Failure

- Microsoft's network went through a single switch at that time
- 25% of the 1000 largest companies had a centralized DNS architecture at that time
- Companies moved to distributed architectures

June 16, 2004 1:37 PM PDT

'Zombie' PCs caused Web outage, Akamai says

By Robert Lemos and Jim Hu
Staff Writers, CNET News

Related Stories

Yahoo launches 100MB of free e-mail

June 15, 2004

Akamai glitch slows sites

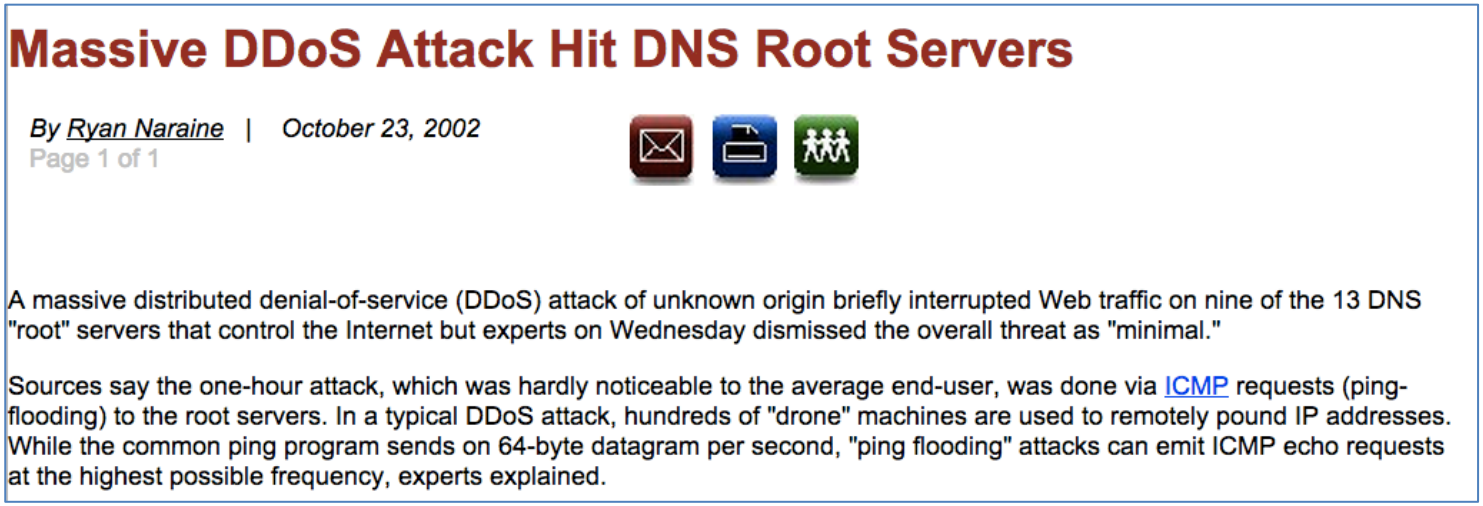
May 24, 2004

The attack that blacked out Google, Yahoo and other major Web sites earlier this week involved the use of a "botnet"--a large network of zombified home PCs--Internet infrastructure provider Akamai Technologies said Wednesday.

The attack, which blocked nearly all access to Apple Computer, Google, Microsoft and Yahoo's Web sites for two hours on Tuesday, took aim at the key domain name system (DNS) servers run by Akamai. These servers translate word-based URLs, such as www.microsoft.com, into

- Botnet defeated distributed architecture
  - Link Ch 1b

2002 Attack on DNS Root Servers



Massive DDoS Attack Hit DNS Root Servers

By Ryan Naraine | October 23, 2002

Page 1 of 1

A massive distributed denial-of-service (DDoS) attack of unknown origin briefly interrupted Web traffic on nine of the 13 DNS "root" servers that control the Internet but experts on Wednesday dismissed the overall threat as "minimal."

Sources say the one-hour attack, which was hardly noticeable to the average end-user, was done via ICMP requests (ping-flooding) to the root servers. In a typical DDoS attack, hundreds of "drone" machines are used to remotely pound IP addresses. While the common ping program sends on 64-byte datagram per second, "ping flooding" attacks can emit ICMP echo requests at the highest possible frequency, experts explained.

- Attacked all 13 root servers simultaneously
- ICMP flood, 900 Mbps
  - Links Ch 1c, 1d

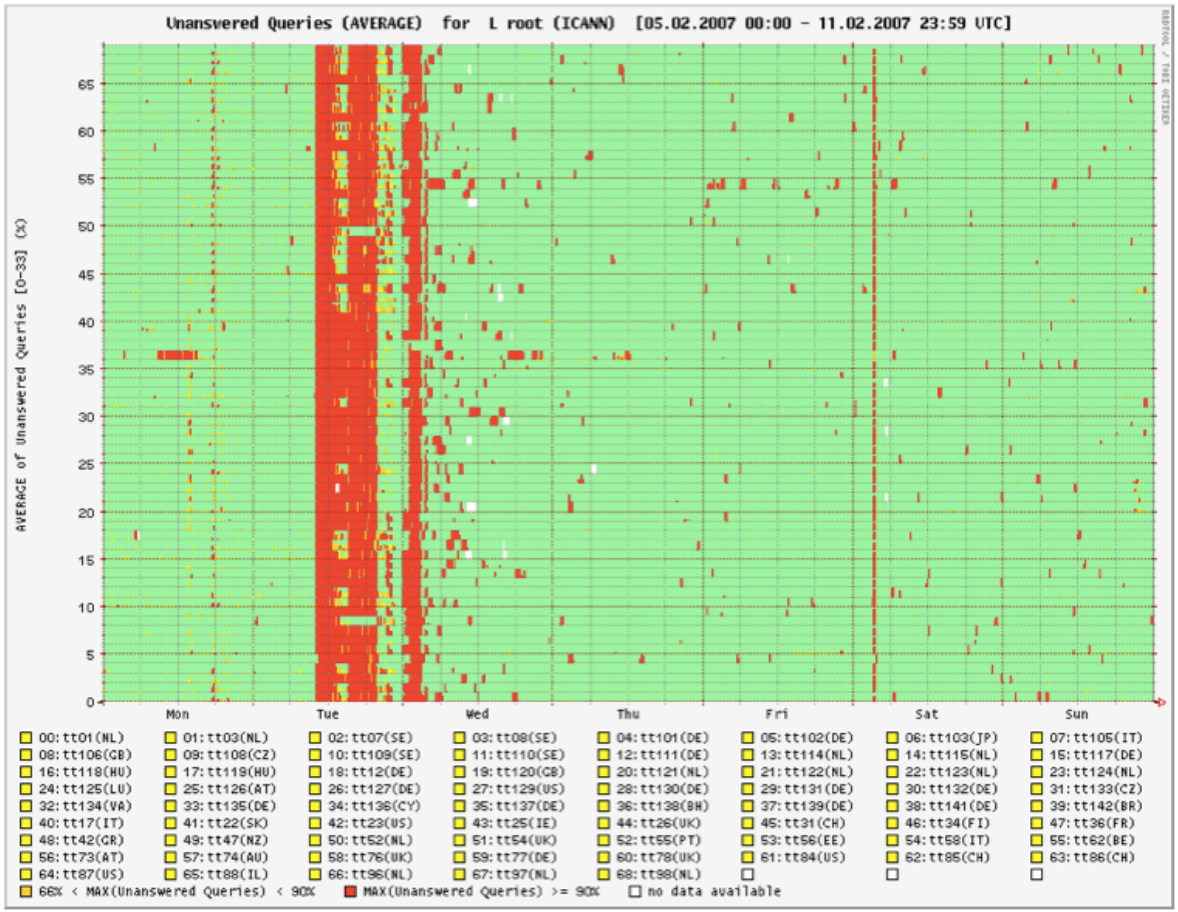
Defenses in 2002

- The attack had little effect, because
- Root DNS servers are vastly over-provisioned
- Attack was short; 1 hour
  - DNS records were cached in downstream servers

2007 Attack on DNS Root

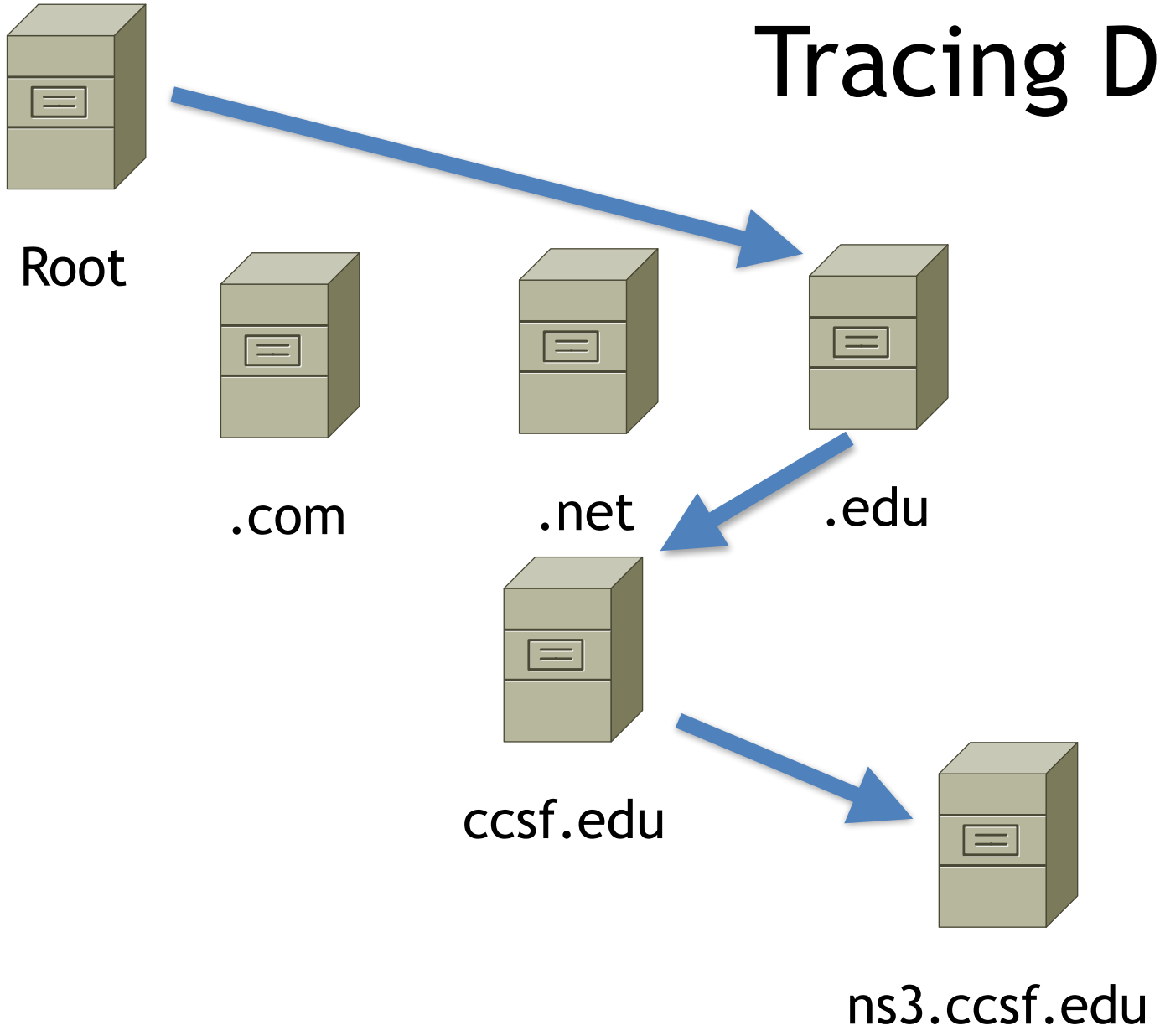
- Six root servers attacked from Asia
- Volume 1 Gbps per server, bogus DNS requests
- Only two were affected, because they did not yet have Anycast configured
- Anycast allows one IP address to be shared by many different servers
  - Traffic automatically goes to closest working serer via BGP
  - Link Ch 1e

2007 Attack on DNS Root



The attack on L-root in the week of 5 February 2007 (source: RIPE NCC dnsmon)

Tracing DNS



Tracing DNS

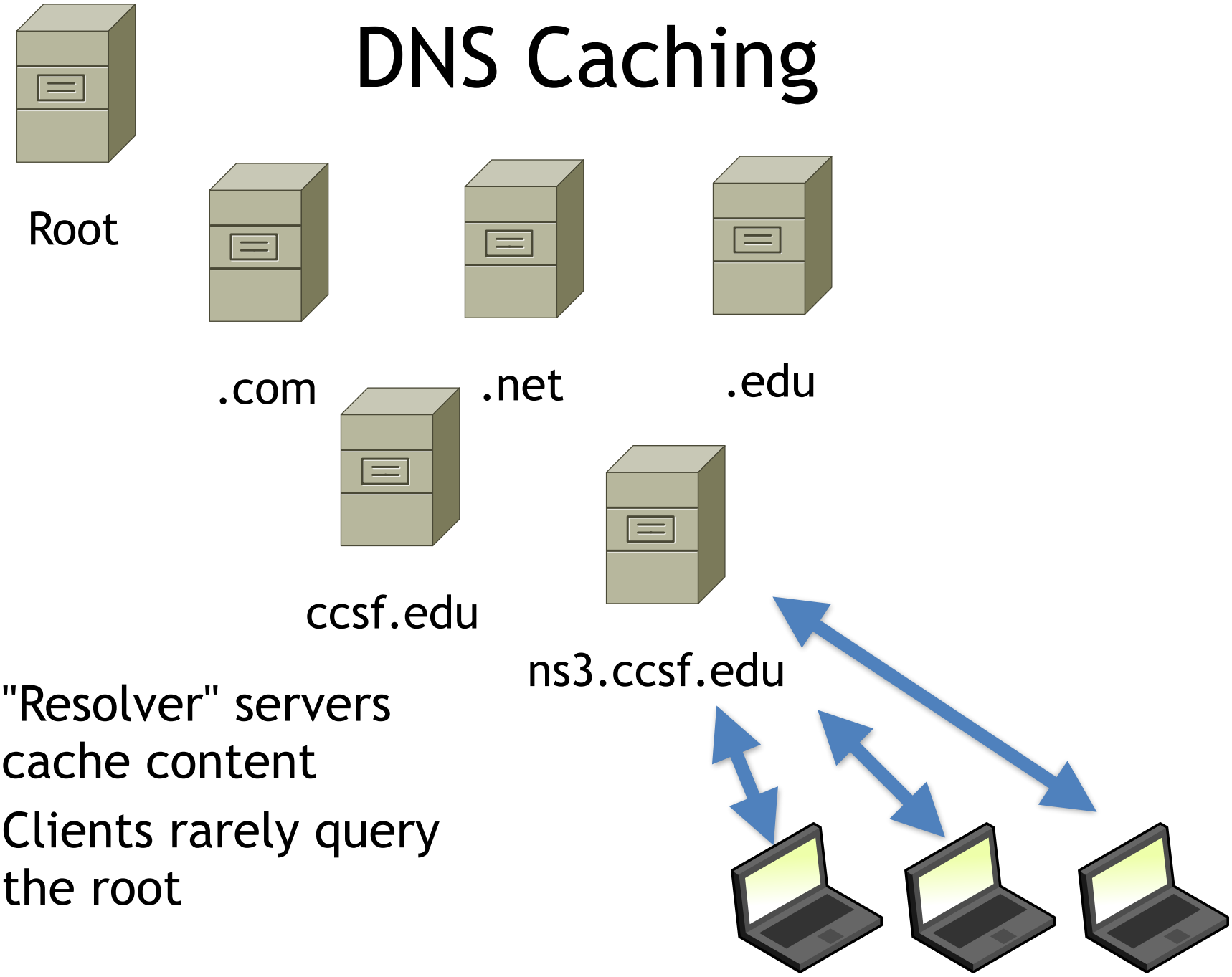
- Use the **+trace** option with dig

+[no]trace
Toggle tracing of the delegation path from the root name servers for the name being looked up. Tracing is disabled by default. When tracing is enabled, **dig** makes iterative queries to resolve the name being looked up. It will follow referrals from the root servers, showing the answer from each server that was used to resolve the lookup.

Tracing DNS

```
Sams-MacBook-Air-2:~ sambowne$ dig ccsf.edu +trace

; <<>> DiG 9.8.3-P1 <<>> ccsf.edu +trace
;; global options: +cmd
.                       2859    IN      NS      l.root-servers.net.
.                       2859    IN      NS      a.root-servers.net.
.                       2859    IN      NS      f.root-servers.net.
.                       2859    IN      NS      k.root-servers.net.
.                       2859    IN      NS      e.root-servers.net.
.                       2859    IN      NS      c.root-servers.net.
.                       2859    IN      NS      m.root-servers.net.
.                       2859    IN      NS      h.root-servers.net.
.                       2859    IN      NS      i.root-servers.net.
.                       2859    IN      NS      b.root-servers.net.
.                       2859    IN      NS      g.root-servers.net.
.                       2859    IN      NS      d.root-servers.net.
.                       2859    IN      NS      j.root-servers.net.
;; Received 228 bytes from 8.8.8.8#53(8.8.8.8) in 537 ms

edu.                    172800  IN      NS      a.edu-servers.net.
edu.                    172800  IN      NS      c.edu-servers.net.
edu.                    172800  IN      NS      d.edu-servers.net.
edu.                    172800  IN      NS      l.edu-servers.net.
edu.                    172800  IN      NS      f.edu-servers.net.
edu.                    172800  IN      NS      g.edu-servers.net.
;; Received 261 bytes from 202.12.27.33#53(202.12.27.33) in 626 ms

ccsf.edu.               172800  IN      NS      ns3.csu.net.
ccsf.edu.               172800  IN      NS      rudra3.ccsf.cc.ca.us.
ccsf.edu.               172800  IN      NS      ns4.cenic.org.
ccsf.edu.               172800  IN      NS      ns5.cenic.org.
ccsf.edu.               172800  IN      NS      ns6.cenic.org.
;; Received 164 bytes from 192.31.80.30#53(192.31.80.30) in 275 ms

ccsf.edu.               3600    IN      A       147.144.1.212
;; Received 42 bytes from 137.164.29.69#53(137.164.29.69) in 19 ms

Sams-MacBook-Air-2:~ sambowne$
```

DNS Caching



- "Resolver" servers cache content
- Clients rarely query the root

DNS Cache Poisoning

- Malicious altering of cache records redirects traffic for users of that server
- 2005 attack redirected traffic for more than 1000 companies
  - Link Ch 1g, from 2005

DNS Poisoning Scam Raises Wariness of 'Pharming'

A new attack using DNS cache poisoning has raised concerns about "pharming," a next-generation phishing scam in which malware or DNS hacks are used to invisibly redirect victims to spoofed web sites.

DNS cache poisoning injects false information into DNS servers, which route Internet traffic by matching domain

Kaminsky DNS Vulnerability

Steve Friedl's Unixwiz.net Tech Tips

An Illustrated Guide to the Kaminsky DNS Vulnerability

The big security news of Summer 2008 has been Dan Kaminsky's discovery of a serious vulnerability in DNS. This vulnerability could allow an attacker to redirect network clients to alternate servers of his own choosing, presumably for ill ends.

Table of Contents

- Terminology
- Following a simple DNS query
- What's in a DNS packet?
- Resource Record Types
- Drilling down to a real query
- What's in the cache?
- Poisoning the cache
- Shenanigans, Version 1

This all led to a mad dash to patch DNS servers worldwide, and though there have been many writeups of just how the vulnerability manifests itself, we felt the need for one in far more detail. Hence, one of our Illustrated Guides.

This paper covers how DNS works: first at a high level, then by picking apart an individual packet exchange field by field. Next, we'll use this knowledge to see how weaknesses in common implementations can lead to cache poisoning.

Nice work, Dan

- Serious vulnerability in 2008
- Allowed poisoning caches on many servers
- Patched before it was widely exploited
  - Link Ch 1h

DNSChanger

From Wikipedia, the free encyclopedia

DNSChanger was a DNS hijacking Trojan active from 2007 to 2011. The work of an Estonian company known as Rove Digital, the malware infected computers by modifying a computer's DNS entries to point toward its own rogue name servers, which then injected its own advertising into Web pages. At its peak, DNSChanger was estimated to have infected over 4 million computers, bringing in at least US$14 million in profits to its operator from fraudulent advertising revenue.[1]

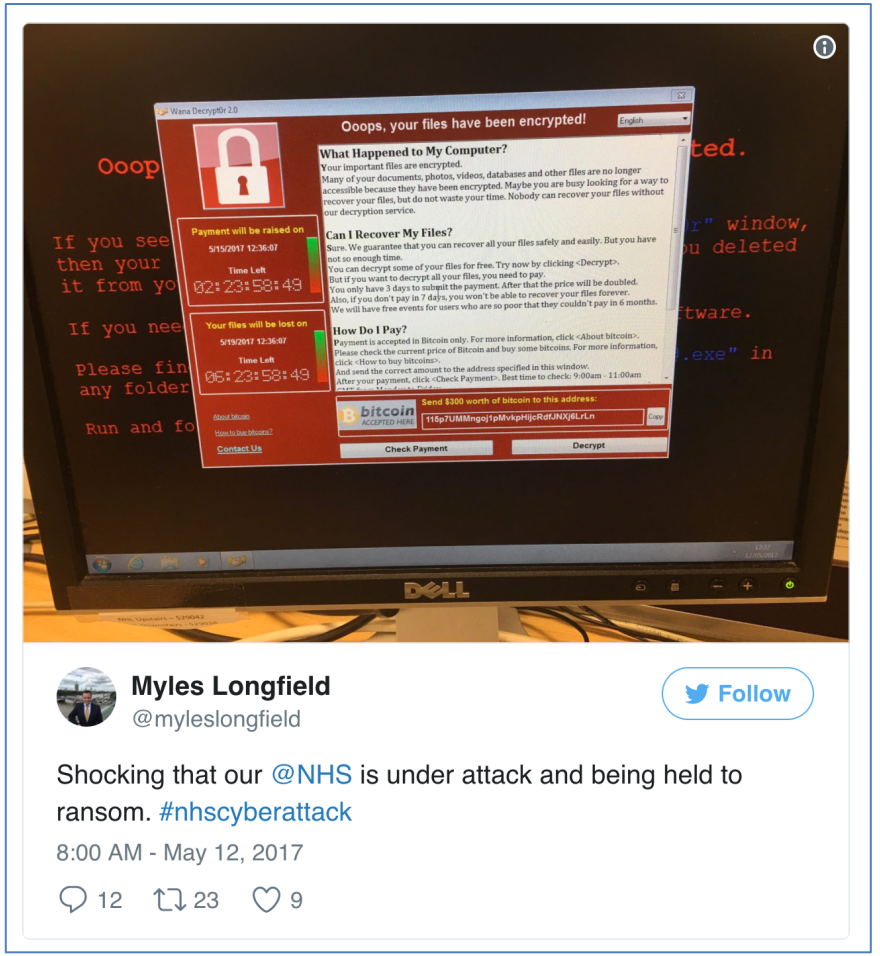
- Changed local DNS server address
  - Link Ch 1h


Kahoot!

DNS Assisting Attacks

Wannacry Ransomware

- Caused hospitals across England to divert emergency patients in May 2017
- Used NSA-developed attacks leaked by "Shadow Brokers" (Russians)
- Microsoft released a patch but hospital systems didn't install it in time
  - Link Ch 1y



How to Accidentally Stop a Global Cyber Attacks

May 13, 2017 MalwareTech ms17-010, ransowmare, worm 442

have to be propagated using another method). I was quickly able to get a sample of the malware with the help of Kafeine, a good friend and fellow researcher. Upon running the sample in my analysis environment I instantly noticed it queried an unregistered domain, which i promptly registered.

Darien Huss
@darienhuss

Follow

#WannaCry propagation payload contains previously unregistered domain, execution fails now that domain has been sinkholed

10:29 AM - May 12, 2017

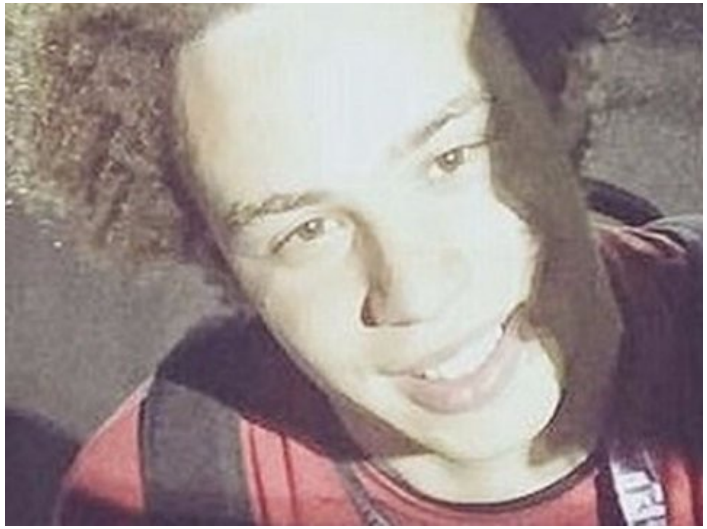
65 1,458 2,186

- Link Ch 1z1

Is the Hacker Hutchins a Good Guy or Bad Guy?

Jeff John Roberts
Aug 05, 2017

- Saved American hospitals & other businesses by freezing Wannacry
- Arrested in the US after DEF CON; accused of selling banking malware
  - Link Ch 1z, 1z2



Dynamic DNS (DDNS)

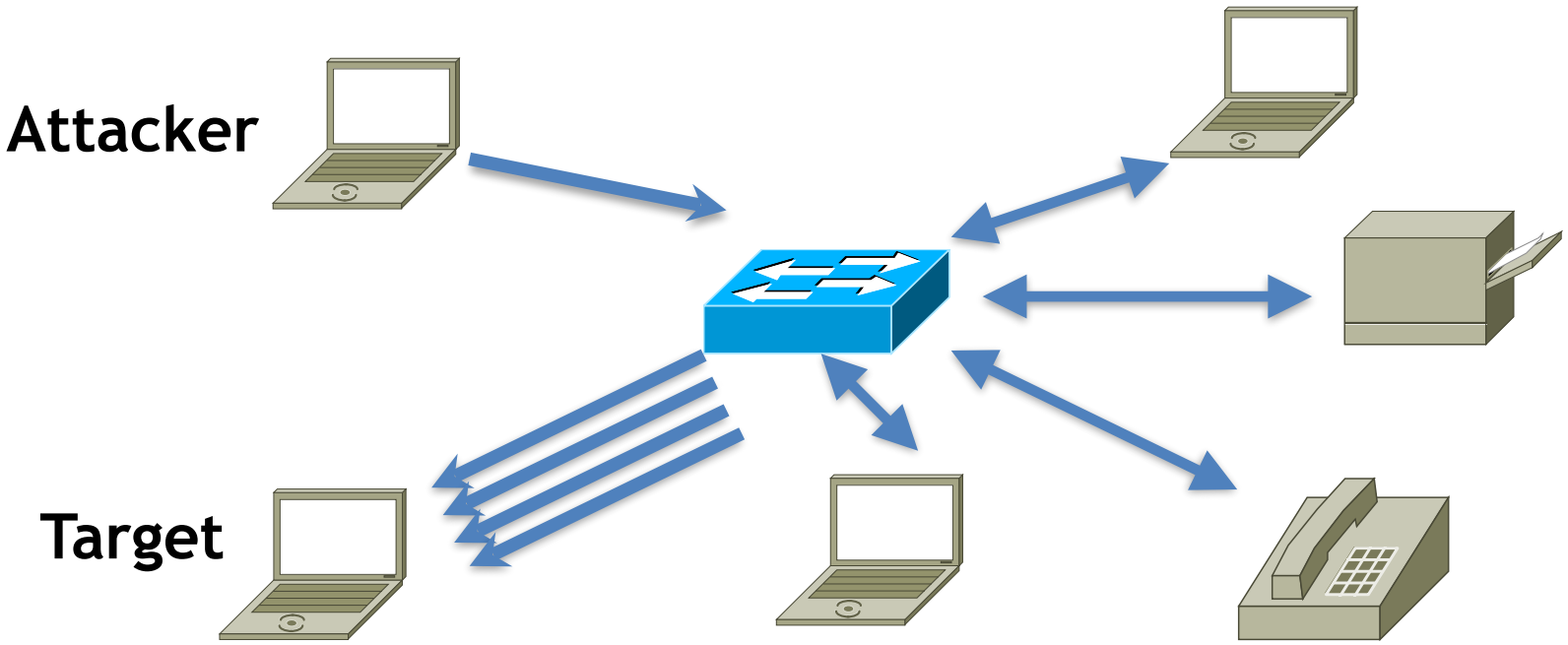
- Allows the IP address of a domain name to change quickly
- This allows home users to host servers on transient addresses
- Abused by botnet operators, phishers, and malware download sites
  - Change address rapidly to avoid detection and shutdown

Fast Flux DNS

- Changes DNS addresses rapidly
- Hides servers behind reverse proxies that rapidly change
- Makes it difficult to find the central servers
  - Link Ch 1j

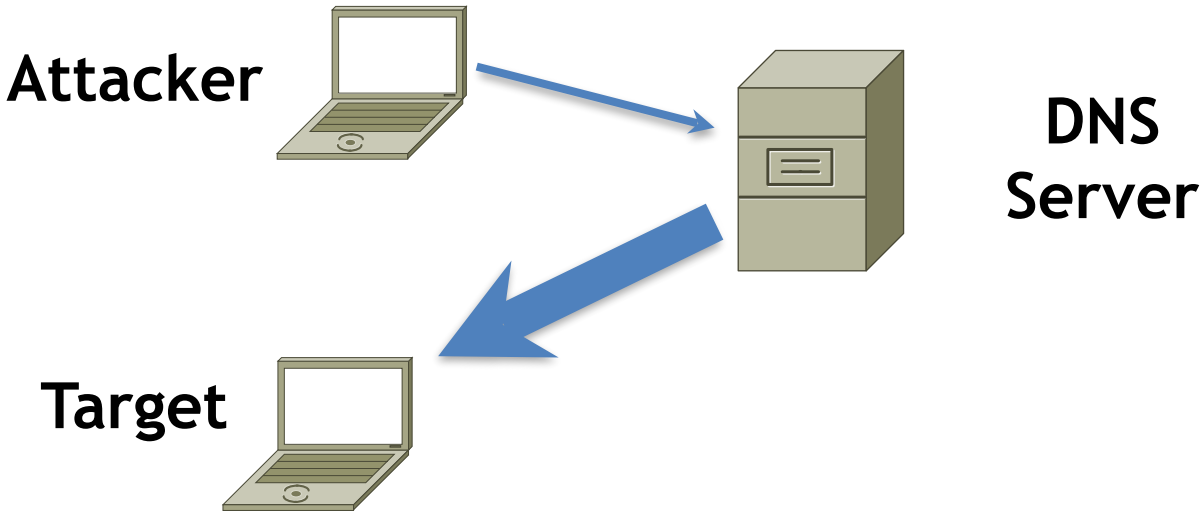
Packet Amplification

- Smurf attack
  - PING echo request sent to a broadcast address
  - Many replies for each request



DNS Amplification

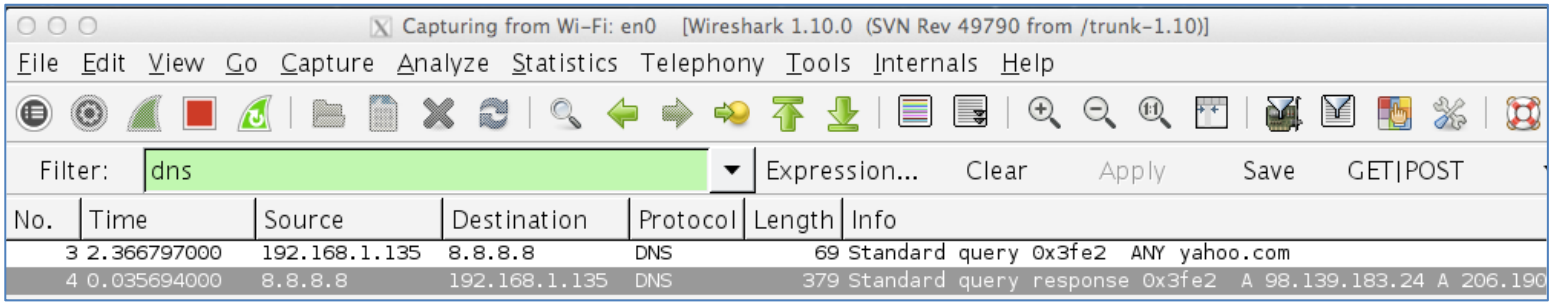
- Find a domain name that gives a large response
- Also called "DRDoS Attack" (Distributed Reflection and Amplification Denial of Service)
  - Link Ch il



dig any yahoo.com

```
Sams-MacBook-Air-2:~ sambowne$ dig any yahoo.com

; <<>> DiG 9.8.3-P1 <<>> any yahoo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16354
;; flags: qr rd ra; QUERY: 1, ANSWER: 14, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;yahoo.com.                     IN      ANY

;; ANSWER SECTION:
yahoo.com.              1632    IN      A       98.139.183.24
yahoo.com.              1632    IN      A       206.190.36.45
yahoo.com.              1632    IN      A       98.138.253.109
yahoo.com.              1632    IN      MX      1 mta5.am0.yahoodns.net.
yahoo.com.              1632    IN      MX      1 mta7.am0.yahoodns.net.
yahoo.com.              1632    IN      MX      1 mta6.am0.yahoodns.net.
yahoo.com.              21432   IN      NS      ns1.yahoo.com.
yahoo.com.              21432   IN      NS      ns5.yahoo.com.
yahoo.com.              21432   IN      NS      ns2.yahoo.com.
yahoo.com.              21432   IN      NS      ns6.yahoo.com.
yahoo.com.              21432   IN      NS      ns3.yahoo.com.
yahoo.com.              21432   IN      NS      ns4.yahoo.com.
yahoo.com.              21432   IN      NS      ns8.yahoo.com.
yahoo.com.              1632    IN      SOA     ns1.yahoo.com. hostmaster.yahoo-
inc.com. 2013082607 3600 300 1814400 600

;; Query time: 36 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Aug 26 16:59:24 2013
;; MSG SIZE  rcvd: 337
```

dig any yahoo.com



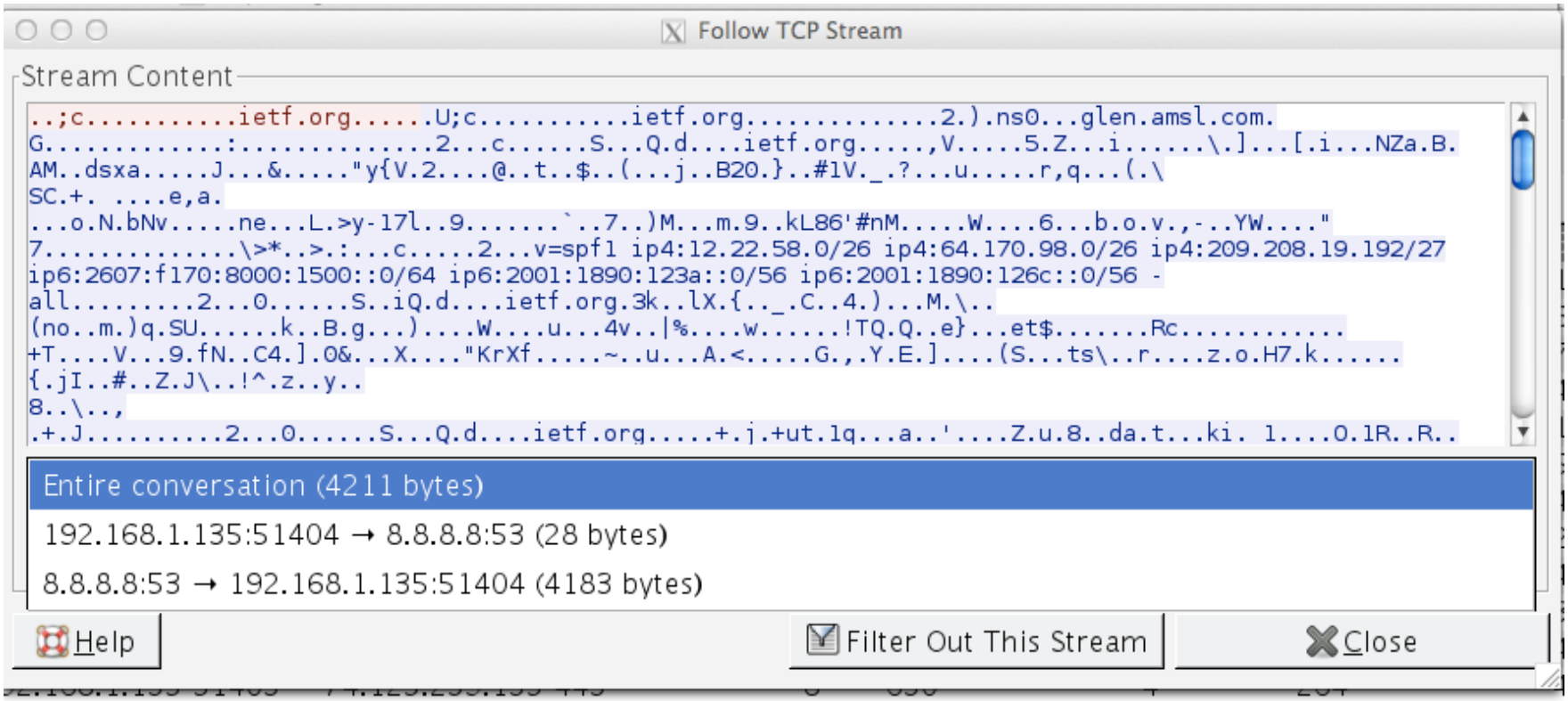
- Request: 69 bytes
- Reply: 379 bytes
- Amplification: 5.5 x

dig any ietf.org

```
Sams-MacBook-Air-2:~ sambowne$ dig any ietf.org
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.8.3-P1 <<>> any ietf.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15203
;; flags: qr rd ra; QUERY: 1, ANSWER: 25, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;ietf.org.                      IN      ANY

;; ANSWER SECTION:
ietf.org.               818     IN      SOA     ns0.ietf.org. glen.amsl.com. 1200000184 1800 1800 604800 1800
ietf.org.               818     IN      RRSIG   SPF 5 2 1800 20140722175706 20130722165742 40452 ietf.org. Gr+MvyxWDx3nleU1EFqC+uhpyZLzv
ZOvXNpd6RIRW8Zp7qmjTlphwELT DUFN1x1kc3hh4+DG1vhK0pnvJhvCFb+OInl7Vp0y2LC3pUCXC3SyGCQa hygOx85qlKVCMjDEfRwWIzFW2F+dP6sUhHWCGegejXIscQ/tECi
JXA1T Q4srDCCiiLODZSxhgwqz5Ahv+E6gYk52g7/tFIxuZeqctkzMPnktMTds we85p8Xe1PwdLmAZrTeyGClN0JCobbE529BrTDg2JyNuTQiB27ShV/Wr BuI2jLMZYvpvq3b4
LC3m+llX6ZGW5yI3/uuzisPX9qnXjOzmoYxcPiof rD7fOg==
ietf.org.               818     IN      SPF     "v=spf1 ip4:12.22.58.0/26 ip4:64.170.98.0/26 ip4:209.208.19.192/27 ip6:2607:f170:8000:15
00::0/64 ip6:2001:1890:123a::0/56 ip6:2001:1890:126c::0/56 -all"
ietf.org.               818     IN      RRSIG   DNSKEY 5 2 1800 20140722175449 20130722165742 45586 ietf.org. M2v32WxYpnvDy1/+QwTuNH8pE7
0ZTRRcrxUobm/ppG2NKXEeU1XWgrIP k9ZrGolCo2cLtPYpnxG+r1eU2+CNdZffGTR20h58JYbb1Mt3g62Intm1 IVRRk1H3lWV9AaOCZXQkmcPHGeEQylJjGwKAi874odCaGark
K1S9BhIe VqcU/TmbZk6y+UM0FF3mMCbUkJhYhboGvyJLclhmiar/0BZ+t/h1pNn+ QbA80bfKjBJHjSyQWeNFkl2+AZnlKFO0red0c1yr/nKliQvheuxv+Ug3 nmvDlIcWfx17h
GpJjJcjEAFaHkpctYwhXol6m+J5o/oKOBAPXB/ZLAqK KxtKkA==
ietf.org.               818     IN      RRSIG   DNSKEY 5 2 1800 20140722175632 20130722165742 40452 ietf.org. y8jNBiuJatkrdXSUMXHYrd9hru
8nkpGzsVr1ddE4Aw9kYfF0+O9/a2mP IDHb25iAT+ExUpGNUue9e4WSWhFeQw9V4yK0Aivhr89MDVa4kztV7xzQ MEEU/6SmXADelS/QDYBA5fyAJFaN6qPyS0Y1c1qaOMZfVln2
dYRavKrP 2FhubdmHIdj7cc5WJU5fxImkJN/I0x2cR83H6y4NJ+lJ7qXFYE7gRNhN rWPh2Z2r/RCfuc/o6V0jLrPTK98/TKas2fC35tuxIpQv+rS9ZpToCmN1 KSYKenNVZYudk
ifTnhFnZMGD/Gj4/vWcPN5VmSp0ZY9xvOubiOmMAUoC g4sudQ==
```

- Large DNSSEC signatures

dig any ietf.org



- Request: 28 bytes (+66 header)
- Reply: 4183 bytes (+ headers)
- Amplification: 45 x (but via TCP)

Extension Mechanisms for DNS (EDNS)

- Allows transmission of larger packets via UDP
- Normal max. is 512 bytes
- This extends it to larger values, such as 4096
- Essential for DNSSEC efficiency, but will make DNS amplification much more powerful
  - Link Ch 1k

DNS as a Conduit of Attacks

- Sinit Trojan (2003)
  - Used port UDP 53
  - Allowed by firewalls
    - Link Ch 1m

How It Works:
The Sinit Trojan has a communication protocol based on six types of packets, each one prefixed with a byte of value 1-6 and maximum size of 512 bytes. It listens on UDP port 53 and also a high-numbered random UDP port. Either port will respond to the protocol packets described below:

DNS Traffic as a Gauge of Malicious Activity

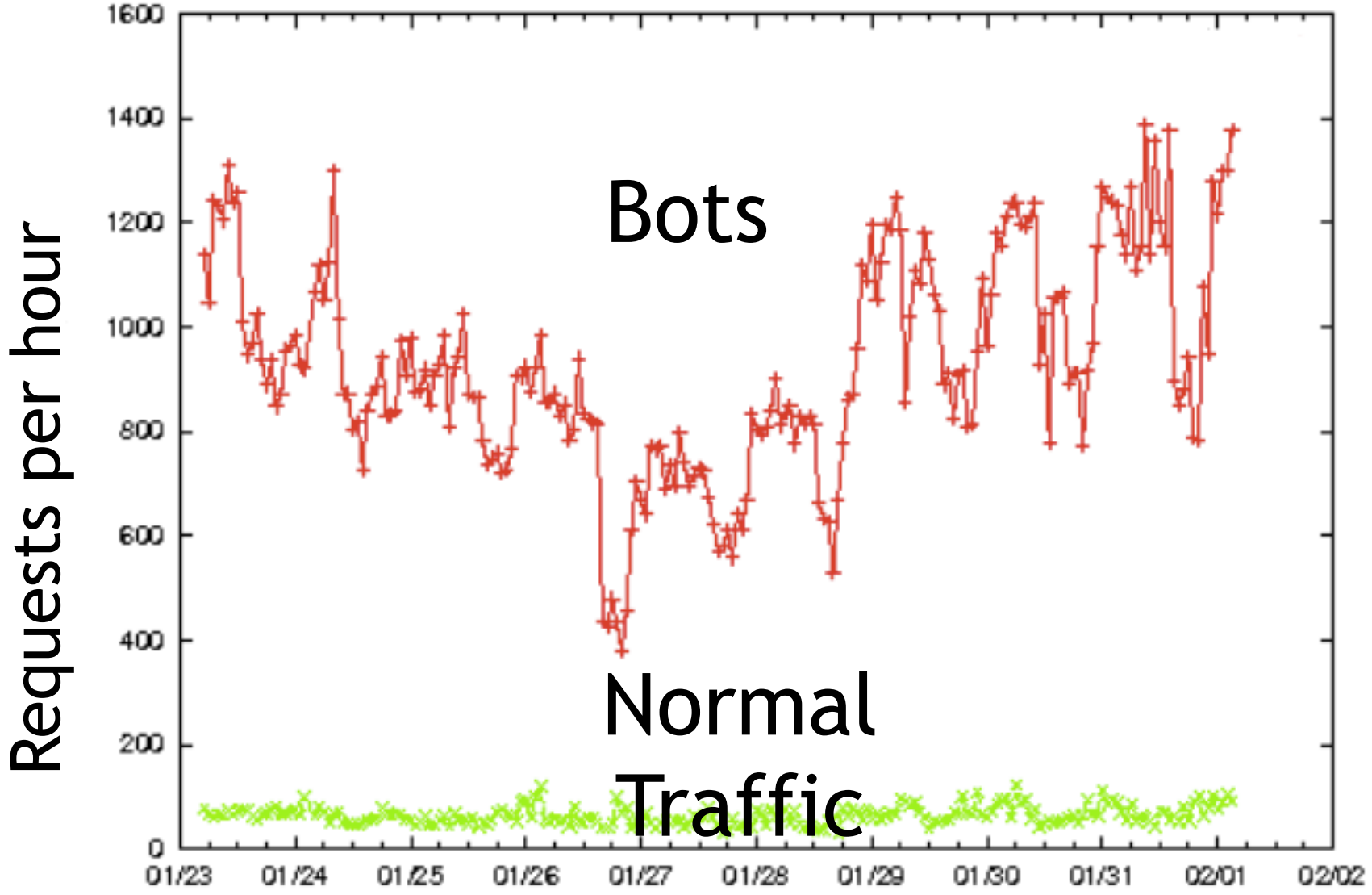
DNS Monitoring

- Infected machines often make many DNS queries
- Spam relays make DNS requests to find addresses of mail servers
- Botnets often make many DNS requests to obscure domains

Conficker Worm Domains

- Algorithm made 50,000 new domains per day
- Registrars tried to block them all
  - Links Ch 1u, 1v

```
Variant, Date, Index, Hostname
A, 02/12/2009, 0, puxqy.net
A, 02/12/2009, 1, elvyodjjtao.net
A, 02/12/2009, 2, ltxbshpv.net
A, 02/12/2009, 3, ykjzaluthux.net
A, 02/12/2009, 4, lpiishmjlb.net
A, 02/12/2009, 5, arpsyp.com
A, 02/12/2009, 6, txkjngucnth.org
A, 02/12/2009, 7, vhslzulwn.org
A, 02/12/2009, 8, jcqavkkhg.net
A, 02/12/2009, 9, dmszsyfp.info
. . .

B, 02/12/2009, 0, tvxwoajfwad.info
B, 02/12/2009, 1, blojvbcbrwx.biz
B, 02/12/2009, 2, wimmugmq.biz
B, 02/12/2009, 3, fwnvlja.org
B, 02/12/2009, 4, umgrzaybbf.ws
B, 02/12/2009, 5, btgoyr.cc
B, 02/12/2009, 6, zboycplmkhc.cc
B, 02/12/2009, 7, qsqzphbn.biz
B, 02/12/2009, 8, xqdvmavs.cn
B, 02/12/2009, 9, wgrrrr.biz
```



- From Link Ch 1q

Blocking DNS Resolution for Known Malicious Domains

OpenDNS

- Anycast for reliability
- Reports of DNS activity for management
- Blocks malicious servers
- Can enforce other rules like Parental Controls

Storm Worm (2007)

Gathering 'Storm' Superworm Poses Grave Threat to PC Nets

Bruce Schneier 10.04.07

- Distributed C&C (Command and Control) via a peer-to-peer system
- Fast flux DNS
- Mutates every 30 minutes
  - Link Ch 1s

Microsoft Intercepts 'Nitol' Botnet And 70,000 Malicious Domains

- Microsoft took over the 3322.org domain, with authorization from a court order, in 2012
- Controversial process
  - Only temporary botnet disruption
  - Takes down C&C servers controlled by other researchers; "collateral damage"
  - Link Ch 1t

Lack of DNS Authentication and Privacy

DNS Monitoring

- DNS monitoring shows every domain visited
- Used by security team to monitor network usage

```
#!/usr/bin/env python
from scapy.all import *

def findDNS(p):
  if p.haslayer(DNS):
    print p[IP].src, p[DNS].summary()

sniff(prn=findDNS)
```

```
root@kali:~/packt# python dnsmon2.py
172.16.1.187 DNS Qry "yahoo.com."
172.16.1.187 DNS Qry "yahoo.com."
172.16.1.2 DNS Ans "2001:4998:44:204::a7"
172.16.1.2 DNS Ans "98.138.253.109"
172.16.1.187 DNS Qry "109.253.138.98.in-addr.arpa."
172.16.1.2 DNS Ans "ir1.fp.vip.ne1.yahoo.com."
```

Intrinsic Protocol Weakness

- DNS requests and responses are not encrypted
- No strong authentication
  - Responses cannot be fully trusted
- Responses can be spoofed or intercepted and modified
- Altered responses may be cached for a long time

Financial Impacts and Intangible Losses

- **Availability**: DNS outage causes direct loss of revenue
- **Fraud**: Modified DNS services can
  - Send spam
  - Drive users to phishing sites
  - Connect bots to C&C servers
  - Locate malware download sites

Cyberwar

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

E-mail this to a friend Printable version

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Estonia says many state websites have been affected

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.


Kahoot!