



Responsible Disclosure

A Case Study of CERT VU#800133, “DNS Cache Poisoning Issue”

Sid Faber, sfaber@cert.org
2008 OARC Workshop
September 24, 2008



Agenda

- Discovery
- Patch
- Disclosure
- Exploit
- Conclusions

Acknowledgements

This work would not have been possible without assistance from:

- The Security Information Exchange, <https://sie.isc.org> (data)
- Paul Vixie (coordination, validation)
- Duane Wessels (computing resources)
- Chad Dougherty (CERT Vulnerability Analysis)
- Nick Ianelli (CERT Malicious Code)



Discovery

(ssshhhh....)

Timeline

Kaminsky Discovery

- February 2008 (?)

Notification to a small number of interested parties

- 2008.03.19

DNS Summit, 2008.03.31

- Detailed disclosure
- Proposed solution
- Proposed patch date 2008.08.07
- Detailed release date at Blackhat

What is this?

DNS cache poisoning is not a new concept

- Query ID (QID, aka TXID) is only a 16-bit number
- UDP spoofing

Not so much a vulnerability as a new technique:

- Additional resource records (RRs) in the spoofed responses get cached
- Avoid the timeout wait by asking random questions
- Payload is in Additional RRs rather than Answers

What's the (interim) fix?

Increase entropy with a random ephemeral port

- Traditionally most name servers grab a random port at startup and hang on to it for all future queries

Before: guess TrxID: one in 65,536 (2^{16})

After: guess TrxID (2^{16}) and ephemeral port ($\sim 2^{14}$)

Timeline



Vulnerability coordination/response

After DNS summit, CERT begins notifying vendors

- First round: survey message, no details seeking independent DNS implementers
- Second round: detailed technical message and timeline

Roughly 150 vendors contacted

- Vendor communication is performed securely using PGP and our custom internal contact management application

2008.07.08: Announcement and patches released



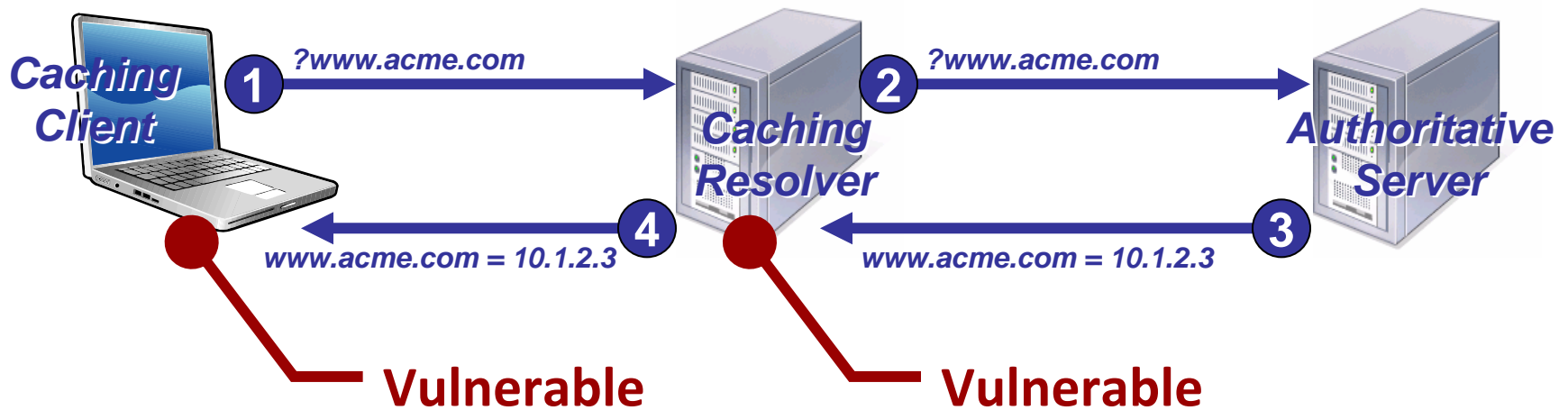
Patch

...and patch, and patch, and patch...

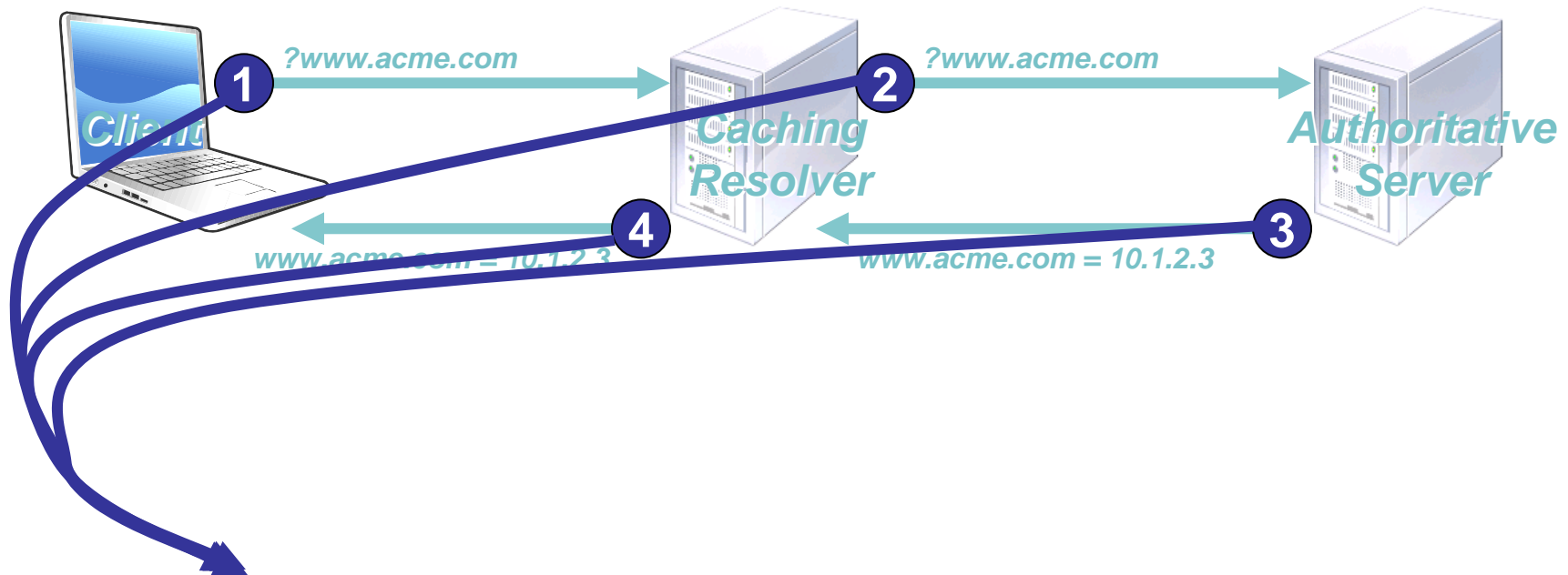
Timeline



Review: Basic DNS Architecture

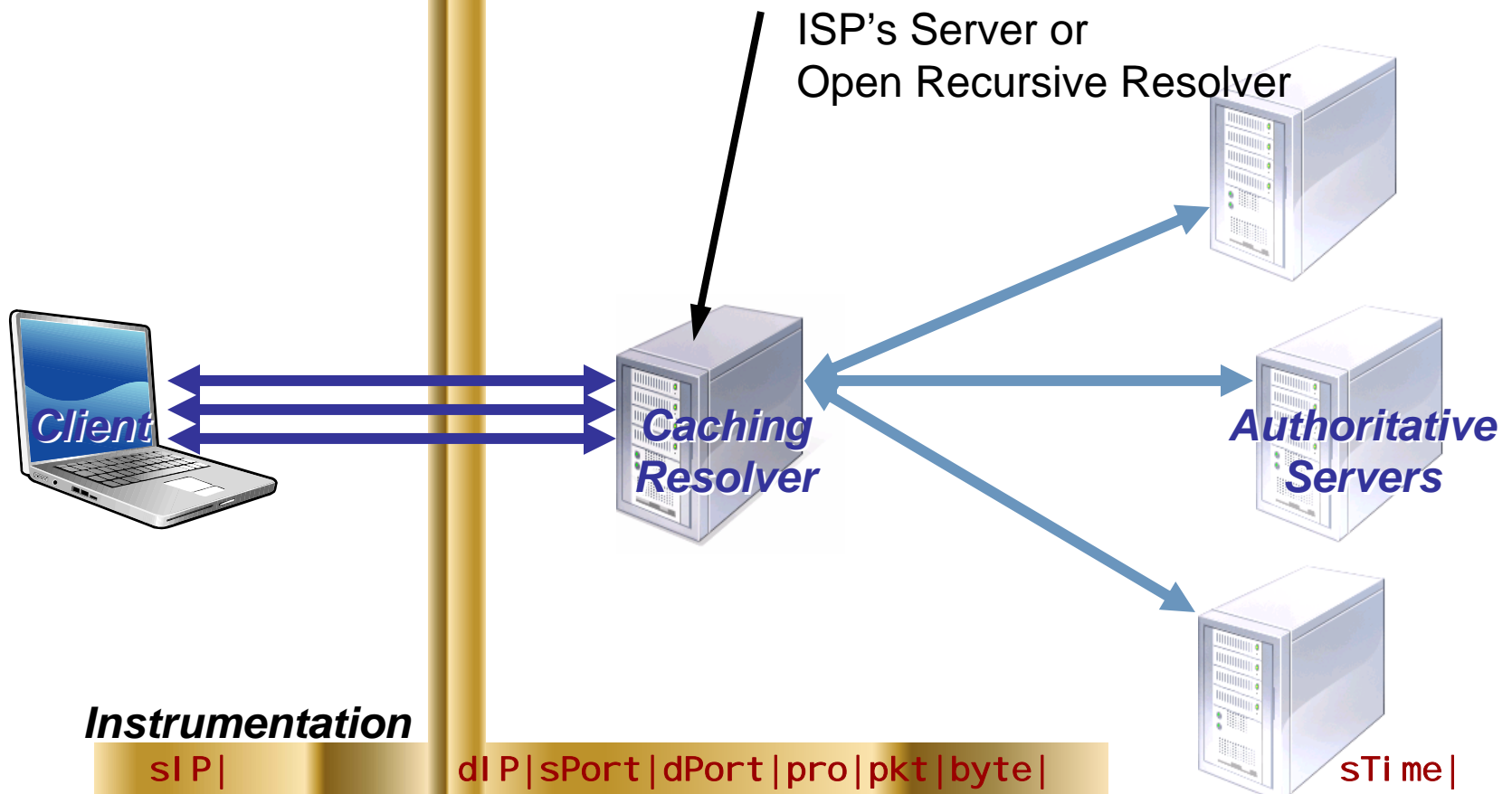


Review: Flow Collection



	sIP	dIP	sPort	dPort	pro	pkt	byte	sTime
(1)	10.254.105.86	186.54.105.135	1027	53	17	1	282	2008/06/11T12:00:02
(2)	186.54.105.135	17.131.109.185	34574	53	17	1	306	2008/06/11T12:00:02
(3)	17.131.109.185	186.54.105.135	53	34574	17	1	554	2008/06/11T12:00:03
(4)	186.54.105.135	10.254.105.86	53	1027	17	1	403	2008/06/11T12:00:03

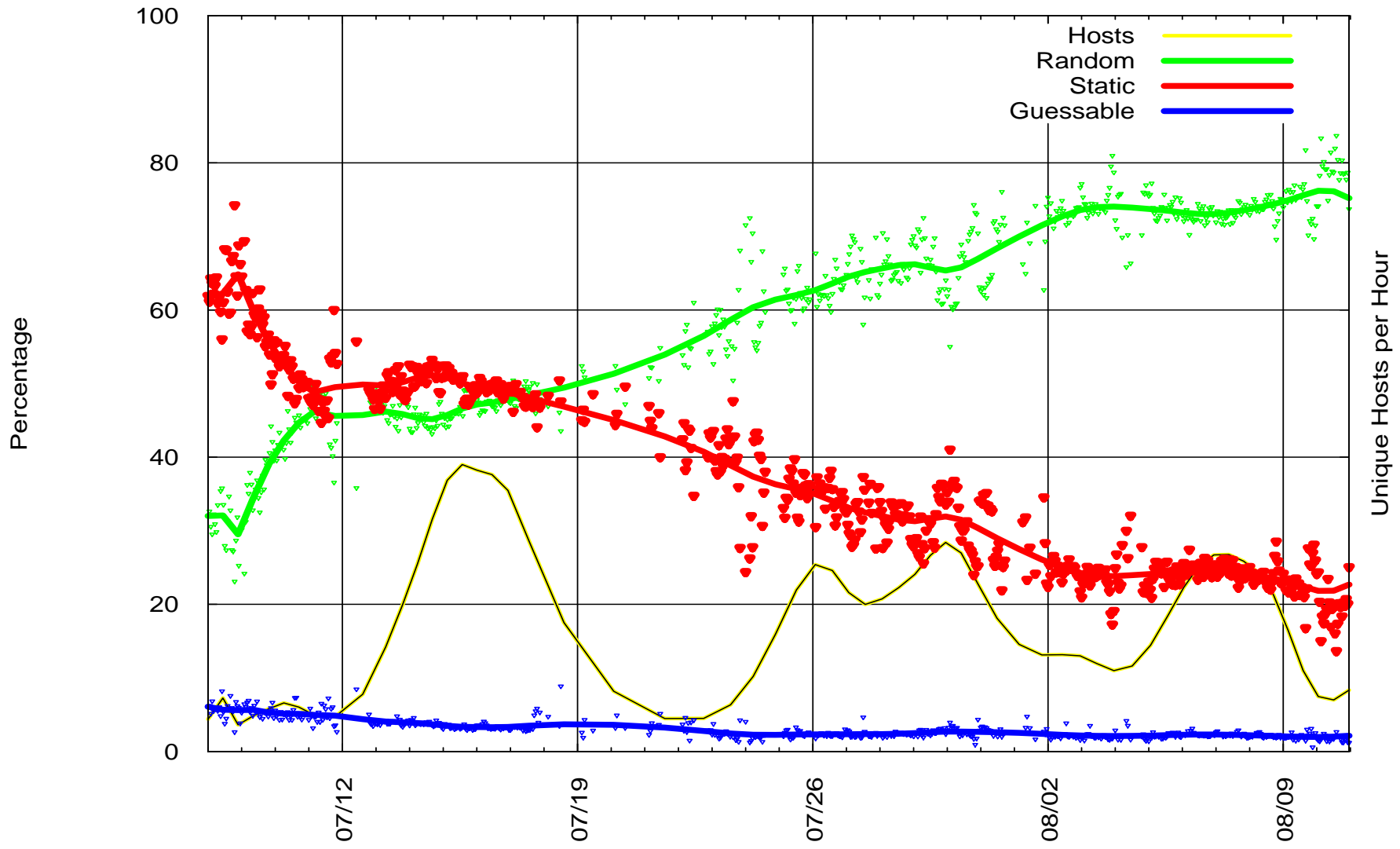
Identifying Unpatched Workstations



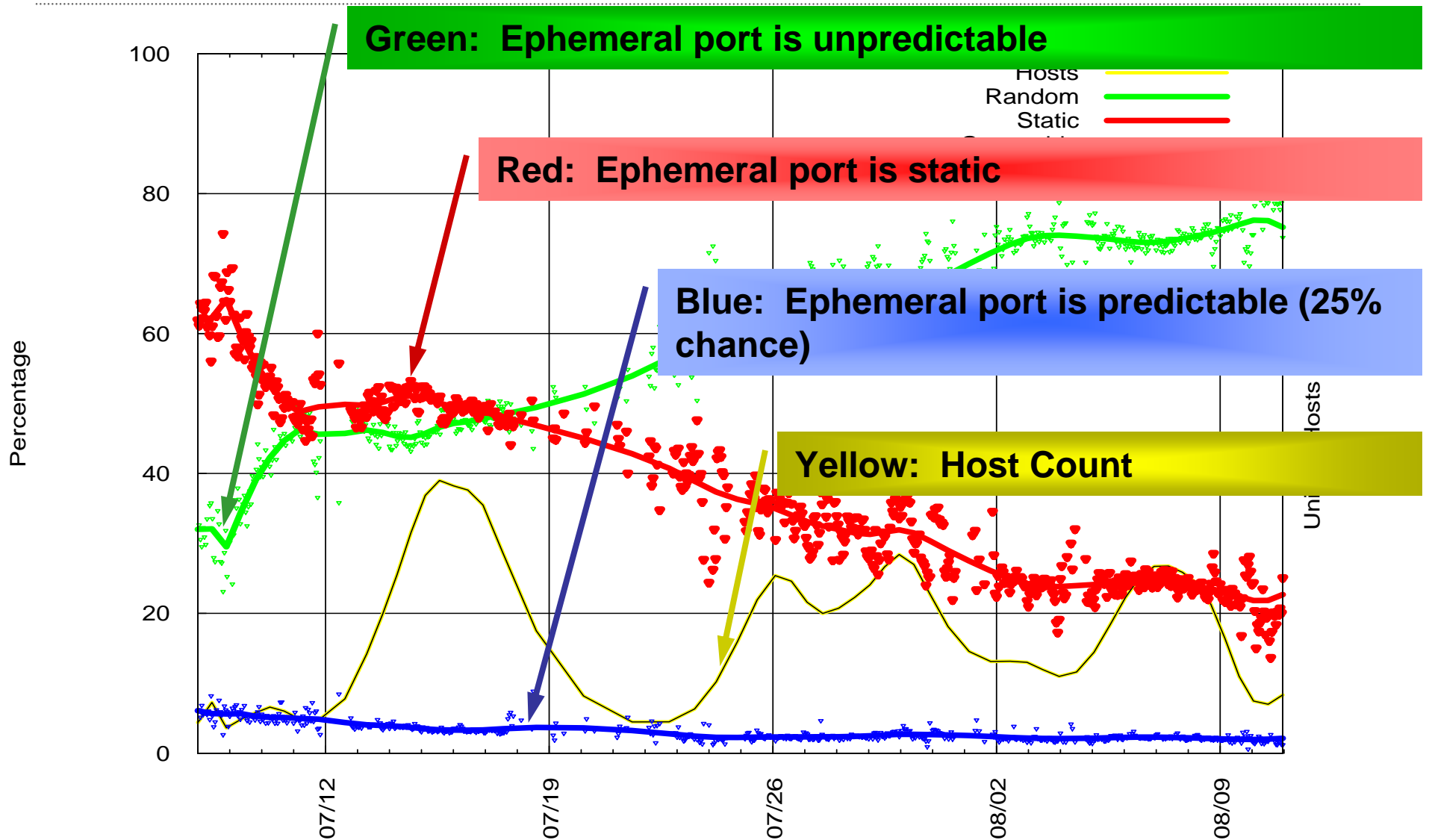
Instrumentation

sIP	dIP	sPort	dPort	pro	pkt	byte	sTime
10.254.105.86	186.54.105.135	1027	53	17	1	282	2008/06/11T12:00:02
10.254.105.86	186.54.105.135	1031	53	17	1	282	2008/06/11T12:00:21
10.254.105.86	186.54.105.135	1032	53	17	1	282	2008/06/11T12:00:21
10.254.105.86	186.54.105.135	1058	53	17	1	282	2008/06/11T12:01:03

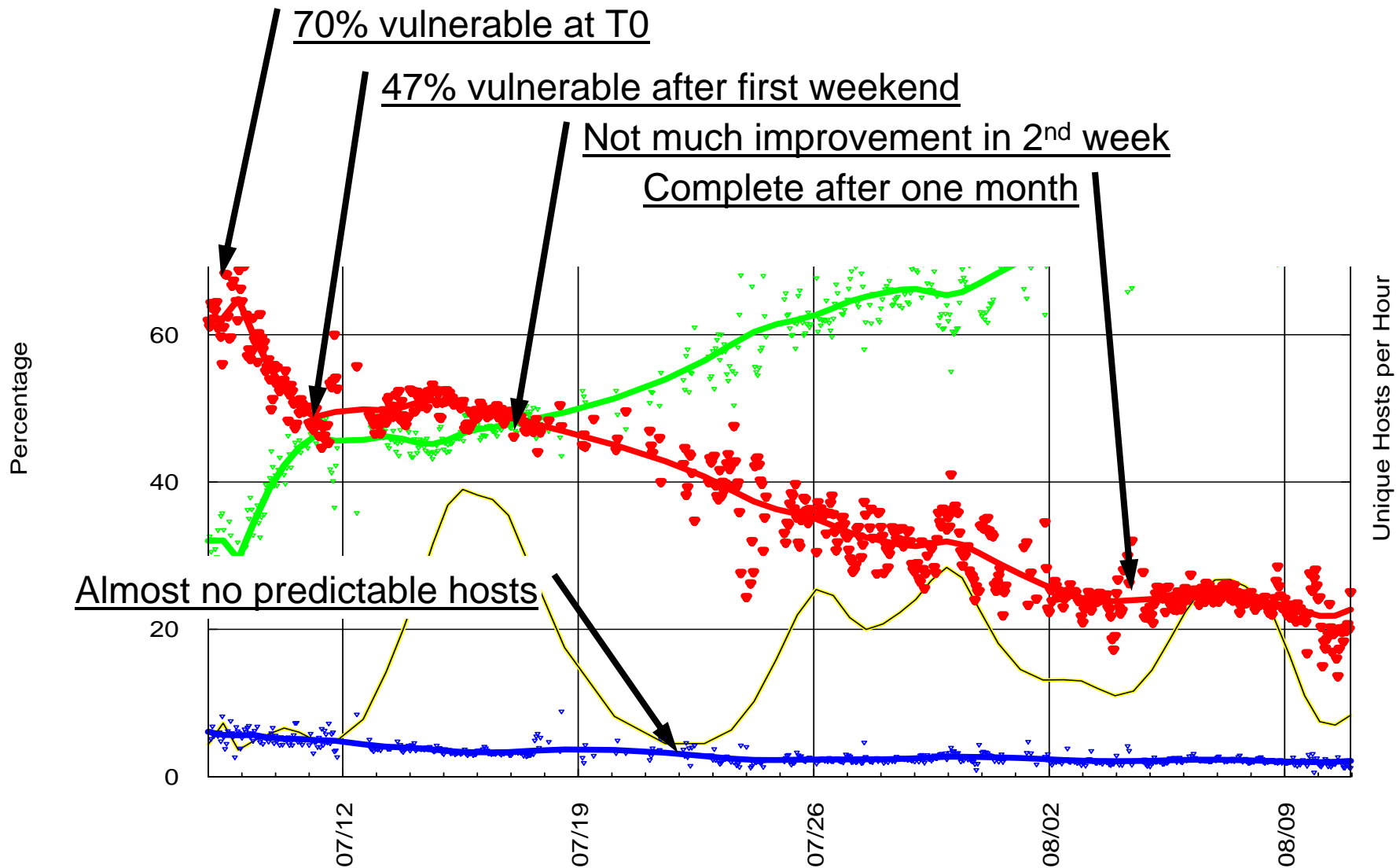
Home User Results



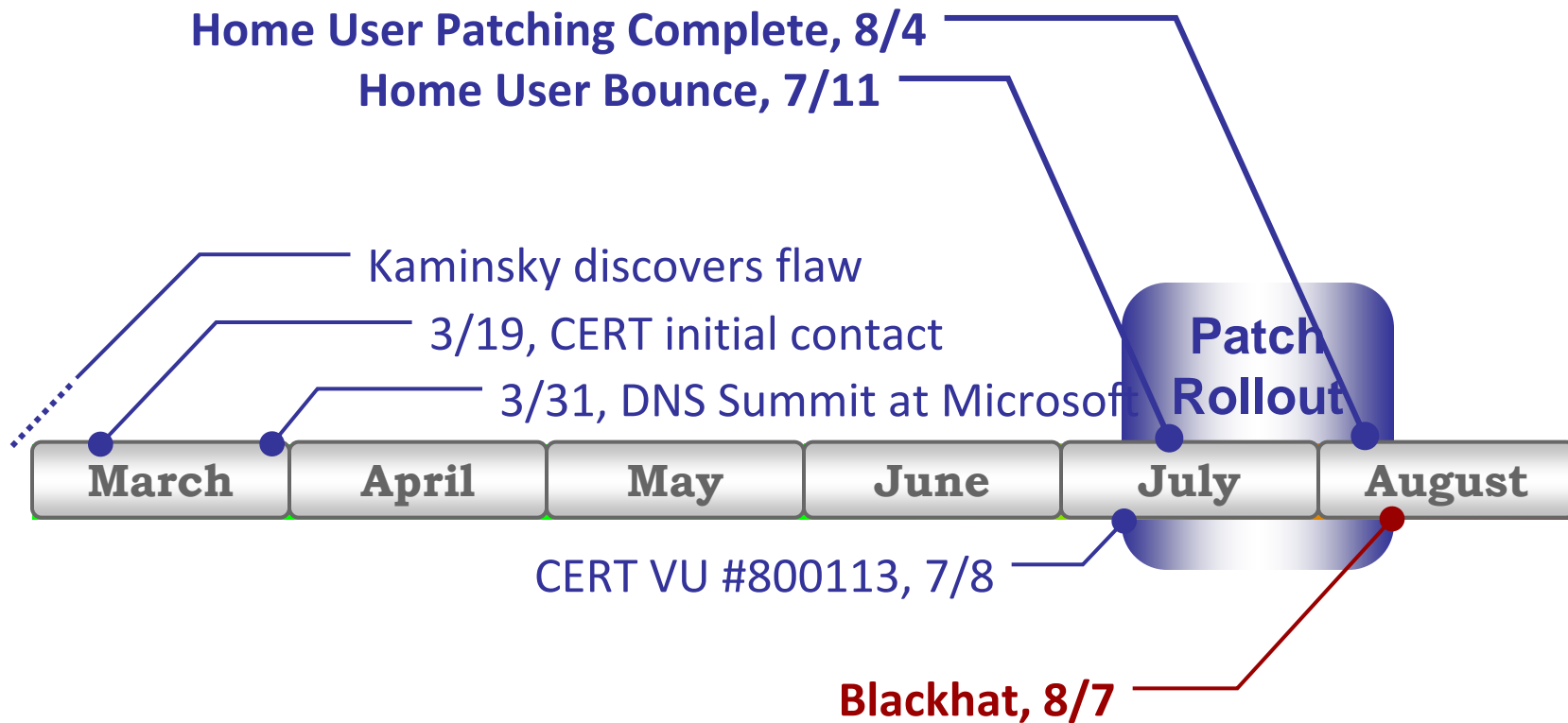
Results Explained



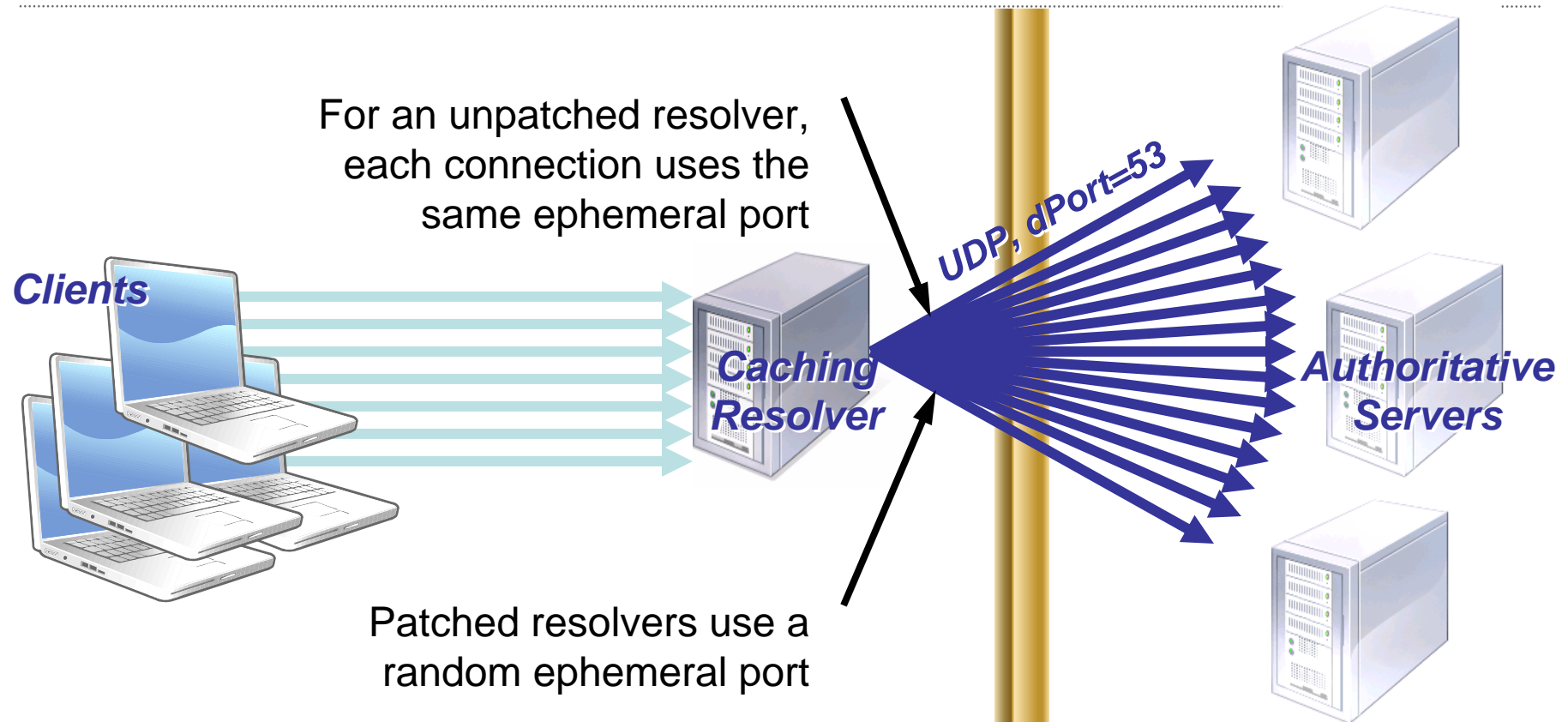
Home User Timeline



Timeline revisited



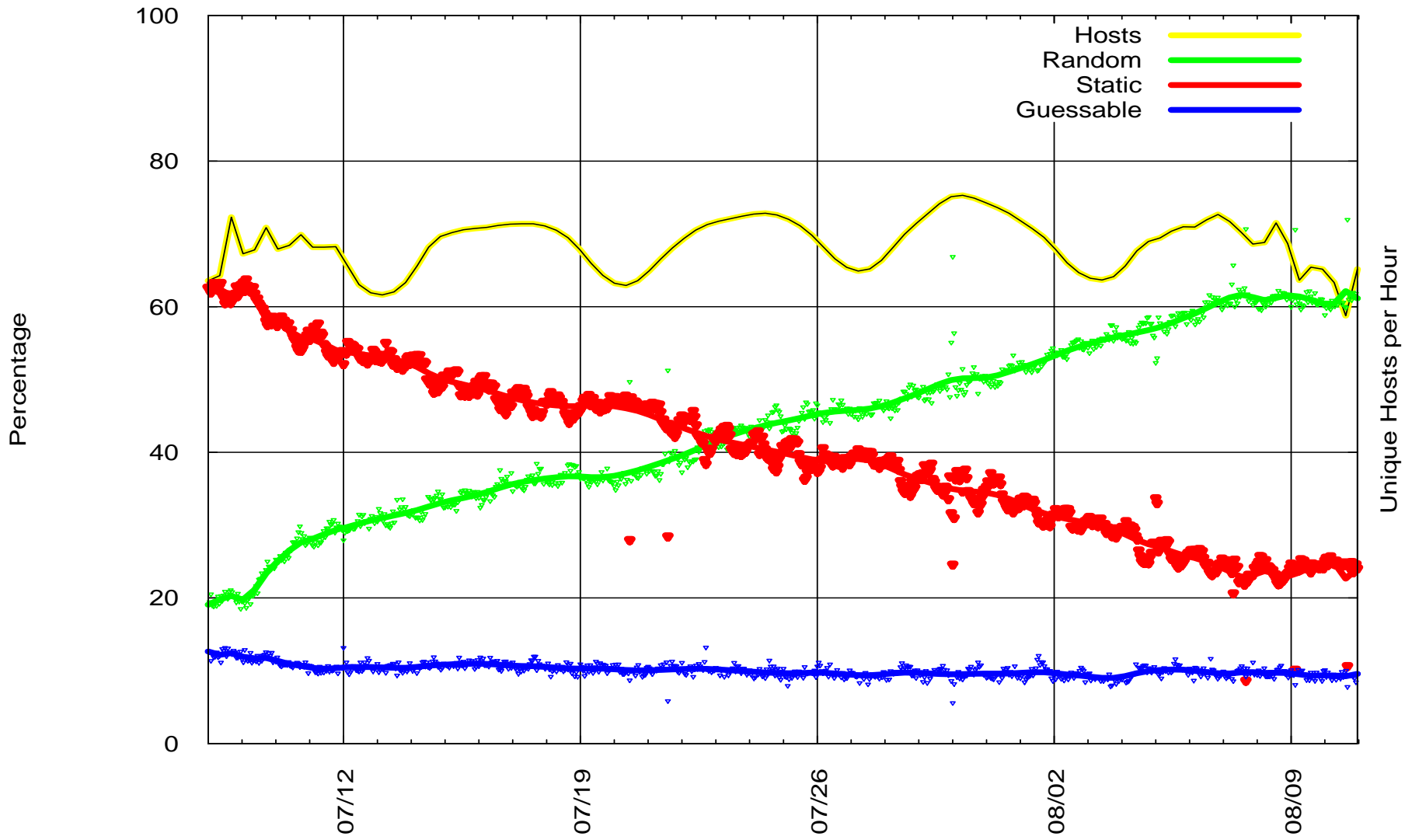
Identifying unpatched servers



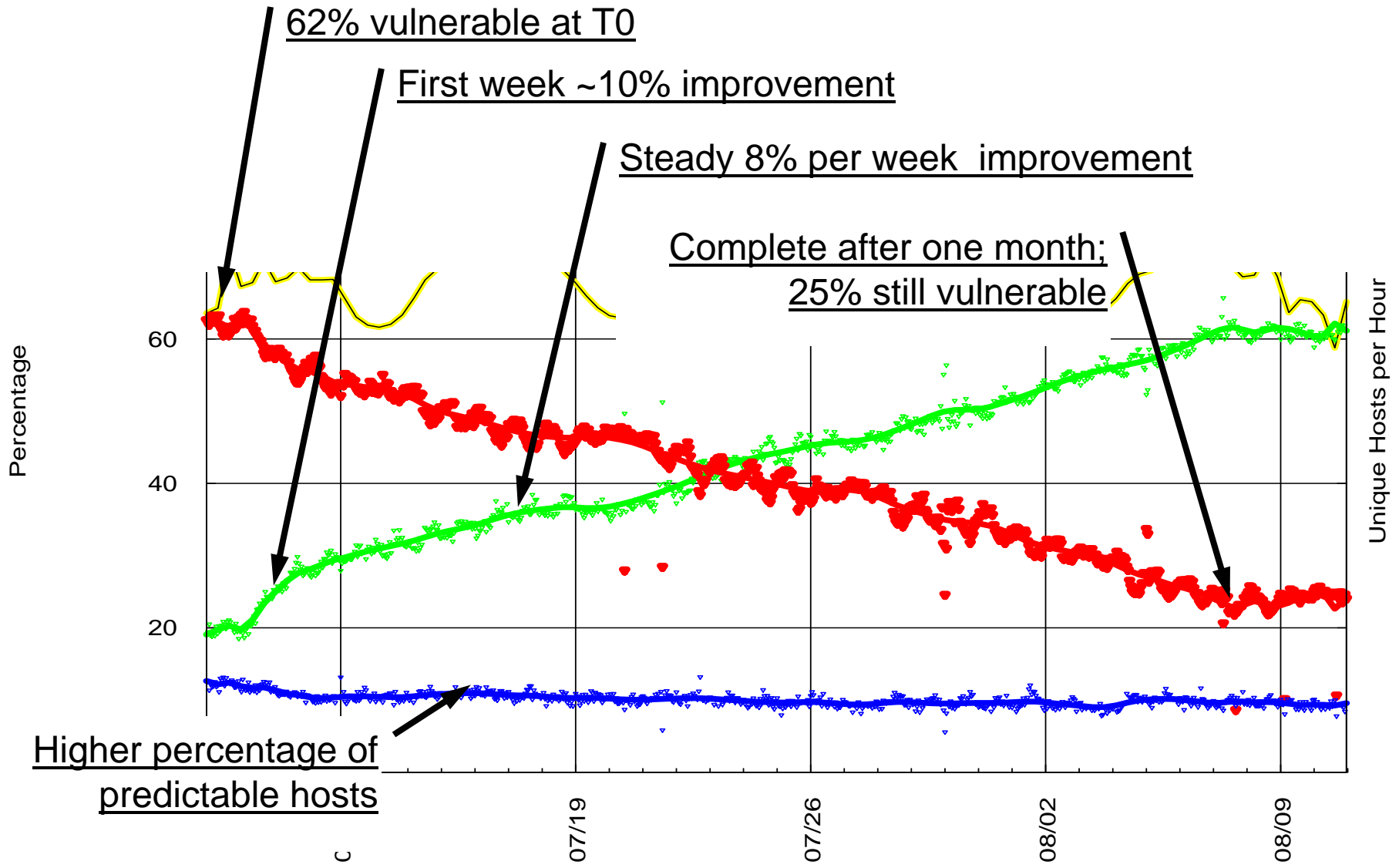
Instrumentation

sIP	dIP	sPort	dPort	pro	pkt	byte	sTime
186.54.105.135	16.64.195.188	32556	53	17	1	282	2008/06/11T12:00:02
186.54.105.135	203.37.75.8	32557	53	17	1	258	2008/06/11T12:00:21
186.54.105.135	114.154.44.64	32558	53	17	1	322	2008/06/11T12:00:21
186.54.105.135	21.87.225.250	32559	53	17	1	196	2008/06/11T12:01:03

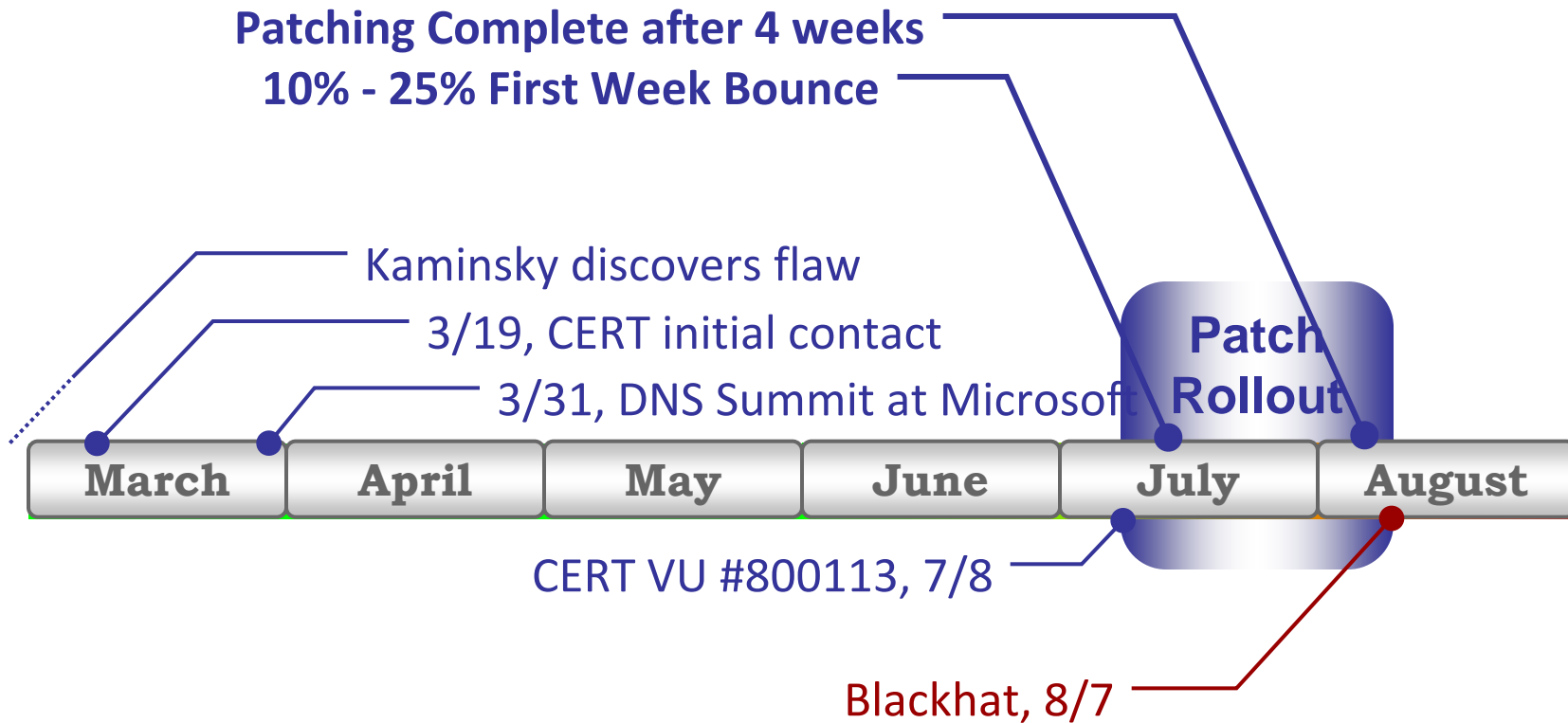
Enclave Server Results



Enclave Server Results (2)



Timeline--including patching





Disclosure

What was that again? Oh, of course...

Reaction to initial release

Posted in an Underground IRC channel (which was talking about marijuana):

- <http://securosis.com/2008/07/08/dan-kaminsky-discovers-fundamental-issue-in-dns-massive-multivendor-patch-released/>
- Reaction: "haha nice"



Is your server vulnerable?

Community tools to test if your server was vulnerable:

- 2008.07.11(OARC) dig +short porttest.dns-oarc.net TXT
- 2008.07.14:
 - <http://www.provos.org/index.php/?archives/42-DNS-and-Randomness.html>
 - <http://www.doxpara.com>



Details disclosed...no...wait...well...umm...

- **2008.07.21:** IRC bot pushes the following URL:
 - [Slashdot] Kaminsky's DNS Attack Disclosed, Then Pulled (it)
- <http://it.slashdot.org/article.pl?sid=08/07/21/2212227>
- **2008.07.22:** The following link is posted in various underground IRC channels:
 - <http://blog.invisibledenizen.org/2008/07/kaminskys-dns-issue-accidentally-leaked.html>

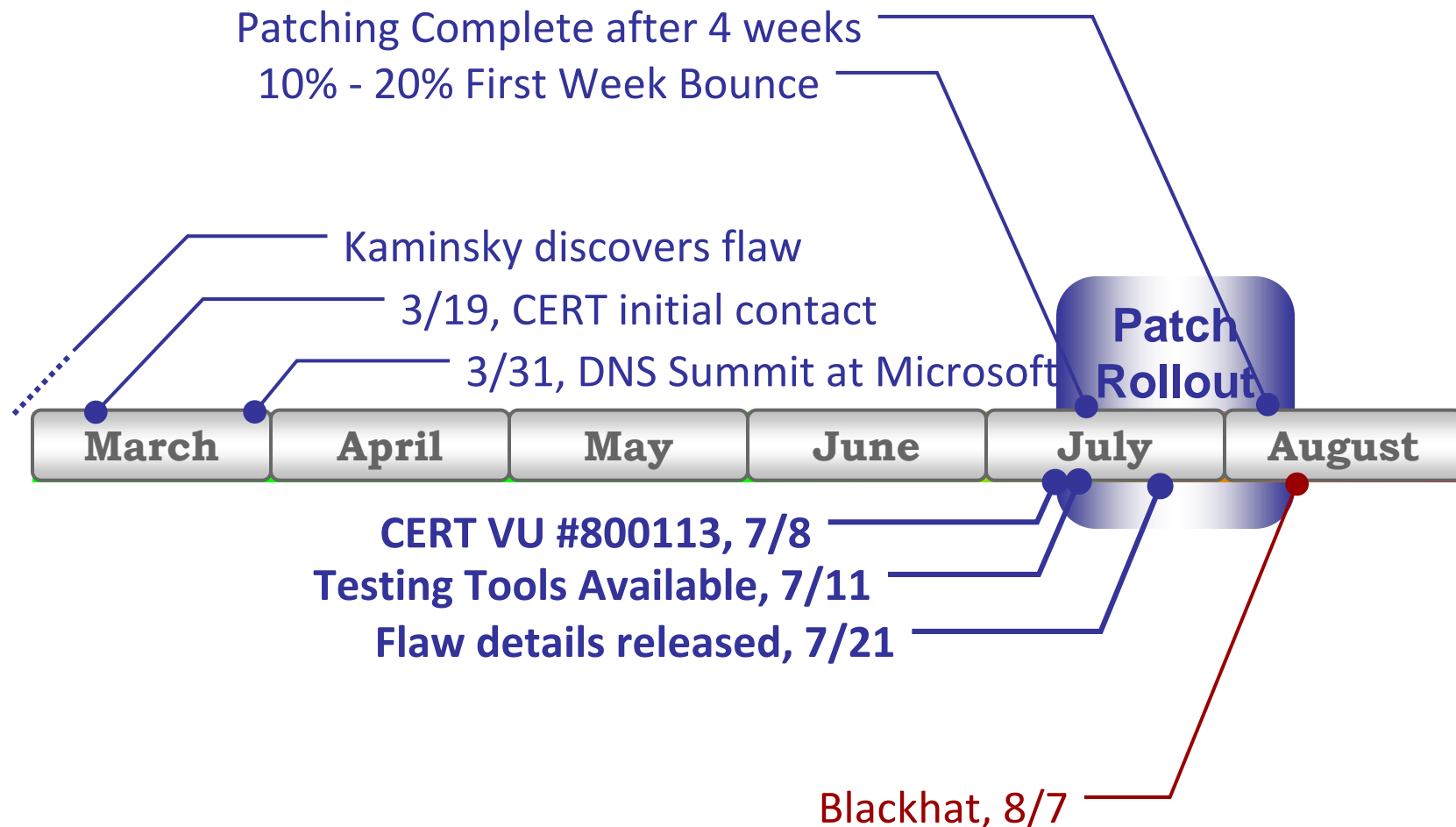


Information in the underground (2)

- **2008.07.22:** In the middle of a discussion the following two items were posted:
 - <http://blog.invisibledenizen.org/2008/07/kaminskys-dns-issue-accidentally-leaked.html>
 - "It seems the cat might be out of the bag regarding Dan Kaminsky's upcoming presentation at Blackhat."
- Link also posted in various underground IRC channels



Timeline--including disclosure





Exploit

*mwa ha ha ha*¹

¹An interjection. Used to denote evilness.

Grant. "mwa ha ha ha ha." *Urban Dictionary*. 22 Feb 2004. 17 Sep 2008.

<<http://www.urbandictionary.com/define.php?term=mwa%20ha%20ha%20ha%20ha>>

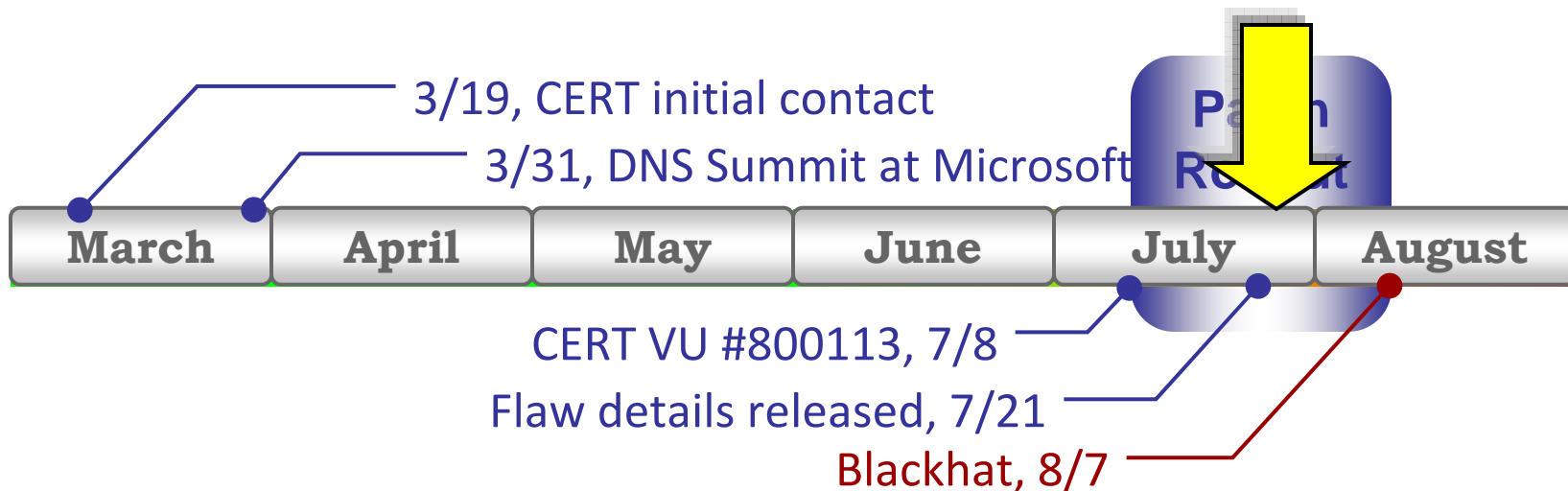
Publicly available exploits

- **2008.07.23:** Metasploit
 - Two days after details released
 - Part of the Metasploit framework
 - <http://www.caughq.org/exploits/CAU-EX-2008-0002.txt>
 - Posted on various Underground IRC channels on **2008.07.27** and **2008.08.09**



Publicly available exploits (2)

- **2008.07.24:** Metasploit v2
 - <http://www.caughq.org/exploits/CAU-EX-2008-0003.txt>
 - Primary difference: NS injection
 - Part of the Metasploit framework



Publicly available exploits (3)

- **2008.07.24:** milw0rm
 - <http://www.milw0rm.com/exploits/6130>
 - C based exploit



Publicly available exploits (4)

- **2008.07.28:** Evilgrade
 - Evilgrade framework includes DNS cache poisoning
 - URL picked up on some underground IRC Channels:

<http://www.infobyte.com.ar/down/isr-evilgrade-Readme.txt>



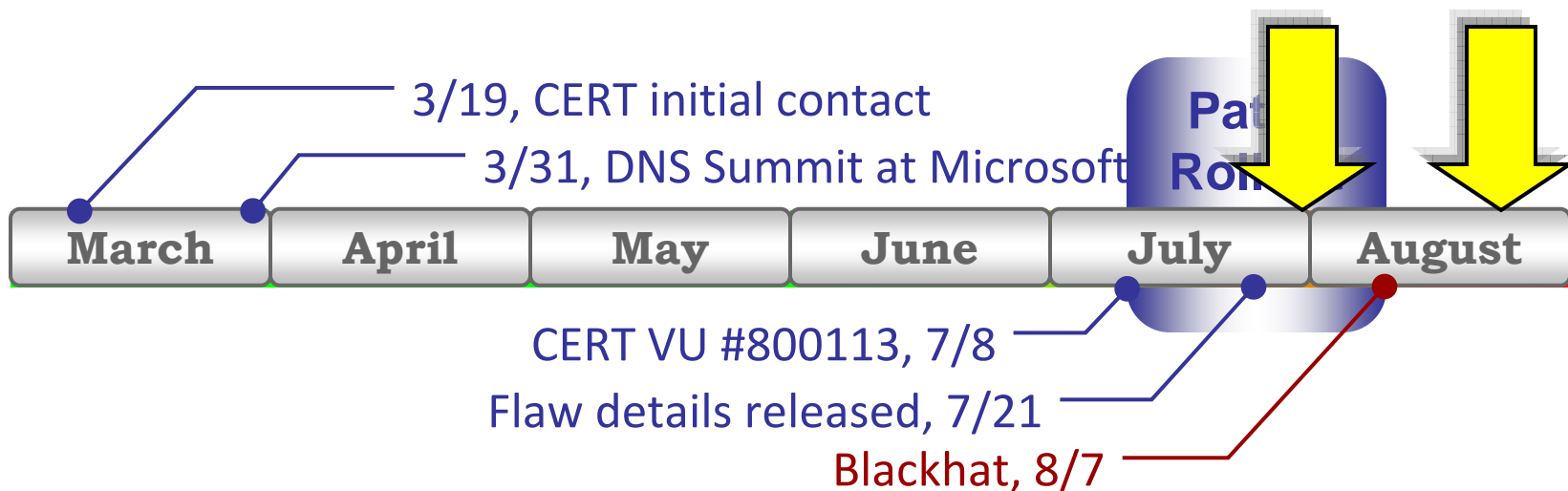
Publicly available exploits (5)

- **2008.08.04:** adns
 - Asynchronous-capable DNS client library and utilities
 - Two weeks following detailed disclosure
 - Minor DNS utility, yet enough of a following to generate an exploit

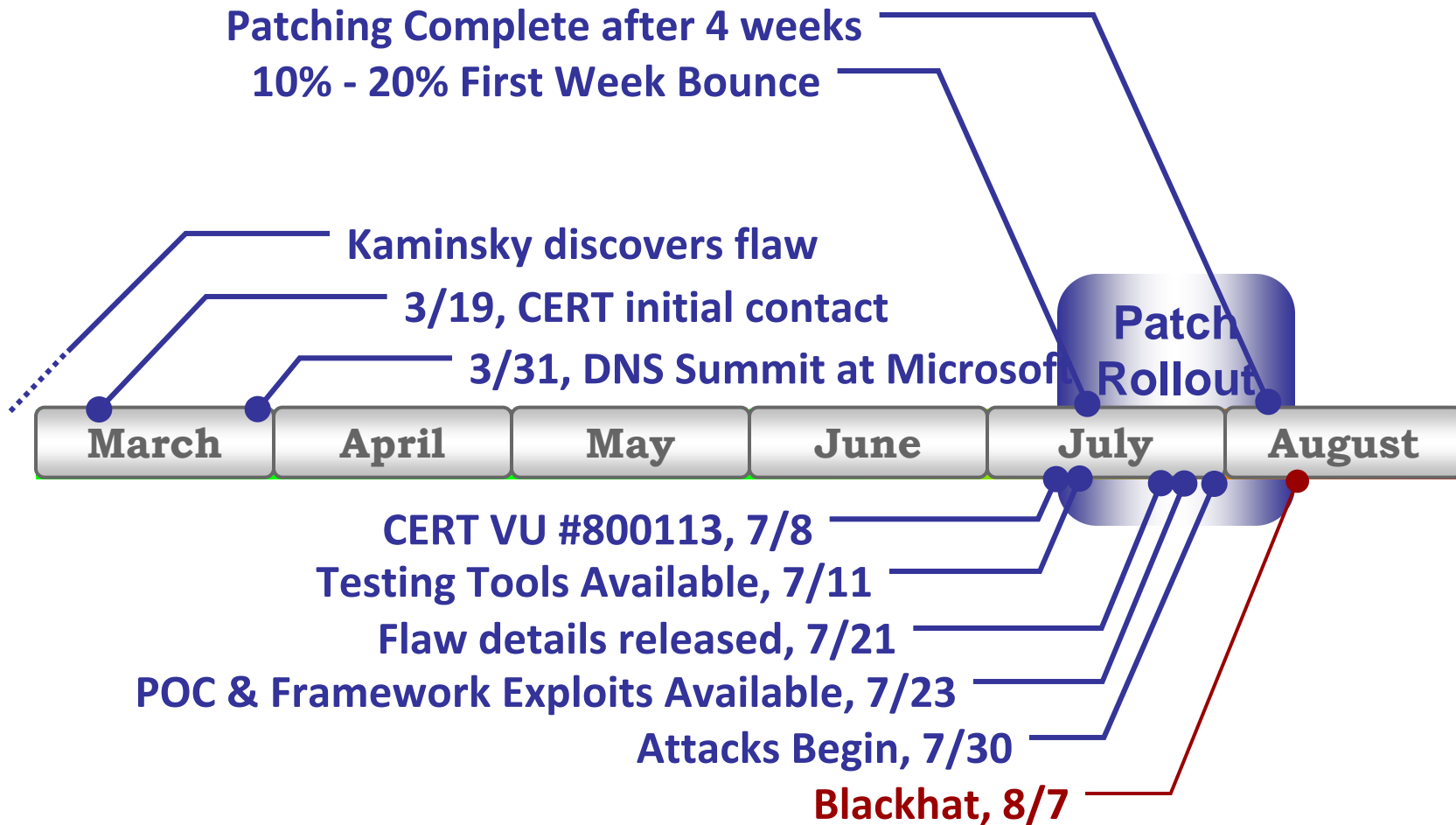


We have attacks!

- **2008.07.30**
 - Confirmation obtained that sites are compromised via DNS Cache poisoning attacks
 - A full week after exploits were available
- **2008.08.21**
 - DNS cache flaw used to poison Chinese ISP's server



Timeline Yet Again



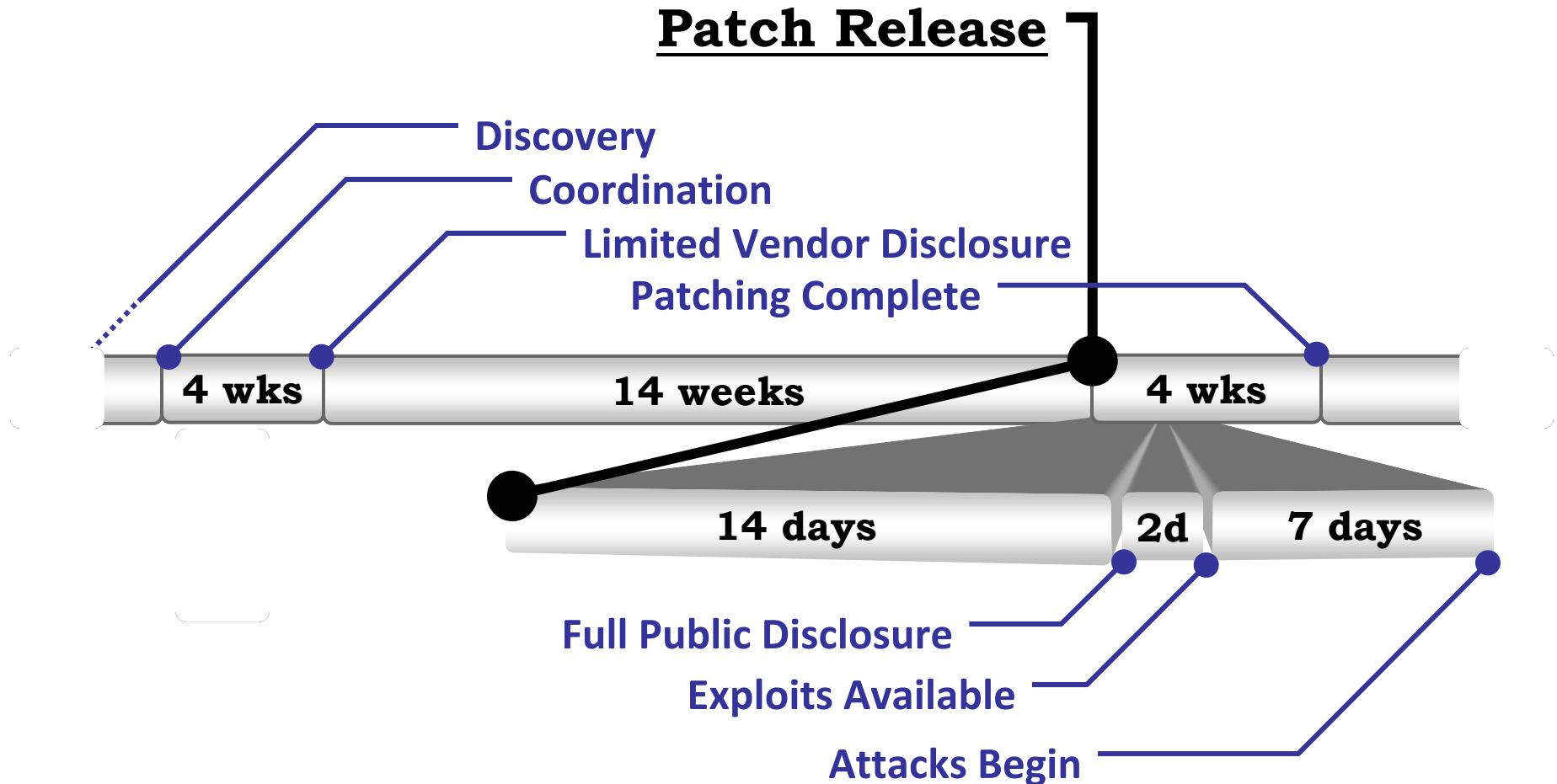


Conclusions

Gee, I think I already knew that...

Perhaps two timelines?

Patch Release



Specific Observations

Timeline

- Extended time between private disclosure and patch only added minimal risk
- Proposed 30-day window between patch and disclosure was sufficient
- Early disclosure caused attacks before patch rollout had been completed

Who has patched?

- 20-25% remained vulnerable
- 5-10% impacted by “gateway” issue

General Conclusions

Responsible Disclosure Worked

- Despite publicity, only 10-20% of machines patched within a week
- Within a month, most patches had been applied
- Critical milestone / warning sign for risk management is detailed disclosure
- There's still some time between disclosure and attack.

There's nothing really new here, just a quantitative confirmation of past qualitative observations.



Responsible Disclosure

A Case Study of CERT VU#800133, “DNS Cache Poisoning Issue”

Sid Faber, sfaber@cert.org
2008 OARC Workshop
September 24, 2008



For More Information

Visit the CERT® web site

<http://www.cert.org/>

Contact Presenter

Sid Faber, sfaber@cert.org

Contact CERT

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890

Hotline:

412-268-7090

CERT/CC personnel answer 8:00 a.m.–5:00 p.m.
and are on call for emergencies during other hours.

Fax:

412-268-6989

E-mail:

cert@cert.org