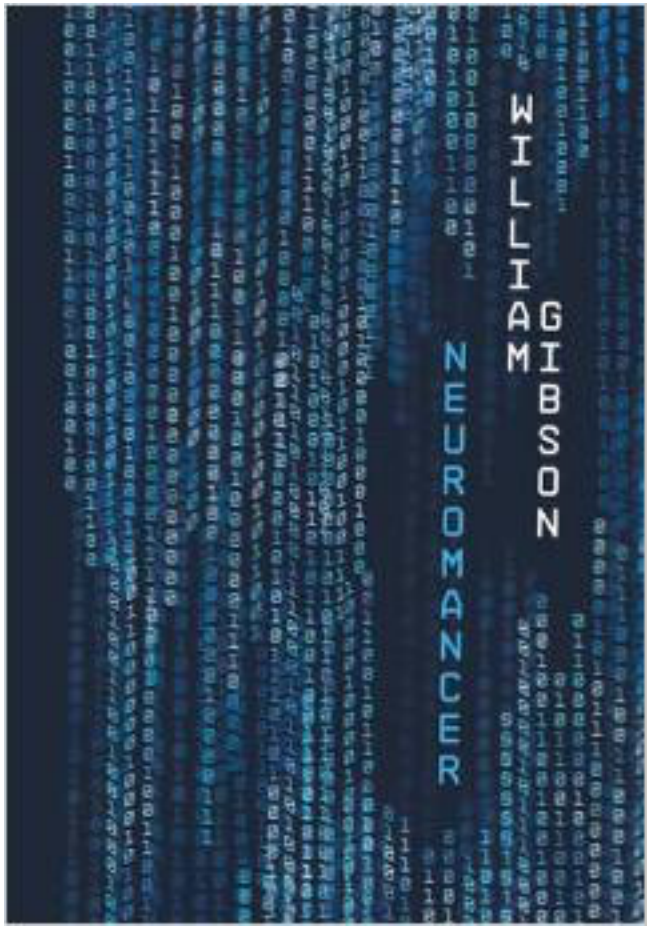
Lecture 18 – Worms, Botnets

Michael Bailey
University of Illinois
ECE 422/CS 461 – Spring 2018

The early years: Cyber-Vandalism

”Virus-writers seemed, at least at first, to be in it for anything but money. The outcome was simply vandalism...Random strangers were anonymously discommoded. Somewhere, I assumed, someone had a rather abstract giggle.”

– William Gibson, Author of Neuromancer



Worm

- A worm is self-replicating software designed to spread through the network
  - Typically, exploit security flaws in widely used services
  - Can cause enormous damage
    - Launch DDOS attacks, install bot networks
    - Access sensitive information
    - Cause confusion by corrupting the sensitive information
- Worm vs Virus vs Trojan horse
  - A virus is code embedded in a file or program
  - Viruses and Trojan horses rely on human intervention
  - Worms are self-contained and may spread autonomously

Cost of worm attacks

- Morris worm, 1988
  - Infected approximately 6,000 machines
    - 10% of computers connected to the Internet
  - cost ~ $10 million in downtime and cleanup
- Code Red worm, July 16 2001
  - Direct descendant of Morris' worm
  - Infected more than 500,000 servers
    - Programmed to go into infinite sleep mode July 28
  - Caused ~ $2.6 Billion in damages,
- Love Bug worm: $8.75 billion
- Conficker Worm: $9.1 billion

  - Statistics: Computer Economics Inc., Carlsbad, California

Internet Worm (First major attack)

- Released November 1988
  - Program spread through Digital, Sun workstations
  - Exploited Unix security vulnerabilities
    - VAX computers and SUN-3 workstations running versions 4.2 and 4.3 Berkeley UNIX code
- Consequences
  - No immediate damage from program itself
  - Replication and threat of damage
    - Load on network, systems used in attack
    - Many systems shut down to prevent further attack

Code Red

- Initial version released July 13, 2001
  - Sends its code as an HTTP request
  - HTTP request exploits buffer overflow
  - Malicious code is not stored in a file
    - Placed in memory and then run
- When executed,
  - Worm checks for the file C:\Notworm
    - If file exists, the worm thread goes into infinite sleep state
  - Creates new threads
    - If the date is before the 20th of the month, the next 99 threads attempt to exploit more computers by targeting random IP addresses

Manual Code Red Exploit

```
C:\ telnet www.targetsystem.com 80
GET/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucb
d3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u
9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
```

“The vulnerability lies within the code that allows a Web server to interact with Microsoft Indexing Service functionality, which is installed by default on all versions of IIS. The problem lies in the fact that the .ida (Indexing Service) ISAPI filter does not perform proper "bounds checking" on user inputted buffers and therefore is susceptible to a buffer overflow attack.”

-sans.org

Code Red of July 13 and July 19

- Initial release of July 13
  - 1st through 20th month: Spread
    - via random scan of 32-bit IP addr space
  - 20th through end of each month: attack.
    - Flooding attack against 198.137.240.91 (www.whitehouse.gov)
  - Failure to seed random number generator ⇒ linear growth
- Revision released July 19, 2001.
  - White House responds to threat of flooding attack by changing the address of www.whitehouse.gov
  - Causes Code Red to die for date ≥ 20th of the month.
  - But: this time random number generator correctly seeded

Slides: Vern Paxson

Spread of Code Red

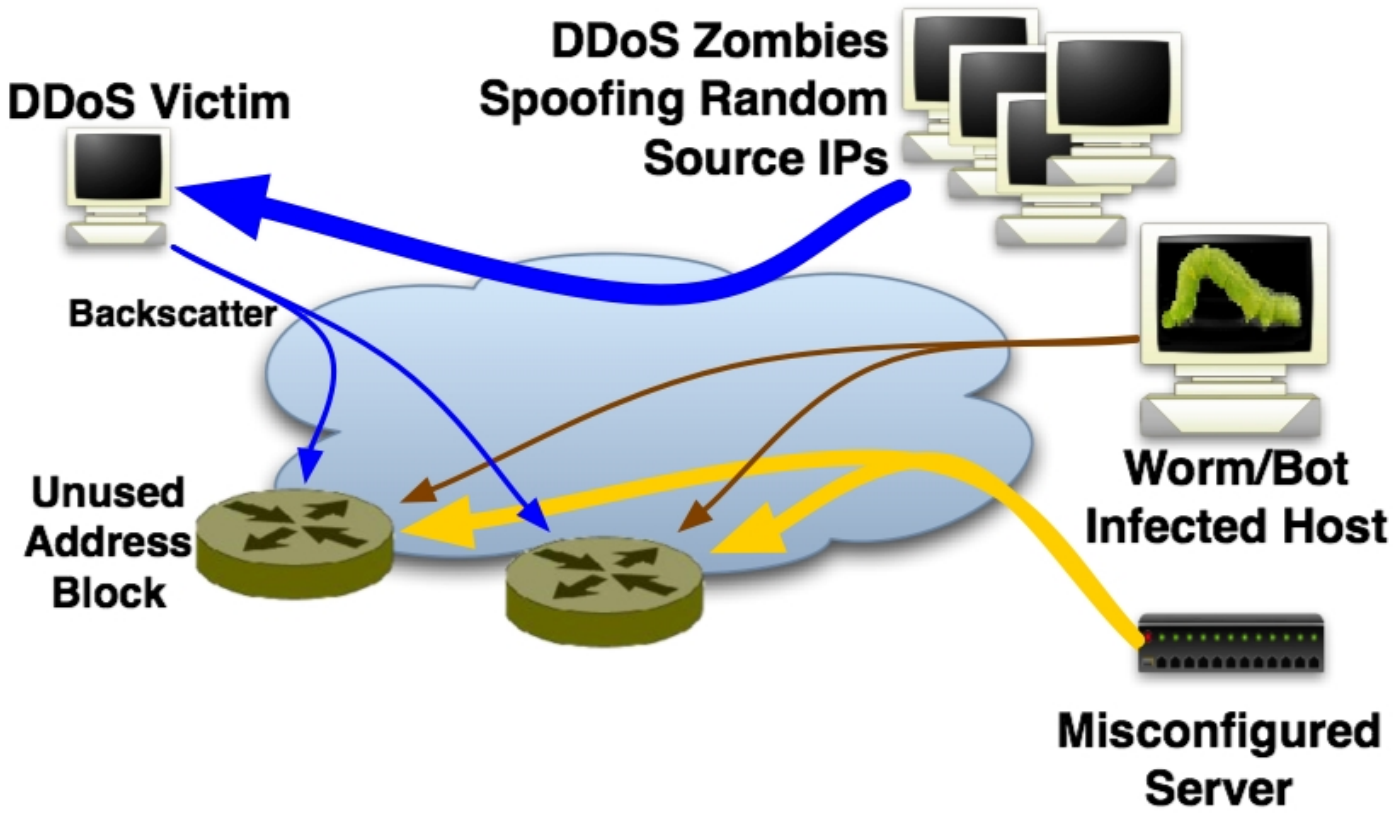
- Network telescopes estimate of # infected hosts: 360K. (Beware DHCP & NAT)
- Course of infection fits classic logistic.
- Note: larger the vulnerable population, faster the worm spreads.

- That night (⇒ 20th), worm dies …

  … except for hosts with inaccurate clocks!
- It just takes one of these to restart the worm on August 1st …

Slides: Vern Paxson

Network Telescopes



- Network telescopes capture this scanning activity (as well as misconfigurations and backscatter) by observing unused addresses.

• Bailey et al., The Internet Motion Sensor - A Distributed Blackhole Monitoring System (NDSS '05)

Code Red 2

- Released August 4, 2001.
- Comment in code: “Code Red 2.”
  - But in fact completely different code base.
- Payload: a root backdoor, resilient to reboots.
- Bug: crashes NT, only works on Windows 2000.
- Localized scanning: prefers nearby addresses.

- Kills Code Red 1.

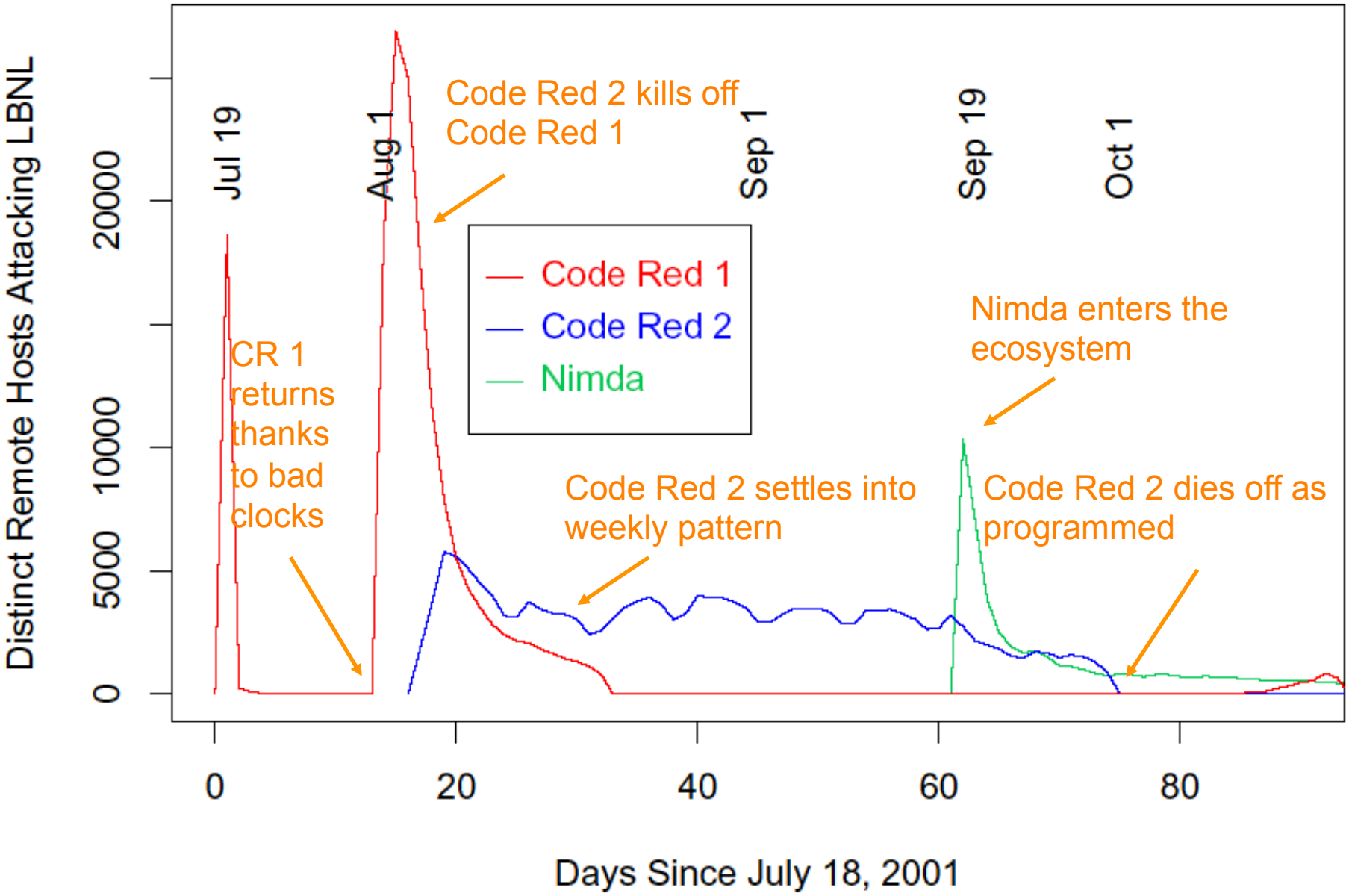
- Safety valve: programmed to die Oct 1, 2001.

Slides: Vern Paxson

Striving for Greater Virulence: Nimda

- Released September 18, 2001.
- Multi-mode spreading:
  - attack IIS servers via infected clients
  - email itself to address book as a virus
  - copy itself across open network shares
  - modifying Web pages on infected servers w/ client exploit
  - scanning for Code Red II backdoors (!)
- worms form an ecosystem!
- Leaped across firewalls.

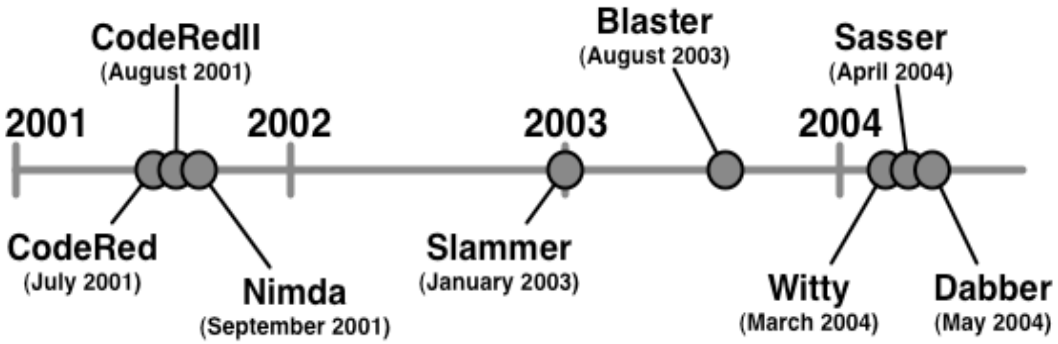
Slides: Vern Paxson



Slides: Vern Paxson

Early Worms

Worm	CodeRedII	Nimda	Sapphire	Blaster	Witty	Sasser	Dabber
Vulnerability	Index Server ISAPI Extension	Unicode Web Traversal CodeRedII Backdoor Open Shares	MS SQL Server 2000 and MSDE2000	DCOM RPC	ISS/PAM ICQ module	LSASS (MS04-011)	Sasser-FTP
Infected Hosts	Millions	Millions	Hundreds of Thousands	Hundreds of Thousands	Tens of Thousands	Tens of Thousands	Thousands
Ports	TCP/80	TCP/80 TCP/25 TCP/137-139,445	UDP/1434	TCP/135	UDP/4000 (src)	TCP/445	TCP/5554



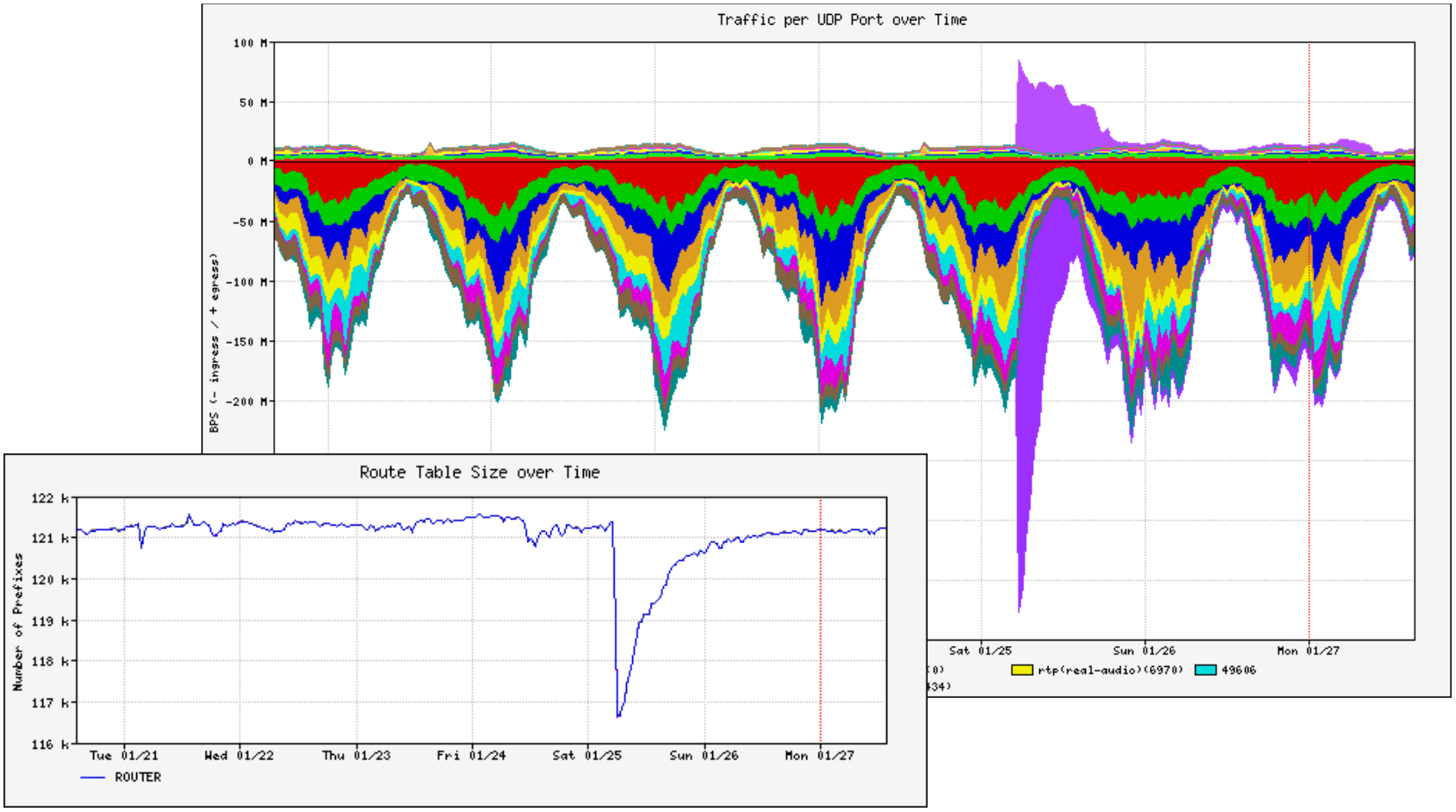
How do worms propagate?

- Scanning worms : Worm chooses “random” address
- Coordinated scanning : Different worm instances scan different addresses
- Flash worms
  - Assemble tree of vulnerable hosts in advance, propagate along tree
    - Not observed in the wild, yet
    - Potential for 106 hosts in < 2 sec ! [Staniford]
- Meta-server worm :Ask server for hosts to infect (e.g., Google for “powered by phpbb”)
- Topological worm: Use information from infected hosts (web server logs, email address books, config files, SSH “known hosts”)
- Contagion worm : Propagate parasitically along with normally initiated communication

Sherman, Set the Way Back Machine to 2000

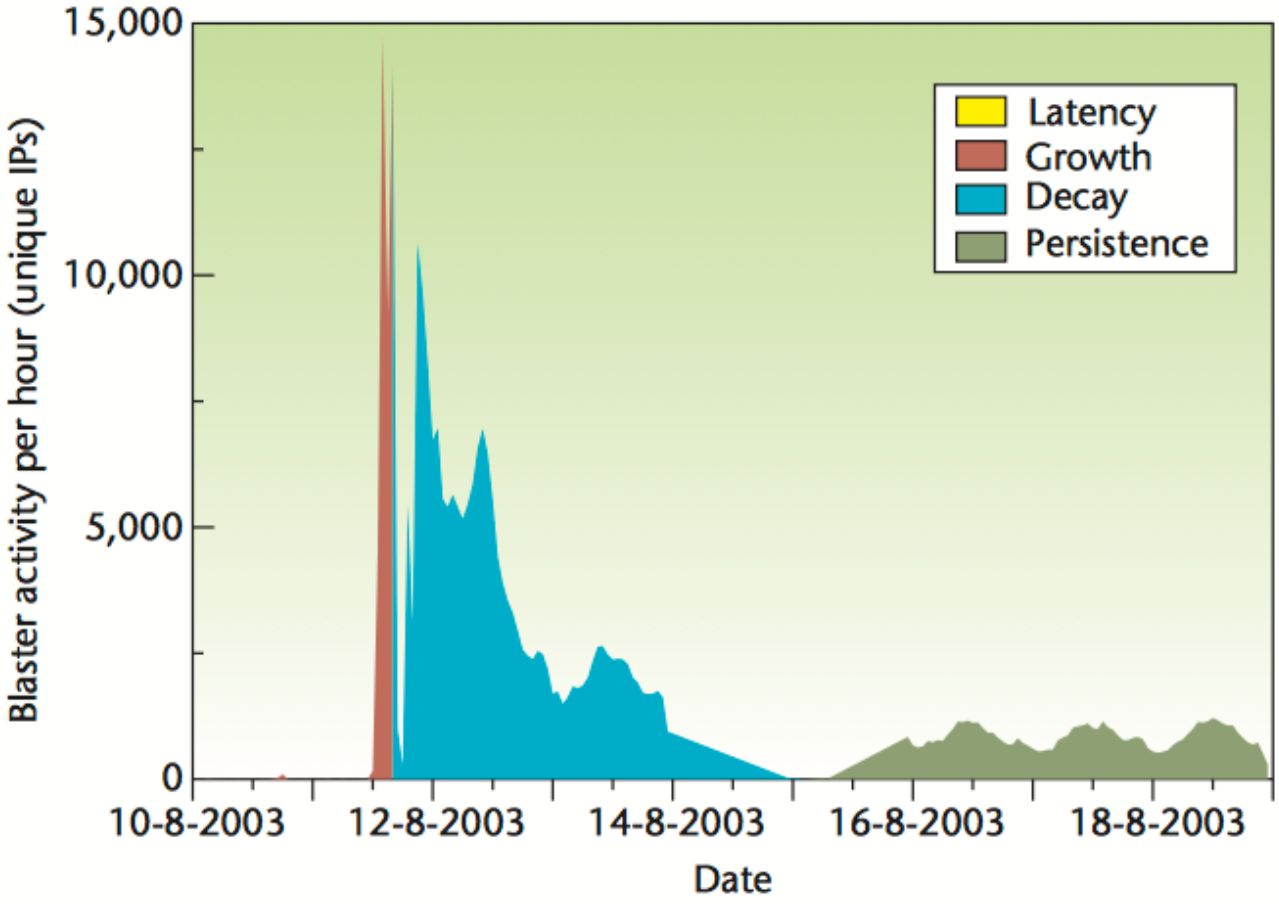
- **Globally scoped**, respecting no geographic or topological boundaries.
  - At peak, 5 Billion infection attempts per day during Nimda including significant numbers of sources from Korea, China, Germany, Taiwan, and the US. [Arbor Networks, Sep. 2001]
- Exceptionally **virulent**, propagating to the entire vulnerable population in the Internet in a matter of minutes.
  - During Slammer, 75K hosts infected in 30 min. [Moore et al, NANOG February, 2003]
- **Zero-day** threats, exploiting vulnerabilities for which no signature or patch has been developed.
  - In Witty, "victims were compromised via their firewall software the day after a vulnerability in that software was publicized”

• Bailey et al., The Internet Motion Sensor - A Distributed Blackhole Monitoring System (NDSS ’05)



During Slammer, 75K hosts infected in 30 min.

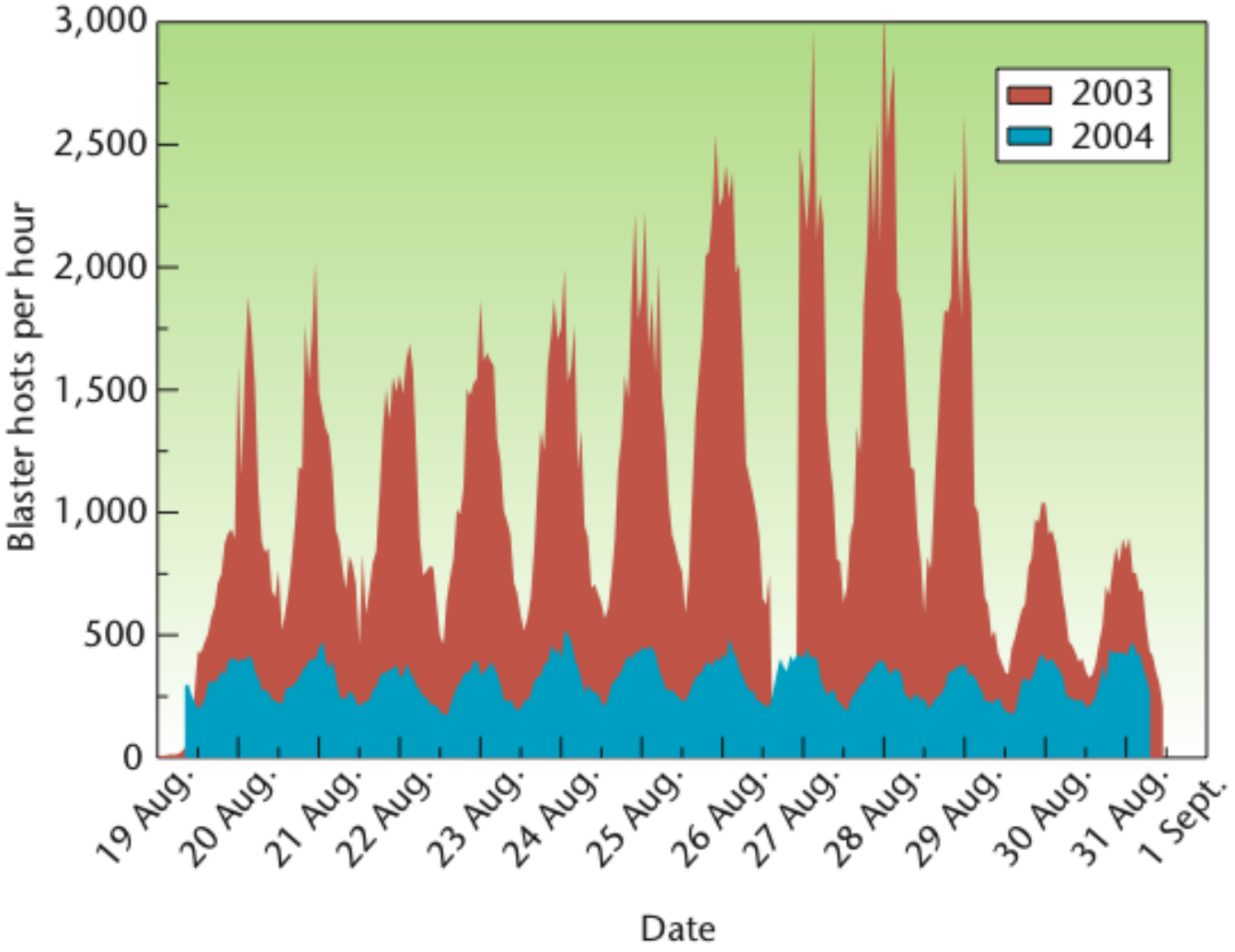
Blaster Worms Lifecycle



- Blaster released on August 11, 2003
- IMS Observed 286K IP addresses
- Doubling every 2.3 hours
- 40,000 hosts/hour
- Half-life = 10.4 hours

• Bailey et al., The Blaster Worm: Then and Now (IEEE S&P '05)

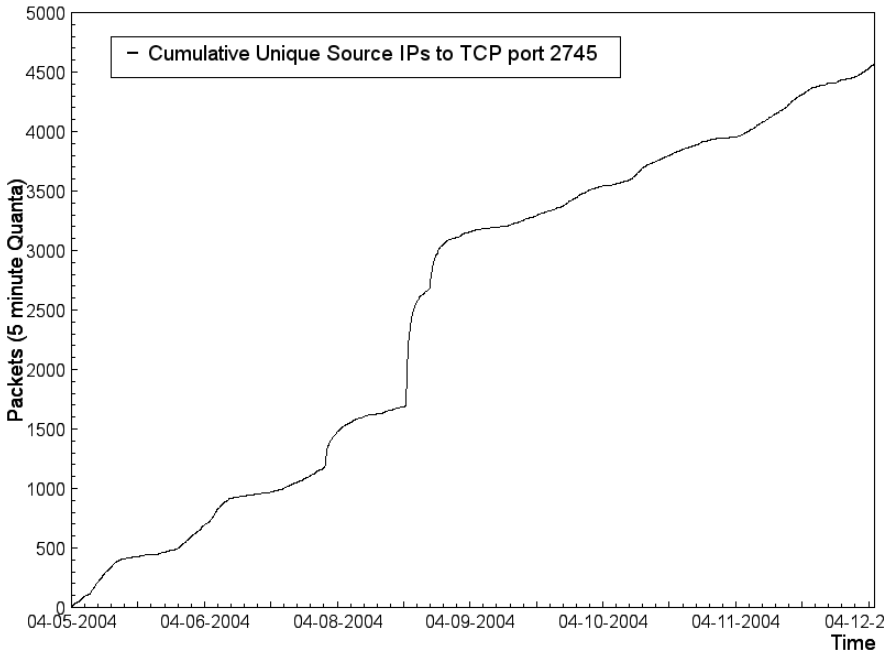
Blaster Worm Cyclic behavior and Persistence



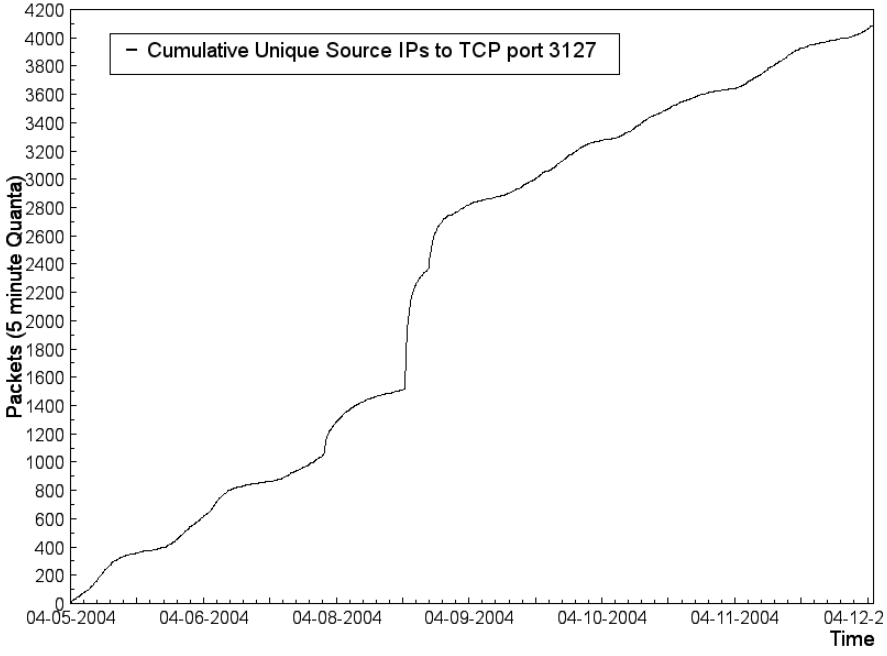
- Infected hosts still probing years later.
- Something interesting was happening here…

Bagle/MyDoom Backdoors

- The backdoors left by viruses like Bagle and MyDoom are being probed



2745 = Bagle.C-G and J-K



3127 = MyDoom.A

Virulent Activity

- This activity is not just benign scans
- People are running programs on these boxes

UPX Packed Binary Payload

```
00000000  85 13 3c 9e a2 4d 5a 90  00 03 00 00 00 04 00 00  |..<..MZ.........|
00000010  00 ff ff 00 00 b8 00 00  00 00 00 00 00 40 00 00  |.............@..|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000040  00 f8 00 00 00 0e 1f ba  0e 00 b4 09 cd 21 b8 01  |.............!..|
00000050  4c cd 21 54 68 69 73 20  70 72 6f 67 72 61 6d 20  |L.!This program |
00000060  63 61 6e 6e 6f 74 20 62  65 20 72 75 6e 20 69 6e  |cannot be run in|
00000070  20 44 4f 53 20 6d 6f 64  65 2e 0d 0d 0a 24 00 00  | DOS mode....$..|
00000080  00 00 00 00 00 df 3e 75  fb 9b 5f 1b a8 9b 5f 1b  |......>u.._..._.|
00000090  a8 9b 5f 1b a8 18 57 46  a8 89 5f 1b a8 f4 40 10  |.._...WF.._...@.|
000000a0  a8 98 5f 1b a8 18 43 15  a8 9e 5f 1b a8 e0 43 17  |.._...C..._...C.|
000000b0  a8 9e 5f 1b a8 f4 40 11  a8 90 5f 1b a8 f4 40 1f  |.._...@..._...@.|
000000c0  a8 9e 5f 1b a8 9b 5f 1a  a8 7d 5f 1b a8 cf 7c 2b  |.._..._..}_...|+|
000000d0  a8 9a 5f 1b a8 cf 7c 2a  a8 a2 5f 1b a8 52 69 63  |.._...|*.._..Ric|
000000e0  68 9b 5f 1b a8 00 00 00  00 00 00 00 00 00 00 00  |h._.............|
000000f0  00 00 00 00 00 00 00 00  00 00 00 00 00 50 45 00  |.............PE.|
00000100  00 4c 01 03 00 2d bc 4f  3e 00 00 00 00 00 00 00  |.L...-.O>.......|
00000110  00 e0 00 0f 01 0b 01 06  00 00 50 01 00 00 10 00  |..........P.....|
00000120  00 00 f0 02 00 d0 45 04  00 00 00 03 00 00 50 04  |......E.......P.|
00000130  00 00 00 40 00 00 10 00  00 00 02 00 00 04 00 00  |...@............|
00000140  00 00 00 00 00 04 00 00  00 00 00 00 00 00 60 04  |..............`.|
...
000001f0  00 00 00 00 00 55 50 58  30 00 00 00 00 00 f0 02  |.....UPX0.......|
00000200  00 00 10 00 00 00 00 00  00 00 04 00 00 00 00 00  |................|
00000210  00 00 00 00 00 00 00 00                           |........|
```

Why?

Wed May 19 23:58:15 EDT 2004

1085025451 00501338 24.150.154.217 4141 > 141.212.123.138 5000 TCP
1085025451 00501360 24.150.154.217 4141 > 141.212.123.138 5000 TCP

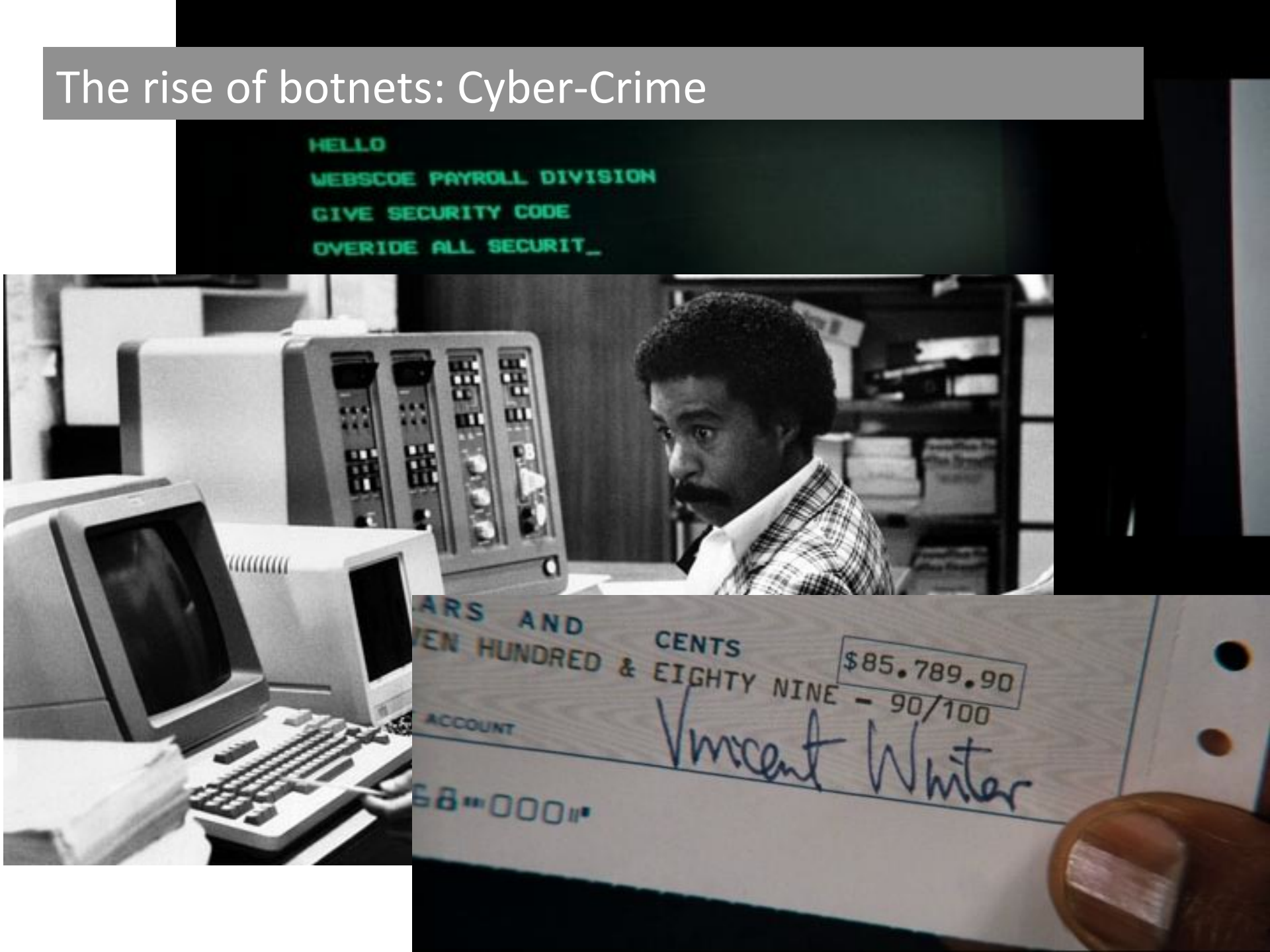
Fri, 21 May 2004 07:19:37 -0400 (EDT)

Received: from d150-154-217.home.cgocable.net (d150-154-217.home.cgocable.net [\
24.150.154.217])
by crimelabs.net (Postfix) with SMTP id 78299DEDB
for <XXX>; Fri, 21 May 2004 07:19:37 -0400 (EDT)
Received: from 24.150.154.217 by 88.10.208.96 Fri, 21 May 2004 11:10:57 -0100
Message-ID: <qfmibfhpnvjAaKznbMPJRT1laK@hotmail.com>
From: "abolish" <Alphonsozyhs@msn.com>
Reply-To: "abolish" <Alphonsozyhs@msn.com>
To: XXX
Subject: this is what you asked for

Attacker Ah Ha! Moment

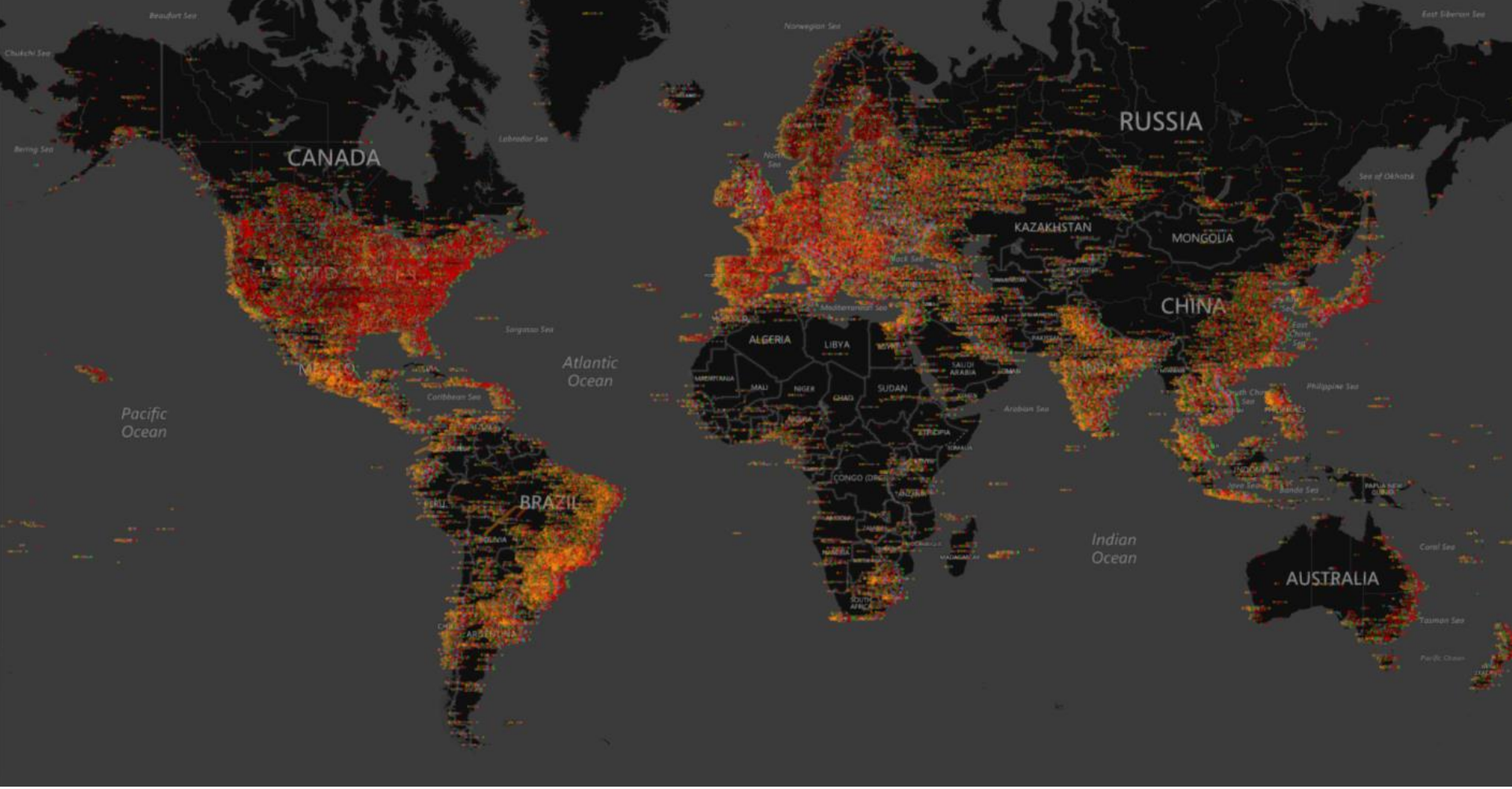
- A compromised system is more useful alive than dead!
- A compromised system provides anonymity
- A network of compromised hosts provides a powerful delivery platform

The rise of botnets: Cyber-Crime



The rise of botnets: Cyber-Crime

- "3. Protect the United States against cyber-based attacks and high-technology crimes"
  - US Federal Bureau of Investigation (FBI)'s website listing cyber crime as the FBI's third highest priority behind such dramatic threats as counter- terrorism and counter-espionage.
- The annual loss due to computer crime was estimated to be $67.2 billion for U.S. organizations, according to a 2005 Federal Bureau of Investigation (FBI) survey.



Botnets represent today's attack platform

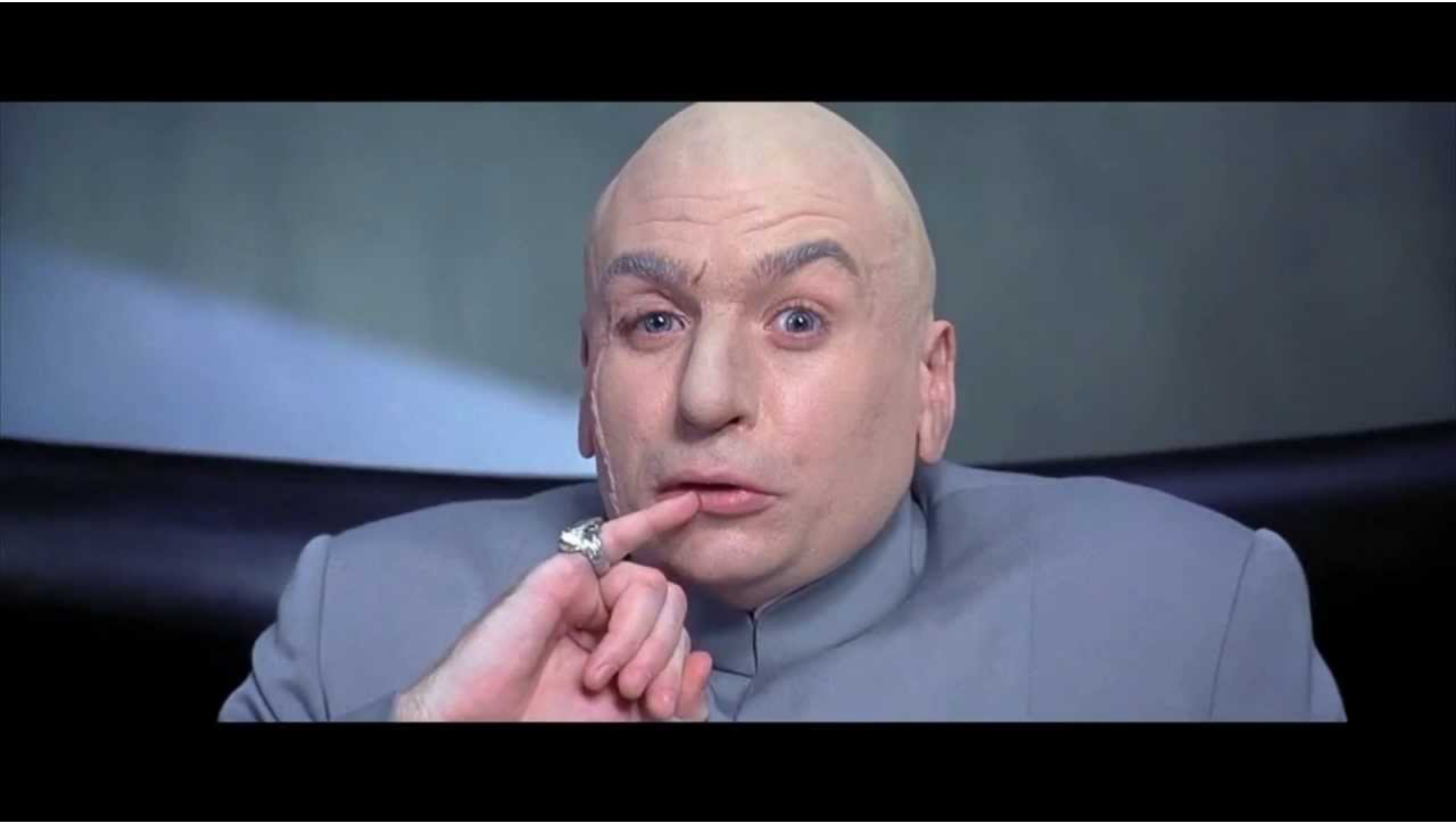
- DoS Extortion, Identity Theft, Phishing, SPAM, Spyware

What's a "botnet"?

- A bot is a servant process on a compromised system
- Usually installed by a trojan, though worms have evolved to install bots as well (e.g., deloder)
- Communicates with a handler or controller, often running on public IRC servers or other compromised systems
- Almost always unbeknownst to the systems owner - 'got bot?'
- A botmaster or botherder commands bots to perform any of an array of different functions
- System of bots and controller(s) is referred to as a botnet or zombie network

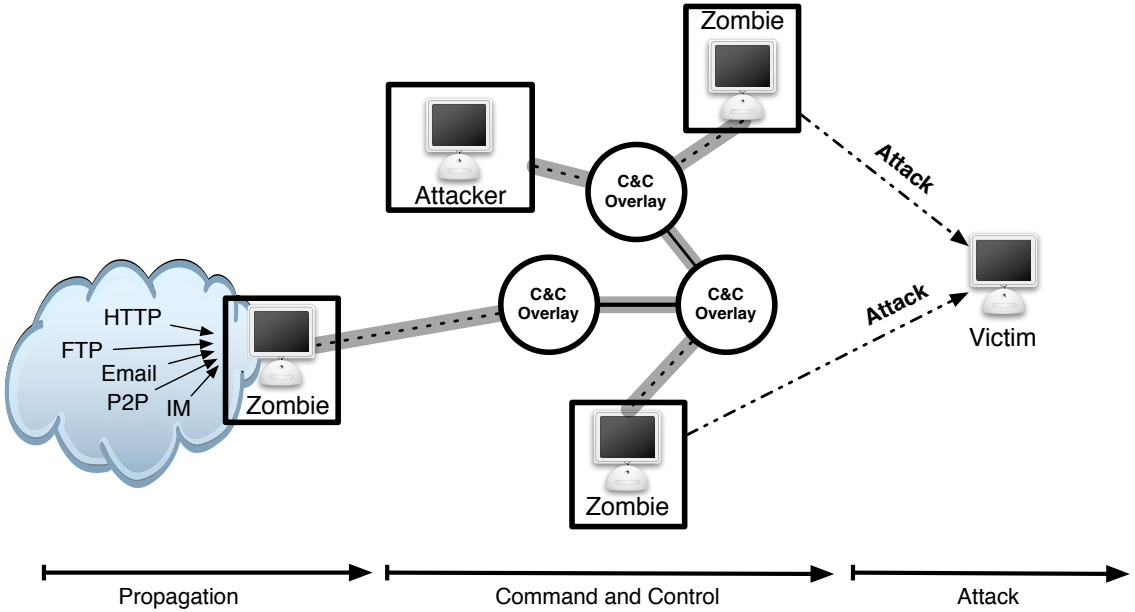
• Cooke et al., The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets (SRUTI '05)


程式相容性助理
小畫家
小畫家
NVIDIA Setup Error
刪除數個項目
Windows Internet Explorer
Windows Internet Explorer
Windows Internet Explorer
無法下載 list.asp%3fid=2213 從 hk.wrs.yahoo.com。
找不到網站。請確定網址正確然後重試。
確定
刪除數個項目
Windows Internet Explorer
Windows Internet Explorer
Windows Internet Explorer
無法下載 list.asp%3fid=2213 從 hk.wrs.yahoo.com。
找不到網站。請確定網址正確然後重試。
確定
Microsoft Office Word 已開啟此
請關閉檔案，然後再試一次。
刪除數個項目
刪除數個項目
您確定要永久刪除這 2 個項目嗎?
是(Y)
否(N)
刪除數個項目
刪除數個項目
您確定要永久刪除這 2 個項目嗎?
是(Y)
否(N)
取消
確定
資源回收筒
14:15
18/8/2009



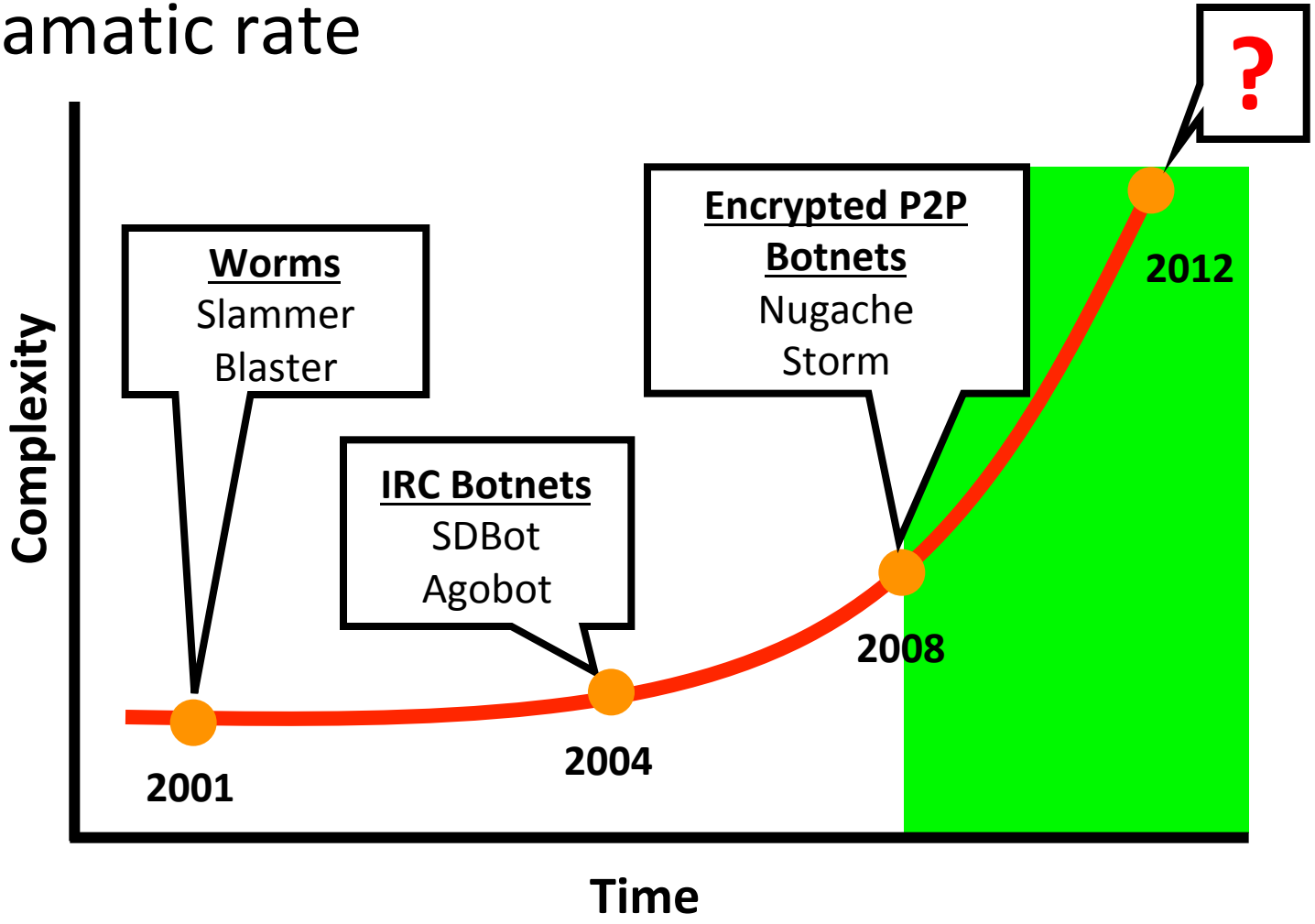
A Botnet lifecycle framework

- We maintain that all bots MUST exhibit these lifecycle behaviors:
  - **Propagation**: To recruit new members, bots rely on an array of built-in propagation vectors.
  - **Communication**: After a new infection, a bot establishes a C&C connection with a controller.
  - **Attacks**: Malicious bots attack Internet users and infrastructure.



Ecosystem complexity

- Attack ecosystem complexity is increasing at a dramatic rate



Botnet evolving propagation

Propagation Methodology		Design Complexity	Detectability	Propagation Speed	Population Size
Exploit:	Operating System	*Medium*	*High*	*Low*	*High*
	Services	*Medium*	*Medium*	*Medium*	*Medium*
	Applications	*High*	*Low*	*High*	*Low*
Social Engineering		*Low*	*Medium*	*Low*	*High*

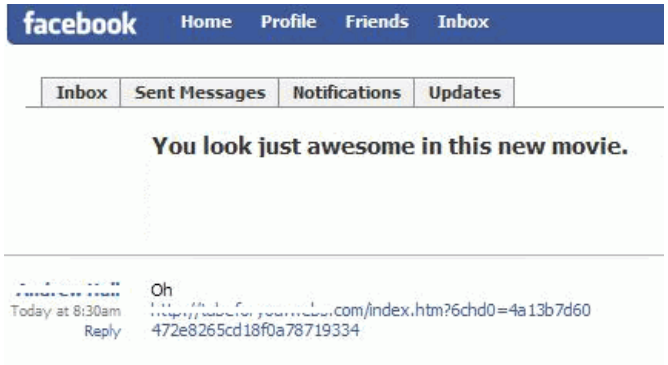
- Attacks moving “up” (i.e., application attacks, social engineering)
  - People continue to be the weakest link
  - Web centric (e.g., browsers as operating systems)
- Targeted behaviors
- Piggyback on other’s trust

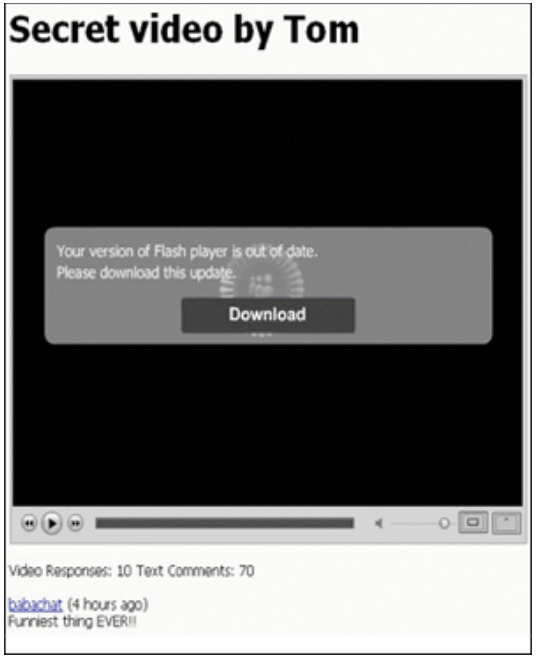
Application level attack: the drive-by

- Today email and other application-level functions laden with Trojans
- Now delivered via web sites - drive-by installs
  - Projected 1 in 10 web sites hosts malicious content
  - Web-based delivery means outpacing email, viruses, etc..

Social networking and messaging

Koobface:





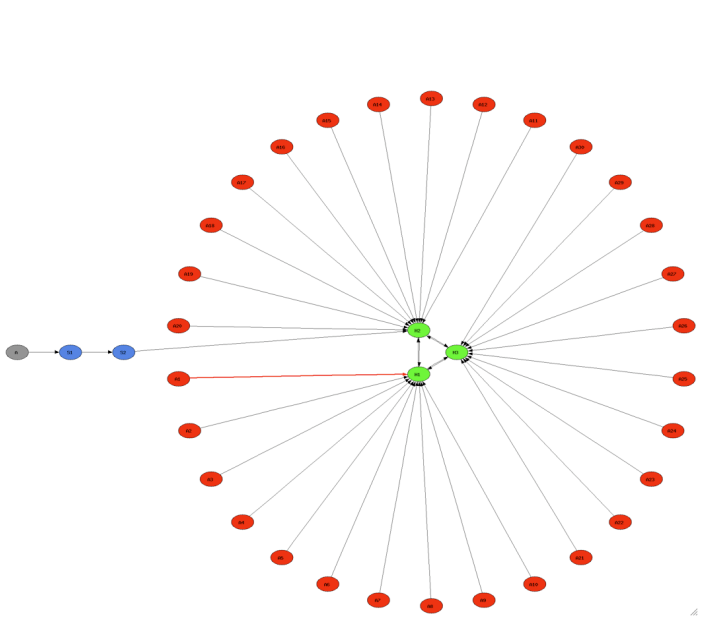
- Attackers using social networks to spread via social engineering and internal messaging
- Difficult to maintain visibility into these vectors to collect and analyze malware

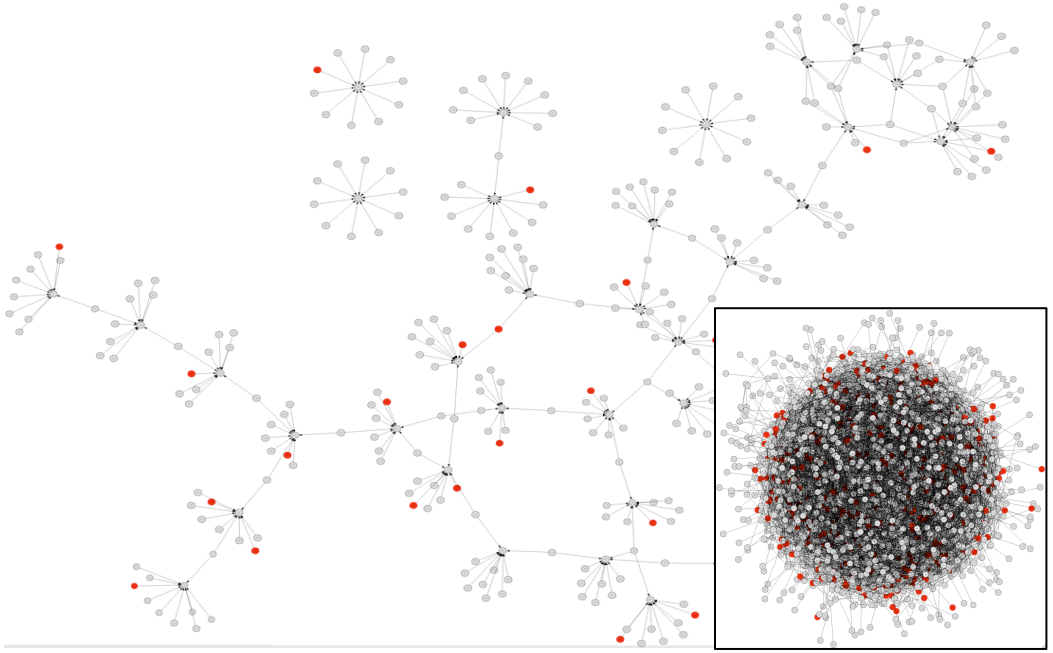
Evolving botnet topologies and communication

Topology	Design Complexity	Detect-ability	Message Latency	Surviv-ability
Centralized	*Low*	*Medium*	*Low*	*Low*
Peer-to-Peer	*Medium*	*Low*	*Medium*	*Medium*
Unstructured	*Low*	*High*	*High*	*High*

- More resilient topologies
- Obfuscating C&C
  - Hide in the open (e.g., Twitter, Google App Engine)
  - Encryption
- Agility
  - Fast flux
  - Domain generation algorithms

E.g., more resilient structures





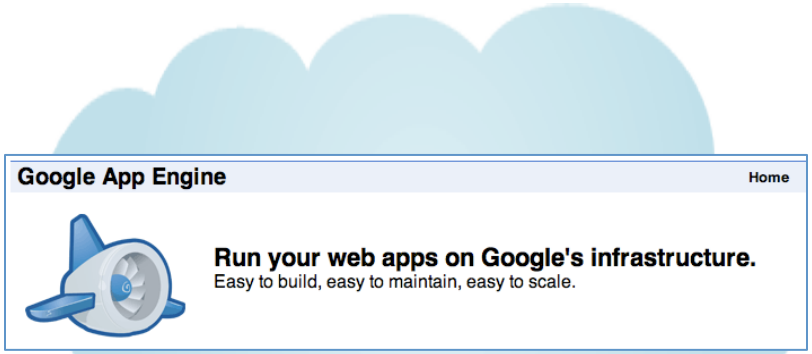
A *B*

Dave Dittrich and Sven Dietrich, USENIX ;login: vol. 32, no. 6, December 2007, pp. 8-17

E.g., more scalable and reliable communications?

Why write application in Google's app engine?

- Easy to get Started
- Automatic scalability
- The reliability, performance and security of Google's infrastructure
- Cost efficient hosting
- Risk free trial period



http://xiaoiboxip.appspot.com/[OMITTED]?
hostname=&&systemcpoy=&&userName=

http://XX.XX.76.85/aa.exe</br>

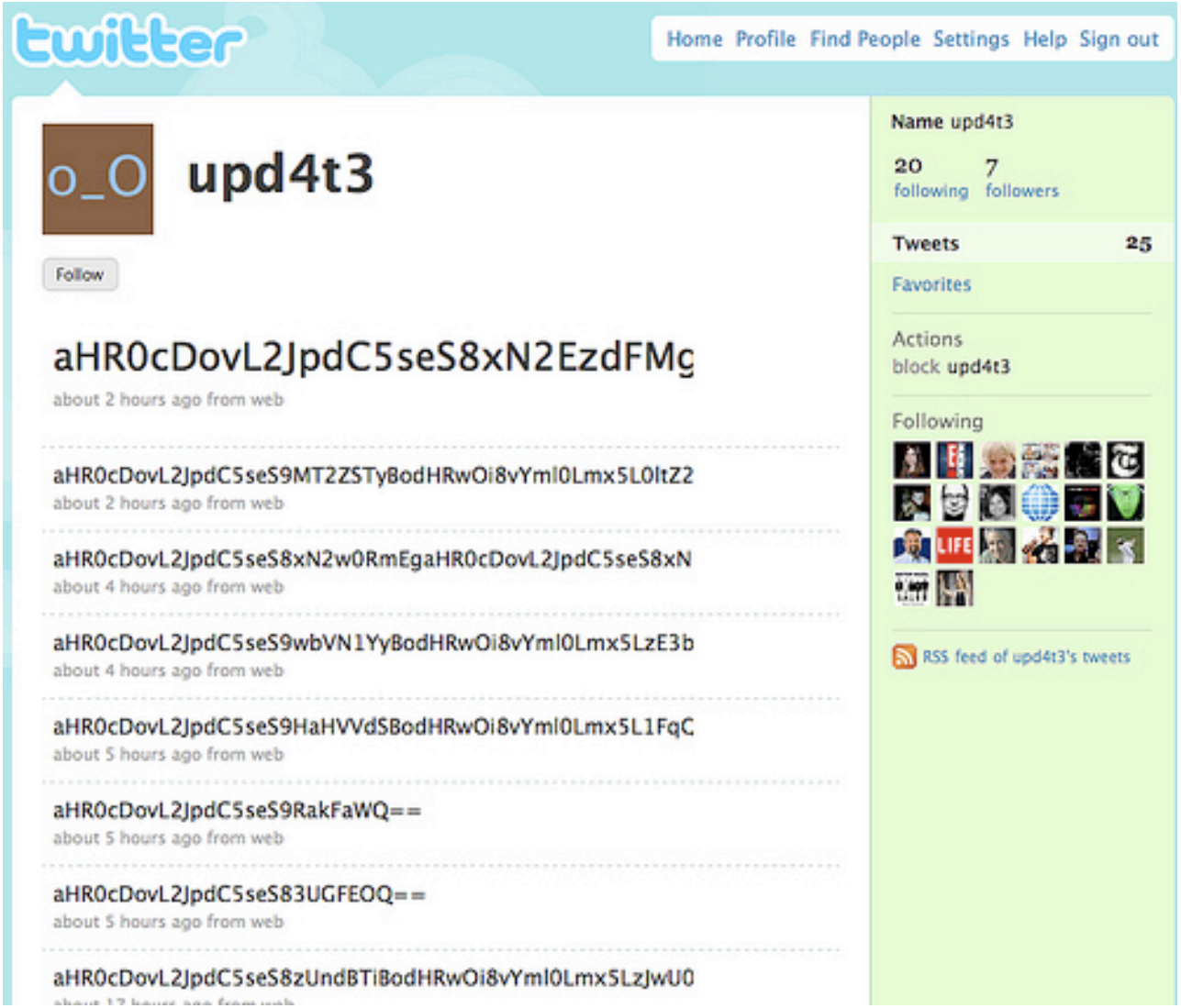
cmd

MD5: 2143a7b9a9de6ea26987ed8ece29d2c6
SHA1: 30f6befc76e4e269e5aa9c01c735d55d7ca4099a
File type: application/x-ms-dos-executable
File size: 65024 bytes

aa.Exe
(PCClient Backdoor)

Jose Nazario, ASERT Blog, November 7th, 2009

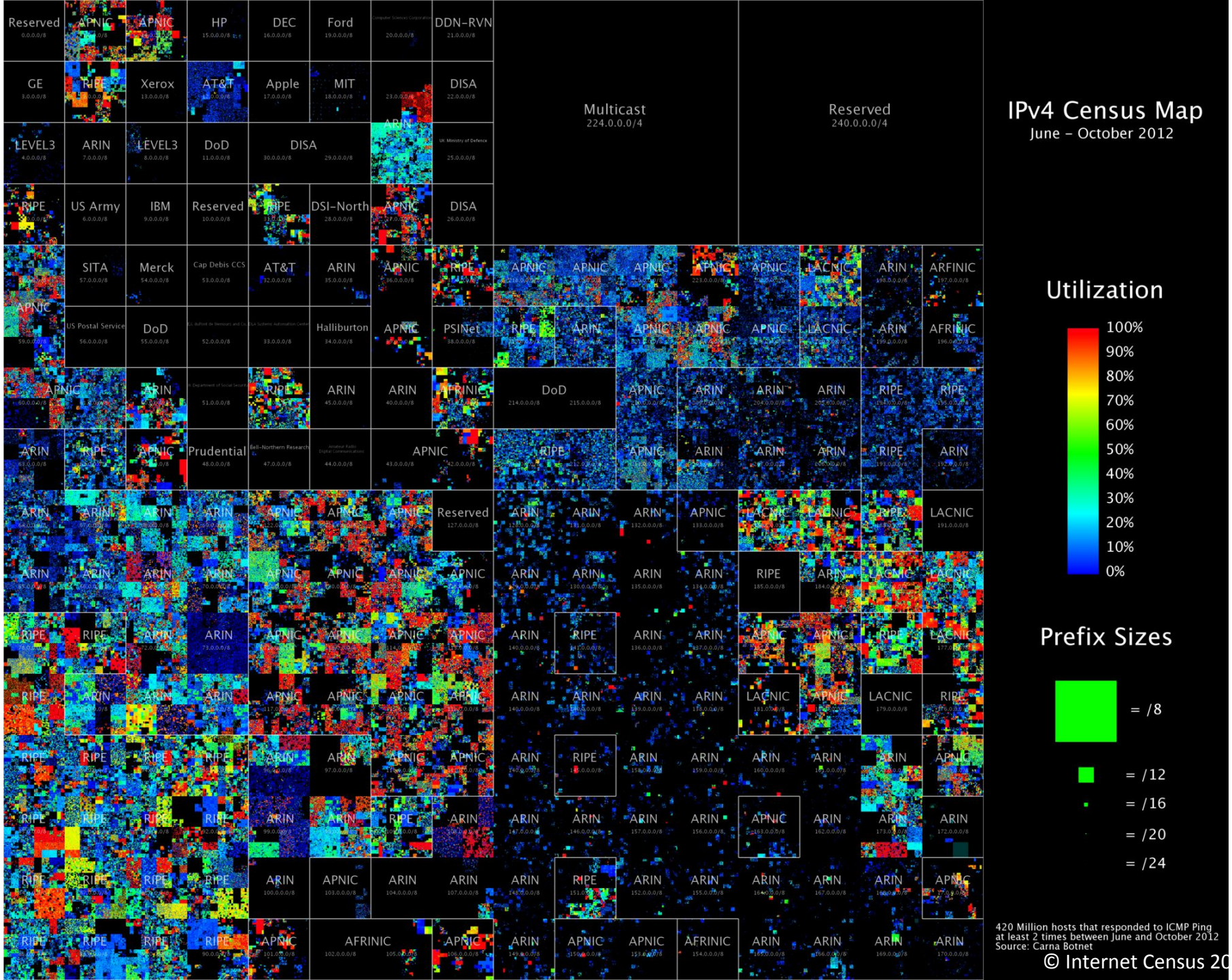
E.g., Tweeting C&C



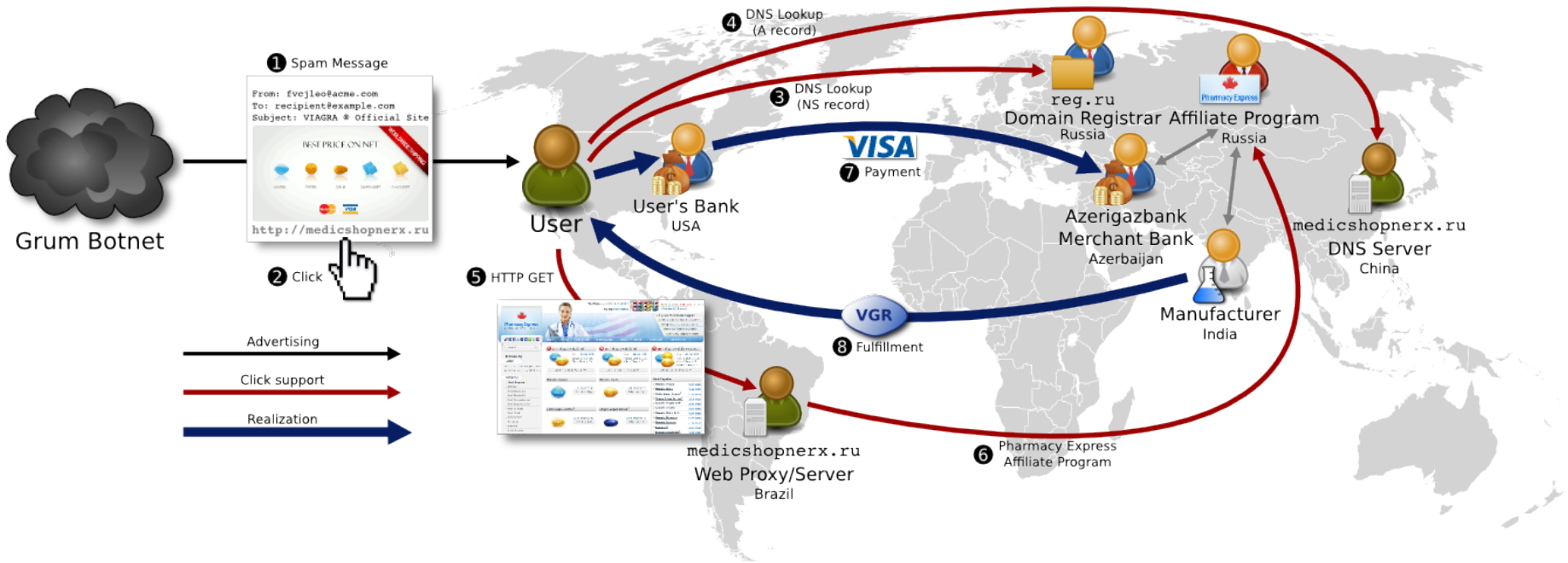
Evolving botnet attacks

Topology	Detectability	Design Complexity	Attack Value
Single Host DDoS	*High*	*Low*	*Low*
Multi Host DDoS	*Medium*	*Medium*	*Medium*
Identity Theft	*Low*	*High*	*Medium*
Spam	*Medium*	*Medium*	*High*
Phishing	*Medium*	*High*	*Medium*

- Impact (e.g., shift towards HTTP GET floods in DDoS campaign)
- Targeted Attacks


Reserved
0.0.0.0/8
APNIC
HP
15.0.0.0/8
DEC
16.0.0.0/8
Ford
19.0.0.0/8
DDN-RVN
21.0.0.0/8
GE
3.0.0.0/8
RIPE
Xerox
13.0.0.0/8
AT&T
Apple
17.0.0.0/8
MIT
18.0.0.0/8
DISA
22.0.0.0/8
ARIN
Multicast
224.0.0.0/4
Reserved
240.0.0.0/4
LEVEL3
4.0.0.0/8
ARIN
7.0.0.0/8
LEVEL3
8.0.0.0/8
DoD
11.0.0.0/8
DISA
30.0.0.0/8
29.0.0.0/8
UK Ministry of Defence
25.0.0.0/8
RIPE
US Army
6.0.0.0/8
IBM
9.0.0.0/8
Reserved
10.0.0.0/8
DSI-North
28.0.0.0/8
DISA
26.0.0.0/8
SITA
57.0.0.0/8
Merck
54.0.0.0/8
Cap Debis CCS
53.0.0.0/8
AT&T
32.0.0.0/8
ARIN
35.0.0.0/8
US Postal Service
56.0.0.0/8
DoD
55.0.0.0/8
52.0.0.0/8
33.0.0.0/8
Halliburton
34.0.0.0/8
PSINet
38.0.0.0/8
LACNIC
ARFINIC
197.0.0.0/8
AFRINIC
196.0.0.0/8
51.0.0.0/8
45.0.0.0/8
40.0.0.0/8
DoD
214.0.0.0/8
215.0.0.0/8
Prudential
48.0.0.0/8
47.0.0.0/8
44.0.0.0/8
43.0.0.0/8
Reserved
127.0.0.0/8
LACNIC
191.0.0.0/8
AFRINIC
102.0.0.0/8
105.0.0.0/8
IPv4 Census Map
June – October 2012
Utilization
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Prefix Sizes
= /8
= /12
= /16
= /20
= /24
420 Million hosts that responded to ICMP Ping at least 2 times between June and October 2012
Source: Carna Botnet
© Internet Census 20

The Spam “Value Chain”



Affiliate Program	orders/month	*Spamalytics* single order	*Spamalytics* rev/month	Min product price single order	Min product price rev/month	Basket-weighted average single order	Basket-weighted average rev/month
33drugs	9,862	$100	$980,000	$45.00	$440,000	$57.25	$560,000
4RX	8,001	$100	$800,000	$34.50	$280,000	$95.00	$760,000
EuroSoft	22,776	N/A	N/A	$26.50	$600,000	$84.50	$1,900,000
EvaPharmacy	26,962	$100	$2,700,000	$50.50	$1,300,000	$90.00	$2,400,000
GlavMed	17,933	$100	$1,800,000	$54.00	$970,000	$57.00	$1,000,000
Online Pharmacy	5,856	$100	$590,000	$37.00	$220,000	$58.00	$340,000
Pharmacy Express	7,933	$100	$790,000	$51.00	$410,000	$58.75	$460,000
Royal Software	13,483	N/A	N/A	$55.25	$750,000	$133.75	$1,800,000
Rx–Promotion	6,924	$100	$690,000	$45.00	$310,000	$57.25	$400,000
SoftSales	1,491	N/A	N/A	$20.00	$30,000	$134.50	$200,000

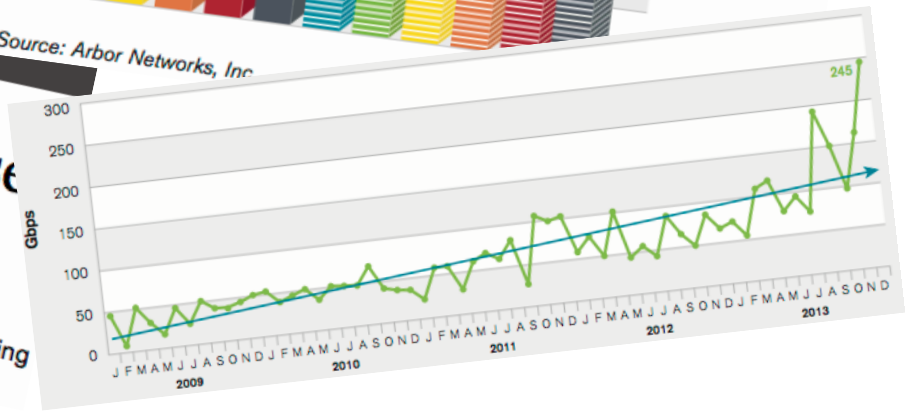
Kanich et al., Show Me the Money: Characterizing Spam-advertised Revenue. The Economist, 2011

The DDoS "Hockey Stick Era"

February 11, 2014, 7:54 PM ET

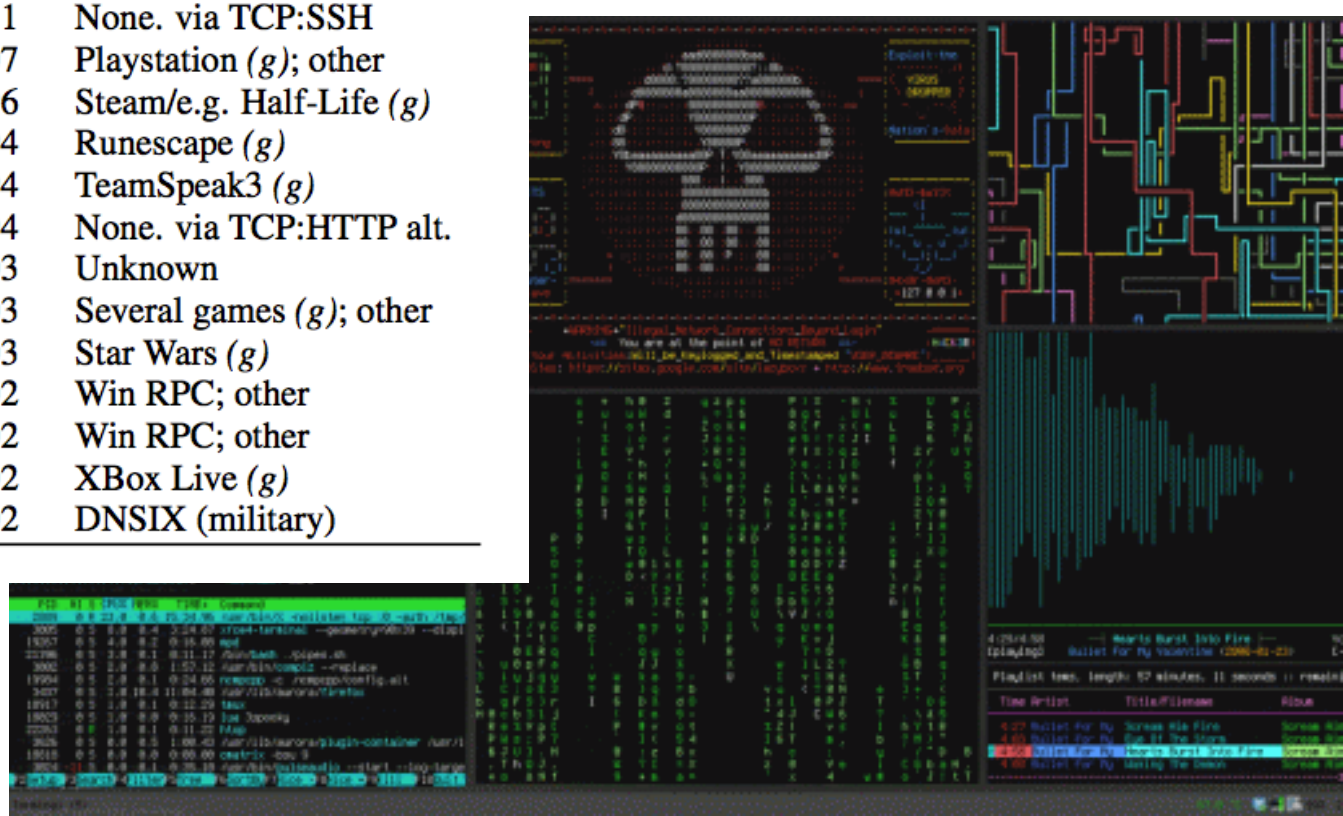
Record-Breaking Cyberattack Use New Technique

A record-breaking cyberattack used a new technique to exploit servers and generate exponentially more traffic in an attempt to take down a website, according to CloudFlare CEO Matthew Prince.

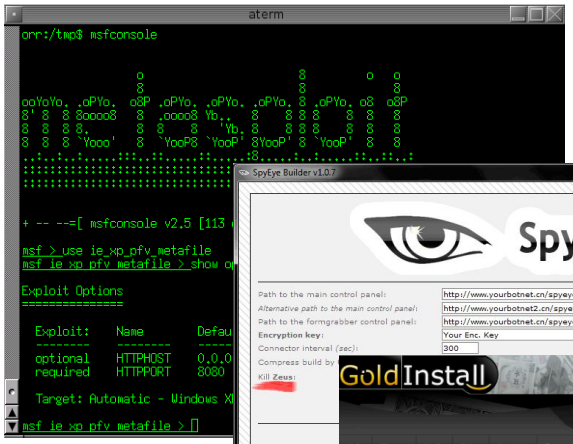


Top Attacked Ports

Rank	Attacked Port	Fraction	Common UDP Use
1	80	0.362	None. via TCP:HTTP *(g)*
2	123	0.238	NTP server port
3	3074	0.079	XBox Live *(g)*
4	50557	0.062	Unknown
5	53	0.025	DNS; XBox Live *(g)*
6	25565	0.021	Minecraft *(g)*
7	19	0.012	chargen protocol
8	22	0.011	None. via TCP:SSH
9	5223	0.007	Playstation *(g)*; other
10	27015	0.006	Steam/e.g. Half-Life *(g)*
11	43594	0.004	Runescape *(g)*
12	9987	0.004	TeamSpeak3 *(g)*
13	8080	0.004	None. via TCP:HTTP alt.
14	6005	0.003	Unknown
15	7777	0.003	Several games *(g)*; other
16	2052	0.003	Star Wars *(g)*
17	1025	0.002	Win RPC; other
18	1026	0.002	Win RPC; other
19	88	0.002	XBox Live *(g)*
20	90	0.002	DNSIX (military)



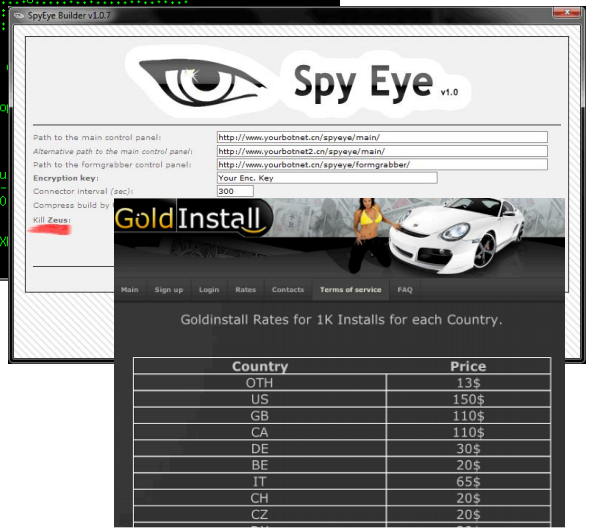
Infrastructure



Exploit packs

Spamit.com

Spam Services



Botnet Toolkits

Pay per Install

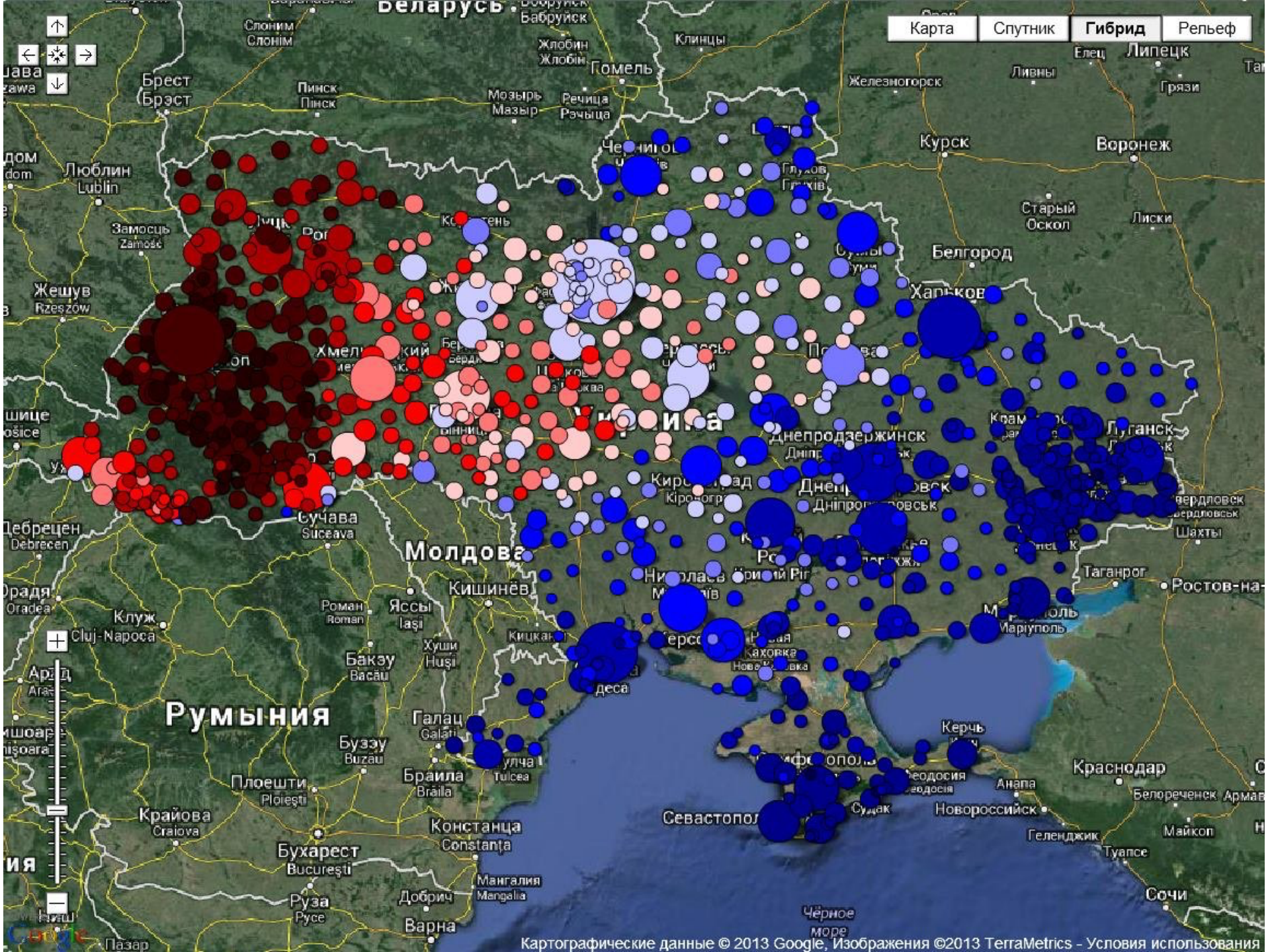
DeCaptcha and Packing Services

DEATH BY CAPTCHA

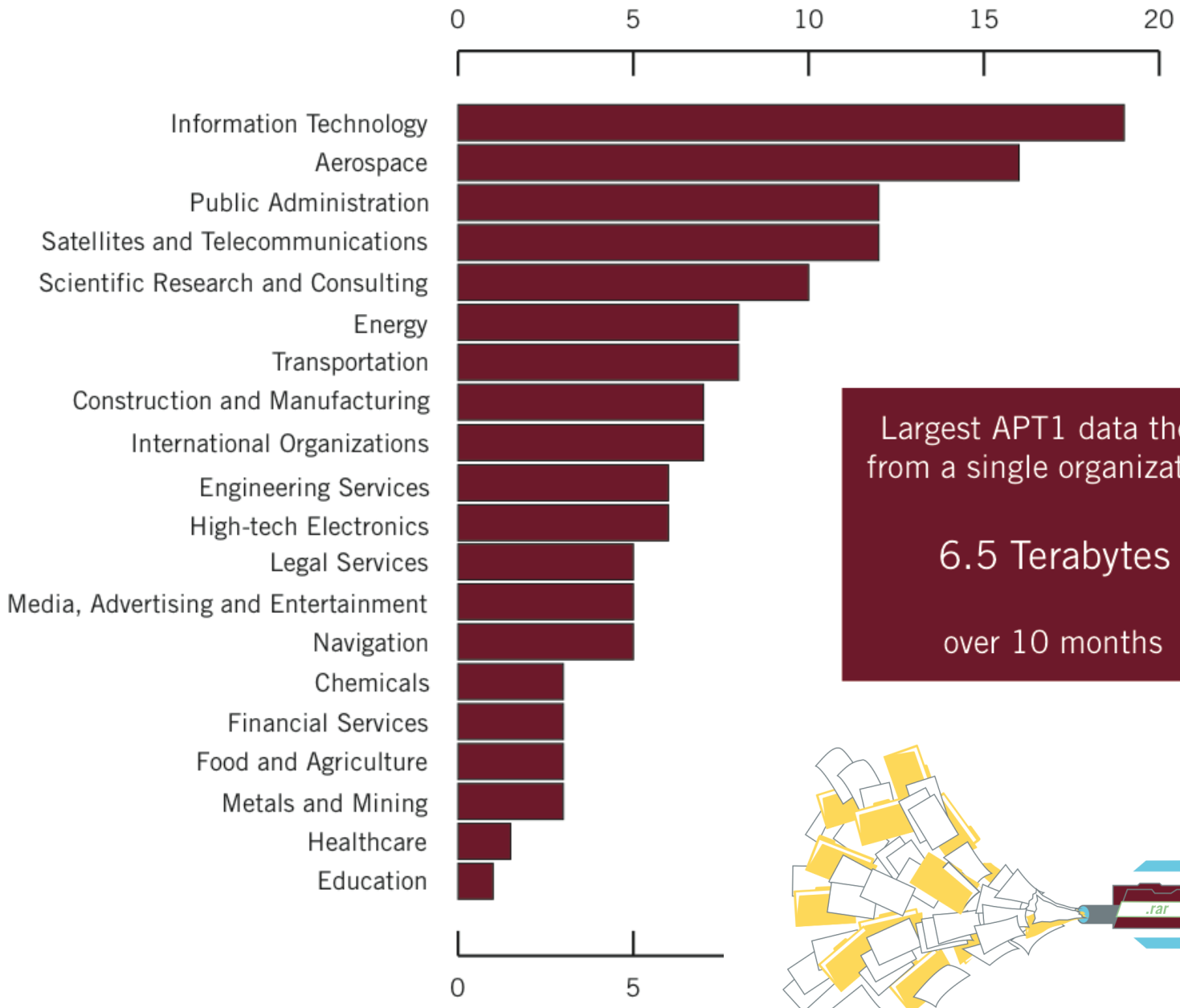
FASTEST DISCOUNT CAPTCHA SOLVERS

Cloud Type	Legitimate	Crimeware
IaaS	Amazon EC2, Mosso	Renting out infected bots
PaaS	Google App Engine, Azure	Botnet-backed spam services
SaaS	SalesForce, SAP ByDesign	Packing services, Decaptcha!

Projecting power into cyberspace


Карта
Спутник
Гибрид
Рельеф
Беларусь
Брест
Пинск
Гомель
Могилев
Курск
Воронеж
Белгород
Харьков
Луганск
Днепродзержинск
Кременчуг
Кировоград
Днепропетровск
Запорожье
Мариуполь
Таганрог
Ростов-на-Дону
Молдова
Кишинёв
Сучава
Яссы
Бакэу
Румыния
Галац
Бузэу
Плоешти
Браила
Крайова
Констанца
Бухарест
Мангалия
Добрич
Варна
Руза
Севастополь
Керчь
Краснодар
Новороссийск
Сочи
Чёрное море
Люблин
Жешув
Замосць
Дебрецен
Орадя
Клуж-Напока
Арад
Тимишоара
Картографические данные © 2013 Google, Изображения ©2013 TerraMetrics - Условия использования


Reuters



http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf


전쟁이
전쟁은


CPU319-3 PN/DP
SIEMENS
SF
DC5V
FRCE
RUN
STOP
SIMATIC
S7-300
SM323
DI16/DO16xDC24V
SM322
DO 32xDC24V/0.5A
SM322
DO 32xDC24V/0.5A
IN
OUT
2
4
5
6


MADE IN
AMERICA
07041776


Wikileaks

Future security challenges will continue to follow technology trends and Internet adoption patterns.

Three Emerging Trends

Smart Systems and IOT

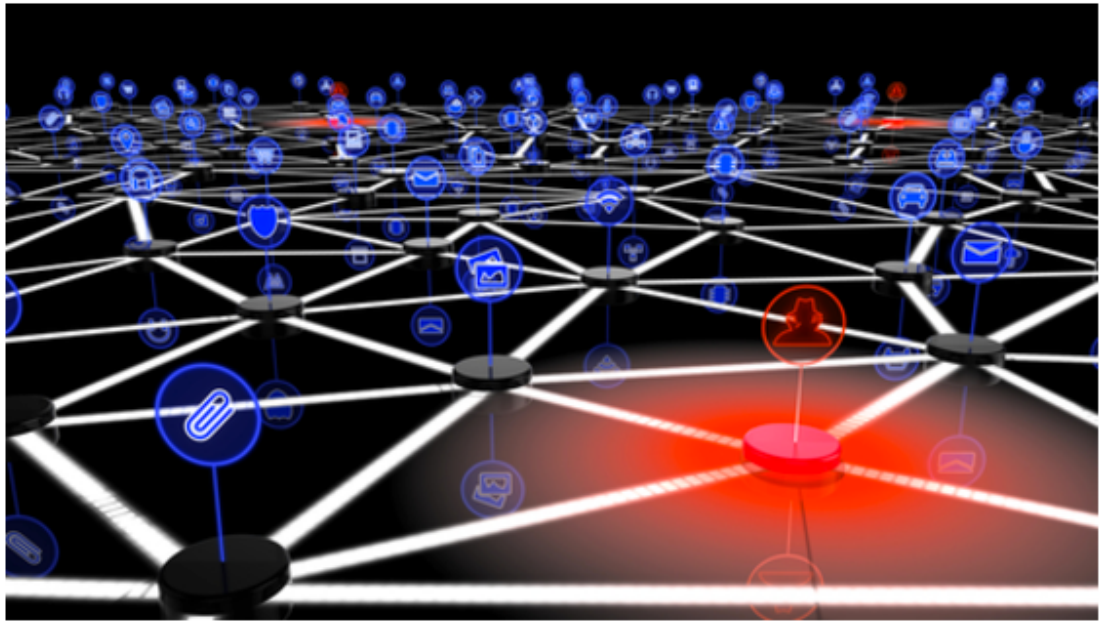
Data Explosion and Analytics

Autonomy and Robotics

21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.



My New Book!

// root xc3511
// root vizxv
// root admin
// admin admin
// root 888888
// root xmhdipc
// root default
// root juantech

Map of Scanners

Map based on Longitude (generated) and Latitud