STONY BROOK
STATE UNIVERSITY OF NEW YORK

Malware

Current Threats (Fourth generation)

- Steal confidential information
  - Credit-card/bank account #s, passwords, …
  - Trade secrets and other proprietary information
  - Security-sensitive information
    - Useful for breaching physical world security
- Establish base for future operations
  - Conduit for future attacks
- Surveillance
  - Capture keystrokes, microphone or camera input
  - Reveal information about software installed
  - Snoop on web sites visited

Current Threats (Continued)

- Driven by commercialization of Malware
  - Thriving black-market for exploits
    - Zero-day exploits have arrived
  - “Bot”-centric model for cyber crime
    - Relay spam (e-mail scam, phishing)
    - Extortion (using DDoS or targeted attacks)
    - Focus on desktop (rather than server) vulnerabilities
  - Profit-driven adware and spyware
    - Customer-profiling, niche-marketing
    - IP protection (digital rights management)
    - aggressive installation, stealth (rootkits, spyware)
  - Targeted attacks on high-value targets
    - Political activists
    - International adversaries
    - People with access to valuable information
      - CEO/CFO with access to financial information on publicly traded companies
      - Researchers with access to proprietary formulas or other valuable IP

Modern Threats: A Glance

- Software
  - Viruses
  - Worms
  - DDoS and Botnet
  - Rootkits
  - Spyware

- Goal of software
  - Spam
  - Phishing
  - Online extortion
  - …

Computer Virus

- **Properties**
  - Replicates itself
  - Attaches to other non-malicious code
- **Early versions spread via floppy disks, while recent viruses spread through the internet.**
- **Examples**
  - Boot sector virus (difficult on OS with memory protection)
  - Other OS level virus
  - Virus that attaches to programs, scripts, libraries
  - Macro virus
  - Mail attachments
  - …

Disk-based Computer Viruses

- **1982, Elk Cloner**
  - First virus in the wild
  - Targeting Apple II
- **1986, (c)Brain**
  - First virus for IBM PC
  - A boot sector virus
- **1995, Concept virus**
  - First Macro virus
- **1998, CIH**
  - One of the most harmful widely circulated viruses
  - Overwrites both hard disks (**data loss**) and Flash BIOS (**hardware damage**)

Macro Virus

- Written in a macro language.
- Macros can perform operations that the software can do.
- Often, a simple solution: turning off the macro feature

CIH Virus

- Spreads via Portable Executable files under Windows 95/98/Me.
- Damages:
  - Overwriting the first 1024KB of the hard drive with zeroes ➔

    Loss of data on the entire hard drive
  - Overwriting the Flash BIOS with junk code ➔

    Computers cannot boot any more
- Activated in the public eye on April 26, 1999
- An untold number of computers worldwide were affected, much in Asia

Melissa

- Found on March 26, 1999
- Targetting Microsoft Word and Outlook-based systems, and creating considerable network traffic
- Shut down many Internal mail systems
  - That got clogged with infected e-mails propagating from the worm
- Inside a file called “List.DOC”
- Spread on Microsoft Word 97 and Word 2000.
- Can mass-mail itself from email client Microsoft Outlook 97 or Outlook 98.
- Attempts to mass mail itself once an infected Word document is opened.

ILOVEYOU

- First appeared on May 3, 2000
- Caused widespread e-mail outages, an estimated $10 billion in economic damage
- Written in VBScript
- E-mail
  - Subject: “ILOVEYOU”
  - Attachment “LOVE-LETTER-FOR-YOU.TXT.vbs”
- Overwrote important files with a copy of itself
- Sent out itself to everyone in a user’s contact list

Computer Worm

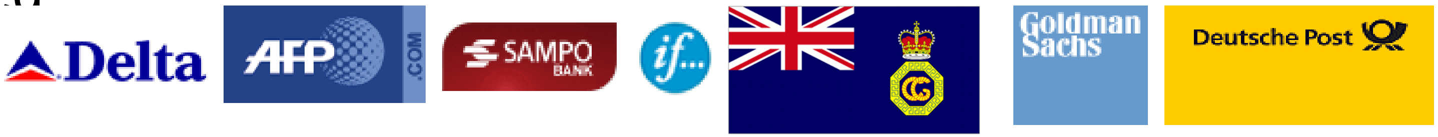
- **Replicates over the network (usually by itself)**
  - First worm appeared at Xerox PARC in 1978
- **What a worm can do?**
  - Replicates itself, and thus consumes network bandwidth
  - Deletes files on a host system
  - Sends documents via e-mail
  - Carries other executables as a payload
    - Installs a backdoor in an infected computer (zombie computer)
- **Modern worms**
  - Large scale infection
  - Fast spread rate
    - spread over the Internet within a second

Timeline of Notable Worms (1)

- **Nov 1988, Morris worm**
  - First well-known worm
- **March 1999, Melissa** (E-mail worm)
  - Targeting Microsoft Word & Outlook-based systems
- **May 2000, VBS/Loveletter or ILOVEYOU** (E-mail worm)
  - Caused an estimated $10 billion in economic damage
- **July 2001, Code Red** (Exploited IIS bugs)
  - Considerably slowed down Internet traffic
- **Jan 2003, SQL Slammer** (Exploited MS SQL Server bugs)
  - Very fast: infected most of its 75,000 victims within ten minutes
  - Amazingly small, only 376 bytes

Timeline of Notable Worms (2)

- **Aug 2003, Blaster, Welchia (Nachi), SoBig**
  - **Blaster** (Exploited DCOM RPC bugs)
    - Coded to start a SYN flood on Aug 15 against windowsupdate.com
  - **Welchia (Nachi)**
    - A goodwill worm to remove Blaster and patch Windows
  - **SoBig** (E-mail worm)
    - Infected millions of Windows computers in Aug 2003
    - Microsoft wanted information of the worm creator for $250,000
- **Apr 2004, Sasser** (Exploited LSASS bugs)
  - Affected:



- Jan 2007, Storm worm
  - Very stealthy, established botnets.
  - Used obfuscation and rootkit-techniques to hide its behavior as well as its presence

Code Red

- Released on July 13, 2001
- Considerably slowed down the Internet traffic
- Details:
  - Attacked computers running Microsoft's IIS web server
  - Defaced the affected web site
  - Tried to spread itself by looking for more IIS servers on the Internet
  - Waited 20-27 days after it was installed to launch DoS attacks on several fixed IP addresses, including White House.
- Exploited a buffer overflow vulnerability in IIS; Used illegal GET requests to trigger the vulnerability

SLAMMER

- January 2003
- Caused DoS on some Internet hosts and dramatically slowed down general Internet traffic
- Fast
  - Infect most of its 75,000 victims within ten minutes
- A buffer overflow based attack targeting Microsoft SQL Server
- Amazingly small, only 376 bytes
- Generate random IP addresses and send itself out to those addresses.
- If the selected address happens to belong to a host that is running an unpatched copy of Microsoft SQL Server, the host immediately becomes infected and begin spraying the Internet with more copies of the worm program.
- Only stays in memory.

Blaster

- Spread during August 2003 (first noticed on August 11, peaked on August 13)
- Programmed to start a SYN flood on August 15 against port 80 of windowsupdate.com.
- Exploited a buffer overflow in the DCOM RPC service on the affected Windows operating systems

Welchia (Nachi)

- Welchia (Nachi), a worm that tries to remove the Blaster worm and patch Windows
  - Discovered in August 18, 2003
- Not good
  - Create vast amount of network traffic, thereby slowing down the Internet
  - Make the system unstable (e.g. reboot after patching)
  - Without user’s explicit consent

SoBig

- Consequences:
  - Infected millions of Microsoft Windows computers in August 2003
  - Microsoft wanted information of the worm creator for $250,000
- Details:
  - Appear as an e-mail with one of the following subjects:
    - Re: Approved Re: Details Re: Thank you …
  - Contain the text: “See the attached file for details” or the like
  - Contain an attachment by one of the following names:
    - application.pif details.pif thank_you.pif …
- Infection and spreading
  - Infect a host computer once the attachment is opened
  - Replicate by sending out the above-mentioned emails
  - E-mail addresses are gathered from files on the host computer

MyDoom

- First sighted on January 26, 2004.
- One of the fastest spreading e-mail worms
- Details
  - Primarily transmitted via e-mail, appearing as a transimission error
  - Subject lines including “Error”, “Mail Delivery System”, “Test” or “Mail Transaction Failed”
  - Contains a malicious attachment
- Infection and Spreading
  - Resend the worm to e-mail addresses found in local files once the attachment is opened.
  - Copies itself to the “shared folder” of KaZaA (a P2P file-sharing app)
- Backdoor
  - Installs a backdoor on port 3127/tcp to allow remote control of the subverted PC
  - A DoS attack against SCO Group, Microsoft, and antivirus sites

Sasser

- First noticed in April 2004. Affected:

Delta AFP .COM SAMPO BANK if... Goldman Sachs Deutsche Post

- Can spread without the help of the user.
  - Exploit a buffer overflow in LSASS (Local Security Authority Subsystem Service)
  - Scan different ranges of IP addresses and connect to victims’ computers primarily through TCP port 445.

- Can be easily stopped by a properly configured firewall, or by downloading patches

Goals of Worms

- "bragging rights" in early days
  - infect as many sites as possible
  - be as noticeable as possible
  - values fast spread, DoS effect
- Detection techniques could hence be targeted at these features
- More recently, worms used to establish botnets
  - Need to remain stealthy
    - Spread slowly so as to evade detection
    - Attacks launched on demand, but infection itself should not cause any noticeable surge in network trafiic or other feature changes that can be easily spotted
    - So, we no longer hear about "high-profile" worms.

Distributed Denial-of-Service (DDoS)

- **DoS**
  - An attack on a computer system or network that causes a loss of service to users
- **Methods**
  - Consumption of computational resources, such as bandwidth, disk space, or CPU time
  - Disruption of configuration information, such as routing information
  - Disruption of physical network components
- **DDoS**
  - Use of multiple hosts (often through Botnet) in a DoS

Botnet

- **What is a Botnet?**
  - A collection of compromised computers
  - The computers are implanted with backdoor programs
    - Usually by worms, viruses
  - The programs are under a common control infrastructure
  - Botnet’s originator can control the group remotely
    - Earlier botnets used means such as IRC
    - **But modern botnets have begun to rely means that are harder to spot**
      - **HTTP**
      - **P2P networks**
- **Purpose**
  - DDoS
  - SMTP mail relays for SPAM
  - Theft of sensitive information
    - E.g. login IDs, credit card numbers, application serial numbers

Rootkit

- **Stealthy backdoor programs**

- **Intended to maintain “invisibility” of intruders**
  - Intercepts data from terminals, network connections, and the keyboard
  - Conceals logins, running processes, files, logs, or other system data

- **Origins of “rootkit”**
  - Originally referred to such kind of programs in Unix systems (root – the administrator)

Rootkits

- Userlevel rootkits
  - Early ones on UNIX used to replace many programs used to examine system state
    - ls, ps, netstat,…
  - Drawback: if an administrator uses a custom C-program to examine system state, he can discover the presence of rootkit
- Kernel rootkits
  - System call interception based
    - All user level requests are intercepted and modified to hide the presence of rootkit
    - Problem: can be difficult to block all ways to learning about the presence of rootkit

More Advanced Rootkits

- May reside entirely within the kernel, with no user-level processes
- Hide themselves from system monitoring tools
  - e.g., put themselves on a scheduler queue, but not task queue
- In the most extreme case, avoid changing any data that is predictable or is read-only
  - Hide within kernel data structures that change all the time
- Rootkits that hide underneath the OS
  - Lift the OS into a VM!

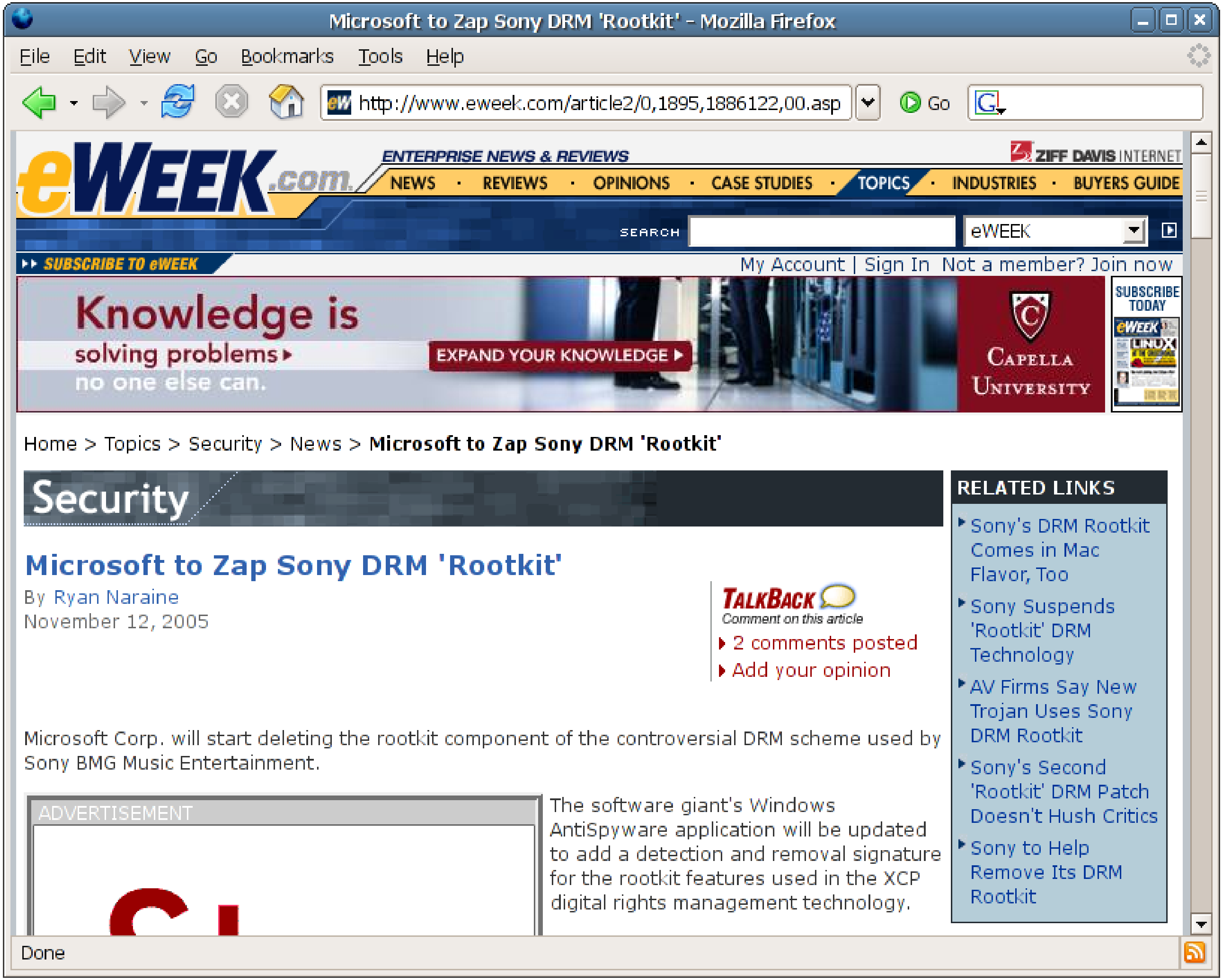
SonyBMG DRM Rootkit (2005)

- Extended Copy Protection (XCP) DRM for CD copy protection
  - User is required to install XCP software contained in the CD to play XCP-protected CD on a Windows system.
  - XCP intercepts all accesses of the CD drive and only allows XCP-bundled media player to access music tracks on the CD
  - **(Rootkit)** XCP conceals itself from the user by installing a patch to the Windows operating system. This patch stops ordinary system tools from displaying processes, registry entries, or files who names begin with sys.
- About 4.7 million XCP-CDs shipped, 2.1 million sold [*New York Times*]

SonyBMG DRM Rootkit (2005)

- A Controversial DRM mechanism

- Weakened system security
  - XCP rootkit could be used by other malware
    - The first one was discovered in November 2005
  - XCP uninstaller, which was released later, left serious security holes on the system
- This episode set back DRM efforts for a while
  - But ultimately, DRM forces won
    - Included in HTML 5 (March 2017)
    - Relies on protection offered by the platform (iOS, Adroid, Kindle)
    - or code obfuscation (e.g., SilverLight, Flash)
      - Obfuscation is security by obscurity, but pretty effective in practice because the effort (for defeating) is not often worth the cost.
        - Piracy is a more serious problem where cost is relatively high



Home > Topics > Security > News > **Microsoft to Zap Sony DRM 'Rootkit'**

Security

Microsoft to Zap Sony DRM 'Rootkit'

By Ryan Naraine
November 12, 2005

TALKBACK
Comment on this article
- 2 comments posted
- Add your opinion

Microsoft Corp. will start deleting the rootkit component of the controversial DRM scheme used by Sony BMG Music Entertainment.

The software giant's Windows AntiSpyware application will be updated to add a detection and removal signature for the rootkit features used in the XCP digital rights management technology.

RELATED LINKS
- Sony's DRM Rootkit Comes in Mac Flavor, Too
- Sony Suspends 'Rootkit' DRM Technology
- AV Firms Say New Trojan Uses Sony DRM Rootkit
- Sony's Second 'Rootkit' DRM Patch Doesn't Hush Critics
- Sony to Help Remove Its DRM Rootkit

Spyware

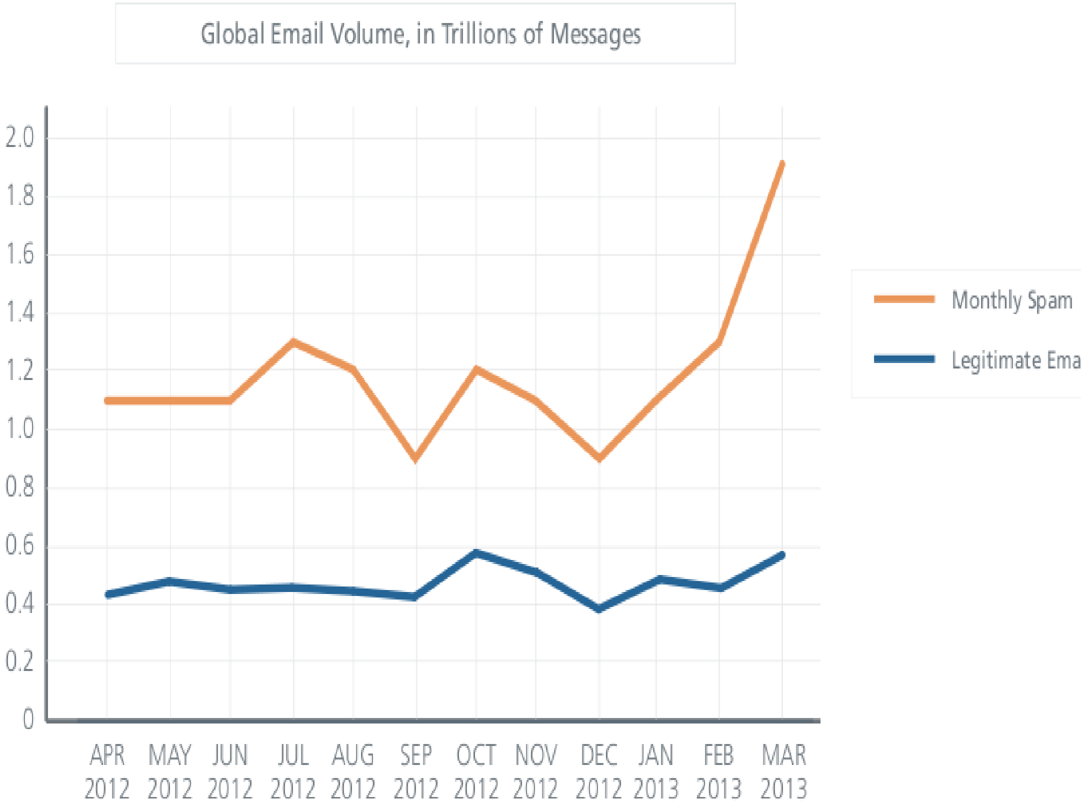
- **Properties**
  - Intercept or take partial control of computer’s operation
  - Without the informed consent of that computer’s legitimate user.
  - Does not usually self-replicate.
- **Purpose**
  - Delivery of unsolicited pop-up advertisements
  - Theft of personal information
  - Monitoring of Web-browsing activity for marketing purposes
  - Routing of HTTP request to advertising sites

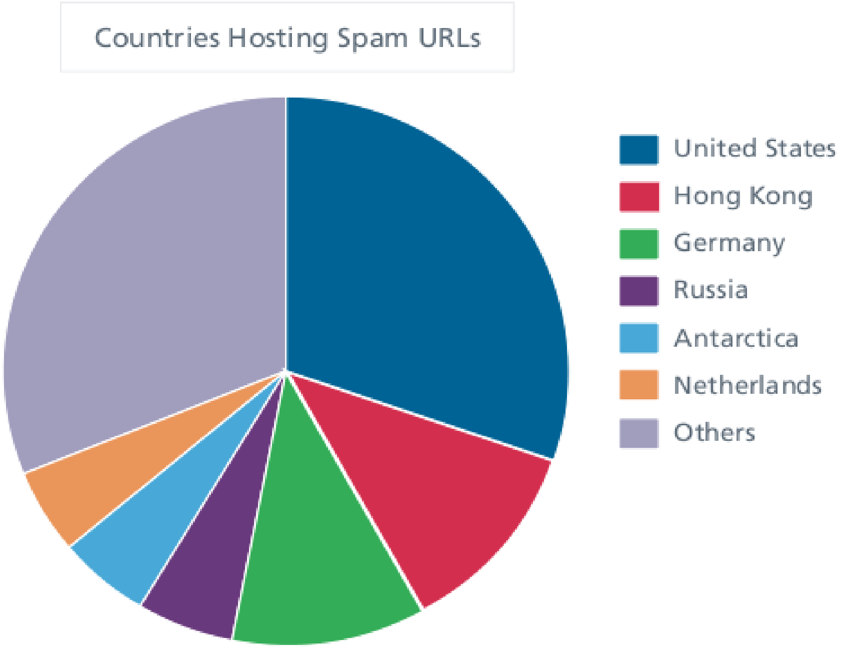
Spam

- Properties
  - Sending of *unsolicited* (commercial) emails
  - Sending nearly identical messages to thousands (or millions) of recipients
- Spamming in different media
  - *E-mail spam, Messaging spam, Newsgroup spam and Forum spam, Mobile phone spam, Internet telephony spam, Blog, wiki, guestbook, and referrer spam, etc*

Spam

- Spam volumes hold steady
  - After falling from a high of 6T to about 1T/month
- Expands to social networks
  - Facebook, Twitter, Instagram, …

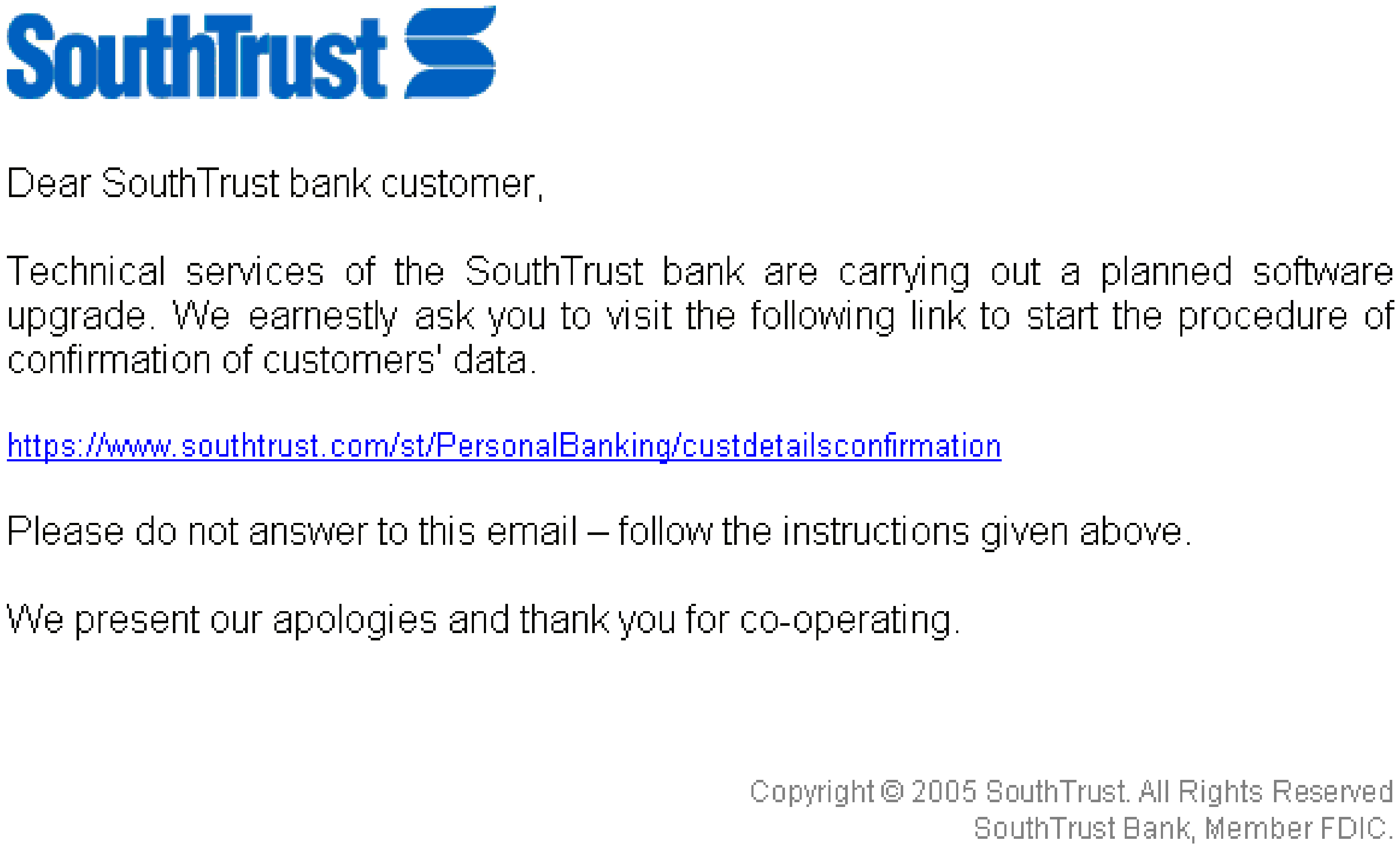




Source: McAfee Threats Report: First Quarter 2013

Phishing

- Uses social engineering techniques
  - Masquerading as a trustworthy person or business in an apparently official electronic communication
  - Attempts to fraudulently acquire sensitive information
    - Such as passwords and credit card details
- Spear-phishing
  - Phishing attack that is narrowly targeted at a single individual or a group of individuals



SouthTrust

Dear SouthTrust bank customer,

Technical services of the SouthTrust bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation

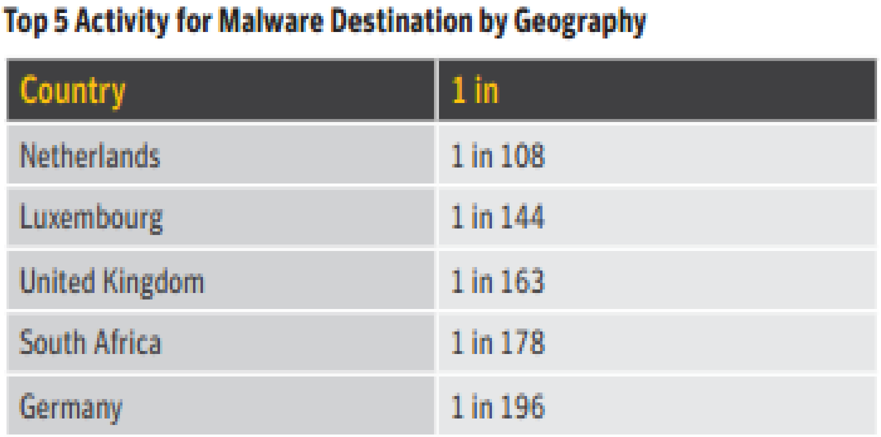
Please do not answer to this email – follow the instructions given above.

We present our apologies and thank you for co-operating.

Copyright © 2005 SouthTrust. All Rights Reserved
SouthTrust Bank, Member FDIC.

Phishing

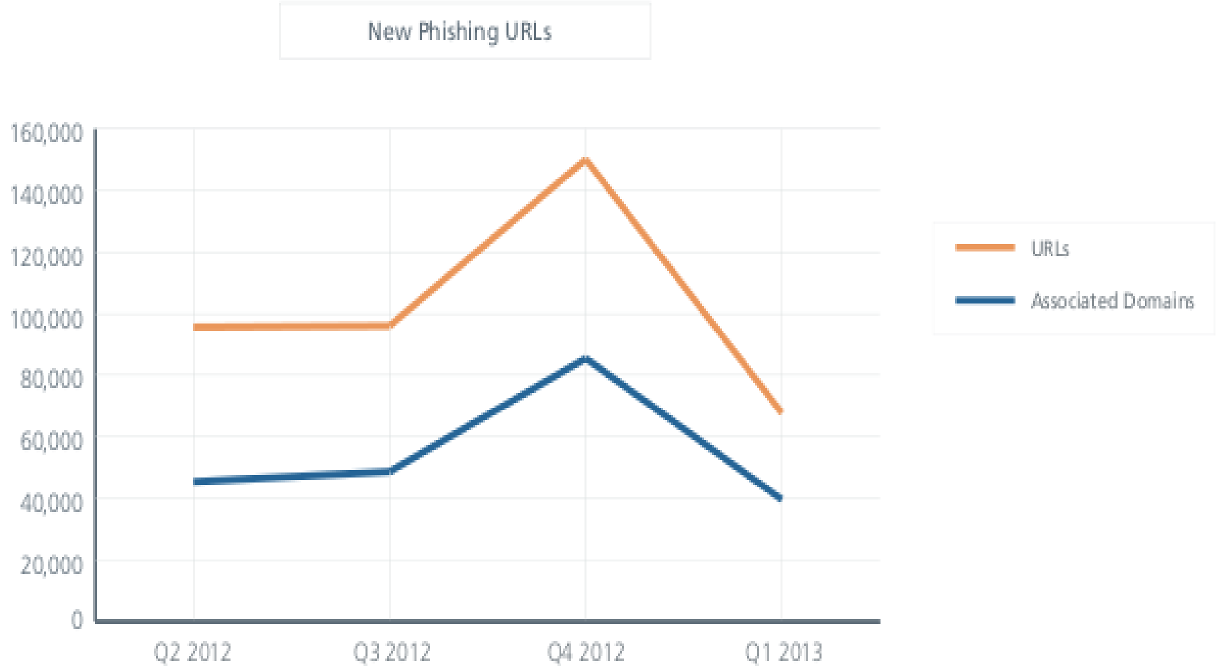
- New types of phishing
  - Watering hole
  - Clone phishing
  - Tabnapping



Top 5 Activity for Malware Destination by Geography

Country	1 in
Netherlands	1 in 108
Luxembourg	1 in 144
United Kingdom	1 in 163
South Africa	1 in 178
Germany	1 in 196

Source: Internet Security Threat Report 2013, Symantec



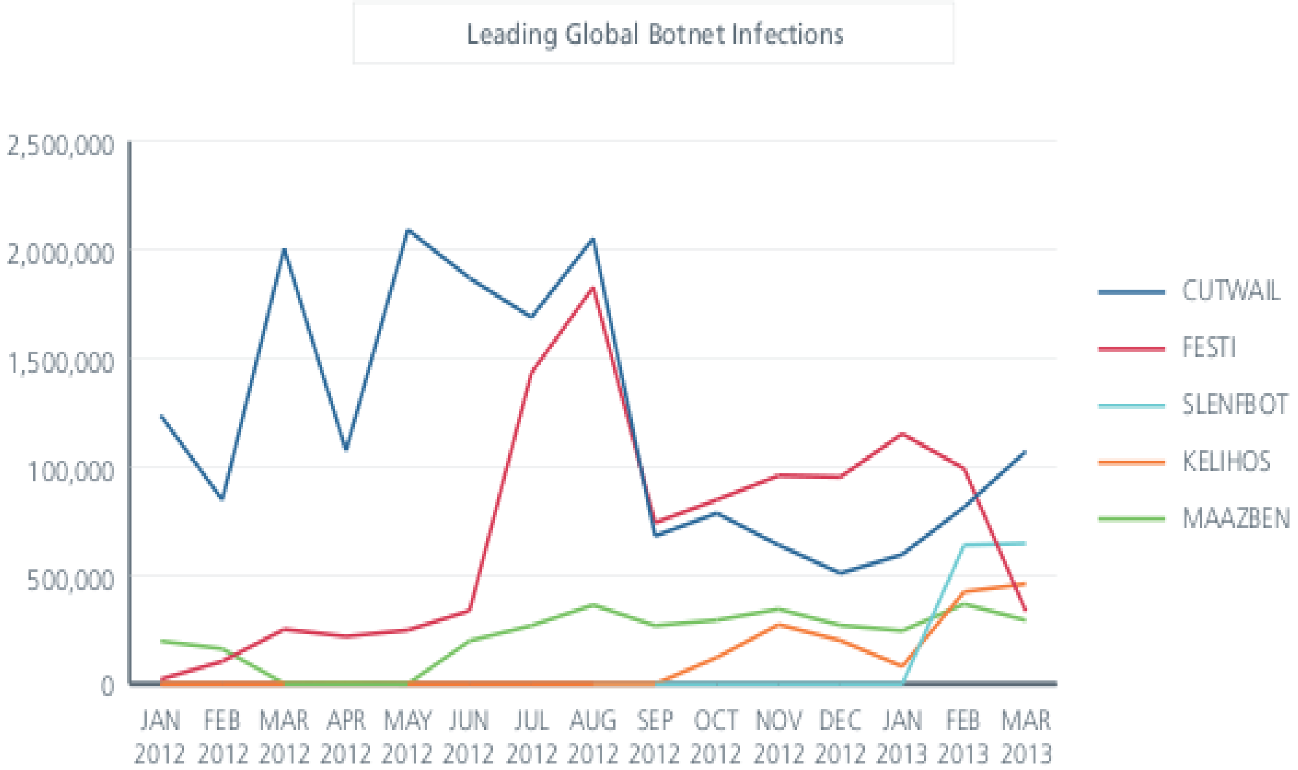
Source: McAfee Threats Report: First Quarter 2013

Online DDoS Extortion

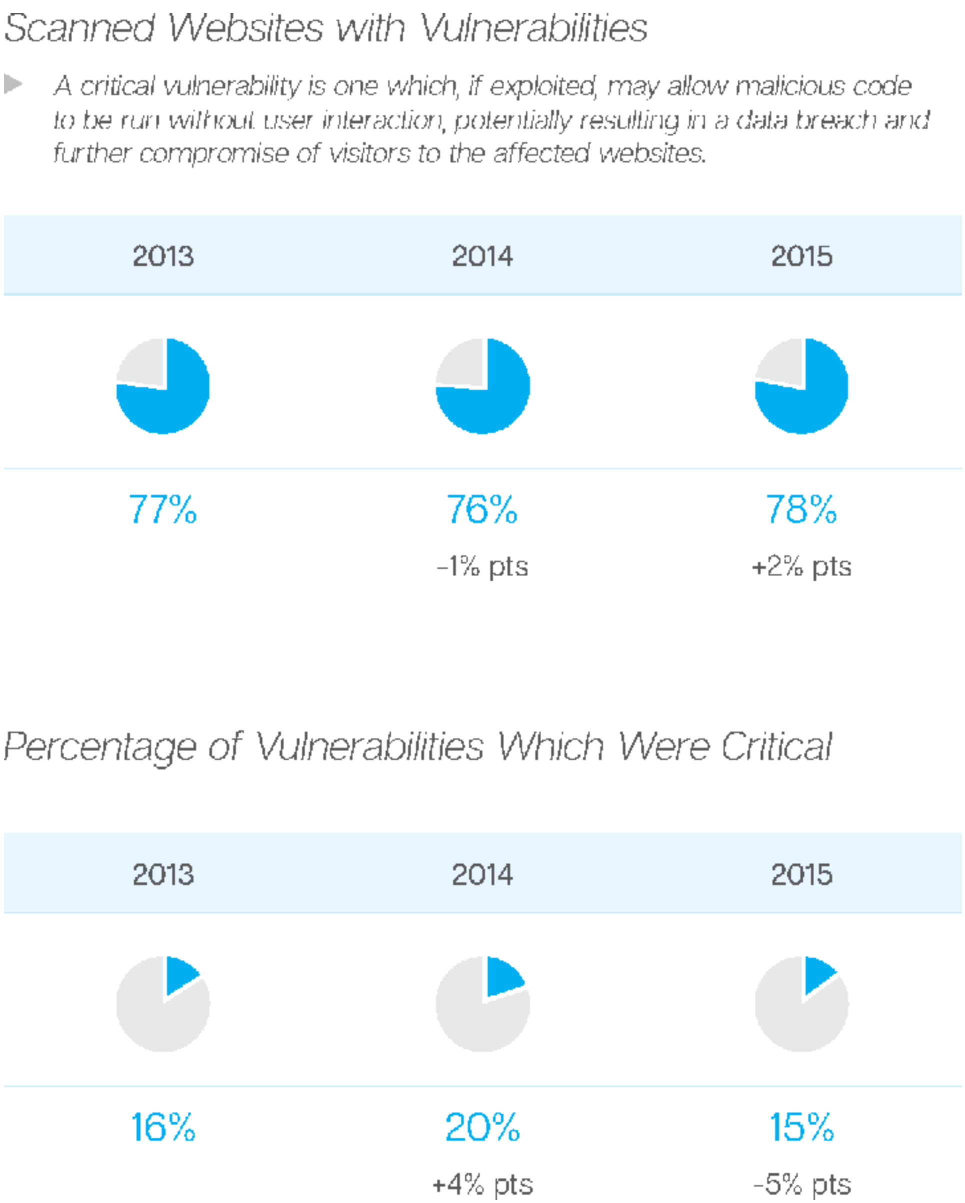
- Extortion: you pay us or you will be attacked
- [*CMU and Information Week, 2004*]
  - 17% of companies surveyed are victims of online extortion.
- [*Alan Paller, SANS Institute, 2004*]
  - 6 or 7 thousand organizations are paying extortion
  - Every online gambling site is paying extortion
- Currently, targets seem to be more selected
  - “Shady” businesses, e.g., Online gambling

Botnets & DDOS

- Botnets now include mobile devices
  - Android botnets
    - http://mobile.slashdot.org/story/13/01/19/0735259/android-botnet-infects-1-million-plus-phones
- DDoS used as a diversion
  - http://www.ic3.gov/media/2012/FraudAlertFinancialInstitutionEmployeeCredentialsTargeted.pdf



Web Vulnerabilities



Scanned Websites with Vulnerabilities

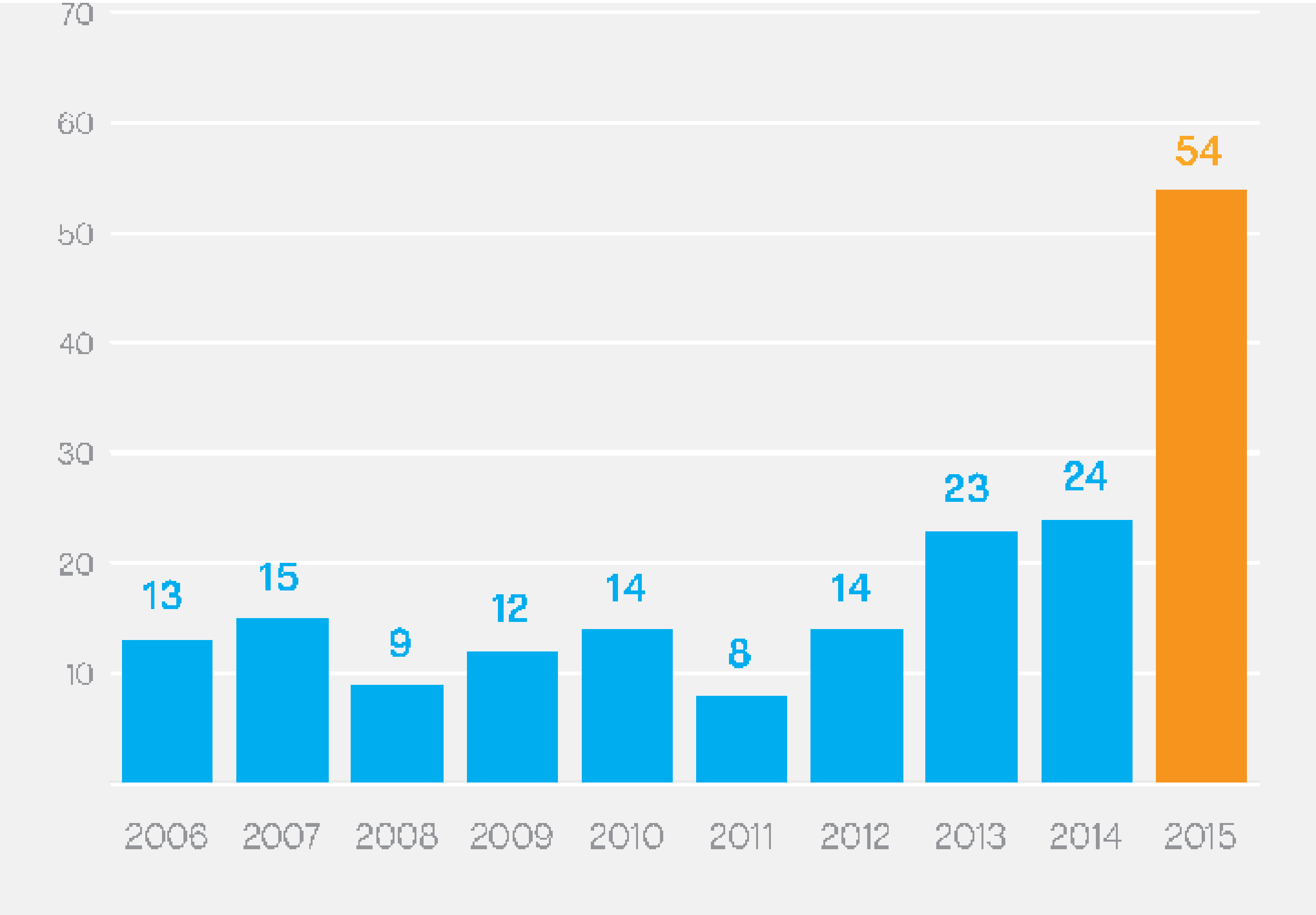
- *A critical vulnerability is one which, if exploited, may allow malicious code to be run without user interaction, potentially resulting in a data breach and further compromise of visitors to the affected websites.*

2013	2014	2015
77%	76%	78%
	-1% pts	+2% pts

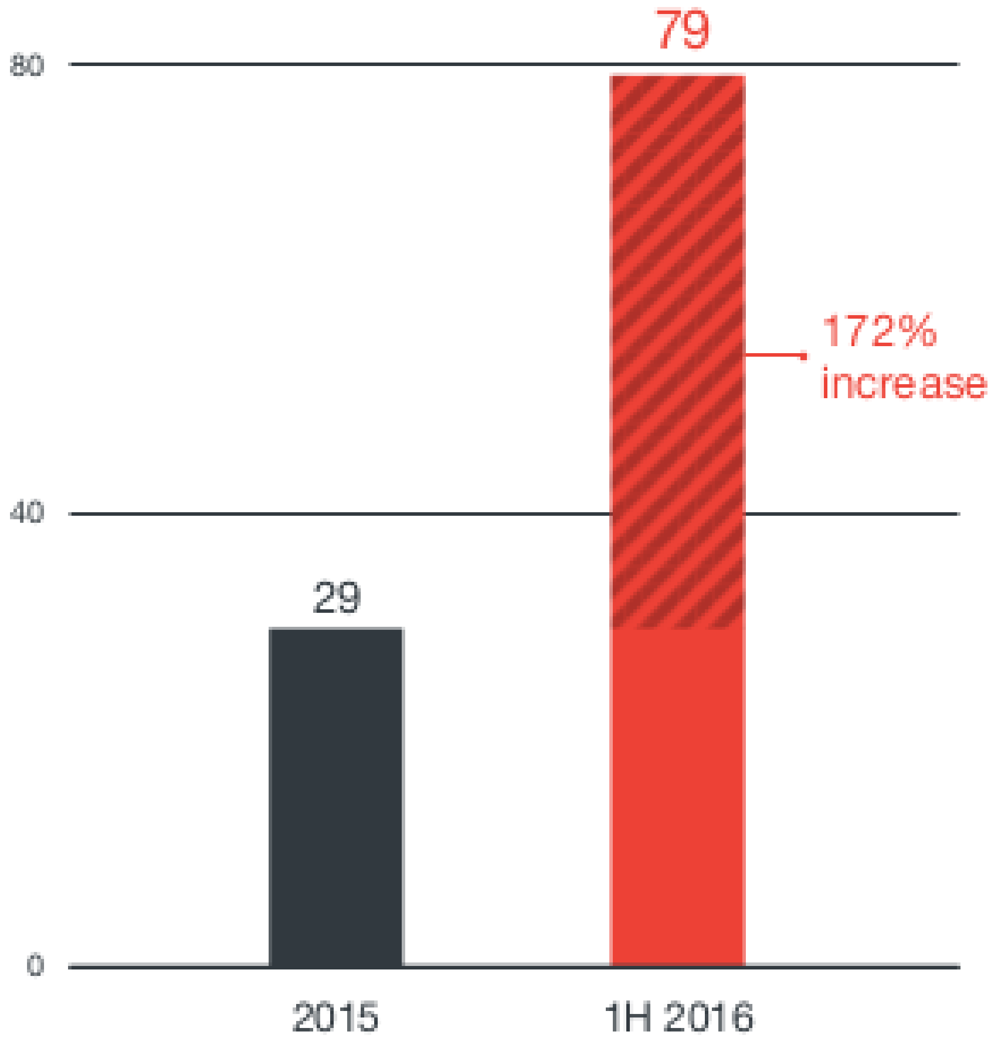
Percentage of Vulnerabilities Which Were Critical

2013	2014	2015
16%	20%	15%
	+4% pts	-5% pts

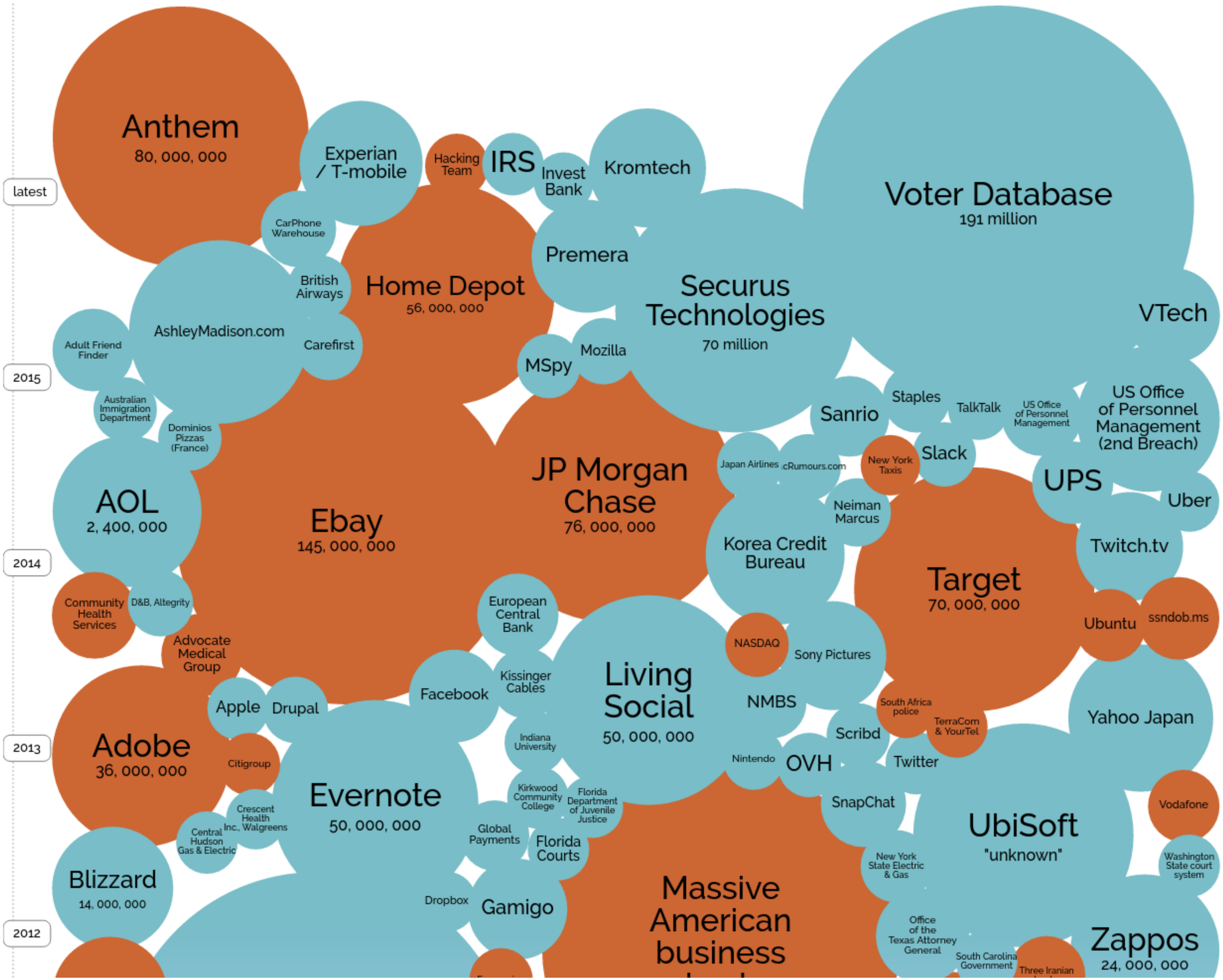
Zero Day Exploits …



Ransomware …



Data Leaks ...


latest
2015
2014
2013
2012
Anthem
80, 000, 000
Experian / T-mobile
Hacking Team
IRS
Invest Bank
Kromtech
Voter Database
191 million
CarPhone Warehouse
Home Depot
56, 000, 000
Premera
Securus Technologies
70 million
VTech
British Airways
AshleyMadison.com
Carefirst
Adult Friend Finder
Mozilla
MSpy
Australian Immigration Department
Dominios Pizzas (France)
Sanrio
Staples
TalkTalk
US Office of Personnel Management
US Office of Personnel Management (2nd Breach)
JP Morgan Chase
76, 000, 000
Japan Airlines
cRumours.com
New York Taxis
Slack
UPS
AOL
2, 400, 000
Ebay
145, 000, 000
Neiman Marcus
Uber
Korea Credit Bureau
Twitch.tv
Target
70, 000, 000
Community Health Services
D&B, Altegrity
European Central Bank
Ubuntu
ssndob.ms
Advocate Medical Group
NASDAQ
Sony Pictures
Living Social
50, 000, 000
Facebook
Kissinger Cables
NMBS
Apple
Drupal
South Africa police
TerraCom & YourTel
Yahoo Japan
Adobe
36, 000, 000
Citigroup
Indiana University
Scribd
Evernote
50, 000, 000
Nintendo
OVH
Twitter
Crescent Health Inc., Walgreens
Kirkwood Community College
Florida Department of Juvenile Justice
SnapChat
Vodafone
Central Hudson Gas & Electric
Global Payments
Florida Courts
UbiSoft
"unknown"
Blizzard
14, 000, 000
New York State Electric & Gas
Washington State court system
Massive American business
Dropbox
Gamigo
Office of the Texas Attorney General
South Carolina Government
Three Iranian
Zappos
24, 000, 000

Underlying Causes

- Untrusted software
  - Malware, including viruses, worms, bots, …
- Configuration errors
  - Default passwords, permissive firewall rules, …
- Human element
  - Insider threats, operator mistakes, social engineering
- Vulnerabilities in trusted software
  - These may be the result of errors in
    - Threat modeling
    - Design/logic
    - Implementation
    - Testing

Stealth and Obfuscation

- Malware wants to remain stealthy
  - So that it can be used in cyber crime (or to achieve other goals of attacker) without being detected
  - Protect “intellectual property”
- Intellectual property protection for legitimate code
  - Make it difficult to reverse-engineer code
  - Introduce watermarks
  - Prevent unauthorized copy of content
- Result
  - Obfuscation techniques

Types of obfuscation

- To thwart static analysis (code obfuscation):
  - Low-level code obfuscations
    - Insert data in the middle of code
    - Violate typical ABI conventions, e.g., call/return, stack use, jumping to the middle of code, dynamic generation or modification code, etc.
    - Code encryption and transformation
  - Higher level code obfuscation
    - Rename functions and variables
    - Control-flow obfuscation
  - Data obfuscation
- To thwart dynamic analysis (behavior obfuscation):
  - Evasion: Carefully match behavior with that of benign software, or employ code/behaviors that do not trigger suspicion
  - Anti-analysis techniques
    - Detect execution within VM, emulator, or a sandbox and alter behavior
  - Combine benign and malicious behaviors, complicating detection

Polymorphic viruses and encryption

- Historically, virus detection relied on “signatures” that captured byte sequences in code that were unique to the virus
- Polymorphism
  - Encrypt virus code so that it can change from one instance to another
  - Basically, change the encryption key from one generation to the next, causing massive changes to byte sequences
- Defense
  - Focus on invariant parts used to pack/unpack
  - Capture unpack/launch behavior (runtime detection)
  - Run virus scanner after unpack

Obfuscation/Metamorphic Viruses

- Metamorphic viruses rewrite their entire code from one generation to next
- No “fixed” part in their code
  - Need not have any code encryption/decryption, so behavior based techniques can be defeated as well
- Metamorphic techniques
  - Use alternative instruction sequences to achieve the same effect
  - More general program obfuscation techniques

Control-flow Obfuscation

- Split or aggregate
    - Basic blocks
    - Loops
        - e.g., one loop becomes two loops or vice-versa
    - Procedures
        - Replace one procedure by two or merge two procedures
        - Inline a procedure, or outline (i.e., create new procedure)
- Reorder
- Insert dead-code (i.e., unreachable code)
    - Obfuscate using conditions
- Replace instruction sequences w/ alternate ones
- Insert conditional jumps using “opaque” predicates
- Insert indirect jumps
- Exploit aliasing and memory errors

Data Obfuscation

- Rename variables
- Split or aggregate variables
  - Split structures into individual variables or vice-versa
- Split individual variables
  - E.g., A = B - C – instead of A, use B and C
  - Clone a variable
- Pad arrays (and possibly structures) with junk elements
- “Encrypt” data values
- Introduce extra levels of indirection
  - Instead of a simple variable, declare a pointer
- Introduce aliasing
- Introduce memory errors
- Introduce additional (or remove) function parameters

Key Issues in Malware Defense

- Plenty of motivation for attackers to remain stealthy
  - Many techniques are available to achieve this
    - Anti-virtualization, anti-analysis, obfuscation, …
- Adaptive
  - Will employ evasion techniques specifically designed to defeat commonly deployed defenses
- Need to assume a strong adversary model
  - Rely on self-protecting defense techniques
    - Ensure defense mechanisms are not compromised by malware
  - Complete mediation
  - Robustness against multi-step attacks (“stepping stones”)

The Human Element

- Growing system complexity contributes to more operator errors
  - misconfigured systems
  - especially problematic in settings where many components interact
- Insider attacks
- Social engineering attacks
- ***Intentionally introduced vulnerabilities***
  - Infiltration into key software or open-source teams
  - Hardware Trojans