Emerging Threats and Attack Trends

Paul Oxman

Cisco Security Research and Operations

Agenda

- What? Where? Why?
- Trends
- 2008/2009 - Year in Review
- Case Studies
- Threats on the Horizon
- Threat Containment

What? Where? Why?

What? Where? Why?

- What is a Threat?

  A warning sign of possible trouble

- Where are Threats?

  Everywhere you can, and more importantly cannot, think of

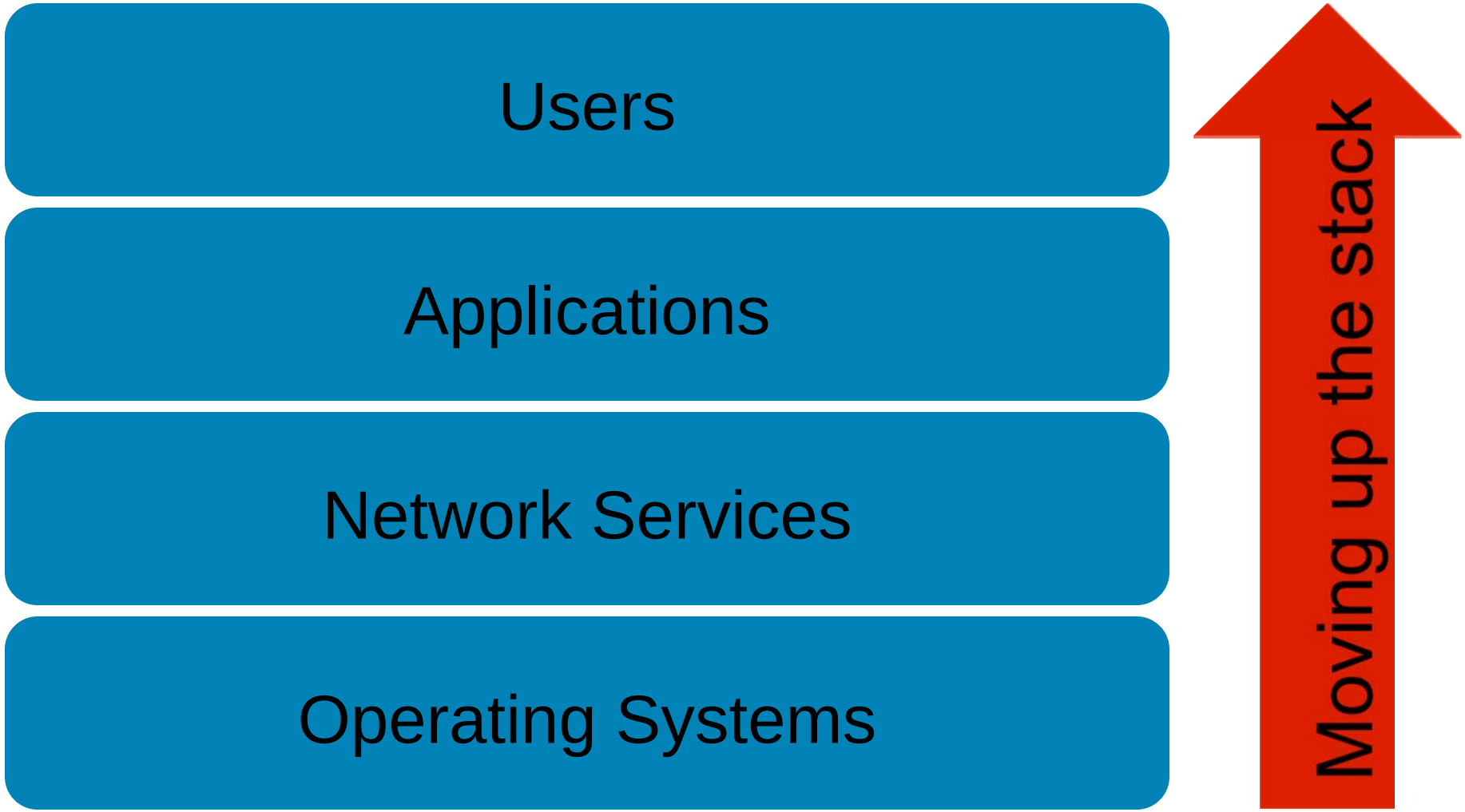
- Why are there Threats?

  The almighty dollar (or euro, etc.), the underground cyber crime industry is growing with each year

Examples of Threats

- Targeted Hacking
- Vulnerability Exploitation
- Malware Outbreaks
- Economic Espionage
- Intellectual Property Theft or Loss
- Network Access Abuse
- Theft of IT Resources

Areas of Opportunity



Why?

- Fame

  Not so much anymore (more on this with Trends)

- Money

  The root of all evil… (more on this with the Year in Review)

- War

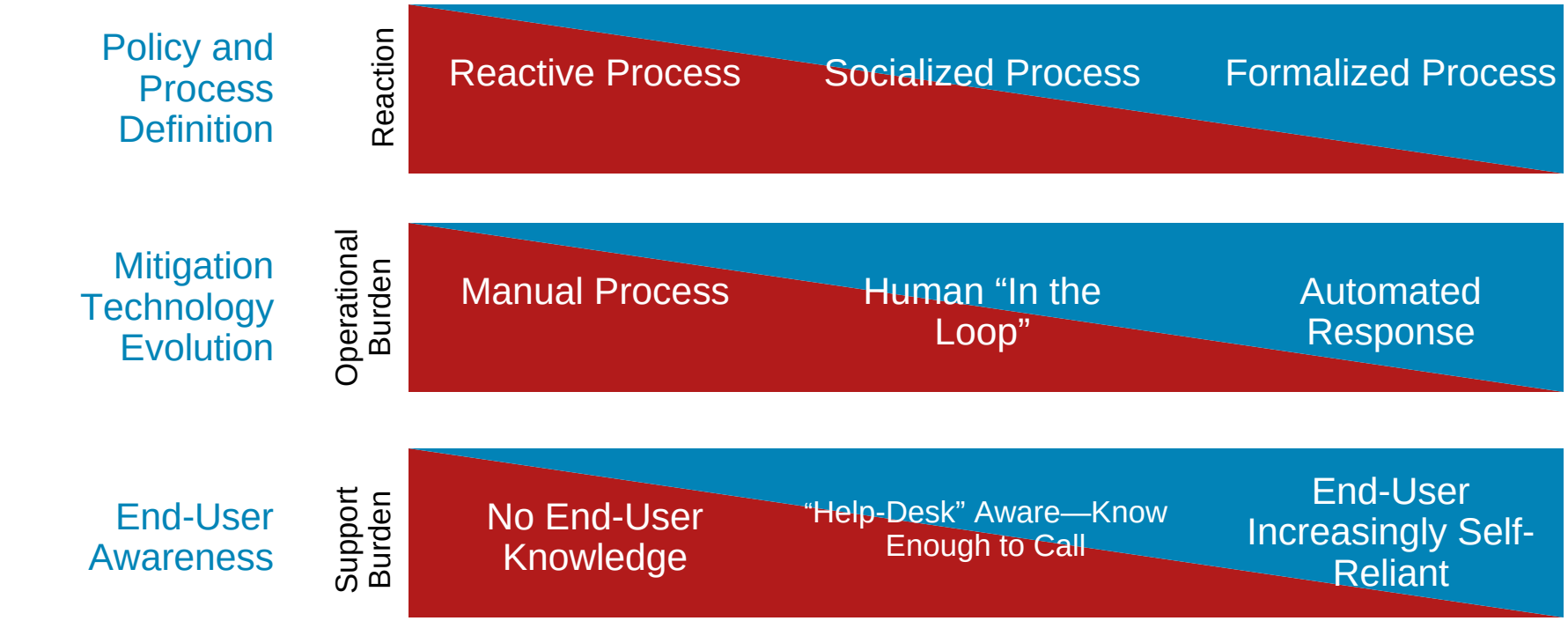
  A battlefront just as real as the air, land, and sea

Operational Evolution of Threats

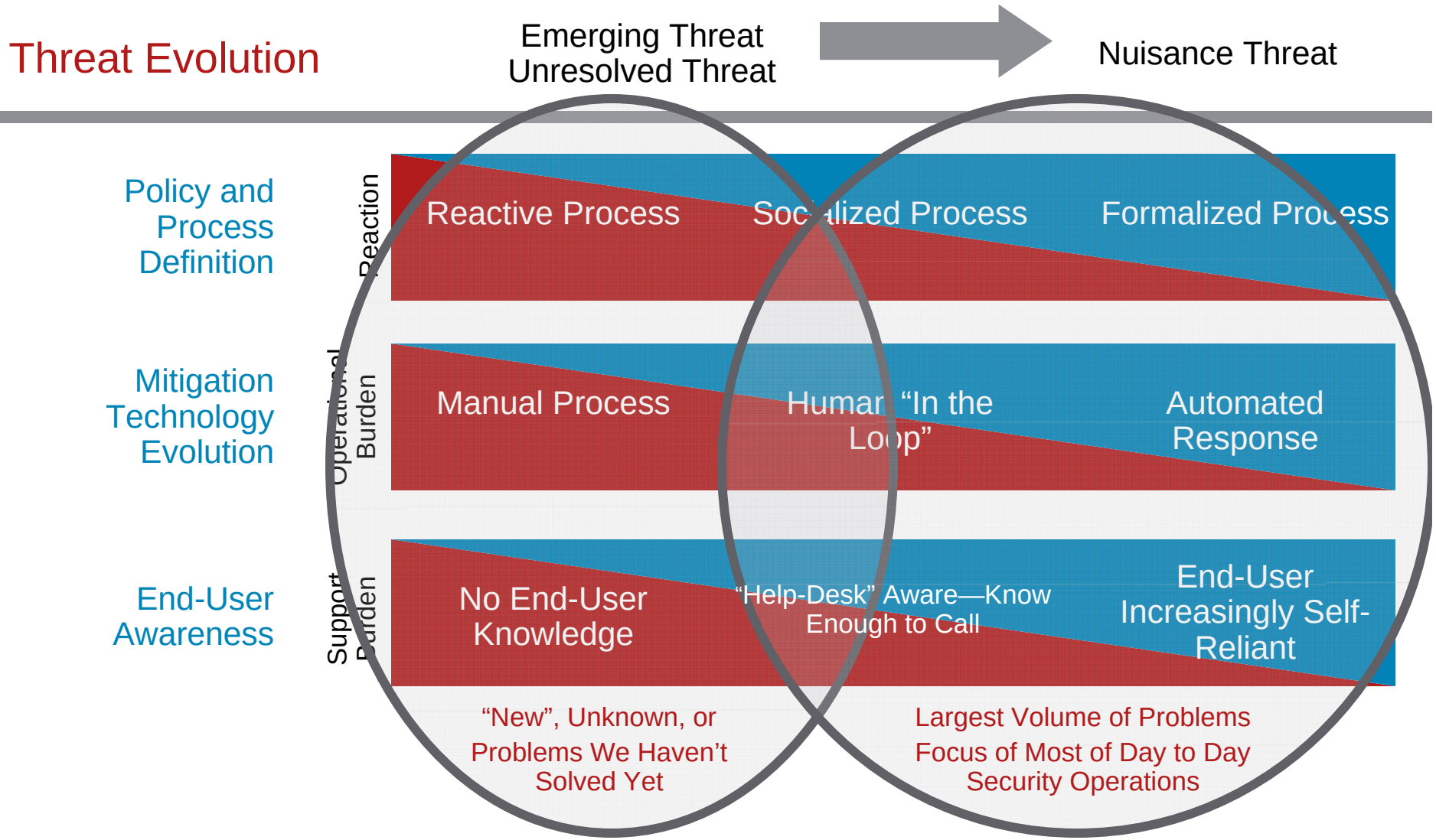
Threat Evolution

Emerging Threat
Unresolved Threat

Nuisance Threat



Operational Evolution of Threats

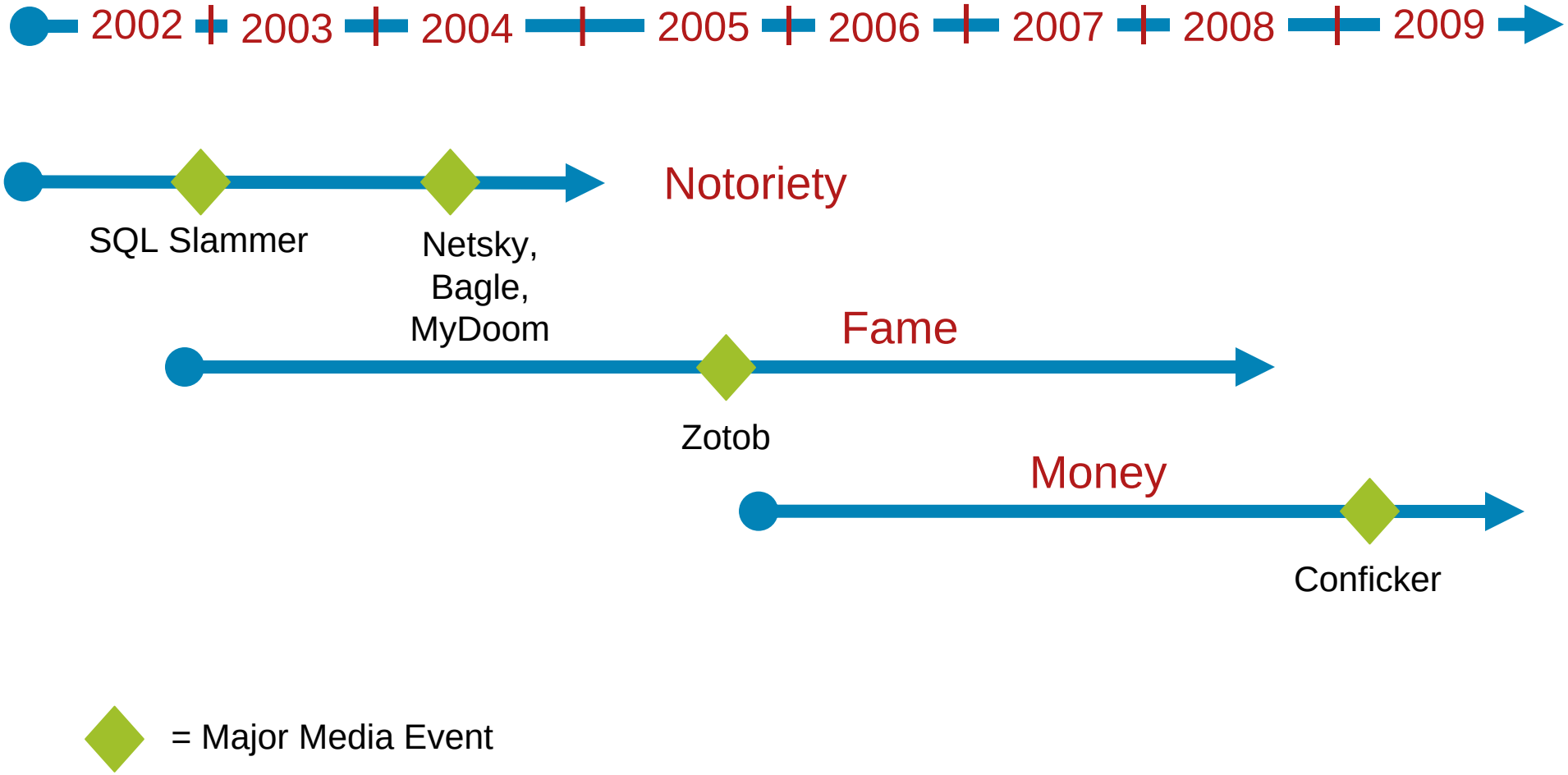


Trends

Trends

- Evolution of intent
- The cybercrime industry
- Designer malcode
- Botnets
- Fast Flux
- Port 80
- Blended attacks
- Phishing
- Web 2.0 abuse
- Data Leakage
- Hacktivism/Cyberwarfare

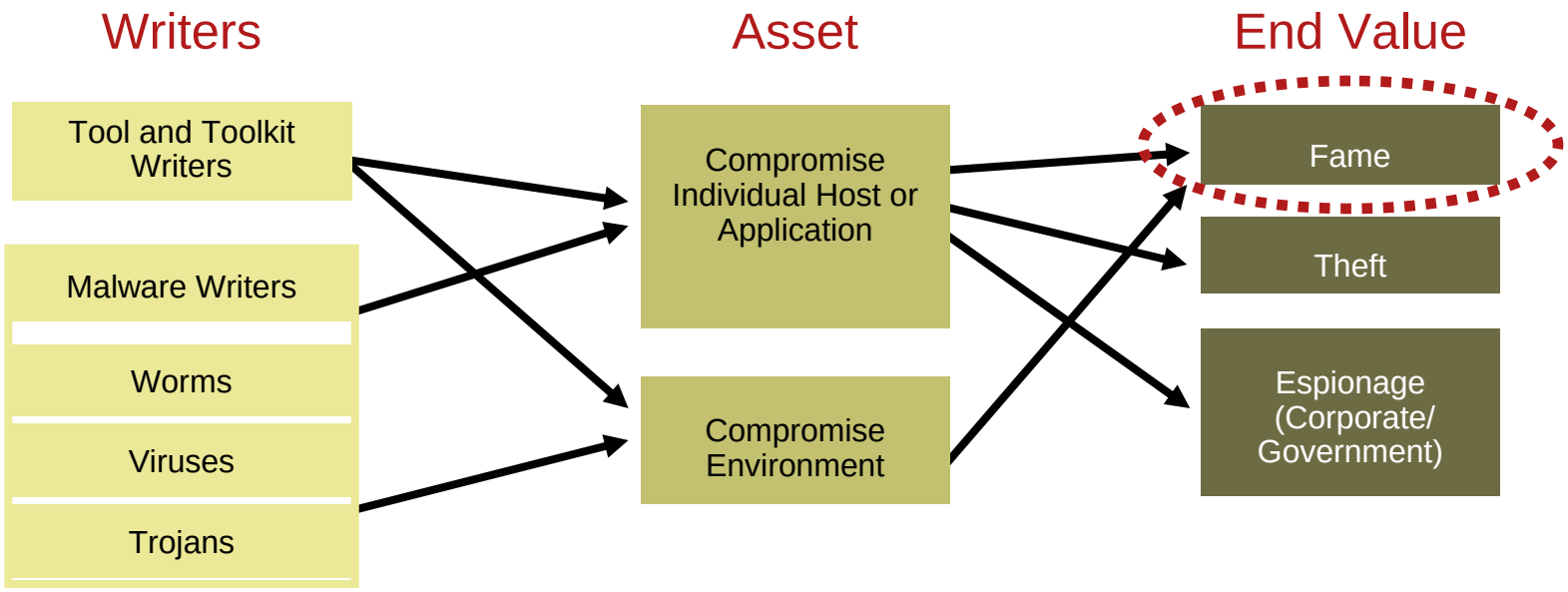
Evolution of Intent



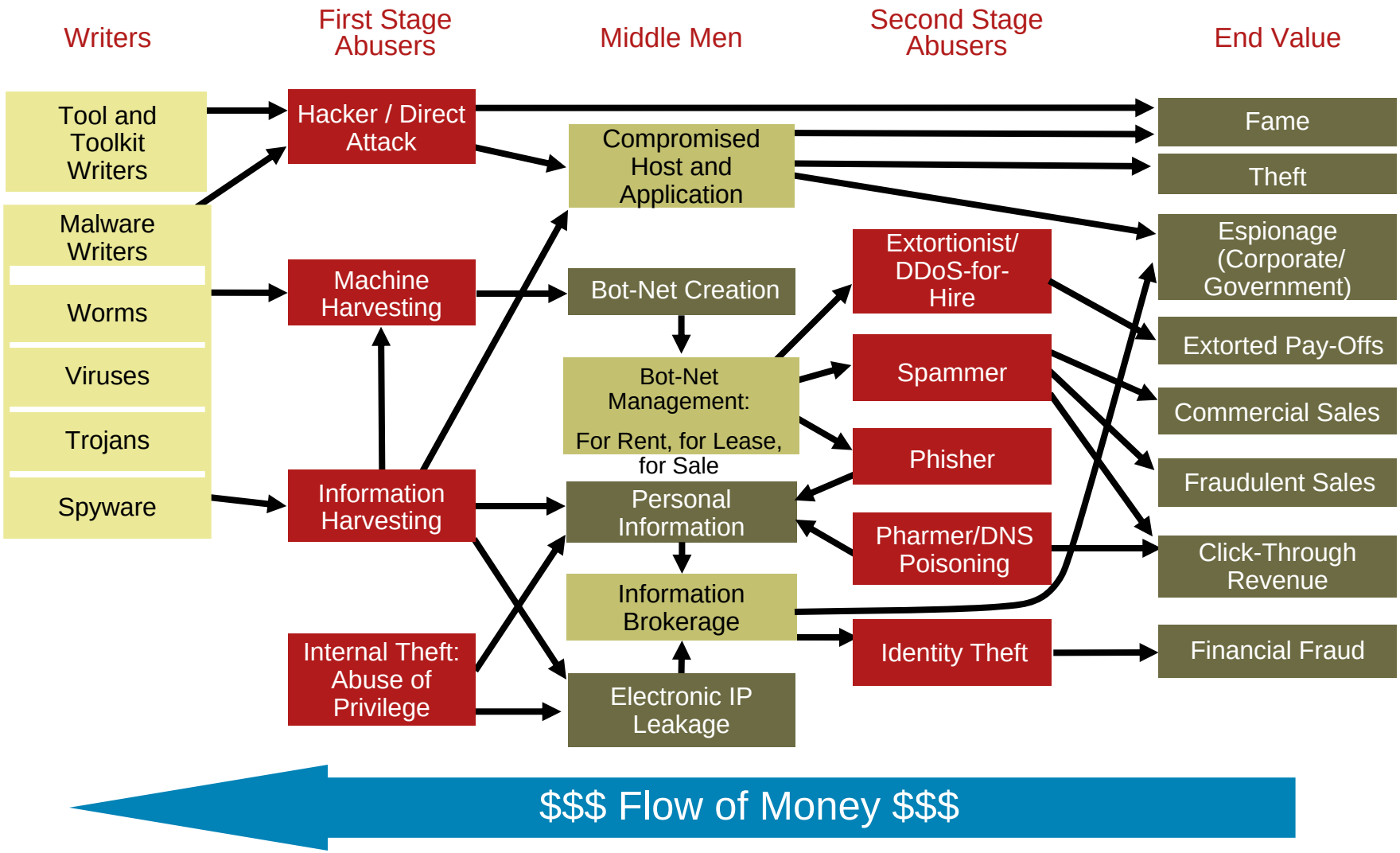
Cybercrime Industry

- Highly intelligent individuals are collaborating to create new viruses and other malicious code
- Software development tools for handling large projects are being used
- Development is not unlike normal software development in the IT industry
- The shared information and talents of many very skilled hackers when working together can be worse than any one working alone

Cybercrime Industry : In the Past



Cybercrime Industry : Today



The Cybercrime Industry

- Group develops custom malcode
- Custom malcode is made available for purchase
- Hosting environments are paid to host malicious code on sites that they control
- Malcode collects usernames and passwords as well as credit card numbers
- Credit card numbers and usernames and passwords are for sale

Designer Malcode – Targeted Attacks

- Malcode that is designed to bypass virus scanners is made for sale
- Malcode is designed to collect information and upload it to a database
- Backup malcode is also available

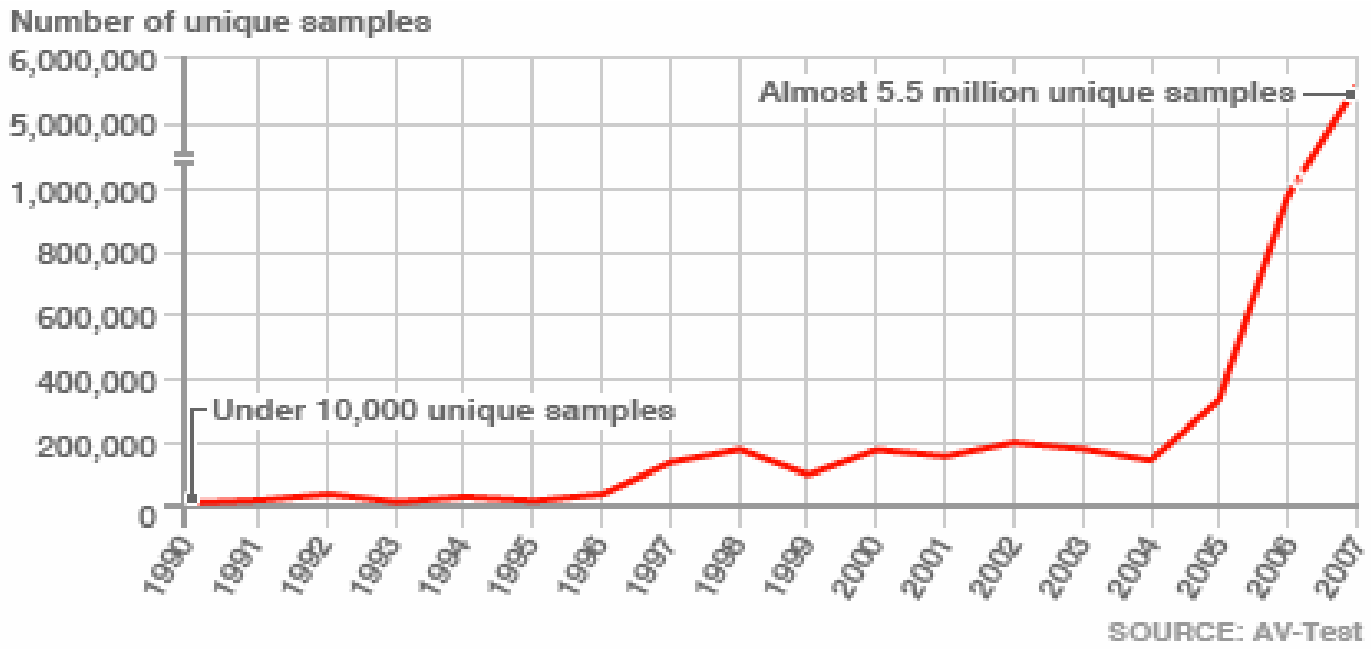
  Replaces the active malcode once it begins to be detected by virus scanners

- Malcode is designed to be very difficult to reverse engineer

  Harder to detect and harder to trace where the data is being sent

Rise of unique malcode

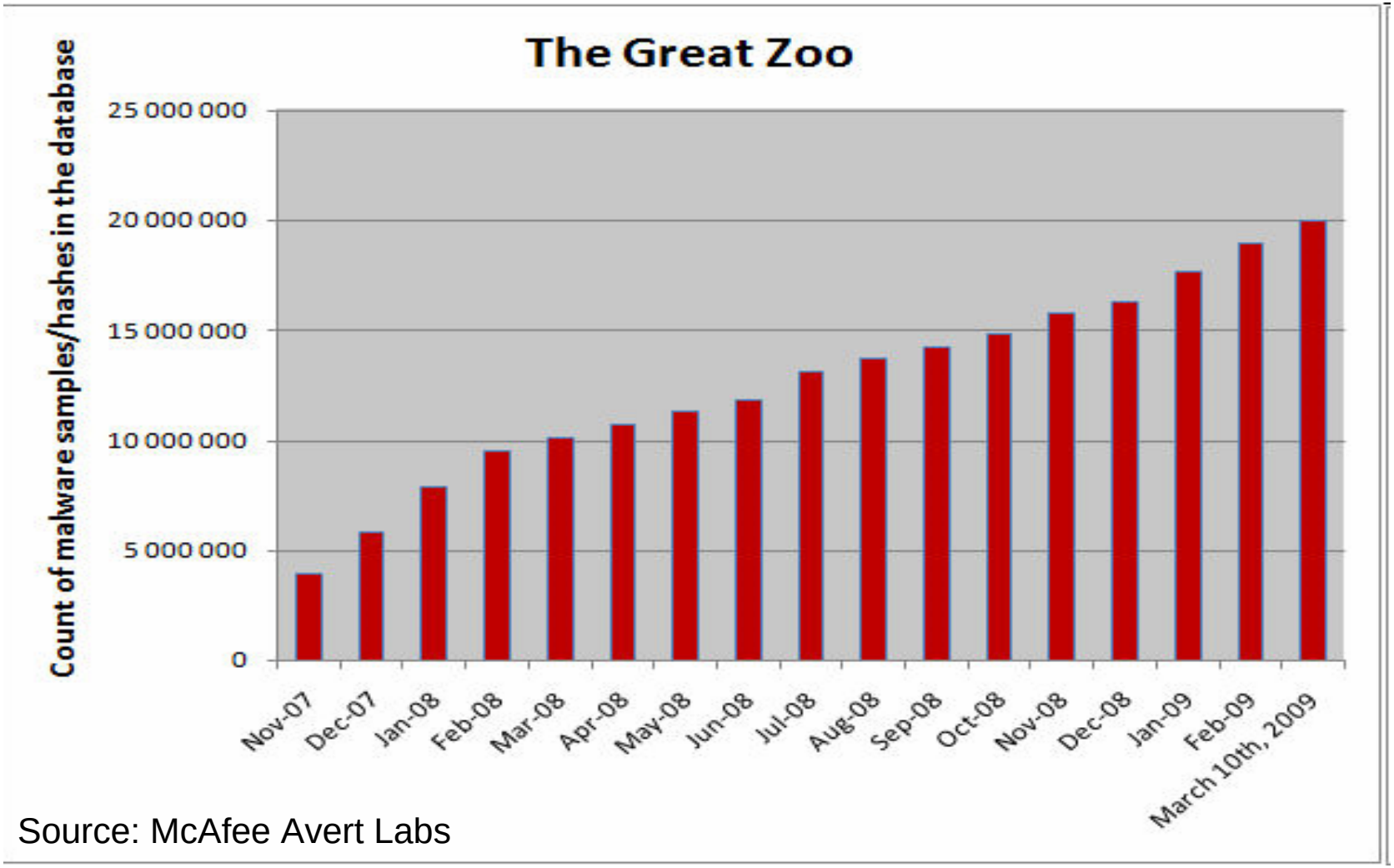
Unique Samples of Malicious Programs



# of Unique Malware Samples in 2006: 972K
# of Unique Malware Samples in 2007: 5.5M

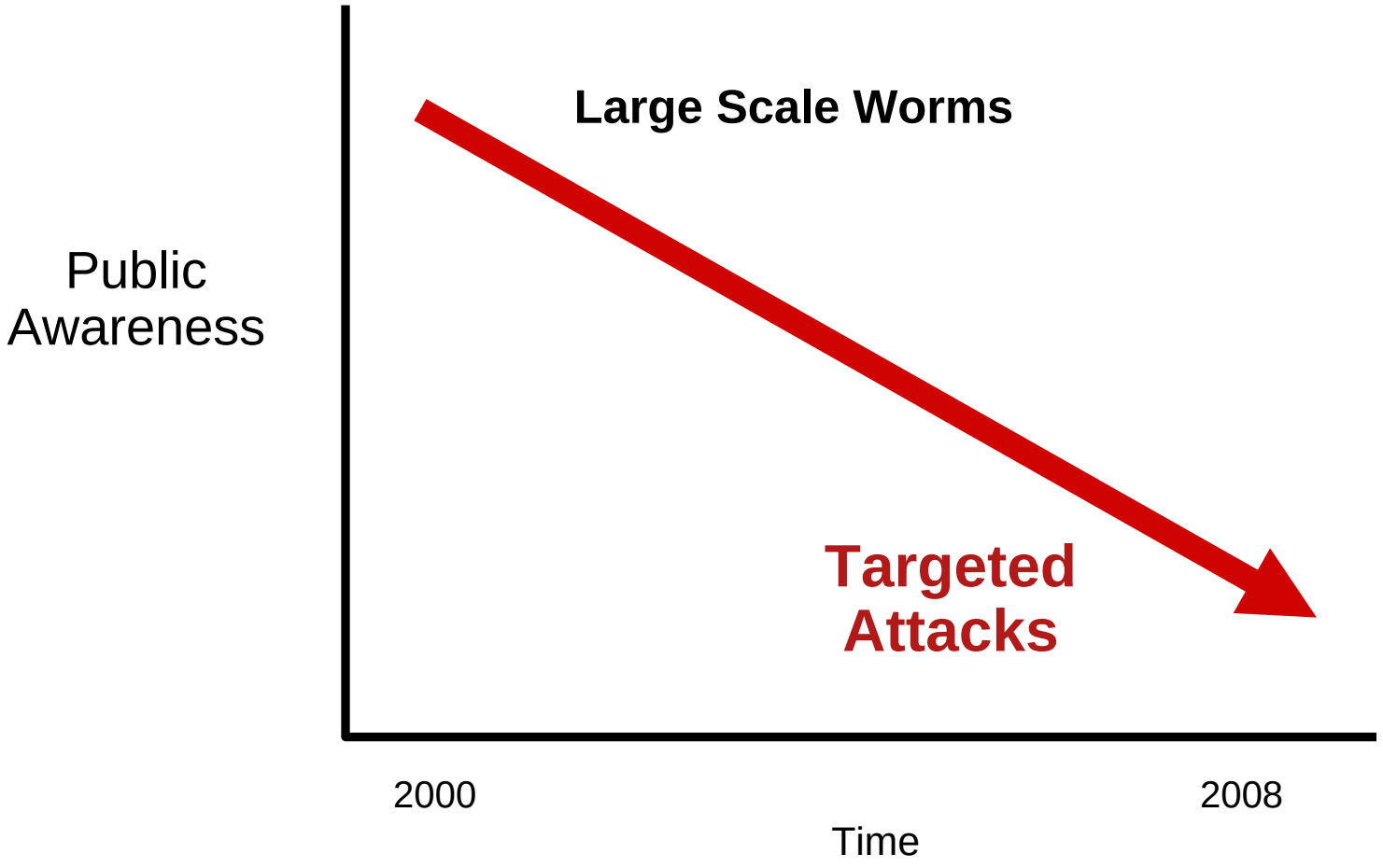
500% Increase in 12 Months

Rise of unique malcode (cont)

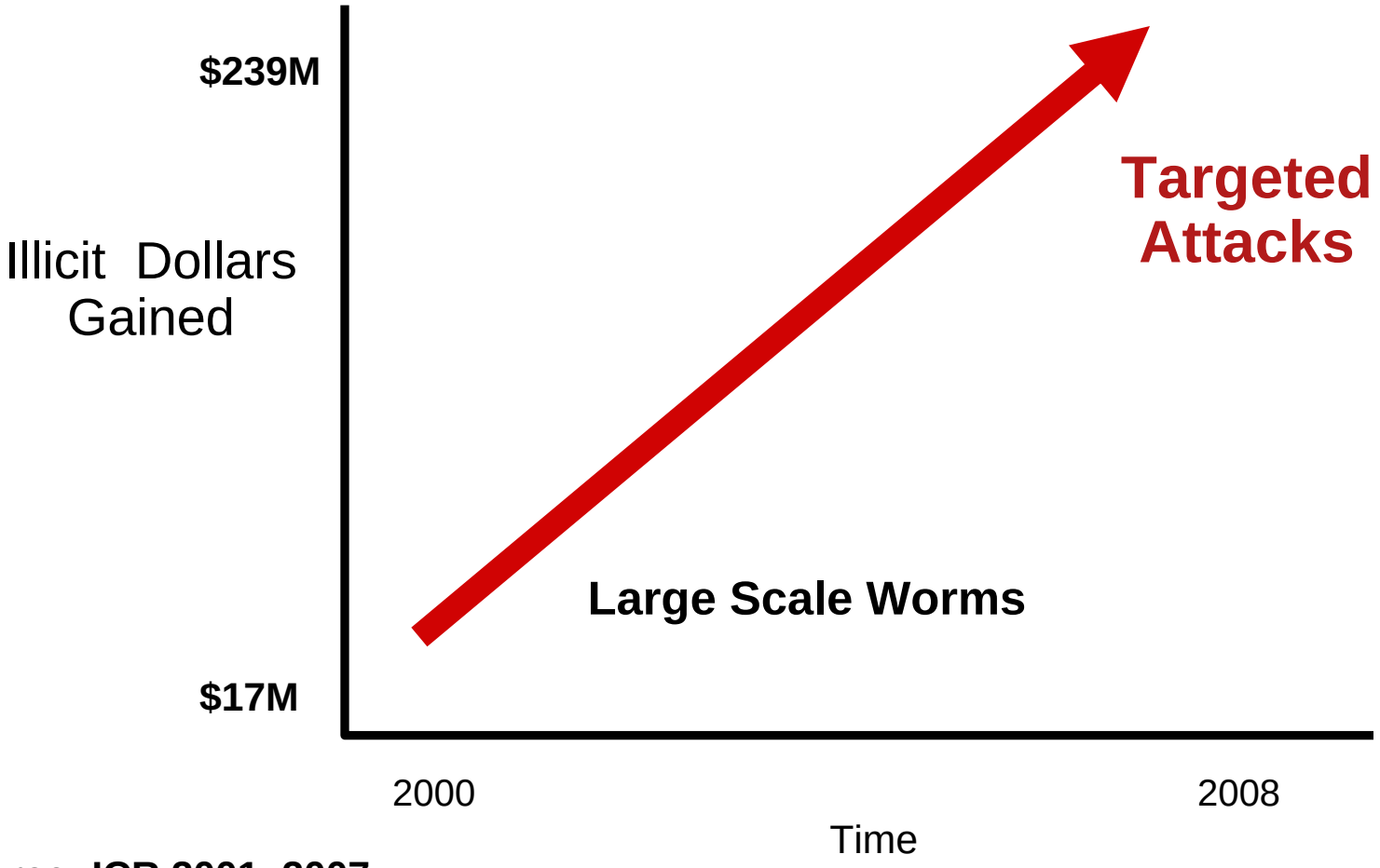


Source: McAfee Avert Labs

“Noise” Level



Cyber Crime Profit Level



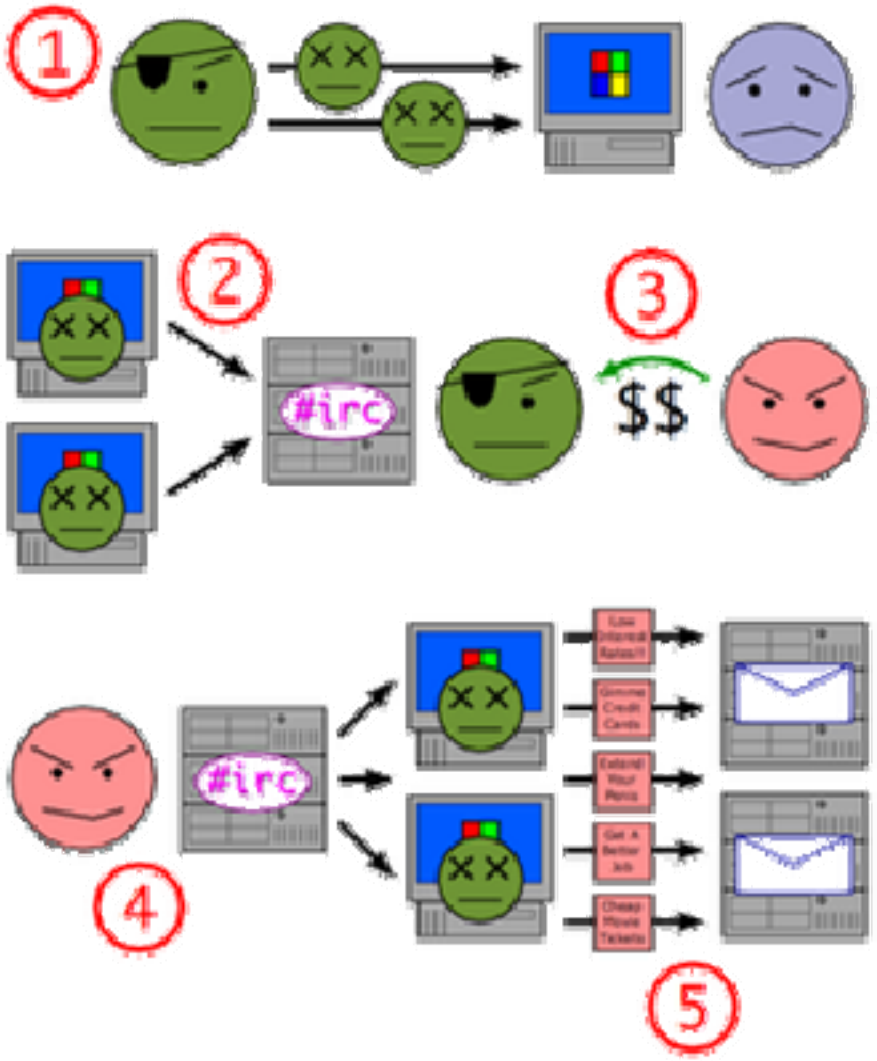
Source: ICR 2001, 2007

Botnets

- Botnet: A collection of compromised machines running programs under a common command and control infrastructure
- Building the Botnet:
  - Viruses, worms; infected spam; drive-by downloads; etc.
- Controlling the Botnet:
  - Covert-channel of some form; typically IRC or custom IRC-like channel
  - Historically have used free DNS hosting services to point bots to the IRC server
  - Recent attempts to sever the command infrastructure of botnets has resulted in more sophisticated control systems
  - Control services increasingly placed on compromised high-speed machines (e.g. in academic institutions)
  - Redundant systems and blind connects are implemented for resilience
- See **Infiltrating a Botnet**: http://www.cisco.com/web/about/security/intelligence/bots.html

Source: www.wikipedia.com

Using a Botnet to Send Spam

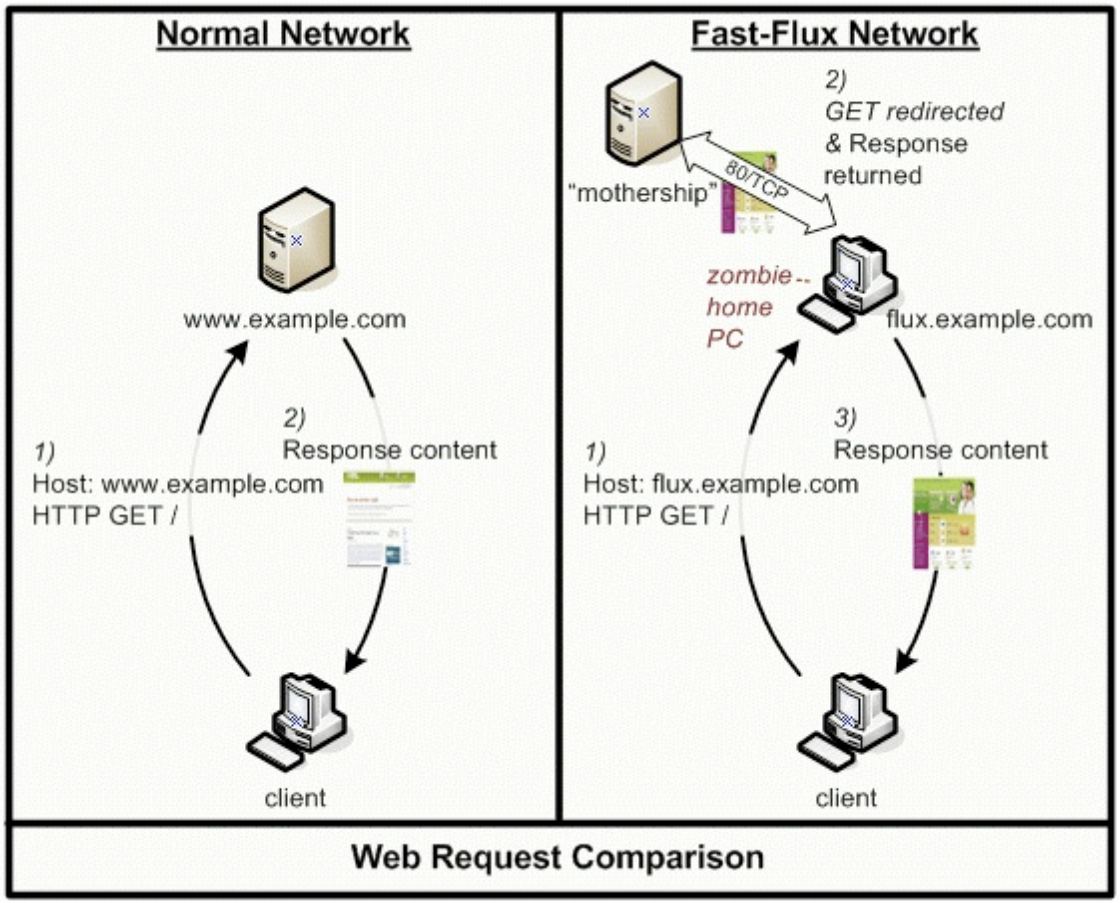


1. A botnet operator propagates by viruses, worms, spam, and malicious websites
1. The PCs log into an IRC server or other communications medium
1. A spammer purchases access to the botnet from the operator
1. The spammer sends instructions via the IRC server to the infected PCs—
1. ... causing them to send out spam messages to mail servers

Source: www.wikipedia.com

Fast Flux

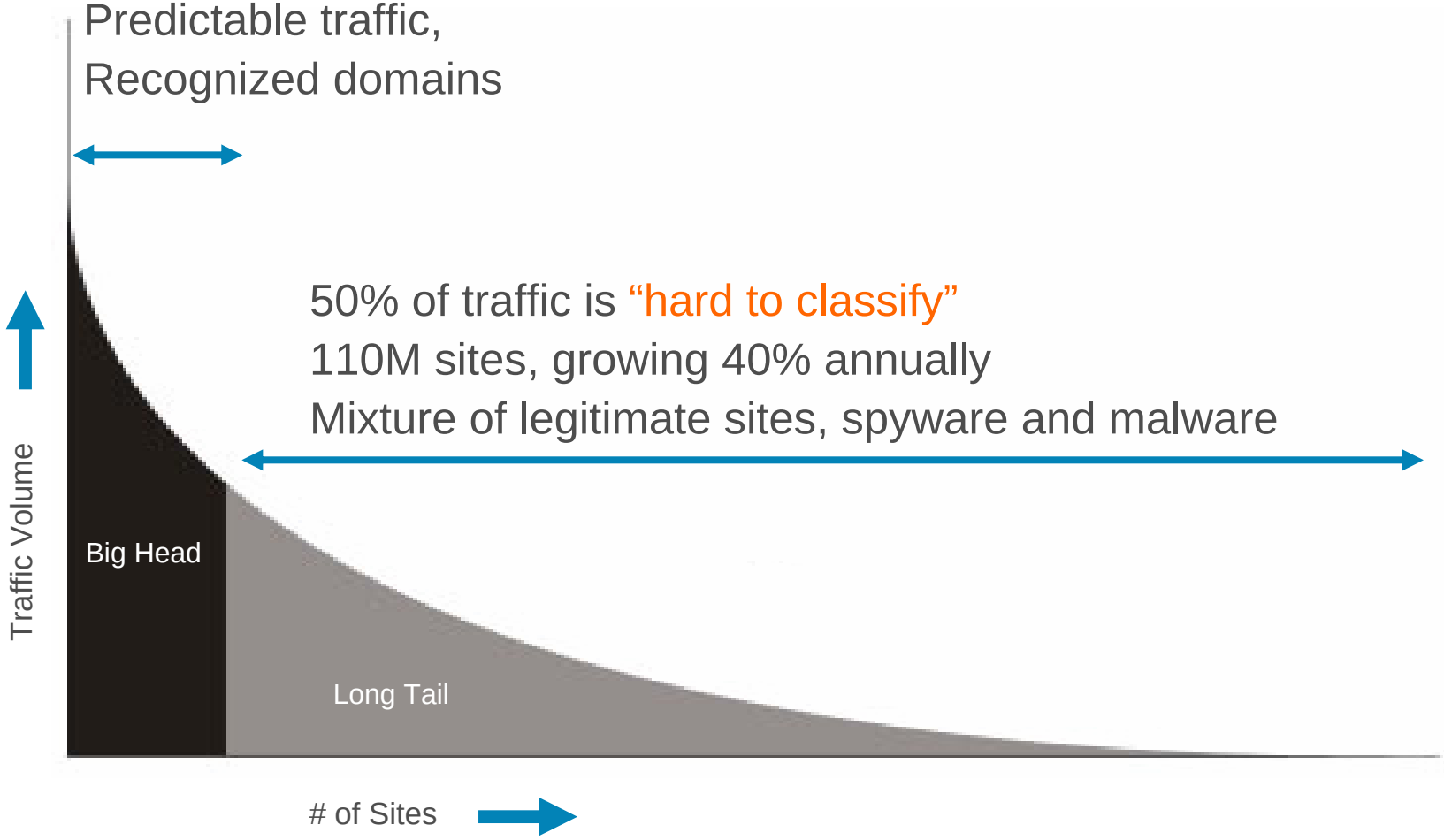
- Control system is hidden
- Very low time to live (TTL) in A Record
- Botnets are the new DNS servers



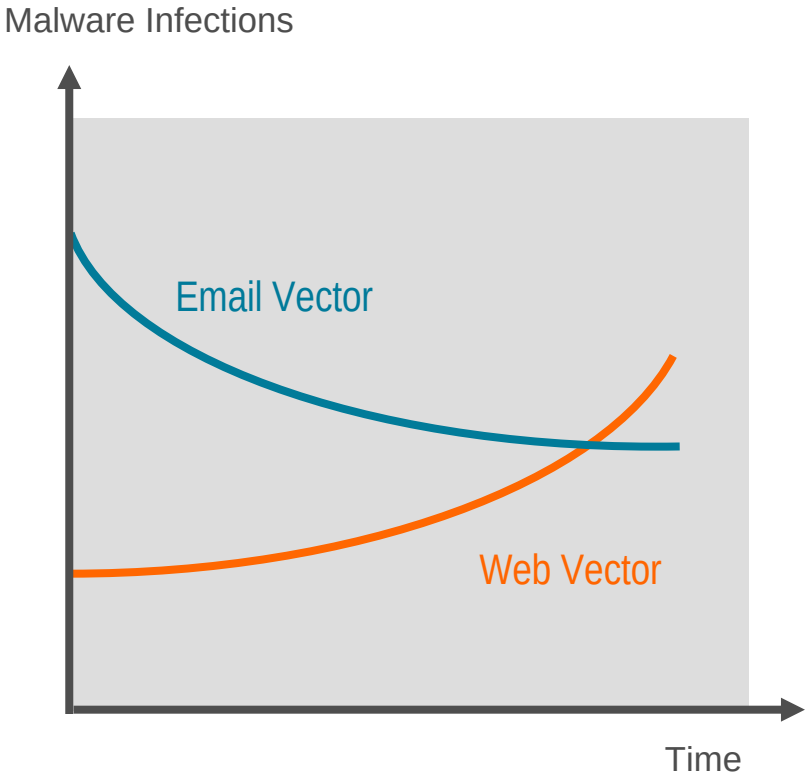
Source: honeynet.org

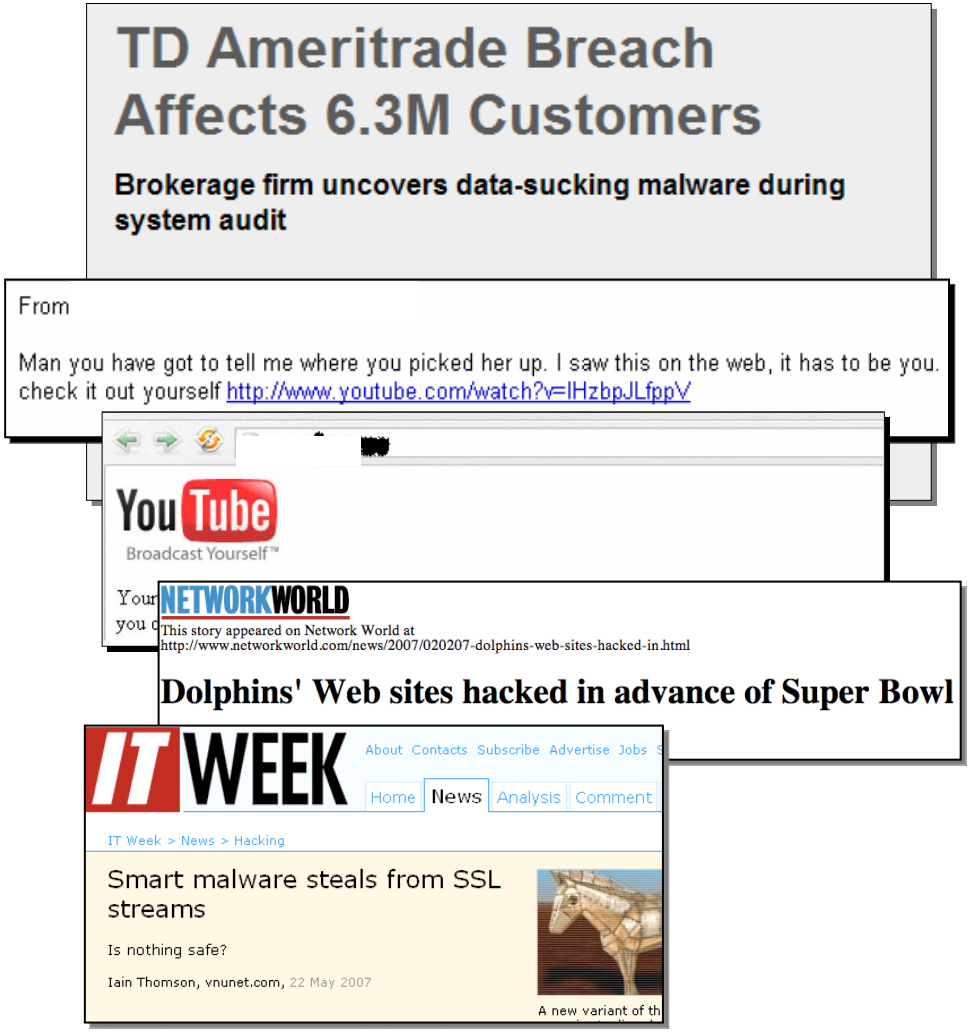
Port 80 – The New Internet

50% of traffic is "easy to classify"
Predictable traffic,
Recognized domains



Malware Threat Distribution





Malware infection vectors are shifting from email to web

Blended Attacks

- Malicious “anti-spyware” sites.

  antispyware911.com

- Spoofed NFL sites

  Game tracker download was actually Storm

- Spurious Youtube sites

  Click play actually downloads malware

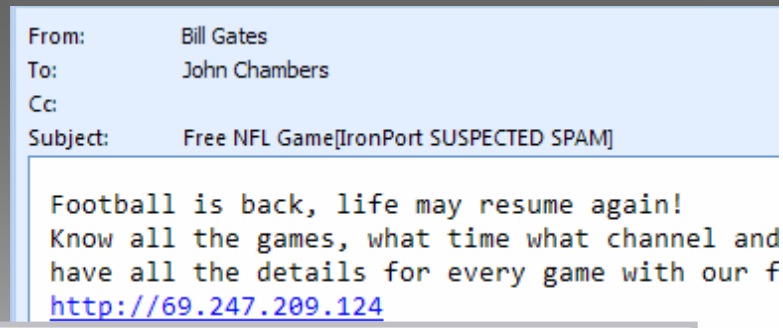
- Youth-oriented applications and sites

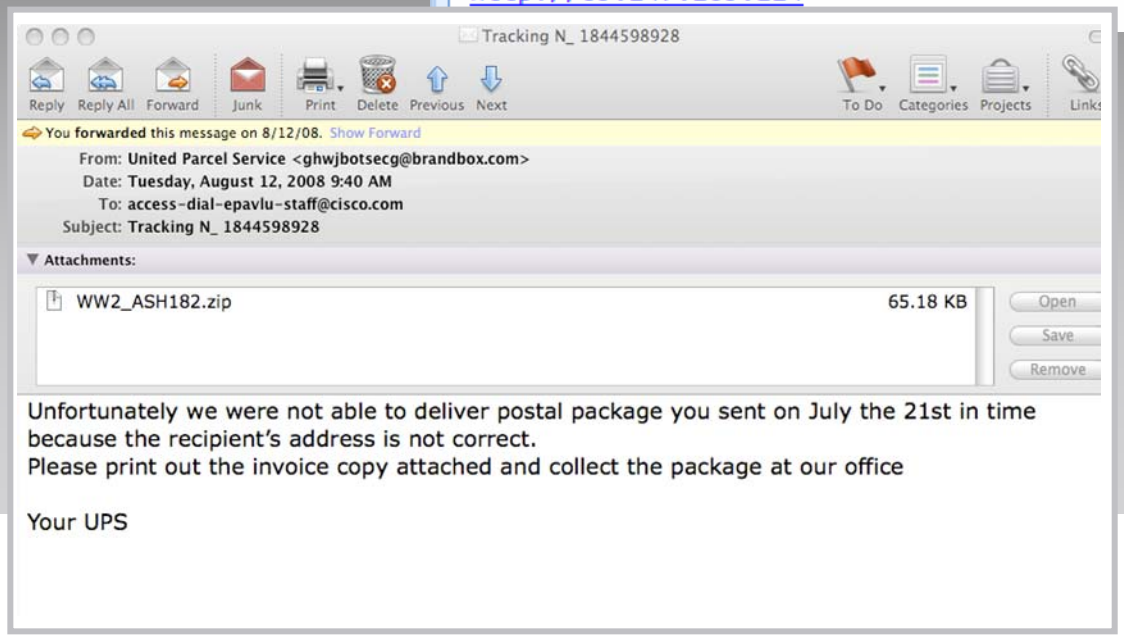
  Free Games, Psycho kitty

* More on this later

Next Generation Spam

- Growing in sophistication
  - Targeted
  - Blending email and web
- New vectors, including SMS vishing
- Extensive use of social engineering



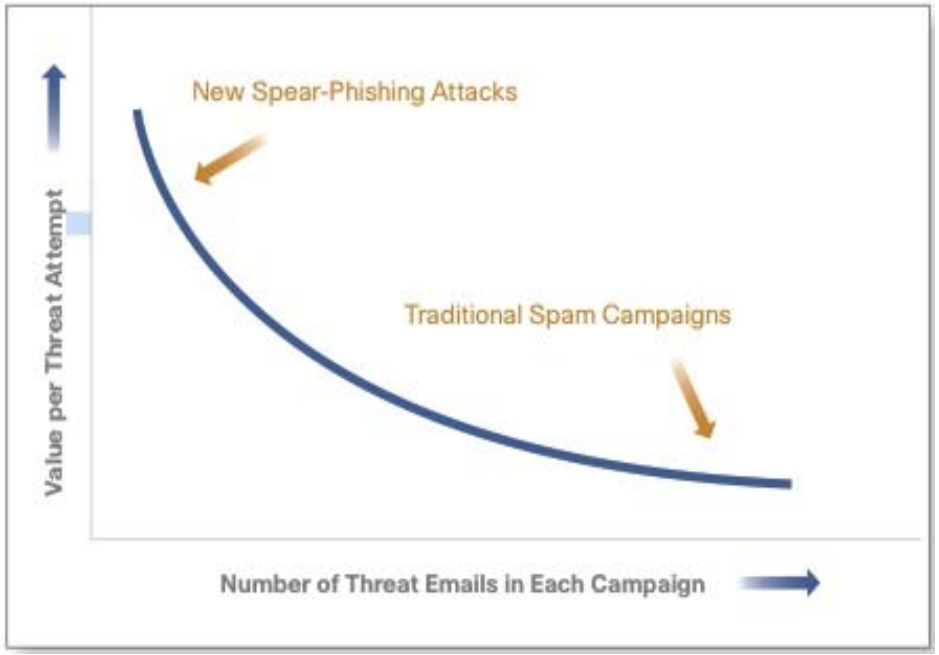


Phishing and its variants

- Traditional phishing still in use
- Spear-phishing

  Targeted phishing attempts
- Whaling

  Phishing attempts specifically targeting a high value target



Web 2.0 Abuse

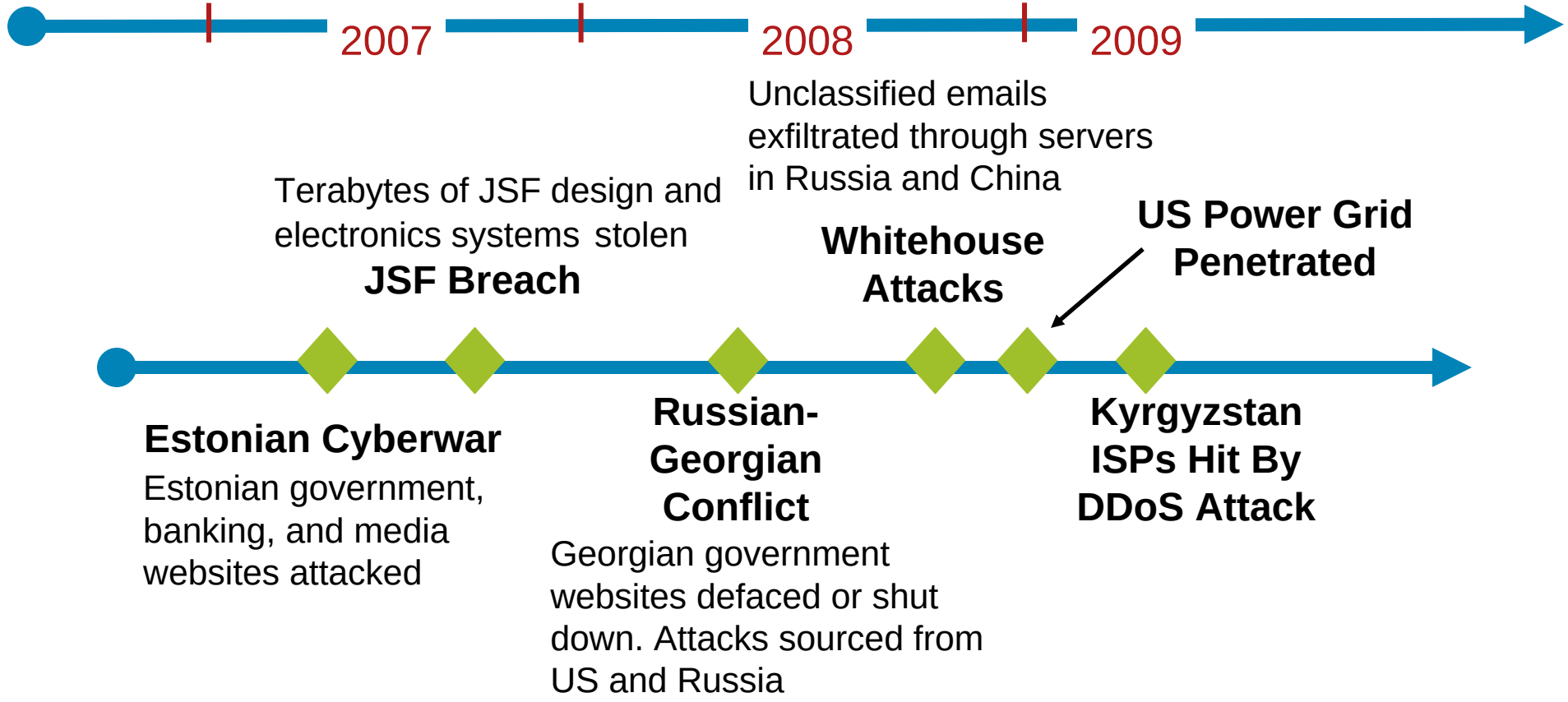
- Commercial tools for account creation, posting, CAPTCHA*, IP rotation are readily available
- Targets popular sites and blogs including including gmail, Yahoo!, MySpace and Craigslist
- Enables abuse of many services including webmail account creation for spamming

*Completely Automated Public Turing test to tell Computers and Humans Apart."

Data Leakage

- Marine One classified data found on computer in Iran
  - Included avionics info, schematics on radar and missile defense
  - Peer-to-peer to blame
- Los Alamos National Labs has 80 computers go missing
  - 13 computers stolen
  - 67 missing
  - BlackBerry lost in a sensitive foreign country

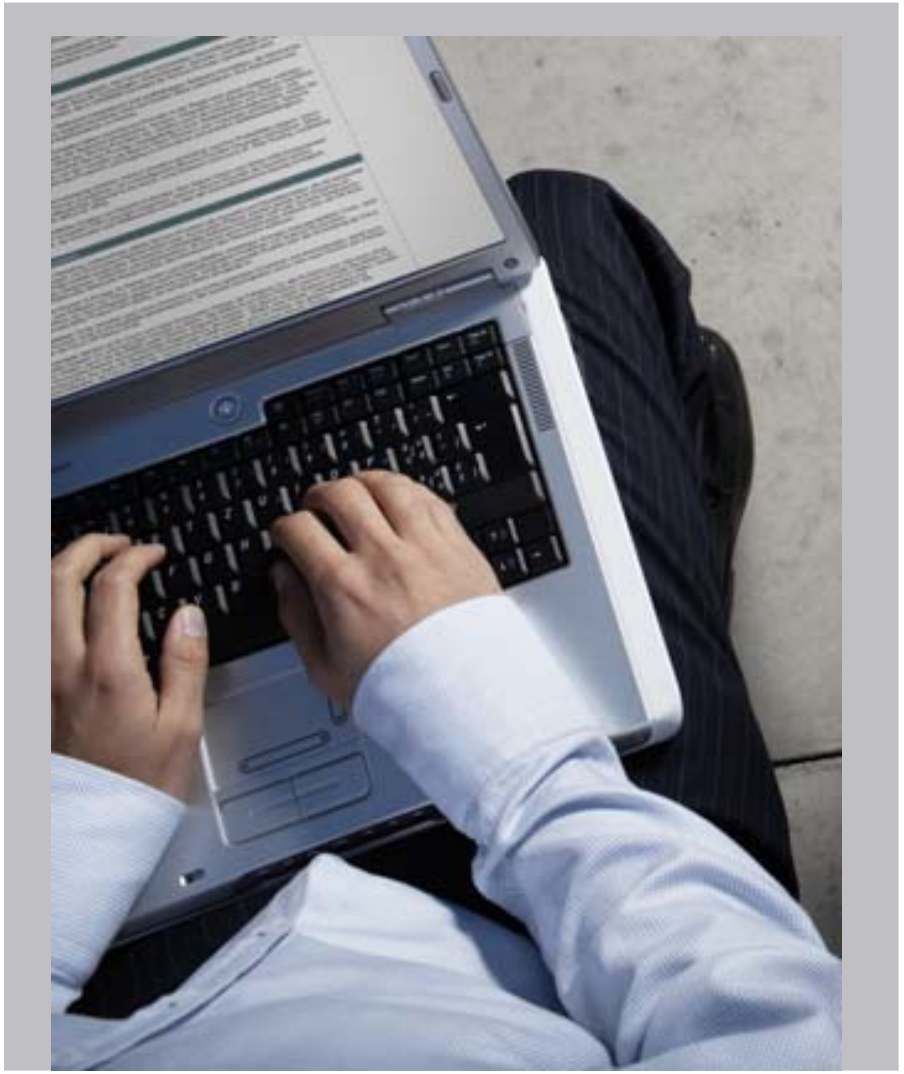
Hacktivism/Cyberwarfare



- Future conflicts more likely to include Internet component
- Botnet activity likely to increase during conflicts
- Cyber-commands forming to counter

What Does This Mean?

- Threats and criminals are faster, smarter & more covert
- Criminals have more vulnerabilities to exploit
- Criminals are evolving their techniques, users must stay current



Year in Review

2008 as a year

- 70% of top 100 web sites pointed to (or contained) malware

  According to a Websense report

- Number of vulnerabilities up 11% from 2007

  According to the Cisco IntelliShield

- Spam accounts for 90% of email today

  According to IronPort

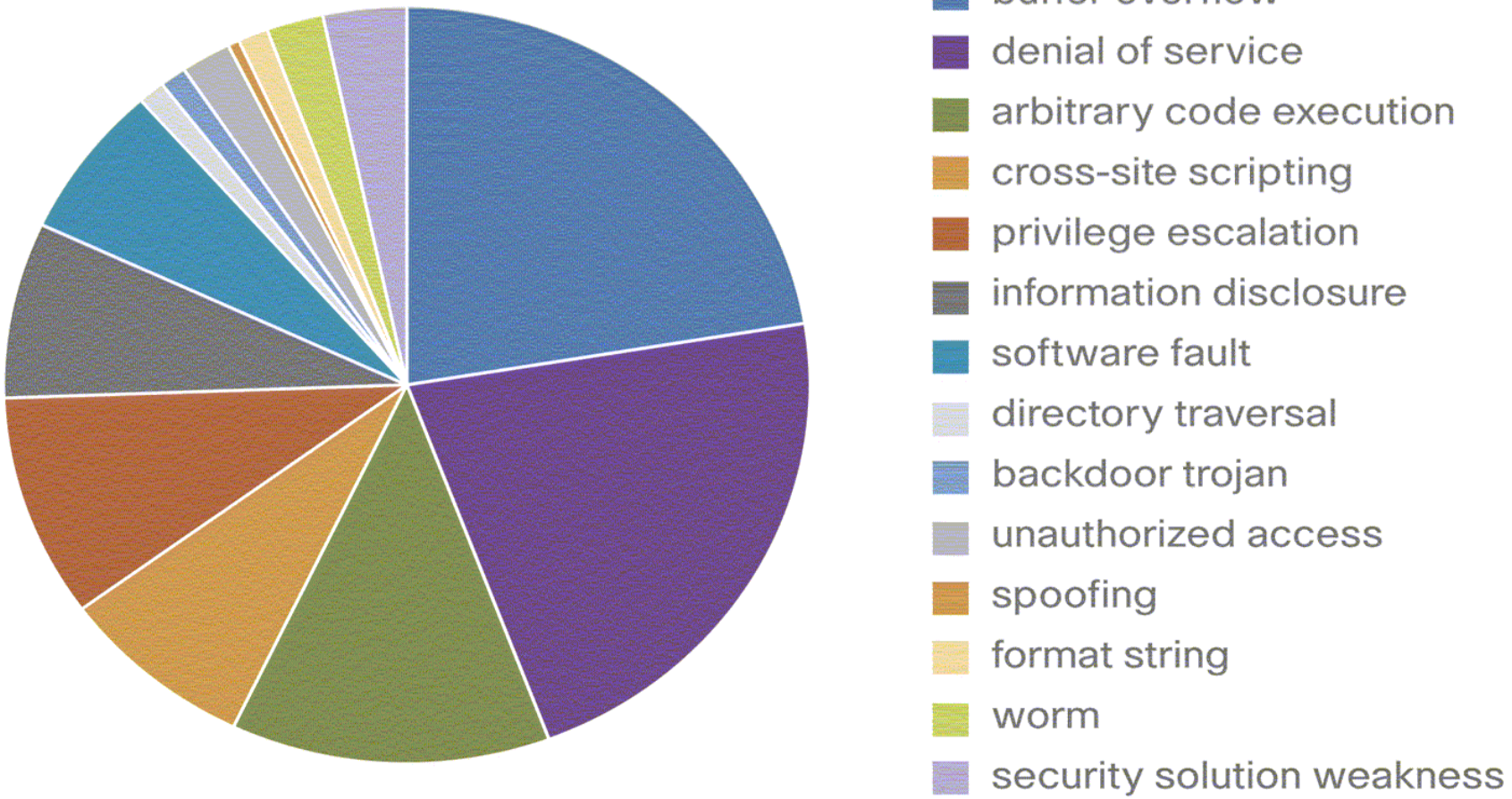
- Targeted attacks: 10 per day in 2007, up to 57 in 2008

  According to MessageLabs

2008 – Top Security Concerns

- Specialization and innovation in the online crime economy continues.
- Attacks are increasingly targeted to help maximize their effectiveness.
- Reputation HiJacking are gaining in prevaleance and popularity
- More blended threats

Vulnerabilities of 2008



Digital Devices Carry Unwanted Guests

- January 2008, consumers report the digital photo frames they received contained malware that attempted to install on their computer.
- Limited number of infection; Highlights that attackers are always trying something new
- Also of note, number of devices that contain some sort of memory is always on the rise

30,000 legitimate websites host malware

- January 2008, web security firm Finjan warned that tens of thousands of legitimate websites were hosting malware designed to compromise unknowing visitors.
- Toolkit named “Random JS toolkit” used to speed the spread of infections
- Used the “single copy to single person” technique to avoid getting caught

Universities targeted by phishing attacks

- February 2008, a large number of ".edu" domains including Columbia, Duke, Princeton, Purdue and Notre Dame were target of a sophisticated phishing attack.
- Students and faculty were sent emails that appeared to come from the help desk.
- Targeted username and passwords

Windows, MacOS, and Linux face off

- March 2008, a hacking contest was held at CanSecWest pitting fully patched copied of Windows Vista, MacOS (leopard), and Ubuntu against each other to see who would get compromised first.
- MacOS was compromised on day two with an attack on a previously unknown vulnerability in Safari.
- Windows Vista was compromised on day three with an attack on a previously unknown vulnerability in Adobe Flash
- Ubuntu survived the contest
- First MacOS X Botnet launching DoS attacks
- CanSecWest 2009 – MacOS X compromised in 10 Sec

SSH brute-force attacks

- May 2008, an order of magnitude increase of SSH password attacks was reported.
- Illustrates how a botnet can speed the time it takes to brute-force attack a service.
- Strong passwords are still very much needed and should be required.

45% of browsers vulnerable

- July 2008, a study using data collected from Google reveled that greater than 45 percent of internet broswers going to google contain vulnerabilities that have already been patched.
- Despite auto-updates, browsers still not getting patched.
- Are you clients turning off auto-updates?.

Major vulnerability discovered in DNS

- July 2008, Dan Kaminsky announced a fundamental flaw in how DNS operates.
- Massive multivendor patch was released, in one month only 52% of DNS servers were patched.
- The flaw allowed an attacker to poison DNS records of any domain in a matter of seconds.
- This could lead to major DNS poisoning attacks – no need to “trick the user”.

* More on this later

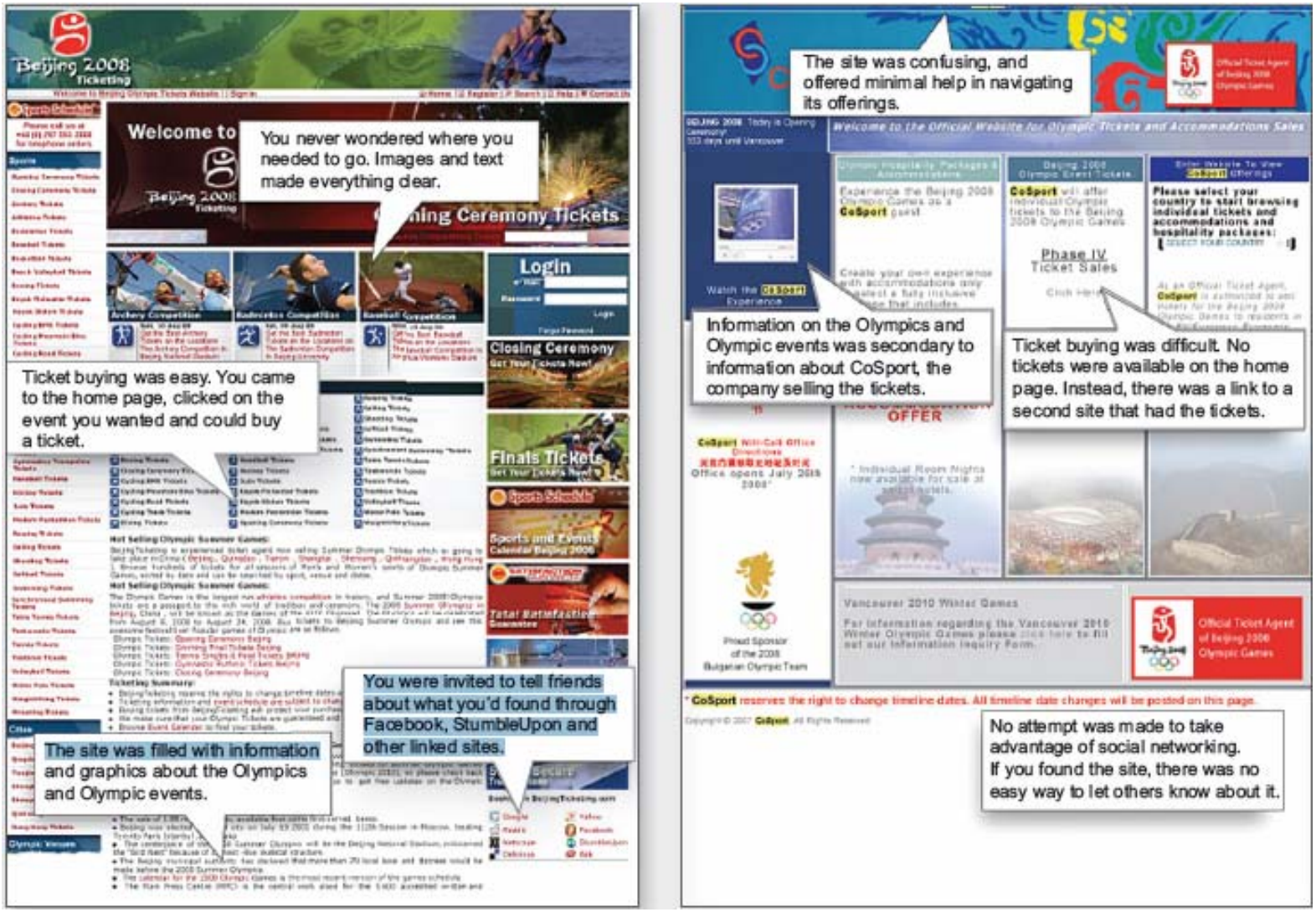
“Race to Zero” completed in record time

- August 2008, the “Race to Zero” was held and completed in a record time of 2 hours 25 minutes.
- Contest consisted on 7 well know viruses and 2 well known exploits, the goal was the modify them so they couldn’t be detected by Anti-Virus solutions.
- Highlights the need to move away from a pure signature based detection method.

Malware Targets Current Events

sident of the

Malware Targets Current Events



Heartland Payment Systems

- January 2009, disclosed a network compromise
- Process 100 M payment card transactions per month
- Work with over 175,000 merchants
- Described as a “very sophisticated” attack

  Computers compromised with rootkits with keyloggers

  Network data compromised
- Heartland was abiding by PCI standards
- Expected to be more that 100 M records compromised
- “Beats” previous record of 95M by TJX (TJ MAXX)

Web signing shown to be flawed

- January 2009, researchers showed how the Internet public key infrastructure (PKI) could be subverted using a known weakness of the MD5 hash functions
- The researchers were able to create fake SSL certificates that all major browsers would treat as legitimate
- 14% of all websites use certificates signed using the MD5 functions
- Fear the now undetectable phish

Exploiting Cisco Routers

- January 2009, security researcher “FX” presented a paper of efforts to exploit Cisco routers with minimal knowledge about the router itself
- Previously, detailed knowledge about image version and configuration is needed
- Still, very much a “lab” exploit

Cisco Routers

- In the past, people didn’t worry about Cisco vulnerabilities as they hadn’t been shown to be exploitable
- FX’s work takes exploiting Cisco routers one step closer
- Now is the time to take updating IOS seriously (if you don’t already)

Conclusions from 2008/2009

- Attackers are always modifying their methods
- Users are the main focus of attacks at this point
- Major systems (DNS, Internet PKI) have been shown to have flaws, nothing is perfect
- Blended attacks are numerous and evolving
- Botnet infestation remains common and dangerous
- Known vulnerabilities are going unpatched and existing security policies are being ignored.

Case Studies

Case Studies

- Dangerous infrastructure
  - DNS vulnerability analyzed
- Malware sophistication
  - Modern malware source code analyzed

DNS

- Discovered by Dan Kaminsky in early 2008
- Security community, internet community at large was on high alert
- Allowed attackers to spoof and manipulate the IP for a DNS record

DNS – The Attack

- Attack was always possible
- Only 1:65,000 chance it could work (Guess the QID)
- Assumed attacker could only try once the TTL expired

DNS – The Basics

Question

Src Port = SP1

Dst Port = DP1

Query ID = QID1

Question = Q1

Response

Src Port = DP1

Dst Port = SP1

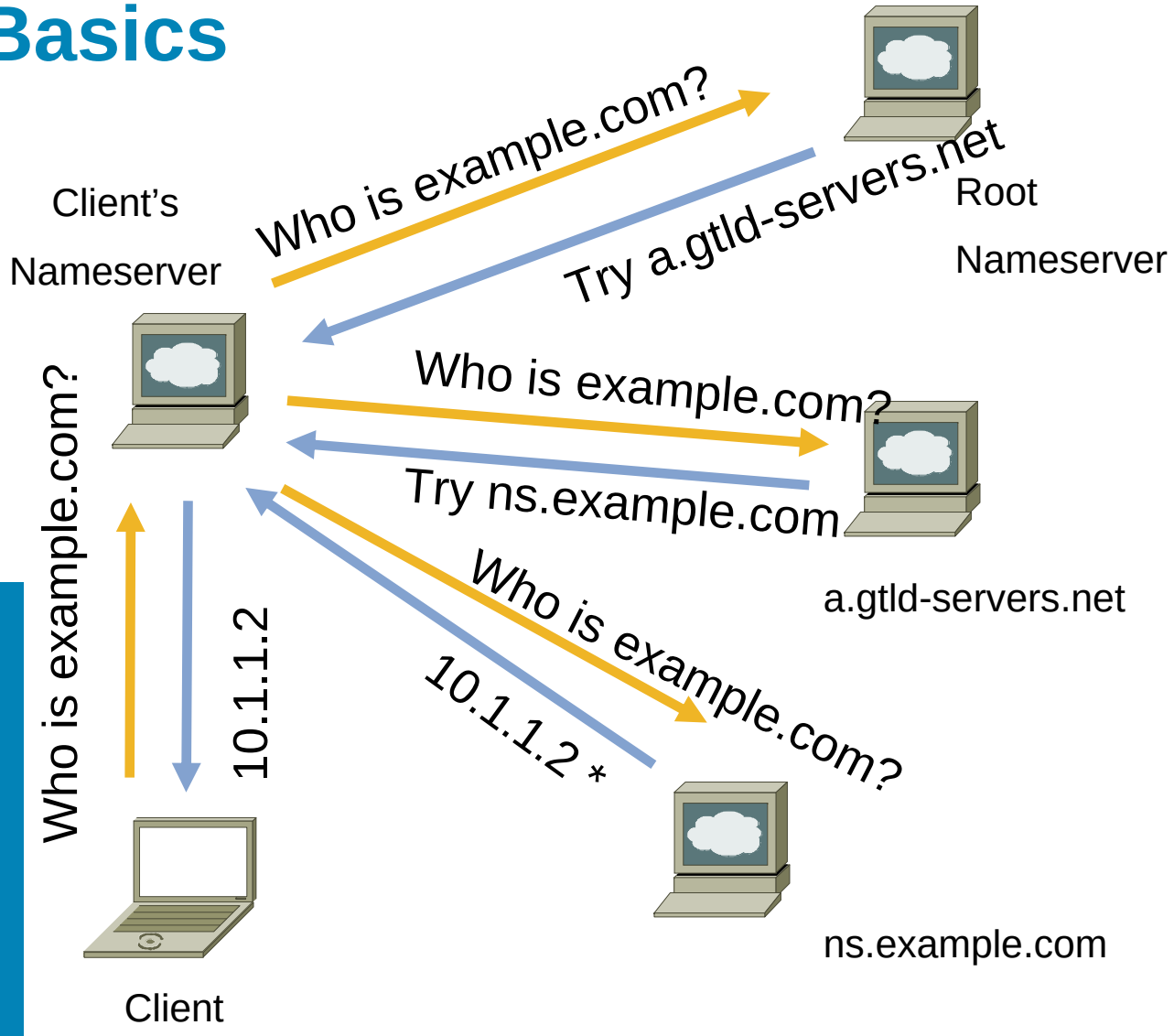
Query ID = QID1

Question = Q1

Answer = A1

Authority = ?

Additional = ?



DNS – Poisoning Attack

Question

Src Port = SP1

Dst Port = DP1

Query ID = QID1

Question = Q1

Response

Src Port = DP1

Dst Port = SP1

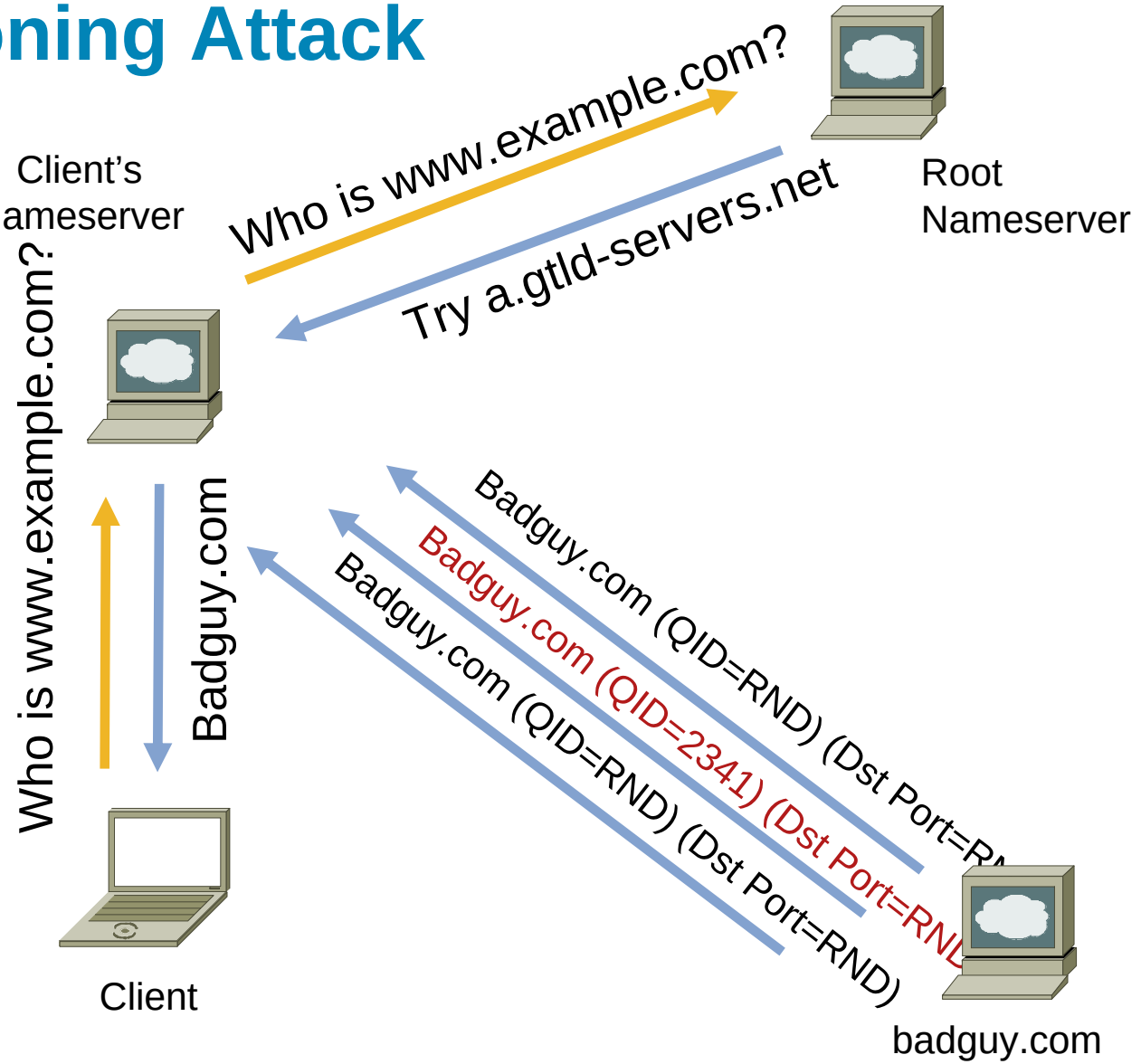
Query ID = QID1

Question = Q1

Answer = badguy.com

Authority = ?

Additional = ?



DNS – Dan's Attack

Question

Src Port = SP1

Dst Port = DP1

Query ID = QID1

Question = Q1

Response

Src Port = DP1

Dst Port = SP1

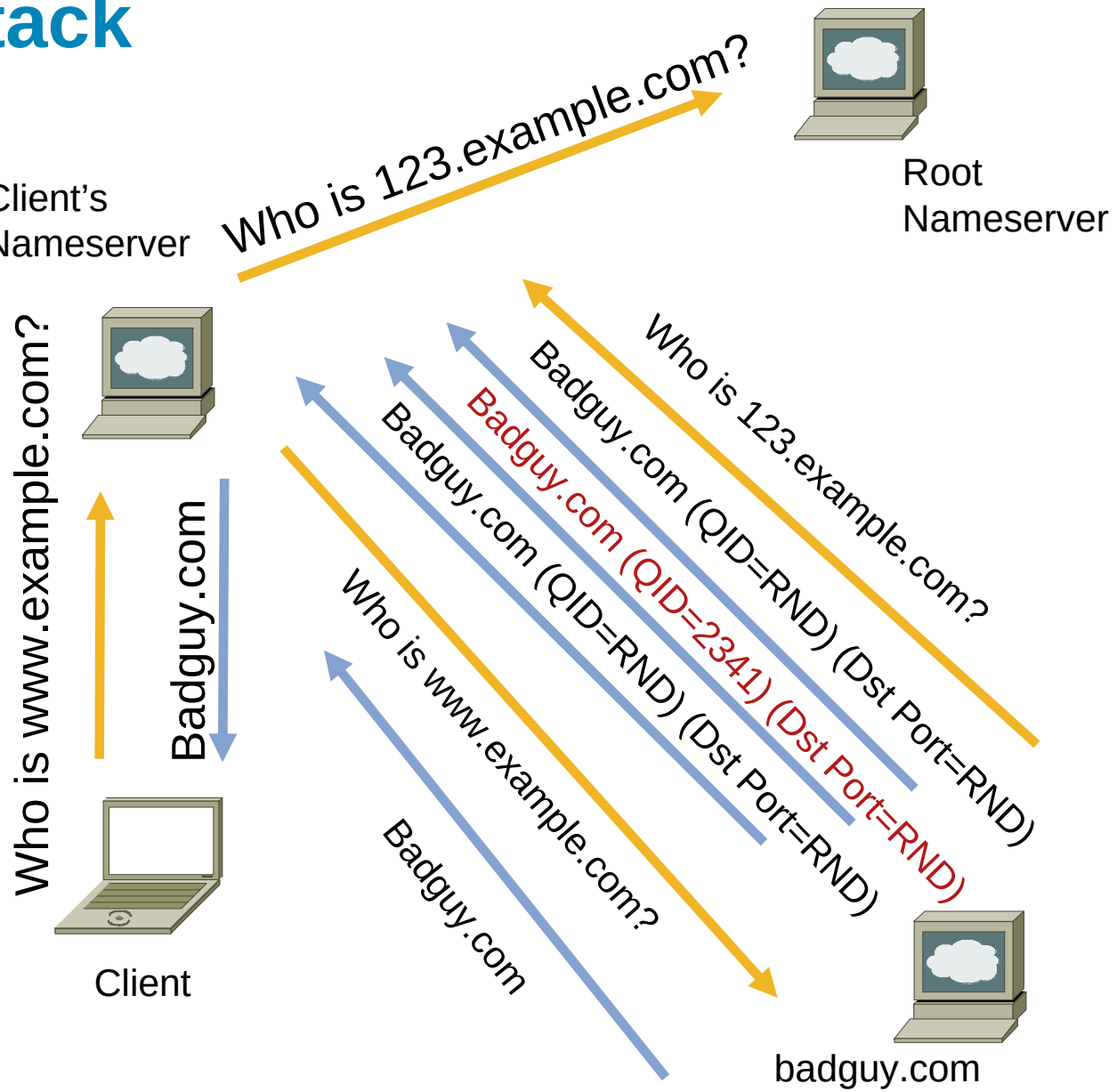
Query ID = QID1

Question = Q1

Answer = badguy.com

Authority = badguy.com

Additional = badguy.com



DNS – The Implications

- “Gold Standard” DNS poisoning attacks
- Is email staying on site?
- **Click here if you forgot your password**

DNS – The Remedy

- Major DNS software developers were told in secret
  - Focus was to develop patches before attack became known
- Once patches were ready the vulnerability was announced
  - 30 days before details were to be released
- Large effort by big names in the networking and network security industry to convince people to patch immediately
- 70% fortune 500 companies patched within 30 days

Modern Malware Sophistication

- Propagation techniques
- Security countermeasures
- Capabilities

Conficker/Downadup At Work

- Exploits vulnerability in Windows Server service
  - MS08-067 (445/tcp)
- Originally uses HTTP as it's Command and Control (C&C) channel
- Criminals are smart, they monitor advancements in technology and use it to their advantage
  - Conficker.A uses MD5 with 1024-bit RSA digital certs
  - Conficker.B moves to MD6 with 4096-bit RSA digital certs
  - Buffer Overflow patched in MD6 on 15 January 2009
  - Criminals patch MD6 in the Conficker.D variant, 4 March 2009

Conficker/Downadup At Work

- Adds ability to infect via network shares and removable media
- DNS Hooking used to prevent infected devices from accessing security-related sites for assistance
  - Blacklist updated with new variants
- Process list monitoring and process termination
  - Process list updated with new variants

Conficker/Downadup At Work

- Criminals monitor what the industry is doing to prevent their malicious behaviors and move to a new Peer-to-Peer (P2P) C&C channel
  - Formation of Conficker Working Group (CWG)
  - DNS Mitigations
- New P2P C&C channel is more resilient and accepts commands from other Conficker infected nodes
- Media frenzy for “April Fools” doesn’t pan out
- While nothing major happened - Conficker is still hard at work and devices are still infected, being infected, being updated, along with other malicious behaviors
  - Begins to download new/existing malware - Waledac

Conficker and Downadup at a Glance

Conficker.B Spreads
29 December 2008
38 days after Conficker.A
Network share exploitation using 445/tcp added
Removable drive propagation added
Connects to a different set of 250 randomly generated domains/hosts day
MD6 hashing w/4096-bit RSA digital certificate

Conficker.A Spreads
21 November 2008
Exploits MS08-067
DNS Hooking
Connects to 250 randomly generated domains/hosts day
MD5 hashing w/1024-bit RSA digital certificate

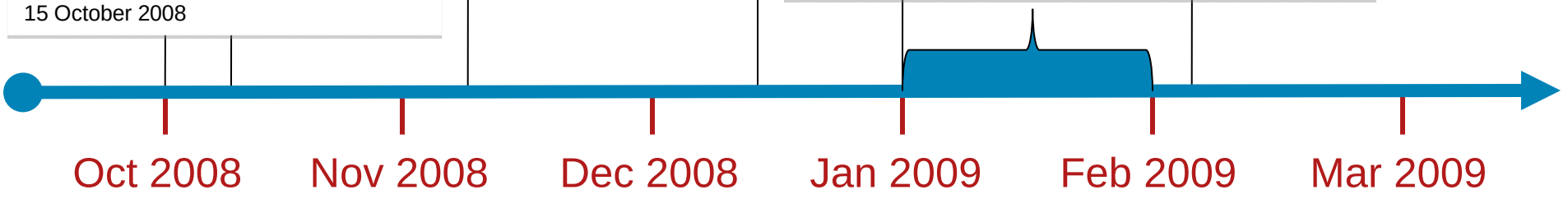
SRI Conficker Analysis Published
4 February 2009

MS08-067 Published
23 October 2008
Cisco Security Agent prevents exploitation using 'Default Desktop' or 'Default Server' Policies

MIT MD6 Buffer Overflow Patched
15 January 2009
Conficker.A+B affected by this vulnerability

Major Growth in Conficker.A+B Population
15 January 2009 – 15 February 2009

MIT MD6 Hash Released
15 October 2008



Conficker and Downadup at a Glance (cont.)

Conficker.D Discovered
4 March 2009
65 days after Conficker.B and 12 days after Conficker.C
Connects to 500 random hosts per-day (24hours) out of 50k randomly generated domains on 1 April 2009
Peer-to-Peer with other Conficker.D infected nodes
MIT MD6 Vulnerability Patched
MS08-067 scanning removed
More processes added to termination list
DNS blacklist updated for security-related web sites

Conficker.E
8 April 2009
27 days after Conficker.D
Updates Conficker.B+.C+.D
Deletes itself on May 3

Conficker.D
1 April 2009, "April Fools" is here – everything is melting :D
Transition to the new phone-home method

Conficker.C Discovered
20 February 2009
53 days after Conficker.B
Accept commands from other Conficker nodes using Peer-to-Peer (P2P) via MS08-067 vulnerability
Conficker begins to shift to a resilient P2P architecture

Media Goes Crazy over Conficker.D
30 March 2009 – 3 April 2009

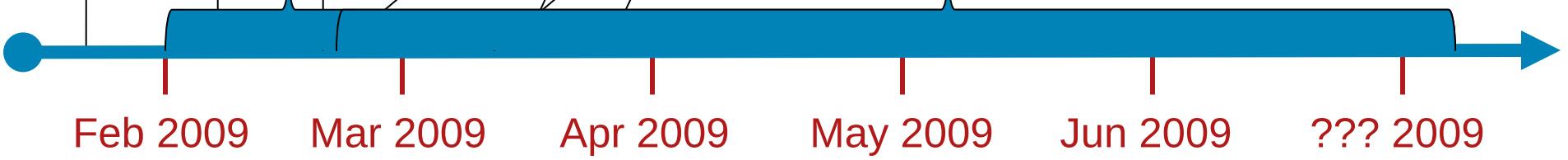
Various Detection Tools and Research Published
30 March 2009 – 4 April 2009

Conficker Working Group Announced
12 February 2009

SRI Conficker.C Analysis Published
8 March 2009

DNS Mitigation by CWG for Conficker.A+B
15 February 2009 – ???

DNS Mitigation by CWG for Conficker.C
4 March 2009 – ???



Feb 2009 Mar 2009 Apr 2009 May 2009 Jun 2009 ??? 2009

Threats on the Horizon

Threats on the Horizon

- Smaller, faster, more covert attacks
- Productivity technologies
- Proliferation of devices
- Continued increase of vulnerabilities
- Video Files Format Vulnerabilities
- Data Leakage
- Outsourcing
- Distributed Workforce

Smaller, Faster, More Covert Attacks

- Highly targeted and sophisticated
- New vectors, including SMS vishing
- Extensive use of social engineering

Tracki

Reply Reply All Forward Junk Print Delete Previous Next

You forwarded this message on 8/12/08. Show Forward

From: United Parcel Service <ghwjbotsecg@brandbox.com>
Date: Tuesday, August 12, 2008 9:40 AM
To: access-dial-epavlu-staff@cisco.com
Subject: Tracking N_ 1844598928

Attachments:

WW2_ASH182.zip

Unfortunately we were not able to deliver postal package you sent on July the 21st in time because the recipient's address is not correct.
Please print out the invoice copy attached and collect the package at our office

Your UPS

Productivity Technologies
Enable or Limit?

- Corporate network has expanded and is key platform for growth
- Also more permeable:
  - Remote access
  - Web-based tools
  - Mobile devices
- Essential to today's workforce

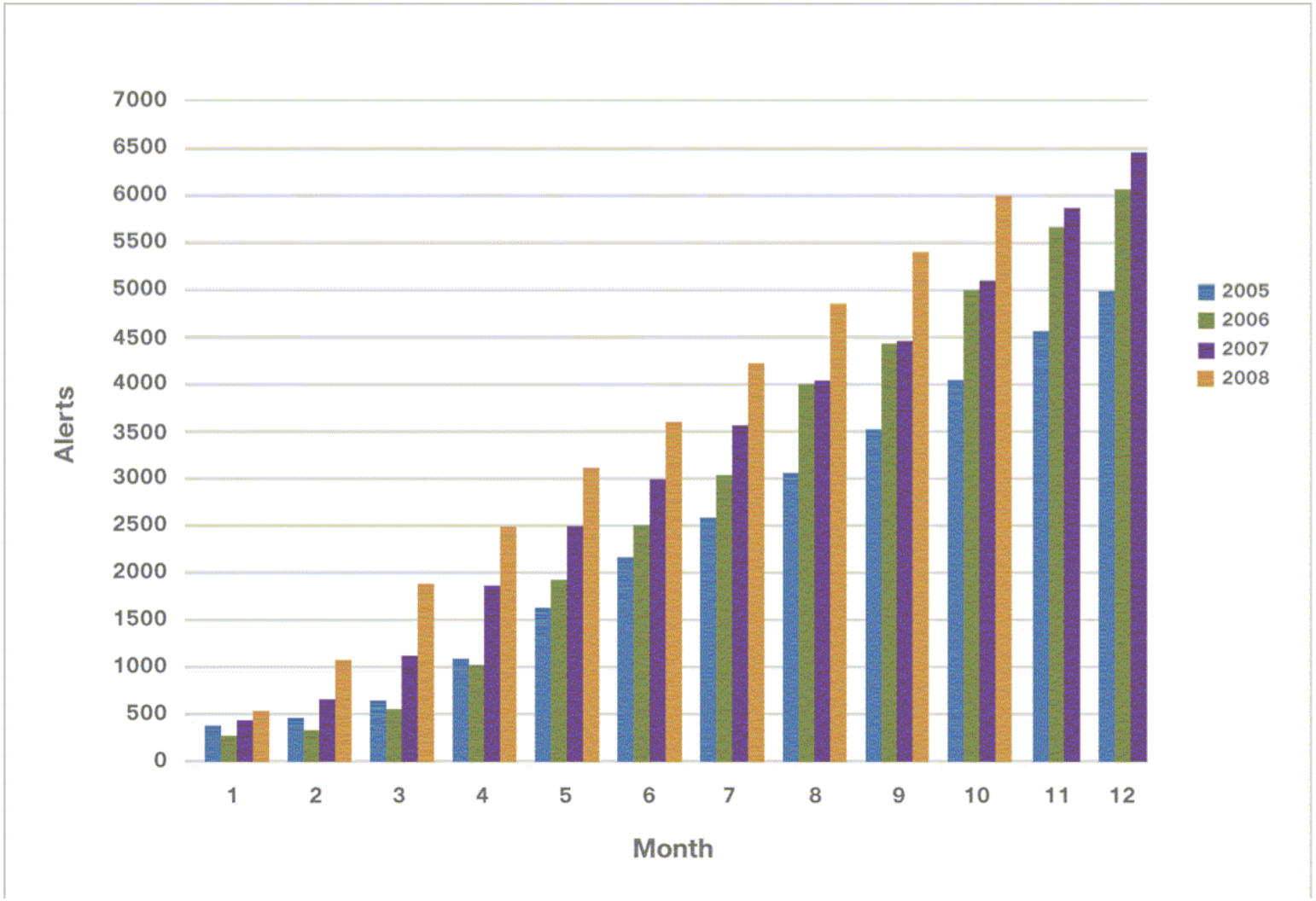
Proliferation of Devices

- New devices as been added to network
- Diversity of OS
- New entrance and exit points
- More data in motion

"…software glitches that need to be fixed -- are part of the 'new reality' of making complex cell phones in large volumes." – Jim Balsillie, RIM CEO

Cumulative Annual Alert Totals

- **The number of reported vulnerabilities in 2008 increased by 115%**



Video File Format Vulnerabilities

- Researchers in 2008 continued to uncovered many important to critical video file format vulnerabilities in:

  Quicktime

  Real Player

  Windows Media Player

  Flash

- Documented examples of video file attacks in 2008, not yet mainstream
- With rise of video it is only a matter of time
- The next “hot” YouTube video just might be dangerous…

Data Leakage

- Broad term encompassing multiple different challenges:
  - Security of Data at rest
  - Security of Data in motion
  - Identity-based access control
  - Both malicious and inadvertent disclosures

- Issue has become topical typically for “Compliance” reasons
- However, broader topic involves business risk management
  - How do I avoid inadvertent disclosures?
  - How do I protect my information assets from flowing to my competitors?
  - How do I avoid ending up in the news?

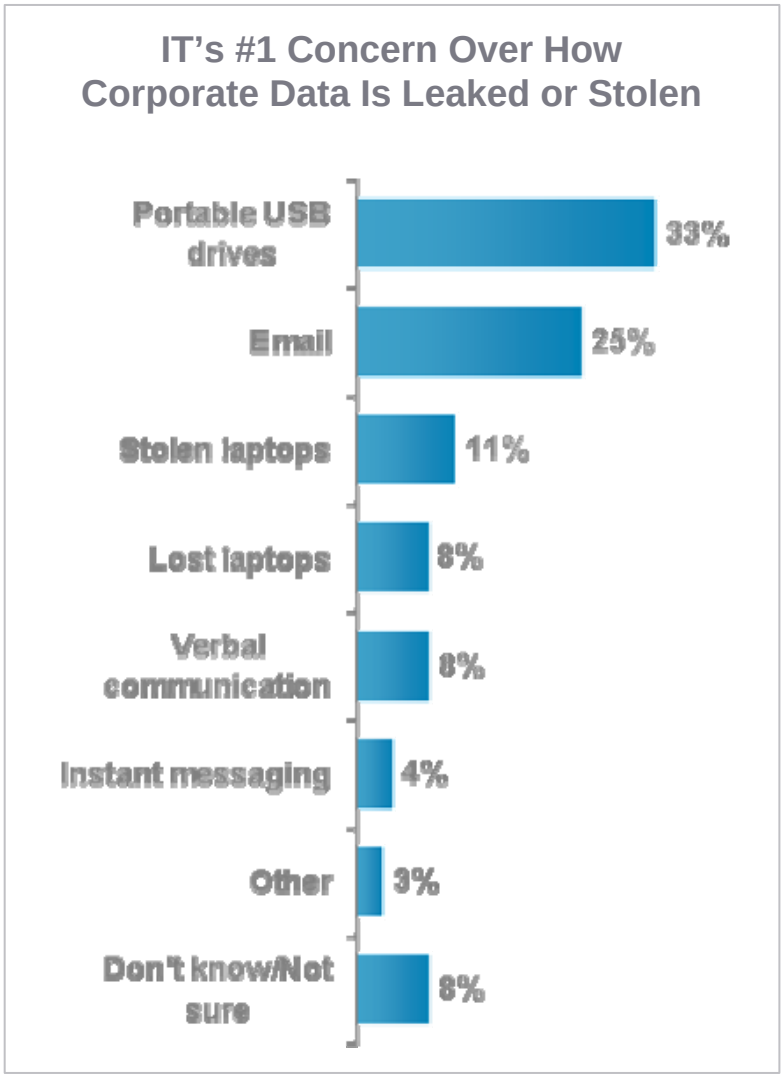
Mobile Data Continues: PC on a Stick

- New “smart drives” and other similar technology extending the existing threats to data posed by portable storage devices
- Devices carry a virtual computing environment in a secure storage, typically plugged in via USB to any open computer
- All workspace, preference, and data information is kept within the device, but computing resources of the host machine are used for manipulation and processing

Challenges:

- Analogous to SSL VPN security challenges, only now you can lose the device in a cab
- Unknown endpoint environment challenges: keyboard loggers and splicers, monitor taps, webcams
- Malicious software embedded in data or documents

Mobile Data Continues: PC on a Stick



Trend: Outsourcing

- Motivations

  Outsourcers typically feel less loyalty to the outsourcing organization

- Opportunity

  In many organizations, outsourcers are given full intranet access

- Considerations

  How do you balance the need to access required applications while providing necessary controls to mitigate risk?

  When negotiating contracts, are there any provisions for data security and integrity? Are there any provisions to audit the security posturue

  What legal recourses does the organization have in the event of compromise? Jurisdictional issues, liability and responsibility, etc.

Trend: Distributed Workforce

- De-perimeterization is real

  True “federated” security systems are a long ways off yet

- Layers of defense and policy enforcement are critical

  Drop bad traffic as close to the source as possible, but ensure you’ve got at least a couple of “last lines of defense”

- Costs and risks to data integrity should be a part of any calculation to adopt new business practices

  There may be hidden costs that are not well understood

- People and Processes Key to Mitigate Risk

  User awareness and effective business processes are as important to technology solutions

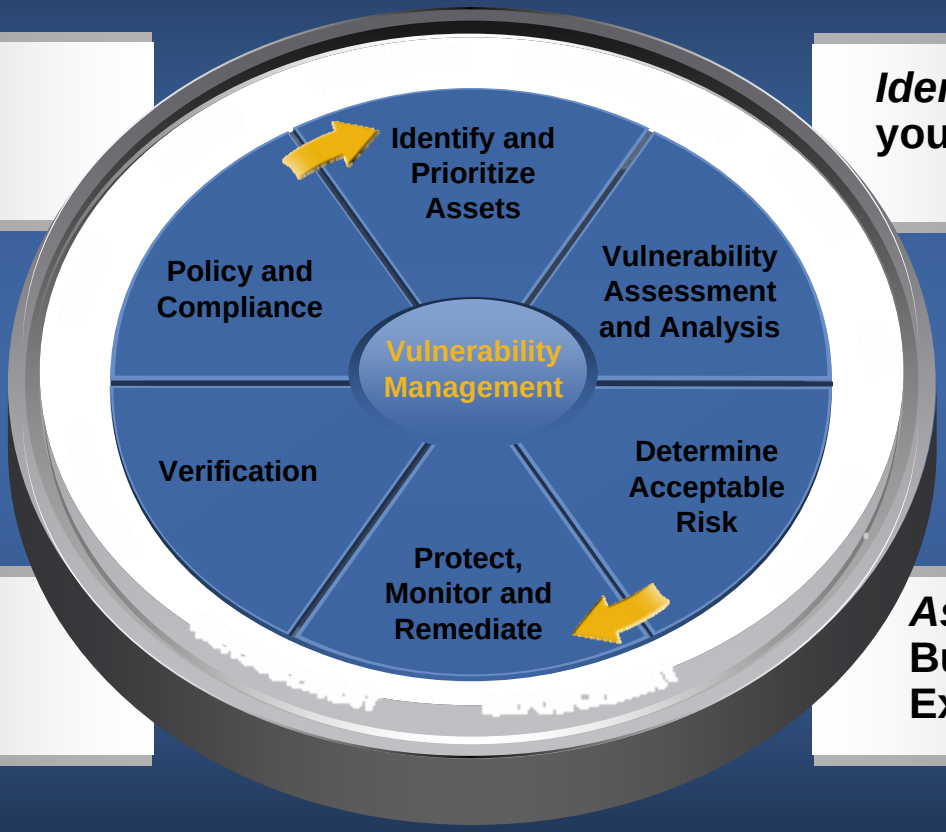
Threat Containment

Conclusion and Recommendations

The Business of Vulnerability Management

Enforce Security Compliance

Identify Issues: Know your Vulnerabilities



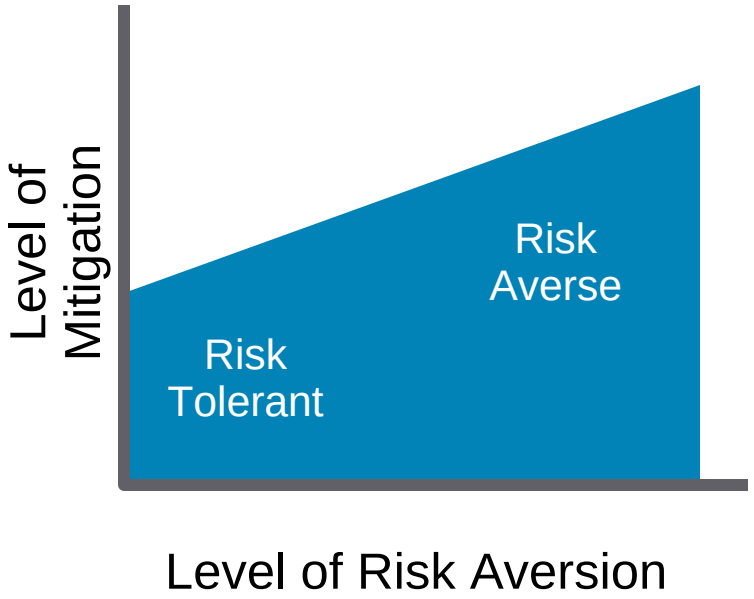
Report Security Posture

Assess Threat / Risk: Business Risk, Exploitation Risk

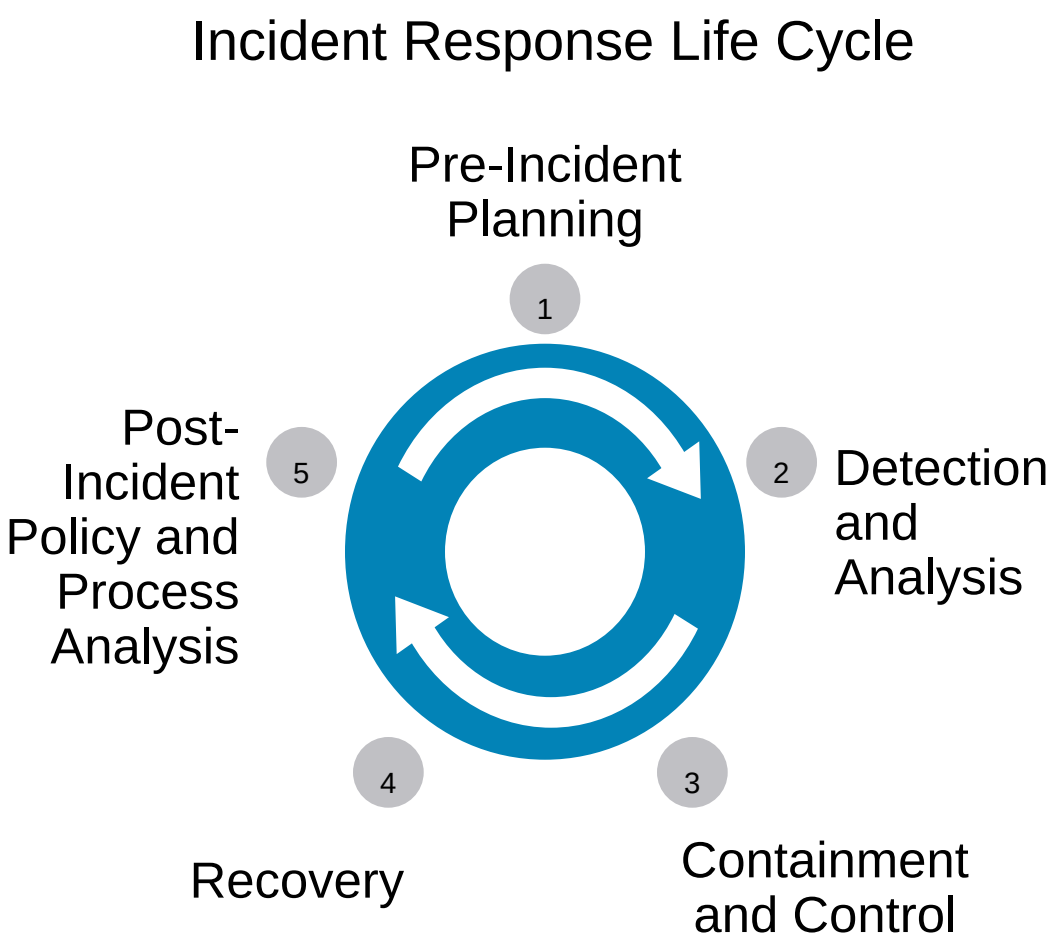
Eliminate Vulnerabilities, Observe / stop exploits

What's My Exposure? Appropriate Risk Mitigation

- Risk is at the core of all security policy decisions
- With emerging threats, there's always something out there that can affect your business
- Effective understanding of business risk is critical to determining priorities in your response plan
- The Challenge: Every application is business critical to someone



Incident Response Basics



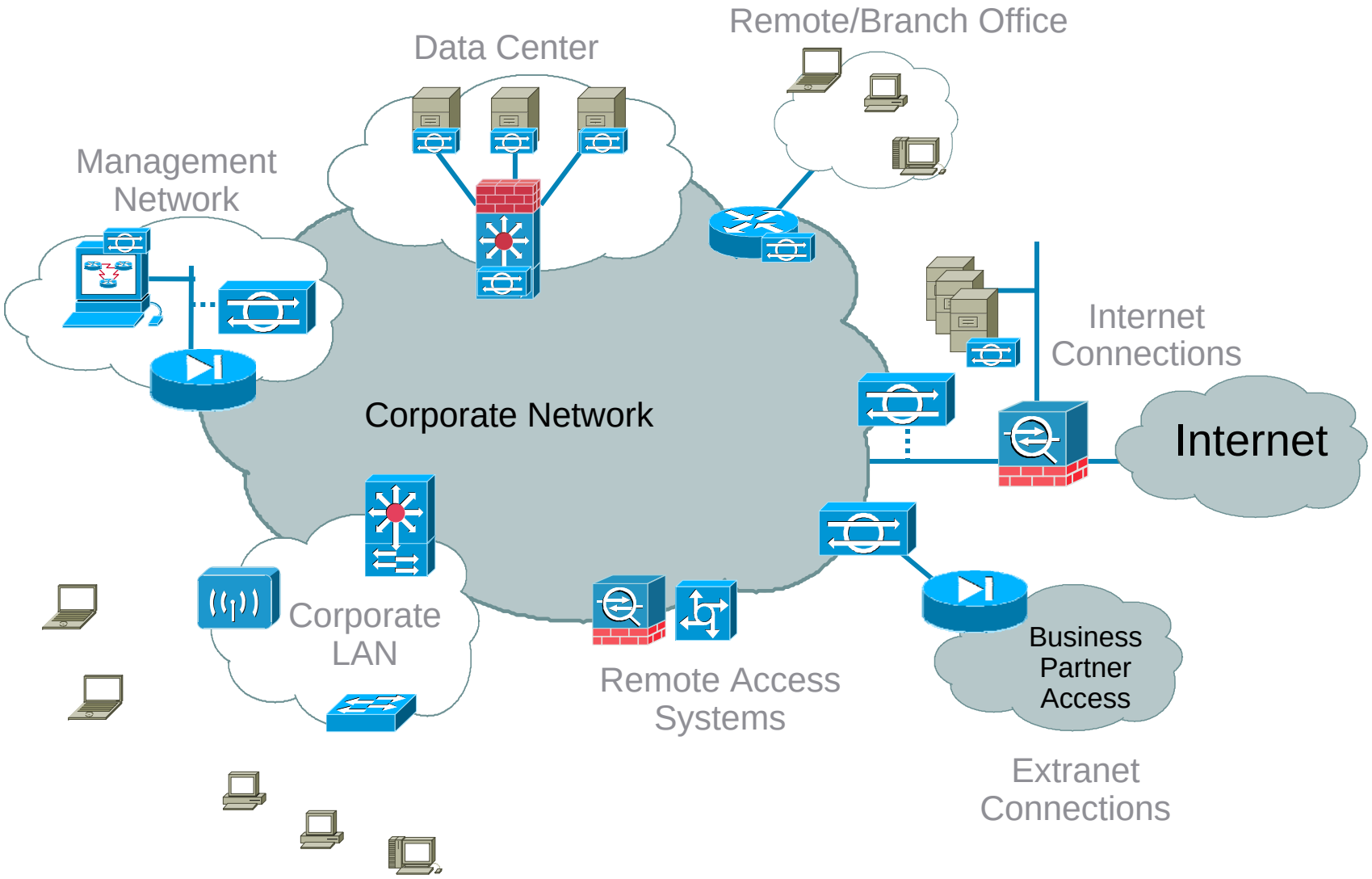
- Most important step: Step 1
- Second most important step: Step 5
- Most commonly skipped step: Step 1
- Second most commonly skipped step: Step 5

Adapted from reports at www.gartner.com and www.securityfocus.com

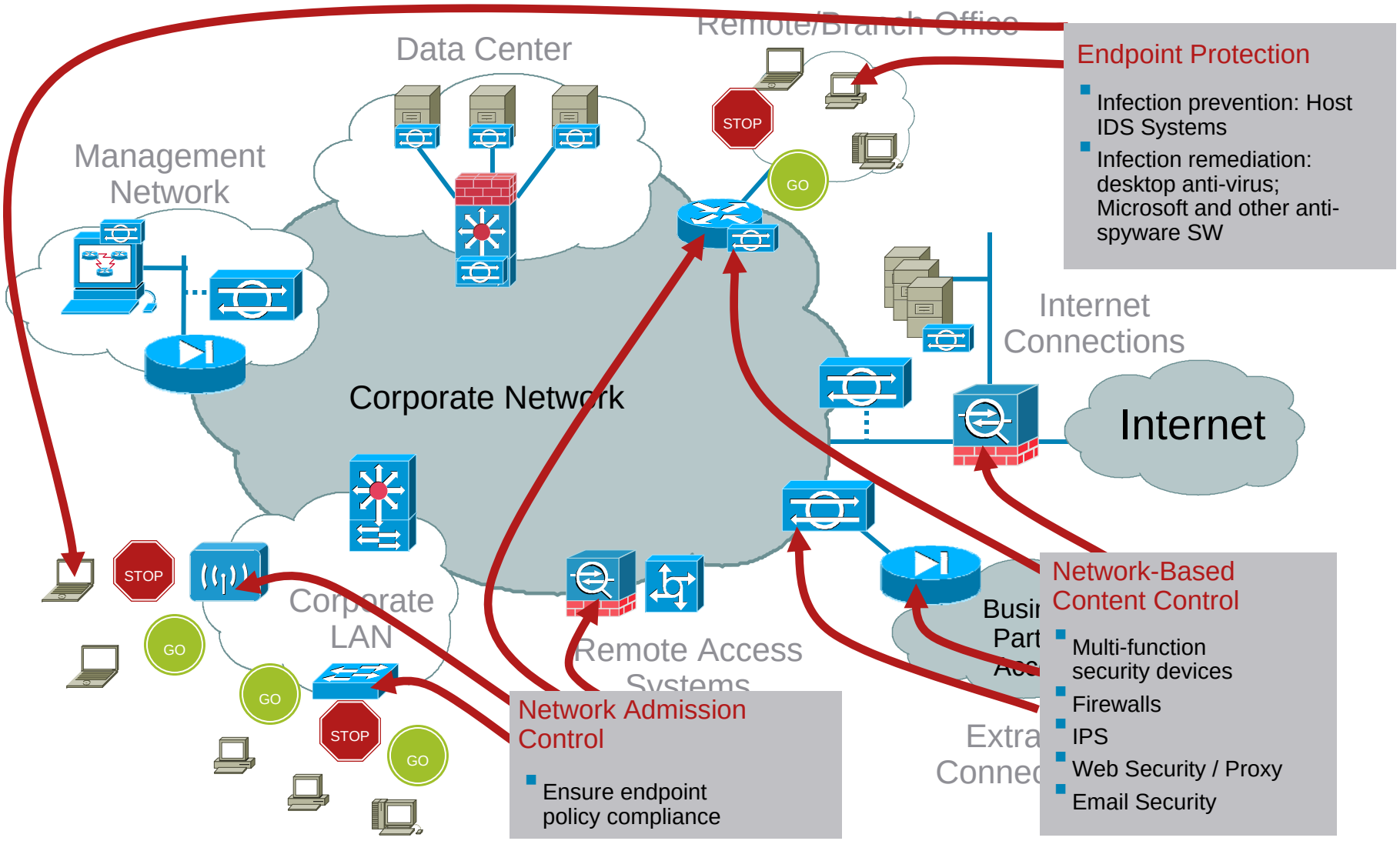
Key Recommendations

- Stay Focused
- Stop Users from Inadvertently Downloading Malware onto the network *
- Patch known vulnerabilities
- Prevent Data Loss
- Take Insider Threats Seriously
- Remember the Network
- Think Beyond Compliance
- Make Security Simpler
- Stay Informed

Tackling Malware: Solutions Across the Network



Tackling Malware: Solutions Across the Network

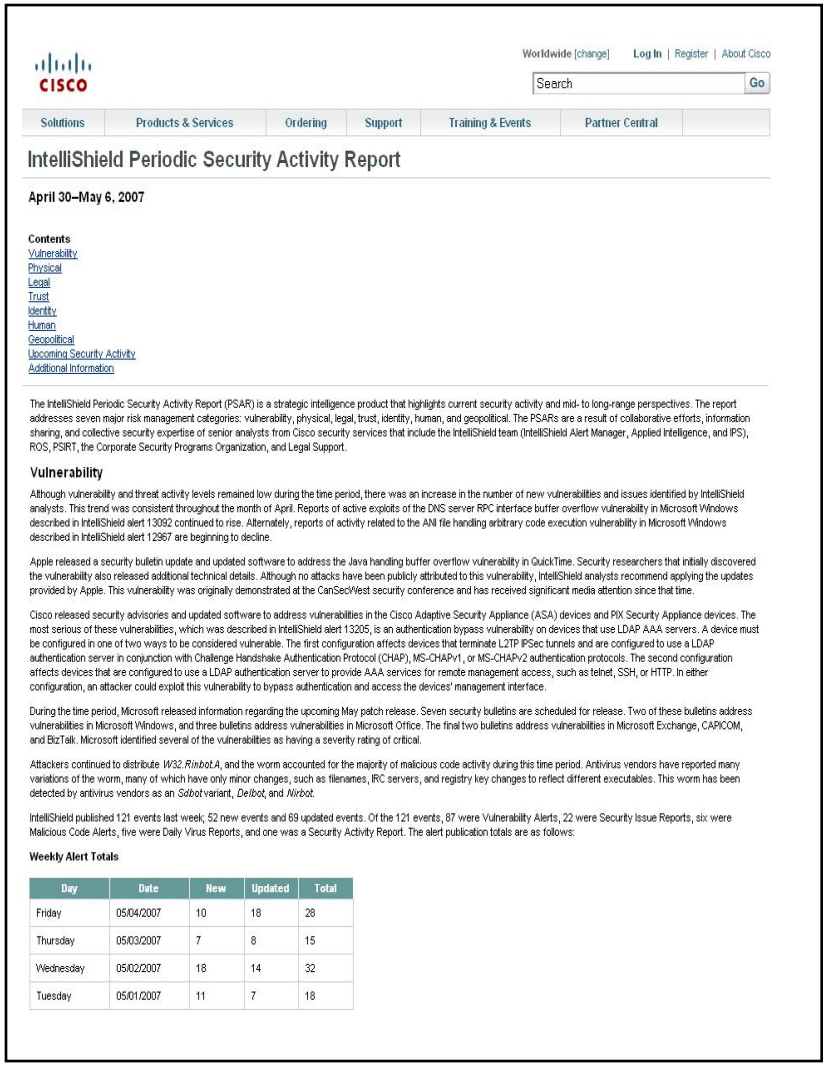


Intelligence Summary Example

Cisco IntelliShield Cyber Risk Report

A Strategic Intelligence Report that Highlights Current Security Activity and Mid-to Long-range Perspectives

- Addresses seven major risk management categories: vulnerability, physical, legal, trust, identity, human, and geopolitical.
- The CRRs are a result of collaborative efforts, information sharing, and collective security expertise of senior analysts from Cisco security services that include the IntelliShield and Ironport teams



Worldwide [change] Log In | Register | About Cisco

Search Go

Solutions | Products & Services | Ordering | Support | Training & Events | Partner Central

IntelliShield Periodic Security Activity Report

April 30–May 6, 2007

Contents

The IntelliShield Periodic Security Activity Report (PSAR) is a strategic intelligence product that highlights current security activity and mid- to long-range perspectives. The report addresses seven major risk management categories: vulnerability, physical, legal, trust, identity, human, and geopolitical. The PSARs are a result of collaborative efforts, information sharing, and collective security expertise of senior analysts from Cisco security services that include the IntelliShield team (IntelliShield Alert Manager, Applied Intelligence, and IPS), ROS, PSIRT, the Corporate Security Programs Organization, and Legal Support.

Vulnerability

Although vulnerability and threat activity levels remained low during the time period, there was an increase in the number of new vulnerabilities and issues identified by IntelliShield analysts. This trend was consistent throughout the month of April. Reports of active exploits of the DNS server RPC interface buffer overflow vulnerability in Microsoft Windows described in IntelliShield alert 13092 continued to rise. Alternately, reports of activity related to the ANI file handling arbitrary code execution vulnerability in Microsoft Windows described in IntelliShield alert 12967 are beginning to decline.

Apple released a security bulletin update and updated software to address the Java handling buffer overflow vulnerability in QuickTime. Security researchers that initially discovered the vulnerability also released additional technical details. Although no attacks have been publicly attributed to this vulnerability, IntelliShield analysts recommend applying the updates provided by Apple. This vulnerability was originally demonstrated at the CanSecWest security conference and has received significant media attention since that time.

Cisco released security advisories and updated software to address vulnerabilities in the Cisco Adaptive Security Appliance (ASA) devices and PIX Security Appliance devices. The most serious of these vulnerabilities, which was described in IntelliShield alert 13205, is an authentication bypass vulnerability on devices that use LDAP AAA servers. A device must be configured in one of two ways to be considered vulnerable. The first configuration affects devices that terminate L2TP IPSec tunnels and are configured to use a LDAP authentication server in conjunction with Challenge Handshake Authentication Protocol (CHAP), MS-CHAPv1, or MS-CHAPv2 authentication protocols. The second configuration affects devices that are configured to use a LDAP authentication server to provide AAA services for remote management access, such as telnet, SSH, or HTTP. In either configuration, an attacker could exploit this vulnerability to bypass authentication and access the devices' management interface.

During the time period, Microsoft released information regarding the upcoming May patch release. Seven security bulletins are scheduled for release. Two of these bulletins address vulnerabilities in Microsoft Windows, and three bulletins address vulnerabilities in Microsoft Office. The final two bulletins address vulnerabilities in Microsoft Exchange, CAPICOM, and BizTalk. Microsoft identified several of the vulnerabilities as having a severity rating of critical.

Attackers continued to distribute *W32.Rinbot.A*, and the worm accounted for the majority of malicious code activity during this time period. Antivirus vendors have reported many variations of the worm, many of which have only minor changes, such as filenames, IRC servers, and registry key changes to reflect different executables. This worm has been detected by antivirus vendors as an *Sdbot* variant, *Delbot*, and *Nirbot*.

IntelliShield published 121 events last week; 52 new events and 69 updated events. Of the 121 events, 87 were Vulnerability Alerts, 22 were Security Issue Reports, six were Malicious Code Alerts, five were Daily Virus Reports, and one was a Security Activity Report. The alert publication totals are as follows:

Weekly Alert Totals

Day	Date	New	Updated	Total
Friday	05/04/2007	10	18	28
Thursday	05/03/2007	7	8	15
Wednesday	05/02/2007	18	14	32
Tuesday	05/01/2007	11	7	18

Some Closing Thoughts

- Do not get overwhelmed
- Small steps can make a big difference
- Remember, to survive a bear attack, you don't have to be fastest person…you just need to be faster than the next guy
- Do not be the least prepared