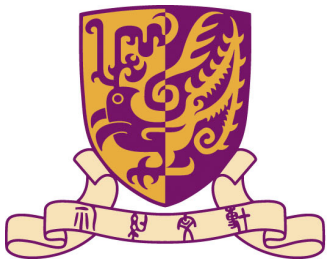
Introduction to Cyber Security

Fall 2017 | Sherman Chow | CUHK IERG 4130



香港中文大學
The Chinese University of Hong Kong

信息工程學系
Department of Information Engineering

Acknowledgement

- Text of slides mostly from Prof. Wing Lau
- Incorporated / adapted from the following sources:
  - Kurose and Ross, Chapter 7 of "Computer Networking – a top down approach featuring the Internet 2nd ed."
  - William Stallings, "Cryptography and Network Security, 3rd ed."
  - Simon Garfinkel, Gene Spafford, "Web Security, Privacy and Commerce, 2nd ed."
  - Charlie Kaufman, Radia Perlman, Mike Spenciner,"Network Security, 2nd ed."
  - Lincoln D. Stein, "Web Security"
  - Ed Skoudis, "Counter Hack"
  - Steve Burnett, Stephen Paine, "RSA Security's Official Guide to Cryptography"
- Some sources of data:
  - CERT/CC CMU
  - Microsoft Security Intelligence Report (http://www.microsoft.com/security/portal/Threat/SIR.aspx)

Acknowledgement (cont.)

- Kris Gaj, George Mason University
- Vincent Costa, Hofstra University
- Henric Johnson Blekinge, Institute of Technology
- Henning Schurzinne, Columbia University
- Felix Wu, UC Davis
- Wenke Lee, Georgia Tech
- Yehuda Afek, Tel Aviv University
- Jeff Yan, University of New Castle
- Jesse Walker, Intel
- James Kempf, DoCoMo Labs, USA

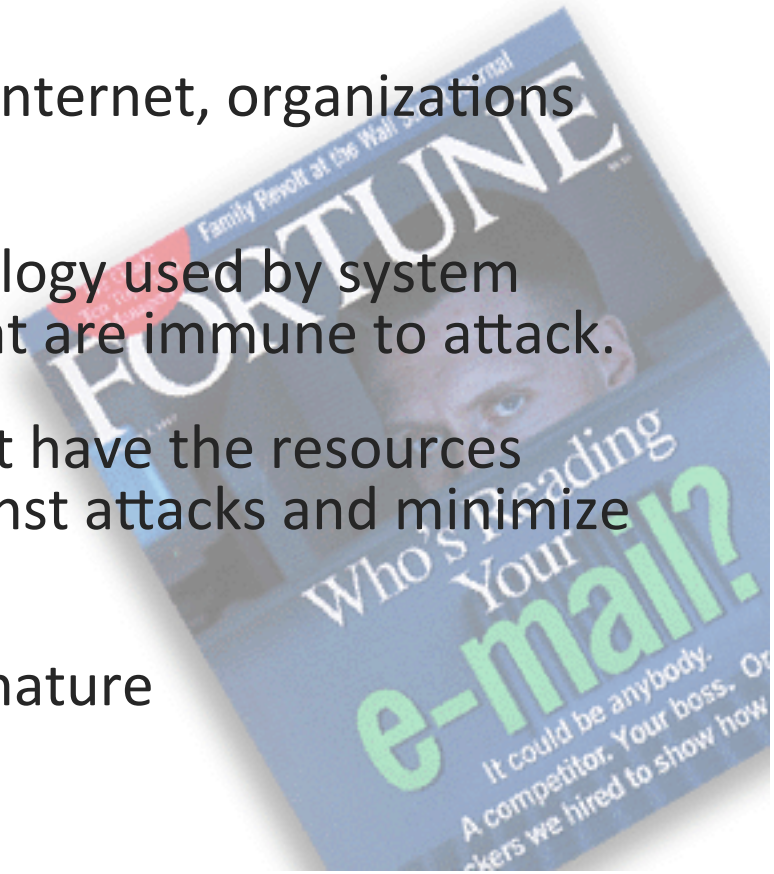
The copyrights and contribution of the original authors are hereby acknowledged

Cyber Landscape

- Desktop workstation, Laptops
- Smartphones, Tablets
- Cloud
- Smart Grid
- Vehicular Network
- Cyber-Physical Systems
- Internet of Things, *etc*.

Landscape of Cyber Security

- Presence in the Cyber space has become Indispensable to any organization and business worldwide.
- In the rush to benefit from using the Internet, organizations often overlook significant risks.
- The engineering practices and technology used by system providers do not produce systems that are immune to attack.
- Network and system operators do not have the resources (people) and practices to defend against attacks and minimize damage.
- Policy and law in cyber-space are immature and lag the pace of change



What is Cyber Security

- The Science and Engineering of guarding computer-related systems and assets against unintentional or malicious behaviours of intelligent adversaries.
- Security vs. Reliability (e.g., airplane/building/car safety)
  - Intentional vs. Accidental fault/failure
  - Bad guys in security can be very smart and creative
- "Cyber World" vs. "Physical World"
  - Street-smart users may become silly in the cyberspace

What is Cyber Security (cont.)

- Security is a relative concept
- vs. functional requirements (e.g., usability) of honest users
  - E.g., how much time you wait at the gate for security check ✈
  - E.g., how do you unlock your smartphone?
- vs. goal and capabilities of the adversary
  - E.g., fingerprint unlock
  - What if the attacker has “access” of your finger (while you Zzz…)?

Example: Cloud Security

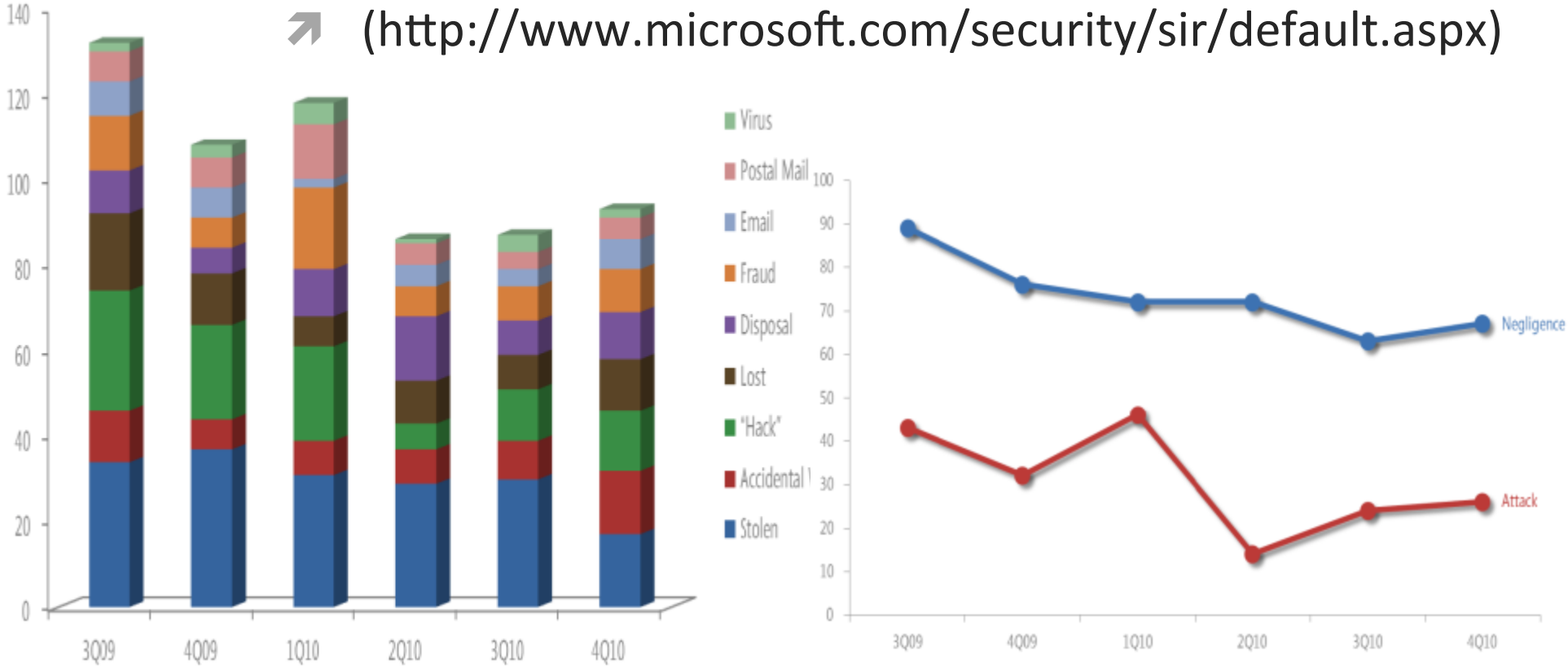
- Multi-tenant cloud environment
- Isolation via virtual-machine
- Cloud operator may not be trustworthy
- Outsourced (computation over) sensitive data
  - E.g. Big Data Analytics

Introduction (Part 1)

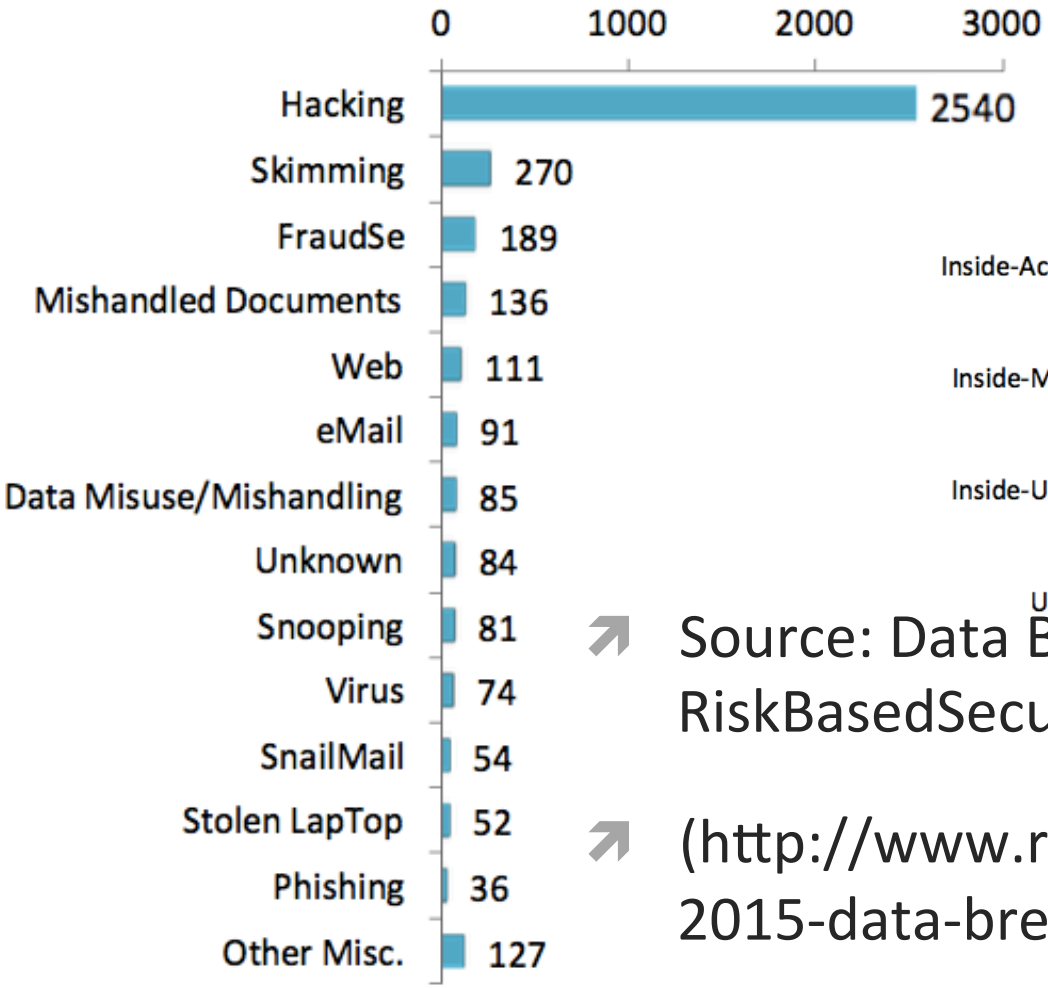
- Security Breaches, Vulnerabilities, Attack Sophistication
- Vulnerability Exploit Cycle
- How secure our web is? Window of Exposure, and global stat.
- Digital Pests, Spam, Phishing, Rogue Software, *etc.*
- Common exploit

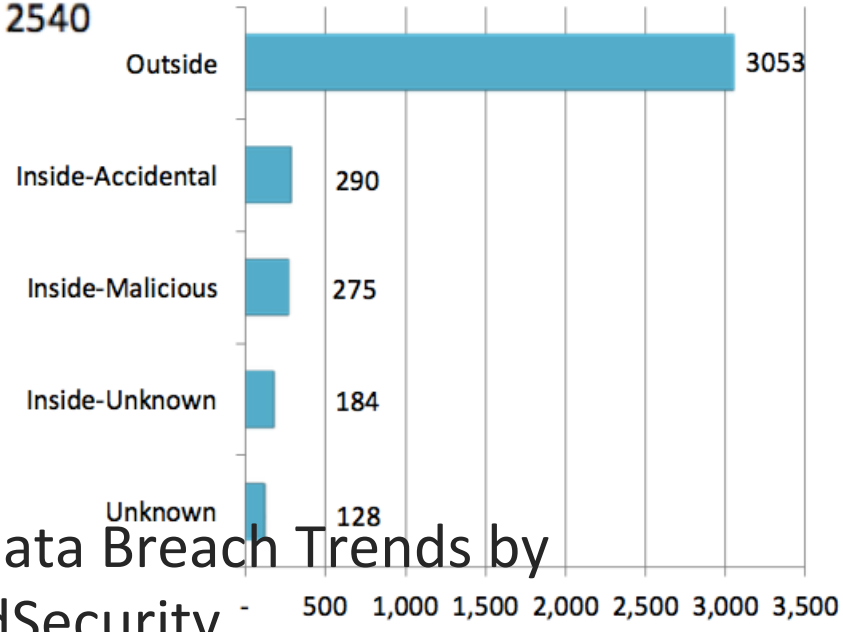
Security Breach Incident Types (2010)

- Source: Microsoft Security Intelligence Report (SIR)
- (http://www.microsoft.com/security/sir/default.aspx)



Security Breach Incident Types



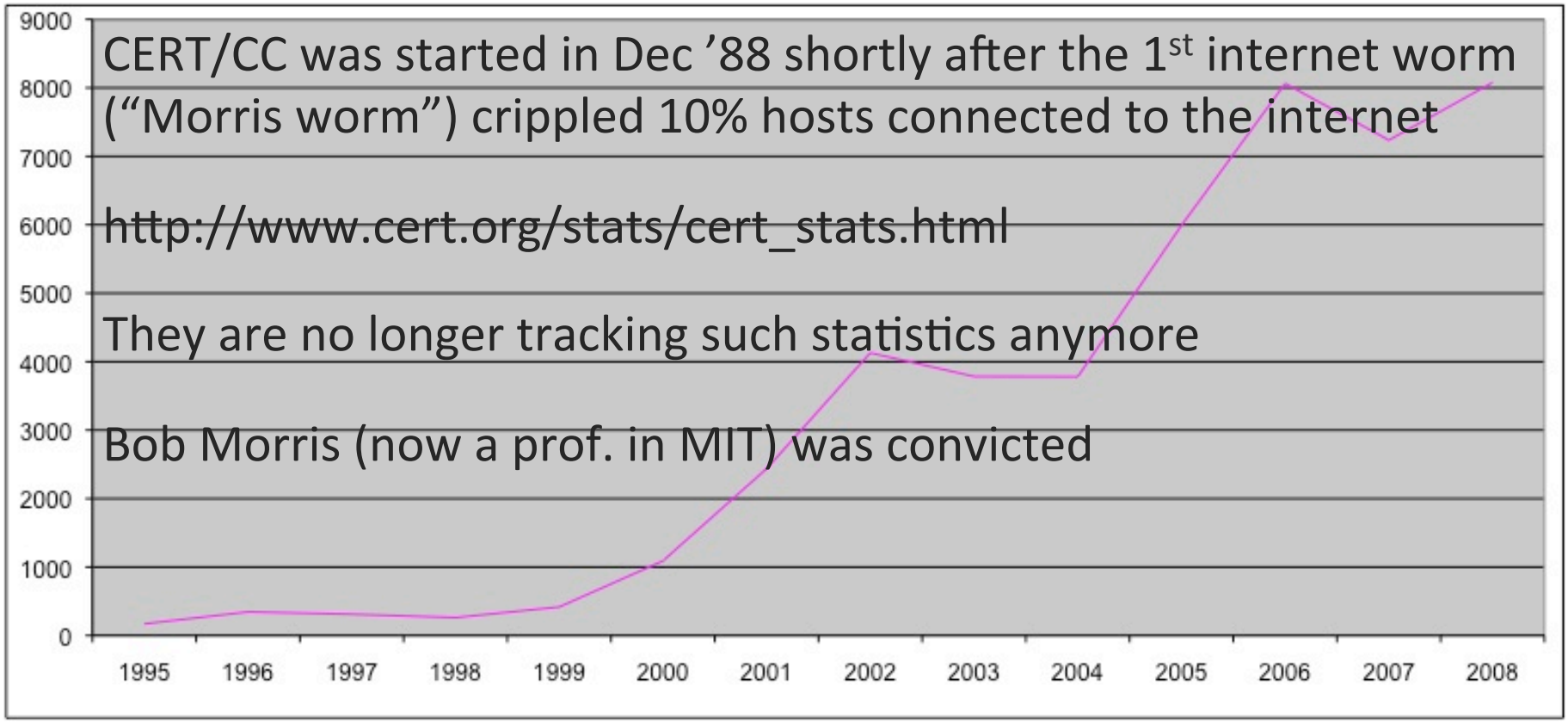


- Source: Data Breach Trends by RiskBasedSecurity
- (http://www.riskbasedsecurity.com/2015-data-breach-quickview)

Security Breach Incident Types (cont.)

SIR Label	Definition	DataLossDB Breach Types
Stolen equipment	Stolen computers, disks, tapes, or documents	Stolen computer / document / drive / laptop / media / tape
"Hack"	Reported as some type of computer intrusion where the data is not available to the public	Hack
Lost equipment	Reported as lost computers, disks, tapes, or documents	Lost computer / doc. / …
Accidental web	Accidental exposure on a web site, available to the public with a browser	Web
Fraud	Frauds and scams, perpetrated by insiders or outsiders; this includes dispute cases, on which Microsoft takes no position	Fraud Se
Postal Mall	Information exposed by physical mail, either sent to an incorrect recipient or with data visible outside the envelope	Snail Mail
E-Mail	E-mail sent to an unintended or unplanned recipient	Email
Disposal	Improper disposal of any sort	Disposal comp. / doc. / …
Malware	Malware was blamed	Virus
Missing	One or more laptop computers gone missing without explanation	Missing Laptop

Vulnerabilities Catalogue by CERT/CC



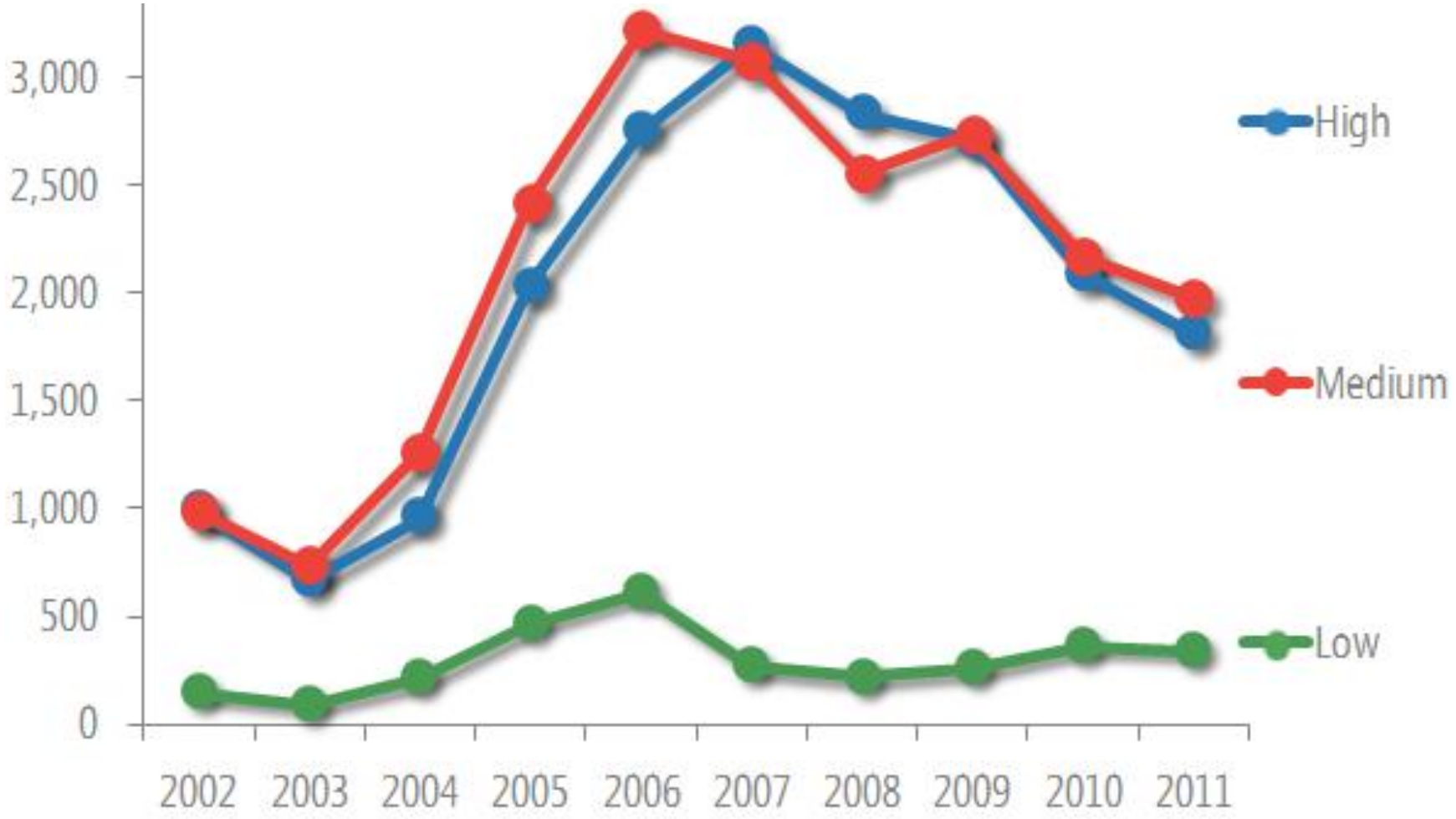
CERT/CC was started in Dec '88 shortly after the 1st internet worm ("Morris worm") crippled 10% hosts connected to the internet

http://www.cert.org/stats/cert_stats.html

They are no longer tracking such statistics anymore

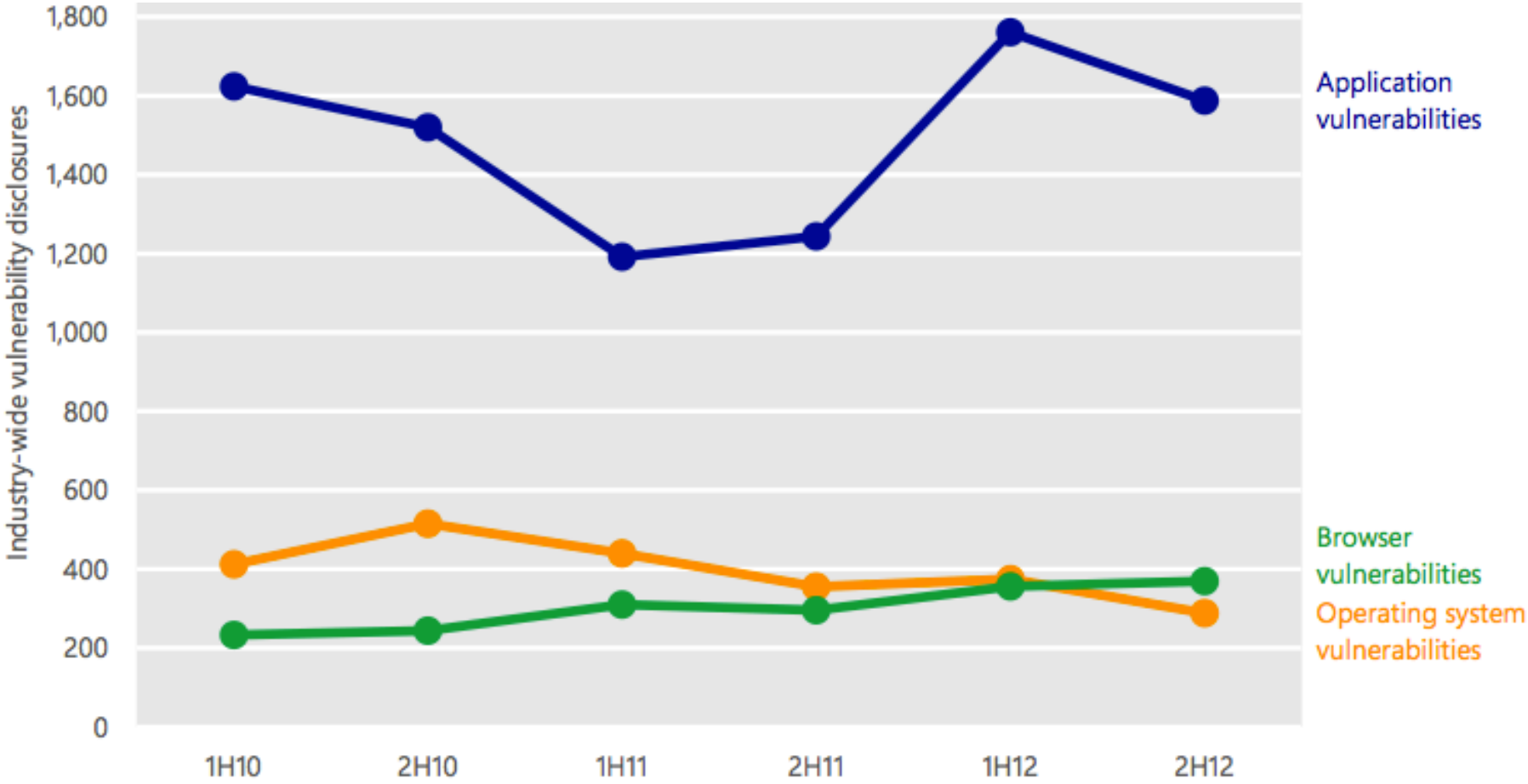
Bob Morris (now a prof. in MIT) was convicted

Industry-wide #. of Vulnerabilities Disclosures by Severity (’02 – ’11)



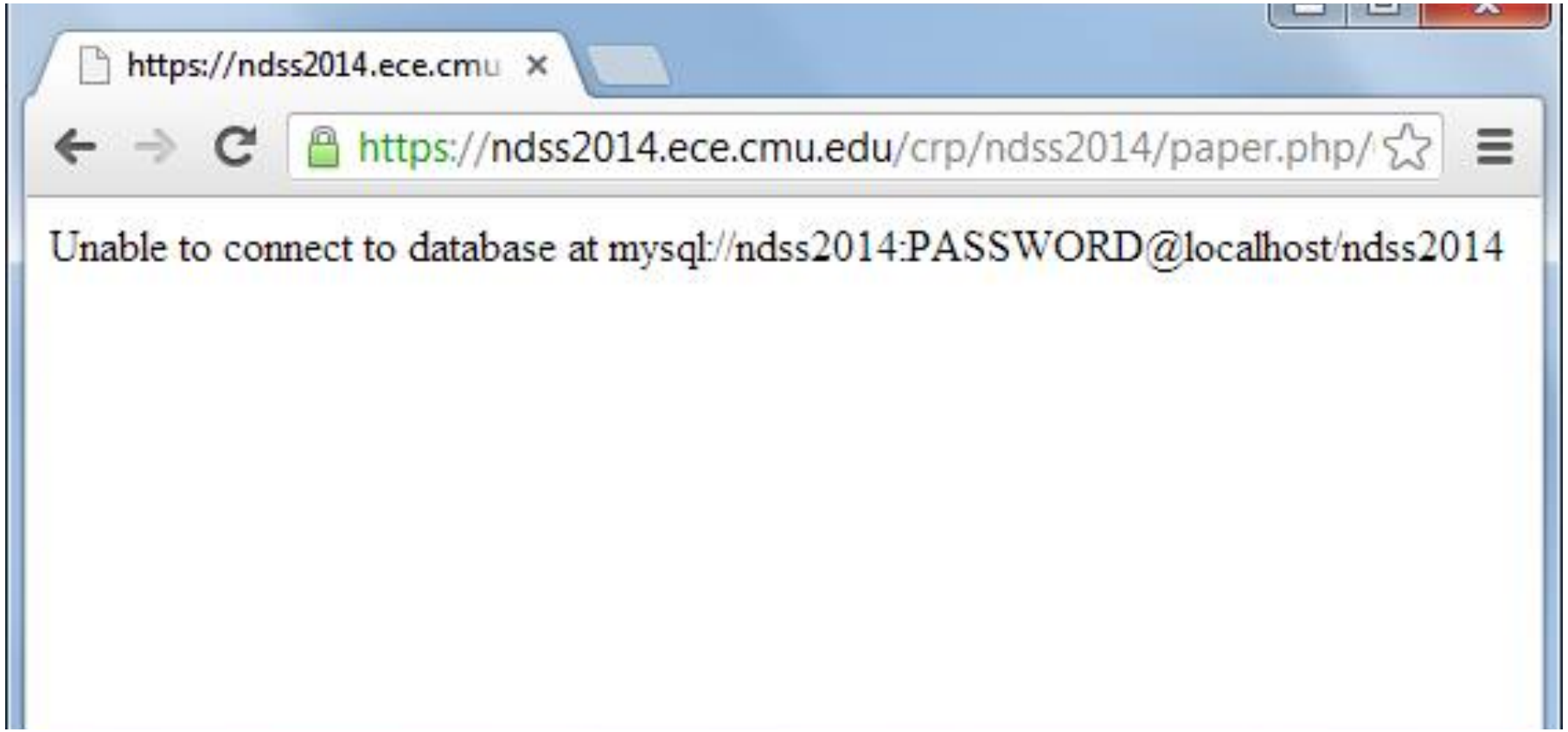
Source: MS Security Intelligence Report

Source of Vulnerabilities

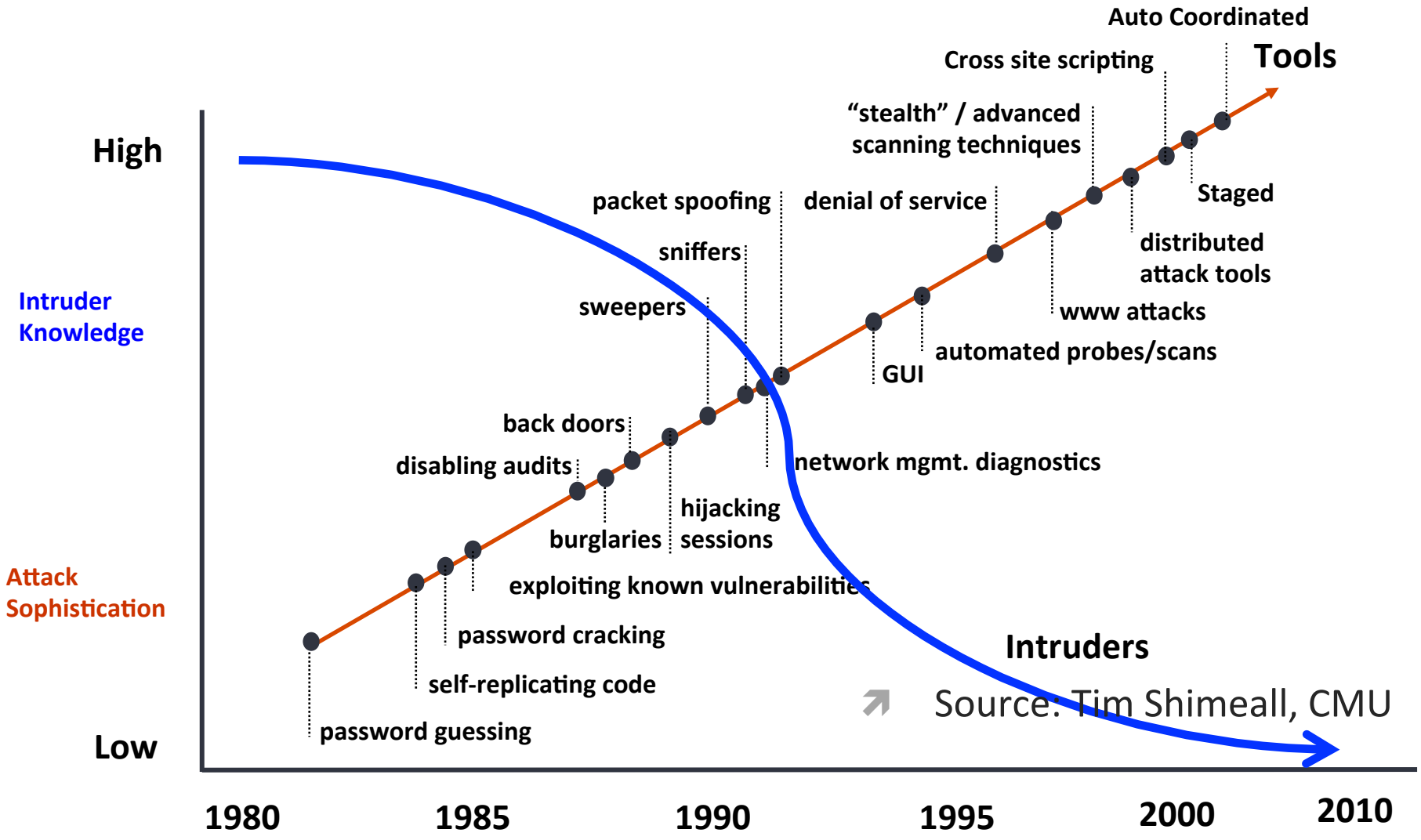


Source: MS Security Intelligence Report

Network and Distributed System Security

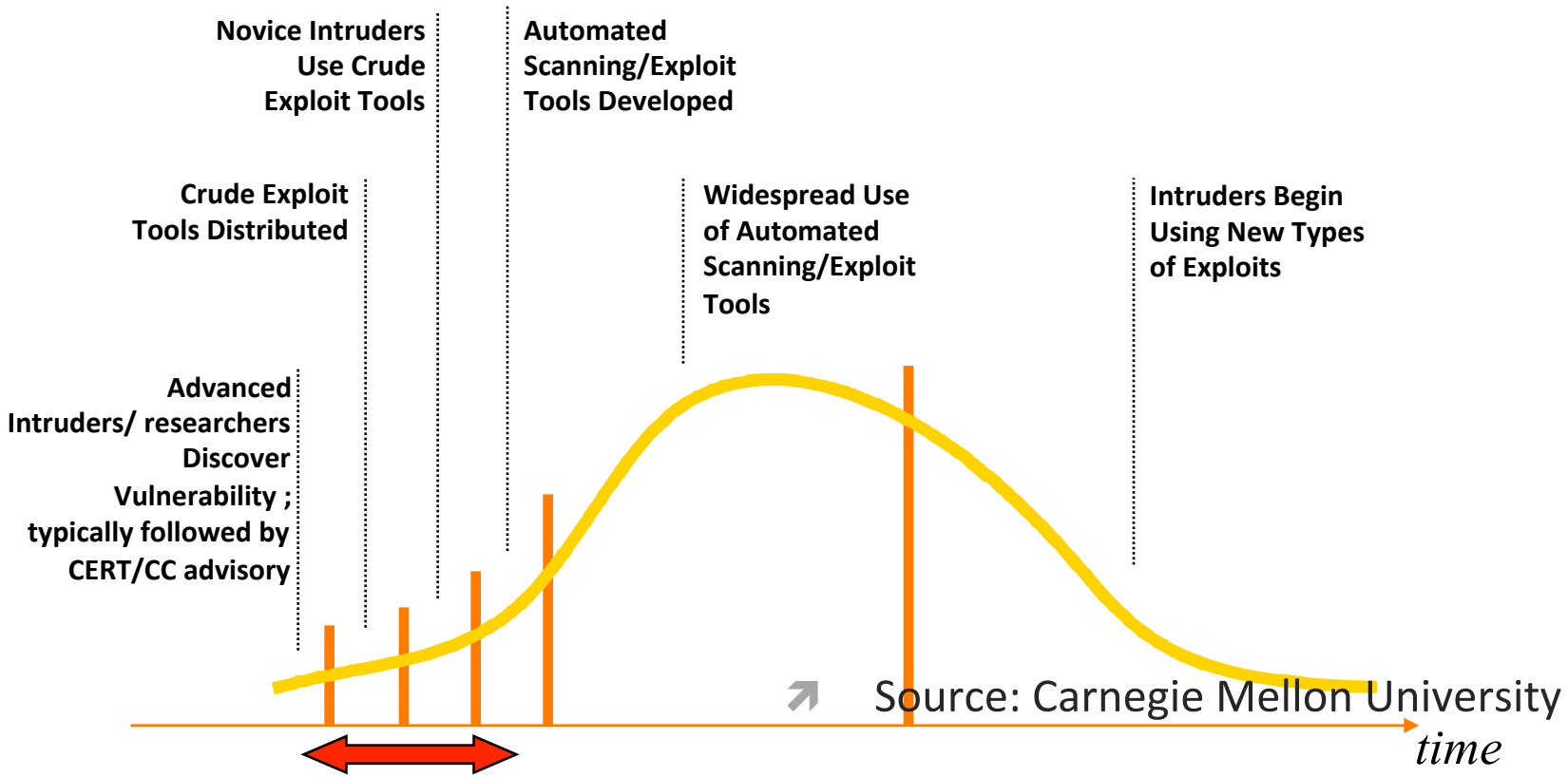


Attack Sophistication vs. Intruder Technical Knowledge



Source: Tim Shimeall, CMU

Shortening of Vulnerability Exploit Cycle



Source: Carnegie Mellon University

- Used to be several months, e.g., 6 months for SQL Slammer Worm (Jan 2003)
- Now, a matter of weeks or shorter. Thanks to framework tools e.g., Metasploit

How soon will your door be knocked?

- Experiment run by the worm.sdsc.edu Project:
  - Attach and Monitor an "Out of the Box" system on the Internet
  - First got probe for RPC vulnerabilities detected (after 8 hours)
  - The system was then completely compromised and a network sniffer was installed by the intruder (within a few weeks)
- You may be under similar risk if your home PC is hooked onto the Internet (Dial up or Broadband) "naked"
  - Forgot to turn the host-based firewall of the networked laptop back on => got totally compromised over the weekend

Sources: "The Laws of Vulnerabilities." Gerhard Eschelbeck, BlackHat Conf. '04
Slide from Prof. Wing Lau

The Window of Exposure

- Websites are an ongoing business concern and security must be assured all the time, not just at a point in time.
- Window-of-Exposure is the number of days in a year a website is exposed to at least one serious* vulnerability.
  - Serves as a true Key Performance Indicator
  - *Those vulnerabilities with a High, Critical, or Urgent severity as defined by PCI-Data Security Standard naming conventions.

Source: Jeremiah Grossman, Whitehead Security Inc.

The Window of Exposure (cont.)

- Not only be measured by the number of vulnerabilities
- But also take into account remediation rates and time-to-fixes.
- SiteA had 10 vulnerabilities identified during last year, 365 of those days it had at least one of those issues publicly exposed.
- SiteB had 100 vulnerabilities identified during last year, 10 of those days it had at least one of those issues publicly exposed.
- Which has a better security posture?

Source: Jeremiah Grossman, Whitehead Security Inc.

State of Web Security in ’11 (by Industry)

Industry	Annual Avg. Vulnerabilities	Std. Dev.	Avg. Time-to-Fix (Days)	Average Remediation	Std. Dev.	Window of Exposure (Days)	Std. Dev.
ALL	79	670	38	63%	36	231	159
Banking	17	554	45	74%	37	185	147
Education	53	885	30	46%	37	261	153
Financial Services	67	853	80	63%	35	227	157
Healthcare	48	461	35	63%	36	239	155
Insurance	***92***	171	40	58%	32	211	154
IT	***85***	36	35	57%	31	208	159
Manufacturing	30	56	17	50%	33	252	125
Retail	***121***	125	27	66%	36	238	160
Social Networking	31	431	41	62%	43	264	162
Telecom	52	82	50	69%	31	271	136
Non-Profit	37	56	94	56%	40	320	168
Energy	31	62	4	40%	35	250	154

Source: Whitehat Security Website Statistics Report

The Window of Exposure ’10 and ’11

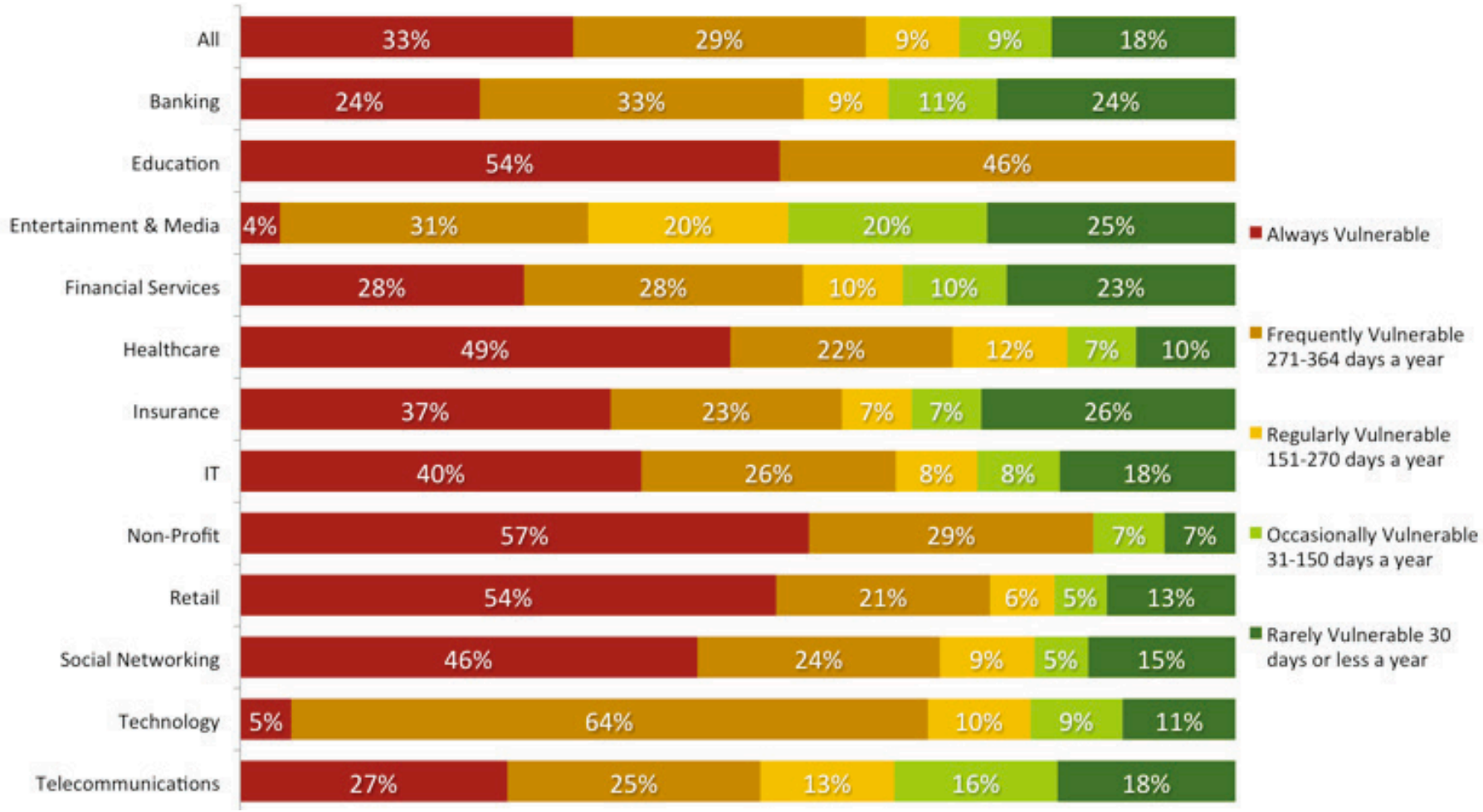
- Most websites were exposed to at least one serious vulnerability every single day of 2010, or nearly so (9-12 months of the year).
  - Exploitation could lead to breach or data loss.
- Only 16% of websites were vulnerable less than 30 days of the year overall.
- # of days improved from 233 to 231 days over a year…

State of Web Security in ’12 (by Industry)

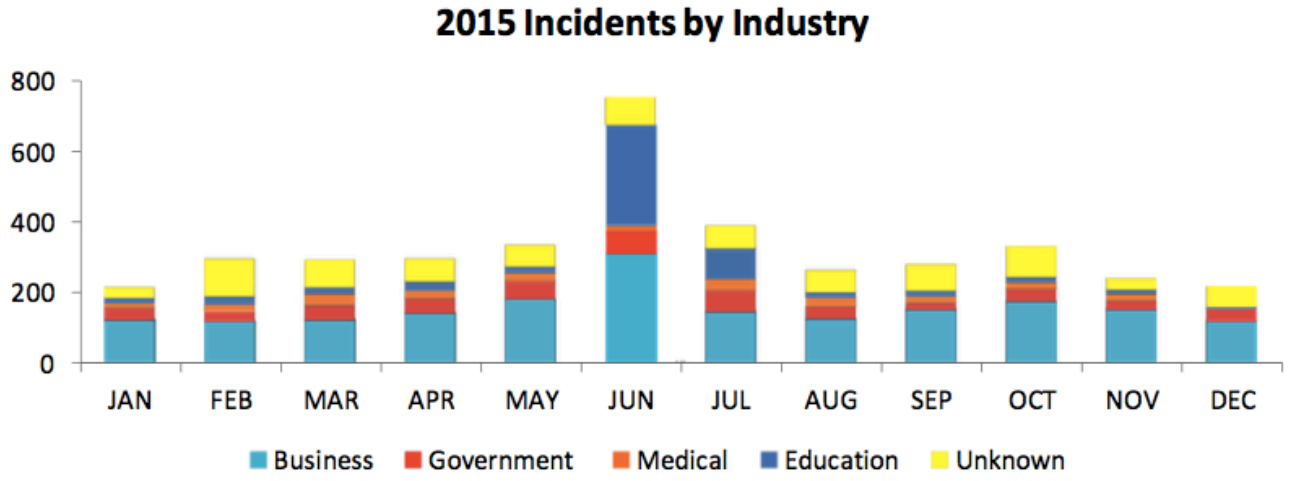
Industry	Avg Vuln Sites	Annual Avg Vulns	Remediation Rate	Avg. Time-to-Fix (Days)
All	86%	56	61%	193
Entertainment & Media	91%	12	81%	33
Financial Services	81%	50	67%	226
Retail	91%	106	54%	224
Technology	85%	18	61%	71
IT	85%	114	54%	185
Healthcare	90%	22	53%	276
Banking	81%	11	54%	107
Manufacturing	100%	27	55%	197
Social Networking	86%	20	46%	175
Telecommunications	89%	20	74%	163
Education	100%	47	58%	342
Energy	100%	59	71%	144
Insurance	78%	39	55%	274
Government	100%	8	65%	48
Non Profit	95%	28	41%	236
Food & Beverage	100%	18	46%	36
Gaming	92%	17	46%	67

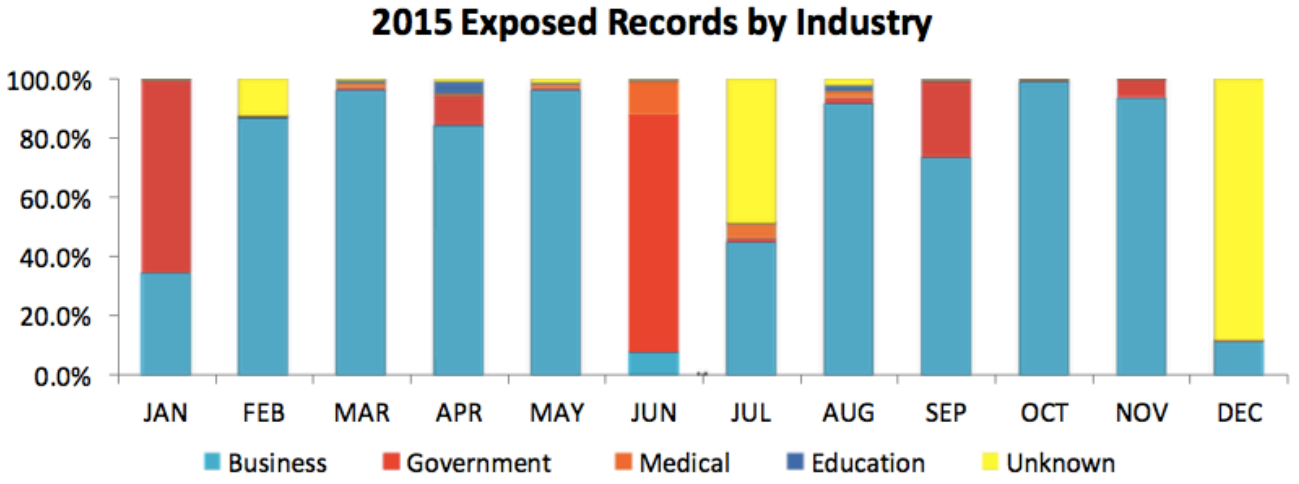
- https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf

The Window of Exposure in ’12



State of (In)Security in ’15 (by Industry)





Why do vulnerabilities go unfixed?

- No one at the organization understands or is responsible for maintaining the code.
- Development group does not understand or respects the vulnerability.
- Feature enhancements are prioritized ahead of security fixes.
- Lack of budget to fix the issues.
- Affected code is owned by an unresponsive third-party vendor.
- System/Application/Website will be decommissioned or replaced “soon.”
- Risk of exploitation is accepted.
- Solution conflicts with business use case.
- Compliance does not require fixing the issue.
- www.whitehatsec.com/assets/presentations/11PPT/PPT_topwebvulns_030311.pdf

Prompt Security Testing is Crucial

If the response time from security testing process is:

Then, development time required to fix is:

- Developer introduces code with a vulnerability

Source: http://img.en25.com/Web/WhiteHatSecurityInc/WPstats_summer12_12th.pdf

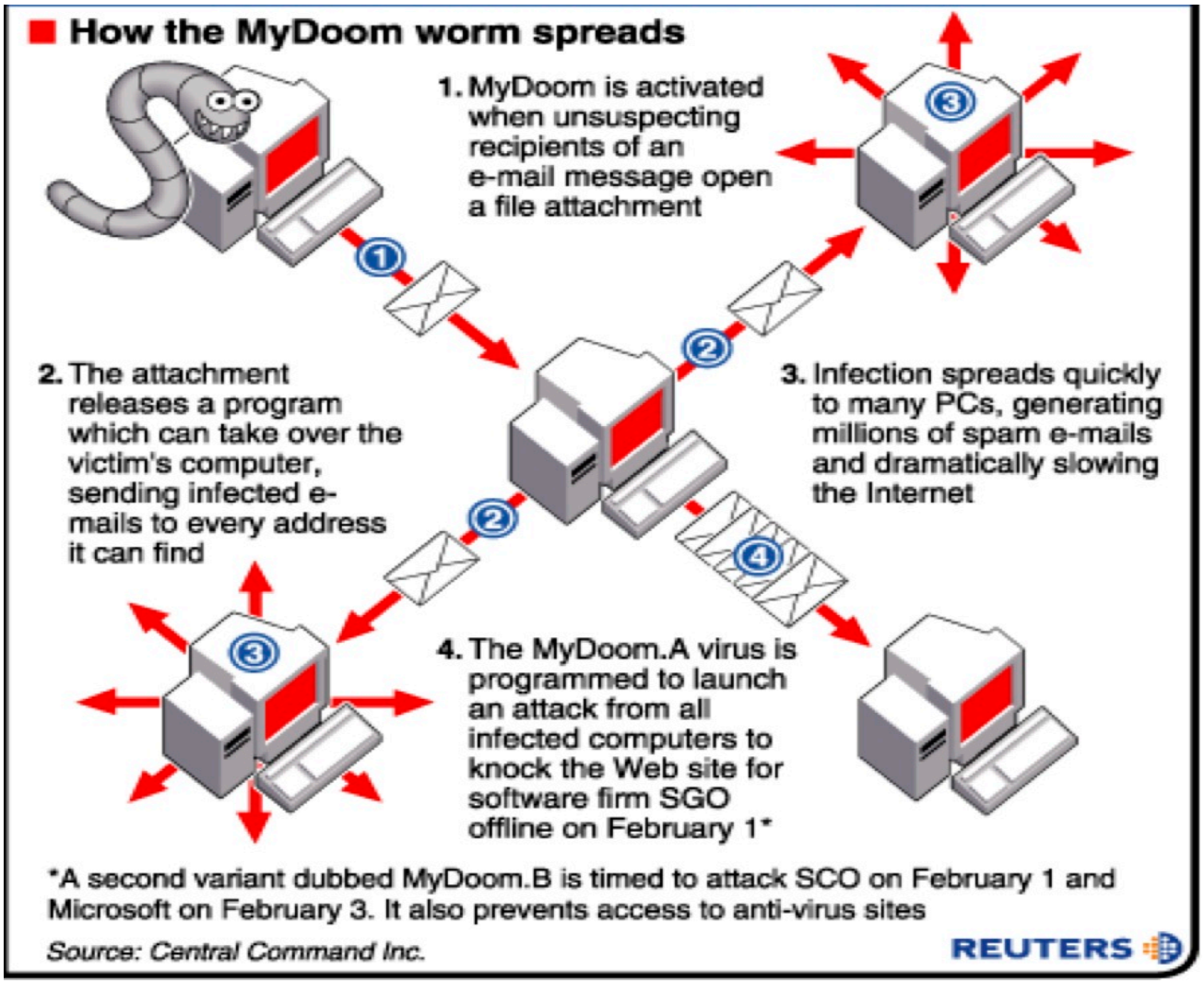
Various Types of Digital Pest

- Logic Bomb: logic embedded in a program that checks for a set of conditions to arise and executes some function resulting in unauthorized actions
- Backdoor/Trapdoor: secret undocumented entry point into a program, used to grant access without normal methods of access authentication (*remember the movie: War Games*)
- Trojan Horse: secret undocumented routine
  embedded within a useful program,
  execution of the program results in execution of the routine
  - Common motivation is to destroy data or provide illegal access

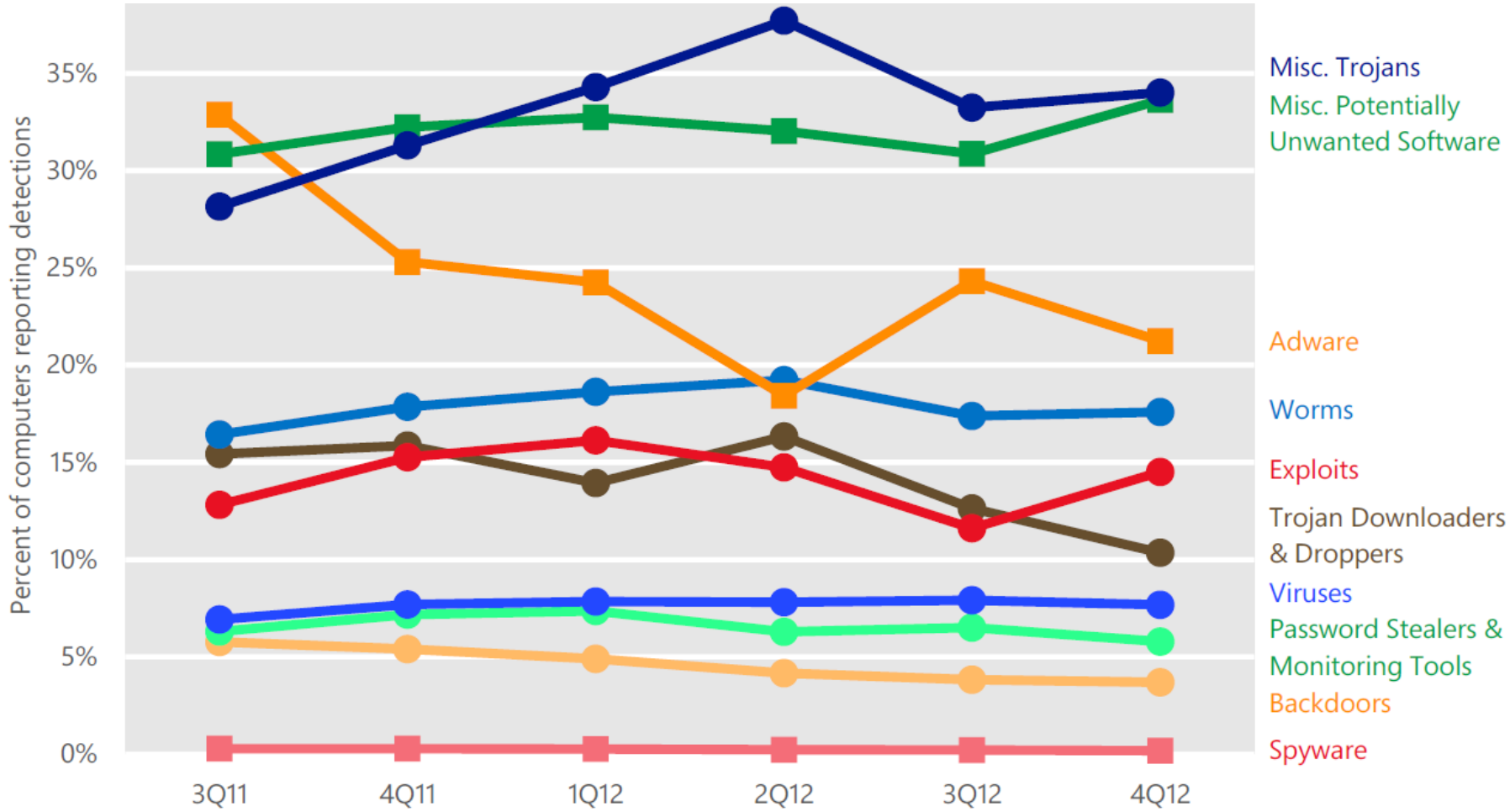
Various Types of Digital Pest (cont')

- Virus: code embedded within a program that causes a copy of itself to be inserted in other programs and performs some unwanted function
  - Infects other programs
- Worm: program that can replicate itself and send copies to computers across the network and performs some unwanted function
  - Uses network connections to spread from system to system
- Zombie/Bot: a program that secretly takes over an Internet attached computer and then uses it to launch an untraceable attack
  - Very common in Distributed Denial-of-Service (DDoS) attacks

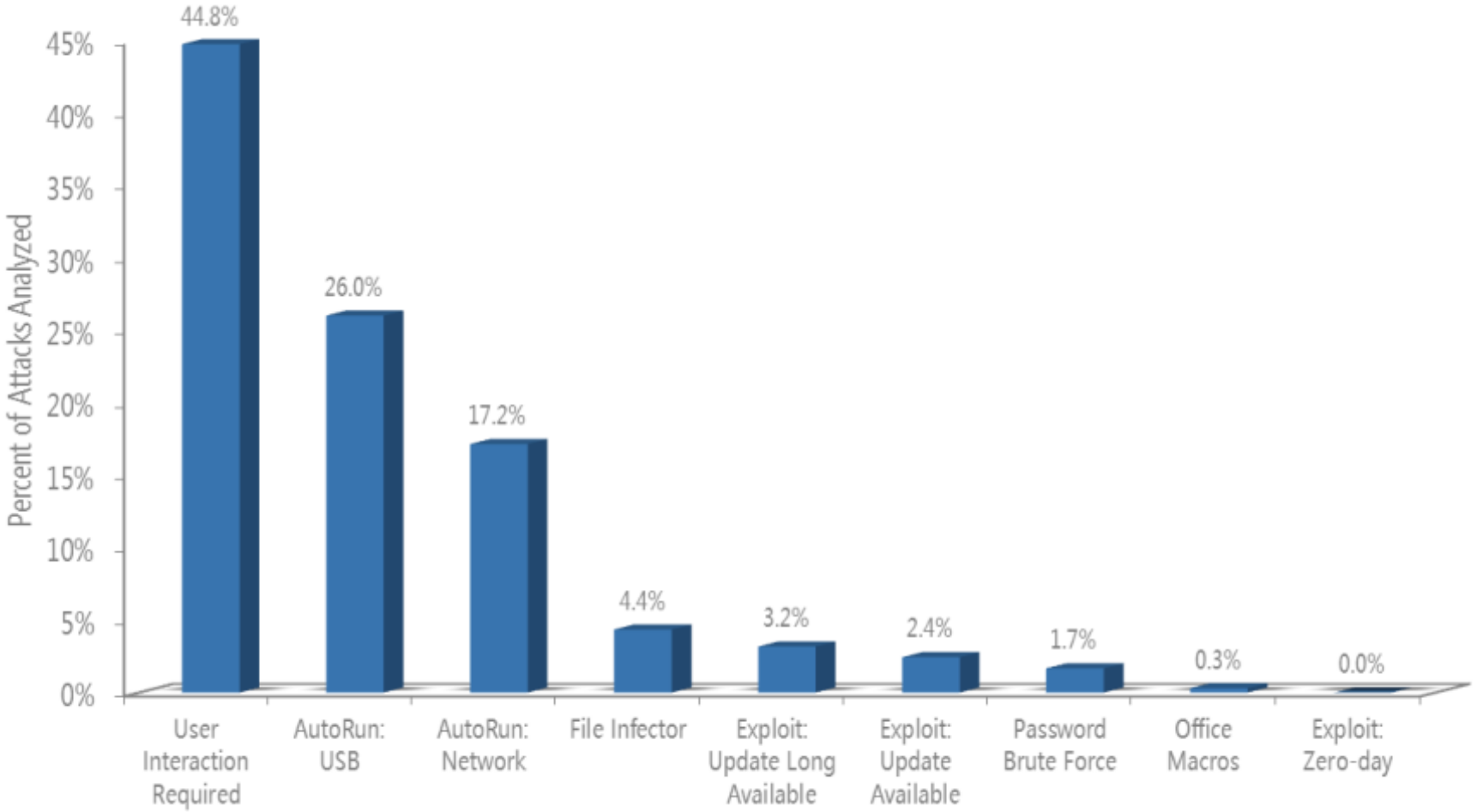
Spreading of Worms



Computer Cleaned by Threat Categories

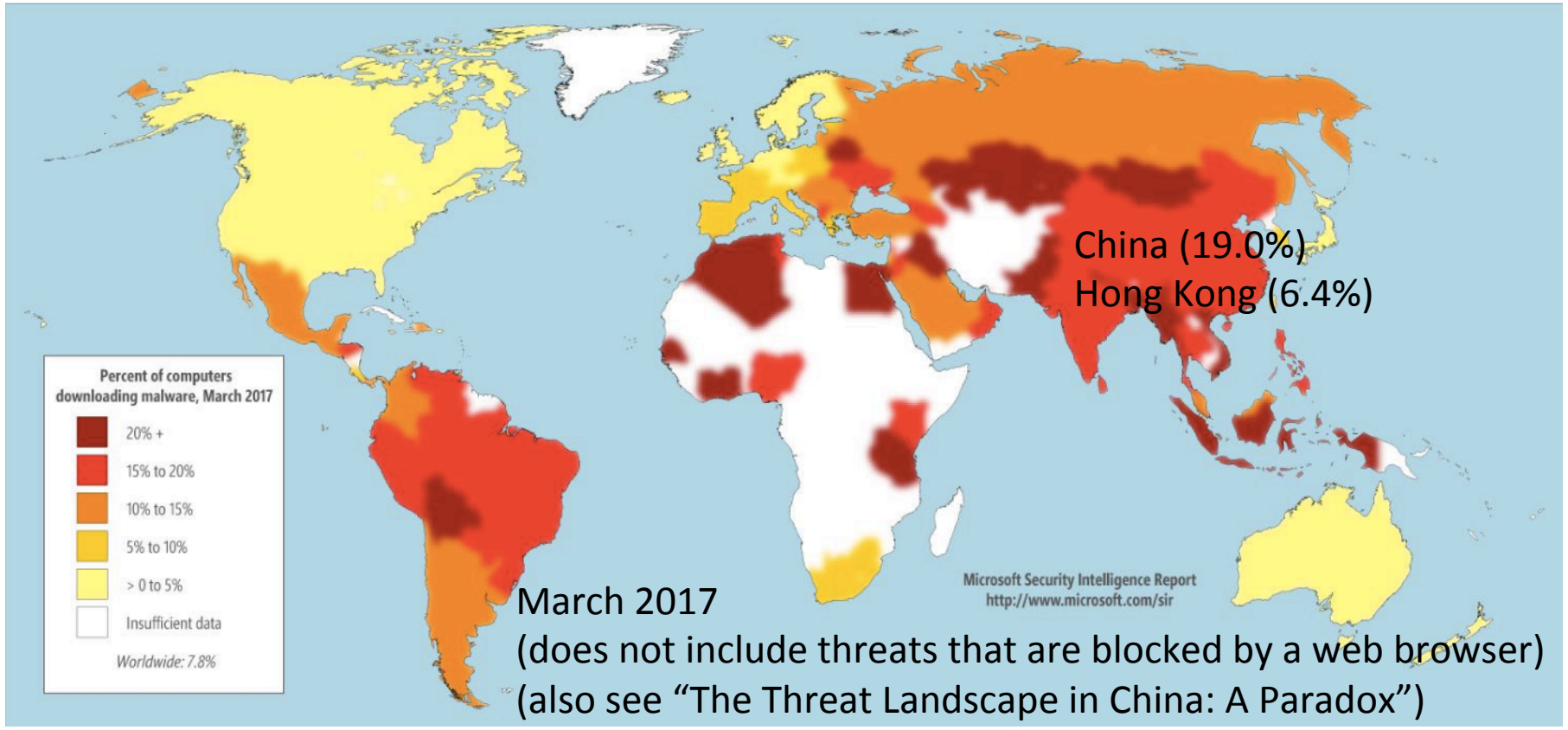


Means of Propagation for Malware (1H'11)



Source: MS Security Intelligence Report

Encounter Rates by Country/Region



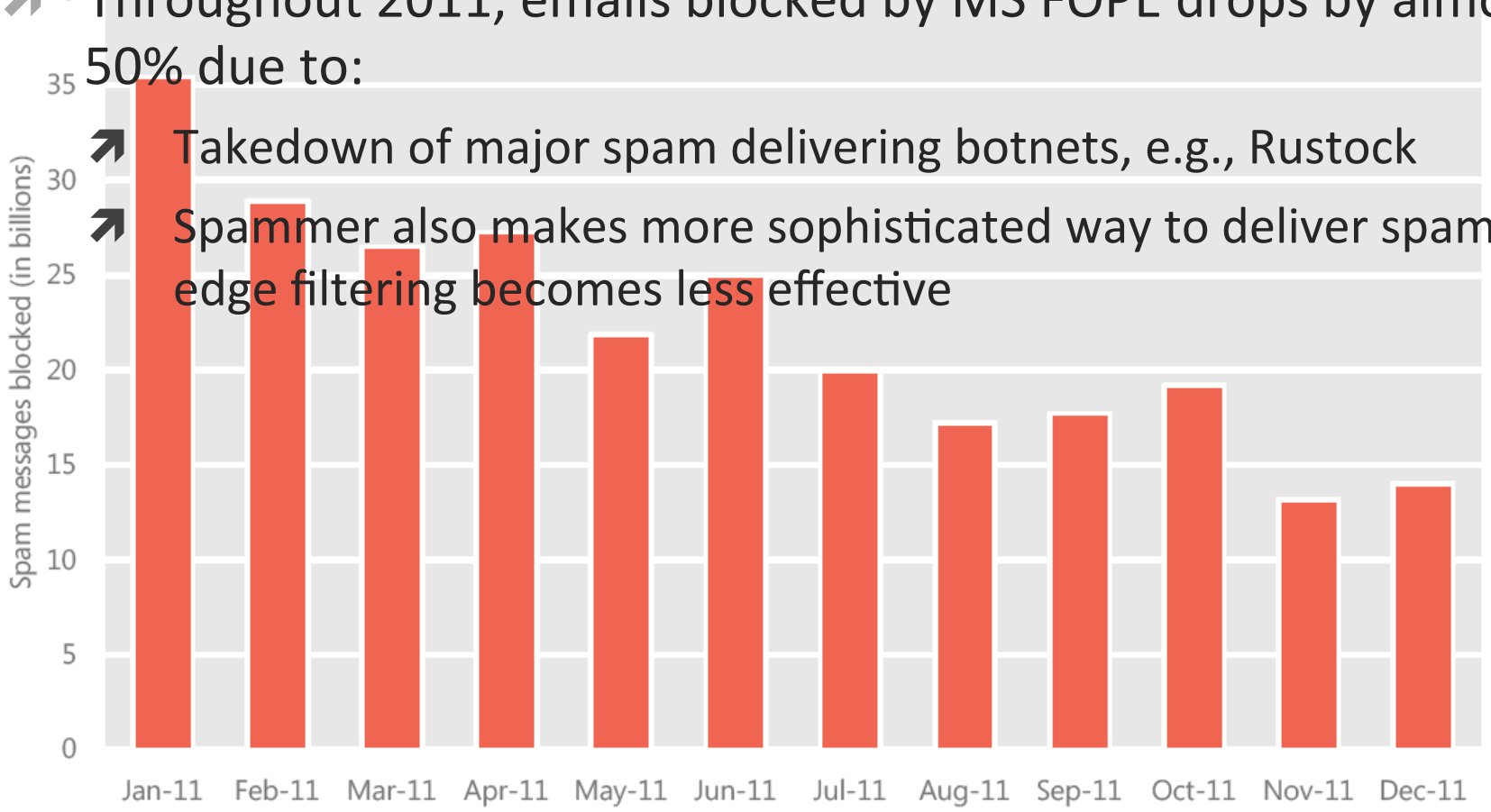
- High: Bangladesh (26.6%), Pakistan, Indonesia, and Egypt
- Low: Japan (1.1%), Finland, Sweden, and Norway

Email Threats: Spam

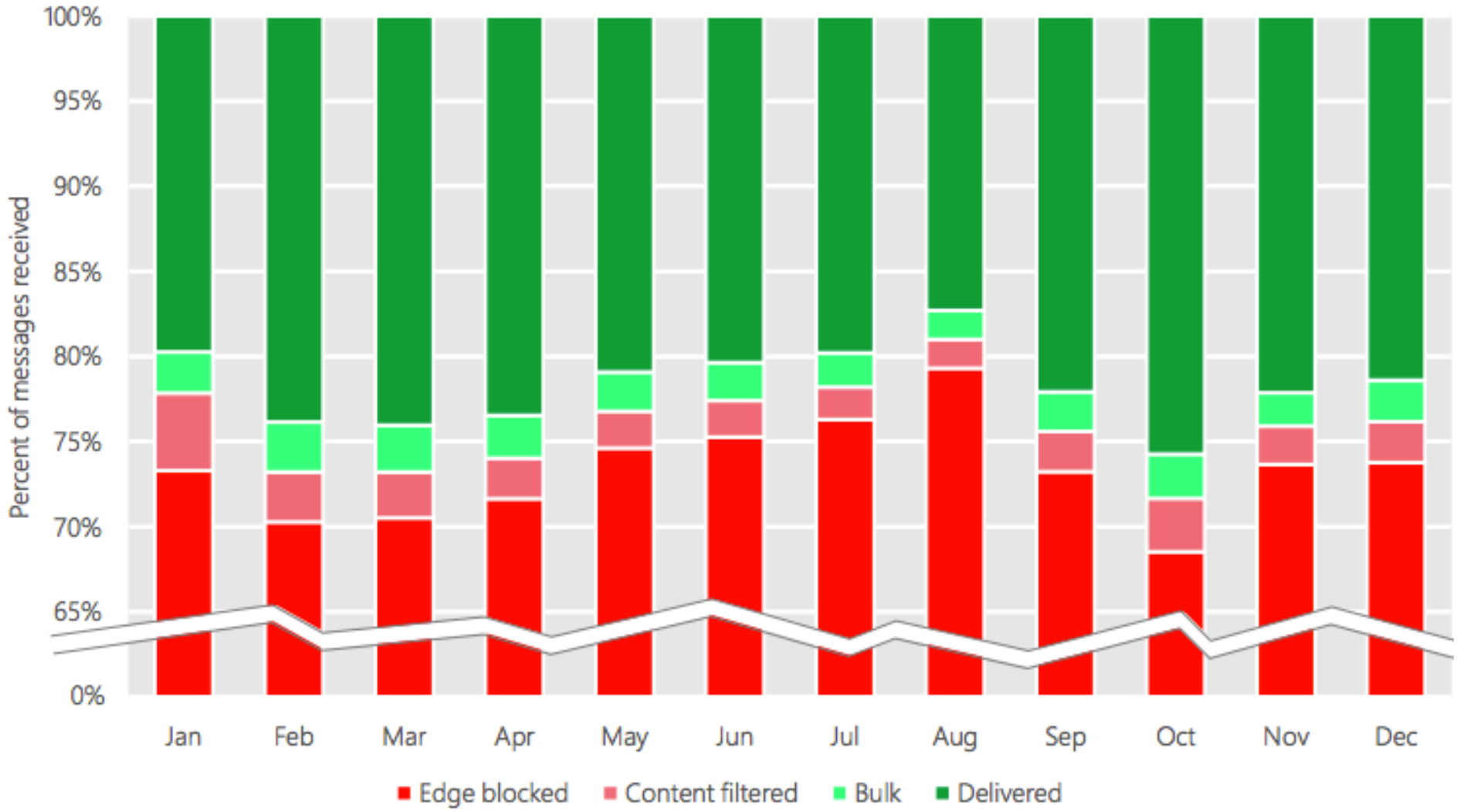
- Greater than 97% emails sent over the Internet are unwanted!
- In 2010, only 1 out of 38.5 incoming messages made it to the inbox. The rest were blocked by either:
  - Network edge filtering (95.3%), e.g., IP addr reputation, SMTP connection analysis, recipient analysis; or
  - Resource-intensive content-based filtering (4.7%)
- Still strong financial incentive for Spammers
- How to prevent your email address from being harvested?
  - $0x80

Combating the botnet menace

- Throughout 2011, emails blocked by MS FOPE drops by almost 50% due to:
  - Takedown of major spam delivering botnets, e.g., Rustock
  - Spammer also makes more sophisticated way to deliver spam, edge filtering becomes less effective

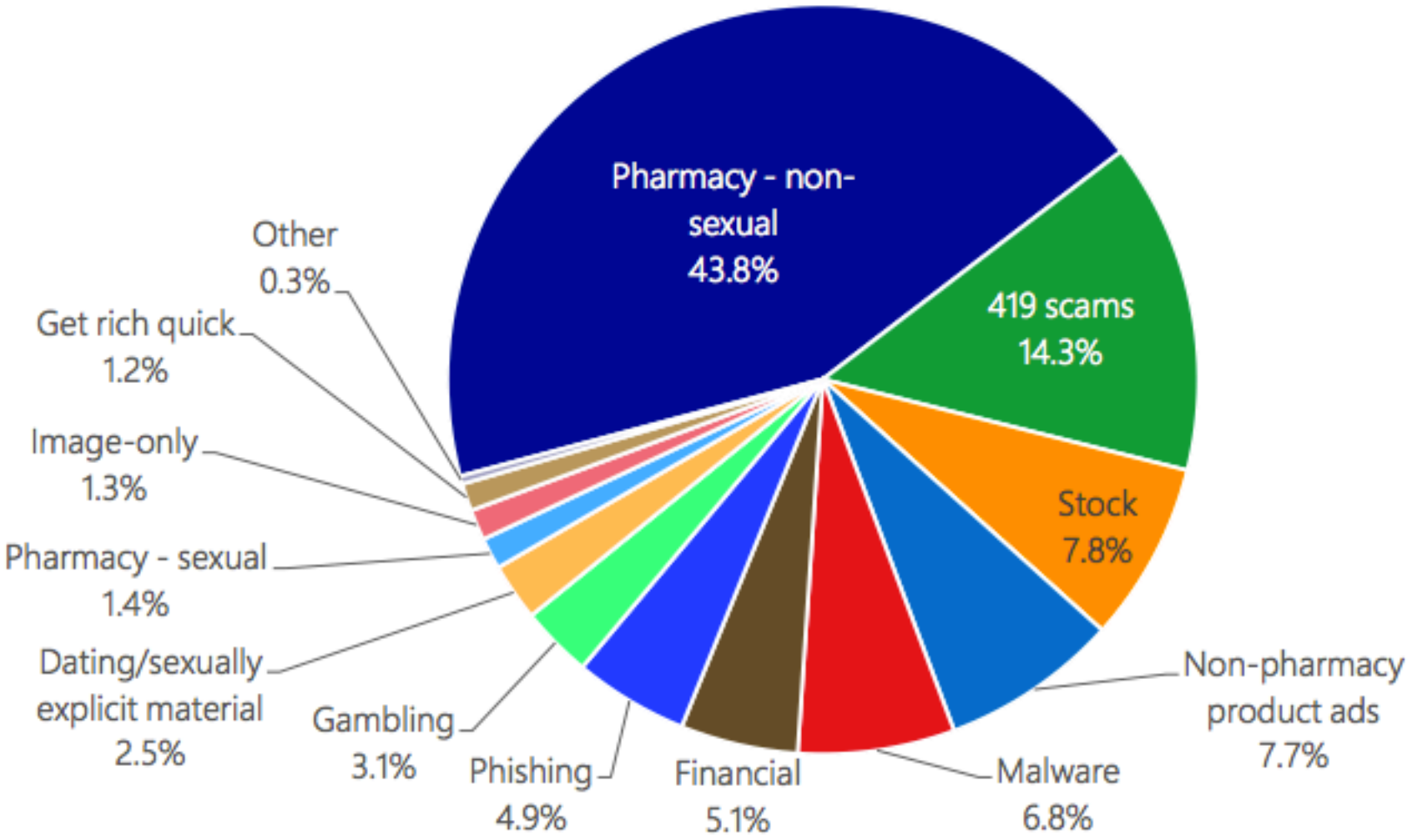


Yet, it strikes back in 2012…



What spam I receive most?

Types of Spam in 2H'12



Phishing (an actual example)

- Phishing: A fraudulent attempt to trick you to provide personal information, e.g., HKID #, password, credit card #, etc.

From: CUHK <JPAGALO@espol.edu.ec>
Date: 13 August 2012 9:06:04 AM GMT+08:00
To: undisclosed-recipients:;
Subject: CUHK Impotant Notification
Reply-To: webmasterss@cuhk.edu.hk

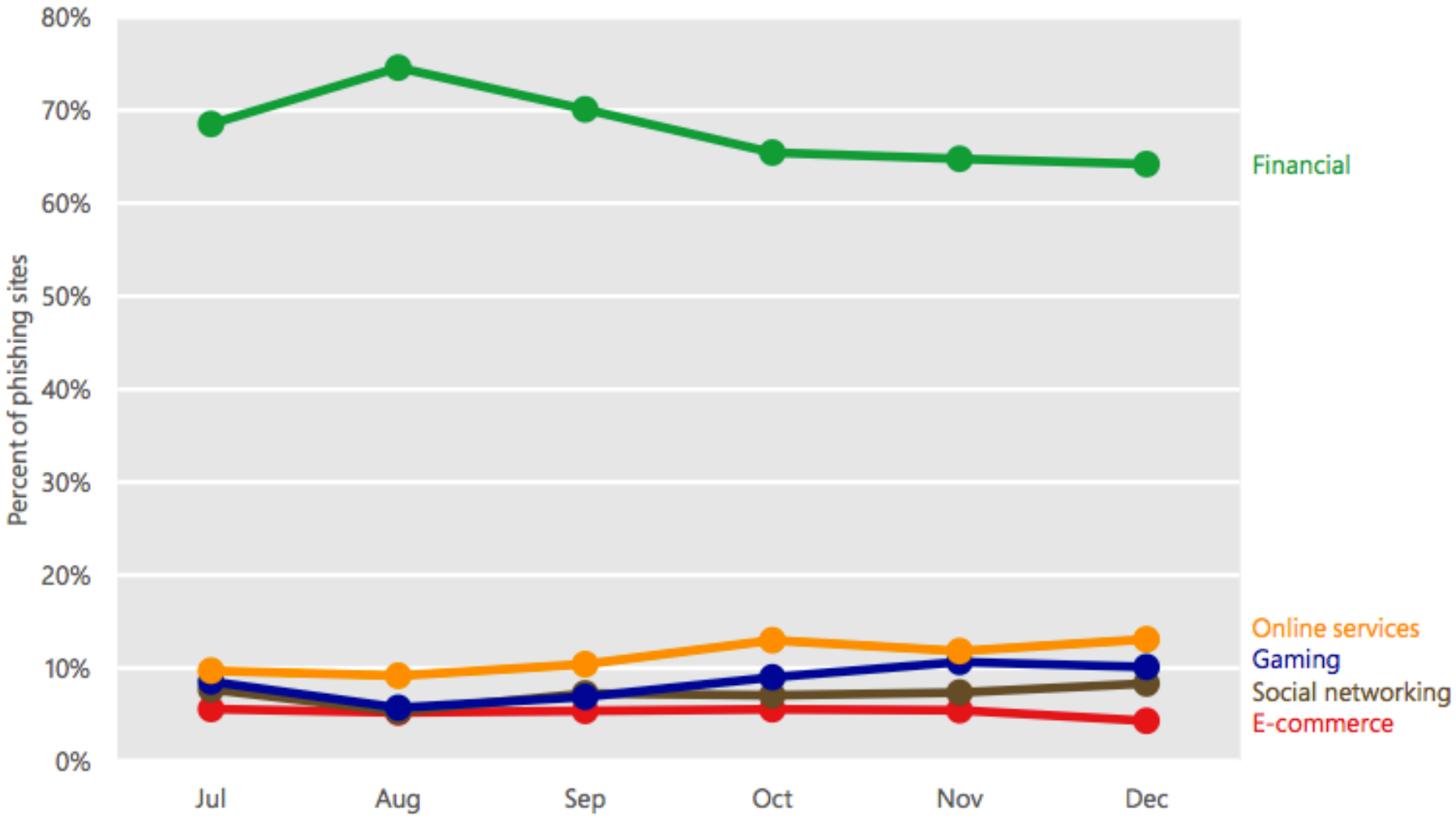
Attention IE account holder,

This message is from the Chinese University of Hong Kong technical support center, we will be making some vital E-mail account maintenance to ensure that we provide high quality in Internet connectivity in the 2012 and fight spam and improve security, all Mail-hub systems will undergo regularly scheduled maintenance.

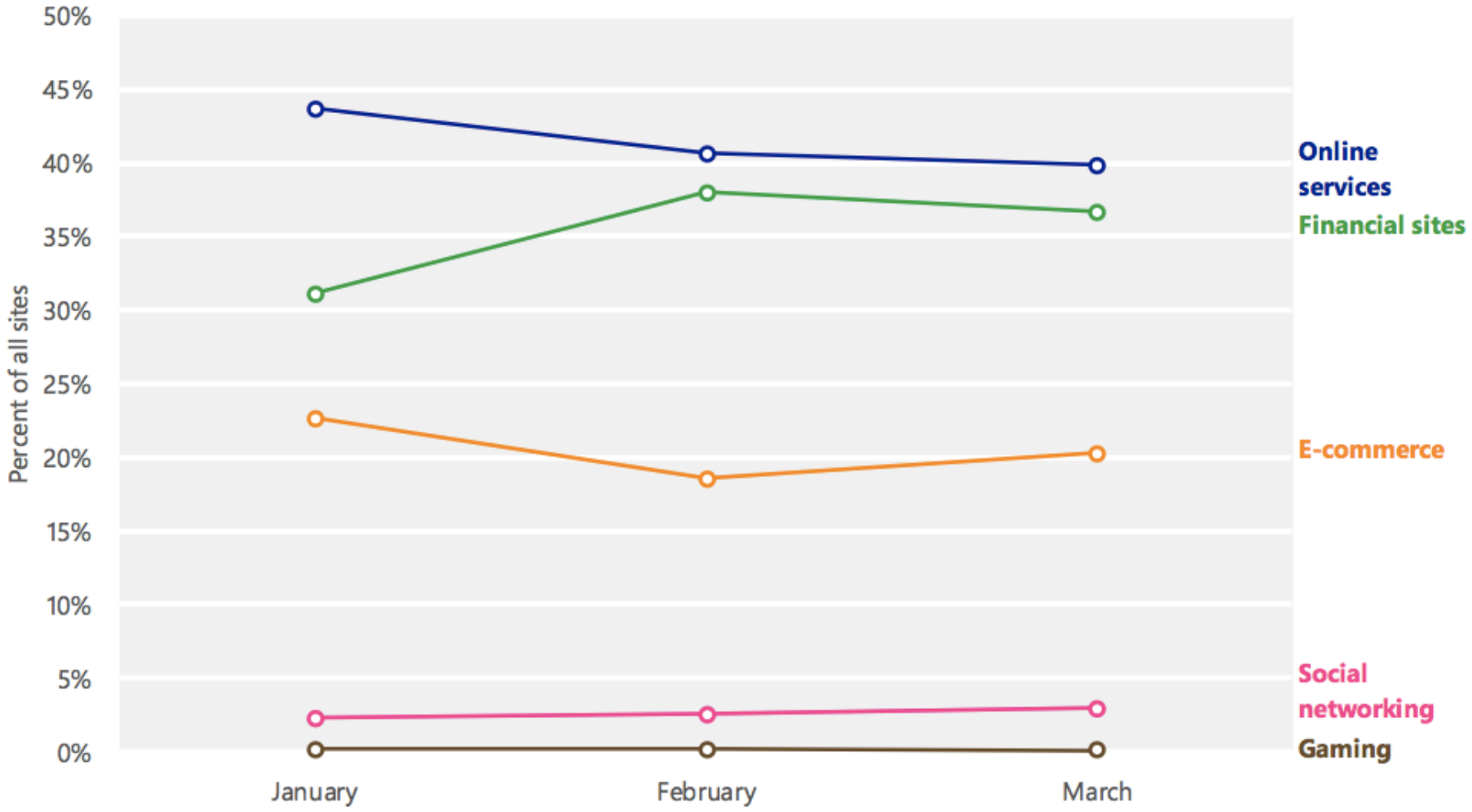
To confirm and to keep your account active during and after this process Kindly Click and fill the following information: **Click**

Web Services / Information Technology Department,
Chinese University of Hong Kong (CUHK)

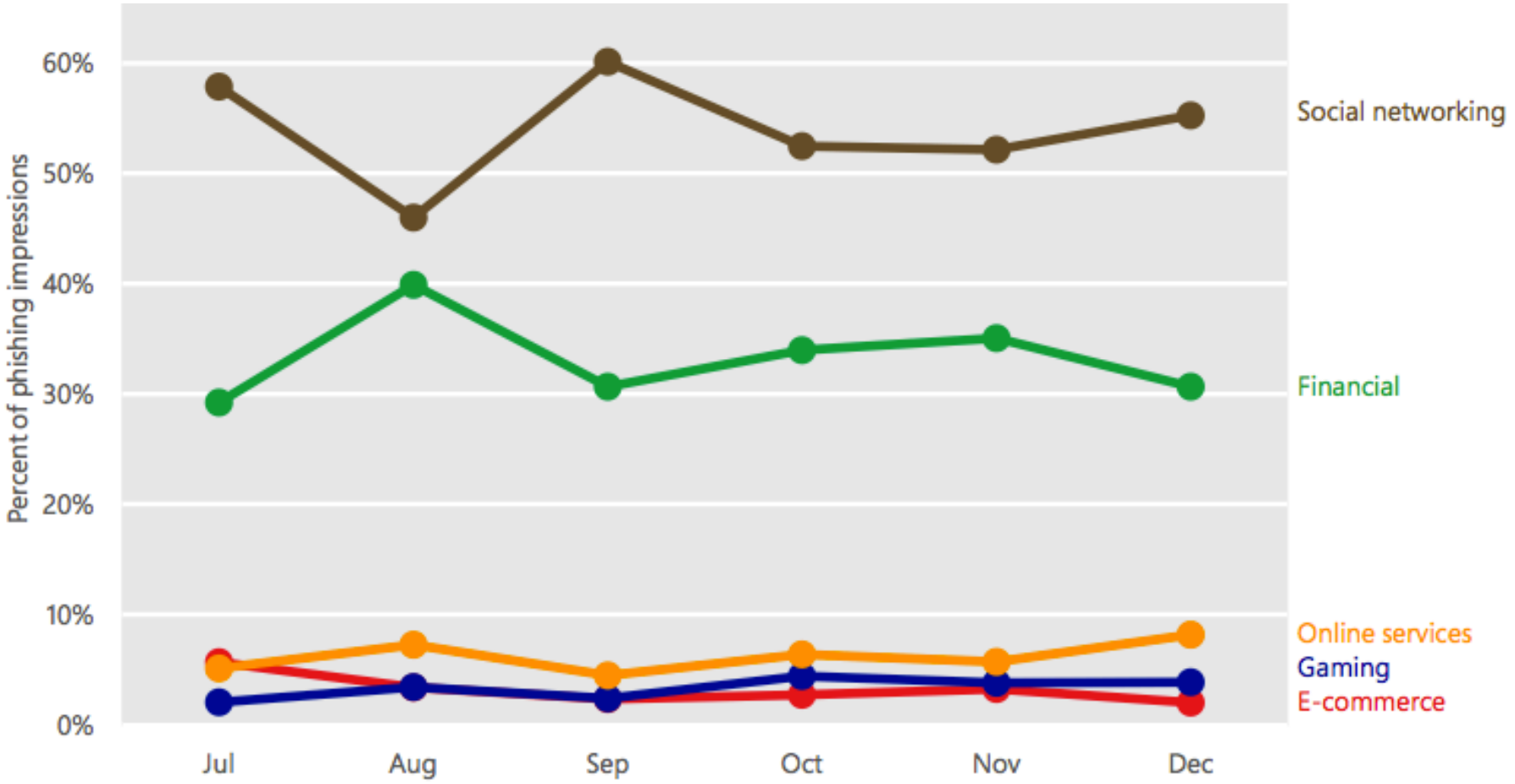
Types of Phishing Target Sites in ’12



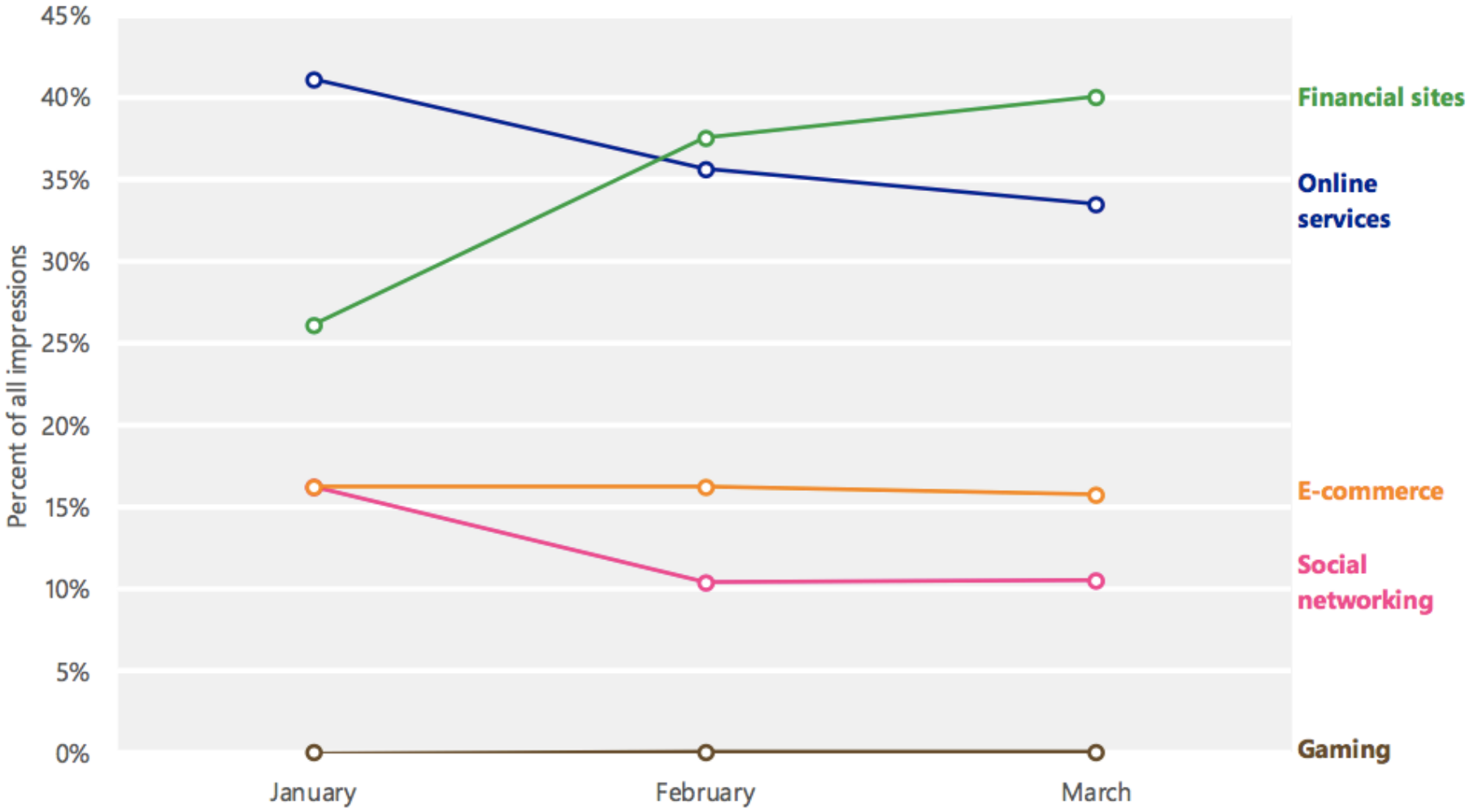
Types of Phishing Target Sites in 1Q17



Impression (’12)

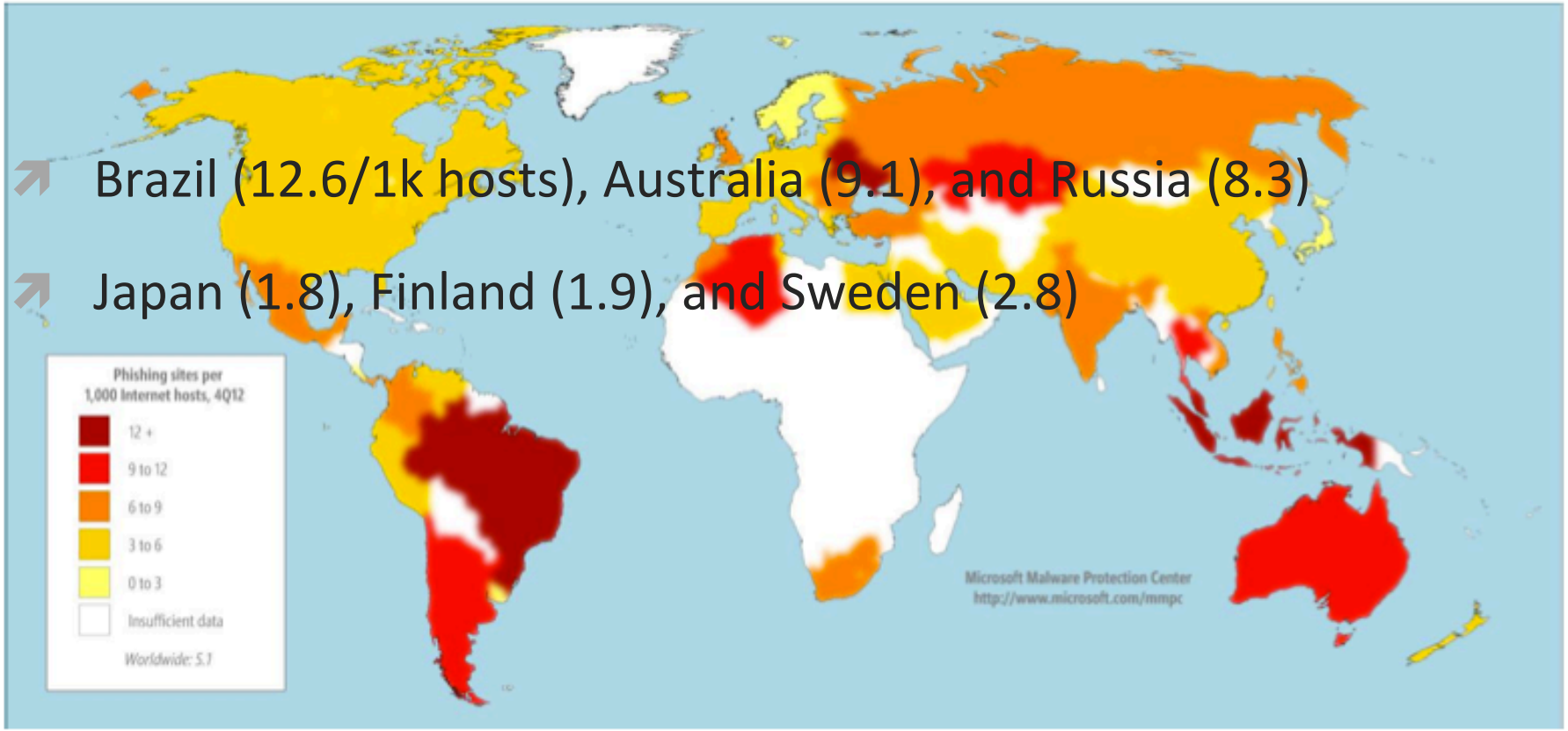


Impression (’17)



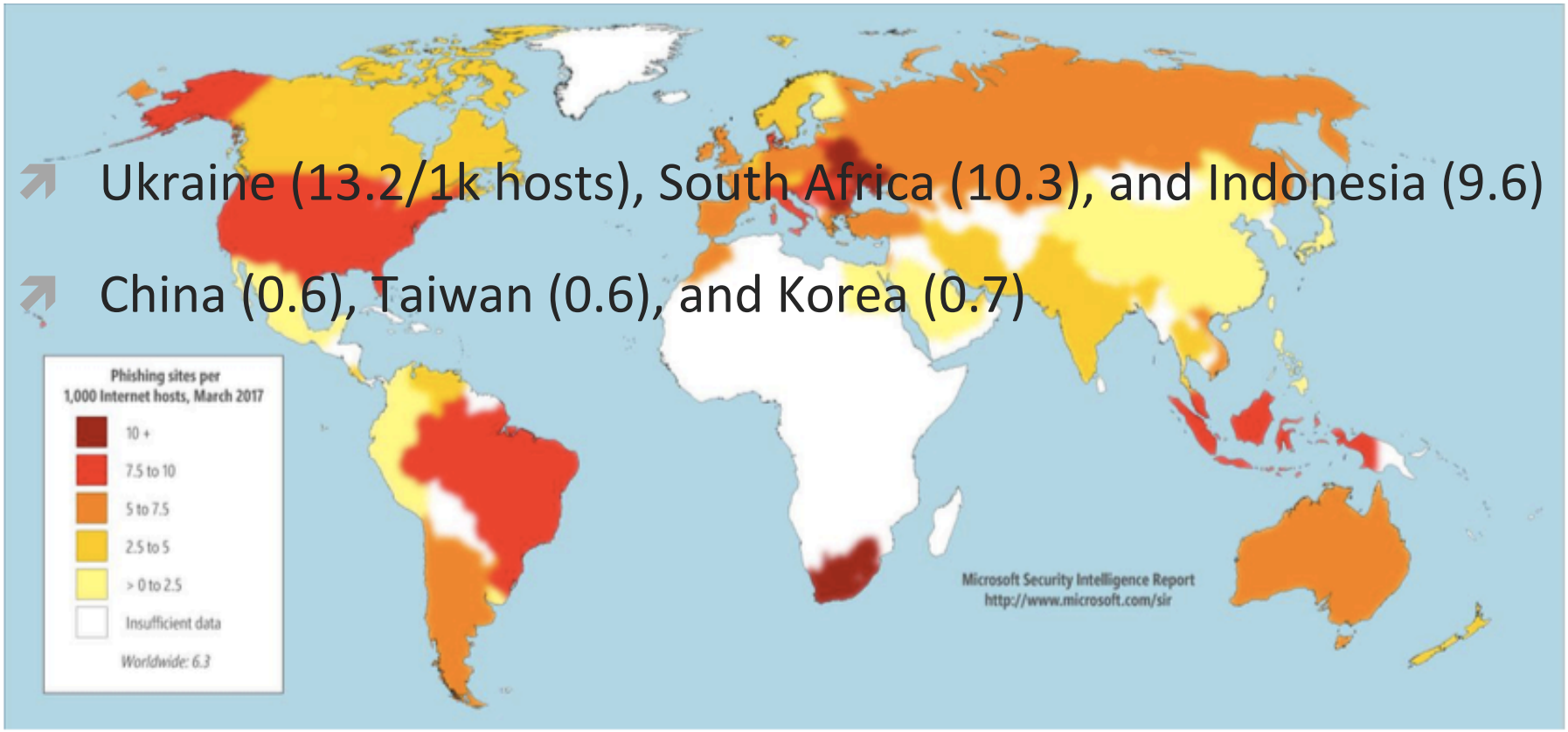
Phishing Sites hosted Worldwide in 4Q'12

- Brazil (12.6/1k hosts), Australia (9.1), and Russia (8.3)
- Japan (1.8), Finland (1.9), and Sweden (2.8)



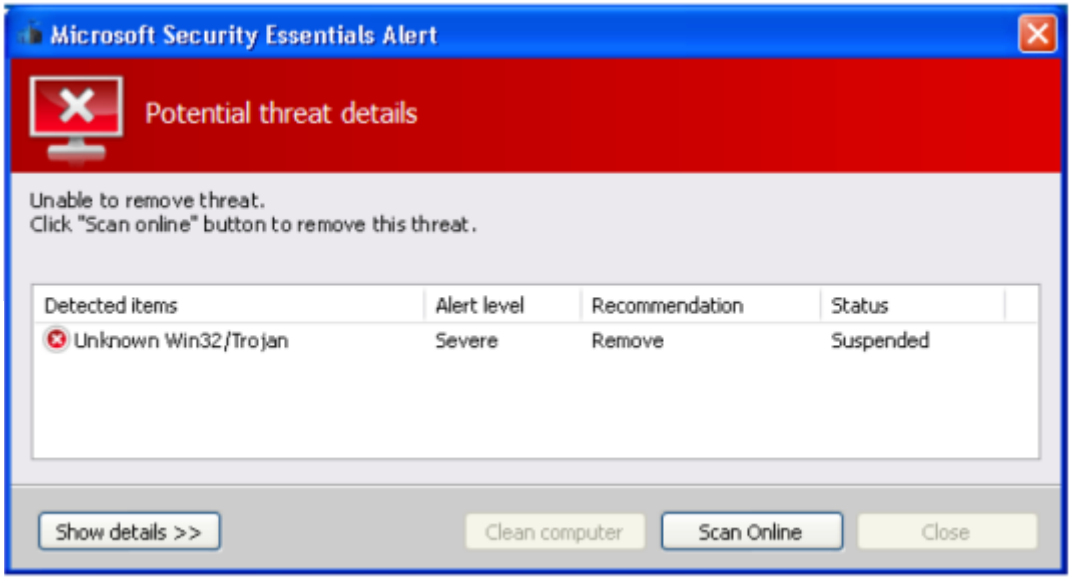
Phishing Sites hosted Worldwide in 1Q'17

- Ukraine (13.2/1k hosts), South Africa (10.3), and Indonesia (9.6)
- China (0.6), Taiwan (0.6), and Korea (0.7)

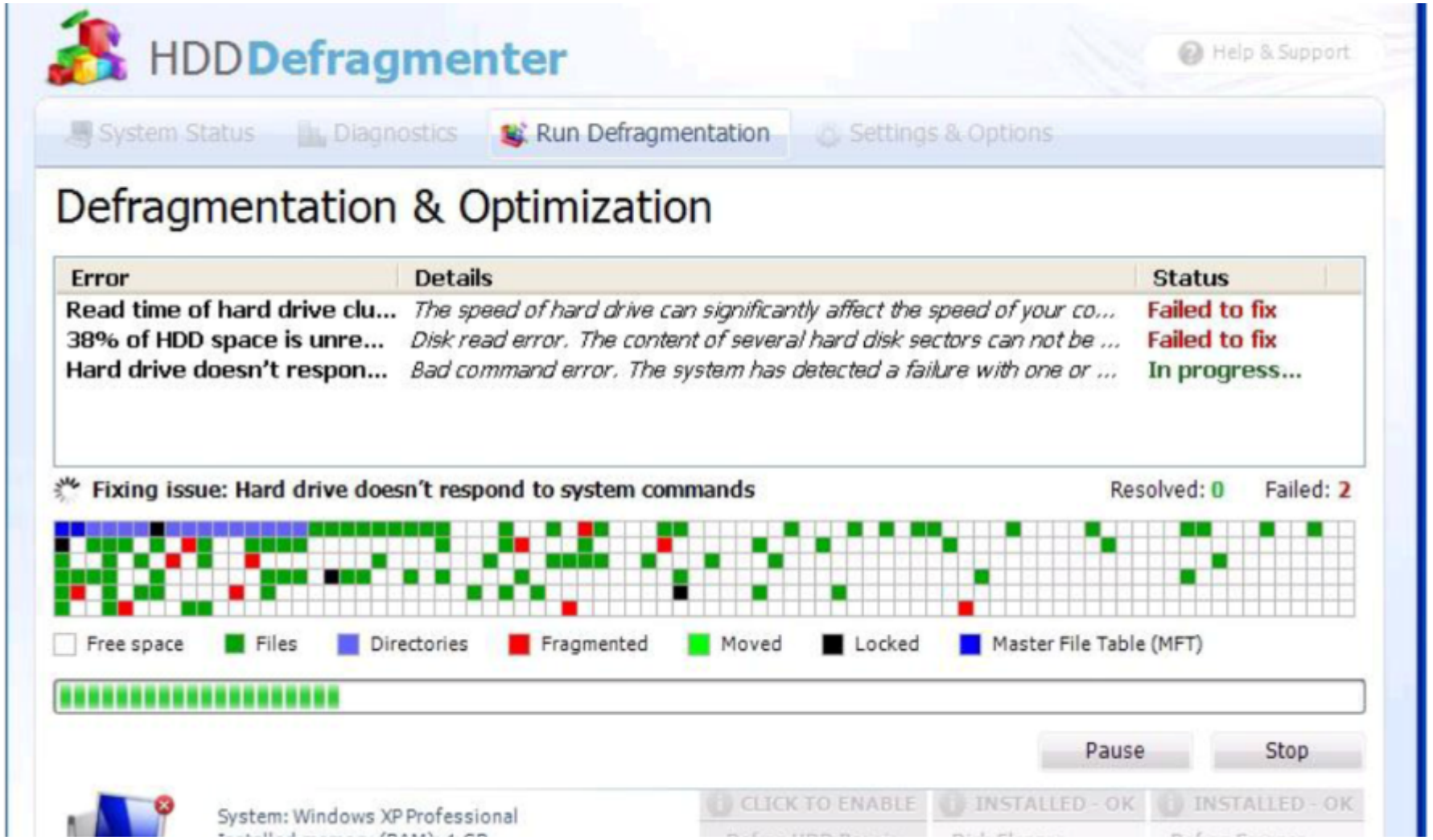


Rogue Security Software

- a.k.a. Rogue Anti-Malware, Scareware
- Rapid growth in the past couple of years
- www.microsoft.com/security/antivirus/rogue.aspx



More Rogue Security Software

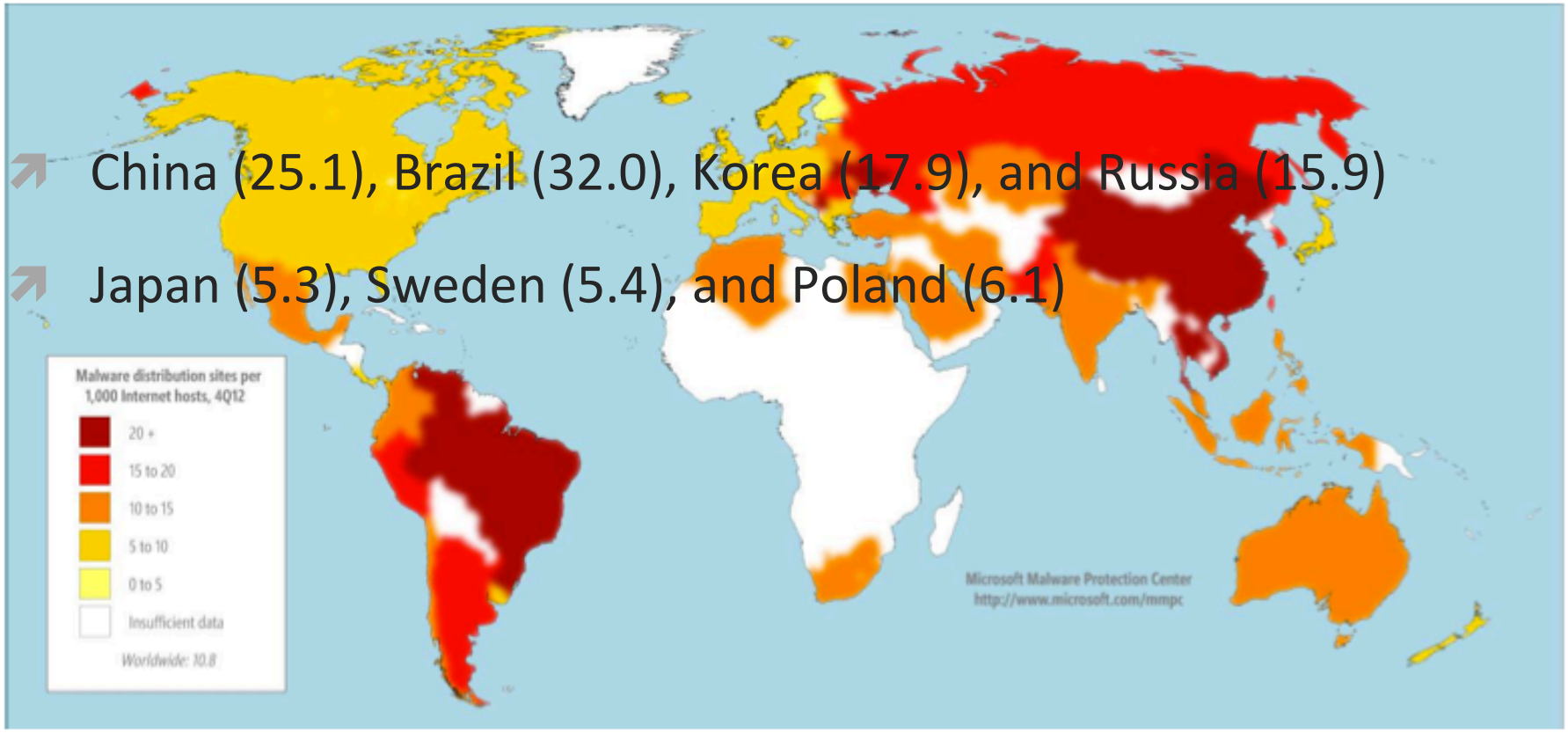


Ransomware


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

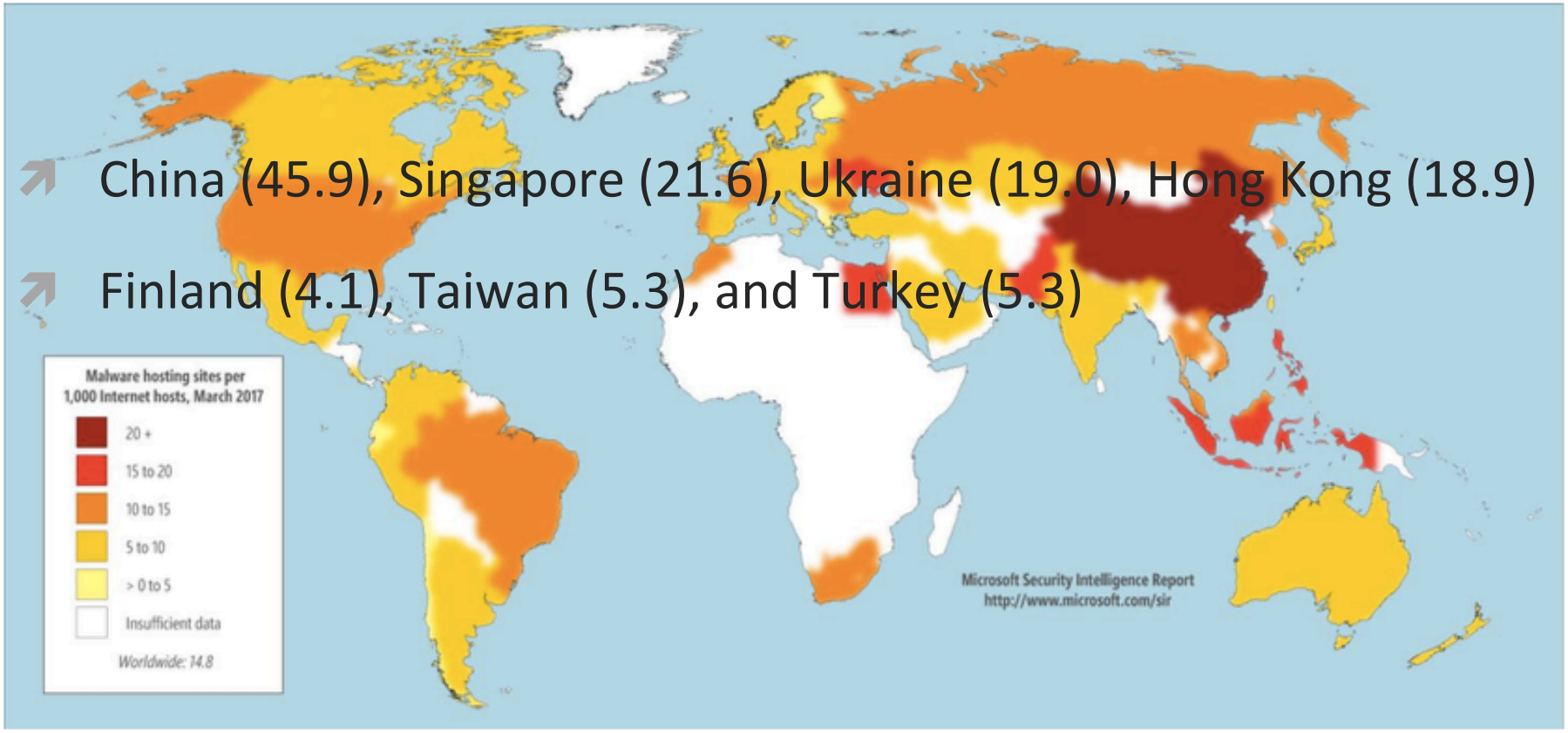
Malware Distribution Sites in ’12

- China (25.1), Brazil (32.0), Korea (17.9), and Russia (15.9)
- Japan (5.3), Sweden (5.4), and Poland (6.1)



Malware Distribution Sites in ’17

- China (45.9), Singapore (21.6), Ukraine (19.0), Hong Kong (18.9)
- Finland (4.1), Taiwan (5.3), and Turkey (5.3)



Drive-by-Download Website

- hosts one or more exploits that target vulnerabilities in web browsers and browser add-ons
- usually hosted on legitimate websites
  - by intrusion / posting malicious code to a poorly secured web form
- Users with vulnerable computers can be infected with malware simply by visiting such a website
- even without attempting to download anything!

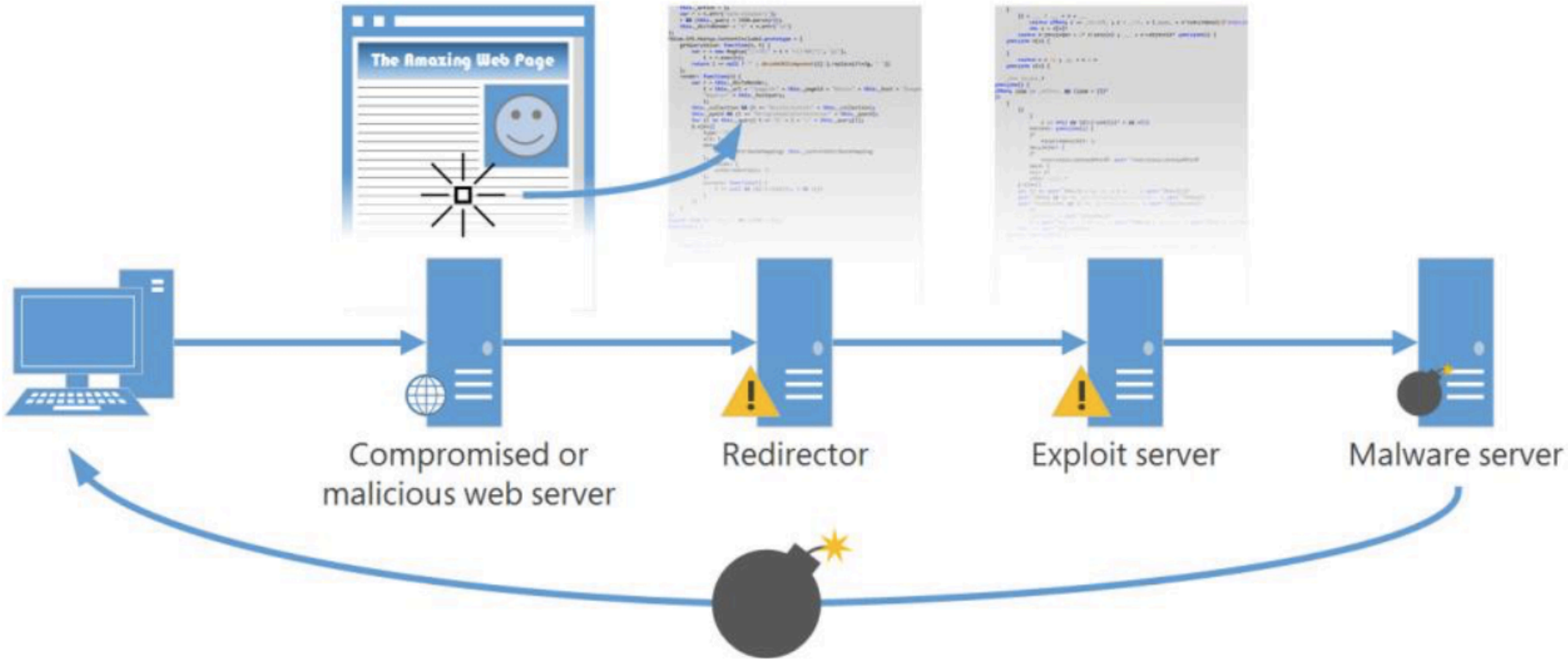
Drive-by-Download Website (Example)

1. User with vulnerable computer visits compromised web page with invisible IFrame

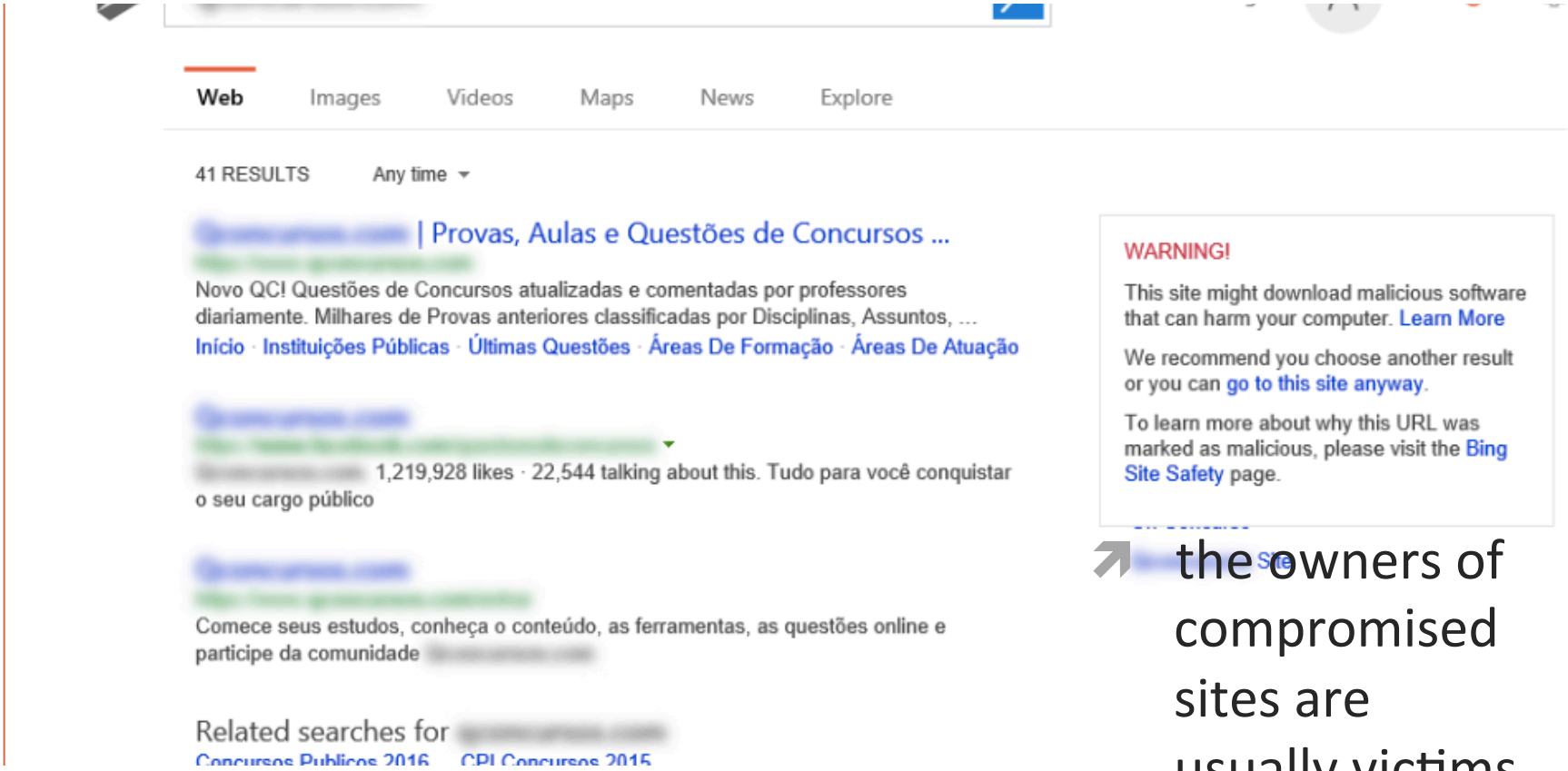
2. IFrame embedded in page secretly loads another page

3. The page redirects to another page containing an exploit

4. If the exploit succeeds, malware downloads from another server to the victim's computer

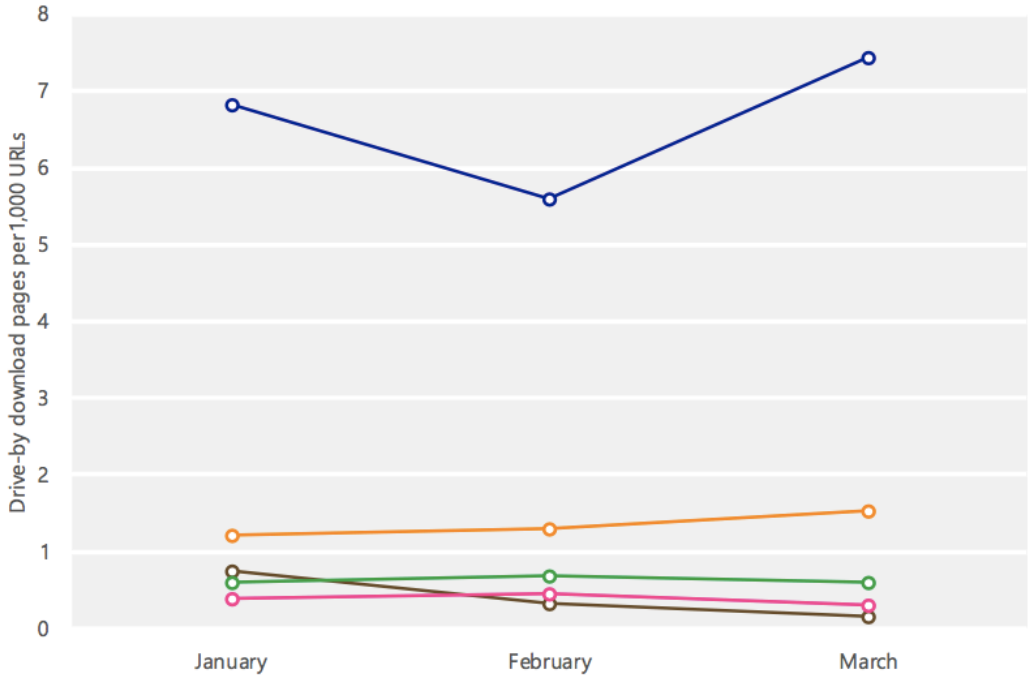


Why just warn but not just remove it?



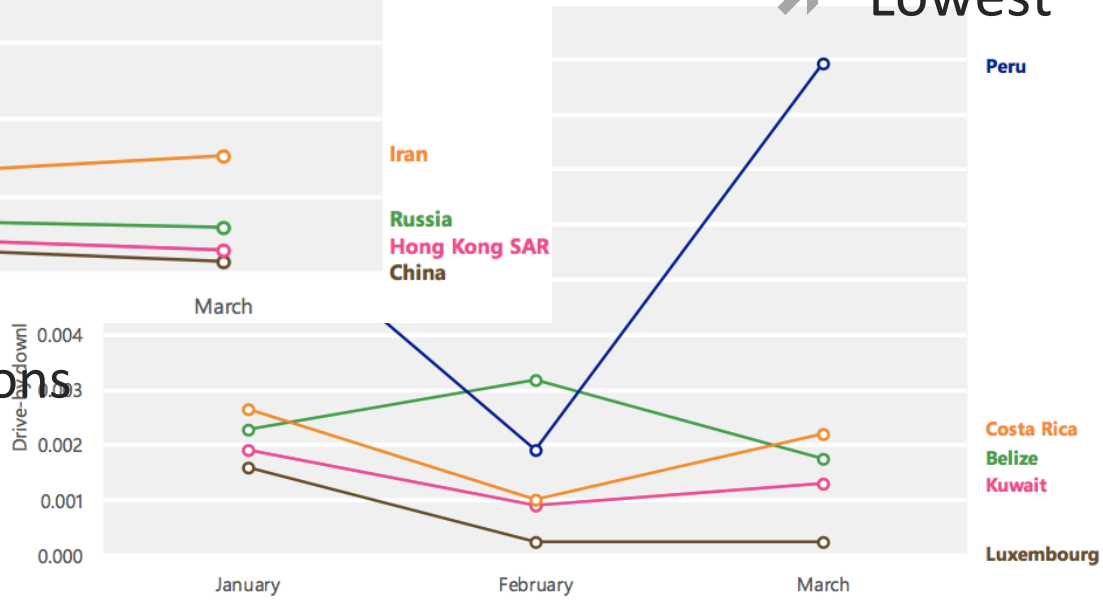
- the owners of compromised sites are usually victims themselves

Concentration of drive-by download pages

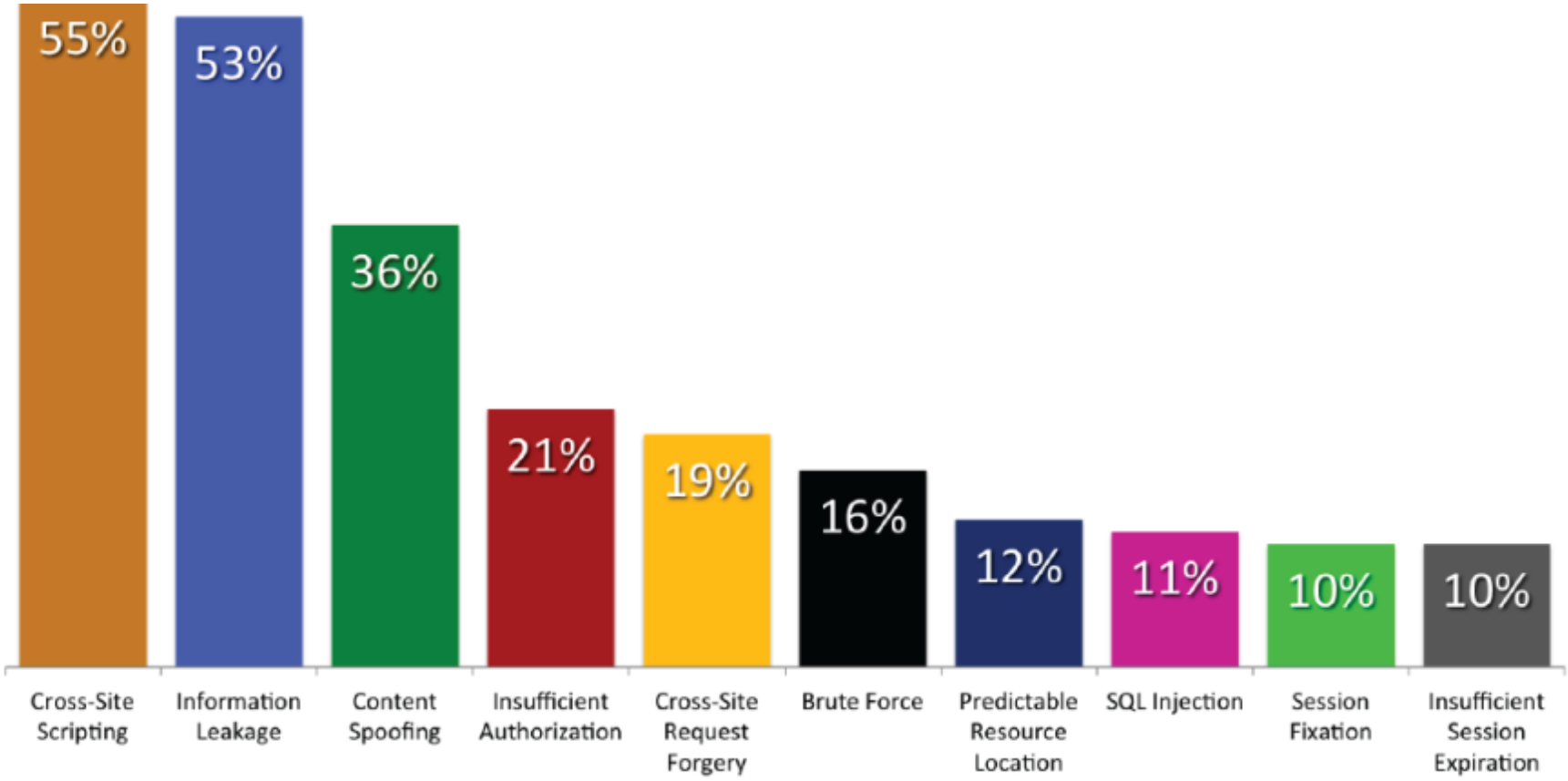


Highest countries/regions

Lowest



Top 10 Vulnerability Classes in ’11



https://www.whitehatsec.com/assets/WPstatsReport_052013.pdf