National Security – Latest Trends in Information Security - Industry View

Robert Kosla, Lt. Col. (Ret.)
Regional Director
Public Safety / National Security / Defense
Microsoft Central and Eastern European Headquarters (CEE HQ)

Bratislava
- 25th October 2011

Questions to be asked…

1) National Security dependancy on Information Assurance?

2) National Cybersecurity/Cyber Defense Capabilities Status?

3) Stay isolated and „potentially secure" but ineffective or manage interconnectivity risks?

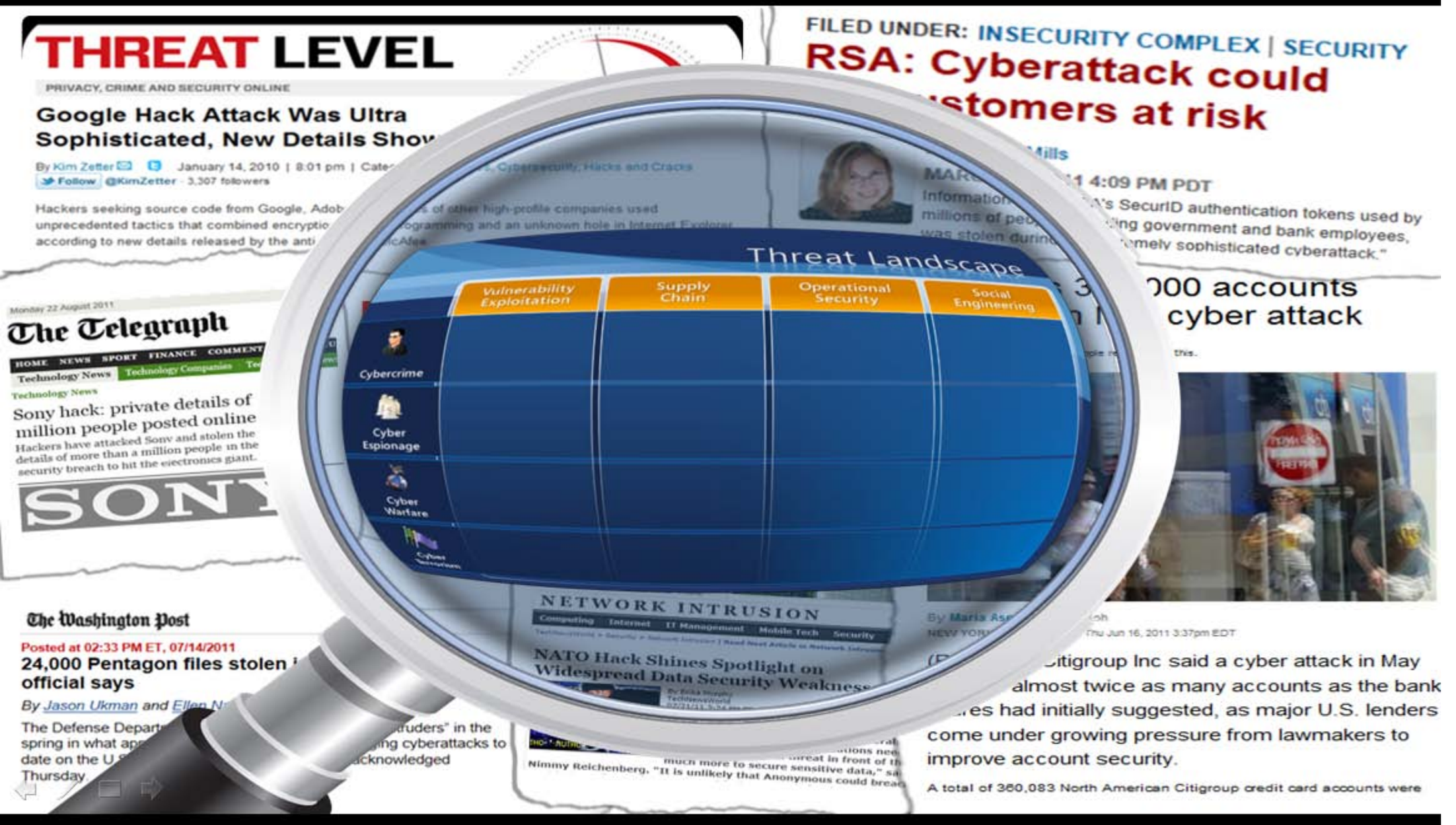
4) New generation of classified network users – Web 2.0 children?

5) National Security vs. Privacy?

6) Role and Position for Industry in National Security efforts?

National Security / Information Assurance / Cybersecurity dependencies and trends…

…but a few tough facts first


THREAT LEVEL
PRIVACY, CRIME AND SECURITY ONLINE
Google Hack Attack Was Ultra Sophisticated, New Details Show
FILED UNDER: INSECURITY COMPLEX | SECURITY
RSA: Cyberattack could
stomers at risk
4:09 PM PDT
Threat Landscape
Vulnerability Exploitation
Supply Chain
Operational Security
Social Engineering
Cybercrime
Cyber Espionage
Cyber Warfare
The Telegraph
Sony hack: private details of million people posted online
SONY
The Washington Post
Posted at 02:33 PM ET, 07/14/2011
24,000 Pentagon files stolen
official says
NETWORK INTRUSION
NATO Hack Shines Spotlight on Widespread Data Security Weakness
000 accounts
cyber attack
Citigroup Inc said a cyber attack in May
almost twice as many accounts as the bank
come under growing pressure from lawmakers to
improve account security.
A total of 360,083 North American Citigroup credit card accounts were

One of many 2011 news – „French government network hacked"

"… In total, hackers took control of 150 computers during many weeks, from secretary computers to the ones of the highest authority…"

"… it was not the ministry IT service who detected the attack, but ministry employees who noticed that people had received emails from their address whereas they had not sent anything…"

"… ANSSI can only count on 30 engineers to perform its mission, while some other states have armies of hackers…"

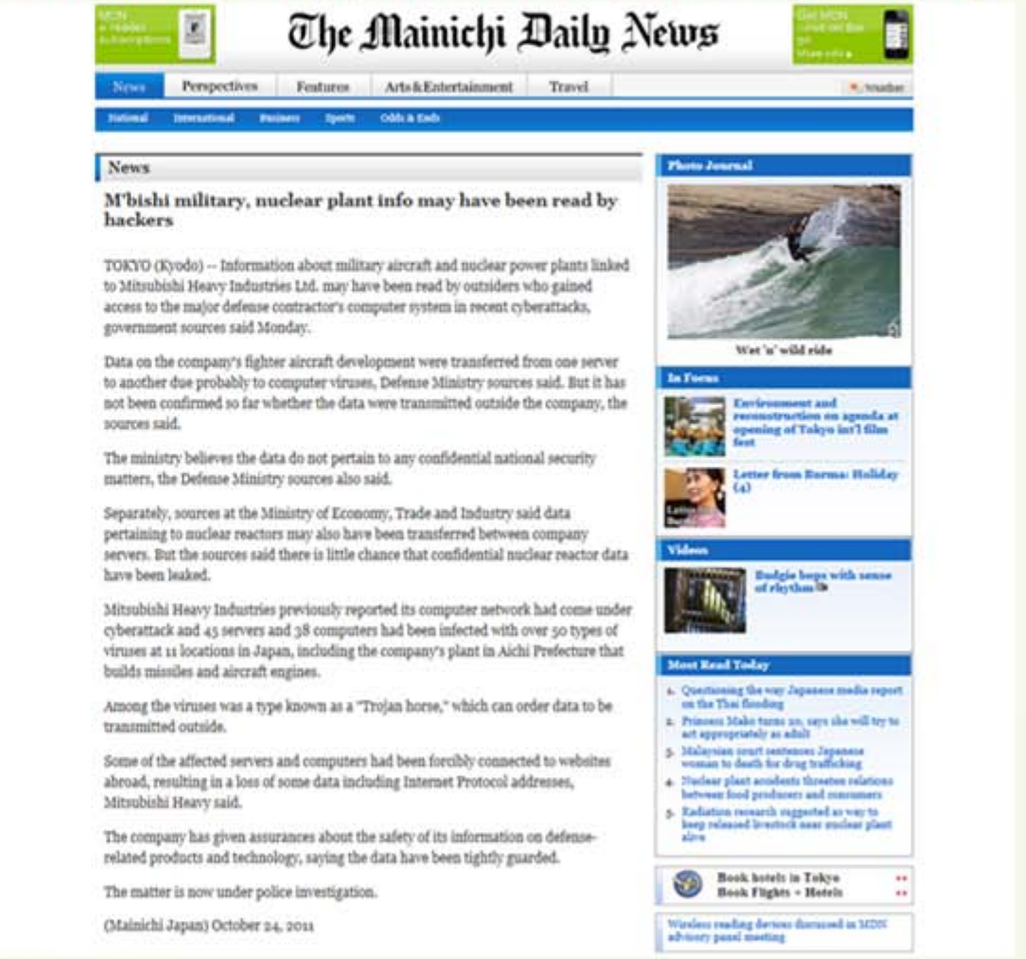
"… A highly ranked source at the ministry of interior revealed that intruders have precisely targeted organizers of the G20 [that is to happen later this year in France] … "

"… The attack is not so incredible given that this already happened 2 months ago in Canada … " said budget minister Christine Lagarde.

Articles mention that data was exfiltrated and outbound network traffic could be traced back to a bounce in China but this "did not constitute a proof of the true origin of the attack"

http://www.lexpansion.com/high-tech/les-dessous-du-cyber-espionnage-de-bercy_250142.html?p=2
http://www.liberation.fr/economie/01012324191-attaque-informatique-l-elysee-et-le-quai-d-orsay-egalement-pirates
http://www.lepoint.fr/high-tech-internet/la-cyber-attaque-contre-la-france-etait-de-l-espionnage-pur-selon-l-anssi-07-03-2011-1303652_47.php

Hot new from this week – „M'bishi military, nuclear plant info may have been read by hackers



The Mainichi Daily News

News | Perspectives | Features | Arts & Entertainment | Travel

National | International | Business | Sports | Odds & Ends

News

M'bishi military, nuclear plant info may have been read by hackers

TOKYO (Kyodo) -- Information about military aircraft and nuclear power plants linked to Mitsubishi Heavy Industries Ltd. may have been read by outsiders who gained access to the major defense contractor's computer system in recent cyberattacks, government sources said Monday.

Data on the company's fighter aircraft development were transferred from one server to another due probably to computer viruses, Defense Ministry sources said. But it has not been confirmed so far whether the data were transmitted outside the company, the sources said.

The ministry believes the data do not pertain to any confidential national security matters, the Defense Ministry sources also said.

Separately, sources at the Ministry of Economy, Trade and Industry said data pertaining to nuclear reactors may also have been transferred between company servers. But the sources said there is little chance that confidential nuclear reactor data have been leaked.

Mitsubishi Heavy Industries previously reported its computer network had come under cyberattack and 45 servers and 38 computers had been infected with over 50 types of viruses at 11 locations in Japan, including the company's plant in Aichi Prefecture that builds missiles and aircraft engines.

Among the viruses was a type known as a "Trojan horse," which can order data to be transmitted outside.

Some of the affected servers and computers had been forcibly connected to websites abroad, resulting in a loss of some data including Internet Protocol addresses, Mitsubishi Heavy said.

The company has given assurances about the safety of its information on defense-related products and technology, saying the data have been tightly guarded.

The matter is now under police investigation.

(Mainichi Japan) October 24, 2011

Photo Journal

Wet 'n' wild ride

In Focus

Environment and reconstruction on agenda at opening of Tokyo int'l film fest

Letter from Burma: Holiday (4)

Videos

Budgie boogs with sense of rhythm

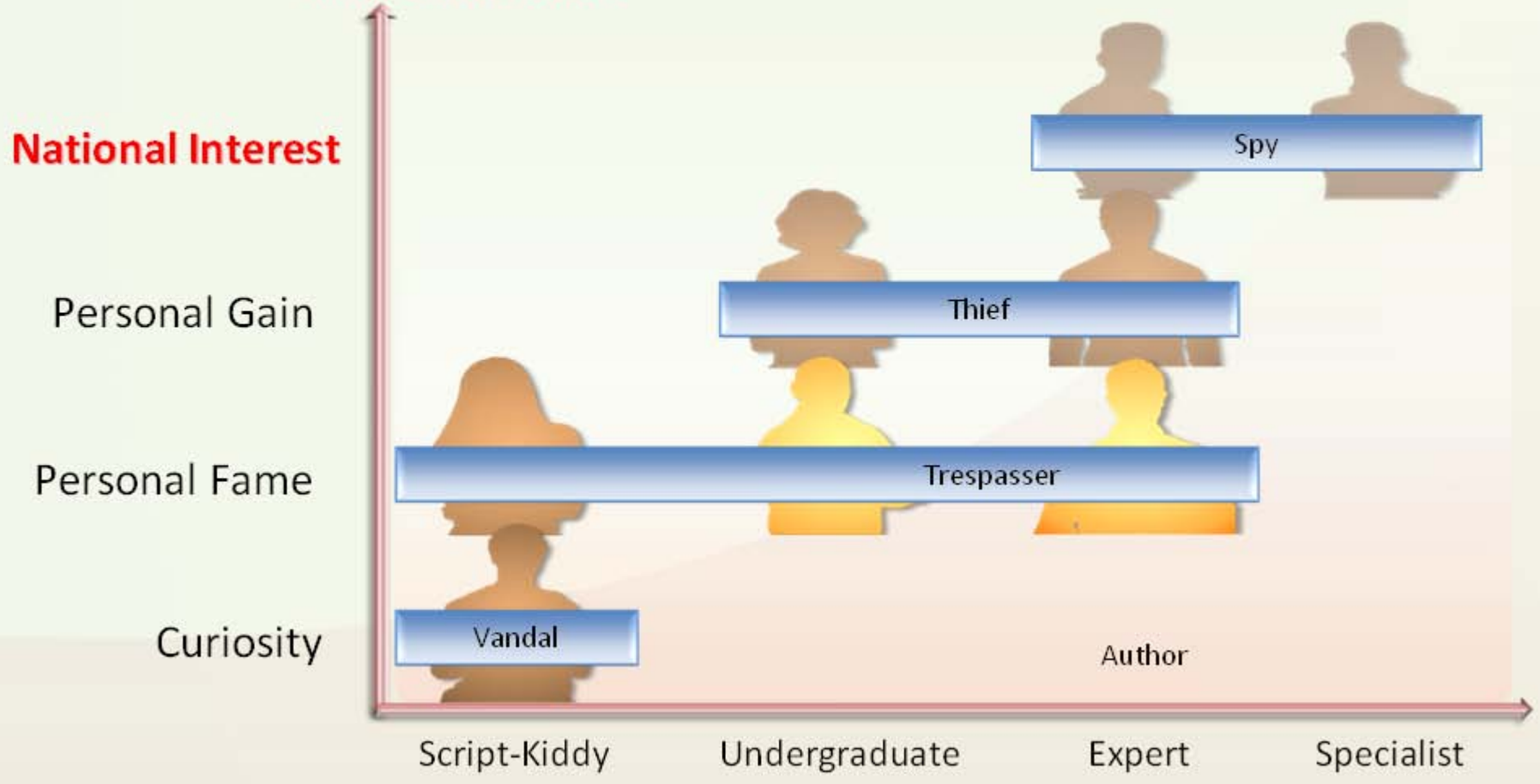
Most Read Today

1. Questioning the way Japanese media report on the Thai flooding
2. Princess Mako turns 20, says she will try to act appropriately as adult
3. Malaysian court sentences Japanese woman to death for drug trafficking
4. Nuclear plant accidents threaten relations between food producers and consumers
5. Radiation research suggested as way to keep released livestock near nuclear plant alive

Book hotels in Tokyo
Book Flights + Hotels

Wireless reading devices discussed in MDN advisory panel meeting

Evolving Information Assurance Threat – who is intersted?



National Information Assurance/Cybersecurity Threat Challenges

National Cyber Threat Landscape

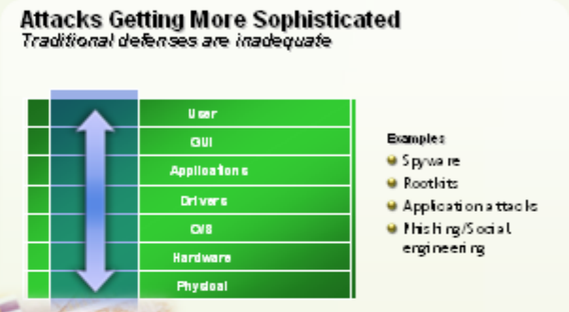
- Many actors/Many Motives
- Similar Tools and Techniques
- A Shared and Integrated Domain
- Accelerated Speed of Attack
- Uncertain Consequences

National Policy Challenges

- National Dependence on ICT
- Applying Elements of National Power to Cyber
- Establishing Norms of Behavior
- Harmonization of Legal Regimes
- Cyber Deterrence

Organizational Challenges

- Keeping pace with dynamic and sophisticated cyber adversaries.
- Challenges in applying a strategic, risk-based approach to cybersecurity.
- Limited budgets, expertise and too many competing priorities.
- Difficulty in mapping industry tools and solutions to solve real cybersecurity problems



Historical Evoluion of Threat Landscape

1986–1995

- Local area networks
- First PC virus
- Boot sector viruses
- Create notoriety or cause havoc
- Slow propagation
- 16-bit DOS

1995–2000

- Internet era
- Macro viruses
- Script viruses
- Create notoriety or cause havoc
- Faster propagation
- 32-bit Windows®

2000–2005

- Broadband prevalent
- Spyware, spam
- Phishing
- Botnets
- Rootkits
- Financial motivation
- Internet-wide impact
- 32-bit Windows

2006-2011

- Hyperjacking
- Peer-to-peer
- Social engineering
- Application attacks
- Financial motivation
- Targeted attacks
- OSS attacks
- Apple OS/iOS
- 64-bit Windows
- Android mobile platform

Anarchists Find Attack Dog in Hackers

- Hackers
  - 4Chan.org
  - Anonymous
  - AnonOps.US
  - LulzSec
  - #AntiSec
- Anarchists
  - Peoples Liberation Front
  - Telecomix

Anonymous / LulzSec

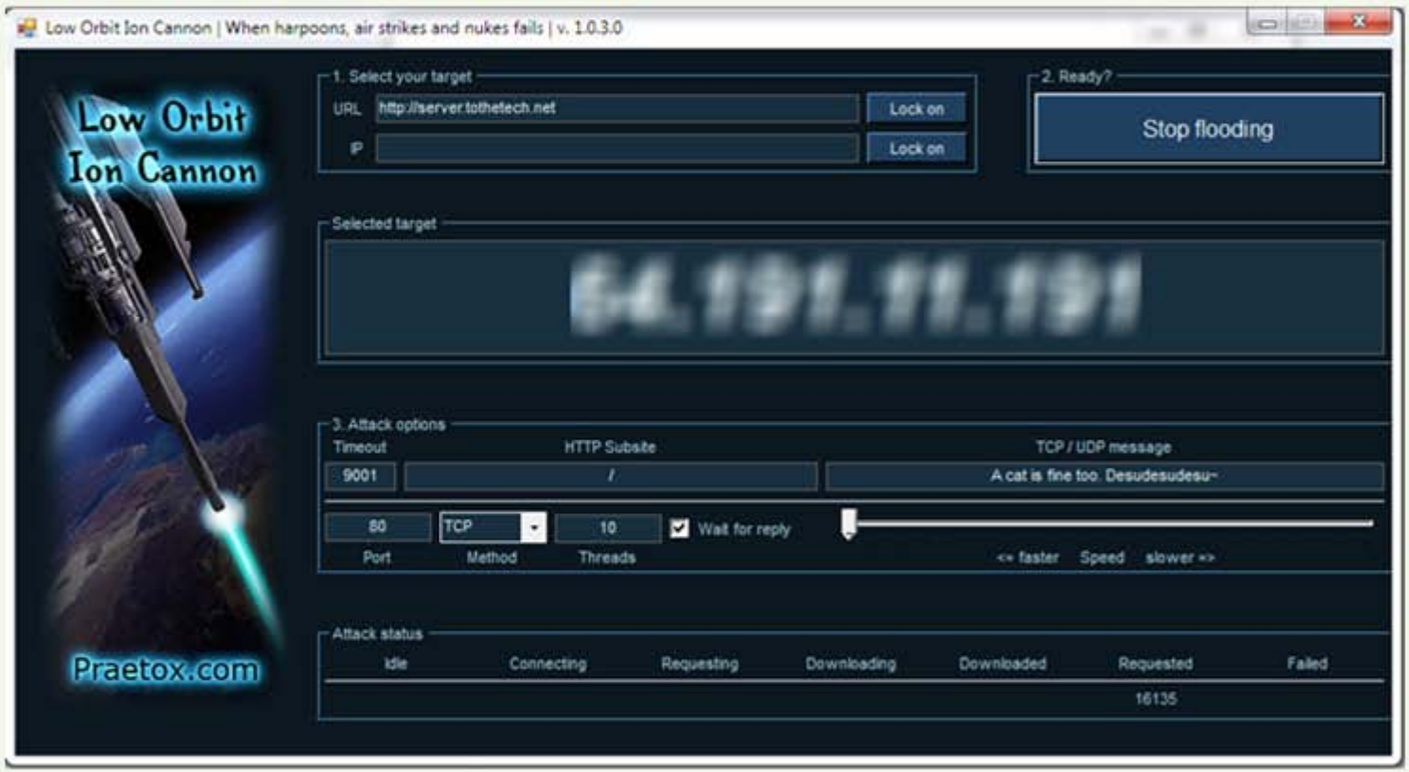
- 2008 – Church of Scientology
- 2010 – Operation Payback
  - Losing members/momentum, decides to co-op Wikileaks for moral support.
  - Initial DDoS attacks on Mastercard/PayPal
- 2011 – LulzSec
- 2011 June - #AntiSec

Low Orbit Ion Canon - LOIC

- LOIC is a volunteer botnet that supporters and members can download
  - Includes conf file that allows 'Anonymous' to direct attacks at actors they wish to target
  - Microsoft Malware Protection Center (MMPC) identifies LOIC as HackTool:Win32/Oylecann.A

- Microsoft has identified over 40,000 reports of LOIC, of which half opted to quarantine or remove the threat
  - This potentially leaves roughly 20,000 active instances of LOIC – enough to generate a >18 Gbps DDoS

Low Orbit Ion Canon - LOIC



- Very primitive – moderate to low skill level needed
- Not Proxy Aware!

Anonymous/Lulz TTP's for System Compromise

- Initial Attack Vectors
  - SQL Injection
  - XSS (Cross-Site-Scripting)
  - Directory Traversal
  - Social Engineering
- Operations
  - Password Reuse
  - Hash Cracker
  - tcp2dns

"The Criminal Cloud"

- Over 300,000 Zombies are activated each day within ISP networks
  - contributing to new malicious activity (SPAM, malware distribution, financial/IP data theft and DoS attacks)

- The rise of easy-to-configure cloud services
  - Botnets can be rented, essentially providing would-be attackers a "criminal" cloud where services can be leased
  - Scaling an attack up is as easy as deploying a new virtual server
  - Very difficult to categorize and therefore respond to the threat
  - All very cheap

Future Cyber Exploitation Trends

64-Bit	• **Most shellcode and exploits today are 32-bit** • **50% of Win7 installed base is 64-bit…**
Isolation Architectures	• Compartmentalization, Isolation, Sandboxing targeted • Driven by content viewer apps and mobile devices
Platform Mitigations	• Targeting and arms race against key features • DEP, ASLR, SEHOP, EMET, etc. make exploits unreliable
Smart Devices	• Connectivity as a target • Full OS feature sets (i.e. Authentication)
Web Modernization	• Beyond Web 2.0 driven by browser advancements • HTML5, JIT'd apps, HW acceleration, etc.
The Cloud	• Utility-scale apps, users and data as targets • Utility-scale cybercrime capabilities w/o capital investment
Cyber "Broken Arrow"	• Loose cyber weapons that drive exploitation advancements • Aurora and Stuxnet as case studies
Cyber Policy	• Disclosure policy exploitation and pressures • Weaknesses in Global policy harmonization

National Security from Industry Perspective … Microsoft on the Front Line…

… great references for National Security Authorities

Microsoft Trustworthy Computing - TwC

- A long time ago (maybe not so long) … we were losing…
- Bill Gate's Trustworthy Computing initiative
  - Change how we write code
  - Change how we defend ourselves
  - Change how we defend our customers
- Understand our adversary
  - Develop an in-house intelligence capability
  - Understand tools and techniques
  - Neutralize and disrupt

Microsoft… on the Front Line

Our Products

- 80% of world's critical infrastructures
- Determined, resourceful, global adversaries

Our Business

- Subject to Phishing, Bots, Root-kits, …

Our Resources

- Attacked > 40,000 times a day
- At least one DDoS a day
- Logged attacks from every country

Microsoft IT Environment

- 90,000 employees
- 600,000 networked devices
- 25,000 data-center servers

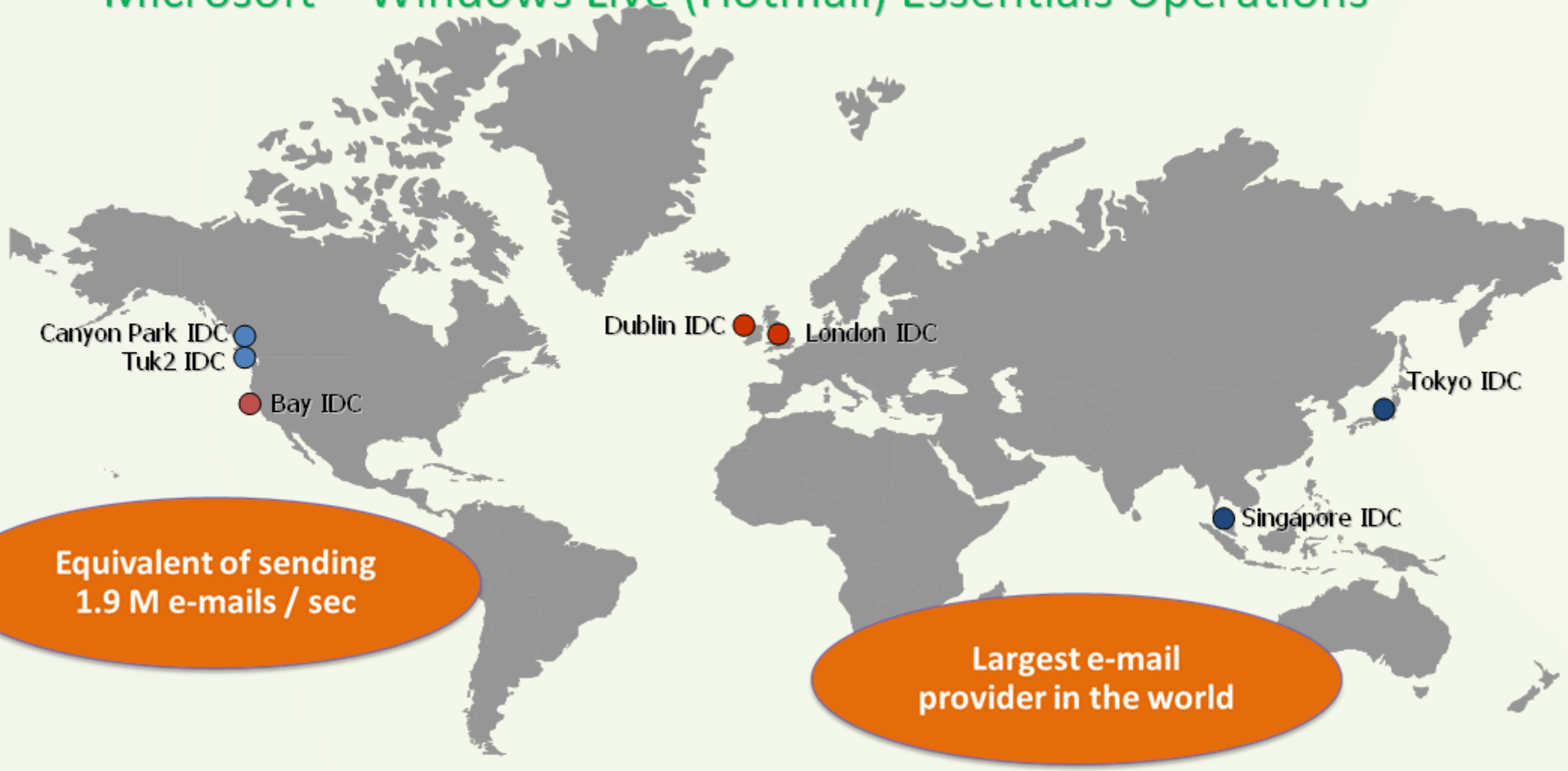
- 180,000 mailboxes

- 260 Exchange servers
- 15-20M e-mail messages per day
- 5M filtered e-
  /day (spam

You must leverage your IT network for intelligence

- 450 primary LOB applications
- 33 million IM's calls per month

Microsoft – Windows Live (Hotmail) Essentials Operations



Equivalent of sending 1.9 M e-mails / sec

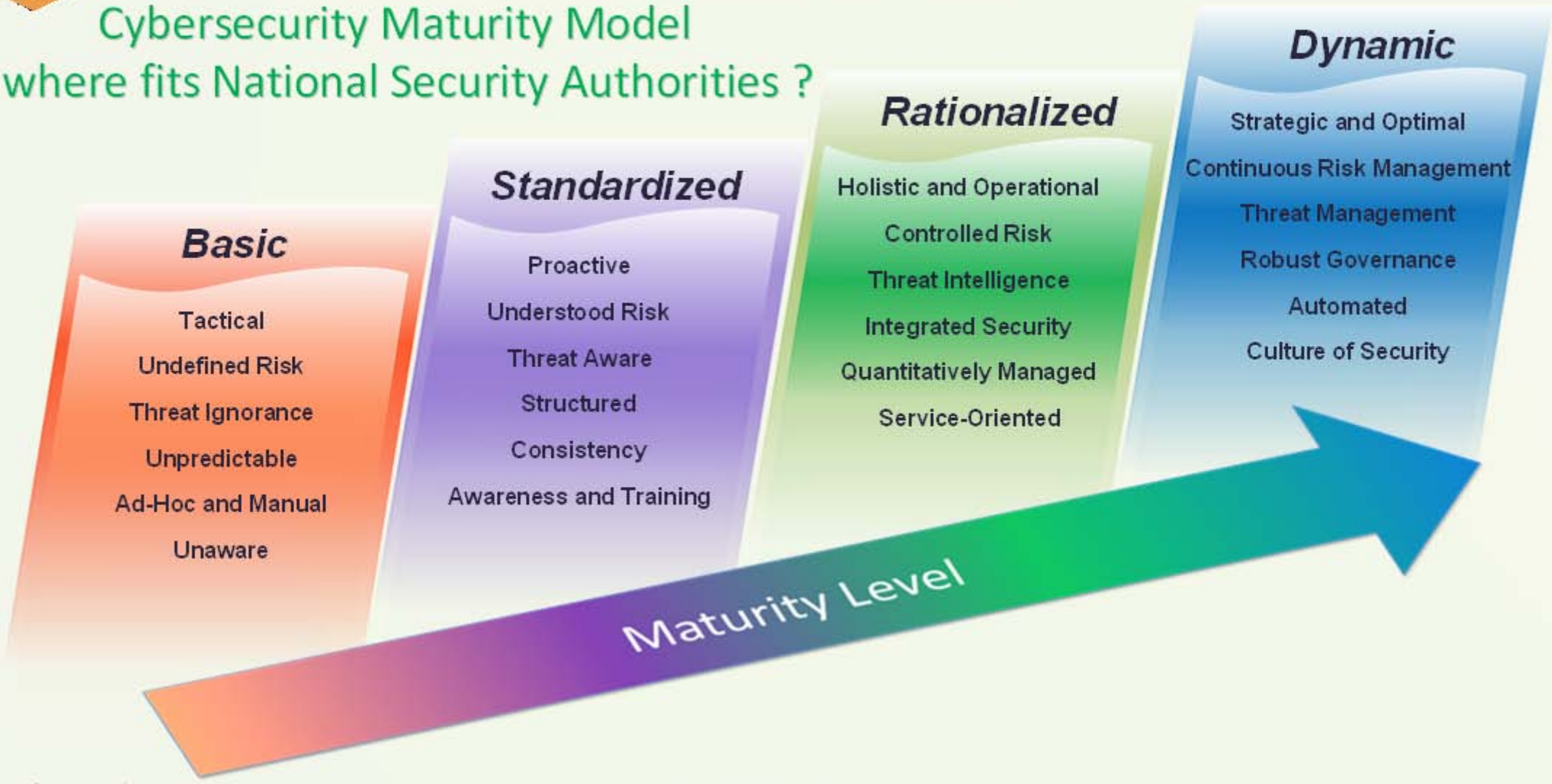
Largest e-mail provider in the world

Microsoft Bing Search Design Scale

- 5 billion documents indexed
  - 10 TB index size (20GB/ISN machine)
  - 25 TB stored cont
  - 200 bil
- 2
  - peaks
  - < 150ms, 95th percentile < 200ms
  - documents indexed/sec
  - Re-crawl entire index in less than 21 days
  - Important frequently changing data refreshed daily
  - Higher crawl rate to improve freshness
- 5000+ machines
  - Scale to handle large number of machines
  - Minimize operation personnel (15 per shift)

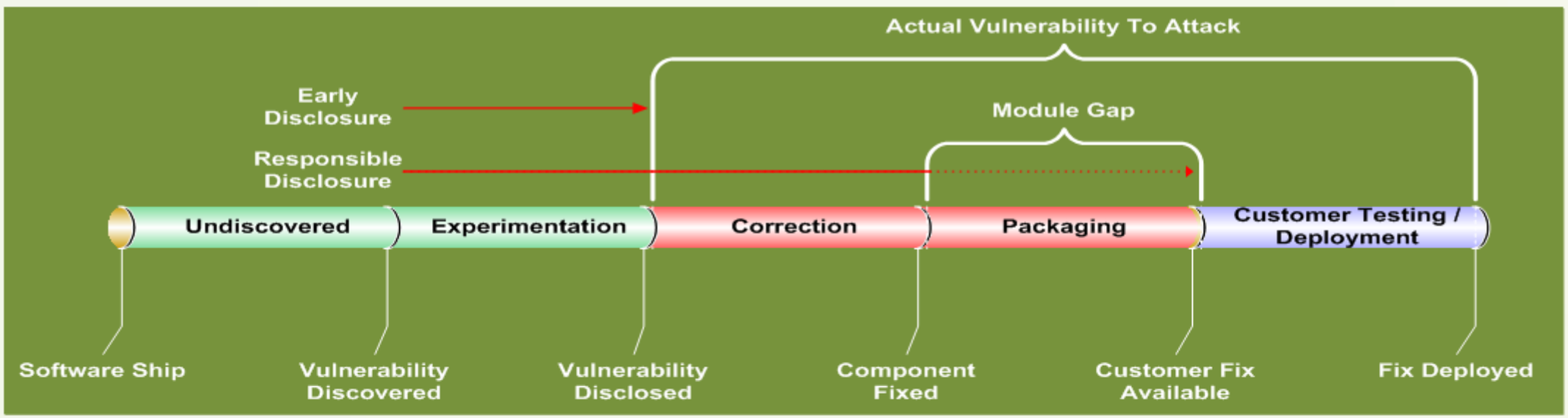
We leverage our search engine for intelligence

Cybersecurity Maturity Model
- where fits National Security Authorities ?

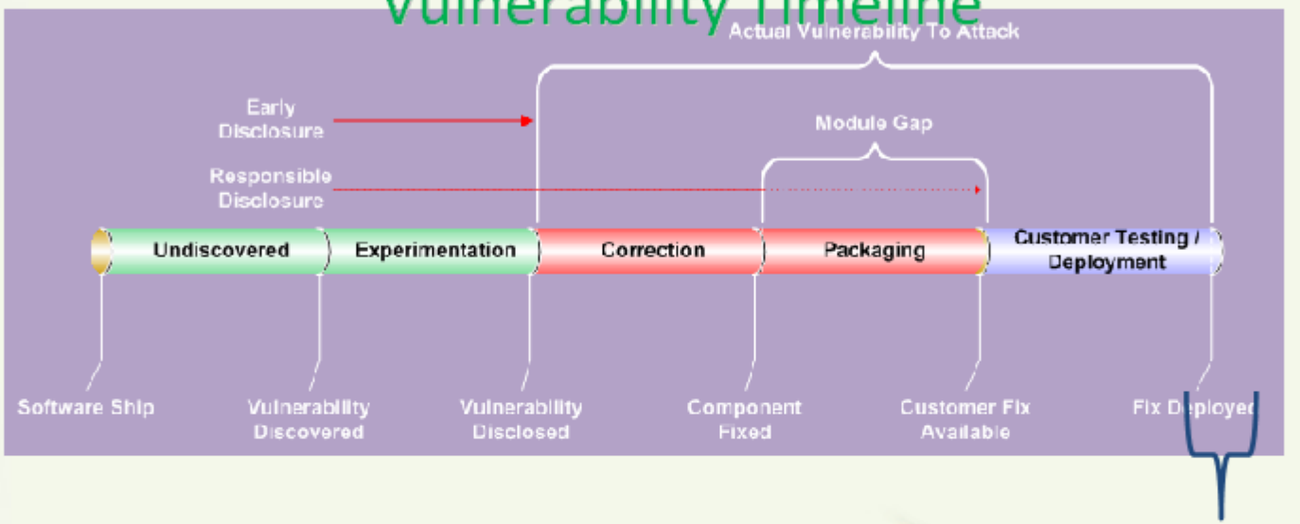


Vulnerabilities, Forensics and Patching
… how much time we have to perform the action

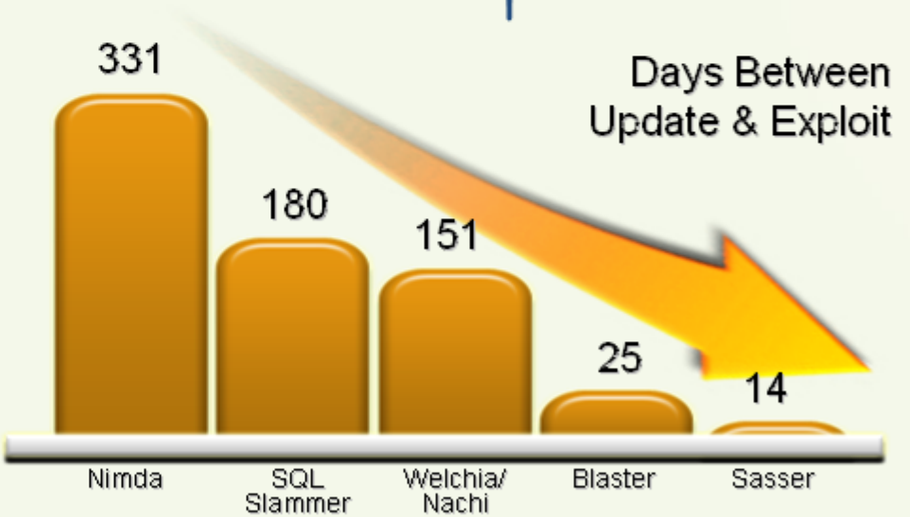
Vulnerability Timeline



Vulnerability Timeline



- Days From Patch To Exploit
  - Have decreased so that patching is not a defense in large organizations
  - Average 6 days for patch to be reverse engineered to identify vulnerability

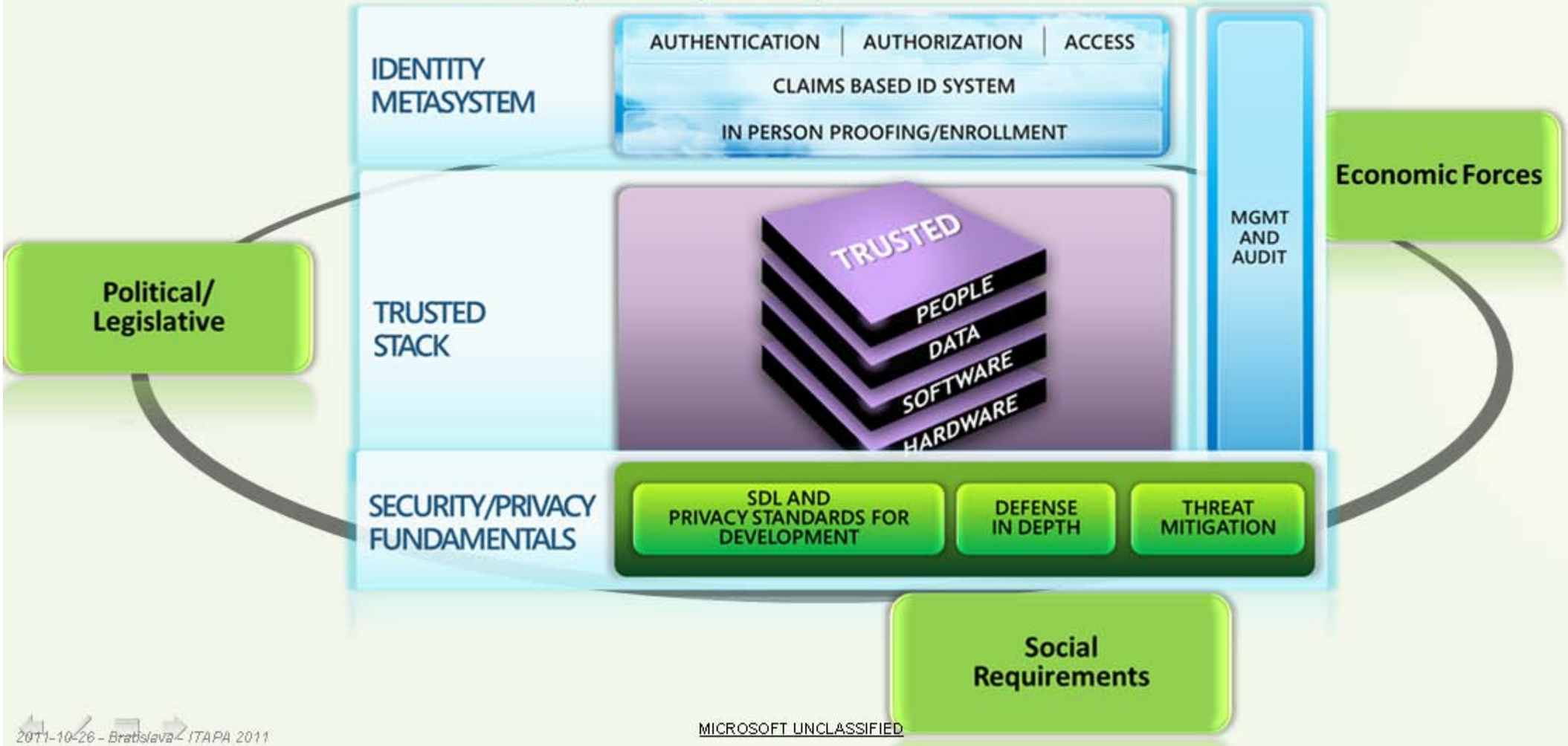


Source: Microsoft

Hardware threat to National Secuirty - Counterfeit Products

Multi-Level National Security Support

Security Complexity – Microsoft View



Microsoft – Privacy and National Security Progress

SDL and SD3

- Security Development Lifecycle process
  - Engineered for security
  - Design threat modeling
- SD3:
  - Secure by Design
  - Secure by Default
  - Secure In Deployment
- Automated patching and update services

Defense in Depth

- Windows Firewalls
- Protected Mode Web browsing
- Windows Server only installs what it needs, reduces attack surface
- Non-administrator users (UAC)
- Server & Domain Isolation (SDI)
- Advanced Memory Management (ASLR)
- Encrypted disk & file systems

Identity & Access

- User controllable, authenticated identity
- Authenticated, authorized groups & individuals
- Policy-enforced access control to resources & data
- Federated personal & corporate identities

Threat Mitigation

- Microsoft Security Response Center (MSRC)
- Microsoft Malware Protection Center (MMPC)
- Windows Live OneCare and Forefront Client Security, powered by the Microsoft Malware Protection Center
- Malicious Software Removal Tool (MSRT)
- (Network Access Protection (NAP/NAC)

Microsoft National Security Partnerships

- Microsoft is committed to continued close partnership with Government and Industry
- Driving ecosystem change
  - **President's National Security Telecommunications Advisory Committee** (NSTAC)
  - **Center for Strategic and International Studies (CSIS)** commission report
  - Defense Science Board Globalization and Security Task Force
  - IT-Sector Coordinating Council
- Managing risk
  - **SAFECode** partnership to enhance supply chain integrity and secure software development
  - The **Transglobal Secure Collaboration Program (TSCP)**
- Enhancing operational coordination
  - **US-CERT, JTF-GNO**
  - Founding member of the IT-Information Sharing and Analysis Center (IT-ISAC)
  - **Cyber Storm I, II and III** large-scale national cyber exercise participation
  - Founding member of the **Industry Consortium for the Advancement of Security on the Internet** (ICASI)
  - Member of the **FBI's InfraGard**

Lost National Security Data

Oops…

Man 'finds US troop data' on MP3

A New Zealand man says he found confidential data about US military personnel on an MP3 player he bought from a thrift shop in Oklahoma.

Chris Ogle, 29, said: "The more I look at it, the more I see and the less I think I should be looking."

The files included names and telephone numbers of American soldiers, according to reports by TV New Zealand …

MoD admits inquiry into 69 lost laptops

The Ministry of Defence is investigating the reported loss of 69 laptops and seven personal computers over the past year, officials revealed yesterday, as Whitehall staff were banned from removing laptops containing sensitive data from their offices. The extent of the lack of security surrounding MoD computers containing un-encrypted information emerged as Des Browne, the defence secretary, announced an inquiry into the latest theft: a laptop

Solutions available today and approved for National Security Support – Bitlocker and Bitlocker To Go

Need a solution which

- Sits underneath Windows
- Has keys available at boot
  - Cannot require user login in order to run
- Secures System Data
- Secures User Data
- Secures Registry
- Works seamlessly with platform (e.g. Code Integrity)
- Secures root secrets
- Protects against offline attacks
- Is super-easy to use

Solution

- Encrypt (nearly) the entire disk
- Protect the encryption key by "sealing" with a Trusted Platform Module (TPM) to the authorized loader
  - Plus other options
- Only authorized (MS) loaders get volume encryption key
- Authorized loaders boot the OS properly

Windows Secure and Optimized Desktop

Windows 7 Enterprise | Microsoft Desktop Optimization Pack for Software Assurance

Anywhere Access for Users

- UI and Navigation
- Federated Search
- Mobile Broadband
- DirectAccess
- BranchCache
- App-V & Med-V

Security and Data Protection

- Defense in depth with Secure Platform
- BitLocker/BitLocker To Go
- AppLocker
- IE 8 Security

End-To-End Management

- PowerShell and Automation
- Group Policy Advancements
- Deployment Tools
- VDI Enhancements

Continuity Management

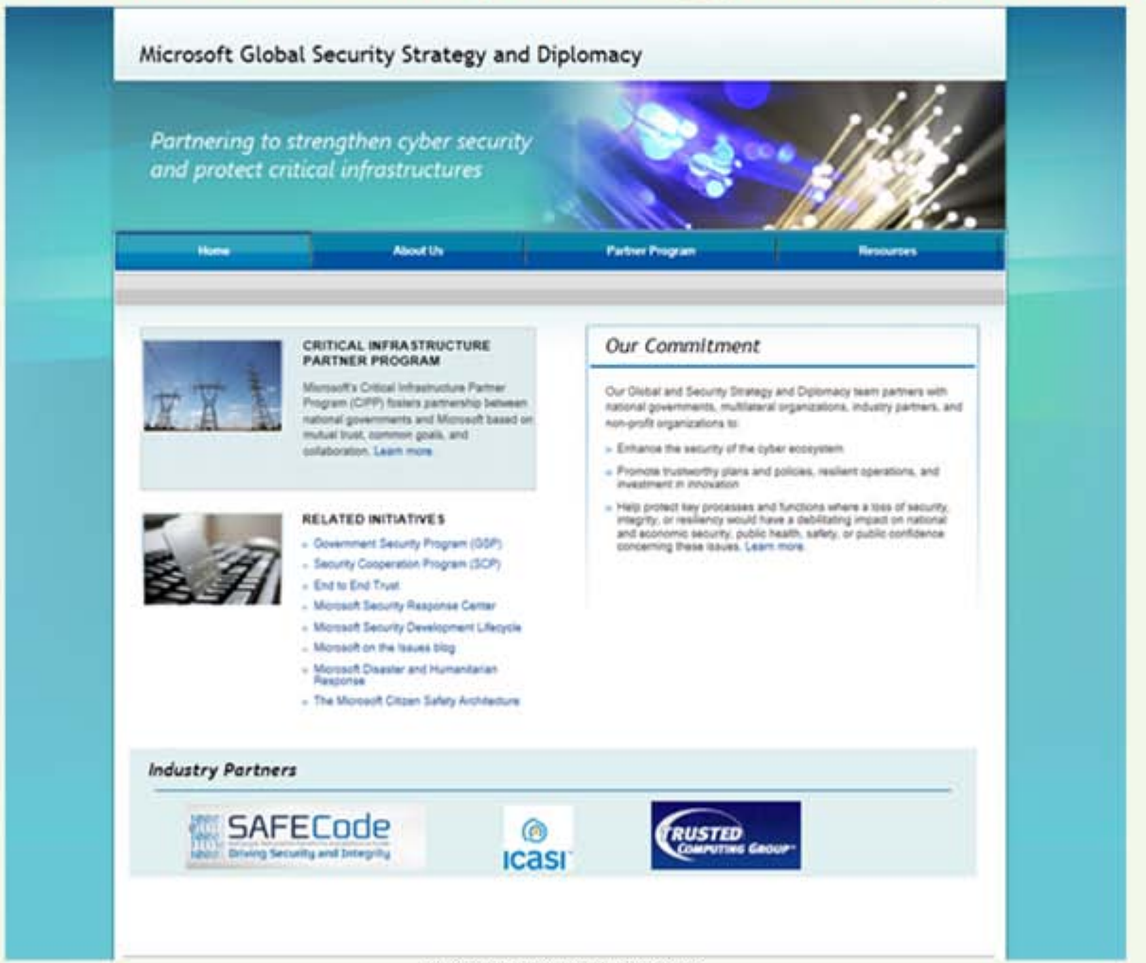
- Troubleshooting Packs
- Problem Steps Recorder
- Desktop Error Monitoring
- Diagnostic and Recovery Toolset

Fundamentals

Performance | Reliability | Compatibility – available now in OS

Microsoft Global Security & Government Programs

Microsoft Global Security Strategy and Diplomacy Portal



Microsoft Government Security Program GSP

What is the Government Security Program (GSP) global initiative?

- GSP provides access to:
  - Source code
  - Technical information
  - Development personnel
  - Security tools and source code training

- GSP enhances governments' ability to:
  - Evaluate and protect existing systems
  - Design, build, deploy, and maintain secure computing infrastructures

Microsoft Security Cooperation Program
SCP

Overview

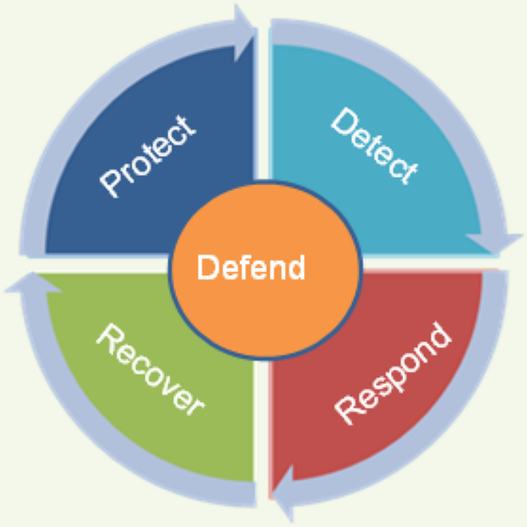
- A worldwide program providing a structured way for governments and governmental organizations responsible for computer incident response, protection of critical infrastructure, and computing safety to *collaborate with Microsoft in the area of IT security*
- Includes incident response, information exchange, and public outreach components

Benefits

- Public/private partnership in incident response and information exchange can help decrease risk to national security, economic strength, and social welfare from attacks on the country's IT infrastructure.
- Microsoft provides a 24/7 hotline for SCP participants, and works with participants to define a process for disseminating information in the event of a critical incident or emergency.

Microsoft Government Cybersecurity Services in Support of National Security

Protect
- System Configuration and Optimization
- Security and Availability Virtualization Solutions
- Network Access Protection and Health Solutions
- Network Isolation Solutions
- Secure and Seamless Remote Access Solutions
- Active Directory Design and Hardening
- Identity Lifecycle Management Solutions
- Secure Public Key Infrastructure Solutions
- Application Server Protection Solutions
- Data Protection and Access Solutions
- Secure Development Lifecycle Solutions



Detect
- Enterprise Configuration Management Solutions
- Enterprise End-to-End Monitoring Solutions
- Mobile Device Management Solutions
- Advanced Server Virtualization Solutions
- Client and Server Anti-Malware Solutions
- Audit Collection Services
- Advanced Intrusion Detection Services
- Automated Vulnerability Assessment Services
- Systems Error Reporting and Analysis Services

Recover
- Enterprise Recovery Services
- Offline System Recovery
- Enterprise Security Education Services
- Forensics Investigations Education Services

Respond
- Windows Online Forensic Services
- Enterprise Incident Response Services
- Critical Asset Analysis and Investigations Services
- Security Response Training Services

Microsoft Digital Crimes Unit - DCU

- A worldwide team of lawyers, investigators, technical analysts and other specialists whose mission it is to make the Internet safer for everyone through game-changing legal solutions, enforcement, partnerships, cooperation and technology that:
  - Defend against digital crime and abuse
  - Protect children from technology-facilitated crimes
  - Advance safety and integrity in the online advertising marketplace
  - Ensure security and safety in cloud computing and emerging technologies

MICROSOFT DIGITAL CRIMES UNIT

Microsoft Digital Crimes Unit – DCU
- botnets down: Waledac, Coreflood, Rustock… more comes

MICROSOFT DIGITAL CRIMES UNIT

Microsoft

Microsoft Malware Prc
Threat Research & Response Blog

Home About Help

What we know (and learned) from the Waledac

Recently, following an investigation to which various members of the MMPC contrib takedown of the Waledac botnet in an action known as Operation b49, an ongoing takedown also marked a new phase of exploration in combating botnets, which we for Security). While it is still too early to know the entire scope of this particular tak has been delivering on the disruption of Waledac and helping to map new territory what we know and what we are still learning regarding the impact of that fight.

To effectively counter a botnet like Waledac, we knew a multi-layered approach wa communication disruption through technical countermeasures, domain-level takedo between zombie PCs and the command and control servers for Waledac, and tradit command and control mechanisms most directly under the control of the bot maste

With the caveats that there are rarely, if ever, any absolutes regarding botnets and impact of this action, early data from Microsoft and other researchers indicate that within the Waledac bot network. For example, researchers from the Shadowserver University of Mannheim, University of Bonn and University of Washington have ana an effective cessation of commands to Waledac 'zombies.' That's good news becau between 70,000 and 90,000 computers from this botnet, meaning that those custo ups, malware downloads, outgoing spam and ID and password theft associated wit

We've also been tracking Operation b49's impact on the symptoms of Waledac infe identity theft and spam attacks from infected computers to other victims. Research have data showing a dramatic decline in new IP addresses appearing within the Wi spreading its infection to other computers. While there will likely always be some fi and we must and will continue to work with the security community to stay on top reported by Sudosecure as of February 27 is a great indicator of the success of the

Microsoft on the Issues
News and perspectives on legal, public policy and citizenship topics

Home Innovation Marketplace Community

- Tue, 25 Oct 2011 — Initiative 1125 is the Wrong Vision for our Transportation Future
- Sun, 23 Oct 2011 — Microsoft's New Patent Agreement with Compal: A New Milestone for Our Android Licensing Program
- Fri, 14 Oct 2011 — Digital Crimes Consortium 2011: Turning the Tables against Cybercrime
- Thu, 13 Oct 2011 — Microsoft Voices Support for Passage of Free Trade Agreements with South Korea, Colombia & Panama

FBI and DOJ take on the Coreflood botnet

13 Apr 2011 6:12 PM | 0

SUBSCRIBE
Blog Home
Email Blog Author

Posted by Richard Boscovich
Senior Attorney, Microsoft Digital Crimes Unit

Today, the FBI and U.S. Department of Justice announced a le down the Coreflood botnet, using a civil suit for a temporary restr the botnet and criminal seizure warrants in order to disable the bc

We commend the FBI and DOJ for the action against Coreflood private momentum in the fight against botnets and the Microsoft provide technical information from the lessons we learned from th takedowns to assist these agencies in their operation.

In addition, in coordination with the FBI, the Microsoft Malware Pr Win32/Afcore (Coreflood) malware detection in our Malicious Soft the malware's future impact. Please see the MMPC blog for mor Win32/Afcore malware.

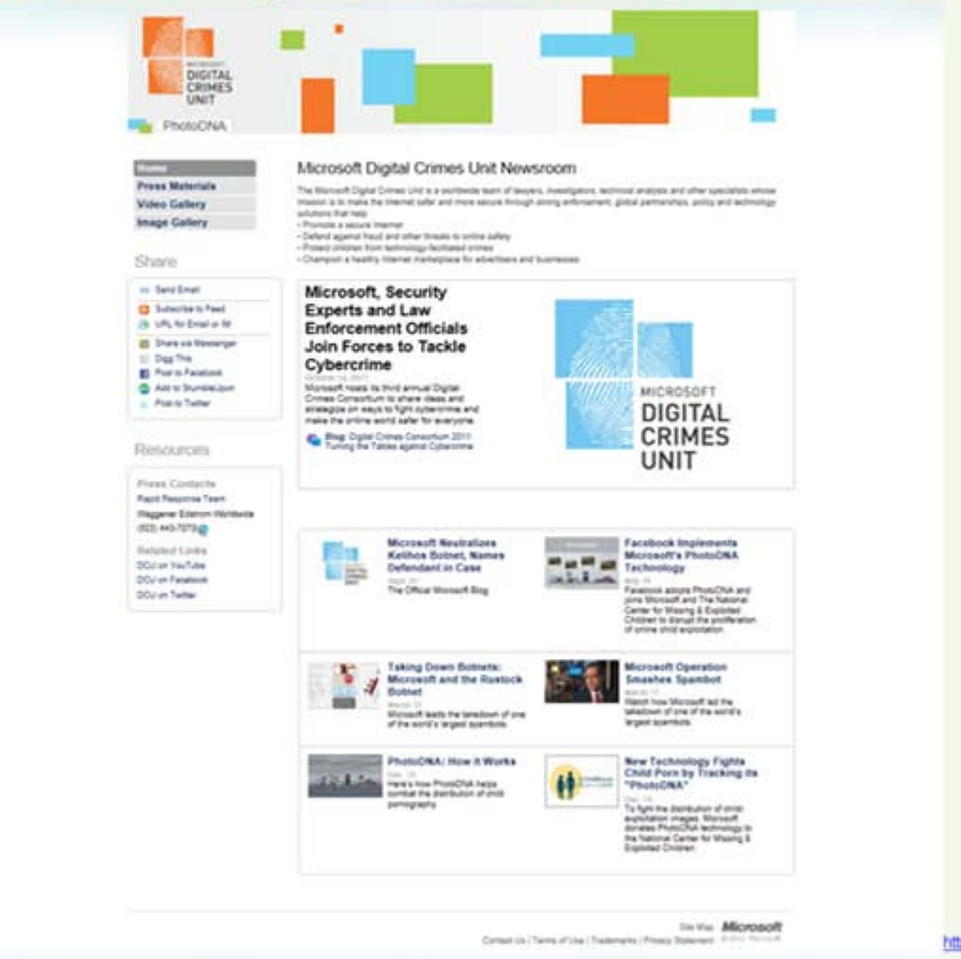
Stemming from previous botnet takedown operations, Microsoft h to provide free information and tools to help people get rid of botn their computers.

Operation b107: The Rustock Takedown Key Messages and Q&A

Key Messages

- Microsoft, in collaboration with Pfizer, FireEye and others, has effectively disrupted the Rustock botnet, which will wipe out a notorious source of spam, fraud and cybercrime.
- Knocking out this botnet will also help reduce threats to public safety in the form of counterfeit drugs.
- Microsoft is creatively and aggressively fighting cybercrime.
- Consumers can get this Rustock malware and other common forms of malware cleaned off their machines for free at http://support.microsoft.com/botnets.

Microsoft Digital Crimes Unit Newsroom



http://www.microsoft.com/presspass/presskits/dcu/

Critical Infrastructure Partner Program Elements

Infrastructure Resiliency Resources

Materials on critical infrastructure and information assurance topics, such as policy formulation, risk management, operational response, and information sharing

- Critical Infrastructure Protection Principles
- Critical Infrastructure Protection Concepts and Continuum
- Microsoft's Critical Infrastructure Resiliency Exercise Guide
- Microsoft's Agile Framework for Infrastructure Risk Management

Customized Critical Information Infrastructure Security & Resiliency Workshops

One- to four-day workshop style sessions on key CIIP topics such as

- Policy and Strategy
- Risk Management
- Operational Response
- Technology Assurance

Designing for resilience

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

- Co-chaired by Phil Reitinger from Microsoft and Janne Uusilehto from Nokia
- Consists of six members: EMC, Juniper, Microsoft, Nokia, SAP, and Symantec
- Dedicated to increasing trust in information and communications technology products and services through the advancement of proven software assurance methods

- Published two papers to improve software security
  - *Software Assurance: An Overview of Current Industry Best Practices*
  - *Fundamental Practices for Secure Software Design and Development*
- Establishing an International Advisory Board

Coordinating operational response

- *Industry Consortium for the Advancement of Security on the Internet*
- ICASI enhances the global security landscape by driving excellence and innovation in security response practices; and by enabling its members to proactively collaborate to analyze, mitigate, and resolve multi-vendor, global security challenges
- Made up of five companies currently: Cisco, IBM, Intel, Juniper, Microsoft

Developing operational coordination and thought leadership products

- The *Unified Security Incident Response Plan* (USIRP)
- A new paper on security response planning

Governments' question No. 1:
Software evaluation and certification status?

US National Information Assurance Partnership (NIAP)
Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) Evaluation List

Product Name	VID	Vendor	Conformance Claim – Evaluation Level /ProtectionProfile	Technology Type	Validated	CC Test Lab
Microsoft Certificate Server 2003	9507	Microsoft Corporation Mike Lal 425.705.4651 mikelal@microsoft.com	EAL4 Augmented with ALC_FLR.3, AVA_VLA.4 PP_CIMC_SL3_V1.0 (Archived)	Certificate Management	2007-04-01	SAIC Common Criteria Testing Laboratory
Microsoft Windows 2003 Server SP1, XP SP2, and XP Embedded SP2 (for specific editions, updates, patches and hotfixessee Section 1 in Security Target)	9506	Microsoft Corporation Mike Lal 425-705-4651 mikelal@microsoft.com	EAL4 Augmented with ALC_FLR.3, AVA_VLA.4 PP_OS_CA_V1.d (Archived)	Operating System	2007-04-01	SAIC Common Criteria Testing Laboratory
Microsoft Certificate Server 2003	4024	Microsoft Corporation Mike Lal 425.705.4651 mikelal@microsoft.com	EAL4 Augmented with ALC_FLR.3 PP_CIMC_SL3_V1.0 (Archived)	Certificate Management	2005-11-15	SAIC Common Criteria Testing Laboratory
Microsoft Windows 2000 Professional, Server, and Advanced Server with SP3 and Q326886 Hotfix	4002	Microsoft Corporation Mike Lal 425.705.4651 mikelal@microsoft.com	EAL4 Augmented PP_OS_CA_V1.d (Archived)	Network Management, Operating System, Sensitive Data Protection, VPN	2002-10-25	SAIC Common Criteria Testing Laboratory
Microsoft Windows 2003 Server SP1, XP SP2, and XP Embedded SP2 (for specific editions, updates, patches and hotfixes see Section 1 in Security Target)	4025	Microsoft Corporation Mike Lal 425.705.4651 mikelal@microsoft.com	EAL4 Augmented with ALC_FLR.3 PP_OS_CA_V1.d (Archived)	Operating System	2005-10-07	SAIC Common Criteria Testing Laboratory
Microsoft Windows Rights Management Services (RMS) 1.0 SP2	10224	Microsoft Corporation Tim Myers 425-707-9422 timmyers@microsoft.com	EAL4 Augmented with ALC_FLR.3	Sensitive Data Protection	2007-08-08	SAIC Common Criteria Testing Laboratory
Microsoft Windows Vista Enterprise; Windows Server 2008 Standard Edition; Windows Server 2008 Enterprise Edition; Windows Server 2008 Datacenter Edition	10291	Microsoft Corporation Tim Myers 425-707-9422 timmyers@microsoft.com	EAL4 Augmented with ALC_FLR.3, AVA_VLA.3 PP_OS_CA_V1.d (Archived)	Operating System	2009-08-31	SAIC Common Criteria Testing Laboratory
Microsoft Windows Server 2003 SP1 (x86) and x64 Edition, Standard, Enterprise, and Datacenter; Windows Server 2003 SP1 (IA64), Enterprise and Datacenter; Windows XP Professional SP2 (x86) and x64 Edition (for specific TOE software updates, patches, and hotfixes see Section 1 of Security Target)	10151	Microsoft Corporation Tim Myers 425.707.9422 timmyers@microsoft.com	EAL4 Augmented with ALC_FLR.3 PP_OS_CA_V1.d (Archived)	Operating System	2006-09-18	SAIC Common Criteria Testing Laboratory
Microsoft Windows Server 2003 SP2 including R2, Standard, Enterprise, Datacenter, x64, and Itanium Editions; Windows XP Professional SP2 and x64 SP2; Windows XP Embedded SP2 (for specific TOE software updates, patches, and hotfixes see Section 1 of Security Target)	10184	Microsoft Corporation Tim Myers 425.707.9422 timmyers@microsoft.com	EAL4 Augmented with ALC_FLR.3 PP_OS_CA_V1.d (Archived)	Operating System	2008-02-07	SAIC Common Criteria Testing Laboratory

Evaluation and certification – Common Criteria

Windows 7 and Windows Server 2008 R2 – EAL4+ evaluated – see National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) web site - http://www.niap-ccevs.org/vpl/?tech_name=Operating+System

Product Name	VID	Vendor	Conformance Claim	Technology Type	Validated
Microsoft Windows 7, Microsoft Windows Server 2008 R2	10390	Microsoft Corporation Tim Myers +1 425-882-8080 timmyers@microsoft.com	EAL4 Augmented with ALC_FLR.3 ■ PP_GPOSPP_V7 ■ PP_OS_BR_V1.0	Operating System	2011-03-24

National Security Authorities role – verification and approval for OS/Applications Security Settings

Microsoft Security Intelligence Report volume 11 (SIR v11)

Volume 11 (January 2011 through June 2011)

Microsoft SIR vol. 11 Website

www.microsoft.com/sir

About Microsoft Security Intelligence Report vol. 11

- Zeroing in on Malware Propagation Methods
- Worldwide Threat Assessment
  - Vulnerability trends
  - Exploit trends
    - O/S, Browser, and applications
  - Malware and potentially unwanted software
- Regional Threat Assessment
  - 105 countries/regions
- Advanced Malware Cleaning Techniques for the IT Professional
- Promoting Safe Browsing using IE

MICROSOFT UNCLASSIFIED

Microsoft Security Intelligence Report Taxonomy

These data sources enable Microsoft to get data from all the relevant points of view: client, server, mail, Internet threats – **globally**

Windows Defender

More than **100 million** users worldwide

Windows Live Hotmail

More than **280 million** active users worldwide

bing

Billions of web-page scans per month

Malicious Software Removal Tool

600 million computers worldwide reporting monthly

3.2 billion executions in 1H10

More than **20 billion** executions since 2005

Microsoft Security Essentials

More than **30 million** users worldwide and performs **millions** of malware removals per year worldwide

SIRv11 Detailed Taxonomy

Product Name	Main Customer Segment		Malicious Software		Spyware & Potentially Unwanted Software		Available at No Additional Charge	Main Distribution Methods
	Consumers	Business	Scan and Remove	Real-time Protection	Scan and Remove	Real-time Protection		
Windows Malicious Software Removal Tool	•		Prevalent Malware Families				•	WU/AU Download Center
Windows Defender	•				•	•	•	Download Center Windows Vista/ Windows 7
Windows Safety scanner	•		•		•		•	Cloud
Microsoft Security Essentials	•		•	•	•	•	•	Cloud
Forefront Online Protection for Exchange		•	•	•				Cloud
Microsoft Forefront Endpoint Protection		•	•	•	•	•		Volume Licensing

- Hotmail – More than 280 million active users
- Internet Explorer; the world's most popular browser with SmartScreen, Microsoft Phishing Filter
- Microsoft Forefront Online Security for Exchange scans billions of e-mail messages a year
- Malware Software Removal Tool (MSRT) has a user base of more than 600 million unique computers worldwide
- Microsoft Security Essentials available in over 30 languages
- Bing billions of Web-pages scanned each month

Zero Day Threats vs. Propagation Methods Trends

Zero Day Threats

- Microsoft conducted an analysis to better understand the frequency of zero-day exploitation and the risk customers face from it
- This analysis was created to give security professionals information they can use to prioritize their concerns and effectively manage risks
- For the analysis, threats detected by the Malicious Software Removal Tool (MSRT) during the first half of 2011 (1H11) were classified by the means of propagation each threat family has been documented to use
- The main malware propagation methods are
  - User interaction, typically employing a form of social engineering
  - Autorun feature abuse
  - File-infection, exploits (with updates available)
  - Brute force password attacks
  - Office macros

Classifying Malware by Propagation Method

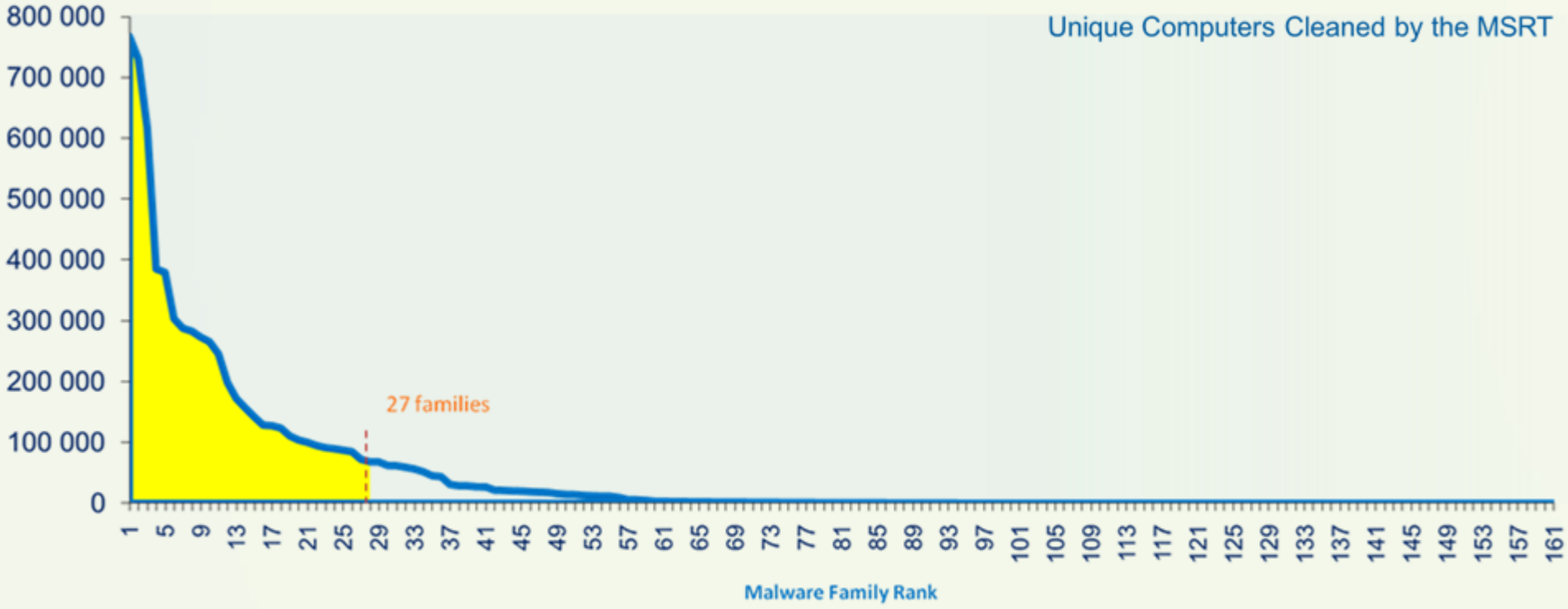
Taxonomy Variables

- User Interaction?
- Vulnerability Exploitation?
- Configurable Prevention?

→

- File Infection
- Password Brute Force
- Office Macros
- Autorun
- ACL
- Social Engineering
- Vulnerability Exploitation

Unique Computer Infections, by Malware Family

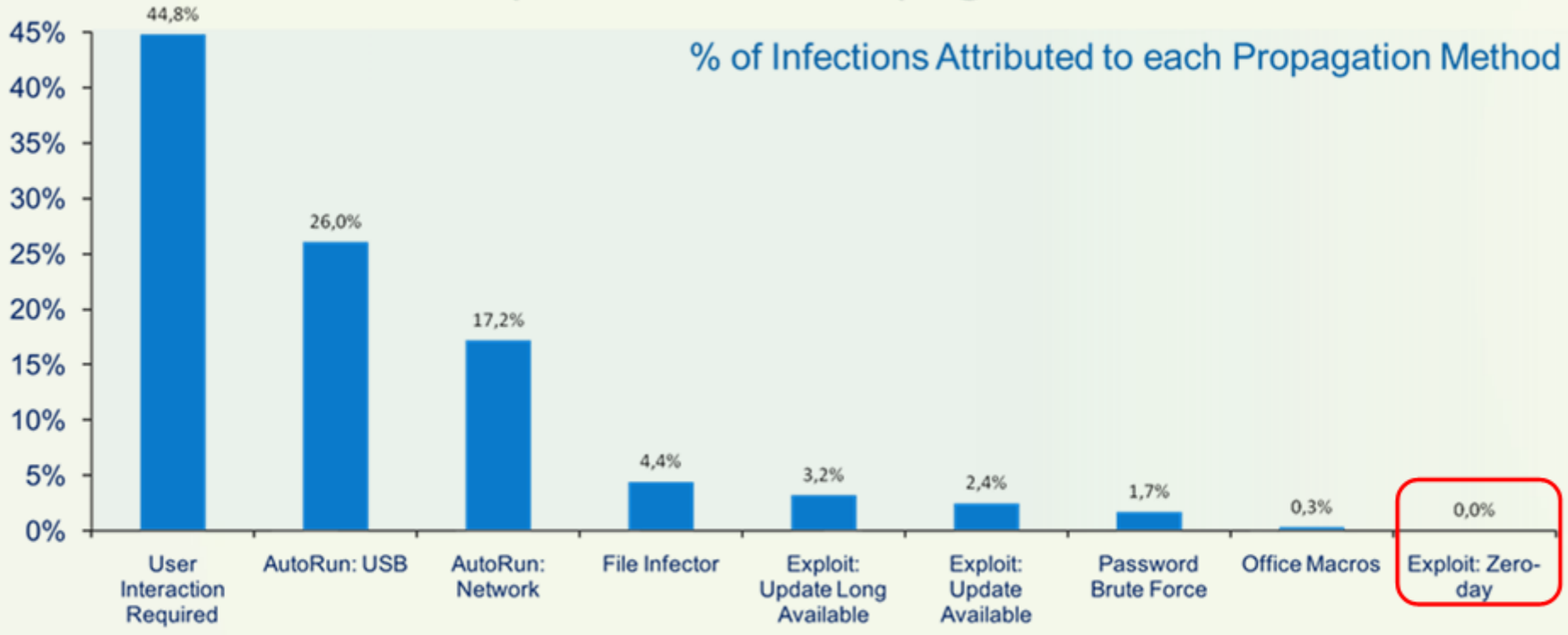


- Malware infections tend to resemble a power law distribution, a few dozen families account for most infections and a "long tail" consisting of thousands of less common families account for the rest

Top Malware Families

	Family	Exploit: Zero-day	Exploit: Update Avail.	Exploit: Update Long Avail.	AutoRun: Network	AutoRun: USB	Office Macro	Password Brute Force	User Interaction	File Infector
1	Win32/Frethog				•				•	
2	Win32/Taterf				•	•				
3	Win32/Vobfus			•	•	•				
4	Win32/FakeRean								•	
5	Win32/Lethic								•	
6	Win32/Conficker			•	•	•		•		
7	Win32/Rimecud				•	•			•	
8	Win32/Zbot		•	•					•	
9	Win32/Sality				•					•
10	Win32/Jeefo									•
11	Win32/Renos								•	
12	Win32/Yimfoca								•	
13	Win32/Ramnit				•	•	•			•
14	Win32/Parite									•
15	Win32/Alureon		•						•	
16	Win32/Cycbot			•					•	
17	Win32/Hamweq					•				
18	Win32/Renocide				•	•			•	
19	Win32/Bubnix								•	
20	Win32/Brontok					•			•	
21	Win32/Bredolab			•						
22	Win32/Cutwail								•	
23	Win32/Randex							•		
24	Win32/Bancos								•	
25	Win32/FakeXPA								•	
26	Win32/Pushbot			•		•			•	
27	Win32/FakeSpypro								•	

Infections by Estimated Propagation Method



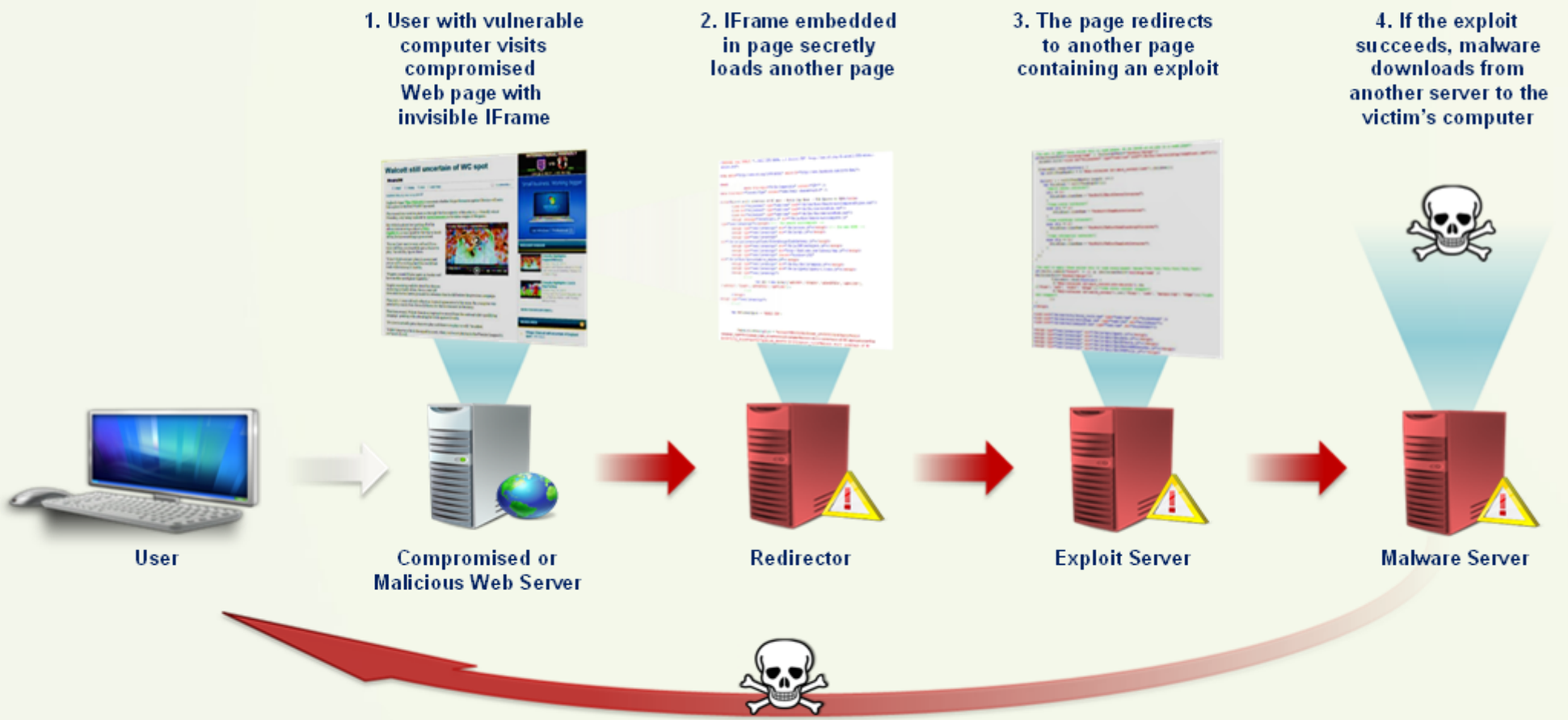
- User interaction was attributed to nearly half (45%) of all infections

Attacks Trends

Malicious And Potentially Unwanted Software

Rogue Security Software

Drive-By Download Attacks



Automated SQL Injection Attacks

1. The automated tool searches for vulnerable Web applications and uses multiple SQL injection techniques to insert malicious HTML <script> tags into every string column in multiple tables.

2. If a Web page loads string data from a compromised database without checking for second-order XSS attacks, invisible "drive-by" exploits occur on the page.

3. When a visitor loads the infected page, it secretly contacts an exploit server to download the exploits.

4. Users with vulnerable browsers become infected.

Microsoft Malware Protection Center
http://www.microsoft.com/security/portal

Phishing Impressions Tracking by Microsoft

1. The user views a phishing message, in e-mail or elsewhere, and is tricked into clicking a link that leads to a malicious Web site

2. SmartScreen Filter in Internet Explorer checks the Microsoft URL Reputation Service, determines that the Web site is malicious, and blocks it

3. The URL Reputation Service records the anonymized details of the incident as a phishing impression

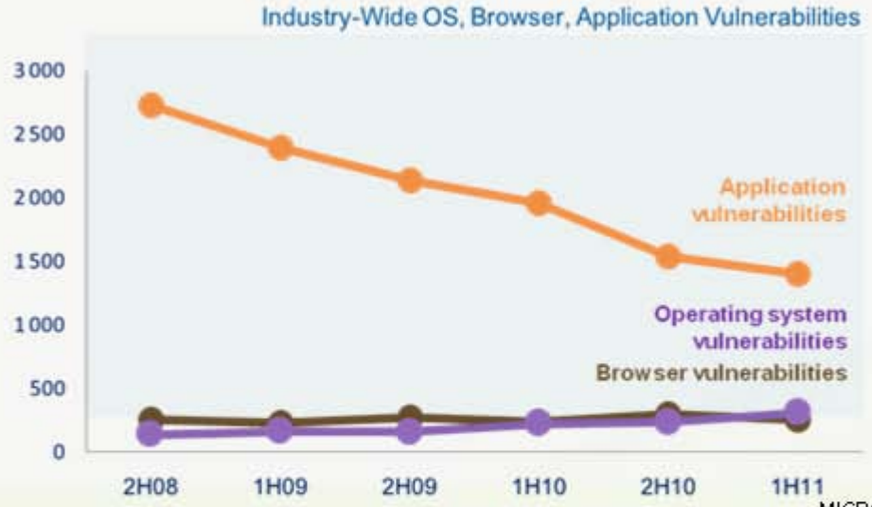
Microsoft Malware Protection Center
http://www.microsoft.com/security/portal

Impressions for Each Type of Phishing Site

- The largest share of phishing impressions were for sites that targeted social networks, reaching a high of 83.8% of impressions in April

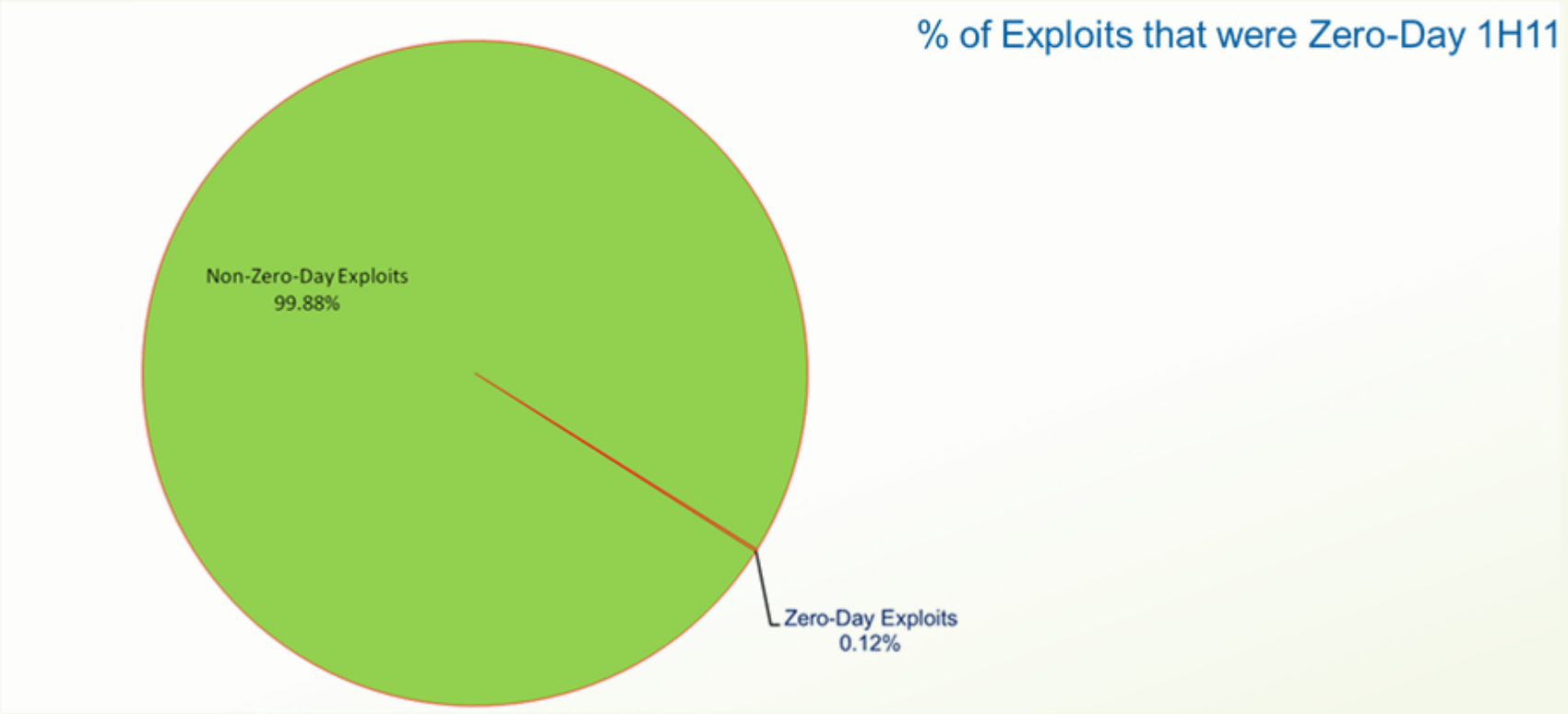
Vulnerability Trends

Industry-Wide Vulnerability Disclosures

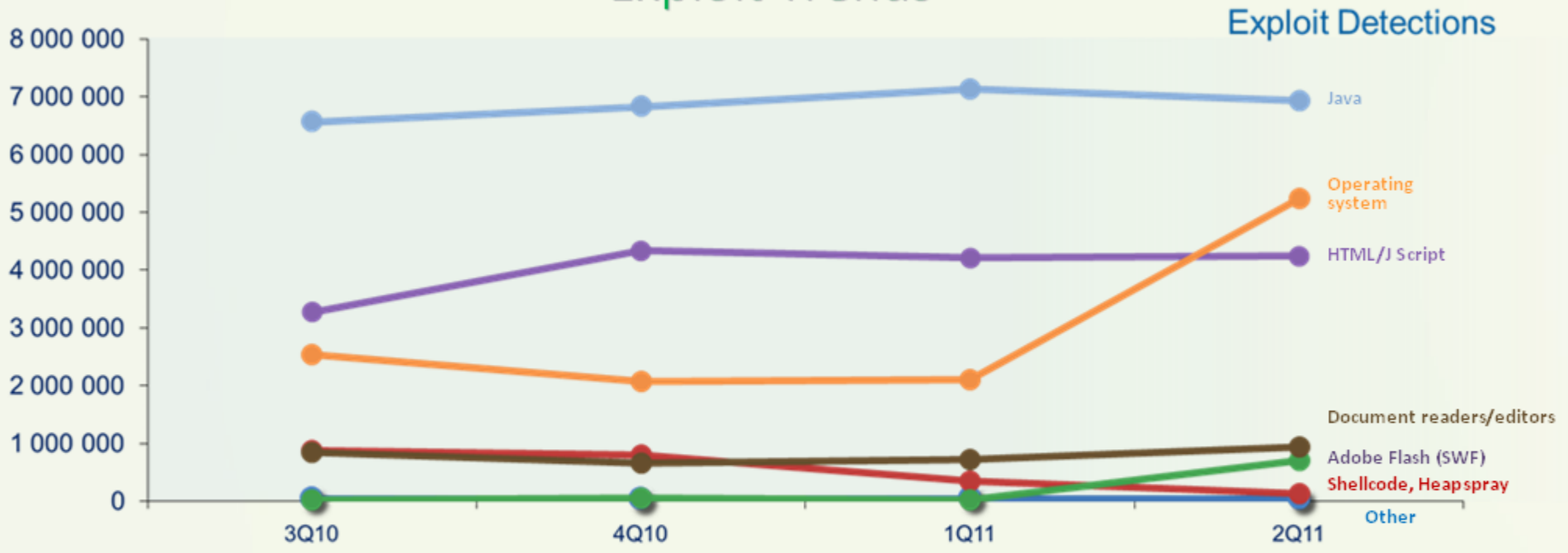


Exploit Trends

Zero-Day Versus Non-Zero-Day

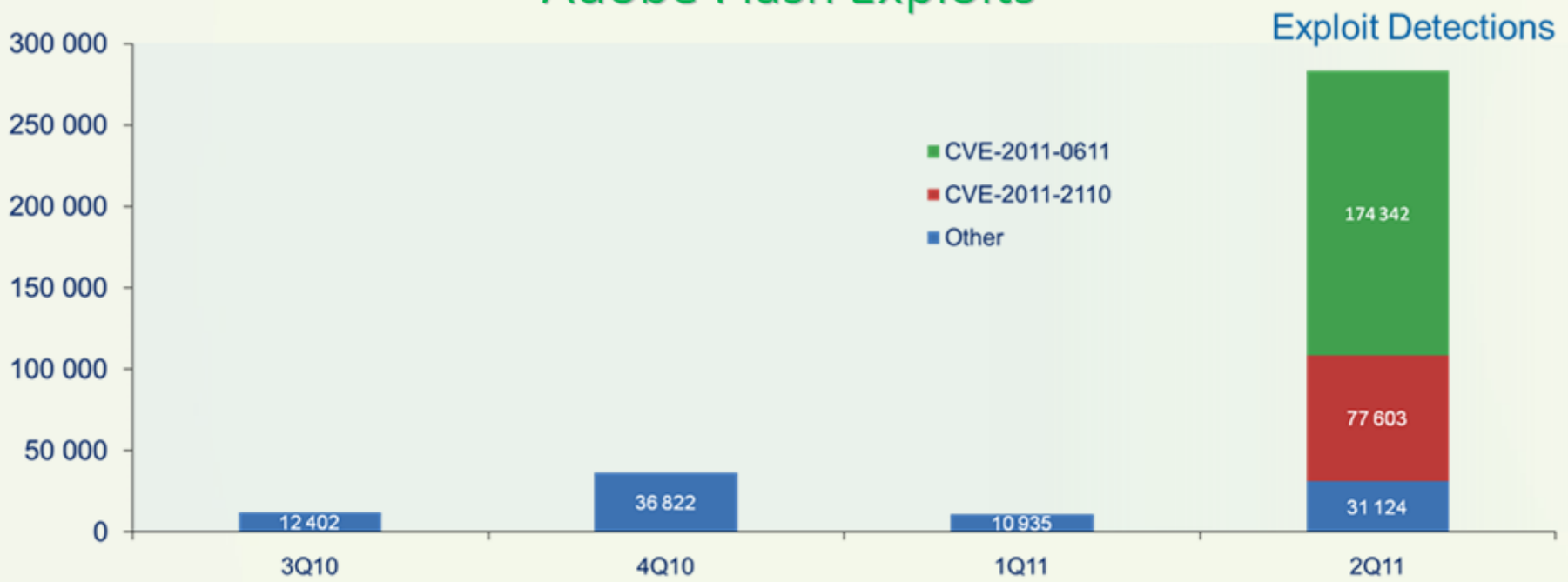


Exploit Trends



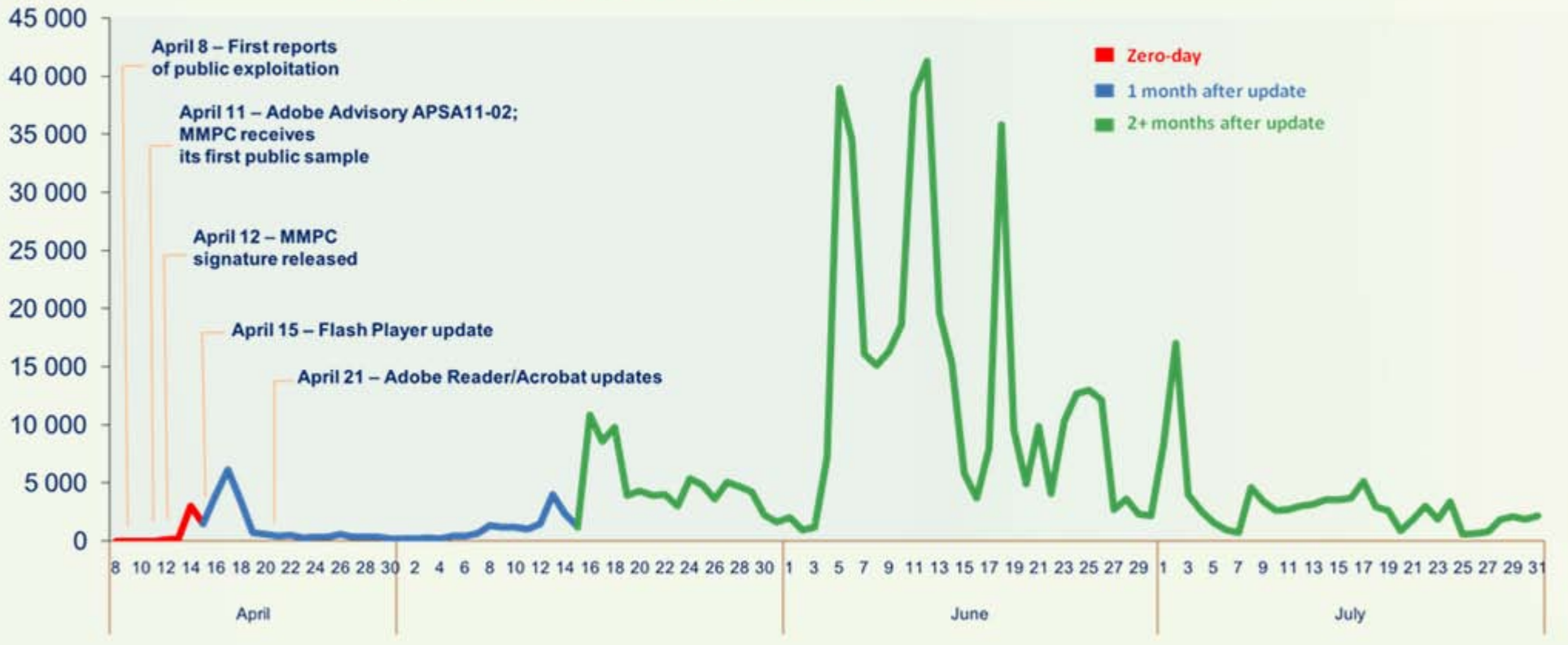
- The most commonly observed type of exploits were those targeting vulnerabilities in the Oracle (formerly Sun) Java Runtime Environment (JRE)
- Detections of operating system exploits result of CVE-2010-2568
- More than 934,000 detections of exploits targeting Adobe Flash

Adobe Flash Exploits

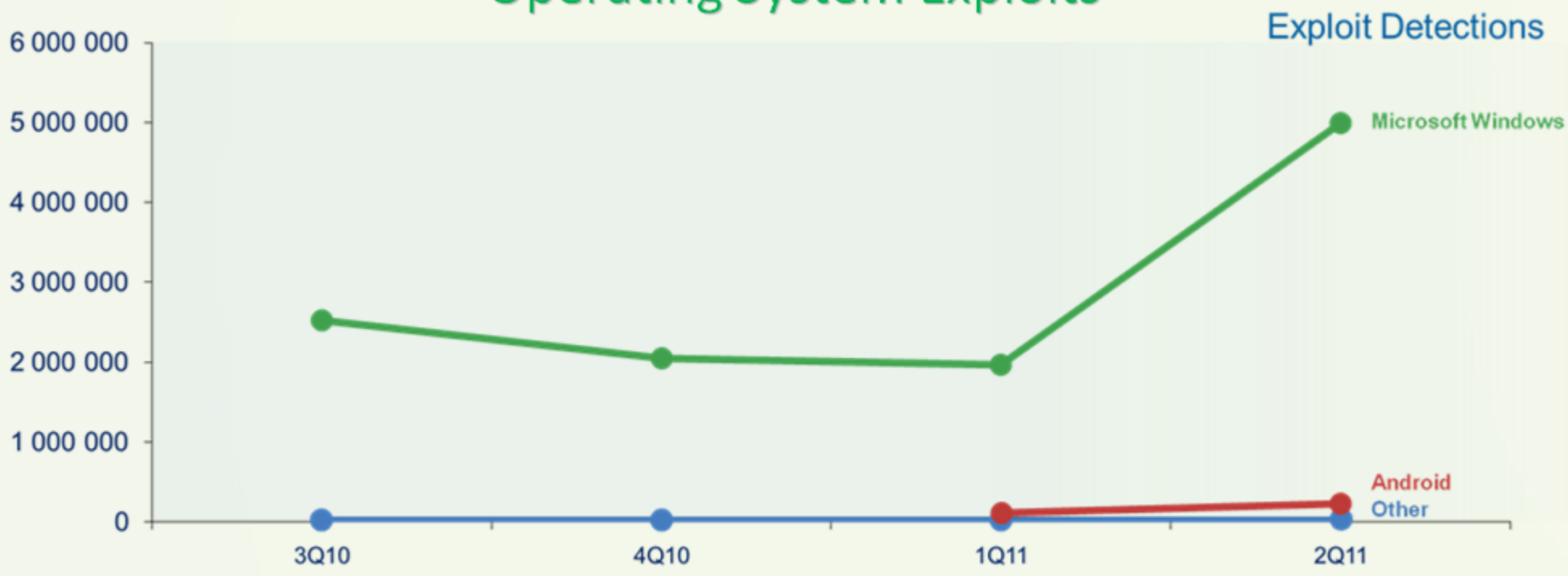


- Exploitation of Adobe Flash increased dramatically in 2Q11 with the disclosure of two new vulnerabilities, CVE-2011-0611 and CVE-2011-2110

Exploits Targeting CVE-2011-0611

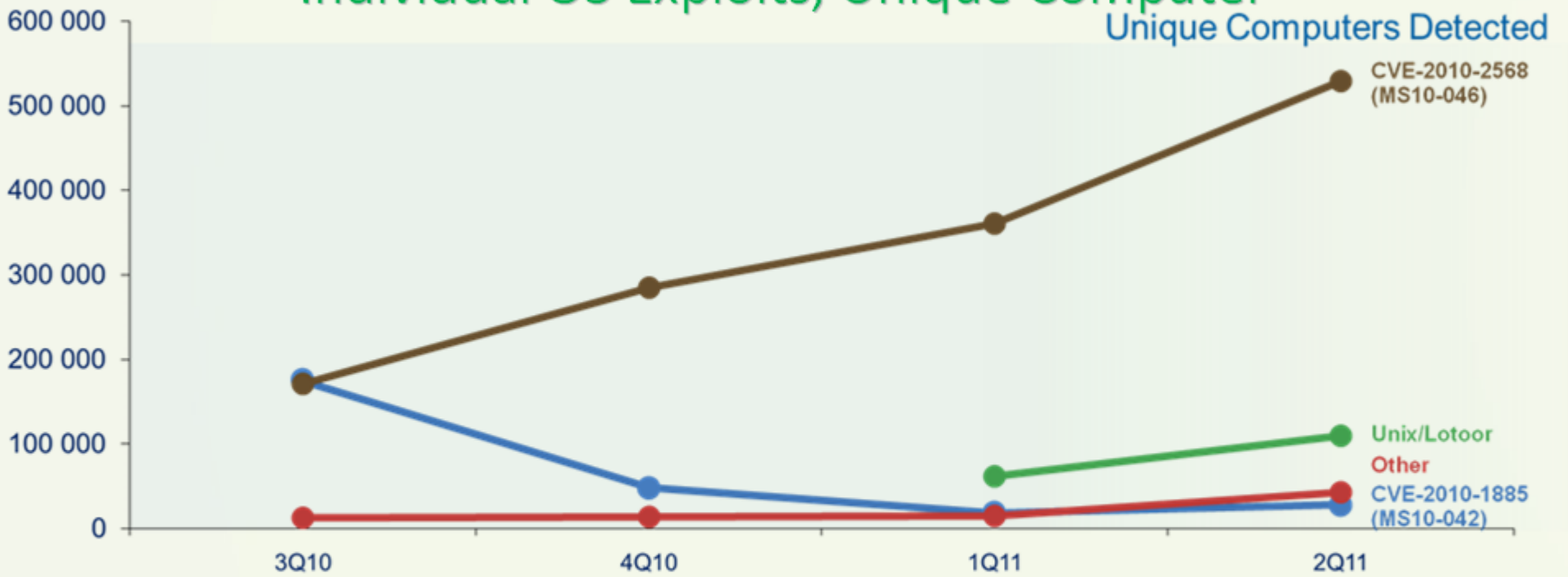


Operating System Exploits



- Exploits targeting Windows are inflated by detections of CVE-2010-2568, which is detected repeatedly on the same computer due to the mechanism it uses to spread
- Exploits affecting the Android operating system detected in significant volume beginning in 1H11

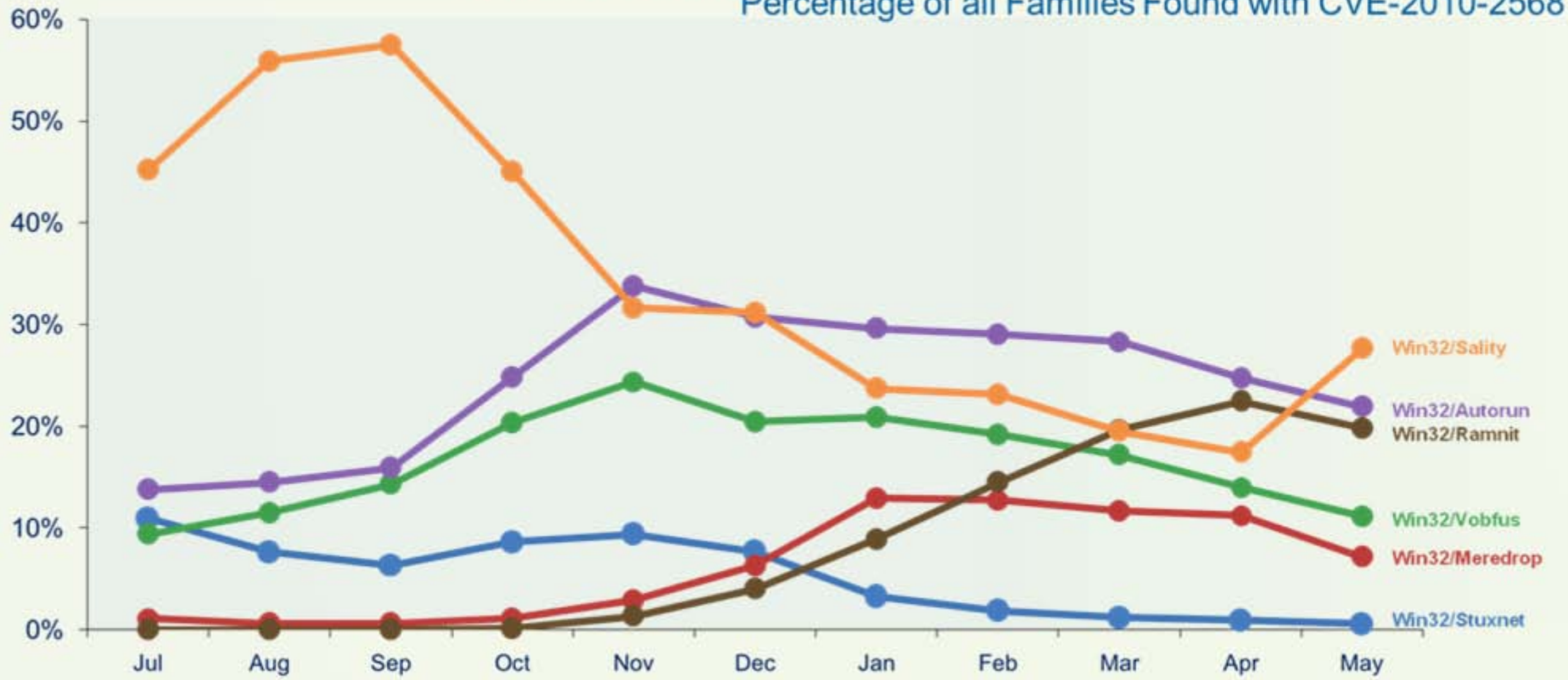
Individual OS Exploits, Unique Computer



- CVE-2010-2568 exploits have a tendency to be reported by the same computer many times, due to the way the exploit technique works, which could give a misleading impression of the exploit's impact
- The increase in Android-based threats has been driven primarily by the exploit family Unix/Lotoor, the second most commonly detected operating system exploit

Families Using .LNK Vulnerability

Percentage of all Families Found with CVE-2010-2568



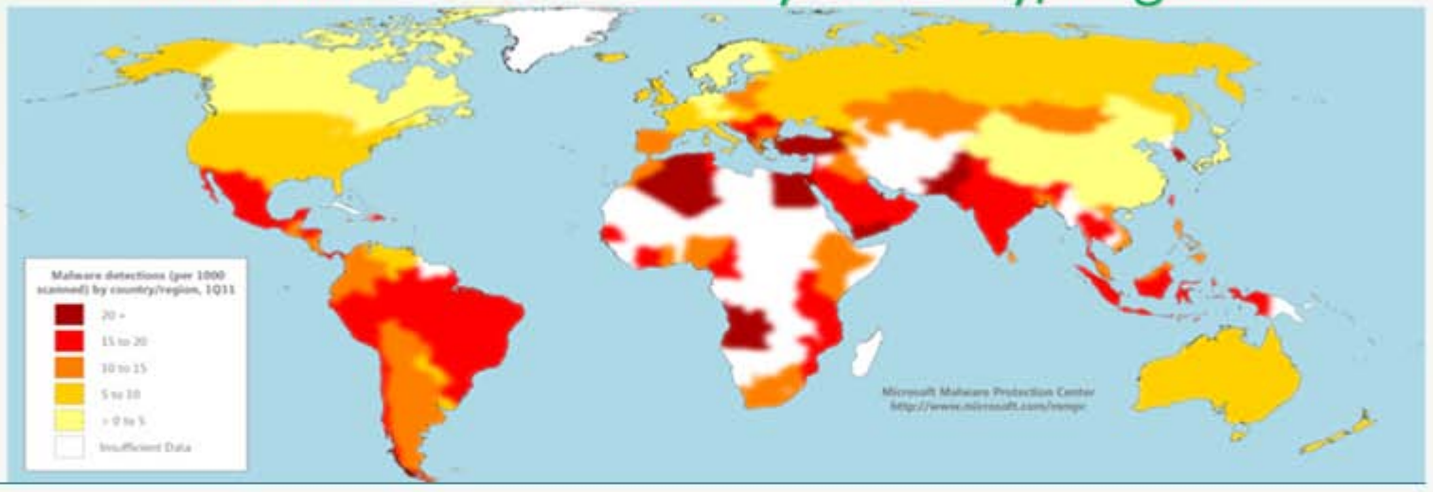
Malware and Potentially Unwanted Software

Most Computers Reporting Detections and Removals, by Location

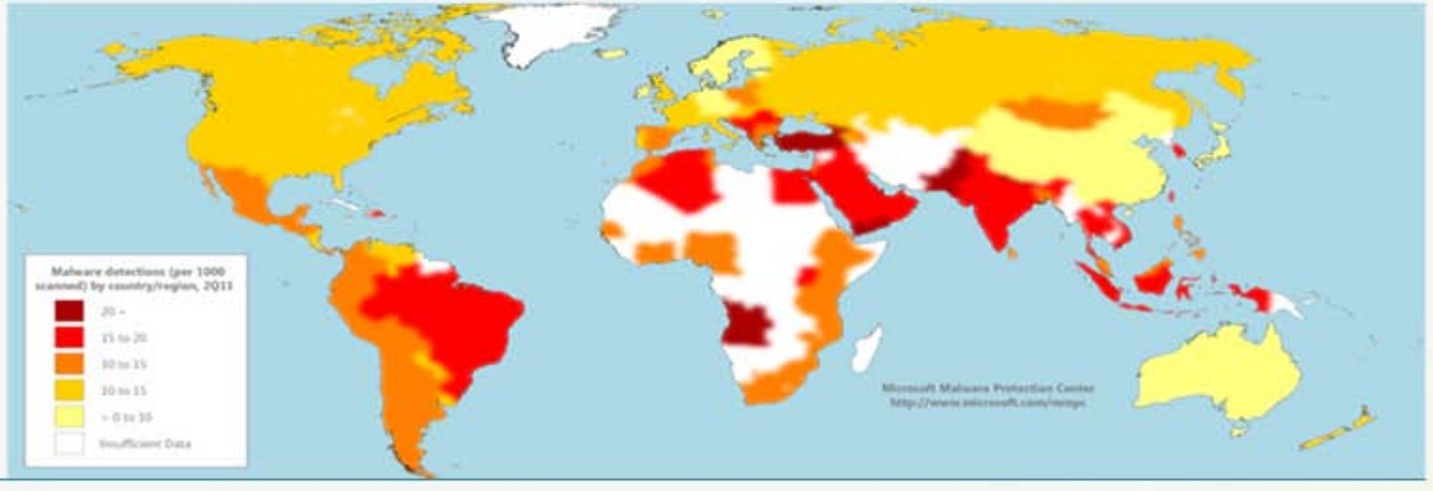
Rank	Country/Region	1Q11	2Q11	Chg. 1Q to 2Q
1	United States	10,727,964	10,471,335	↓ 2.5%
2	Brazil	3,463,973	3,724,844	↑ 7.0%
3	France	2,351,941	2,674,775	↑ 12.1%
4	United Kingdom	2,175,201	2,089,883	↓ 4.1%
5	China	2,017,682	1,883,578	↓ 7.1%
6	Germany	1,622,081	1,530,551	↓ 6.0%
7	Russia	1,296,208	1,583,857	↑ 18.2%
8	Italy	1,358,166	1,509,148	↑ 10.0%
9	Canada	1,377,173	1,353,164	↓ 1.8%
10	Turkey	1,248,978	1,359,181	↑ 8.1%

Malware Detections by Country/Region

Q1



Q2

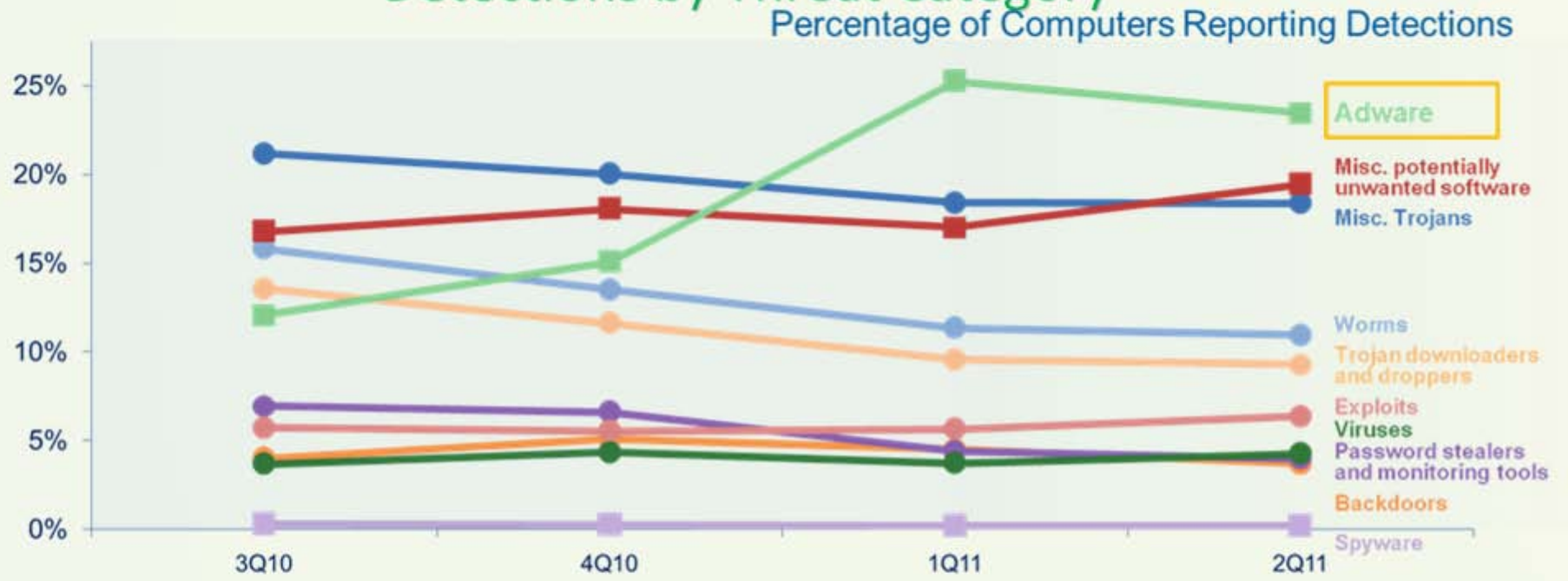


Infection Rates by OS and Service Pack

Computers Cleaned per Thousand

- Charts are Normalized
- Infection rates for more recently released operating systems and service packs are consistently lower than earlier ones, for both client and server platforms
- Infection rates for the 64-bit versions of Windows Vista and Windows 7 are lower than for the corresponding 32-bit versions of those operating systems

Detections by Threat Category



- Adware rose to become the most commonly detected category due in large part to a pair of new families, Win32/OpenCandy and Win32/ShopperReports

Threat Category Prevalence by Location

Category	World	US	Brazil	France	UK	China	Germany	Russia	Italy	Canada	Turkey
Adware	37.0%	39.7%	26.1%	72.4%	49.1%	5.3%	44.1%	9.7%	60.0%	45.8%	37.7%
Misc. Potentially Unwanted Software	30.6%	22.1%	35.2%	27.7%	27.9%	48.8%	26.5%	60.3%	26.1%	26.7%	34.7%
Misc. Trojans	28.9%	38.9%	22.6%	12.1%	31.9%	36.6%	25.4%	34.1%	15.5%	36.2%	41.9%
Worms	17.2%	6.3%	24.2%	7.3%	5.9%	14.0%	8.6%	19.9%	11.9%	5.0%	31.3%
Trojan Downloaders and Droppers	14.7%	17.8%	21.0%	7.0%	13.8%	20.4%	13.4%	9.7%	9.1%	17.4%	13.5%
Exploits	10.0%	14.4%	16.3%	2.7%	10.5%	15.0%	7.9%	7.1%	4.0%	13.1%	3.4%
Viruses	6.7%	2.0%	10.1%	1.2%	3.4%	8.0%	2.9%	8.4%	1.7%	2.0%	17.7%
Password Stealers & Monitoring Tools	6.3%	2.9%	18.9%	2.4%	3.9%	4.8%	6.8%	5.1%	4.2%	2.8%	7.8%
Backdoors	5.8%	4.8%	7.7%	3.3%	3.9%	8.4%	5.8%	6.3%	7.1%	4.6%	5.4%
Spyware	0.3%	0.4%	0.1%	0.1%	0.2%	1.8%	0.2%	0.3%	0.1%	0.3%	0.1%

- Totals for each location may exceed 100 percent because some computers reported threats from more than one category

Top 10 Threat Families

Family	Category	3Q10	4Q10	1Q11	2Q11
Win32/Hotbar	Adware	997,111	1,661,747	3,149,677	4,411,501
JS/Pornpop	Adware	2,659,054	3,666,856	4,706,968	4,330,510
Win32/Autorun	Worms	2,454,708	2,624,241	3,718,690	3,677,588
Win32/OpenCandy	Adware	—	—	6,797,012	3,652,658
Win32/ShopperReports	Adware	—	—	3,348,949	2,902,430
Win32/Keygen	Misc. Potentially Unwanted Software	981,051	1,402,417	2,299,870	2,680,354
Win32/ClickPotato	Adware	451,407	2,074,751	4,694,442	2,592,125
Win32/Zwangi	Misc. Potentially Unwanted Software	1,637,316	2,236,990	2,785,111	2,586,630
Win32/Rimecud	Misc. Trojans	1,673,312	1,872,449	2,123,298	1,818,530
Win32/Conficker	Worm	1,648,481	1,636,201	1,859,498	1,790,035

Malware trends in Slovakia

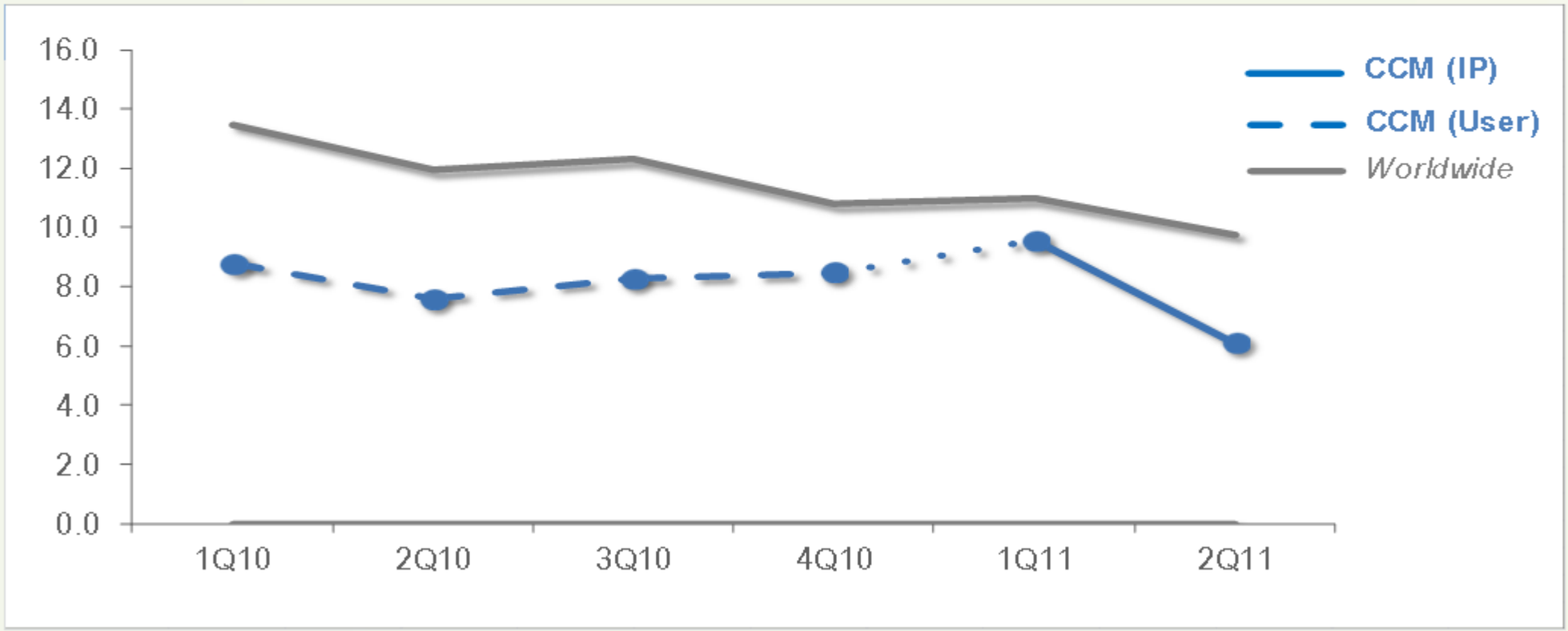
Infection Trends in Slovakia

Metric	3Q10	4Q10	1Q11	2Q11
Host infection rate (CCM) calculated using IP geolocation	N/A	N/A	9.6	6.1
CCM calculated using user-specified location information	8.3	8.5	7.5	4.8
Worldwide infection rate	*12.3*	*10.8*	*11.0*	*9.8*

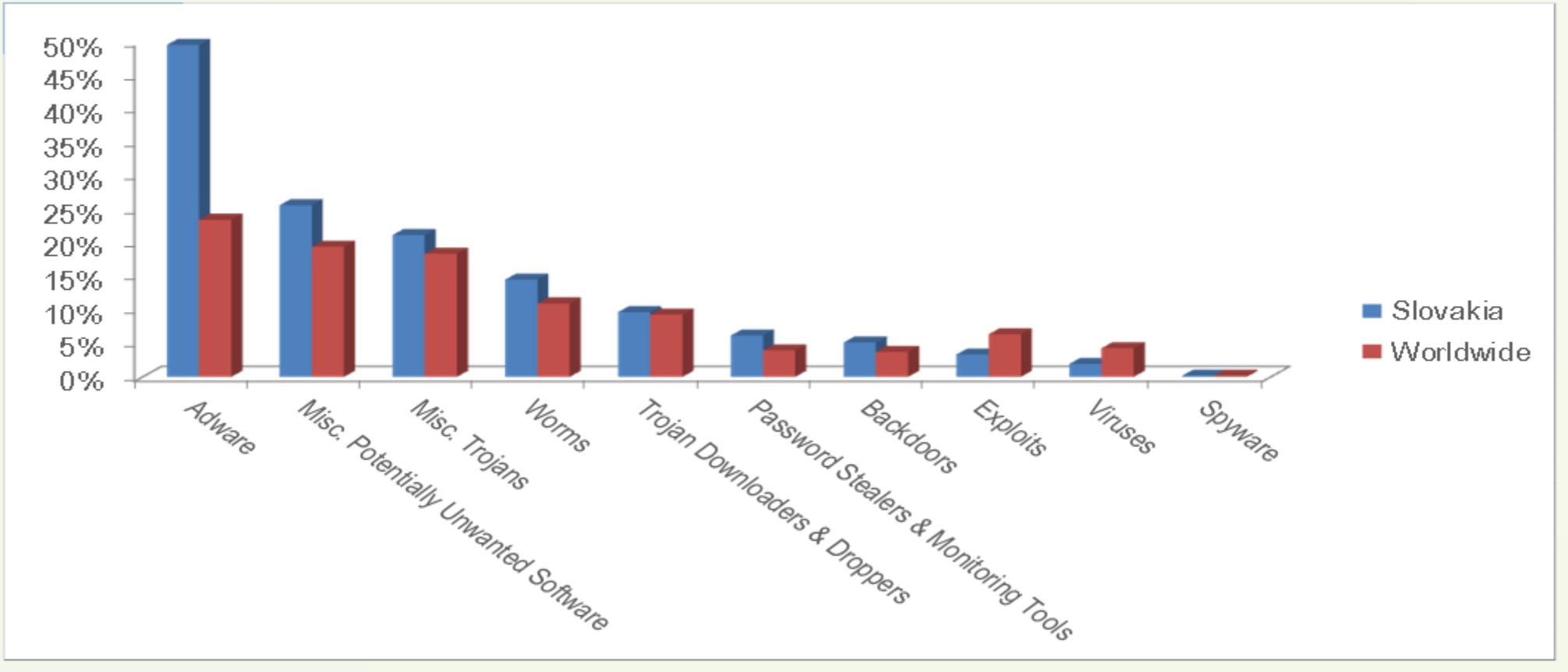
Malicious & Potentially Unwanted Software

Slovakia Infection Rate Trends

CCM (100,000 MSRT executions)



Threat Categories in Slovakia vs. Worldwide



Threat Categories in Slovakia

- The most common category in Slovakia in 2Q11 was Adware, which affected 49.5 percent of all infected computers, up from 37.8 percent in 1Q11
- The second most common category in Slovakia in 2Q11 was Miscellaneous Potentially Unwanted Software, which affected 25.6 percent of all infected computers, down from 27.8 percent in 1Q11
- The third most common category in Slovakia in 2Q11 was Miscellaneous Trojans, which affected 21.2 percent of all infected computers, down from 26.9 percent in 1Q11

Threat Families in Slovakia

	Family	Most Significant Category	% of Computers Affected
1	Win32/GamePlayLabs	Adware	25.8%
2	Win32/OpenCandy	Adware	10.4%
3	JS/Pornpop	Adware	9.2%
4	Win32/Autorun	Worms	8.0%
5	Win32/Keygen	Misc. Potentially Unwanted Software	7.6%
6	Win32/Rimecud	Worms	5.4%
7	Win32/Obfuscator	Misc. Potentially Unwanted Software	4.6%
8	Win32/Taterf	Worms	4.5%
9	Win32/Hotbar	Adware	3.9%
10	Win32/Renos	Trojan Downloaders & Droppers	3.2%

Threat Families in Slovakia – 2Q11

- Win32/GamePlayLabs (25.8% of detected computers)
  - A program that collects browsing data from an affected user that is then used to serve targeted advertising to the user
- Win32/OpenCandy (10.4%)
  - An adware program that may be bundled with certain third-party software installation programs. Some versions may send user-specific information, including a unique machine code, operating system information, locale, and certain other information to a remote server without obtaining adequate user consent
- JS/Pornpop (9.2%)
  - A generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content
- Win32/Autorun (8.0%)
  - A family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives

Malicious Websites and Spam in Slovakia

Metric	3Q10	4Q10	1Q11	2Q11
Phishing sites per 1000 hosts *(Worldwide)*	N/A *(N/A)*	N/A *(N/A)*	0.13 *(0.33)*	0.12 *(0.38)*
Malware hosting sites per 1000 hosts *(Worldwide)*	N/A *(N/A)*	N/A *(N/A)*	0.70 *(2.24)*	0.22 *(2.02)*
Percentage of sites hosting drive-by downloads *(Worldwide)*	0.110% *(0.229%)*	0.069% *(0.131%)*	0.622% *(0.223%)*	0.957% *(0.273%)* ↑
Percentage of world spambot IP addresses	0.000	0.000	0.269	0.131

Spambots in Slovakia

- In 2Q11, Forefront Online Protection for Exchange (FOPE) determined that 0.131 percent of all spambot IP addresses were located in Slovakia; this figure is down from 0.269 in 1Q11

The top 3 spambots hosted in Slovakia in 1Q11

	Botnet	% of All Spambot IP Addresses
1	Win32/Cutwail - trojan that **downloads and executes arbitrary files, usually to send spam**. Win32/Cutwail has also been observed to download the attacker tool Win32/Newacc	29.5%
2	Win32/Lethic - trojan that **connects to remote servers**, which may lead to unauthorized access to an affected system	26.9%
3	Win32/Tedroo - **trojan that sends out spammed e-mail messages**. It allows backdoor access and control of the infected computer, and may modify certain system settings. It also disables the Windows Firewall	13.3%

Spambot Families Description

Family	Description
Win32/Asproxy	A Trojan - Proxy. In the context of a proxy trojan, a proxy serves as an agent between the attacker and the Internet.
Win32/Bagle	A worm that spreads by e-mailing itself to addresses found on an infected computer. Some variants also spread through P2P networks. Bagle acts as a backdoor trojan and can be used to distribute other malicious software.
Win32/Bobax	A worm that targets certain versions of Microsoft Windows. The worm can spread by sending a copy of itself as an attachment to e-mail addresses gathered from an infected computer.
Win32/Cutwail	A trojan that downloads and executes arbitrary files, usually to send spam. Win32/Cutwail has also been observed to download the attacker tool Win32/Newacc.
Win32/Festi	A trojan backdoor that allows backdoor access and control to an infected computer.
Win32/Nedsym	A trojan that distributes spam email messages.
Win32/Tofsee	A Trojan backdoor that provides remote, usually surreptitious, access to affected systems.
Win32/Tedroo	A trojan that sends out spammed e-mail messages. It allows backdoor access and control of the infected computer, and may modify certain system settings. It also disables the Windows Firewall.
Win32/Lethic	A trojan that connects to remote servers, which may lead to unauthorized access to an affected system.
Win32/Cycbot	A backdoor trojan that allows attackers unauthorized access and control of an affected computer. After a computer is infected, the trojan connects to a specific remote server to receive commands from attackers.
Win32/Ponmocup	A is a trojan that silently downloads and installs other programs without consent. This could include the installation of additional malware or malware components to an affected machine.
Win32/Sinowal	A family of password-stealing and backdoor Trojans.
Win32/Waledac	A trojan that collects e-mail addresses found on the computer on which it is installed and distributes spam e-mail messages.
Win32/Rlsloup	A family of trojans that are used to send spam (unsolicited bulk email).

Protect Your Environment

Security Intelligence Report (SIR) helps customers protect:

Organizations

Protect your organization's network from security threats.

Software

Protect your applications and minimize malware threats.

People

Protect workers against privacy and security threats.

Keep all software on your systems updated
Third party, as well as Microsoft

Use Microsoft Update, not Windows update
Updates all Microsoft software

Run anti-virus software from a trusted vendor
Keep it updated

Use caution when clicking on links to Web pages

Use caution with attachments and file transfers

Avoid downloading pirated software

Protect yourself from social engineering attacks

Summary…

Conclusions

- Microsoft is **not just a desktop software provider**
- Microsoft actively participates in National Information Assurance and Critical Information Infrastructure Protection efforts – Government/Law Enforcement/Defense bodies may use Government Security Program and Security Cooperation Program
- Microsoft Digital Crime Unit (DCU) partners with governments, law enforcement, and industry partners worldwide
- Main Microsoft focus: Trustworthy Computing (TwC), Citizens Safety Architecture, Security Settings, Cloud Computing Security (Public and Private) and Secure Optimized Desktop

Recommendations

Take advantage of the resources

Reduce Risk

- Know YOUR threat and innovate proactive and holistic approaches to help mitigate
- Automate when feasible

Keep all software on your systems up to date

- Apply the updates
- Adopt newer versions
- Third party as well as Microsoft

Develop using the Software Development Lifecycle - SDL

- Attackers don't limit themselves to Microsoft or other vendors software

Enhance Resiliency

- Enable rapid detection of attacks
- Use analysis to drive action
- Know your traffic

Security, Identity, and Access Management (SIAM) Reactive and Proactive Components

REACTIVE

Technologies

- Active Directory® Domain Services (AD DS)
- Active Directory Federation Services (AD FS)
- Active Directory Rights Management Services (AD RMS)
- Active Directory Certificate Services (AD CS)
- Forefront™ Client Security (FCS)
- Forefront Identity Manager (FIM)
- Forefront Identity Manager - Certificate Management (FIM – CM)
- Forefront Protection 2010 for Exchange Server (FPE)
- Forefront Protection 2010 for SharePoint (FPSP)
- Forefront Threat Management Gateway (TMG)
- Forefront Unified Access Gateway (UAG)
- Identity Lifecycle Manager 2007 (ILM)
- Network Access Protection (NAP)
- Windows® Bitlocker®
- Windows DirectAccess

PROACTIVE

Offerings

Secure Messaging

Secure Collaboration

Secure Endpoint

Information Protection

Identity and Access Management

Security Guidance and Resources in support of National Security

- Microsoft Security Home Page: www.microsoft.com/security
- Microsoft Trustworthy Computing: www.microsoft.com/security/twc
- Microsoft Forefront® : www.microsoft.com/forefront
- Infrastructure Optimization: www.microsoft.com/io
- Microsoft Security Assessment Tool: www.microsoft.com/security/msat

General Information

- Microsoft Live Safety Center: safety.live.com
- Microsoft Security Response Center: www.microsoft.com/security/msrc
- Security Development Lifecycle: msdn.microsoft.com/security/sdl
- Get the Facts about Windows and Linux: www.microsoft.com/windowsserver/compare

Guidance Centers

- Security Guidance Centers: www.microsoft.com/security/guidance
- Security Guidance for IT Professionals: www.microsoft.com/technet/security
- The Microsoft Security Developer Center: msdn.microsoft.com/security
- The Security at Home Consumer Site: www.microsoft.com/athome/security

Anti-malware

- Microsoft Security Essentials http://www.microsoft.com/Security_Essentials/
- Windows Defender: www.microsoft.com/athome/security/spyware/software
- Spyware and Unwanted Software Criteria: www.microsoft.com/athome/security/spyware/software/isv

Software Vulnerability Disclosures

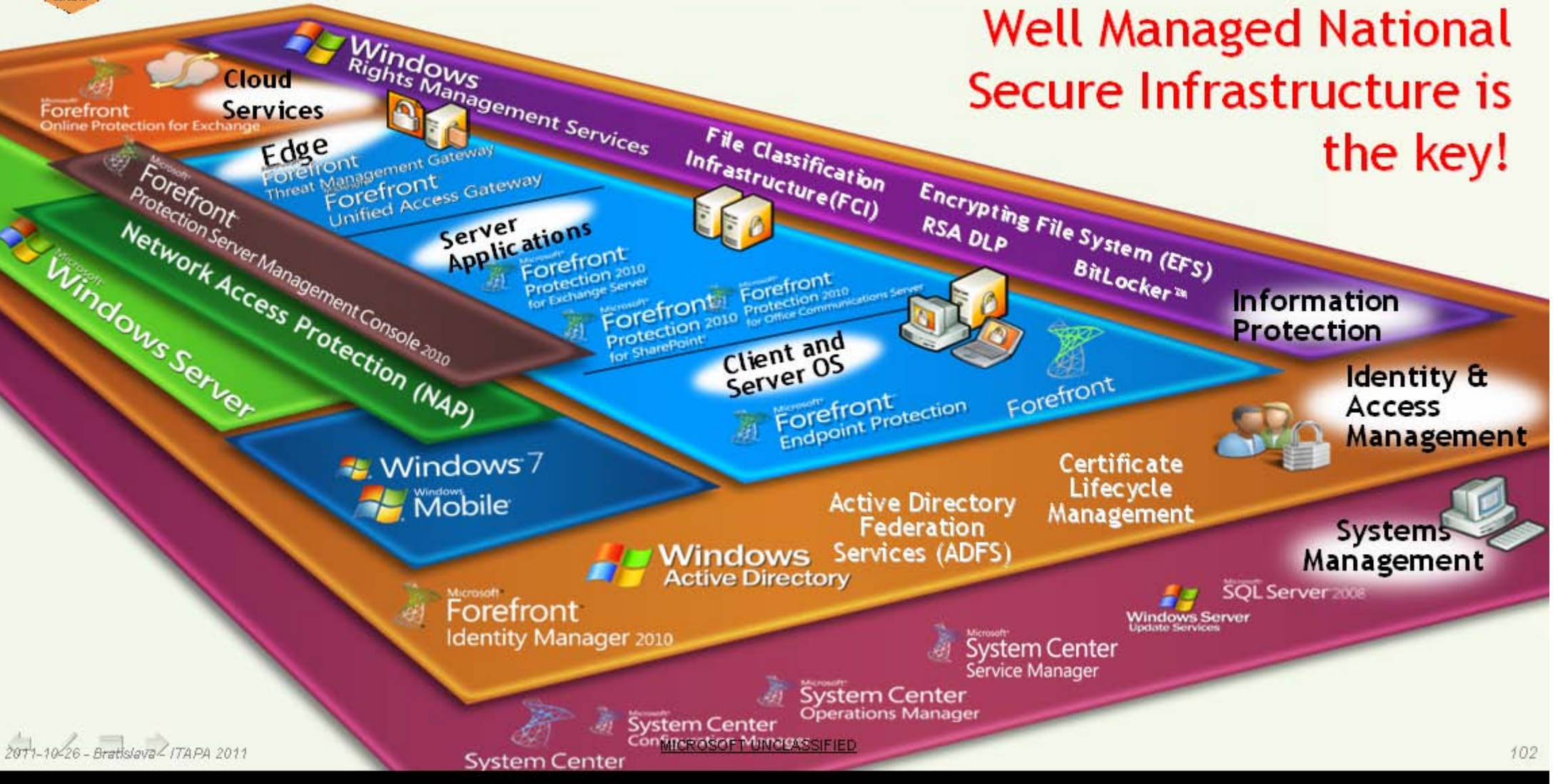
Strategies, mitigations, and countermeasures

- Adjust risk management processes to ensure that operating systems and applications are protected
  - Security Risk Management Guide for IT professionals is available http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/default.mspx
- Free prescriptive guides for IT professionals
  - http://www.microsoft.com/technet/security/guidance/default.mspx
- Participate in IT security communities
  - Example: The Microsoft IT Pro Security Zone community
  - http://technet.microsoft.com/security
- Subscribe to the Microsoft Security Newsletter
  - http://www.microsoft.com/technet/securitysecnews/default.mspx

Conclusion on National (Infrastructure) Security ...

National (Infrastructure) Security is a key ☺ … but …

Well Managed National Secure Infrastructure is the key!



Contact info:

Robert Kosla, Lt.Col. (Ret.)

E-mail: robert.kosla@microsoft.com
Phone: +49 89 31765821

Microsoft®
Your potential. Our passion.™