Collective Defense
How the defenders are playing to win!

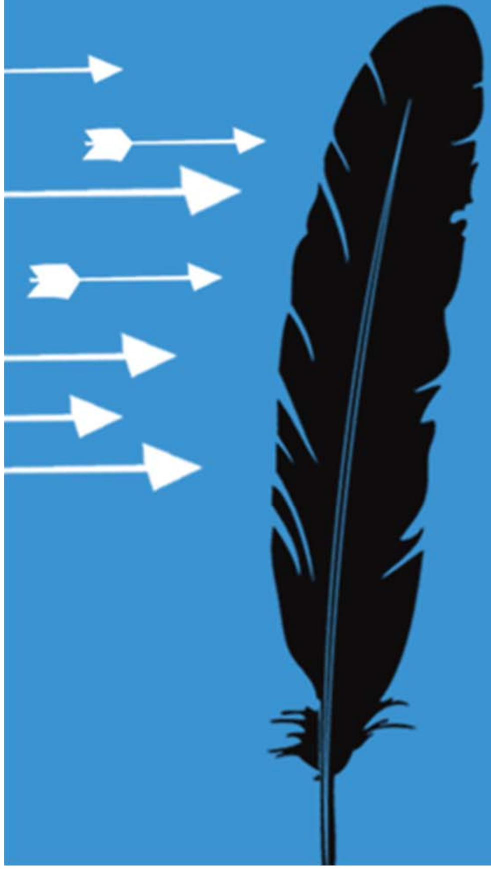
Maarten Van Horenbeeck

Microsoft Corporation

Session ID: GRC-304

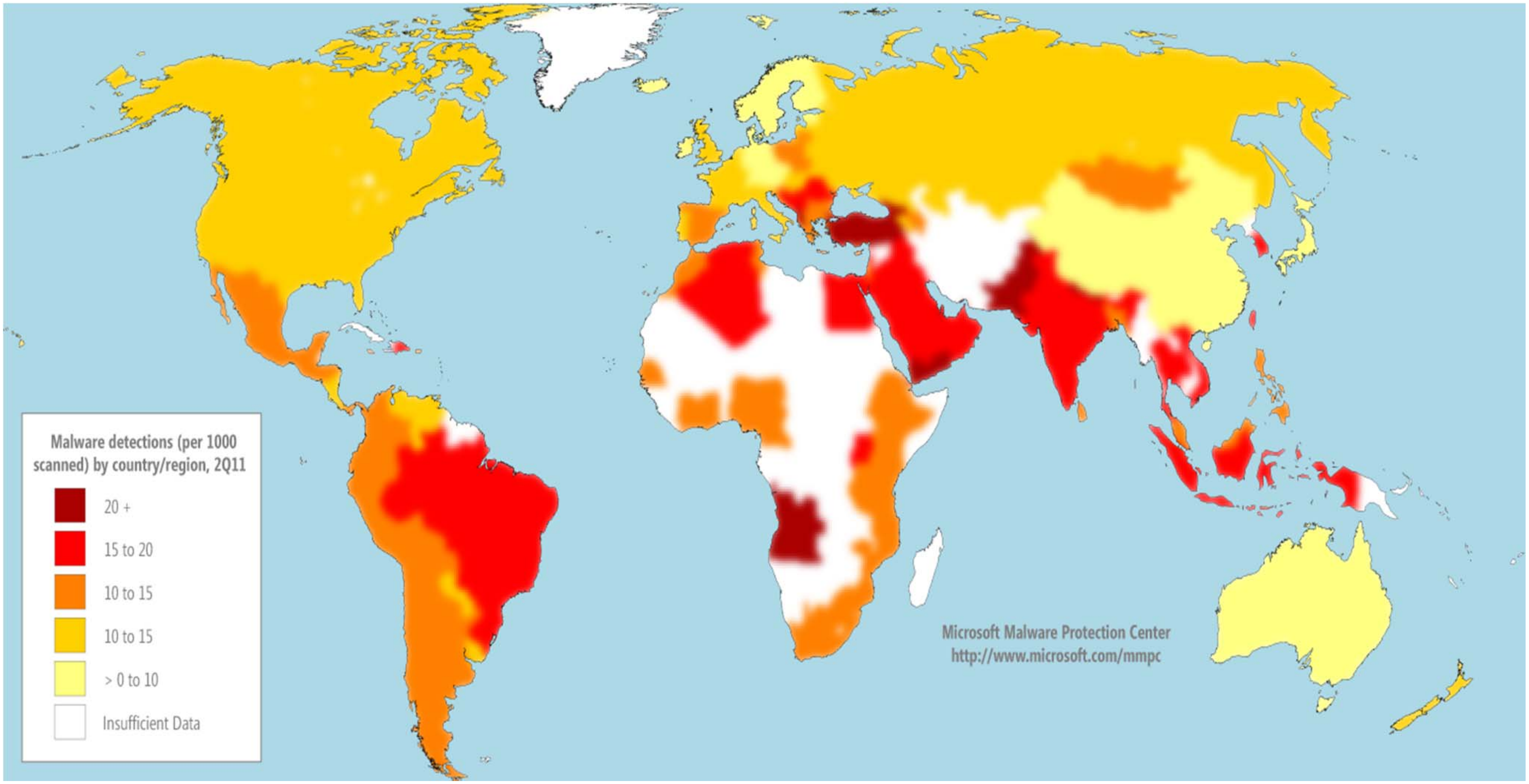
Session Classification: Intermediate

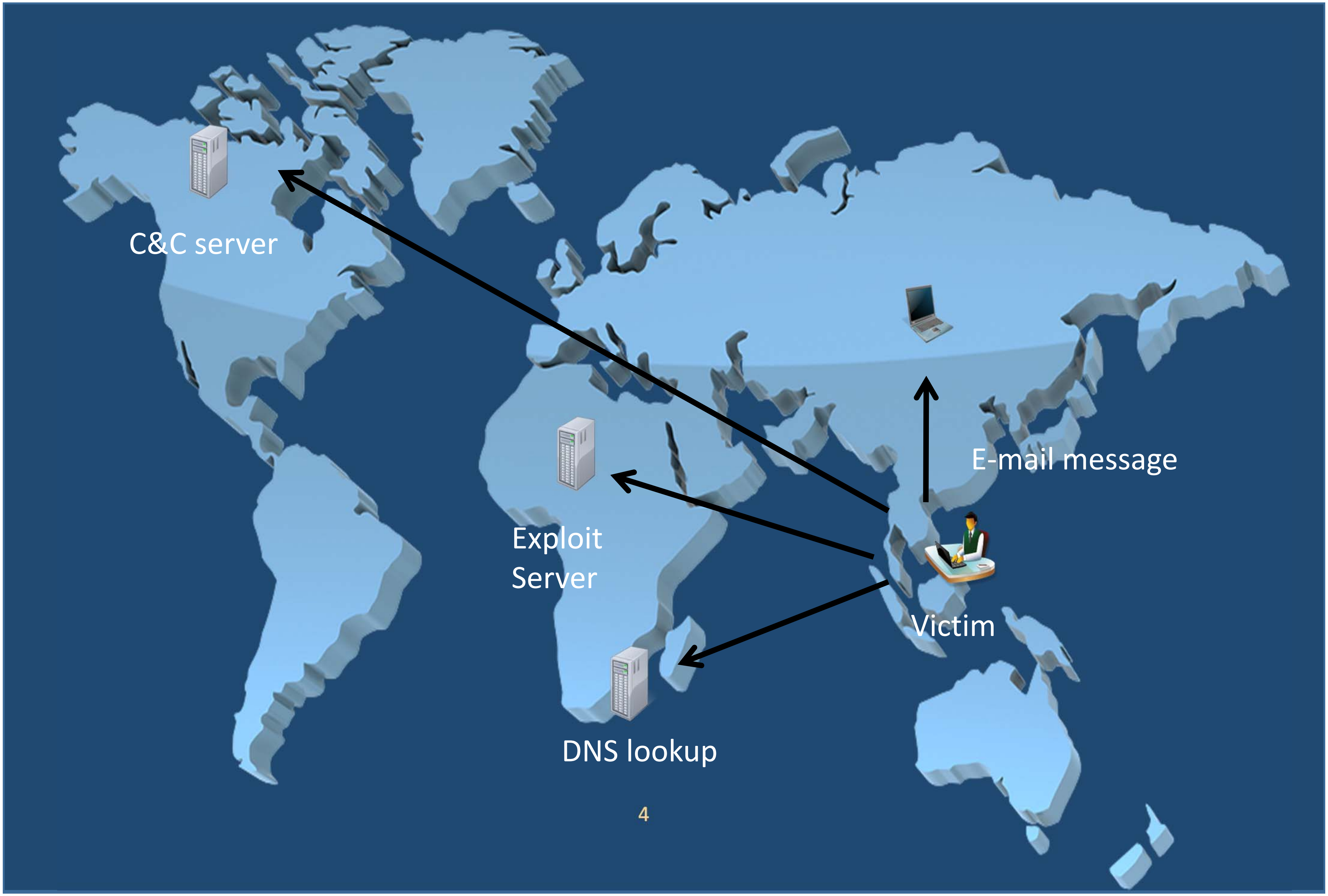
RSACONFERENCE2012

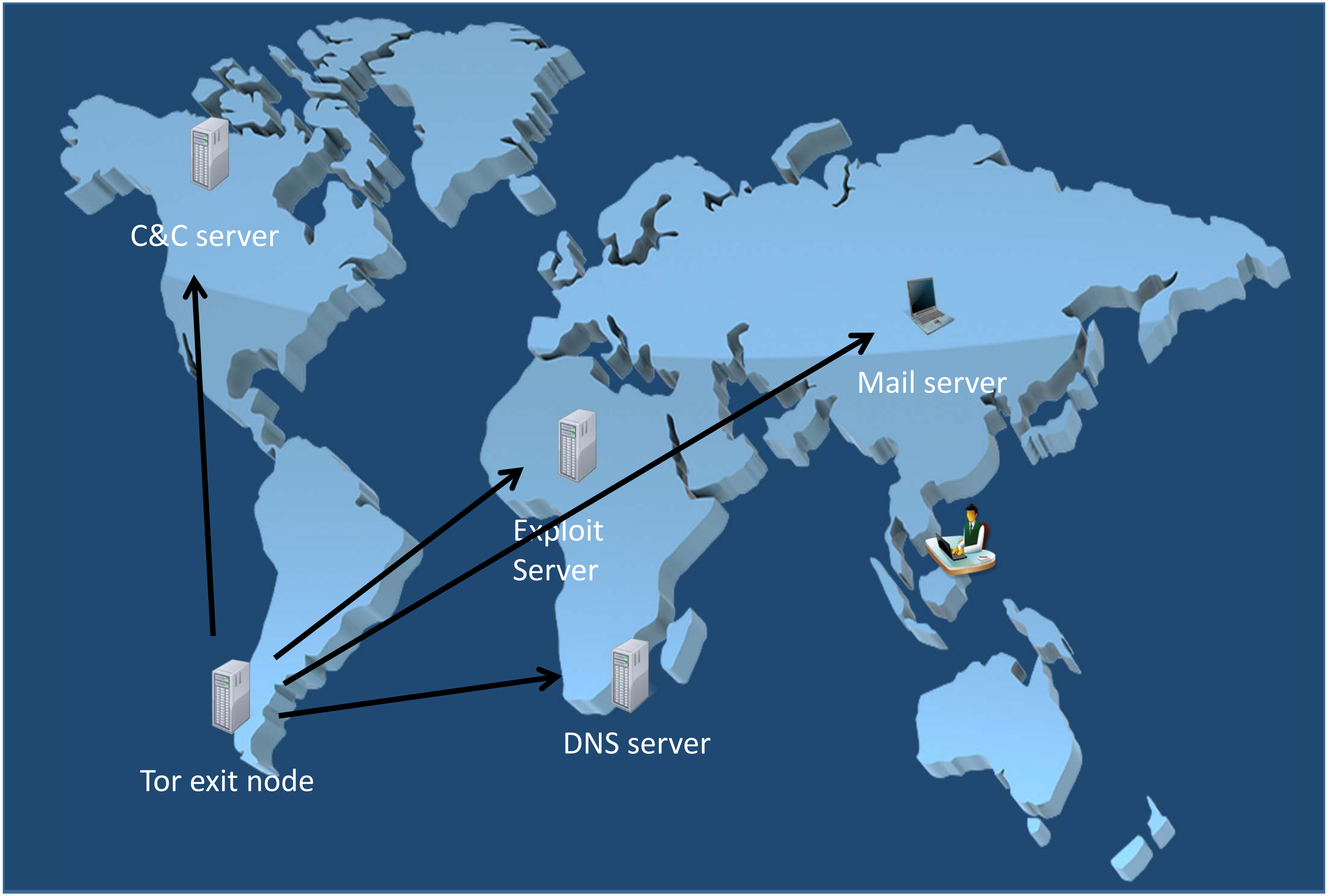


The security problem

It’s global


Malware detections (per 1000 scanned) by country/region, 2Q11
20 +
15 to 20
10 to 15
10 to 15
> 0 to 10
Insufficient Data
Microsoft Malware Protection Center
http://www.microsoft.com/mmpc


C&C server
E-mail message
Exploit
Server
Victim
DNS lookup


C&C server
Mail server
Exploit
Server
DNS server
Tor exit node

Disrupting the incident lifecycle

Security Partner

CERT Teams

Microsoft

Security Updates
Exploitability Information
Prioritization Information
Protection Signatures
Customer Guidance

Disrupting the incident lifecycle

Security Partner

CERT Teams

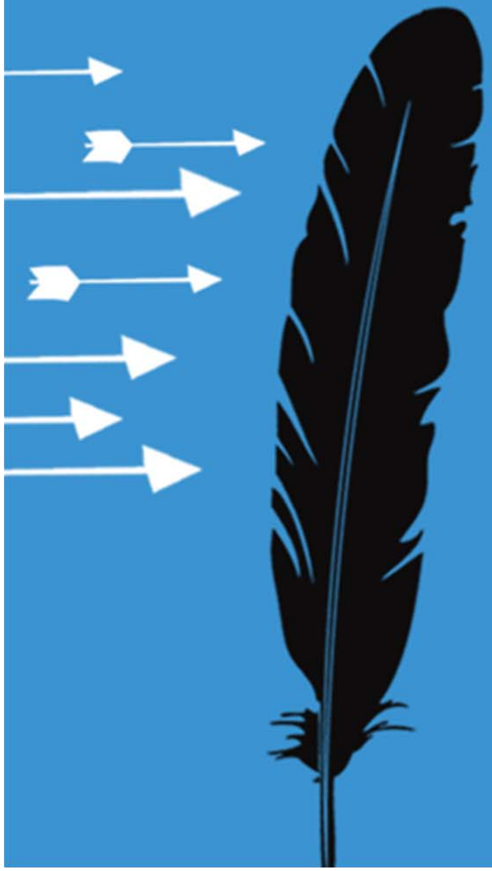
Protection Signatures
Customer Guidance
Threat Intelligence

Microsoft

Disrupting the incident lifecycle

Constituency Awareness
Local Relationships
Technical Expertise
Customer Guidance

Microsoft



Finding partners

A history of collective defense

- In 2005, Microsoft Hotmail launched Simple Network Data Services (SNDS)

- Early 2007, Microsoft realized that we had an immense amount of vulnerability related data which could be leveraged to protect users;

- In 2008, we formally launched a set of programs to help partners and customers protect themselves better.
  - Microsoft Active Protections Program
  - Exploitability Index
  - Microsoft Vulnerability Research Program

Simple Network Data Services

IP Address [?]	Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FROM [?]	Comments [?]
Total: 4 IPs		88,246	55,643	79,969	2 Red IPs	2%		97			
5.16.xx.xx	5/22/2005 12:00 AM - 5/23/2005 12:00 AM	12752	9346	12752	YELLOW	0.3%	5/22/2005 1:53 AM - 5/22/2005 8:38 PM	6	mail3.provider.com	customer@provider.com	
5.16.xx.xx	5/22/2005 12:00 AM - 5/23/2005 12:00 AM	43725	29751	36471	RED	3%	5/22/2005 12:02 AM - 5/22/2005 10:33 PM	54	host-5-16-104-146.provider.com	fake@hotmail.com	
5.16.xx.xx	5/22/2005 10:00 AM - 5/22/2005 11:00 PM	132	110	132	GREEN	< 0.1%		0	mail.contoso.com	dad@contoso.com	
5.16.xx.xx	5/22/2005 12:00 AM - 5/23/2005 12:00 AM	31637	16436	30614	RED	2%	5/22/2005 1:29 AM - 5/22/2005 6:14 PM	37	host-5-16-134-242.provider.com	fake2@hotmail.com	
Total: 4 IPs		88,246	55,643	79,969	2 Red IPs	2%		97			

Incident Response at Microsoft

Vulnerability Reporting

- MSRC receives incoming vulnerability reports through
  - Secure@Microsoft.com – Direct contact with MSRC
  - Microsoft TechNet Security Site – anonymous reporting
- MSRC responds to all reports
  - 24 hour response Service Level Agreement to finder
  - Internal response can be immediate when required

Triaging

- Assess the report and the possible impact on customers
- Understand the severity of the vulnerability
- Rate the vulnerability according to severity and likelihood of exploit, and assign it a priority

Investigation

- MSRC Engineering
  - Reproduce the Vulnerability
  - Locate variants
  - Investigate surrounding code and design

Managing Finder Relationship

- Establish communications channel
  - Quick response
  - Regular updates
- Build the community
- Encourage responsible reporting

Fix Validation

- MSRC Engineering and Product Team
  - Test against reported issue
  - Test against variants

Content Creation

- Security bulletin
  - Affected software/components
  - Technical description
  - FAQs
  - Acknowledgments

Technical guidance

- MSRC Engineering
  - Workarounds and mitigations
  - SVRD blog
  - MAPP detection guidance

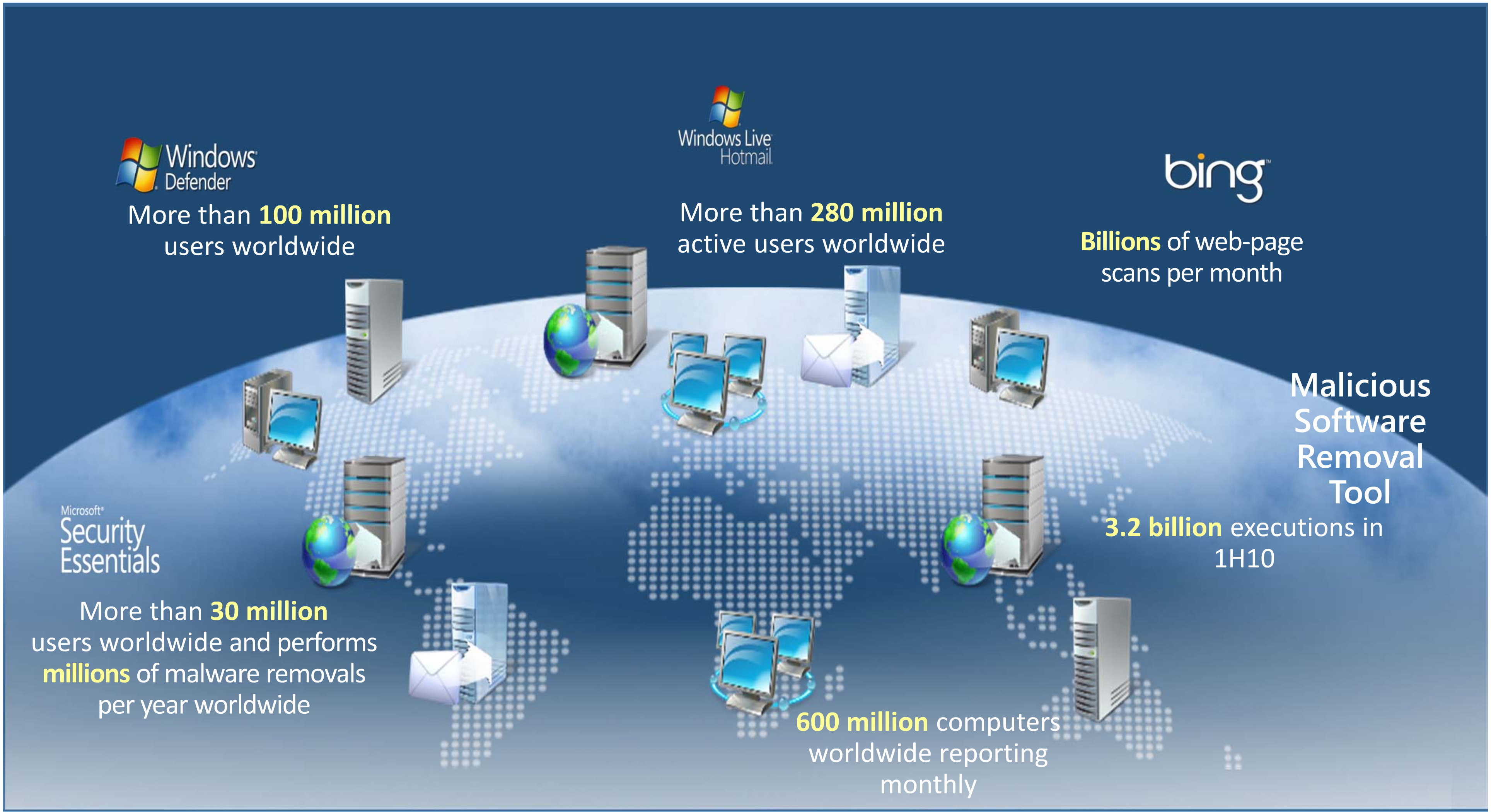
Release

- Security bulletins – second Tuesday of every month
- Coordinate all content and resources
- Information and guidance to customers
- Monitor customer issues and press

Update Developer Tools and Practices

- Update best practices
- Update testing tools
- Update development and design process

Incident Response at Microsoft



More than **100 million** users worldwide

More than **280 million** active users worldwide

Billions of web-page scans per month

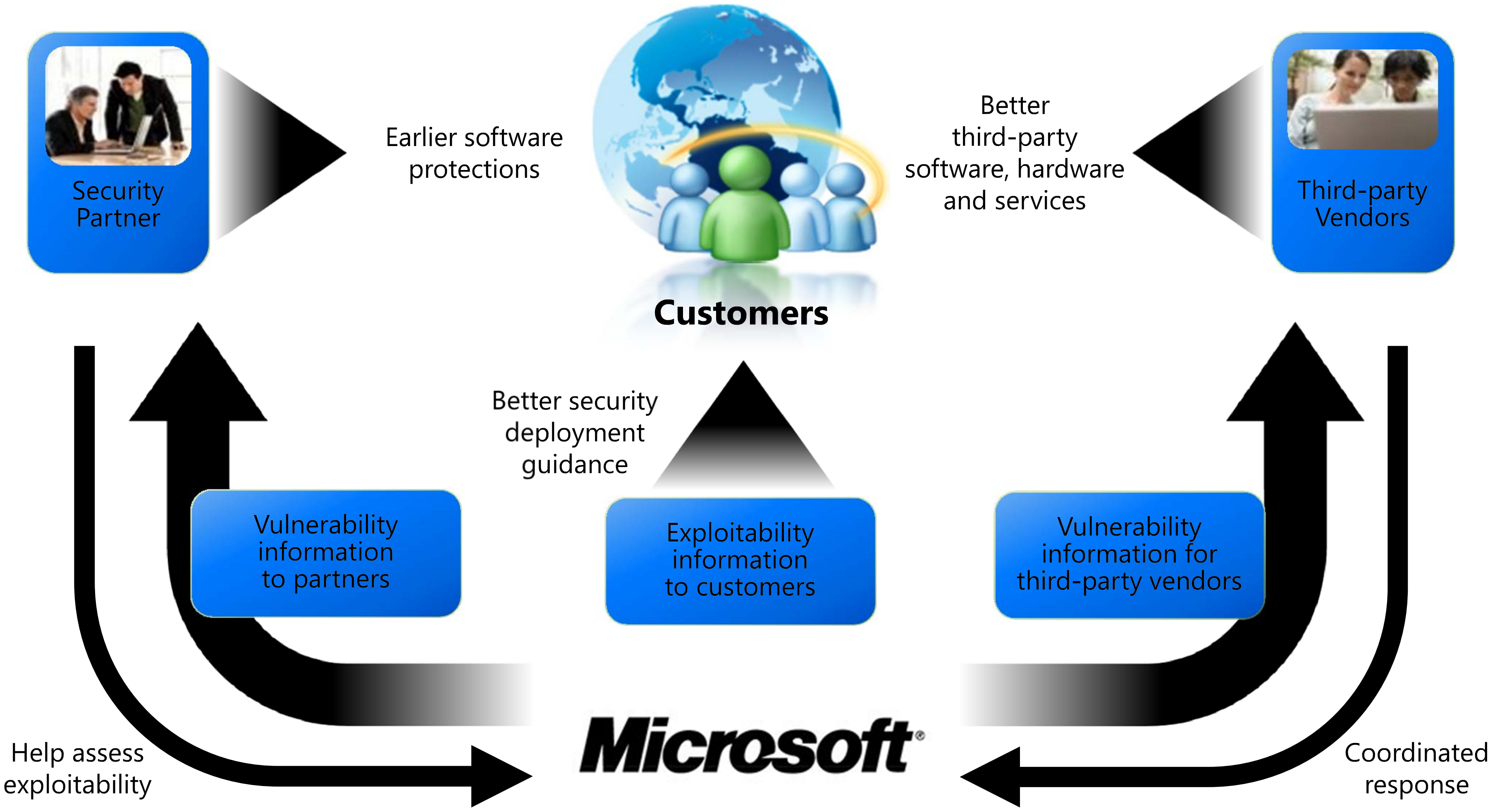
Malicious Software Removal Tool

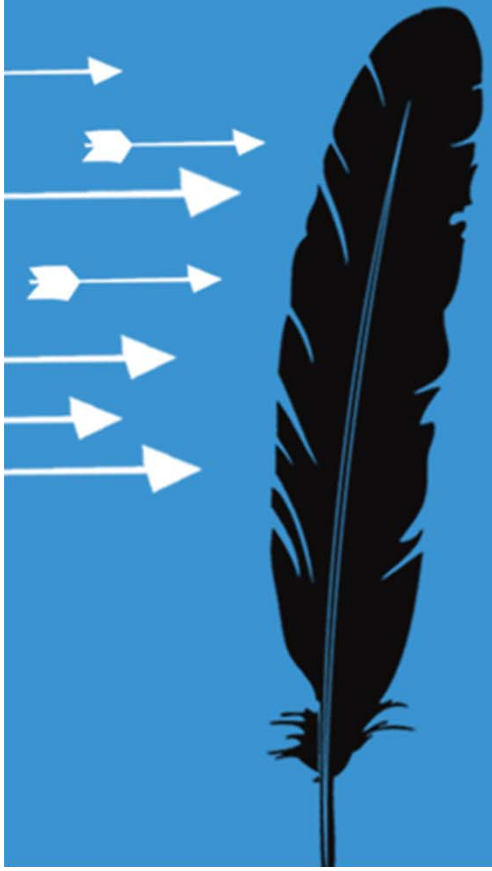
3.2 billion executions in 1H10

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

600 million computers worldwide reporting monthly

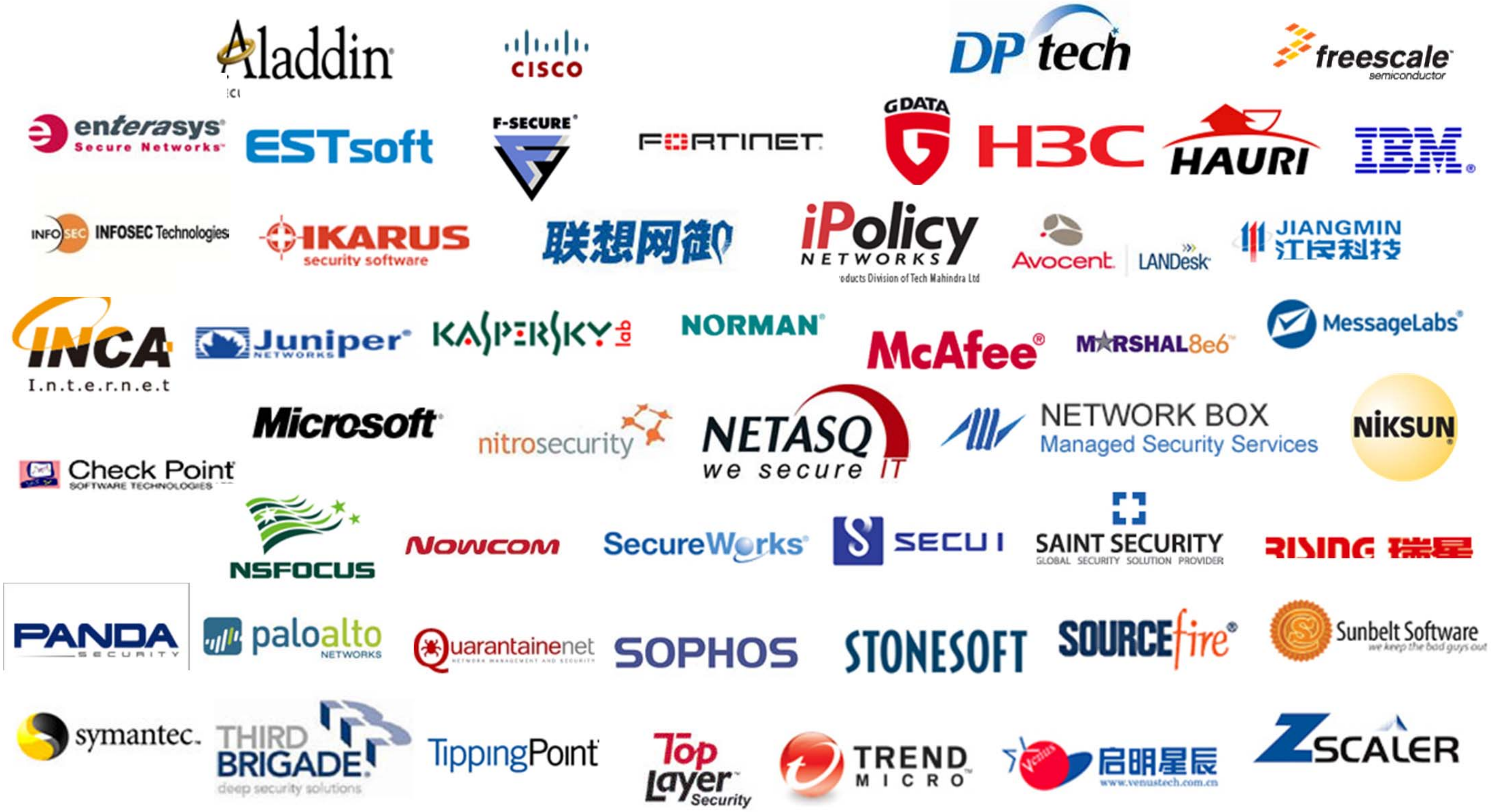
Sharing threat information


Security Partner
Earlier software protections
Customers
Better third-party software, hardware and services
Third-party Vendors
Better security deployment guidance
Vulnerability information to partners
Exploitability information to customers
Vulnerability information for third-party vendors
Help assess exploitability
Microsoft
Coordinated response

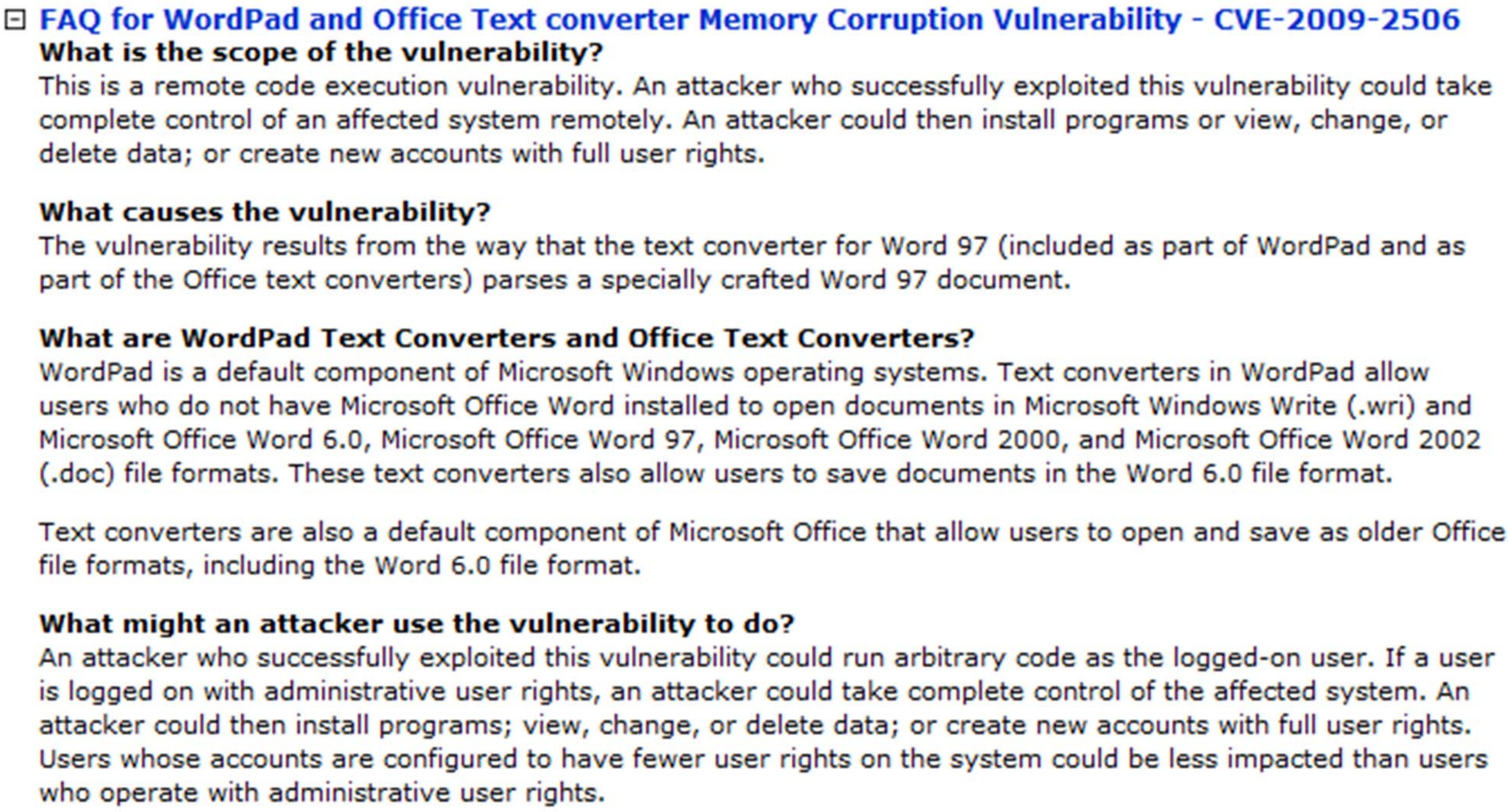


What does sharing look like?

Microsoft Active Protections Program



Microsoft Active Protections Program



⊟ **FAQ for WordPad and Office Text converter Memory Corruption Vulnerability - CVE-2009-2506**

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system remotely. An attacker could then install programs or view, change, or delete data; or create new accounts with full user rights.

What causes the vulnerability?

The vulnerability results from the way that the text converter for Word 97 (included as part of WordPad and as part of the Office text converters) parses a specially crafted Word 97 document.

What are WordPad Text Converters and Office Text Converters?

WordPad is a default component of Microsoft Windows operating systems. Text converters in WordPad allow users who do not have Microsoft Office Word installed to open documents in Microsoft Windows Write (.wri) and Microsoft Office Word 6.0, Microsoft Office Word 97, Microsoft Office Word 2000, and Microsoft Office Word 2002 (.doc) file formats. These text converters also allow users to save documents in the Word 6.0 file format.

Text converters are also a default component of Microsoft Office that allow users to open and save as older Office file formats, including the Word 6.0 file format.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could run arbitrary code as the logged-on user. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

What are Active Protections?

- **Actionable** information that can help protect a Microsoft customer right here, right now.
  - Anti-virus signatures
  - IPS signatures
  - Information on bots and infected hosts

- **Actionable** depends on the audience
  - Governments, protecting their constituency
  - Customers, protecting the enterprise
  - Vendors, protecting their customers

Microsoft Active Protections Program

- Indicators of exploit

  Indicators of exploit include event log entries or other distinguishing markers that would help an administrator identify whether the vulnerability has been exploited against a specific machine.

- Stack trace

  A stack trace helps identify in which component of an application the crash happened. It can be particularly useful in helping identify whether an exploit exploits this particular issue.

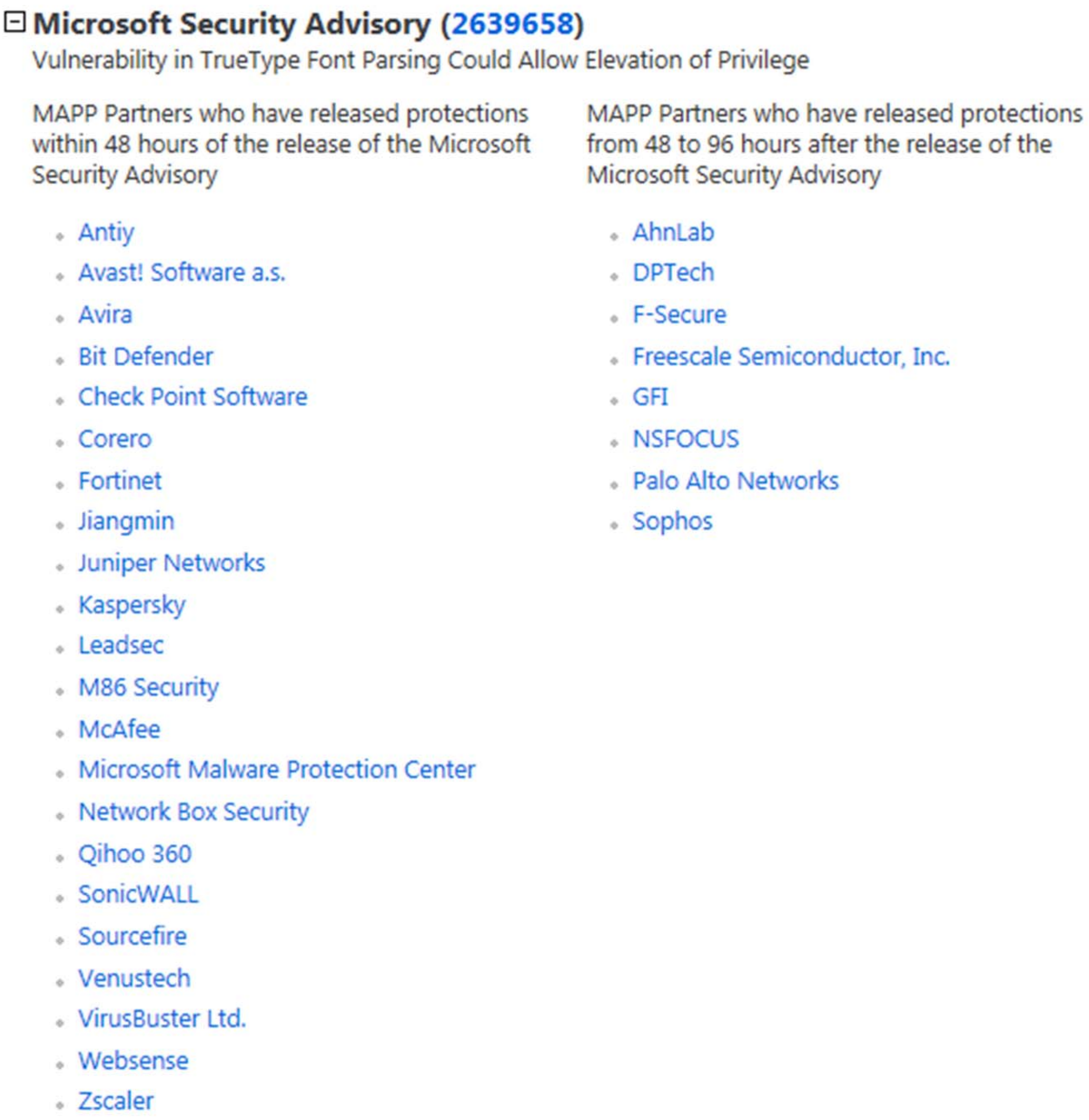
Microsoft Active Protections Program

- Disassembly of the vulnerable code

  The disassembly indicates how the vulnerability truly works, for instance by illustrating how the stack registers are influenced by an operation the vulnerable application performs.

- Proof of Concept file

  The Proof of Concept file, while not an exploit, will allow a security analyst to reproduce the vulnerability locally, and allows him to test existing defenses for effectiveness in blocking the threat.



⊟ Microsoft Security Advisory (2639658)

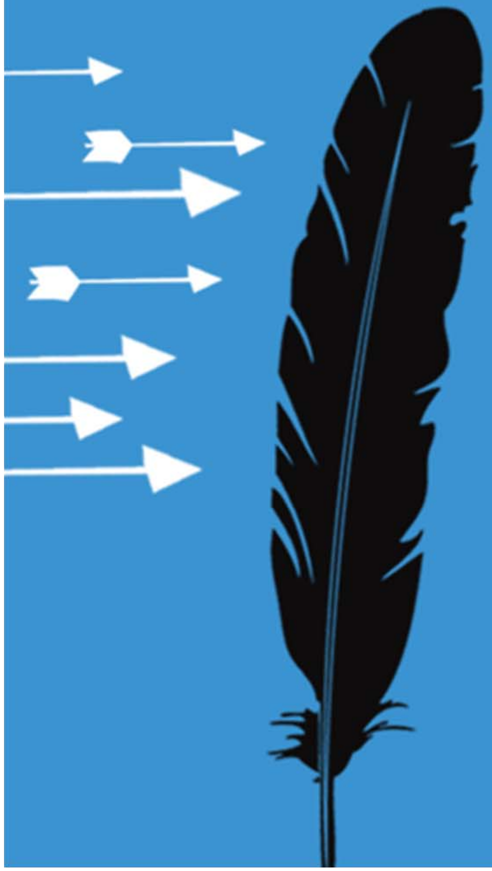
Vulnerability in TrueType Font Parsing Could Allow Elevation of Privilege

MAPP Partners who have released protections within 48 hours of the release of the Microsoft Security Advisory

- Antiy
- Avast! Software a.s.
- Avira
- Bit Defender
- Check Point Software
- Corero
- Fortinet
- Jiangmin
- Juniper Networks
- Kaspersky
- Leadsec
- M86 Security
- McAfee
- Microsoft Malware Protection Center
- Network Box Security
- Qihoo 360
- SonicWALL
- Sourcefire
- Venustech
- VirusBuster Ltd.
- Websense
- Zscaler

MAPP Partners who have released protections from 48 to 96 hours after the release of the Microsoft Security Advisory

- AhnLab
- DPTech
- F-Secure
- Freescale Semiconductor, Inc.
- GFI
- NSFOCUS
- Palo Alto Networks
- Sophos



Sharing partnerships go both ways

The CVE-2010-3333 incident

- MS10-087 released **November 2010**
- First exploits appear **December 28th**
  - Detected by the MMPC, a MAPP partner
  - Limited, targeted attacks
    - Social engineering attempts in Pakistan
    - Anti-malware detection not as good as expected
    - Opportunity to share better information on exploits

The CVE-2010-3333 incident

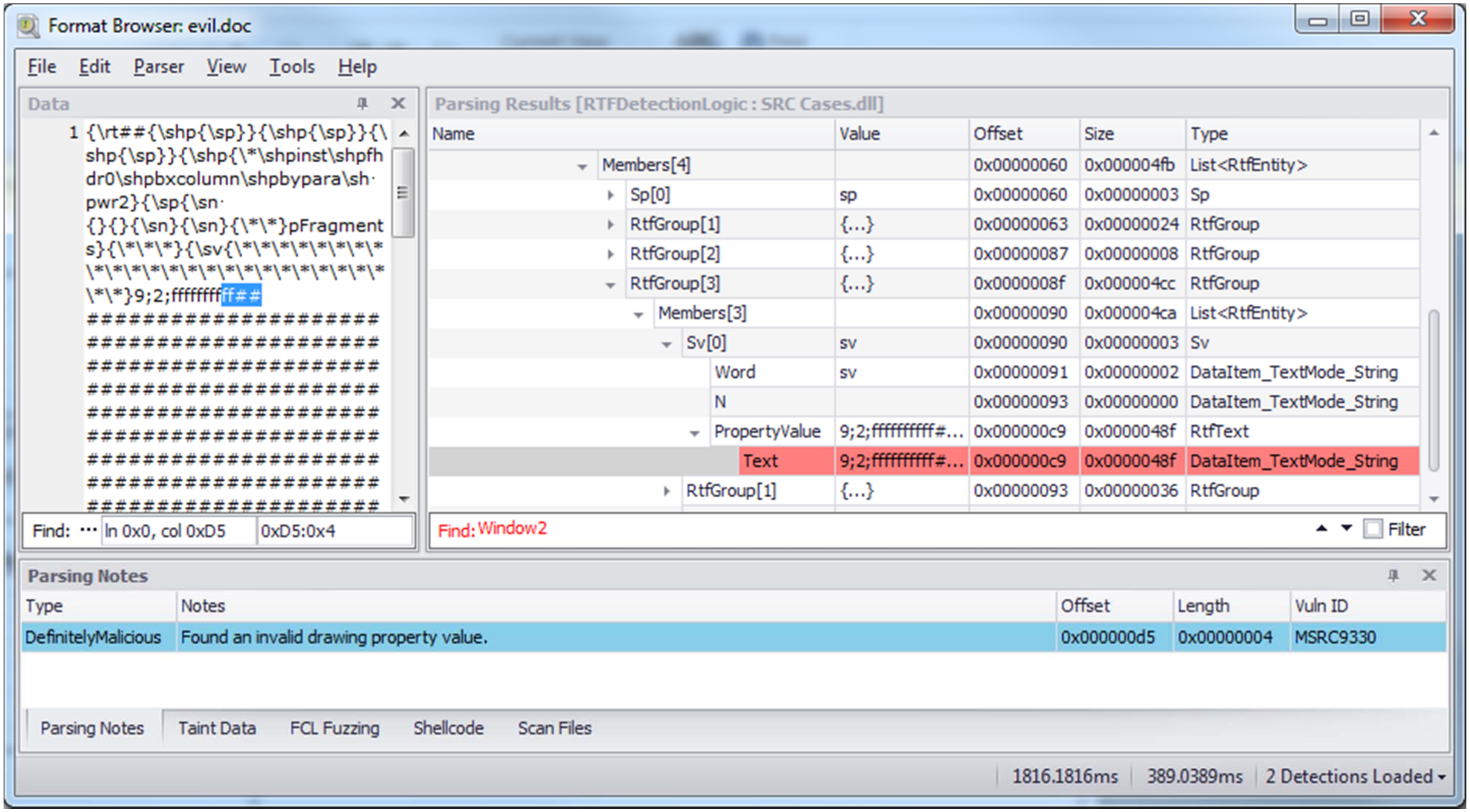
- Look for the following sequence of control words: **\sp** then **\sn pFragments** and then **\sv**

  ```
  {\sp{\sn pFragments}{\sv
  0;0;0123456789AB1111111111111111111111111111111111111111ffffffff}}
  ```

  The parameter to \sv is of particular interest. Start examining the data after the second semicolon - this is hex data. Skip 8 bytes, and examine the next 4 bytes (highlighted in the example above).

  If these 4 bytes, treated as a little endian 16 bit unsigned integer are > 0x4 (don't forget to swap the 2 bytes since it's little endian), then this file attempts to exploit CVE-2010-3333.

The CVE-2010-3333 incident



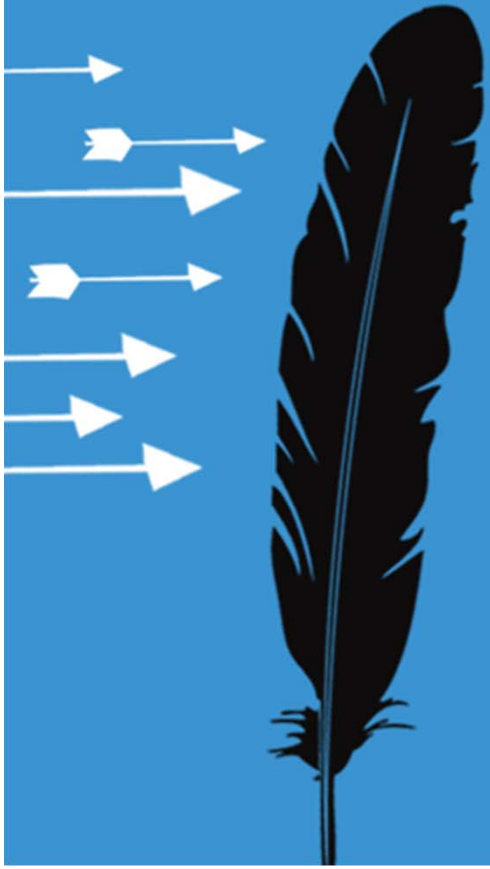
```
{\rt##{\shp{\sp}}{\shp{\sp}}{\
shp{\sp}}{\shp{\*\shpinst\shpfh
dr0\shpbxcolumn\shpbypara\sh·
pwr2}{\sp{\sn·
{}{}{\sn}{\sn}{\*\*}pFragment
s}{\*\*\*}{\sv{\*\*\*\*\*\*\*\*
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
\*\*}9;2;ffffffffff##
#####################
#####################
#####################
#####################
#####################
#####################
#####################
#####################
#####################
```

Find: ··· ln 0x0, col 0xD5 | 0xD5:0x4

Name	Value	Offset	Size	Type
Members[4]		0x00000060	0x000004fb	List<RtfEntity>
Sp[0]	sp	0x00000060	0x00000003	Sp
RtfGroup[1]	{...}	0x00000063	0x00000024	RtfGroup
RtfGroup[2]	{...}	0x00000087	0x00000008	RtfGroup
RtfGroup[3]	{...}	0x0000008f	0x000004cc	RtfGroup
Members[3]		0x00000090	0x000004ca	List<RtfEntity>
Sv[0]	sv	0x00000090	0x00000003	Sv
Word	sv	0x00000091	0x00000002	DataItem_TextMode_String
N		0x00000093	0x00000000	DataItem_TextMode_String
PropertyValue	9;2;ffffffffff#...	0x000000c9	0x0000048f	RtfText
Text	9;2;ffffffffff#...	0x000000c9	0x0000048f	DataItem_TextMode_String
RtfGroup[1]	{...}	0x00000093	0x00000036	RtfGroup

Type	Notes	Offset	Length	Vuln ID
DefinitelyMalicious	Found an invalid drawing property value.	0x000000d5	0x00000004	MSRC9330

1816.1816ms | 389.0389ms | 2 Detections Loaded



Botnet takedowns

Joining hands to protect customers

Operation b49 Feb 2010

Target: *Waledac*

Cleanup Goal: Build relationships and processes to reach customers

Operation b107 Mar 2011

Target: *Rustock*

,

Cleanup Goal: Disinfect systems before attackers can regain control

Microsoft

- Execute of takedown by the Microsoft MARS team and partners, provide data, resources and tooling.

CERTs

- Amplify reach to global partners

ISPs

- Notify impacted customers

End Users

- Take an active role in keeping their devices secure

Joining hands to protect customers

Operation b49

Feb 2010

Target: *Waledac*

Cleanup Goal: Build relationships and processes to reach customers

ISP Results

Network	Reduction
1	97%
2	96%
3	93%
4	78%
5	82%
6	66%

Country Results

Country	Reduction
KR	80%
TH	71%
RU	68%
ES	62%
PL	60%
AU	56%

Status

~22,000 infected IPs remaining

~70% reduction world wide

Operation b107

Mar 2011

Target: *Rustock*

Cleanup Goal: Disinfect systems before attackers can regain control

Enhancements:

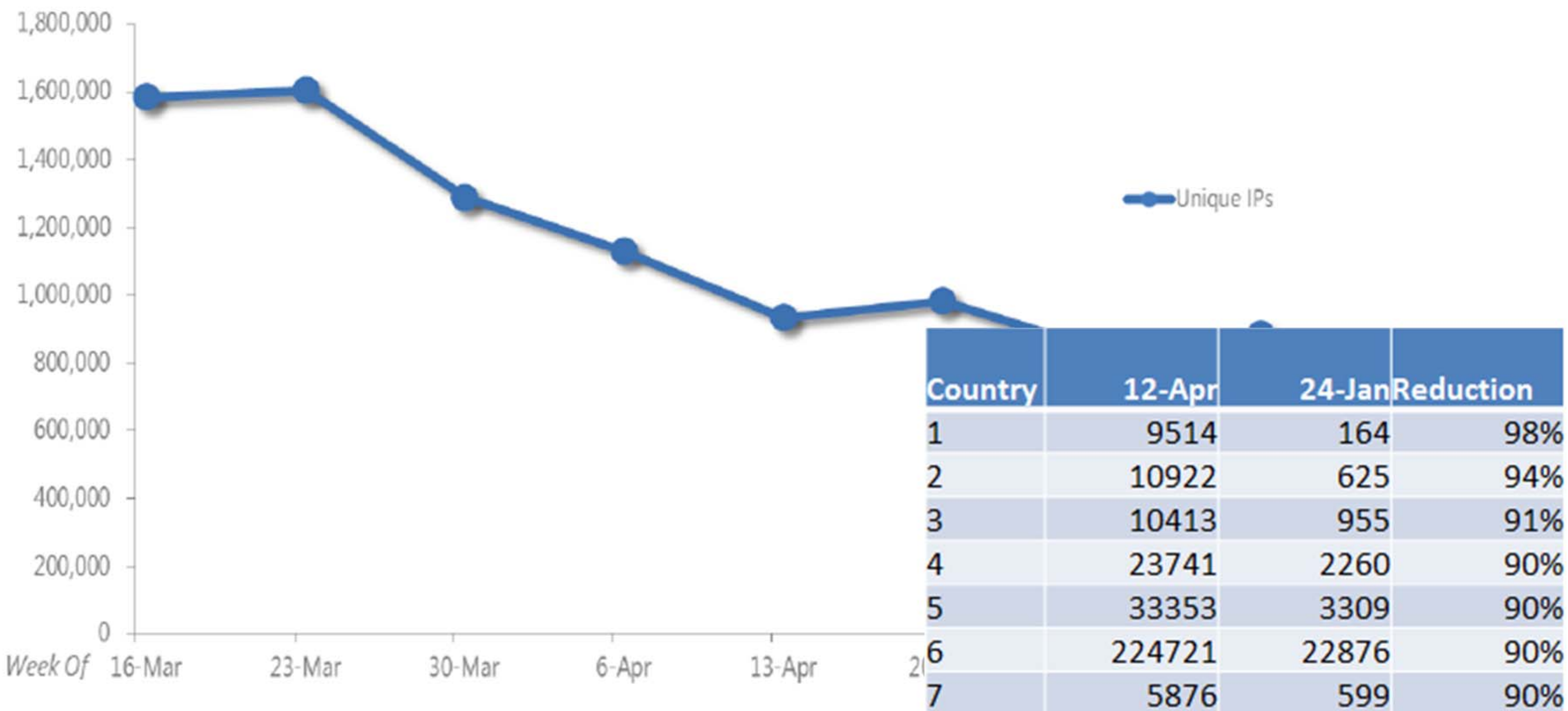
- Expanded Remediation
- Removal Tools
- Updated support site
- SNDS

Target

70% reduction within 60 days

Operation b107

Figure 8. Unique IP addresses contacting the Rustock sinkhole during the first 8 weeks after the takedown, by week

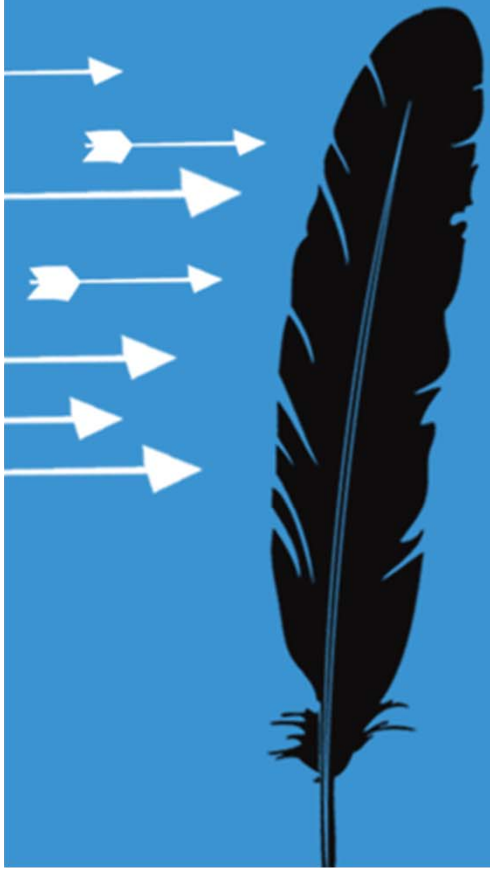


Country	12-Apr	24-Jan	Reduction
1	9514	164	98%
2	10922	625	94%
3	10413	955	91%
4	23741	2260	90%
5	33353	3309	90%
6	224721	22876	90%
7	5876	599	90%
8	1898	202	89%
9	68399	9056	87%
10	32454	4307	87%

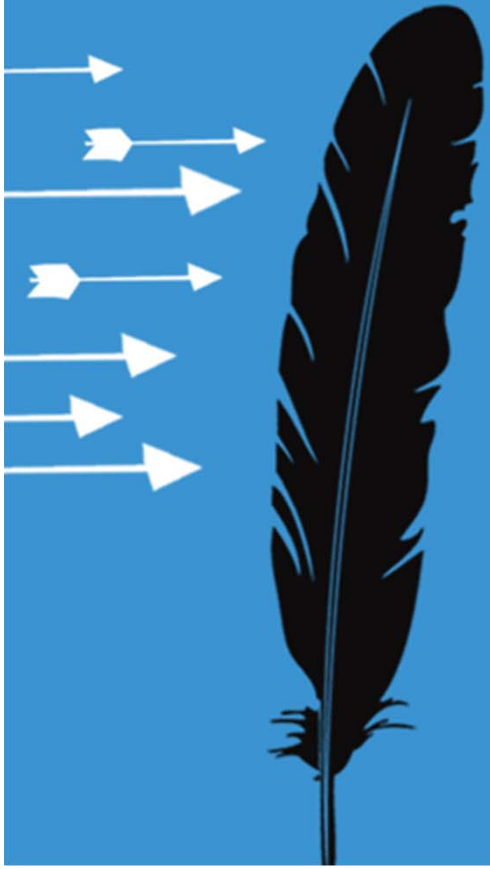
Operation b107 remediation

- US-based Internet Service Providers

ArCERT, *Argentina*
CERT.AT, *Austria*
Cert.BE, *Belgium*
CERT-BR, *Brazil*
CERT-EE, *Estonia*
CERT-FI, *Finland*
CERT.LV, *Latvia*
CERT-UA, *Ukraine*
CNCERT, *China*
Federal Office for Information Security (BSI), *Germany*
GovCERT.nl, *The Netherlands*
GovCertUK, *United Kingdom*
HKCERT, *Hong Kong*
INTECO CERT, *Spain*
JPCERT/CC, *Japan*
MYCERT, *Malaysia*
PISA CERT, *Pakistan*
Public Safety Canada – CCIRC, *Canada*
Sri Lanka CERT|CC, Sri Lanka
CERT-SA, *Saudi Arabia*
ThaiCERT, *Thailand*
TwCERT/CC, *Taiwan*



Where do we go from here?



What can I do?

How to apply what I learned here today?

- When you get back into the office

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

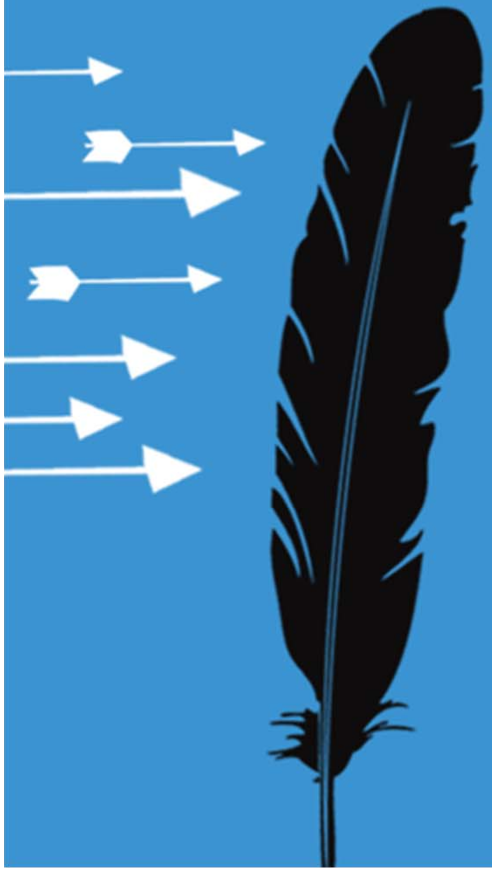
Avoid downloading pirated software

Protect yourself from social engineering attacks

- Enroll in SNDS!
  http://postmaster.live.com/snds

How to apply what I learned here today?

- Within the next 3 months:
  - Identify what type of information would help you better protect your organization.
  - Identify what information your organization has that may help protect other organizations.
  - Identify legal means to share information on attacks.
  - Build a good relationship with your regional CERT, ISAC, Anti Virus vendor and Internet Service Provider.



Got vulns?

secure@microsoft.com