SECURITY CASE STUDY 2014

How the largest botnets were been taken down – the case studies

Robert Kośla, Lt.Col. (Ret.)
Microsoft Central and Eastern Europe HQ

Microsoft

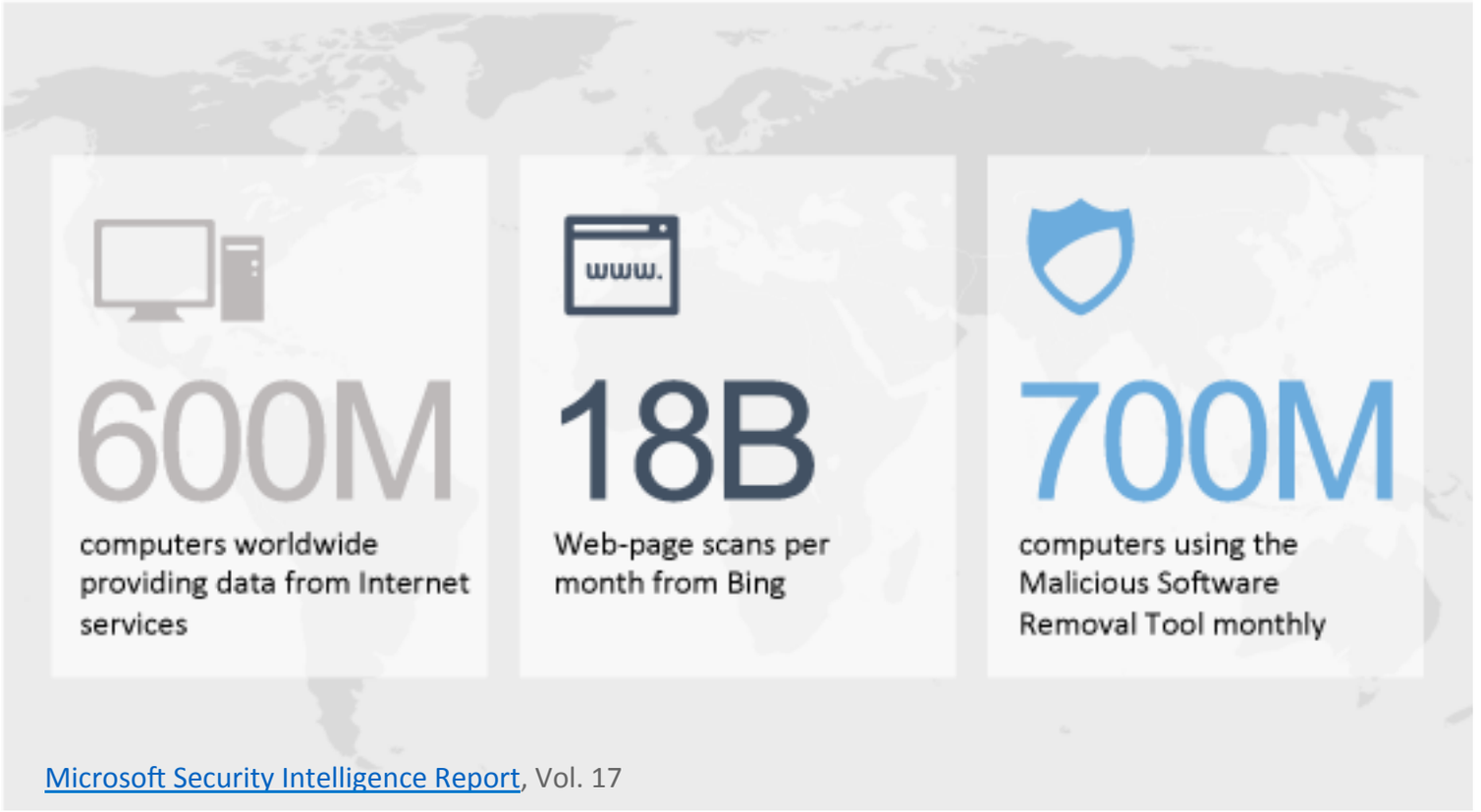
SCS 2014

Global Threats Understanding

Deep understanding of today's threats

Microsoft Security Intelligence Report

In-depth analysis of the threat landscape of exploits, vulnerabilities, and malware



Microsoft Security Intelligence Report, Vol. 17

Security Intelligence Report

"Encounter rate: a new metric for analyzing malware prevalence"

Worldwide threat assessment

Vulnerability trends

Exploit trends

- O/S, browser, and applications

Malware

Potentially unwanted software

Email threats

Malicious websites

Regional threat assessment

100+ countries/regions

www.microsoft.com/sir

Security Intelligence Data Sources

Product name	Main customer segment		Malicious software		Spyware and 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 8 Defender	•		•	•	•	•	•	Windows 8
Windows Safety Scanner	•		•		•		•	Cloud
Microsoft Security Essentials	•		•	•	•	•	•	Cloud
Exchange Online Protection		•	•	•				Cloud
System Center Endpoint Protection		•	•	•	•	•		Volume licensing

- Outlook.com—more than 400 million users.
- Internet Explorer—the world's most popular browser with SmartScreen, Microsoft Phishing filter.
- Exchange Online Protection—scans billions of email messages a year.
- Windows Malicious Software Removal Tool—executes on more than 600 million unique computers worldwide each month
- Microsoft Security Essentials—available in over 30 languages.
- Bing—billions of webpages scanned each month.

Encounter rate (ER)

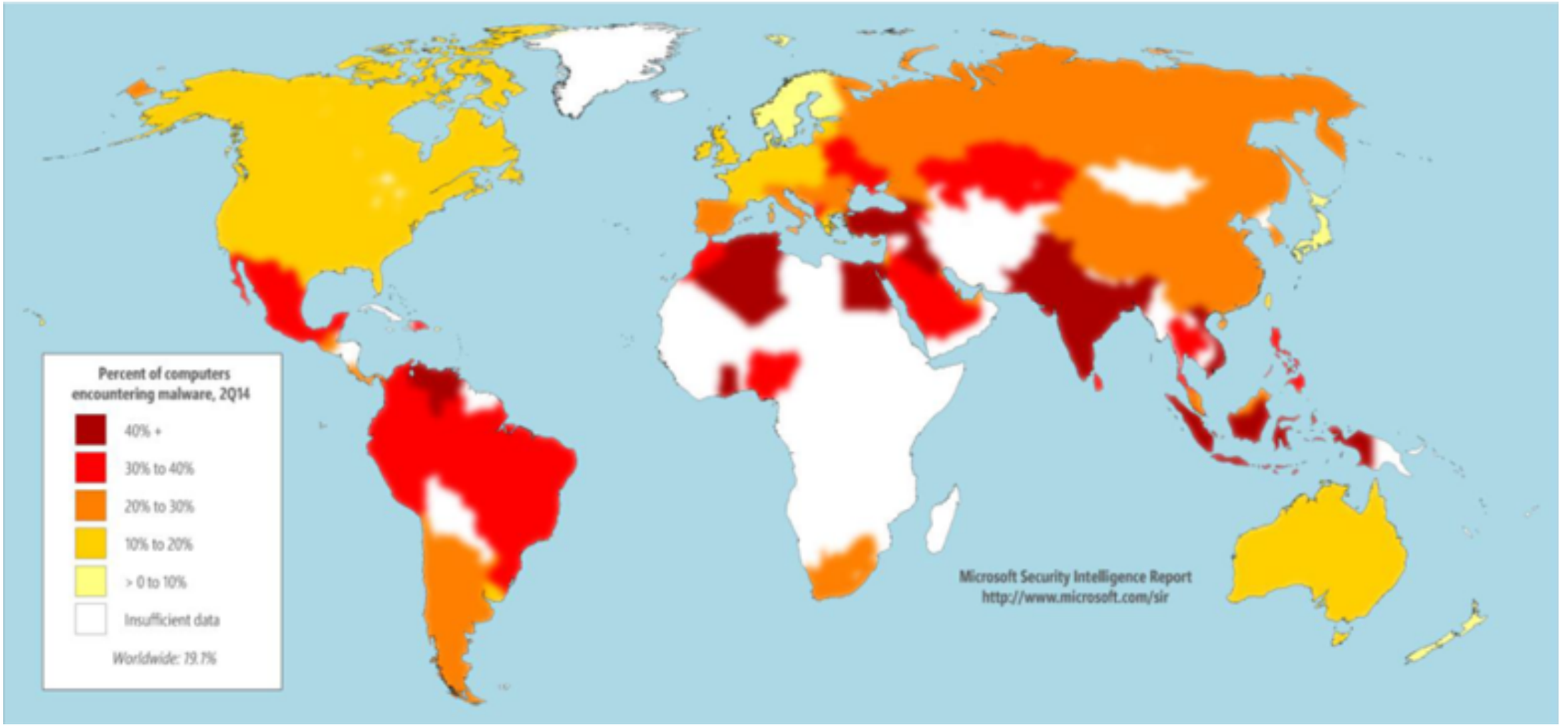
A measure of malware prevalence

Percent of computers encountering malware

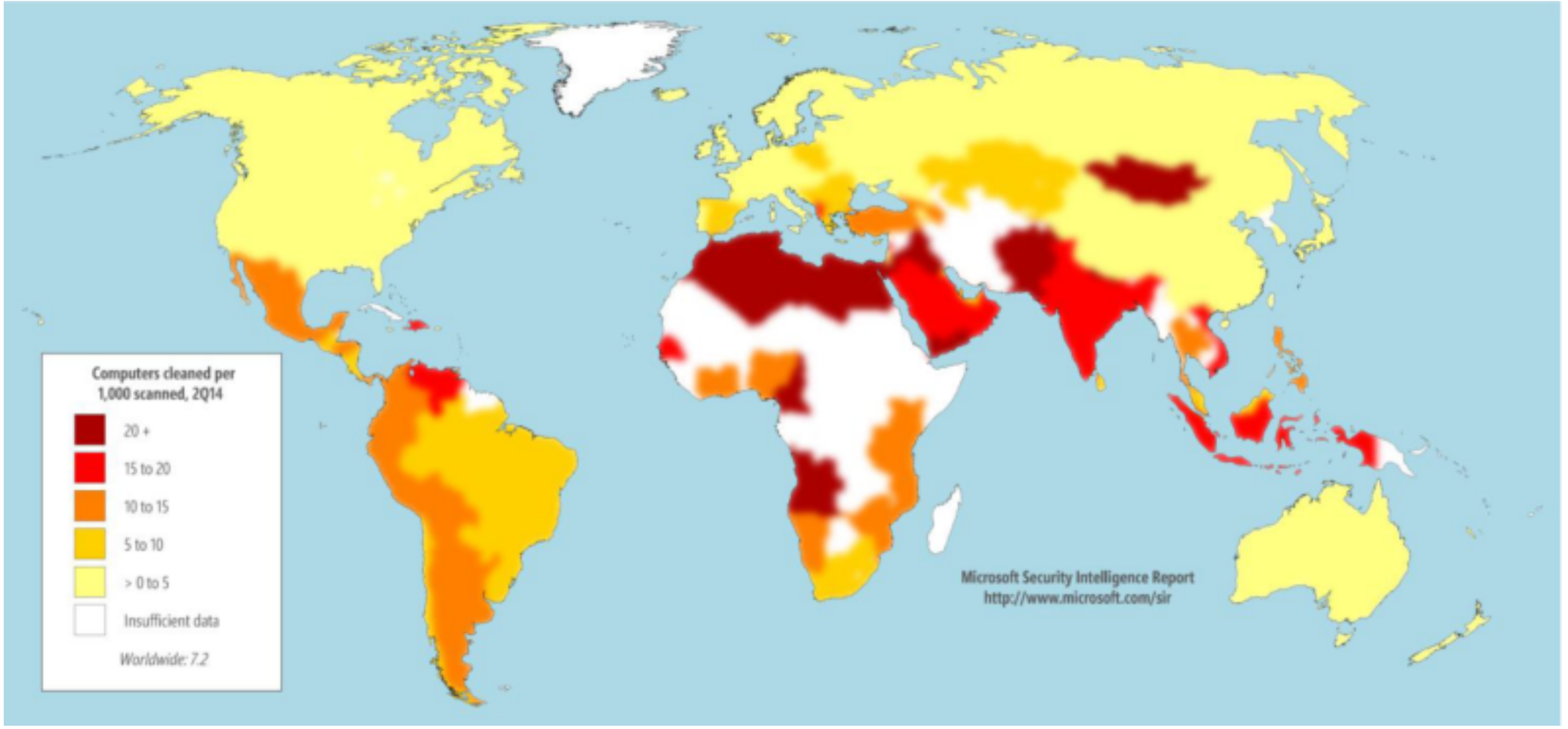
Microsoft antimalware products detect malware or malicious activity

Includes blocks and infections

Encounter rate (ER)

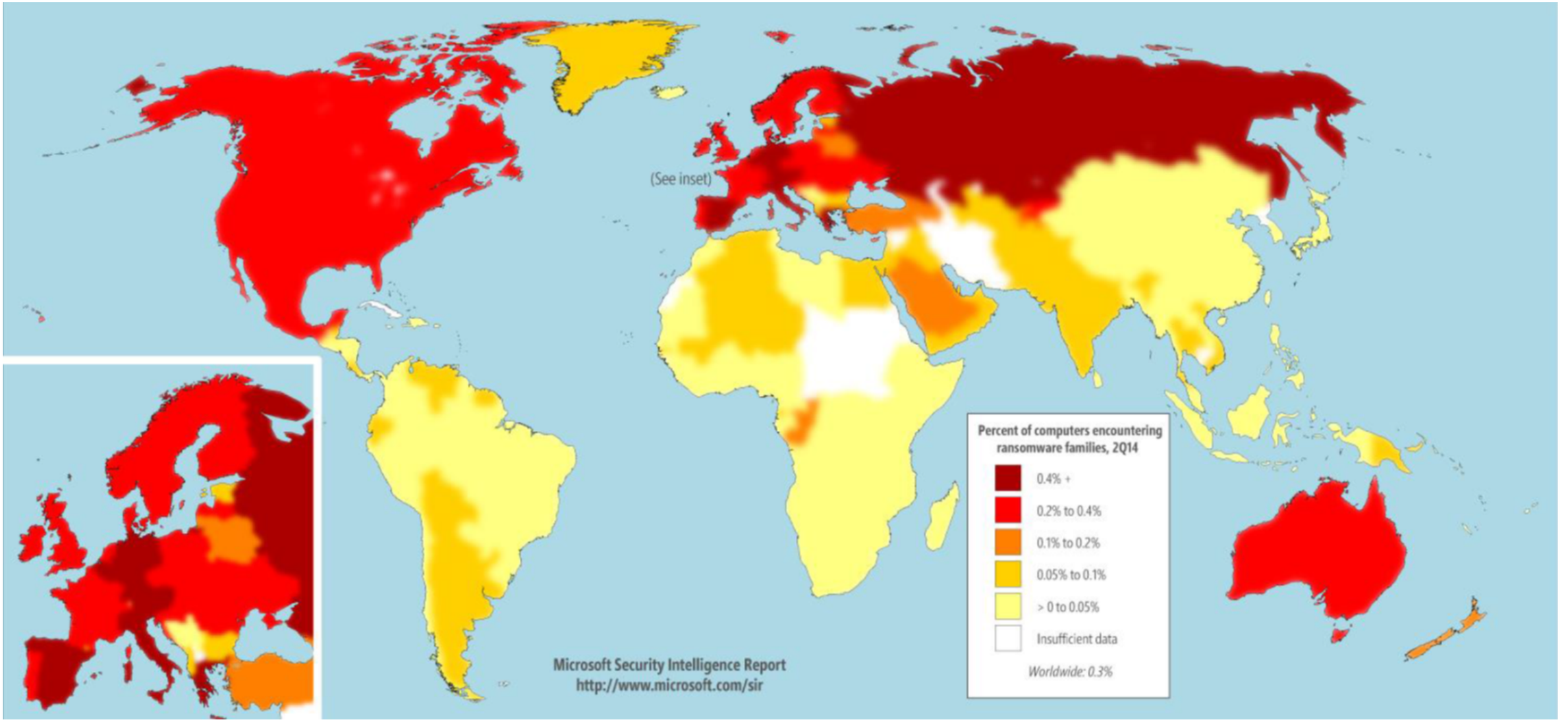


Computer Cleaned per 1.000 scanned (CCM)

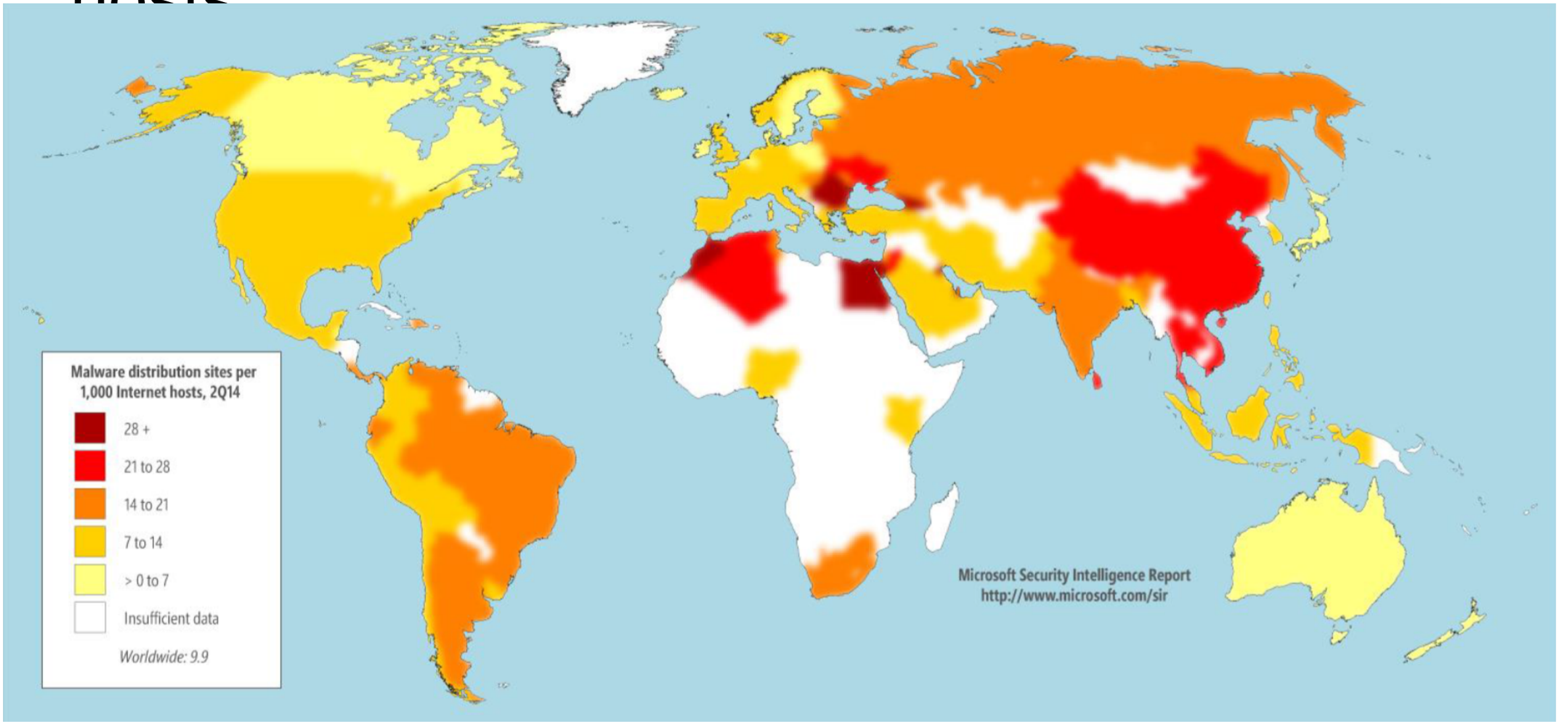


Ransomware sample screenshots

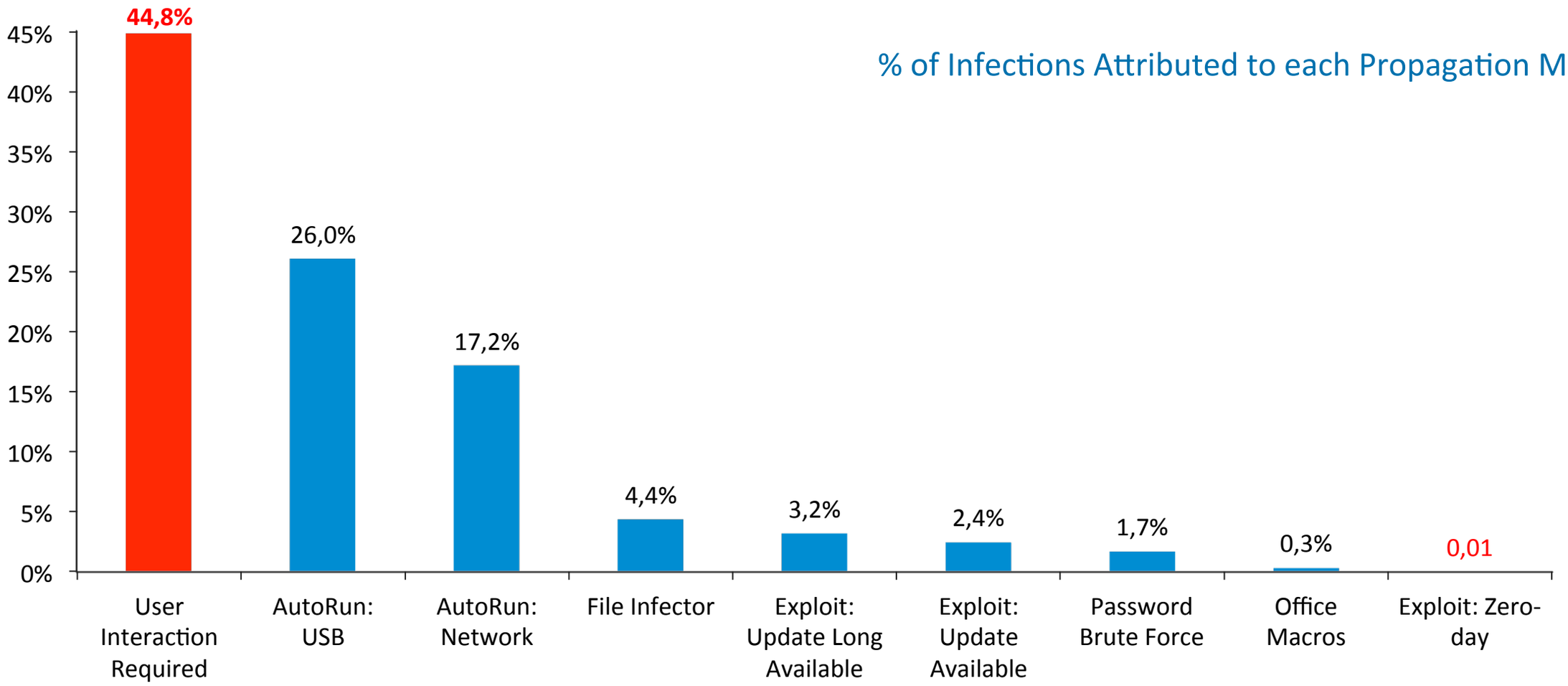
Encounter rates for ransomware families



Malware distribution sites per 1,000 Internet hosts



Zero-day percentage within successful infections



User interaction was attributed to nearly half (45%) of all infections (Zero-day 0.01%)

SCS 2014

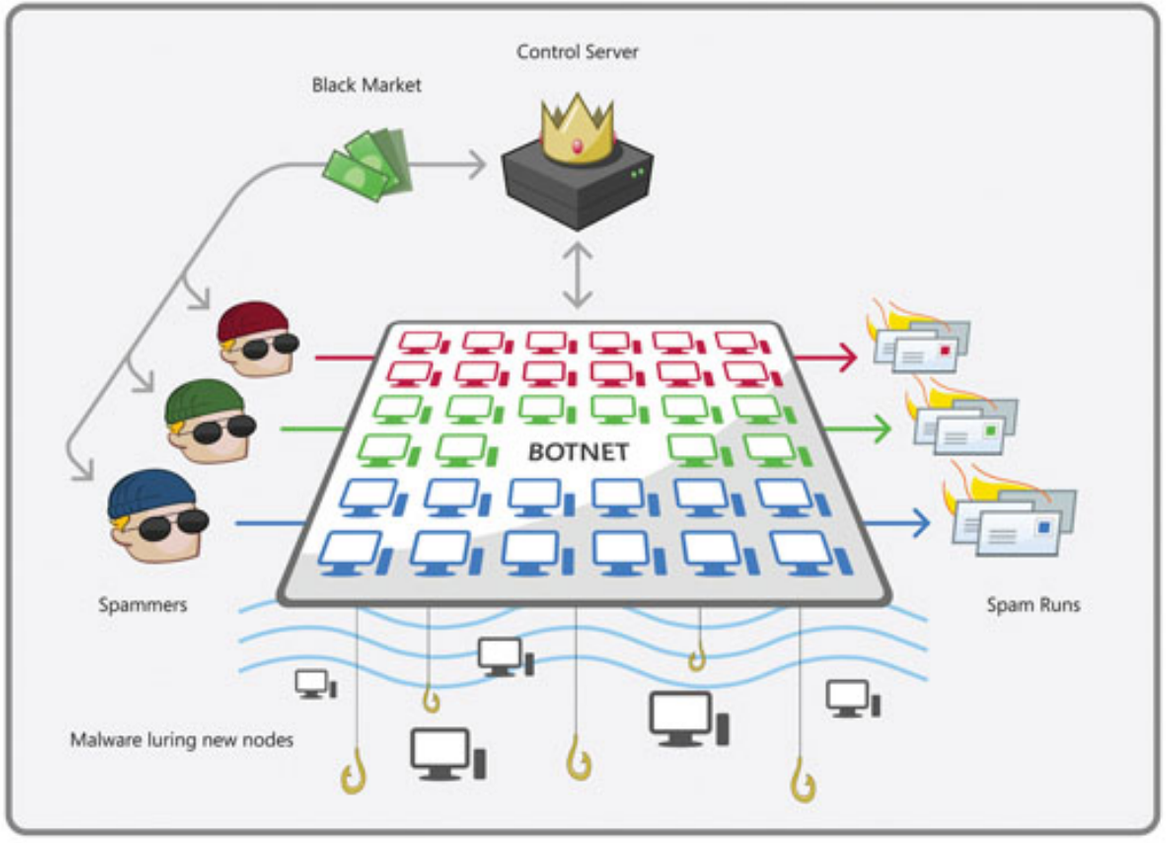
From observation to action - Fighting cybercrimes – Microsoft Digital Crimes Unit

SCS 2014

Disrupting the Criminal Infrastructure: "Botnets"

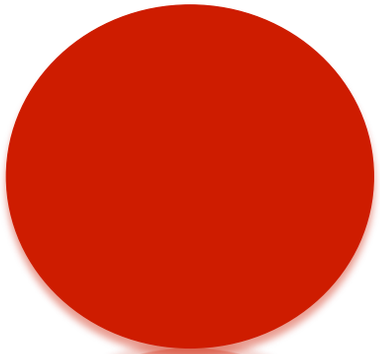
- Botnets are networks of infected computers that can be remotely controlled by an individual or organization

- Used to conduct a variety of attacks
  - Spam
  - Denial of service
  - Click fraud
  - More malware distribution

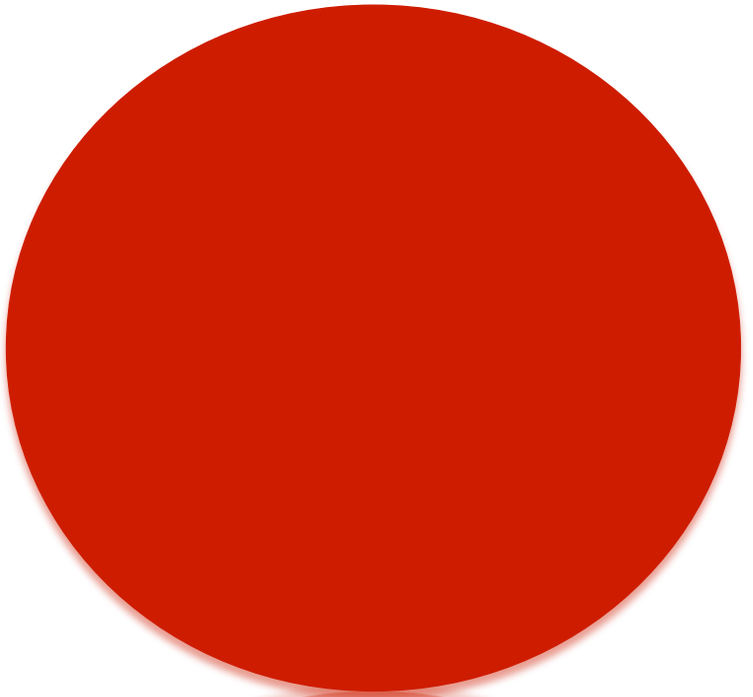


www.microsoft.com/mscorp/twc/operationb49

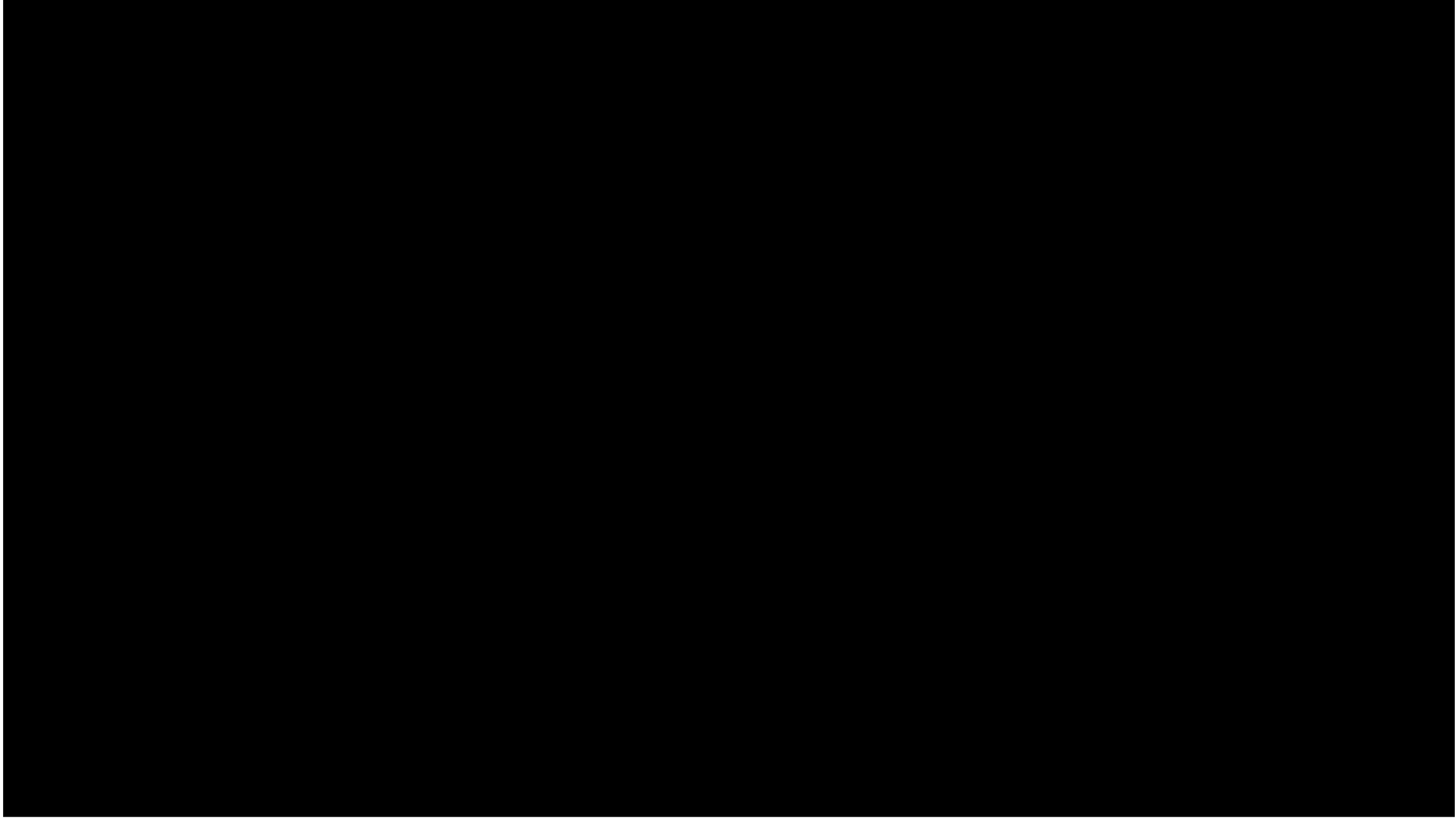
Disrupting Criminal Business



Cost of Business



Value of Infection



Digital Crimes Unit Mission

Digital Crimes Unit

Disrupt malware attacks

Target intellectual property crimes

Protect vulnerable populations

Taking the fight directly to cybercriminals

Mission:

Aggressively **fight** cybercrime and advocate extensively for **enhancing** cybersecurity

Malware disruption

IP Protection

Protection of vulnerable populations

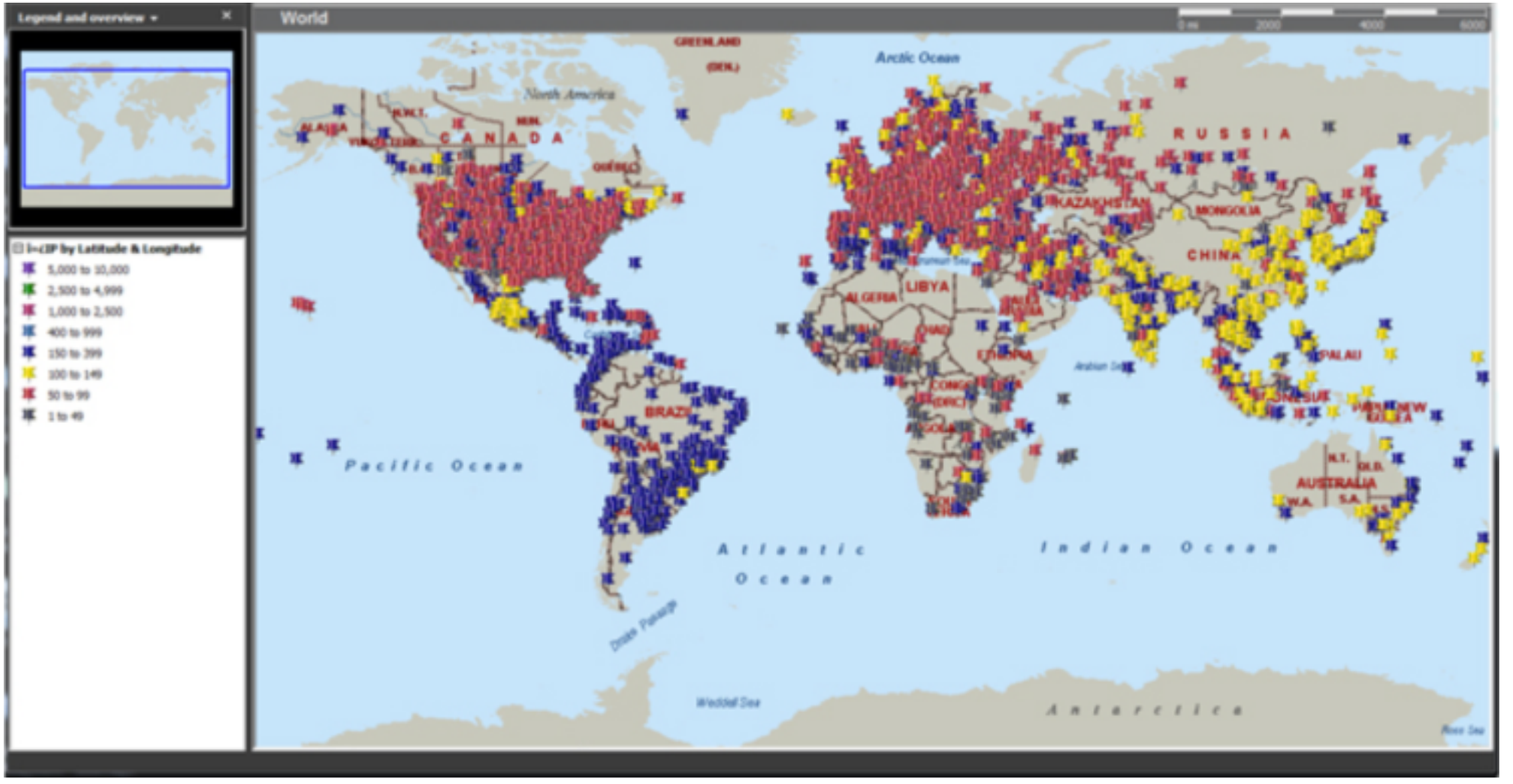
Making an impact

- ✓ **Taking down botnets and disrupting malware,** in partnership with governmental and commercial organizations, to clean and protect tens of millions of devices
- ✓ **Improving products and services** by embedding collected data and intelligence into our platform and services
- ✓ **Disrupting and dismantling cybercriminal operations** that promote a range of illegal goods and services
- ✓ **PhotoDNA tool protecting** children from online exploitation built into LE tools and used by Enterprises

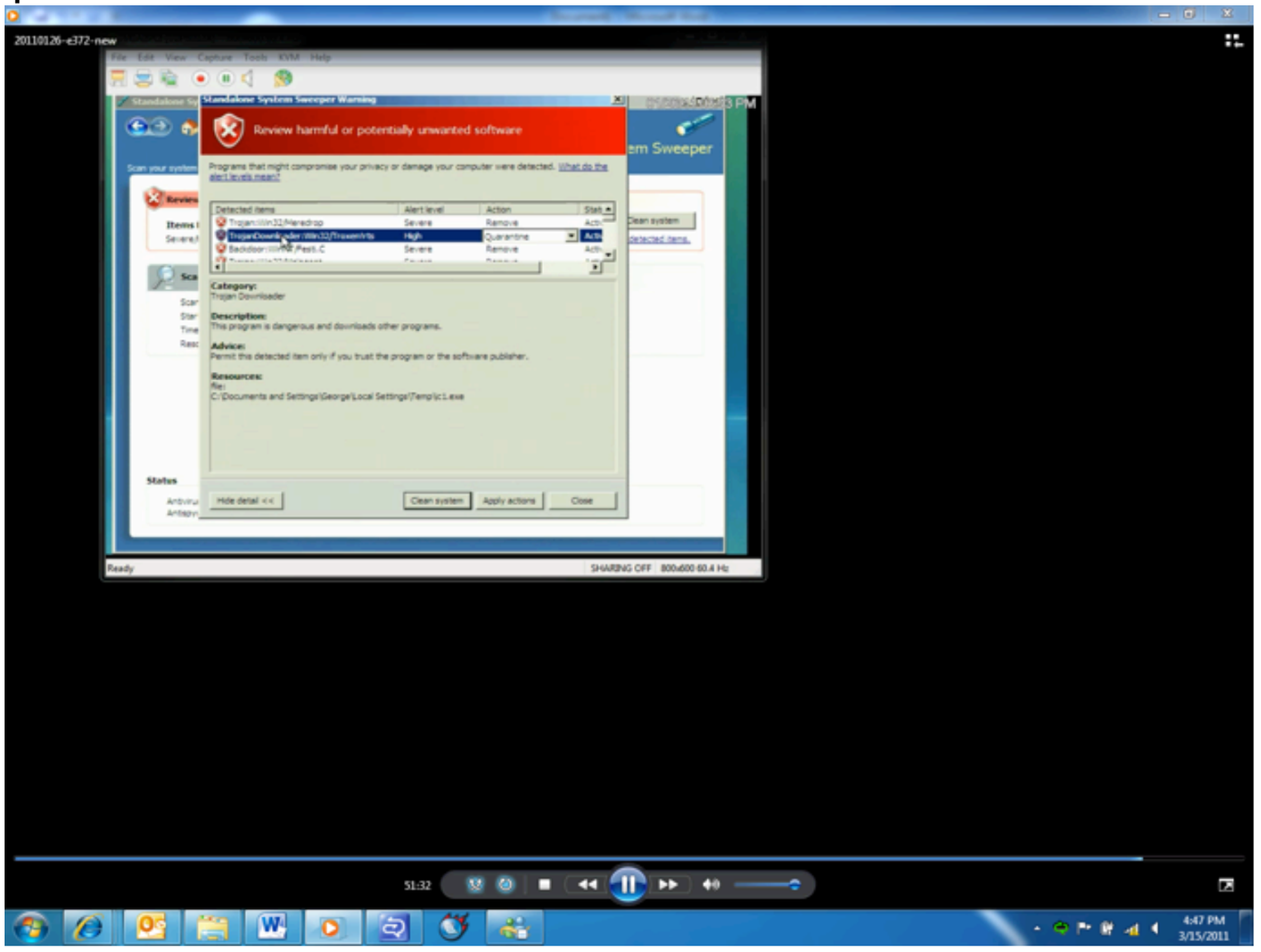
Operation b49: Waledac takedown – February 2010

- In February 2010, Microsoft got a court order to sever 277 domains believed to be part of the Waledac botnet
- Operation b49 effectively severed ~70,000-90,000 computers from the botnet
- In October 2010, the court permanently awarded the 277 domains to Microsoft so they are never used for cybercrime again
- Due to cleanup efforts with ISPs/CERTs worldwide and natural decay of the inactive botnet, we estimate there are ~22,000 remaining infected IPs (as it was of March 2011)

Operation b107: Rustock takedown – March 2011



Operation b107: Rustock takedown



SCS 2014

Operation b107: Rustock takedown

Operation b107: Rustock takedown

- Photo provided courtesy of Pfizer Corporation

Operation b107: Rustock takedown

11-CV-00222-DOND

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,

Defendants.

Case No. C11-02

COMPLAINT

FILED UNDER SEAL

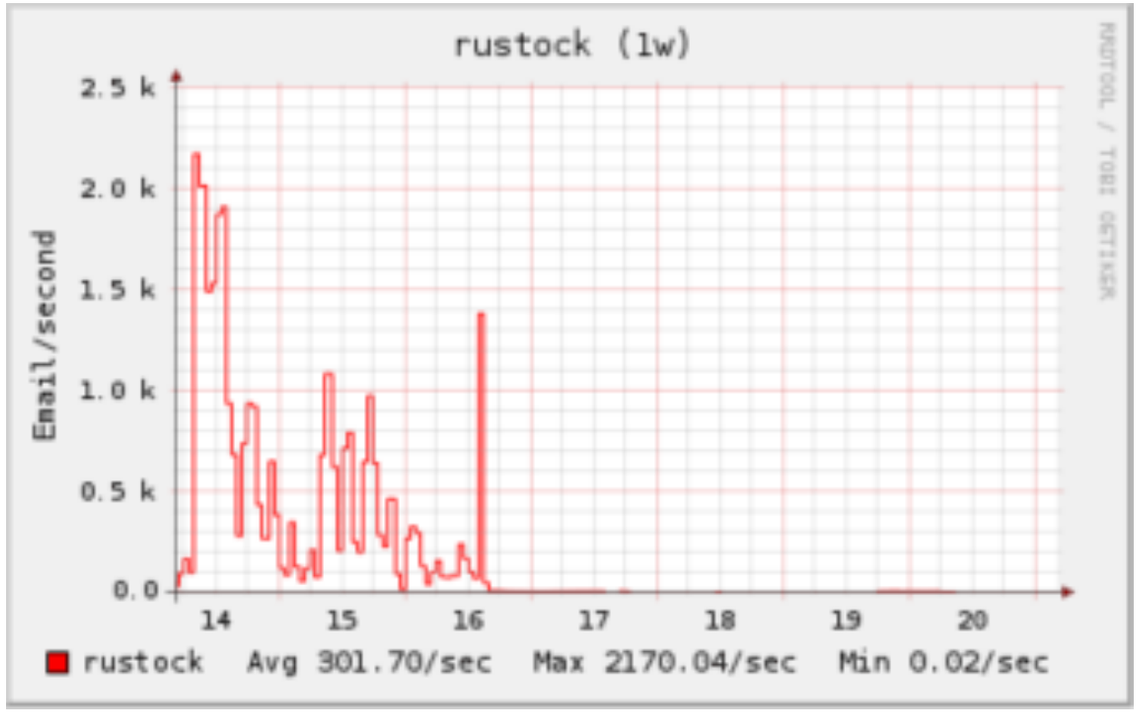
Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges that JOHN DOES 1-11 ("Defendants") are controlling an illegal, notorious, and world-wide computer network known as the "Rustock botnet," made up of end-user computers connected to the Internet, which Defendants have infected with malicious software, and which Defendants consequently can and do direct and control for nefarious and illegal purposes through servers connected to the Internet.

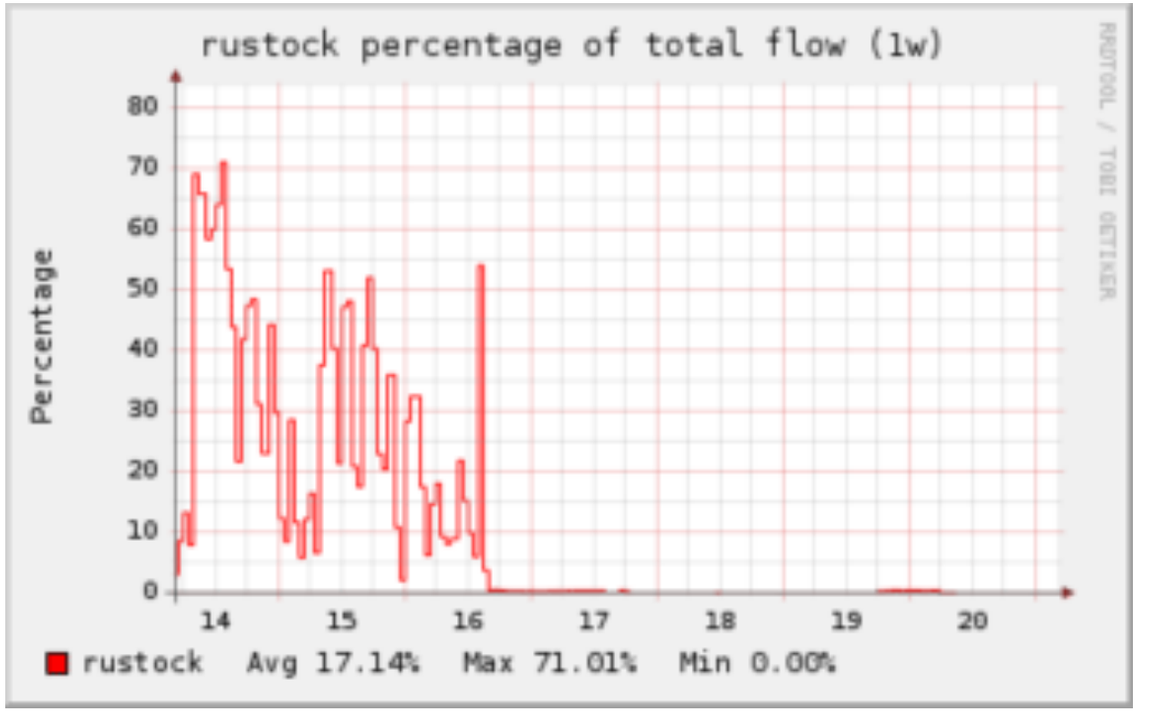
CNCERT/CC

POLITIE

SCS 2014

Operation b107: Impact on spam





http://cbl.abuseat.org/rustock.html

Operation b107: Cleanup

http://support.microsoft.com/botnets

Rustock infection (by IP)

Worldwide reduction rate		
Observed Mar 20-26	Observed Sept 11-17	Reduction Mar – Sept
1,601,619	421,827	73.66%

Data released:
Sept 22, 2011

Top 10 Countries at start		
Country	Observed Mar 20-26	Reduction Mar – Sept
India	322,566	85.47%
Russia	93,703	82.76%
Turkey	89,122	68.43%
USA	86,375	58.01%
Italy	53,656	62.31%
Brazil	46,978	72.32%
Ukraine	45,828	83.84%
Germany	43,946	66.43%
Malaysia	42,541	83.60%
Mexico	39,648	72.54%

Top 10 Countries as of today		
Country	Observed Sept 11-17	Reduction Mar – Sept
India	46,865	85.47%
USA	36,269	58.01%
Turkey	28,135	68.43%
Italy	20,225	62.31%
Russia	16,150	82.76%
France	15,037	51.66%
Germany	14,753	66.43%
Brazil	13,005	72.32%
UK	11,521	49.98%
Poland	11,493	64.78%

*Note: Exact numbers can fluctuate. These capture a particular snapshot in time observed in the stated 7-day period.

Operation b107: Legal case continued

Russian advertisements for notice

$250k USD reward offer

INTRODUCTION

Microsoft has decided to augment its civil discovery efforts to identify those principally responsible for controlling the notorious Rustock bot-net by issuing a monetary reward for information that results in the identification, arrest and criminal conviction of such individual(s).

Microsoft specifically encourages anyone with information regarding those principally responsible for controlling the Rustock bot-net to contact Microsoft Corporation, and is offering a $250,000.00 reward for information that results in their identification, arrest and criminal conviction. Information should be provided directly to Microsoft Corporation by email to rxreward@microsoft.com.

RUSTOCK REWARD

July 18, 2011

In order to determine the identities of the John Doe defendants principally responsible for the control of the Rustock bot-net, Microsoft Corporation is offering a $ 250,000.00 dollar reward (USD) for any new information that results in the identification, arrest and criminal conviction of whoever is responsible for the control of the Rustock bot-net. Anyone with such information should contact Microsoft Corporation by email to rxreward@microsoft.com. Microsoft Corporation reserves the exclusive right to review and evaluate the legitimacy of all leads submitted, and further reserves the right to provide such leads to United States law enforcement.

Microsoft DIGITAL CRIMES UNIT

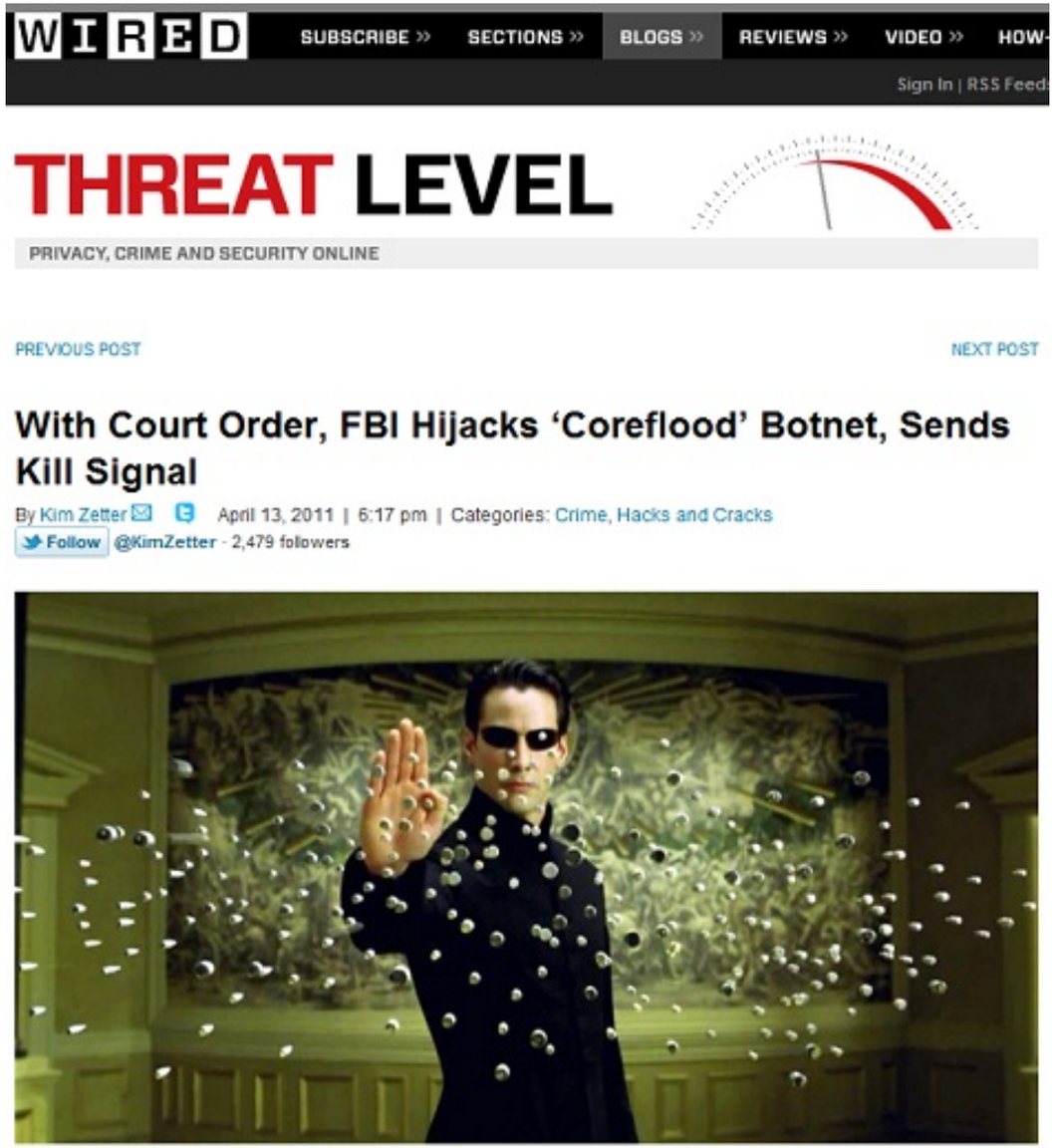
Microsoft

http://www.noticeofpleadings.com

Civil case closure and FBI referral

Send tips to:
MS_Referrals@ic.fbi.gov

Law enforcement action: Coreflood



WIRED SUBSCRIBE » SECTIONS » BLOGS » REVIEWS » VIDEO » HOW-

Sign In | RSS Feeds

THREAT LEVEL

PRIVACY, CRIME AND SECURITY ONLINE

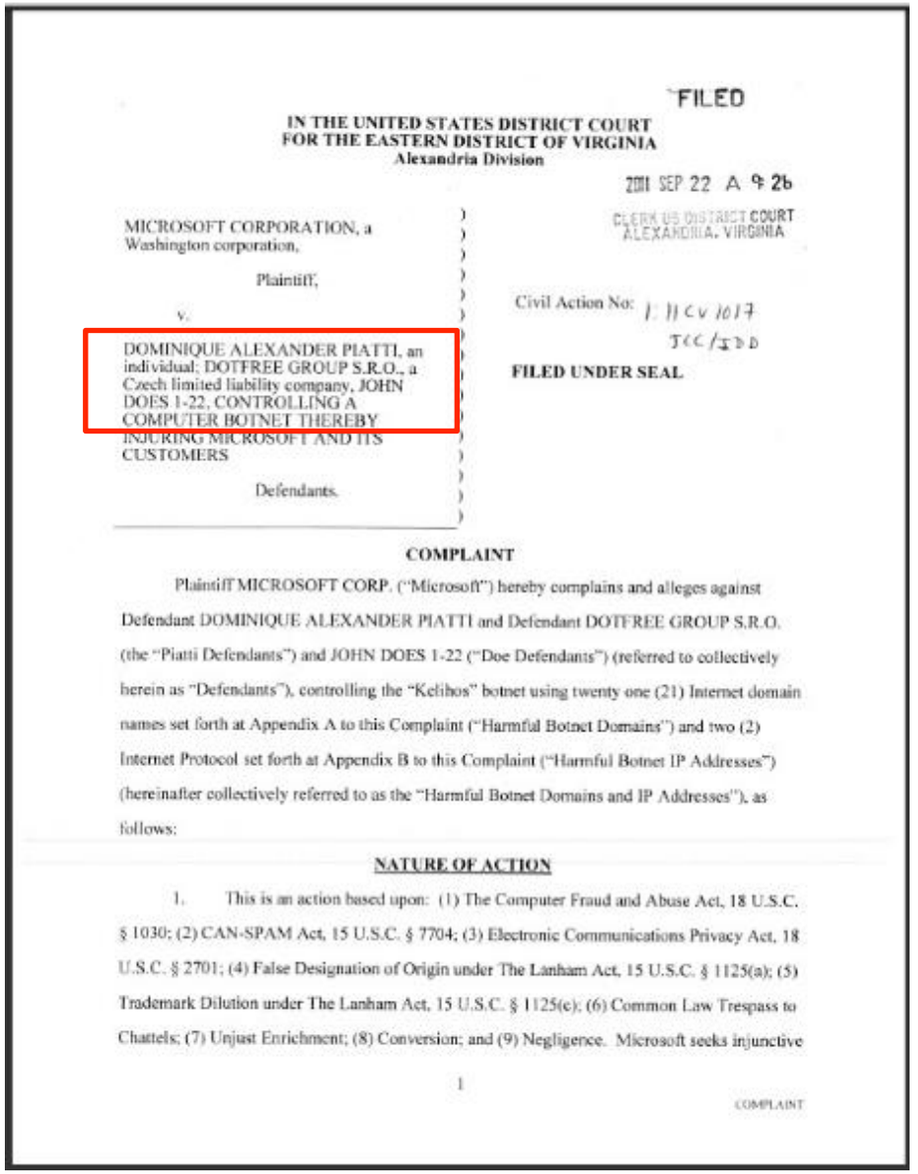
PREVIOUS POST NEXT POST

With Court Order, FBI Hijacks 'Coreflood' Botnet, Sends Kill Signal

By Kim Zetter April 13, 2011 | 6:17 pm | Categories: Crime, Hacks and Cracks

Follow @KimZetter - 2,479 followers

Operation b79: Kelihos takedown – September 2011



FILED

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

2011 SEP 22 A 9:26

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

DOMINIQUE ALEXANDER PIATTI, an individual; DOTFREE GROUP S.R.O., a Czech limited liability company, JOHN DOES 1-22, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS

Defendants.

Civil Action No: 1:11cv1017

FILED UNDER SEAL

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges against Defendant DOMINIQUE ALEXANDER PIATTI and Defendant DOTFREE GROUP S.R.O. (the "Piatti Defendants") and JOHN DOES 1-22 ("Doe Defendants") (referred to collectively herein as "Defendants"), controlling the "Kelihos" botnet using twenty one (21) Internet domain names set forth at Appendix A to this Complaint ("Harmful Botnet Domains") and two (2) Internet Protocol set forth at Appendix B to this Complaint ("Harmful Botnet IP Addresses") (hereinafter collectively referred to as the "Harmful Botnet Domains and IP Addresses"), as follows:

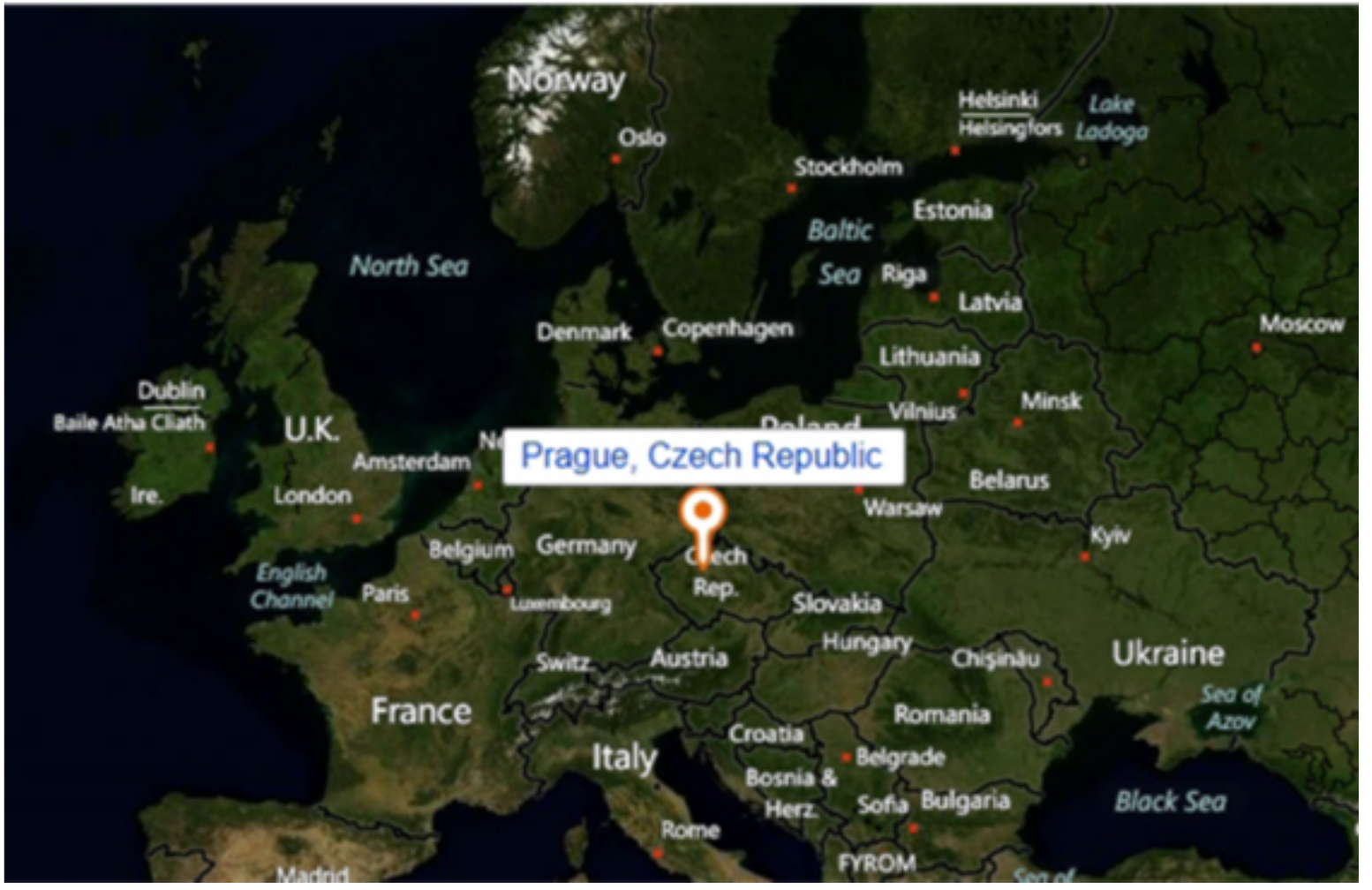
NATURE OF ACTION

1. This is an action based upon: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) CAN-SPAM Act, 15 U.S.C. § 7704; (3) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (4) False Designation of Origin under The Lanham Act, 15 U.S.C. § 1125(a); (5) Trademark Dilution under The Lanham Act, 15 U.S.C. § 1125(c); (6) Common Law Trespass to Chattels; (7) Unjust Enrichment; (8) Conversion; and (9) Negligence. Microsoft seeks injunctive

1

COMPLAINT

Operation b79: Kelihos takedown



SCS 2014

Operation b79: Kelihos takedown

Microsoft

Microsoft Malware Protection Center

Threat Research & Response Blog

TechNet Blogs > Microsoft Malware Protection Center > Kelihos and Waledac- Separated at Birth?

Kelihos and Waledac- Separated at Birth?

msft-mmpc 10 Jan 2011 5:45 PM

RATE THIS

In another instance of malware utilizing holiday-themed spam emails, our researchers had the opportunity to review in detail the threat we call Backdoor:Win32/Kelihos.A. An interesting aspect to this threat is its use of fast-flux in much the same way as the Win32/Waledac family. This similarity is not a coincidence. Analysis of Kelihos shows large portions of the code of Kelihos are shared with Waledac suggesting it is either from the same parties or that the code was obtained, updated and reused.

Still, based on our analysis, we have classified this as a new family and not a variant of Waledac. It is important to note that this new family is not communicating with nor is it reactivating the original Waledac which had its command and control infrastructure neutralized last year. We are actively monitoring this emerging malware in cooperation with industry and academic partners who were previously involved in Operation b49.

Microsoft Malware Protection Center

KASPERSKY lab

KYRUS

Microsoft

Operation b79: Kelihos takedown

Microsoft

Account ▾ Sign in

Malware Protection Center

Home | Security software | Malware encyclopedia | Our research | Help | Developers

Follow:

TRANSLATE with bing

Get updates
Update your Microsoft security software

Get protected
Download Microsoft security software

Get support
Explore Microsoft support options

I want to...

- Get help
  - Remove difficult malware
  - Avoid tech support phone scams
  - See and search the latest threats
  - Find answers to other problems
- Fix my software
- Download and update
- Submit a file

Operation 71: Disruption of Zeus – March 2012

MICROSOFT DIGITAL CRIMES UNIT

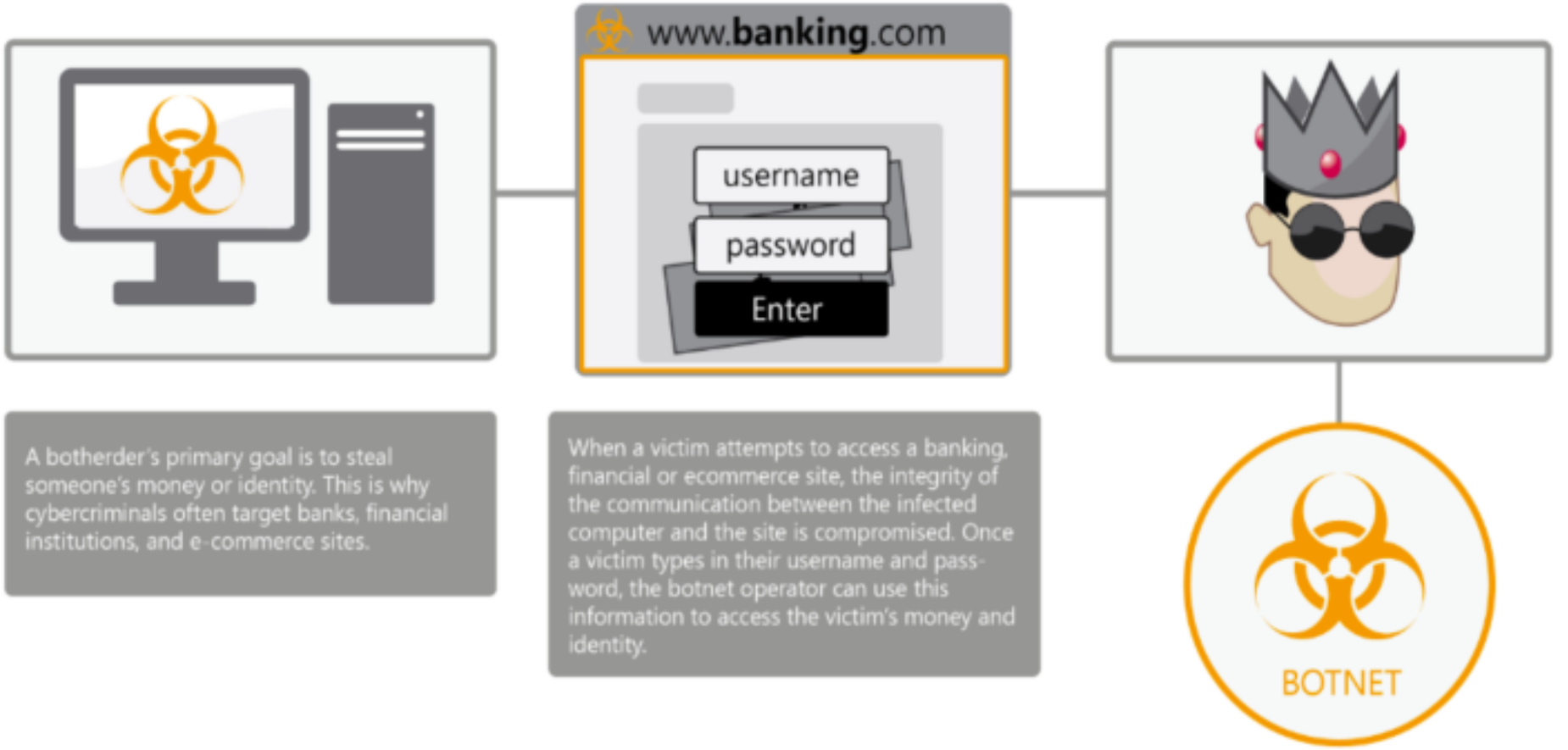
FINANCIAL SERVICES ISAC

NACHA The Electronic Payments Association

KYRUS

SCS 2014

Operation 71: Disruption of Zeus



A botherder's primary goal is to steal someone's money or identity. This is why cybercriminals often target banks, financial institutions, and e-commerce sites.

When a victim attempts to access a banking, financial or ecommerce site, the integrity of the communication between the infected computer and the site is compromised. Once a victim types in their username and password, the botnet operator can use this information to access the victim's money and identity.

Operation 71: Disruption of Zeus

Operation b70: Nitol Disruption – September 2012

The Official Microsoft® Blog

NEWS & PERSPECTIVE FROM MICROSOFT

Microsoft Disrupts the Emerging Nitol Botnet Being Spread through an Unsecure Supply Chain

13 Sep 2012 12:15 AM

Earlier this week, the U.S. District Court for the Eastern District of Virginia granted Microsoft's Digital Crimes Unit permission to disrupt more than 500 different strains of malware with the potential for targeting millions of innocent people. Codenamed "Operation b70," this legal action and technical disruption proceeded from a Microsoft study which found that cybercriminals infiltrate unsecure supply chains to introduce counterfeit software embedded with malware for the purpose of secretly infecting people's computers. In disrupting these malware strains, we helped significantly limit the spread of the developing Nitol botnet, our second botnet disruption in the last six months.

SCS 2014

Operation b70: Nitol

AP

THE BIG STORY

Latest News · 10 Things to Know · Why it Matters · Class of 2012

FROM BRAND NEW LAPTOP TO INFECTED BY PRESSING 'ON'

By RICHARD LARDNER

Home » Business » From brand new laptop to infected by pressing 'on'

WASHINGTON (AP) — A customer in Shenzhen, China, took a brand new laptop out of its box and booted it up for the first time. But as the screen lit up, the computer began taking on a life of its own. The machine, triggered by a virus hidden in its hard drive, began searching across the Internet for another computer.

The laptop, supposedly in pristine, super-fast, direct-from-the-factory condition, had instantly become part of an illegal, global network capable of attacking websites, hosting bank accounts and stealing personal data.

THURSDAY SEPT. 13 ONLY

RAGU PASTA SAUCE

$0.88

LATEST NEWS

Date of First Publication: September 13, 2012

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION,
a Washington corporation

Plaintiff,

vs.

Peng Yang, an individual;
Changzhou Bei Te Kang Mu Software Technology Co., LTD., d/b/a Bitcomm, Ltd; John Does 1-3

Defendants.

Case No. 1:12cv1004 GBL/IDD

Plaintiff Microsoft has sued defendants Peng Yang; Bei Te Kang Mu Software Technology, d/b/a Bitcomm Ltd.; and John Does 1-3, associated with 3322.org and sub-domains of 3322.org, and the Nitol botnet. Microsoft alleges that Defendants have violated Federal and state law by operating a computer botnet and other malicious software through more than 70,000 sub-domains of 3322.org, causing the unlawful intrusion into, infection of, and further illegal conduct involving, the personal computers of innocent persons, thereby causing harm to those persons, Microsoft, and the public at large. Microsoft seeks a preliminary injunction directing that it be made the authoritative name server for 3322.org in order to block traffic to the sub-domains of 3322.org being used to support Nitol and other malware operations. Microsoft seeks a permanent injunction and damages. Full copies of the pleading documents are available at http://www.noticeofpleadings.com.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the plaintiff's attorney, Gabriel Ramsey, Orrick, Herrington & Sutcliffe LLP, 1000 Marsh Road, Menlo Park, California, 94025. If you have questions, you should see an attorney immediately. If you need help in finding an attorney, you may call the Virginia State Bar at (804) 775-0808 (in Richmond) or (800) 552-7977 (Statewide or Nationwide).

SCS 2014

Operation b58: Bamital takedown – February 2013

The Official Microsoft Blog

NEWS & PERSPECTIVES

TechNet Blogs > The Official Microsoft Blog

Excerpt View Full Post View

Microsoft and Symantec Take Down Bamital Botnet That Hijacks Online Searches

6 minutes ago

*The following is a post from **Richard Domingues Boscovich**, Associate General Counsel, Microsoft Digital Crimes Unit.*

As reported by Reuters earlier today, the Microsoft Digital Crimes Unit, in collaboration with Symantec, has taken down the dangerous Bamital botnet which hijacked people's search results and took them to potentially dangerous websites that could install malware onto their computer, steal their personal information, or fraudulently charge businesses for online advertisement clicks. Microsoft and Symantec's research shows that in the last two years, more than eight million computers have been attacked by Bamital, and that the botnet's search hijacking and click fraud schemes affected many major search engines and browsers, including those offered by Microsoft, Yahoo and Google. Because this threat exploited the search and online advertising platform to harm innocent people, Microsoft and Symantec chose to take action against the Bamital botnet to help protect people and advance cloud security for everyone.

Exclusive: Software makers disrupt cyber ring, halt searches

Recommend 12 people recommend this.

Tweet 0 Share 1 Share this +1 0 Email Print

By Jim Finkle

BOSTON | Wed Feb 6, 2013 3:26pm EST

(Reuters) - Software makers Microsoft Corp and Symantec Corp said they disrupted a global cyber crime operation by shutting down servers that controlled hundreds of thousands of PCs without the knowledge of their users.

The move made it temporarily impossible for infected PCs around the world to search the web, though the companies offered free tools to clean

Related News

Fed says internal site breached by hackers, no critical functions affected

Google moves closer to resolving EU investigation

Microsoft launches new Office for consumers

U.S. government warns of hack threat to network gear

SCS 2014

Operation b58: Bamital takedown

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-18, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS

Defendants.

Civil Action No.

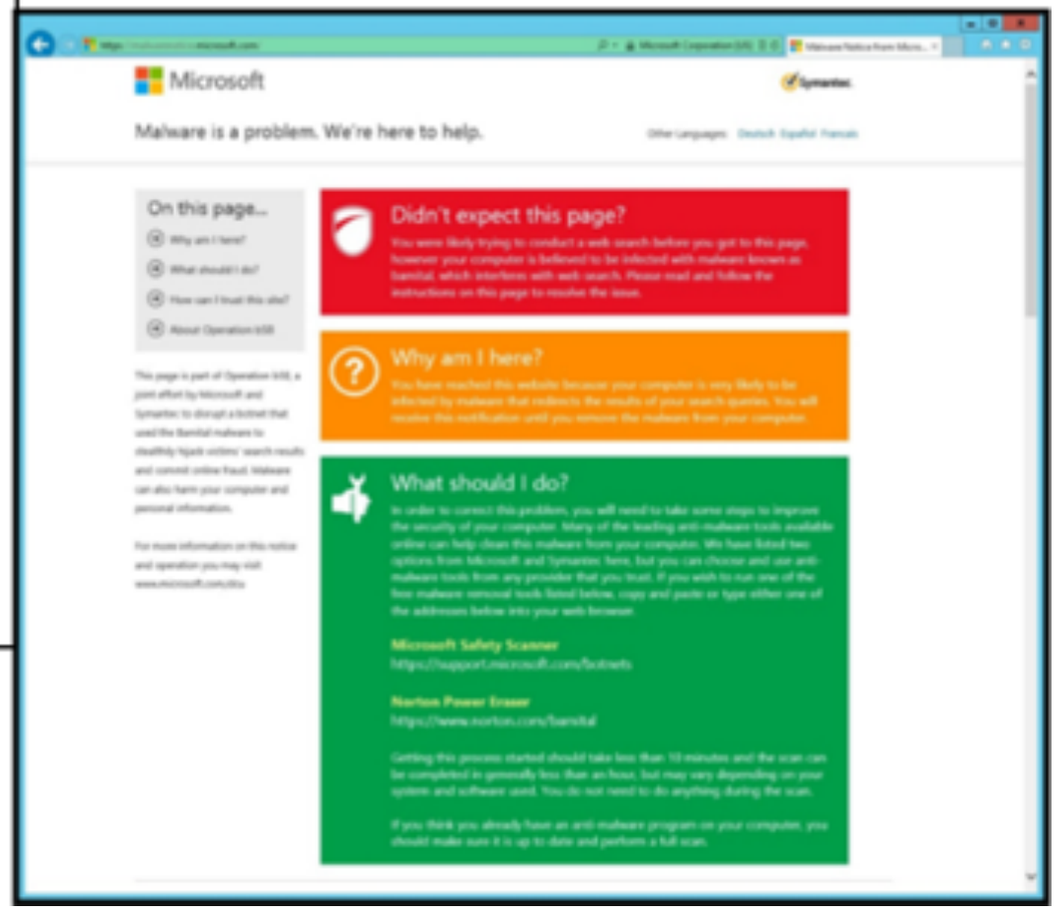
FILED UNDER SEAL

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges against JOHN DOES 1-18 ("Doe Defendants") (referred to collectively herein as "Defendants"), controlling the "Bamital" botnet using the Internet domains and Internet Protocol (IP) addresses set forth at Appendices A, B, and C to this Complaint ("the Bamital IP addresses and domains"), as follows:

NATURE OF ACTION

1. This is an action based upon: (1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701, (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.* (4) False Designation of Origin under The Lanham Act, 15 U.S.C. § 1125(a), (5) Trademark Dilution under The Lanham Act, 15 U.S.C. § 1125(c), (6) Common Law Trespass to Chattels, (7) Unjust Enrichment, and (8) Conversion.



DCU Botnet Takedowns and Malware Disruptions

OPERATION Conficker	OPERATION b49 Waledac	OPERATION b107 Rustock	OPERATION b79 Kelihos	OPERATION b71 Zeus	OPERATION b70 Nitol	OPERATION b58 Bamital	OPERATION b54 Citadel	OPERATION b68 ZeroAccess	OPERATION b157 Game over Zeus	OPERATION b106 Bladabindi & Jenxcus	OPERATION b93 Caphaw
February 2010	February 2010	March 2011	September 2011	March 2012	September 2012	February 2013	June 2013	December 2013	June 2014	June 2014	July 2014
Microsoft-lead model of industry-wide efforts	Proving the model of industry-led efforts	Supported by stakeholders across industry sectors	Partnership between Microsoft and security software vendors	Cross-sector partnership with financial services	Nitol was introduced in the supply chain relied on by Chinese consumers	Bamital hijacked people's search results, took victims to dangerous sites	Citadel committed online financial fraud responsible for more than $500Min losses	ZeroAccess hijacked search results, taking victims to dangerous sites	GameoverZeus (GOZ) was a banking Trojan	Malware using Dynamic DNS for command. It involved password and identity theft, webcam and other privacy invasions.	Caphaw was focused on online financial fraud responsible for more than $250M in losses
Severed 70,000-90,000 infected devices from the botnet	Involved US and Dutch law enforcement, and CN-CERT	First operation with named defendant	Focused on disruption because of technical complexity	Settled with operator of malicious domain	Takedown in collaboration with Symantec, proactive notification and cleanup process	Coordinated disruption with public-private sector partnerships to combat cybercrime	It cost online advertisers upwards of $2.7 million each month	Worked in partnership with LE providing Technical Remediation	Over 200 different types of malware impacted.	Coordinated disruption with public-private sector partnerships
Botnet Worm	Spam	Spam	Spam, Bitcoin Mining, Distributed Denial of Service Attacks	Identity Theft / Financial Fraud	Malware Spreading Botnet, Distributed Denial of Service Attacks	Advertising Click Fraud	Identity Theft / Financial Fraud	Advertising Click Fraud	Identity Theft / Financial Fraud	Identity Theft / Financial Fraud / Privacy Invasion	Identity Theft / Financial Fraud

SCS 2014

Disrupting Cybercrime - Project MARS

Quotes	
"Microsoft has long led the tech industry fight against the scourge of botnets." Tom Jowitt/*TechWeekEurope* 	"This proves once again that only a company the size of Microsoft can muster the resources and pull to get this kind of sting done." Andy Patrizio/*Network World* 
"Microsoft trumpeted its disruption of the ZeroAccess peer-to-peer botnet late last week, but some experts are holding off on scheduling a celebratory ticker-tape parade." Michael Mimoso/ *ThreatPost* 	"'It is not a simple task to take down a decentralized botnet. However, Microsoft's DCU seems to be motivated and their drive to team up with the right law enforcement agencies sounds really promising.'" Tommy Chin, CORE Security via Jennifer LeClaire/*CIO Today* 

Notable Coverage and Quotes on Botnets

Spam Network Shut Down

Microsoft gets legal might to target spamming botnets

Microsoft Raids Tackle Internet Crime

Exclusive: Microsoft and Symantec disrupt cyber crime ring

MICROSOFT FINDS MALWARE ON NEW COMPUTERS IN CHINA

"Taking the disruption into the courthouse was a brilliant idea and is helping the rest of the industry to reconsider what actions are possible, and that action is needed and can succeed."

- Richard Perlotto, Shadowserver Foundation, about Microsoft and FS-ISAC's disruption of the Zeus botnets

"Anything which makes life more difficult for the cybercriminals, and disrupts their activities, has to be applauded."

- Graham Cluley, Sophos, about Microsoft's action against the Nitol botnet

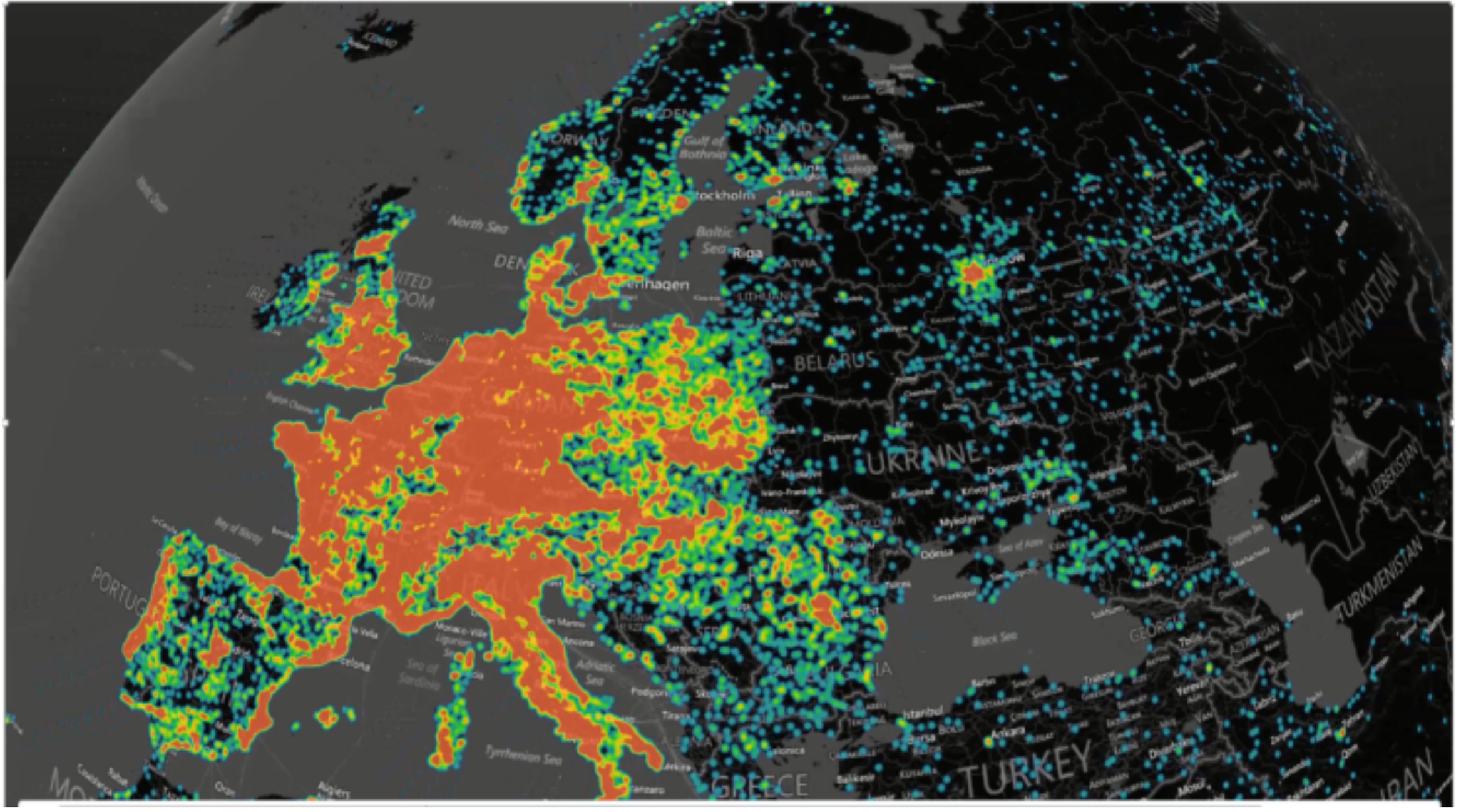
"It may be odd seeing a private company take the lead in a law enforcement action, but overall I'm glad it's happening. Shutting down these criminal operations, freeing up the infected computers and prosecuting the cyberscum involved can't happen quickly enough."

- Dwight Silverman, San Francisco Chronicle, about Microsoft and FS-ISAC's disruption of the Zeus botnets

"Microsoft has done the online world a great service by establishing a repeatable process and a legal framework for taking down botnets and bringing malware distributors to justice."

- Stephen Cobb, ESET Security Evangelist, about Microsoft and FS-ISAC's disruption of the Zeus botnets


Citadel Malware Infection Pattern WW
CANADA
RUSSIA
KAZAKHSTAN
MONGOLIA
CHINA
INDIA
ALGERIA
LIBYA
SUDAN
BRAZIL
AUSTRALIA
Atlantic Ocean
Pacific Ocean
Indian Ocean


Stockholm
Riga
BELARUS
UKRAINE
KAZAKHSTAN
UZBEKISTAN
TURKMENISTAN
TURKEY
GREECE
Istanbul
Ankara
Black Sea
North Sea
Baltic Sea
Gulf of Bothnia
Tyrrhenian Sea
Adriatic Sea
Bay of Biscay

Microsoft Cybercrime Center

Microsoft

Microsoft Cybercrime Center

Redmond

Windows Server Running Hadoop

Windows Azure for SinkHole distribution

Microsoft SQL Server – Big Data

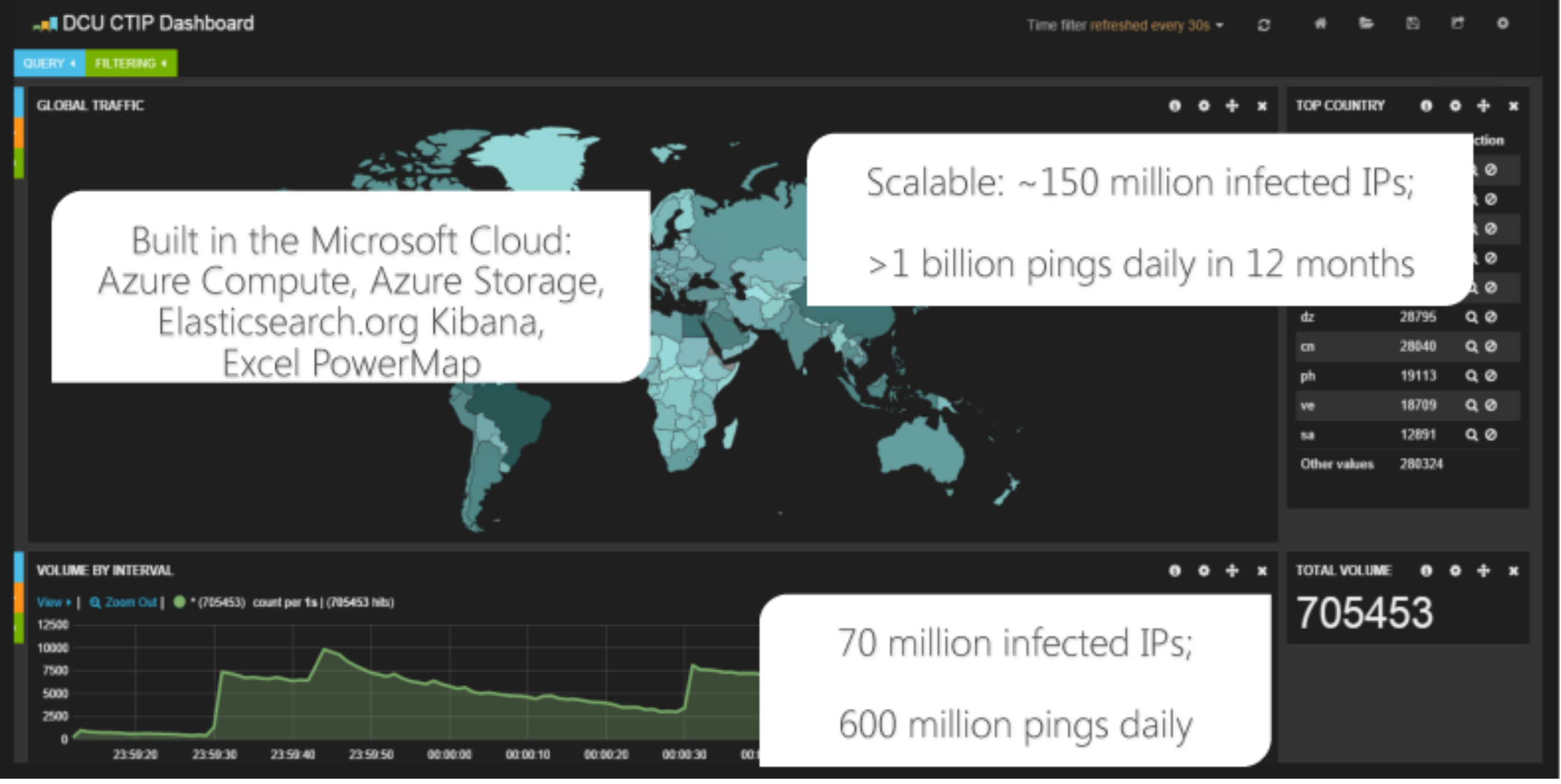
Interested? Contact local Microsoft Team

Cyber Threat Intelligence Big Data Processing

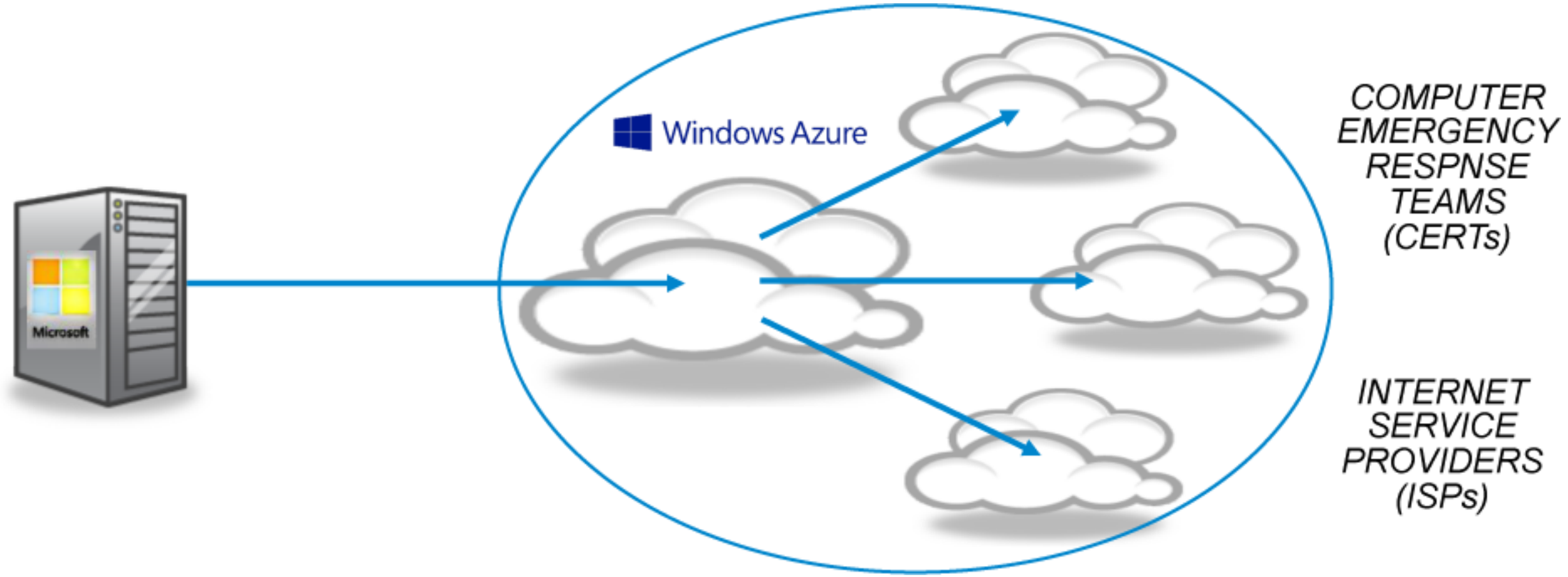
Year	Month	Day	SourceIP	SRCIP_OCT1	SRCIP_OCT2	SRCIP_OCT3	SRCIP_OCT4	ASN	CountryCode	ThreatName	Latitude	Longitude	Hits
2013	Feb	23	39008591	2	83	57		79AS3243	PT	b70-Generic	39.7477	-8.805	2
2013	Feb	23	1.05E+09	62	169	122		64AS24698	PT	Rustock	38.7597	-9.2397	8
2013	Feb	23	1.37E+09	81	193	128		224AS3243	PT	Conficker	38.7167	-9.1333	18
2013	Feb	23	1.39E+09	82	154	189		52AS3243	PT	Conficker	37.1366	-8.5398	4
2013	Feb	23	1.44E+09	85	138	33		195AS12542	PT	Conficker	38.7167	-9.1333	6
2013	Feb	23	1.44E+09	85	243	18		200AS3243	PT	Conficker	37.7333	-25.6667	5
2013	Feb	23	1.44E+09	85	247	188		118AS3243	PT	Conficker	38.5333	-8.9	32
2013	Feb	23	1.44E+09	85	247	251		91AS3243	PT	Conficker	38.645	-9.1484	25
2013	Feb	23	1.5E+09	89	155	17		154AS12542	PT	Conficker	41.4444	-8.2962	53
2013	Feb	23	1.57E+09	93	102	35		83AS24698	PT	b70-Generic	41.1445	-8.5322	4
2013	Feb	23	1.57E+09	93	102	35		83AS24698	PT	Conficker	41.1445	-8.5322	4
2013	Feb	23	1.57E+09	93	108	50		30AS12353	PT	Conficker	41.1336	-8.6174	4
2013	Feb	23	1.57E+09	93	108	226		251AS12353	PT	Conficker	38.7167	-9.1333	6
2013	Feb	23	1.59E+09	94	132	230		175AS12542	PT	Conficker	41.195	-8.5103	1
2013	Feb	23	3.16E+09	188	80	185		231AS3243	PT	Conficker	41.4542	-8.168	25
2013	Feb	23	3.17E+09	188	250	70		43AS3243	PT	Conficker	39.7477	-8.805	10

Fast Facts:

- The C-TIP collection tier processes ~700 million events per day (~5% capacity)
- We add over 150 million events to the database each day
- We are tracking ~ 3 million infected IP addresses daily
- We are capable of distributing “real time” feeds to 1000’s of entities
- We can filter on any attribute we collect at line speed


DCU CTIP Dashboard
Time filter refreshed every 30s
QUERY
FILTERING
GLOBAL TRAFFIC
TOP COUNTRY
dz 28795
cn 28040
ph 19113
ve 18709
sa 12891
Other values 280324
Built in the Microsoft Cloud:
Azure Compute, Azure Storage,
Elasticsearch.org Kibana,
Excel PowerMap
Scalable: ~150 million infected IPs;
>1 billion pings daily in 12 months
VOLUME BY INTERVAL
View | Zoom Out | * (705453) count per 1s | (705453 hits)
12500
10000
7500
5000
2500
0
23:59:20
23:59:30
23:59:40
23:59:50
00:00:00
00:00:10
00:00:20
00:00:30
TOTAL VOLUME
705453
70 million infected IPs;
600 million pings daily

C-TIP Feed Distribution



C-TIP Botnet Feeds sharing with

Microsoft partners with financial services industry on fight against cybercrime

Posted September 29, 2014 by Richard Domingues Boscovich - Assistant General Counsel, Microsoft Digital Crimes Unit

New collaboration with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to share cyber-threat intelligence, free of charge, to better protect our mutual customers and partners

Through this pilot program, Microsoft will make its Cyber Threat Intelligence Program feed available to participating FS-ISAC members, which will receive near real-time information on known malware infections affecting more than 67 million unique IP address

Technologies used by Digital Crime Unit

Office

Lync

Microsoft SQL Server

Windows Server

Excel

Windows Azure

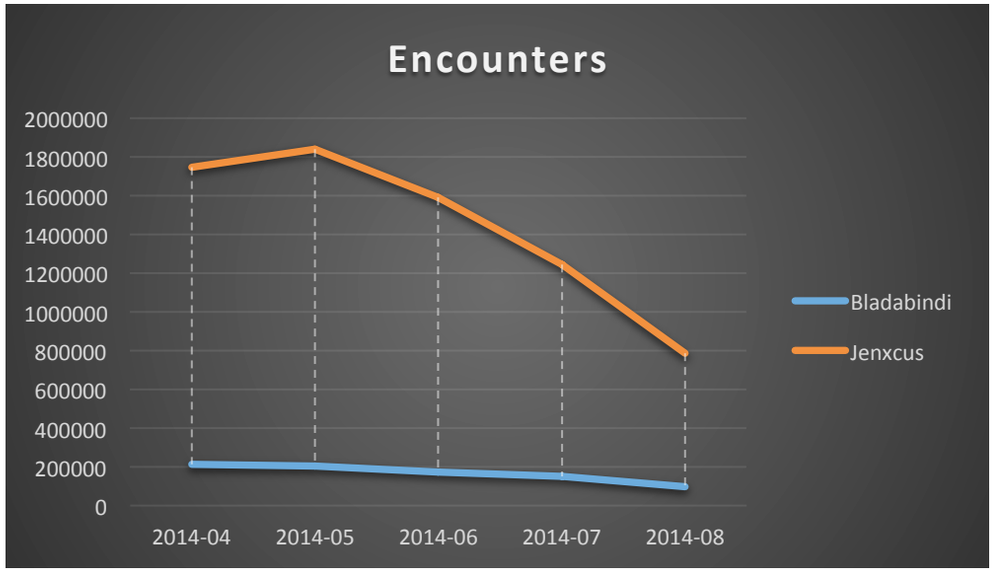
Office 365

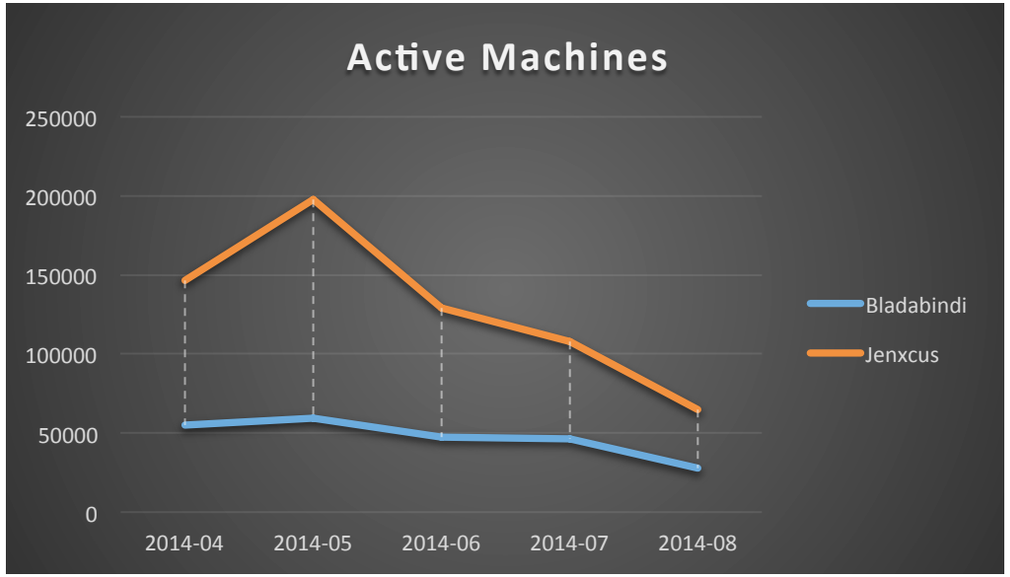
SharePoint

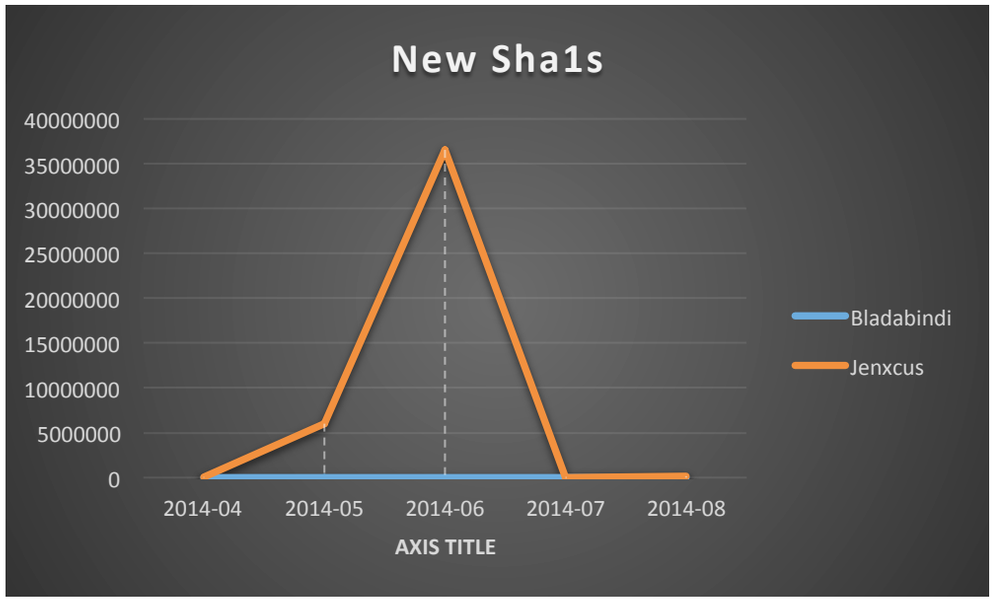
SCS 2014

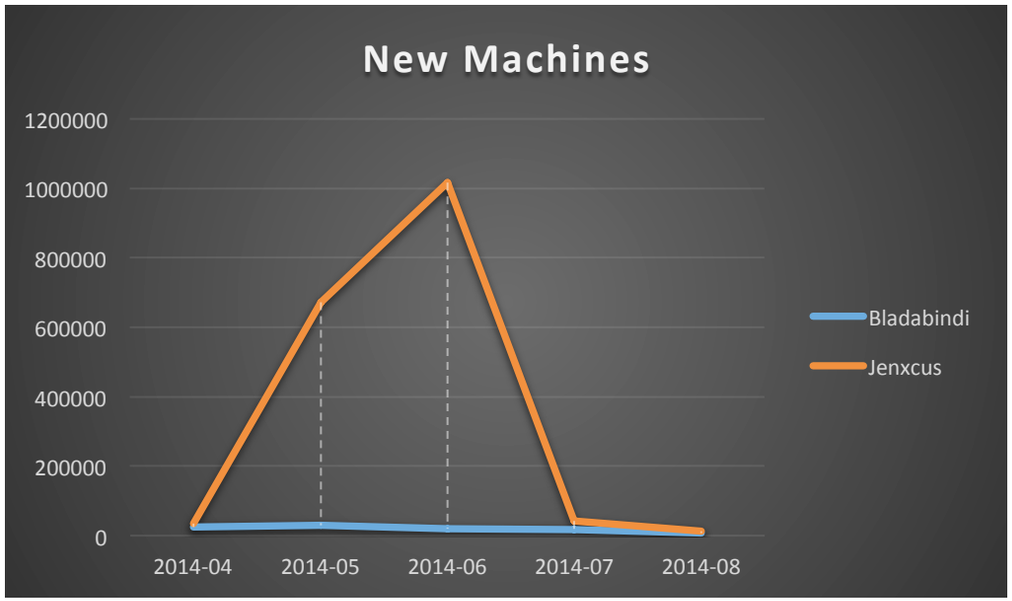
Partnering with Microsoft's Technology Centers, we will have a Cybercrime Center presence in more than 30 locations.

Threat Ecosystem – Impact of DCU Operations









Description : Encounters spread sheet is telemetry spreadsheet that contains detailed information about threats including encounters, remediation and new samples

Anti-Botnet Operation B106 Summary

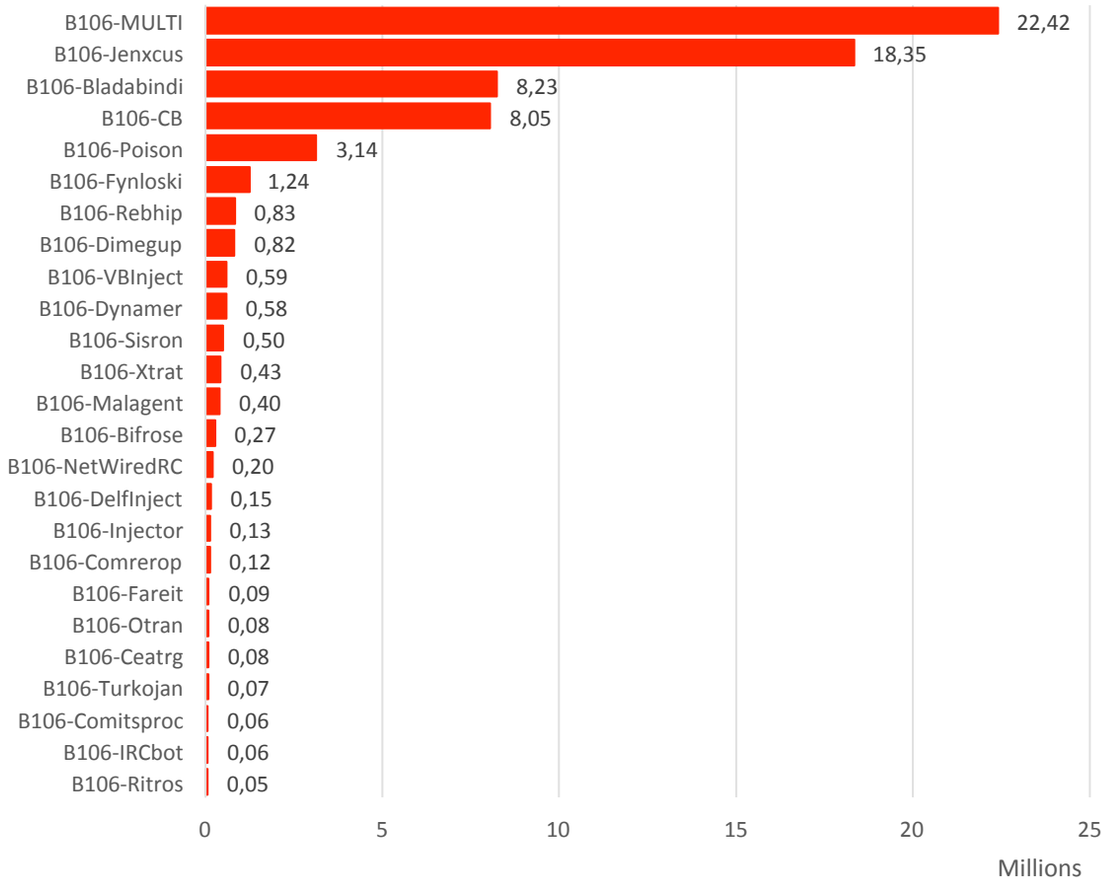
42,867,639
Unique IPs

239
Countries

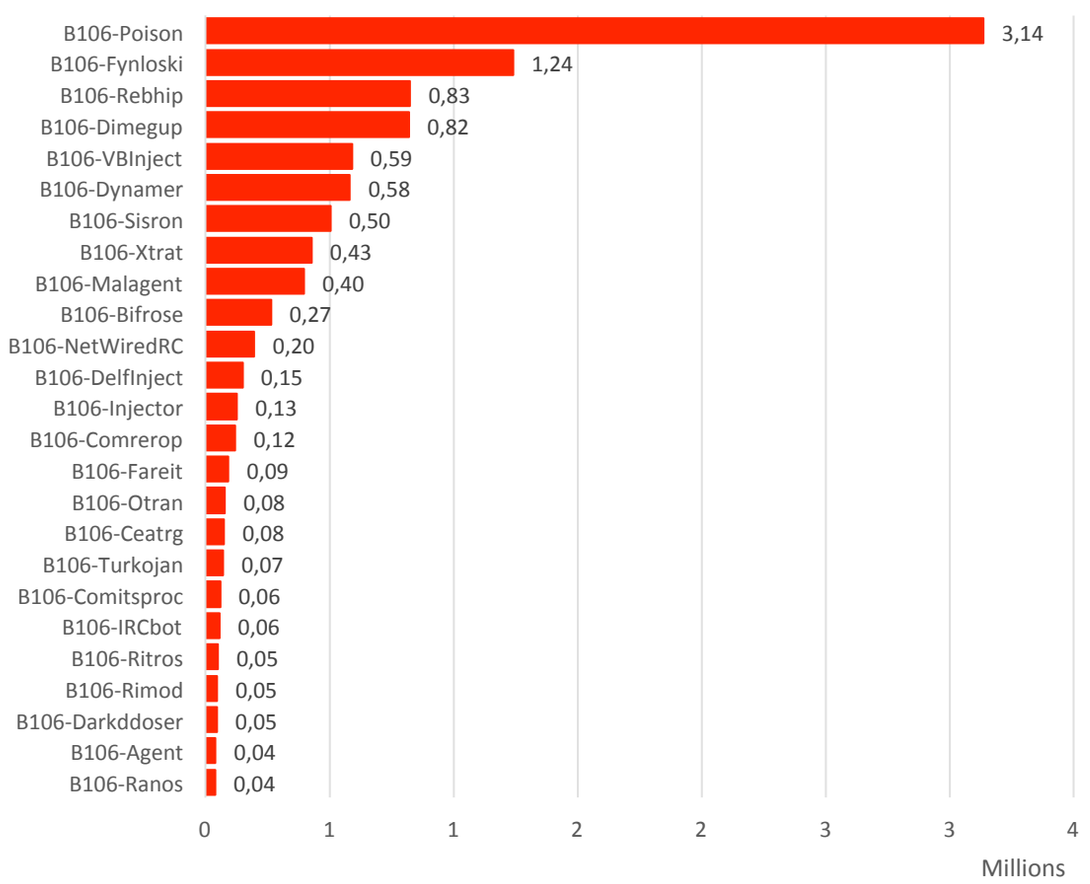
199
Threats

B106 Threats

Top 25 Threats



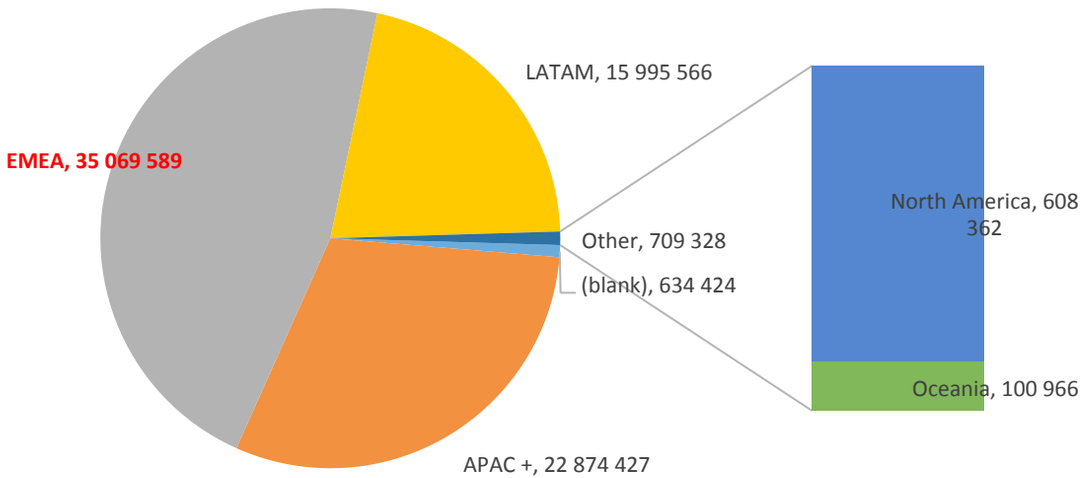
Top 25 Threats without Bladabindi & Jenxcus



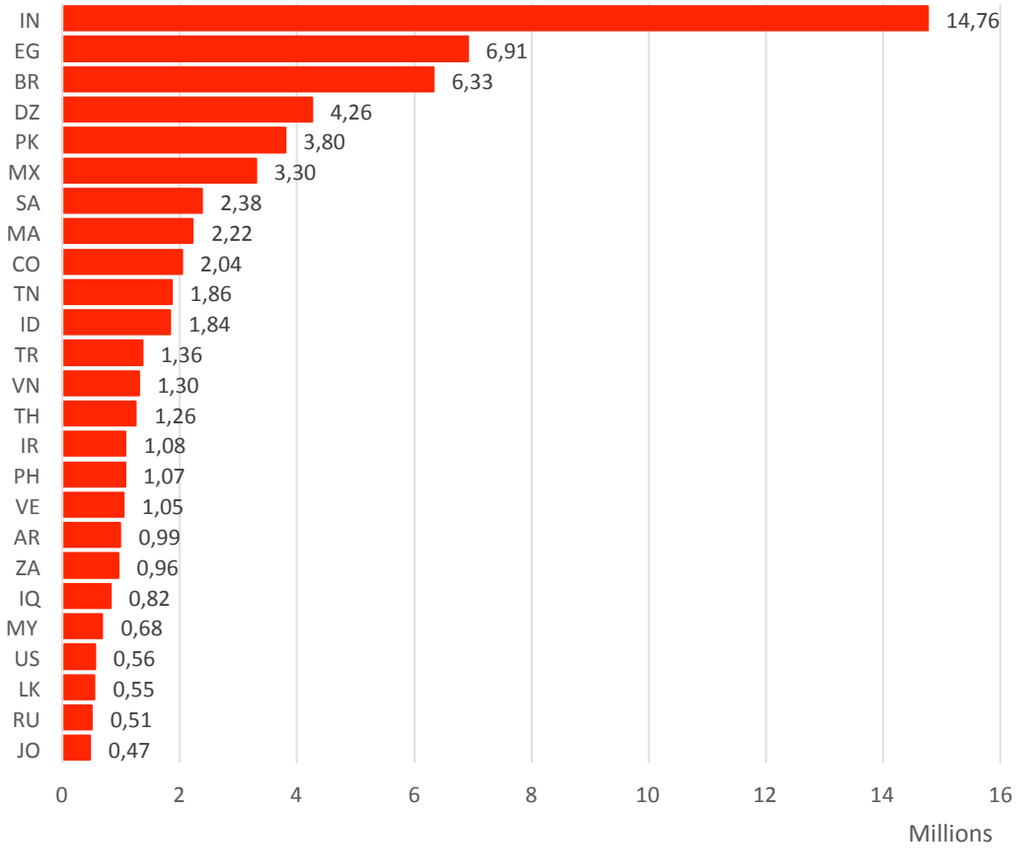
SCS 2014

B106 Threats

Threats by Continent

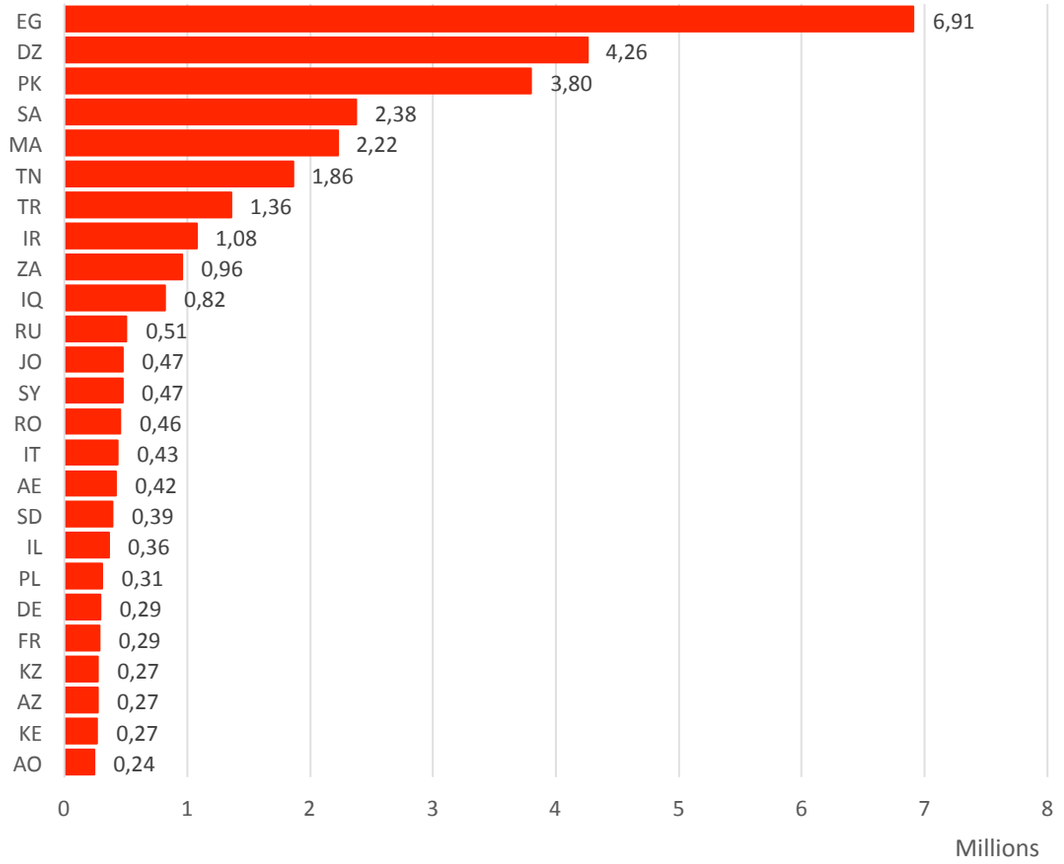


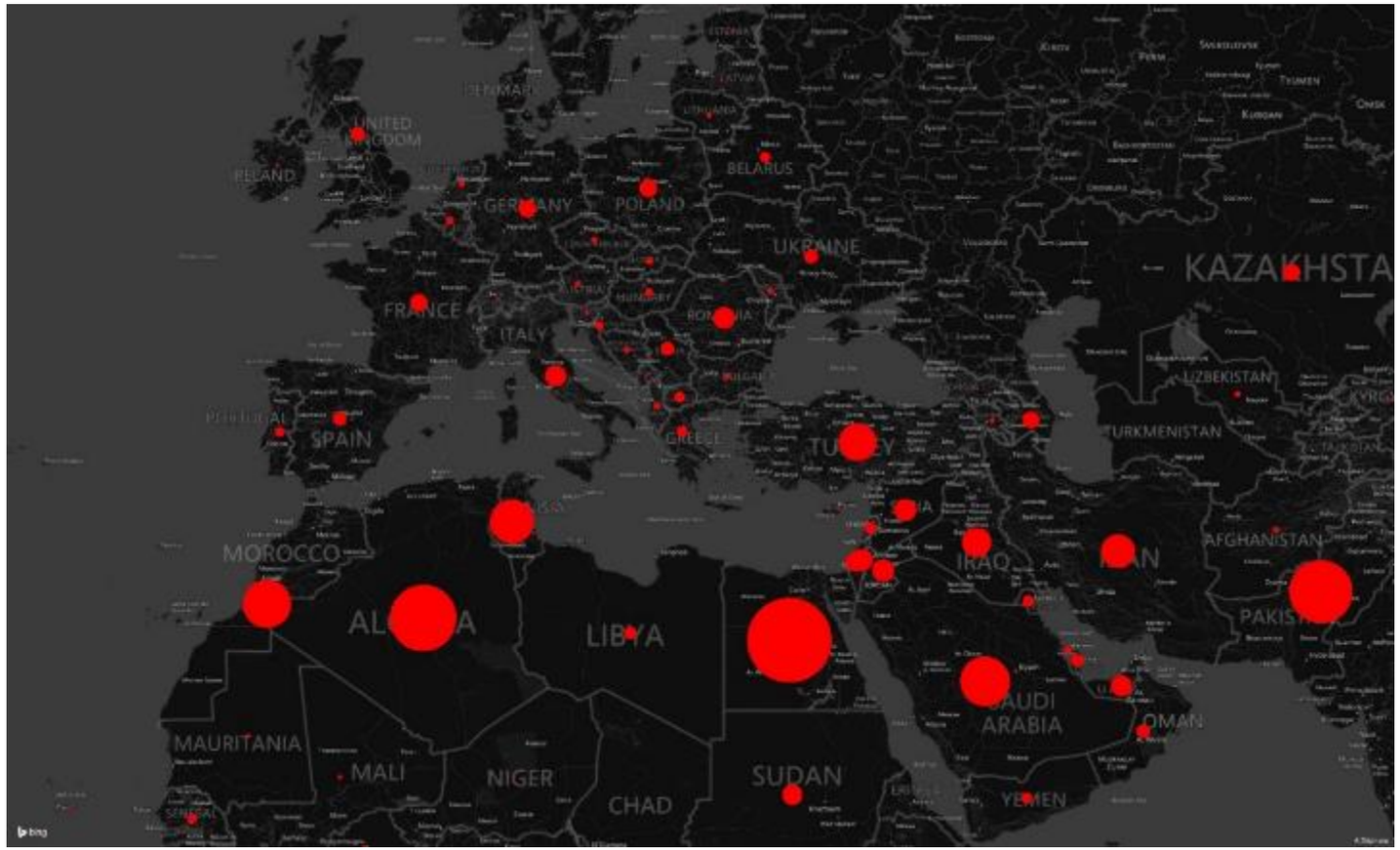
Top 25 Infected Countries



SCS 2014

B106 Top 25 Infected Countries EMEA

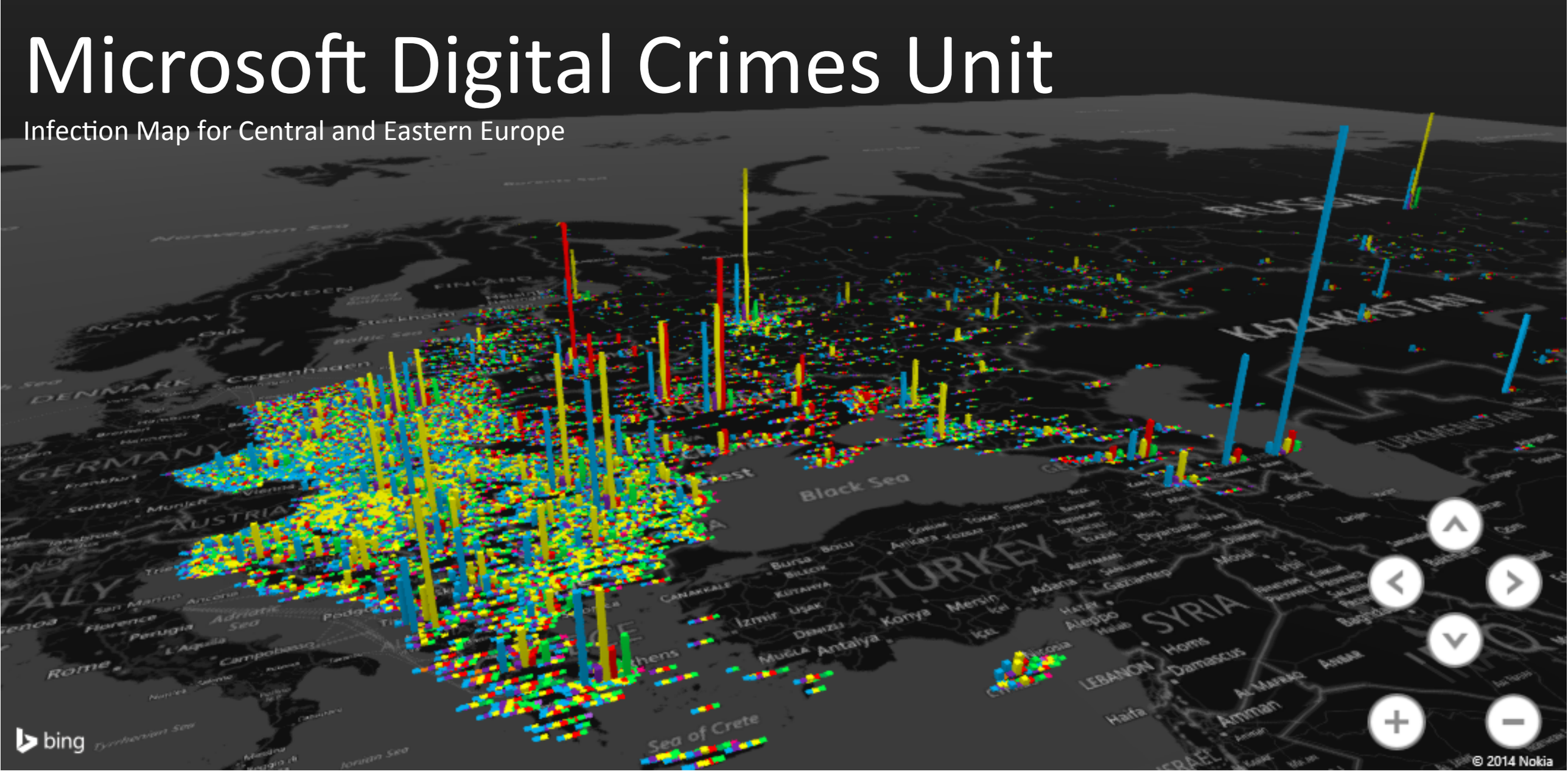




SCS 2014

Microsoft Digital Crimes Unit

Infection Map for Central and Eastern Europe

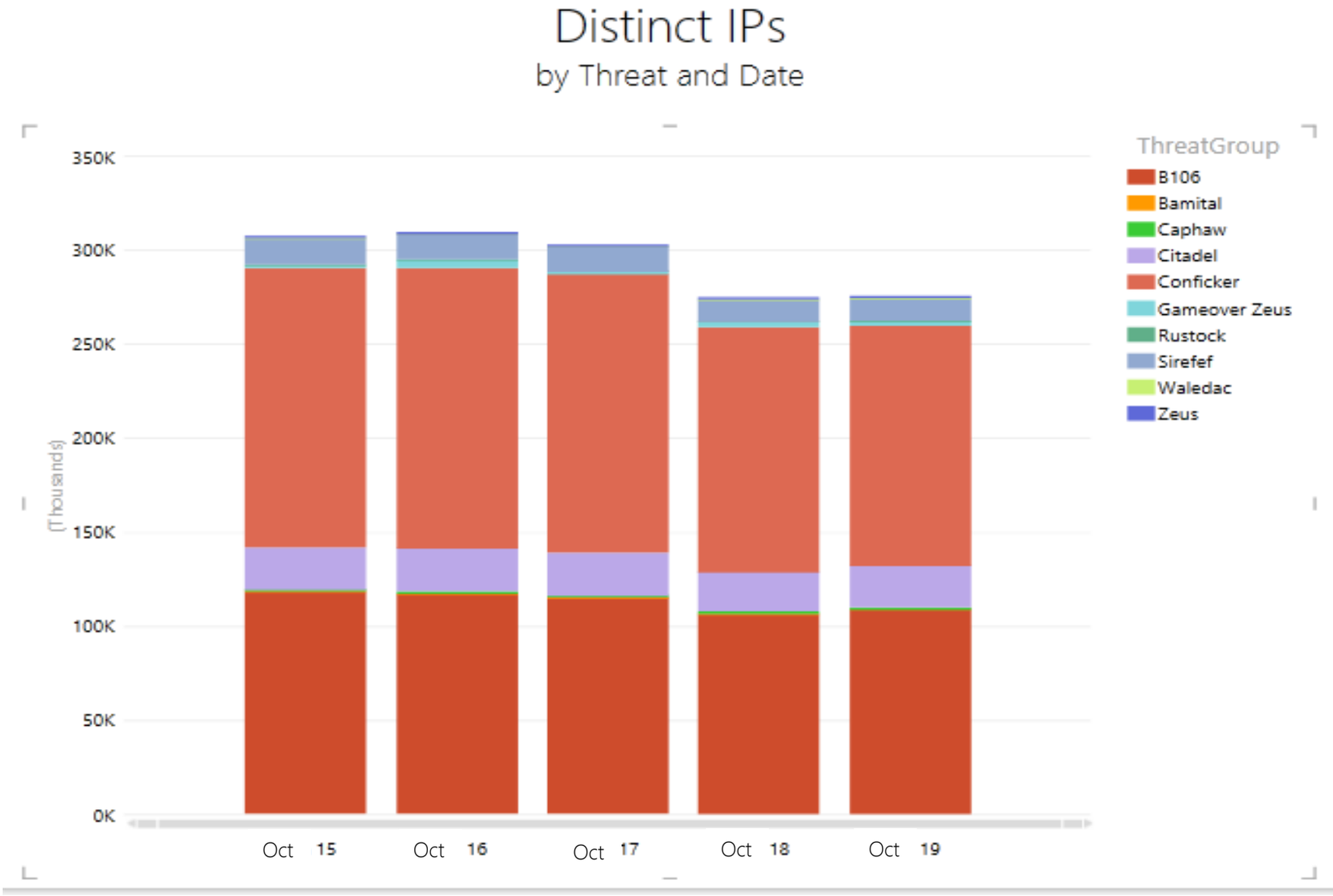


SCS 2014

Central and Eastern Europe Overview

The time frame is October 15th -19th, 2014.

The graphic shows the Distinct IPs connected to our Microsoft servers in CEE.



Poland Five Days Overview

The time frame is October 15th -19th, 2014.

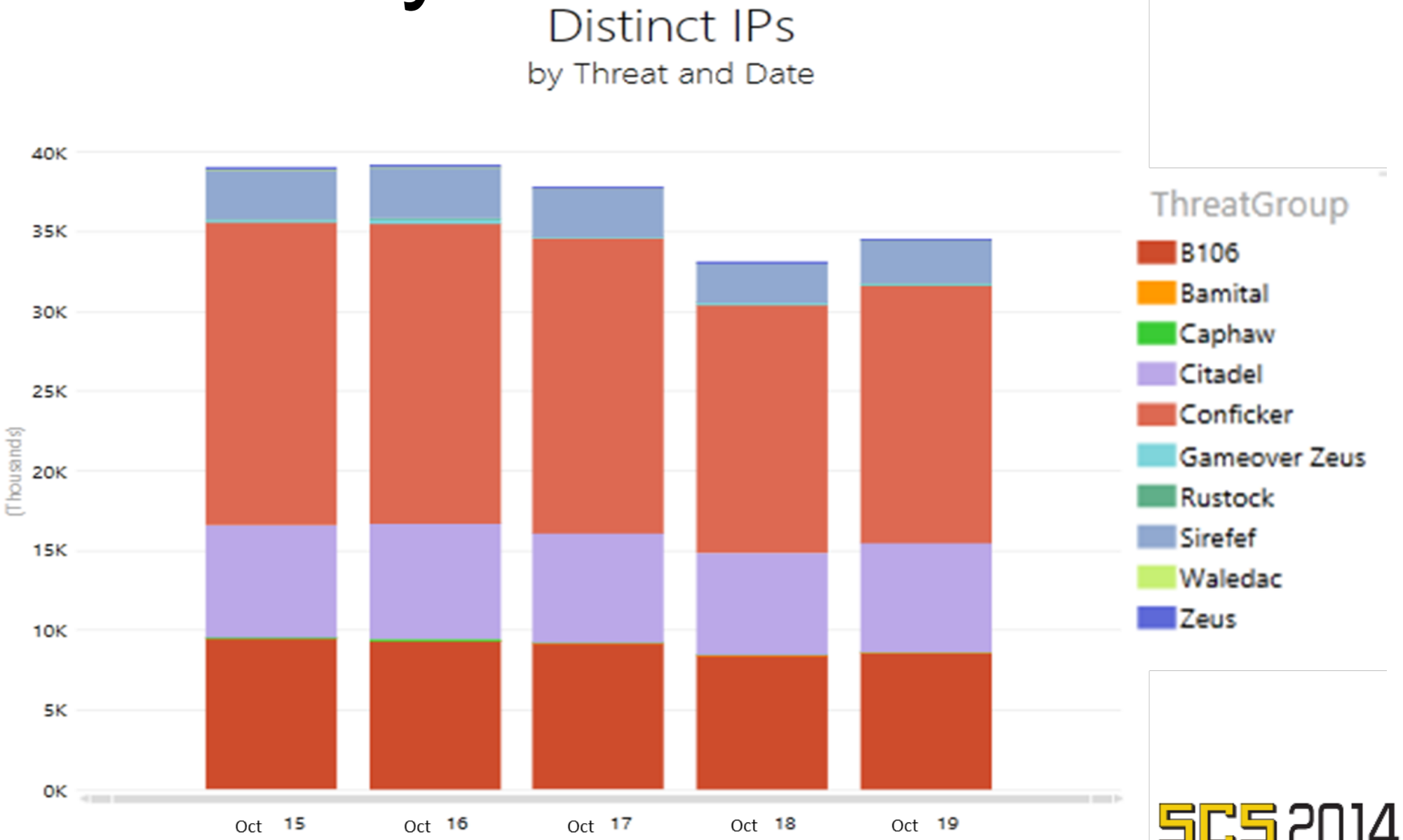
The graphic shows the distinct IPs in Poland through which the infected devices connect to Microsoft servers

SCS 2014

Poland Five days Overview

The time frame is October 15th -19th, 2014.

The graphic shows the distinct IPs in Poland through which the infected devices connect to Microsoft servers

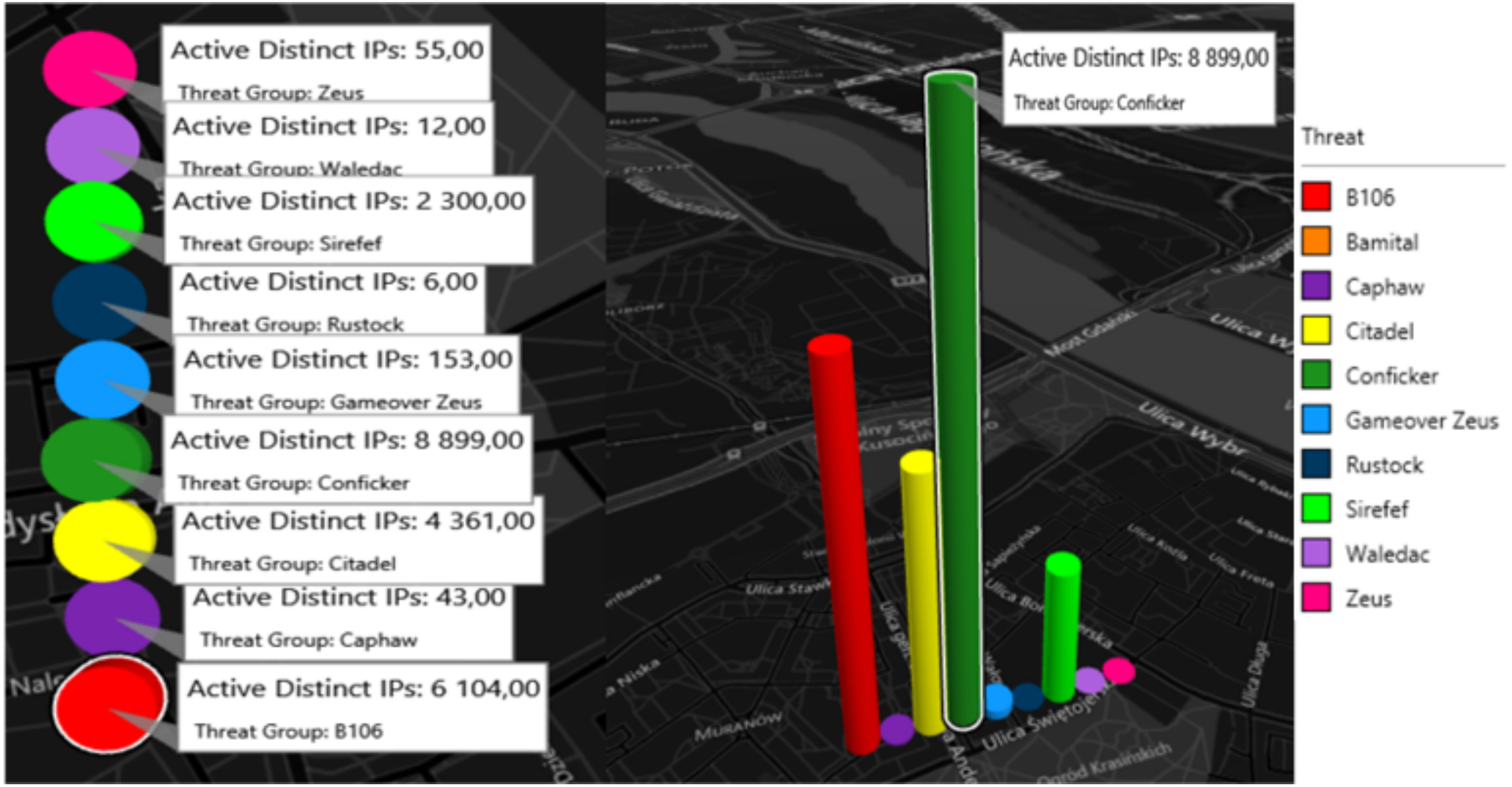


SCS 2014

Warsaw Five Days Overview

The time frame is October 15th -19th, 2014.

The graphic shows the distinct IPs in Poland through which the infected devices connect to Microsoft servers

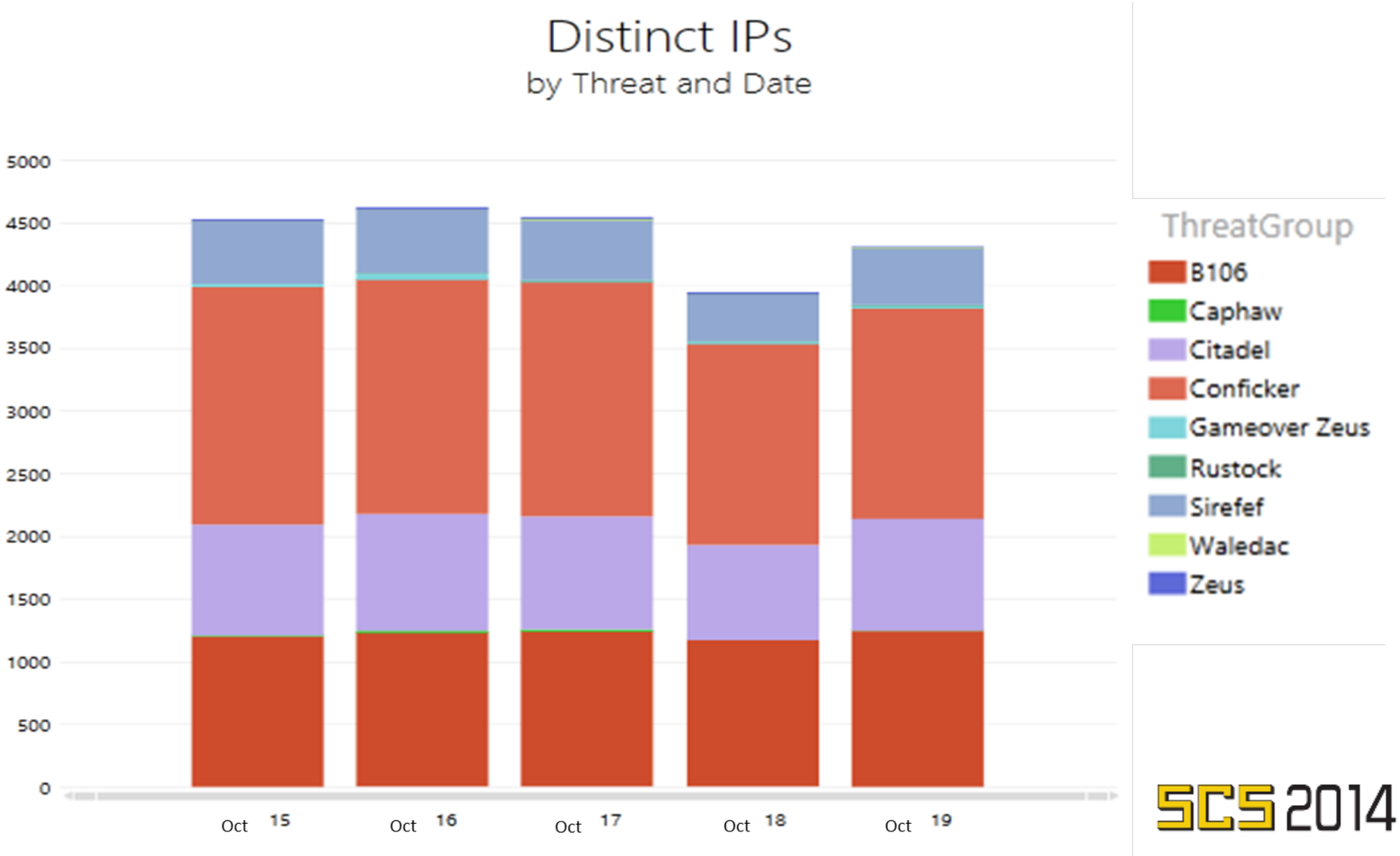


SCS 2014

Warsaw Five days Overview

The time frame is October 15th -19th, 2014.

The graphic shows the distinct IPs in Warsaw through which the infected devices connect to Microsoft servers



SCS 2014

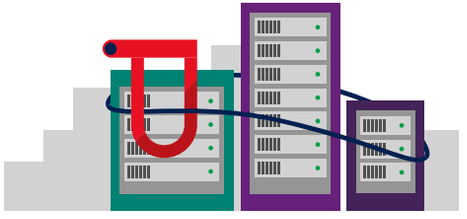
Most Common Malware Threats in Warsaw

OPERATION Conficker

February 2010

This family of worms can disable several important Windows services and security products. They can also download files and run malicious code on your PC if you have file sharing enabled

Botnet Worm



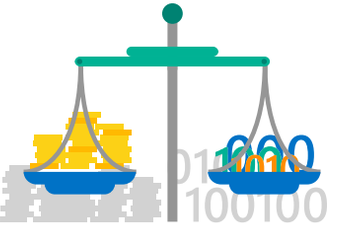
OPERATION b54 Citadel

June 2013

Citadel committed online financial fraud responsible for more than $500M in losses

Coordinated disruption with public-private sector partnerships to combat cybercrime

Identity Theft / Financial Fraud



OPERATION b68 ZeroAccess/Sirefef

December 2013

ZeroAccess or Sirefef hijacked search results, taking victims to dangerous sites

It cost online advertisers upwards of $2.7 million each month

Advertising Click Fraud

OPERATION b106 Bladabindi & Jenxcus

June 2014

Malware using Dynamic DNS for command. It involved password and identity theft, webcam and other privacy invasions

Over 200 different types of malware impacted by the take down

Identity Theft / Financial Fraud / Privacy Invasion

SCS 2014

MICROSOFT DIGITAL CRIMES UNIT

Botnets in September - October 2014

SCS 2014

Help us to help you… stay up to date

Workstyle 2001…
… still valid in 2014?

Software security does not follow the Lada car evolution model…

Already Retired Windows XP

Eliminate risks of Windows XP End of Support

Deployment tools and services available to assist in migration

Blog post from Tim Rains around the risks of XP after EOL:
http://blogs.technet.com/b/security/archive/2013/08/06/the-risk-of-running-windows-xp-after-support-ends.aspx

What Windows Server 2003 End of Support means

No updates

No compliance

Lack of PCI compliance could mean that Visa and MasterCard will no longer do business with your organization

Now is the time to act

37 critical updates released in 2013 for Windows Server 2003/ R2

Discontinued support for many applications

Migrate before July 2015

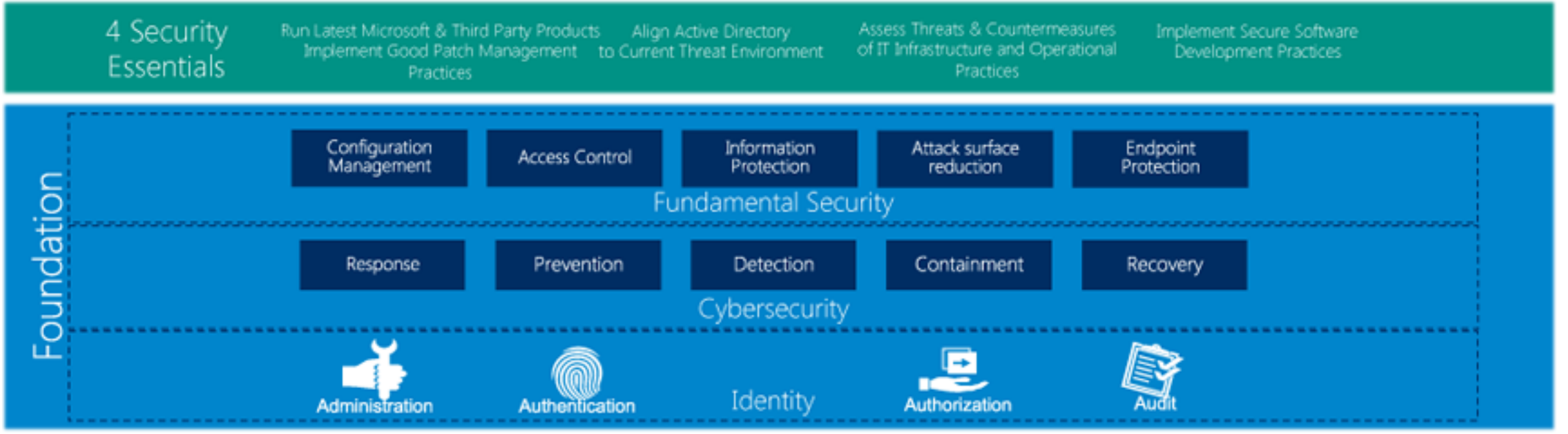
SCS 2014

CERT.GOV.PL info on Windows Server 2003 End of Support

SCS 2014

Summary

Summary - Security foundation



Useful Cybersecurity Resources

Security Response Center www.microsoft.com/security/msrc	Security Intelligence Report www.microsoft.com/security/sir	Security Development Lifecycle www.microsoft.com/sdl	Security TechCenter technet.microsoft.com/security	Microsoft Security Update Guide www.microsoft.com/securityupdateguide
Identity and Access www.microsoft.com/ida	Trustworthy Computing www.microsoft.com/twc	End to End Trust www.microsoft.com/endtoendtrust	Malware Protection Center www.microsoft.com/security/portal	Security Blog www.microsoft.com/about/twc/en/us/blogs.aspx

How the largest botnets were been taken down – the case studies

Thank you

robert.kosla@microsoft.com