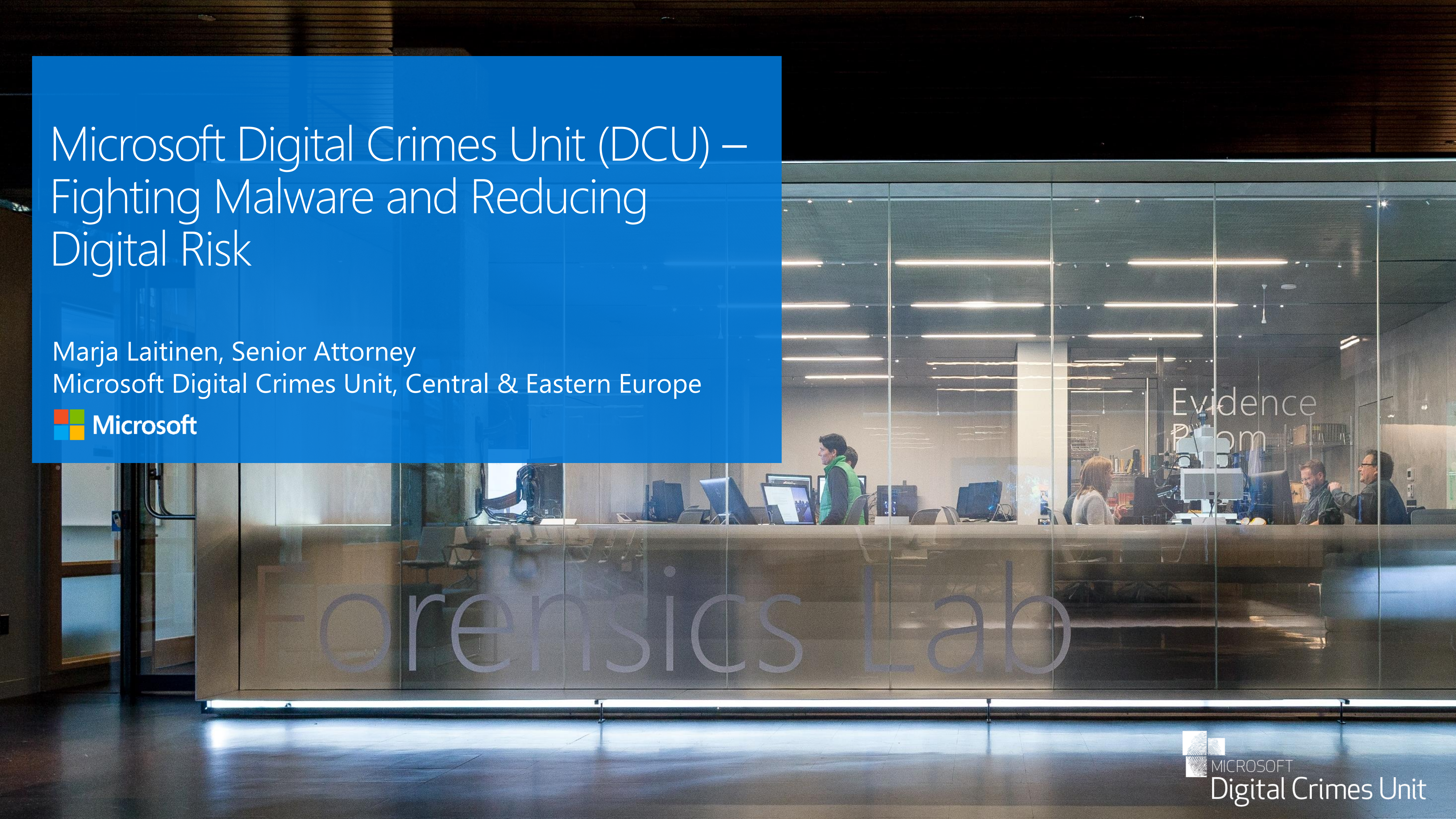
Microsoft Digital Crimes Unit (DCU) – Fighting Malware and Reducing Digital Risk

Marja Laitinen, Senior Attorney
Microsoft Digital Crimes Unit, Central & Eastern Europe

Microsoft



MICROSOFT
Digital Crimes Unit

"Cybersecurity is a CEO level issue."

McKinsey & Co, "Risk and responsibility in a hyperconnected world: Implications for enterprise, January 2014"

"There has been a significant rise in the cost of individual breaches. The overall cost of security breaches for all type of organizations has increased."

"**10%** of organizations that suffered a breach in the last year were so badly damaged by the attack that they had to change the nature of their business."

The Guardian, "INFORMATION SECURITY BREACHES SURVEY 2014"

200+
Median # of days **attackers are present** on a victim's network before detection

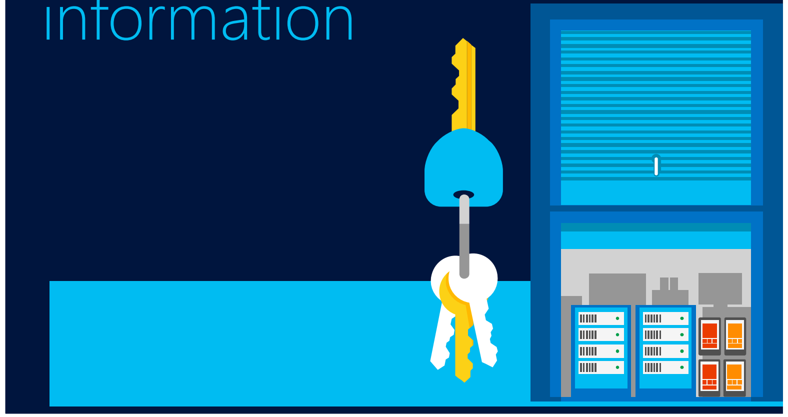
140
Estimated number of countries developing **cyber weapons**

Impact of cyber attacks could be as much as **$3 trillion** in **lost productivity** and growth

$3.5M
Average **cost of a data breach** to a company (15% YoY increase)

Microsoft is committed to protecting our customers and being a global cybersecurity advocate

We have **strong principles** and **policies** that empower **customers** to be in control of their information



We invest deeply in building a **trustworthy computing platform** and **security expertise**

We aggressively fight **cybercrime** and advocate extensively for enhancing **cybersecurity**

Compliance Security Advocacy

Privacy Risk management Transparency Governance

Digital Crimes Unit (DCU)

The Microsoft Digital Crimes Unit is committed to fighting cybercrime around the globe.

We use our expertise in data analytics, cyberforensics, and law to strategically partner with public and private organizations, law enforcement, and our customers – to protect the world from digital harm.

In our work we focus on fighting malware and reducing digital risk, and protecting vulnerable populations.

Protecting Vulnerable Populations

Senior fraud | Online child exploitation

Technical Support Scams

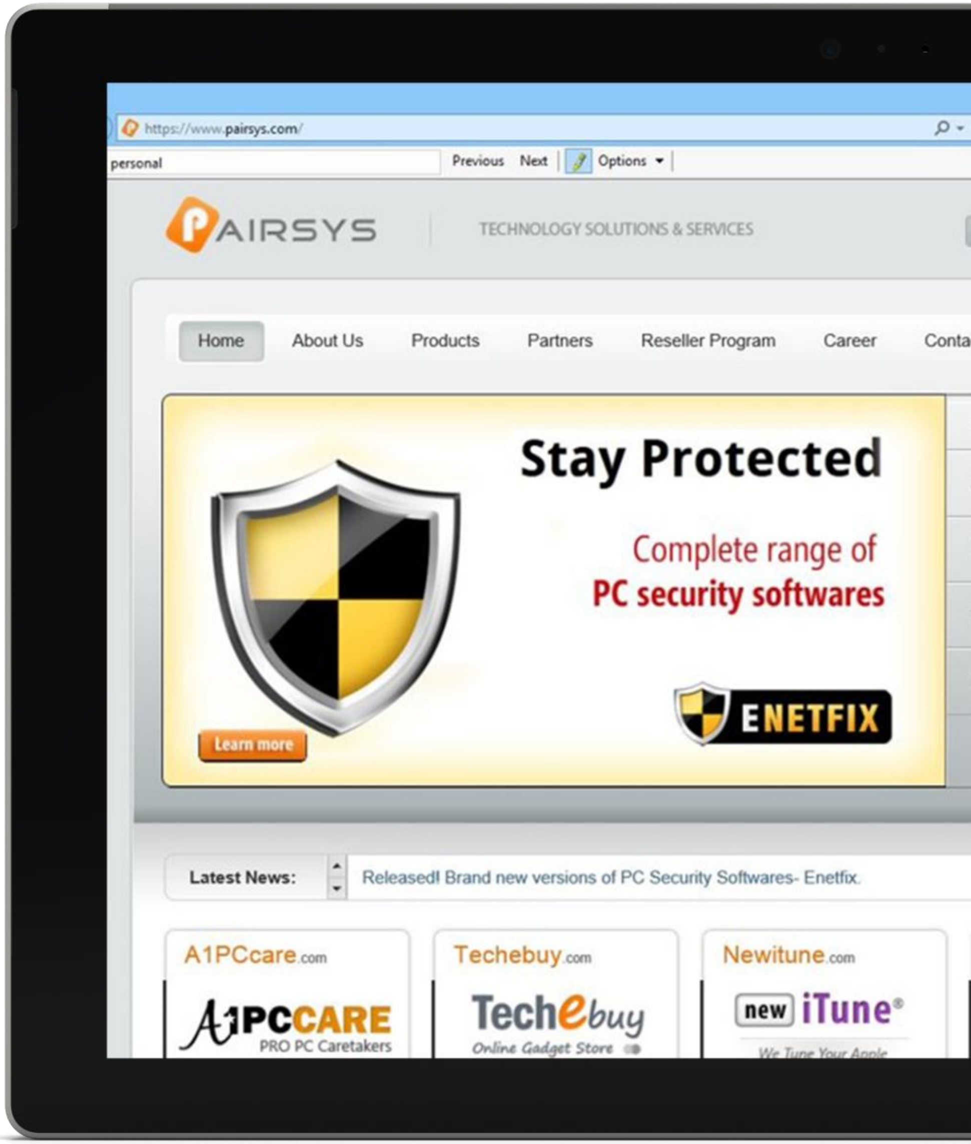
How the scam works

Fraudsters pose as technical support from Microsoft or another reputable tech company

Scams reach customers either by the cybercriminals calling victims, or by search engine ads directing customers to the fraudsters' websites

Victims give access to their PCs, pay for the fake service, and are harmed by the cybercriminals' malware and identity theft

3.3 million Americans become victims every year, suffering losses over $1.5 billion



https://www.pairsys.com/

personal

Latest News: Released! Brand new versions of PC Security Softwares- Enetfix.

The Problem

1 in 5 girls

1 in 10 boys

will be
sexually abused
by the age of 18.

500 images of sexually abused children will be traded online approximately every 60 seconds.

The Problem

1.8 billion images are uploaded and shared online **every single day.**

Finding a child sexual abuse image out of billions is like **finding a needle in a haystack.**

The Solution: Microsoft PhotoDNA

- Computes a unique hash of a known abusive image
- Converts image to black and white, re-sizing it, breaking it into a grid, and looking at intensity gradients or edges
- Hashes are resistant to alterations
- Law Enforcement – embedded in tools such as NetClean, BlueBear, ViziX, Autopsy, Access Data, PenLink, MCMSolutions, and others
- Industry Standard with over 70 enterprise customers

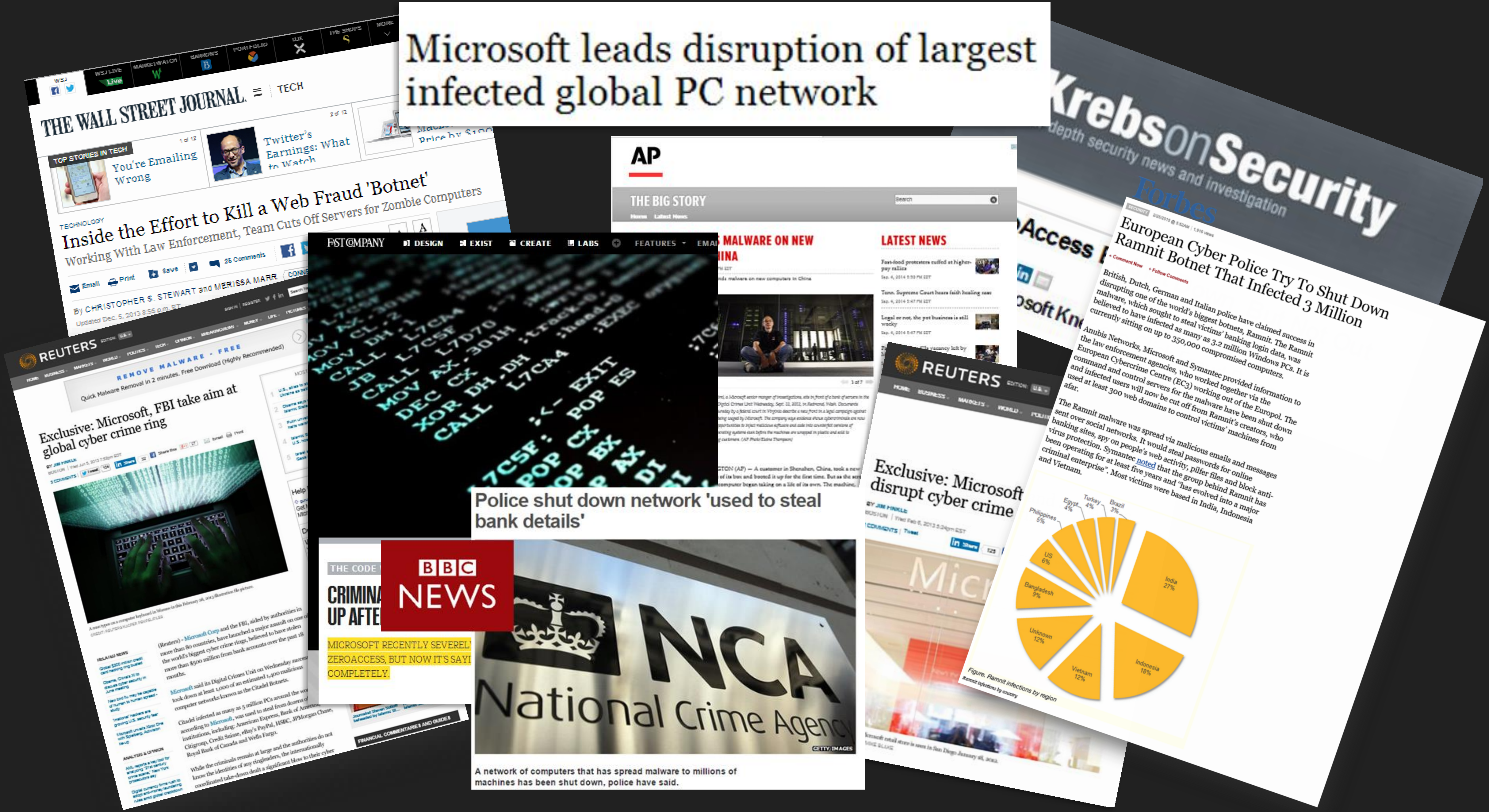
In 2014, 58 arrests from Microsoft's notifications to NCMEC

Free: Available via the Azure Marketplace

www.microsoft.com/photodna

Outlook.com facebook. bing Google OneDrive

Fighting Malware & Reducing Digital Risk



Microsoft leads disruption of largest infected global PC network

THE WALL STREET JOURNAL. TECH

TOP STORIES IN TECH

You're Emailing Wrong

Twitter's Earnings: What to Watch

TECHNOLOGY

Inside the Effort to Kill a Web Fraud 'Botnet'

Working With Law Enforcement, Team Cuts Off Servers for Zombie Computers

By CHRISTOPHER S. STEWART and MERISSA MARR

Updated Dec. 5, 2013 8:55 p.m. ET

AP

THE BIG STORY

…S MALWARE ON NEW …HINA

LATEST NEWS

Fast-food protesters cuffed at higher-pay rallies

Tenn. Supreme Court hears faith healing case

Legal or not, the pot business is still wacky

…GTON (AP) — A customer in Shenzhen, China, took a new … of its box and booted it up for the first time. But as the … computer began taking on a life of its own. The machine,

REUTERS

Exclusive: Microsoft, FBI take aim at global cyber crime ring

BY JIM FINKLE

(Reuters) - Microsoft Corp and the FBI, aided by authorities in more than 80 countries, have launched a major assault on one of the world's biggest cyber crime rings, believed to have stolen more than $500 million from bank accounts over the past 18 months.

Microsoft said its Digital Crimes Unit on Wednesday … took down at least 1,000 of an estimated 1,400 malicious computer networks known as the Citadel Botnets.

Citadel infected as many as 5 million PCs around the world … according to Microsoft, was used to steal from dozens of … institutions, including: American Express, Bank of America, Citigroup, Credit Suisse, eBay's PayPal, HSBC, JPMorgan Chase, Royal Bank of Canada and Wells Fargo.

While the criminals remain at large and the authorities do not know the identities of any ringleaders, the internationally coordinated take-down dealt a significant blow to their cyber …

FAST COMPANY

THE CODE …

CRIMINA… UP AFTE…

MICROSOFT RECENTLY SEVEREL… ZEROACCESS, BUT NOW IT'S SAYI… COMPLETELY.

BBC NEWS

Police shut down network 'used to steal bank details'

A network of computers that has spread malware to millions of machines has been shut down, police have said.

REUTERS

Exclusive: Microsoft … disrupt cyber crime …

KrebsonSecurity

In-depth security news and investigation

…Access …

…osoft Kn…

Forbes

European Cyber Police Try To Shut Down Ramnit Botnet That Infected 3 Million

British, Dutch, German and Italian police have claimed success in disrupting one of the world's biggest botnets, Ramnit. The Ramnit malware, which sought to steal victims' banking login data, was believed to have infected as many as 3.2 million Windows PCs. It is currently sitting on up to 350,000 compromised computers.

Anubis Networks, Microsoft and Symantec provided information to the law enforcement agencies, who worked together via the European Cybercrime Centre (EC3) working out of the Europol. The command and control servers for the malware have been shut down and infected users will now be cut off from Ramnit's creators, who used at least 300 web domains to control victims' machines from afar.

The Ramnit malware was spread via malicious emails and messages sent over social networks. It would steal passwords for online banking sites, spy on people's web activity, pilfer files and block anti-virus protection. Symantec noted that the group behind Ramnit has been operating for at least five years and "has evolved into a major criminal enterprise". Most victims were based in India, Indonesia and Vietnam.

Figure. Ramnit infections by region

DCU Botnet Takedowns and Malware Disruptions

Conficker

February 2010

Microsoft-lead model of industry-wide efforts to counter the threat

Botnet Worm sending SPAM and attempting to steal confidential data and passwords

b49 Waledac

February 2010

First MS takedown operation, proving the model of industry-led efforts

Disconnected70,000-90,000 infected devices from the botnet

Botnet Worm sending SPAM (1,5B)

b107 Rustock

March 2011

Supported by stakeholders across industry sectors

Involved US and Dutch law enforcement, and CN-CERT

SPAM, in average 192 spam messages per compromised machine per minute

b79 Kelihos

September 2011

Partnership between Microsoft and security software vendors

First operation with named defendant

SPAM, Bitcoin Mining, Distributed Denial of Service Attacks

b71 Zeus

March 2012

Cross-sector partnership with financial services

Focused on disruption because of technical complexity

Identity Theft / Financial Fraud

b70 Nitol

September 2012

Nitol was introduced in the supply chain relied on by Chinese consumers

Settled with operator of malicious domain

Malware Spreading, Distributed Denial of Service Attacks

b58 Bamital

February 2013

Bamital hijacked people's search results, took victims to dangerous sites

Takedown in collaboration with Symantec, proactive notification and cleanup process

Advertising Click Fraud

b54 Citadel

June 2013

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

Coordinated disruption with public-private sector

Identity Theft / Financial Fraud

b68 ZeroAccess

December 2013

ZeroAccess hijacked search results, taking victims to dangerous sites

It cost online advertisers upwards of $2.7 million each month

Advertising Click Fraud

b157 Game over Zeus

June 2014

GameoverZeus (GOZ) was a banking Trojan

Worked in partnership with LE providing Technical Remediation

Identity Theft / Financial Fraud

b106 Bladabindi & Jenxcus

June 2014

Malware using Dynamic DNS for command. It involved password and identity theft, webcam, etc.

Over 200 different types of malware impacted.

Identity Theft / Financial Fraud / Privacy Invasion

b93 Caphaw

July 2014

Caphaw was focused on online financial fraud responsible for more than $250M in losses

Coordinated disruption with public-private sector

Identity Theft / Financial Fraud

b75 Ramnit

February 2015

Module-based malware, stealing credential information from banking websites. Configured to hide itself.

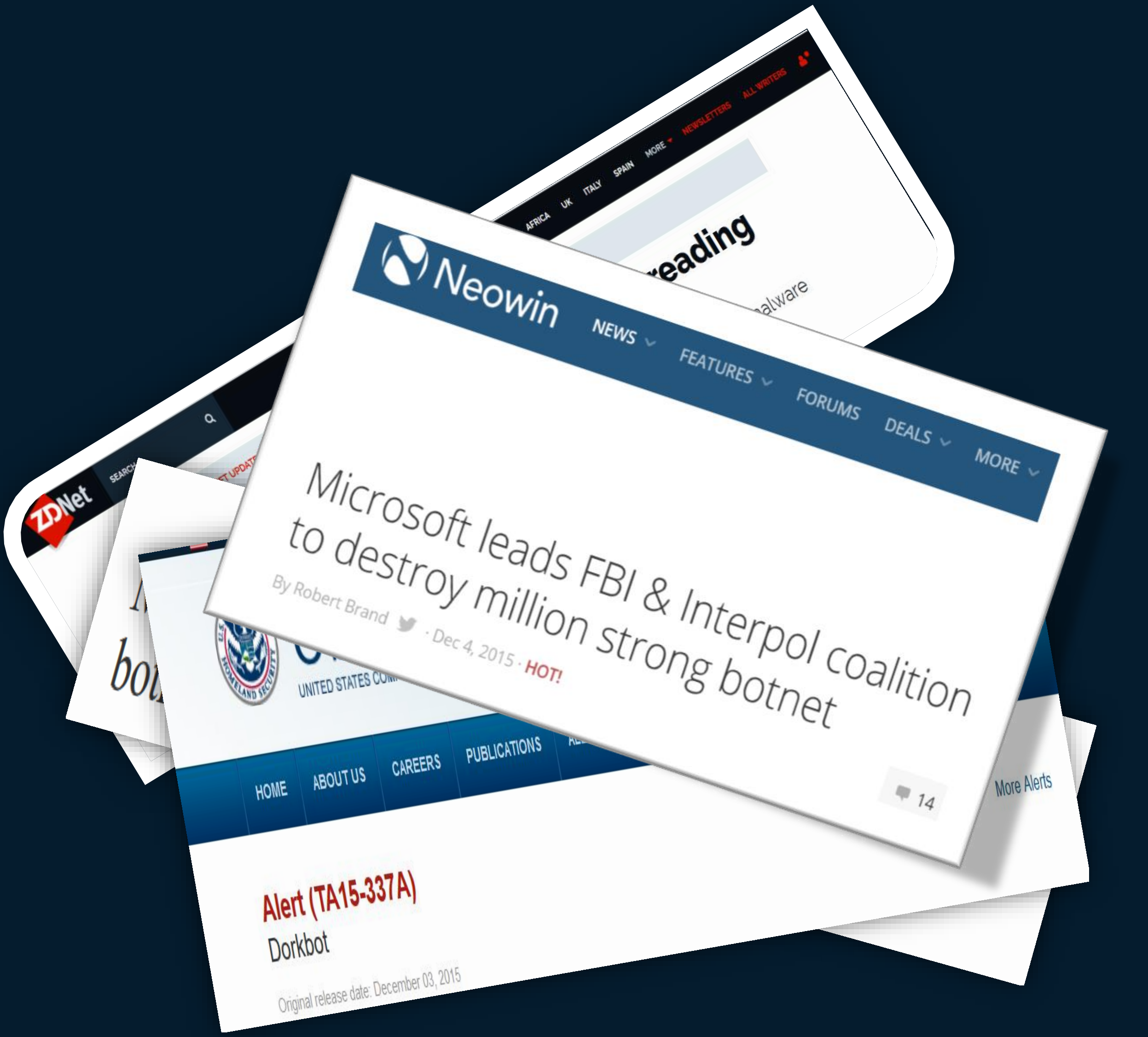
Credential Information Theft/Disable Security Defenses

b46 Simda

April 2015

Theft of personal details, including banking passwords, as well as to install and spread other malicious malware.

Theft personal data/Install and spread other malware



Microsoft leads FBI & Interpol coalition to destroy million strong botnet

By Robert Brand · Dec 4, 2015 · HOT!

14

Alert (TA15-337A)

Dorkbot

Original release date: December 03, 2015

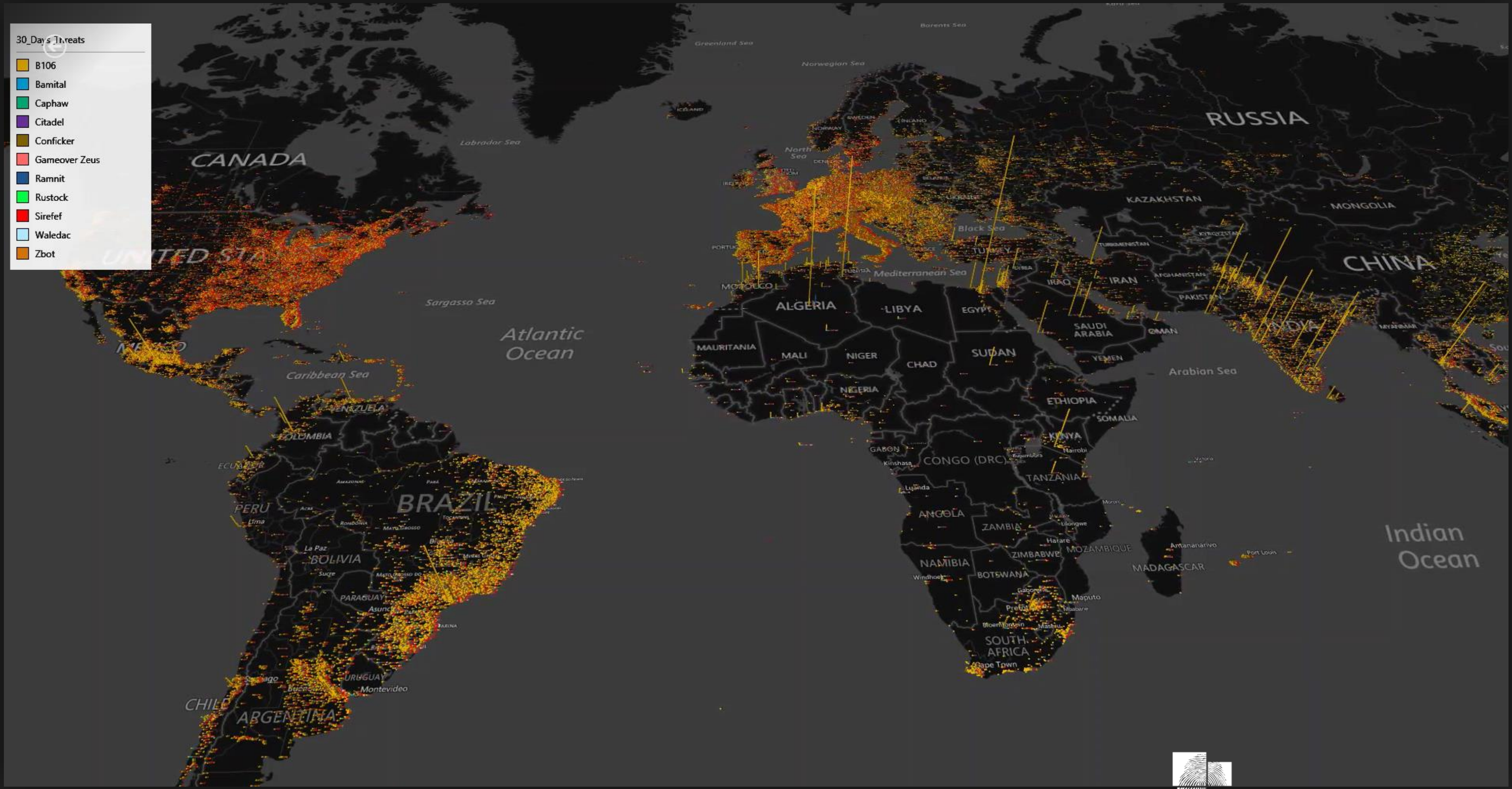
> Our latest disruption, “Dorkbot, a botnet used for cyber criminal activities such as **credential harvesting for financial fraud, DDoS attacks**, and the **downloading of malicious payloads**.”
>
> FBI release December 2015

Cyber Threat Intelligence Program (CTIP)

60 million IP addresses

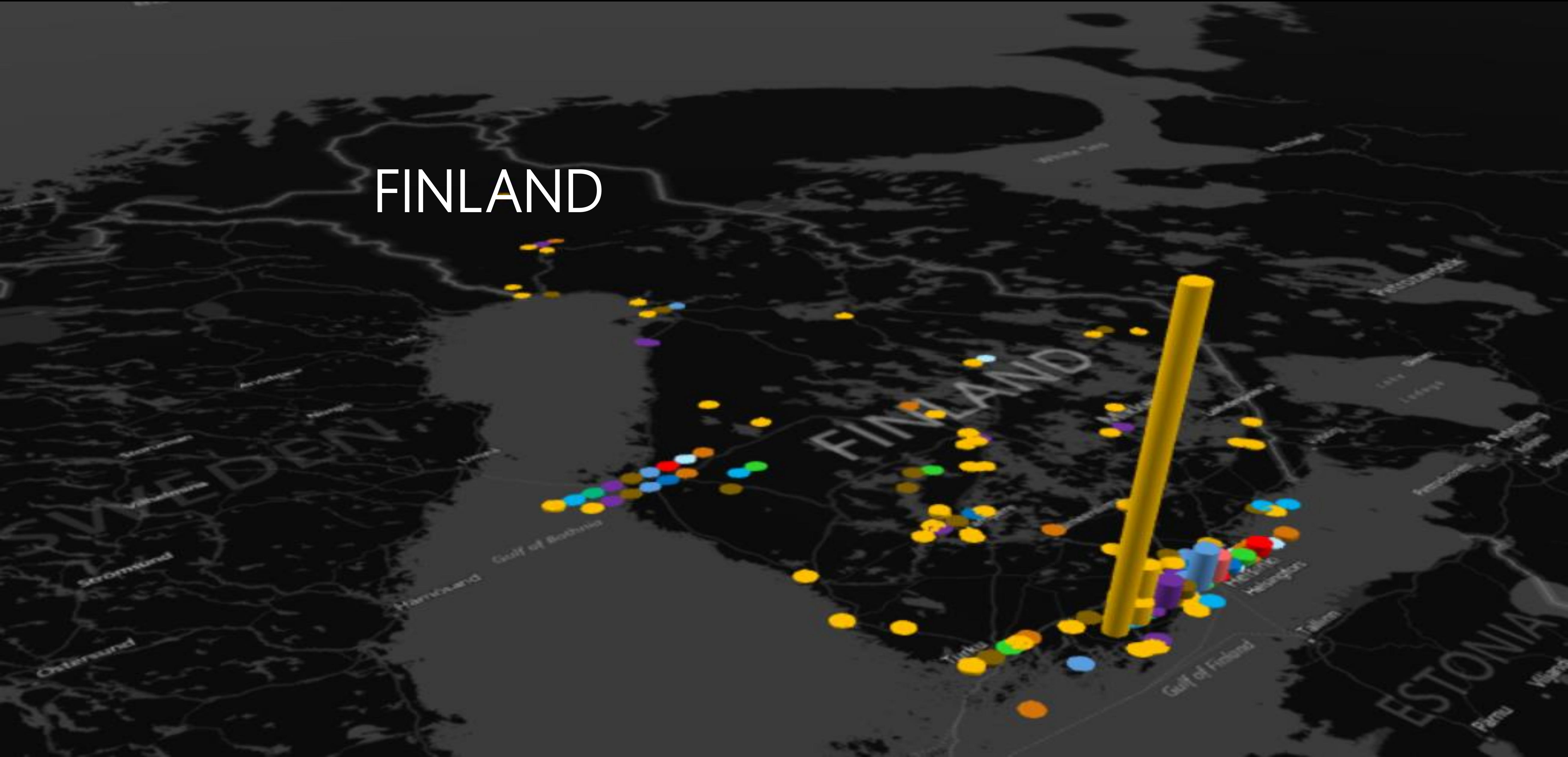
400 million pings/day

Volume constantly changing



MICROSOFT
Digital Crimes Unit

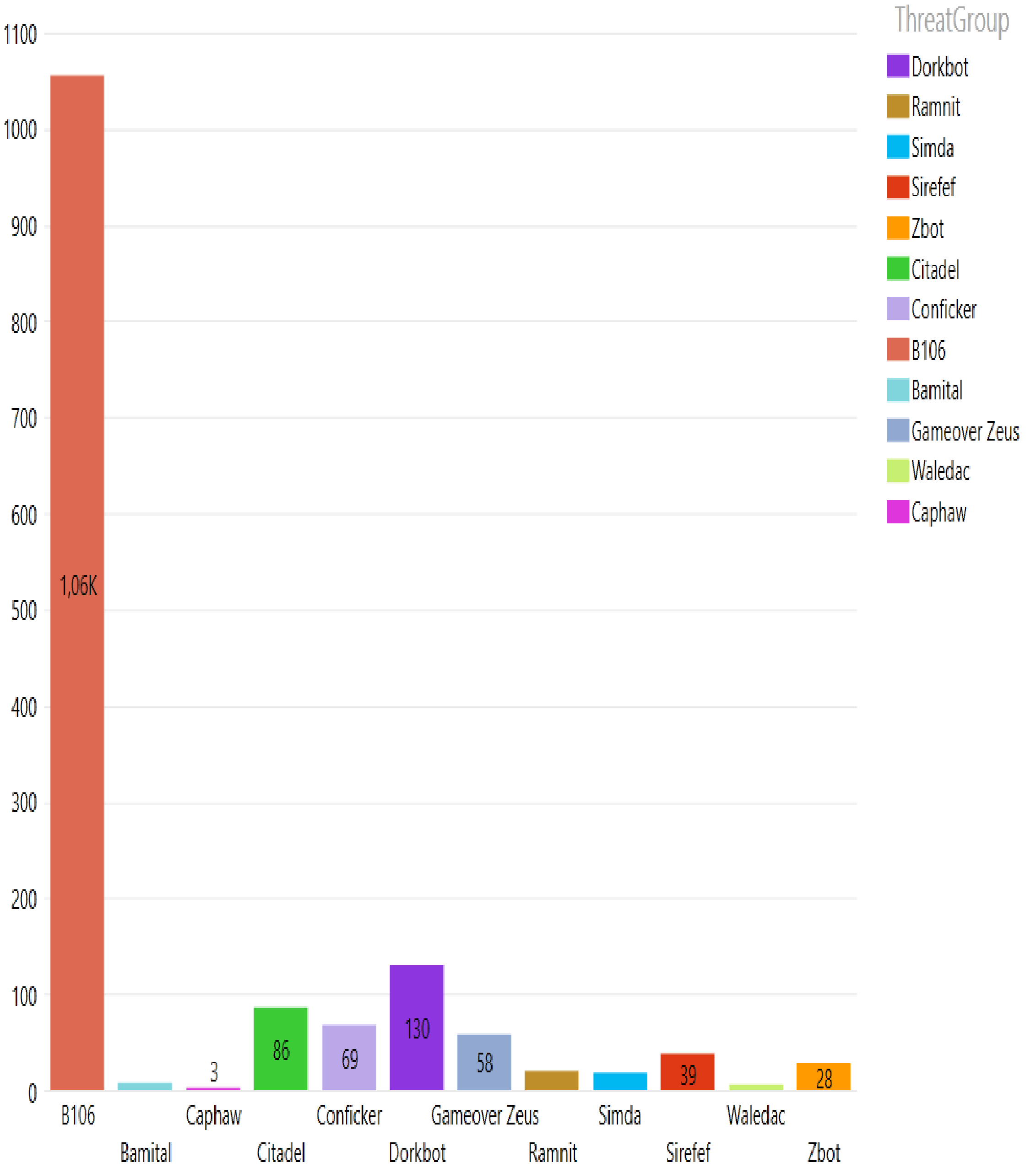
30 Day Malware Infection Powermap – December, 2015

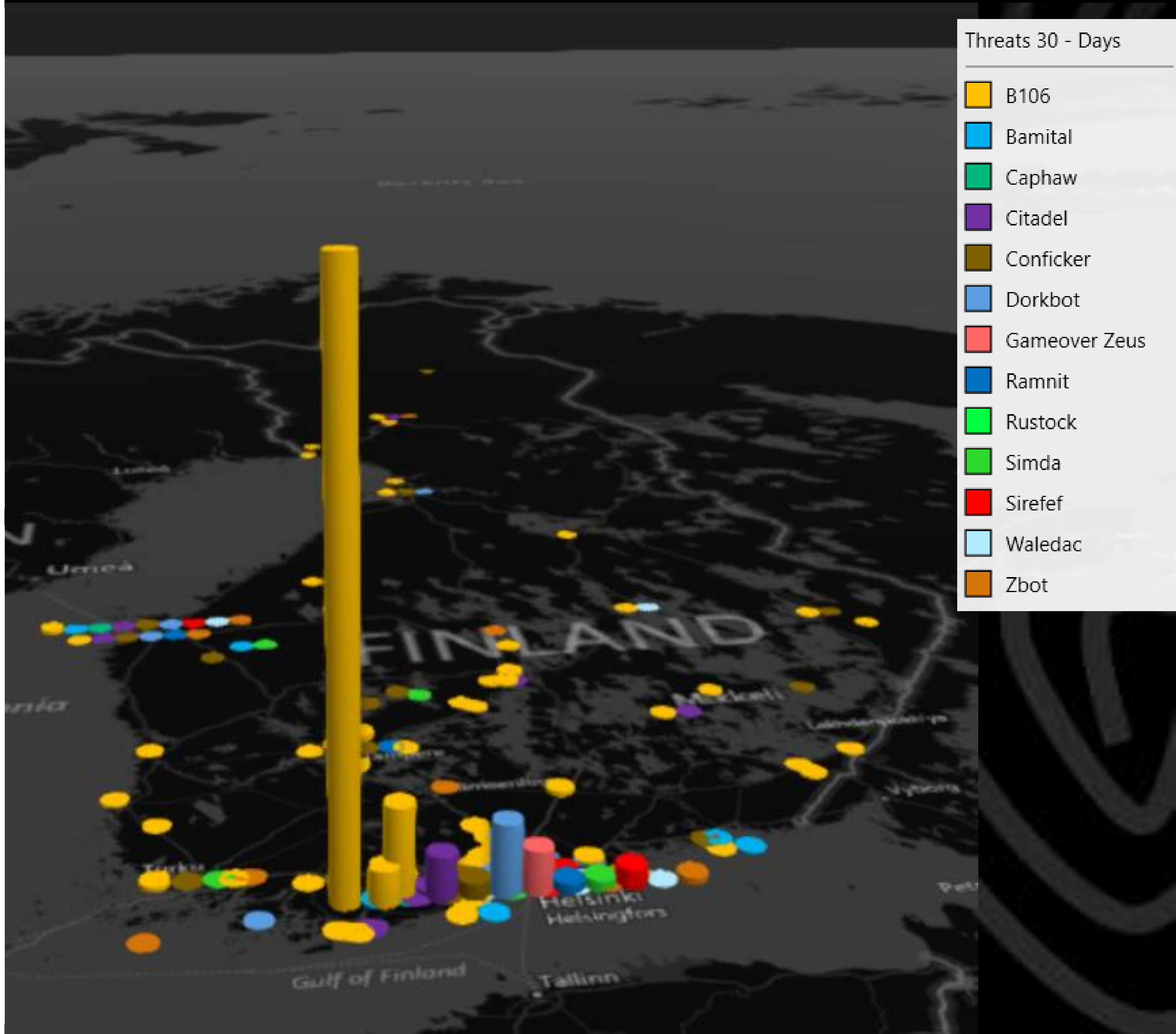


FINLAND

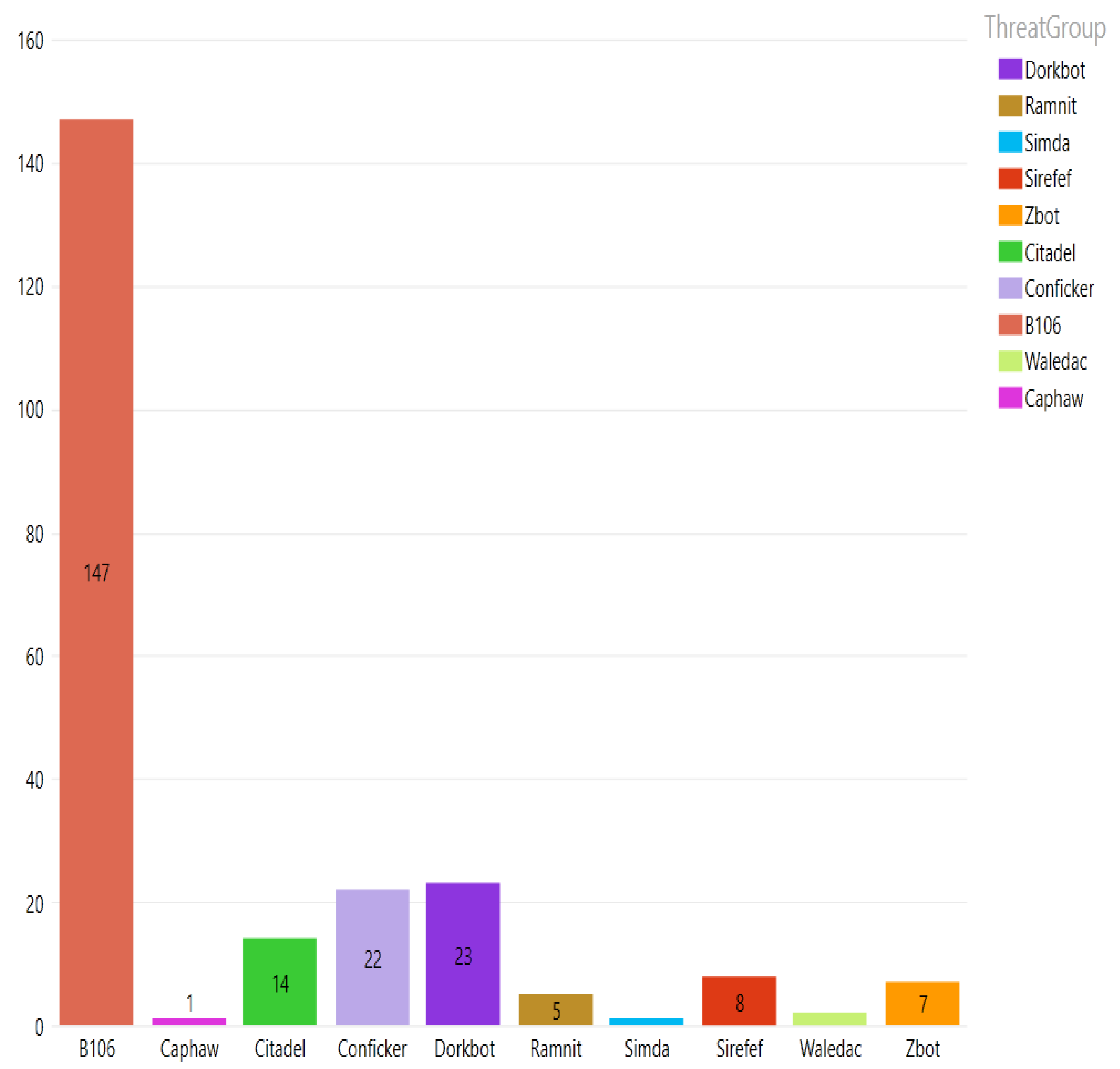
ICELAND
SWEDEN
FINLAND
NORWAY
RUSSIA
ASIA
Labrador Sea
CANADA
Hudson Bay
Gulf of Alaska
North Sea
UNITED KINGDOM
EUROPE
BELARUS
Sea of Okhotsk
NORTH AMERICA
GERMANY
POLAND
UKRAINE
KAZAKHSTAN
MONGOLIA
FRANCE
ROMANIA
ITALY
Black Sea
UZBEKISTAN
KYRGYZSTAN
UNITED STATES
SPAIN
TURKEY
TURKMENISTAN
JAPAN
TUNISIA
Mediterranean Sea
SYRIA
CHINA
Yellow Sea
MOROCCO
IRAQ
IRAN
AFGHANISTAN
East China Sea
Sargasso Sea
ALGERIA
LIBYA
EGYPT
PAKISTAN
Gulf of Mexico
SAUDI ARABIA
MEXICO
Atlantic Ocean
MAURITANIA
OMAN
INDIA
MALI
NIGER
SUDAN
Philippine Sea
Caribbean Sea
CHAD
YEMEN
Arabian Sea
Bay of Bengal
South China Sea
PHILIPPINES
Pacific Ocean
NIGERIA
VENEZUELA
ETHIOPIA
COLOMBIA
AFRICA
MALAYSIA
Gulf of Guinea
SOMALIA
KENYA
ECUADOR
GABON
INDONESIA
CONGO (DRC)
Java Sea
Banda Sea
PAPUA NEW GUINEA
TANZANIA
BRAZIL
PERU
ANGOLA
ZAMBIA
SOUTH AMERICA
BOLIVIA
Indian Ocean
NAMIBIA
BOTSWANA
MADAGASCAR
PARAGUAY
AUSTRALIA
SOUTH AFRICA
URUGUAY
CHILE
ARGENTINA

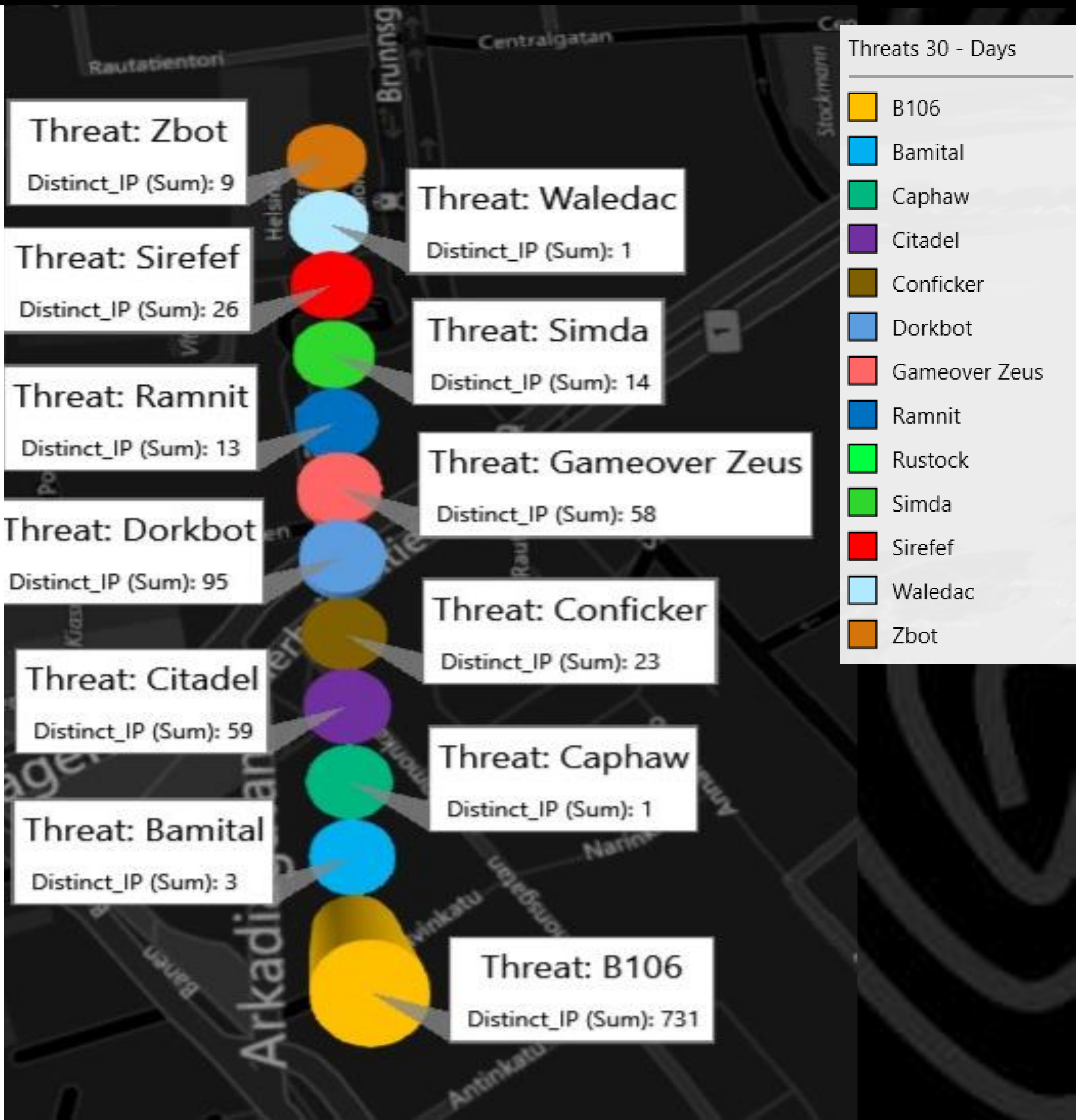
Finland – December, 2015



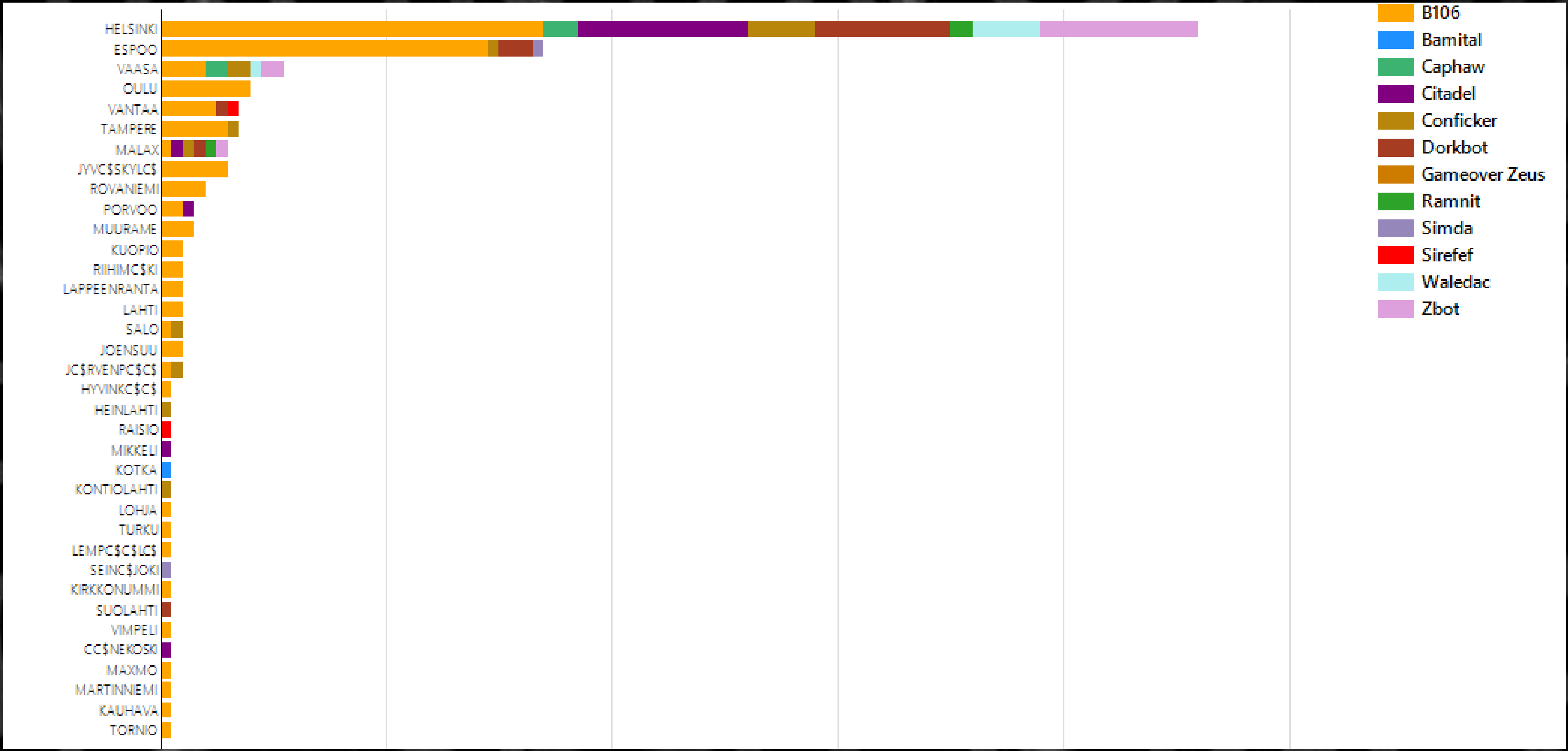


Helsinki – December, 2015





25 Top Cities in Finland by Threat December, 2015



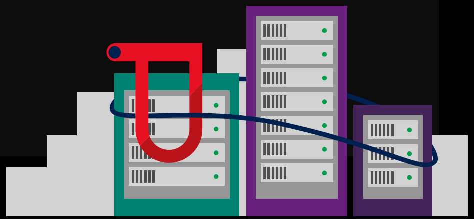
Most Common Malware Threats in Finland

Conficker
69

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



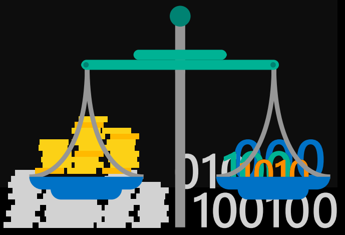
Citadel
86

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



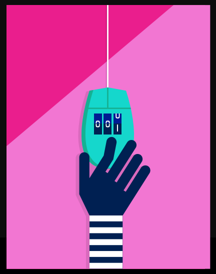
Bladabindi & Jenxcus
1 055

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



Dorkbot
130

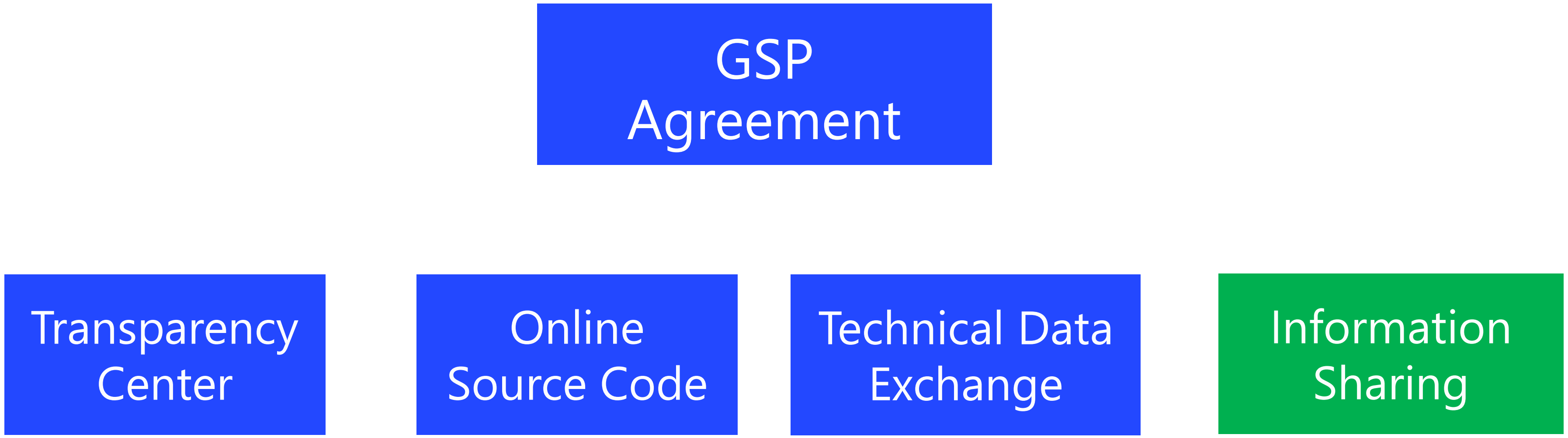
December 2015

Used for cyber criminal activities such as credential harvesting for financial fraud, DDoS attacks, and the downloading of malicious payloads. Disrupted in cooperation with FBI and international law enforcement.

Financial Fraud / DDoS attacks / Malicious Payloads

Partnering with governments

Government Security Program (GSP)



GSP Agreement

Transparency Center

Online Source Code

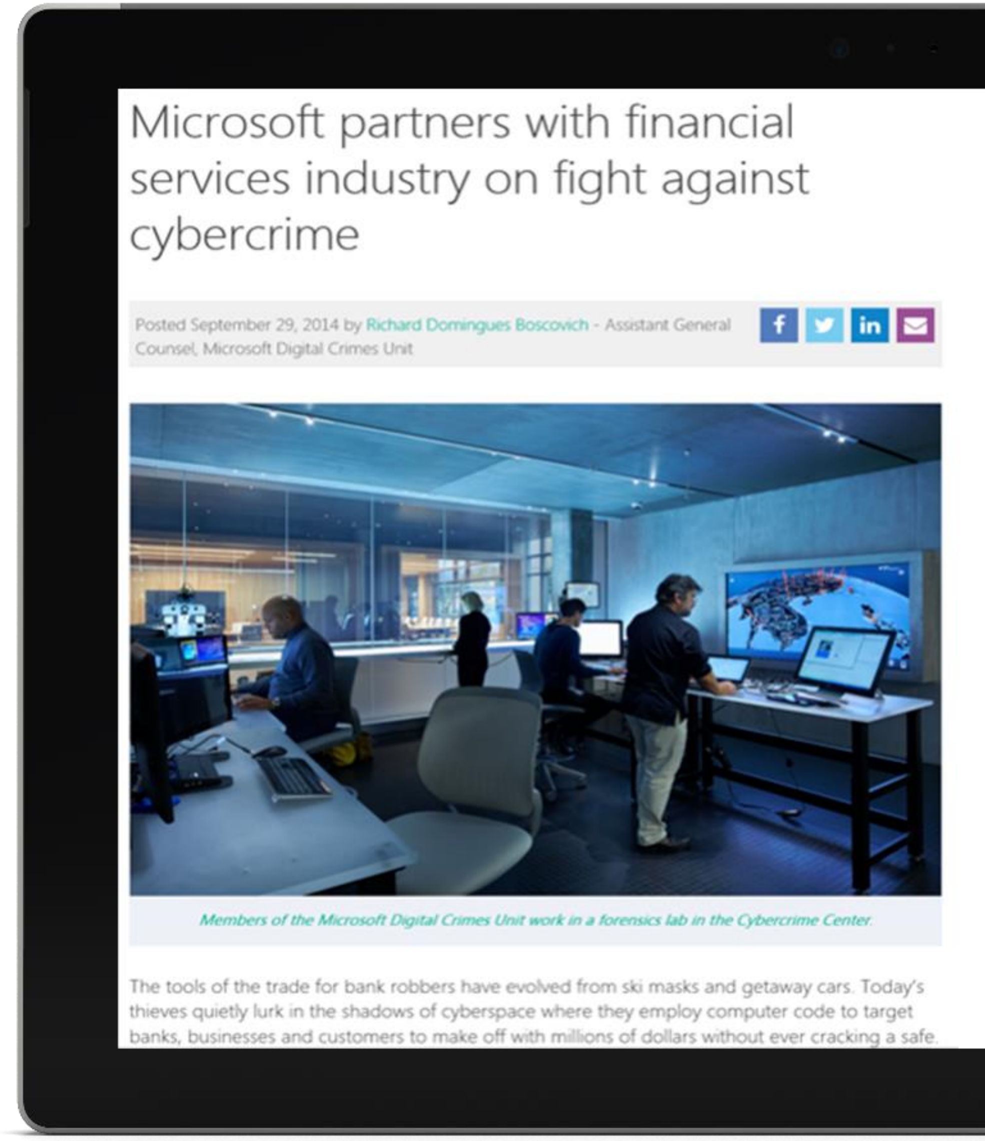
Technical Data Exchange

Information Sharing

Partnering with industry

On September 29, 2014, the Microsoft Digital Crimes Unit announced a partnership with Financial Services Information Sharing and Analysis Center **FS-ISAC**

FINANCIAL SERVICES | Information Sharing and Analysis Center



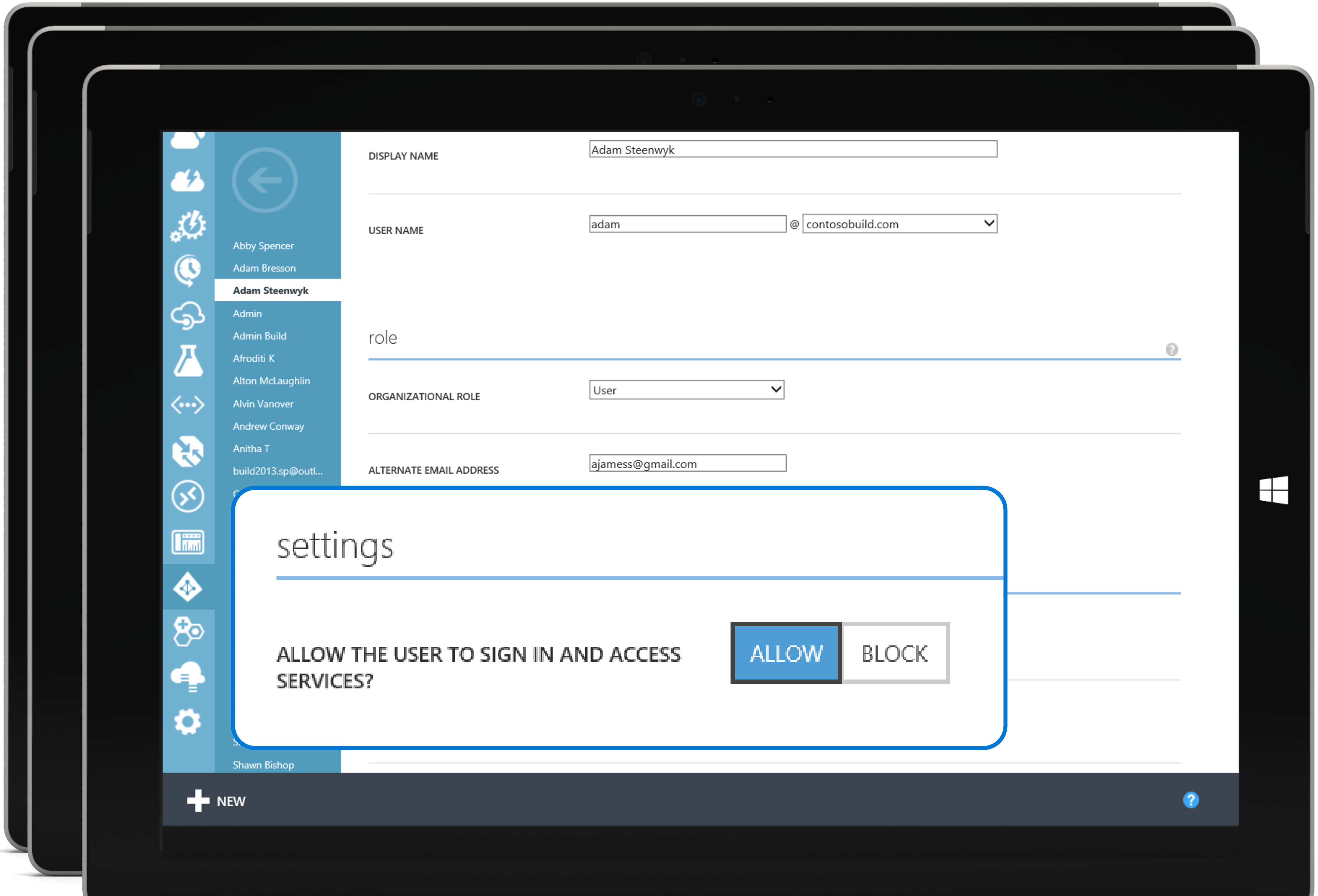
Microsoft partners with financial services industry on fight against cybercrime

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

Members of the Microsoft Digital Crimes Unit work in a forensics lab in the Cybercrime Center.

The tools of the trade for bank robbers have evolved from ski masks and getaway cars. Today's thieves quietly lurk in the shadows of cyberspace where they employ computer code to target banks, businesses and customers to make off with millions of dollars without ever cracking a safe.

Azure Active Directory Premium



Abby Spencer
Adam Bresson
Adam Steenwyk
Admin
Admin Build
Afroditi K
Alton McLaughlin
Alvin Vanover
Andrew Conway
Anitha T
build2013.sp@outl...
Shawn Bishop

DISPLAY NAME: Adam Steenwyk

USER NAME: adam @ contosobuild.com

role

ORGANIZATIONAL ROLE: User

ALTERNATE EMAIL ADDRESS: ajamess@gmail.com

settings

ALLOW THE USER TO SIGN IN AND ACCESS SERVICES? [✓ ALLOW] BLOCK

Protecting Your Organization And Yourself

- Re-invest in security fundamentals including robust identity management and strong authentication and leveraging anti-virus products
- Inspect your business processes, suppliers, and org practices, not just your technology
- Understand your potential Digital Risk working with your technology partners
- Download Free Tools to Clean Up Machines: http://www.microsoft.com/security/portal/mmpc/products/default.aspx

Microsoft

Thank You!