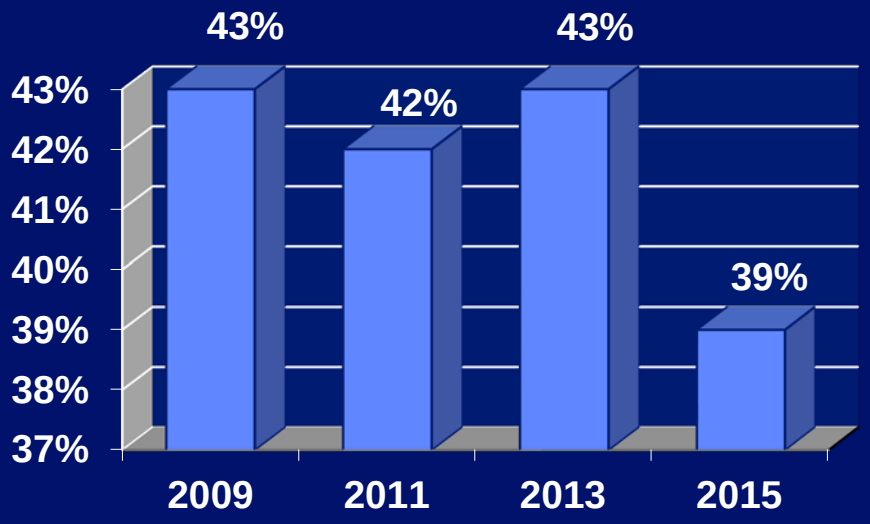
Unlicensed Software and Cyber Threats

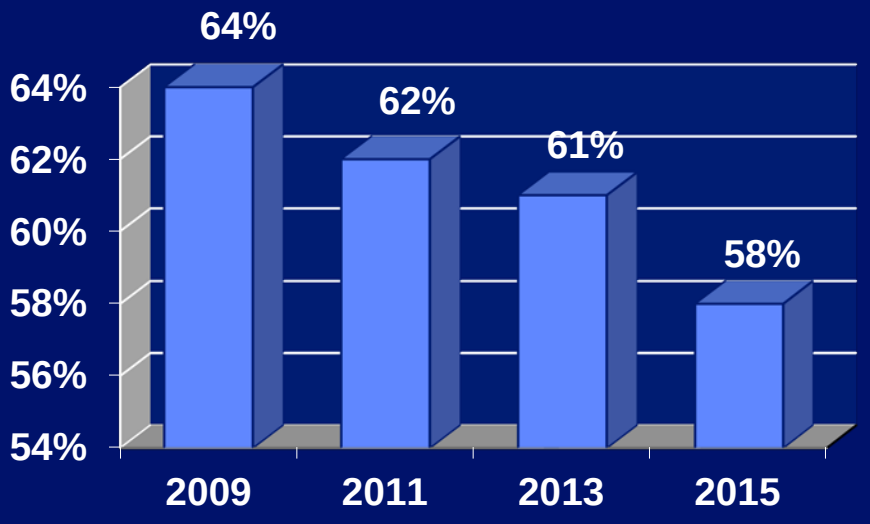
Magda Popescu
BSA Outside Counsel, Romania
Microsoft Regional Outside Counsel, CEE New Markets

27.09.2016

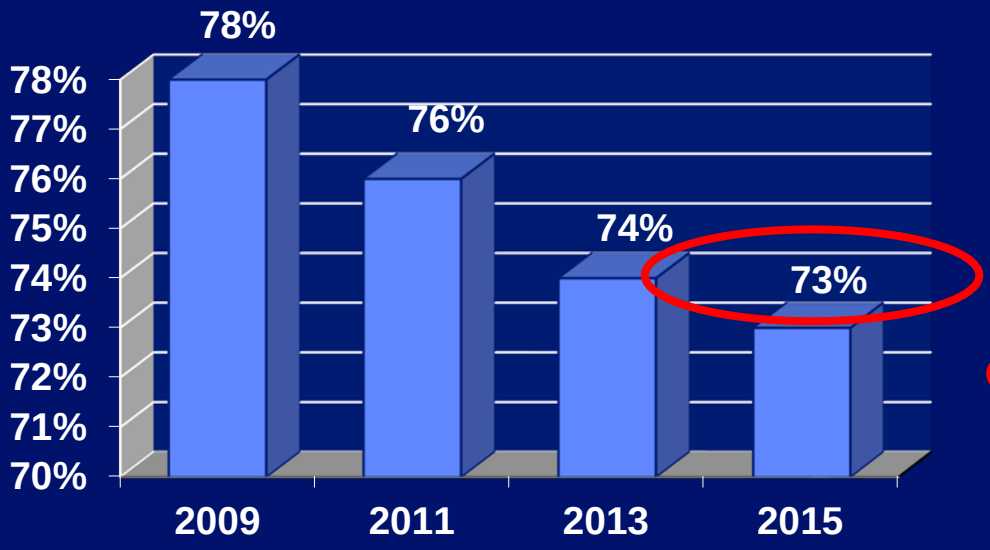
BSA Global Software Survey (May 2016)



World Wide
2015 – 52.24 billion US$ losses



CEE
2015 – 3.13 billion US$ losses

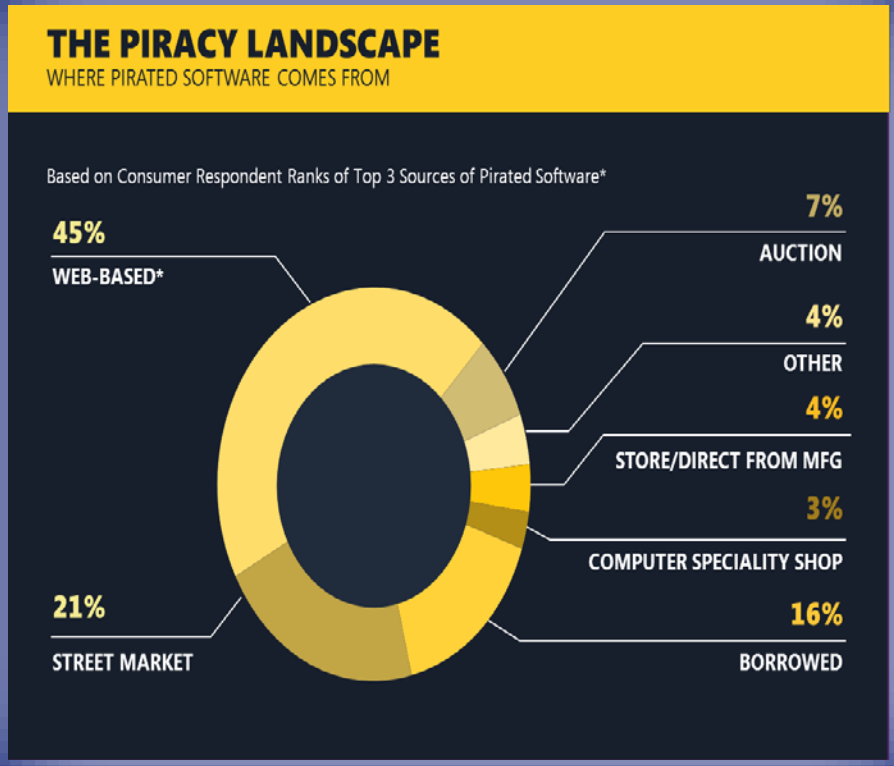


Kazakhstan
2015 – 89 million US$ losses

Growing Trends in Online Piracy

Cybercriminals are:

- Adapting, getting smarter, and going where the money is
- Transitioning from physical counterfeit discs to download business model
- Utilizing more sophisticated techniques to advertise via spam sent through botnets and Trojan-hijacked PCs



Connection between Piracy and Malware…

OF THE 203 COMPUTERS PURCHASED IN 11 COUNTRIES WITH PIRATED SOFTWARE ON THEM,

61%

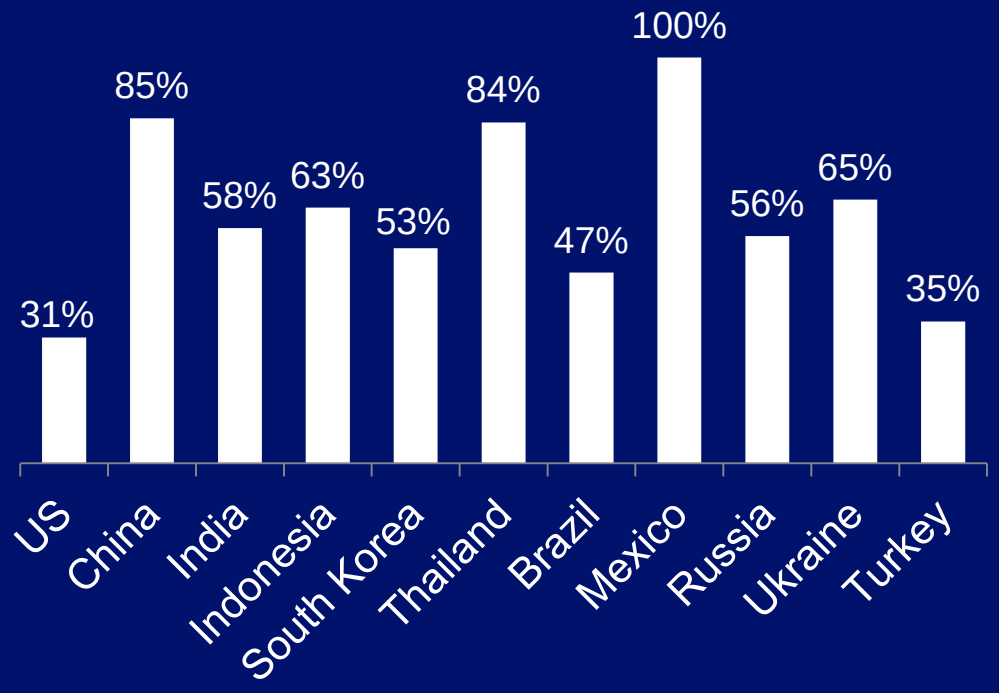
WERE

INFECTED

WITH DANGEROUS

MALWARE.

New PCs sold with pirated software infected with malware



Connection between Piracy and Malware…

- Unlicensed software – Malware = 0.79
- Smoking – Lung cancer = 0.72
- Education – Income = 0.77
- Anti-corruption policies - Economic growth = 0.77

IDC White Paper, Feb. 18, 2015 - correlation between the Unlicensed Software Use Rate* and Malware Encounter Rate**

*BSA Bi-Annual Global Software Survey 2014
**Microsoft Security Intelligence Report (SIR)

FBI alert – pirated software may contain malware

www.fbi.gov/news/stories/2013/august/pirated-software-may-contain-malware

Aplicații | Suggested Sites | Legal2m Private Sha... | www.oriunde.net/ut...

THE FBI FEDERAL BUREAU OF INVESTIGATION

CONTACT US | ABOUT US | MOST WANTED | NEWS | STATS &

Stories

Home • News • Stories • 2013 • August • Pirated Software May Contain Malware

Twitter (79) Facebook (1,280) Share

Pirated software like this could be laced with malicious software, or malware.

Consumer Alert

Pirated Software May Contain Malware

08/01/13

You decide to order some software from an unknown online seller. The price is so low you just can't pass it up. What could go wrong?

Plenty. Whether you're downloading it or buying a physical disc, the odds are good that the product is pirated and laced with malicious software, or malware.

Today, the National Intellectual Property Rights Coordination (IPR) Center—of which the FBI is a key partner—is warning the American people about the real possibility that illegally copied software, including counterfeit products made to look authentic, could contain malware.

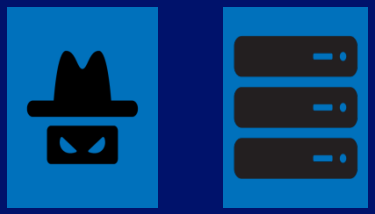
Is Your Software Pirated?

Possible signs of what to look for:

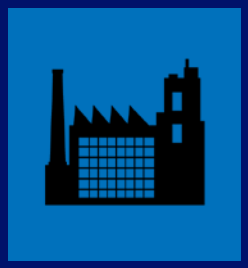
- No packaging, invoice, or other documentation...just a disc in an envelope

…and Malware, Botnets and Organized Crime

Organized Crime



Unsecure Supply Chain



Botnet

- Botnet is a network of infected computers controlled from a distance by a commanding computer.
- Botnets are typically created through infecting devices - usually by sending fraudulent emails asking users to open an attachment or click on a link infected with malware
- Computers and other digital devices that are acquired from unknown or unauthorized sources can contain malware that connects them to a Botnet operated by Cybercriminals

Cybersecurity is a Boardroom-Level Issue

430M
new pieces of malware were discovered in 2015, up 36 percent from 2014

71%
of companies admit they fell victim to a successful cyber attack the prior year

556M
victims of cybercrime per year

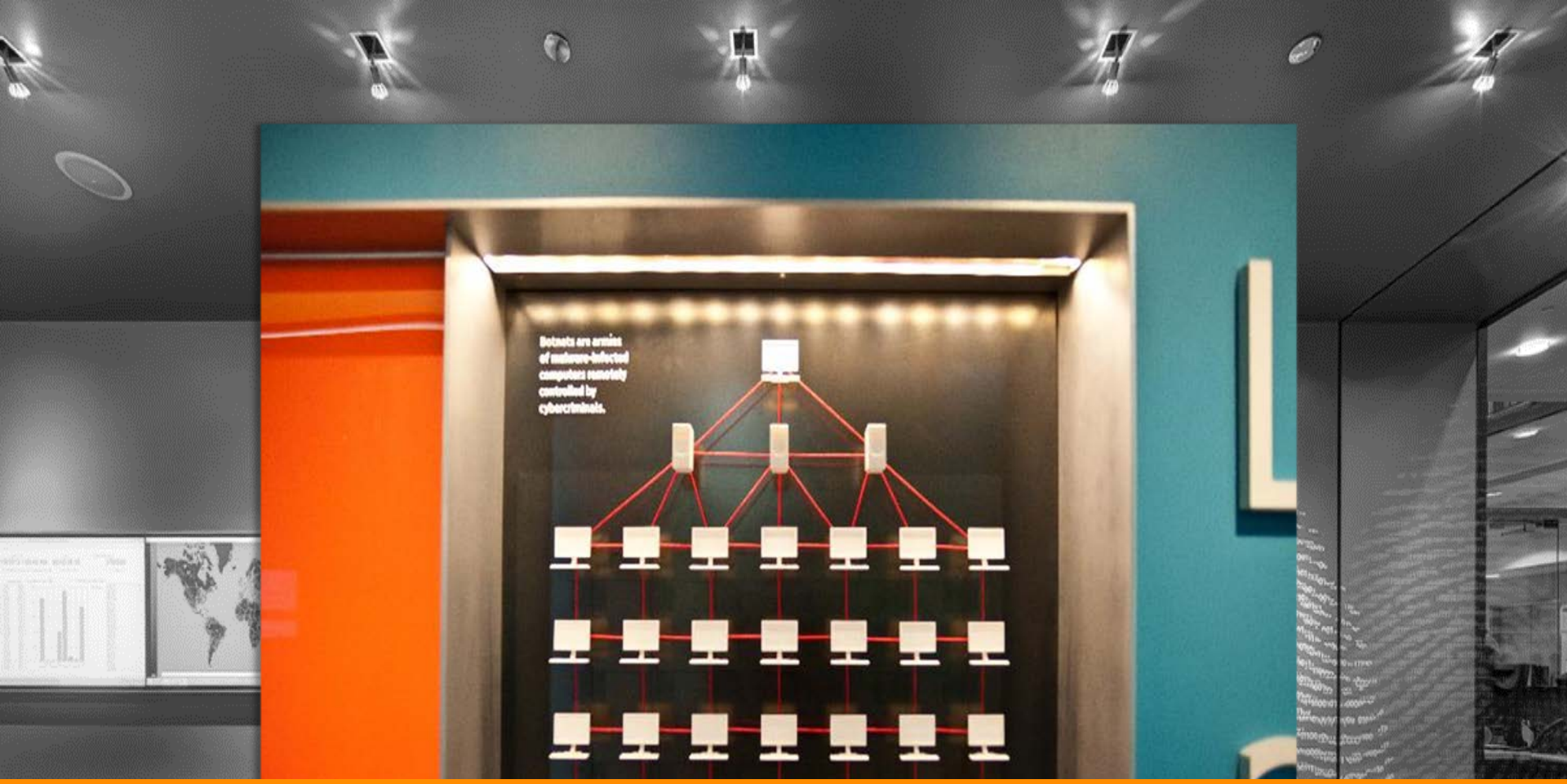
$3 Trillion
estimated cost in economic value from cybercrime industry by 2020

160M
Data records compromised from top 8 breaches in 2015

$400B
cost of cyberattacks to companies each year

63
Vulnerabilities (key-loggers, viruses, Trojans) in Windows ZverCD, the most popular pirate version of Windows in CIS

140+
Median # of days between infiltration and detection



Fighting Malware and Reducing Digital Risk

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

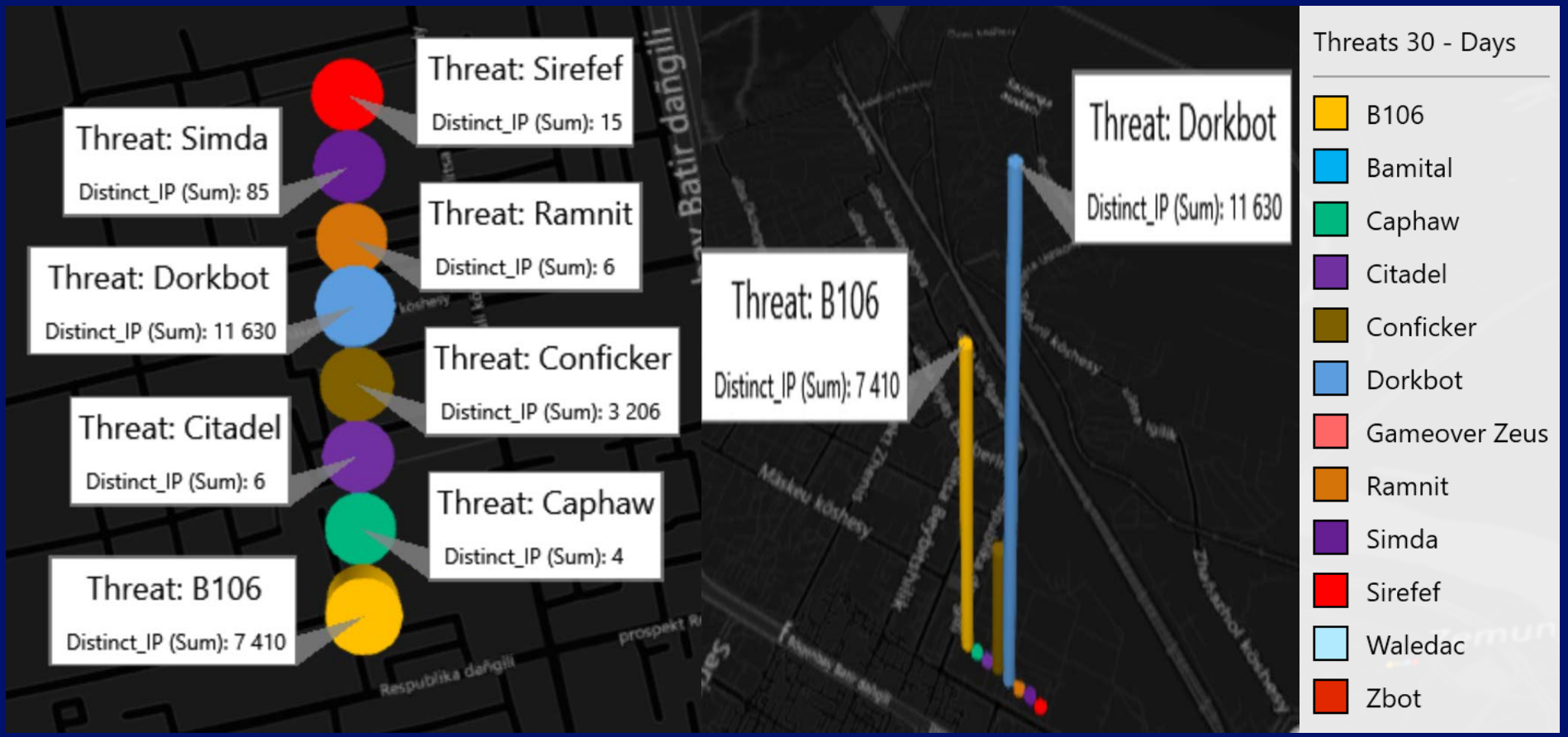
OPERATION Dorkbot

December 2015

Used for Cybercriminal activities such as credential harvesting for financial fraud DDoS attacks and the downloading of malicious payloads.

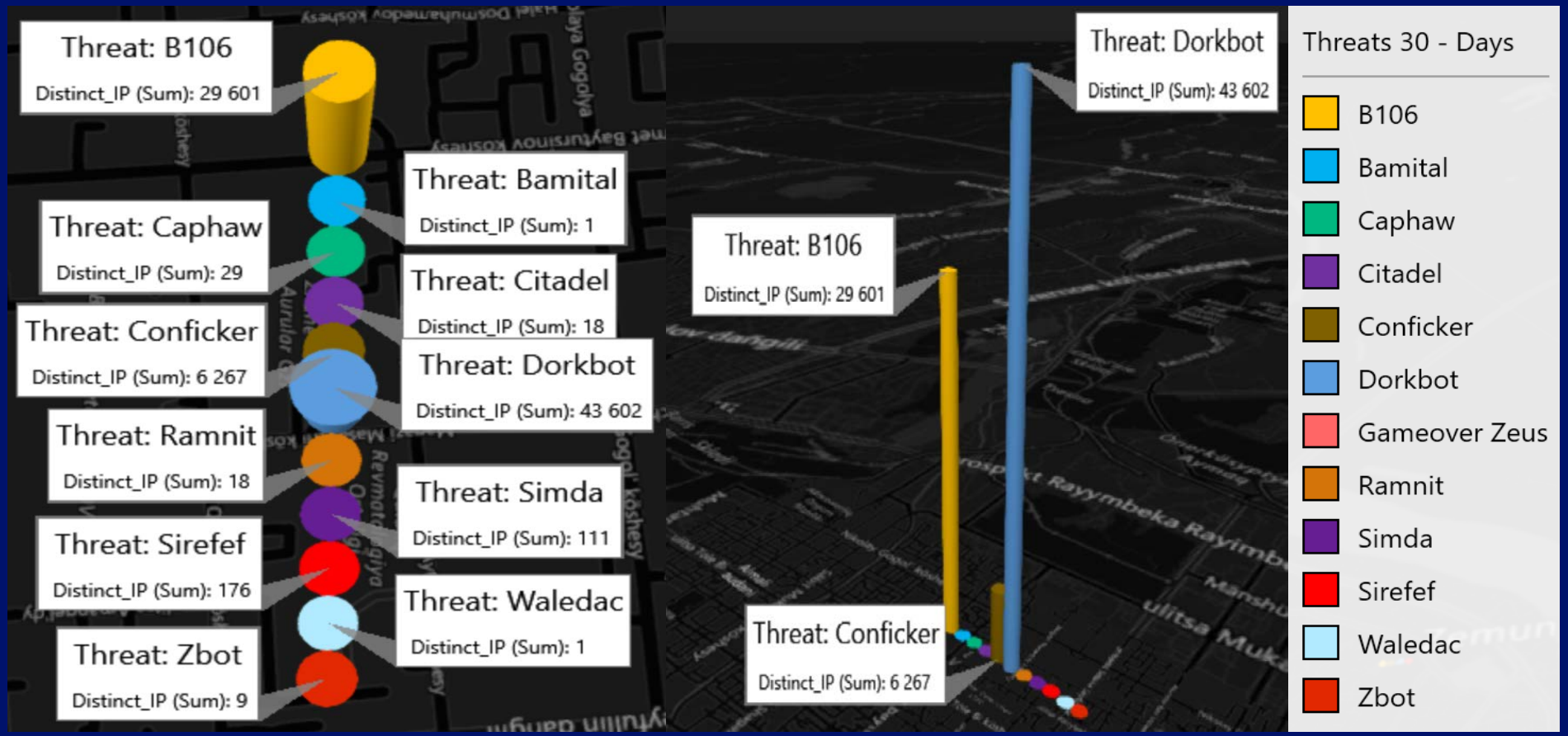
Financial Fraud, DDoS Attacks

Astana Overview 1-30 June, 2016



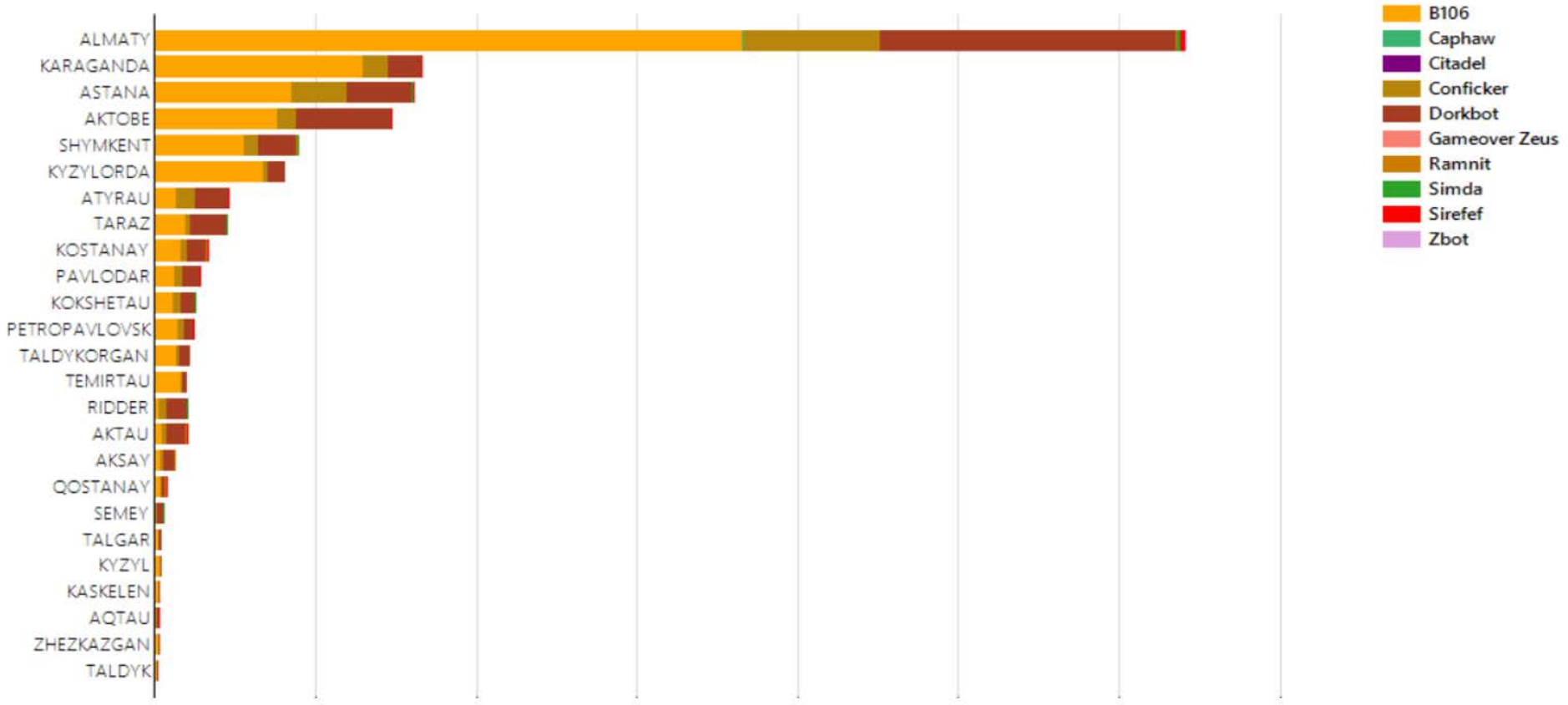
Microsoft

Almaty Overview 1-30 June, 2016



Microsoft

Kazakhstan Top 25 Cities by Threat, 12-18 September 2016



Microsoft

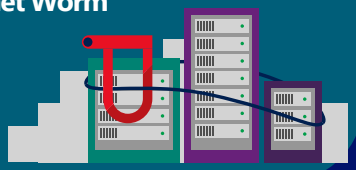
Most Common Malware Threats in Kazakhstan, 1-30 June 2016

Conficker

24 007

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

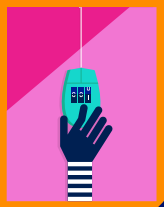


Bladabindi & Jenxcus

87 297

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

141 267

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

Microsoft

Risks management

Thank you!