Security risks and patches – The effects of IT-vulnerabilities on the society

OTKA PD-109740

Attila Horváth PhD

foundationforinformationsociety

Project environment

- ICT became standard infrastructure
- Part of critical infrastructure
- Vulnerablities are a common issue
  - IT point of view is general
  - No standardized methodology to handle spillover effects on the economy
- End-user, Corporate, Government levels

OTKA PD-109740

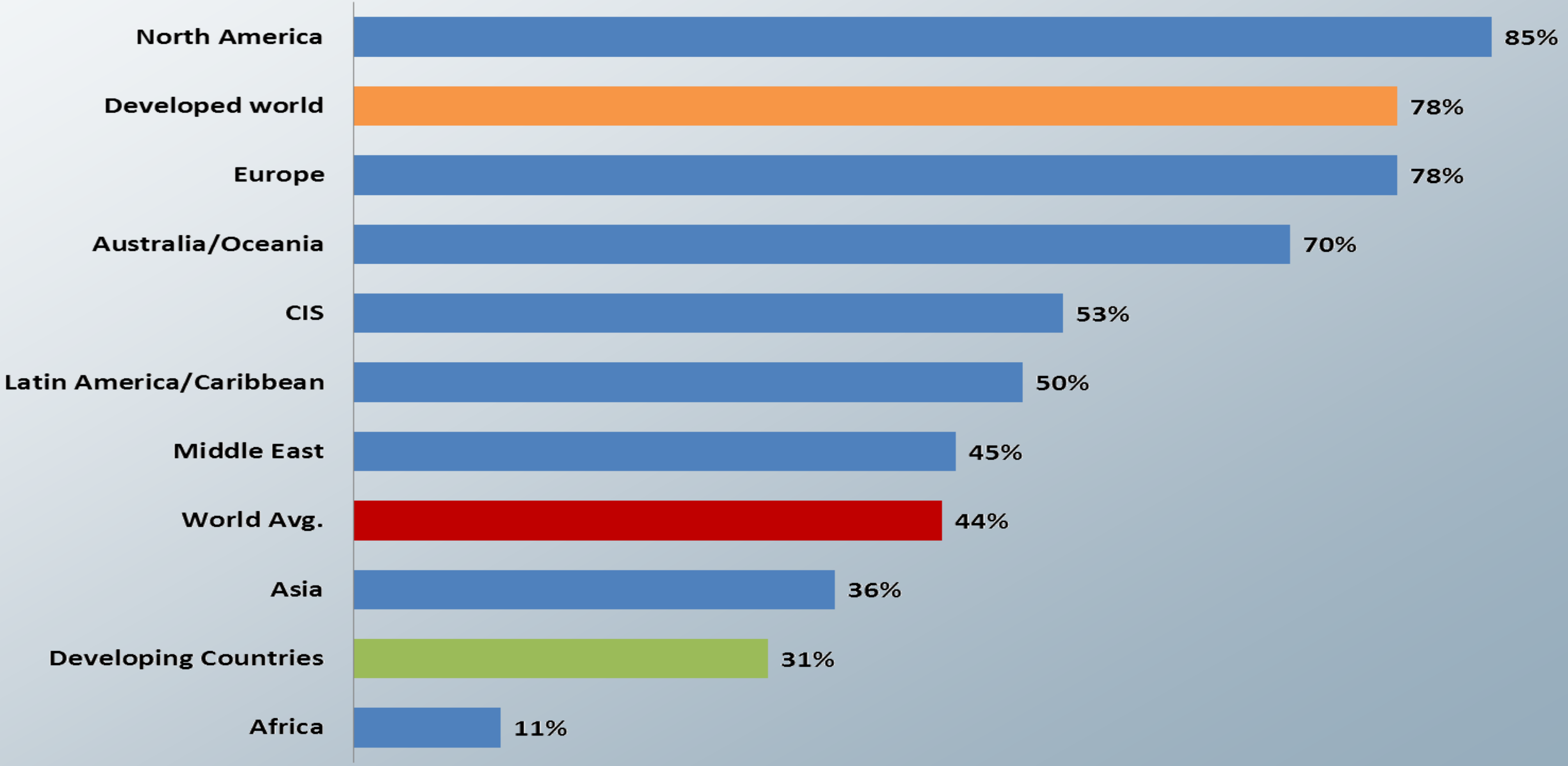
foundationforinformationsociety

Aims of the project

- Identify the effects of software vulnerabilities
- Create a representative modeling environment
- Define a standardized methodology to handle the spillover effects in monetary terms

foundationforinformationsociety

A World connected as never before



OTKA PD-109740

The true costs of cyber-crime

- $400 billion/year ($375 - $575 billion)
- GDP loss
  - High income countries: 0,9%
  - Developing countries: 0,2%
  - Average 0,5%
- Hiding and denial is common

The true costs of cyber-crime

- Components
  - The loss of intellectual property,
  - the theft of financial assets and sensitive business information,
  - opportunity costs, additional costs for securing networks,
  - the cost of recovering from cyberattacks,
  - reputational damage, etc.

The true costs of cyber-crime

- Unreported incidents
  - Reputation issues
  - Lack of organizational background
  - Lack of obligatory statistics
- Ambiguous data
  - Difficult to make estimates

OTKA PD-109740

Software vulnerabilities

- A security exposure
- A product weakness
- Allow an attacker to compromise the integrity, availability, or confidentiality
- Developers should fix ASAP.

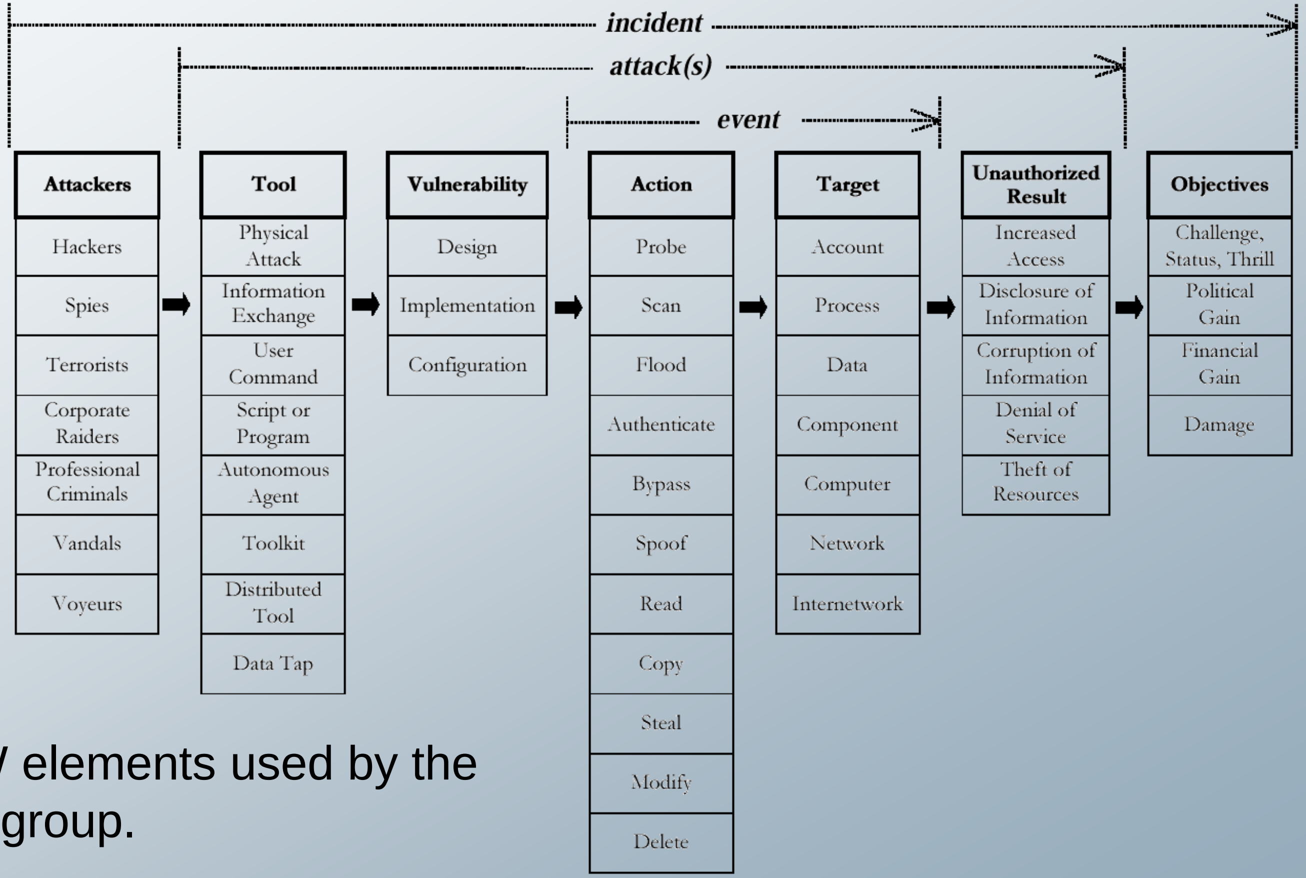
Phase 1: Vulnerability research

- Goal: identify how certain IT environments are affected by the vulnerabilities on the accessible vulnerability lists
- Methodology for risk analysis
  - Model based on the main risk analysis methodologies
    - Quantitative
    - Qualitative
    - Stochastic

Basic inputs

- Expected value
  - **Damage caused × Probability of occurance**
- Effective damage calculation
  - • The difference between the first total value of the residual value (loss of tangible value)
  - Re-production value (new value)
  - The costs of the elimination of the outcomes (recovery value)
  - The damage of intangible assets (loss of intangible value) (goodwill, consumer trust, etc.)

IT-environments and involvement



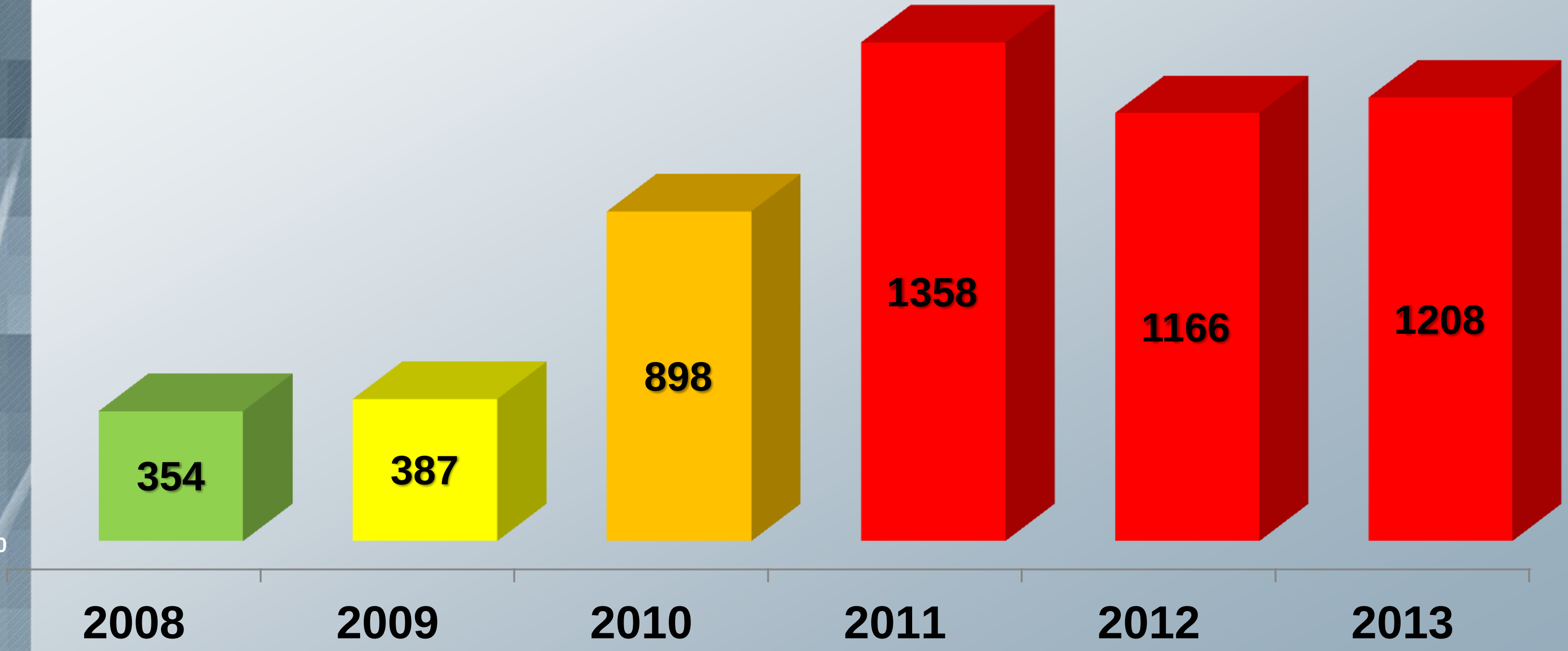
Attackers	Tool	Vulnerability	Action	Target	Unauthorized Result	Objectives
Hackers	Physical Attack	Design	Probe	Account	Increased Access	Challenge, Status, Thrill
Spies	Information Exchange	Implementation	Scan	Process	Disclosure of Information	Political Gain
Terrorists	User Command	Configuration	Flood	Data	Corruption of Information	Financial Gain
Corporate Raiders	Script or Program		Authenticate	Component	Denial of Service	Damage
Professional Criminals	Autonomous Agent		Bypass	Computer	Theft of Resources	
Vandals	Toolkit		Spoof	Network		
Voyeurs	Distributed Tool		Read	Internetwork		
	Data Tap		Copy			
			Steal			
			Modify			
			Delete			

All SW elements used by the target group.

Data sources

- The National Vulnerability Database operated by US-Cert (USA Homeland Security)
- The vulnerability database of Secunia Advisories
- Mitre.org – Common Weakness Enumeration (CWE)
- Vendor reactions and data (based on internet search)

5 year vulnerablity trend



foundationforinformationsociety

OTKA PD-109740

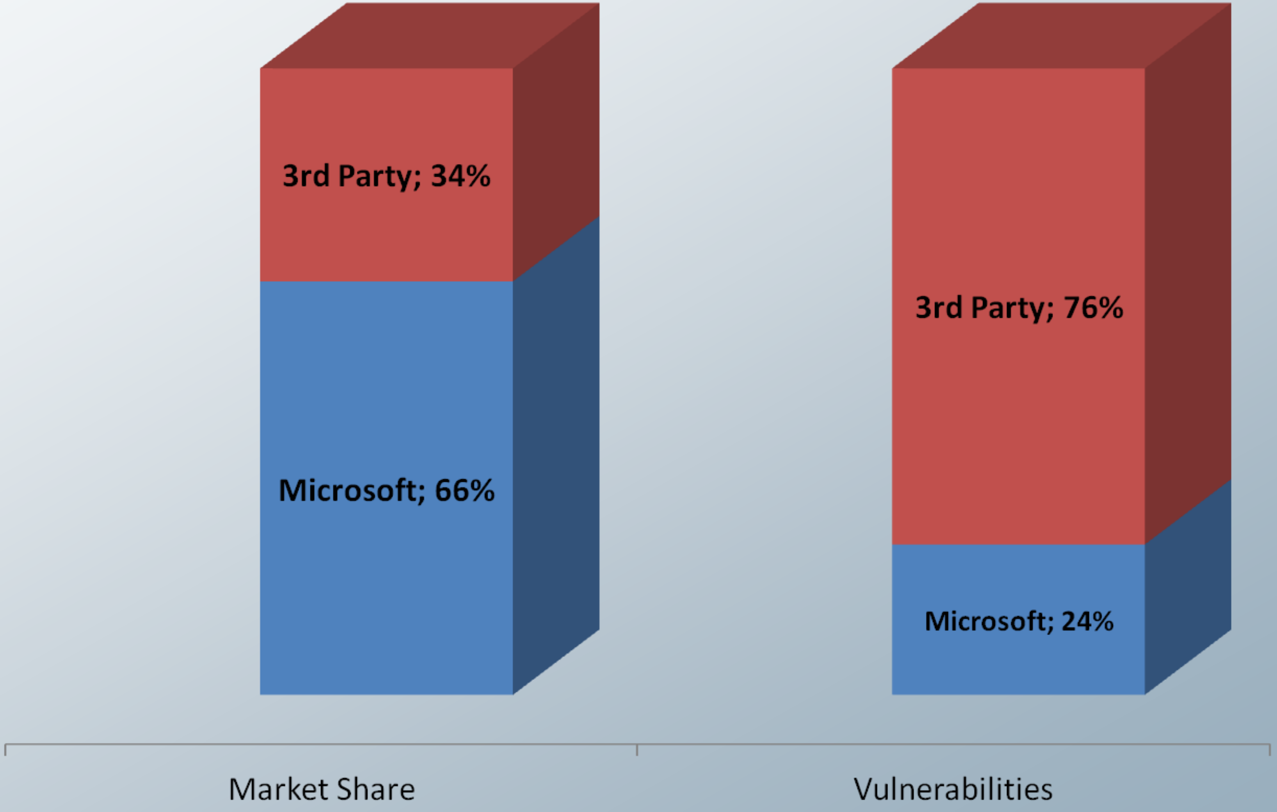
Installed software on a typical endpoint – 50 most popular SW

- 33 – Microsoft programs
- 17 – 3rd party programs

The end-user sample 2014. OS:Windows7

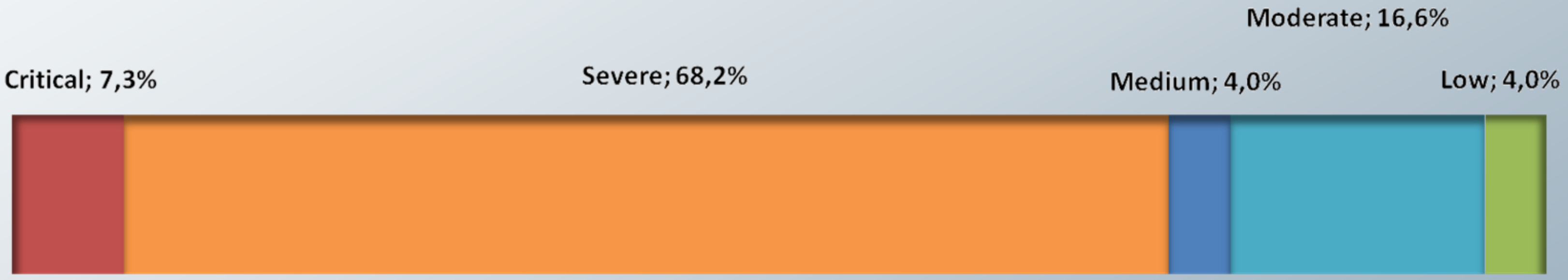
- MICROSOFT XML CORE SERVICES (MSXML)
- MICROSOFT WINDOWS MEDIA PLAYER
- MICROSOFT INTERNET EXPLORER
- MICROSOFT .NET FRAMEWORK
- ADOBE FLASH PLAYER
- MICROSOFT VISUAL C++ REDISTRIBUTABLE
- ADOBE READER
- MICROSOFT SILVERLIGHT
- MICROSOFT POWERSHELL
- ORACLE JAVA JRE
- MICROSOFT WINDOWS DEFENDER
- MICROSOFT WORD
- MICROSOFT EXCEL
- MICROSOFT POWERPOINT
- WINDOWS DVD MAKER
- MOZILLA FIREFOX
- GOOGLE CHROME
- WINDOWS MEDIA CENTER
- MICROSOFT VISIO VIEWER
- DRIVER PACKAGE INSTALLER (DPINST)
- MICROSOFT OUTLOOK
- COMDLG32 ACTIVEX CONTROL
- REALTEK AC 97 UPDATE AND REMOVE DRIVER TOOL
- ADOBE AIR
- APPLE QUICKTIME
- MSCOMCT2 ACTIVEX CONTROL
- MICROSOFT XPS-VIEWER
- MICROSOFT SQL SERVER
- CCLEANER
- MICROSOFT ACCESS
- WINDOWS LIVE MAIL
- MICROSOFT PUBLISHER
- MICROSOFT POWERPOINT VIEWER
- MICROSOFT WINDOWS MALICIOUS SOFTWARE REMOVAL TOOL
- SKYPE
- WINDOWS LIVE MESSENGER
- APPLE BONJOUR FOR WINDOWS
- WINDOWS LIVE WRITER
- REALTEK VOICE MANAGER
- WINDOWS LIVE MOVIE MAKER
- APPLE ITUNES
- VLC MEDIA PLAYER
- GOOGLE EARTH
- WINDOWS LIVE ESSENTIALS
- WINDOWS LIVE PHOTO GALLERY
- INSTALLSHIELD UPDATE SERVICE
- MICROSOFT OFFICE PICTURE MANAGER
- MICROSOFT OFFICE TEMPLATE AND MEDIA CONTROL ACTIVEX CONTROL
- GOOGLE TOOLBAR
- ADOBE SHOCKWAVE PLAYER

The share of Ms and 3rd party SW



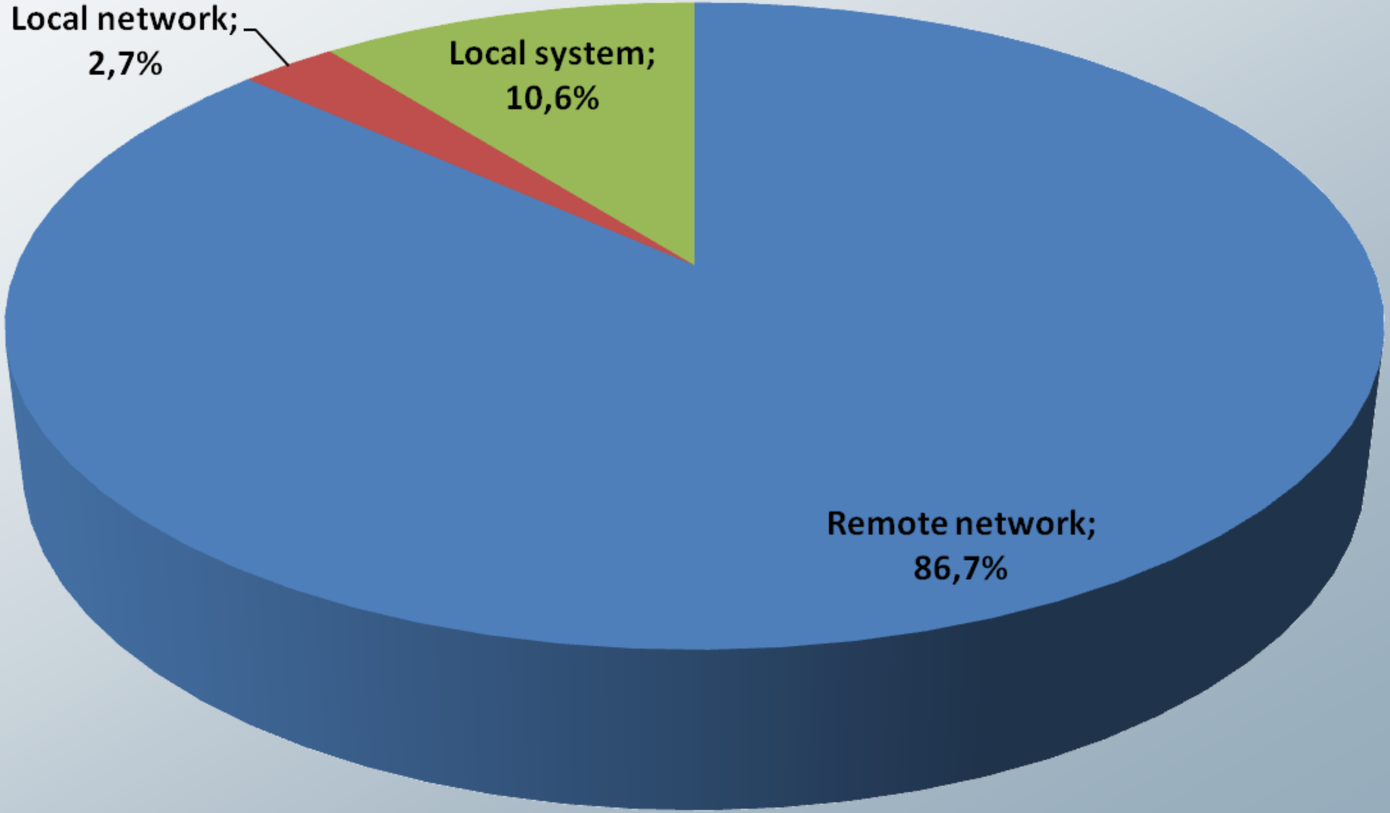
OTKA PD-109740

Vulnerablity severity

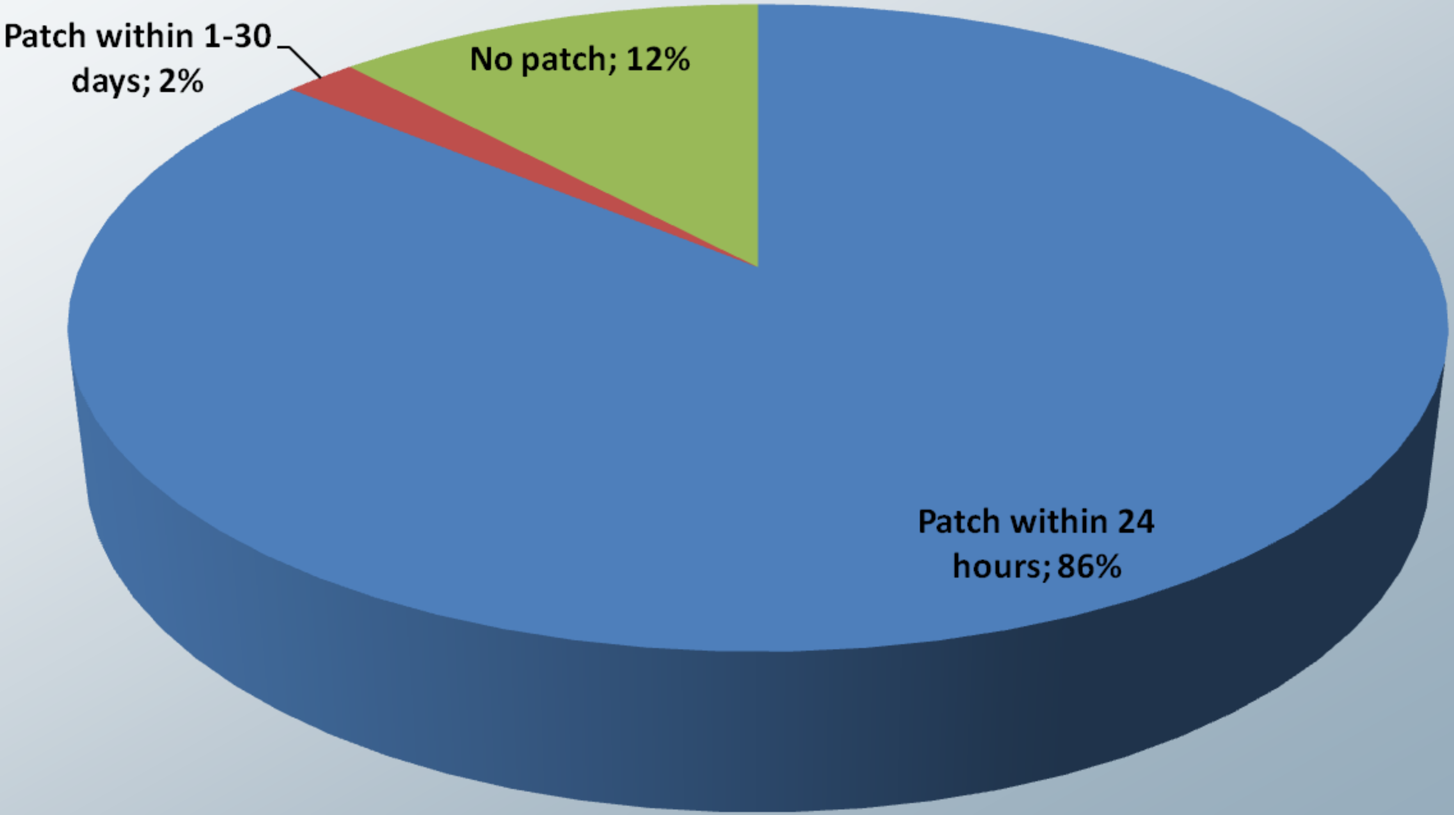


OTKA PD-109740

Attack vectors



Time to patch



Zero-day exploits

- 10 vulnerabilities in 2013
- 7-13 in the previous years

The effects on

End-user requirements

- Don’t think, just click.
- Someone else must protect me.
- For free

OTKA PD-109740

End-user behaviour

- Trust is binary
- Trust decisions can change at any time.
- There is no rational thought process behind it.

Most common solutions

- Communication is the key!
- Make users to do their part of the job!
- Apply “no-brain” security measures!

Thank you for your attention!

horvath.attila@infota.org