CYBER SPACE SECURITY. CURRENT STATE AND TREND.

Peter Zegzhda (prof., dphil.)
St.Petersburg State Polytechnic University

Information as attack means

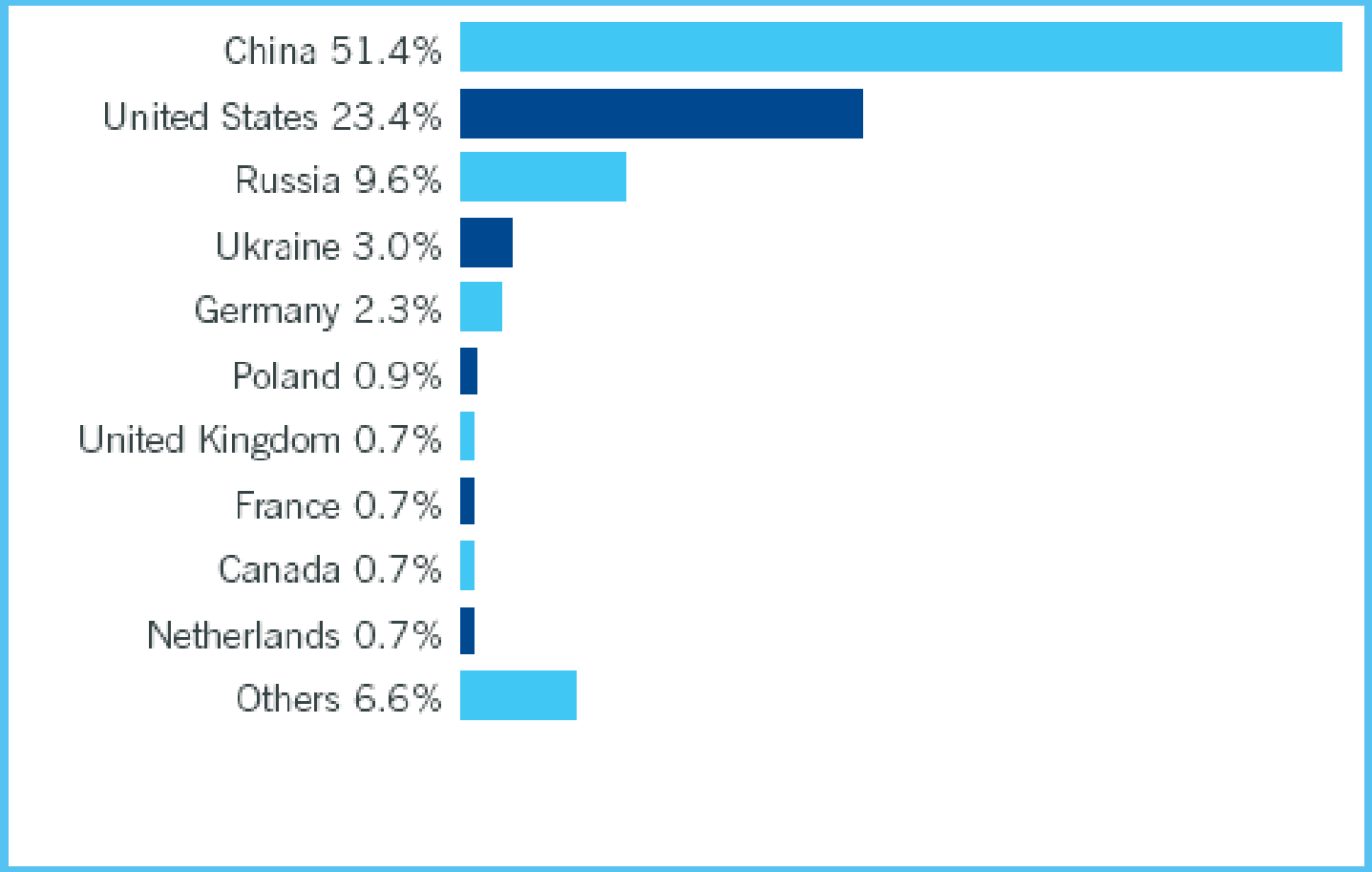
The New Yorker magazine publishes an interview with the director of American national intelligence services admiral Mike McConnell. He said, that every day U.S. department of defense observe three million (!) intrusion attempts in its data bases. U.S. State department is little more lucky – it beats two million of such attempts every day.

For six months, the Ministry of Defense spent no less than 100 million dollars to protect their computers from hackers, said brigadier General John Davis, responsible for cyber defense in the Pentagon

THE VOLUME OF LOSSES FROM VARIOUS TYPES OF ATTACKS

1	Viruses	15691460
2	Unauthorized data access	10617000
3	Theft of laptops and other mobile devices	6642660
4	Theft of confidential information	6034000
5	DOS-attacks	2922010
6	Financial fraud	2556900
7	Illegal use of network by internal violator	1849810
8	Telecommunication fraud	1262410
9	Bots inside the organization	923700
10	Intrusion in the system by external violator	758000
11	Fishing	647510
12	Wireless network intrusion	469010
13	Illegal use of IM	291510
14	Illegal use of web-applications	269500
15	Sabotage	260000
16	Web-site cracking	162500
17	Password tracking	161210
18	Company DNS-server exploit	90100
19	Other	885000

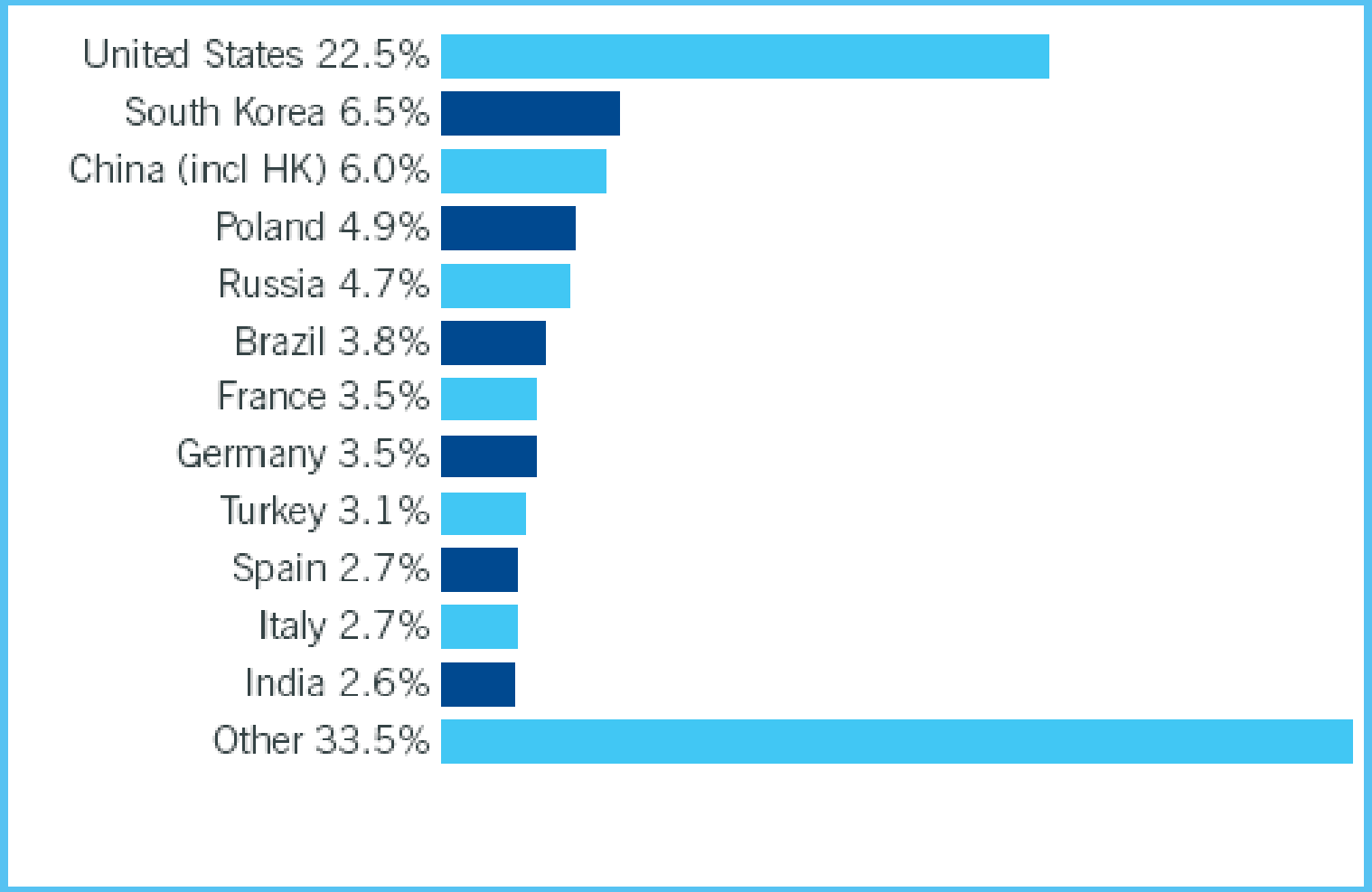
DISTRIBUTION OF MALWARE IN DIFFERENT COUNTRIES



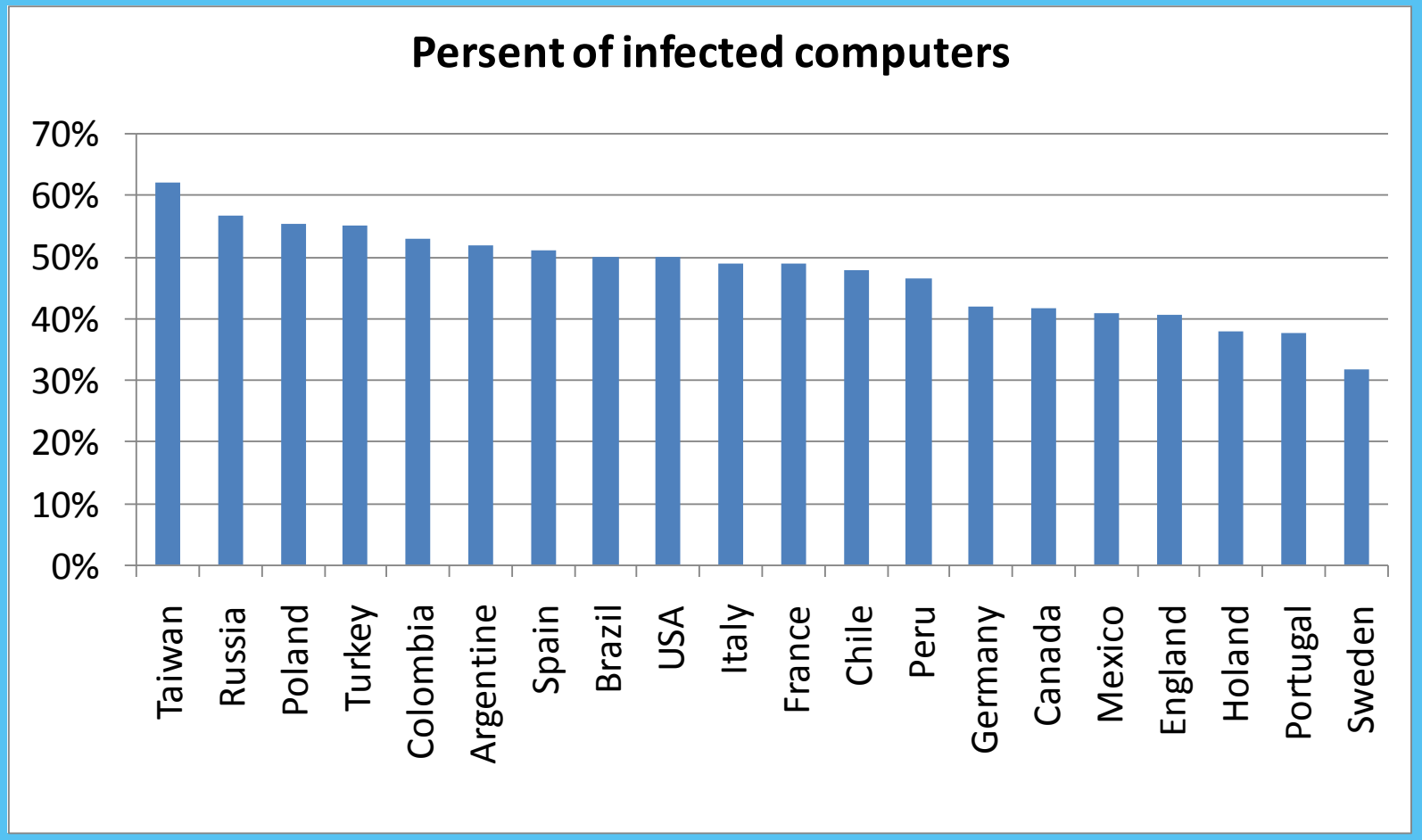
COUNTRIES OF MALWARE CREATION

Country	% of malware written
China	21.0%
Brazil	12.5%
Russia	9.2%

INTENSITY OF SPAM FROM THE TERRITORIES OF VARIOUS COUNTRIES



THE STATISTICS OF INFECTED COMPUTERS



CYBER TERRORISM

2007

- Attack against Estonia has left much of the country without the Internet

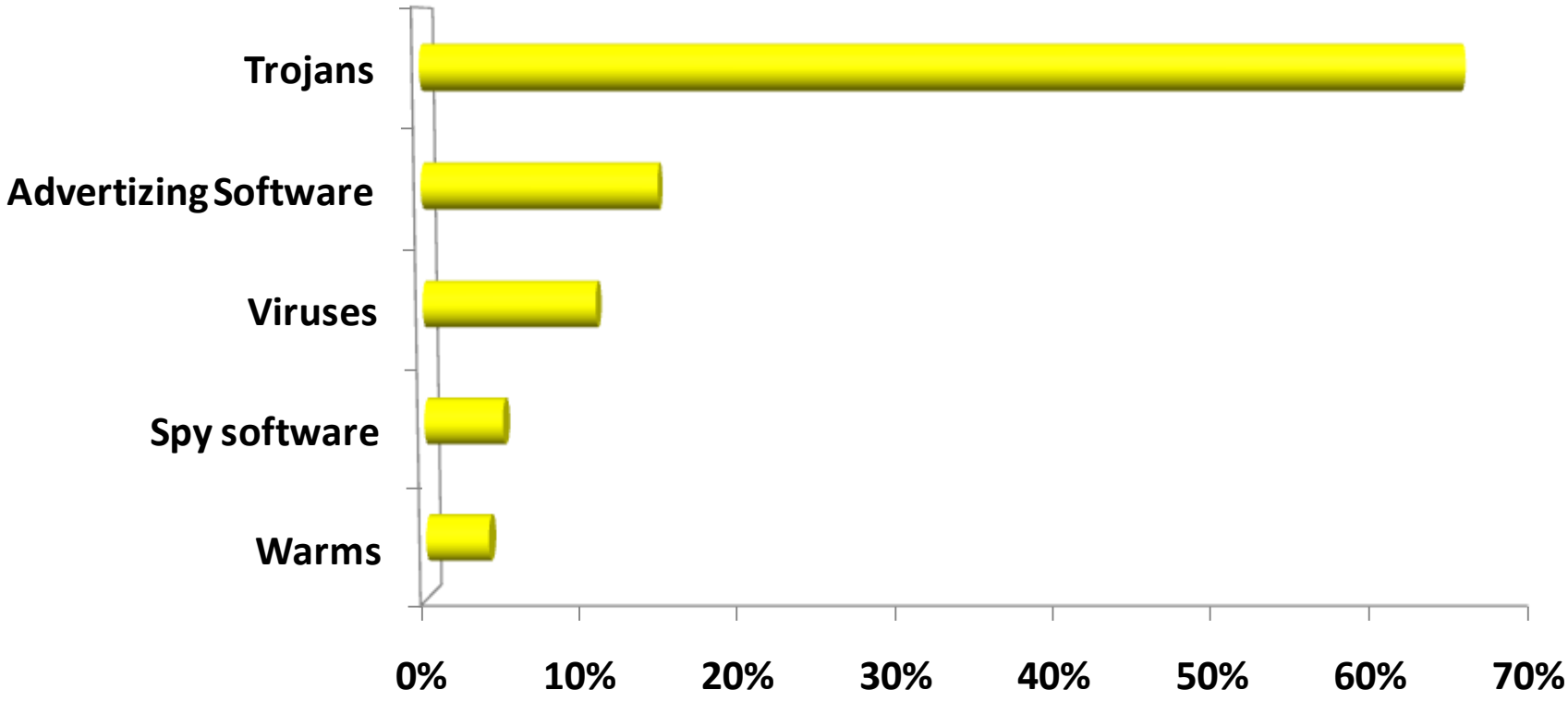
2008

- The attack on Georgia had left part of the country without the Internet

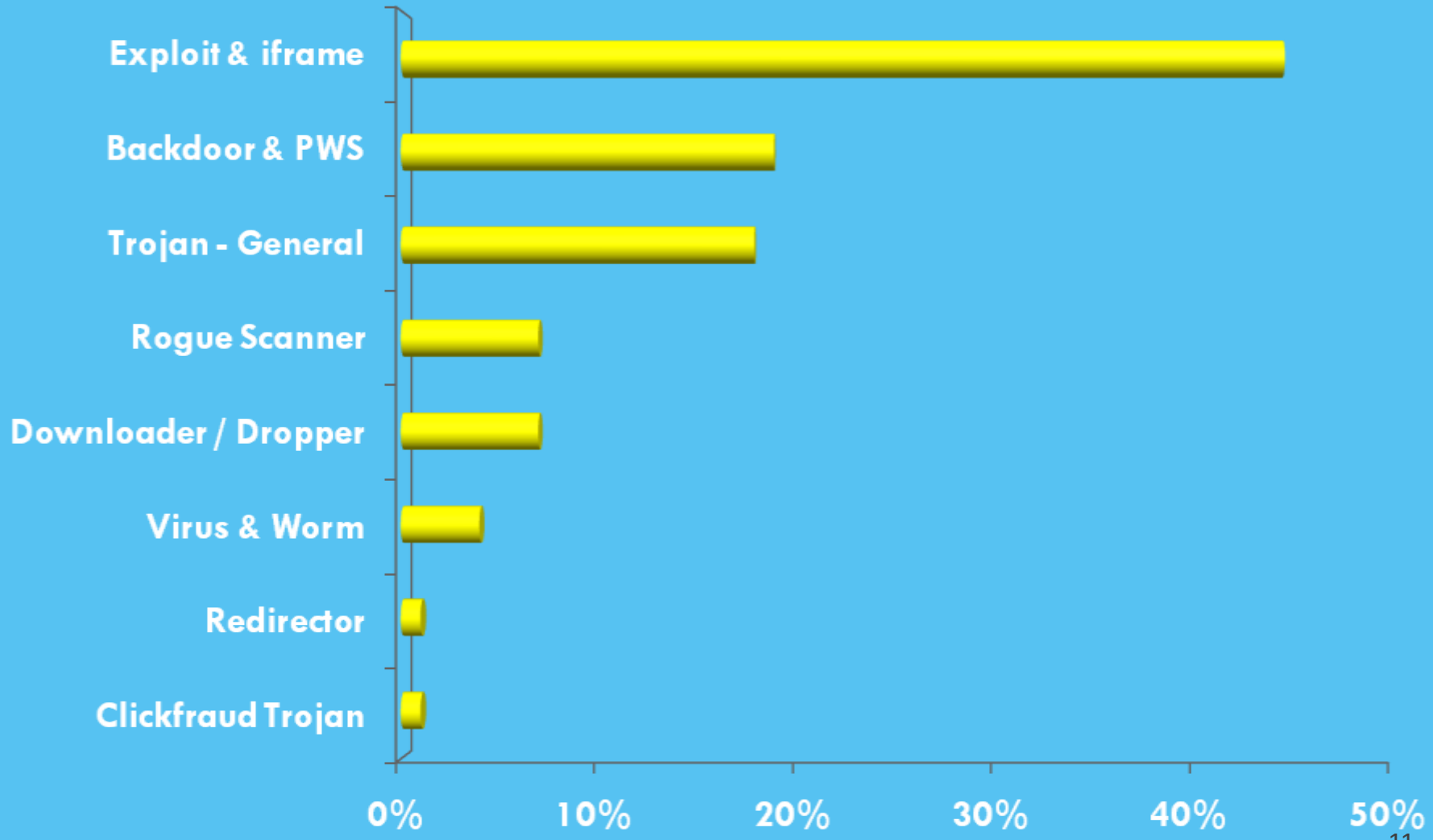
2009

- January 18 DDoS-attack left Kyrgyzstan without Internet
- In February, web page of Consulates in Shanghai hacked

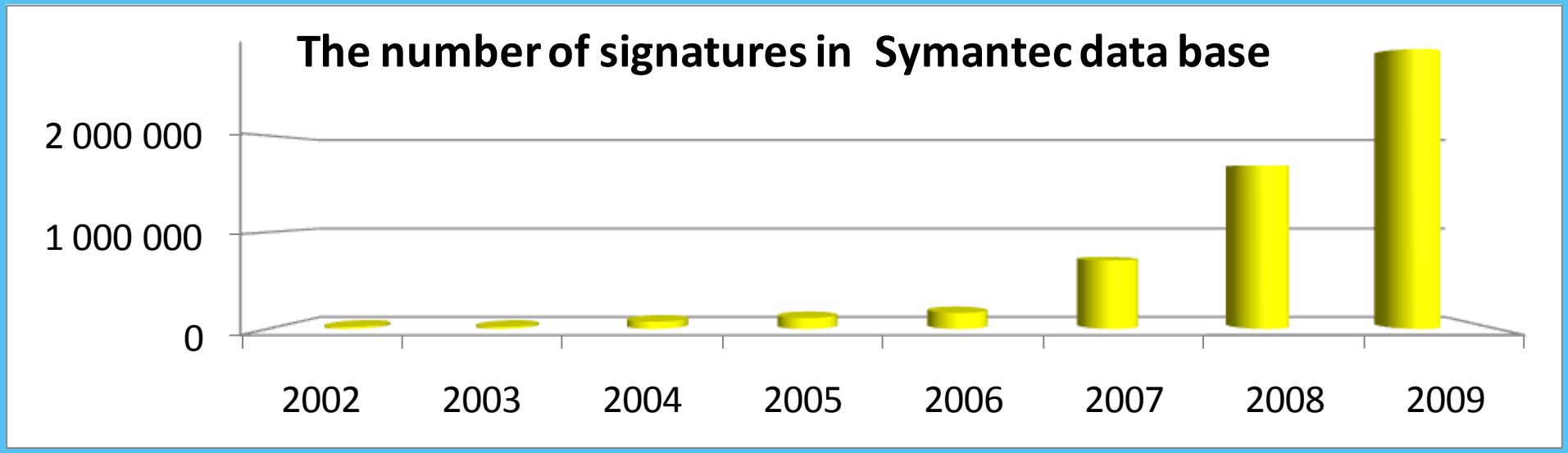
PREVALENT OF MALWARE BY CATEGORY

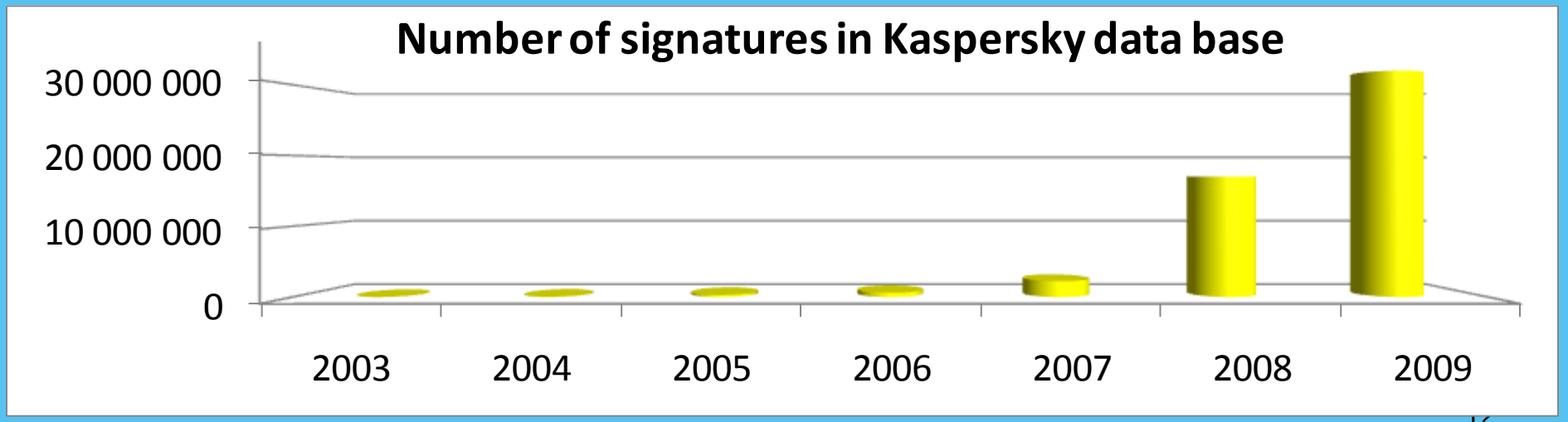


TYPES OF MALWARE OBTAINED FROM THE WEB, BY CATEGORY



THE AMMOUNT OF MALWARE





Malicious software development trend

Differentiation of mechanisms of distribution

- The popularity of using social networks for malware distribution is increasing.
- Cybercriminals are still using social engineering
- The number of vulnerabilities that allows malware distribution is not decreasing
- The number of attacks on the web sites and using of web sites for malware distribution is increasing.

The number of malicious software increases exponentional

- The speed of new threats creation is increasing (to beat means of protection)

Malware development based on cloud technologies

- Bot-networks allows to perform concentrated DDoS-attacks, password cracking and other.

Heterogeneity of malicious software

- The number of Mac users is almost reached a critical level, beyond which cybercriminals will be interested in Mac platform
- The amount of malware for mobile devices increases
- Windows 7 is popular. It is reasonable to predict the increasing of amount of malware for Windows 7.

X-FORCE R&D – LEADERSHIP IN SECURITY AREA

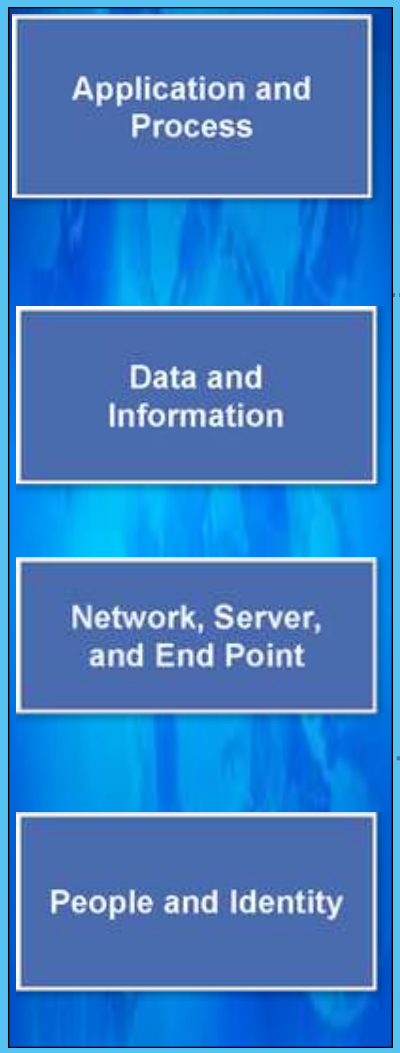
X-Force Research

- 10 billion web-pages and images analyzed
- 150 million s intrusion attempts every day
- 40 million spam and fishing attacks
- 48 thousand vulnerability documented
- Millions of malware source code samples

Purposeful analytics:

- Vulnerabilities and attacks
- Malware code
- Malicious/unwanted web-sites
- Spam and fishing
- Other trends

RESUME OF THE REPORT – ATTACKS CONTINUE TO EXISTS IN ALL SECURITY DOMAINS



- 6,601 new vulnerabilities in 2009, **11%** less then in 2008, basically because of decrease in new vulnerabilities in SQL injection and Active X.
- **49%** of all vulnerabilities – vulnerabilities of Web-applications.
- **52%** of all vulnerabilities does not have any patch from manufacturer on the end of 2009.

- Vulnerabilities of PDF format are much valuable then of Office ones.
- The vast majority of attacks on Web applications are done via special tools.
- USA – top hoster of malicious web-links.

- **7.5%** of the Internet is socially unacceptable, unwanted or malicious content.
- The number of new malicious web-links increased on **345%** comparing to 2008.

- The most part of spam **(80%) -** is URL-spam.
- The amount of URL-spam, coming from known and trusted domains continuously grow.
- **60.9%** of fishing targeting a financial area, **20.4%** - targeting government organizations.

CYBERCRIME ECONOMICS

- **Economics plays a significant role - vulnerability profitability is important**
- **Web-browser and PDF-readers vulnerabilities are easy to use and they are very profitable**

1 December 13, 2008 Adobe Acrobat and Acrobat Reader Remote Code Execution
October 9, 2008 Adobe Acrobat and Acrobat Reader Remote Code Execution
July 22, 2008 Adobe Acrobat and Adobe Flash Remote Code Execution

2 November 23, 2008 Microsoft Internet Explorer mshtml.dll RCE
July 8, 2008 Multiple Microsoft Video Control ActiveX Remote Code Execution Vulnerabilities
July 30, 2008 Microsoft Office Web Components Spreadsheet ActiveX Control RCE

3 September 10, 2008 Microsoft Windows SRV2.SYS Remote Code Execution Vulnerability

4 July 16, 2008 Mozilla Firefox Font HTML Tags Remote Code Execution

5 July 14, 2008 Multiple Microsoft DirectShow Remote Code Execution Vulnerabil-

November 10, 2008 Microsoft Windows WSDAPI Remote Code Execution Vulnerability

7 October 13, 2008 Microsoft Windows Indexing Service ActiveX Control Remote Code Execution Vulnerability
September 8, 2008 Microsoft Windows JScript Remote Code Execution Vulnerability

8 August 11, 2008 Network Security Services (NSS) Parser Remote Code Execution Vulnerability

9 August 11, 2008 Network Security Services (NSS) Certificate Security Bypass Vulnerability

10 October 13, 2008 Multiple Microsoft Windows GDI+ Image Remote Code Execution Vulnerabilities
August 11, 2008 Microsoft Windows AVI Remote Code Execution Vulnerability
November 10, 2008 Microsoft Windows Kernel Font Code Execution Vulnerability
July 14, 2008 Multiple Microsoft Windows Embedded OpenType Font Engine Remote Code Execution Vulnerabilities

11 August 11, 2008 Microsoft WINS Replication Remote Code Execution Vulnerability

12 August 11, 2008 Microsoft Windows RDP Services Client ActiveX Control Remote Code Execution Vulnerability
July 28, 2008 Microsoft Internet Explorer ATL Killbit Evasion Vulnerability
July 28, 2008 Multiple Microsoft Visual Studio Active Template Remote Code Execution Vulnerabilities

13 November 9, 2008 Transport Layer Security (TLS) Handshake Renegotiation

14 August 11, 2008 ISC BIND dns_db_findrdataset() DoS Vulnerability

15 September 2, 2008 Microsoft Internet Information Services FTP Remote Code Execution Vulnerability

16 December 9, 2008 HP OpenView Network Node Manager Remote Code Execution Vulnerability

17 December 1, 2008 Novell eDirectory Remote Code Execution Vulnerability

18 July 14, 2008 ISC DHCP Client Buffer Overflow Vulnerability

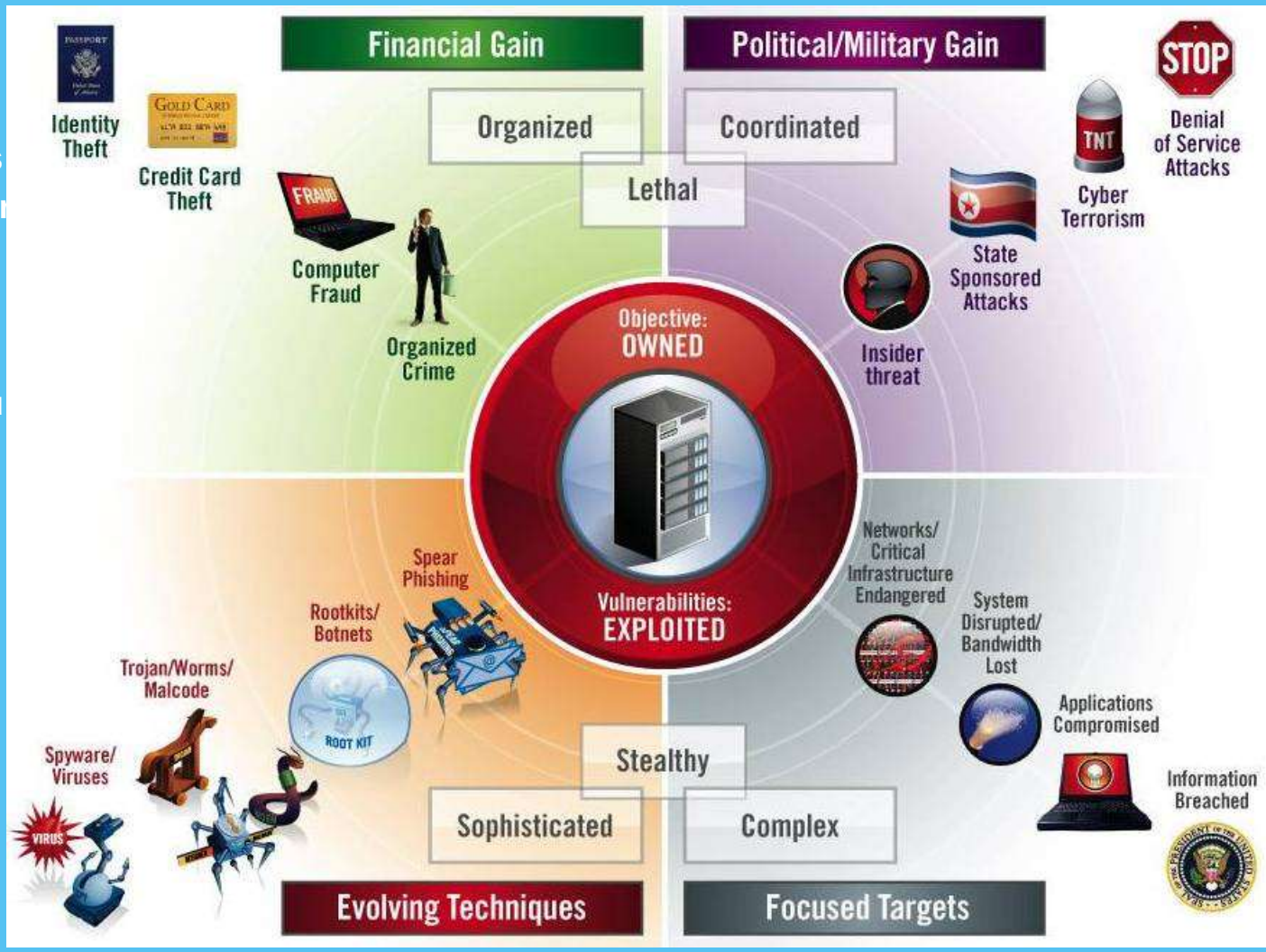
19 October 13, 2008 Microsoft Internet Explorer Arguments Remote Code Execution Vulnerability

Source: IBM X-Force®

CYBERCRIME ECONOMICS

Threats evolution:

- **Attackers take into account ROI and continually improve its tools to re-use them for the next wave of attacks**
- **In order to properly prioritize the risks, you should take into account the economic component of hacking**

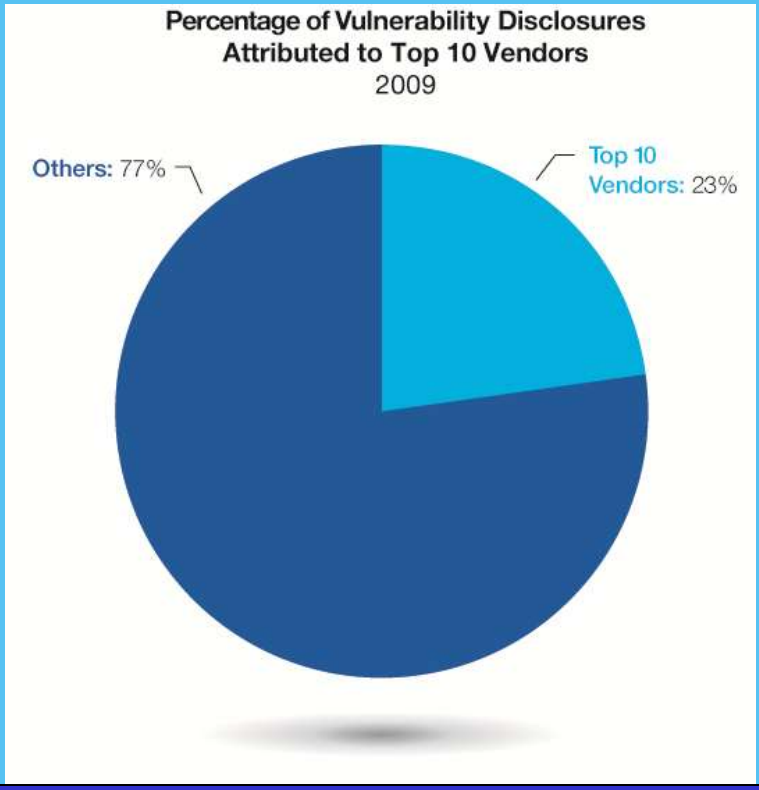


APPLE, SUN AND MICROSOFT – "LEADERS" IN VULNERABILITIES

- Top-ten companies has almost a quarter (23%) of all vulnerabilities, against 19% in 2008.
- Significant changes in raiting:
  - Microsoft dropped from #1 to #3 after holding top spot since 2006.
  - Adobe makes it's debut on the top ten list at number nine.

Ranking	Vendor	Disclosures
1.	Apple	3.8%
2.	Sun	3.3%
3.	Microsoft	3.2%
4.	IBM	2.7%
5.	Oracle	2.2%
6.	Mozilla	2.0%
7.	Linux	1.7%
8.	Cisco	1.5%
9.	Adobe	1.4%
10.	HP	1.2%

Table 3: Vendors with the Most Vulnerability Disclosures, 2009

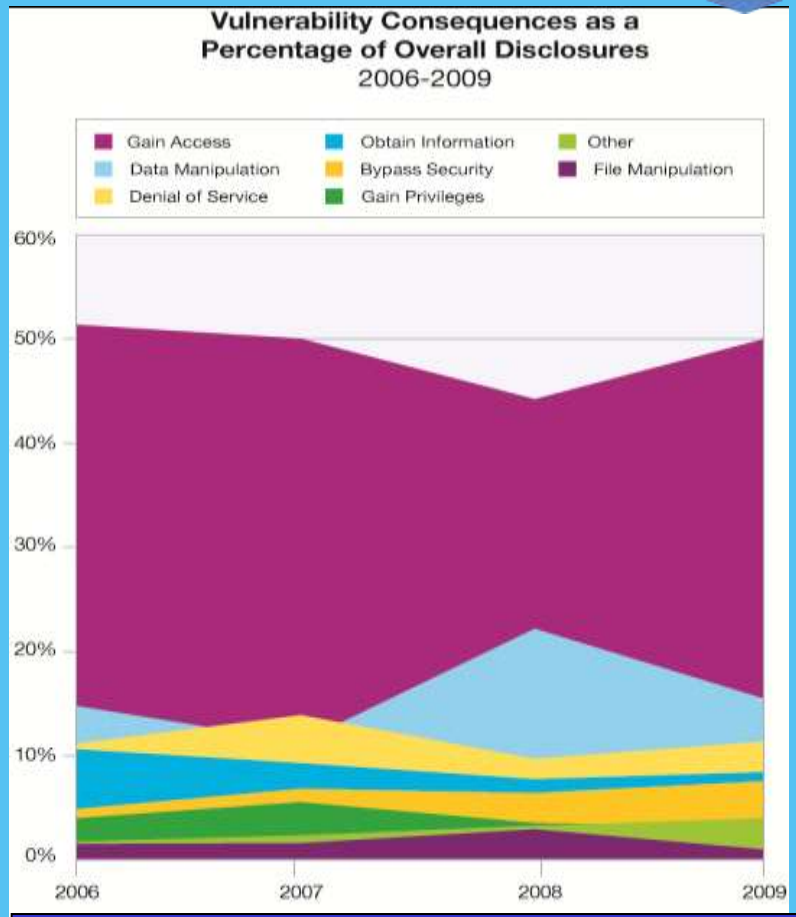


It is not a good idea to thing that software from manufactures not from this list is safe!

Note: In 2009, web application vendors are not on the top ten list because we now only count vulnerabilities in the base platform. We are not including plug ins associated with Web application platform vulnerabilities because they are often not produced by the vendor themselves.

MOTIVATION OF THE ATTACKER, 2009 – ACCESS GAIN AND DATA MANIPULATION

- "Gain access" remains the primary consequence of vulnerability exploitation.
  - Approaching the 50% mark that was previously seen throughout 2006 and 2007.
- "Data Manipulation" took a plunge but still higher in comparison to 2006 and 2007.
- "Bypass Security" and "Denial of Service" is increasing.



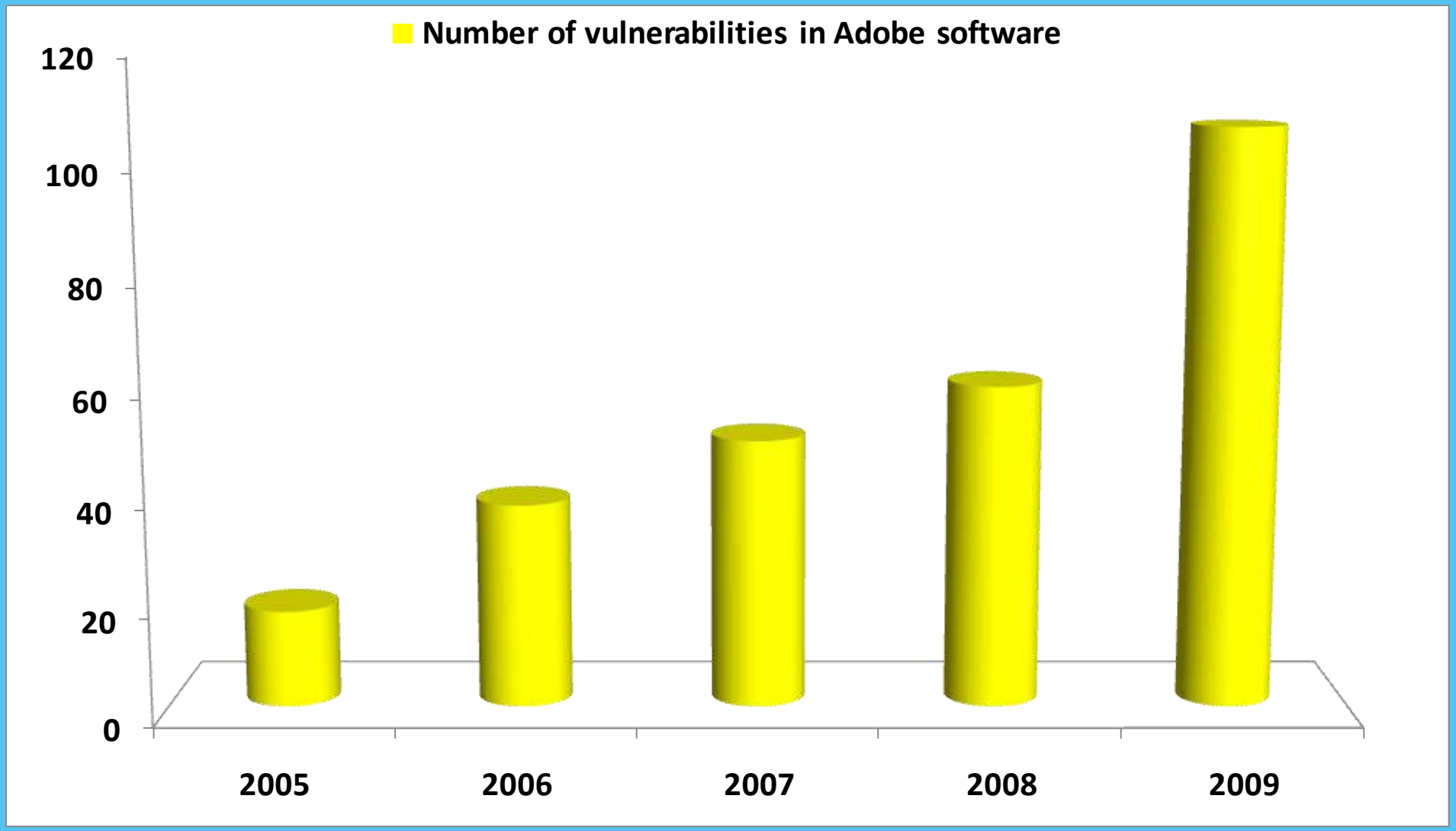
Questions:

- Are you sure that attacker will not be able to gain access to your system?
- Are your confidential information is in safe?

IBM Security Offerings:

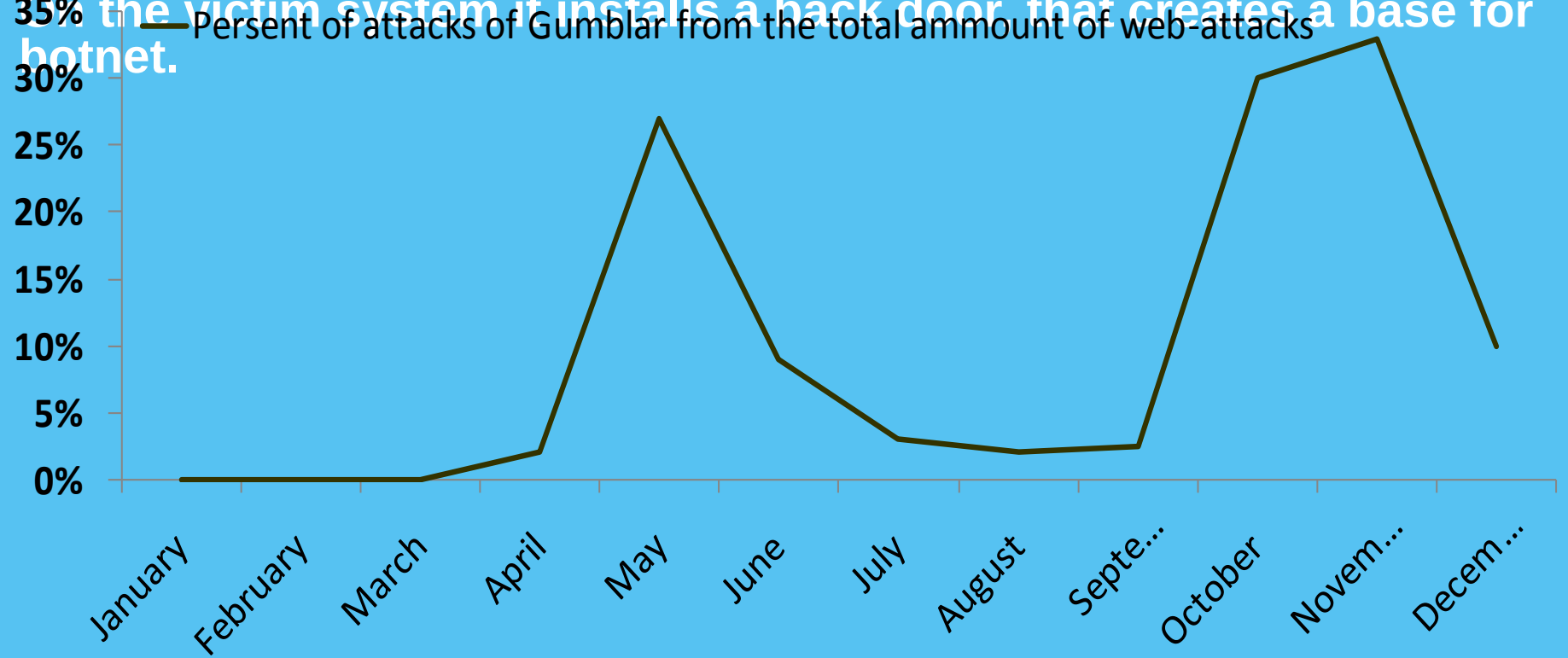
- IBM Security Network, Server and Endpoint Intrusion Detection and Prevention products and services
- IBM Web Application Security
- IBM Data Security products and services

ADOBE – VULNERABILITY LEADER



GUMBLAR BOTNET ACTIVITY

- Populates using scripts in web-pages
- Intrudes into internet browser of infected computer and begins manipulation of Google search results. New search results references to the attacker controlled web sites (new threats can be presented on those web sites)
- Monitors the information required for FTP server access (required for script injection into web-pages)
- On the victim system it installs a back door, that creates a base for botnet.



CYBER ATTACK = MISSILE ATTACK

- The expert group of NATO, headed by former Secretary of State Madeleine Albright came to the conclusion that the cyber attacks against critical infrastructures of the Alliance to be equated with armed attack to justify a retaliatory strike by military means (The Sandy Times)
- At the same time, The Sandy Times notes that determination of who is responsible for cyber attacks and whether this kind of hacker activities are related with the governments of various countries is often impossible

TRENDS OF MEANS OF SECURITY

Vulnerability defend progress

- Progress of software development tools (Visual Studio 2010) and programming languages (Java, C #) to prevent the emergence of vulnerabilities at the design phase
- Progress of techniques of exploitation of vulnerabilities protection (including hardware support at the processor level)
- Progress of methods in vulnerabilities search in classic software products and Web applications

Security environment progress

- Developing new approaches to the architecture of protection, since protection is necessary, regardless of operating system and devices
- The first 100% cloud antivirus CloudAntivirus from Panda
- The development of means of security based on hardware virtualization

SECURITY ISSUES OF MODERN CONSOLIDATED SYSTEMS

- High level of function concentration and closed communication protocols existence
- Huge amount of interactions that is impossible to control without performance impact
- Huge amount of source code produces vulnerabilities
- Difficulty in adaptation of trusted means to the modern information systems
- Integration of different forms and representations of information

FROM THE TRUSTED ENVIRONMENT TO CONTROLLED ONE

- Secure OS. Difficulty and trends. Alternative – security or compatibility
- Controlled environment paradigm – the system with predictable properties. Application, user, external environment behavior monitoring
- The development of the security concept as a balance between confidentiality, integrity, accessibility
- The concept of dynamic integrity

SECURITY TECHNOLOGIES ORGANIZATION

The nature of protection	Monitoring objects			Methods of security assessing	Basic properties
	System state	Security system state	Exchange with external environment		
Static	None	None	Partial	Assessing by regularity documents	Adequacy according to threats
Active	Partial	None	Input data analytic	Information environment analytics	Reliability of input information analytics
Adaptive	Partial	Partial	Input data analytic	Security system state control	Tolerance to threats, Stability of control
Dynamic	Full	Full	Input data and communication channels analytic	System security monitoring, risks assessing	Invariance of security, sufficiency, Vulnerability resistance