

Security Intelligence.  
Think Integrated.

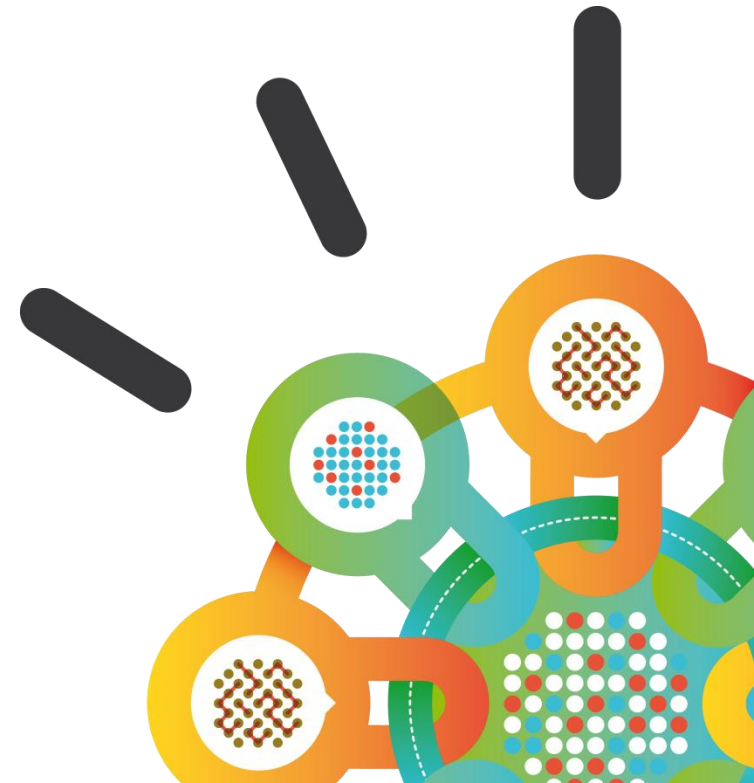


# IBM X-Force 2013 Mid-Year Trend and Risk Report

Andris Soroka  
Thinker at Data Security Solutions

[andris@dss.lv](mailto:andris@dss.lv)

23<sup>rd</sup> of October, 2013





# 4<sup>th</sup> international annual conference “DSS ITSEC 2013 – IT Security is not enough” (07.11.2013)

**DSS Conference 2013**  
for ITSEC professionals

7th of November, 2013  
Maritim Hotel, Riga, Latvia

**IT SECURITY IS NOT ENOUGH!**

Smart clouds emit smart rain. You better be smart not to get wet.  
7th of November is the day, when You can learn how.

Latest IT security trends

3 paralel sessions

World class solutions

Business networking

Learn more at

<http://event.dss.lv>

7th of November, 2013 **DSS Conference 2013** for ITSEC professionals Maritim Hotel, Riga, Latvia

- ✓ 4th annual international IT Security Conference
- ✓ 3 parallel sessions and one technical demo room
- ✓ Visited by 230 ITSEC pro's from the Baltic States in 2012
- ✓ Keynote speech from Minister of the Defense of Latvia
- ✓ Keynote from CERT LV - Cybersecurity in Baltics
- ✓ Supported and participation of Latvia ISACA Chapter
- ✓ Supported by Latvian IT Cluster and Latvian Association of Telecommunications
- ✓ More than 20 expert speakers from more than 10 countries

brought by

**Data Security Solutions**  
Think security first

platinum partners

**IBM** **ALSO**  
more than distribution

gold partners

**radware** **headtechnology**  
Smart Network. Smart Business. it-security

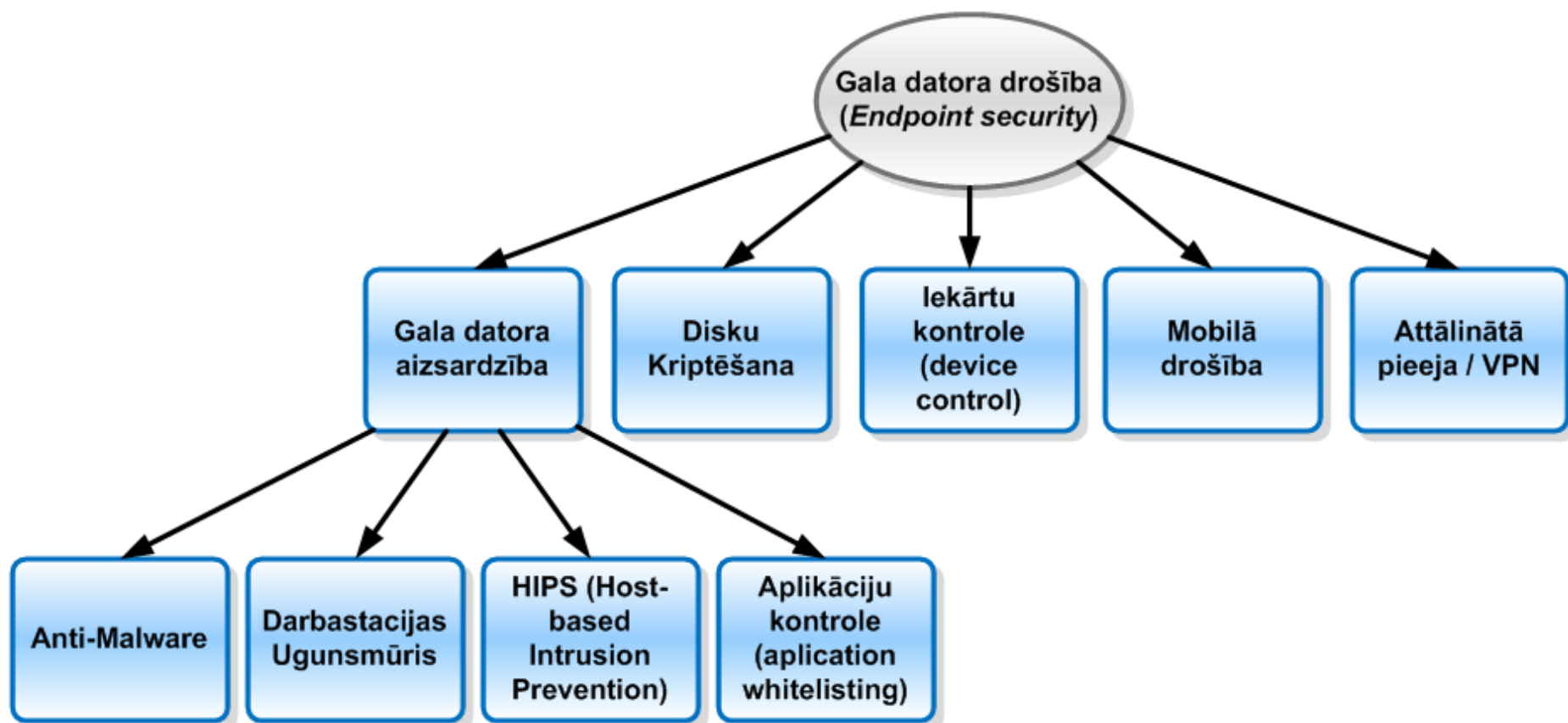
supporters

ANUGW Five Years Out, beyondtrust, Lumension, MobileIron, SAP, SAMSUNG, ISACA, DPA, NewLamp, MIDAS, VASCO, Symantec, Accellion, SafeXs, CERT.LV, THE ART of SYSTEMS, observe it, SearchInf.rm, ORACLE, ipeptis

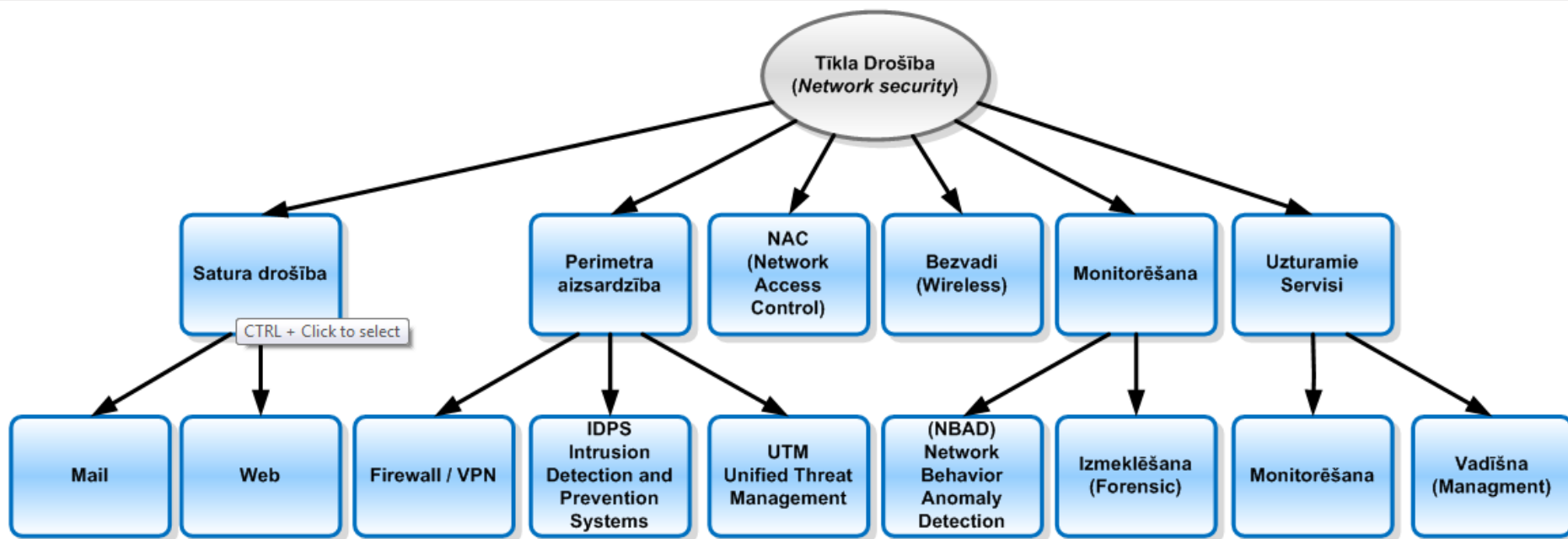
For many companies **security** is like **salt**, people just sprinkle it on top.



We see whole picture bit more complex way.

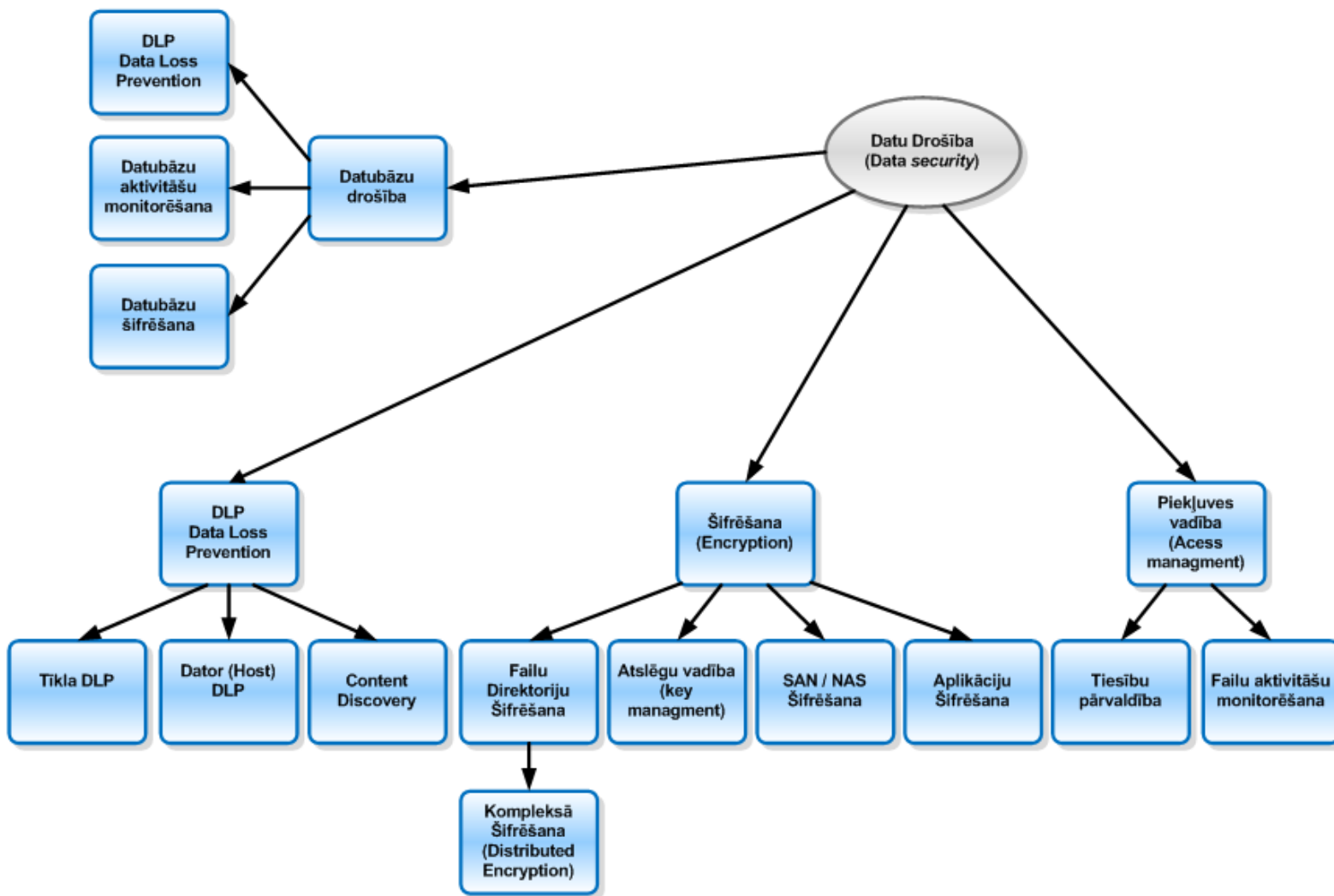


We see whole picture bit more complex way.

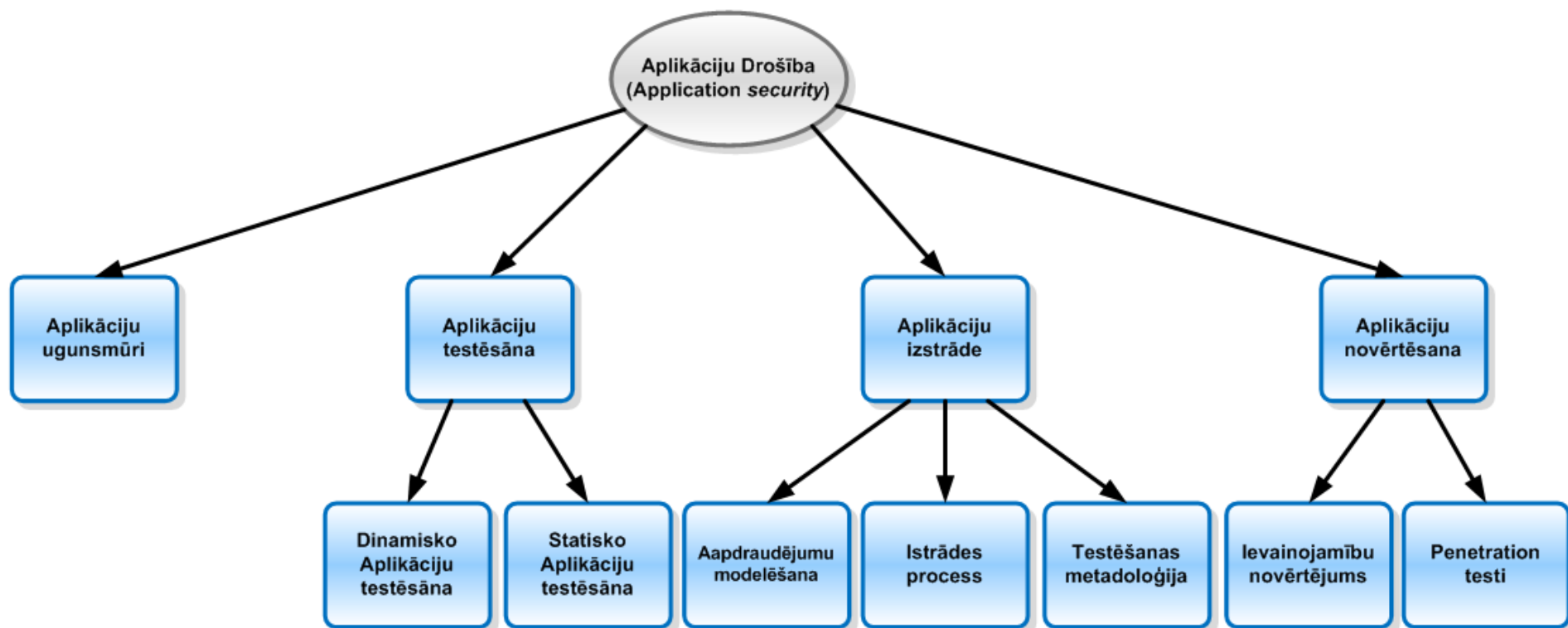




We see whole picture bit more complex way.

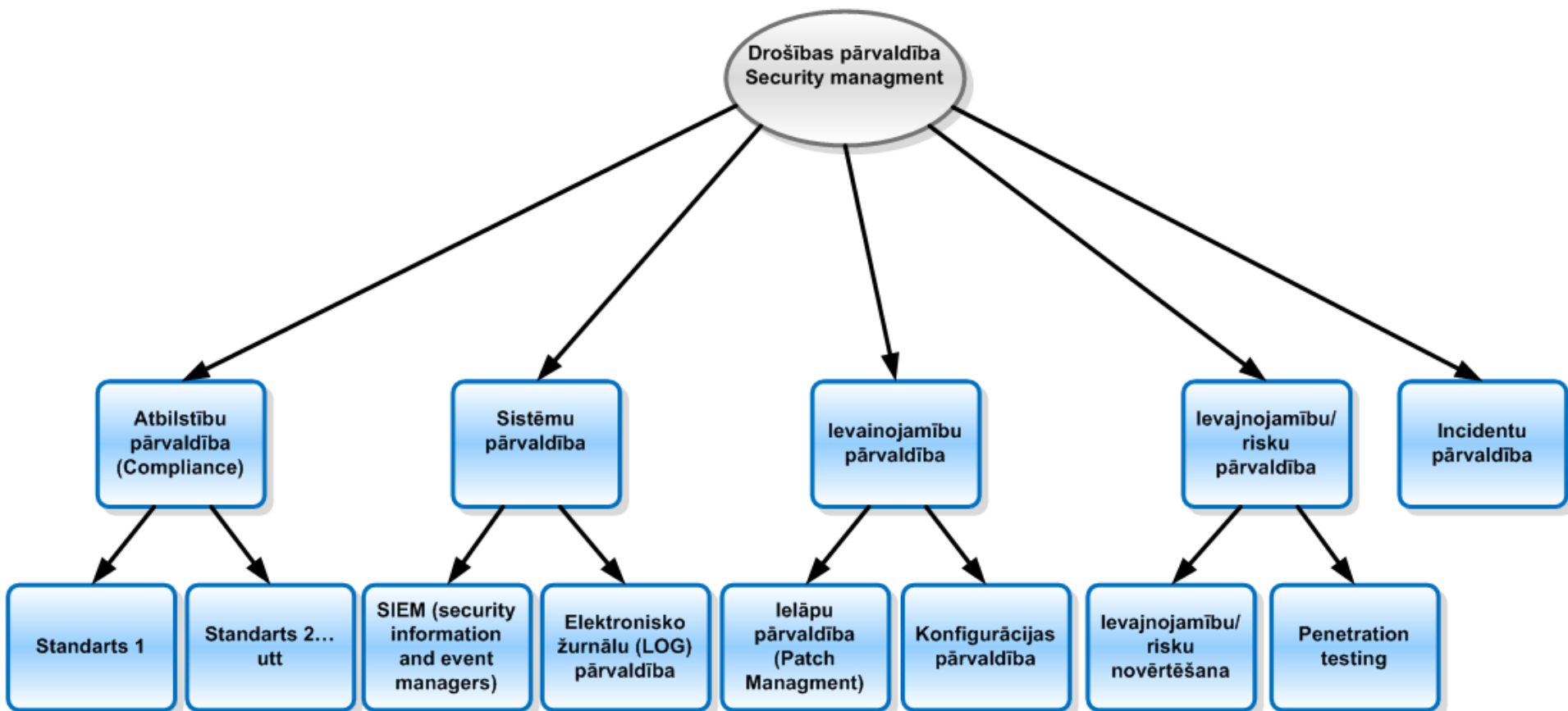


We see whole picture bit more complex way.

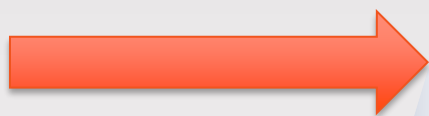




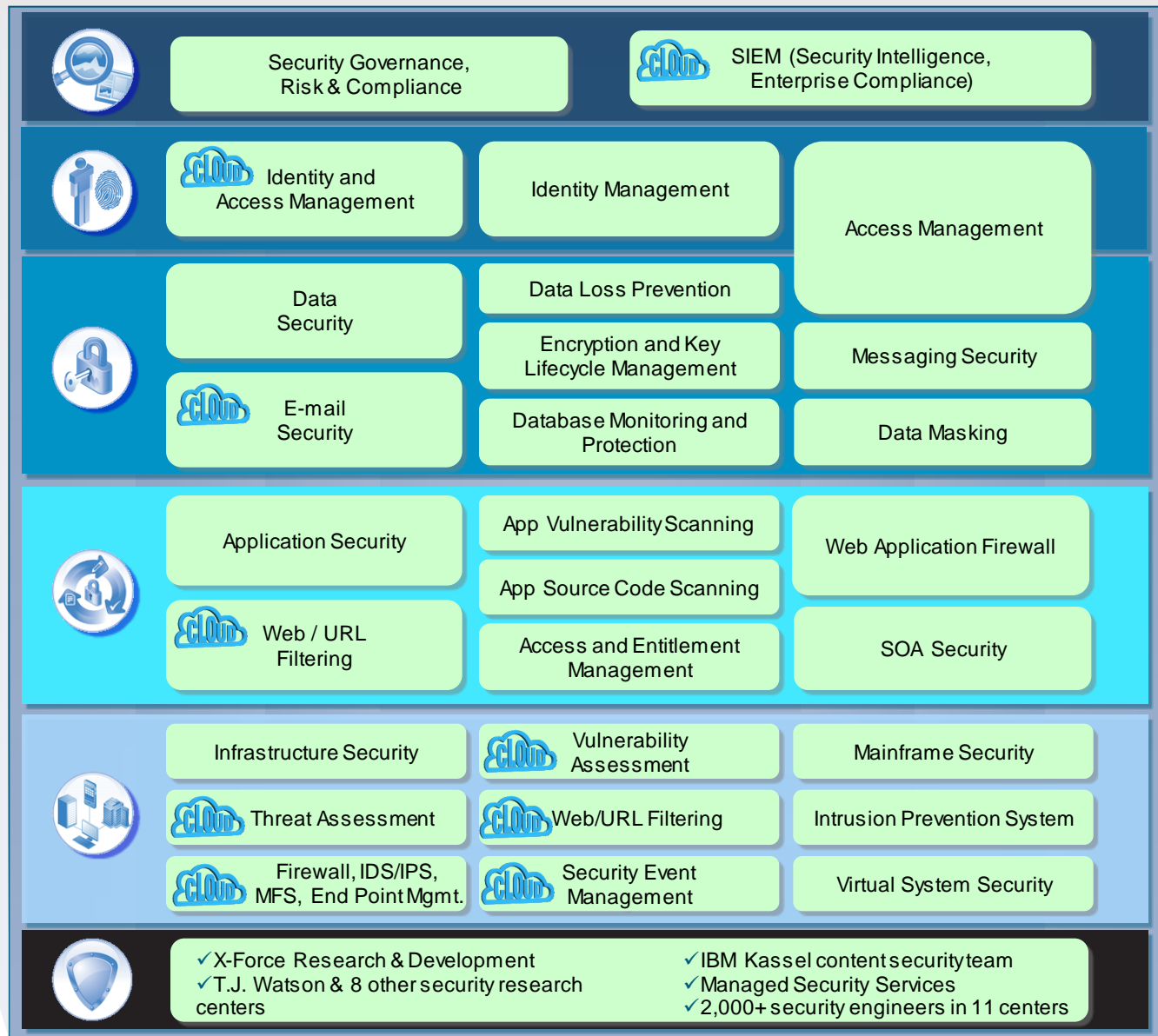
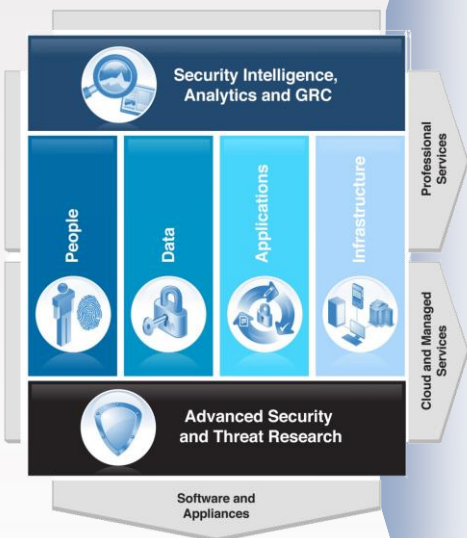
We see whole picture bit more complex way.



# IBM Security – Intelligence, Integration and Expertise

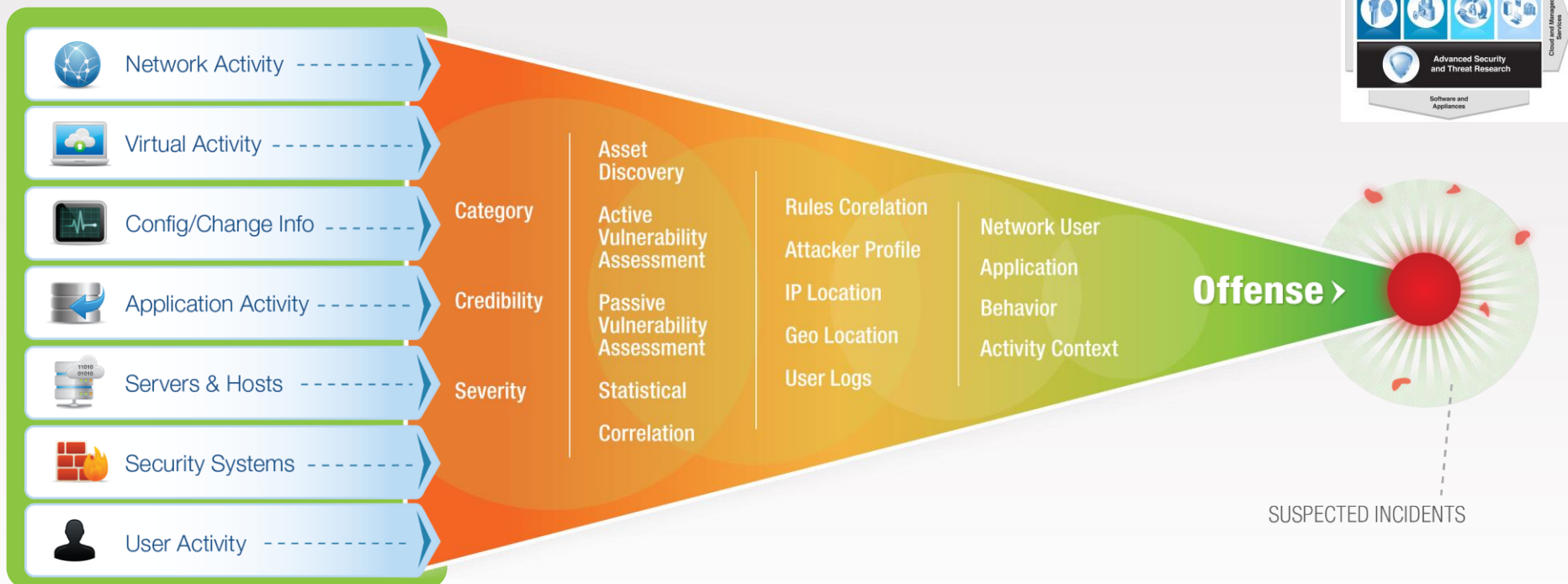


= IBM addresses








**Note:** Unlike the IBM heterogeneous security framework, Oracle focuses on the people level and (partially) the compliance, data, and application levels only.

# Intelligent: Context & Correlation Drive the Deepest Insight



Sources + Intelligence = Most Accurate & Actionable Insight

# End to end, IBM has a strong security competitive posture

	IBM	HP EDS	CA	Symantec	McAfee	EMC	Oracle (Sun)	Cisco	Verizon
 <b>Intelligence, Analytics, GRC</b>	Green	Yellow	Yellow	Green	Red	Green	Green	Red	Red
 <b>People</b>	Green	Red	Green	Red	Red	Yellow	Green	Red	Yellow
 <b>Data</b>	Green	Red	Yellow	Green	Green	Green	Yellow	Red	Red
 <b>Applications</b>	Green	Green	Green	Red	Green	Red	Yellow	Red	Red
 <b>Infrastructure</b>	Green	Green	Yellow	Green	Green	Red	Red	Green	Red

Updated February 2013

# X-Force is the foundation for advanced security and threat research across the IBM Security Framework



The mission of X-Force is to:

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public

# Collaborative IBM teams monitor and analyze the changing threat landscape

## Coverage

**20,000+** devices  
under contract

**3,700+** managed  
clients worldwide

**15B+** events  
managed per day

**133** monitored  
countries (MSS)

**1,000+** security  
related patents



**IBM Research**

## Depth

**17B** analyzed  
web pages & images

**40M** spam &  
phishing attacks

**73K** documented  
vulnerabilities

**Billions** of intrusion  
attempts daily

**Millions** of unique  
malware samples



Mid-year 2013 theme:

# Attackers Optimize Tactics



# 3 Chapters of this Trend Report presentation

## Targeted Attacks and Data Breaches

Operational sophistication  
Watering hole attacks  
Compromised websites far from home  
DDoS diversions

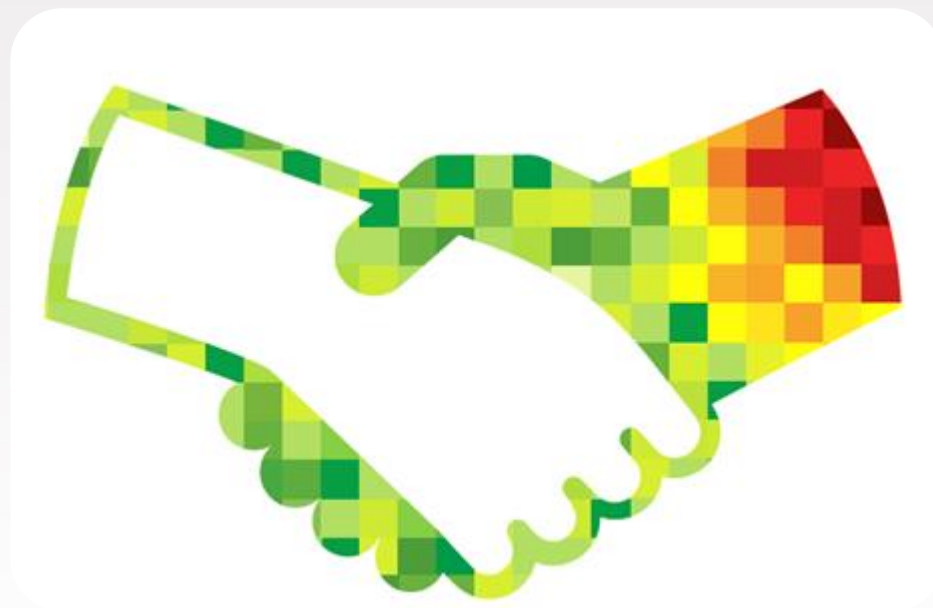
## Social and Mobile

## X-Force by the Numbers

# Exploiting Trust

Security professionals should understand how attackers are taking advantage of trust in relationships to:

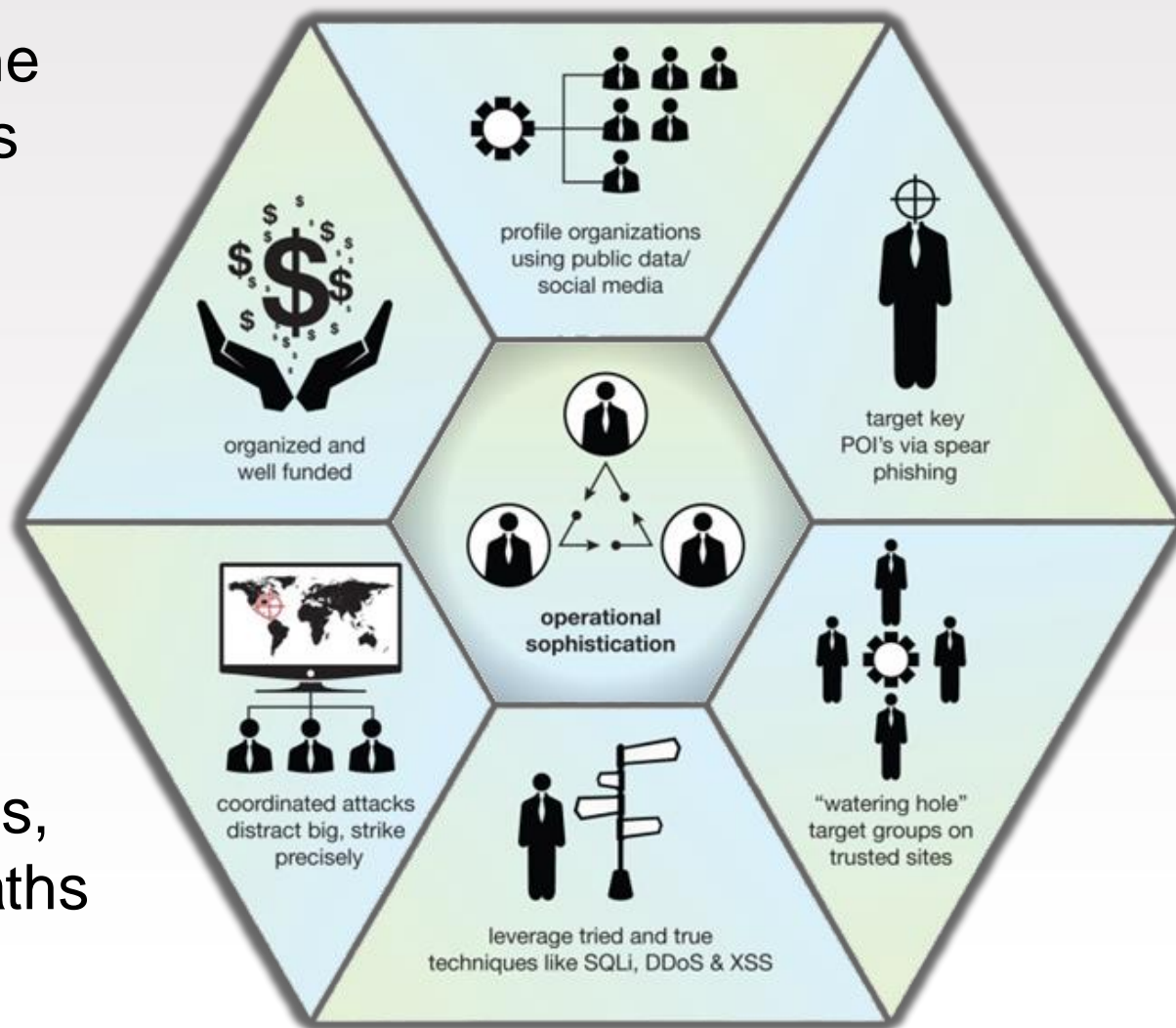
- Breach an organization
- Target groups of users
- Create methods of diversion



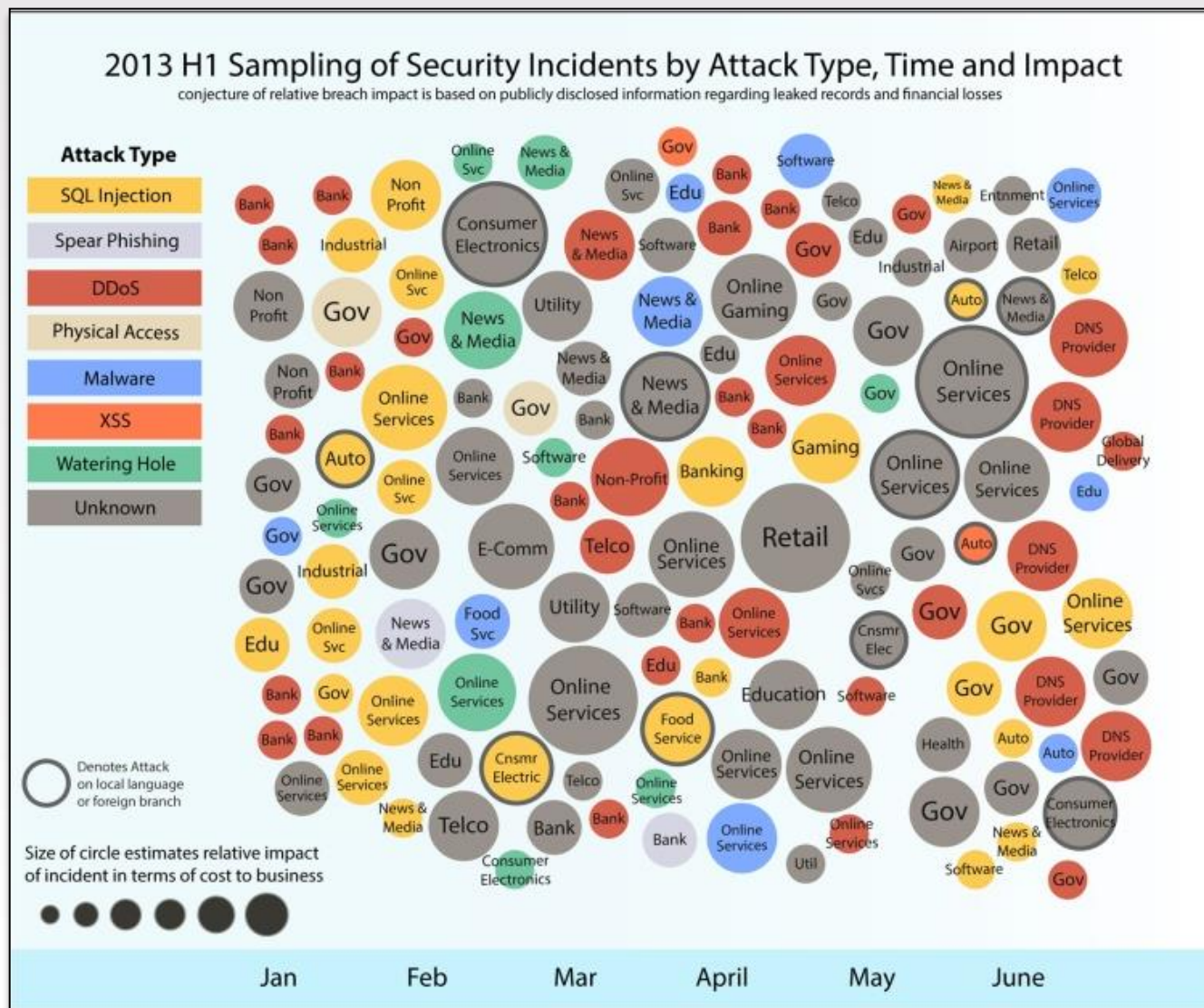
# Operational sophistication

Exploiting trust is one example of attackers becoming more operationally sophisticated to breach targets

Many breaches are not the result of custom malware and zero-day exploits, attackers look for paths of least resistance



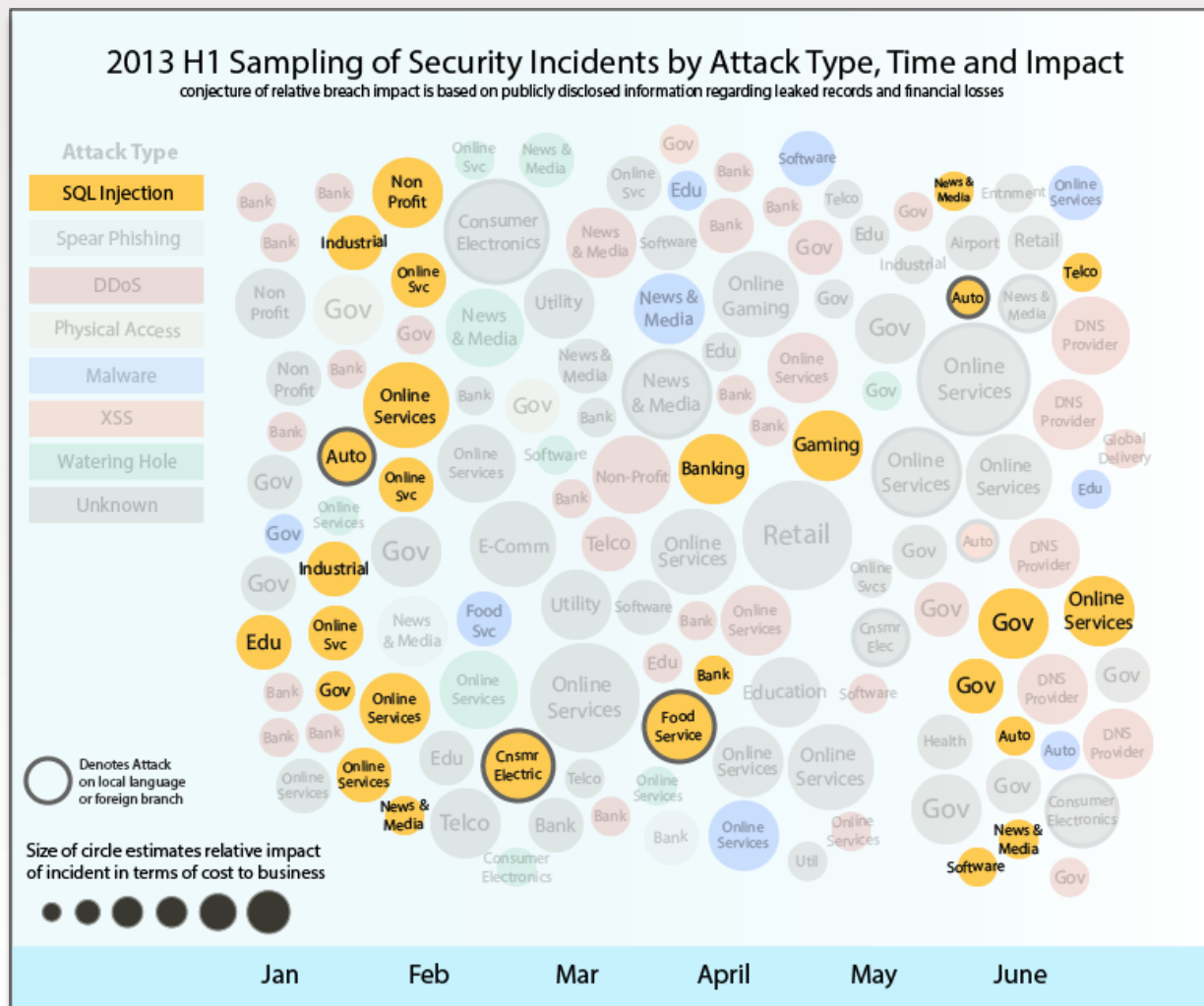
# Security Incidents in the first half of 2013





# SQL Injection

still reliable for breaching databases



**22%** of tracked disclosed breaches

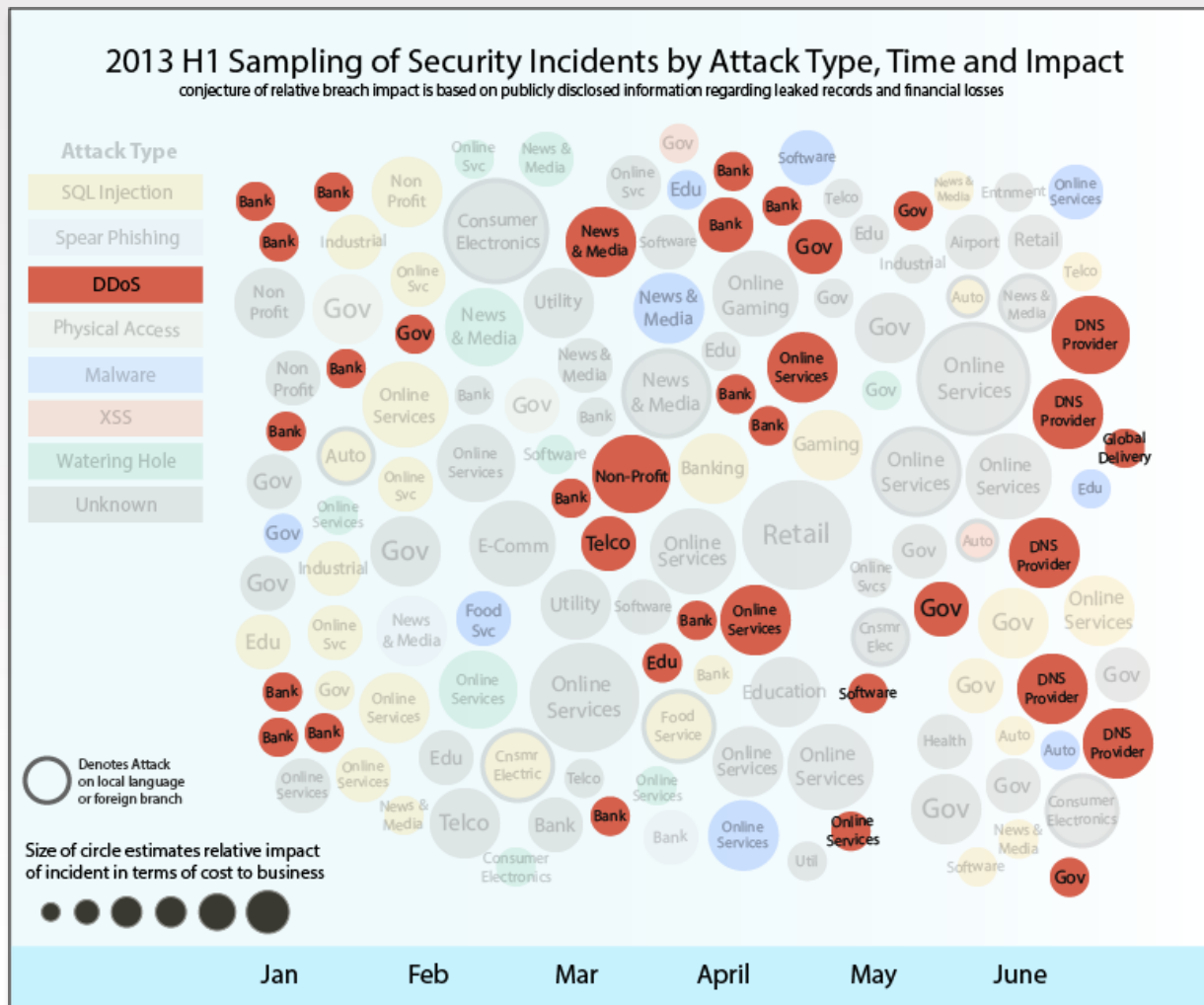
**Low risk / high reward**

- Old CMS installations
- CMS Plugins
- Forum software
- Other popular 3<sup>rd</sup> party scripts



# DDoS Attacks

continue to disrupt businesses



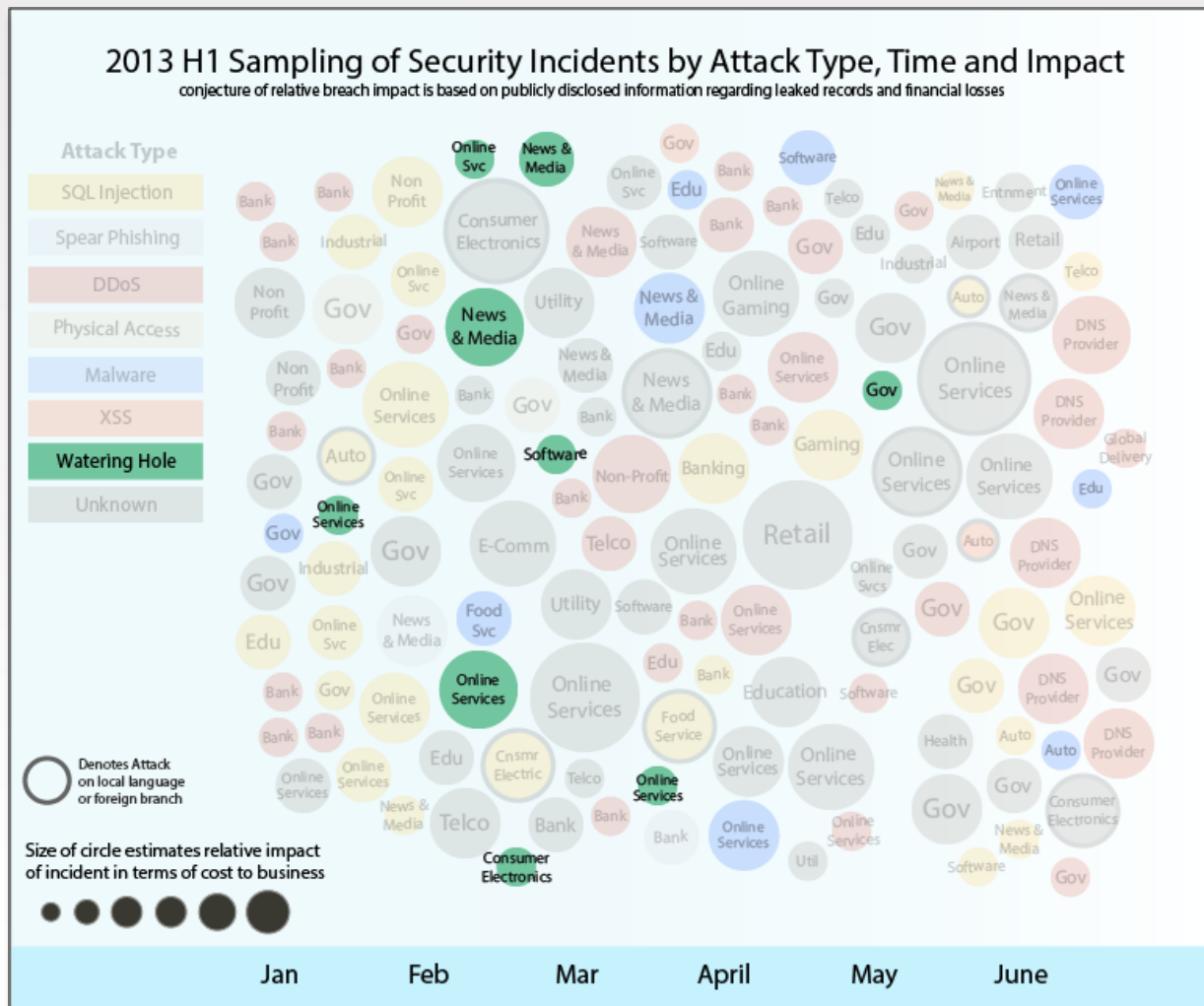
High traffic volume as much as  
**300Gbps**

## Industries affected:

- Banks
- Governments
- DNS Providers

# “Watering Hole”

attacks compromise end user trust



Tainting legitimate sites with zero-day exploits

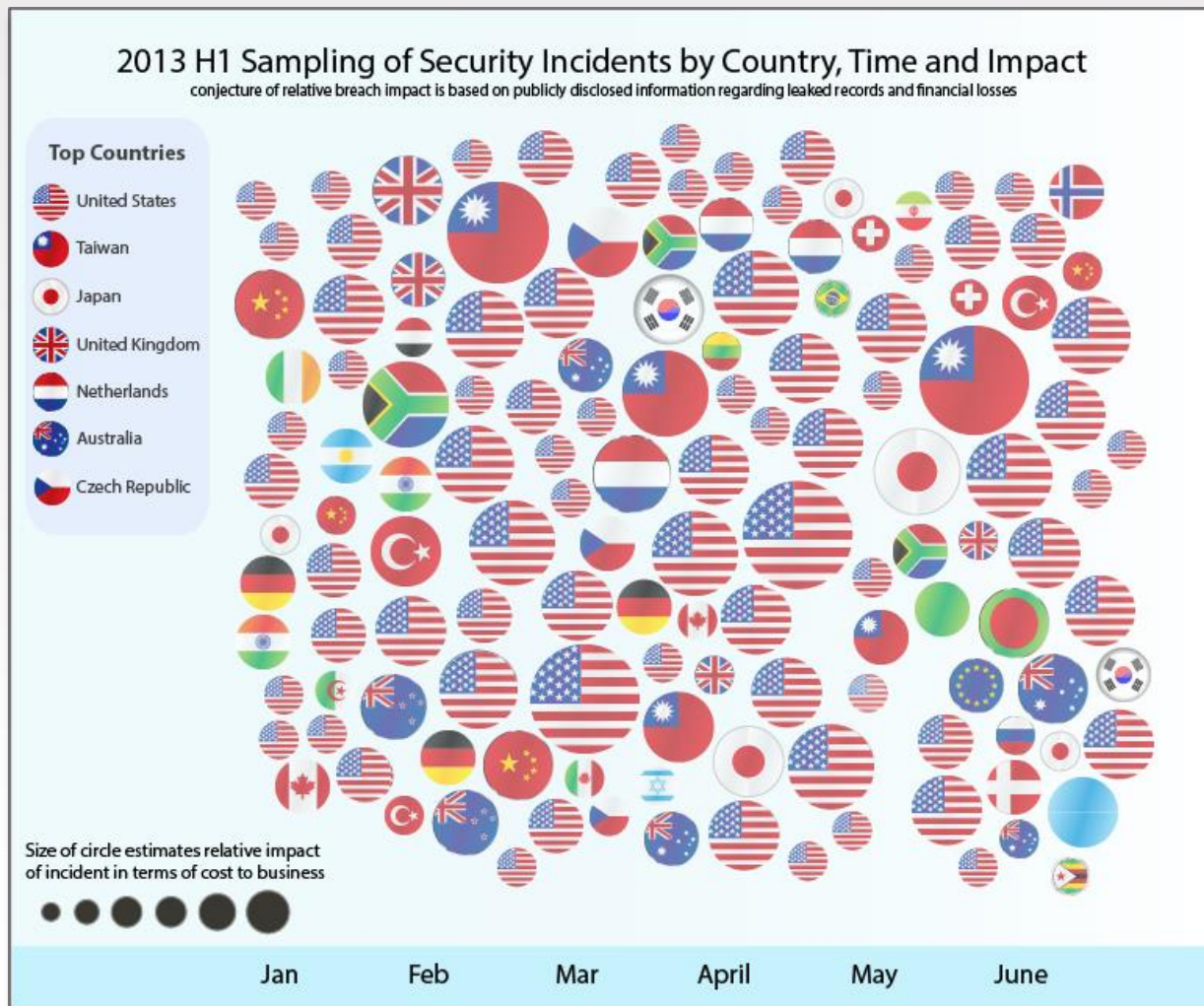
Targeting Savvy Users

- Tech company developers
- Government Employees
- Unsuspecting viewers of trusted sites



# Incidents by Geo

countries most impacted by security incidents



The **United States** most reported breach target location

**Taiwan** was targeted in several foreign branch security incidents

# 3 Chapters of this Trend Report presentation

Targeted Attacks  
and Data Breaches

**Social and Mobile**

Targeting users and abusing trust  
Economic and reputational impact  
Social media Black Market  
Recent advances in Android malware

X-Force by the Numbers



# Social Media

has become a new playground for attackers

**Social Media top target for attacks and mobile devices are expanding those targets**

- Pre-attack intelligence gathering
- Criminals selling accounts
- Campaigns enticing user to click on malicious links





# Economic and Reputational impact

as widespread adoption promotes both personal and business



**Instead of blocking services, organizations should determine how to monitor and mitigate abuses of these platforms**

- Social Media exploits can impact brand and financial loss
- Effective defense is education and to engender suspicion

# Mobile Threats

wherever you go, attackers will follow



**Explosive market growth for Android gets attention of malware authors**

Viable targets with strong intent related to specific organizations

ROI: Malware authors are investing more effort into malware that are more resilient and dangerous



# Advances in **Android Malware**

## **Chuli**

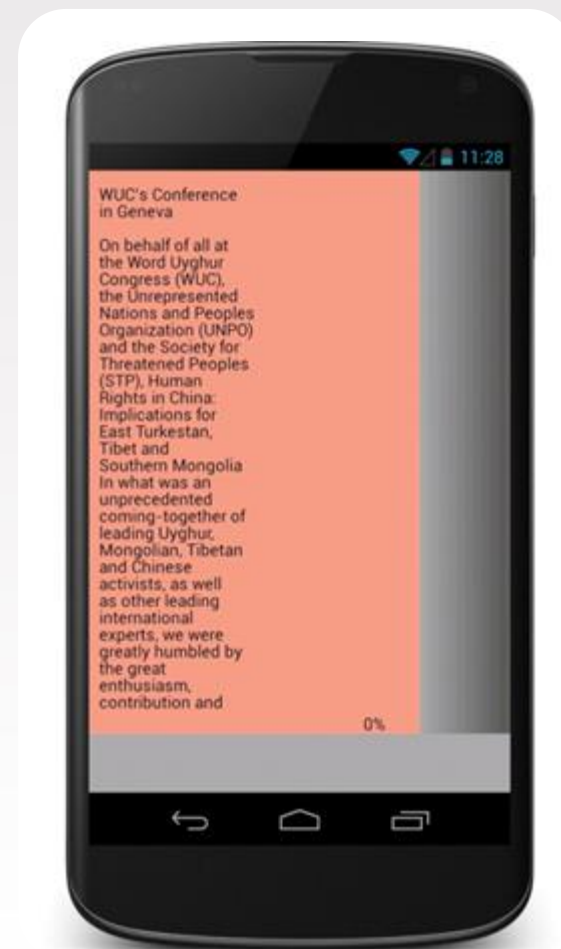
Very targeted attack

- Compromised address book
- Emails sent to targets
- Hooks into Android's SMS service
- Messages routed to remote C&C server

## **Obad**

Spread primarily through SMS spam

- Spreading through Bluetooth
- Device Administration
- Anti-analysis techniques
- Code obfuscation



# X-Force expects the number of Android Malware applications to continue rising

**Degree of sophistication** for this malware will eventually rival those found in desktop malware



**Android Security Enhancements**  
Older devices more at risk with only 6% running latest version

Mobile operating system (OS) fragmentation will remain a problem



# 3 Chapters of this Trend Report presentation

Targeted Attacks  
and Data Breaches

Social and Mobile

**X-Force by the Numbers**

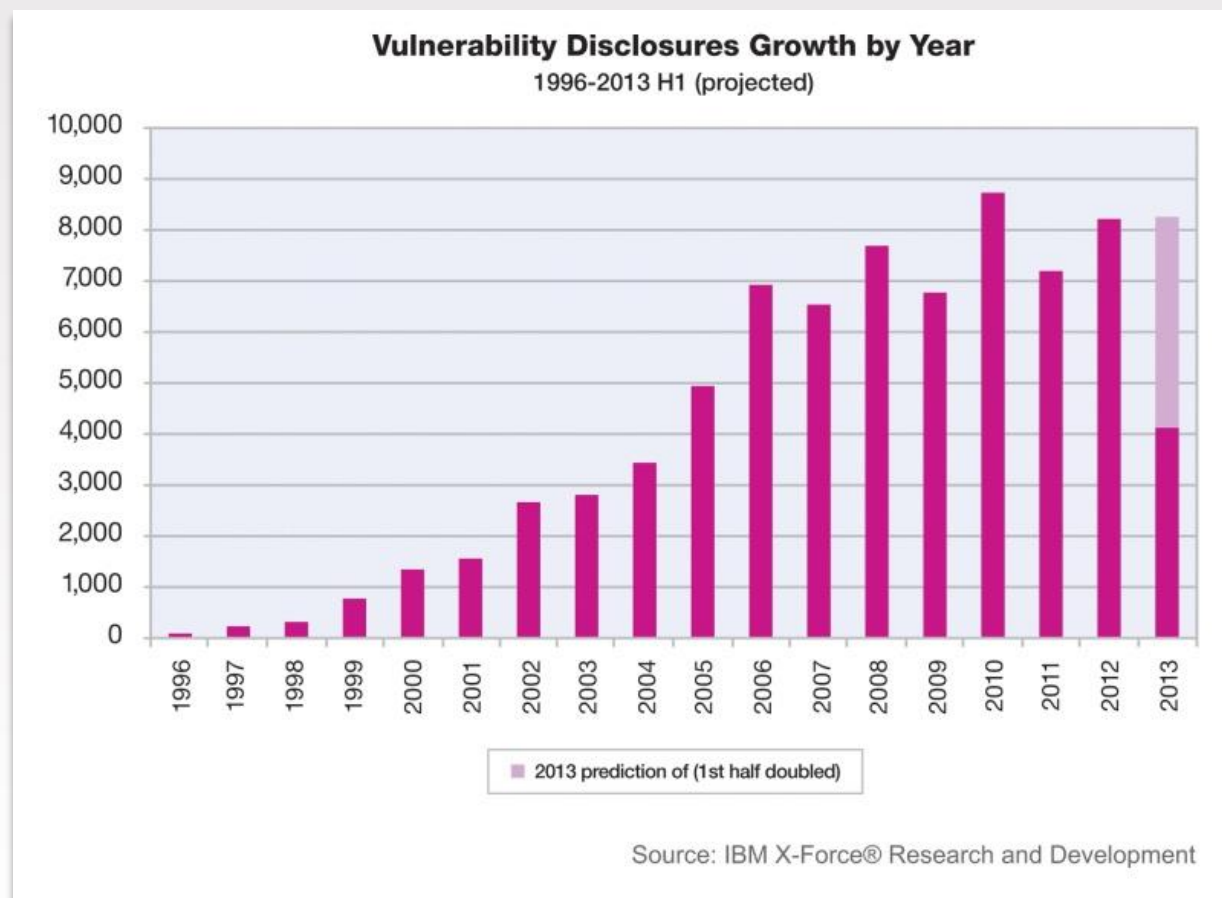
Vulnerabilities  
Exploits  
Web trends  
Spam and Phishing

# Vulnerabilities Disclosures

4,100

publicly  
disclosed  
vulnerabilities

If trend  
continues,  
roughly same  
as 2012





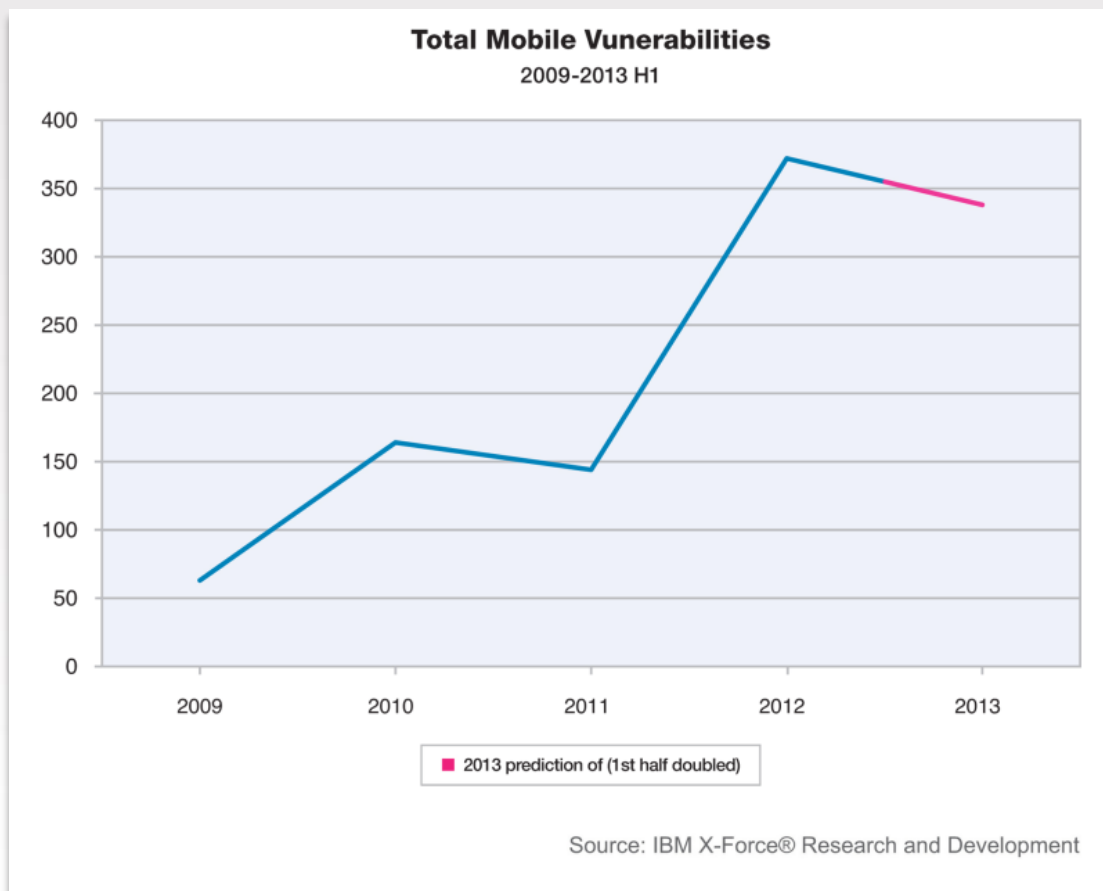
# Vulnerabilities affecting Mobile Software

## Mobile vulnerabilities

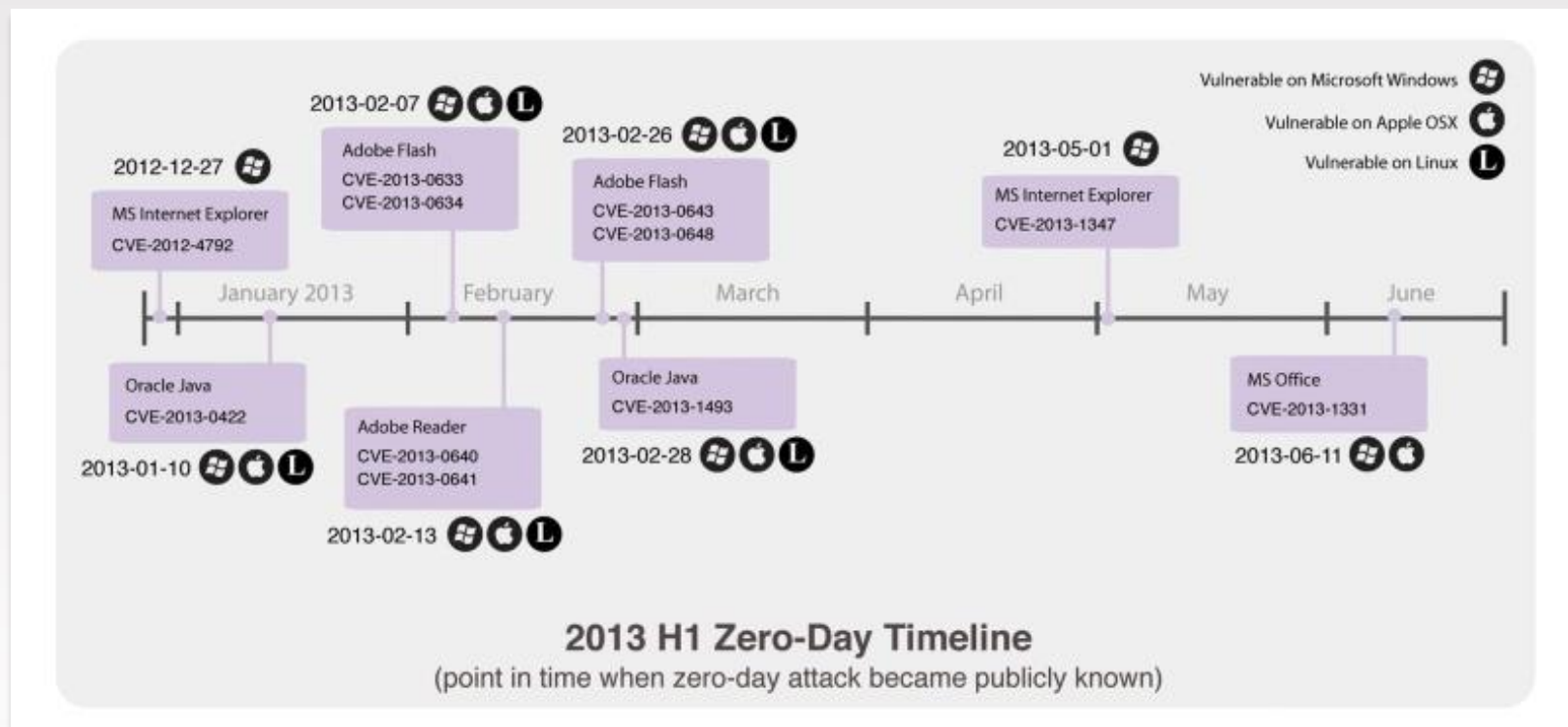
have increased since 2009

Although still small percentage of total overall

Affecting both mobile and desktop software

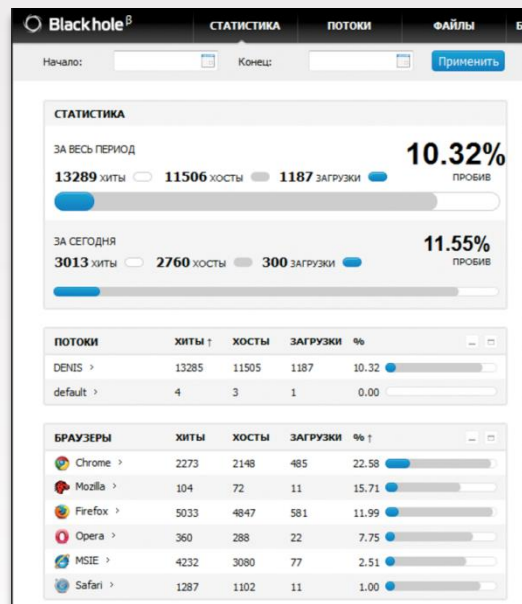


# Zero-Day Vulnerabilities



**80% of zero-day**  
vulnerabilities affect Windows and OSX

# Oracle Java, Adobe Flash, Microsoft IE crucial to protect & patch



## Java

- 0-days quickly utilized in exploit tool kits
- Recent updates allow you to “disable” java
- Default security settings are now “high”

## Adobe Flash

- Most common delivery method, since 2010 Reader sandbox, is via MS Office docs

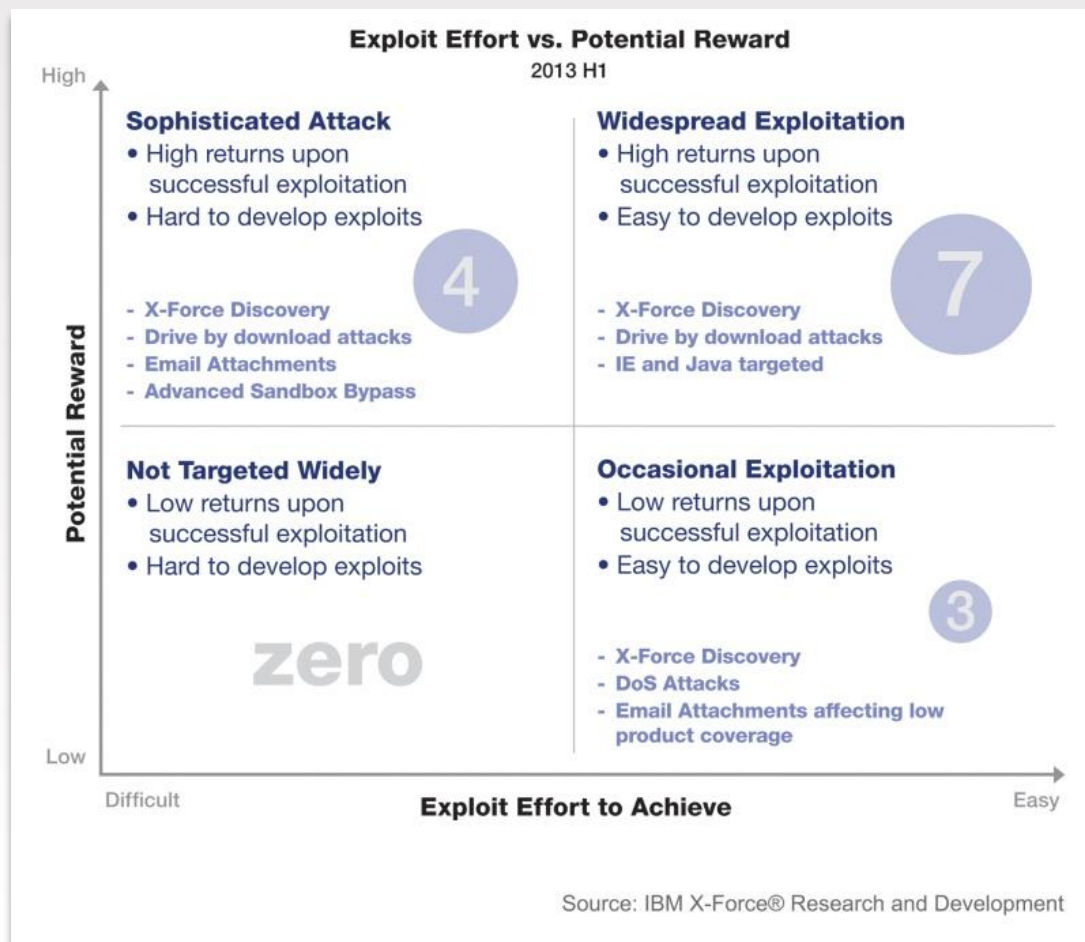
## Microsoft Internet Explorer

- Very targeted attacks and water hole technique

## How to do better:

- Reduce attack surface
- Update installed software
- Get educated on spear-phishing

# Exploit Effort vs. Potential Reward



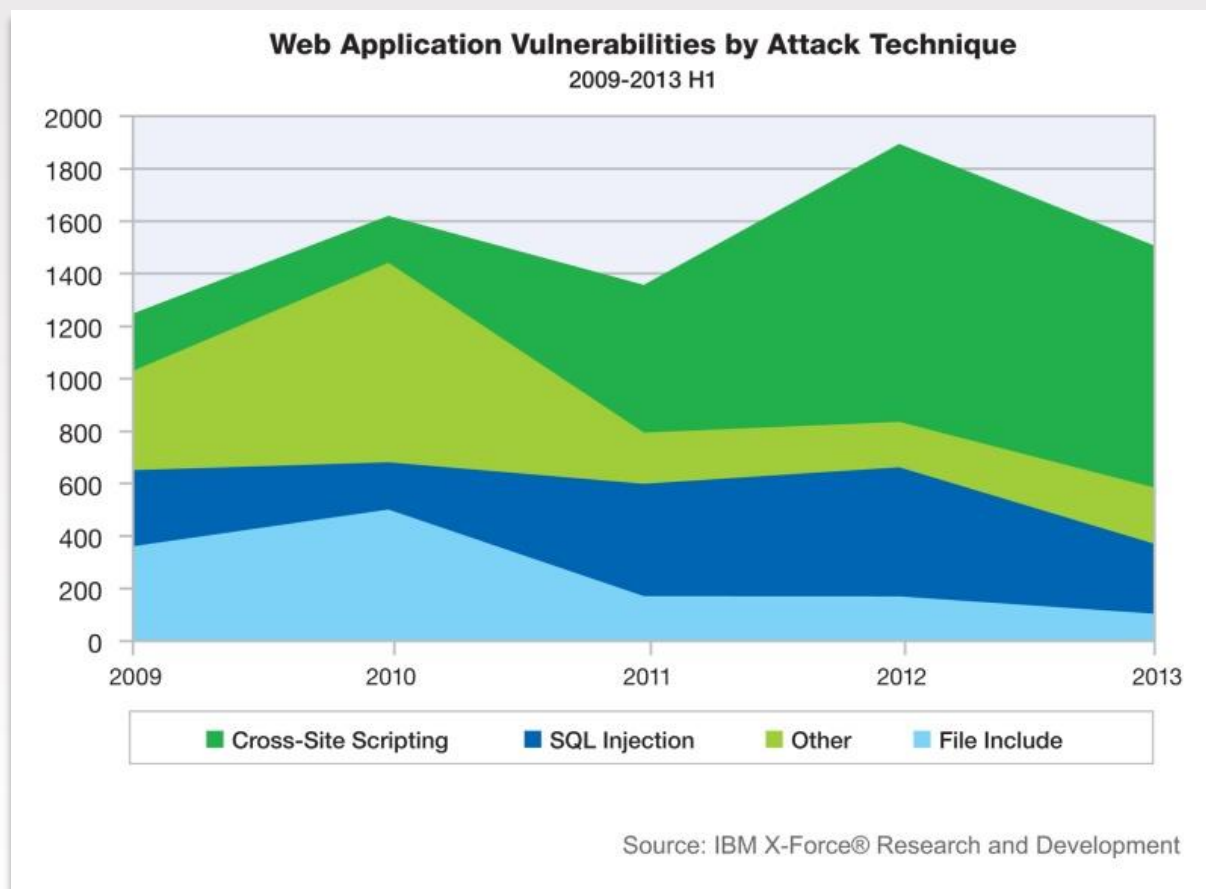
**Drive-by-downloads**  
IE & Java targeted

Easy exploitation with high potential reward – still the sweet spot

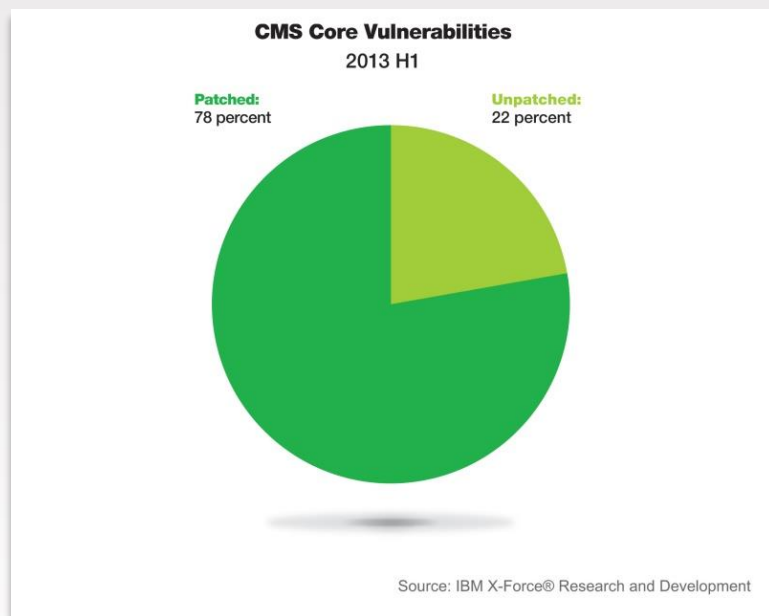
# Web Application Vulnerabilities

**50%**  
of all web  
application  
vulnerabilities  
are XSS

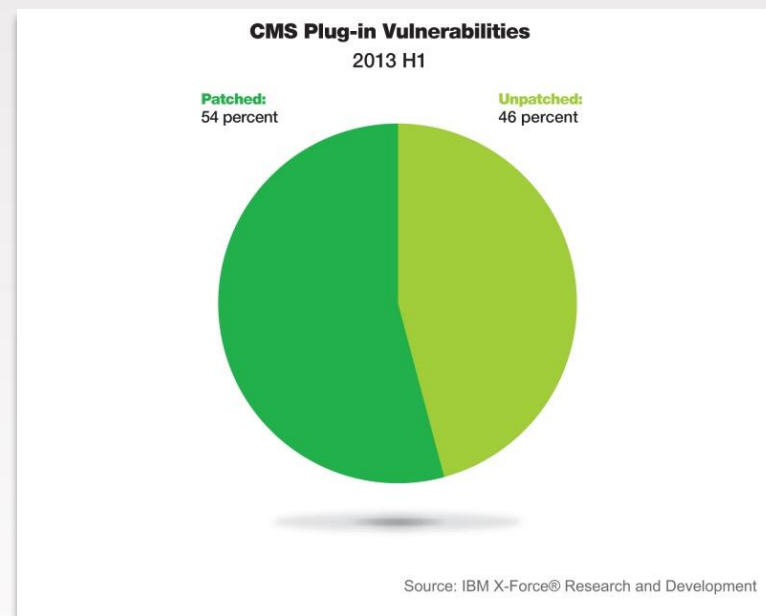
Total slightly  
down in  
comparison  
to 2012



# Content Management System plug-ins continue to provide soft targets



Attackers know that CMS vendors more readily address and patch their exposures



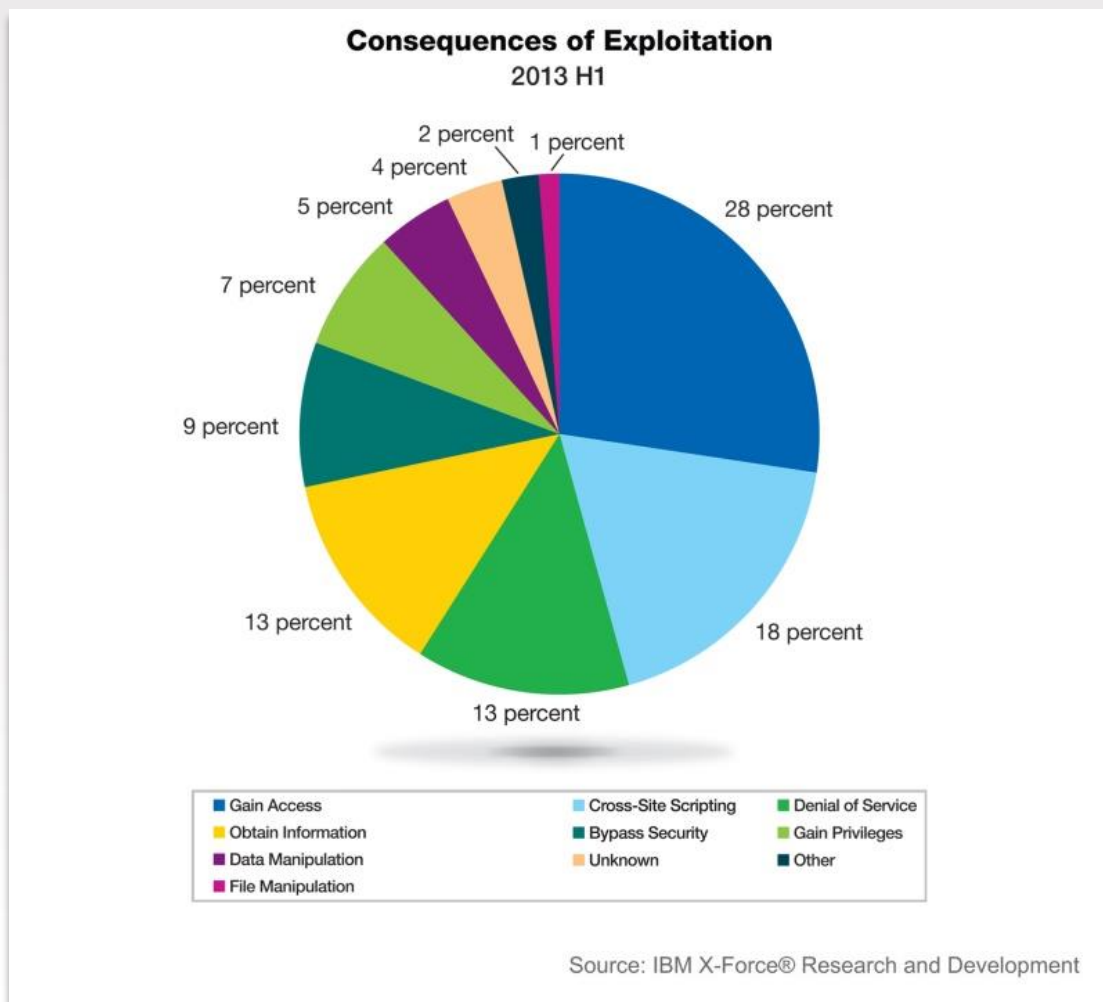
Compared to smaller organizations and individuals producing the add-ons and plug-ins

# Consequences of Exploitation

28%

“gain access”

Provides attacker complete control of system to steal data or launch other attacks



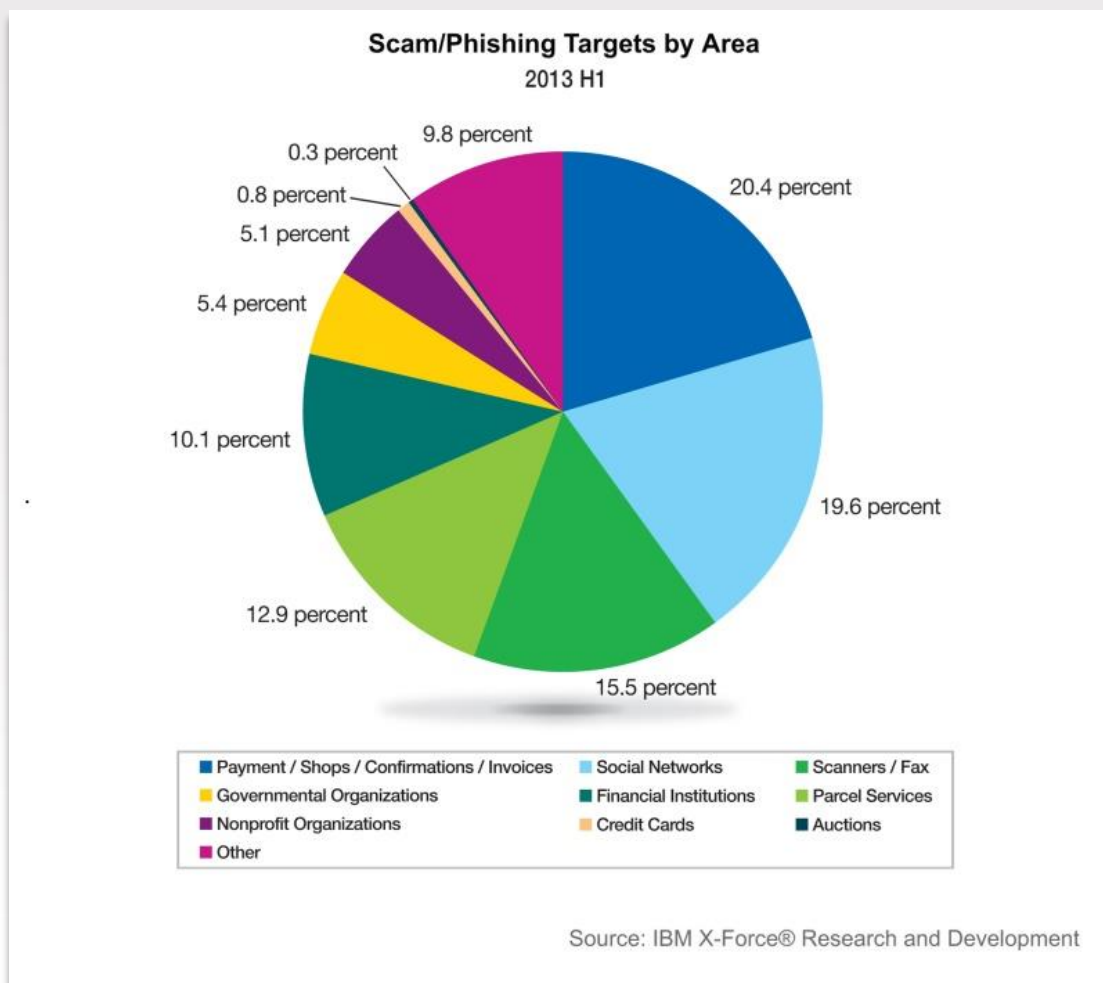


# Scam and Phishing Targets

**55%**

bad links and attachments

- Social networks
- Payment / shops
- Scanners / Fax

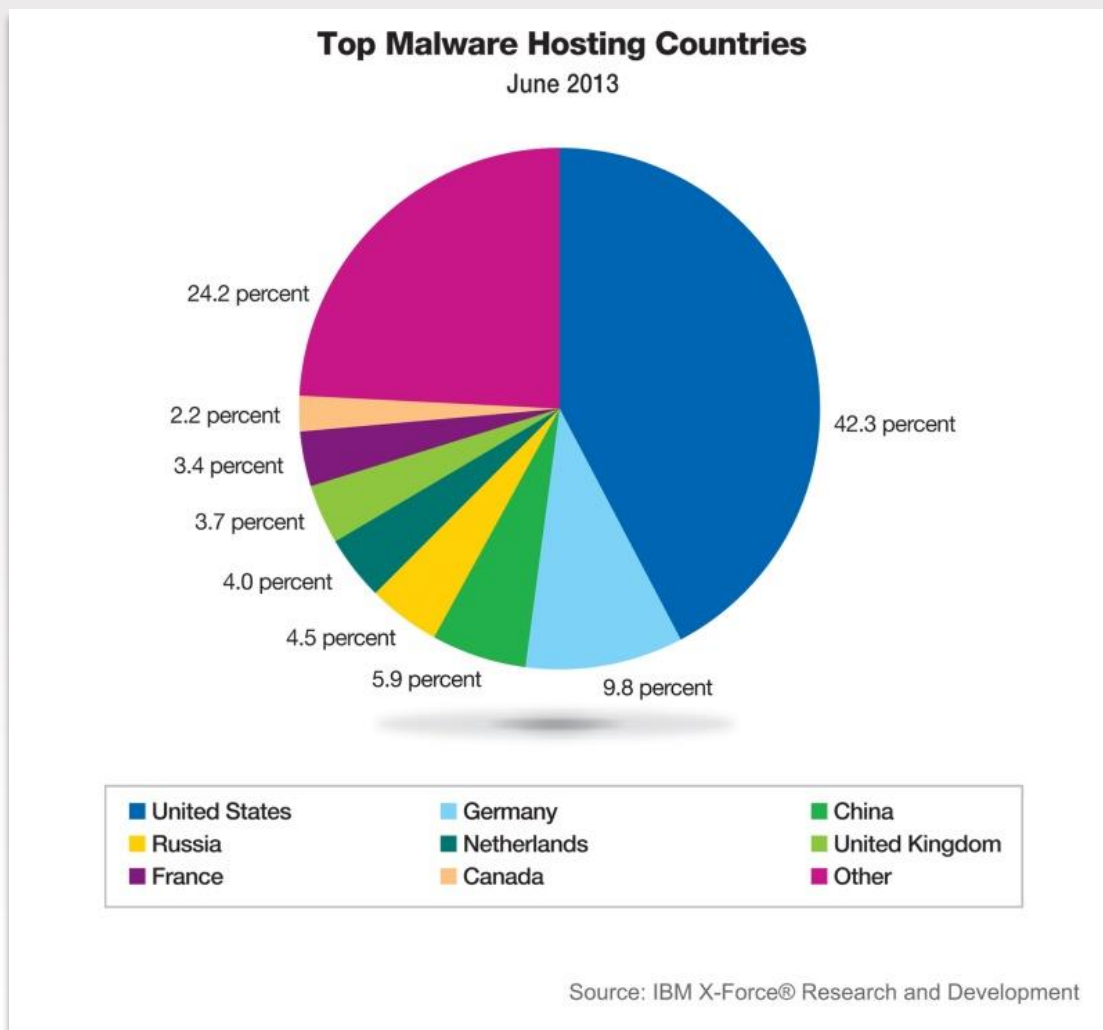


# Malware Hosting

**42%**

malware distributed in U.S.

Germany in second at nearly 10%

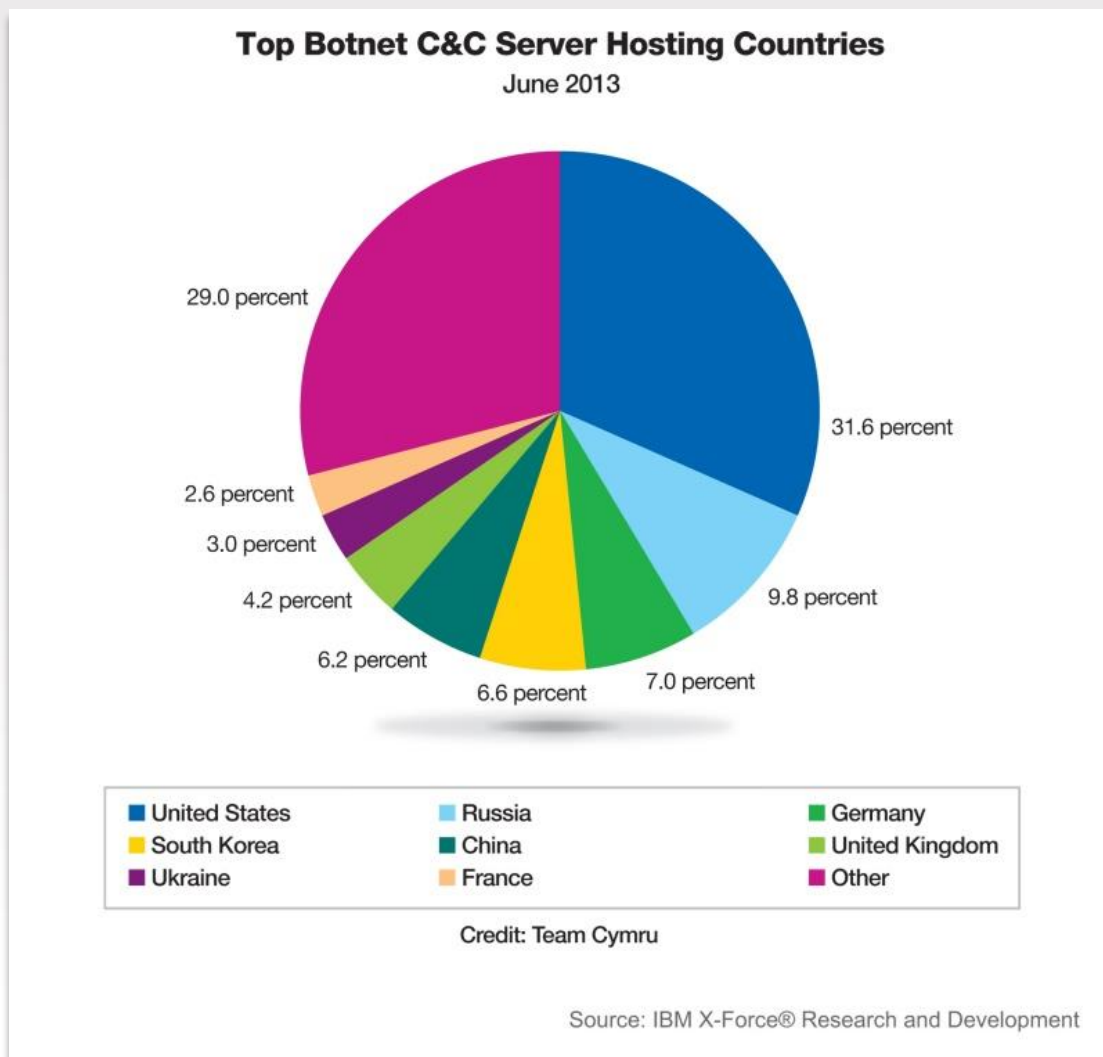


# Botnet Command & Control Hosting

32%

botnet C&C servers in U.S.

Russia in second at nearly 10%



# Key takeaways for **CISOs**



## **Don't forget the basics**

scanning, patching, configurations, passwords

## **Social Defense needs Socialization**

educate users and engender suspicion

## **Defragment your Mobile posture**

constantly apply updates and review BYOD policies

## **Optimize ahead of Attackers**

identify critical assets, analyze behavior, spot anomalies

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

# Thank You

[www.ibm.com/security](http://www.ibm.com/security)



© Copyright IBM Corporation 2013. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.



# 4<sup>th</sup> international annual conference “DSS ITSEC 2013 – IT Security is not enough” (07.11.2013)

**DSS Conference 2013**  
for ITSEC professionals

7th of November, 2013  
Maritim Hotel, Riga, Latvia

**IT SECURITY IS NOT ENOUGH!**

Smart clouds emit smart rain. You better be smart not to get wet.  
7th of November is the day, when You can learn how.

- Latest IT security trends
- 3 paralel sessions
- World class solutions
- Business networking

Learn more at

<http://event.dss.lv>

7th of November, 2013 **DSS Conference 2013** Maritim Hotel, Riga, Latvia  
for ITSEC professionals

- ✓ 4th annual international IT Security Conference
- ✓ 3 parallel sessions and one technical demo room
- ✓ Visited by 230 ITSEC pro's from the Baltic States in 2012
- ✓ Keynote speech from Minister of the Defense of Latvia
- ✓ Keynote from CERT LV - Cybersecurity in Baltics
- ✓ Supported and participation of Latvia ISACA Chapter
- ✓ Supported by Latvian IT Cluster and Latvian Association of Telecommunications
- ✓ More than 20 expert speakers from more than 10 countries

brought by

**Data Security Solutions**  
Think security first

platinum partners

**IBM** **ALSO**  
more than distribution

gold partners

**radware** **headtechnology**  
Smart Network. Smart Business. it-security

supporters