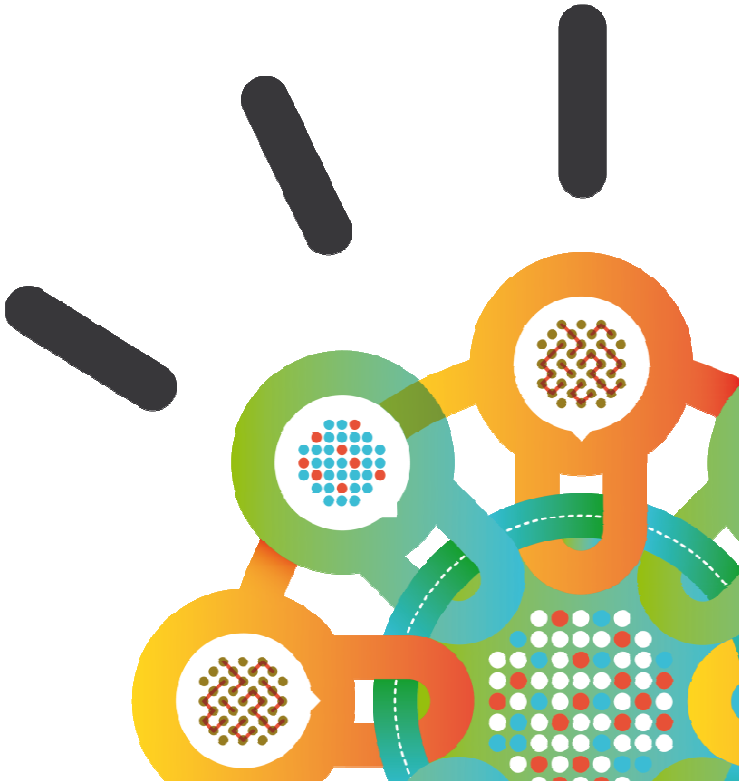
Security Intelligence.
Think Integrated.

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

X-Force Threat Response Team

October 2013



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


X-FORCE

**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

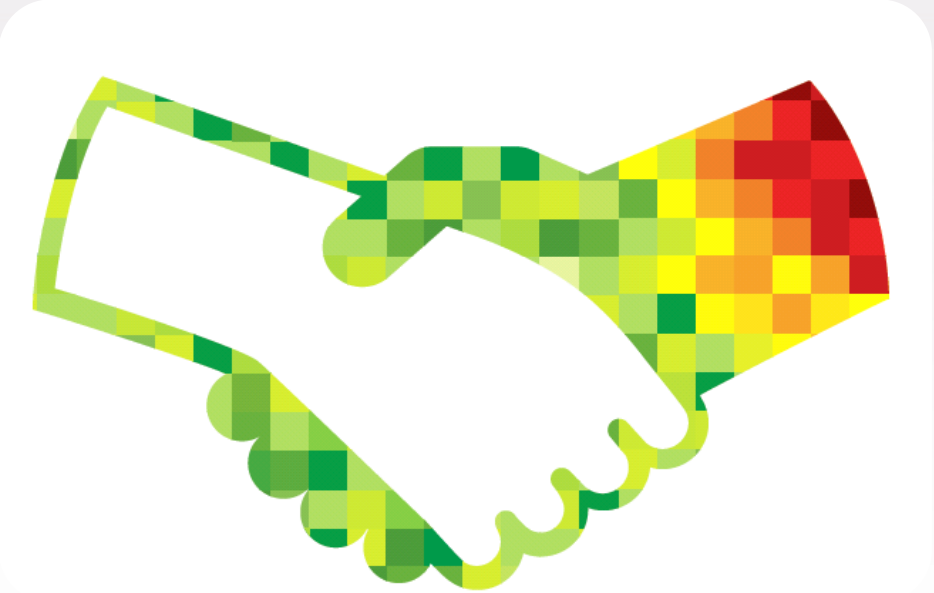
## Social and Mobile

## X-Force by the Numbers

# Exploiting Trust

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

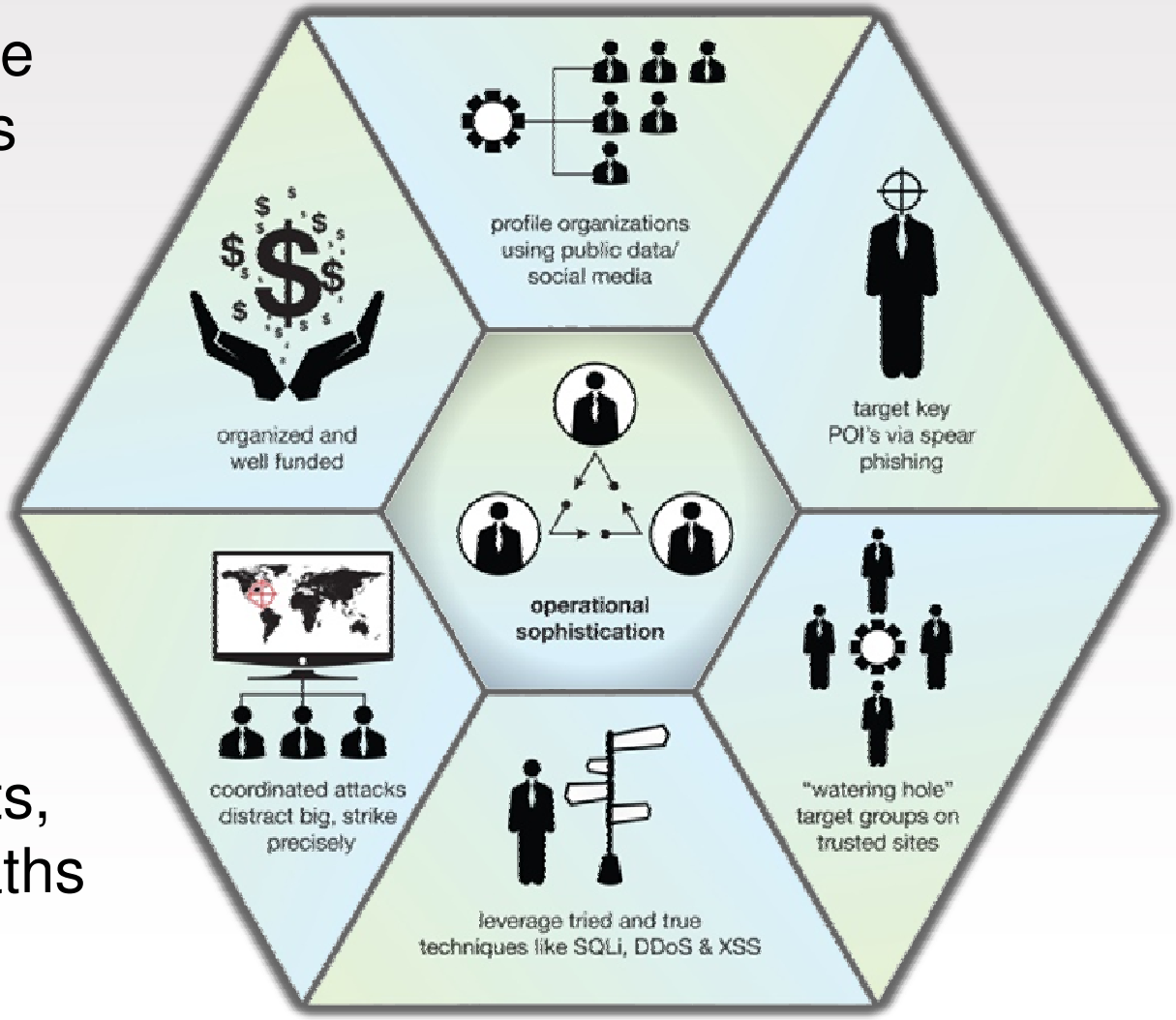
- Breach an organization
- Target groups of users
- Create methods of diversion



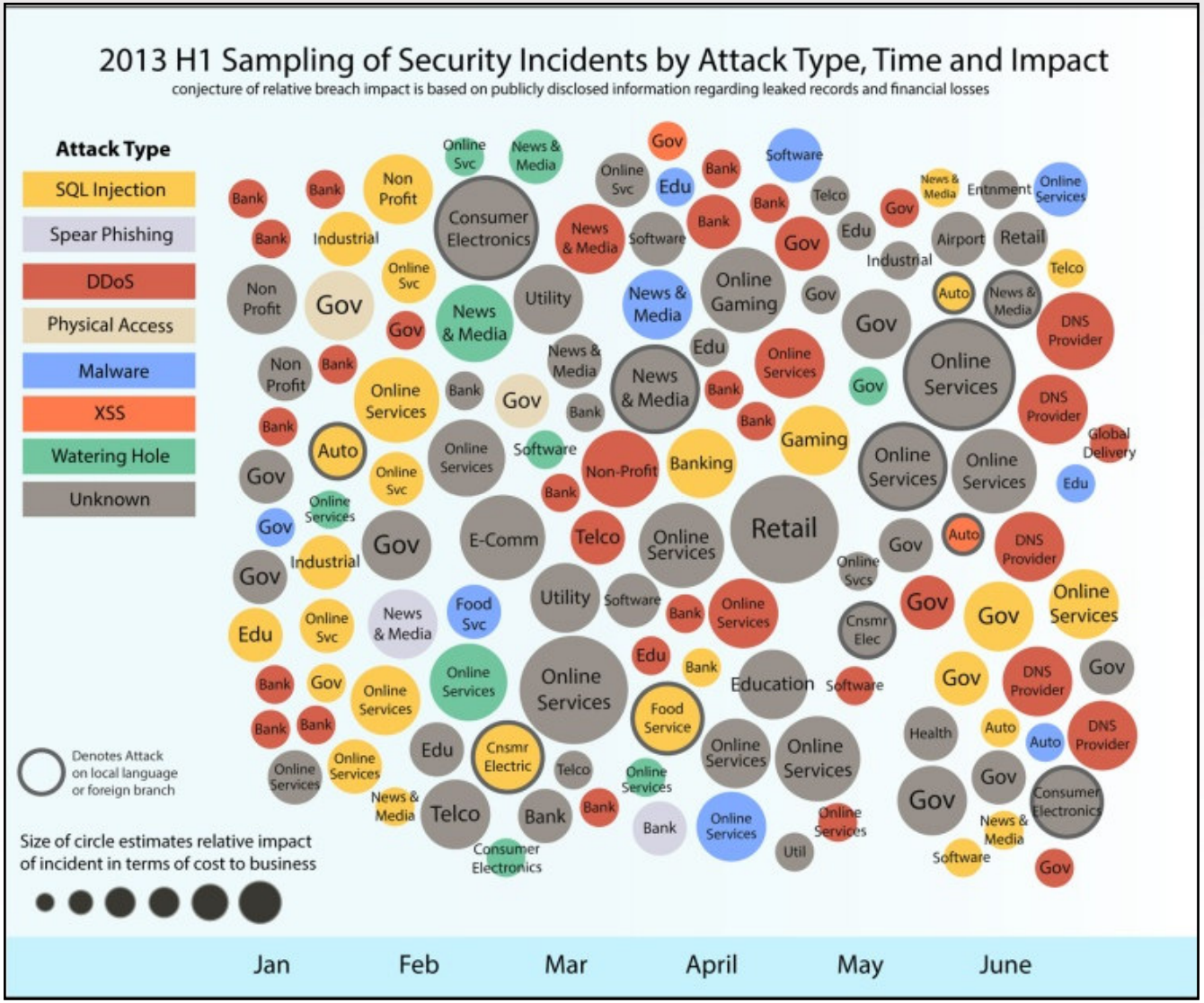
# Operational sophistication

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

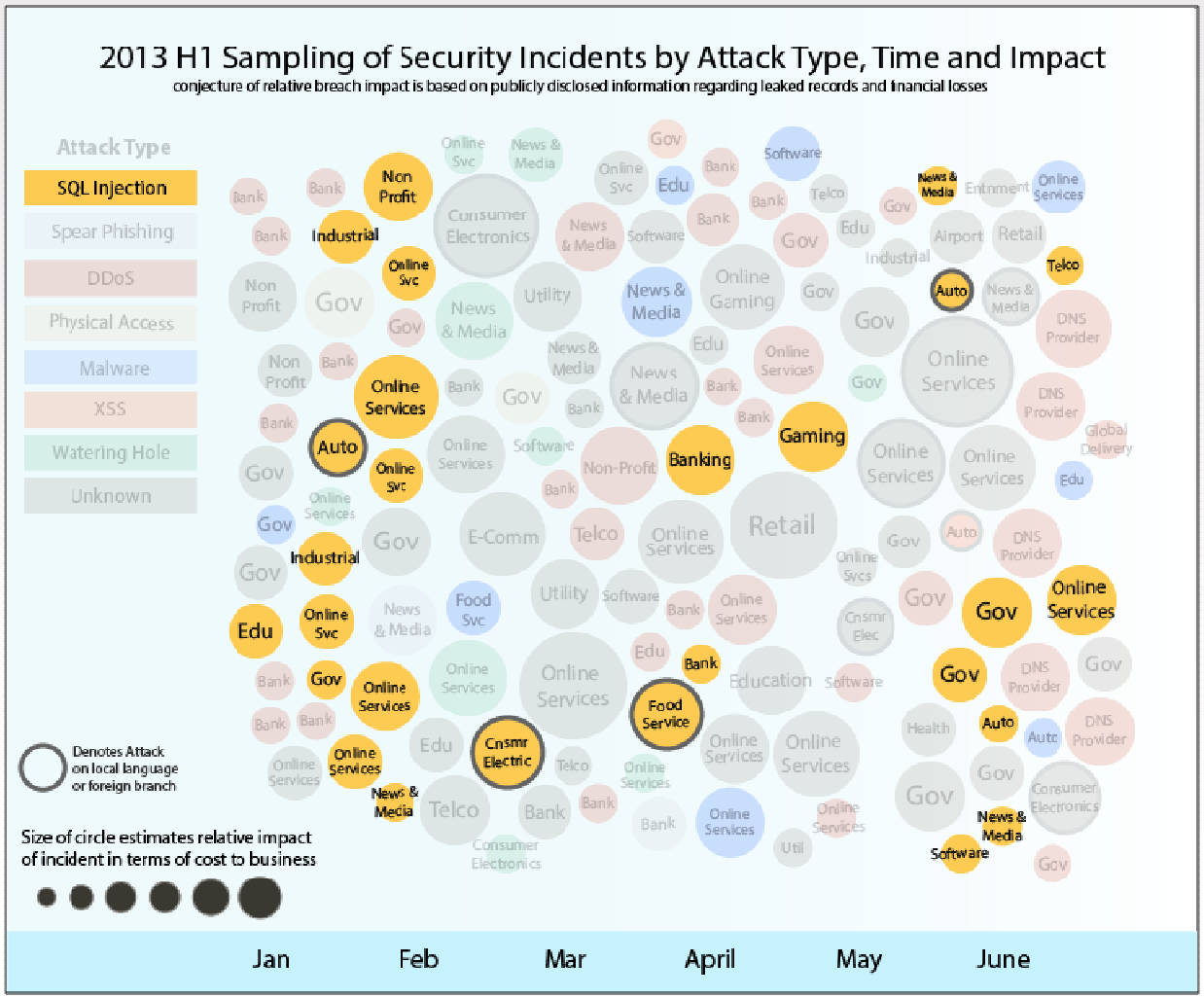


# Security Incidents in the first half of 2013



# SQL Injection

## still reliable for breaching databases

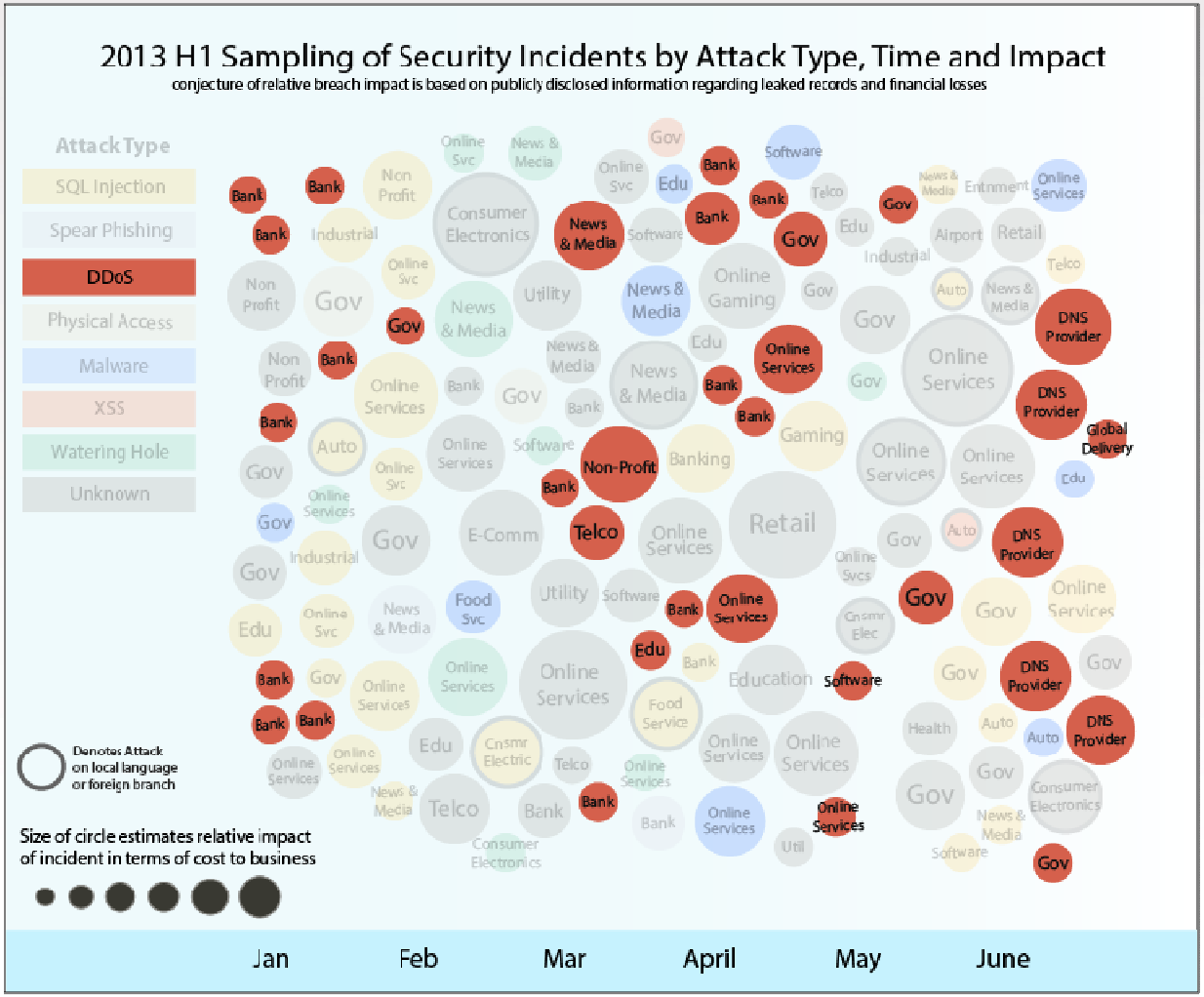



**22%** of tracked disclosed breaches

**Low risk / high reward**

- **Old CMS installations**
- **CMS Plugins**
- **Forum software**
- **Other popular 3rd party scripts**

# DDoS Attacks
## continue to disrupt businesses




**High traffic volume as much as**

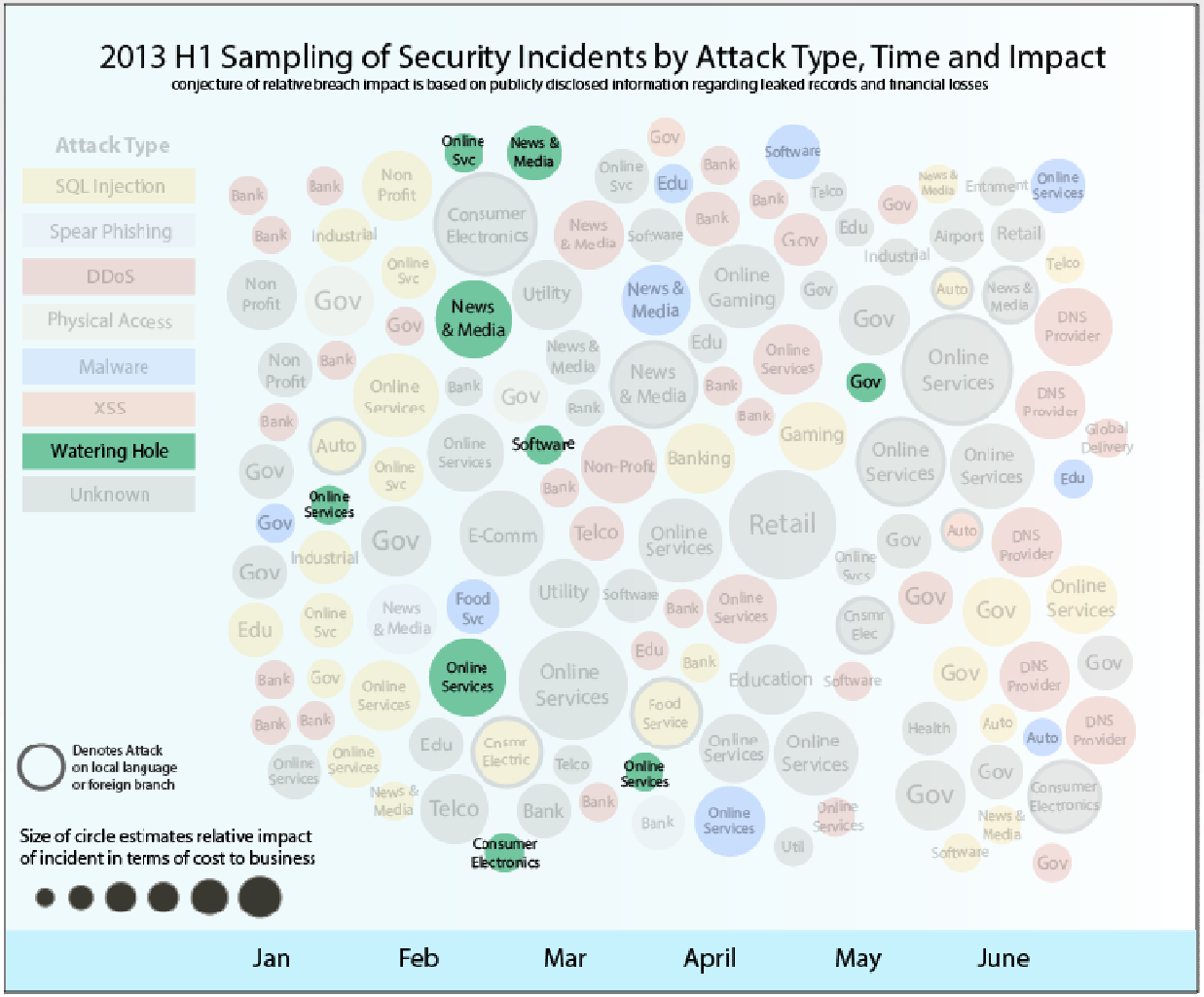
**300Gbps**

**Industries affected:**

- **Banks**
- **Governments**
- **DNS Providers**

# "Watering Hole"

## attacks compromise end user trust



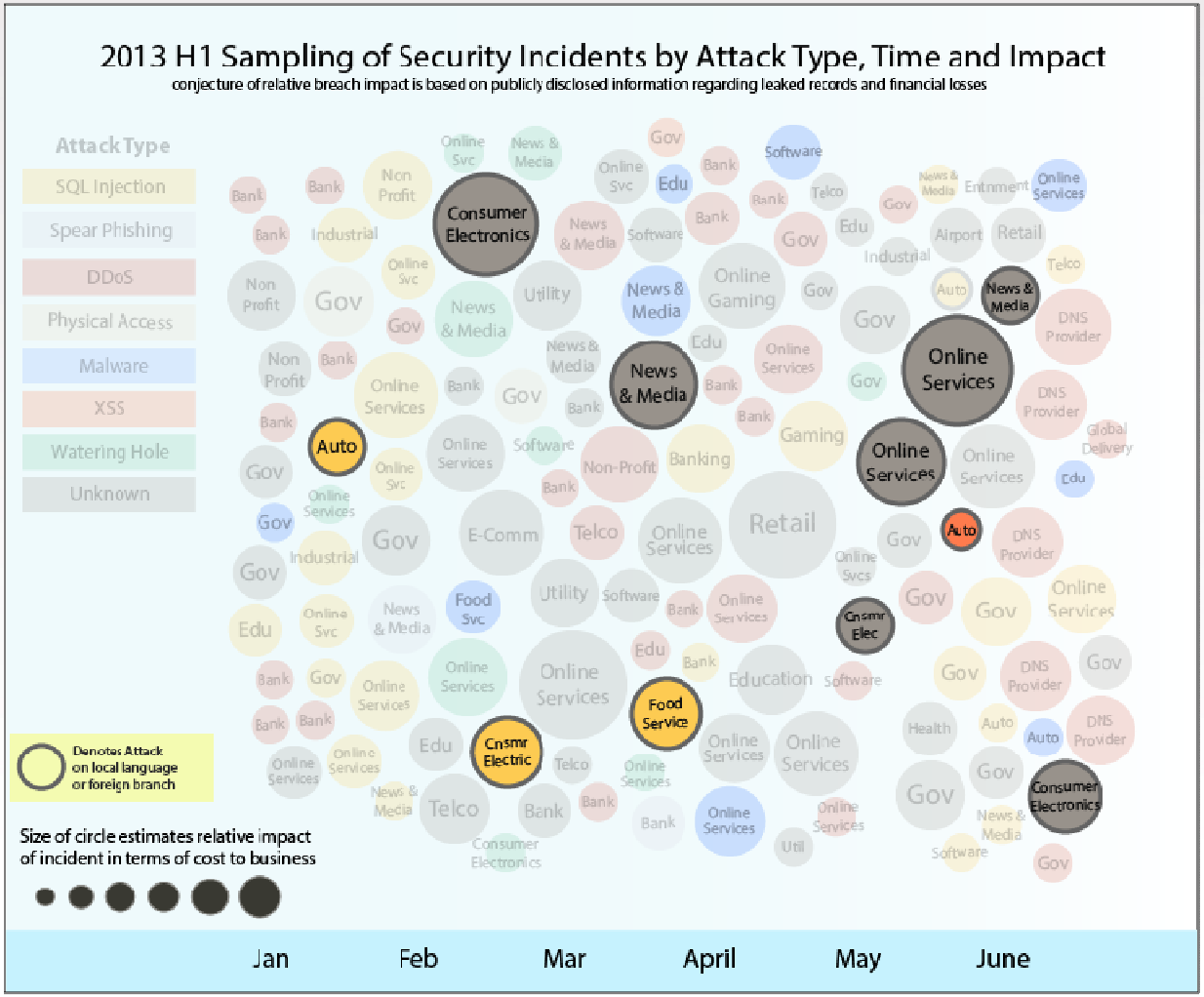

**Tainting legitimate sites with zero-day exploits**

### Targeting Savvy Users

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

# Disenfranchised

## foreign branch or local language sites tarnish brands



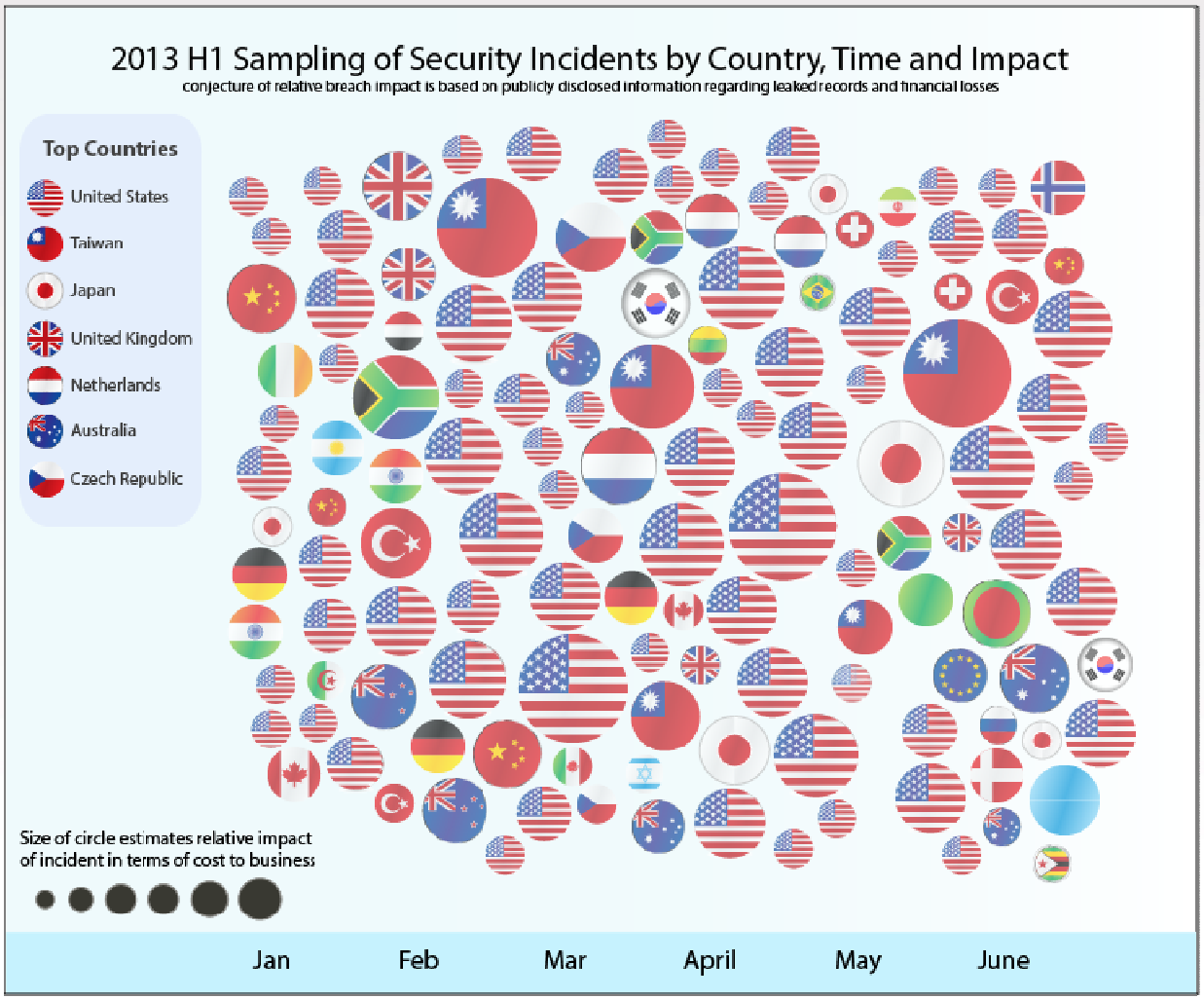

**Global brands targeted in foreign countries outside of home office**

**Attackers rely on**

- **Lower security on local language sites**
- **Temporary micro-sites which gather user data**
- **Tarnish brands with path of least resistance**

# 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

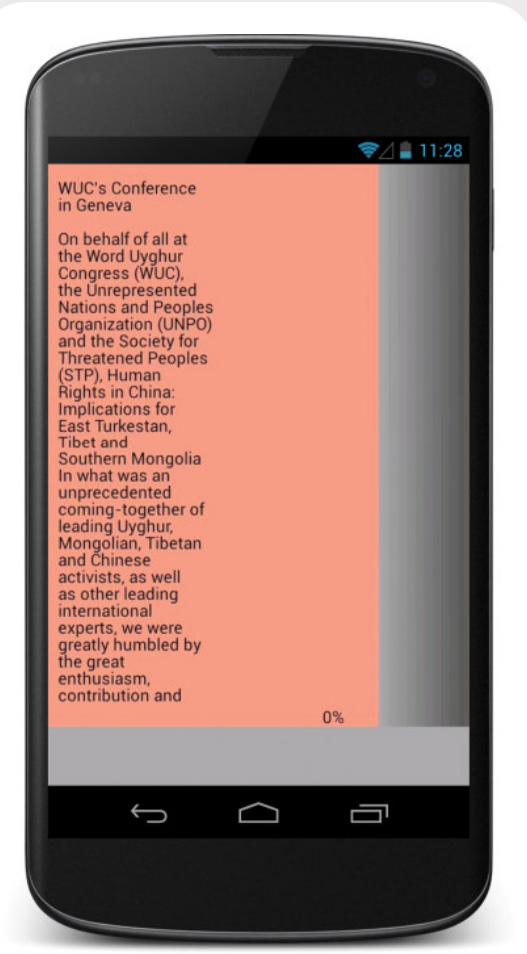
Very targeted attack

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

## Obad

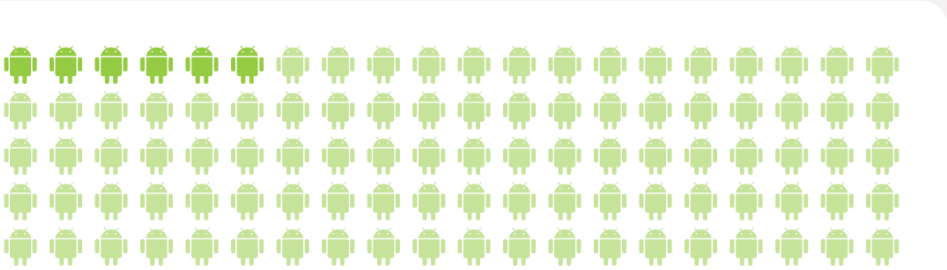
Spread primarily through SMS spam

- 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**

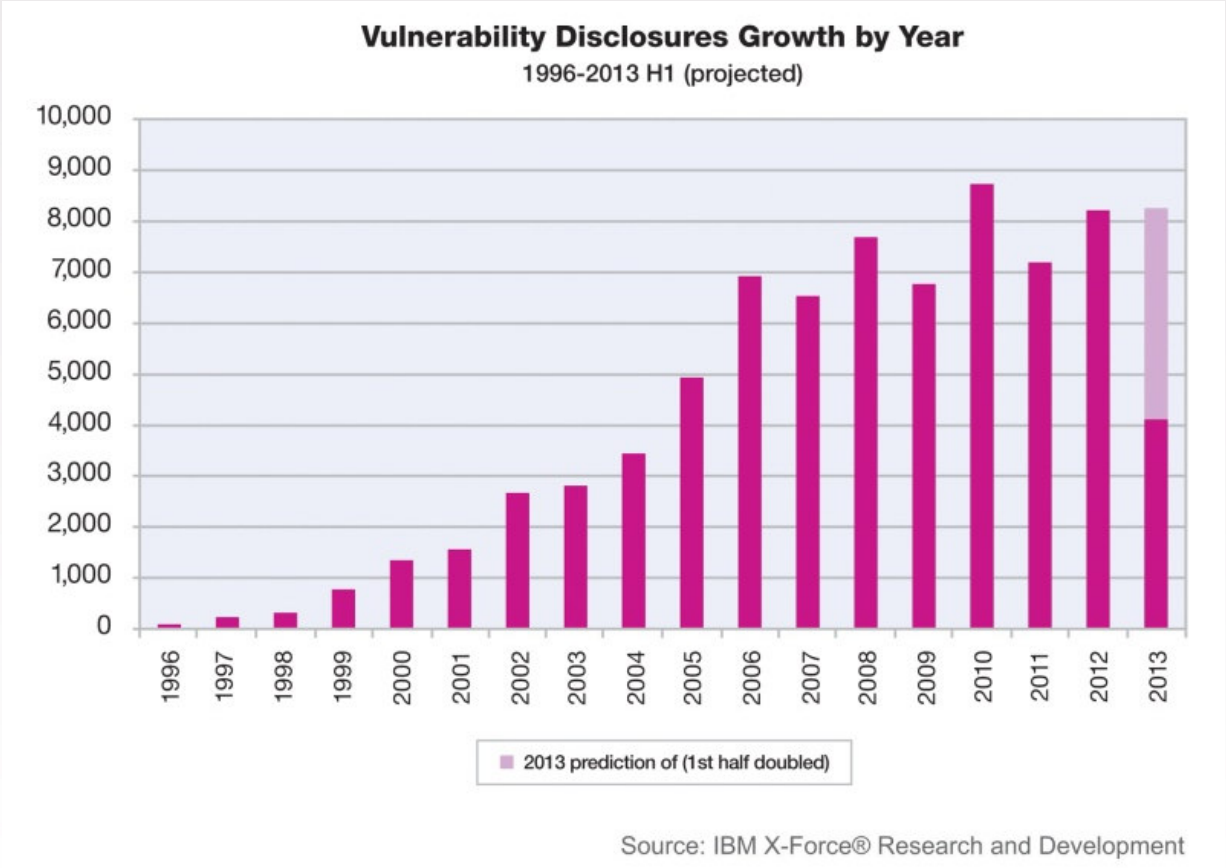
- Vulnerabilities
- Exploits
- Web trends
- Spam and Phishing

# Vulnerabilities Disclosures

**4,100**

publicly disclosed vulnerabilities

If trend continues, roughly same as 2012

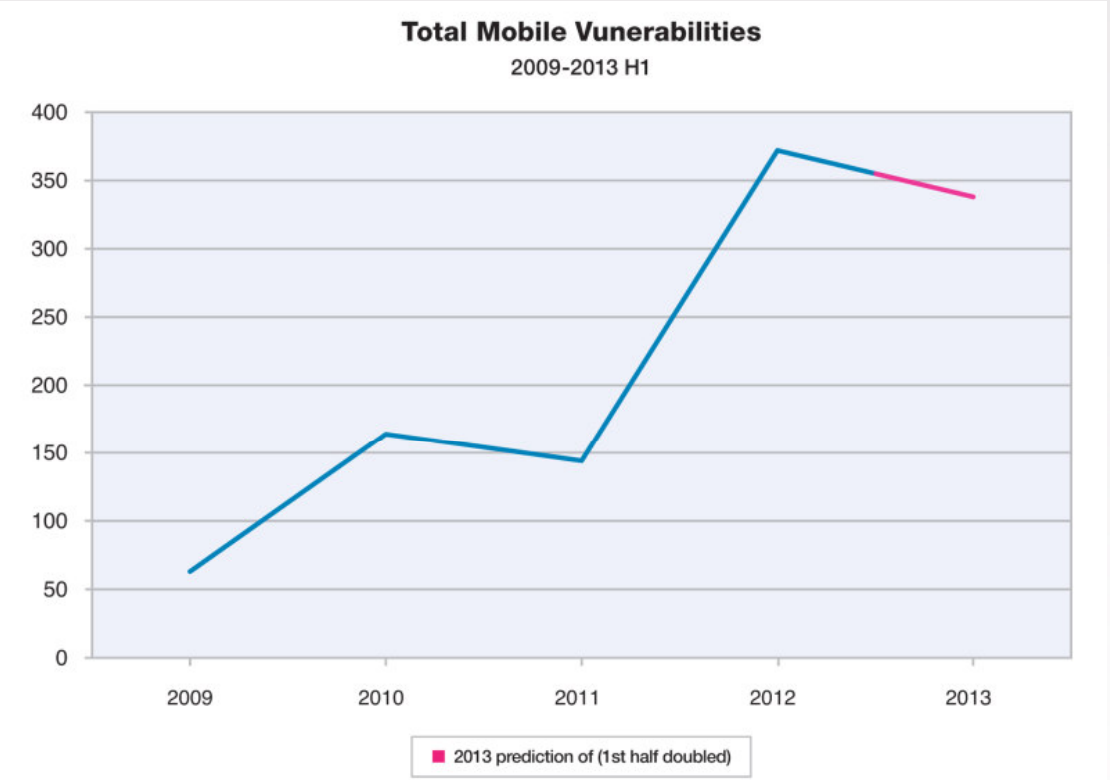


# Vulnerabilities affecting Mobile Software

**Mobile vulnerabilities** have increased since 2009

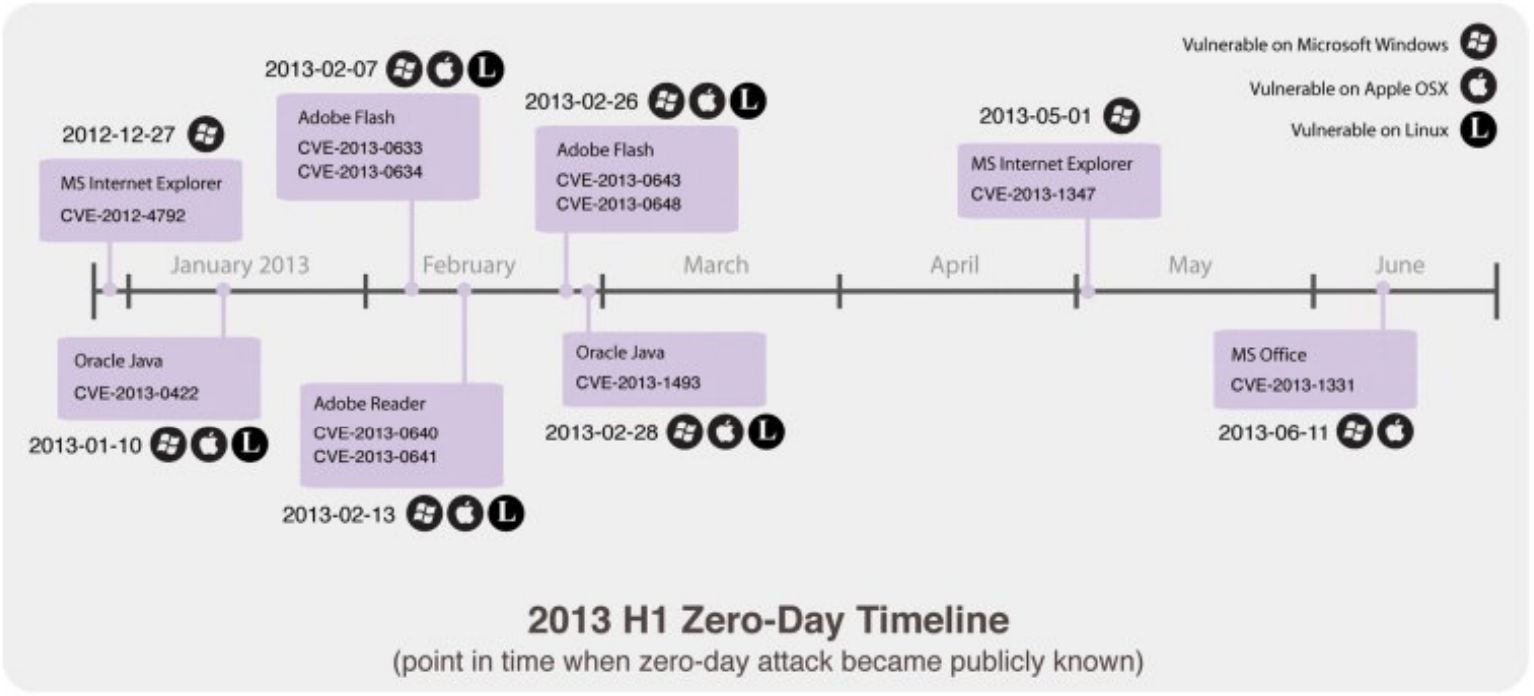
Although still small percentage of total overall

Affecting both mobile and desktop software




Source: IBM X-Force® Research and Development

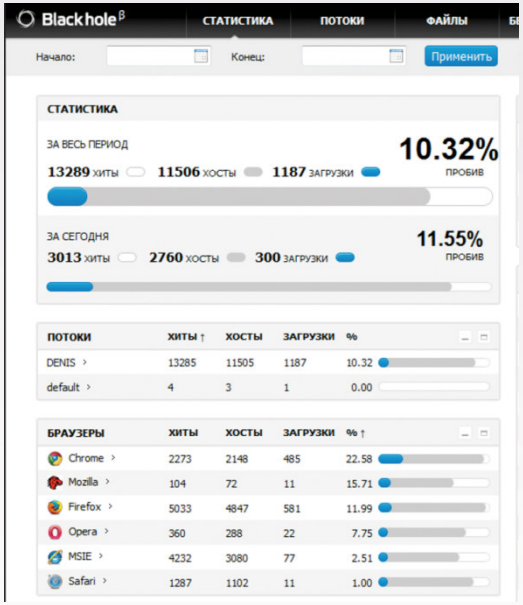
# Zero-Day Vulnerabilities




**2013 H1 Zero-Day Timeline**
(point in time when zero-day attack became publicly known)

**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

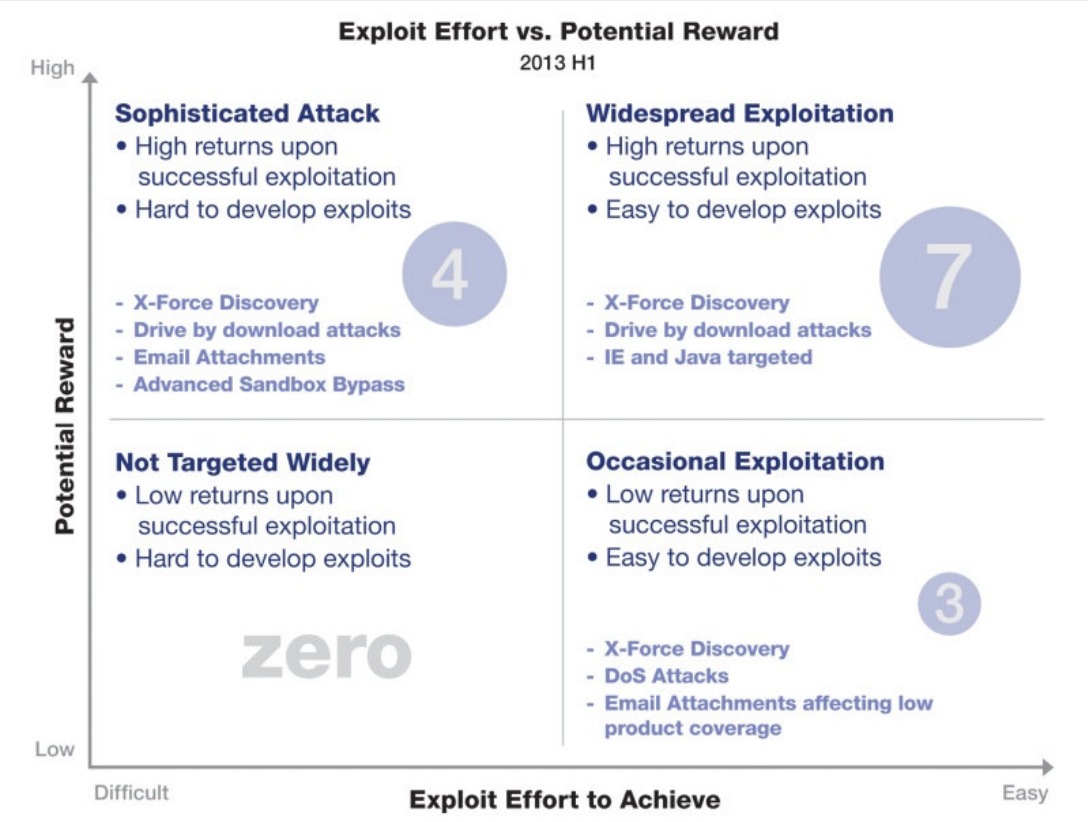
## Microsoft Internet Explorer

- 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




Source: IBM X-Force® Research and Development

**Drive-by-downloads**

IE & Java targeted

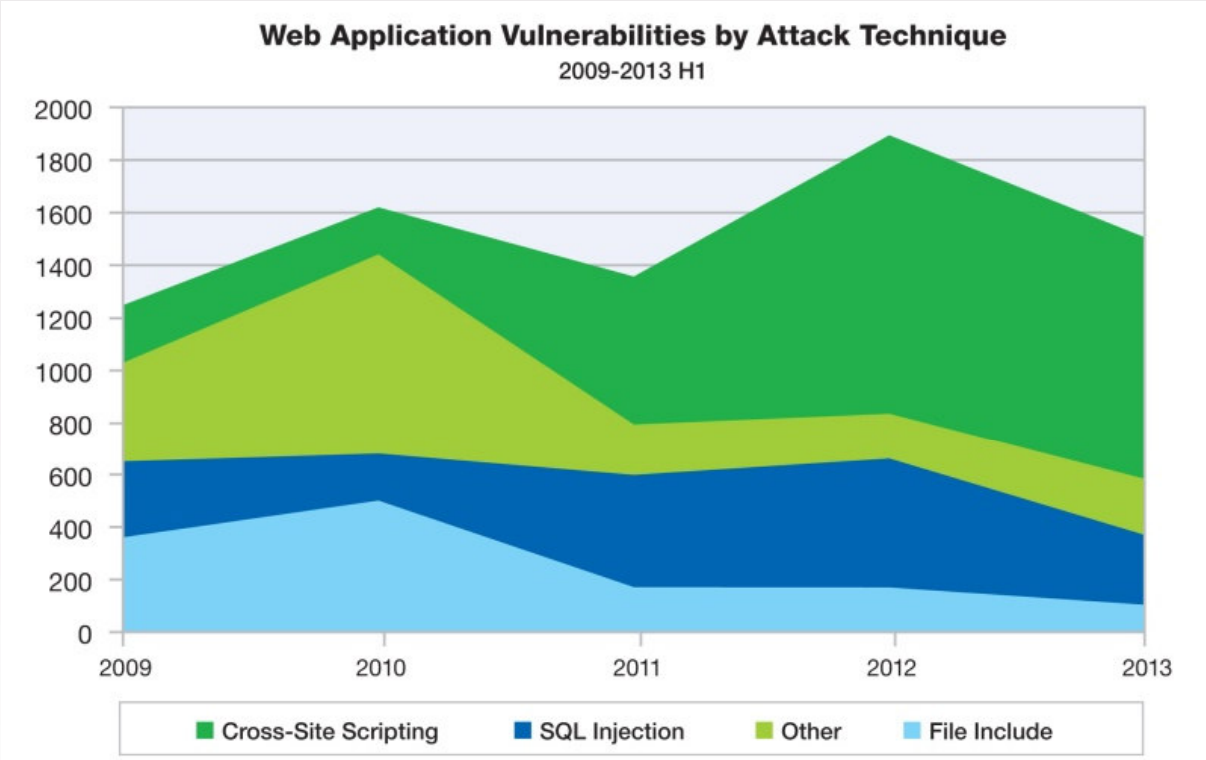
Easy exploitation with high potential reward – still the sweet spot

# Web Application Vulnerabilities

**50%**

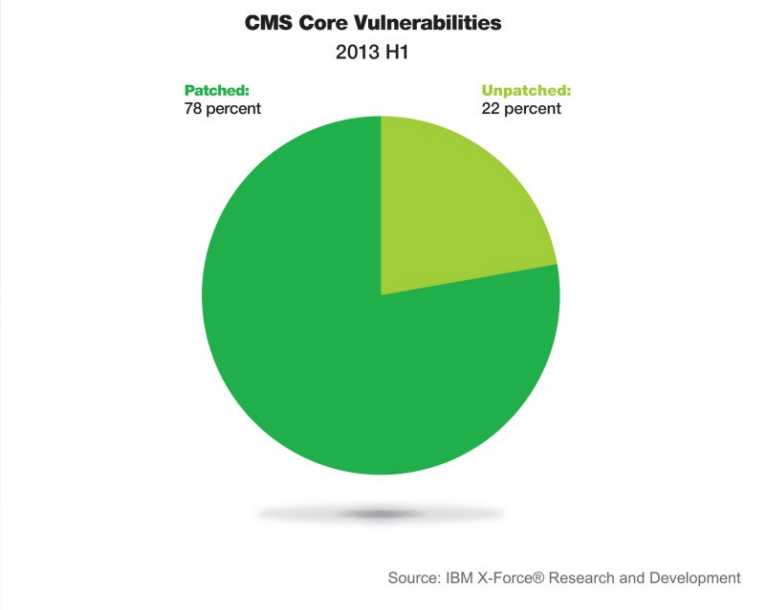
of all web application vulnerabilities are XSS

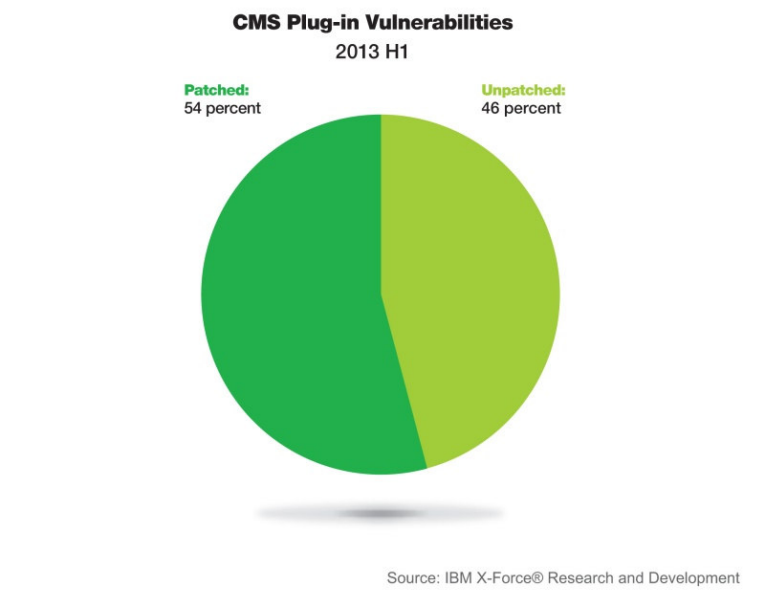
Total slightly down in comparison to 2012




Source: IBM X-Force® Research and Development

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




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

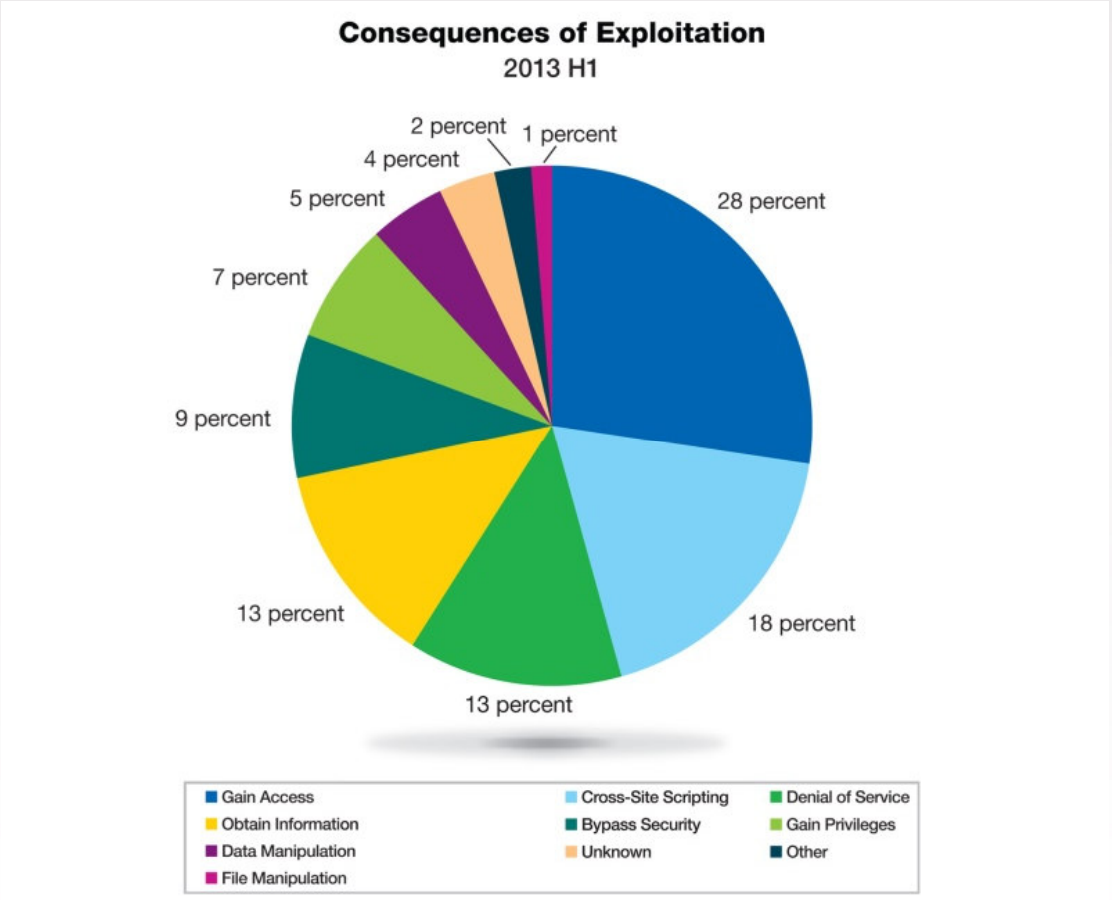
Compared to smaller organizations and individuals producing the add-ons and plug-ins

# Consequences of Exploitation

**28%**

"gain access"

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



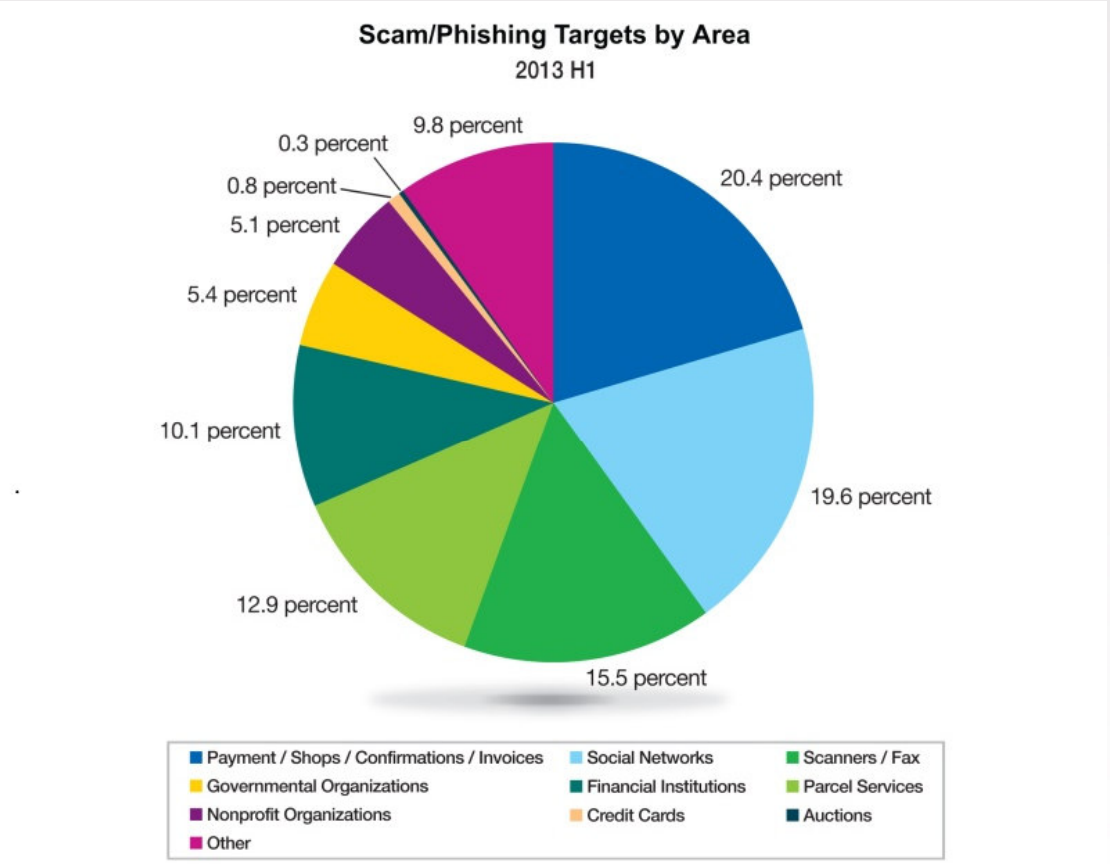

Source: IBM X-Force® Research and Development

# Scam and Phishing Targets

**55%**

bad links and attachments

- Social networks
- Payment / shops
- Scanners / Fax



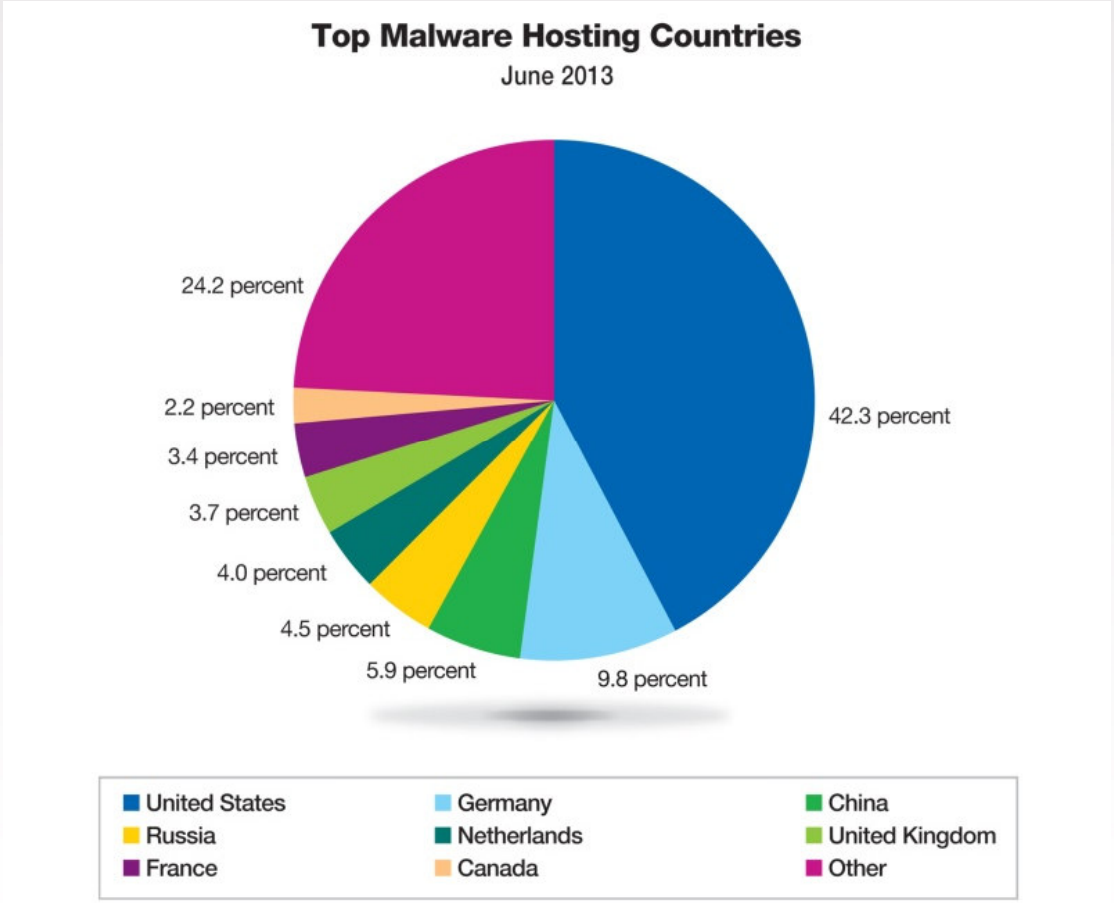

Source: IBM X-Force® Research and Development

# Malware Hosting

**42%**

malware distributed in U.S.

Germany in second at nearly 10%



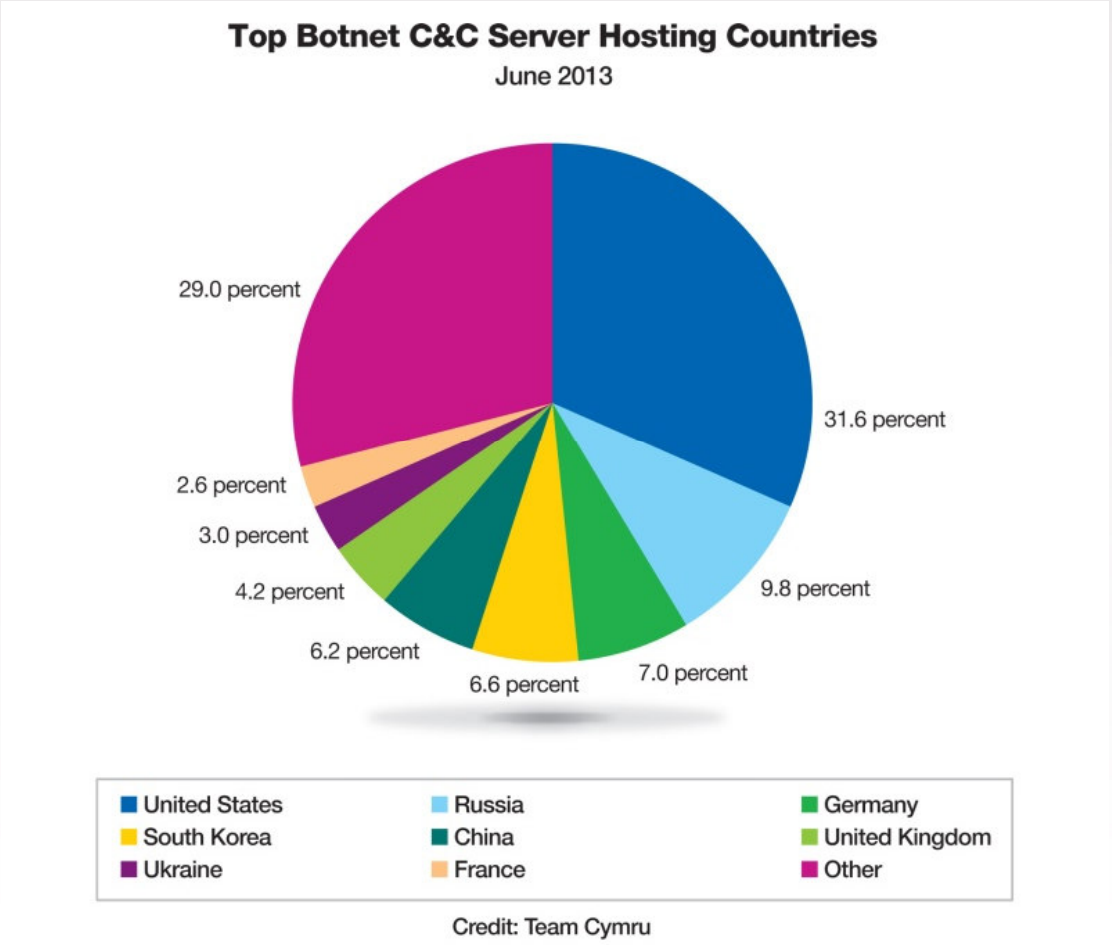

Source: IBM X-Force® Research and Development

# Botnet Command & Control Hosting

**32%**

botnet C&C servers in U.S.

Russia in second at nearly 10%




Source: IBM X-Force® Research and Development

# 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

# Get Engaged with IBM X-Force Research and Development

Follow us at @ibmsecurity and @ibmxforce

Download X-Force security trend & risk reports

http://www-03.ibm.com/security/xforce/

Subscribe to X-Force alerts at http://iss.net/rss.php or X-Force blog at http://securityintelligence.com/x-force/

## Key Seller Contacts

https://w3-connections.ibm.com/files/app?lang=en#/file/9aba0a2b-8e16-4be9-b666-7130a952db73

Robert Freeman, Manager XF Advanced Security Research

rgfreem@us.ibm.com

Leslie Horacek,

XF Threat Response

HORACEK@be.ibm.com

Doron Shiloach,

XF Product Manager

doron@us.ibm.com

Michael Hamelin,

XF Security Architect

michael.hamelin@us.ibm.com

Kevin Skapinetz, Program Director Product Strategy

kskap@us.ibm.com

Mattias Johansson

Sr. Operations Manager

mjohansson@us.ibm.com

Jason Brewer, Manager XF Development

jcbrewer@us.ibm.com

Steve Seidenberg,

Manager XF Security Content

sseidenb@us.ibm.com

Ted Bannon, Manager XF Quality Assurance

tbannon@us.ibm.com

Brad Sherrill, Manager XF Data Intelligence

bsherrill@us.ibm.com

Ralf Iffert ,

Mgr, XF Content Security

ralf.iffert@de.ibm.com

Carsten Dietrich, Product Line Mgr, Content Security

Carsten.Dietrich@de.ibm.com

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**