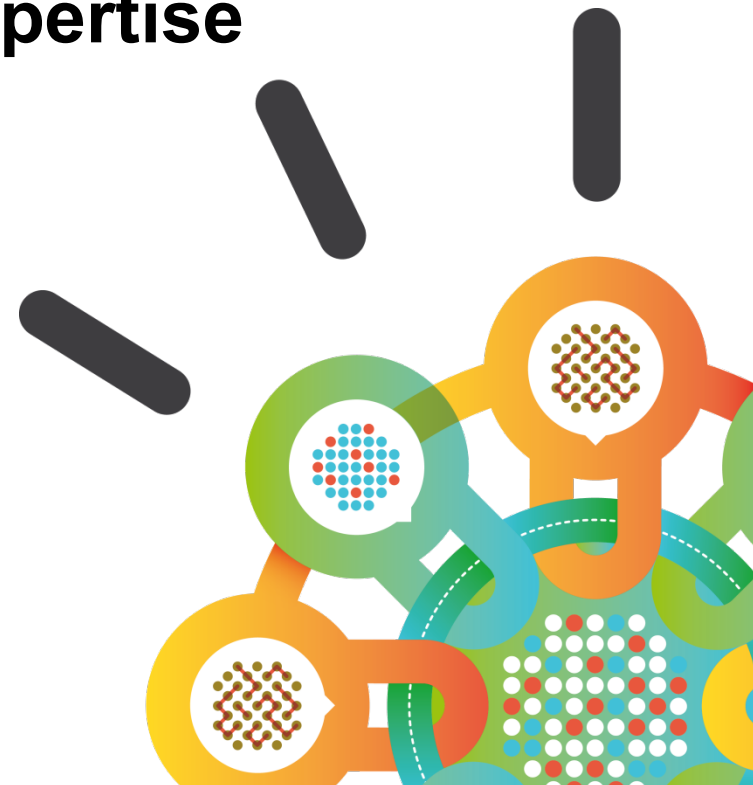
Security Intelligence.
Think Integrated.

IBM Security

Intelligence, Integration and Expertise



IBM Security Systems
November 2013

Agenda

- **Welcome and Introductions**
- Latest Security trends and H1 2013 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent Threats
- Break
- From Identity & Access Management to Identity Intelligence
- Managing Application Security
- Data Security

Agenda

- Welcome and Introductions
- **Latest Security trends and H1 2013 X-Force Report**
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent Threats
- Break
- From Identity & Access Management to Identity Intelligence
- Managing Application Security
- Data Security

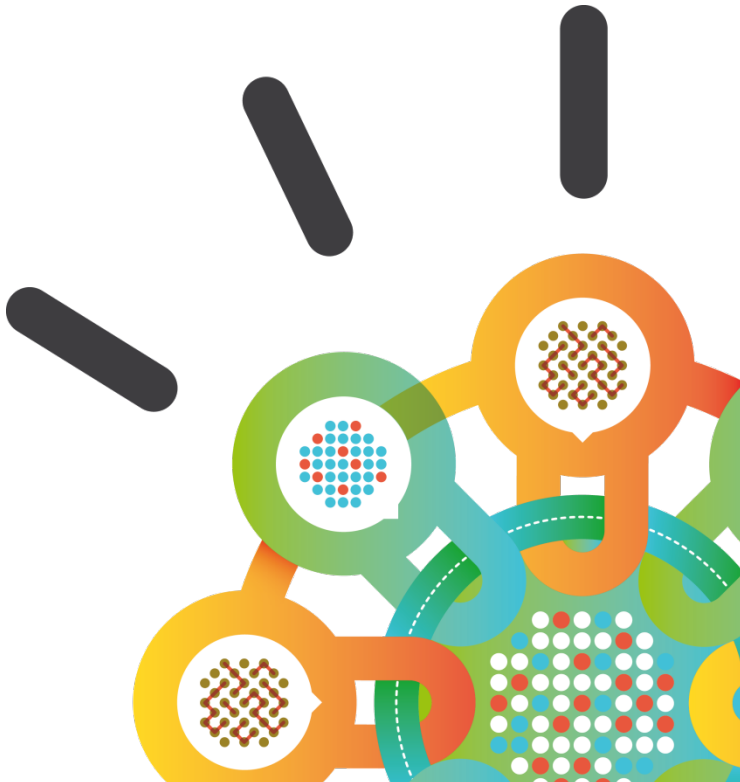
Security Intelligence.
Think Integrated.

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

Greg Sinclair, CISSP, PMP

Associate Practice Leader, IBM Security Services

gregorys@za.ibm.com



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

76K 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

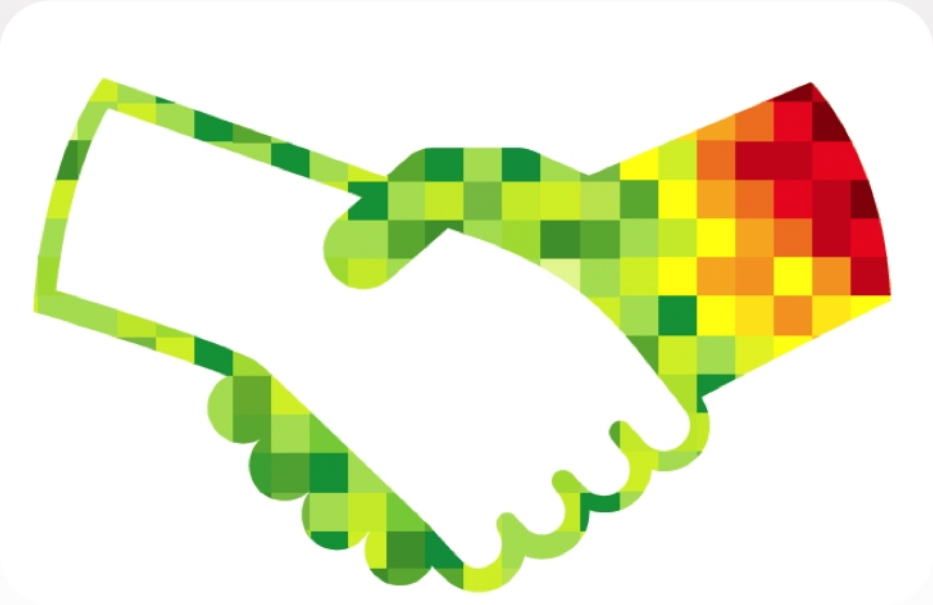
Social and Mobile

X-Force by the Numbers

Exploiting Trust

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

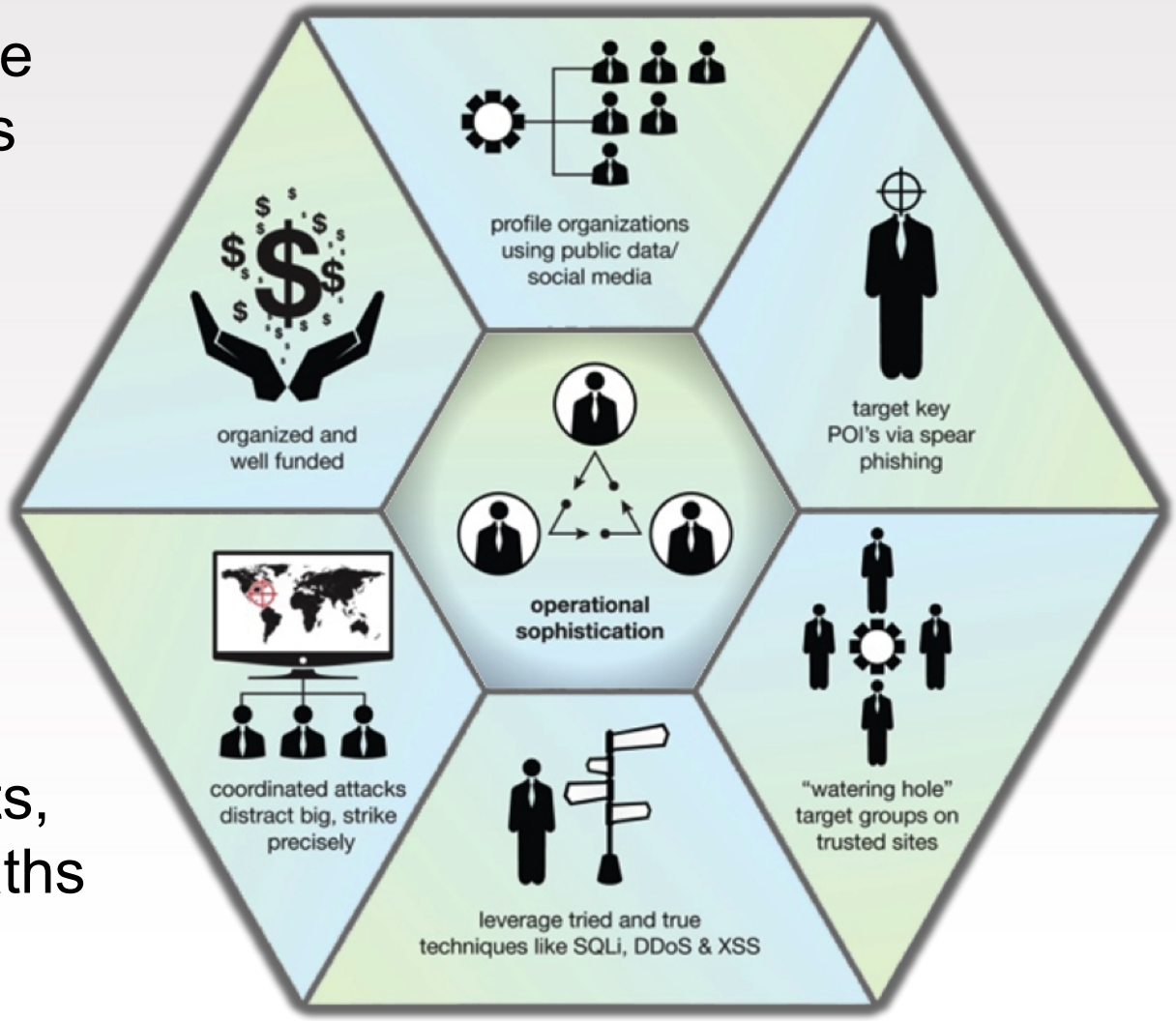
- Breach an organization
- Target groups of users
- Create methods of diversion



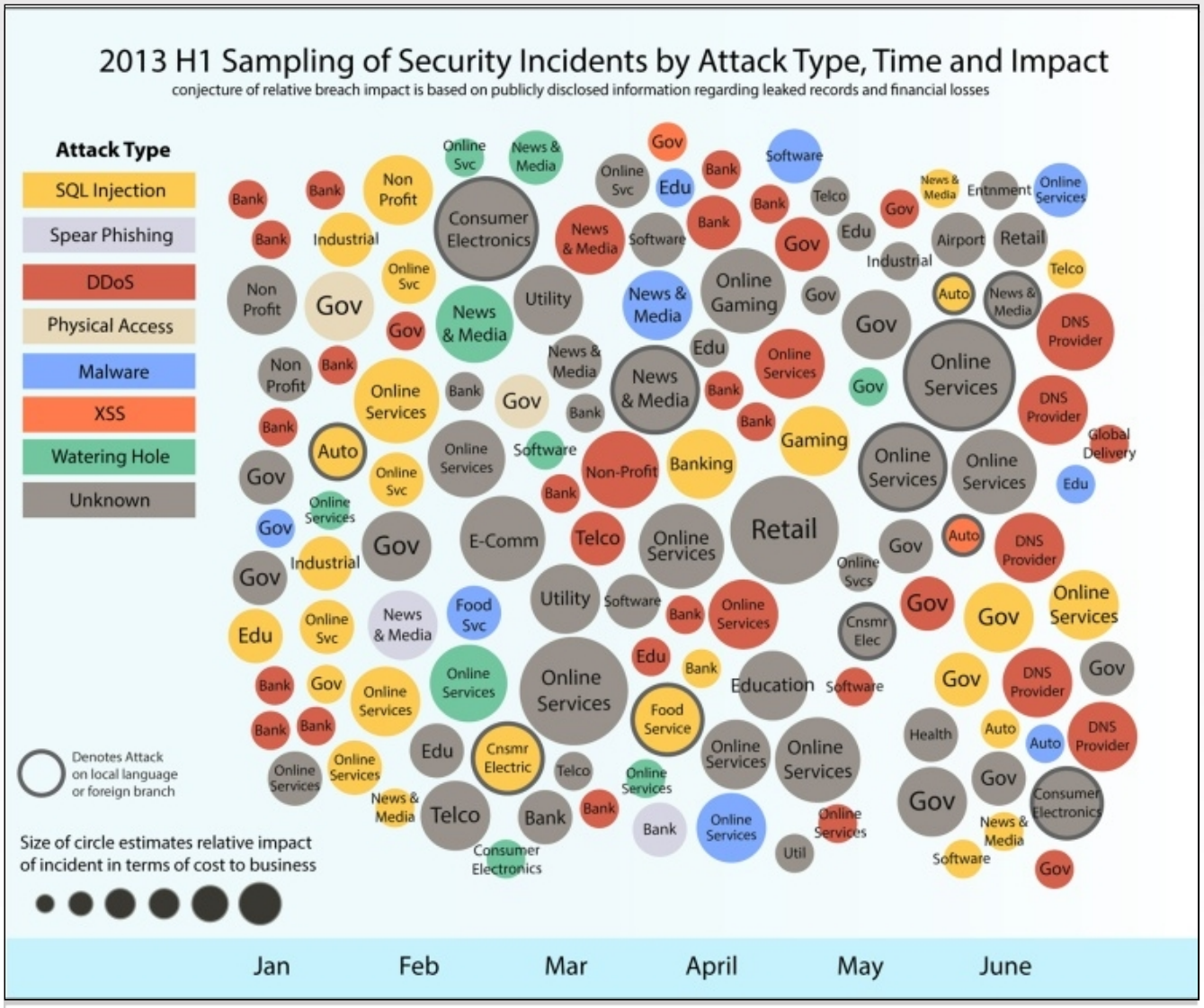
Operational sophistication

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

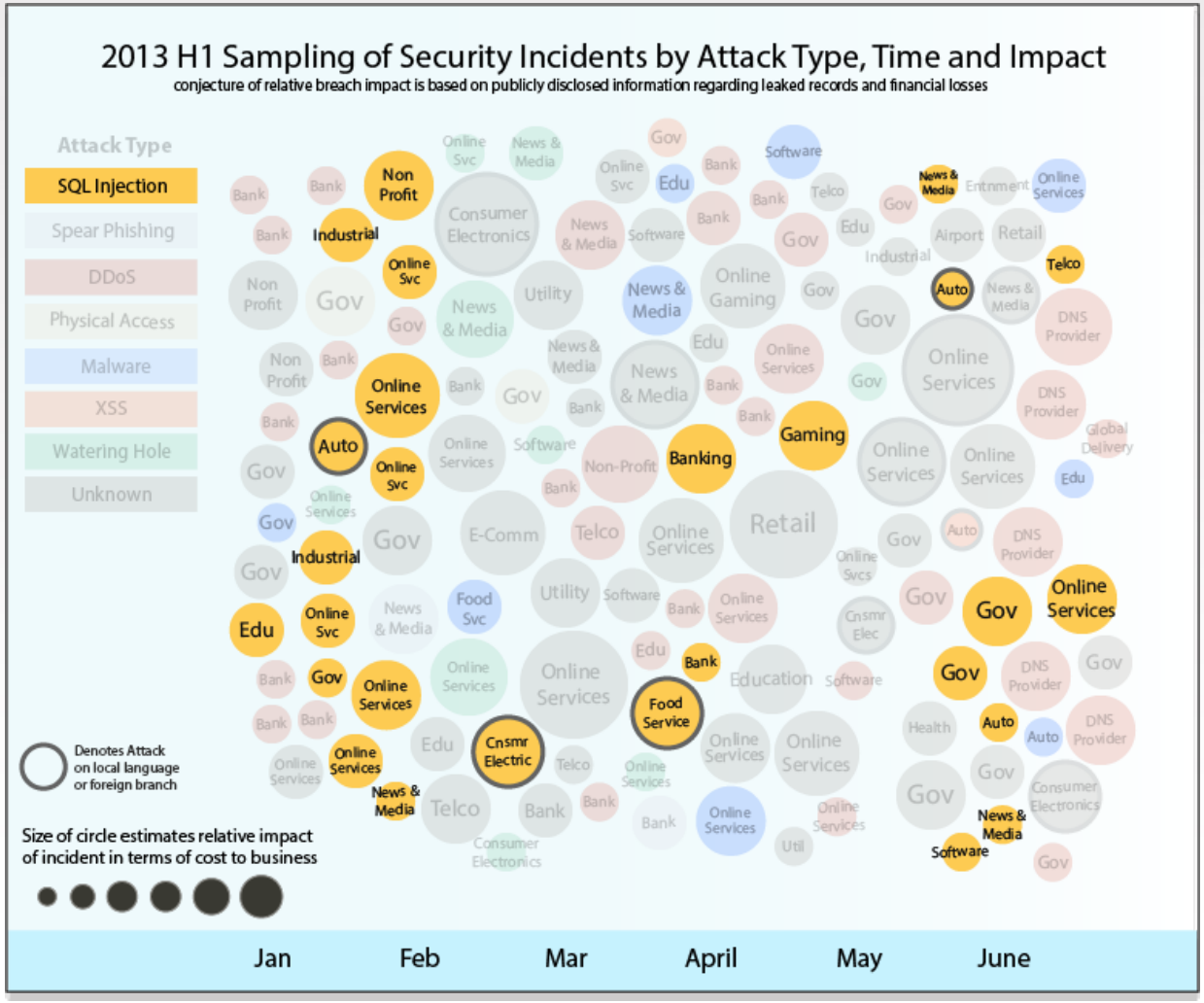


Security Incidents in the first half of 2013



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

Recent local example of SQL Injection

sqlmap

Automatic SQL injection and database takeover tool

Introduction

sqlmap is an open source penetration testing tool t
SQL injection flaws and taking over of database ser
niche features for the ultimate penetration tester a
fingerprinting, over data fetching from the database,
commands on the operating system via out-of-band

Features

- Full support for **MySQL, Oracle, PostgreSQL, M**
SQLite, Firebird, Sybase and SAP MaxDB databa

PASTEBIN | #1 paste tool since 2002

PASTEBIN Follow @pastebin Like 51k

create new paste trending pastes

Pastebin launched a little side project called HostCabi.net, check it out ;-)

www.gov.za

BY: A GUEST ON JUL 11TH, 2013 | SYNTAX: NONE | SIZE: 1.95 KB | HITS: 148 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

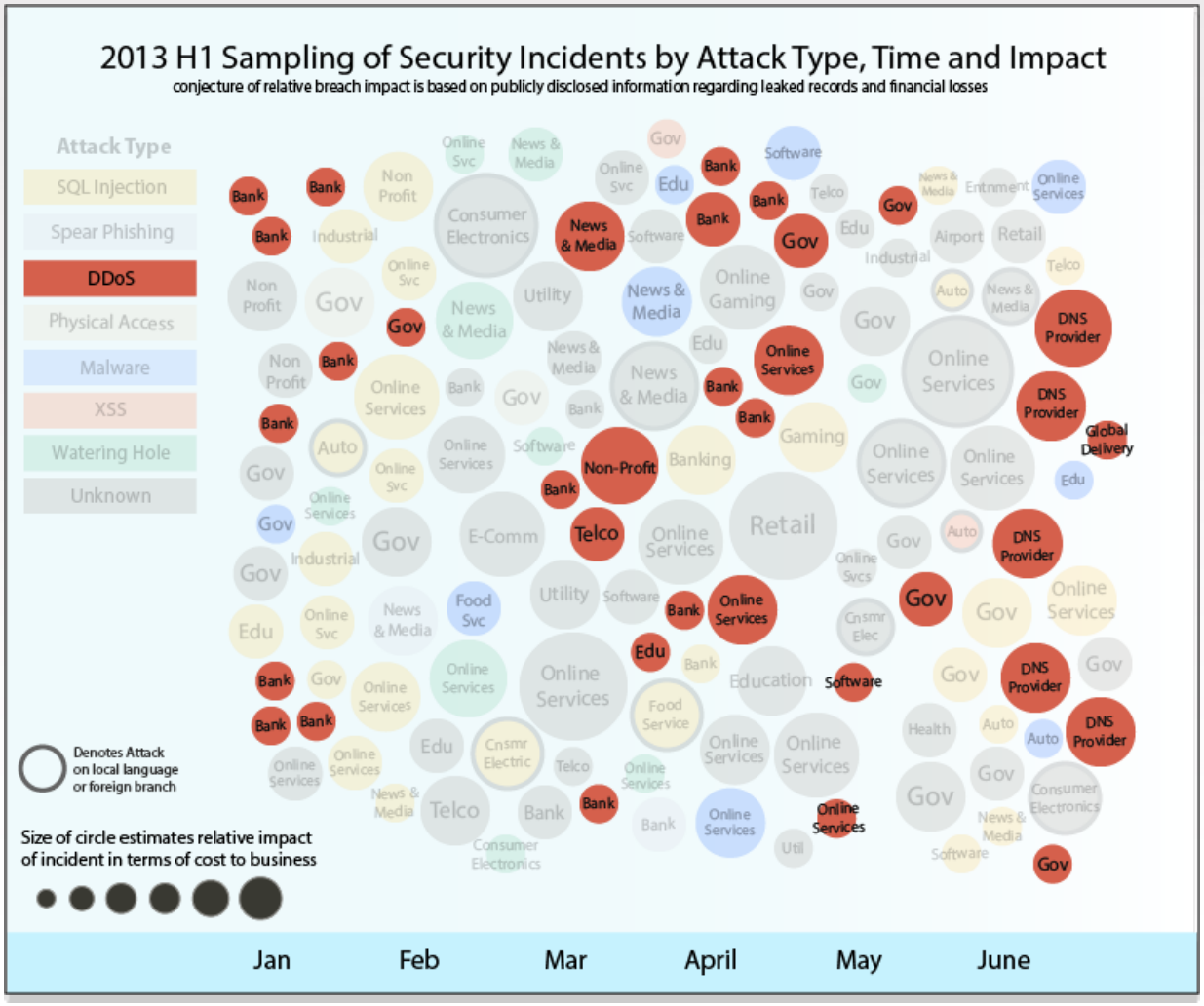
0 4


```
1.  Greetz Netizens,
2.
3.          Today's yums is www.gov.za ... yup South Africa's .gov.  The server is an Oracle db on the internal
    network, yeah got most of the creds but can't get internal access:( too bad cause user: ADMIN1 with pass: ADMIN1
    with ADMIN privs.  lol oh well, did "map" most of the db.
4.
5.          For those interested here is the inj point: http://www.[redacted]and here
    is the sqlmap params I used:
6.
7.  sqlmap -u http://www.i[redacted]-dbms=oracle --random-agent --risk=3 --level=5 -o
    --eta --threads=10  --technique=beu --text-only --no-cast --drop-set-cookie --batch
8.
9.
10.         Technique might as well just be 'b' since it's only blind injectable and minus the options of
    --dbms,--text-only,and drop-set-cookie ,these are what I normally set.  Of course with --dbs --passwords --tables
    . http://www.sqlmap.org for further info.
11.
```

Source: IBM Security Services - Mr. D. Boshoff

DDoS Attacks

continue to disrupt businesses



High traffic volume as much as

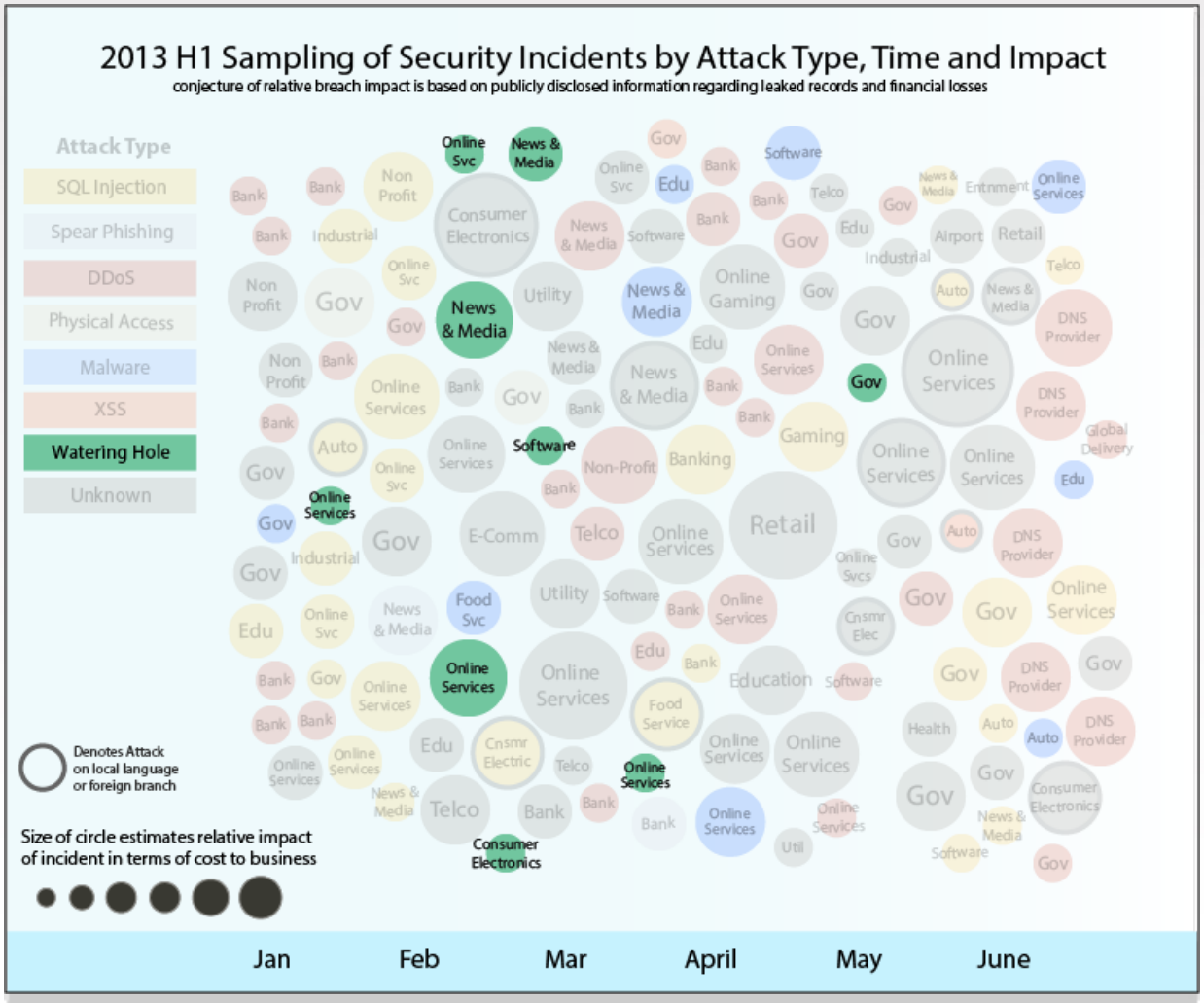
300Gbps

Industries affected:

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

"Watering Hole"

attacks compromise end user trust



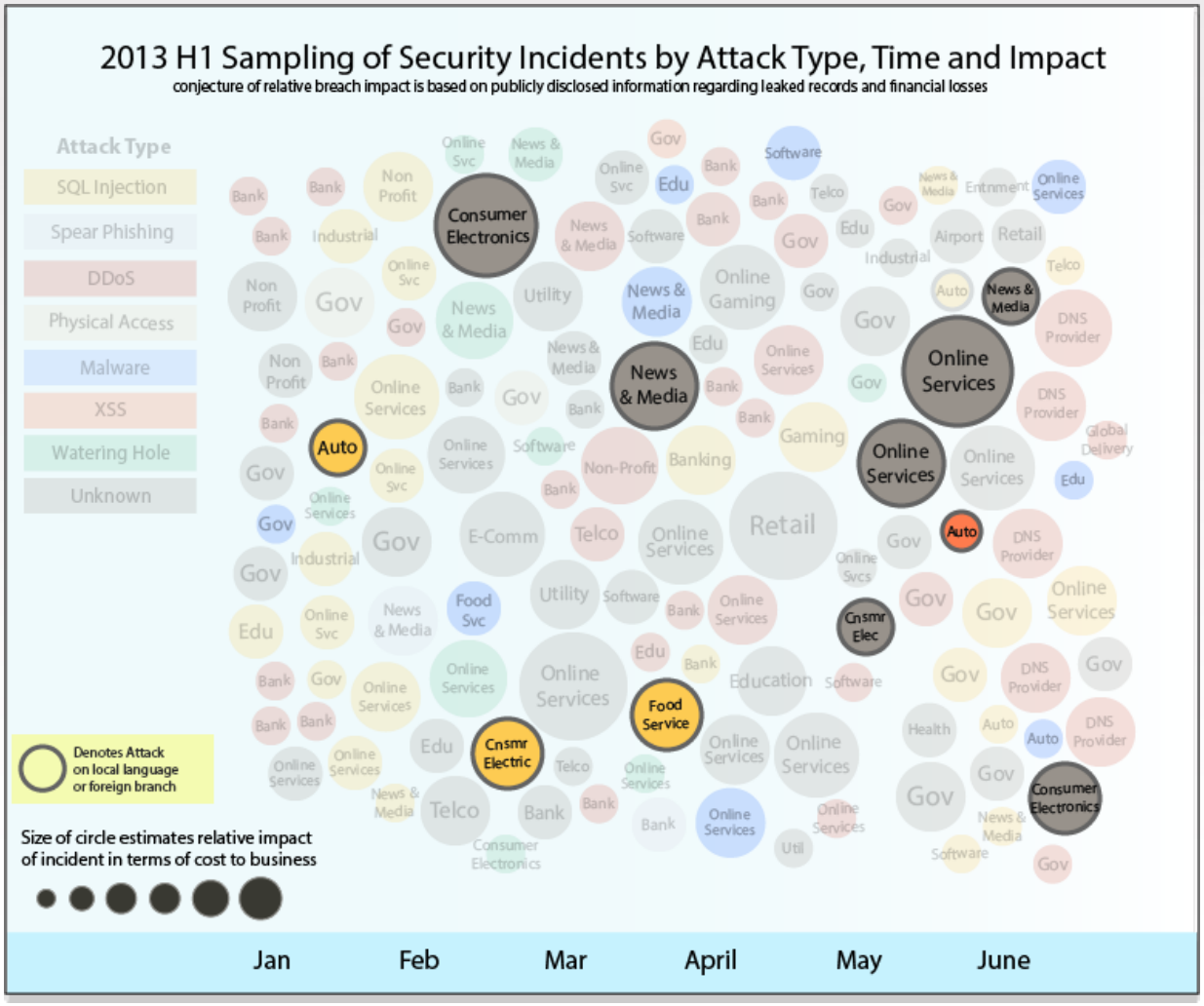
Tainting legitimate sites with zero-day exploits

Targeting Savvy Users

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

Disenfranchised

foreign branch or local language sites tarnish brands



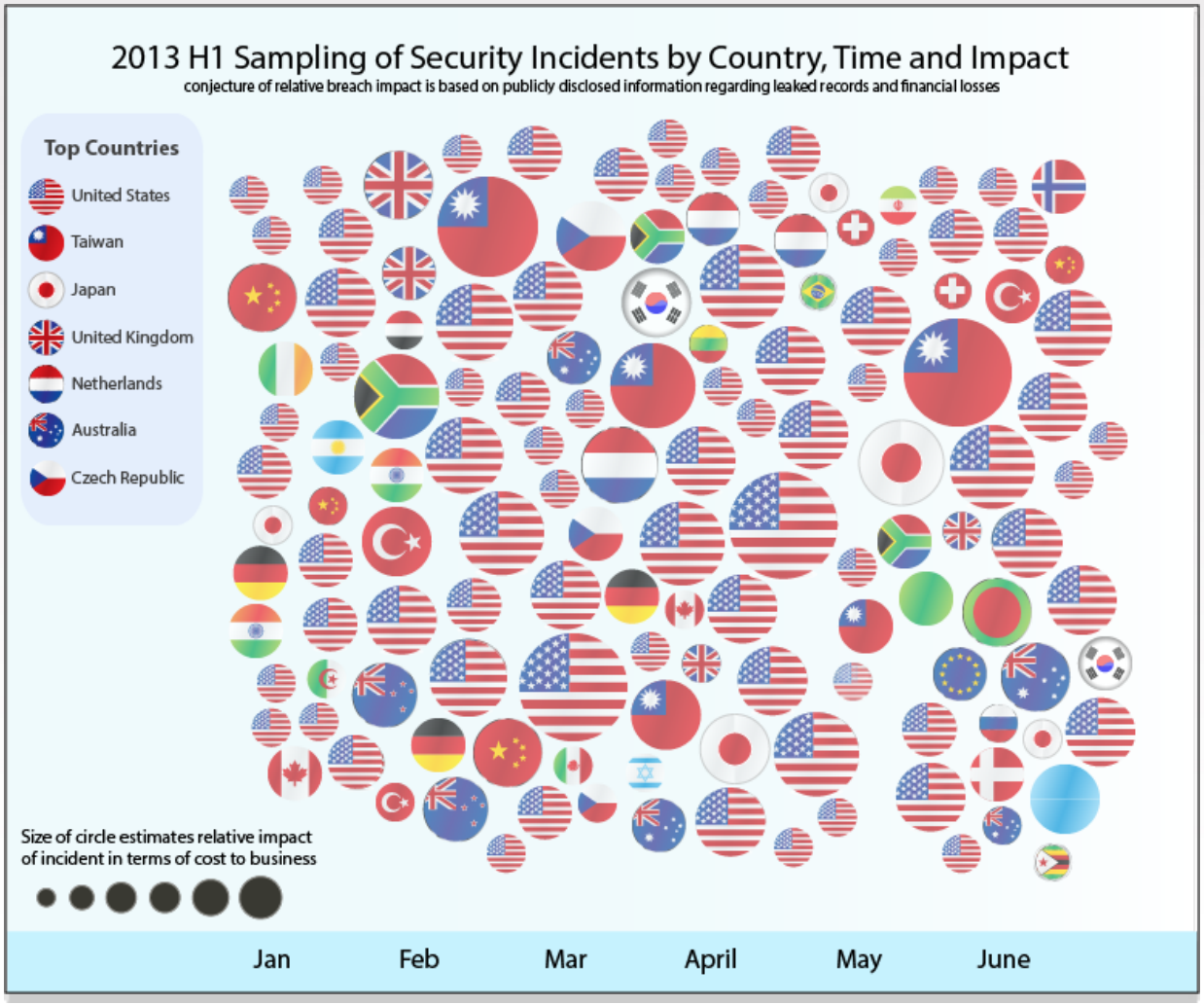
Global brands targeted in foreign countries outside of home office

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

January 29, 2013 – Ghostshell "Project Sunrise"

PASTEBIN | #1 paste tool since 2002

PASTEBIN Follow @pastebin Like 51k

create new paste trending pastes

Pastebin launched a little side project called HostCabi.net, check it out ;-)

#ProjectSunRise - Africa's heart

BY: TEAMGHOSTSHELL ON JAN 28TH, 2013 | SYNTAX: NONE | SIZE: 32.75 KB | HITS: 8,138 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

75 190


```
1.   _  _  _____          _          _   _____          _____ _
2.  _| || |_| ___ \        (_)        | | /  ___|         | ___ (_)
3. |_  __  _| |_/ / __ ___  _  ___  ___| |_\ `--. _   _ _ __ | |_/ /_ ___  ___
4.  _| || |_|  __/ '__/ _ \| |/ _ \/ __| __|`--. \ | | | '_ \|    /| / __|/ _ \
5. |_  __  _| |  | | | (_) | |  __/ (__| |_/\__/ / |_| | | | | |\ \| \__ \  __/
6.   |_||_| \_|  |_|  \___/| |\___|\___|\__\____/ \__,_|_| |_\_| \_|_|___/\___|
7.                        _/ |
8.                       |__/
9.
10.
11. Venturing into the cyber
    something that the rest o
    for the time being, South
    Kenya and Angola.
```

After two months of investigations, Team GhostShell has finally managed to fingerprint the entire top business infrastructure of South Africa, tracing some of it's activities to other countries across the continent. As always, we will provide you with a glimpse of that world, so that everyone else can do their own research and draw their own conclusions from it. Although this time around, the goal was not to release a large portion of data, we will still provide you with enough non-disclosure accounts and records from a variety of businesses; corporations and governments.

The point of it is to find and see for yourselves the connections these entities have with one another, how they conduct themselves on the financial playing field but also economically speaking, how they actually do business world-wide. The data here ranges from government, banking, mining, petroleum, management, networking, transport services, construction, education/academics, other enterprises.

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

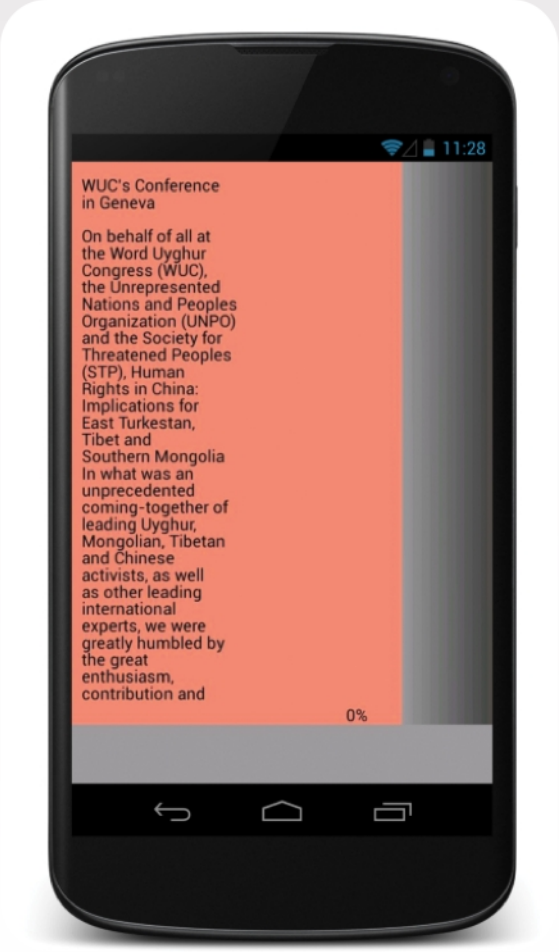
Very targeted attack

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

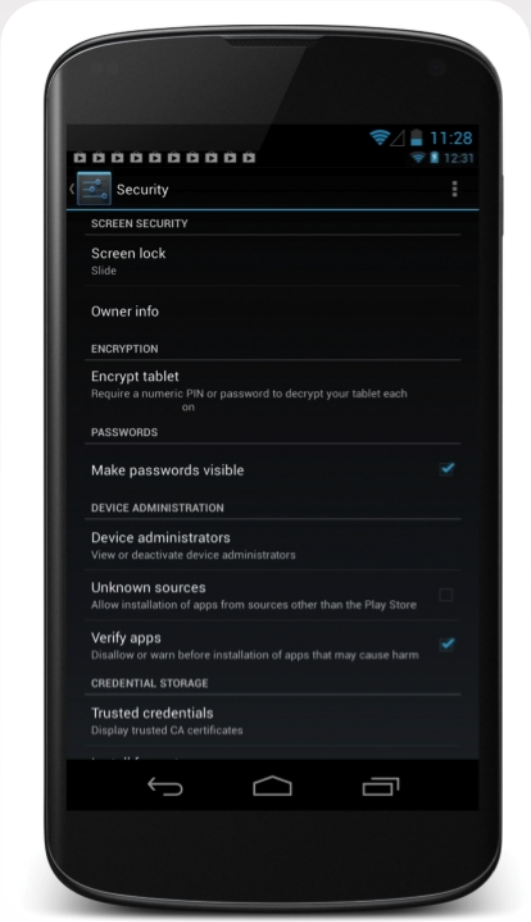
Obad

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

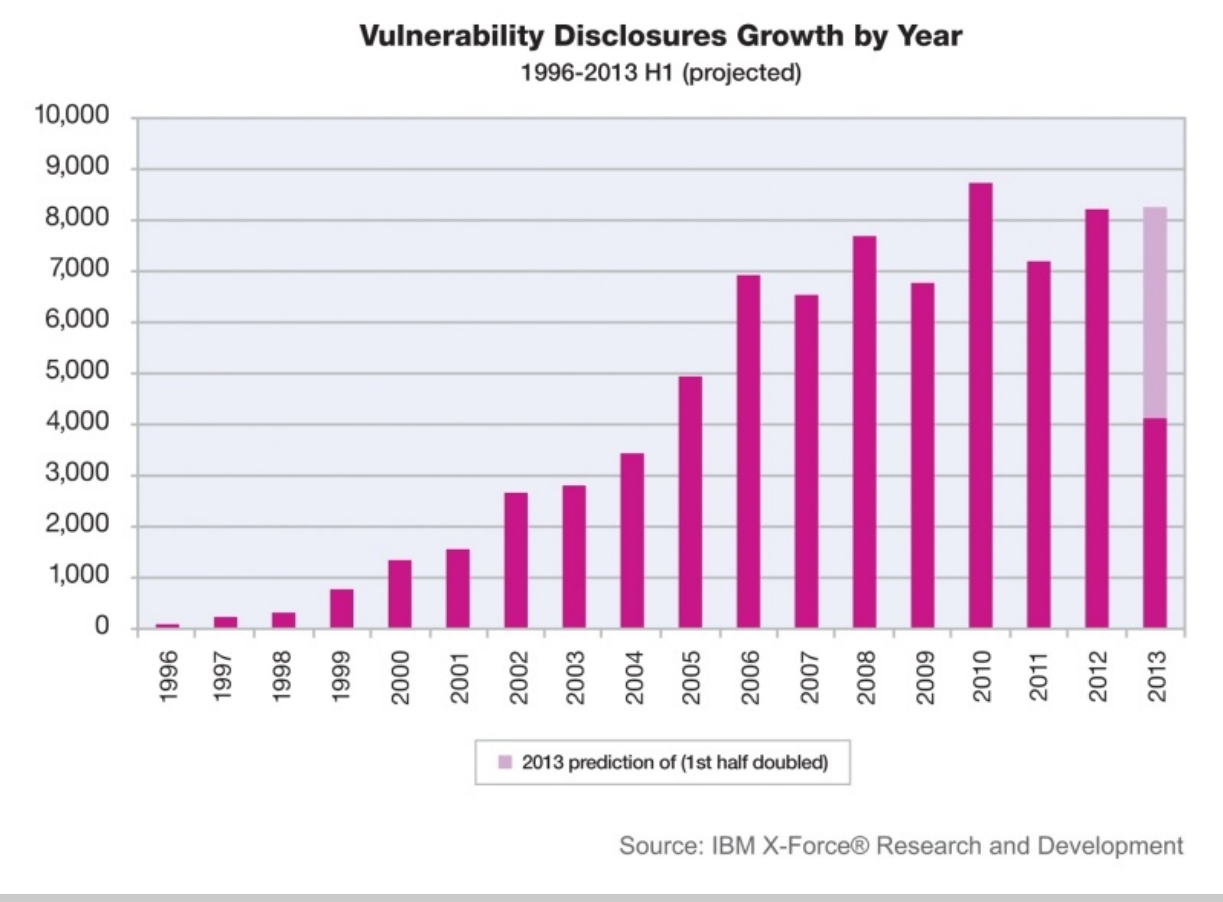
- Vulnerabilities
- Exploits
- Web trends
- Spam and Phishing

Vulnerabilities Disclosures

4,100

publicly disclosed vulnerabilities

If trend continues, roughly same as 2012

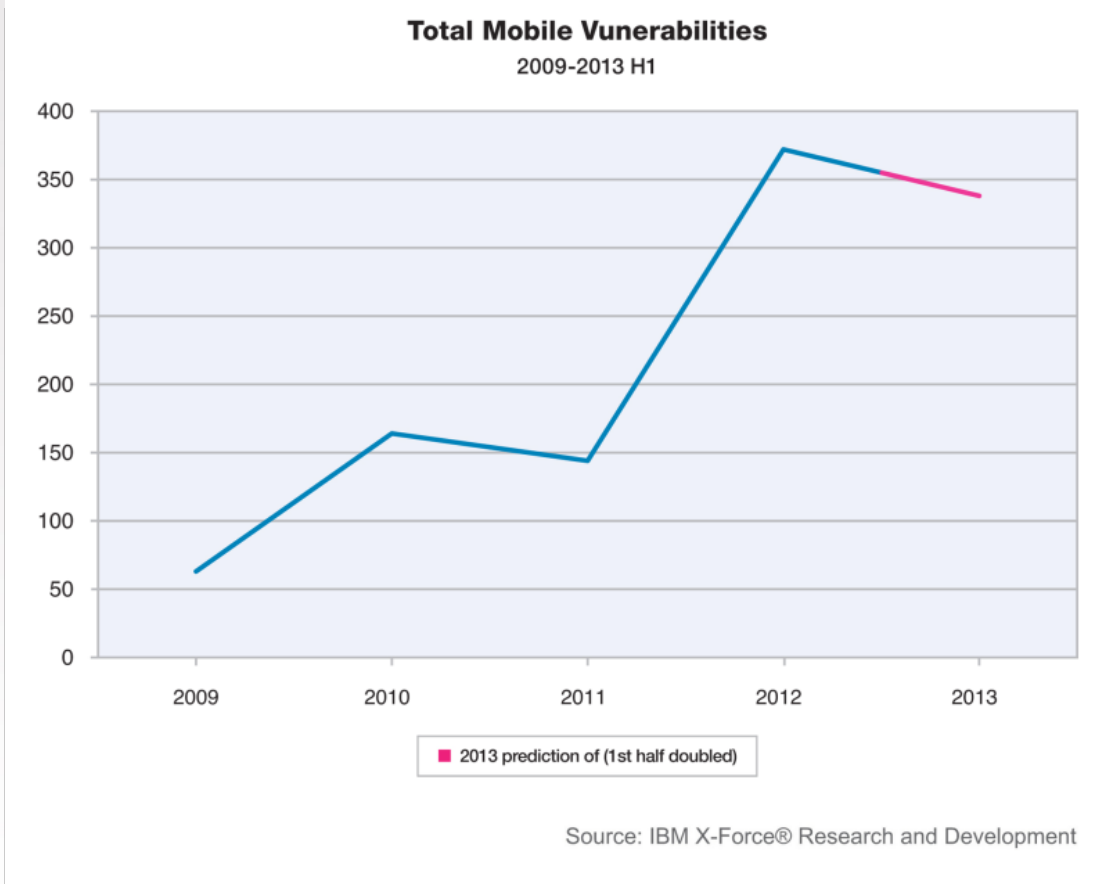


Vulnerabilities affecting Mobile Software

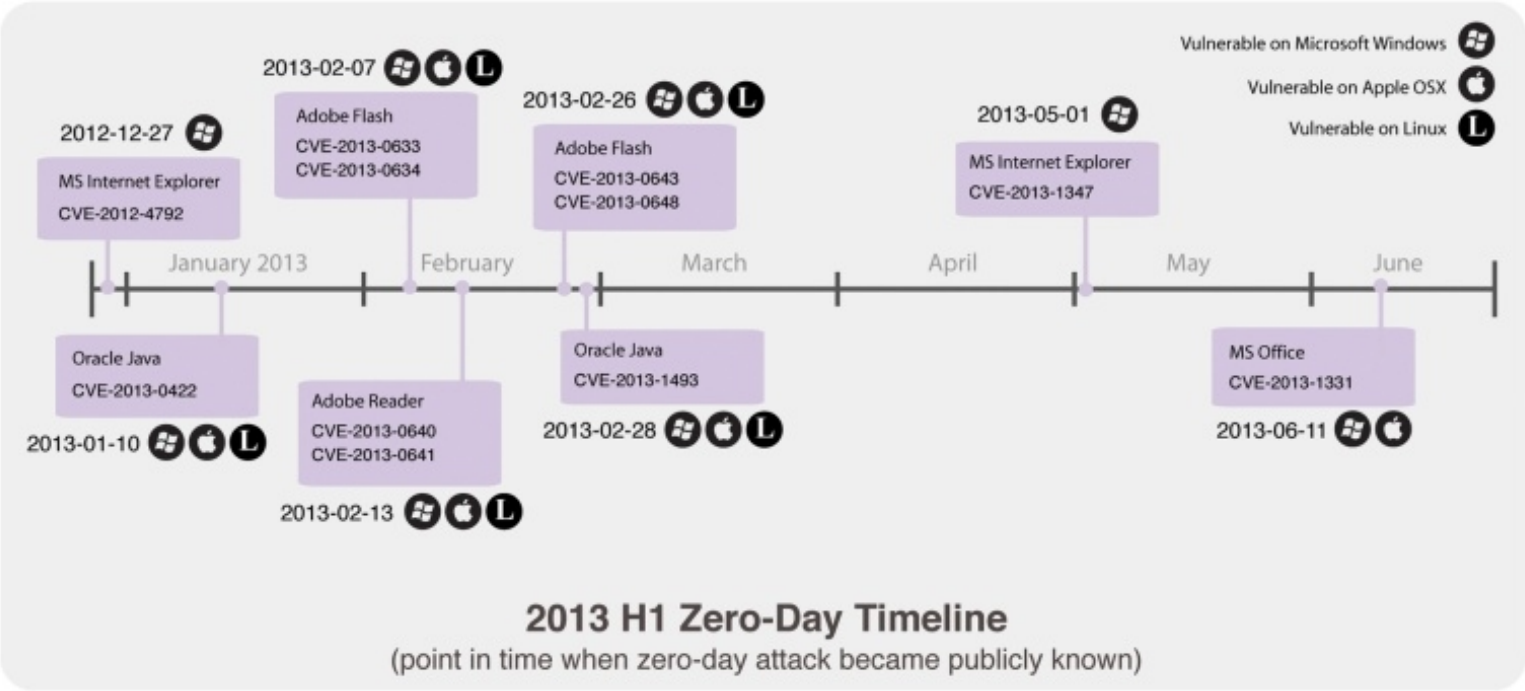
Mobile vulnerabilities have increased since 2009

Although still small percentage of total overall

Affecting both mobile and desktop software



Zero-Day Vulnerabilities

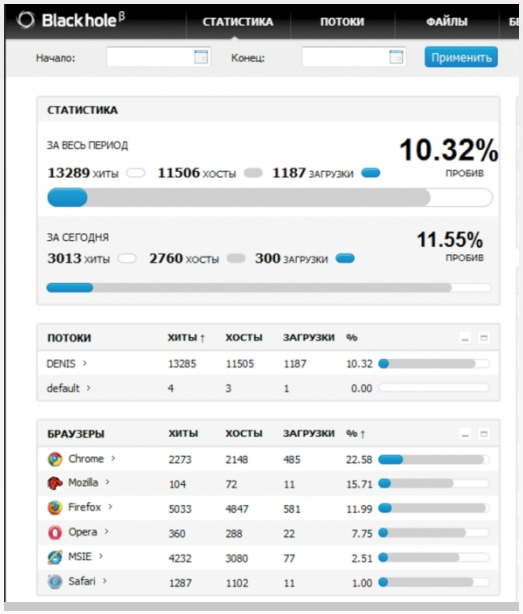


2013 H1 Zero-Day Timeline
(point in time when zero-day attack became publicly known)

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

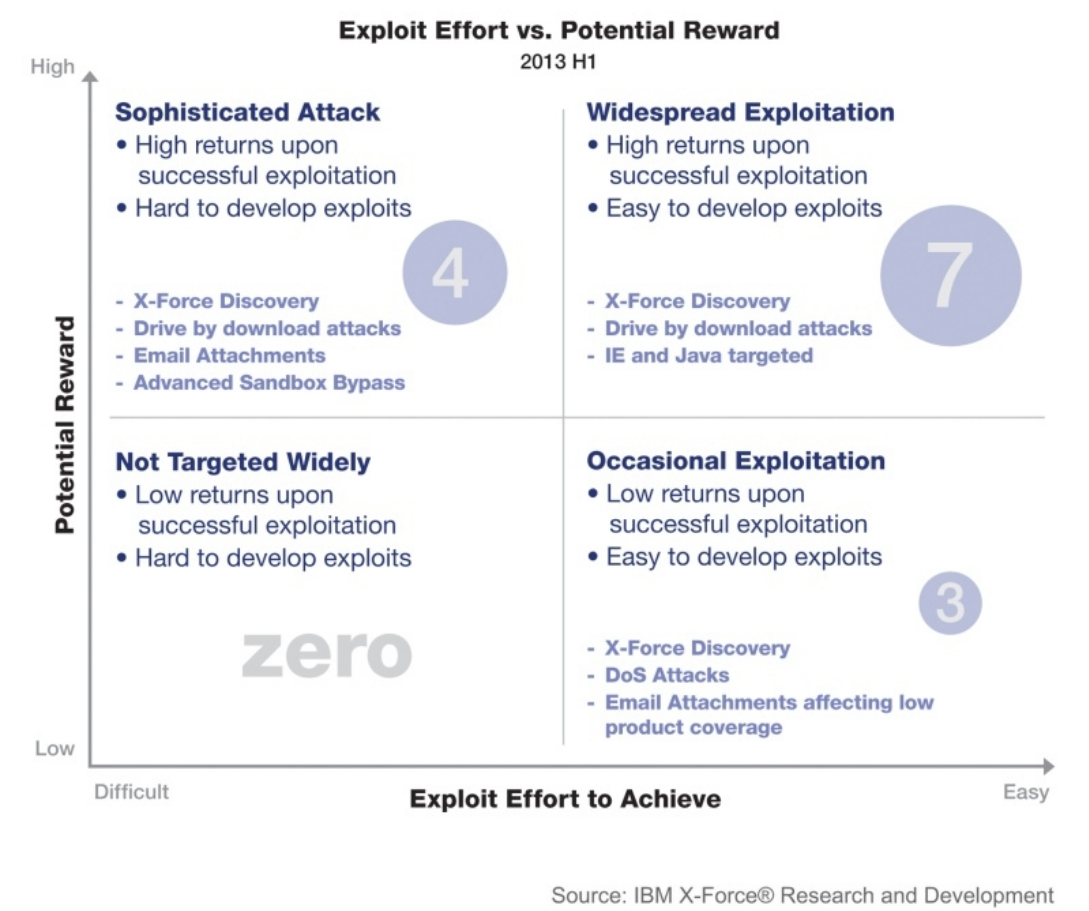
Microsoft Internet Explorer

- 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



Drive-by-downloads

IE & Java targeted

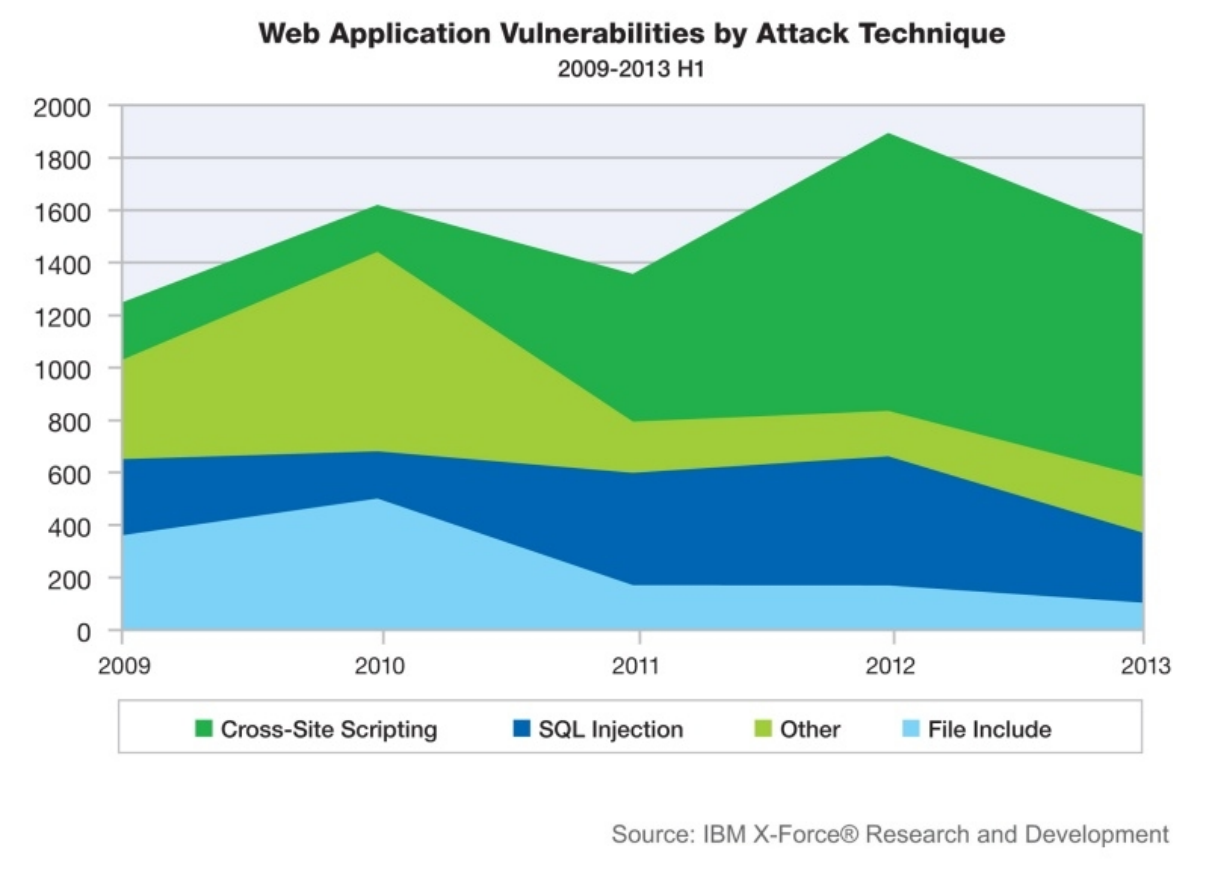
Easy exploitation with high potential reward – still the sweet spot

Web Application Vulnerabilities

50%

of all web application vulnerabilities are XSS

Total slightly down in comparison to 2012

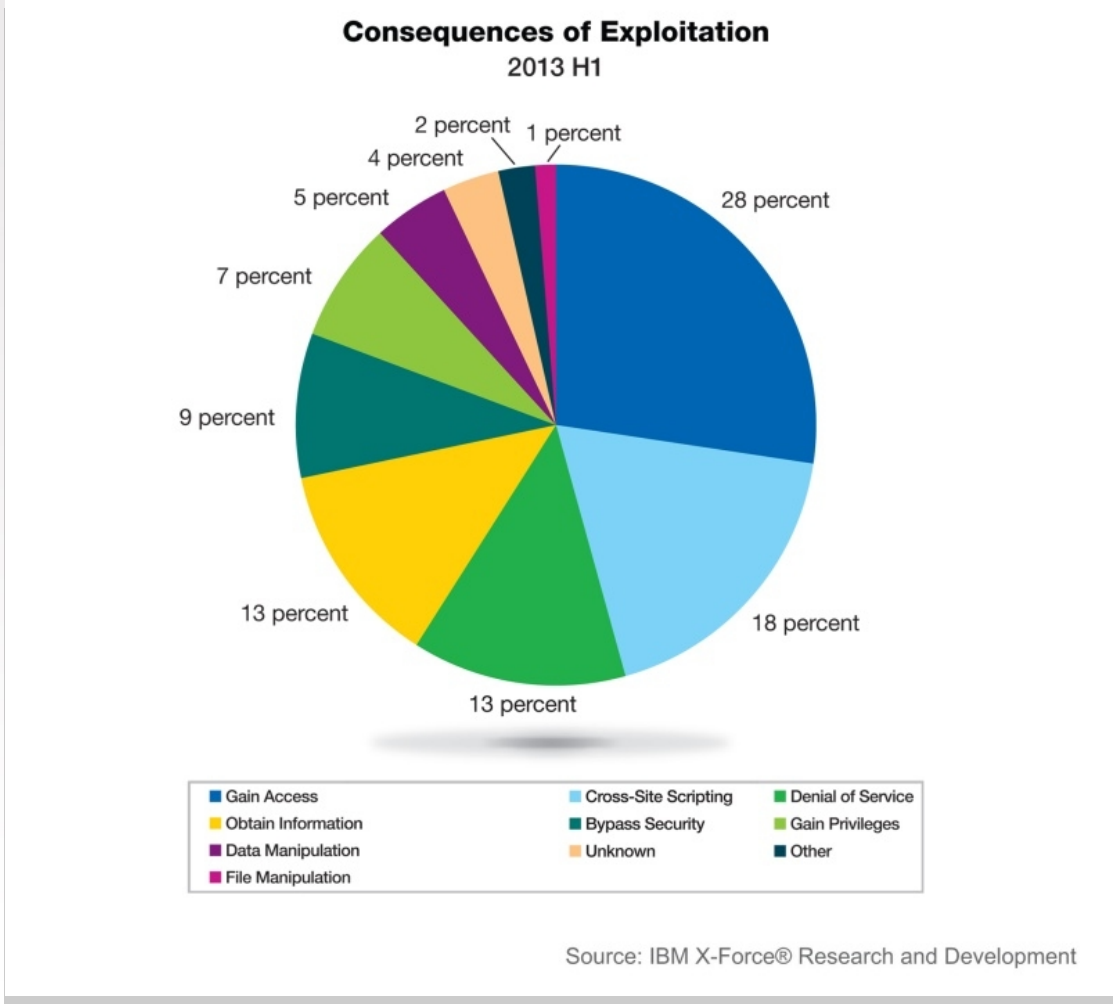


Consequences of Exploitation

28%

"gain access"

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

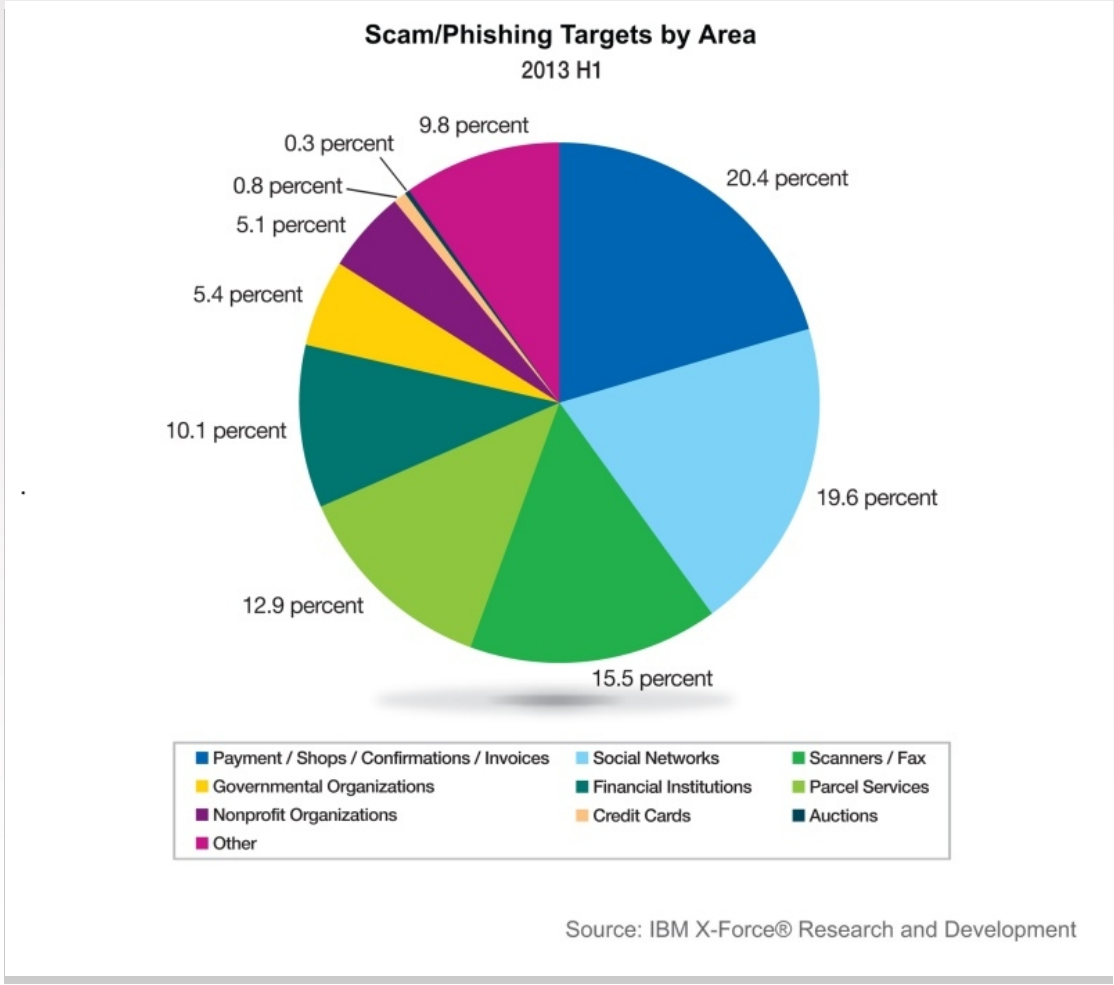


Scam and Phishing Targets

55%

bad links and attachments

- Social networks
- Payment / shops
- Scanners / Fax

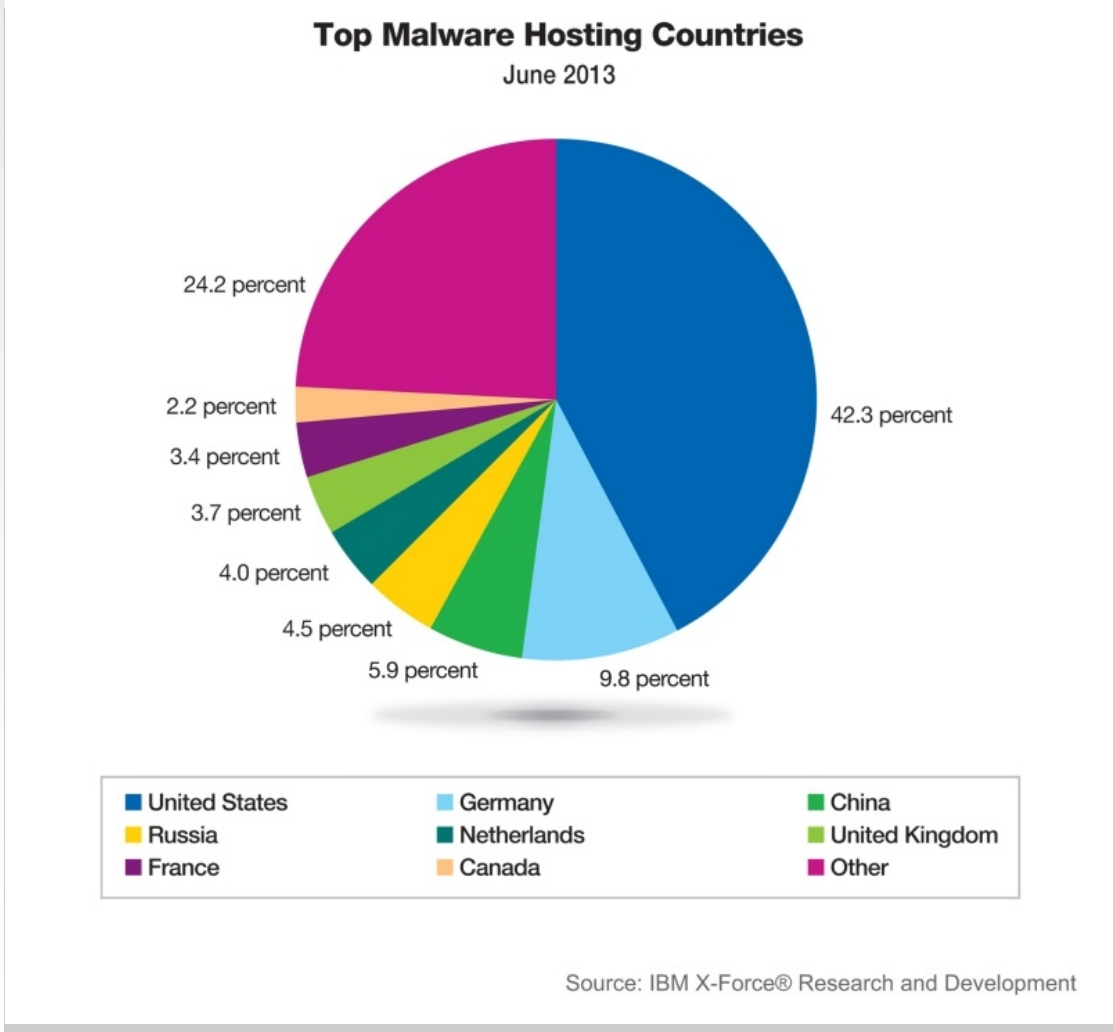


Malware Hosting

42%

malware distributed in U.S.

Germany in second at nearly 10%

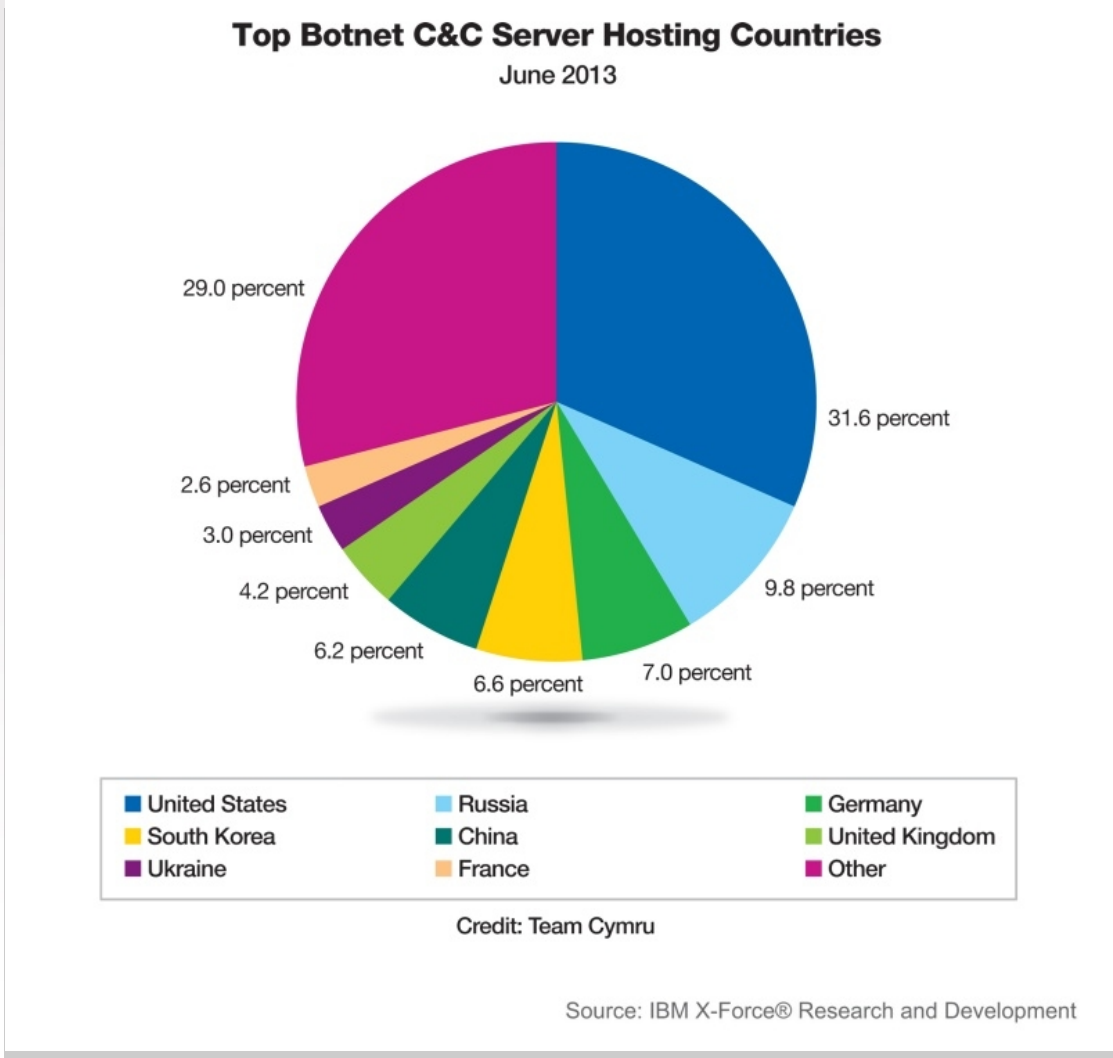


Botnet Command & Control Hosting

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

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/

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

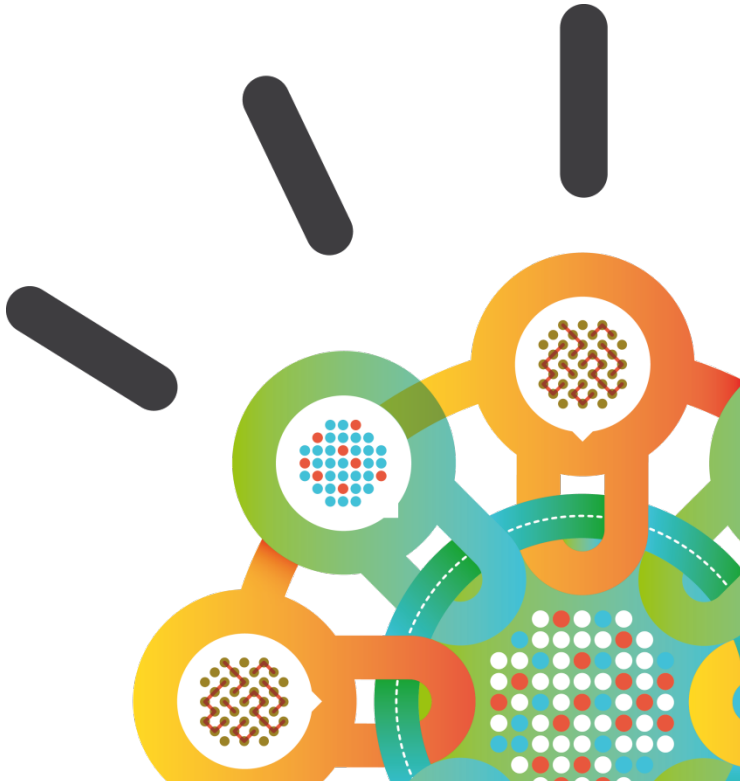
Agenda

- Welcome and Introductions
- Latest Security trends and H1 2013 X-Force Report
- **Security Intelligence - Understanding your Organizational Security Posture**
- Holistic approach to handling Advanced Persistent Threats
- Break
- From Identity & Access Management to Identity Intelligence
- Managing Application Security
- Data Security

IBM

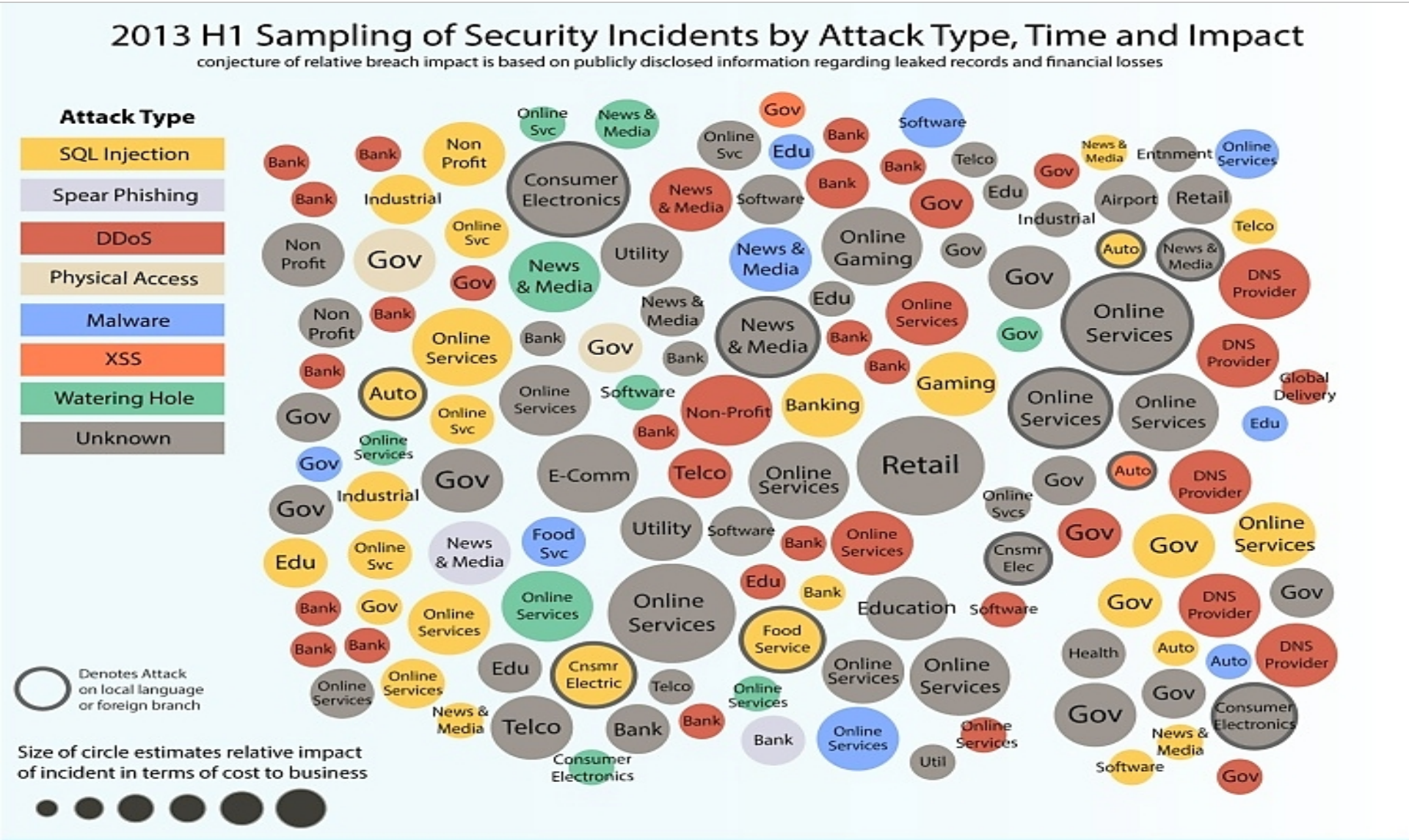
Security Intelligence.
Think Integrated.

Security Intelligence – Understanding your Organizational Security Posture



Nov 2013

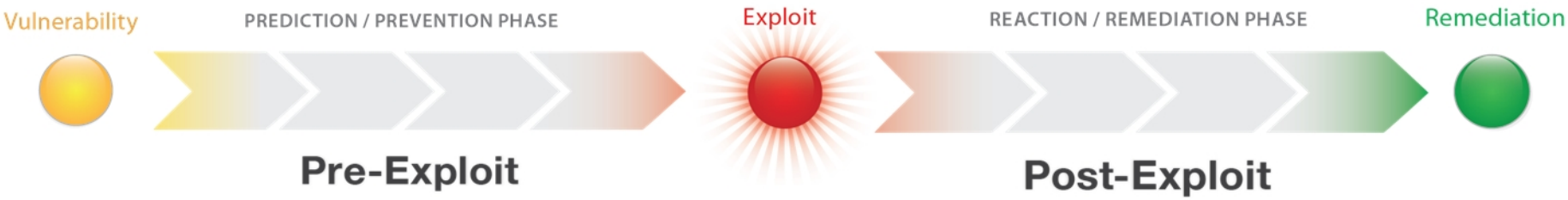
All breaches start with some form of vulnerability



Solving Customer Challenges

Major Electric Utility	Detecting threats	• Discovered 500 hosts with “Here You Have” virus, which other solutions missed
Fortune 5 Energy Company	Consolidating data silos	• 2 Billion logs and events per day reduced to 25 high priority offenses
Branded Apparel Maker	Detecting insider fraud	• Trusted insider stealing and destroying key data
$100B Diversified Corporation	Predicting risks against your business	• Automating the policy monitoring and evaluation process for configuration change in the infrastructure
Industrial Distributor	Addressing regulatory mandates	• Real-time extensive monitoring of network activity, in addition to PCI mandates

Solutions for the Full Compliance and Security Intelligence Timeline



Prediction & Prevention

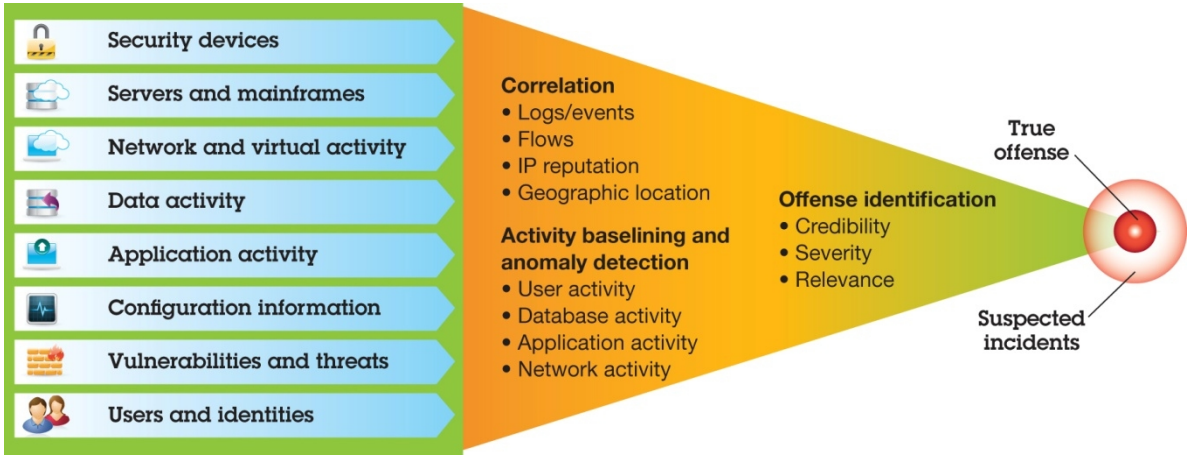
Risk Management. Vulnerability Management.
Configuration Monitoring. Patch Management.
X-Force Research and Threat Intelligence.
Compliance Management. Reporting and Scorecards.

Reaction & Remediation

SIEM. Log Management. Incident Response.
Network and Host Intrusion Prevention.
Network Anomaly Detection. Packet Forensics.
Database Activity Monitoring. Data Loss Prevention.

1Labs®
Total Security Intelligence | An IBM Company

IBM QRadar SIEM is a market leading solution to provide full visibility and actionable insight to an organization's IT infrastructure to help the organization protect itself from a wide range of advanced security threats and effectively address compliance mandates.



QRadar SIEM 7.2 continues QRadar's tradition of continually responding to customer and market needs by delivering new capabilities that include improvement of its asset data model, Console usability, license deployment, and support for data privacy, while at the same time significantly enhancing the product to meet SWG globalization requirements, to support QRadar sibling products (QRM & QVM), and tp create larger customer values based on integration.

Fully Integrated Security Intelligence

Log Management

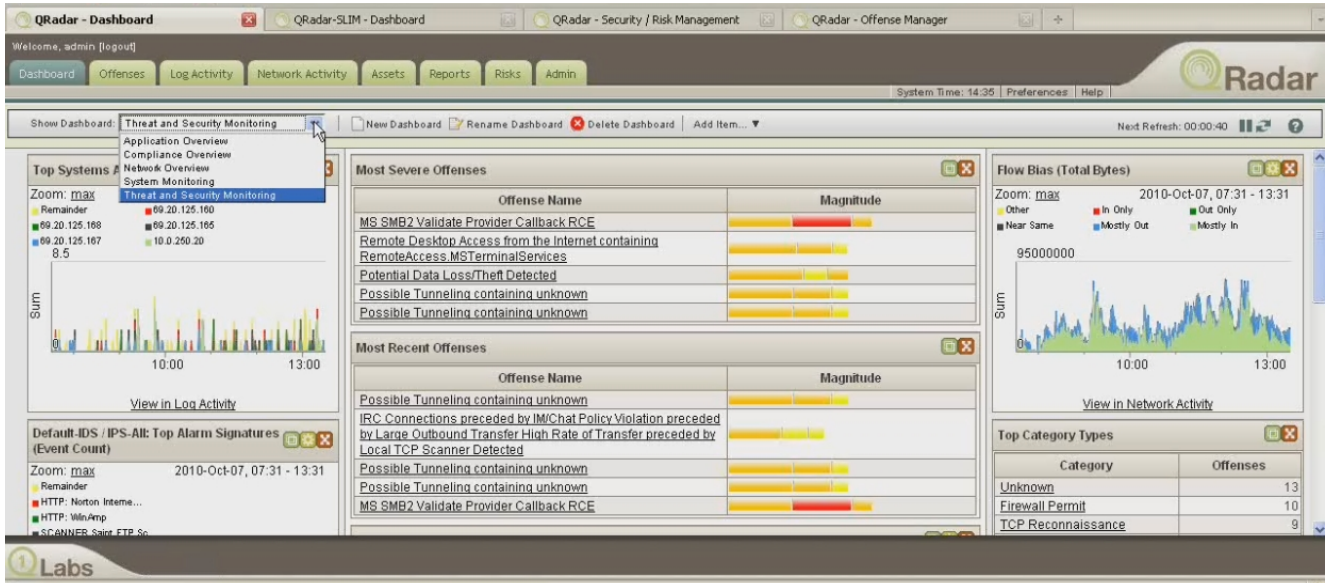
SIEM

Configuration & Vulnerability Management

Network Activity & Anomaly Detection

Network and Application Visibility

One Console Security

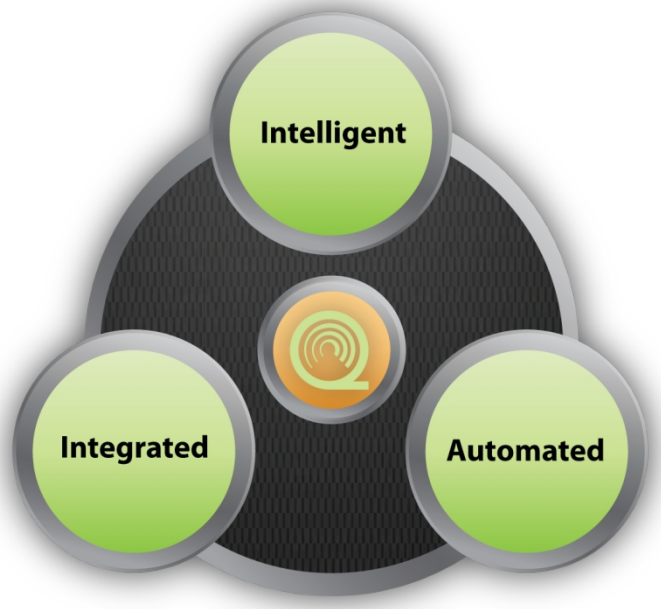


Built on a Single Data Architecture

QRadar: Applying Intelligence, Integration, Automation

- Proactive threat management
- Identifies critical anomalies
- Rapid, extensive impact analysis

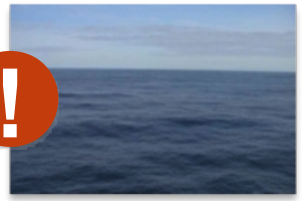
- Bridges silos
- Highly scalable
- Flexible & adaptable



- Easy deployment
- Rapid time to value
- Operational efficiency

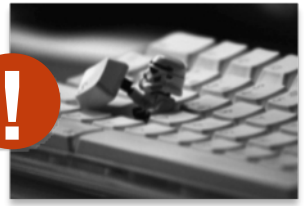
Customer business problems

Problems in current VM deployments:



Data overload inhibitor

Siloed system limitations



Hidden risks remain

Leaves unanswered questions → **Creates security gaps**

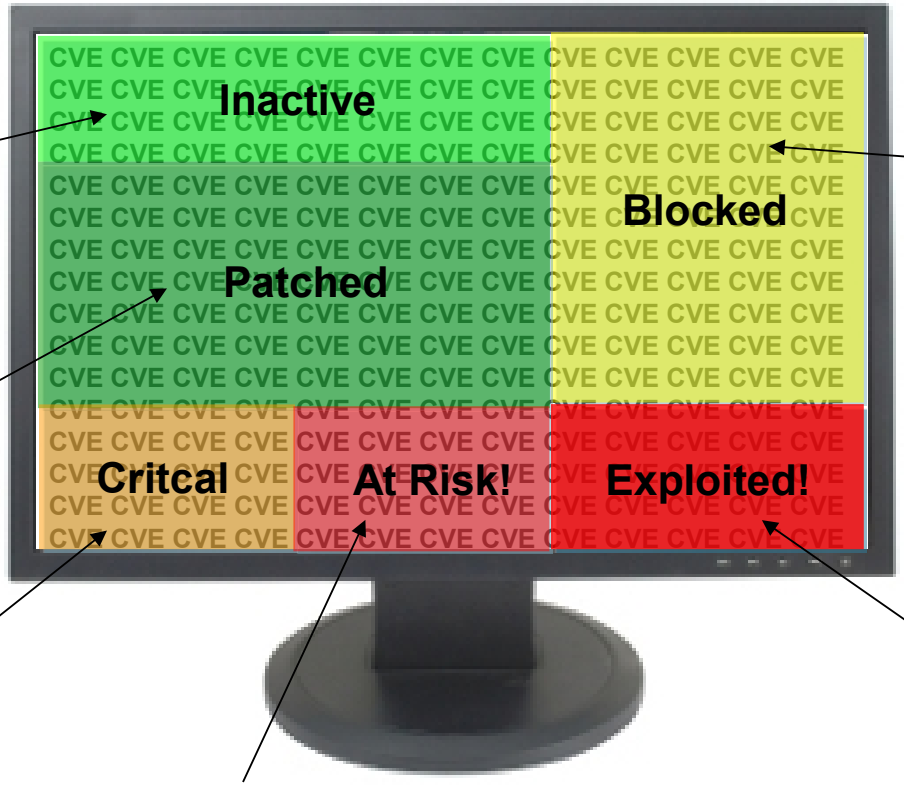
- *Has that been patched?*
- *Has or will it be exploited?*
- *Does my firewall block it?*
- *Does my IPS block it?*
- *Does it matter?*

QVM enables customers to interpret ‘sea’ of vulnerabilities

Inactive: QFlow Collector data helps QRadar Vulnerability Manager sense application activity

Patched: IBM Endpoint Manager helps QVM understand which vulnerabilities will be patched

Critical: Vulnerability knowledge base, remediation flow and QRM policies inform QVM about business critical vulnerabilities



At Risk: X-Force Threat and SIEM security incident data, coupled with QFlow network traffic visibility, help QVM see assets communicating with potential threats

Blocked: QRadar Risk Manager helps QVM understand which vulnerabilities are blocked by firewalls and IPSs

Exploited: SIEM correlation and IPS data help QVM reveal which vulnerabilities have been exploited

Customer roadmap with QRadar Vulnerability Manager

- Upgrade Log Manager to QRadar SIEM
  - Additional security telemetry data
  - Rules-based correlation analysis engine
  - Data overload reduction 'magic' compressing millions or even billions of daily raw events to manageable list of issues
- Add QRadar Risk Manager
  - Enables pre-exploit configuration investigations
  - Simplifies security policy reviews for compliance tests
  - Provides network topology depictions and permits attack simulations
- **Implement QRadar Vulnerability Manager**
  - **Extends pre-exploit analysis activities by adding integrated, vulnerability insights**
  - **Reduces magnitude of pre-exploit conditions as QRadar SIEM does for post-exploit conditions**
  - **Helps identify and measure exposures to external threats**
- Inject IBM X-Force Threat Research Intelligence
  - Provides intelligence feed to QRadar
  - Includes vulnerabilities, IP reputations, malware reports and attack histories

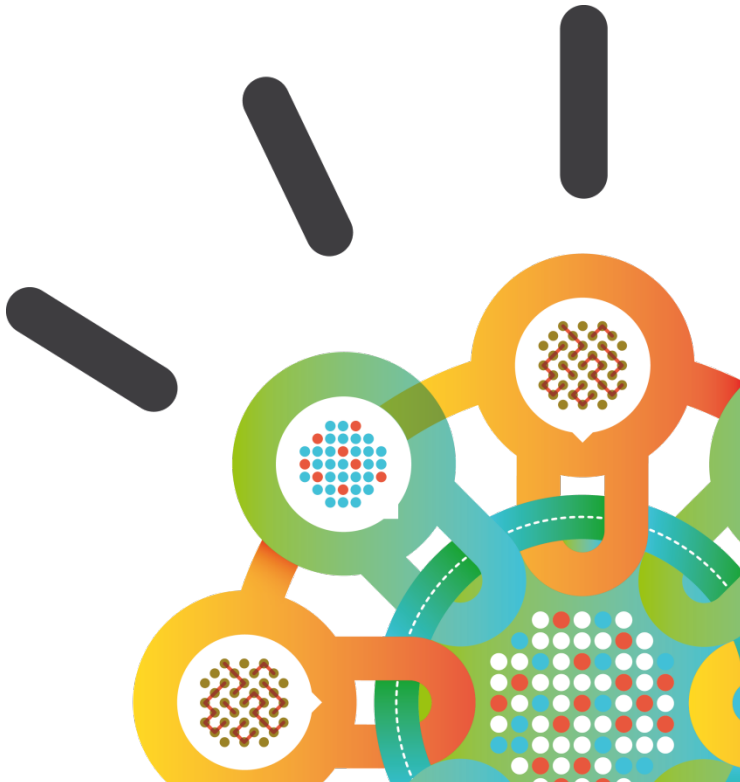
ibm.com/security

Agenda

- Welcome and Introductions
- Latest Security trends and H1 2013 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- **Holistic approach to handling Advanced Persistent Threats**
- Break
- From Identity & Access Management to Identity Intelligence
- Managing Application Security
- Data Security

Security Intelligence.
Think Integrated.

Holistic approach to handling Advanced Persistent Threats



S. Rohit
email: rohits@sg.ibm.com

137,400,000

…Number of cyber-attacks witnessed by IBM in 2012

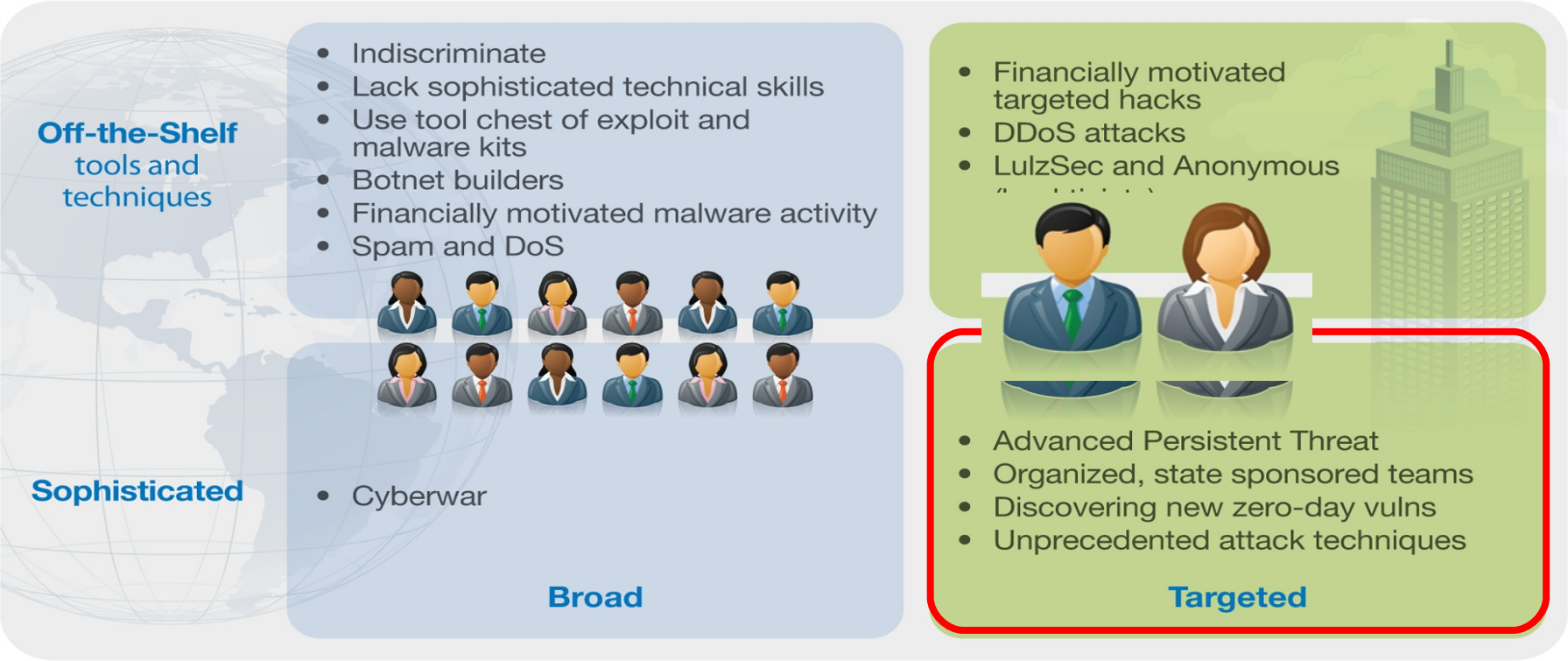
Most Attacked Industries

Industry	Average weekly attacks
Health and Social Services	10.1 million
Transportation	9.8 million
Hospitality	5.5 million
Finance and Insurance	3.6 million
Manufacturing	2.6 million

1.07

Incidents per
one million attacks[1]

Attackers are using sophisticated techniques to bypass defenses



"Advanced Persistent Threat" is the approach often used by State-Sponsored Entities

Source: IBM X-Force Research and Development

What's different about Advanced Persistent Threats?

Advanced

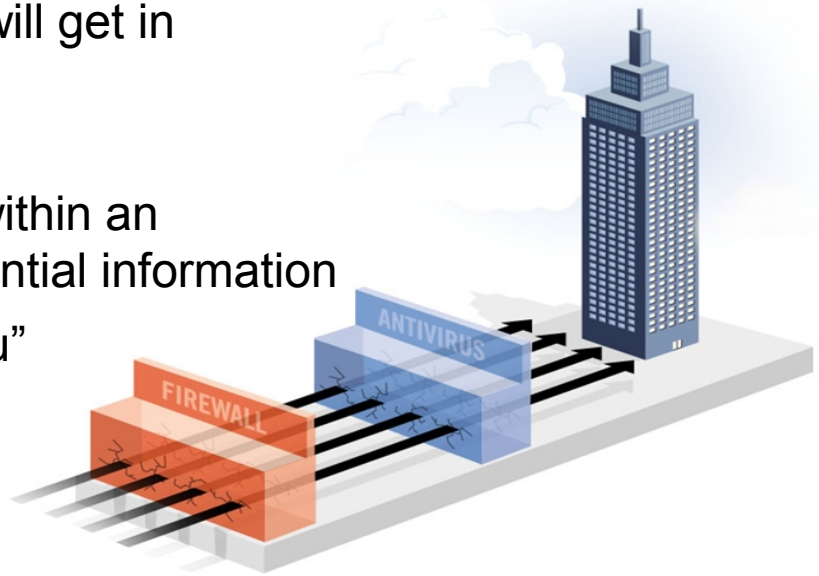
- Exploiting unreported (zero-day) vulnerabilities
- Advanced, custom malware is not detected by antivirus products
- Coordinated, well researched attacks using multiple vectors

Persistent

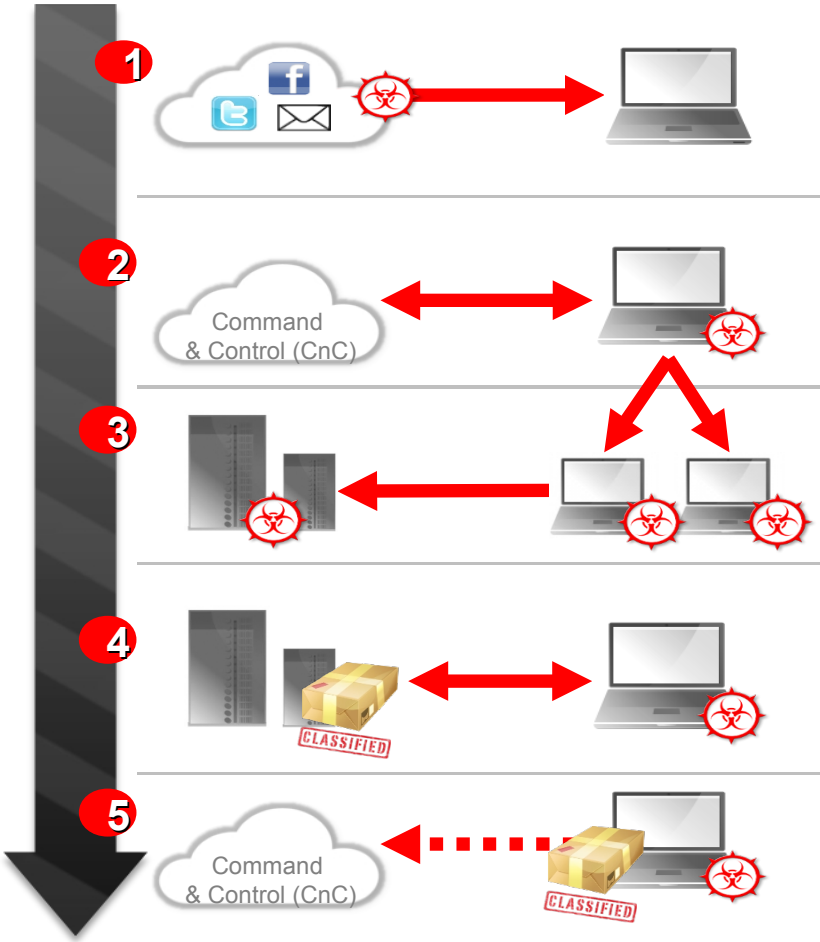
- Attacks last for months or years (average: 1 year; longest: 4.8 years)[1]
- Attackers are dedicated to the target – they will get in

Threat

- Targeted at specific individuals and groups within an organization; aimed at compromising confidential information
- Not random attacks – they are "out to get you"

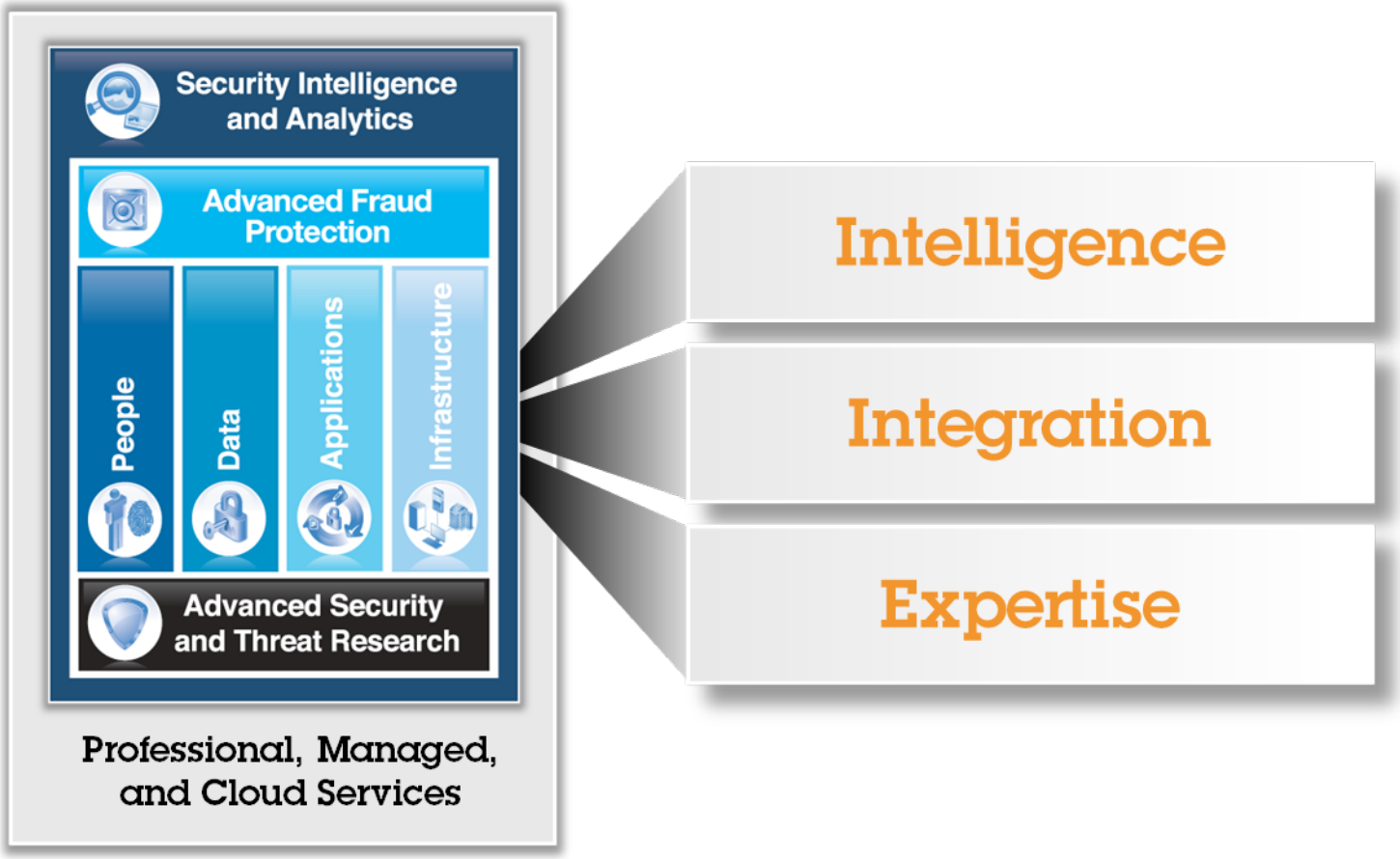


Attackers follow a 5-Stage attack chain



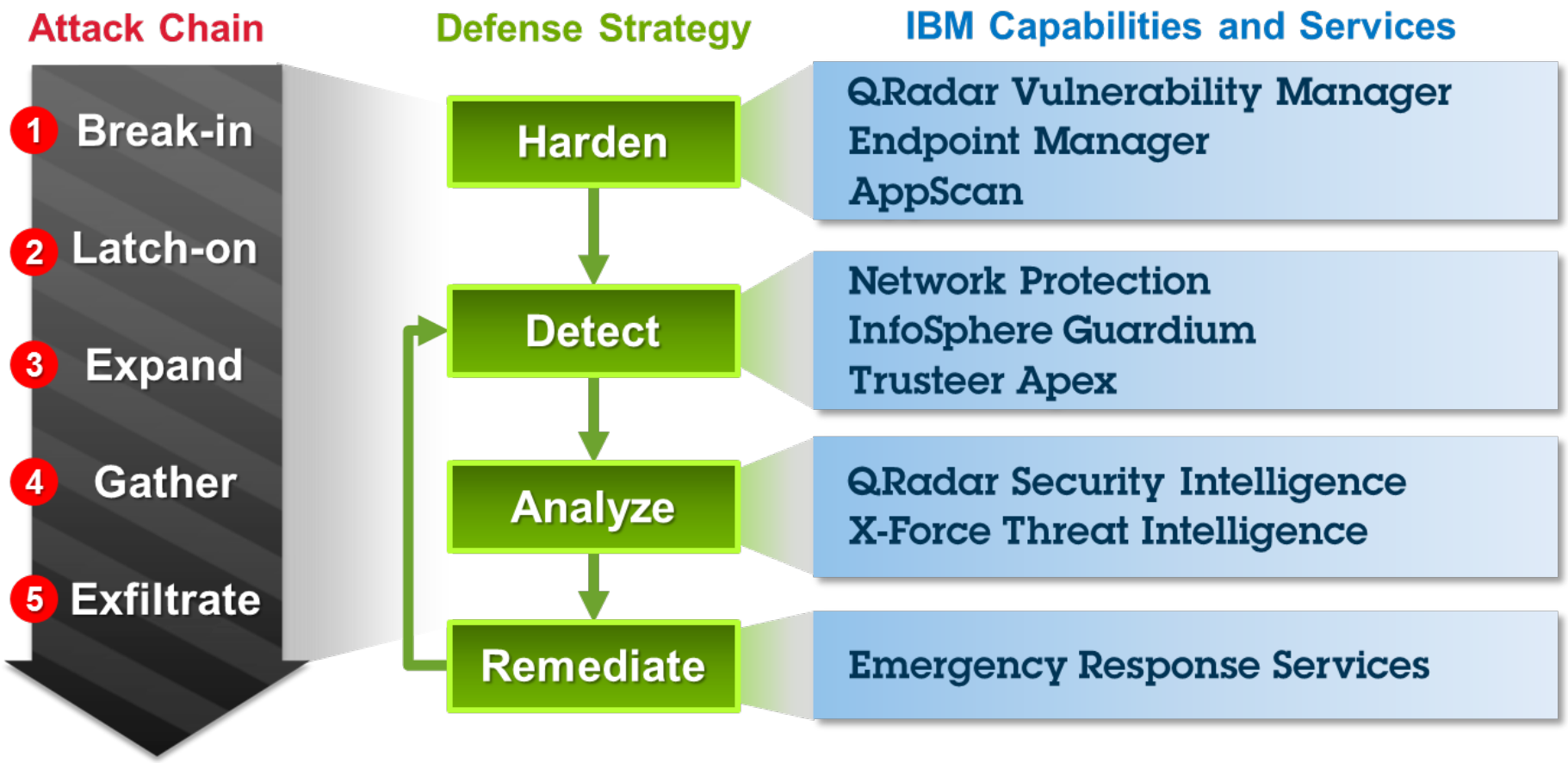
Break-in	Spear phishing and remote exploits to gain access
Latch-on	Malware and backdoors installed to establish a foothold
Expand	Reconnaissance and lateral movement to increase access and maintain a presence
Gather	Acquisition and aggregation of confidential data
Exfiltrate	Data exfiltration to external networks

IBM Security Framework

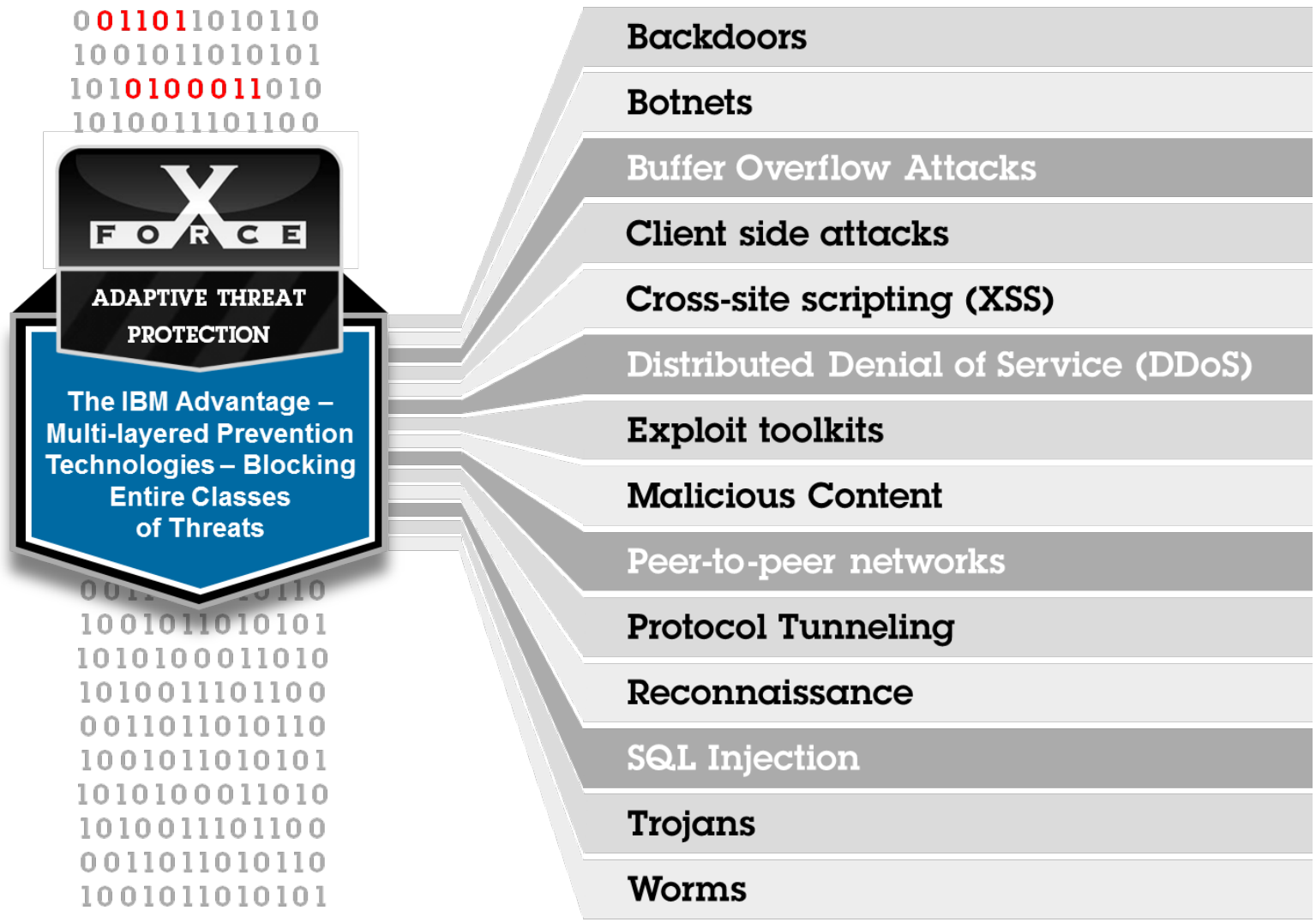


Advanced Threat Protection

Staying ahead of sophisticated attacks



Staying ahead of the threat with IBM Threat Protection

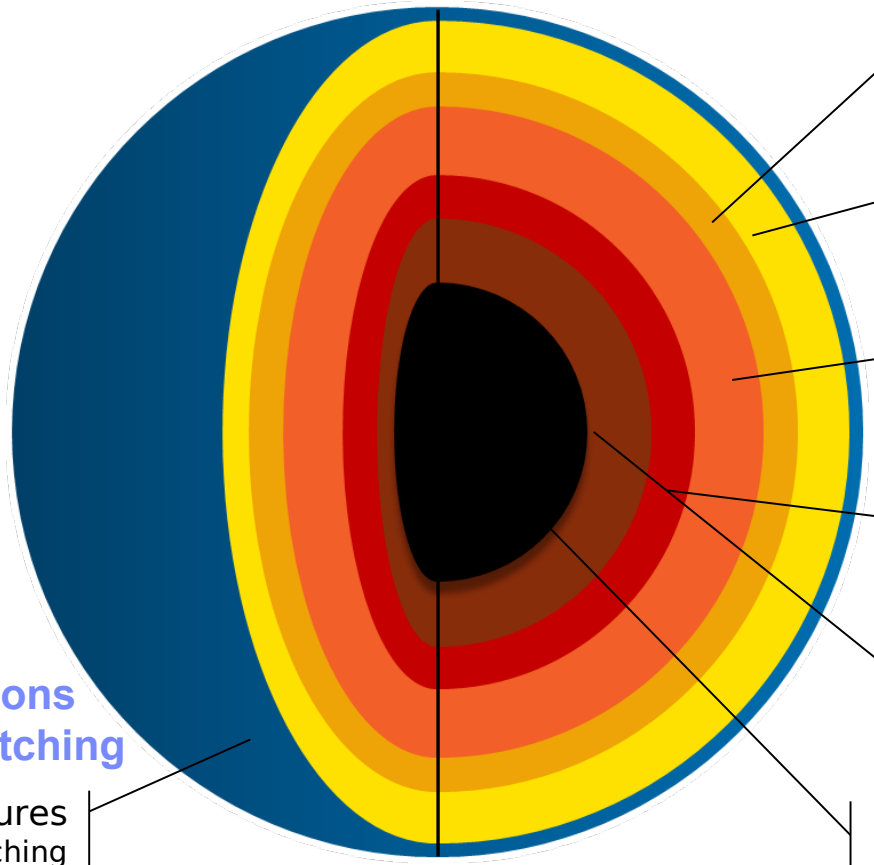


Multiple intrusion prevention technologies working in tandem

Multiple intrusion prevention technologies working in tandem

Spectrum of Vulnerability and Exploit Coverage

IBM stays ahead of the threat with these protection engines



Vulnerability Decodes
Focused algorithms for mutating threats

Application Layer Heuristics
Proprietary algorithms to block malicious use

Web Injection Logic
Patented protection against web attacks - e.g. SQL Injection and Command Injection

Shellcode Heuristics
Behavioral approach to blocking exploit payloads

Content Analysis
File and document inspection

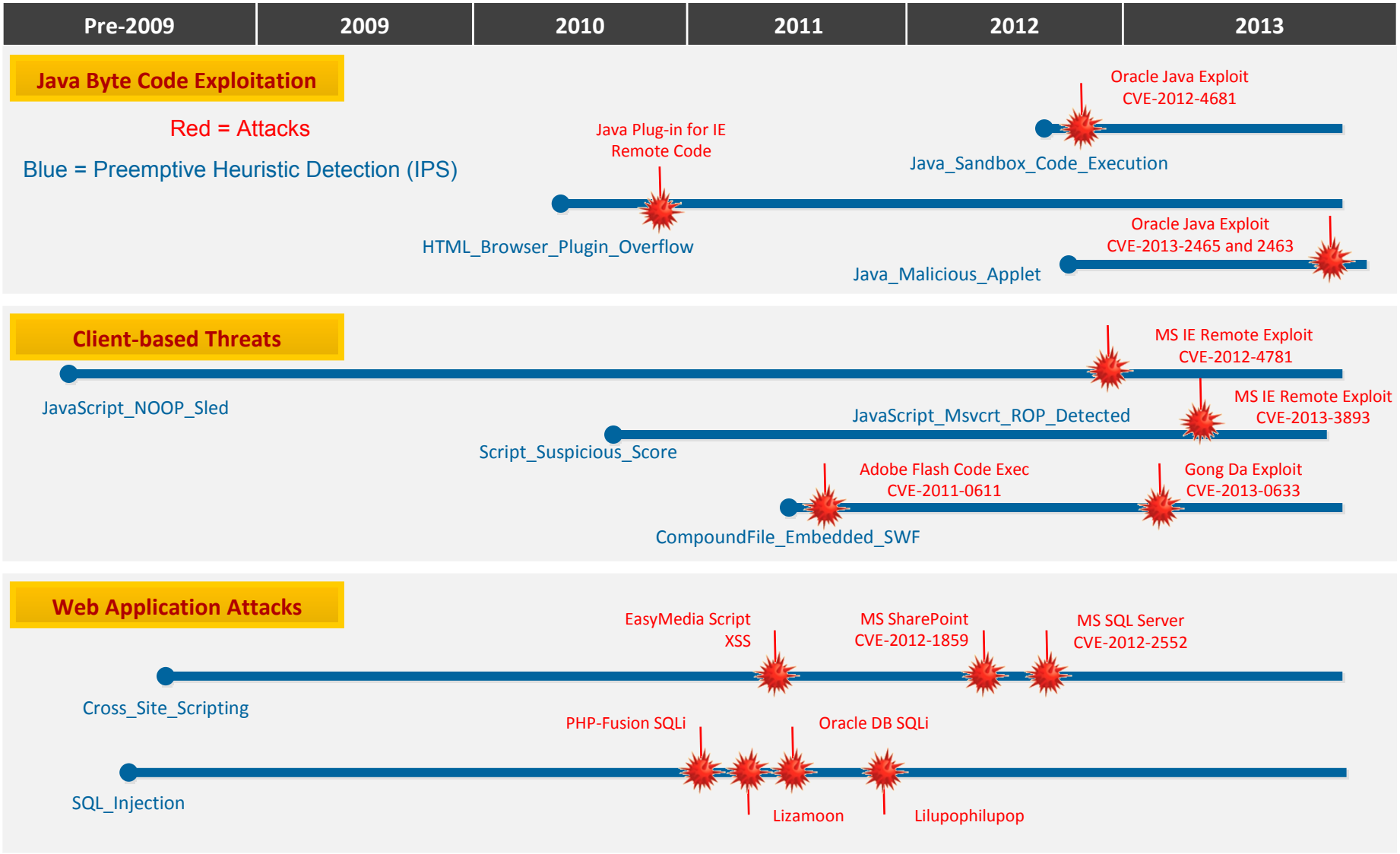
Protocol Anomaly Detection
Protection against misuse, unknown vulnerabilities, and tunneling across over 230+ protocols

Some IPS solutions stop at pattern matching

Exploit Signatures
Attack specific pattern matching

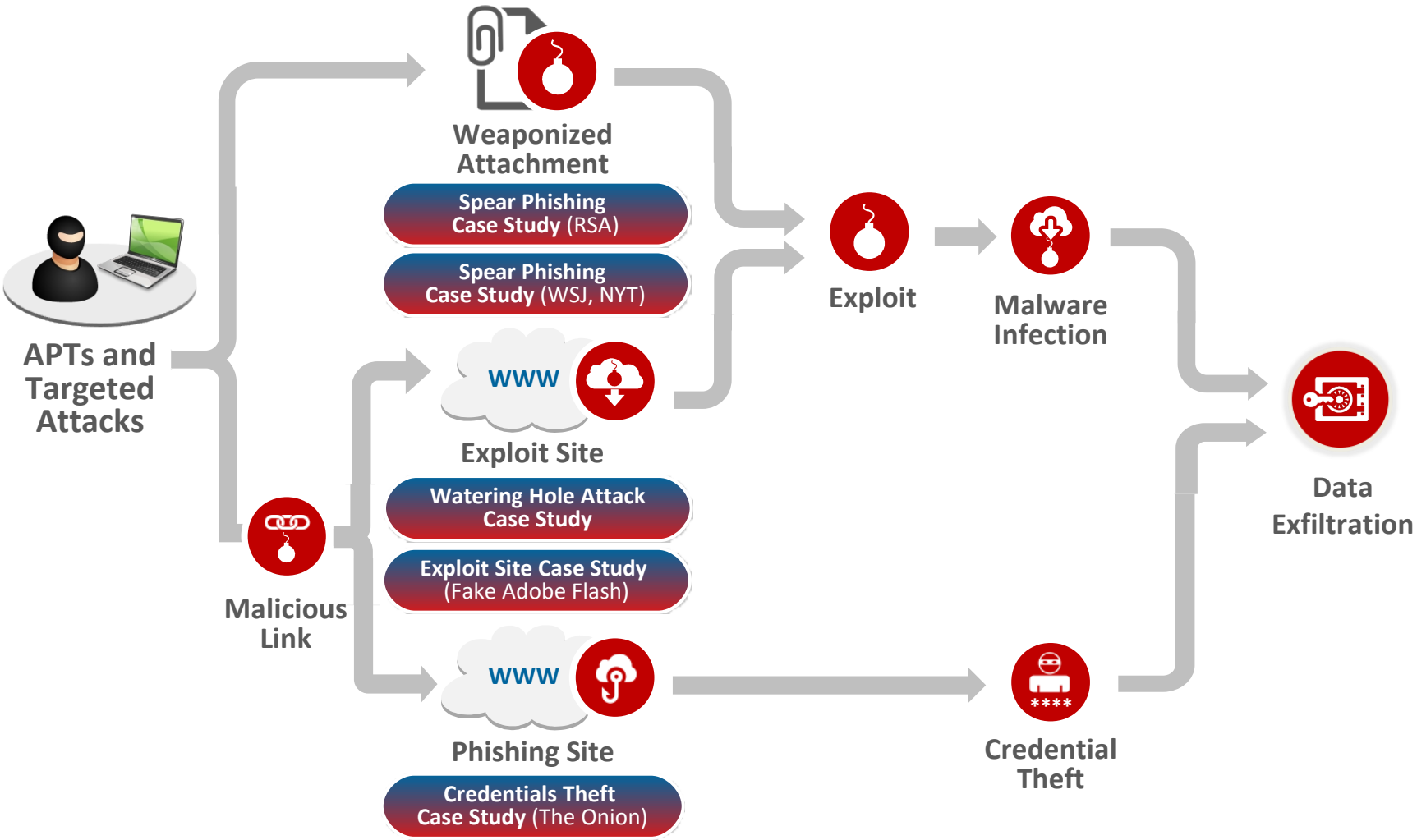
The Result = Preemptive protection for today's threats

The signatures and examples shown in this slide are for representation of the heuristic coverage available and do not demonstrate the entire listing of attacks from the time the signature was created.



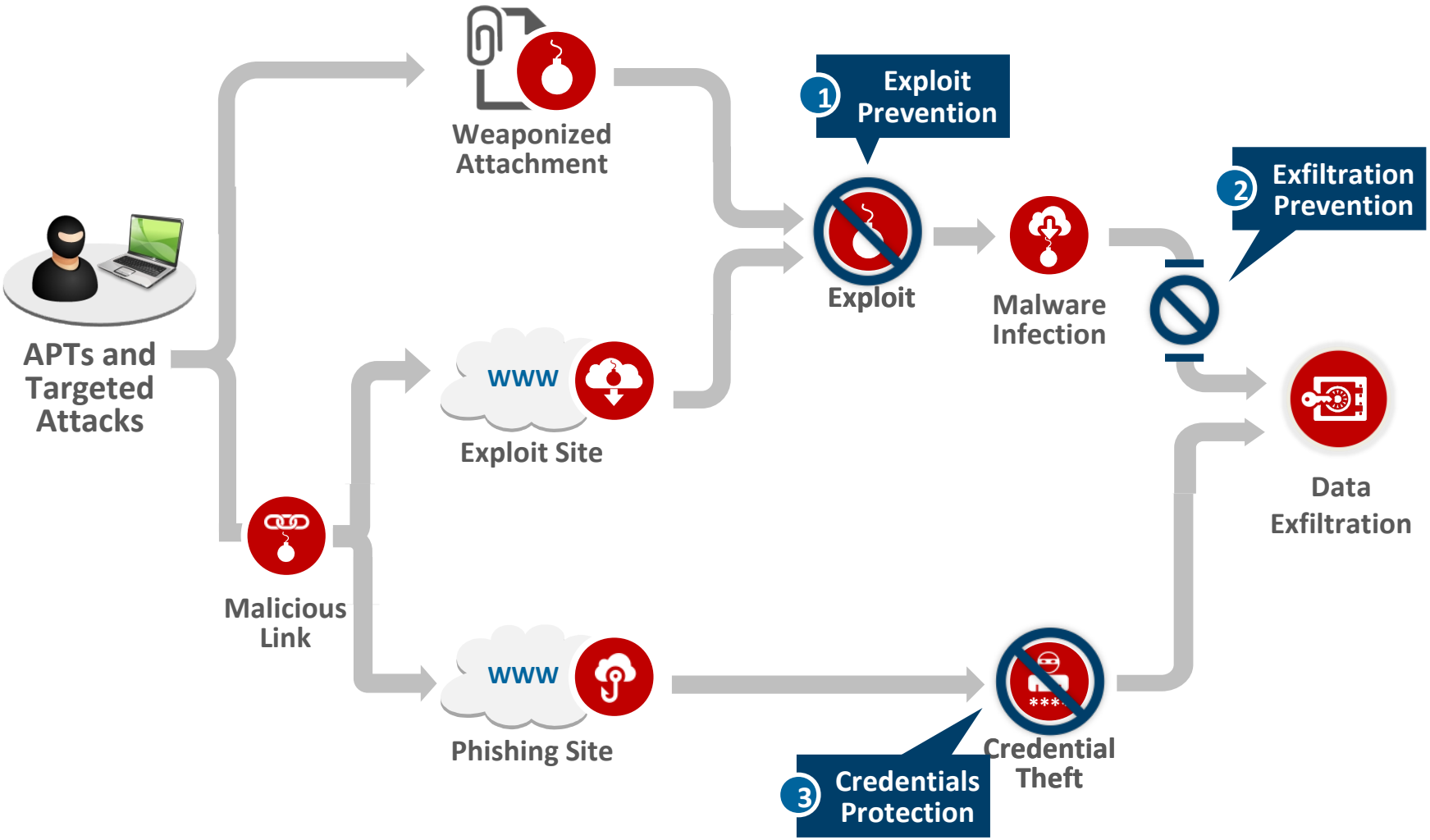
APTs and Targeted Attacks

Trusteer



APTs and Targeted Attacks

Trusteer



Trusteer Apex: Three Security Layers

- Stop exploitation of user application vulnerabilities
- Prevent drive-by downloads

- Block malware communication
- Prevent information theft

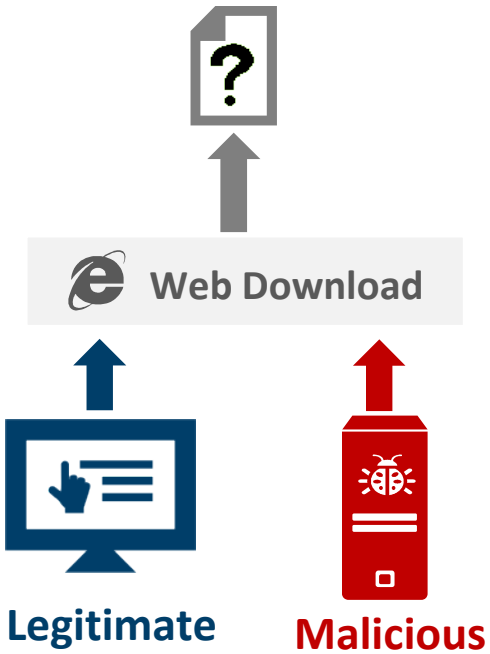
- Block key-loggers
- Prevent submission on phishing sites
- Prevent reuse on public consumer sites

Trusteer Apex Exploit Prevention

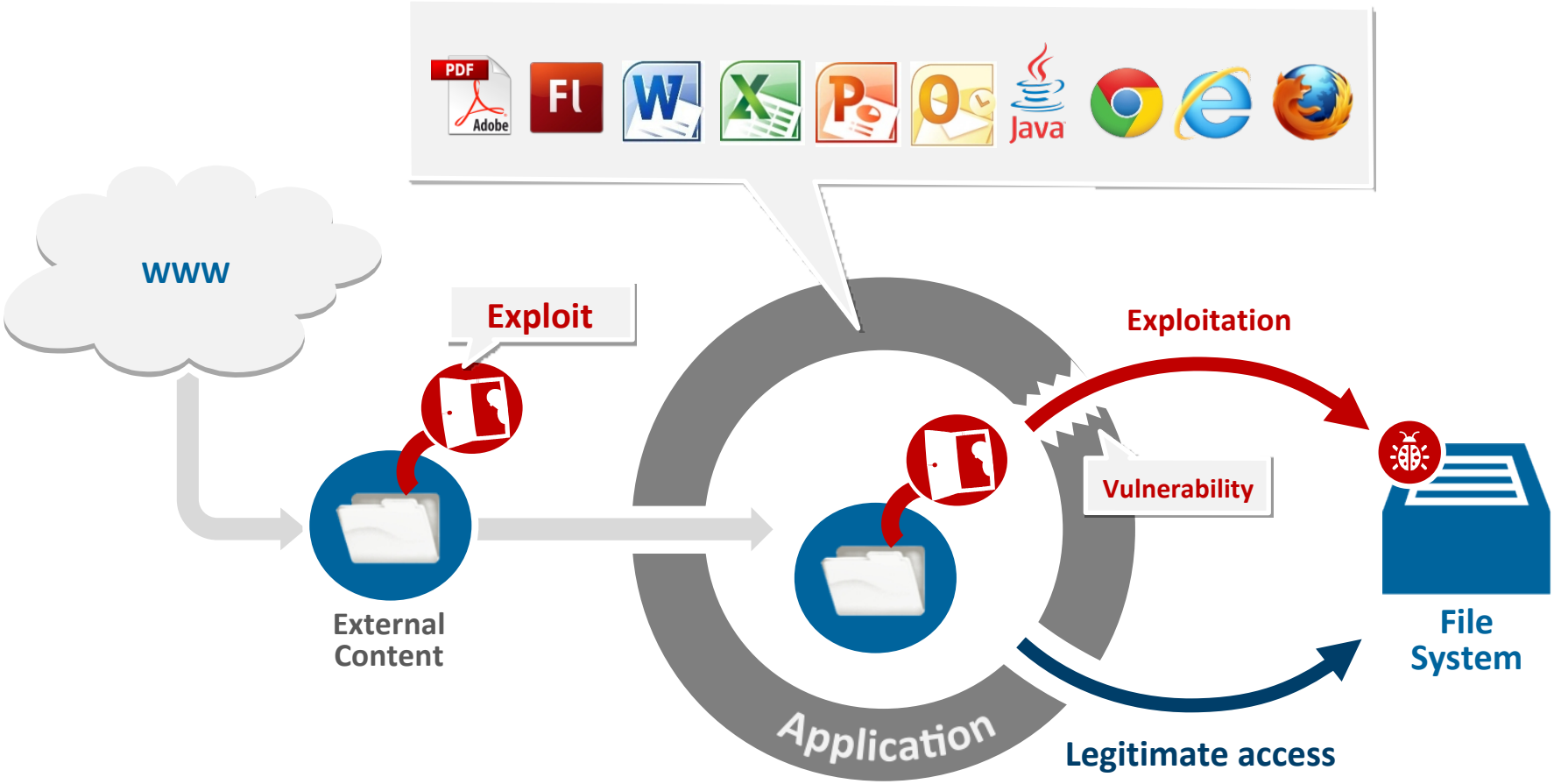
Stateful Application Control

Analyzing Application Action (What?) + Application State (Why?)

What is the application doing?	**Action:** a file is written to the file system and executed
Why is it doing it?	**State:** user initiated download



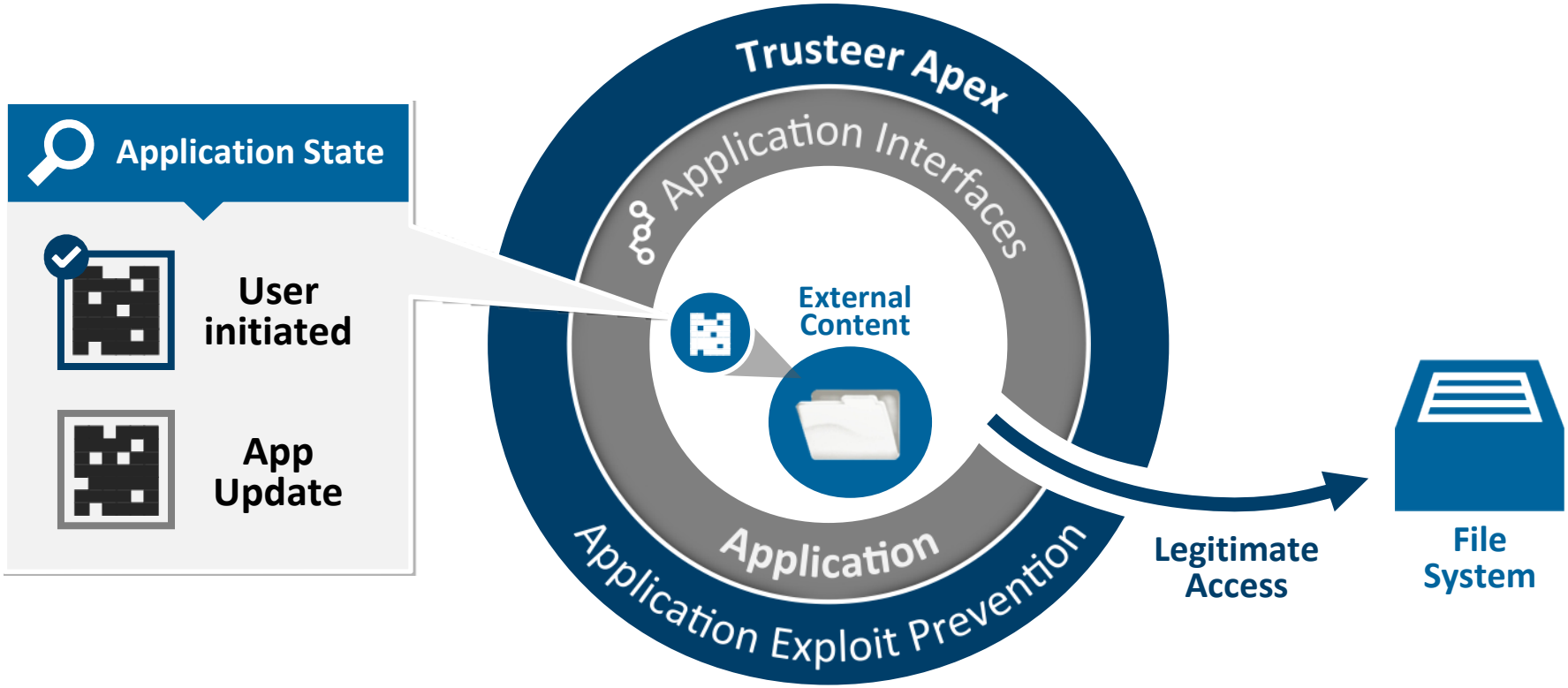
Application Exploit Prevention:
What is an exploit?



An exploit is a piece of software that uses an application vulnerability to cause unintended application behavior

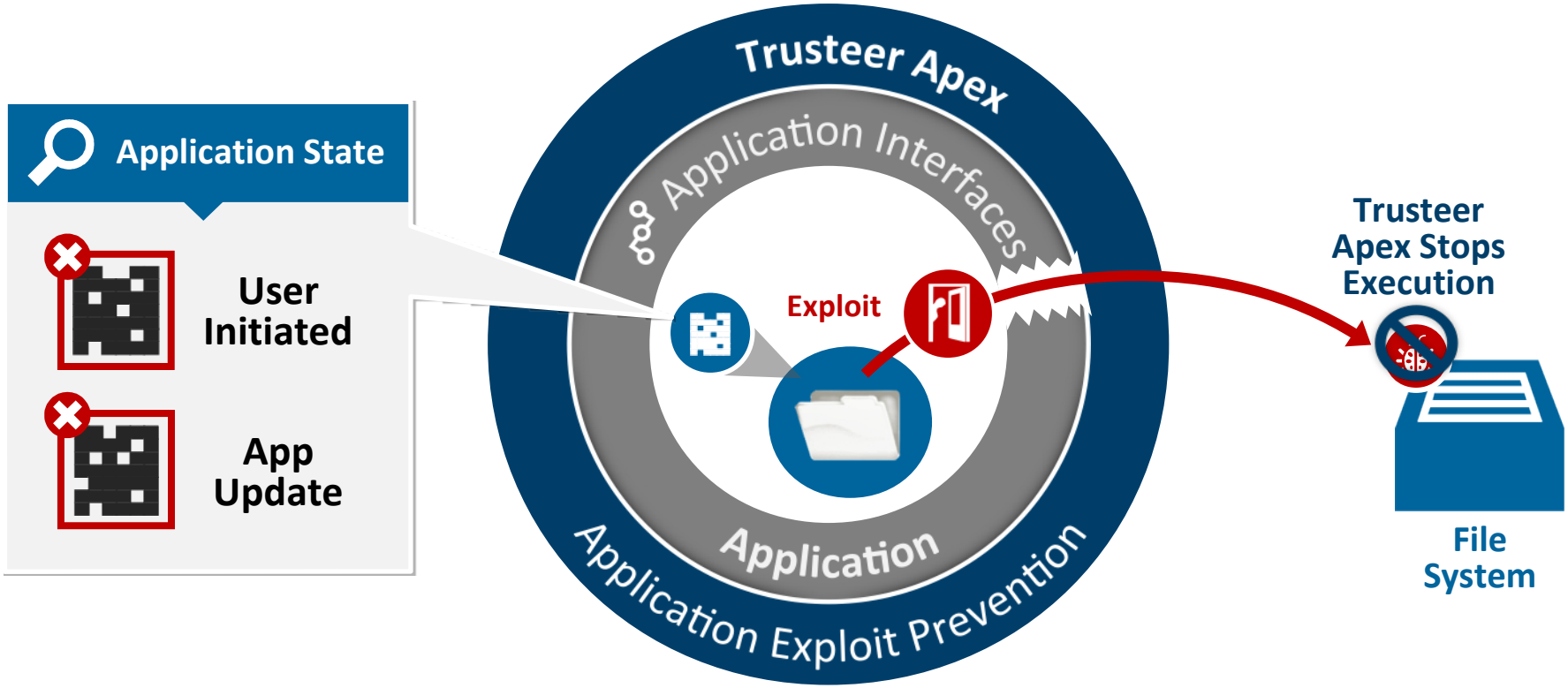
Application Exploit Prevention:
Verify Application State

Allow application action with a approved state



Application Exploit Prevention:
Verify Application State

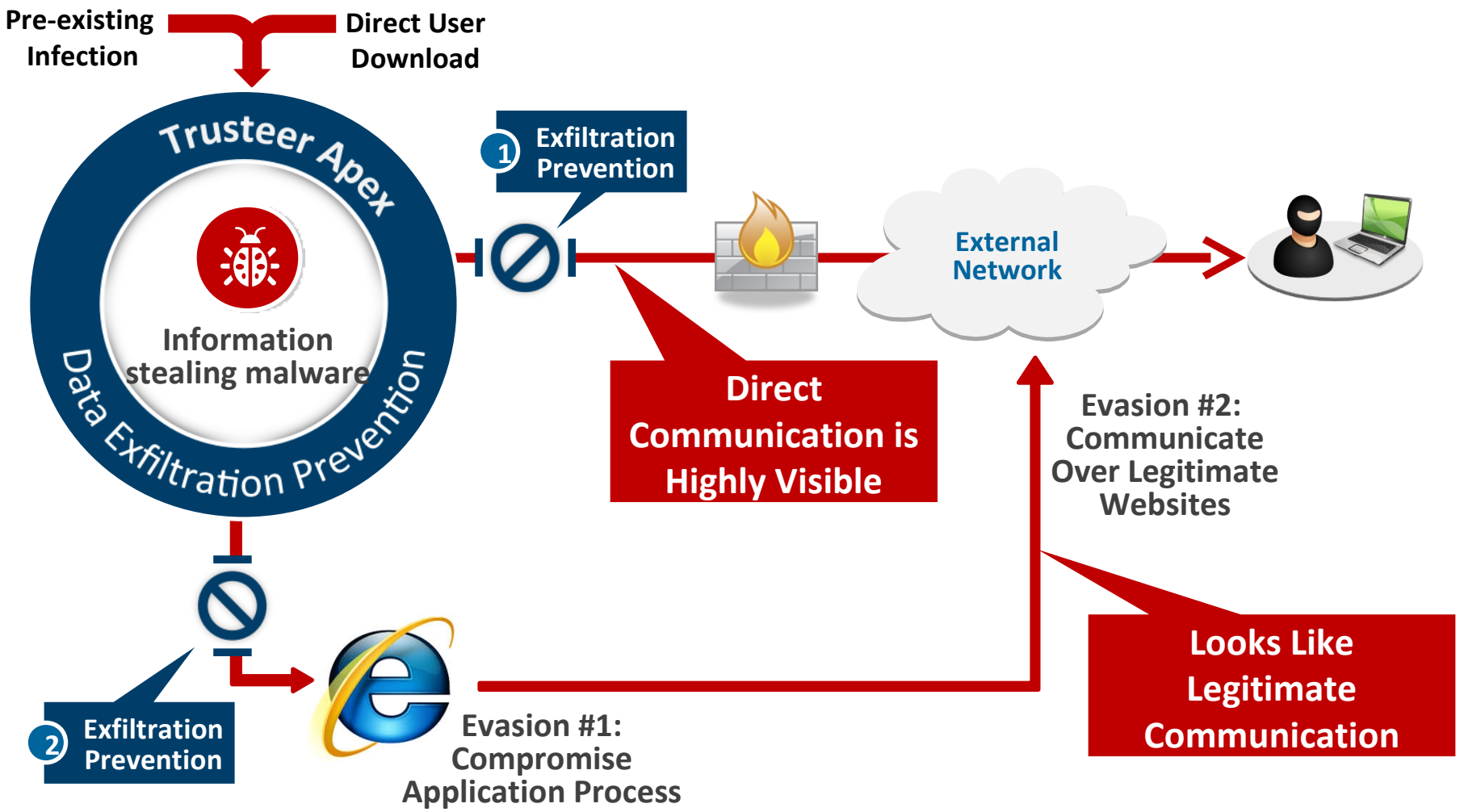
Stop application actions with unknown state



Trusteer Apex Data Exfiltration Prevention

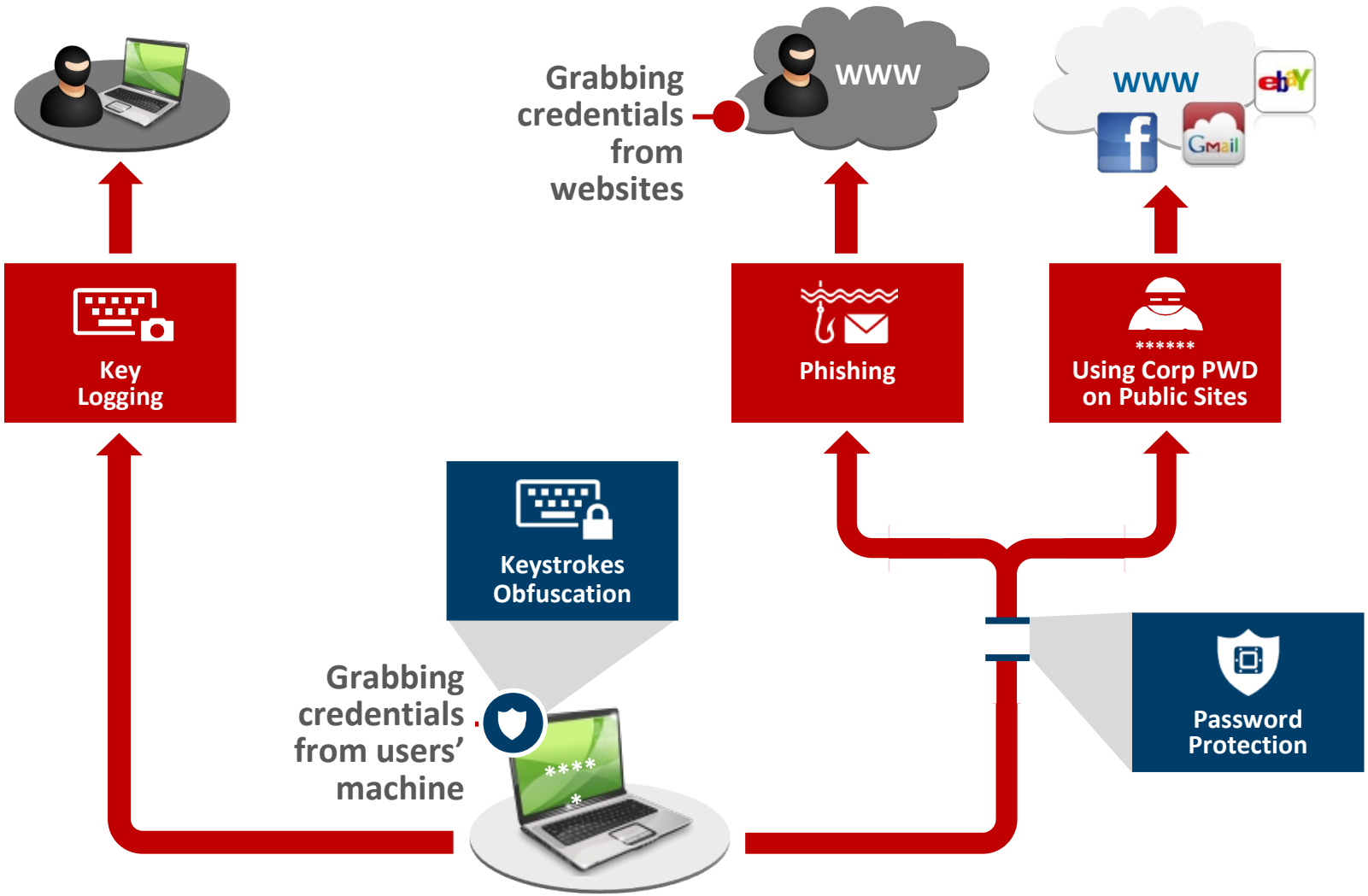
Data Exfiltration Prevention:
Block Malicious External Communication

Block suspicious executables that open malicious communication channels



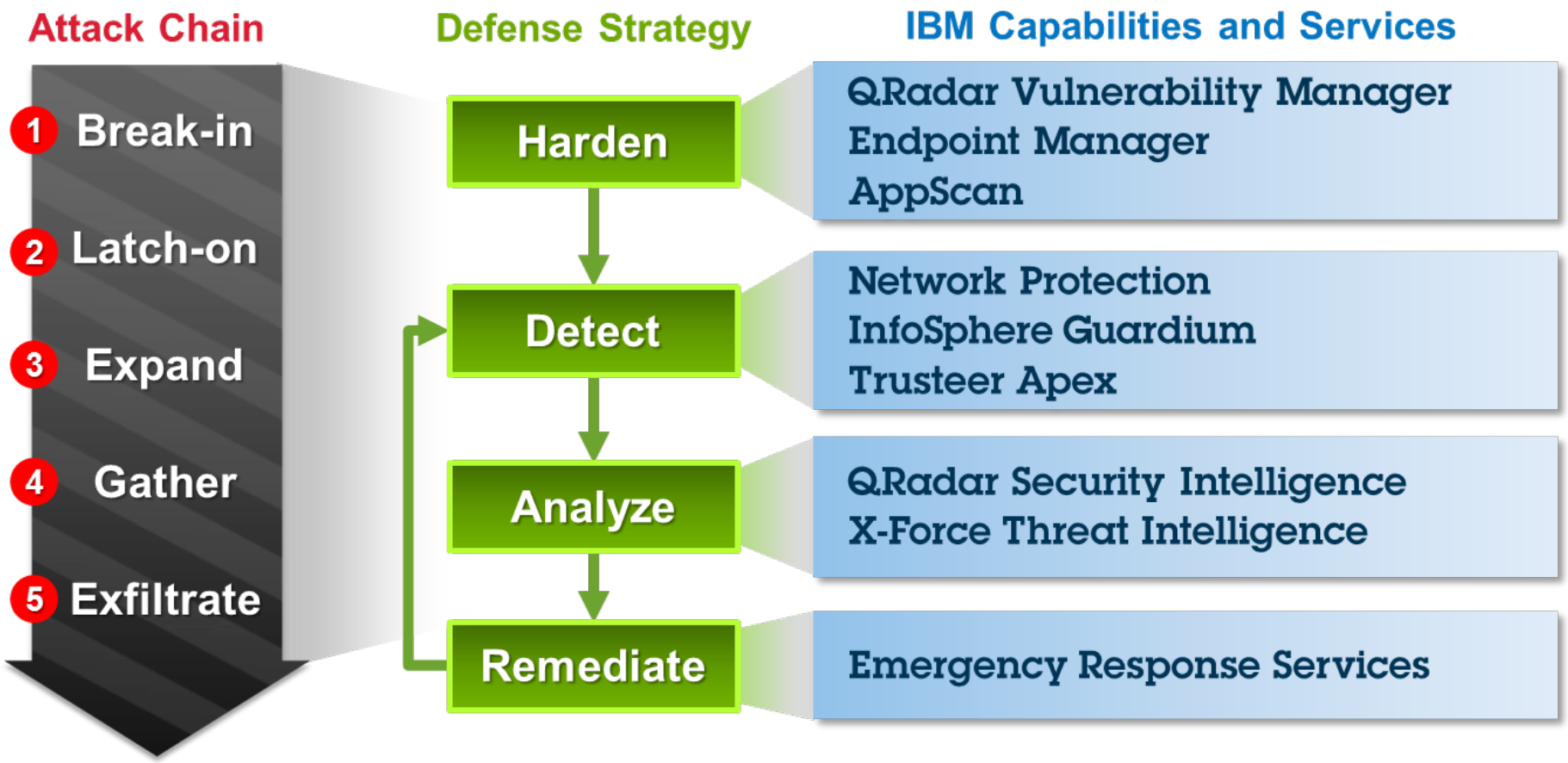
Trusteer Apex Enterprise Credentials Protection

Data Exfiltration Prevention
Prevent Credentials Theft



Advanced Threat Protection

Staying ahead of sophisticated attacks



What to do if you have been breached

1. Call IBM Emergency Response Services (24x7):

24x7

The (cyber)storm is coming. ARE YOU READY?

Emergency? Call: (US) +1.888.241.9812 | (WW) +1.312.212.8034

Or get started with a **penetration test** or an **incident response plan**

2. Proactively assess risk and reduce future breach likelihood:

   - Cyber Incident response training and simulated exercises to determine level of preparedness
   - Incident Response Program gap assessment to ensure enterprise readiness and responsiveness when an incident occurs
   - Active Threat Assessment as a preemptive service to determine weaknesses requiring remediation
   - X-Force threat analysis service is available from IBM experts **24x7**

Key Features

24x7x365 Hotline for clients to call from anywhere worldwide for assistance if they believe they are experiencing an incident

Incident Case Managers who maintain calm, focus, and manage the incident and environment to completion and satisfaction

Advanced tools, expertise and scale for any platform, size client, and location worldwide

Globally collected intelligence applied to each engagement to improve outcomes and efficiencies

Unlimited emergency declarations

Agenda

- Welcome and Introductions
- Latest Security trends and H1 2013 X-Force Report
- Security Intelligence - Understanding your Organizational Security Posture
- Holistic approach to handling Advanced Persistent Threats
- **Break**
- From Identity & Access Management to Identity Intelligence
- Managing Application Security
- Data Security

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.

ibm.com/security