SERVICE & RISK MANAGEMENT FORUM 2011

Addressing Emerging Threats Through Next Generation Intrusion Prevention

Robert Giberson
Security Architect & X-Force Field Liaison
IBM Security Solutions

Agenda

- Changing Threats in 2011 and into 2012
- Good news, we're making headway against threats and vulnerabilities
- Bad news, the landscape is becoming more complicated
  - The Year of the Security Breach
    - Broadly targeted, financially motivated attacks
    - Advanced Persistent Threats
    - Hacktivism
- Drivers of Next Generation Intrusion Prevention
- Emerging Requirements for Intrusion Prevention Systems
- Meeting the Needs of our Clients: Introducing IBM Security's Intrusion Prevention Appliances
- Questions

Mission

To protect our customers from security threats on the Internet by developing a comprehensive knowledge of vulnerabilities and attack methodologies and applying that knowledge through effective protection technologies.

IBM X-Force Research and Development

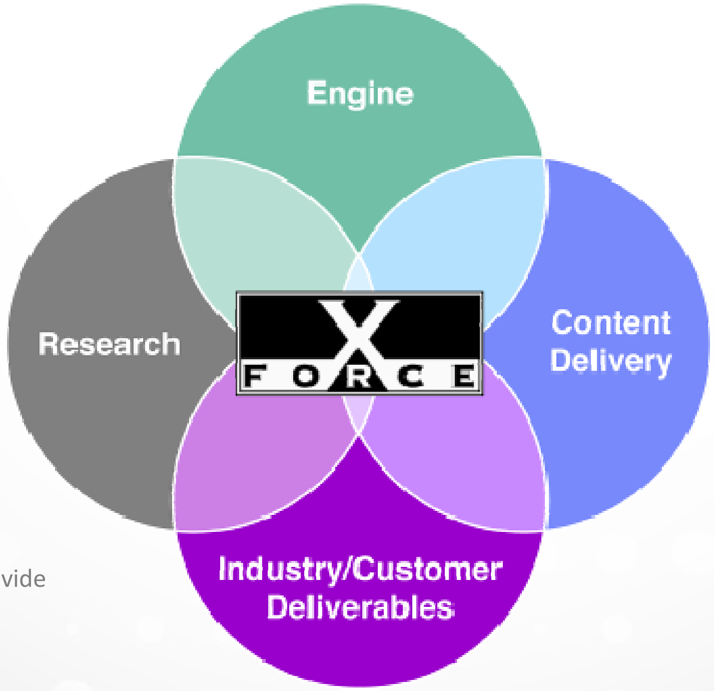
The world's leading enterprise security R&D organization

Engine

- Support content stream needs and capabilities
- Support requirements for engine enhancement
- Maintenance and tool development

Research

- Support content streams
- Expand current capabilities in research to provide industry knowledge to the greater IBM



Global security operations center (infrastructure monitoring)

Content Delivery

- Continue third party testing Dominance
- Execute to deliver new content streams for new engines

Industry/Customer Deliverables

- Blog, Marketing and Industry Speaking Engagements
- X-Force Database Vulnerability Tracking
- Trend Analysis and Security Analytics

SERVICE & RISK MANAGEMENT FORUM 2011

X-Force Research & Development
Unmatched Security Leadership

IBM.

The mission of the IBM X-Force® research and development team is to:

- Research and evaluate threat and protection issues
- Deliver security protection for today's security problems
- Develop new technology for tomorrow's security challenges
- Educate the media and user communities

X-Force Research

14B analyzed Web pages & images

40M spam & phishing attacks

54K documented vulnerabilities

Billions of intrusion attempts daily

Millions of unique malware samples

Provides Specific Analysis of:

- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

Public Vulnerability Disclosures

History repeats itself (probably)

- 2010 = highest # of vulnerabilities
- **2011 = 1H down 21% 1H YoY**
  - Web applications continue to be the largest category of disclosure.
- 2011 likely to have less vulnerability disclosures than 2010. However some categories increased...

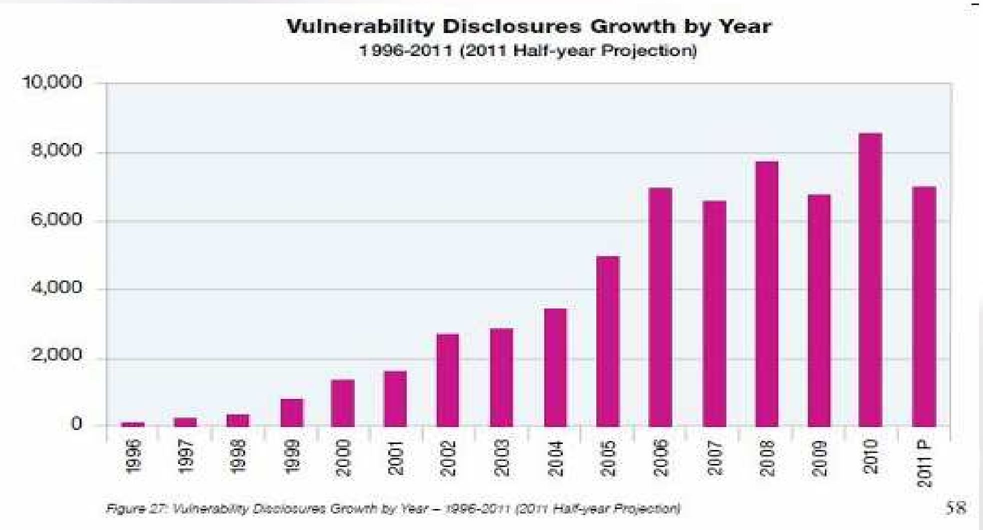
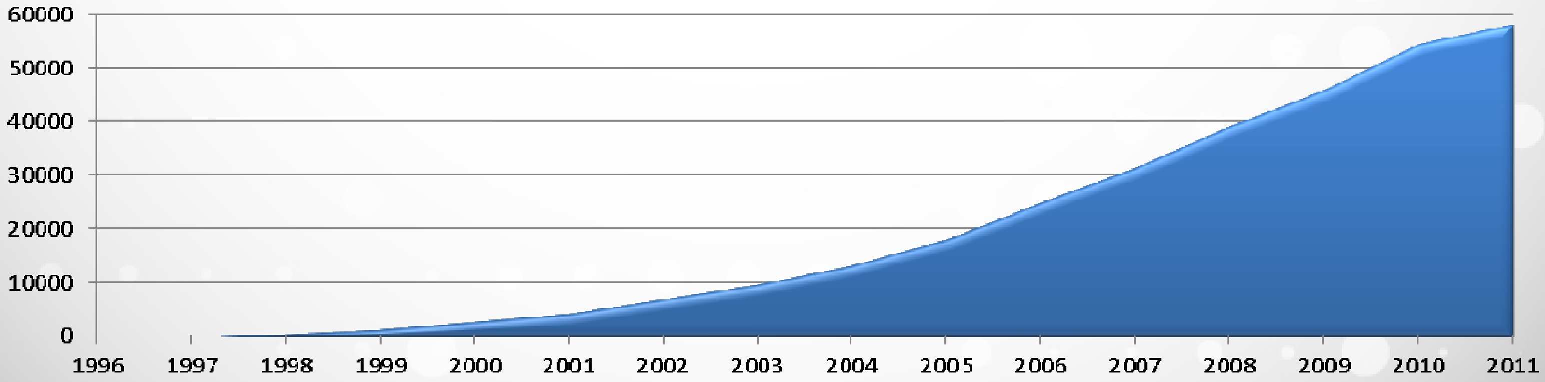


Figure 27: Vulnerability Disclosures Growth by Year – 1996-2011 (2011 Half-year Projection)

Total Cumulative Vulnerabilities 1996-2011 1H



Web Application Vulnerabilities

- Total number of vulnerabilities decline — but it’s cyclical
- Decline is in web application vulnerabilities

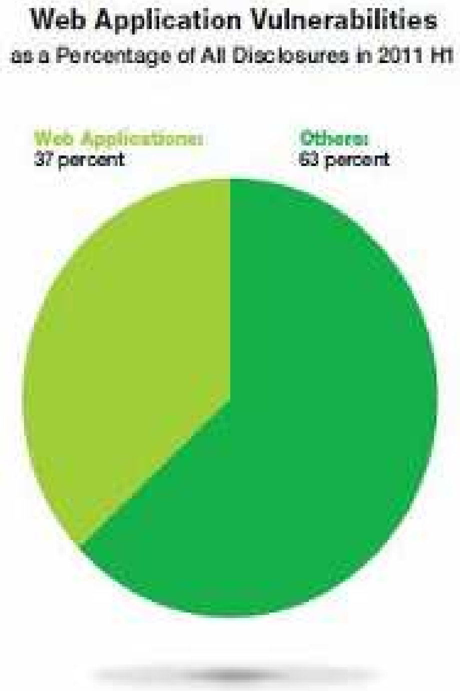


Figure 28: Web Application Vulnerabilitiesas as a Percentage of All Disclosures in 2011 H1

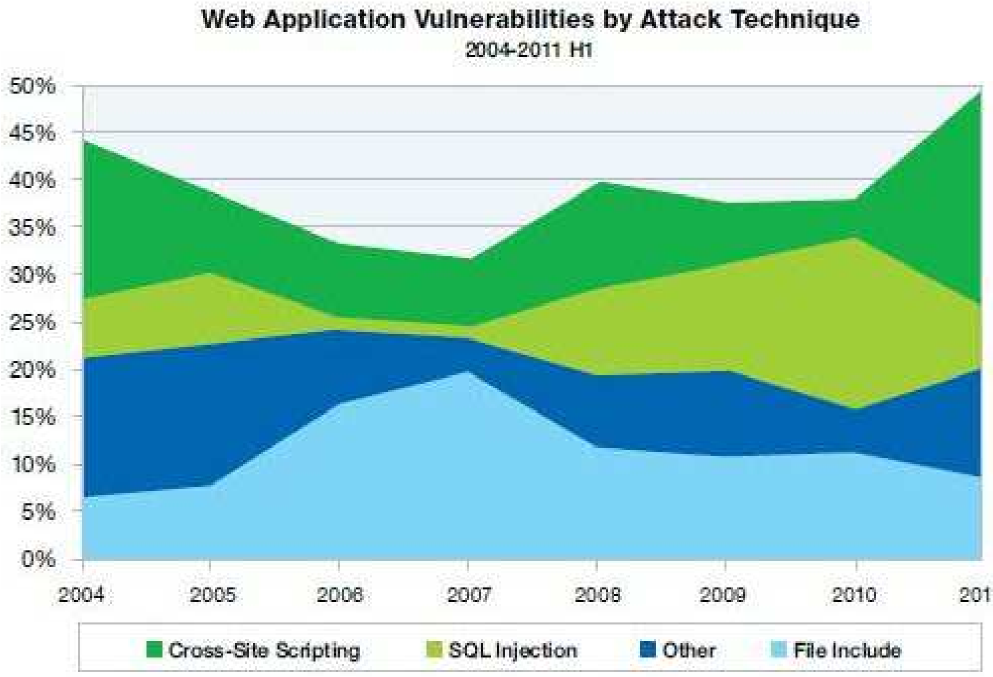


Figure 29: Web Application Vulnerabilities by Attack Technique – 2004-2011 H1

Patching

- Significant improvement in unpatched vulnerabilities

- Hasn't dropped below 44% in over five years

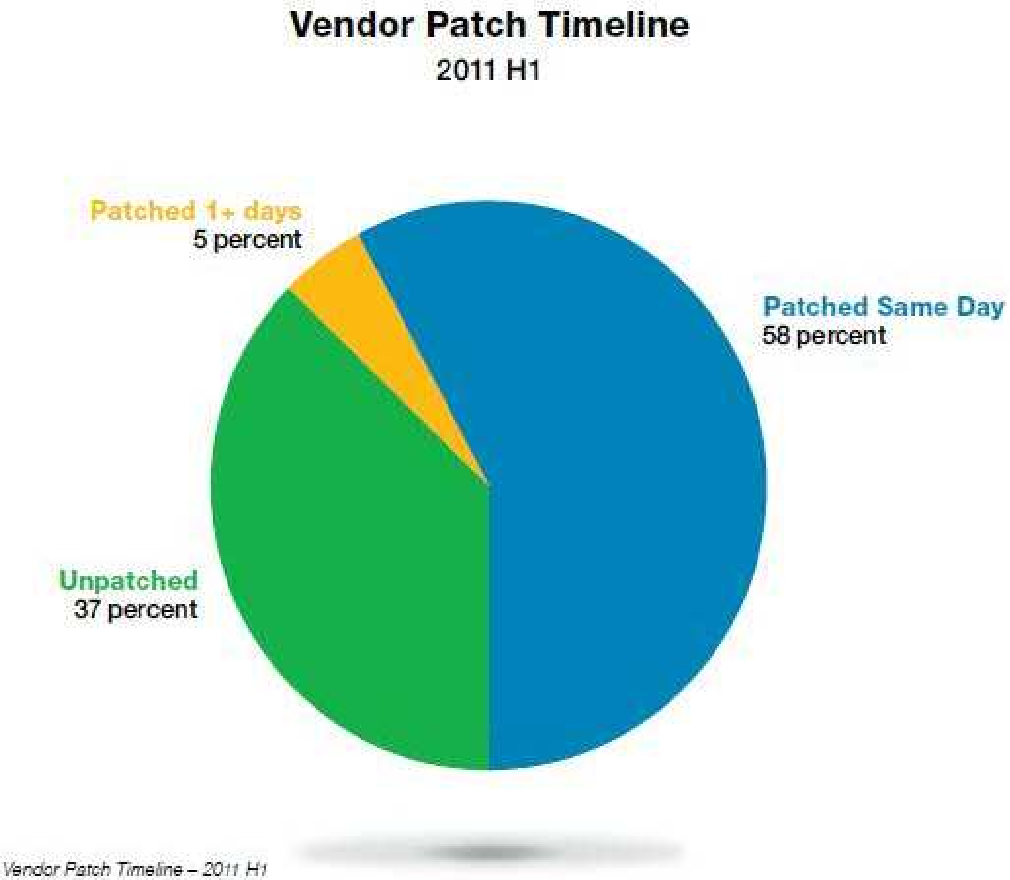
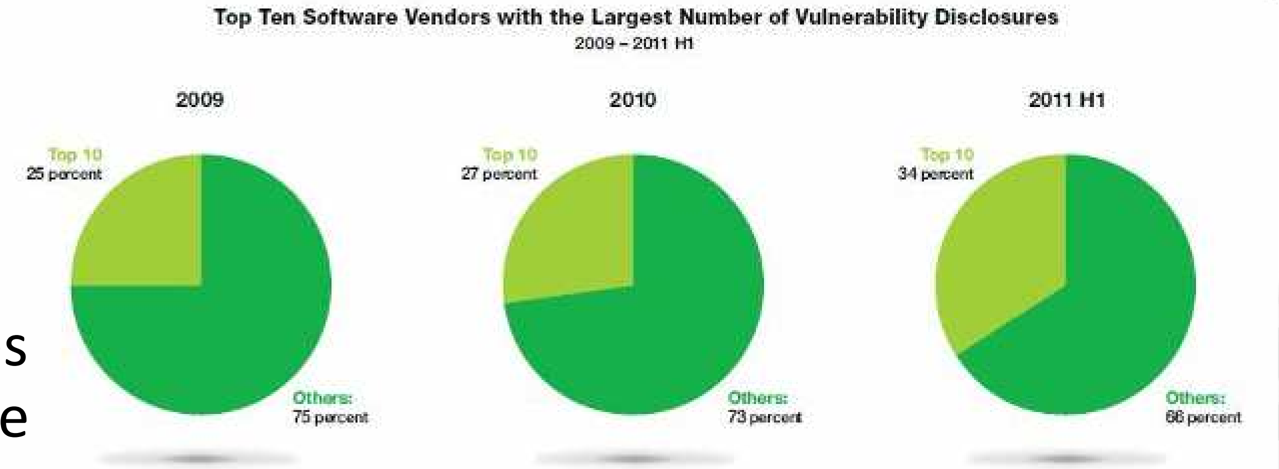


Fig. 33: Vendor Patch Timeline – 2011 H1

Big vendors & critical vulnerabilities

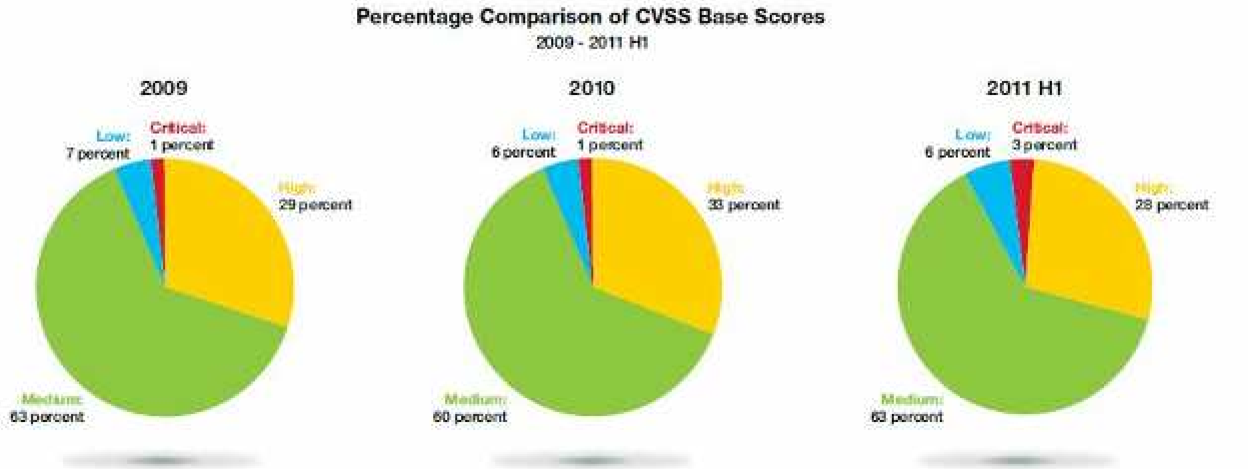
- Top 10 vendors a greater percentage

- Critical vulnerabilities triple as a percentage



Top Ten Software Vendors with the Largest Number of Vulnerability Disclosures

2009 – 2011 H1



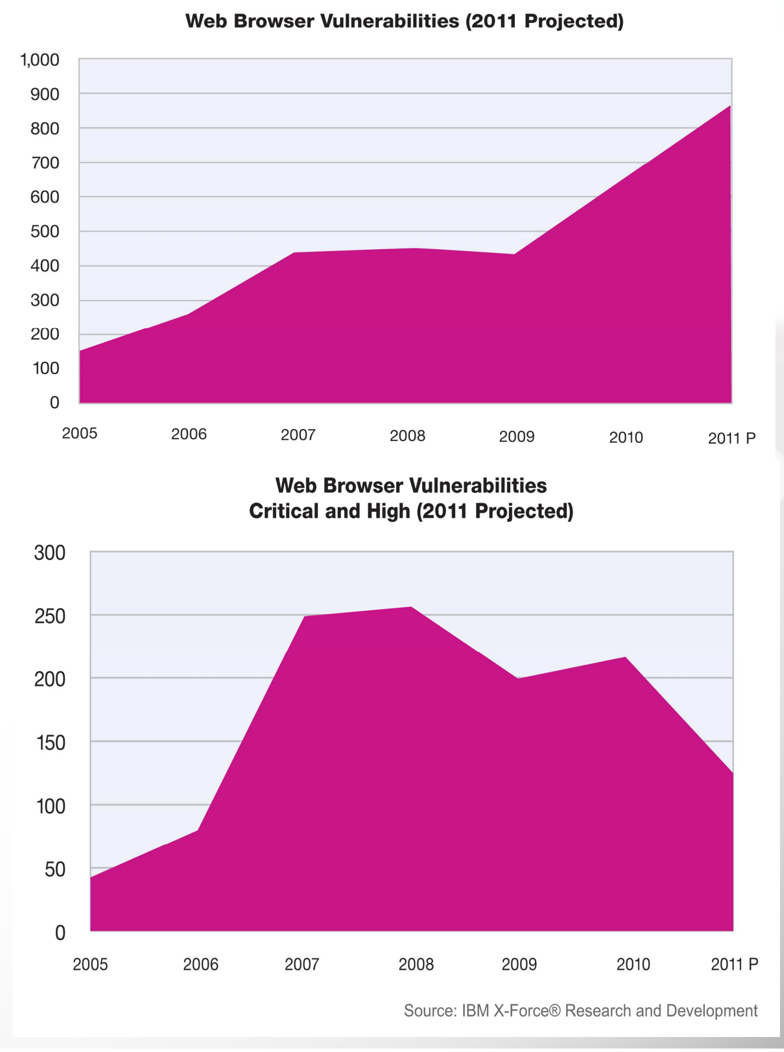
Percentage Comparison of CVSS Base Scores

2009 - 2011 H1

Figure 35: Percentage Comparison of CVSS Base Scores – 2009 – 2011 H1

Safer web browsers

- Total vulnerabilities are up
- Critical and high vulnerabilities to lowest levels not seen since 2007
- Our industry does seem to be getting better at making safe browser software



Source: IBM X-Force® Research and Development

Multi-media & document vulnerabilities

- Significant increases in both categories
- Attackers have zeroed in on software that consumers are running regardless of the browser
- Recent efforts to sandbox these applications are not perfect

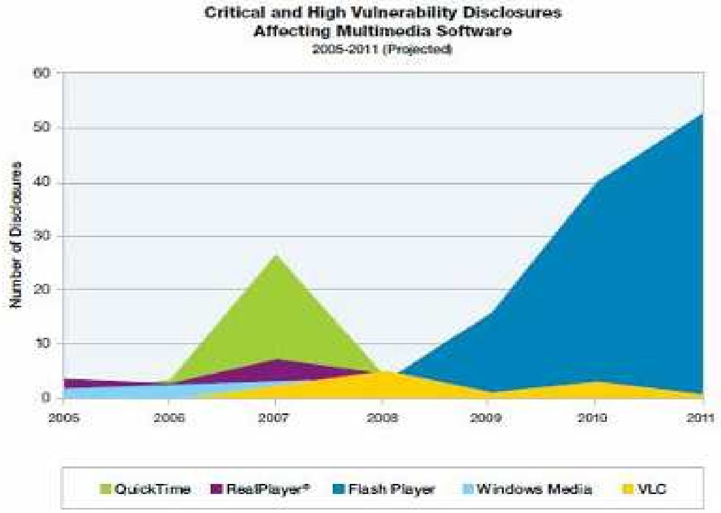


Figure 37: Critical and High Vulnerability Disclosures Affecting Multimedia Software –2005-2011 (Projected)

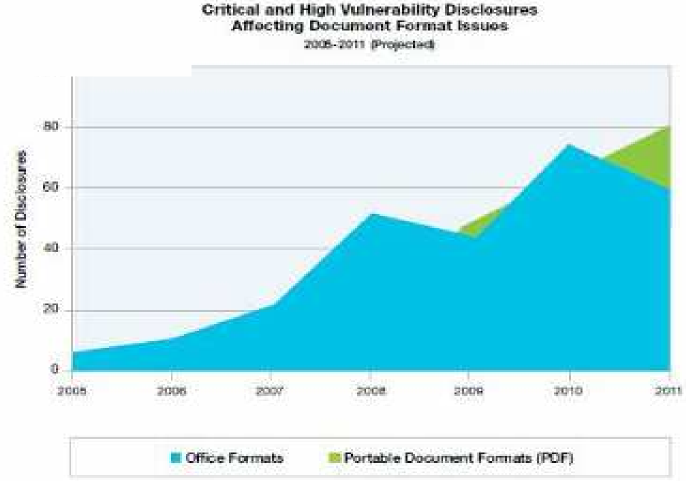


Figure 38: Critical and High Vulnerability Disclosures Affecting Document Format Issues – 2005-2011 (Projected)

Mobile OS Vulnerabilities & Exploits

- Continued interest in Mobile vulnerabilities as enterprise users bring smartphones and tablets into the work place

- Attackers finally warming to the opportunities these devices represent

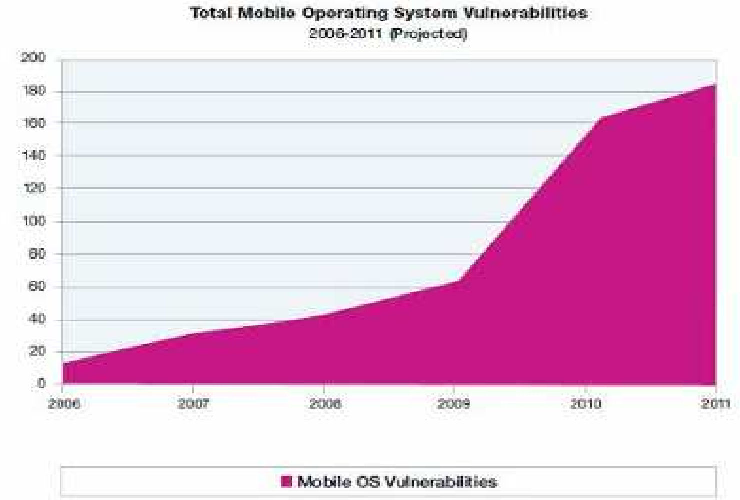


Figure 39: Total Mobile Operating System Vulnerabilities – 2006-2011 (Projected)

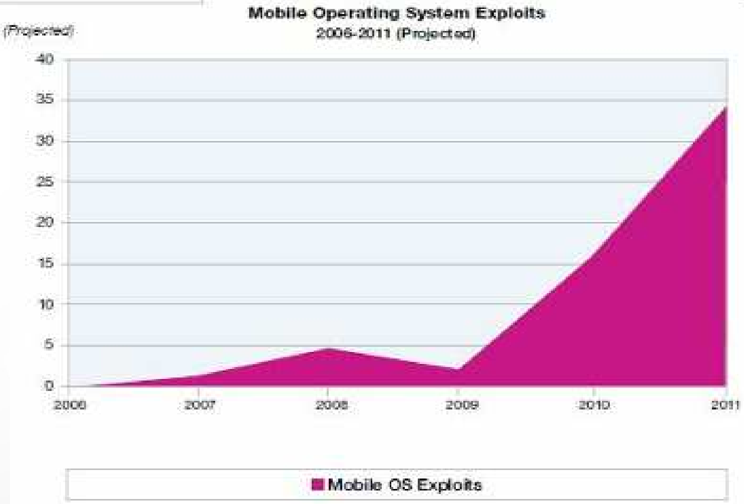


Figure 40: Mobile Operating System Exploits – 2006-2011 (Projected)

Public Exploit Disclosures

- Fewer exploits released so far this year since 2006\
- Down as a percentage of vulnerabilities as well
- Many of these exploits are being released before a vendor patch is available.
- IPS will continue to move to a more behavioral approach at detecting classes of vulnerabilities and rely less on pattern matching static signatures

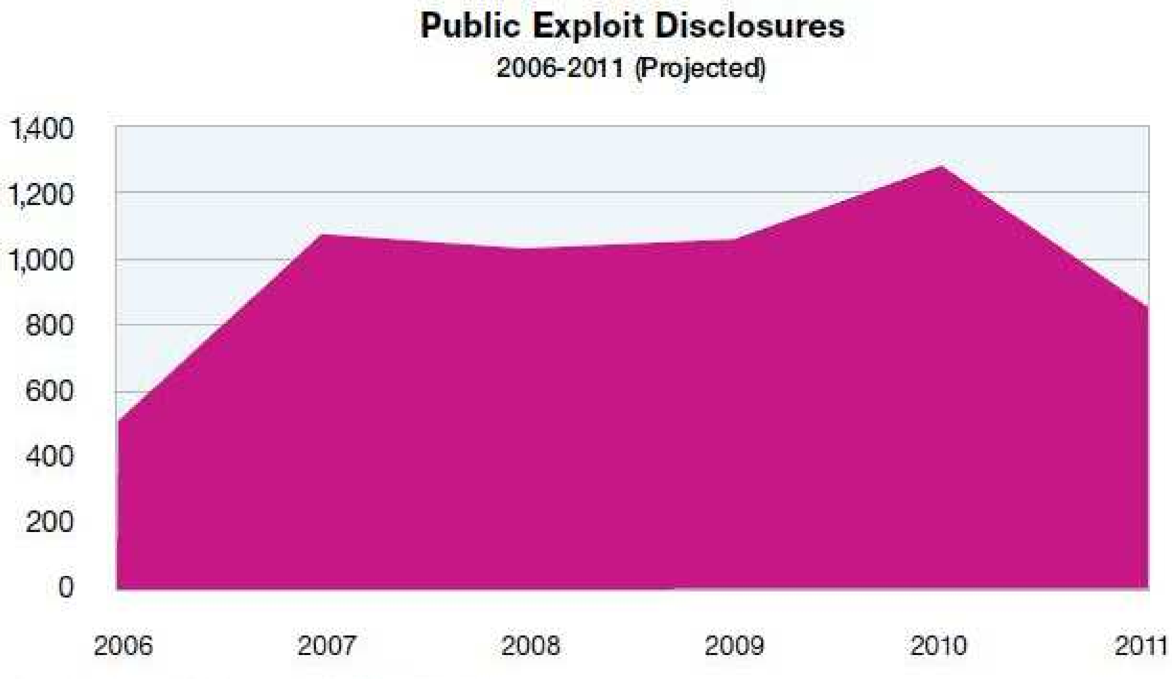
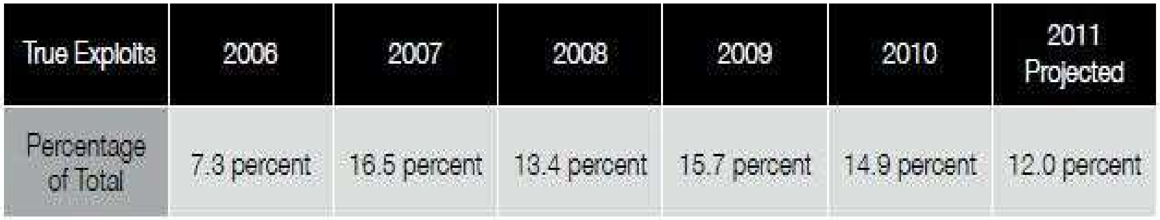


Figure 32: Public Exploit Disclosures – 2006-2011 (Projected)

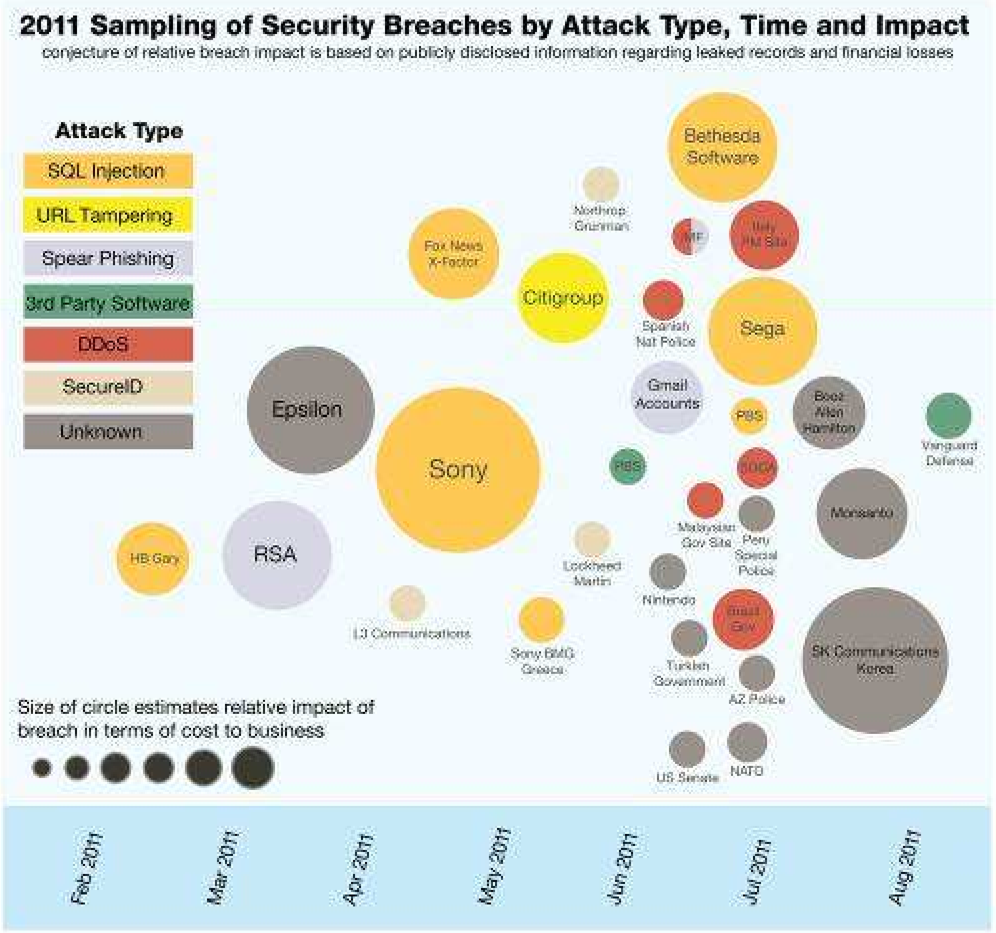


True Exploits	2006	2007	2008	2009	2010	2011 Projected
Percentage of Total	7.3 percent	16.5 percent	13.4 percent	15.7 percent	14.9 percent	12.0 percent

Table 5: Public exploit disclosures – 2006-2011 (Projected)

2011: Year of the Security Breach

- The first half of 2011 has been marked by a litany of significant, widely reported external network security breaches
- Notable not only for their frequency, but for the presumed operational competence of many of the victims.
- The boundaries of business infrastructure are being extended – and sometime obliterated – by the emergence of cloud, mobility, social business, big data and more.
- Attacks are getting more and more sophisticated.



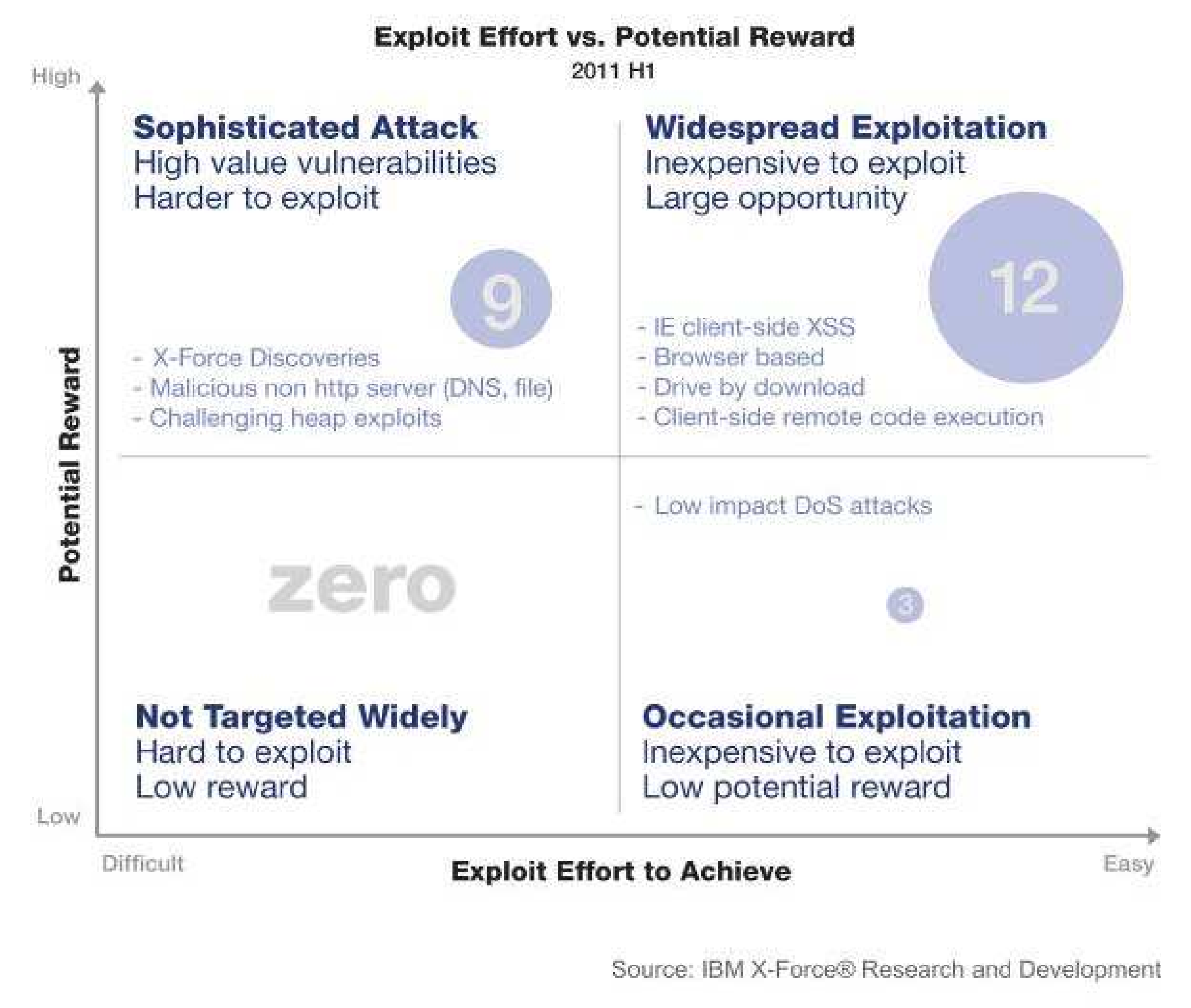
2011 Sampling of Security Breaches by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Source: IBM X-Force® Research and Development

Exploit effort vs. potential reward

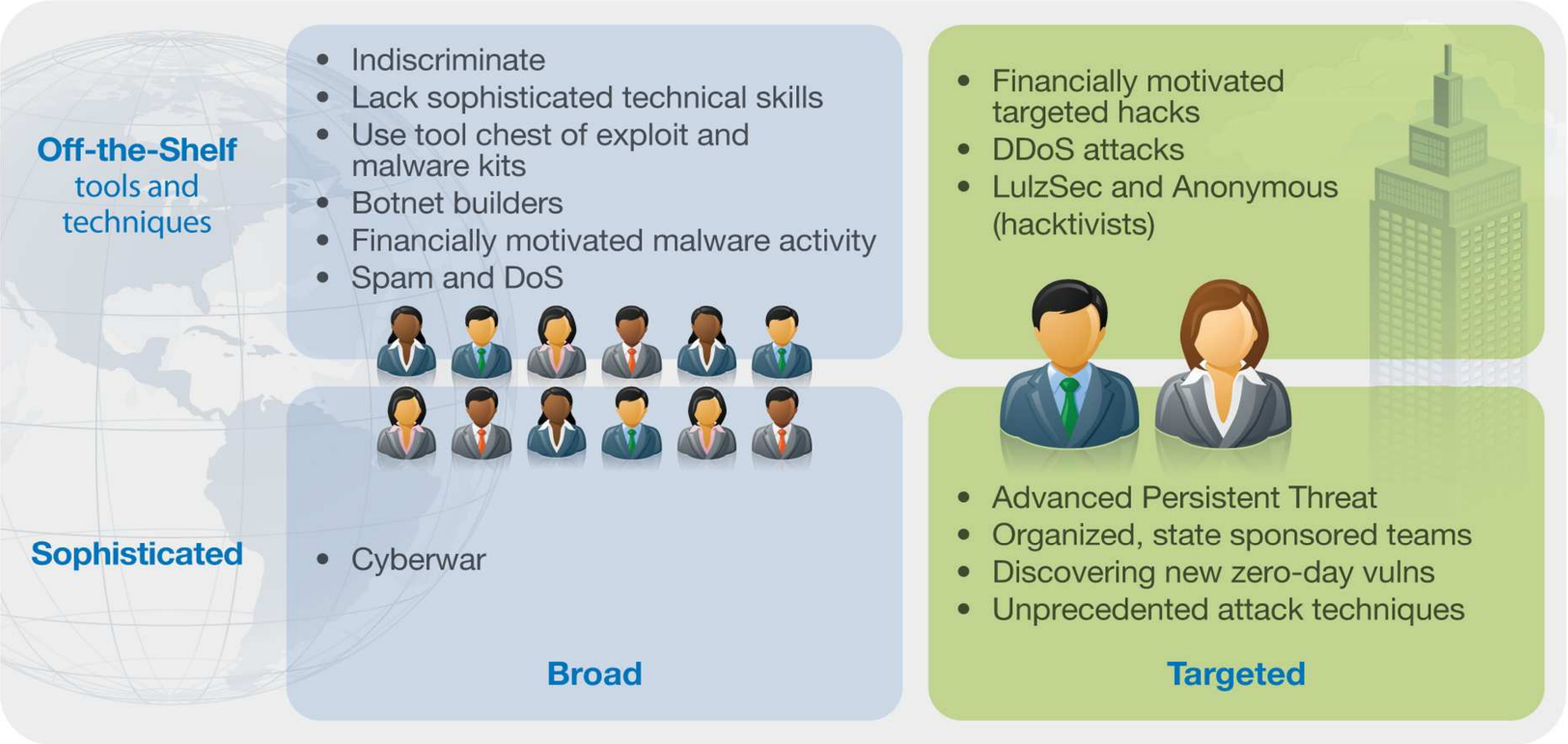
- 24 X-Force alerts and advisories in H1 2011
- 12 high value, cheap-to-exploit
  - Publicly available exploits for 9 of them
- 9 harder to exploit but high value
  - This is a higher number that in previous years



Source: IBM X-Force® Research and Development

Who is attacking our networks?

Attacker Types and Techniques 2011 H1

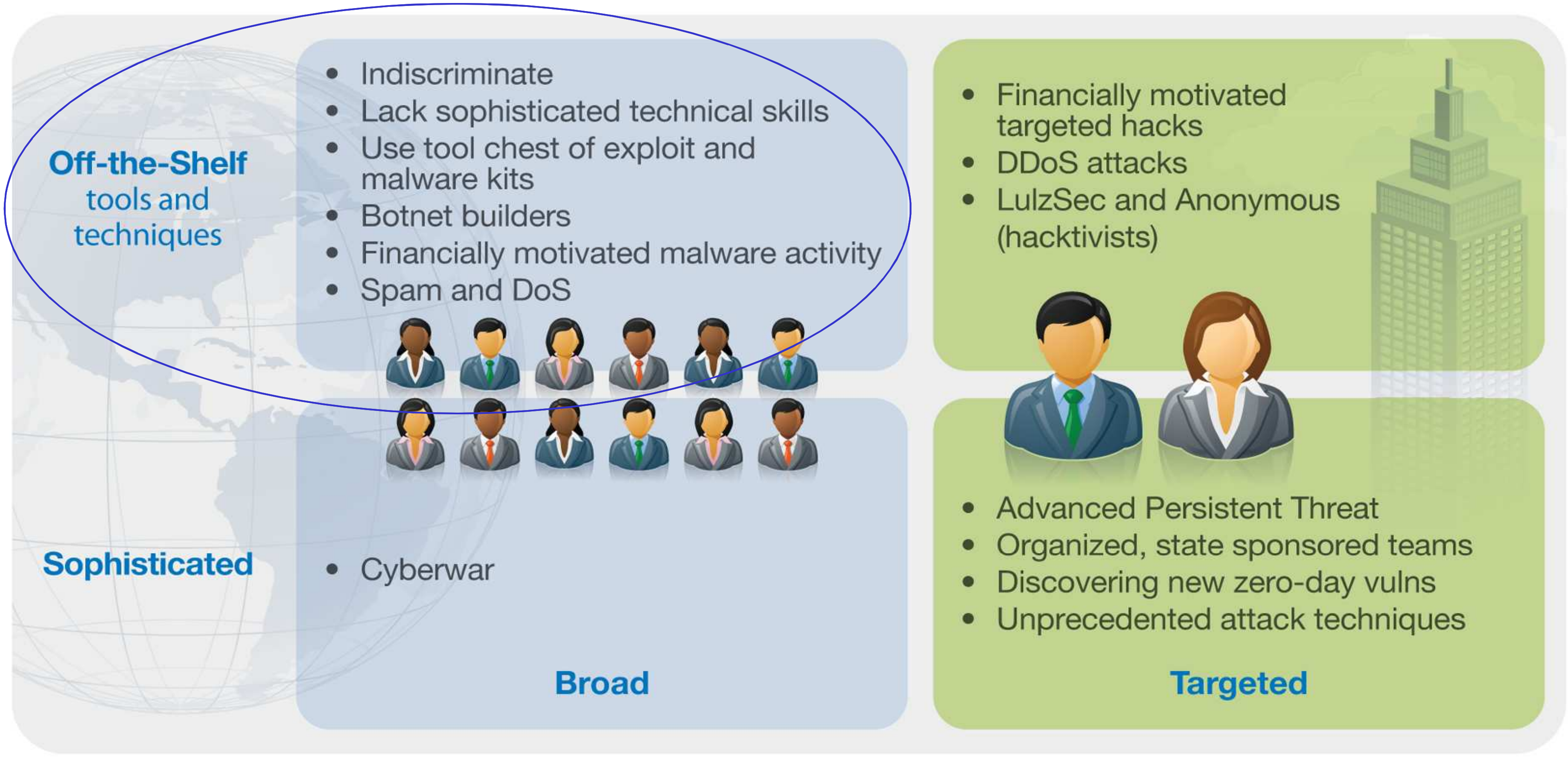


	Broad	Targeted
Off-the-Shelf tools and techniques	• Indiscriminate • Lack sophisticated technical skills • Use tool chest of exploit and malware kits • Botnet builders • Financially motivated malware activity • Spam and DoS	• Financially motivated targeted hacks • DDoS attacks • LulzSec and Anonymous (hacktivists)
Sophisticated	• Cyberwar	• Advanced Persistent Threat • Organized, state sponsored teams • Discovering new zero-day vulns • Unprecedented attack techniques

Source: IBM X-Force® Research and Development

Who is attacking our networks?

Attacker Types and Techniques 2011 H1



	Broad	Targeted
Off-the-Shelf tools and techniques	• Indiscriminate • Lack sophisticated technical skills • Use tool chest of exploit and malware kits • Botnet builders • Financially motivated malware activity • Spam and DoS	• Financially motivated targeted hacks • DDoS attacks • LulzSec and Anonymous (hacktivists)
Sophisticated	• Cyberwar	• Advanced Persistent Threat • Organized, state sponsored teams • Discovering new zero-day vulns • Unprecedented attack techniques

Source: IBM X-Force® Research and Development

High Volume Signatures

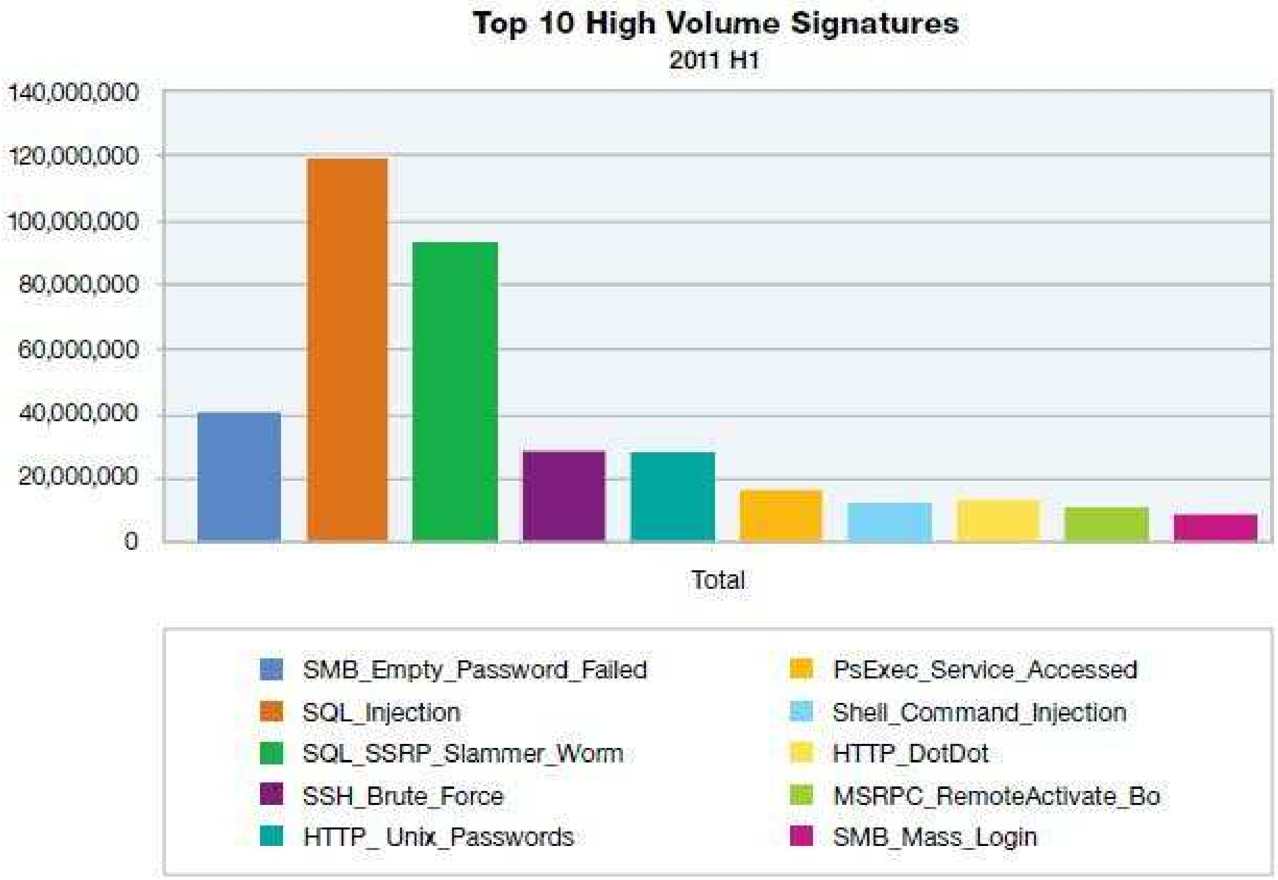


Figure 5: Top 10 High Volume Signatures – 2011 H1

SERVICE & RISK MANAGEMENT FORUM 2011

SQL Injection Attack Activity in 2011 H1

IBM

- Continues to be a favorite attack vector amongst malicious groups
- Attackers are analyzing Web applications (written in .ASP, PHP, etc.) running on the Web server in order to find SQL injection vulnerabilities they can exploit.
- In some cases, once a vulnerable Web application has been identified, attackers use search engines to automate the process of finding target sites using the vulnerable applications.

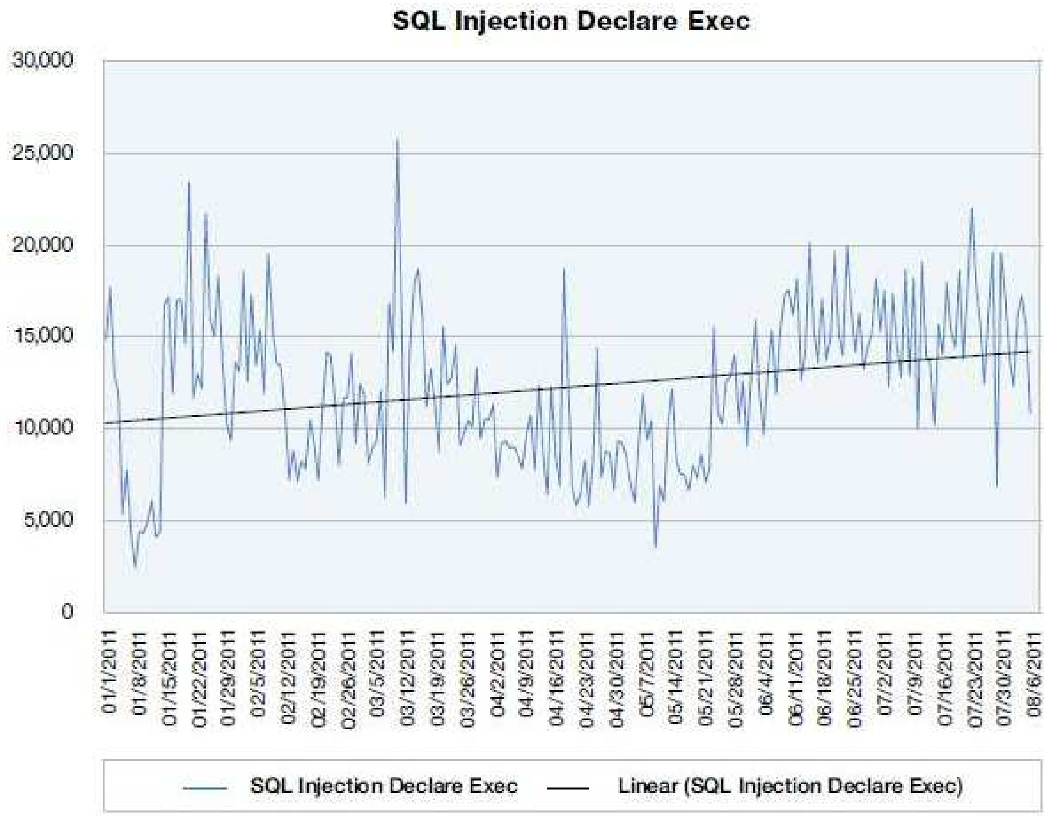
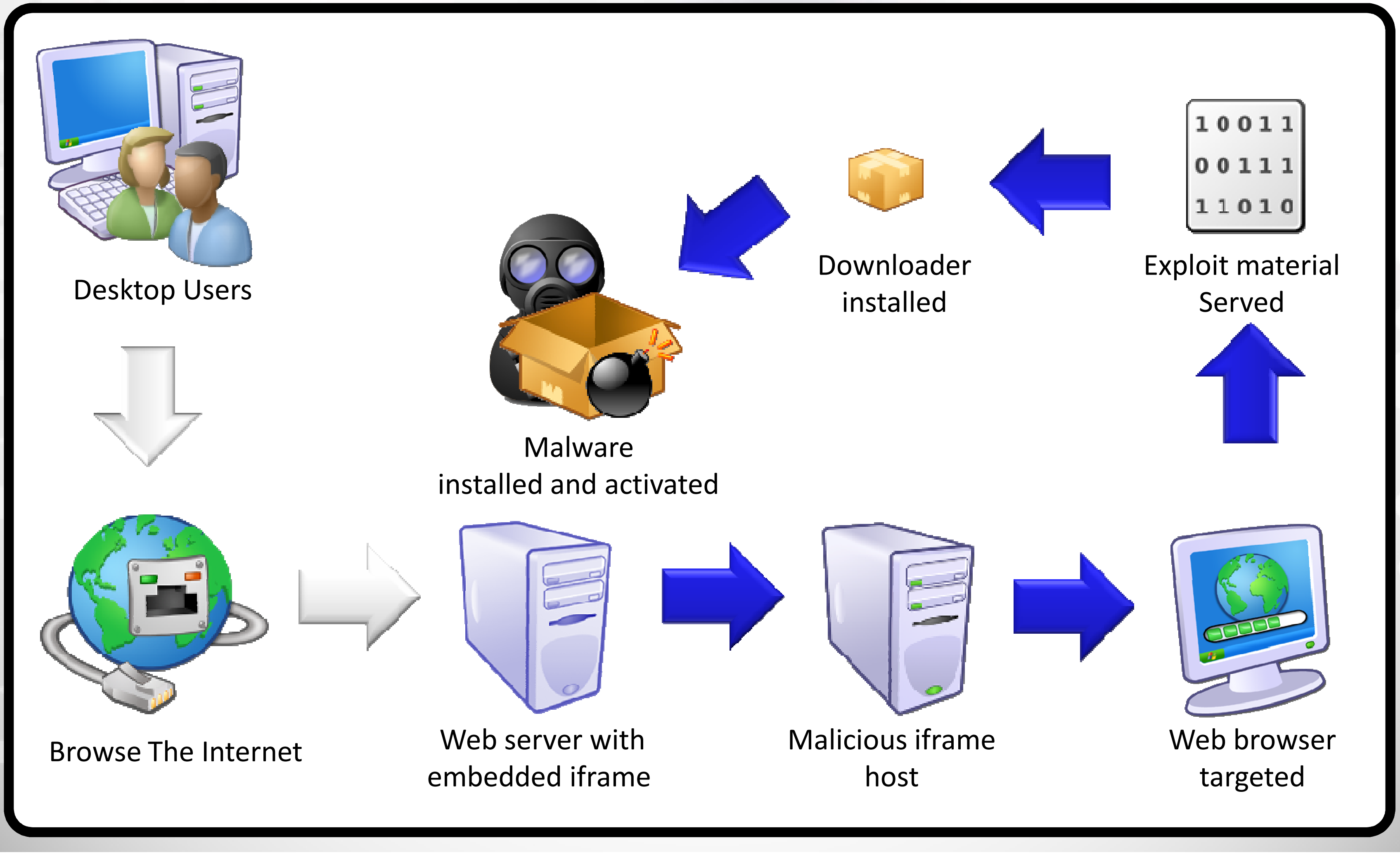


Figure 4: SQL_Injection_Declare_Exec Activity January 2011 – June 2011

The drive-by-download process



Desktop Users

Browse The Internet

Web server with embedded iframe

Malicious iframe host

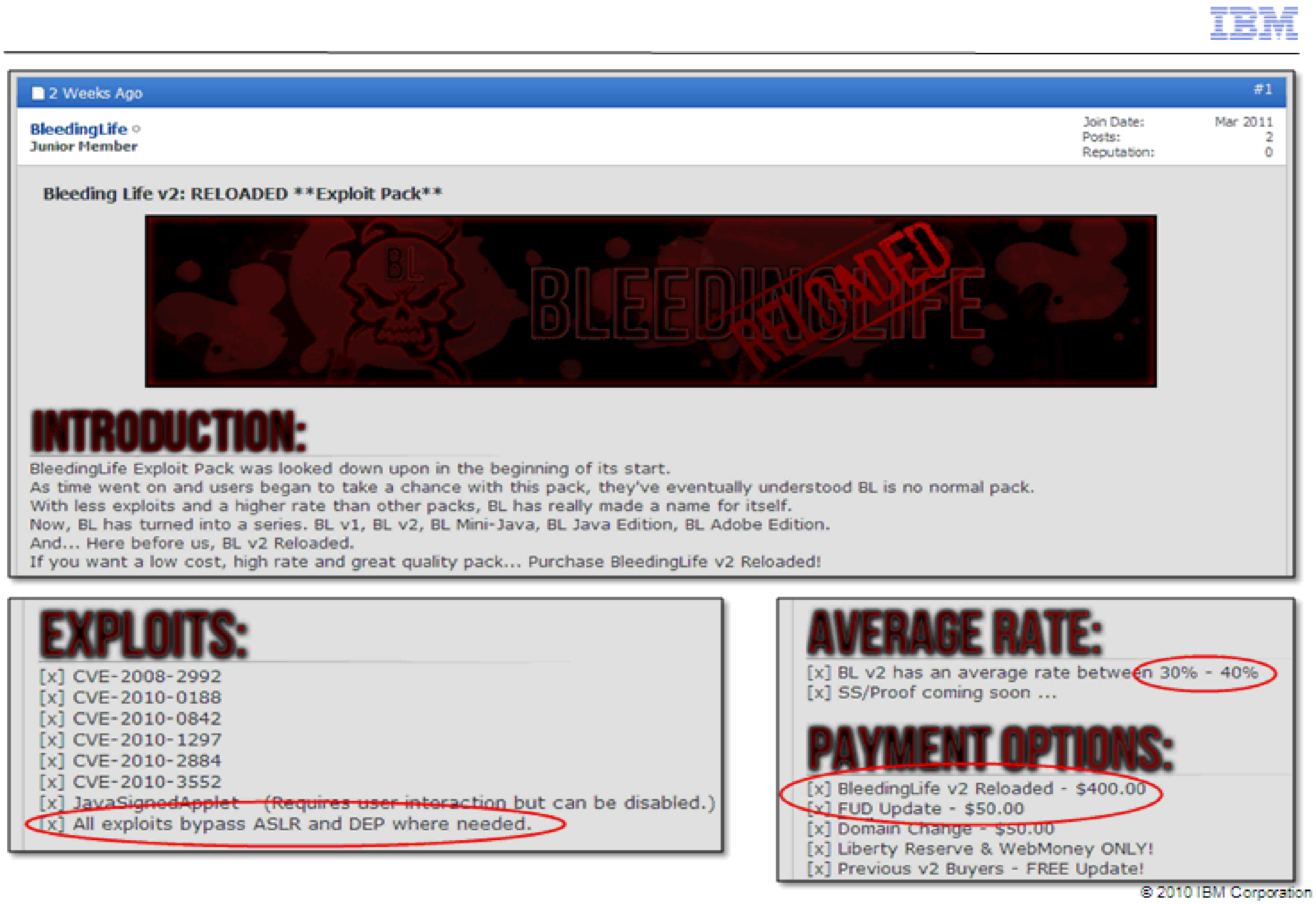
Web browser targeted

Exploit material Served

Downloader installed

Malware installed and activated

New exploit packs show up all the time



BleedingLife
Junior Member

Join Date:	Mar 2011
Posts:	2
Reputation:	0

Bleeding Life v2: RELOADED **Exploit Pack**

INTRODUCTION:

BleedingLife Exploit Pack was looked down upon in the beginning of its start.
As time went on and users began to take a chance with this pack, they've eventually understood BL is no normal pack.
With less exploits and a higher rate than other packs, BL has really made a name for itself.
Now, BL has turned into a series. BL v1, BL v2, BL Mini-Java, BL Java Edition, BL Adobe Edition.
And... Here before us, BL v2 Reloaded.
If you want a low cost, high rate and great quality pack... Purchase BleedingLife v2 Reloaded!

EXPLOITS:

[x] CVE-2008-2992
[x] CVE-2010-0188
[x] CVE-2010-0842
[x] CVE-2010-1297
[x] CVE-2010-2884
[x] CVE-2010-3552
[x] JavaSignedApplet (Requires user interaction but can be disabled.)
[x] All exploits bypass ASLR and DEP where needed.

AVERAGE RATE:

[x] BL v2 has an average rate between 30% - 40%
[x] SS/Proof coming soon ...

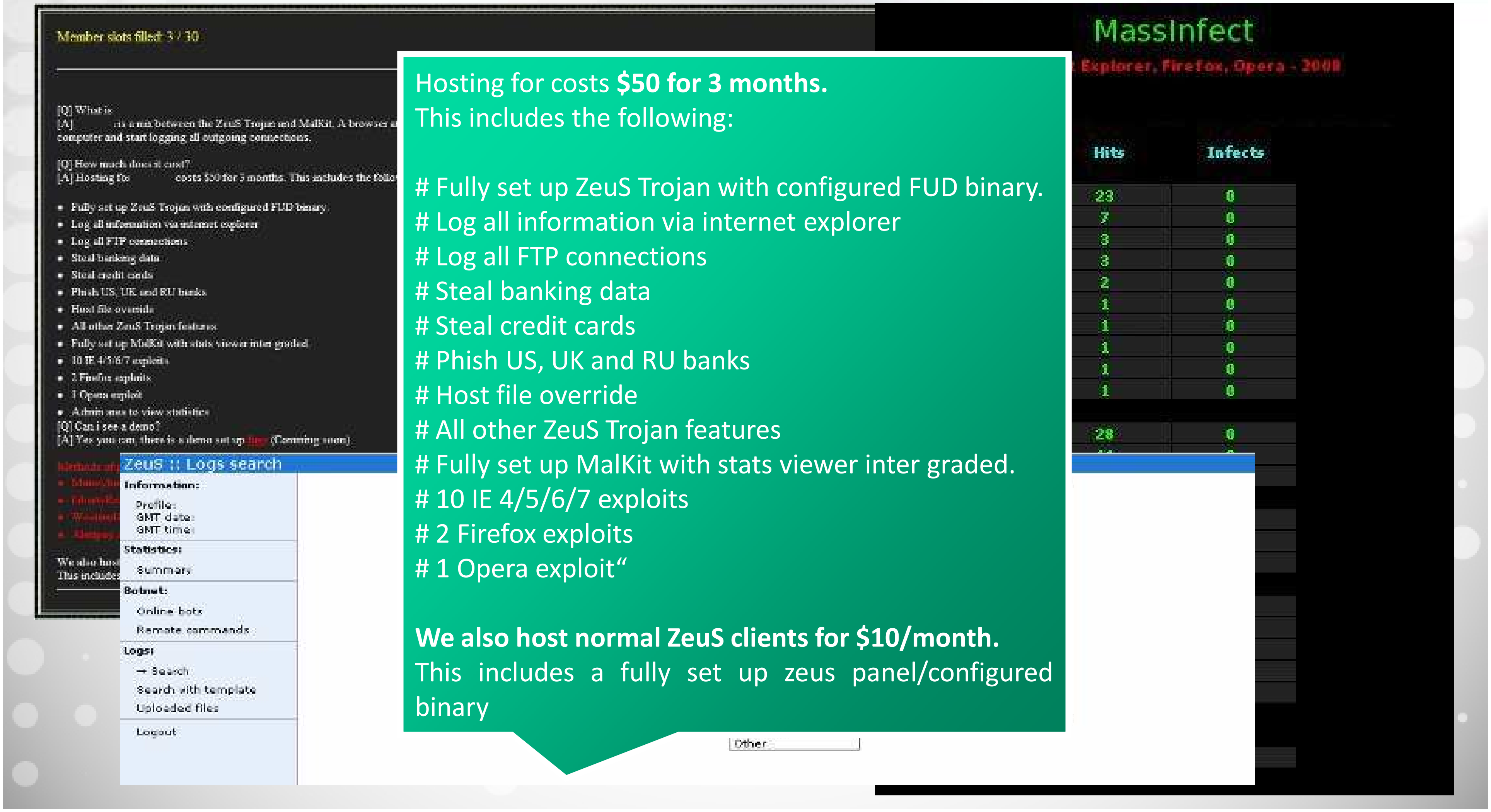
PAYMENT OPTIONS:

[x] BleedingLife v2 Reloaded - $400.00
[x] FUD Update - $50.00
[x] Domain Change - $50.00
[x] Liberty Reserve & WebMoney ONLY!
[x] Previous v2 Buyers - FREE Update!

SERVICE & RISK MANAGEMENT FORUM 2011

Zeus Crimeware Service

IBM



Member slots filled: 3 / 30

[Q] What is
[A] is a mix between the ZeuS Trojan and MalKit. A browser a
computer and start logging all outgoing connections.

[Q] How much does it cost?
[A] Hosting for costs $50 for 3 months. This includes the follo

- Fully set up ZeuS Trojan with configured FUD binary.
- Log all information via internet explorer
- Log all FTP connections
- Steal banking data
- Steal credit cards
- Phish US, UK and RU banks
- Host file override
- All other ZeuS Trojan features
- Fully set up MalKit with stats viewer inter graded.
- 10 IE 4/5/6/7 exploits
- 2 Firefox exploits
- 1 Opera exploit
- Admin area to view statistics

[Q] Can i see a demo?
[A] Yes you can, there is a demo set up here (Comming soon)

We also host
This includes

Hits	Infects
23	0
7	0
3	0
3	0
2	0
1	0
1	0
1	0
1	0
1	0
28	0

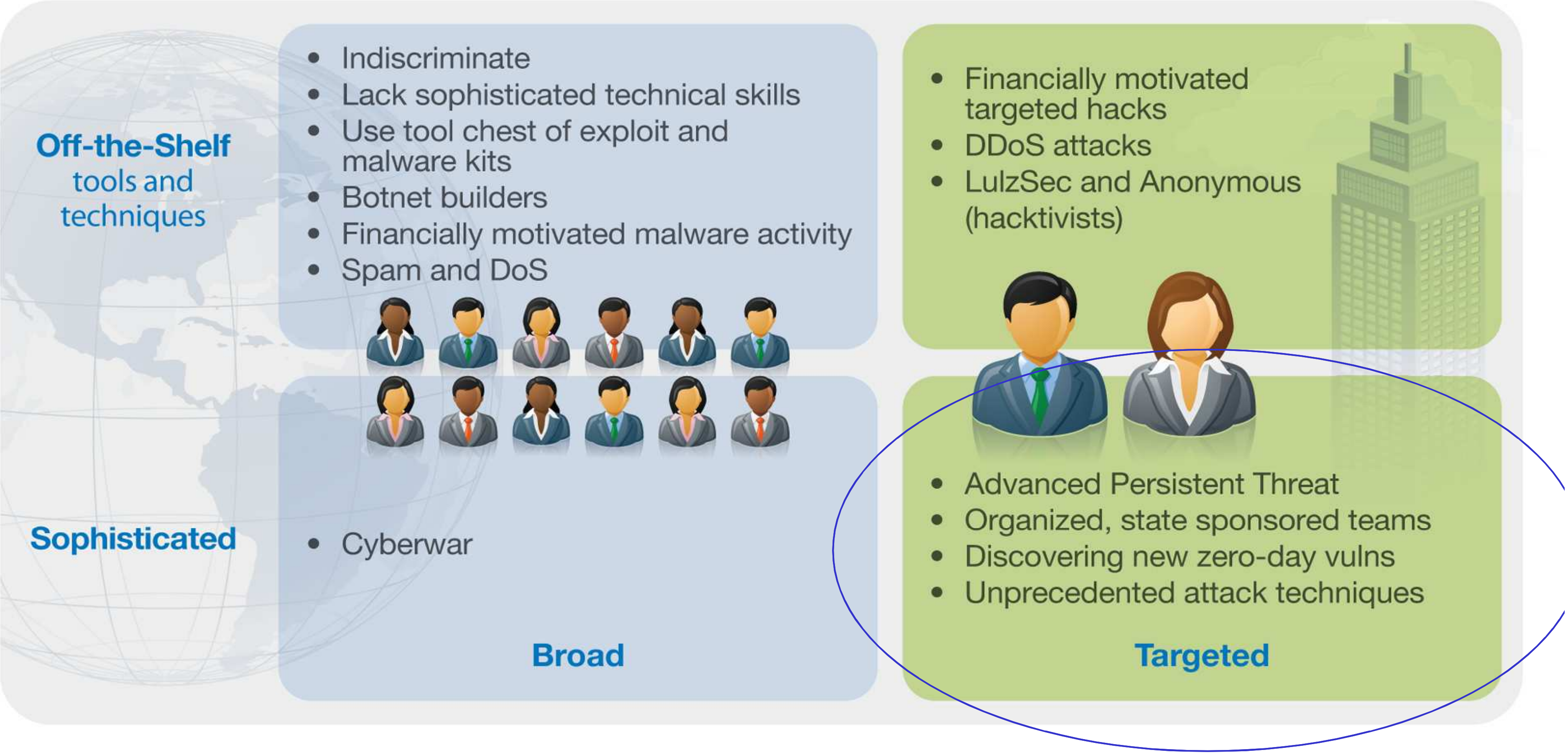
Hosting for costs **$50 for 3 months.**
This includes the following:

# Fully set up ZeuS Trojan with configured FUD binary.
# Log all information via internet explorer
# Log all FTP connections
# Steal banking data
# Steal credit cards
# Phish US, UK and RU banks
# Host file override
# All other ZeuS Trojan features
# Fully set up MalKit with stats viewer inter graded.
# 10 IE 4/5/6/7 exploits
# 2 Firefox exploits
# 1 Opera exploit“

We also host normal ZeuS clients for $10/month.
This includes a fully set up zeus panel/configured binary

Who is attacking our networks?

Attacker Types and Techniques 2011 H1

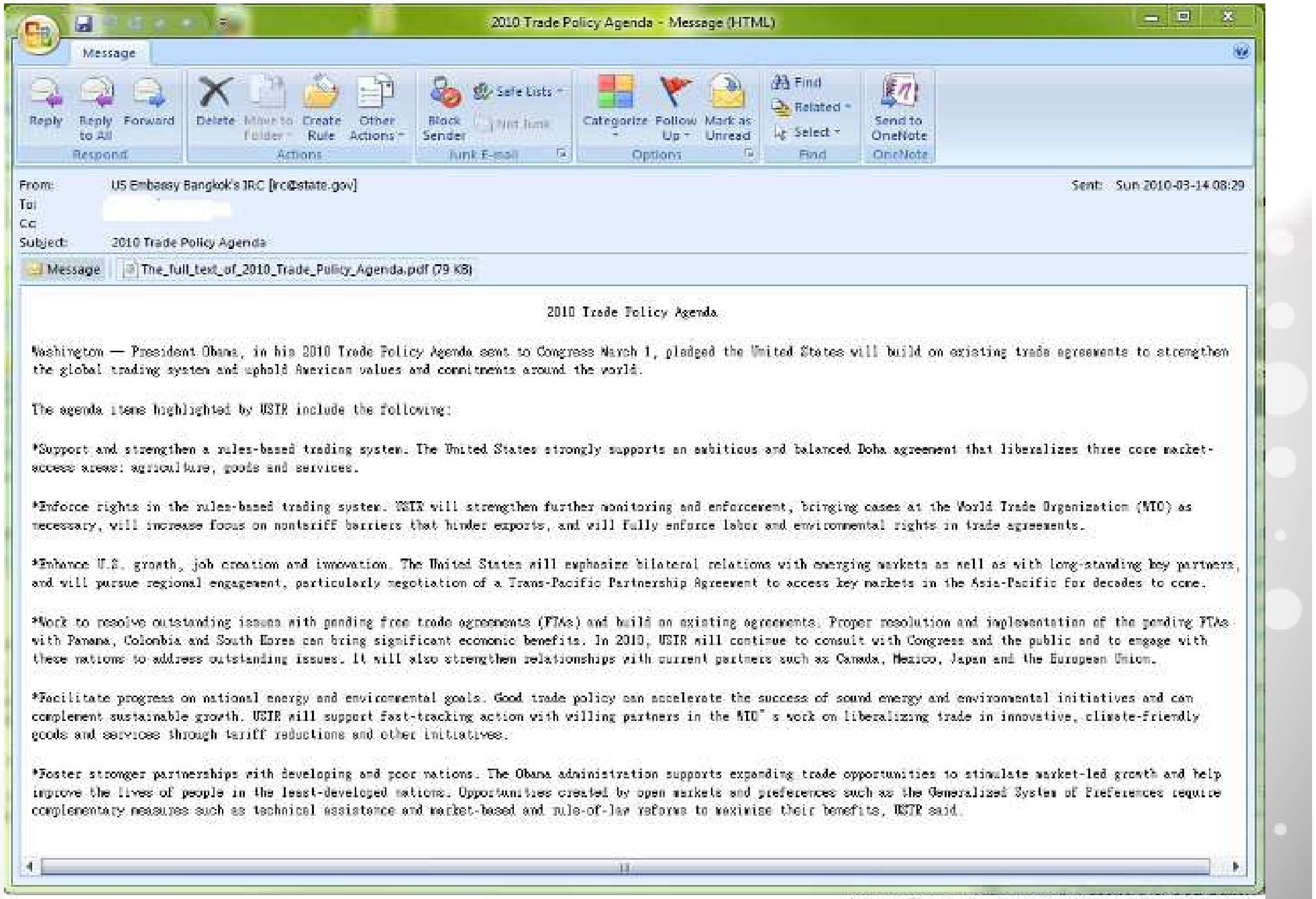


	Broad	Targeted
Off-the-Shelf tools and techniques	• Indiscriminate • Lack sophisticated technical skills • Use tool chest of exploit and malware kits • Botnet builders • Financially motivated malware activity • Spam and DoS	• Financially motivated targeted hacks • DDoS attacks • LulzSec and Anonymous (hacktivists)
Sophisticated	• Cyberwar	• Advanced Persistent Threat • Organized, state sponsored teams • Discovering new zero-day vulns • Unprecedented attack techniques

Source: IBM X-Force® Research and Development

Advanced Persistent Threat

- Example of e-mail with malicious PDF



From: US Embassy Bangkok's IRC [irc@state.gov] Sent: Sun 2010-03-14 08:29
To: [redacted]
Cc:
Subject: 2010 Trade Policy Agenda

Message The_full_text_of_2010_Trade_Policy_Agenda.pdf (79 KB)

2010 Trade Policy Agenda

Washington — President Obama, in his 2010 Trade Policy Agenda sent to Congress March 1, pledged the United States will build on existing trade agreements to strengthen the global trading system and uphold American values and commitments around the world.

The agenda items highlighted by USTR include the following:

*Support and strengthen a rules-based trading system. The United States strongly supports an ambitious and balanced Doha agreement that liberalizes three core market-access areas: agriculture, goods and services.

*Enforce rights in the rules-based trading system. USTR will strengthen further monitoring and enforcement, bringing cases at the World Trade Organization (WTO) as necessary, will increase focus on nontariff barriers that hinder exports, and will fully enforce labor and environmental rights in trade agreements.

*Enhance U.S. growth, job creation and innovation. The United States will emphasize bilateral relations with emerging markets as well as with long-standing key partners, and will pursue regional engagement, particularly negotiation of a Trans-Pacific Partnership Agreement to access key markets in the Asia-Pacific for decades to come.

*Work to resolve outstanding issues with pending free trade agreements (FTAs) and build on existing agreements. Proper resolution and implementation of the pending FTAs with Panama, Colombia and South Korea can bring significant economic benefits. In 2010, USTR will continue to consult with Congress and the public and to engage with these nations to address outstanding issues. It will also strengthen relationships with current partners such as Canada, Mexico, Japan and the European Union.

*Facilitate progress on national energy and environmental goals. Good trade policy can accelerate the success of sound energy and environmental initiatives and can complement sustainable growth. USTR will support fast-tracking action with willing partners in the WTO' s work on liberalizing trade in innovative, climate-friendly goods and services through tariff reductions and other initiatives.

*Foster stronger partnerships with developing and poor nations. The Obama administration supports expanding trade opportunities to stimulate market-led growth and help improve the lives of people in the least-developed nations. Opportunities created by open markets and preferences such as the Generalized System of Preferences require complementary measures such as technical assistance and market-based and rule-of-law reforms to maximize their benefits, USTR said.

Image Source: http://contagiodump.blogspot.com/

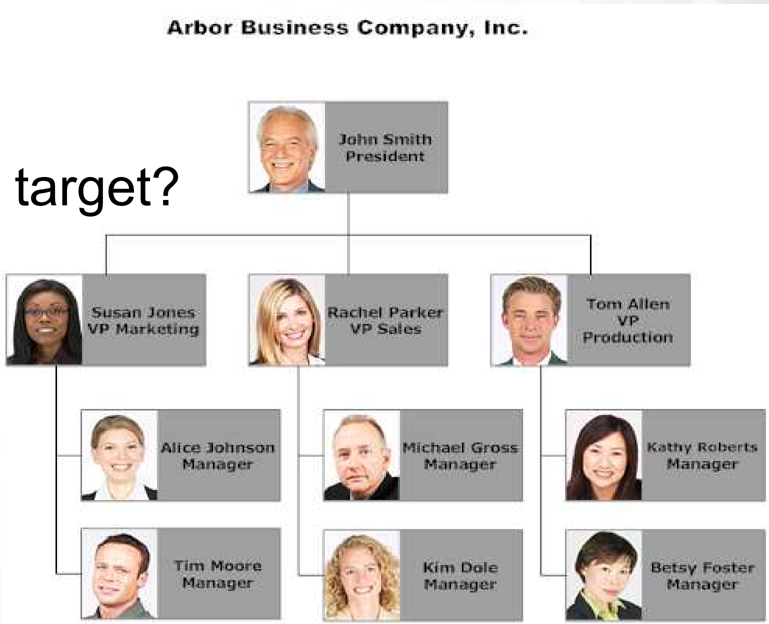
SERVICE & RISK MANAGEMENT FORUM 2011

Internet Intelligence Collection

- Scan the corporate website, Google, and Google News
  - Who works there? What are their titles?
  - Write index cards with names and titles

- Search for Linkedin, Facebook, and Twitter Profiles
  - Who do these people work with?
  - Fill in blanks in the org chart

- Who works with the information we'd like to target?
  - What is their reporting structure?
  - Who are their friends?
  - What are they interested in?
  - What is their email address?
    - At work?
    - Personal email?



Arbor Business Company, Inc.

John Smith President

Susan Jones VP Marketing

Rachel Parker VP Sales

Tom Allen VP Production

Alice Johnson Manager

Michael Gross Manager

Kathy Roberts Manager

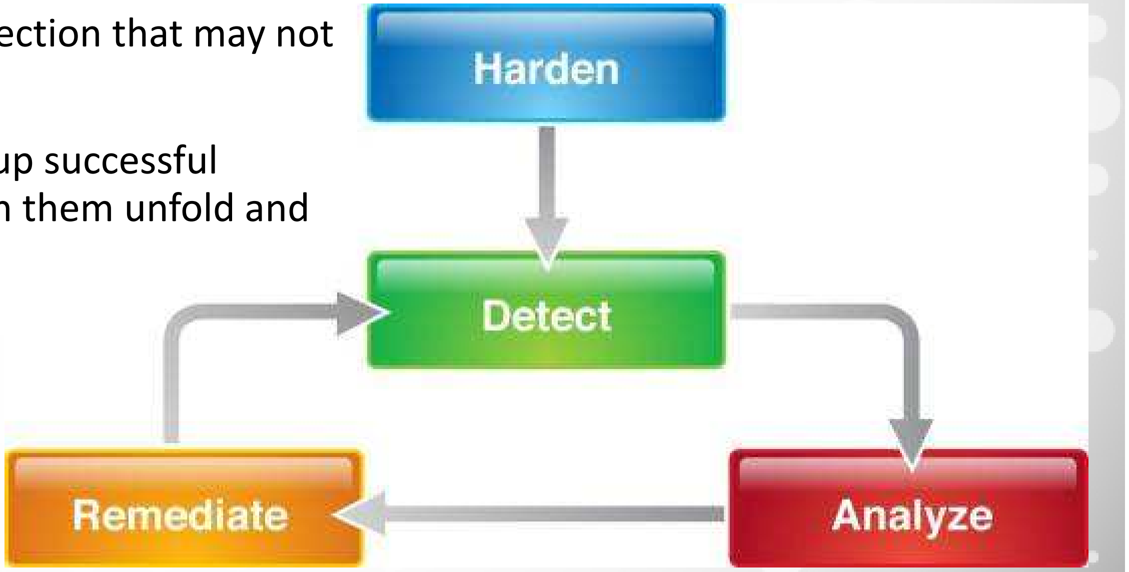
Tim Moore Manager

Kim Dole Manager

Betsy Foster Manager

Advanced Persistent Threats (APT) & Targeted Network Attacks

- Protecting a network from APT is a paradigm shift from the usual "audit and patch" approach to protecting a network from known threats.
- Sophisticated attackers may employ unknown attack techniques and 0day tools.
- Be willing to embrace approaches to detection that may not be 100 percent effective.
- You may not want to immediately clean up successful breaches. It is sometimes better to watch them unfold and collect information.


Harden

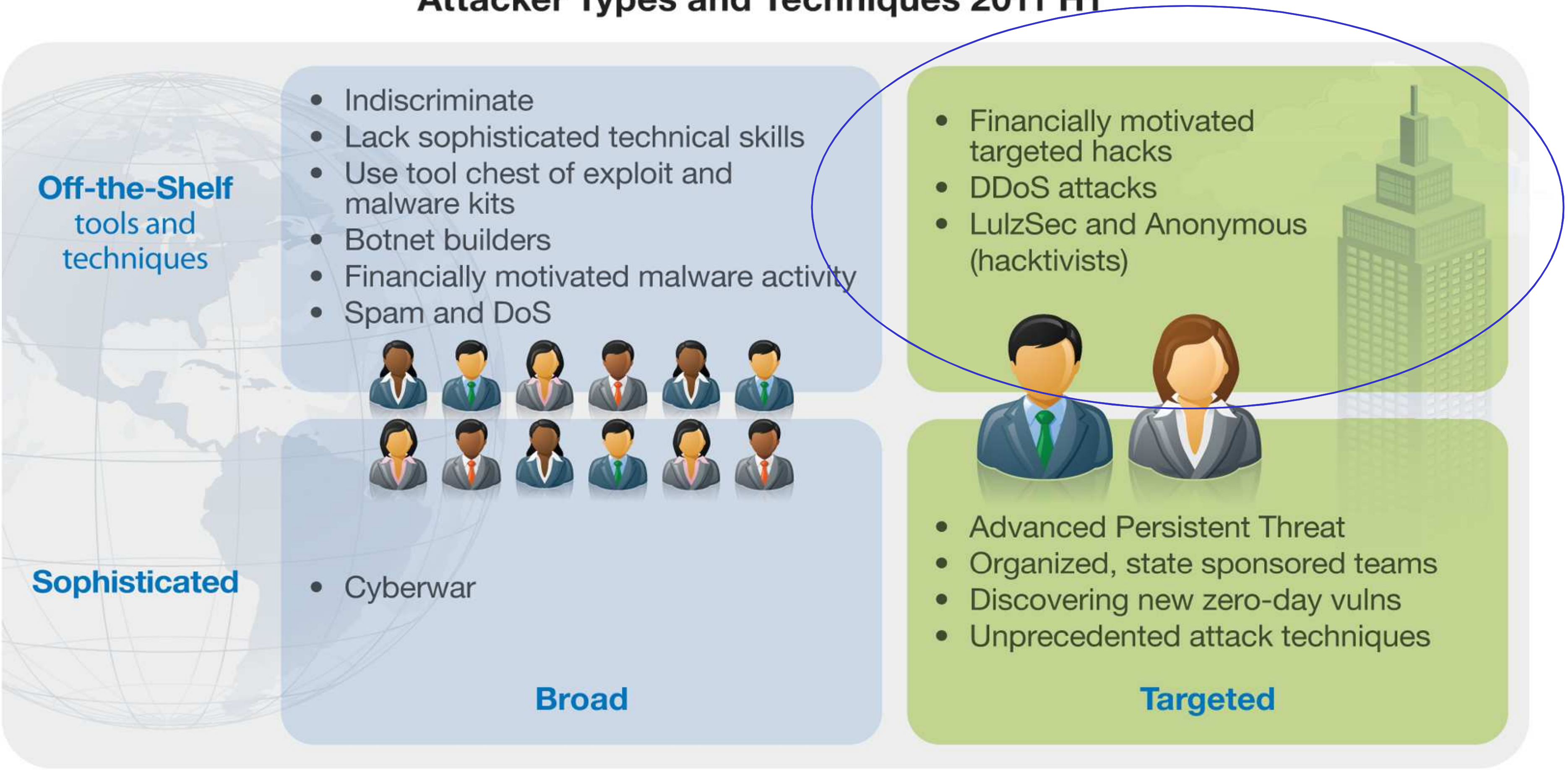
Detect

Analyze

Remediate

Who is attacking our networks?

Attacker Types and Techniques 2011 H1



Off-the-Shelf tools and techniques

- Indiscriminate
- Lack sophisticated technical skills
- Use tool chest of exploit and malware kits
- Botnet builders
- Financially motivated malware activity
- Spam and DoS

- Financially motivated targeted hacks
- DDoS attacks
- LulzSec and Anonymous (hacktivists)

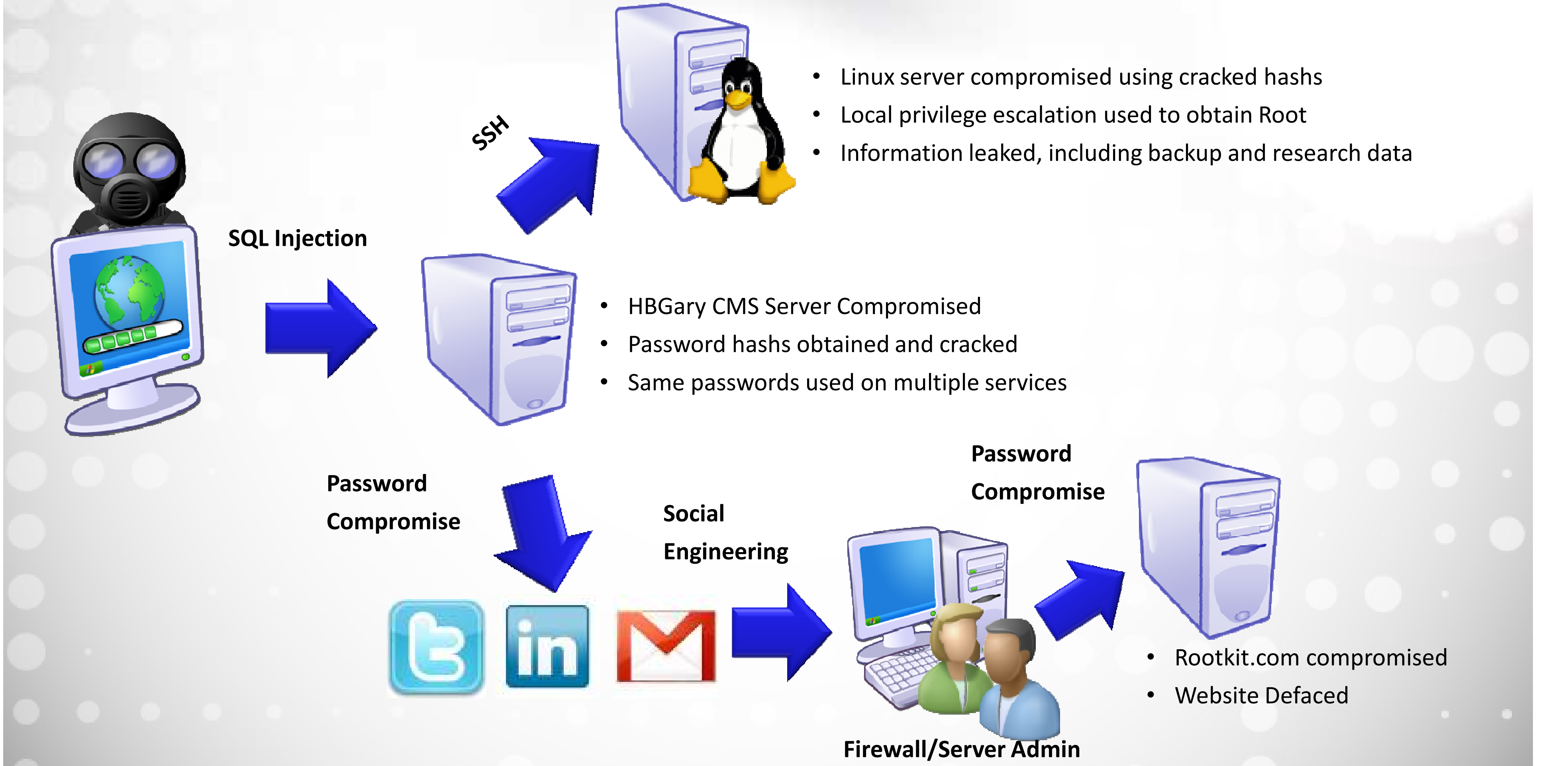
Sophisticated

- Cyberwar

- Advanced Persistent Threat
- Organized, state sponsored teams
- Discovering new zero-day vulns
- Unprecedented attack techniques

Source: IBM X-Force® Research and Development

Off the shelf attack techniques are all that it takes…



SQL Injection

SSH

- Linux server compromised using cracked hashs
- Local privilege escalation used to obtain Root
- Information leaked, including backup and research data

- HBGary CMS Server Compromised
- Password hashs obtained and cracked
- Same passwords used on multiple services

Password Compromise

Social Engineering

Password Compromise

Firewall/Server Admin

- Rootkit.com compromised
- Website Defaced

Many major operations have important security blindspots

- IBM scanned 678 websites
  - – Fortune 500 & 178 popular sites
- 40% contain client-side JavaScript vulnerabilities
- Third party code is primary culprit

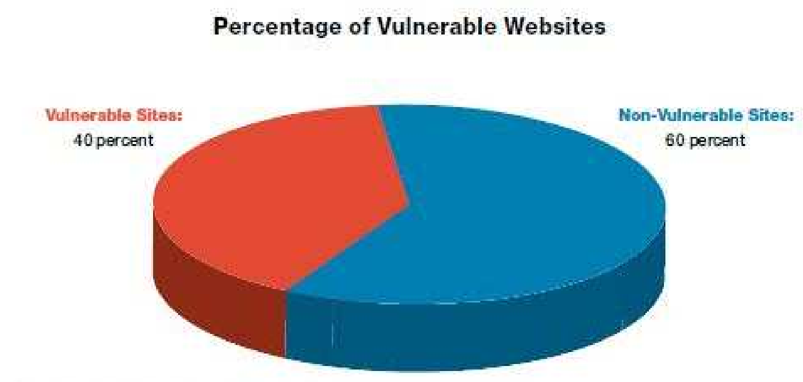


Figure 42: Percentage of Vulnerable websites

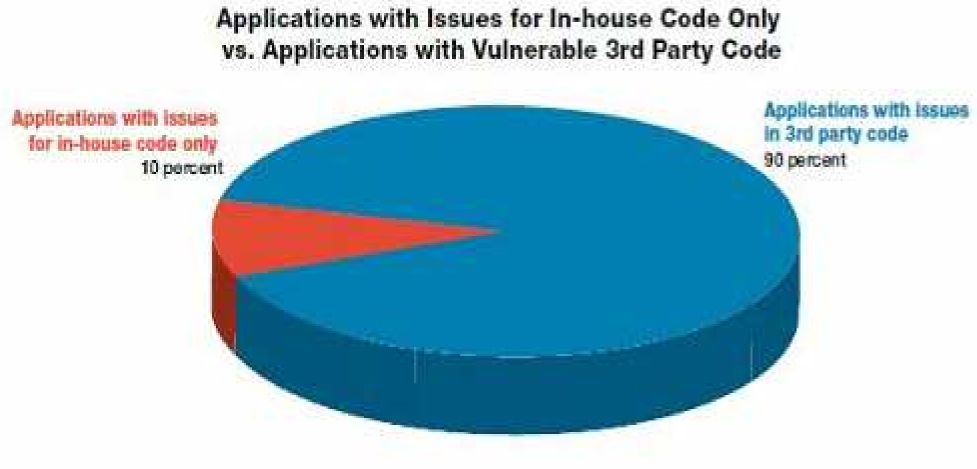


Figure 43: Applications with Issues for In-house Code Only vs. Applications with Vulnerable 3rd Party Code

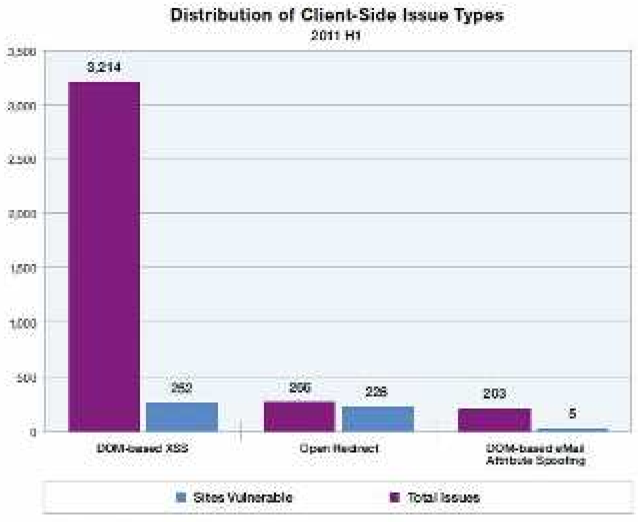
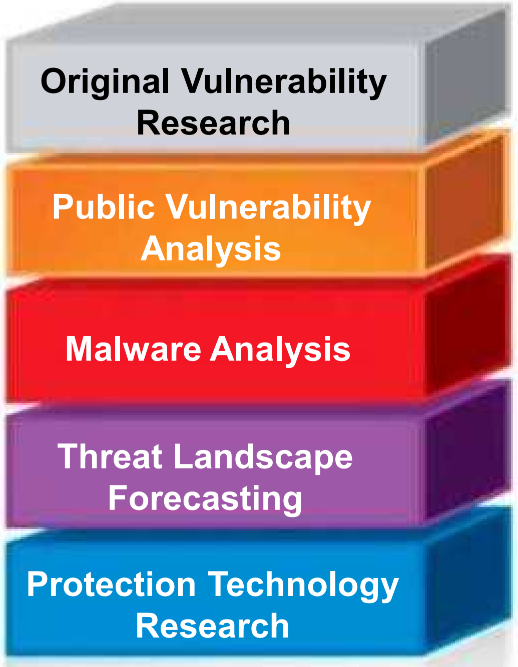


Figure 44: Distribution of Client-Side Issue Types – 2011 H1

SERVICE & RISK MANAGEMENT FORUM 2011

The Value of Security Research

Research → Technology → Solutions


Original Vulnerability Research
Public Vulnerability Analysis
Malware Analysis
Threat Landscape Forecasting
Protection Technology Research

X-Force Protection Engines

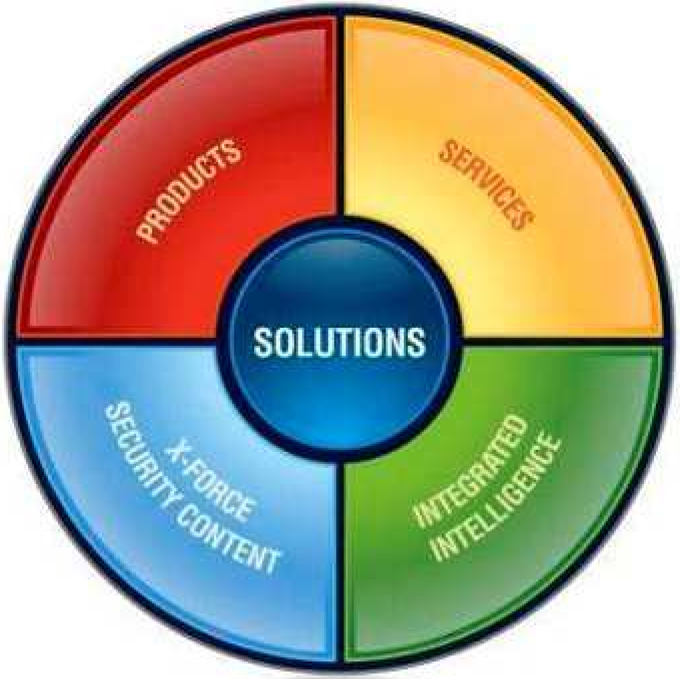
- Extensions to existing engines
- New protection engine creation

X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing



Only IBM Security is backed by the IBM X-Force®

Drivers Influencing IPS Evolution

- **IPv6** – Deployments of IPv6 networks (and heterogeneous IPv4+IPv6) are picking up speed.
- **Vulnerabilities and Exploits** – The number of vulnerabilities and public exploits being disclosed is increasing each year.
  - IPS must use more behavioral and anomaly detection and less pattern matching.
- **Obfuscation** – Increases in the obfuscated web pages and files.
  - Obfuscation detection will continue to evolve in IPS.
- **Evasions** – New evasion techniques will continue to be discovered
- **Applications** – The number of web applications will continue to increase
  - Application identification, control (allow/deny), and QoS will be important.
- **Encryption** – Use of SSL and other encryption methods will continue to be used more by both good and bad guys.
  - Inspection of encrypted packets will become standard
- **Compound Documents** and **Container Files** – Increasingly used in attacks.
  - The need to look “inside” of PDF files and Office documents

Critical Factors for IPS

Performance – 20 gigs and beyond.
- As networks grow larger and faster there will be a need for more speed
- As more technologies converge with IPS more bandwidth will be needed

Encryption – The use of SSL and encryption is increasing among both the good guys and the bad guys
- SSL inspection in IPS is going to be standard

Flexibility – A default configuration is rarely useful.
- Every network is different. Flexibility in tuning is critical in making an IPS usable.

Behavioral Inspection – Beyond Pattern Matching.
- Behavioral deep packet inspection protocol decodes will continue to be more important.
- Attackers are hiding their exploit code inside of compound files and container files, making simple pattern matching IPS techniques less useful.

Web Applications – We certainly see the volume of web applications increasing.
- Applications are using HTTP/HTTPS. Being able to identify and allow/deny those applications will is important today, and will be more important in the years to come.

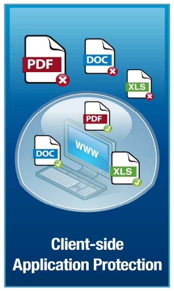
Introducing IBM Security Network IPS

Key Pain Points

- Balance security and performance of business critical applications
- Address changing threats with limited expertise, resources, and budget
- Reduce cost and complexity of security infrastructure
- Larger organizations require security at network core

IBM Security Network Intrusion Prevention GX7800 is the newest addition to IBM's market-leading portfolio of Intrusion Prevention security appliances

Virtual Patch



Client-side Application Protection

Web Application Protection

Threat Detection and Prevention

Data Security

Application Control

Core Capabilities

Beyond traditional network IPS to deliver comprehensive security including:

- •Web application protection
- •Protection from client-side attacks
- •Data Loss Prevention (DLP)
- •Application control
- •Virtual Patch technology

Unmatched Performance delivering 20Gbps+ of throughput and 10GbE connectivity without compromising breadth and depth of security

Evolving protection powered by world renowned X-Force research to stay "ahead of the threat"

Reduced cost and complexity through consolidation of point solutions and integrations with other security tools

SERVICE & RISK MANAGEMENT FORUM 2011

IBM Security Protocol Analysis Module Addressing Today's Evolving Threats

IBM

How it Works

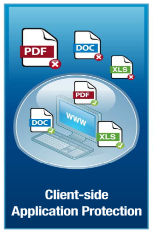
- Deep inspection of network traffic
- Identifies & analyzes >200 network and application layer protocols and data file formats

What it Prevents

- Worms
- Spyware
- P2P
- DoS/DDoS
- Cross-site Scripting
- SQL Injection
- Buffer Overflow
- Web Directory Traversal

Protocol Analysis Module (PAM)

Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response Analysis
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
Proventia Content Analyzer	Injection Logic Engine



SERVICE & RISK MANAGEMENT FORUM 2011

Intrusion Prevention Solutions -that Fit your Needs

IBM

- Block threats before they impact your organization
- Uncompromising security backed by X-Force®
- Inspected throughput from 200 Mbps to 20Gbps+
- Protection for up to 8 network segments
- Scale from remote offices to the network core

IBM Security Network IPS Models

	Remote	Perimeter			Core				
Model	GX4004-200	GX4004	GX5008	GX5108	GX5208	NEW GX7412-5	NEW GX7412-10	NEW GX7412	NEW GX7800
Inspected Throughput	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Protected Segments	2	2	4	4	4	8	8	8	4

The Value of Security Research

Without security researchers we would always be one step *behind* the threat…

Ahead of the Threat – In order to stay one step ahead of the bad guys, you have to understand the vulnerabilities that are being exploited.

Bugs – Security researchers often find bugs before the bad guys do, allowing them to provide protection to customers before vendors have time to deploy a patch.

Understanding the Threat Landscape – By studying the different attack techniques and obfuscation techniques that the bad guys are using – vendors ultimately use this research to create protections that can be less evadable, more apt to detect Botnets and Malware, APT style attack patterns, and new attack techniques.

Thank You

For More IBM X-Force Security Leadership

X-Force Trend Reports

The IBM X-Force Trend & Risk Reports provide statistical information about all aspects of threats that affect Internet security,. Find out more at http://www-935.ibm.com/services/us/iss/xforce/trendreports/

X-Force Security Alerts and Advisories

Only IBM X-Force can deliver preemptive security due to our unwavering commitment to research and development and 24/7 global attack monitoring. Find out more at http://xforce.iss.net/

X-Force Blogs and Feeds

For a real-time update of Alerts, Advisories, and other security issues, subscribe to the X-Force RSS feeds. You can subscribe to the X-Force alerts and advisories feed at http://iss.net/rss.php or the Frequency X Blog at http://blogs.iss.net/rss.php

Thank you for your time today.

TBD

For more information:

- IBM X-Force Page on IBM.com: www.ibm.com/security/x-force
- IBM X-Force Sales Kit on Software Group Sellers Workplace: http://w3-103.ibm.com/software/xl/portal/content?synKey=C850820I16680T38#overview
- IBM Security Solutions Main Page on IBM.com: http://www-01.ibm.com/software/tivoli/solutions/threat-mitigation/?tactic=featuredhome
- IBM Security Sellers Blog: http://w3.ibm.com/connections/blogs/ISS_Sellers_Blog/?lang=en
- If you need help with an issue that is impacting a security sale, contact the cross-brand IBM security war room at secwarrm@us.ibm.com
- Subscribe to X-Force Monthly Newsletter: Send email to rjwissin@us.ibm.com