Trends in the Threat Landscape

Joshua Rosenthal, CISSP
Year in Review

- Data Theft
- Targeted Attacks
- Exploit Kits

Common Theme – Web Component
Malware Adoption Lifecycle

- **2% Innovators**: $100K+ APT - 2011
- **14% Early Adopters**: $1,000 Copycat - 2012
- **34% Early Majority**: $25 Kit - 2012
- **34% Late Majority**: Ineffective - 2013
- **14% Late Adopters**: Ineffective - 2013
- **2% Laggards**: Ineffective - 2013

© 2012 Websense, Inc. CONFIDENTIAL
Time of Exposure

88% of Time Vulnerable
Applying Patches Immediately – 104 days of Exposure

4 Month Period with 6 Vulnerabilities
New Defenses Required

“Signature based tools (anti-virus, firewalls, and intrusion prevention) are only effective against 30-50% of current security threats. Moreover, customers expect the effectiveness of signature-based security to continue to decline rapidly.”

IDC Threat Intelligence Update, 14-Feb-2012
Web Threat Stages

Lure
Redirect
Exploit Kit
Dropper File
Call-Home
Data Theft
Web Threat Stages

Lure

SEO Poisoning
Like-Jacking
YouTube Scams
Twitter Scams
FREE Gift Offers
MUST SEE Videos
Celebrity Events
Natural Disasters
Targeted Email
Alert/Event Email

Social Profiling
Fake Surveys
Fake Facebook Photos
Deaths & World News
Profile Creeper/Watcher
Ex-Girlfriend Topics
Typo-Squatting Hives
Hidden Camera
Guestbook Entries
Blog Postings...

Email Lures:
1. Orders
2. Tickets
3. Delivery
4. Test
5. Tax Refund
Web Threat Stages

Redirect

iFrame Injection
SQL Injection
Wall-Postings
Malvertising
Obfuscation Techniques
Javascript
Active Content
Dynamic Variables
- Twitter ratings
Fake CA Certificates
Fake Plug-ins
Web Threat Stages

Exploit Kit

Blackhole Exploit Kit
- Encrypted, Custom
- Java OBE + JAR files

Neosploit Exploit Kit
- ActiveX, Adobe Reader

Missing Software Patches

Zero-day Vulnerabilities

Adobe & Java Exploits

IE, Firefox, Chrome, Opera

TrueType Font (Duqu)

WordPress TimThumb
Web Threat Stages

Dropper
File

Rogue AV
Mac Defender
Information Harvesting
Fake Apps & Surveys (CPA)
Browser Plug-ins
Malware Droppers
Trojan Droppers
- Zeus/Zbot Trojan
Mal-PDF
Web Threat Stages

Containment is the New Defense
What Defenses Analyze:
- Call-home Requests
- Dynamic DNS
- Data Theft & Loss
- Behavioral (Drip) DLP
- Stolen Password Files
- Custom Encrypted Files
- Destination Awareness
- Geo-Location
Web Threat Analysis

Lure
Redirect
Exploit Kit
Dropper File
Call-Home
Data Theft

ThreatSeeker Network
Uniting over 850M research points
Analyzing 3-5B requests per day
ThreatSeeker Network

Largest Security Intelligence Network
3-5 billion requests per day
850+ million end points

10+ million emails per hour
2.5 billion URLs per day

400+ million sites per day
1 billion pieces of content per day

Threat Detection/Probes
Real-Time Security Updates
Shared Analytics/Feedback

URL and Security Database

© 2012 Websense, Inc. CONFIDENTIAL
ACE (Advanced Classification Engine)
What is your best security solution?

- AV?
- Firewall?
5% of Connections are Encrypted

81% are HTTP GET
19% are HTTP POST

Top5 Countries:
- United States 50.11%
- Canada 13.22%
- Germany 5.38%
- Netherlands 4.90%
- China 4.14%
Top 5 Countries Hosting Malware:
• United States – 36.3%
• Russia – 14.7%
• France – 13.2%
• Germany – 7.0%
• Singapore – 3.4%

Top 5 Countries Hosting Phishing:
• United States – 59.9%
• Canada – 9.8%
• Egypt – 6.8%
• Germany – 2.3%
• United Kingdom – 1.8%
Compromised Hosts

Percentage of Malicious Web Sites hosted on Compromised Hosts

62.4%
Email Threat Profile

- 76% Spam
- 92% Spam w/URL
- 1.62% Phishing Spam
- 0.4% Malware/Email

ThreatSeeker threat protection before AntiMalware detection:

3.46 million instances
Email Threat Profile

Top Five Categories:

1. Information Technology
2. Business and Economy
3. Shopping
4. Financial Data and Services
5. Travel
Top Five Security Categories:

1. Malicious Web Sites
2. Phishing and Other Frauds
3. Malicious Embedded iFrame
4. Potentially Unwanted Software
5. Bot Networks
Facebook Profile

42.8% Streaming Media
7.8%  News and Media
4.1%  Entertainment
3.6%  Blogs & Personal Sites
3.6%  Information Technology
3.3%  Shopping
2.9%  Social Networking
2.1%  Malicious (All Types*)
1.7%  Business & Economy
1.4%  Sports
1.2%  Society & Lifestyles
1.2%  Personal Network Storage & Backup
1.1%  Games
Full 2012 Threat Report available from our website....
More depth on web, email, data and mobile security
Predictions for 2012

1. Social Media accounts and targeted attacks
2. Mobile attacks
3. SSL traffic creating blind spot
4. Containment is new prevention
5. London Olympics, US Presidential Election
That’s it!