

Malware Presentation v0.2

Malware includes [computer viruses](#), [ransomware](#), [worms](#), [trojan horses](#), [rootkits](#), [keyloggers](#), [spyware](#), [adware](#), malicious [BHOs](#) and other malicious programs. According to [Microsoft Malware Protection Center](#), the majority of active malware threats are usually worms or trojans rather than viruses.

Introduction


- Malware (have description in quotes)
 1. Overall Topic that is near and unfortunately dear to my heart.
 2. Share story.
- 1. New Generation of Threats and Countermeasures
 - a. Statistics and select highlight interesting details around the evolution of Malware threats and defenses.
- 2. Real World Forensics Case
 - a. And by that I mean the Pilot at CIBC where we did real production reviews of 3 products, Net Forensics by RSA, FireEye and Damballa.
 - b. To assess the value and effectiveness of Malware Analysis technologies.
- 3. Project Team Listing
 - a. Just wanted to highlight the team here and note that the material here barely scratches the surface of all the work being done.

New Gen Threats and New Gen Countermeasures

1. Some Numbers and Trends
 - a. [Microsoft Volume 13 June 2012 Report](#)
 - i. Figure 7 - Browser Vulnerabilities Upswing while Operating System Downswing
 - ii. Figure 9 - Exploites HTML/JavaScript, Java, Documents
 - b. [Symantec Report December 2012](#)
 - i. Symantec Global Intelligence Network - 64.6 million attack sensors recording thousands of events per second.
 - ii. Looking at about 200 countries.
 - iii. 8 billion emails and 1.4 billion web requests processed each day.
 - c. Zero in on Browser Vulnerabilities... Java - no longer just about clicking yes! Just visiting a website and with iframe technologies (same origin policy protection already being related through [Cross-Origin Resource Sharing](#)), even visiting legitimate websites.
 - i. Java Vulnerability Highlights
 1. [U.S. Department of Homeland Security](#) advising computer users to disable Java on their Web browsers
 2. First patch if you want to call it that ("The default security level for Java applets and web start applications has been increased from 'medium' to 'high,'" Oracle said in an [advisory](#) today.) [did not really work](#) and slow response or no public response from Oracle, [CNET Jan 14, 2013](#).
 3. Disabling does not always work and sometimes not possible through normal means due to a [bug](#).
 4. Oh yeah and upgrading in Java does not always work.
 5. Android - Java platform.
 6. Oracle - Java is on 3 Billion Devices.
2. Malware Evolution
 - a. New Terms "Cyber Attacks" and "Cyber Security"
 - i. APT (Advanced Persistent Threats)
 - ii. Zero-Day
 - iii. Dynamic Trojans
 - iv. Stealth Bots
 - v. Spear Fishing
 - vi. [Botnet with Command and Control](#) (C2 or C&C)
 - b. New Threats
 - i. Traditional Signature Block Rollouts No Longer Viable - See FireEye Diagram
 - c. Traditional Defences - NGFW (Next-Generation Firewalls), Intrusion Prevention Systems(IPS) and Intrusion Detection Systems(IDS), Anti-Virus, Web Gateways
 - i. Currently we use IDS/IPS, web, email security gateways and anti-virus (correlate to real implementation list)
3. "New" Defences (focusing on what we looked at in terms of tools)
 - a. Advancement of malware threats (Botnet Command & Control etc) new malware management solutions have emerged to complement the traditional security solutions to combat malware.
 - b. Analyzing and Blocking Network Traffic,
 - i. Callback Communications
 - ii. Inbound and Outbound Filtering Across Protocols

- iii. Well basically it's still IPS, IDS and Web Gateway technology - still the key is targeting Malware
 - c. Global Intelligence
 - i. Distribution of intelligence
 - ii. Well basically it's real time faster signature updates - still the key is targeting Malware
 - d. Virtual Code Execution - now this is cool
 - i. Describe - detonate
 - ii. Smart Malware that will not execute on virtual machines - so emulate hardware
 - iii. Custom machines for the organization
 - e. Process Improvement
 - f. There's lots more... OS hardening, browser protection tools like Trusteer.

Real World Forensics Case

1. Background
 - a. Pilot summary sentence (using existing slide text)
 - b. Event Detection Summary (use existing)
2. Air Canada Malware/SPAM Campaign (use existing)
3. Event Detection - Effect and Action (use existing)
 - a. Detected where ...
 - b. Proxy Aware versus Not ...
4. Pilot Results (use existing)
 - a. Technology wise that's Blue Coat, Anti-Spam Gateway, ISS (IBM Internet Security System) , Trend (Confirm Desktop or Gateway), SIEM.

Notes

1. Slow and Low (what's the proper term here?) and targeted attacks are coming.