Security Beyond Borders –
The Shifting Threat Landscape

Findings From the NTT Group 2014
Global Threat Intelligence Report
Research Sources

16 SOCs
And 7 R&D Centers
Research Sources
Research Sources

1,300
Security Experts and Researchers Working Globally

6,898
Customers Worldwide

139,963
Devices Monitored, Managed, Secured

250,000
Detection Rules

3.5 Trillion
Logs Analyzed Annually

150 Million
Attacks Detected and Defended Against Each Year
FOCUS ON OPERATIONAL SIDE OF SECURITY

THREAT AVOIDANCE
The value of doing the basics well.
Measure effectiveness of your security program.

THREAT RESPONSE
Advanced detective, investigative and response capabilities.
Respond when your avoidance capability has failed.

FEEDBACK LOOP
Ensure basic and advanced capabilities support each other.

COMPRESS THE MITIGATION TIMELINE

Report Theme and Content Areas
Avoid vs. Respond

Avoidance

- Reduce exploitable footprint
- Provide detective / investigative basis
- Potential ability to respond

Detection, Investigation, Response

- Vulnerability Lifecycle Mgmt.
  Patch Mgmt.

- ADVANCED CAPABILITIES
  Actionable threat intelligence
  Advanced analytics
  24x7 real-time monitoring
  Expert, certified Security Analysis

- Testing of IR Plan
  Customization / tuning

- Technical Indicators
  Malware / Virus Corpus

Compress Mitigation Timeline
Report Key Findings: Attacks by Type

- Client Botnet Activity: 34%
- Anomalous Behavior: 10%
- Network Manipulation: 8%
- Service Specific Attack: 8%
- Web Application Attack: 6%
- Application Specific Attack: 4%
- DoS/DDoS: 5%
- Reconnaissance: 10%
- Other: 15%
Report Key Findings: Web Application Attacks

Web Application Attacks
- Insecure Direct Object Ref: 20%
- Un-validated Redirects & Forwards: 19%
- Injection: 14%
- Other: 10%
- Security Mis-Config: 9%
- XSS: 8%
- Sensitive Data Exposure: 8%
- Authentication & Access Control: 7%
- Session Management: 5%
- CSRF: <1%
Report Key Findings – External Vulnerabilities

TOP 10 EXTERNAL VULNERABILITIES

- Outdated Apache Tomcat Server: 18%
- Outdated Apache Web Server: 13%
- Cross Site Scripting: 10%
- Outdated PHP Version: 9%
- Server Side Includes - Injection: 5%
- Web Clear Text Username/Password: 3%
- Vulnerable 3rd Party Apache Plugins: 3%
- Outdated OpenSSL: 2%
- Cookie Without HTTPOnly Attribute Set: 2%
- Cross Site Request Forgery Detected: 2%
Report Key Findings – Internal Vulnerabilities

TOP 10 INTERNAL VULNERABILITIES

- Missing Security Updates for MS Windows: 6%
- Adobe Reader Vulnerabilities: 6%
- Outdated System Management Consoles: 6%
- Oracle Java SE Critical Patch Update: 5%
- Outdated Apache Web Server: 3%
- Outdated Adobe Reader and Acrobat: 2%
- Outdated OpenSSH Version: 2%
- Sun Java J2SE 1.4.2 < Update 18: 2%
- Outdated Java Runtime Environment: 2%
- Internet Explorer Remote Code Execution: 2%
Are You Doing the Basics, or Doing Them Well?

**Anti-Virus**
Still prevents some issues if you scan, and use current engine and signatures

**Patch Management**
Patch effectively to remove known vulnerabilities

**Vulnerability Lifecycle Management**
Formally track and manage identified vulnerabilities

**Incident Response**
Effectively manage incidents with defined plan
Building a security program is like buying a yacht.
The second-greatest day of a man’s life is the day he buys a yacht, but the greatest day of a man’s life is the day he sells it.

– Donald Trump
Fantasy Versus Reality

The real cost

When you buy a Yacht, you HAVE to maintain it and the cost, much like maintaining a basic security program, can be high.
Report Key Findings - Malware

42% of malware observed in the education vertical

54% of all malware is undetected by 40+ antivirus solutions

43% of incident response engagements were malware related
Report Key Findings – Vulnerabilities by Year

2013 Vulnerabilities by Year of Release

- 2013: 38%
- 2012: 13%
- 2011: 11%
- 2010: 9%
- 2009: 8%
- 2008: 6%
- 2007: 4%
- 2006: 5%
- 2005: 4%
- 2004: 2%
Report Key Findings – CVEs in Exploit Kits

Unique CVEs in Analyzed Exploit Kits 2012

Unique CVEs in Analyzed Exploit Kits 2013
Report Key Findings – Remediation Time

![Average Remediation Time Graph](chart.png)

- **Vulnerability Scan Perspective**
- **Days to Remediate**
  - **External NON-VLM**
  - **External VLM**
  - **PCI External**

- **Total**

---

19
## Compressing the Mitigation Timeline

<table>
<thead>
<tr>
<th>Stage</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.5 hours</td>
<td>10.5</td>
</tr>
<tr>
<td>10.5 hours</td>
<td>2.5</td>
</tr>
<tr>
<td>5.5 hours</td>
<td>2.5</td>
</tr>
<tr>
<td>3.25 hours</td>
<td></td>
</tr>
</tbody>
</table>

- **Detection:** 2.5 hours
- **Investigation:** 5.5 hours
- **Response:** 2.5 hours
Everyone has a plan ‘till they get punched in the mouth.

– Mike Tyson
Case Studies

Rapid response minimized the impact of a ZeroAccess supernode.

A malware infection lasted over 3 months and cost the client over $109,000 in response costs.

Response cost of an SQL injection attack for one client was $196,000.
$196,000
Cost of a single SQL injection attack for one of our clients

78%
78% of 2013 exploit kits include vulns less than two years old

35%
PCI assessed organizations have a 35% faster remediation time for vulnerabilities
Report Key Findings – Incident Types

Types of Incident Response

- Malware: 31%
- DDoS: 17%
- Breach Investigation: 9%
- Other: 43%
Report Key Findings – Incident Response

Organizations with Effective Incident Response

- 77% Yes
- 23% No
The GTIR

The 2014 NTT Group Global Threat Intelligence Report
Thank You!