The Cyber Threat Landscape of 2013

- Ransomware
- Cyberespionage, Privacy, and Malicious Insider
- Internet of Things
- Mobile & Social
- Data Breaches
Zero-Day Vulnerabilities

Zero-Day Vulnerabilities, Annual Total, 2006 - 2013

Source: Symantec

23 zero-day vulnerabilities discovered in 2013

Increase from 14 in 2012

More zero-day vulnerabilities discovered in 2013 than in any year since we started tracking

More zero-days in 2013 than in past two years combined
Malicious Websites

New Unique Malicious Web Domains

<table>
<thead>
<tr>
<th>Year</th>
<th>Number</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>56,158</td>
<td>-24%</td>
</tr>
<tr>
<td>2012</td>
<td>74,001</td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td>74,001</td>
<td></td>
</tr>
</tbody>
</table>

With so many vulnerable websites, cybercriminals don’t need to set up own websites to host malware.
Anatomy Of a Cyber Attack

A majority of cyber attacks follow this path

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Icon</th>
<th>Action</th>
<th>Icon</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RECONNAISSANCE</td>
<td><img src="image1.png" alt="Icon" /></td>
<td><img src="image2.png" alt="Icon" /></td>
<td><img src="image3.png" alt="Icon" /></td>
<td><img src="image4.png" alt="Icon" /></td>
</tr>
<tr>
<td>2</td>
<td>INCURSION</td>
<td><img src="image5.png" alt="Icon" /></td>
<td><img src="image6.png" alt="Icon" /></td>
<td><img src="image7.png" alt="Icon" /></td>
<td><img src="image8.png" alt="Icon" /></td>
</tr>
<tr>
<td>3</td>
<td>DISCOVERY</td>
<td><img src="image9.png" alt="Icon" /></td>
<td><img src="image10.png" alt="Icon" /></td>
<td><img src="image11.png" alt="Icon" /></td>
<td><img src="image12.png" alt="Icon" /></td>
</tr>
<tr>
<td>4</td>
<td>CAPTURE</td>
<td><img src="image13.png" alt="Icon" /></td>
<td><img src="image14.png" alt="Icon" /></td>
<td><img src="image15.png" alt="Icon" /></td>
<td><img src="image16.png" alt="Icon" /></td>
</tr>
<tr>
<td>5</td>
<td>EXFILTRATION</td>
<td><img src="image17.png" alt="Icon" /></td>
<td><img src="image18.png" alt="Icon" /></td>
<td><img src="image19.png" alt="Icon" /></td>
<td><img src="image20.png" alt="Icon" /></td>
</tr>
</tbody>
</table>
The attacker identifies multiple vulnerable employees in the target organization and researches each victim using publicly available sources.
Reconnaissance

1

Using this intelligence, the attacker may spam the target users or leverage a phishing attack to compromise the target users.
Reconnaissance

1

- The attacker may use a Watering Hole attack by compromising a public website the target users are known to frequent as the source of malware.
The attacker will then attempt to trick the target users into accessing malicious content via email or website.
• The users download the attachments and/or follow the malicious links and become infected by remotely-controlled back-door trojans.
• The attacker sets up a Command-and-Control server
• The backdoor malware contacts the attacker via Command-and-Control channels.
• The backdoor malware follows the attacker’s instructions to begin stealing logins and passwords as users log into key enterprise servers.
Armed with the proper credentials, the attacker maps the network, expands to other systems and identifies high-valued data assets.
Capture

4

- The attacker sets up an external Drop server
- Then the attacker copies the desired data to a temporary, on-premise staging server.
• The attacker will use a tool to encrypt the credentials and sensitive data
• Then exfiltration the encrypted file to their external drop server.
Cybersecurity Challenges

**AGGREGATE**
Collect From All Sources

**DETECT**
Detect Indicators of Compromise

**RESPOND**
Understand, contain & remediate

---

**Security Devices**
- Firewalls
- IPS/IDS
- Servers
- SIEMs

**Human/Machine Interactions**
- NGFW
- End points
- Cloud
- Applications

**Intelligence Sources**
- Internal (telemetry)
- External
- Industry vertical
- Vulnerability
Integration Point Of Cyber Security
What is Integration? A Google definition...

1. **Integration**
   - the action or process of integrating.
   - "economic and political integration"

2. **Mathematics**
   - the finding of an integral or integrals. "integration of an ordinary differential equation"

3. **Psychology**
   - the coordination of processes in the system, including diverse sensory information and motor impulses.

4. **Psychoanalysis**
   - the process by which a well-balanced psyche becomes whole as the developing ego organizes the id, and the state that results or that treatment seeks to create or restore by counteracting the fragmenting effect of defense mechanisms.
Integration Point
Requirements

*Integration Point* Technical Characteristics...

1. Data collection from endpoint, network, cloud and app
2. Putting data into context
3. Gaining a global view of security intelligence
4. Flexible analysis to process the multi-TBs of data
Integration Point
Tool Options for the Job

**Insourcing**
Perform all the activities within the Security Monitoring Centre from within the customer environment

**Hybrid**
Outsource certain activities to a third party whilst retaining critical components within the customer control

**Outsourcing**
Engage a third party to perform SOC activities on behalf of the customer

**SIEM/Log Management**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Managed Services**
- Known Threat ID
- Log Management
- Collectors
- Canned Reports
- Raw Log Storage
- Log Search
- Incident Research
- Anomaly ID
- Workflow tools/API
- Always-on - 24x7 monitoring and management
- Active Threat ID/Rules team
- Threat Analyst Reviewed Incidents
- Web-based UI
- Global Intelligence Network
- Escalation Process
- Global SOCs
- Cloud-based Storage/Compute/Power/Maintenance

**Known Threat ID**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Log Management**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Collectors**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Canned Reports**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Raw Log Storage**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Log Search**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Incident Research**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Anomaly ID**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)

**Workflow tools/API**
- Incident Analysis Tool
- Customer operated/managed threat ID
- Custom Rules
- Custom Reports
- Custom Collectors
- Local Storage/Compute/Power/Maintenance
- 3rd party intelligence feeds (some)
- Software Maintenance Required (ad hoc)
Integration Point
Business Characteristics Comparisons

**Insource**
- **Cost**
  - High CAPEX
  - Variable OPEX
- **Control**
  - Team Knows Environment
  - Potentially Most Efficient
  - Complex to Manage
- **Time to Value**
  - People Recruitment, Tools
  - Procurement & Configuration
- **Skill Set**
  - Hard to Acquire, Retain, Train

**Outsource**
- **Cost**
  - Low CAPEX
  - Predictive OPEX
- **Control**
  - Lack of Environment Knowledge
  - SLA Based Services
  - Difficult to Terminate / Change
- **Time to Value**
  - Handover, Service Definition
  - and SLA Measurement
- **Skill Set**
  - 3rd Party Responsibility

**Hybrid**
- **Cost**
  - Moderate CAPEX
  - Predictive OPEX
- **Control**
  - Local and 3rd Party Expertise
  - Partial SLA Service
  - Flexible Future Change
- **Time to Value**
  - Blended Approach
- **Skill Set**
  - Staff Augmentation
How did Australia’s largest Media Company select a Integration Point for CyberSecurity?

- Cost
- Control
- Time
- Skill set
- Situational Awareness
- Contextual awareness
- Global Intelligence
- Analysis
How did Australia’s largest Media Company select a Integration Point for CyberSecurity?

Kevin Shaw – CISO Foxtel
Foxtel, Melbourne, Australia
The Integration Point for Cyber Security

AGGREGATE
Collect From All Sources

DETECT
Detect Indicators of Compromise

RESPOND
Understand, contain & remediate

Integration Point Criteria

✓ Situational & Contextual awareness; Global Intelligence; Threat Analysis
✓ Toolset Options
✓ Cost Effectiveness
✓ Control Needs
✓ Skill set
Information Security Service
Integration Is the Key

Symantec Confidential - NDA Audiences Only

Symantec & 3rd Party Solutions
Applied Intelligence Analysis & Reporting

Advanced Threat Protection
Real-time Monitoring
Policy/Controls & Benchmarking
Intelligence Correlations
Symantec & 3rd Party Solutions

Incident Response
Network & Host Forensics
Forensic Analysis & Visualization
Incident Response & Remediation
Controlled Malware Testing

Advanced Threat Protection Engine
Threat & Vuln Management
Log Discovery
Asset Discovery
Log Analysis & Passive Discovery

Log Collection & Archiving
Global Data Collection

Big Data Analytics
Cyber Intelligence
Intelligence Fusion Cells
Intelligence Feeds
DeepSight
Hosted Intelligence

Security Analysis
Symantec & 3rd Party Solutions
Policy/Controls & Benchmarking
Intelligence Correlations
Log Discovery
Asset Discovery
Log Analysis & Passive Discovery

Advanced Threat Protection
Real-time Monitoring
Policy/Controls & Benchmarking
Intelligence Correlations
Symantec & 3rd Party Solutions

Incident Response
Network & Host Forensics
Forensic Analysis & Visualization
Incident Response & Remediation
Controlled Malware Testing

360° Contextual View
360° Contextual View

Cyber Intelligence
Intelligence Fusion Cells
Intelligence Feeds
DeepSight
Hosted Intelligence

Security Analysis
Symantec & 3rd Party Solutions
Policy/Controls & Benchmarking
Intelligence Correlations
Log Discovery
Asset Discovery
Log Analysis & Passive Discovery

Advanced Threat Protection
Real-time Monitoring
Policy/Controls & Benchmarking
Intelligence Correlations
Symantec & 3rd Party Solutions

Incident Response
Network & Host Forensics
Forensic Analysis & Visualization
Incident Response & Remediation
Controlled Malware Testing

360° Contextual View
360° Contextual View

Cyber Intelligence
Intelligence Fusion Cells
Intelligence Feeds
DeepSight
Hosted Intelligence

Security Analysis
Symantec & 3rd Party Solutions
Policy/Controls & Benchmarking
Intelligence Correlations
Log Discovery
Asset Discovery
Log Analysis & Passive Discovery

Advanced Threat Protection
Real-time Monitoring
Policy/Controls & Benchmarking
Intelligence Correlations
Symantec & 3rd Party Solutions

Incident Response
Network & Host Forensics
Forensic Analysis & Visualization
Incident Response & Remediation
Controlled Malware Testing

360° Contextual View
360° Contextual View

Cyber Intelligence
Intelligence Fusion Cells
Intelligence Feeds
DeepSight
Hosted Intelligence
Three things you should do when you leave this room...

1. Use the criteria to determine gaps in your cyberstrategy
   ...understand your security posture

2. Consider your options to fill the gaps
   ...Cybercriminals are exploiting these gaps

3. If you need help, contact Symantec Sales Rep and ask for a Information Security Services deep dive.
Thank you!

YOUR FEEDBACK IS VALUABLE TO US!

Please take a few minutes to fill out the short session survey available on the mobile app—the survey will be available shortly after the session ends. Watch for and complete the more extensive post-event survey that will arrive via email a few days after the conference.

To download the app, go to https://vision2014.quickmobile.com or search for Vision 2014 in the iTunes or Android stores.