Defending Against Cyber Attacks:
Defense & Response Strategies

Tan Wei Ming, Senior Manager, Government Relations, APJ

2009 ITU Regional Cybersecurity Forum for Asia-Pacific

24 September 2009, Hyderabad
Utility hack led to security overhaul

Michael Crawford (Computerworld) 16/02/2006 9:14:04

Apprehending a notorious hacker rarely involves a car chase or a team of dedicated private investigators, but in the case of Vitek Boden, life imitated a Hollywood script.

Boden had waged a three-month war against the Scada (Supervisory Control and Data Acquisition) system of Marooyah Water Services beginning in January 2000, which saw millions of litres of sewage spill into waterways, hotel grounds and canals around the Sunshine Coast suburb. He was caught only after a team of private investigators hired by Marooyah Water Services alerted police to his location.

After a brief police pursuit from the Sunshine Coast towards Brisbane, Boden was run off the road. In his car was the specialized proprietary Scada equipment he had used to attack the system, and a laptop; however, it was a piece of $25 cable that ultimately bought him undone.

Grounds for charges were slim, but the handmade cable showed he had the technical capability to hack the Scada system.

The laptop found in his car contained enough messages to prove he sent commands to disrupt various pump stations and that, combined with proprietary radio equipment and specialized cable, was enough to find
More malicious programs were detected in the last 18 months than in all the previous years combined.

Cyber Defense – A Mission Impossible?

- Disruption of critical infrastructure operations
- Large-scale DDoS attacks
- Defacing of government websites
- Malware outbreaks within government network
- Stealthy exfiltration or unintended loss of confidential data

Organized Criminal
Well Meaning Insider
Malicious Insider
Effective Cyber Defense & Incident Response Strategy

> 4 important principles

- Understand the threats
- Establish prioritised risk-based framework
- Develop intelligence-in-depth
- Develop strong defense capabilities
Understand The Threats

Threat Landscape

The Web is the focal point
- Primary vector for malicious activity
- Target reputable, high-traffic websites

Attackers want YOUR information
- Focus on exploits targeting end-users for financial gain

Increased sophistication of the Underground Economy
- Well-established infrastructure for monetizing stolen information

Rapid adaptation to security measures
- Relocating operations to new geographic areas
- Evade traditional security protection
Web As The New Focal Point

- Attackers locate and compromise a high-traffic site through a vulnerability specific to the site or in a Web application it hosts.
- Once the site is compromised, attackers modify pages so malicious content is served to visitors.
The Education sector accounted for the majority of data breaches with 27%, followed by Government (20%) and Healthcare (15%).

More than half of breaches (57%) were due to theft or loss with insecure policy accounting for 21%.

Many data breaches are related to loss of small, portable devices such as USB memory keys, portable hard drives, and smart phones.
Convergence Of Attack Methods

Attackers combining malicious code, phishing, spam, exploitation of vulnerabilities, and online attacks

1. Spam containing link to compromised server
2. User visits legitimate site
3. Redirection
4. Downloader installed through browser vulnerability
5. Download and install additional threats
2> Establish Prioritised Risk-based Framework

Laws, Regulations & Policies

Technology

People

Process

Multi-tier protection
Endpoint protection & management
Sensors & correlation
Dashboard monitoring

Maintain adequate staff levels
Recruit, train, certify & retain security specialists
Increase security awareness
amongst users and the public

Present & future threat analysis
Incident response & recovery
Pre-emptive protective measures
Coordinate with international community & related bodies
Information Assurance Framework

NATIONAL INFORMATION ASSURANCE POLICY FRAMEWORK

National Legislation & Regulations
- Data Protection
- Cyber Crime
- Anti Spam
- Online Child Safety

Critical Information Infrastructure Protection Policies & Structures
- Identify CII assets/functions & Interdependencies
- Identify Of CII Owners & Operators
- Establish Trusted Information Sharing & Analysis
- Establish Public/Private Roles & Responsibilities
- Plan & Test Emergency Response Plans

Awareness Building & Threat Notification
- Increase Awareness Of Small Businesses & Individuals
- Issue Notifications Of Threats, Vulnerabilities, Security Incidents

Policy & Operational Coordination & Response
- Military
- Law Enforcement
- Agencies
- CERT (Govt, National, Academic)

Public-Private Partnerships & International Cooperation
- Research Institutes
- Industry Experts
- Other N-CERTS
- Int’l Alliances & Associations

GOVERNMENT
PRIVATE SECTOR
GENERAL PUBLIC
Fundamental Questions to Ask

> How do you prioritize events that occur at your endpoints today? How many malicious events do you experience per day? per week?

> How long does it currently take to respond to those events? How do you manage the workflow of that process?

> How much time does your staff invest in researching effective remediation best practices?

> Do you have visibility to malicious activities before they occur? Are you leveraging the information you have?

> How are you keeping up?

> What are your current requirements for providing security status, audit reports, and general information requests? How do you meet those requirements?

> What are your biggest challenges in effectively responding to malicious activities that occur? Are you optimizing your resources?
Prioritization A Constant Challenge

<table>
<thead>
<tr>
<th>Events</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events Requiring Immediate Customer Contact</td>
<td>2</td>
</tr>
<tr>
<td>Events Provided for Client Review</td>
<td>55</td>
</tr>
<tr>
<td>Security Events</td>
<td>620</td>
</tr>
<tr>
<td>Logs and alerts generated by firewalls and IDSs</td>
<td>9,481,668</td>
</tr>
</tbody>
</table>

Identify and issue warning of serious security threat

Eliminate insignificant events and report valid events

Security threat pattern identification

Based on one month of actual customer data.
Risk-Based Approach

RISK MANAGEMENT

THREAT & VULNERABILITY MANAGEMENT

INCIDENT RESPONSE

AUDIT & RECOVERY / COUNTER-INTELLIGENCE

Situational Awareness

Information Risk Management

Comprehensive Analysis

Sensors & Correlation

Cyber Intelligence

C2

Proactive

Reactive

Response Time Available

Time to act/react

WEEKS

DAYS/HOURS

HOURS/MINUTES

WEEKS

WEEKS

DAYS/HOURS

HOURS/MINUTES

WEEKS

Proactive

Reactive
Develop Intelligence-in-Depth

**Strategic Intelligence**
- **GUIDANCE AND SUPPORT IN DEVELOPING AND MAINTAINING IA POLICY**
  - Strategic threat trend reports (ISTR)
  - Sector specific reports
  - Technology vulnerability assessments
  - Penetration testing
  - Environmental assessments

**Operational Intelligence**
- **DELIVERY OF SITUATIONAL AWARENESS OF IA ACTIVITIES**
  - In depth analysis of targeted malware and attacks
  - Monitoring of network relevant vulnerabilities and exploits
  - Ongoing behavioural anomaly base lining and detection
  - Incident analysis and lessons learned
  - War gaming of potential attack vectors

**Tactical Intelligence**
- **TIMELY AND RELEVANT DELIVERY OF EVALUATED INTELLIGENCE TO ENABLE REAL TIME DECISIONS IN HANDLING AN INCIDENT**
  - Visual representation of suspicious activity and prediction of likely attack paths
  - Prioritisation of threats based on information and infrastructure criticality
  - Presentation of appropriate remediation methods to defeat attacks
Global Intelligence Network
Identifies more threats, takes action faster & prevents impact

Global Scope and Scale
Worldwide Coverage
24x7 Event Logging

Rapid Detection
Threat Activity
- 240,000 sensors
- 200+ countries

Malcode Intelligence
- 130M client, server, gateways
- Global coverage

Vulnerabilities
- 32,000+ vulnerabilities
- 11,000 vendors
- 72,000 technologies

Spam/Phishing
- 2.5M decoy accounts
- 8B+ email messages/day
- 1B+ web requests/daily

Preemptive Security Alerts
Information Protection
Threat Triggered Actions

Copyright © 2009 Symantec Corporation. All rights reserved.
Combining Global, Sector & Local Intelligence

Global Cyber Intelligence

Global Real World Intelligence

Trusted Information Sharing

Local Network Information
4> Develop Strong Defense Capabilities

Prioritised Risk-based Visibility

Protect Systems
- ENDPOINT
- NETWORK
- MESSAGING
- WEB
- NETWORK ACCESS CONTROL

Protect Information
- DISCOVERY
- DATA LOSS PREVENTION
- ENCRYPTION
- DATA PROTECTION

Policy-Driven Compliance

Symantec Management Platform

<table>
<thead>
<tr>
<th>Discover</th>
<th>Inventory</th>
<th>Configure</th>
<th>Provision</th>
<th>Patch</th>
<th>Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow</td>
<td></td>
<td></td>
<td></td>
<td>CMDB</td>
<td></td>
</tr>
</tbody>
</table>
Defending & Managing The Endpoints

Symantec Endpoint Protection

**Threat Protection**

*Keep the Bad things Out*

- Protect against malware
- Protect from known and unknown threats
- Manage multiple endpoint technologies

Symantec Network Access Control

**Network Access Control**

*Trust, but Verify*

- Enforce Endpoint Security policies
- Allow guest access to the network
- Provide access only to properly secured endpoints

Vontu DLP & Symantec Endpoint Encryption

**Data Loss Prevention & Encryption**

*Keep the Good things In*

- Discover confidential data
- Monitor its use
- Enforce policies to prevent its loss
- Encrypt to prevent unauthorized access

Altiris Client Management Suite

**Endpoint Management**

*Keep the Wheels On*

- Integrates security, data loss and management
- Provides automation
- Increases visibility and control
- Lowers total cost of ownership by managing multiple endpoint technologies
Sensor Deployment & Correlation

Symantec Security Information Manager (SSIM)
Executive Dashboard Monitoring

E.g. Vulnerability Assessment Module

Vulnerability information is collected and collated with organisation & asset info.

The analyst team is able to monitor status at a glance and drill down by theatre to individual assets. They can view trends and search for the status of any system.
Thank You!

Tan Wei Ming
weiming_tan@symantec.com
+65 96236998