The Dbriefs Technology Executives series presents:

Combating Cyber-Threats from the Underground Economy: A View from the Front Lines

Rich Baich, Principal, Deloitte & Touche LLP
Peter Makohon, Senior Manager, Deloitte & Touche LLP

December 3, 2009
Agenda

Today’s cyber security state of affairs

Sources of cyber intelligence data

The changing threat landscape

The underground economy

Use cases

A cyber threat intelligence program

Leading practices for cyber intelligence organizations
## Today’s cyber security state of affairs

<table>
<thead>
<tr>
<th>Issue</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current signature based information security controls are not effective against sophisticated, evolving cyber threats and exploits.</td>
<td>• What kind of security controls are necessary to detect cyber threats that are currently flying under the security radar?</td>
</tr>
<tr>
<td>A large number of unique information sources generating even larger number of false positives and false negatives.</td>
<td>• How do we collect data from multiple disparate sources and generate normalized, enriched, and actionable information?</td>
</tr>
</tbody>
</table>
| Lack of automated capability and skilled resources to rapidly identify, contain, analyze and remediate compromised devices. | • Do we have the right resources?  
• How do we ensure that we can quickly find and contain compromised devices? |
| Information provided by various intelligence sources is often outdated, high level, and not actionable. | • How do we collect timely, relevant, and actionable cyber intelligence data? |
| Organizations lack resources, technology, and process capabilities for taking timely action on near real-time intelligence data. | • How can cyber intelligence data be used to appropriately challenge or stop fraudulent transactions? |
Sources of cyber intelligence data

Key Points

• While there are many sources of cyber intelligence data, some sources lend themselves to generating more action-oriented intelligence.

• Cyber intelligence is more useful if the acquisition, enrichment, and normalization of information is automated.
Poll question #1

What is your organization doing to understand what is leaving your network?

- Nothing
- We are using a Data Loss Prevention solution
- We are tracking all outbound conversations against intelligence data
- We are performing Deep Packet Inspection
- Don’t Know/Not Applicable
The changing threat landscape

The cybercrime landscape has evolved into a set of highly specialized criminal products and services that are able to target specific organizations, regions, and customer profiles by using a sophisticated set of malware exploits and anonymization systems which routinely evade present-day security controls.
An entire underground economy has been built for the purpose of stealing, packaging, and reselling electronic information.
Using social engineering to compromise a user

**Sequence of Fraud**

1) Miscreant profiles organization and chooses an employee target.

2) Miscreant finds a business relationship from profile data and decides to spoof an email.

3) Spoofed email is sent to target employee.

4) Target employee opens email and clicks on obfuscated malicious link.

5) Fraudulent web site installs malicious code on target employee workstation.

5a) Target employee logs into bank account to perform payroll function.

6) Payroll user name and password are sent to miscreant key logger server.
1) Cyber criminal anonymously exploits internet facing web site using SQL Injection and gains access into internal network.

2) Once inside of the network, the criminal enumerates the environment.

3) The cyber criminal looks for organization specific credentials that may have already been compromised by a previous malware campaign.

4) Packet capture software is installed on the point of sales system.

5) As customers purchases goods, their account numbers, pins, and names are sent to the cyber criminal.
Wire transfer fraud

Sequence of Fraud

1) Miscreant instructs botnet to send out phishing email.

2) Compromised computer sends out phishing email to ISP servers worldwide.

3) Financial Services customer receives phishing email.

4) Financial Services customer clicks on link and proceeds to be phished.

5) Miscreant retrieves credentials immediately from phishing server.

6) Miscreant signs into Wire Transfer system using Malware proxy enabled computer and transfers funds.
Poll question #2

How does your organization find compromised devices inside of your network?

- Rely on Antivirus
- Rely on Intrusion Detection / Intrusion Prevention
- We don’t have any compromised devices
- Combination of answers 1, 2 and 3
- We actively check perimeter logs for traffic to known cyber criminal controlled destinations using intelligence that is less than 24 hours old
- Don’t Know/Not Applicable
A cyber threat intelligence program

- Cyber Threat Intelligence Acquisition
- Internet Vulnerability Detection Service
- Fraud Detection & Credential Recovery Service
- Cyber Threat Monitoring for Suppliers & Partners
- Compromise Detection Service
- Proactive Brand Protection Service
- Cyber Threat Intelligence Capability

- Cyber Analyst Training
- Emerging Threat Research
- Log Collection & Analysis
- Solution Research and Development
- Cyber Threat Modeling
- Penetration Testing
- Vulnerability Management
- Patch Management
- Network & Malware Forensics
- Incident Response
Making cyber threat intelligence actionable

Cyber Threat Intelligence Collection Research and Analysis Process

Near-Real Time Criminal Surveillance
Recovered Confidential & PII Data

External Intelligence Feeds
Internal Intelligence Feeds
Proactive Surveillance

Infrastructure & Application Logs
Technology Configuration Data

Risk Assessment Process
Risk Acceptance Process
Risk Mitigation & Remediation

Urgent security control updates
IP reputation data for authentication

3rd Parties, Subsidiaries
Line of Business Teams
Security, Fraud and Operational Risk Teams
Poll question #3

What is your greatest challenge with implementing a cyber threat intelligence program?

• Justification of a cyber-security investment on top of other risk and security spend
• Lack of talented, skilled cyber intelligence resources
• Legal team has advised against sharing intelligence
• Current reactive approach does not allow resources to focus on building an intentional cyber-security capability
• Life is good, we really don’t need a program
• Don’t Know/Not Applicable
### Leading practices for cyber intel organizations

<table>
<thead>
<tr>
<th>Area</th>
<th>Leading Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>• Resources dedicated toward reviewing and analyzing emerging threats.</td>
</tr>
<tr>
<td></td>
<td>• Annual budget for security control upgrades, new detection tools, and</td>
</tr>
<tr>
<td></td>
<td>intelligence sources.</td>
</tr>
<tr>
<td></td>
<td>• Cyber command center.</td>
</tr>
<tr>
<td>Process</td>
<td>• Daily regimen to review and communicate emerging threat data.</td>
</tr>
<tr>
<td></td>
<td>• Threat matrix.</td>
</tr>
<tr>
<td></td>
<td>• Scenario planning.</td>
</tr>
<tr>
<td>Malware Forensic Capability</td>
<td>• Ability to rapidly collect and review forensic information from devices that are</td>
</tr>
<tr>
<td></td>
<td>suspect.</td>
</tr>
</tbody>
</table>
## Leading practices for cyber intel organizations (cont.)

<table>
<thead>
<tr>
<th>Area</th>
<th>Leading Practice</th>
</tr>
</thead>
</table>
| **Perimeter Monitoring**    | - Network extrusion monitoring  
                              | - Network conversation recording and reconstruction.                                                                                             |
| **Threat Intelligence Sources** | - Automated, monitored, incremental feeds with aging algorithm.  
                              | - Two-way, cross-industry intelligence sharing.                                                                                                  |
|                              | - Contingency plans for loss of intelligence sources.                                                                                             |
| **Metrics and Reporting**    | - Regular cyber bulletin updates.  
<pre><code>                          | - Threat briefings by line of business / delivery channel.                                                                                     |
</code></pre>
<p>|                              | - Automated custom alerting based on thresholds.                                                                                                   |</p>
<table>
<thead>
<tr>
<th>Area</th>
<th>Leading Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Modeling</td>
<td>• Capability to model and analyze the likelihood that an emerging threat will impact an organization and identify where the weaknesses are that will be exposed.</td>
</tr>
<tr>
<td>Threat Lifecycle Management</td>
<td>• Case management tools to coordinate cyber incidents across multiple business areas and support organizations.</td>
</tr>
<tr>
<td>Research and Development</td>
<td>• Threat intelligence teams should work in conjunction with internal security teams to identify new strategies and solutions for testing and improving the security posture of devices, applications, and banking processes.</td>
</tr>
</tbody>
</table>
| Supporting Capabilities     | • Patch management.  
• Vulnerability management.  
• Incident response.  
• Configuration management.  
• Security event management. |
Poll question #4

Where do you think your greatest cyber risk is today?

• We don’t have enough visibility into our business units, subsidiaries, etc.
• We don’t have enough visibility into our suppliers
• We are at a greater risk when our employees are working or connecting to the Internet remotely
• We aren’t able to account for all of the executable programs loaded on our personal computers
• Our customers are not adequately protected
• All of the above
Questions & Answers
Join us January 14, at 2 PM ET as our Technology Executives series presents:

Information Management Goes Enterprise-Wide: A Unifying Approach to Data Governance
Contact information

Rich Baich, Principal, Deloitte & Touche LLP
704-887-1822
jbaich@deloitte.com

Peter Makohon, Senior Manager, Deloitte & Touche LLP
704-887-1570
pmakohon@deloitte.com
This presentation contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this presentation, rendering business, financial, investment, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.
About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.