IT Examination Hot Topics
Cybersecurity: Now What?

May 2, 2018
Contact Information

Matt Janoski
CISSP, CISA
Manager, IT Examinations
Wipfli LLP
630.368.7019
mjanoski@wipfli.com
From the Headlines
SWIFT Attacks Making Their Way to the U.S.

- Bangladesh Bank in 2016
  - Funds routed through the US SWIFT network
  - Dridex malware used to access bank systems
  - Captured due to typo in request
- Many targets of spear phishing
- FS-ISAC reports two incidents result of compromised bank systems
  - Russian bank ~ $6 million USD
  - Indian bank ~ $2 million USD
What Is Your Institution’s Security Banking On?

- Refresh of Online Banking (reset, enrollment)
  - Sent requirements for password reset
    - Password reset procedures contain easily accessible information (based on dark web research) such as SSN
    - PIN by text sent in plaintext
  - Ensure adequate testing of procedures identification
  - Two-factor authentication
ATM Skimmer Activity

- Increasing levels of sophistication
- Over 2 billion dollar global impact
- Taking advantage of methods to obscure threat actors
  - Bluetooth technology
  - Tools that replace legitimate card readers
  - More difficult to detect
- Reminder to ensure adequate segregation exists within your connections to business partners (third-party risk management)
NIST Publication 800-63-3

- Use passphrase instead of password
- Monitor for indicators of compromise (IoC)
- Test passwords against known compromised password lists
- Change password frequently
- Reset passwords in the event of security incident(s)
Spectre and Meltdown
Data Breach Reports
Increasing encrypted web traffic... A good thing, right?

50% of global web traffic now encrypted.

12% increase since November of 2016.

Now malicious software is utilizing encryption.
Cisco 2018 Annual Cybersecurity Report

- An increase in sophistication of offense requires a like increase in defense.
- Institutions are looking to fortify their network defenders’ tool boxes.
- Tools leveraging automation and artificial intelligence are being implemented.
The low hanging fruit being consumed by today’s threat actors is found in our web browsers (e.g. Internet Explorer, Edge, Firefox, Safari, Chrome).

- HTML attack vectors are being heavily leveraged by threat actors.
- Patching browsers and risks associated with using older, less secure browsers in an environment must be evaluated.
• Social engineering is still a critical launchpad for email attacks.
• Email remains a vital channel for malware distribution.
• The solution remains unchanged:
  • Implement powerful and comprehensive email security defenses.
  • Educate and test users regarding the threat of malicious attachments and links.
Critical advisories and attack activities

Source: Cisco Security Research

**Critical Vulnerabilities**

<table>
<thead>
<tr>
<th>Vulnerability Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle CPU, OIT Vulnerabilities</td>
<td>Jan 18th</td>
</tr>
<tr>
<td>Multiple CVEs</td>
<td></td>
</tr>
<tr>
<td>OpenSSL Vulnerabilities</td>
<td>Jan 26th</td>
</tr>
<tr>
<td>Multiple CVEs</td>
<td></td>
</tr>
<tr>
<td>OpenSSL Vulnerabilities</td>
<td>Feb 6th</td>
</tr>
<tr>
<td>CVE-2017-3733</td>
<td></td>
</tr>
<tr>
<td>Apache Struts 2 Remote Code Execution Vulnerabilities</td>
<td>Mar 6th</td>
</tr>
<tr>
<td>CVE-2017-5638</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Graphics</td>
<td>Mar 14th</td>
</tr>
<tr>
<td>CVE-2017-0108</td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Server Message</td>
<td>Mar 21st</td>
</tr>
<tr>
<td>Block Service Arbitrary Code Execution Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td>CVE-2017-0145</td>
<td></td>
</tr>
<tr>
<td>Microsoft Internet Information Services (BITS)</td>
<td>Mar 29th</td>
</tr>
<tr>
<td>WebDAV</td>
<td></td>
</tr>
<tr>
<td>CVE-2017-7269</td>
<td></td>
</tr>
<tr>
<td>Microsoft Office (Ole2 Exploiting)</td>
<td>Apr 11th</td>
</tr>
<tr>
<td>CVE-2017-0169</td>
<td></td>
</tr>
</tbody>
</table>

**Attack Activities**

<table>
<thead>
<tr>
<th>Attack Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WikiLeaks Vault 7</td>
<td>Mar 7th</td>
</tr>
<tr>
<td>Release</td>
<td></td>
</tr>
<tr>
<td>Multiple CVEs</td>
<td></td>
</tr>
<tr>
<td>WannaCry</td>
<td>May 17th</td>
</tr>
<tr>
<td>Activity MS17-010</td>
<td></td>
</tr>
<tr>
<td>Multiple CVEs</td>
<td></td>
</tr>
<tr>
<td>Operation Cloud</td>
<td>Apr 6th</td>
</tr>
<tr>
<td>Hooper Sustained</td>
<td></td>
</tr>
<tr>
<td>Global Campaign</td>
<td></td>
</tr>
<tr>
<td>Shadow Brokers</td>
<td>Apr 8th</td>
</tr>
<tr>
<td>Group Disclosure of Equation Exploits</td>
<td></td>
</tr>
<tr>
<td>Microsoft .NET Framework Arbitrary</td>
<td>Sep 6th</td>
</tr>
<tr>
<td>Code Execution</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
</tr>
<tr>
<td>CVE-2017-8759</td>
<td></td>
</tr>
</tbody>
</table>

For more info visit: cisco.com/go/aer2018
Kroll Global Fraud & Risk Report
Regulatory Updates
23 NYCRR 500 – New York Cybersecurity Requirements for Financial Services Companies

- CISO Report to the Board
- Frequent Testing
  - Vulnerability Scan
  - Penetration Testing
- Risk Assessment
- Multi-Factor Authentication
- User Awareness Training
- First Wave of Certification on February 15, 2018
ADA Compliance

- No regulatory guidance yet received in 2018
- Court cases in the past year
- Take action if you receive a demand letter
- “The triangle of website compliance”
  - The financial institution
  - The website host
  - The website designer
IT Examination Expectations

- Cybersecurity Assessment Tool (CAT)
  - Meeting baseline objectives
  - Incorporating baseline objectives into strategic plan
  - Budgeting to include ongoing tools
- Moving from Baseline to Evolving and up
IT Examination Expectations

- Quarterly Firewall Reviews
- Monitoring Administrative Access
- Multifactor Authentication
- Third-Party Risk Management
- Board Reporting
- Disaster Recovery
  - Cybersecurity incident response
  - Attacks involving support providers
IT Examination Expectations

● Social Engineering Testing
  • Email spoofing
    – Subscription-based services
  • Pretext calling
  • Physical penetration testing
IT Examination Expectations

- **Vulnerability Testing**
  - Internal Vulnerability Scan
  - Perimeter Vulnerability Assessment
  - External Penetration Testing

- **Vulnerability Management and Tracking**
Both threat actors and vulnerabilities are becoming more sophisticated.

It is important to be armed with current threat intelligence.

Regulatory agencies are expanding expectations; being aware of changes is key.

Maintaining open communications with peers and trusted advisors in the financial industry is critical.
Resources – Industry Threat and Breach Reports

● Cisco Annual Threat Report:

● Symantec Internet Security Threat Report:
  • https://www.symantec.com/security-center/threat-report

● Verizon Data Breach Investigations Report:
  • http://www.verizonenterprise.com/verizon-insights-lab/dbir/
Resources – Financial Institution Specific

- Financial Services Information Sharing and Analysis Center:
  - [http://www.fsisac.com/](http://www.fsisac.com/)

- WipfliSecurity Weekly – The most critical information delivery by email every week:
  - [https://www.wipfli.com/cybersecurity](https://www.wipfli.com/cybersecurity)
Closing