Ransomware Cyber Resiliency Exercise
Preparation, Detection, Response & Recovery
Traditional Objective: To evaluate organizational cyber incident RESILIENCY (prevention, mitigation, detection and response readiness, resources and strategies) from the perspective of the Incident Response Team.

Session Objective(s):

• To determine the best course of action for each scenario.
• To compare and contrast with your institutions readiness and resiliency.
• To “Train-the-Trainer” for internal use.
1. Threat Intelligence & Preparation
2. Detection & Alerting
3. Response & Continuity
4. Restoring Trust
5. After Action Activity
Ransomware is the 2016 attack of choice. On February 18th, the FBI issued alert #MC-000068-MW warning businesses about the MSIL/Samas.A ransomware variant. On March 25th, the FBI issued an update alert #MC-000068-MW targeted vulnerable systems.

Between March 25th and May 9th, FS-ISAC Daily Reports included multiple references to instances and variants of ransomware.

In the past two months, multiple high profile ransomware cases have been reported in the news including the week long shut down of Hollywood Presbyterian Medical Center.

Exercise source materials:
• FBI Advisories
• FS-ISAC Ransomware Extracts
• Threat Intelligence Workflow
<table>
<thead>
<tr>
<th>TLP</th>
<th>Title</th>
<th>Date/Time (UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report April 22, 2016</td>
<td>04/22/2016 14:24</td>
</tr>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report April 20, 2016</td>
<td>04/20/2016 14:54</td>
</tr>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report April 18, 2016</td>
<td>04/18/2016 14:54</td>
</tr>
<tr>
<td>TLP</td>
<td>FS-ISAC Cyber Threat Level - April 14, 2016</td>
<td>04/14/2016 19:28</td>
</tr>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report April 14, 2016</td>
<td>04/14/2016 13:48</td>
</tr>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report April 13, 2016</td>
<td>04/13/2016 13:33</td>
</tr>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report April 12, 2016</td>
<td>04/12/2016 13:42</td>
</tr>
<tr>
<td>TLP</td>
<td>bugzeroo Analysis of Latest Dridex Campaign Reveals Worrisome Changes and Hints at New Threat Actor Involvement</td>
<td>04/11/2016 11:27</td>
</tr>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report April 7, 2016</td>
<td>04/07/2016 14:54</td>
</tr>
<tr>
<td>TLP</td>
<td>RE-ISAC Daily Report for Monday, 04 April 2016</td>
<td>04/04/2016 19:21</td>
</tr>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report April 4, 2016</td>
<td>04/04/2016 15:11</td>
</tr>
<tr>
<td>TLP</td>
<td>RE-ISAC Daily Report for Thursday, 31 March 2016</td>
<td>03/31/2016 10:13</td>
</tr>
<tr>
<td>TLP</td>
<td>DHS Daily Open Source Infrastructure Report March 31, 2016</td>
<td>03/31/2016 14:08</td>
</tr>
</tbody>
</table>
Threat Intelligence Program Workflow

1. Planning
2. Collection
3. Analysis
4. Dissemination
5. Action

Flow diagram showing the cycle of planning, collection, analysis, dissemination, and action.
Threat Intelligence & Preparation

1. There is no shortage of ransomware threat intelligence. Using the Threat Intelligence Workflow diagram, document who (by role/department) in a financial institution should be included at each stage. Assign specific responsibilities.

2. You feel the threat of ransomware should be escalated to executive management. What would your approach be? What immediate actions would you recommend? What longer term strategy would you recommend?

3. How would you know if your organization was “at-risk” for MSIL/Samas.A? Consider the exposure that third-party managed systems pose.
Ransomware exploits vulnerable systems, applications and users. Unlike most ransomware, MSIL/Samas.A (also known as SamSam) is not launched via user focused attack vectors, such as phishing campaigns and exploit kits. It is a targeted attack that exploits vulnerable external facing systems.

MSIL/Samas.A spreads quickly. Once inside the network, the ransomware uses csvde.exe to harvest Active Directory details. This information is used to create a list of hosts, achieve lateral movement across the network and deploy tools and scripts (e.g. psexec.exe) to multiple systems.

The ransomware maps the network and “pings” computers to compile a list of active hosts. Public and private encryption keys are generated based upon the hostnames. The private keys are sent to the attacker.

The ransomware and corresponding public key are distributed to all of the active computers on the network. The ransomware launches in a coordinated attack hitting the entire network in a few minutes.

Once active, the volume shadow copies of the computers are deleted, and files on the computer are encrypted. Backup related files are specifically sought out for encryption / deletion.
Detection and Alerting

`PsExec v2.0 – Execute processes remotely
Copyright (C) 2001-2013 Mark Russinovich
Sysinternals - www.sysinternals.com`

PsExec executes a program on a remote system, where remotely executed console applications execute interactively.

Usage: psexec [\computer[.\computer2[...]] | @file] [-u user [-p passwd][-n s] [-r servicename][-h][-l][-s][-e][-x][-i [session]] [-c [-f] [-v]] [-w directory] [-d][-<priority>] [-a n, n,...] cmd [arguments]

- **a** Separate processes on which the application can run with commas where 1 is the lowest numbered CPU. For example, to run the application on CPU 2 and CPU 4, enter: 
  
  "-a 2,4"

- **c** Copy the specified program to the remote system for execution. If you omit this option the application must be in the system path on the remote system.

- **d** Doesn’t wait for process to terminate (non-interactive).

- **e** Does not load the specified account’s profile.

- **f** Copy the specified program even if the file already exists on the remote system.

- **i** Run the program so that it interacts with the desktop of the specified session on the remote system. If no session is specified the process runs in the console session.
1. What detection tools or processes might identify a predictor of ransomware compromise (POC) or indicator of ransomware compromise (IOC)?

2. What type of activity could indicate the presence of MSIL/Samas.A?

3. If an anomaly is detected, how should it be responded to? Who should be notified? What is the detection process during non-business hours?
Very often, the first indication that something is wrong is a ransom note on the desktop. You are at the NYB Technology, Risk and Compliance Forum. You receive a panicked call from your bank’s IT Manager reporting that email is down and it appears to be related to ransomware.

You ask what happened? He replied that at approximately 4:00pm, The Help Desk began receiving calls that email was not working. The on-call network engineer logged onto the Exchange Server. The “HELPDECRYPT_YOUR_FILES.html” icon and ransom note was discovered on the desktop. You ask him to get you a copy of the note.

He puts you on hold to take another call. When he comes back on the line he says something about Customer Care getting calls about mobile banking problems.

Exercise source materials
• HELPDECRYPT_YOUR_FILE ransom note
#What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm. For more information you can use Wikipedia.

*attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files.*
1. If you email system isn’t working, how would he get you a copy of the ransom note?

2. What should be the protocol for responding to this incident (remember that as of right now you only know about one server)? Detail your next three steps.

3. What documentation would be useful to have as you evaluate the situation?
By 5:15pm, it has become obvious that this is more than an isolated incident.

The IT Managers calls you to report that almost all of institution’s files appear to be encrypted and are inaccessible. The encrypted files have the same name as the original, except that the extension .encryptedRSA has been added. It appears that the original files have been deleted.

The “HELPDECRYPT_YOUR_FILES.html” ransomware appears on a majority of the bank’s servers and storage devices including domain controllers, SQL database servers, Call Center servers, loan processing servers, mobile banking servers, backup servers and cold storage. A total of 92 servers and storage devices are known to be infected. At this time, it is unknown if any workstations have been impacted.
1. It is after business hours, you have no access to any files stored on your network. What could you have done to ensure that your incident response and business continuity plans are accessible.

2. What external resources should be contacted (identify at least three and the order you would contact them in)? What would you expect each to do?

3. How and what should you communicate to employees and customers?
The replication and backup system at your institution is twofold. Every hour files are backup up to a local NAS. The NAS data is replicated to a off-site data center SAN at 6pm, 12am, 6am and 12pm. The replication system stores the last four copies.

The ransomware has infected the NAS device. It appears that the 6pm replication is also encrypted. The files from noon appear to be intact. This means that a restore would be missing five business hours of customer files, emails, transactions, etc..
The ransom note indicated that the cost for the decryption keys for each device would be 1.5 BTC or 22 BTC for all of the devices.
1. How much is 22BTC? How would you calculate the cost of paying the ransom vs. replication and work to recover? If the bank choose to pay the 22BTC, how does one establish a Bitcoin account? How quickly could payment be made?

2. Who at the institution should make the final decision on paying ransom? Who might they consult? Are there any reputation or compliance issue to consider?

3. While this issue is being considered, what other response activities should be in play?
At 8pm, a decision was made to pay the 22 Bitcoins which according to the ransom note would cover all of the servers. As instructed, this was communicated to the attackers via the ‘helpbyzeus’ WordPress site comment section. The attackers responded that they would release 15 private keys used for decryption; it would cost an additional 18 Bitcoins to receive the remaining keys. Decryption keys for 15 mission critical servers were obtained and the process of decryption initiated.

A decision was made to pay the additional ransom. 104 keys were delivered at 6am next morning. Some of the keys were for servers that had not been active on the network for more than three months. It is estimated that the decryption process could take most of the day.
1. Do you agree or disagree with the decision to pay the additional ransom? Why or why not?

2. For approximately 24 hours, the bank was unable to rely on technology. What is the relationship between cyber incident response and business continuity planning?

3. Some of the private keys that were delivered were for servers that had not been active on the network for more than three months. What does this potentially mean? Does this warrant further investigation? Where would you start? What if the origin remains a mystery?
Someone internally leaked the story to a cyber investigative reporter. The story went viral and was repeated on social media, blogs and news outlets across the country including the fact that keys were delivered to servers that hadn’t been online for months – leading listeners to question if the situation was truly under control.
1. It is generally assumed that the CEO/President should be the spokesperson for the bank but this person isn’t always the best candidate. What are the characteristics of crisis management spokesperson?

2. At this point, what should insiders know and how are you going to communicate with them?

3. Could this event impact any long term strategic plans that an institution might have? Explain how.
Recap

- Threat Intelligence
- Incident Detection
- Incident Response and Management
- External Resources and Relationships
- Maximum Tolerable Downtime, Recovery Time Objectives and Work Recovery Time
- Contingency Plans
- Dealing with Extortion
- Internal and External Communications
- Customer and Community Relations
- Strategic Impact
Best practices for an exercise or an event if to prepare an After Action Report that summaries the situation, lessons learned and recommendations.

For this exercise’s After Action Report you should:
Compare your answers with your institutions preparedness, identify the gaps and make recommendations to enhance your institutions cyber resiliency and preparedness.
Explore DR/BCP/IR plan synergies and convergence potential (and the use of playbooks).
Cybersecurity 2.0 Leadership Seminar for Banking Professionals – Transforming your Institution

September 26-28, 2016 – Albany Marriot
Enroll online at the NYBA.com
Limited to 28 participants – Register early