Bellevue Bank and Trust Cyber Fusion Team

Ransomware Tabletop Exercise (TTX)

Table of Contents

1 Document Information and History

1.1 Version History

Version	Change Date	Changes and Description	Editor	Approval Date	Approver
1.0	7/8/2022	Initial Template Creation	Steven Maestas	7/8/2022	SMM
2.0	2/1/2023	Template completion	Lathan Birmingham		

1.2 Distribution

This threat assessment is intended to be stored by the BB&T lead security administrator. This report can be utilized by BB&T both cybersecurity red and blue teams to improve the overall security posture. This threat assessment is confidential information owned by BB&T.

2 Introduction

The purpose of this comprehensive tabletop exercise is to determine BB&T's ability to detect and respond accordingly to a ransomware attack targeting the organization.

2.1 Purpose

The purpose of tabletop exercises is to prepare an organization for potential cyber incidents. By walking through the process of responding to a cybersecurity incident can improve team responses, communication, and fill in gaps in the incident response plan.

2.2 Definitions

Red Team A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment. Also known as Cyber Red Team [1].

Blue Team "The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically the Blue Team and its supporters must defend against real or simulated attacks 1) over a significant period of time, 2) in a representative operational context (e.g., as part of an operational exercise), and 3) according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team) [1]."

Tabletop Exercise "A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario [1]."

Ransomware "Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. StopRansomware.gov is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively [3]."

Third-party "A third party, such as a CA, that is trusted by its clients to perform certain services. (By contrast, the two participants in a key-establishment transaction are considered to be the first and second parties) [1]."

Incident Response "The mitigation of violations of security policies and recommended practices [1]."

2.3 Handling Instructions

TLP: WHITE

"The title of this document is BB&T Ransomware Situation Manual. This document is unclassified and designated as "Traffic Light Protocol (TLP):WHITE": Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction [2]."

3 Exercise Overview

Exercise Name	Exercise Name	
Exercise Date, Time, and Location	Monday, February 6th, 2023 9 am – 5 pm Bellevue University	
Exercise Schedule	**Time**	**Activity**
	9:00 am	Scenario 1
	10:45 am	Break
	11:00 am	Scenario 1
	1:00 pm	Lunch
	2:00 pm	Scenario 2
	3:45 pm	Break
	4:00 pm	Scenario 2
	5:30 pm	TTX closing
Scope	7-hour facilitated, discussion-based Tabletop Exercise	
Purpose	To examine the coordination, collaboration, information sharing, and response capabilities of BB&T in reaction to a significant cyber incident.	
Team	BB&T TTX Group & Leaders	
Objectives	1. Examine the ability for BB&T to respond to a significant cyber incident. 2. Evaluate the ability for BB&T to coordinate information sharing during a significant cyber incident. 3. Inform development/update of BB&T's cyber incident response plans. 4. Explore processes for requesting additional incident response resources once BB&T's resources are exhausted. 5. Explore BB&T's processes for addressing public affairs.	
Threat or Hazard	Cybersecurity	

Exercise Name	Exercise Name
Scenario	A phishing attack targeting BB&T's employees resulted in malicious actors accessing internal networks & systems. The actors compromise data using ransomware with a payment deadline of 48 hours.
Sponsor	Bellevue University

4 General Information

4.1 Roles and Responsibilities

This Table Top Exercise includes many types of participants including those playing the exercise. The types of participants include:

Players **"**have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency [2]."

Observers "do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise [2]."

Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise [2]."

Note-takers "are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures [2]."

4.2 Exercise Structure

Module 1 This session focuses on the first 4 steps of the IR process: Preparation, Identification, Containment, and Eradication.

Module 2 This section focuses on the last two steps of the incident response process, including recovery, and lessons learned.

A. Module 1

Day 1: 11:00 am

Several employees receive a personalized email that appears to come from the CEO of BB&T. This email details that they have been nominated for the company's annual excellence awards and if they would like to accept their nomination, they should fill out the attached document and return to him. The email has a brief description of the award and a Microsoft Word document attached to it.

Three employees open the word document, fill it out, and return it to the same email address. Another employee fills out the word document and sends it in a separate email to the CEO thanking him for the nomination. The CEO replies to the employee and says he had no idea what they were talking about and did not think much of it, he forwarded the email chain to BB&T help desk citing that this document could possibly be a potential hacker.

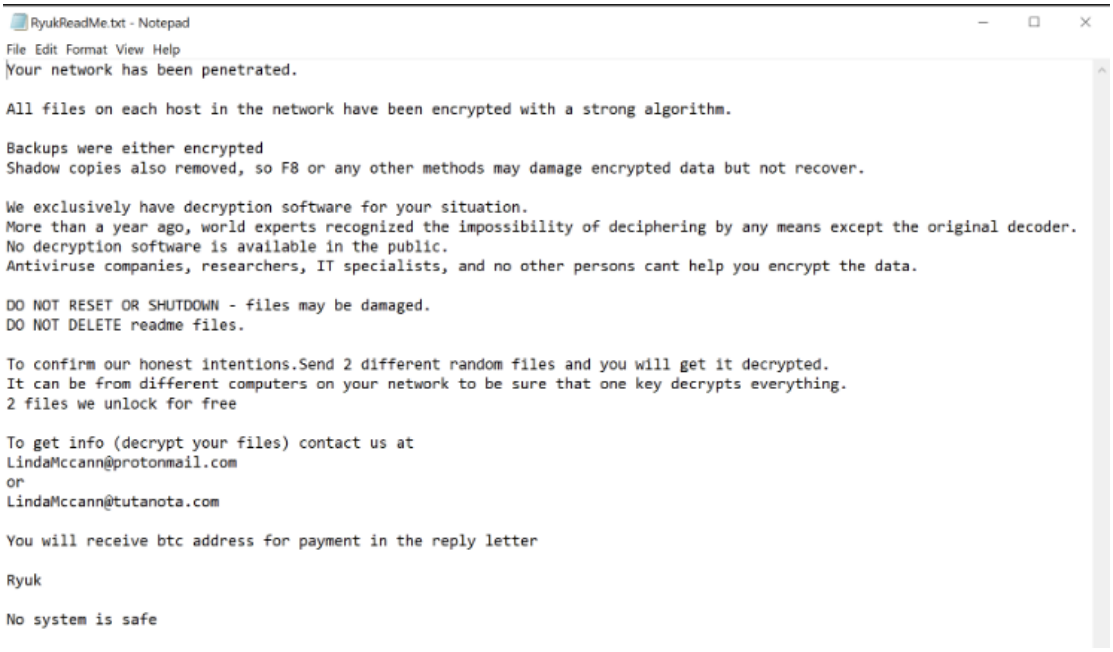
Help desk views the email at the end of the workday and decides that this matter can wait until tomorrow as it is getting late.

Day 2: 8:30 am

By this time, help desk is swamped with emails and phone calls from employees in all sectors not being able to open their files. They gather the following information from the complaints:

- All file extensions have been changed to .ryk
- A file named 'RyukReadMe.txt' is now saved to every folder and desktop

RyukReadMe.txt:



The CEO and other executives are demanding for this to be resolved immediately. The CEO of the company learns that help desk did see his initial email alerting them of a potentially malicious file and is furious that they did not investigate immediately.

Day 2: 3:00 pm

By this time, help desk has learned that the initial word document executed malicious VBA code causing this attack. They learn that BB&T has been a target for the ryuk ransomware, and they are suspecting it is the new variant due to how quickly this spread over BB&T's internal networks.

Someone within the company anonymously reaches out to a new agency and the incident becomes public and receives national attention.

Day 3: 10:00 am

With BB&T IT working around the clock to resolve this, they decide to call in a third-party incident response team to assist with the process.

An example set of records from BB&T's customer database is pasted on pastebin and the dark web and an external cybersecurity company, the Cyber Defense Group (CDG) notifies the bank of the message/records.

BB&T decides to contract with the Cyber Defense Group (CDG) to help with identification and recovery from this incident.

Operations are significantly delayed. Executives are furious about various things – the halting of company operations, the steep price of a quality incident response team, the potential legal issues facing BB&T, and the fear of having no option but to pay the ransom to retrieve encrypted files

Day 3: 12:00 pm

The CDG calls into BB&T and finally gets a formal brief on the situation.

Day 3: 1:00 pm

The CDG begins investigating the ransomware incident. By this time, around 50% of employee files and company servers are encrypted.

Day 3: 3:00 pm

The CDG has isolated the infected computers and servers from the uninfected computers and servers. The CDG launches an overnight investigation to identify, contain, and eradicate the ransomware virus affecting BB&T.

Day 4: 6:00 am

The CDG begans preparing a synopsis of the incident to report to the CEO and other executives. CDG will include a summary of events that occurred since the initial infection and a plan for the eradiation of the virus.

Day 4: 7:00 am

The CDG is preparing to deliver the synopsis to BB&T executives around 8:00 am, but by this time the executives are already pestering asking for updates on the situation and demands to know immediately whether they will have to pay the ransom or not.

CDG explains that they are in the process of preparing a synopsis to present to BB&T within the hour and this synopsis will explain everything they know at the time and the current recommended mitigations.

Discussion Questions

Discussion questions included in each module may be modified as desired.

A. Would the events from Day 1 be identified as cybersecurity incidents or events? If so, how would they be handled?

B. What sources of cybersecurity threat intelligence does BB&T have? Ex. information from CISA, FBI, open-source reporting, security service providers, or others?

a. Which of these sources is most useful?
b. Is the information you receive timely and actionable?
c. Who is responsible for collating information across your organization?

C. Does your organization provide cybersecurity awareness training to all users, including managers and senior executives)?
   a. How often is training provided?
   b. Does the training cover:
      i. Awareness of leading cyber threats,
      ii. Password procedures, and
      iii. Whom to contact and how to report suspicious activities?
   c. Is training required to gain network access?
   d. What security-related training does your organization provide to, or contractually require of, IT personnel and vendors with access to your organization's information systems?
   e. How often do they receive the training?

D. How do employees report suspected phishing attempts?
   a. What actions does your department take when suspicious emails are reported?
   b. Are there formal policies or plans that would be followed?
   c. Does your organization conduct phishing self-assessments?

E. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
   a. What are your most significant threats and vulnerabilities?
   b. What are your highest cyber security risks?

F. Does your IT department have a patch management plan in place? If so,
   a. Are risk assessments performed on all servers on the network?
   b. Are processes in place to proactively evaluate each server's criticality and applicability to software patches?
   c. Does this plan include a risk management strategy that addresses the following considerations?
      i. The risks of not patching reported vulnerabilities,
      ii. Extended downtime,
      iii. Impaired functionality, and
      iv. The loss of data?

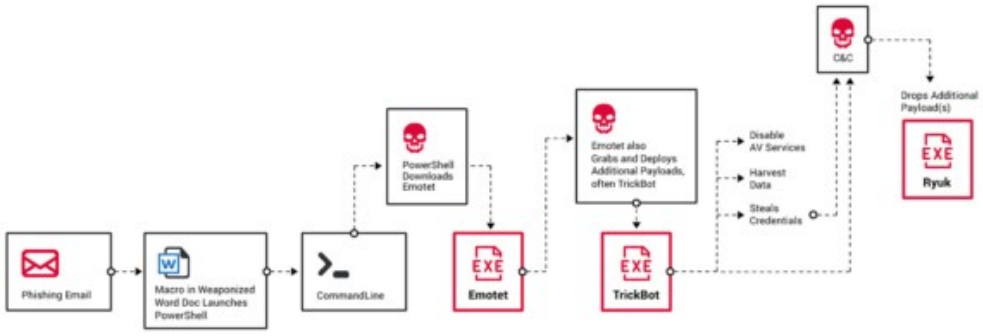
G. What do you look for in choosing an appropriate cyber incident response team?

B. Module 2

Day 4: 8:00 am

The CDG invites BB&T IT and executives to a call to review their prepared synopsis. This synopsis includes a summary of events that occurred since the initial infection and a plan for the eradiation of the virus. Here are some main points from the synopsis:

- CDG was able to isolate the infected computers and servers, meaning the uninfected computers and servers likely will not become infected.
- CDG confirms that this is an infection of the Ryuk virus.
- CDG has created a diagram like the one below to display the infection chain of the virus.



- CDG has determined that the best possible solution at this point is to erase operating systems and servers and resinstall them from a previous data backup.

BB&T responds positively to this solution and confirms that the last major backup was made a little over a week ago. Even though they will lose a small amount of company data, the executives are happy with any solution that does not involve paying a ransom.

Day 4: 9:00 am

CDG & BB&T begins working together to restore company data from backup. Infected computers and servers are wiped clean and fresh installs of the operating system are installed. Data is restored from the most recent backup.

BB&T executives & HR discuss plans to contract legal help as well as decide how to address the breach to media outlets.

Day 5: 5:00 pm

By this time, over half of the infected computers and servers are restored with fresh operating systems and restored data. CDG & BB&T decide to pause on their progress and resume tomorrow morning.

Day 6: 8:00 am

CDG & BB&T resume the restoration process from the previous day.

Day 6: 3:00 pm

CDG & BB&T completes the restoration process on all previosly infected computers and servers. CDG & BB&T work together to prepare a mitigation plan.

Day 6: 5:00 pm

CDG has a formal meeting with BB&T IT and executives. They determine the appropriate reglatory authorites to report the security breach to. CDG works with BB&T to determine how to patch and manage security tools such as a SIEM and EDRs to prevent a data breach like this from happening again.

Discussion Questions

Discussion questions included in each module may be modified as desired.

A. What notifications would be made? Consider internal (e.g., to leadership) and external (e.g., to law enforcement, government partners, etc.) notifications.

B. How does your organization baseline network activity? How would you be able to distinguish between normal and abnormal traffic?

C. What capabilities and resources are required for responding to this series of incidents?
    a. What internal resources do you depend on?
    b. Are your current resources sufficient?
    c. Do you have personnel tasked with incident response or a designated cyber incident response team within your organization?
        i. If so, what threshold must be reached for the cyber incident response personnel to be activated? Does this scenario reach that threshold?
        ii. Who is responsible for activating the cyber incident response personnel and under what circumstances?
        iii. What are the cyber incident response team/personnel's roles and responsibilities?

d. Who do you contact if you need additional third-party assistance?

D. What are your public affairs concerns?

a. Who is responsible for coordinating the public message? Is this process a part of any established plan?
b. How would your department respond to the media reports?
c. What information are you sharing with the public? Employees?
d. Are public information personnel trained to manage messaging related to cyber incidents?
e. Does your department have pre-drafted statements in place to respond to media outlets?
f. Does your department have staff trained to manage your social media presence?

E. What impact will the sale of sensitive or Personally Identifiable Information (PII) have on your response and recovery activities?

a. Have your public relations priorities changed?
b. Will it trigger any additional legal and/or regulatory notifications?

5 References

[1] "Glossary," *CSRC*. [Online]. Available: https://csrc.nist.gov/glossary. [Accessed: 05-Feb-2023].

[2] CISA, CISA Tabletop Exercise Package – Ransomware (2022).

[3] "Glossary," *CSRC*. [Online]. Available: https://csrc.nist.gov/glossary. [Accessed: 05-Feb-2023].