

The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice and does not necessarily reflect the opinion or policy position of the Municipal Association of South Carolina. Consult your attorney for advice concerning specific situations.




Choose Your Own Adventure Ransomware

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY



Exercise Objectives

1. Research suspicious alerts.
2. Investigate and respond to the incident to contain the threat.
3. Isolate and secure systems to prevent further compromise.
4. Communicate effectively with internal and external stakeholders.
5. Conduct a thorough post-incident analysis to improve future response.



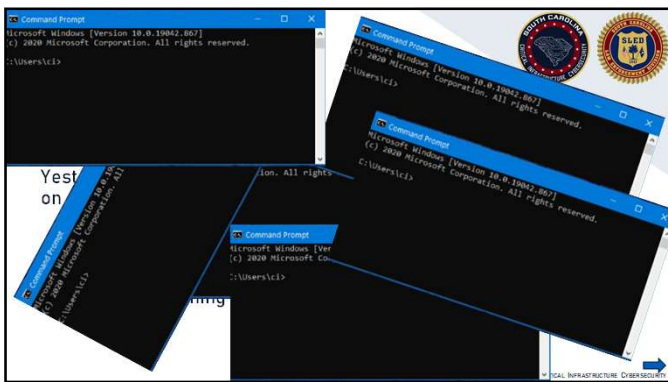
Exercise Guidelines

1. The entire scenario is **fictitious** but is based on real examples seen in the wild.
2. This exercise will be held in an **open, no-fault environment**. Varying viewpoints are expected.
3. Respond to the scenario using your knowledge of existing plans and capabilities, and insights derived from your training and experience.
4. Decisions are **not precedent-setting** and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions and/or suggested actions to resolve or mitigate a problem.

Once upon a time...



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

Upon receiving the device, what do you do?

1. Quarantine the device
2. Re-image the device
3. Inspect logs
4. Uninstall PuTTY



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

After re-imaging the computer...

You begin to receive
lateral movement alerts
for the File Share
Server.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

After uninstalling PuTTY....

The user continues to
experience the same
issues as before...

You decide to **quarantine**
the device before looking
into the issues further.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

Do You...

RE-IMAGE THE
DEVICE

INSPECT LOGS

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

You have decided to look at the File Share Server...



WHAT DO YOU LOOK FOR?

1. Look for running services?
2. Inspect logs?
3. Check installed software?

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

As you begin to look for your logs...



You quickly realize that they have all been **deleted**.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

You decide to evaluate the installed software on the File Share Server...



Upon further review, you notice that **ScreenConnect** was not supposed to be installed on the File Server.

Do you:

1. Uninstall ScreenConnect
2. Re-image the server
3. Quarantine the server

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

After quarantining the server...

You begin to receive **ransomware alerts** on the **domain controller** for the compromised user.

What do you do?

INVESTIGATE
USER ACTIVITY
ON THE SERVER

RE-IMAGE

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

Upon quarantining the device,

The **infected device** can no longer make network connections. What do you do?

1. Reimage the device
2. Inspect logs
3. Uninstall PuTTY

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

You start reviewing the logs...

Upon further review, you notice that a strange DLL file, titled **vulkan1.dll**, was created after the PuTTY file was unzipped and installed.

After this event occurred, you begin to notice odd network connections over **port 443** to an IP address associated with **Digital Ocean**.

Do you:

1. Look for the same DLL and hash on other devices
2. Check for traffic to malicious IP address
3. Block Malicious IP at Firewall
4. Check Initial Access User Login activity

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

As you check for the same hash
and DLL on other devices...

It comes back with no
matches.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

As you check for traffic to
malicious IP address

It comes back with no
matches.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

You try blocking the malicious IP
Address on the firewall.

The IP address block
was **successful**...

Until a **new malicious IP**
address pops up.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

As you review the initial access user login activity...



You find that the user has logged into the **File Share Server**. This requires further investigation, prompting you to look at the **File Share Server**.

When accessing the File Share Server, what do you look for?

Do you :

1. [Look for running services?](#)
2. [Inspect logs?](#)
3. [Check installed software?](#)

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

As you review the running services...



You notice that there are **several services** running on the File Share Server.

Which service do you want to investigate?

1. [PsExec](#)
2. [XblGameSave](#)
3. [ScreenConnect](#)

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

You decide to investigate the PsExec service...



The PsExec service running on the File Share Server is (surprisingly) not malicious

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

You decide to investigate XblGameSave...

As you are investigating **XblGameSave**, you notice that there is suspicious network traffic to your Domain Controller over **Port 139**.

Additionally, there was a subsequent user network login by the compromised user on the domain controller.

How do you proceed?

QUARANTINE SERVER

INVESTIGATE USER ACTIVITY ON THE SERVER

RE-IMAGE

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

The File Share Server is now quarantined...

Choose how to proceed...

LOOK FOR RANSOMWARE IOCS ON OTHER DEVICES

INVESTIGATE OTHER USER ACTIVITY

DECLARE THAT THE INCIDENT IS OVER & BEGIN RECOVERY

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

When looking for ransomware IOCs...

You are unable to find anything.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

You are now investigating other user activity on the File Share Server...

You notice spoolsvc.exe located in **C:\StorageReports\Scheduled**.

The executable did make network connections.

What do you do?


BLOCK IP AT FIREWALL

CHECK COMMANDLINE OF PROCESS

YOU DECIDE TO LOOK INTO THE SPOOL SVC.EXE FILE

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

When blocking the IP at the Firewall.



You are unable to find anything.

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY



You determine that this is a false positive.

You learn that **spoolsvc.exe** is expected to make network traffic

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

As you check the command line of the process...

It reveals that the traffic is actually **rclone** exfiltrating your data.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

Upon further review, you notice that **ScreenConnect** was not supposed to be installed on the File Server.

Do you:

1. Uninstall ScreenConnect
2. Re-image the server
3. Quarantine the server

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

After re-imaging the Server...

You begin to receive **ransomware alerts** on the **domain controller** for the compromised user.

What do you do?

QUARANTINE
SERVER

INVESTIGATE
USER
ACTIVITY ON
THE SERVER

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

After uninstalling ScreenConnect...

You begin to receive **ransomware alerts** on the **domain controller** for the compromised user.

What do you do?

QUARANTINE
SERVER

INVESTIGATE
USER ACTIVITY
ON THE SERVER

RE-IMAGE

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

After quarantining the server...

You begin to receive **ransomware alerts** on the **domain controller** for the compromised user.

What do you do?

QUARANTINE
SERVER

INVESTIGATE
USER ACTIVITY
ON THE SERVER

RE-IMAGE

SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

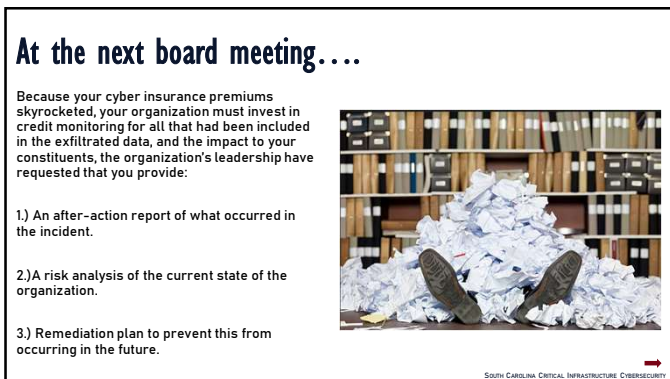
After re-imaging the server, you feel like the incident has concluded and you can begin recovery efforts...



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY








Congratulations! You have reached a resume generating event!


Someone had to be the scapegoat for the fallout from the incident.

You are sent packing.



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

DISCUSSION




SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY

CONTACT SC CIC

Want to learn more about SC CIC?

Visit the SC CIC Website for more information

<https://sccic.sc.gov/>



SOUTH CAROLINA CRITICAL INFRASTRUCTURE CYBERSECURITY
