Incident handler's journal

Scenario

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.

Additionally, employees also reported that a ransom note was displayed on their computers. The ransom note stated that all the company's files were encrypted by an organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. In exchange for restoring access to the encrypted files, the ransom note demanded a large sum of money in exchange for the decryption key.

The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, causing major disruptions in their business operations. The company was forced to shut down their computer systems and contact several organizations to report the incident and receive technical assistance.

Date: May 27, 2023	**Entry:** Entry # 1
Description	Documenting cybersecurity event
Tool(s) used	None
The 5 W's	● **Who:** A group of unethical hackers ● **What**: A ransomware security event ● **When:** Tuesday at 9:00AM ● **Where:** U.S. Health care clinic ● **Why**: The incident occurred due to a group of unethical hackers successfully shutting down business operations with a ransomware attack. This attack encrypted critical files causing major disruption into business operations. As a result the hacker is requesting a large sum of money in order to provide the decryption key.
Additional notes	How can the company prevent this ransomware event in the future? Should the company pay the large amount for the decryption key?

Scenario

You are a level-one security operations center (SOC) analyst at a financial services company. Previously, you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert.

Your organization's security policies and procedures describe how to respond to specific alerts, including what to do when you receive a phishing alert.

Ticket ID	**Alert Message**	**Severity**	**Details**	**Ticket status**
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	Escalated ▾

Ticket comments
An alert was sent of a detected phishing attempt of possible malware exposed to a member of the HR team. After further investigation there are several inconsistencies apparent in this email. To begin, the sender "76tguyhh6tgftrt7tg.su" signs as "Clyde West". Secondly there are many typos including in the subject line, the company name and in the body. Next, the email contains an .exe file which is uncommon for a cover letter and resume. Finally, the hashing of the file is a well known malicious file hashing. Based on the information collected the ticket A-2703 will be escalated to level-two SOC analyst.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, July 20, 2022 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,

I am writing for to express my interest in the engineer role posted from the website.

There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,

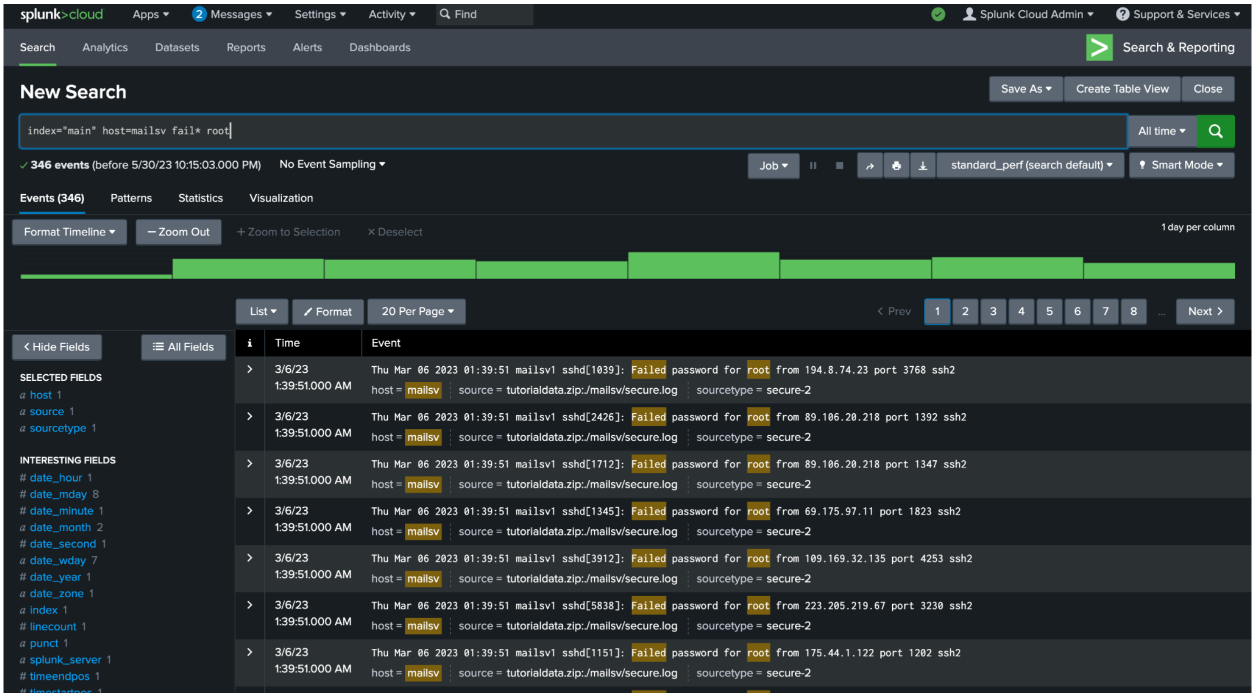
Clyde West
Attachment: filename="bfsvc.exe"

Date: May 27,	**Entry:** Entry #2
Description	Documenting
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. - **Who**: Def Communications - **What**: Phishing email event - **When:** July 20, 2022 - **Where**: Inergy

	● **Why**: A member of the human resource team had received an email from a threat actor expressing their interest in an engineering role. The HR member proceeded to download and open the file containing malware
Additional notes	Were members of the HR team properly trained to mitigate risk?

Scenario

You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.



New Search

```
index="main" host=mailsv fail* root
```

✓ **346 events** (before 5/30/23 10:15:03.000 PM) No Event Sampling

Events (346) Patterns Statistics Visualization

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 8
# date_minute 1
a date_month 2
# date_second 1
a date_wday 7
# date_year 1
a date_zone 1
a index 1
# linecount 1
a punct 1
a splunk_server 1
# timeendpos 1
# timestartpos 1

i	Time	Event
›	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
›	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[2426]: Failed password for root from 89.106.20.218 port 1392 ssh2 host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
›	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1712]: Failed password for root from 89.106.20.218 port 1347 ssh2 host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
›	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1345]: Failed password for root from 69.175.97.11 port 1823 ssh2 host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
›	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[3912]: Failed password for root from 109.169.32.135 port 4253 ssh2 host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
›	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[5838]: Failed password for root from 223.205.219.67 port 3230 ssh2 host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2
›	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv1 sshd[1151]: Failed password for root from 175.44.1.122 port 1202 ssh2 host = mailsv source = tutorialdata.zip:./mailsv/secure.log sourcetype = secure-2

Using Splunk we can determine the analysis of all login attempts to the e-commerce store Buttercup Games. Using the following command index=”main” host=”mailsv” fail* root we can filter the search query to find the specific information of failed login attempts. Each step of the query provides us valuable information index=”main” provides all the repository data from main. host =”mailsv” specifies the network host from which the event originated, in this case “mailsv” refers to the mail server in which our security issue is located. Finally fail* root searches all prefixes of fail this includes failure, failed, etc. and root searches any term with the root. As a result we have discovered there are more the 300 failed login attempts on the root server.

Date: 05.29.23	**Entry:** Entry #3
Description	Explore security issues with mail server
Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. ● **Who** N/A ● **What** N/A ● **When** N/A ● **Where** N/A ● **Why** N/A
Additional notes	Never used Splunk before but seems very user friendly and easy to filter the information that is needed.

Date: 05.29.23	**Entry:** Entry #4
Description	Capturing packet
Tool(s) used	tcpdump
The 5 W's	Capture the 5 W's of an incident. ● **Who** N/A ● **What** N/A ● **When** N/A ● **Where** N/A ● **Why** N/A
Additional notes	Using tcpdump to monitor network traffic was interesting , but also challenging. The syntax is a little more complex and I had to refer to stackoverflow to get some of the commands down. Ultimately I should practice with tcpdump some more to get better.

Reflections/Notes: **Were there any specific activities that were challenging?**
I really found the activity of tcpdump challenging due to the syntax used for the command line. I am still new to the command line and learning the syntax took sometime, but I believe with more practice I will become more proficient at it.