Incident Handlers Journal

Scenario 1

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: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None were provided
The 5 W's	**Who caused the incident?**: An organized group of unethical hackers **What happened?**: A ransomware security incident **Where did the incident happen?**: At a health care company **When did the incident occur?**: Tuesday 9:00 a.m. **Why did the incident happen**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? **Training awareness of phishing emails** 2. Should the company pay the ransom to retrieve the decryption key? **No, it will not guarantee that the systems are restored and may encourage further attacks**

Investigate a Suspicious Hash File

Scenario 2

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.

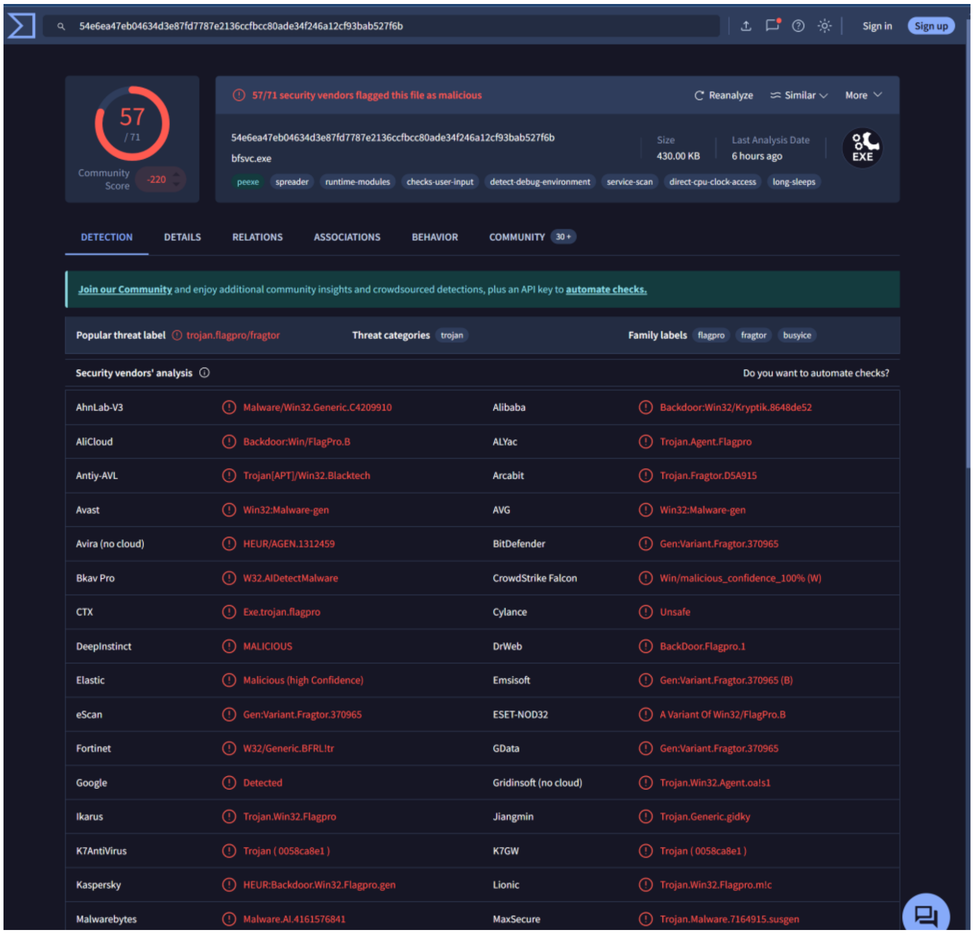
You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a hash function is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint.

Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

Response

The file hash has been reported as malicious by over 50 vendors. The community score is -220. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.

Using the Pyramid of Pain, we can list attributes as Indicators of compromise.



57/71 security vendors flagged this file as malicious

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe

Size: 430.00 KB
Last Analysis Date: 6 hours ago

peexe · spreader · runtime-modules · checks-user-input · detect-debug-environment · service-scan · direct-cpu-clock-access · long-sleeps

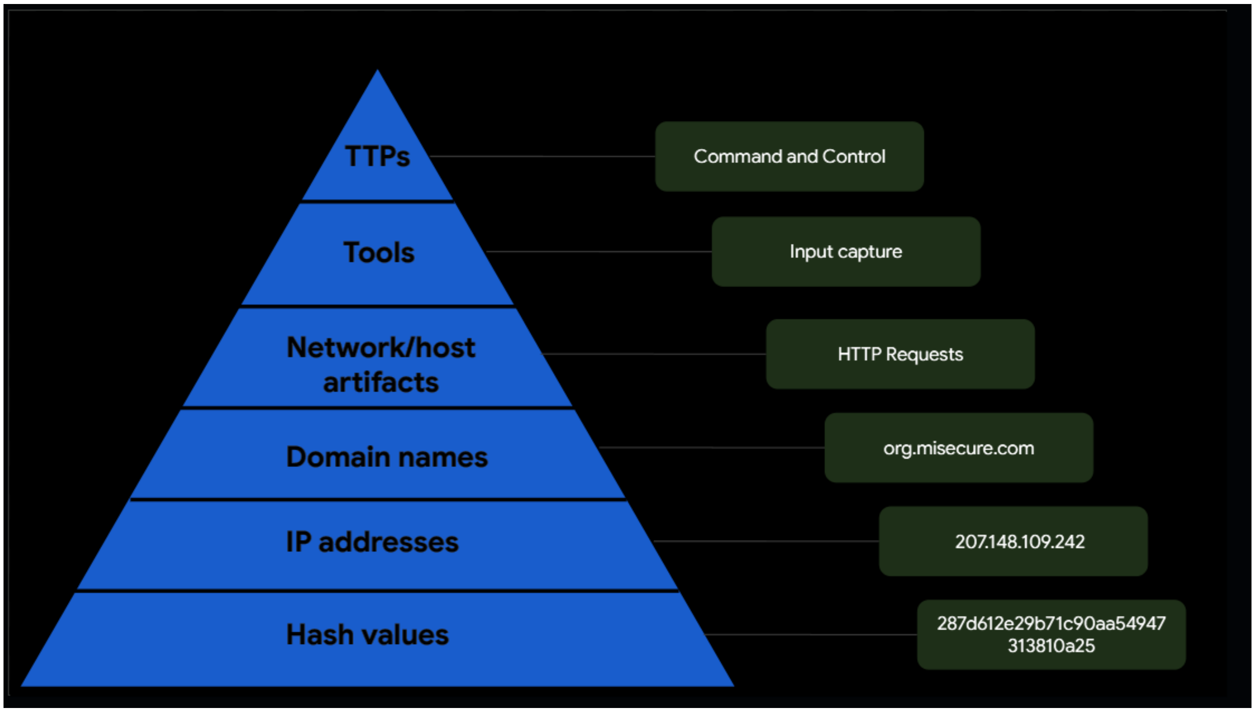
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.flagpro/fragtor
Threat categories: trojan
Family labels: flagpro · fragtor · busyice

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C4209910	Alibaba	Backdoor:Win32/Kryptik.8648de52
AliCloud	Backdoor:Win/FlagPro.B	ALYac	Trojan.Agent.Flagpro
Antiy-AVL	Trojan[APT]/Win32.Blacktech	Arcabit	Trojan.Fragtor.D5A915
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1312459	BitDefender	Gen:Variant.Fragtor.370965
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.flagpro	Cylance	Unsafe
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Flagpro.1
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Fragtor.370965 (B)
eScan	Gen:Variant.Fragtor.370965	ESET-NOD32	A Variant Of Win32/FlagPro.B
Fortinet	W32/Generic.BFRL!tr	GData	Gen:Variant.Fragtor.370965
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.oa!s1
Ikarus	Trojan.Win32.Flagpro	Jiangmin	Trojan.Generic.gidky
K7AntiVirus	Trojan (0058ca8e1)	K7GW	Trojan (0058ca8e1)
Kaspersky	HEUR:Backdoor.Win32.Flagpro.gen	Lionic	Trojan.Win32.Flagpro.m!c
Malwarebytes	Malware.AI.4161576841	MaxSecure	Trojan.Malware.7164915.susgen



Date: January 18, 2024	**Entry:** #1
Description	A malicious file was detected, and needs to be analyzed to determine if the alert is a true positive.
Tool(s) used	VirusTotal : Investigative tools to analyze files and URLs for malicious content such as viruses, worms, trojans, and more.
The 5 W's	**Who caused the incident?**: Threat actor **What happened?**: An email contained a malicious file **Where did the incident occur?** : Email **When did the incident happen?**: 1:20 pm : an IDS alerted of the executable file **Why did the Incident happen?**: Upon receiving the malicious content on the email, the employee downloaded and executed the malicious file.
Additional notes	**How to prevent the incident?** Files should only be download/ opened from trusted sources. Training should be given to employees on phishing awareness

Respond to a Phishing Incident

Scenario 3

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.

In the playbook, there is a flowchart and written instructions to help you complete your investigation and resolve the alert. At the end of your investigation, you will update the alert ticket with your findings about the incident.

Date: January 18, 2024	**Entry:** #1
Description	Playbook to respond to phishing incidents. Playbooks are created during the Preparation phase. However, it can be used during Detection & Analysis, Containment Eradication and Recovery, and Post Incident Activity.
Tool(s) used	Playbook Alerting ticket status (JIRA, etc.)
The 5 W's	**Who caused the incident?**: Threat actor **What happened?**: Upon investigating, the ticket ID was created (A-AD3CO). The alet was flagged as a phishing attempt. The severity of the damage is medium. The user opened a malicious email and opened attachments. The status is escalated. **Where did the incident occur?** : Email **When did the incident happen?**: January 17th, 1:20 pm **Why did the Incident happen?**: This happened as a result of an employee opening a malicious file and clicking a link from an unknown sender.
Additional notes	**Escalated**

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
The alert detected that an employee downloaded and opened a malicious file from a phishing email. The senders email address is a sequence of randomized characters. The email body and subject line contained grammatical errors. The email's body also contained a password-protected attachment, "bfsvc.exe," which was downloaded and opened on the affected machine. The alert severity is reported as medium. With these findings, the ticket should be escalated for further action.

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"

Phishing Playbook

Step 1: Receive phishing alert

The process begins when you receive an alert ticket indicating that a phishing attempt has been detected.

Step 2: Evaluate the alert

Upon receiving the alert, investigate the alert details and any relevant log information. Here is a list of some of the information you should be evaluating:

1. **Alert severity**
    - **Low**: Does not require escalation
    - **Medium**: May require escalation

      High: Requires immediate escalation to the appropriate security personnel
2. **Receiver details**
    - The receiver's email address
    - The receiver's IP address
3. **Sender details**
    - The sender's email address
    - The sender's IP address
4. **Subject line**
5. **Message body**
6. **Attachments or links**.

Note: **Do not** open links or attachments on your device unless you are using an authorized and isolated environment.

Step 3.0: Does the email contain any links or attachments?

Phishing emails can contain malicious attachments or links that are attempting to gain access to systems. After examining the details of the alert, determine whether the email contains any links or attachments. If it does, **do not** open the attachments or links and proceed to **Step 3.1**. If the email does not contain any links or attachments, proceed to **Step 4**.

Step 3.1: Are the links or attachments malicious?

Once you've identified that the email contains attachments or links, determine whether the links or attachments are malicious. Check the reputation of the link or file attachment through its hash values using threat intelligence tools such as VirusTotal. If you've confirmed that the link or attachment is **not malicious,** proceed to **Step 4**.

Step 3.2: Update the alert ticket and escalate

If you've confirmed that the link or attachment is **malicious**, provide a summary of your findings and the reason you are escalating the ticket. Update the ticket status to **Escalated** and notify a level-two SOC analyst of the ticket escalation.

Step 4: Close the alert ticket

Update the ticket status to **Closed** if:

- You've confirmed that the email does not contain any links or attachments
  or

- You've confirmed that the link or attachment **is not malicious.**

Include a brief summary of your investigation findings and the reason why you've closed the ticket.