Phishing Incident Investigation 2024-12-18 #1

Globe Sistemas - Av. Libertador Jardin America

Activity summary

A phishing incident involving a malicious file hash will be responded to. This is the same SHA256 File Hash that was previously investigated and verified as malicious. The instructions in the organization's Phishing Playbook will be followed to investigate and resolve the incident alert ticket.

Playbooks describe the step-by-step actions required to properly respond to a security incident. For security analysts, playbooks serve as a guide to effectively support an organization's incident response efforts.

Coordinated, effective and rapid action is critical during incident response and can help security teams minimize the impact of an incident and reduce incident response time.

Scenery

As a Tier1 Analyst in the Security Operations Center (SOC) at an IT, Analytics, and Cybersecurity services company, a phishing alert was received regarding a suspicious file being downloaded to an employee's computer. After investigating the hash of the file attached to the email, it was found that the attachment is malicious.

Now that you have this information, you should follow your organization's process to complete the 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.

At the end of the investigation, the alert ticket will be updated with the findings regarding the incident.

Update alert ticket status

In the alert ticket, the investigation is started by updating the Ticket Status drop-down list to Investigating.

Alert evaluation

The content of the alert ticket will then be evaluated, including the content of the Additional Information section:

**Sender Details** : There is an inconsistency between the sender email address “ 76tguy6hh6tgftrt7tg.su '”, the name used in the email body “ Clyde West ”, and the sender name, “ Def Communications ”.

**Message body** : The email body and subject line contained grammatical errors . The email body also contained a password-protected attachment, “ bfsvc.exe ,” which was downloaded and opened on the affected machine.

**Attachments or Links** : After having previously investigated the file hash, it was confirmed that it is a known malicious file.

Attachment: filename=" bfsvc.exe "

5W Research

* Who caused the incident?

Research through VirusTotal indicates that This Hash file is the Flagpro malware , which has been used by the BlackTech actor .

* What happened?

IDS software alert detected and alerted the SOC of a malicious file downloaded from a phishing email.

* When did the incident occur?

Thursday, December 16, 2024 09:30:14 AM . Below is a timeline of events leading up to this alert:

09:30:14 AM : An employee receives an email containing an attachment.

09:33:18 AM : The employee successfully downloads and opens the file.

09:34:01 AM : Several unauthorized executable files are created on the employee's computer.

09:35:22 AM : An intrusion detection system detects the executables and sends an alert to the SOC.

* Where did the incident occur?

Security Operations Center (SOC) of Globe Systems, a computer services, IT, analysis and cybersecurity company providing IDS cybersecurity services for a third party.

* Why did it happen?

Because an employee downloaded and opened a malicious file from a phishing email.

Exhaustive Research

A more comprehensive crowdsourcing investigation has determined that More than 50 vendors have reported that the file hash is malicious.

Also This file hash has been discovered to be the Flagpro malware , which has been commonly used by the advanced threat actor BlackTech .

**Hash value:** 287d612e29b71c90aa54947313810a25 is also an MD5 Hash associated with this malware according to the Details tab of the VirusTotal report .

**IP Address** : The IP address 104.115.151.81 is the one this malware contacted, it appears as one of many IP addresses in the Relationships tab of the VirusTotal report. This IP address is also associated with the domain org.misecure.com as listed in the DNS Resolutions section under the Behavior tab of the Zenbox sandbox\* report.

\* Sandbox = is an isolated testing environment used as offensive/active cybersecurity measures, allowing users and businesses to run programs or execute files without affecting the application, system, or platform they are running on . )

**Domain name:** org.misecure.com ( *http://org.misecure.com/index.html* ) is reported as a contacted malicious domain in the Relationships tab of the VirusTotal Report.

**Network artifact/host artifact** : Network-related artifacts observed in this malware are HTTP Requests made to the org.misecure.com domain. This appears in the Network Communications section of the Behavior tab of the Venus Eye isolated spaces and Rising MOVES sandbox reports.

**Tools** : Input Capture appears in the Collection section of the Behavior tab of the Zenbox Sandbox report.

**Malicious actors use input capture to steal user data such as passwords, credit card numbers, and other sensitive information.**

**Tactics, Techniques, and Procedures (TTPs)** : TTPs describe an attacker's behavior. Command and Control appears as a tactic in the Behavior tab of the Zenbox Sandbox Report. Malicious actors use Command and Control to establish communication channels between an infected system and their own system.

Determine if the alert should be escalated and update ticket status

**Escalation** : The ticket requires escalation to a Tier2 SOC analyst for further action, because the email contains/had known malicious attachments and was opened and executed as per the playbook instructions.

**Alert Severity** : Alert severity is raised to MEDIUM .

Attached is a graphic called The Pain Pyramid explaining the importance of each IoC (indicator of commitment and its degree of importance according to its position in the pyramid).