IOC Indicators 2024-12-16 #2

Globe Sistemas - Av. Libertador Jardin America

Activity summary

will be analyzed using VirusTotal and details about its related indicators of compromise will be captured using the Pyramid of Pain.

The Pyramid of Pain, which is used to understand the different types of indicators of compromise (IoC). An IoC is observable evidence that suggests signs of a potential security incident.

The Pyramid of Pain describes the relationship between IoCs and the level of difficulty malicious actors experience when IoCs are blocked by security teams.

VirusTotal is one of the many tools that security analysts use to identify and respond to security incidents. VirusTotal is a service that allows you to scan suspicious files, domains, URLs, and IP addresses for malicious content.

Through crowdsourcing, VirusTotal collects and reports threat intelligence from the global cybersecurity community. This helps us determine which IoCs have been reported as malicious.

Scenery

As a Tier One Security Operations Center (SOC) analyst, you have received an alert about a suspicious file being downloaded to an employee's computer.

This alert has been investigated and it was discovered that the employee received an email containing an attachment.

The attachment was a password-protected spreadsheet. The password for the spreadsheet was provided in the email. The employee downloaded the file and entered the password to open it. When the employee opened the file, a malicious payload was executed on the employee's computer.

The malicious file was recovered and a SHA256 hash of the file was created. The hash is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint. VirusTotal will be used to discover other IoCs associated with the file.

Reviewing alert details

The following information contains details about the alert. Details include a file hash and a timeline of the event.

**SHA256 file hash** : 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

More than 50 vendors have reported that the file hash is malicious .

Upon further investigation, this file hash has been discovered to be the Flagpro malware , which has been commonly used by the advanced threat actor BlackTech .

Here 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 executable files and sends an alert to the SOC.

Indicators of Compromise IOC (Indicator of Compromise)

After exploring the sections of the VirusTotal report, other IoCs were discovered that are associated with the file according to the VirusTotal report.

**Hash value:** 287d612e29b71c90aa54947313810a25 is 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.

**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 Sandbox 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.

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