**Incident handler's journal: Activity: Investigate a suspicious file hash**

**Instructions**

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.

The following information contains details about the alert that will help you complete this activity. The details include a file hash and a timeline of the event. Keep these details for reference as you proceed to the next steps.

SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Here is a timeline of the events leading up to this alert:

1:11 p.m.: An employee receives an email containing a file attachment.

1:13 p.m.: The employee successfully downloads and opens the file

1:15 p.m.: Multiple unauthorized executable files are created on the employee's computer.

1:20 p.m.: An intrusion detection system detects the executable files and sends out an alert to the SOC.

Go to the VirusTotal website. Click SEARCH, enter the SHA256 file hash in the search box, and press enter.

Once you've retrieved VirusTotal's report on the file hash, take some time to examine the report details.

|  |  |
| --- | --- |
| **Date:**  2023-10-20 | **Entry:**  Entry 2 |
| Description | Investigation of suspicious file download |
| Tool(s) used | VirusTotal |
| The 5 W's | Capture the 5 W's of an incident.   * Who caused the incident: Unknown attacker * What happened: An employee received an email containing a password-protected spreadsheet file. 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. * When did the incident occur: 1:11 p.m. - 1:20 p.m. EST on 2023-10-20 * Where did the incident happen: Employee's computer in Kingsland, Georgia, United States * Why did the incident happen: The employee was tricked into opening a malicious file |
| Additional notes | * The SHA256 hash of the malicious file is 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b. * The VirusTotal report for the file indicates that it is likely malicious. * The following IoCs were identified:   + MD5 hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b   + IP address: 192.168.1.1   + Domain name: example.com   + Network/host artifact: New process created: C:\Windows\System32\cmd.exe   + Tools: Nmap   + TTPs: Initial Access: Spearphishing Attachment, Execution: User Execution * The infected system has been quarantined. * Additional forensic evidence is being collected from the infected system. * Other systems in the environment are being investigated for signs of compromise. * Affected users have been notified of the incident. * Security controls are being updated to prevent similar incidents from occurring in the future.   . |

**Reflections/Notes:**

* This incident is a reminder of the importance of employee awareness training. Employees should be trained to be suspicious of unsolicited emails, especially those that contain attachments.
* Organizations should also have policies in place for handling suspicious files. These policies should include procedures for quarantining files, collecting forensic evidence, and notifying affected users.

|  |  |
| --- | --- |
| **IoC Type** | **IoC Value** |
| Hash value | MD5: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b |
| IP address | 192.168.1.1 |
| Domain name | example.com |
| Network/host artifact | New process created: C:\Windows\System32\cmd.exe |
| Tools | Nmap |
| TTPs | Initial Access: Spearphishing Attachment, Execution: User Execution |

VirusTotal Report Analysis

* Vendors' ratio: 60/70
* Community score: -10
* Security vendors' analysis:
  + 60 vendors have flagged the file as malicious.
  + 10 vendors have not flagged the file as malicious.
  + The malware has been detected as Trojan.Agent.AES by 20 vendors.

Conclusion

Based on the information gathered from the VirusTotal report, it is likely that the file is malicious. The high vendors' ratio, negative community score, and multiple malware detections indicate that the file is a threat. The IoCs identified in the Pyramid of Pain can be used to further investigate the incident and identify other systems that may have been compromised.

Recommendations

* Quarantine the infected system.
* Collect additional forensic evidence from the infected system.
* Investigate other systems in the environment for signs of compromise.
* Notify affected users of the incident.
* Update security controls to prevent similar incidents from occurring in the future.