

## Scenario

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.

**Has this file hash been reported as malicious? Explain why or why not.**

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

**TTPs**

Command and Control

**Tools**

Input capture

**Network/host  
artifacts**

HTTP Requests

**Domain names**

org.misecure.com

**IP addresses**

207.148.109.242

**Hash values**

287d612e29b71c90aa54947  
313810a25

