Case Study:

Investigate a Suspicious File Hash

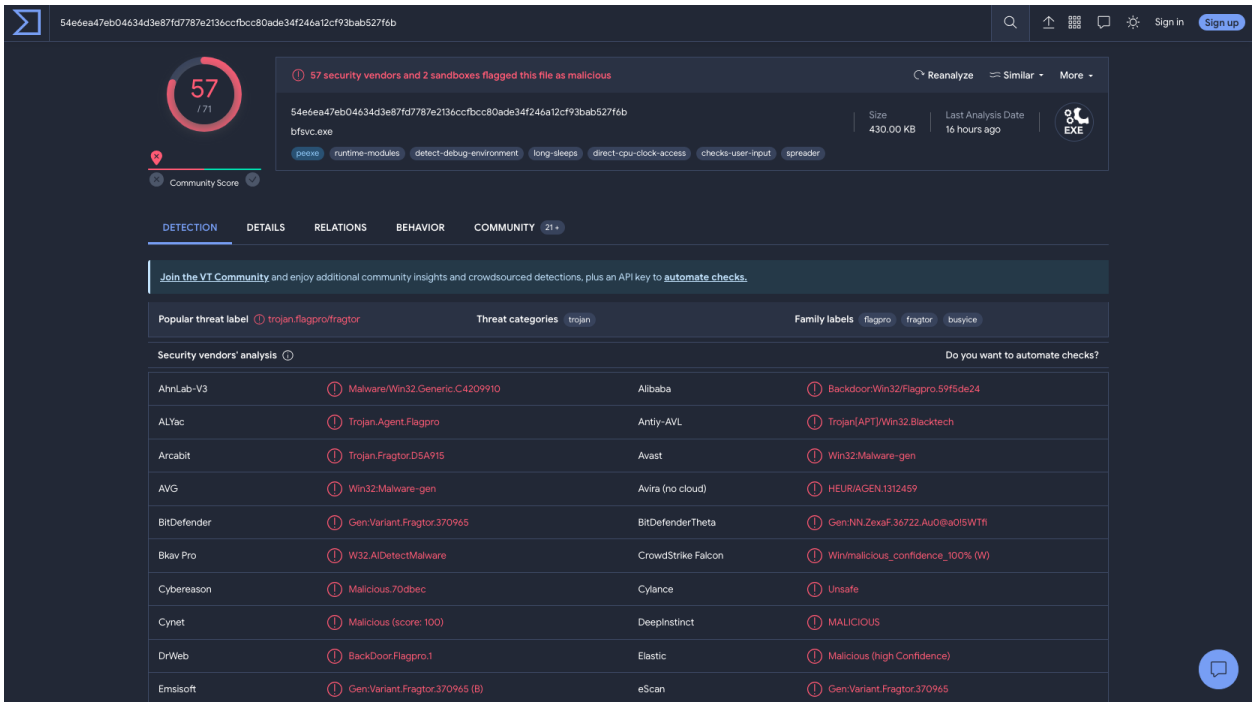
Scenario:

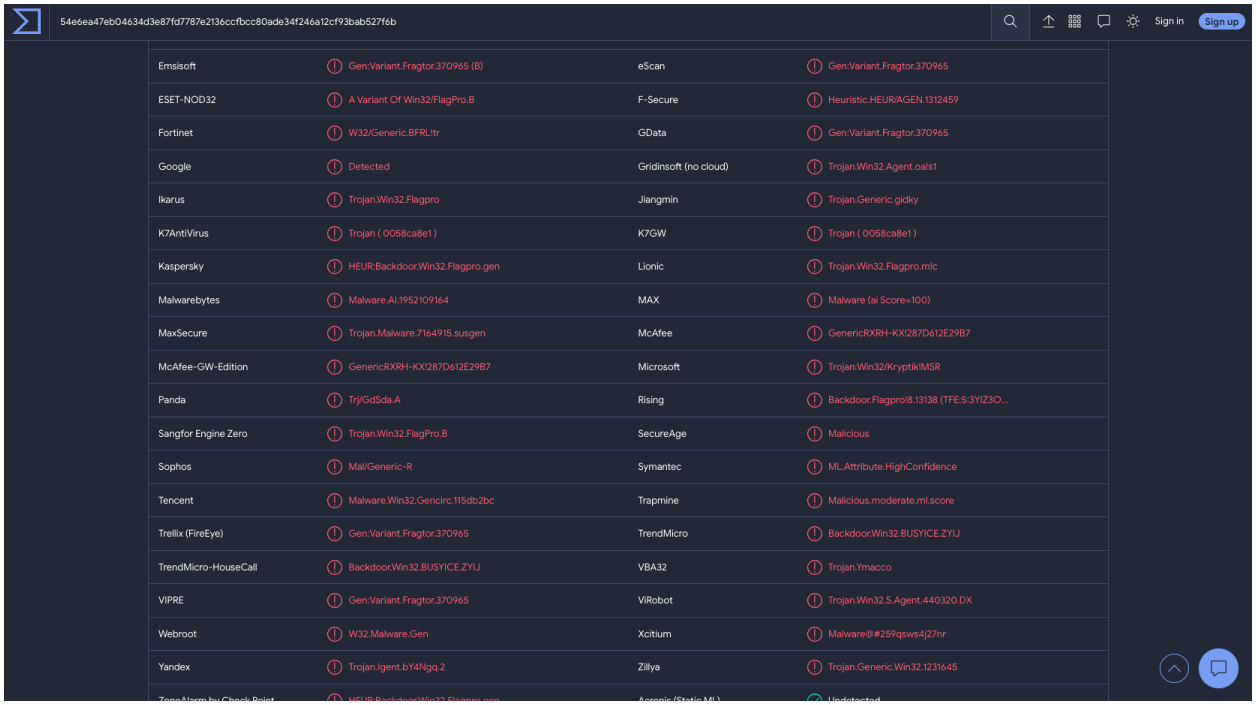
You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

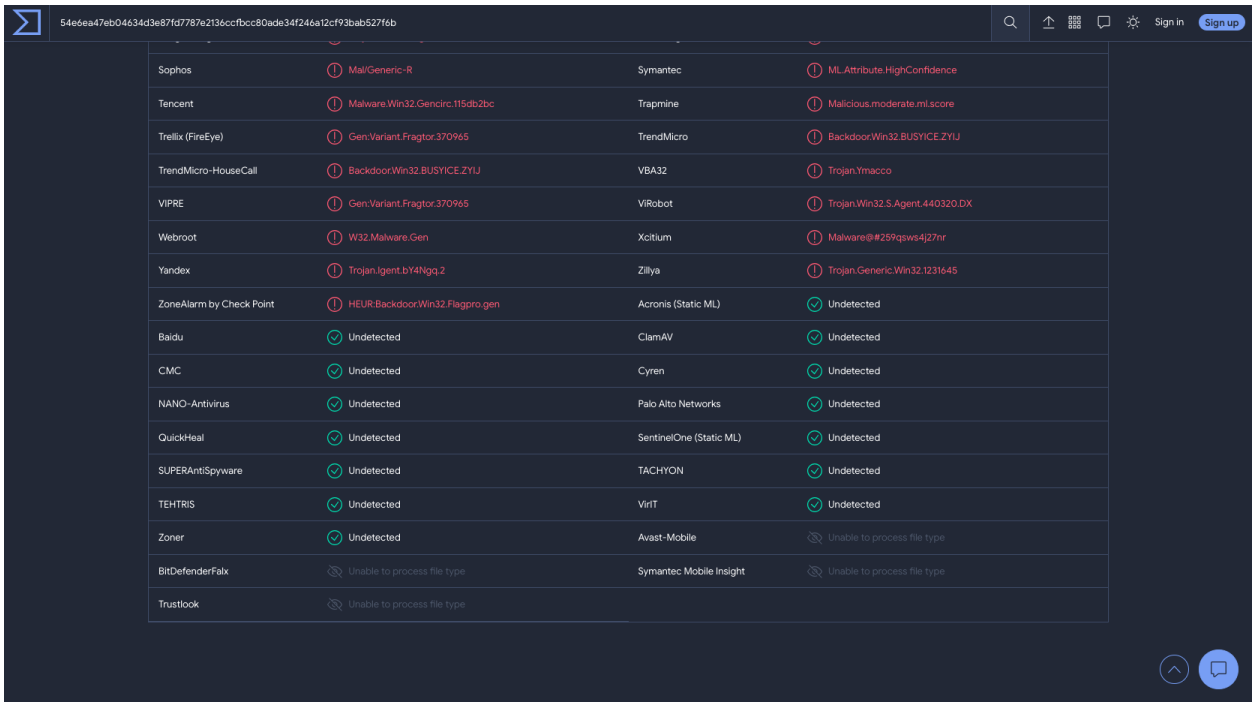
You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the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


54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Sign in
Sign up
57
/ 71
Community Score
57 security vendors and 2 sandboxes flagged this file as malicious
Reanalyze
Similar
More
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe
peexe
runtime-modules
detect-debug-environment
long-sleeps
direct-cpu-clock-access
checks-user-input
spreader
Size
430.00 KB
Last Analysis Date
16 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 21+
Join the VT 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/Flagpro.59f5de24
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
BitDefenderTheta Gen:NN.ZexaF.36722.Au0@a0l5WTfi
Bkav Pro W32.AIDetectMalware
CrowdStrike Falcon Win/malicious_confidence_100% (W)
Cybereason Malicious.70dbec
Cylance Unsafe
Cynet Malicious (score: 100)
DeepInstinct MALICIOUS
DrWeb BackDoor.Flagpro.1
Elastic Malicious (high Confidence)
Emsisoft Gen:Variant.Fragtor.370965 (B)
eScan Gen:Variant.Fragtor.370965


54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Sign in
Sign up
Emsisoft Gen:Variant.Fragtor.370965 (B)
eScan Gen:Variant.Fragtor.370965
ESET-NOD32 A Variant Of Win32/FlagPro.B
F-Secure Heuristic.HEUR/AGEN.1312459
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.1952109164
MAX Malware (ai Score=100)
MaxSecure Trojan.Malware.7164915.susgen
McAfee GenericRXRH-KX!287D612E29B7
McAfee-GW-Edition GenericRXRH-KX!287D612E29B7
Microsoft Trojan:Win32/Kryptik!MSR
Panda Trj/GdSda.A
Rising Backdoor.Flagpro!8.13138 (TFE:5:3YIZ3O...
Sangfor Engine Zero Trojan.Win32.FlagPro.B
SecureAge Malicious
Sophos Mal/Generic-R
Symantec ML.Attribute.HighConfidence
Tencent Malware.Win32.Gencirc.115db2bc
Trapmine Malicious.moderate.ml.score
Trellix (FireEye) Gen:Variant.Fragtor.370965
TrendMicro Backdoor.Win32.BUSYICE.ZYIJ
TrendMicro-HouseCall Backdoor.Win32.BUSYICE.ZYIJ
VBA32 Trojan.Ymacco
VIPRE Gen:Variant.Fragtor.370965
ViRobot Trojan.Win32.S.Agent.440320.DX
Webroot W32.Malware.Gen
Xcitium Malware@#259qsws4j27nr
Yandex Trojan.Igent.bY4Ngq.2
Zillya Trojan.Generic.Win32.1231645



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.