

## Analysis of Files and URLs for malicious content and IoCs using VirusTotal, Utilizing the Pyramid of Pain Framework

---

### Incident Report

<b>Date:</b> May 13, 2023	<b>Entry:</b>  175-A2
Description	Investigating a suspicious file hash. This incident occurred in the <b>Detection and Analysis</b> phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.
Tool(s) used	<ul style="list-style-type: none"><li>• VirusTotal</li></ul> <p>An investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. I used VirusTotal to analyze a file hash, which was reported as malicious.</p>
The 5 W's	<ul style="list-style-type: none"><li>• <b>Who:</b> An unknown malicious actor</li><li>• <b>What:</b> An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b</li><li>• <b>Where:</b> An employee's computer at a financial services company</li><li>• <b>When:</b> At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file</li><li>• <b>Why:</b> An employee was able to download and execute a malicious file attachment via e-mail.</li></ul>
Additional notes	How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on?

---

The activity is about analyzing an artifact using VirusTotal, a threat intelligence platform, and capturing details about its indicators of compromise (IoCs) using the Pyramid of Pain. It involves investigating a suspicious file downloaded on an employee's computer, retrieving its hash, and using

VirusTotal to gather more information about the file, such as detection verdicts, related IoCs, and behavioral patterns.

Details about the alert include a file hash and a timeline of the event:

**SHA256 file hash:** 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

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 alerts the SOC.

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

hash lookup

56 security vendors and 2 sandboxes flagged this file as malicious

Reanalyze Download Similar More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size 430.00 KB Last Analysis Date 11 hours ago

peexe runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input spreader

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label **trojan.flagpro/jaik** Threat categories trojan Family labels flagpro jaik busyice

Security vendors' analysis

AhnLab-V3	Malware/Win32.Generic.C4209910	Alibaba	Backdoor/Win32/Flagpro.59f5de24
ALYac	Trojan.Agent.Flagpro	Anity-AVL	Trojan(APTJ)/Win32.Blacktech
Arcabit	Trojan.Jaik.D1594C	Avast	Win32/Malware-gen
AVG	Win32/Malware-gen	Avira (no cloud)	HEUR/AGEN.1312459
BitDefender	Gen:Variant.Jaik.88396	BitDefenderTheta	Gen:NN.ZexaF.36250.Au0@a015W7f

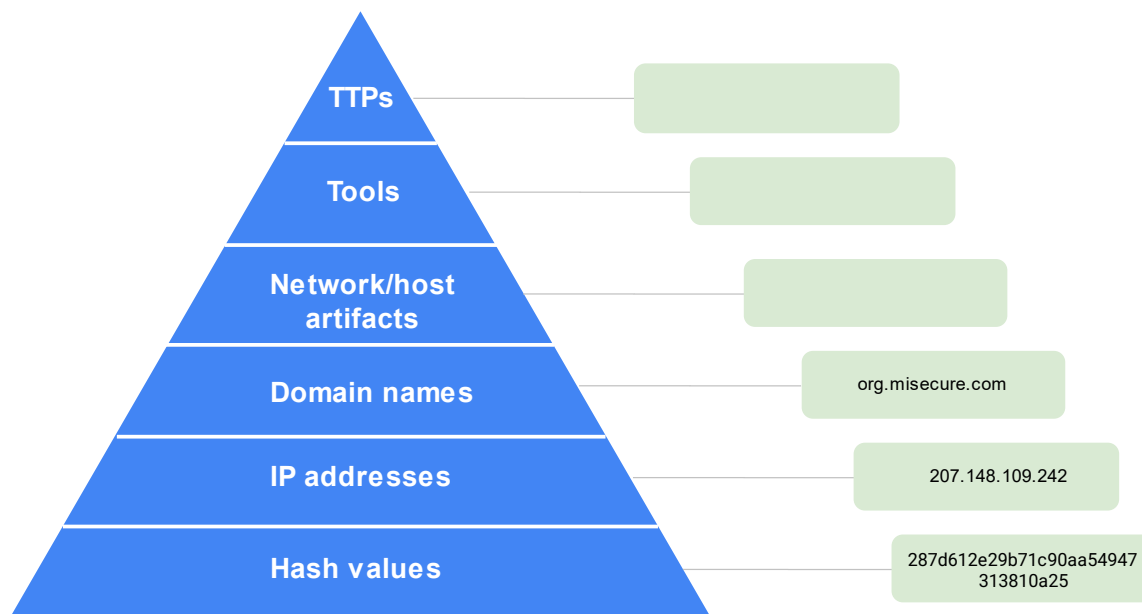
Do you want to automate checks?

Basic properties

MD5	287d612e29b71c90aa54947313810a25
SHA-1	8f35a9e70dbec8f1904991773f394cd4f9a0775e
SHA-256	54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Vhash	045056655d155510232122577z305bz2fz
Authenticity hash	019439329ea87e4559b653ad7df933d20623bdd00d3793abc7ff35e57db24853
Imphash	a59ed1599cc2f8311b215c83c51a2cc4
Rich PE header hash	1f4064adca28866f7447aaf031074807
SSDEEP	6144:CdaRD0n4URr6zIKgDCVh84DLn5X3WIDSVS1dGSLaYWis:XRompRr0lKgDCY4DLVW3UJSL4R
TLSH	T13594AD933541C371CA177D7695789AAD4B3F8D3816BAB967B3B83B8F5C303918636902
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (7.6%) Win32 Executable (generic) (6.8%)
DetectItEasy	PE32 Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] Compiler: Microsoft Visual C/C++ (2008) [libcm] Linker: Microsoft Linker (9.0) [GUI32]
File size	430.00 KB (440320 bytes)

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.

## Utilizing the Pyramid of Pain Framework



In this lab, I learned how to effectively use VirusTotal as a security analyst to gain insights into potential security incidents. I gained skills in:

- Utilizing VirusTotal to analyze files, domains, URLs, and IP addresses for malicious content.
- Understanding the importance of shared threat intelligence from the global cybersecurity community.
- Assessing detection verdicts from multiple security vendors to evaluate the maliciousness of a file.
- Identifying and documenting different types of IoCs, such as hash values, IP addresses, domain names, network/host artifacts, tools, and tactics/techniques/procedures (TTPs).
- Analyzing sandbox reports to gain insights into the behavioral patterns and actions of malware.
- Using the Pyramid of Pain framework to categorize and prioritize IoCs based on their difficulty for malicious actors to evade detection or mitigate.

Overall, this activity enhanced my skills in investigating security incidents, leveraging threat intelligence platforms, and making informed decisions based on the analysis of IoCs. It emphasized the importance of using multiple sources of information, staying updated with the latest security trends, and continuously learning to improve detection capabilities.