Ticket ID	Alert Message	Severity	Details	Ticket status
A-2703	SERVER-MAIL Phishing attempt possible download of malware	Medium	The user may have opened a malicious email and opened attachments or clicked links.	Escalated

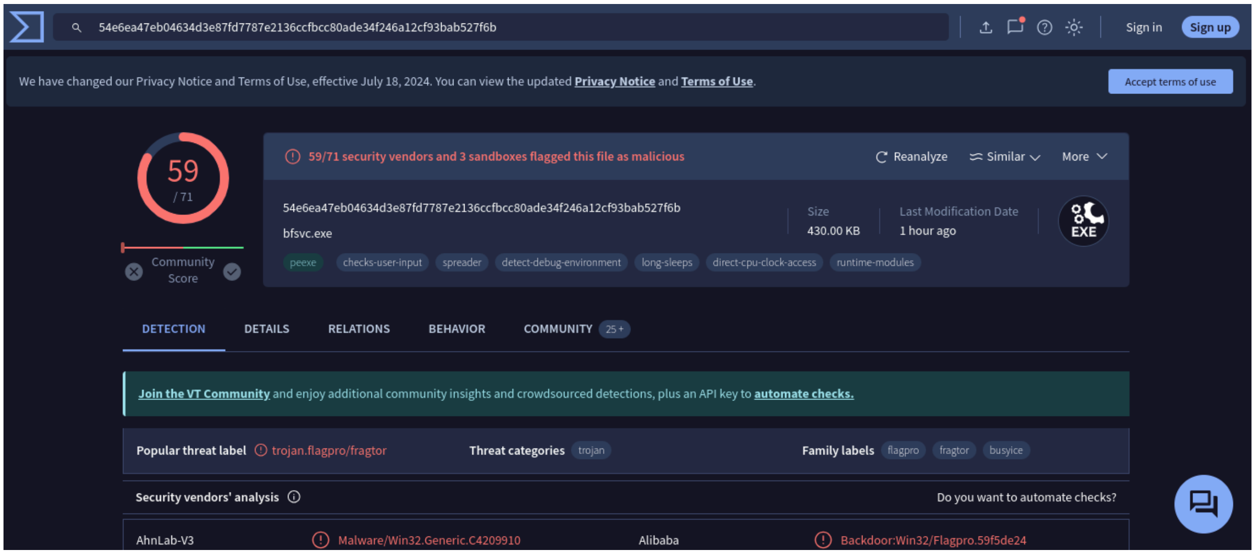
Ticket comments
I received an alert of a phishing attempt with a possible malicious file attachment, I proceeded to evaluate the alert and found multiple indications of it being a legitimate alert. There were inconsistencies between the sender's email address and the name signed at the end of the email, as well as the subject of the email containing multiple spelling and grammatical errors. The email contained an attachment that I investigated with VirusTotal using a file hash value and determined it as malicious. I'm escalating the ticket to the level-two SOC analyst.

Additional information

Known malicious file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Email:
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>
Sent: Wednesday, July 20, 2022 09:30:14 AM
To: <hr@inergy.com> <176.157.125.93>
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,
I am writing for to express my interest in the engineer role posted from the website.
There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.
Thank you,
Clyde West
Attachment: filename="bfsvc.exe"



We have changed our Privacy Notice and Terms of Use, effective July 18, 2024. You can view the updated **Privacy Notice** and **Terms of Use**.

59/71 security vendors and 3 sandboxes flagged this file as malicious

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size	Last Modification Date
430.00 KB	1 hour ago

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

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

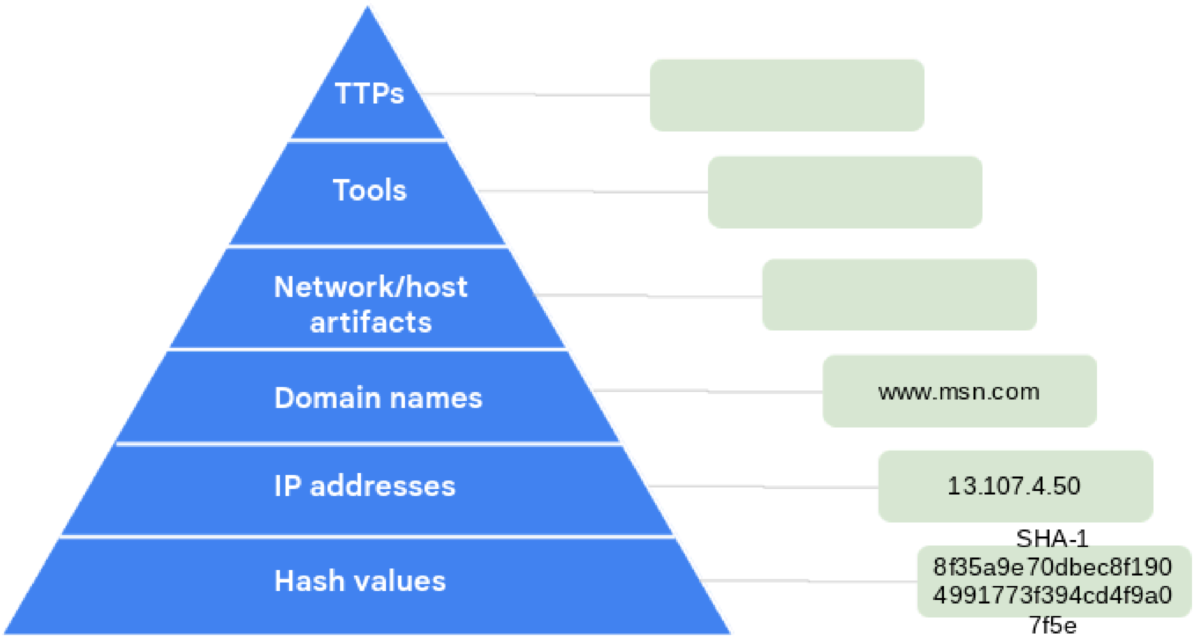
Popular threat label trojan.flagpro/fragtor **Threat categories** trojan **Family labels** flagpro fragtor busyice

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C4209910	Alibaba	Backdoor:Win32/Flagpro.59f5de24

Has this file been identified as malicious? Explain why or why not.

This file is malicious. Based on the file hash 59 out of 73 security vendors marked it as either a Trojan, malicious, suspicious or unsafe, as well as a community score of -89 its safe to assume that the file is malicious



TTPs

Tools

Network/host artifacts

Domain names — www.msn.com

IP addresses — 13.107.4.50

Hash values — SHA-1 8f35a9e70dbec8f190 4991773f394cd4f9a0 7f5e