Threat Intelligence with Virus Total

Executive Summary

Subject: Use of VirusTotal for Threat Intelligence and Malware Analysis
Case Focus: Analysis of a Malicious Executable (bfsvc.exe)

Purpose of VirusTotal

VirusTotal is a widely used threat intelligence platform that aggregates file, URL, domain, and IP data from dozens of antivirus engines, sandboxes, and reputation sources.

It enables:
- Rapid detection of malware and suspicious files
- Behavior analysis through sandbox execution
- Infrastructure mapping via URLs, IPs, and domains
- Threat intelligence enrichment using TTPs and malware family identifiers
- Community-driven insights and rule-sharing (YARA, IDS, MITRE mapping)

Case Summary: Malicious File bfsvc.exe

An executable file masquerading as a legitimate Windows utility (bfsvc.exe) was uploaded to VirusTotal. The multi-layered analysis yielded the following:

Key Findings:
- 58 out of 72 antivirus engines flagged the file as malicious.
- Behavioral analysis identified tactics such as persistence, defense evasion, self-deletion, and runtime module injection.
- Sandbox reports from CAPE, DAS-Security Orcas, and Yomi Hunter confirmed real-world malicious activity.
- The file dropped multiple scripts and binary payloads and established network communication with over 100 domains and IP addresses.
- It was associated with malware families such as Flagpro and Fragtor, which are known for espionage and backdoor capabilities.

Strategic Threat Intelligence Value

Using the Pyramid of Pain framework, this file exhibited:
- High-value TTPs and tools that offer durable detection and attribution opportunities
- Mid-tier infrastructure indicators (domains, IPs) that assist in threat hunting
- Low-value IOCs (hashes) that support fast incident triage

Recommendations

1. **Enable behavior-based detection in SIEM/SOAR**
   - Correlate behavior patterns observed in VirusTotal (e.g., self-delete, crypto, debug detection, persistence) with your organization's endpoint detection rules.

   - Update SIEM rules to trigger alerts for:
     - .bat or .bin file creation post-spreadsheet access
     - Unusual section entropy or unsigned executables mimicking Windows files (e.g., bfsvc.exe)
     - Attempts to evade sandboxes (e.g., long sleeps, debug checks)

2. **Block Indicators of Compromise (IOCs)**
   - Immediately block all identified malicious domains and IPs found in the Relations tab (e.g., misecure.com, multiple suspicious IPs).
   - Add identified URLs to your secure web gateway denylist.
   - Block JA3 TLS fingerprints if supported by your intrusion prevention system (IPS).

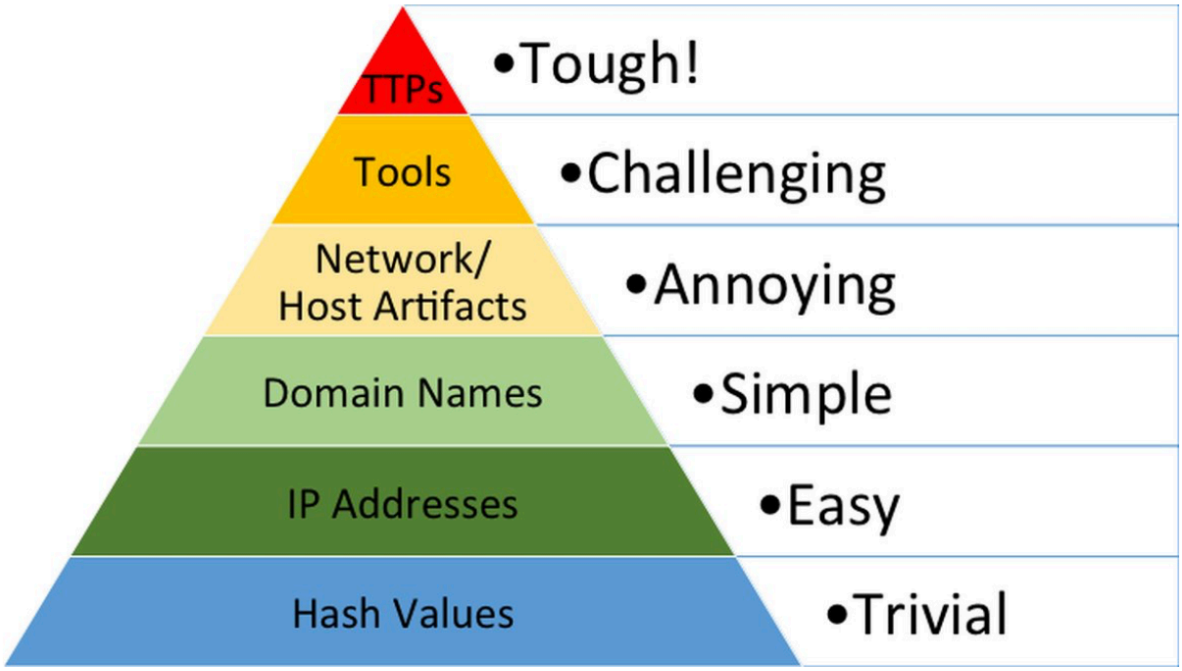
3. **Hunt for related file behaviors inside your environment**
   - Search for other endpoints that may have:
     - The same hash or imphash
     - Used the same network indicators (domains, IPs)
     - Dropped or executed similar payloads (from .bmp, .tmp, .js, .json files)

   - Inspect logs from the employee's machine for artifacts matching the observed MITRE ATT&CK techniques.

4. **Monitor for tool reuse across campaigns**
   - Use VirusTotal's metadata (Flagpro, Fragtor, bfrl) to create threat hunting queries.
   - Flag any future files associated with these malware families.
   - Stay subscribed to intelligence feeds (e.g., Malpedia, MITRE ATT&CK) for updates on these tools.

5. **Report the attack internally and escalate if needed**
   - Include VirusTotal findings in the incident report for your Tier 2 SOC team.
   - Provide a list of detected tactics (MITRE) and capabilities for long-term monitoring.
   - Recommend a wider internal awareness effort on malicious attachments with passwords.

Appendix A: Pyramid of Pain Analysis



The Pyramid of Pain is a cybersecurity model that ranks various types of Indicators of Compromise (IOCs) by how disruptive they are to threat actors.

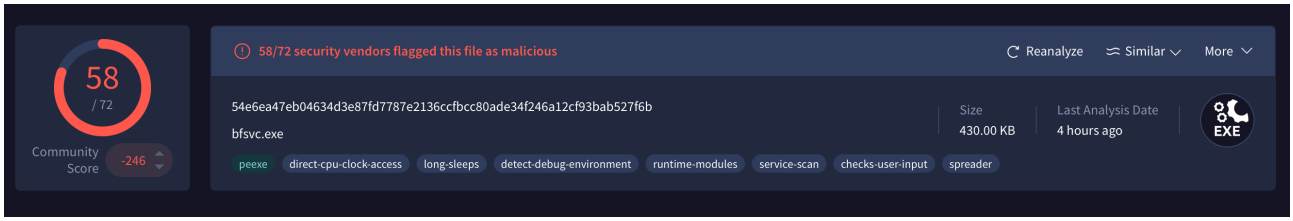
The higher an indicator sits on the pyramid, the more effort it takes for an adversary to modify or evade it—making it more effective for detection and defense.

By applying this model to the malicious file investigated (SHA256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b), we can strategically prioritize our response and mitigation efforts.

Pyramid Level	Your Observed Indicators	Pain Level to Attacker	Example from VirusTotal Data
TTPs (Tactics, Techniques, Procedures)	- MITRE ATT&CK IDs like `TA0005`(Defense Evasion), `TA0007` (Discovery) - Malware behavior tags like `self-delete`, `runtime-modules`, `crypto`, `detect-debug-environment`	High – hard to change core tactics	Seen in Behavior tab, mapped to MITRE and malware catalog trees
Tools	- Identified tools: Flagpro, Fragtor families - Possible custom build with MSVC++ 2008	High – tools take time to replace or rewrite	Identified via YARA rule matches, detection names (e.g., `Trojan.Agent.Flagpro`)
Network/Host Artifacts	- Self-delete - Registry usage - .bat/.bin file creation - Unusual section entropy in `.rsrc`	Medium – may require malware rebuilds or testing	From Details tab (file structure), Behavior tab (dropped files)
Domain Names	- misecure.com, windowsupdate.com, apis.google.com - Tracked in Relations	Low-Medium – domains can be cycled but are traceable	Seen in Relations tab, flagged in sandbox and URL scanners
IP Addresses	- Dozens of contacted IPs (e.g., 104.115.151.81) linked to malware infra	Low – easy for attacker to rotate	Found in Relations tab, low detection but correlated
Hash Values	- SHA-256: 54e6ea47eb... - MD5: 287d612e29b...	Very Low – attacker can easily recompile or repackage	From Details tab, used in initial scan

Appendix B: Virus Total Analysis

Header Section



The header is the **topmost part** of any VirusTotal file report. It provides a quick yet powerful summary of the file's threat level, community feedback, metadata, and options for further analysis.

Detection Ratio (Top Left Circle)

Displayed as: 58 / 72

Meaning: Out of 72 antivirus engines, 58 vendors have flagged the file as malicious.

Visual Element: A red circular progress indicator shows the percentage visually.

Purpose: This is the primary threat indicator. A high ratio like this (over 80%) strongly suggests the file is harmful.

Community Score (Below Detection Circle)

Displayed as: -246

Meaning: This score is based on user votes. A highly negative value suggests that VirusTotal community members (security researchers, analysts) have identified this file as suspicious or confirmed malware.

Purpose: This adds a human-driven reputation layer on top of automated scans.

File Hash & Identity (Center Panel)

SHA-256 Hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

A **unique fingerprint** for the file. Helps identify it across platforms and tools.
Filename: bfsvc.exe
The file masquerades as a legitimate Windows utility, but its behavior and detection results show it is likely malicious.

Behavior Tags:
Tags are derived from static/dynamic analysis.

File Metadata (Right Panel)

File Size: 430.00 KB
Provides a basic measurement of the file's footprint.

Last Analysis Date: 4 hours ago
Shows when VirusTotal last analyzed the file. A recent timestamp means the data is **fresh** and up-to-date.

File Type Icon:
A circular icon showing a gear inside a document labeled EXE.
This visually confirms it's a Windows executable file.

Action Bar (Top Right)

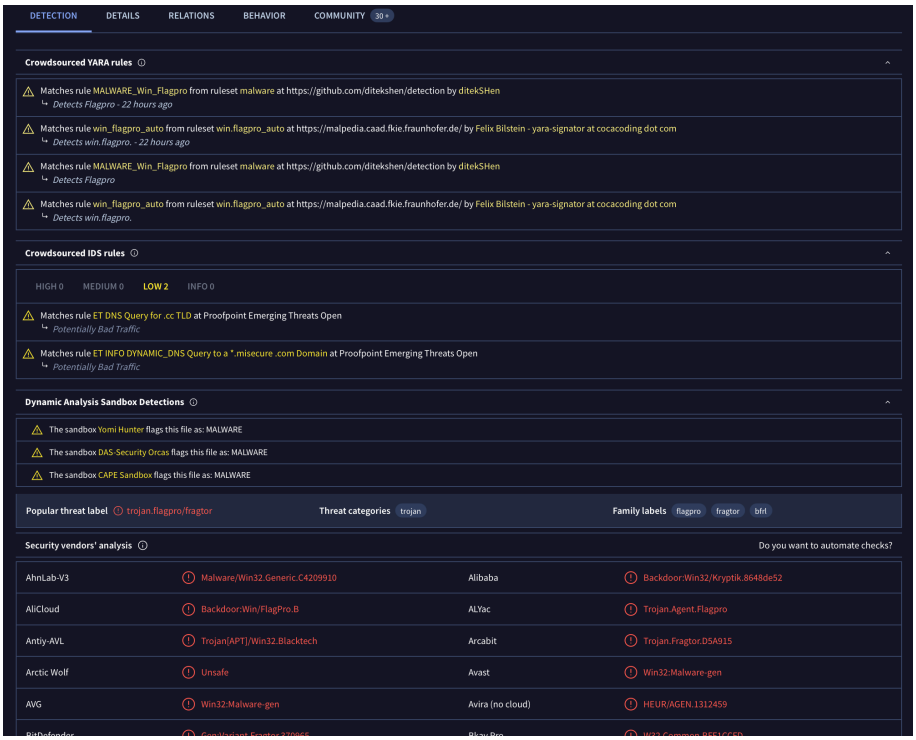
Reanalyze:
Allows users to request a new scan of the file using updated engines.

Similar:
Helps locate files with similar behavior or code, useful for identifying malware variants.

More:
A dropdown for further options, such as downloading, viewing API response, or sharing.

Detection Tab

The **Detection** tab is the core of any VirusTotal report. It consolidates detection results from antivirus engines, behavioral sandboxes, community-contributed YARA/IDS rules, and threat classification systems to offer a comprehensive view of how a file behaves and is perceived.



Crowdsourced YARA Rules

YARA rules are community-created pattern-matching definitions used to detect malware families by identifying specific byte sequences or structures.

Each rule shows:
The rule name
The ruleset source
The author
The malware family detected (e.g., Flagpro, win.flagpro)
When the rule last matched (e.g., “22 hours ago”)

Description:
These rules confirm that the file matches known byte patterns of malware families associated with targeted attacks.

Used for manual reverse engineering and threat hunting.

Crowdsourced IDS Rules

Intrusion Detection System (IDS) rules monitor network behavior and flag unusual or malicious activity.

Description:
.cc TLD and dynamic DNS domains are often used in Command & Control (C2) infrastructure.
These flags suggest the malware may attempt to communicate with remote servers using evasive DNS techniques.

Dynamic Analysis Sandbox Detections

Displays how the file behaves when executed in a controlled sandbox environment.

Description:
Each sandbox uses different sensors and heuristics to monitor runtime activity.

Consensus among multiple sandboxes indicates confirmed malicious behavior, like:
Creating processes
Network beacons
File manipulation
Registry changes

Threat Classification

Helps categorize the malware and associate it with known families.

Description:
These labels help you identify what the malware is designed to do (e.g., remote control, stealing data).

Family tags allow researchers to track campaigns, threat actors, or malware evolution.

Security Vendors' Analysis

Shows how different antivirus vendors label the file, including the detection name/signature.

Description:
Malware names vary across vendors (due to signature naming schemes).
But consistent themes appear: Backdoor, Trojan, Flagpro, Fragtor.
Helps confirm the type of malware and its known variants.

Use this info to cross-reference with public threat databases (e.g., Malpedia, MITRE ATT&CK, Hybrid Analysis).

Details Tab

The Details tab provides static file metadata and low-level structural information. This is crucial for identifying file origins, composition, and potential tampering or obfuscation—without executing the file.

Basic Properties

Purpose: These properties uniquely identify and describe the binary file using cryptographic hashes and metadata.

Explanation:
Multiple hash values are provided for comparison across systems and to check for duplicates or mutations.

Tags like peexe and win32 confirm the file is a Portable Executable on Windows.

Imphash, Authentihash, and Rich PE Header Hash are often used in malware hunting to identify closely related binaries (e.g., same malware family).

DetectItEasy and TrID help identify the compiler and packaging, useful for attribution and reverse engineering.

PEBIN shows the structure fits a standard Windows PE binary forma

History

Purpose: Indicates the timeline of file visibility and submission to VirusTotal.

Explanation:
"First seen in the wild" suggests it has been observed on real systems before the first VirusTotal submission.

A file with a long history may belong to an active or persistent malware campaign.

Names

Purpose: Lists all the filenames VirusTotal has encountered for this binary.

Explanation:
Malware often renames itself or is downloaded under different filenames to evade detection.

Use of names like .bat, .bin, .js, and .crdownload implies delivery via scripts or browser-based downloads.

Unicode filenames (e.g., 開發.bin) may indicate targeting of non-English users or deliberate obfuscation.

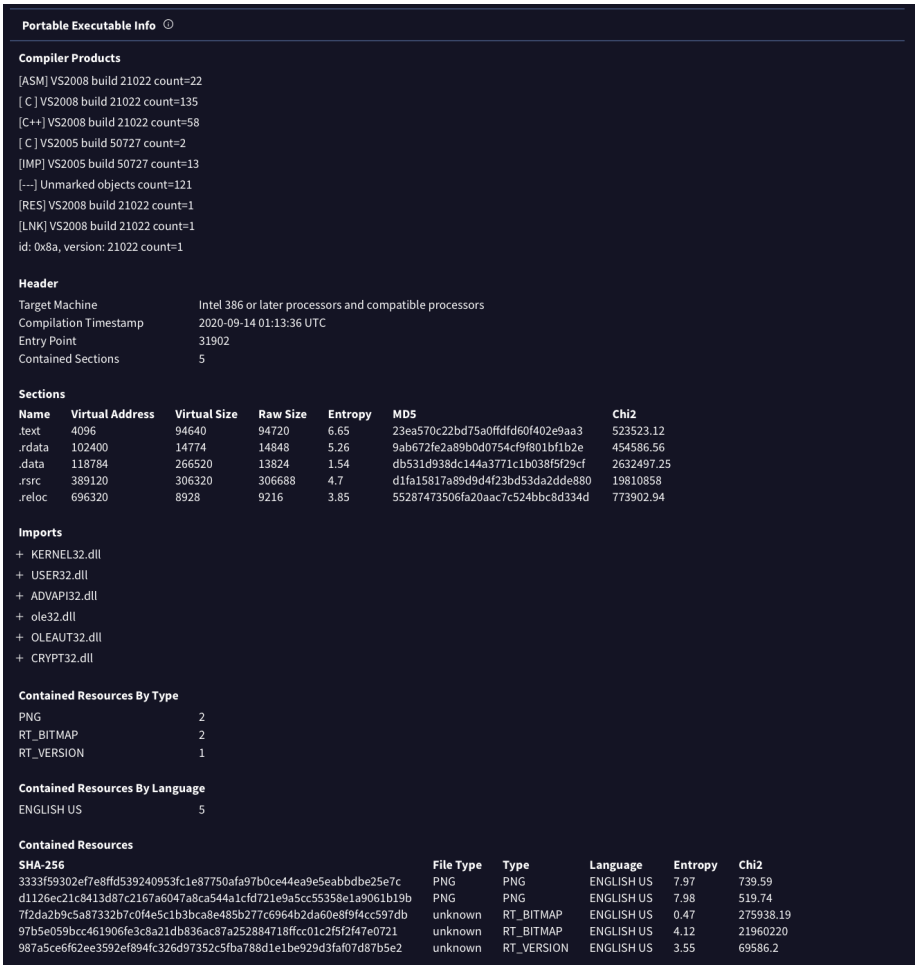
Signature Info

Purpose: Verifies whether the file was digitally signed and pretends to be legitimate software.

Explanation:
The file claims to be a Windows system component, which is a common tactic for deception.

It is not digitally signed, which strongly indicates it is not from Microsoft despite the claimed metadata.

Legitimate Windows binaries are always signed with Microsoft’s trusted certificate.



Portable Executable Info

Compiler Products

[ASM] VS2008 build 21022 count=22
[C] VS2008 build 21022 count=135
[C++] VS2008 build 21022 count=58
[C] VS2005 build 50727 count=2
[IMP] VS2005 build 50727 count=13
[---] Unmarked objects count=121
[RES] VS2008 build 21022 count=1
[LNK] VS2008 build 21022 count=1
id: 0x8a, version: 21022 count=1

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2020-09-14 01:13:36 UTC
Entry Point	31902
Contained Sections	5

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	94640	94720	6.65	23ea570c22bd75a0ffdfd60f402e9aa3	523523.12
.rdata	102400	14774	14848	5.26	9ab672fe2a89b0d0754cf9f801bf1b2e	454586.56
.data	118784	266520	13824	1.54	db531d938dc144a3771c1b038f5f29cf	2632497.25
.rsrc	389120	306320	306688	4.7	d1fa15817a89d9d4f23bd53da2dde880	19810858
.reloc	696320	8928	9216	3.85	55287473506fa20aac7c524bbc8d334d	773902.94

Imports

+ KERNEL32.dll
+ USER32.dll
+ ADVAPI32.dll
+ ole32.dll
+ OLEAUT32.dll
+ CRYPT32.dll

Contained Resources By Type

PNG	2
RT_BITMAP	2
RT_VERSION	1

Contained Resources By Language

ENGLISH US	5

Contained Resources

SHA-256	File Type	Type	Language	Entropy	Chi2
3333f59302ef7e8ffd539240953fc1e87750afa97b0ce44ea9e5eabbdbe25e7c	PNG	PNG	ENGLISH US	7.97	739.59
d1126ec21c8413d87c2167a6047a8ca544a1cfd721e9a5cc55358e1a9061b19b	PNG	PNG	ENGLISH US	7.98	519.74
7f2da2b9c5a87332b7c0f4e5c1b3bca8e485b277c6964b2da60e8f9f4cc597db	unknown	RT_BITMAP	ENGLISH US	0.47	275938.19
97b5e059bcc461906fe3c8a21db836ac87a252884718ffcc01c2f5f2f47e0721	unknown	RT_BITMAP	ENGLISH US	4.12	21960220
987a5ce6f62ee3592ef894fc326d97352c5fba788d1e1be929d3faf07d87b5e2	unknown	RT_VERSION	ENGLISH US	3.55	69586.2

Portable Executable Info

Compiler Products

These entries indicate which compiler and version were used to build the executable.

The high counts for C/C++ suggest a mixed codebase likely compiled with Microsoft Visual Studio 2008.

Presence of unmarked objects and resource/linker data gives insights into build complexity.

Useful for attributing malware to a development environment.

Header

Indicates the binary targets Intel 386+ architecture (standard for 32-bit Windows apps).

The entry point is where the program starts executing. Analysts use this to locate unpacking or malicious logic.

Timestamp may be faked by malware authors but still helpful for timeline analysis.

Sections

PE sections show how code, data, and resources are laid out.

Imports

These imports suggest the file is interacting deeply with the system.

Contained Resources

The file contains embedded resources.

Details Tab

The Relations tab displays how the analyzed file is connected to external infrastructure or related artifacts. It helps uncover a larger attack surface, such as command & control (C2) infrastructure, bundled payloads, and dropped files.

Contacted URLs

Description:
URLs listed are ones the file attempted to contact or is associated with.

Status 200 means the request succeeded.

URLs related to Google Fonts, Microsoft, or Ad services may be legitimate, but some—like misecure.com—could indicate malicious infrastructure.

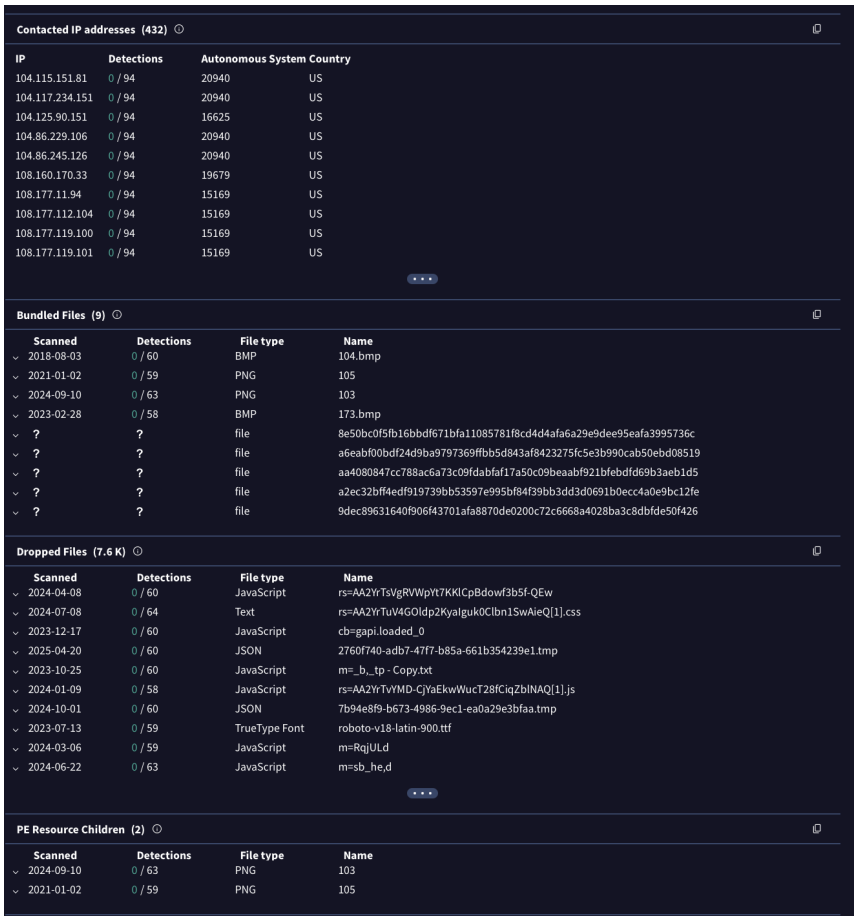
One URL (windowsupdate.com/.../disallowedcertstl.cab) has 10/97 detections, likely flagged as hosting suspicious files.

Contacted Domains

Description:
These domains are resolved or connected to during the file's activity.

Many are registered with MarkMonitor Inc., a registrar used by major tech companies (Google, Microsoft).

Absence of detections doesn’t confirm legitimacy; attackers often abuse legitimate domains via misconfigurations or indirect exploitation.



Contacted IP addresses (432)

IP	Detections	Autonomous System	Country
104.115.151.81	0 / 94	20940	US
104.117.234.151	0 / 94	20940	US
104.125.90.151	0 / 94	16625	US
104.86.229.106	0 / 94	20940	US
104.86.245.126	0 / 94	20940	US
108.160.170.33	0 / 94	19679	US
108.177.11.94	0 / 94	15169	US
108.177.112.104	0 / 94	15169	US
108.177.119.100	0 / 94	15169	US
108.177.119.101	0 / 94	15169	US

Bundled Files (9)

Scanned	Detections	File type	Name
2018-08-03	0 / 60	BMP	104.bmp
2021-01-02	0 / 59	PNG	105
2024-09-10	0 / 63	PNG	103
2023-02-28	0 / 58	BMP	173.bmp
?	?	file	8e50bc0f5fb16bbdf671bfa11085781f8cd4d4afa6a29e9dee95eafa3995736c
?	?	file	a6eabf00bdf24d9ba9797369ffbb5d843af8423275fc5e3b990cab50ebd08519
?	?	file	aa4080847cc788ac6a73c09fdabfaf17a50c09beaabf921bfebdfd69b3aeb1d5
?	?	file	a2ec32bff4edf919739bb53597e995bf84f39bb3dd3d0691b0ecc4a0e9bc12fe
?	?	file	9dec89631640f906f43701afa8870de0200c72c6668a4028ba3c8dbfde50f426

Dropped Files (7.6 K)

Scanned	Detections	File type	Name
2024-04-08	0 / 60	JavaScript	rs=AA2YrTsVgRVWpYt7KKlCpBdowf3b5f-QEw
2024-07-08	0 / 64	Text	rs=AA2YrTuV4GOldp2Kyalguk0Clbn1SwAieQ[1].css
2023-12-17	0 / 60	JavaScript	cb=gapi.loaded_0
2025-04-20	0 / 60	JSON	2760f740-adb7-47f7-b85a-661b354239e1.tmp
2023-10-25	0 / 60	JavaScript	m=_b,_tp - Copy.txt
2024-01-09	0 / 58	JavaScript	rs=AA2YrTvYMD-CjYaEkwWucT28fCiqZbINAQ[1].js
2024-10-01	0 / 60	JSON	7b94e8f9-b673-4986-9ec1-ea0a29e3bfaa.tmp
2023-07-13	0 / 59	TrueType Font	roboto-v18-latin-900.ttf
2024-03-06	0 / 59	JavaScript	m=RqjULd
2024-06-22	0 / 63	JavaScript	m=sb_he,d

PE Resource Children (2)

Scanned	Detections	File type	Name
2024-09-10	0 / 63	PNG	103
2021-01-02	0 / 59	PNG	105

Contacted IP Addresses

Description:
Shows the IP addresses contacted by the sample.

Often mapped to Content Delivery Networks (CDNs) or cloud services (e.g., Akamai, Google).

If detections rise, these may be part of Command & Control (C2) or malicious hosting.

Bundled Files

Description:
These files were packaged or distributed alongside the analyzed file.

Common in multi-stage malware, where images or binaries hide additional payloads (sometimes in steganographic form).

Filenames like .bmp suggest use in obfuscation or decoy UI elements.

Dropped Files

Description:
These files were created or written to disk during execution.

JavaScript and JSON files suggest web-based or modular behavior.

*.tmp and .ttf (font) files could be decoys or disguised payloads.

PE Resource Children

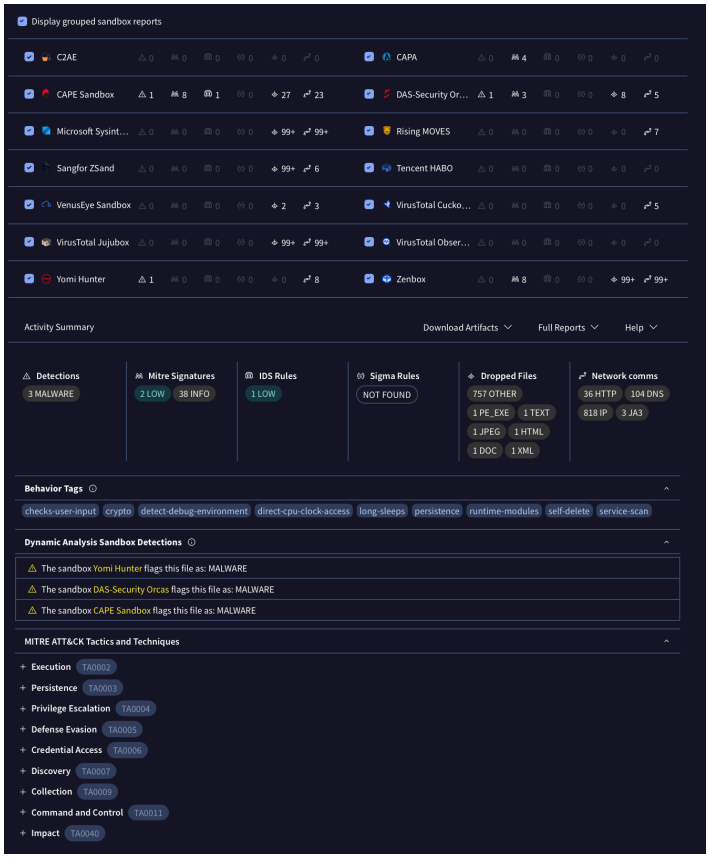
Description:
These are embedded resources extracted from the PE file.

PNG images could be part of GUI elements or used to hide malicious content.

Useful for static inspection or steganographic analysis.

Behavior Tab

The Behavior tab presents dynamic analysis results from various sandbox environments where the file is executed and observed. This section reveals what the file does when it runs, including system manipulation, file drops, network activity, and suspicious techniques.



Sandbox Report Overview (Grouped Reports)

Description:
Displays output from multiple sandbox systems.

Shows whether each sandbox flagged the file as malware, how many files were dropped, and how many network connections were made.

Consistent malware detection across CAPE, DAS-Orcas, and Yomi Hunter adds confidence that the file is malicious.

The number of dropped files (e.g., “27”) and connections (e.g., “23”) shows high post-execution activity, typical of malware.

Activity Summary

Description:
Summary of sandboxed behavior:

Files dropped include executables and documents, indicating potential for payload delivery.

JA3 is a TLS fingerprint used in network traffic fingerprinting (relevant for threat hunting).

Sigma rules not triggered, but Mitre ATT&CK signatures were observed.

Behavior Tags

Description:
Tags highlight techniques or behaviors observed during analysis.

Examples:
crypto: May encrypt files or use encryption.
self-delete: Attempts to erase itself post-execution (anti-forensics).
long-sleeps: Used to evade sandboxes that timeout quickly.

Dynamic Sandbox Detections (Text Summary)

Description:
Confirms malicious behavior observed during live execution.
Helps differentiate false positives from actual threats.

MITRE ATT&CK Techniques (Blue Tags)

Description:
Indicates what tactics and techniques from the MITRE ATT&CK framework were used.
This structured mapping is essential for incident response and threat classification.

Malware Behavior Catalog Tree

Description:
A tree of behavioral traits drawn from open-source malware behavior classification systems.

The structure reflects what system components are touched, how, and why.

Capabilities

Description:
Reflects the malware's high-level functionality, such as:

Reading keyboard input (host interaction)
Exfiltrating files (collection)
Modifying data
Making external network requests