Incident description

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 been identified as malicious? Explain why or why not.

Yes. This file seems malicious. Looking at the high vendor score and negative community score.
The file is

Supporting Evidence:

Detections:

58/71 vendors found the file malicious. The community score is -256, negative figures indicate levels of maliciousness. The higher the absolute score (positive or negative), the stronger the community consensus.

Supporting evidence

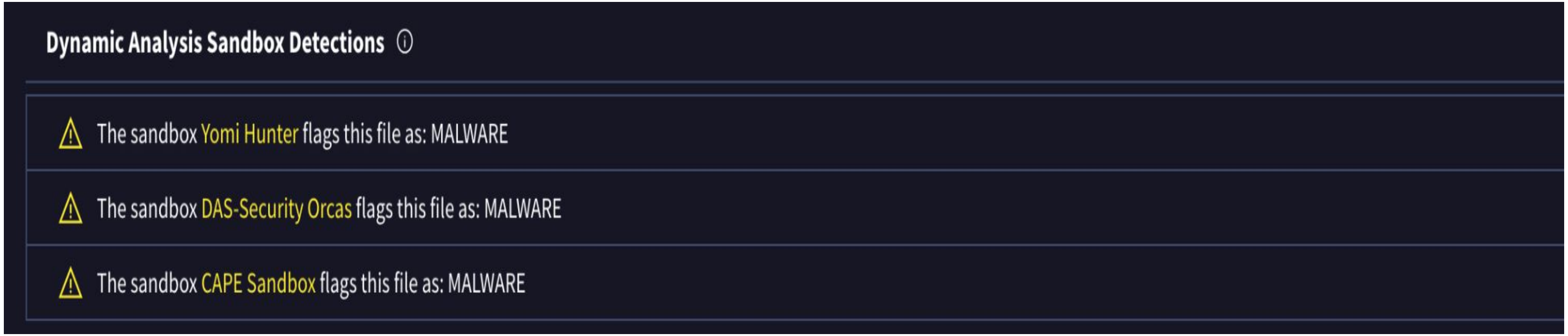
Details: Associated hashes:

MD5	287d612e29b71c90aa54947313810a25
SHA-1	8f35a9e70dbec8f1904991773f394cd4f9a07f5e
SHA-256	54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Vhash	045056655d15551023z12z577z305bz2fz
Authentihash	019439328ea87e4559b653ad7df933d20623bdd00d3793abc7ff35e57db24853
Imphash	a59ed1599cc2f8311b215c83c51a2cc4
Rich PE header hash	1f4064adca28866f7447aaf031074807
SSDEEP	6144:CdaRD0n4URr6zIKgDCVh84DLn5X3lWiDSVS1dGSLaYWis:XRonpRroIKgDCY4DLVlW3UiSL4R
TLSH	T13594AD933541C371CA177D7695789AAD4B3F8D3816BAB987B3B83B8F5C303918636902

Supporting evidence

Relation:
The relations tab shows the number of vendors who have marked the file as malicious. In 2025, 10/97 vendors reported file to be malicious.

These sandboxes detected malware in the file.



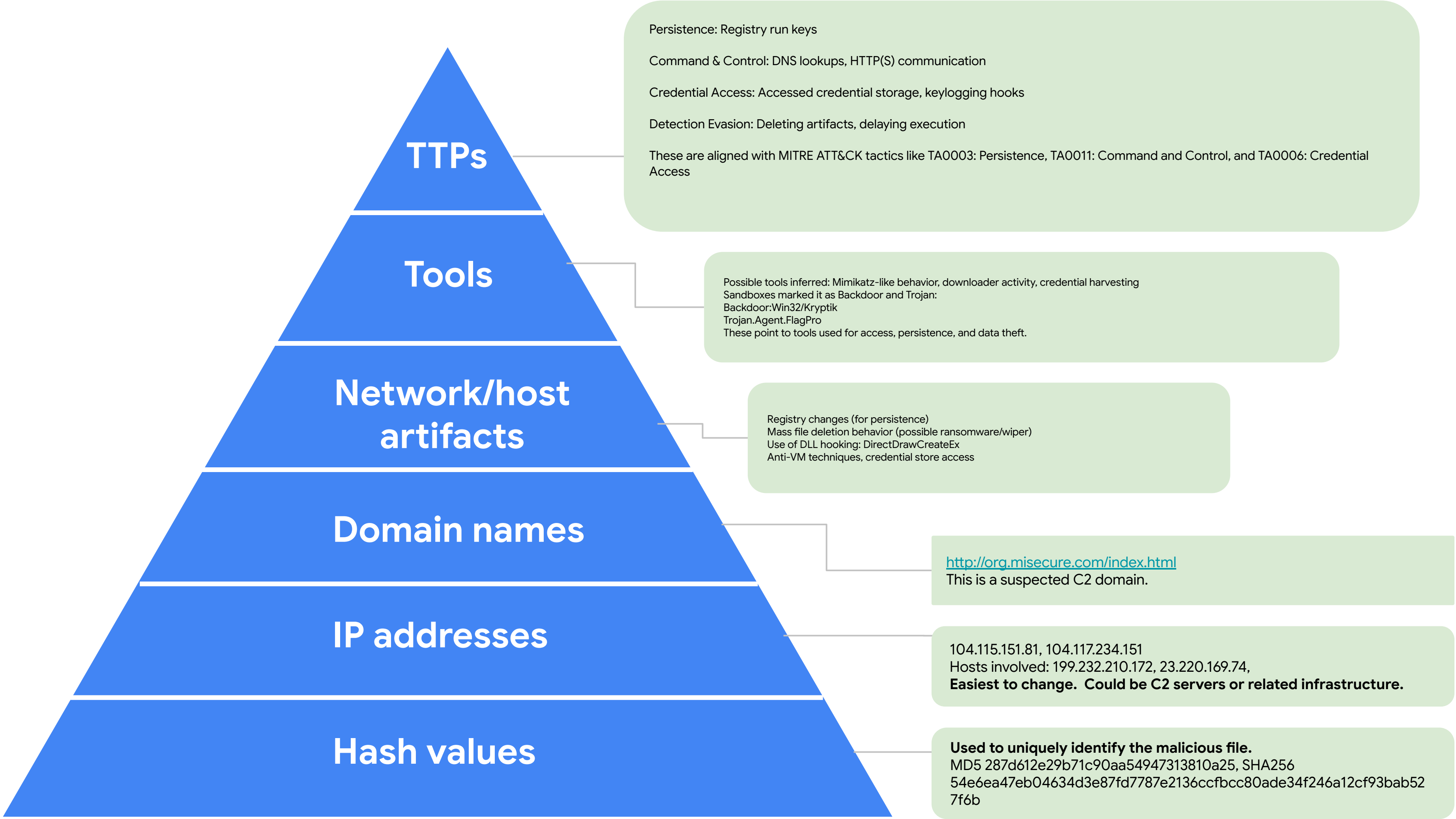
Dynamic Analysis Sandbox Detections ⓘ

⚠ The sandbox Yomi Hunter flags this file as: MALWARE

⚠ The sandbox DAS-Security Orcas flags this file as: MALWARE

⚠ The sandbox CAPE Sandbox flags this file as: MALWARE

Pain Level (From easiest to most Painful)	Associated Values
Hash values	MD5: 287d612e29b71c90aa54947313810a25, SHA256: 54e6ea47eb04634d3e87fd7787e2136ccfbc
IP addresses	104.115.151.81, 104.117.234.151
Domain names	http://org.misecure.com/index.html, http://org.misecure.com/favicon.ico
Network/host artifacts	Anomalous file deletion behavior detected (10+), A process attempted to delay the analysis task by a long amount of time., Installs itself for autorun at Windows startup, Exhibits possible ransomware or wiper file modification behavior: mass_file_deletion, Collects information about installed applications, Enumerates services, possibly for anti-virtualization, Accessed credential storage registry keys,
Tools	Trojan.Win32.Agent.oa!s1, Malware/Win32.Generic.C4209910, Backdoor:Win/FlagPro.B, Backdoor:Win32/Kryptik.8648de52, Trojan.Agent.Flagpro, Trojan.Win32.Agent.oa!s1
TTP	Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. **Execution:** Adversaries may execute malicious payloads via loading shared modules. **Persistence**: Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. **Privilege escalation:** Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems and by adding a program to a startup folder or referencing it with a Registry run key. **Detection Evasion:** encrypt data using DPAPI, Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools.Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. **Credential access:** Creates a DirectInput object (often for capturing keystrokes) - <HOOK MODULE="DDRAW.DLL" FUNCTION="DirectDrawCreateEx"/> **Discovery**: Reads software policies, Checks if Microsoft Office is installed, Reads ini files, **Creation**: Creates a DirectInput object (often for capturing keystrokes) - <HOOK MODULE="DDRAW.DLL" FUNCTION="DirectDrawCreateEx"/> **Command and control:** perform dns lookup, uses https, download files from web server using http, Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic, Uses HTTPS for network communication, use the SSL MITM Proxy cookbook for further analysis



TTPs

Persistence: Registry run keys

Command & Control: DNS lookups, HTTP(S) communication

Credential Access: Accessed credential storage, keylogging hooks

Detection Evasion: Deleting artifacts, delaying execution

These are aligned with MITRE ATT&CK tactics like TA0003: Persistence, TA0011: Command and Control, and TA0006: Credential Access

Tools

Possible tools inferred: Mimikatz-like behavior, downloader activity, credential harvesting
Sandboxes marked it as Backdoor and Trojan:
Backdoor:Win32/Kryptik
Trojan.Agent.FlagPro
These point to tools used for access, persistence, and data theft.

Network/host artifacts

Registry changes (for persistence)
Mass file deletion behavior (possible ransomware/wiper)
Use of DLL hooking: DirectDrawCreateEx
Anti-VM techniques, credential store access

Domain names

http://org.misecure.com/index.html
This is a suspected C2 domain.

IP addresses

104.115.151.81, 104.117.234.151
Hosts involved: 199.232.210.172, 23.220.169.74,
Easiest to change. Could be C2 servers or related infrastructure.

Hash values

Used to uniquely identify the malicious file.
MD5 287d612e29b71c90aa54947313810a25, SHA256
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab52
7f6b