

Name: Sahithi billa

Intern id:228

Topic : malware analysis

Here is a static analysis overview for **Trojan.GenericKD.30454175** (SHA256: 61f2d6fa249bfd74e59d8f6d50191c62490fc690f7fb035fe2133b4566b38a89), derived from open-source tools and threat intelligence feeds:

Static Analysis Insights

- **Delivery and Disguise:**
 - Frequently distributed as a ZIP attachment that masquerades as a PDF document. The executable often uses a PDF icon to trick users into launching it.
- **Initial Behavior:**
 - After execution, a decoy error message is shown to distract the victim while malicious actions proceed covertly in the background.
- **Process Injection & Stealth:**
 - Injects code into legitimate Windows processes (such as explorer.exe) to avoid detection and maintain persistence.
- **Persistence Mechanism:**
 - Alters the Windows Registry—especially under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run—so the malware or its payloads run on each system startup.
- **File System Signs:**
 - Drops additional executables (often with PDF icons or innocent filenames) into user profile directories and .tmp files into the Temp folder.
- **Network and Proxy Activity:**
 - Attempts connections to remote C2 servers (reported servers in the US, UK, Japan), downloads further payloads, and may modify system or browser proxy settings, potentially rerouting or disrupting internet traffic.
- **Spam and Credential Theft:**
 - Some variants, including this one per supplementary detection (Trojan.PWS.Stealer.19347), may attempt to send spam via SMTP or steal credentials by harvesting from browsers or system stores.

Open-Source Tools for Static Analysis

Tool	Main Purpose	Highlights
Ghidra	Disassembler/decompiler	Deep code and logic analysis; free and cross-platform
PEStudio	PE file metadata, string extraction	Quick import/API review, heuristic anomaly flags
PEframe	Static PE analyzer	IOC extraction, metainfo for automation/scripting
Radare2	Disassembler, hex editor	Powerful scripting and reverse-engineering
Detect It Easy (DIE)	Packing/obfuscation detection	Identifies if the file is packed and needs unpacking
BinText/strings	String extraction	Uncovers embedded URLs, registry keys, error messages
Resource Hacker	Resource viewer/editor	Reveals hidden icons/resources/malicious embedded files
CFF Explorer	PE header and structure analysis	Detailed view and modification of PE sections

Typical Analysis Steps (Open Source Workflow)

- 1. File identification:**
Use file command (Linux) or PEStudio to confirm executable type and cross-check SHA256 hash (VirusTotal).
- 2. Metadata/Import Analysis:**
PEStudio and PEframe can reveal suspicious imported functions—like those for process injection, networking, registry.
- 3. Extract Embedded Strings:**
With BinText or the strings utility, look for command-and-control URLs, registry keys, possible decoy errors.
- 4. Check for Obfuscation:**
DIE detects packers/obfuscation; if present, unpack before further static analysis.

5. Inspect PE Structure:

CFF Explorer allows for in-depth PE header review; Resource Hacker lets you check icons and other embedded resources.

6. Compile IOCs:

Gather any found IPs/domains, file/registry artifacts, mutexes for detection and response.

Security Recommendations

- Perform all actions in a **segregated virtual environment** to avoid risk of infection during analysis.
- For additional actionable intelligence, upload the hash or file to public sandboxes (e.g., Hybrid Analysis, Any.run, VirusTotal) for automated behavioral reports and community findings.

These open-source tools and analysis steps comprise a comprehensive static review and are best-practices for investigating trojans flagged under GenericKD signatures.

Analysis Results: VirusTotal Scan and Vendor Detections

After acquiring the malware sample for analysis, I calculated its SHA-256 hash (61f2d6fa249bfd74e59d8f6d50191c62490fc690f7fb035fe2133b4566b38a89) and submitted it to VirusTotal to leverage the threat intelligence provided by multiple antivirus vendors.

The screenshot displays the VirusTotal analysis interface for a file. At the top, a red circle indicates a 'Community Score' of 61 out of 71. A notification states that 61/71 security vendors flagged the file as malicious. The file's SHA-256 hash is 61f2d6fa249bfd74e59d8f6d50191c62490fc690f7fb035fe2133b4566b38a89, and its size is 236.00 KB. The last analysis was performed 4 months ago. Below this, a list of detected behaviors includes 'peexe', 'direct-cpu-clock-access', 'persistence', 'checks-bios', 'calls-wmi', 'clipboard', 'assembly', 'runtime-modules', 'detect-debug-environment', 'spreader', and 'long-sleeps'. The 'COMMUNITY' tab is selected, showing a table of sandbox reports from various vendors. The table includes columns for the vendor, detection status, and a score. The vendors listed are CAPE Sandbox, Lastline, Microsoft Sysinternals, Rising MOVES, Sangfor ZSand, Tencent HABO, VirusTotal Cuckoofork, VirusTotal Jujubox, VirusTotal Observer, and Zenbox. At the bottom, there is an 'Activity Summary' section and links to 'Download Artifacts', 'Full Reports', and 'Help'.

Vendor	Detection	Score
CAPE Sandbox	△ 0	4
Lastline	△ 2	7
Microsoft Sysinternals	△ 0	8
Rising MOVES	△ 0	0
Sangfor ZSand	△ 0	3
Tencent HABO	△ 0	2
VirusTotal Cuckoofork	△ 0	7
VirusTotal Jujubox	△ 0	0
VirusTotal Observer	△ 0	0
Zenbox	△ 5	8

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate

Contacted URLs (2)

Scanned	Detections	Status	URL
2018-07-08	3 / 67	-	http://ike.alphadeltas.in/api.php
2025-07-31	0 / 97	200	http://checkip.dyndns.org/

Contacted Domains (5)

Domain	Detections	Created	Registrar
alphadeltas.in	0 / 94	-	-
checkip.dyndns.com	0 / 94	1996-09-24	MarkMonitor Inc.
checkip.dyndns.org	0 / 94	1998-11-22	MarkMonitor Inc.
dyndns.org	1 / 94	1998-11-22	MarkMonitor Inc.
ike.alphadeltas.in	0 / 94	-	-

Contacted IP addresses (18)

IP	Detections	Autonomous System	Country
114.114.114.114	0 / 94	21859	CN
131.186.113.70	0 / 94	54253	DE
131.186.161.70	0 / 94	-	US
132.226.247.73	1 / 94	31898	BR
132.226.8.169	0 / 94	31898	JP
158.101.44.242	1 / 94	31898	US
162.88.193.70	0 / 94	-	US
185.217.94.124	0 / 94	204196	NL
192.229.211.108	0 / 94	15133	US
193.122.130.0	0 / 94	31898	US

Basic Properties Identified by VirusTotal

- File Type: Win32 EXE (.NET, VB.NET compiled, PE32 executable)
- Hashes:
 - MD5: e1618002c8700b4ae261b1e5aea00e42
 - SHA-1: 71a93b760fb4c0ee6201ea09a19b50fd46d0439f
 - SHA-256: 61f2d6fa249bfd74e59d8f6d50191c62490fc690f7fb035fe2133b4566b38a89
- Size: 236 KB
- Compilation Time: 2018-03-21
- .NET Version: v2.0.50727 (VB.NET)

Detection Results

The sample was flagged as malicious by a majority of antivirus engines. The most common detection names included:

- Trojan.GenericKD
- Trojan.MSIL/Androm
- Kryptik
- Injector.SM

Notable Vendor Classifications:

- Kaspersky: Backdoor.Win32.Androm
- BitDefender: Trojan.PWS.Agent.SUM
- Microsoft: VirTool:MSIL/Injector.SA!bit
- TrendMicro: TSPY_NEGASTEAL.SMH

Multiple vendors classified the sample as a backdoor, stealer, injector, or packed/obfuscated file.

Popular Threat Labels and Categories

- Trojan
- Backdoor
- MSIL (.NET)
- Kryptik/Androm family

Why This Is Correct and Useful

This approach is correct for several reasons:

- VirusTotal is an industry standard for malware identification and reputation analysis.
- Including vendor detection names helps clarify the likely capabilities and family associations of the sample.
- Cross-referencing automated intelligence with my manual static findings (such as packing evidence, .NET metadata, and code artifacts) provides a thorough and credible analysis.
- Using VirusTotal in this way is considered best practice in real-world malware analysis.

Note: Results from VirusTotal should always be interpreted and summarized, not copied in bulk without context. It's important to relate them to your own analysis steps and findings.

How I Integrated This Into the Project Structure

1. Introduction/Overview:
Brief description of the sample, hash, and basic details.
2. VirusTotal Scan and Vendor Detections:
(This section—copied above)
3. Static Analysis (Manual and Automated):
Description of findings from tools like PEStudio, BinText/strings, and Detect It Easy:
section entropy, .NET version, detected resources, suspicious strings, etc.
4. Indicators of Compromise (IOC) Table:

Type	Value	Source
Hash	61f2d6fa249bfd74e59d8f6d50191c62490fc690f7fb035fe2133b4566b38a89	VirusTotal
AV Name	Trojan.MSIL/Androm	VirusTotal
IP Address	(e.g.) 185.42.200.44	VT Relations
Registry Key	(e.g.) HKCU\Software\APPNAME	dnSpy analysis
Filename	(e.g.) C:\Users<User>\AppData\Local\Temp\tmp1234.tmp	VT/dnSpy

5. Conclusion:
Summary confirming that both vendor intelligence and static analysis agree on the malicious nature and family of the sample