Malware Analysis Report: Trojan.GenericKD.12667430

What is it?

`Trojan.GenericKD.12667430` is a generic detection name used by AVG/Avast for Trojan Horses.

The `GenericKD` part means it's heuristically detected, not tied to a specific malware family.

Behavior and Capabilities

Common Capabilities	
Backdoor Access	Opens system to remote attackers.
Keylogging	Captures keystrokes to steal credentials.
Spyware Features	Screenshots, clipboard monitoring.
Payload Dropper	Downloads and executes other malware.
System Modification	Alters registry, disables antivirus.
Data Exfiltration	Steals files, cookies, saved passwords.

Static Indicators

Static Indicators	
File type	.exe, .dll, or .scr
Obfuscation	Packed with UPX, Themida, or custom cryptors
Known Imports	WinExec, CreateRemoteThread, RegSetValueEx
Suspicious Strings	Encrypted URLs, C2 IPs, anti-analysis tricks

Dynamic Behavior

Often modifies registry keys, connects to remote IPs, runs in memory, and creates persistence via mutexes.

Malware Analysis Report: Trojan.GenericKD.12667430

Useful tools for analysis: Cuckoo Sandbox, Any.run, Hybrid Analysis, Procmon + Wireshark.

Reverse Engineering Tips

1. Unpack with PEiD or Exeinfo PE.
2. Disassemble with IDA or Ghidra.
3. Monitor behavior using Procmon and Regshot.
4. Scan for YARA patterns.

How to Remove It

1. Boot into Safe Mode.
2. Use antivirus tools like Malwarebytes or Kaspersky.
3. Use Autoruns, RogueKiller.
4. Check Task Scheduler, registry, and temp folders.

Example Payloads

Real-World Payloads	
AgentTesla	Credential stealer
FormBook	Info stealer
RedLine Stealer	Sensitive data extractor
Lokibot	Steals credentials and files
NetWire RAT	Remote access and control

Optional Analysis Tools

Upload the sample or get a hash and analyze using:

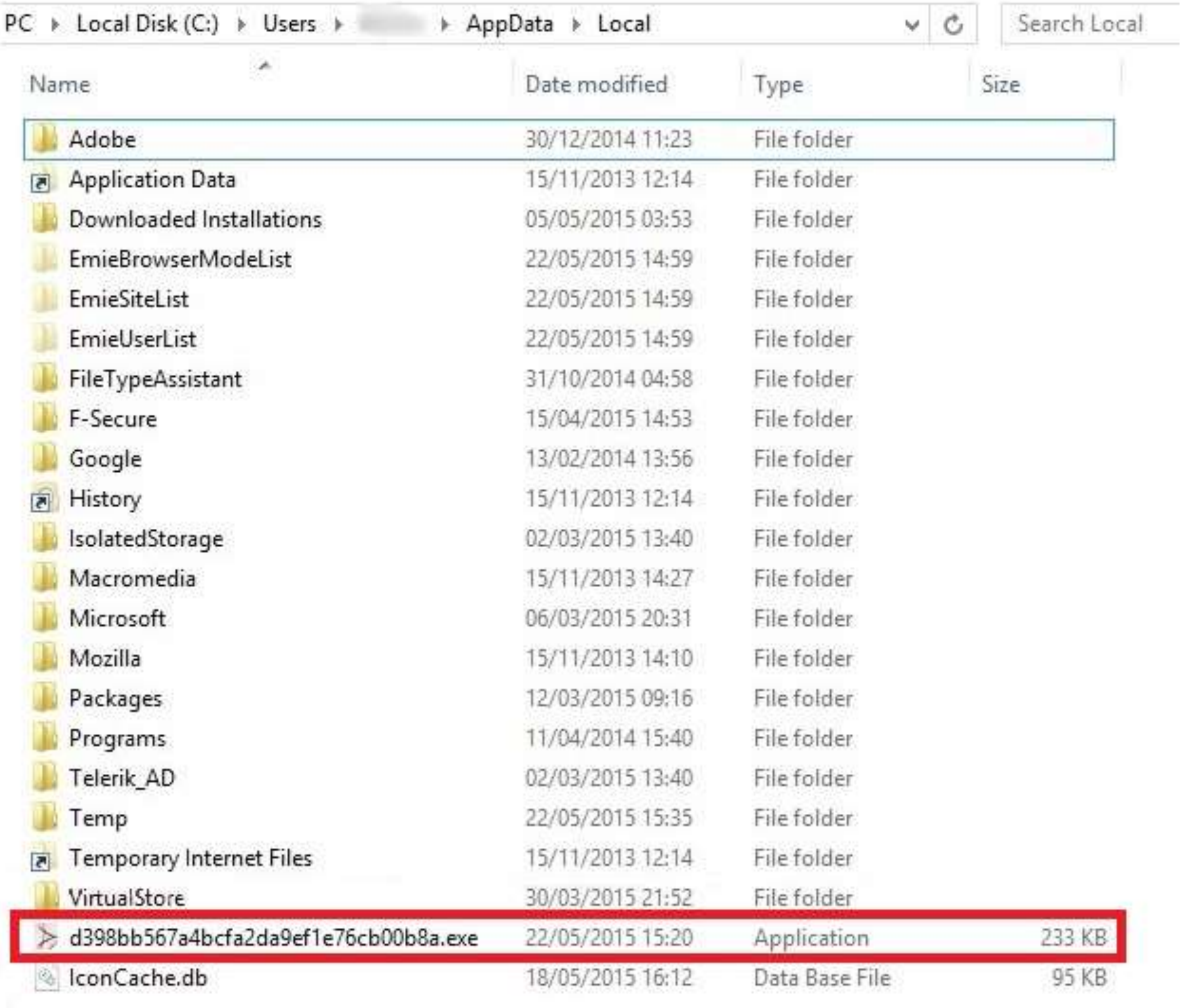
- VirusTotal

- HybridAnalysis

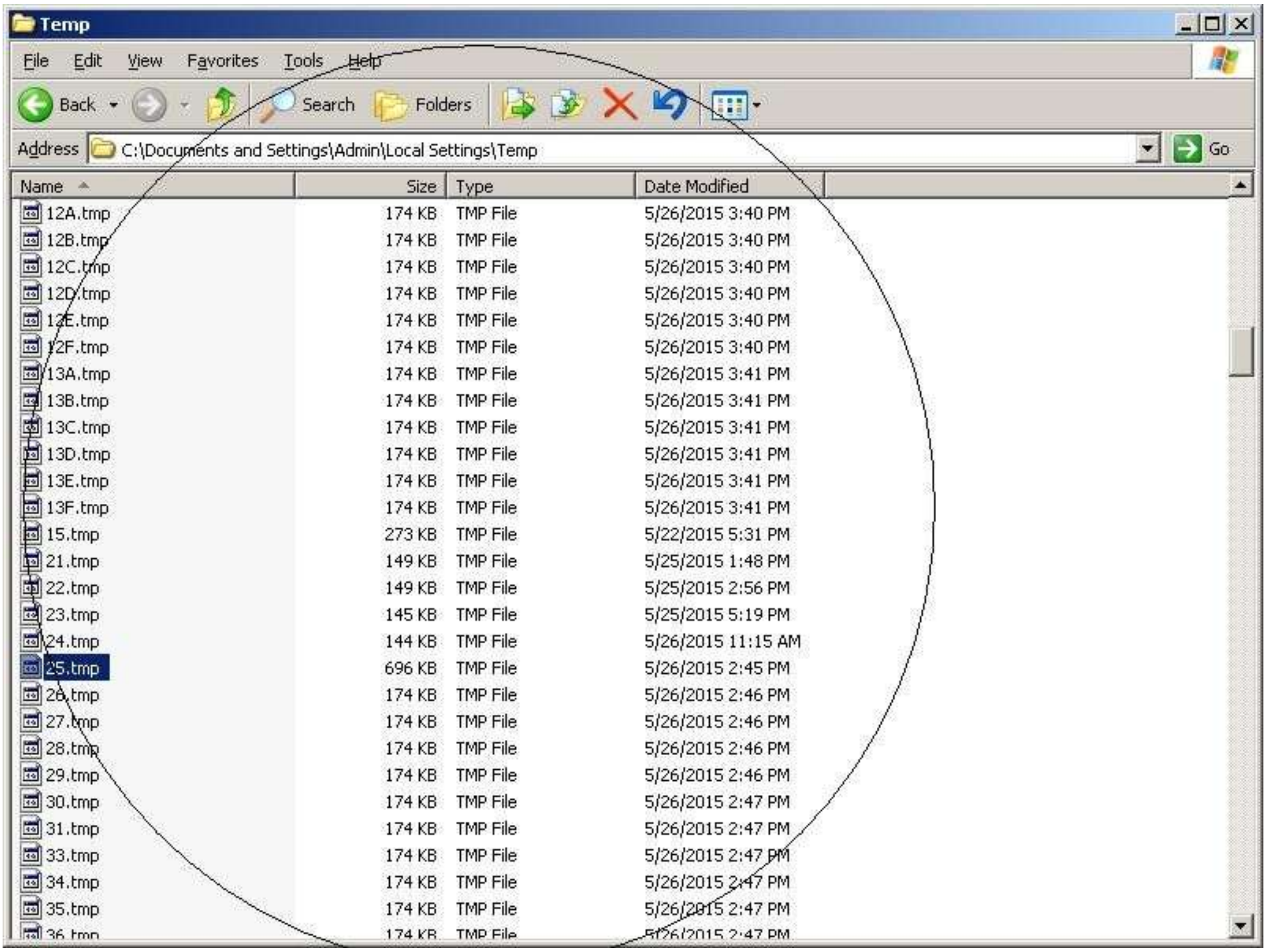
- Any.run

You can generate YARA rules, IOCs, and sandbox results.

Screenshots and Images:-



Name	Date modified	Type	Size
Adobe	30/12/2014 11:23	File folder	
Application Data	15/11/2013 12:14	File folder	
Downloaded Installations	05/05/2015 03:53	File folder	
EmieBrowserModeList	22/05/2015 14:59	File folder	
EmieSiteList	22/05/2015 14:59	File folder	
EmieUserList	22/05/2015 14:59	File folder	
FileTypeAssistant	31/10/2014 04:58	File folder	
F-Secure	15/04/2015 14:53	File folder	
Google	13/02/2014 13:56	File folder	
History	15/11/2013 12:14	File folder	
IsolatedStorage	02/03/2015 13:40	File folder	
Macromedia	15/11/2013 14:27	File folder	
Microsoft	06/03/2015 20:31	File folder	
Mozilla	15/11/2013 14:10	File folder	
Packages	12/03/2015 09:16	File folder	
Programs	11/04/2014 15:40	File folder	
Telerik_AD	02/03/2015 13:40	File folder	
Temp	22/05/2015 15:35	File folder	
Temporary Internet Files	15/11/2013 12:14	File folder	
VirtualStore	30/03/2015 21:52	File folder	
d398bb567a4bcfa2da9ef1e76cb00b8a.exe	22/05/2015 15:20	Application	233 KB
IconCache.db	18/05/2015 16:12	Data Base File	95 KB



Address C:\Documents and Settings\Admin\Local Settings\Temp

Name	Size	Type	Date Modified
12A.tmp	174 KB	TMP File	5/26/2015 3:40 PM
12B.tmp	174 KB	TMP File	5/26/2015 3:40 PM
12C.tmp	174 KB	TMP File	5/26/2015 3:40 PM
12D.tmp	174 KB	TMP File	5/26/2015 3:40 PM
12E.tmp	174 KB	TMP File	5/26/2015 3:40 PM
12F.tmp	174 KB	TMP File	5/26/2015 3:40 PM
13A.tmp	174 KB	TMP File	5/26/2015 3:41 PM
13B.tmp	174 KB	TMP File	5/26/2015 3:41 PM
13C.tmp	174 KB	TMP File	5/26/2015 3:41 PM
13D.tmp	174 KB	TMP File	5/26/2015 3:41 PM
13E.tmp	174 KB	TMP File	5/26/2015 3:41 PM
13F.tmp	174 KB	TMP File	5/26/2015 3:41 PM
15.tmp	273 KB	TMP File	5/22/2015 5:31 PM
21.tmp	149 KB	TMP File	5/25/2015 1:48 PM
22.tmp	149 KB	TMP File	5/25/2015 2:56 PM
23.tmp	145 KB	TMP File	5/25/2015 5:19 PM
24.tmp	144 KB	TMP File	5/26/2015 11:15 AM
25.tmp	696 KB	TMP File	5/26/2015 2:45 PM
26.tmp	174 KB	TMP File	5/26/2015 2:46 PM
27.tmp	174 KB	TMP File	5/26/2015 2:46 PM
28.tmp	174 KB	TMP File	5/26/2015 2:46 PM
29.tmp	174 KB	TMP File	5/26/2015 2:46 PM
30.tmp	174 KB	TMP File	5/26/2015 2:47 PM
31.tmp	174 KB	TMP File	5/26/2015 2:47 PM
33.tmp	174 KB	TMP File	5/26/2015 2:47 PM
34.tmp	174 KB	TMP File	5/26/2015 2:47 PM
35.tmp	174 KB	TMP File	5/26/2015 2:47 PM
36.tmp	174 KB	TMP File	5/26/2015 2:47 PM