Malware Analysis-POC

Malware Name: W32.HfsAdware.5066

Hash (SHA-256): ad214449c1eede7eb98547790f89e86522fe1993bfce3b3279cee96bd4a952a0

Name : MISHTHI NILESH CHAVAN

INTERN ID :- 368

- Introduction :-

This Proof of Concept (PoC) aims to analyze the behavior of the malware sample identified as W32.HfsAdware.5066. This malware belongs to the adware category, which typically displays intrusive advertisements, modifies browser settings, and may collect user data.The objective of this PoC is to document the steps taken to observe and understand the malware's behavior in a controlled environment.

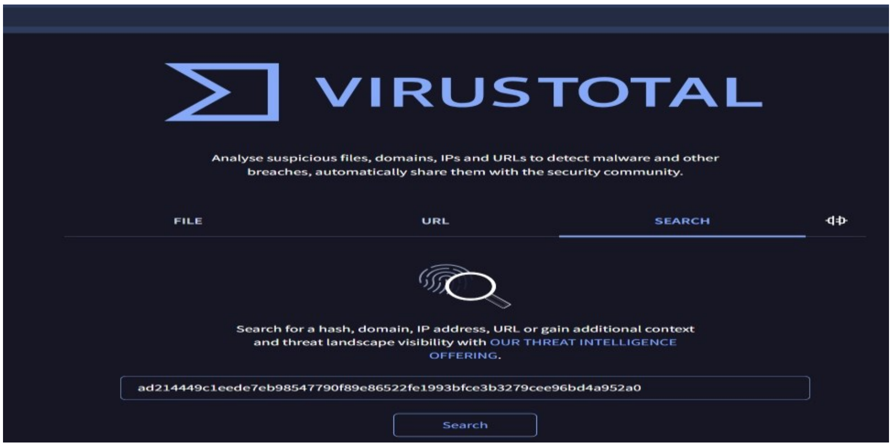
- Mitigation Steps :-

  Terminated malicious processes via Task Manager , Deleted dropped files from disk, Removed persistence entries from the registry , Performed full antivirus scan to ensure removal, Reset browser settings to default.

- Conclusion :-

The W32.HfsAdware.5066 malware primarily functions as adware, displaying unwanted advertisements and maintaining persistence through registry autorun entries. The PoC demonstrates how the malware operates and outlines steps for safe removal.This analysis has provided insights into handling similar adware threats in real-world environments.

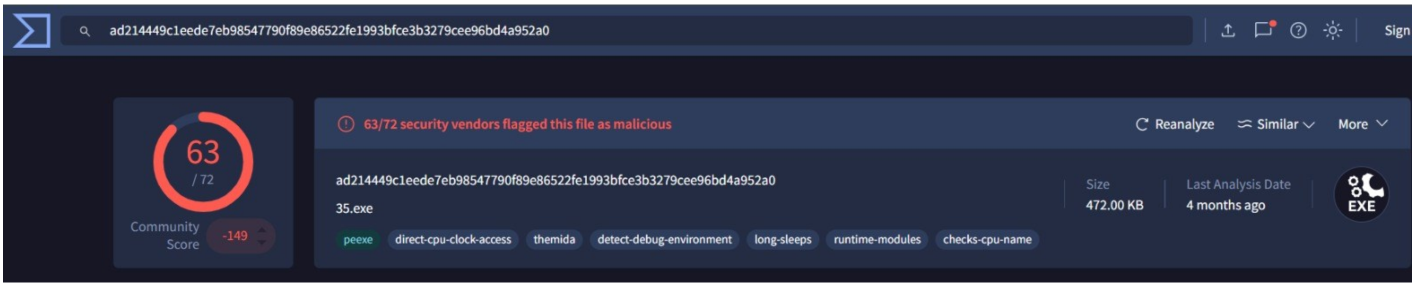
- Screenshots :-



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with OUR THREAT INTELLIGENCE OFFERING.

ad214449c1eede7eb98547790f89e86522fe1993bfce3b3279cee96bd4a952a0


ad214449c1eede7eb98547790f89e86522fe1993bfce3b3279cee96bd4a952a0

63
/ 72

Community Score -149

63/72 security vendors flagged this file as malicious

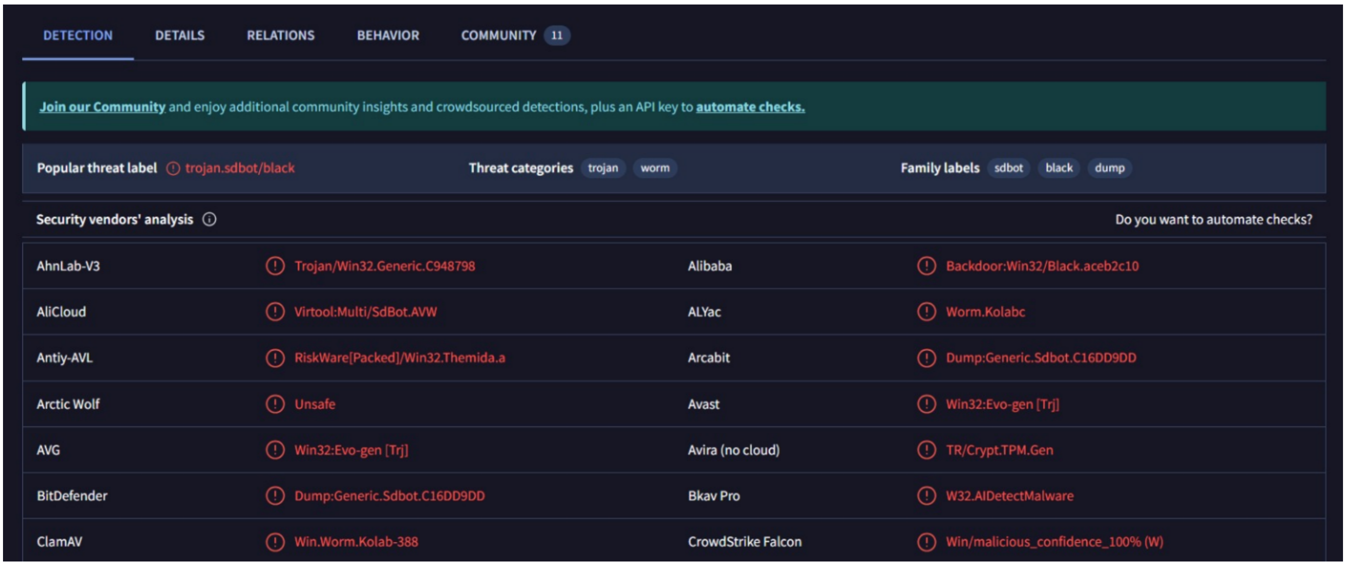
ad214449c1eede7eb98547790f89e86522fe1993bfce3b3279cee96bd4a952a0

35.exe

peexe direct-cpu-clock-access themida detect-debug-environment long-sleeps runtime-modules checks-cpu-name

Size
472.00 KB

Last Analysis Date
4 months ago

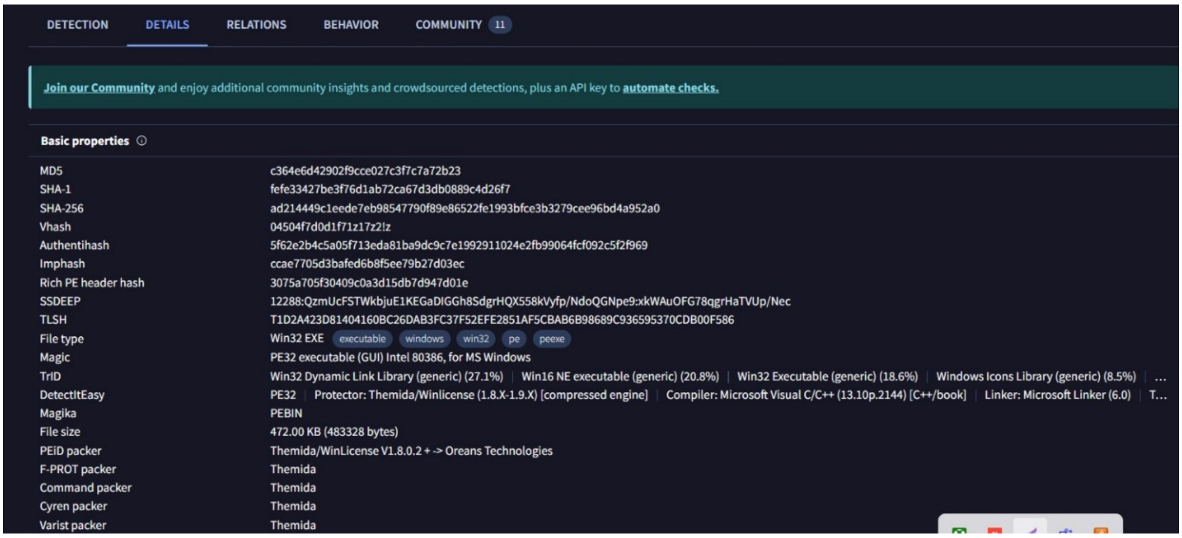


Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Popular threat label trojan.sdbot/black **Threat categories** trojan worm **Family labels** sdbot black dump

Security vendors' analysis Do you want to automate checks?

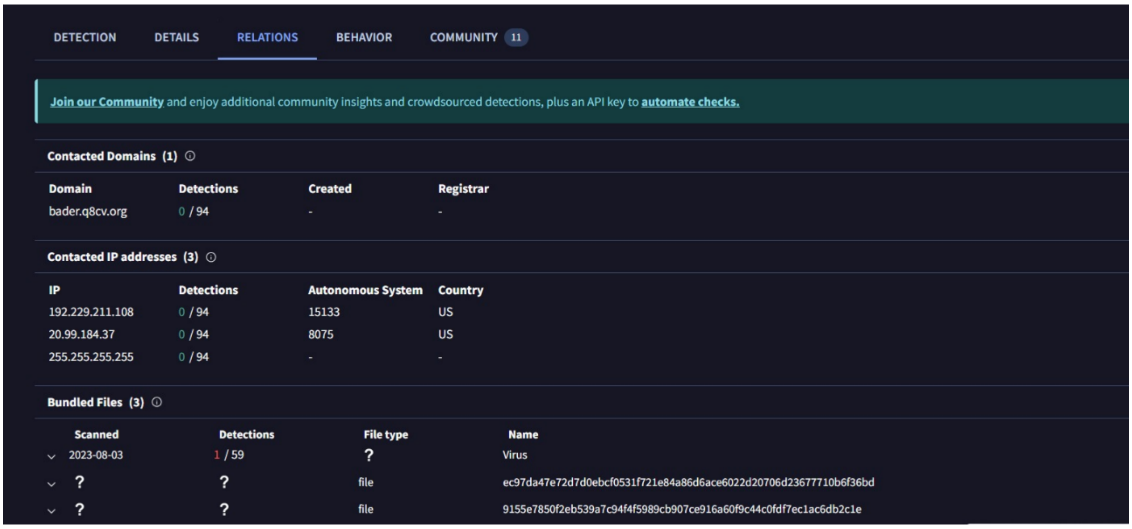
AhnLab-V3	Trojan/Win32.Generic.C948798	Alibaba	Backdoor:Win32/Black.aceb2c10
AliCloud	Virtool:Multi/SdBot.AVW	ALYac	Worm.Kolabc
Antiy-AVL	RiskWare[Packed]/Win32.Themida.a	Arcabit	Dump:Generic.Sdbot.C16DD9DD
Arctic Wolf	Unsafe	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	TR/Crypt.TPM.Gen
BitDefender	Dump:Generic.Sdbot.C16DD9DD	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Worm.Kolab-388	CrowdStrike Falcon	Win/malicious_confidence_100% (W)



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

Basic properties ⓘ

MD5	c364e6d42902f9cce027c3f7c7a72b23
SHA-1	fefe33427be3f76d1ab72ca67d3db0889c4d26f7
SHA-256	ad214449c1eede7eb98547790f89e86522fe1993bfce3b3279cee96bd4a952a0
Vhash	04504f7d0d1f71z17z2!z
Authentihash	5f62e2b4c5a05f713eda81ba9dc9c7e1992911024e2fb99064fcf092c5f2f969
Imphash	ccae7705d3bafed6b8f5ee79b27d03ec
Rich PE header hash	3075a705f30409c0a3d15db7d947d01e
SSDEEP	12288:QzmUcFSTWkbjuE1KEGaDIGGh8SdgrHQX558kVyfp/NdoQGNpe9:xkWAuOFG78qgrHaTVUp/Nec
TLSH	T1D2A423D81404160BC26DAB3FC37F52EFE2851AF5CBAB6B98689C936595370CDB00F586
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Dynamic Link Library (generic) (27.1%) | Win16 NE executable (generic) (20.8%) | Win32 Executable (generic) (18.6%) | Windows Icons Library (generic) (8.5%) | ...
DetectItEasy	PE32 | Protector: Themida/Winlicense (1.8.X-1.9.X) [compressed engine] | Compiler: Microsoft Visual C/C++ (13.10p.2144) [C++/book] | Linker: Microsoft Linker (6.0) | T...
Magika	PEBIN
File size	472.00 KB (483328 bytes)
PEiD packer	Themida/WinLicense V1.8.0.2 + -> Oreans Technologies
F-PROT packer	Themida
Command packer	Themida
Cyren packer	Themida
Varist packer	Themida



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

Contacted Domains (1) ⓘ

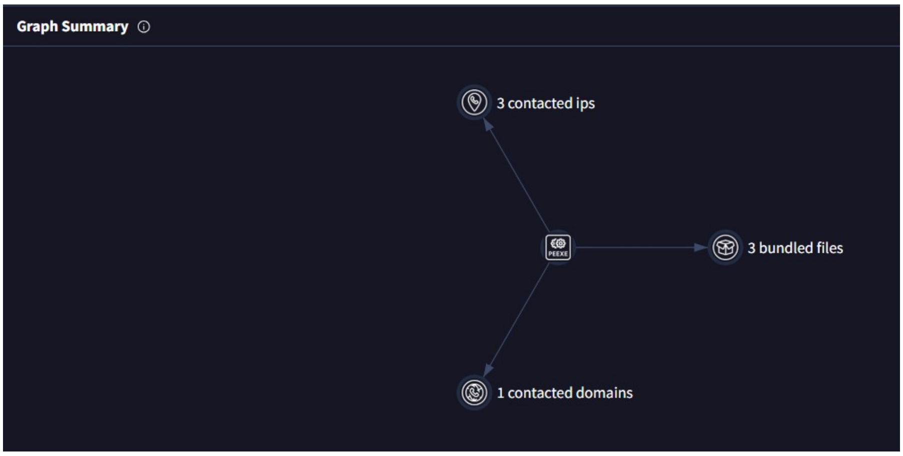
Domain	Detections	Created	Registrar
bader.q8cv.org	0 / 94	-	-

Contacted IP addresses (3) ⓘ

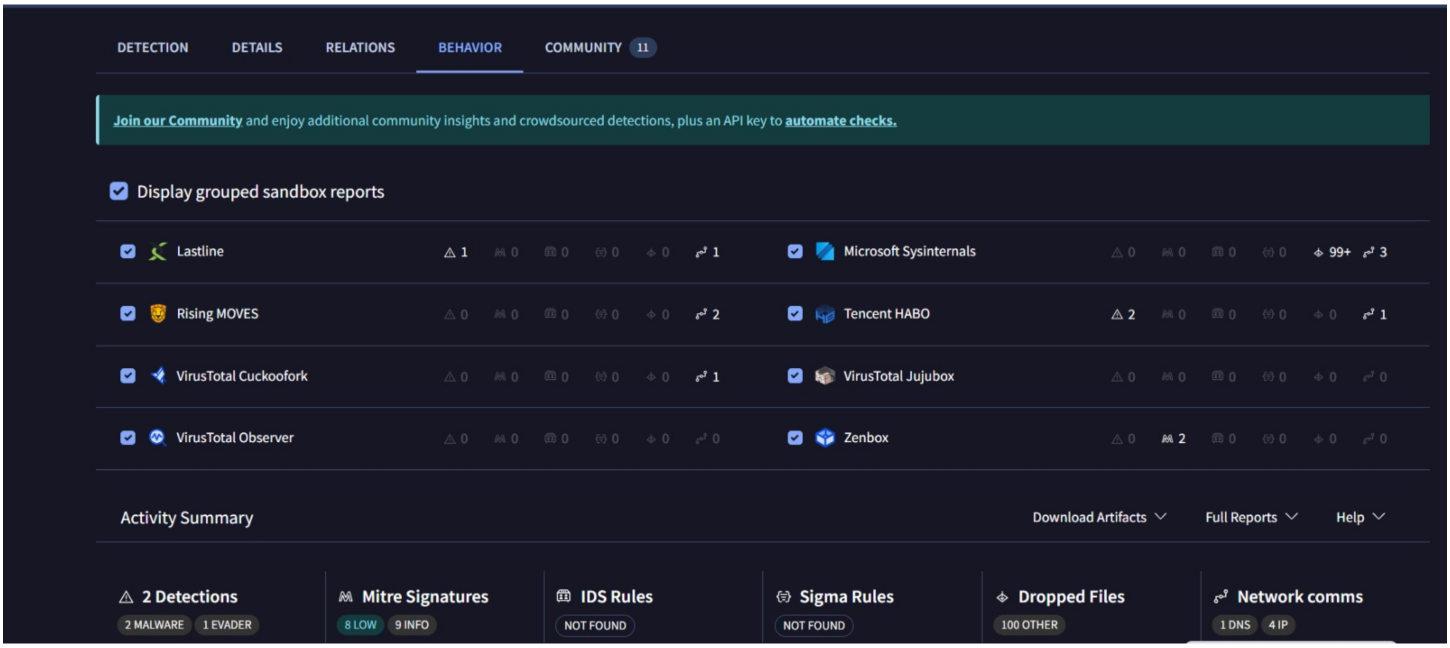
IP	Detections	Autonomous System	Country
192.229.211.108	0 / 94	15133	US
20.99.184.37	0 / 94	8075	US
255.255.255.255	0 / 94	-	-

Bundled Files (3) ⓘ

Scanned	Detections	File type	Name
2023-08-03	1 / 59	?	Virus
?	?	file	ec97da47e72d7d0ebcf0531f721e84a86d6ace6022d20706d23677710b6f36bd
?	?	file	9155e7850f2eb539a7c94f4f5989cb907ce916a60f9c44c0fdf7ec1ac6db2c1e



Graph Summary ⓘ



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

☑ Display grouped sandbox reports

☑ Lastline	⚠ 1	0	0	0	0	1	☑ Microsoft Sysinternals	⚠ 0	0	0	0	99+	3
☑ Rising MOVES	⚠ 0	0	0	0	0	2	☑ Tencent HABO	⚠ 2	0	0	0	0	1
☑ VirusTotal Cuckoofork	⚠ 0	0	0	0	0	1	☑ VirusTotal Jujubox	⚠ 0	0	0	0	0	0
☑ VirusTotal Observer	⚠ 0	0	0	0	0	0	☑ Zenbox	⚠ 0	2	0	0	0	0

Activity Summary

⚠ 2 Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
2 MALWARE 1 EVADER	8 LOW 9 INFO	NOT FOUND	NOT FOUND	100 OTHER	1 DNS 4 IP