

ALL screenshots from virus total

The screenshot shows the VirusTotal analysis interface for a specific file. At the top, it displays a community score of 61/70. Below this, the file's SHA256 hash is shown as 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a. The file is identified as a DLL file. The analysis section shows various detection results from different security vendors. A prominent green bar at the bottom encourages users to join the community for additional insights and automation features.

Security vendor	Detected	Analysis	Security vendor	Detected	Analysis
AhnLab-V3	Win-Trojan/Suspig16.Exp	Alibaba	Ransom:Win32/Kryptik.dab15db1		
AliCloud	Ransomware:Win/Maze.PM8PHU	ALYac	Trojan.Ransom.ChaCha		
Antly-AVL	Trojan[Ransom]/Win32.Gen	Arcabit	Trojan.Ursu.DC94A1		
Arctic Wolf	Unsafe	Avast	Win32:DangerousSig [Tr]		
AVG	Win32:DangerousSig [Tr]	Avira (no cloud)	TR/AD.MazeRansom.nkjxl		
BitDefender	Gen:Variant.Ursu.824481	Bkav Pro	W32.AIDetectMalware		

This screenshot shows a detailed table of vendor analysis results for the same file. The table lists 20 different security vendors along with their detected threat types and associated confidence levels or file names. The interface includes a search bar at the top and a sign-in/up button.

Vendor	Detected	Analysis	Vendor	Detected	Analysis
BitDefender	Gen:Variant.Ursu.824481	Bkav Pro	W32.AIDetectMalware		
ClamAV	Win.Ransomware.Packer-7473772-1	CrowdStrike Falcon	Win/malicious_confidence_100% (W)		
CTX	Dll.trojan.maze	Cynet	Malicious (score: 99)		
DeepInstinct	MALICIOUS	DrWeb	Trojan.Encoder.28416		
Elastic	Windows.Ransomware.Maze	Emsisoft	MalCert.A (A)		
eScan	Gen:Variant.Ursu.824481	ESET-NOD32	Win32/Kryptik.HBPZ!tr.ransom		
Fortinet	W32/Kryptik.HBPZ!tr.ransom	GData	Gen:Variant.Ursu.824481		
Google	Detected	Gridinsoft (no cloud)	Ransom.Win32.Generic.oals1		
Huorong	HVM:TrojanSpy/Stealer.l	Ikarus	Trojan.Win32.Crypt		
Jiangmin	Trojan.Gen.arj	K7AntiVirus	Ransomware (005653641)		
K7GW	Ransomware (005653641)	Kaspersky	HEUR:Trojan-Ransom.Win32.Gen.vho		
Kingsoft	Win32.Trojan-Ransom.Gen.vho	Lionic	Trojan.Win32.Maze.jlc		
Malwarebytes	Malware.Al.1171781579	MaxSecure	Trojan.Malware.87180300.susgen		
McAfee Scanner	Tl4218214F32F9	Microsoft	Ransom.Win32/Maze.GGI/MTB		
Palo Alto Networks	Generic.ml	Panda	Trj/Cl.A		
Rising	Trojan.MalCert!1.C603 (CLASSIC)	Sangfor Engine Zero	Ransom.Win32.Maze.GGI/MTB		

Σ 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a Sign in Sign up

Skyhigh (SWG)	ⓘ Ransom-MAZE 910AA49813EE	Sophos	ⓘ Troj/Maze-R
Symantec	ⓘ Ransom.Mazelgm	TACHYON	ⓘ Ransom/W32.Maze.615624
Tencent	ⓘ Malware.Win32.Gencirc.10bf47ce	Trellix ENS	ⓘ Ransom-MAZE 910AA49813EE
TrendMicro	ⓘ Ransom.Win32.MAZE.AC	TrendMicro-HouseCall	ⓘ Ransom.Win32.MAZE.AC
Varist	ⓘ W32/Ransom.NM.gen!Eldorado	VBA32	ⓘ TrojanRansom.Gen
VIPRE	ⓘ Gen:Variant.Ursu.824481	ViriT	ⓘ Trojan.Win32.Genus.CFY
ViRobot	ⓘ Trojan.Win32.Z.Maze.615624	Webroot	ⓘ W32.Trojan.Gen
WithSecure	ⓘ Trojan.TR/AD.MazeRansom.nkjl	Xcitium	ⓘ Malware#@375sicv81dro7
Yandex	ⓘ Trojan.GenAsalvy1K2963juo	Zillya	ⓘ Trojan.Kryptik.Win32.1983884
ZoneAlarm by Check Point	ⓘ Troj/Ransom-FXF	Acronis (Static ML)	ⓘ Undetected
Baidu	ⓘ Undetected	CMC	ⓘ Undetected
QuickHeal	ⓘ Undetected	SecureAge	ⓘ Undetected
SentinelOne (Static ML)	ⓘ Undetected	SUPERAntiSpyware	ⓘ Undetected
Trapmine	ⓘ Undetected	Zoner	ⓘ Undetected
Avast-Mobile	❌ Unable to process file type	BitDefenderFalk	❌ Unable to process file type
	❌ Unable to process file type	Trustlook	❌ Unable to process file type

<https://www.virustotal.com/gui/home> File Insight 

Σ 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a Sign in Sign up

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties ⓘ

MD5	910aa49813ee4cc7e4fa0074db5e454a
SHA-1	45831987fabeb7b32c70f662be8cb24e2efef1dc
SHA-256	4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
Vhash	165056655d65156a43723
Authentihash	88c3ee0737bc492764691686ab91c575193b59a2a694f530a8cca6530ac535ca
ImpHash	97f9186939da28c5438363e7e2ca2d2d
Rich PE header hash	13ad8ccdf1f27dd6622a824eedebc8844
SSDEEP	12288:yp44JUL8sjy/3/x+w4cJ6ANGriTUA1qDoj2h9TY+gle0rnGLUVHso:uCGBQp3aW44cCIYBeOsMMo
TLSH	T10CD4120105C490B7E4F16381067B9B877939B1AB71DA85AAC0175DFB6031EF39A27
File type	Win32 DLL executable windows win32 pe peddl
Magic	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (7.2%)
DetectItEasy	PE32 Compiler: Microsoft Visual C/C++ [2013] [DLL32] Compiler: Microsoft Visual C/C++ [18.00.21005] [LTCG/C] Linker: Microsoft Linker [12.00.21005] Tool: Vis...
Magika	PEBIN
File size	601.20 KB (615624 bytes)

History ⓘ

Creation Time	2020-04-15 23:09:33 UTC
Signature Date	2020-04-16 00:35:00 UTC
First Seen In The Wild	2020-04-20 14:50:06 UTC
First Submission	2020-04-17 20:35:37 UTC
Last Submission	2024-09-26 02:23:18 UTC
Last Analysis	2026-01-11 14:51:18 UTC

Names ⓘ

910AA49813EE4CC7E4FA0074DB5E454A
45831987fabeb7b32c70f662be8cb24e2efef1dc
4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a.dll
Sample.bin
partmgr.sys
fHuFFchMCwJfBZJtM6XQMyTa.dll
FH0ZyINAo5Rb17xIhVtHs7a11PEJJE.dll
FBq7MScAMO5VuYfPD9SRXJ.dll
u6yZRhGrHnkymOEbzIayAOQt.dll
Ba4NIVJJoEk5yvSdha.dll

Σ 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a Sign in Sign up



Community Score -106

61/70 security vendors flagged this file as malicious

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a.dll

pedi detect-debug-environment revoked-cert calls-wmi spreader long-sleeps signed checks-user-input overlay

Size 601.20 KB | Last Analysis Date 12 days ago | DLL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 29+

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

Contacted Domains (4)

Domain	Detections	Created	Registrar
arc.msn.com	0 / 92	1994-11-10	MarkMonitor Inc.
crl.sectigo.com	0 / 92	2018-08-16	CSC Corporate Domains, Inc.
msftstore.s.lnwi.net	0 / 92	2013-07-31	MarkMonitor Inc.
ocsp.sectigo.com	0 / 92	2018-08-16	CSC Corporate Domains, Inc.

Contacted IP addresses (3)

IP	Detections	Autonomous System	Country
114.114.114.114	0 / 92	21859	CN
178.79.208.1	1 / 92	-	US
20.82.209.183	0 / 92	8075	IE

Σ 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a Sign in Sign up

Execution Parents (2)

Scanned	Detections	Type	Name
2023-10-01	3 / 64	ZIP	Sample.bin.zip
2020-06-16	48 / 65	ZIP	maze.zip

Bundled Files (7)

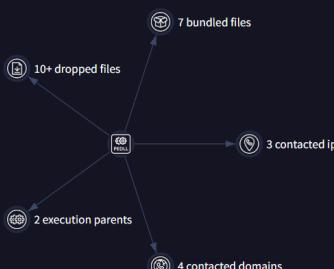
Scanned	Detections	File type	Name
2020-04-20	0 / 58	?	.data
2026-01-23	0 / 61	XML	2
?	?	file	ed77b9039554269b6cd345f50fa1ab6c042a9cad756ac28304b66cba6b58fbcb
?	?	file	d99547e8776811fSaabb2bc1a452eb67229c20ba90f1a921e36737f614b77c
?	?	file	002898c0a7af8df377acb96d60d6099a19081ff983e3e280a151b8bc143a581
?	?	file	522cf13a61c0e83d953bdab6b461e7f11e934e51768cd7d3736464fc20767c
?	?	file	315c23010b6bb14a42ee2be41896a44dec26163cd8d5d729c83846f2f6273b87

Dropped Files (2.4 K)

Scanned	Detections	File type	Name
2022-05-09	0 / 58	?	1621321779437.50adb97-72b2-49c6-b71b-bb57fcdf86d7.update.jsoniz4.vRPO (copy)
2022-12-22	0 / 61	DOS COM	GostTitle.XSL.DVHN0G8 (copy)
2022-03-30	0 / 55	DOS COM	GostName.XSL.wlc17 (copy)
2022-05-09	0 / 58	DOS EXE	HarvardAnglia2008OfficeOnline.xls.n6z3Fo1 (copy)
2022-10-26	0 / 61	?	TM10001115 [fn=Parcel]].thmx.Wksa (copy)
2022-05-06	0 / 58	DOS EXE	IPKGELNTQY.mp3.wl29yoB (copy)
2023-02-12	0 / 60	DOS EXE	Built-In Building Blocks.dotx.0mvonT (copy)
2023-02-12	0 / 60	?	2918063365piupsah.sqlite.nAnGvr (copy)

Σ 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a Sign in Sign up

Graph Summary



The graph illustrates the connections between various entities:

- 7 bundled files
- 3 contacted ips
- 4 contacted domains
- 2 execution parents
- 10+ dropped files

Our product

- Contact Us
- Get Support
- How It Works
- ToS | Privacy Notice
- Blog | Releases

Community

- Join Community
- Vote and Comment
- Contributors
- Top Users
- Community Buzz

Tools

- API Scripts
- YARA
- Desktop Apps
- Browser Extensions
- Mobile App

Premium Services

- Get a demo
- Intelligence
- Hunting
- Graph
- API v3 | v2
- Use Cases

Documentation

- Searching
- Reports
- API v3 | v2
- Use Cases

S 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a Sign in Sign up

61 / 70 security vendors flagged this file as malicious

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a
4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a.dll

pedll detect-debug-environment revoked-cert calls-wmi spreader long-sleeps signed checks-user-input overlay

Detection Details Relations Behavior Community 29+

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

Display grouped sandbox reports

Sandbox	Score	File Type	Behavior
CAPA	2	0	0
DAS-Security Orcas	5	0	99+ 1
QiAnXin RedDrip	0	0	99+ 0
Zenbox	9	0	99+ 3
CAPE Sandbox	1	0	0
Lastline	0	0	0
VMRay	0	0	99+ 0

Activity Summary Download Artifacts Full Reports Help

Activity Summary

S 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a Sign in Sign up

Activity Summary Download Artifacts Full Reports Help

6 Detections Mitre Signatures IDS Rules Sigma Rules Dropped Files Network comms

Type	Count
RANSOM	2
MALWARE	2
STEALER	1
PHISHING	1
TROJAN	1
EVADER	1

Level	Count
HIGH	4
MEDIUM	9
LOW	15

Rule	Count
NOT FOUND	0

Type	Count
OTHER	716
ZLIB	1
DOC	1
BMP	1
JAVASCRIPT	1
TEXT	1

Comms	Count
DNS	3
IP	1

Behavior Tags

calls-wmi checks-hostname checks-user-input crypto detect-debug-environment long-sleeps runtime-modules

Dynamic Analysis Sandbox Detections

- The sandbox VMRay flags this file as: RANSOM
- The sandbox Zenbox flags this file as: MALWARE STEALER RANSOM PHISHING TROJAN EVADER
- The sandbox DAS-Security Orcas flags this file as: MALWARE

Search for technique, subtechnique and its matching entries

None Info Low Medium High

Category	Technique	Count
Execution	TA0002 Windows Management Instrumentation	1
Persistence	TA0003 Boot or Logon Autostart Executable	1
Privilege Escalation	TA0004 Process Injection	2
Defense Evasion	TA0005 Obfuscated Files or Infected Components	2
Credential	TA0006 OS Credential Theft	1

Malware Behavior Catalog Tree

S 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Activity Summary

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and its matching entries

Discovery TA0007 | 13 Techniques

Collection TA0009 | 5 Techniques

Command and Control TA0011 | 3 Techniques

Impact TA0040 | 1 Techniques

System Owner/User Discovery T1033

System Network Connections... T1049

Process Discovery T1057

Data from Local System T1005

Data from Network Shared Dr... T1039

Input Capture T1056

Application Layer Protocol T1071

Proxy T1090

Non-Application Layer Protocol T1095

Data Encrypted for Impact T1486

Custom Information Discovery

Browser Session Hijacking

None Info Low Medium High

This screenshot shows the 'Tactics and Techniques' section of the MITRE ATT&CK interface. It displays a grid of 17 techniques across four main categories: Discovery, Collection, Command and Control, and Impact. Each technique is represented by a card with an icon, name, ID, and a count of subtechniques. A search bar at the top allows users to find specific techniques. A legend at the bottom indicates the severity levels: None (light blue), Info (medium blue), Low (dark blue), Medium (yellow), and High (red).

S 4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Activity Summary

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and its matching entries

Virtualization/Sandbox... T1497

Hide Artifacts T1564

Hijack Execution Flow T1574

Peripheral Device Discovery T1120

Network Share Discovery T1135

Virtualization/Sandbox... T1497

Software Discovery T1518

None Info Low Medium High

Malware Behavior Catalog Tree

+ Anti-Static Analysis OB0002

+ Defense Evasion OB0006

+ Execution OB0009

This screenshot shows the 'Tactics and Techniques' section with a different set of techniques. It includes 'Virtualization/Sandbox...', 'Hide Artifacts', and 'Hijack Execution Flow' under the Discovery tactic, and 'Peripheral Device Discovery', 'Network Share Discovery', 'Virtualization/Sandbox...', and 'Software Discovery' under the Collection tactic. The sidebar on the left displays the 'Malware Behavior Catalog Tree' with nodes for 'Anti-Static Analysis', 'Defense Evasion', and 'Execution'. A blue speech bubble icon in the bottom right corner indicates a comment or message.