

# ALL screenshots from virus total

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

61

Community Score

-106

61/70 security vendors flagged this file as malicious

Reanalyze Similar More

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Size

601.20 KB

Last Analysis Date

12 days ago

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.

Popular threat label

trojan.maze/ursu

Threat categories

trojan ransomware

Family labels

maze ursu dangeroussig

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Win-Trojan/Suspigi16.Exp	Alibaba	Ransom:Win32/Kryptik.dab15db1
AliCloud	Ransomware:Win/Maze.PM8PHU	ALYac	Trojan.Ransom.ChaCha
Antiy-AVL	Trojan(Ransom)/Win32.Gen	Arcabit	Trojan.Ursu.DC94A1
Arctic Wolf	Unsafe	Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.MazeRansom.nkjl
BitDefender	Gen:Variant.Ursu.824481	Bkav Pro	W32.AIDetectMalware

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

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 Trojan
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.AI.1171781579	MaxSecure	Trojan.Malware.87180300.susgen
McAfee Scanner	TII4218214F32F9	Microsoft	Ransom:Win32/Maze.GGIMTB
Palo Alto Networks	Generic.ml	Panda	Trj/CI.A
Rising	Trojan.MalCert!1.C603 (CLASSIC)	Sangfor Engine Zero	Ransom.Win32.Maze.GGIMTB

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Sign in

Sign up

Skyhigh (SWG)	<div><div></div><div>Ransom-MAZEI910AA49813EE</div></div>	Sophos	<div><div></div><div>Troj/Maze-R</div></div>
Symantec	<div><div></div><div>Ransom.Mazelgm</div></div>	TACHYON	<div><div></div><div>Ransom/W32.Maze.615624</div></div>
Tencent	<div><div></div><div>Malware.Win32.Gencirc.10bf47ce</div></div>	Trellix ENS	<div><div></div><div>Ransom-MAZEI910AA49813EE</div></div>
TrendMicro	<div><div></div><div>Ransom.Win32.MAZE.AC</div></div>	TrendMicro-HouseCall	<div><div></div><div>Ransom.Win32.MAZE.AC</div></div>
Varist	<div><div></div><div>W32/Ransom.NM.genIEldorado</div></div>	VBA32	<div><div></div><div>TrojanRansom.Gen</div></div>
VIPRE	<div><div></div><div>Gen:Variant.Ursu.824481</div></div>	VirIT	<div><div></div><div>Trojan.Win32.Genus.CFY</div></div>
ViRobot	<div><div></div><div>Trojan.Win32.Z.Maze.615624</div></div>	Webroot	<div><div></div><div>W32.Trojan.Gen</div></div>
WithSecure	<div><div></div><div>Trojan.TR/AD.MazeRansom.nkjd</div></div>	Xcitiium	<div><div></div><div>Malware@#3759icv61dro7</div></div>
Yandex	<div><div></div><div>Trojan.GenAsalvy1K2963juo</div></div>	Zillya	<div><div></div><div>Trojan.Kryptik.Win32.1983884</div></div>
ZoneAlarm by Check Point	<div><div></div><div>Troj/Ransom-FXf</div></div>	Acronis (Static ML)	<div><div></div><div>Undetected</div></div>
Baidu	<div><div></div><div>Undetected</div></div>	CMC	<div><div></div><div>Undetected</div></div>
QuickHeal	<div><div></div><div>Undetected</div></div>	SecureAge	<div><div></div><div>Undetected</div></div>
SentinelOne (Static ML)	<div><div></div><div>Undetected</div></div>	SUPERAntiSpyware	<div><div></div><div>Undetected</div></div>
Trapmine	<div><div></div><div>Undetected</div></div>	Zoner	<div><div></div><div>Undetected</div></div>
Avast-Mobile	<div><div></div><div>Unable to process file type</div></div>	BitDefenderFalx	<div><div></div><div>Unable to process file type</div></div>
Trustlook	<div><div></div><div>Unable to process file type</div></div>		

https://www.virustotal.com/gui/home

File Insight

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

165056655d65156a2437z3

Authentihash

88c3ee0737bc492764691686ab91c575193b59a2a694f530a8cca6530ac535ca

Imphash

9f79186939da28c9438363e7e2ca2d2d

Rich PE header hash

13ad8ccd1f27dd6622a824eedebcb844

SSDEEP

12288:yqq40JLtl8sJ3y3/xi+aW4cJ6ANGRitRUA1qD0j2h9TY+gleOmGLUVHso:uGCBQp3aW44cCIYBeOsMMo

TLSH

T10CD4120105C490B7E4EF16381067B9B8877939B1AB71DA85AAC0175DFB603C1EF39A27

File type

Win32 DLL 

executable windows win32 pe pedll

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) (7.3%)

DetectItEasy

PE32 | Compiler: EP: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
fHuFFchMCwJfBZjJT1M6XQMyTa.dll
FH02yYINA0sRb17xiHvThS7a11PEjJE.dll
FBq7MScAMOSVuyfPD9SRXJ.dll
u6yZRhGlRhnkymOEDzIAyyAOQt.dll
Ba4NIVJaoEkSyvSdha.dll

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

61/70

Community Score

-106

61/70 security vendors flagged this file as malicious

ReanalyzeSimilarMore

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Size601.20 KB

Last Analysis Date12 days ago

DLL

pedll

detect-debug-environment

revoked-cert

calls-wmi

spreader

long-sleeps

signed

checks-user-input

overlay

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY29+

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.llnwi.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

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

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	ed77b9039554269b6cd345f50fa1ab6c042a9cad756ac28304b66cba6b58bfcb
?	?	file	d99547e8776811f5aabb2bc1a452eb67229c20ba90f1a921e36737f61f4b777c
?	?	file	002898c0a7a7f8df377ac96d60d6099a19081ff383e3e280a151b8bc143a581
?	?	file	522ccf13a61c0e83d953bdab6b461e7f11e934e51768ed7d3736454f0c20767c
?	?	file	315c23010b6bb14a42ee2be41896a44dec26163cd8d5d729c83846f2f6273b87

Dropped Files (2.4 K)

Scanned	Detections	File type	Name
2022-05-09	0 / 58	?	1621321779437.50adbb97-72b2-49c6-b71b-bb57fcd86d7.update.jsonlz4.vRPO (copy)
2022-12-22	0 / 61	DOS COM	GostTitle.XSL.DVHN0G8 (copy)
2022-03-30	0 / 55	DOS COM	GostName.XSL.wld7 (copy)
2022-05-09	0 / 58	DOS EXE	HarvardAnglia2008OfficeOnline.xsl.n6zFo1 (copy)
2022-10-26	0 / 61	?	TM10001115[[fn=Parcel]].thmx.Wxsa (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)

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Graph Summary

7 bundled files

10+ dropped files

2 execution parents

3 contacted ips

4 contacted domains

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

Documentation

Searching

Reports

API v3 | v2

Use Cases

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

61/70

Community Score

-106

61/70 security vendors flagged this file as malicious

Reanalyze Similar More

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Size601.20 KB

Last Analysis Date12 days ago

DLL

pedll

detect-debug-environment

revoked-cert

calls-wmi

spreader

long-sleeps

signed

checks-user-input

overlay

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY29+

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

Display grouped sandbox reports

CAPE

0

2

0

0

0

0

0

0

0

CAPE Sandbox

0

1

0

0

0

0

0

0

0

DAS-Security Orcas

1

5

0

0

0

99+

1

0

0

Lastline

0

0

0

0

0

0

0

0

0

QIANXIN RedDrip

0

0

0

0

0

99+

0

0

0

VMRay

1

0

0

0

0

0

99+

0

0

Zenbox

6

9

0

0

0

99+

3

0

0

Activity Summary

Download Artifacts

Full Reports

Help

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Sign in

Sign up

Activity Summary

Download Artifacts

Full Reports

Help

6 Detections

2 RANSOM

2 MALWARE

1 STEALER

1 PHISHING

1 TROJAN

1 EVADER

Mitre Signatures

4 HIGH

3 MEDIUM

15 LOW

35 INFO

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

716 OTHER

1 ZLIB

1 DOC

1 BMP

1 JAVASCRIPT

1 TEXT

Network comms

3 DNS

1 IP

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 in its matching entries

None

Info

Low

Medium

High

Execution

TA0002 | 5 Techniques

Windows Management Instru...  
T1047

Command and Scripting Inte...  
T1059

Shared Modules  
T1129

Inter-Process Communication

Persistence

TA0003 | 4 Techniques

Boot or Logon Autostart Execu...  
T1547

Hijack Execution Flow  
T1574

Privilege Escalation

TA0004 | 5 Techniques

Process Injection  
T1055

Boot or Logon Autostart Execu...  
T1547

Hijack Execution Flow  
T1574

Defense Evasion

TA0005 | 17 Techniques

Obfuscated Files or Inf...  
T1027

Masquerading  
T1036

Process Injection  
T1055

Indicator Removal

Credential

TA0006 | 2

OS Cn...  
T1003

Input  
T1056

Malware Behavior Catalog Tree

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Sign inSign up

Activity Summary

Download ArtifactsFull ReportsHelp

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and in its matching entries

None

Info

Low

Medium

High

Discovery  
TA0007 | 13 Techniques

System Owner/User Discovery  
T1033  
1

System Network Connections...  
T1049  
1

Process Discovery  
T1057  
2

System Information Discovery  
T1058  
4

Collection  
TA0009 | 5 Techniques

Data from Local System  
T1005  
2

Data from Network Shared Dr...  
T1039  
1

Input Capture  
T1056  
1

Browser Session Hijacking  
T1059  
1

Command and Control  
TA0011 | 3 Techniques

Application Layer Protocol  
T1071  
2

Proxy  
T1090  
1

Non-Application Layer Protocol  
T1095  
1

Impact  
TA0040 | 1 Techniques

Data Encrypted for Impact  
T1486  
2

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

Sign inSign up

Activity Summary

Download ArtifactsFull ReportsHelp

MITRE ATT&CK Tactics and Techniques

Search for technique, subtechnique and in its matching entries

None

Info

Low

Medium

High

Virtualization/Sandbox...  
T1497  
2

Hide Artifacts  
T1564

Hijack Execution Flow  
T1574

Peripheral Device Discovery  
T1120  
1

Network Share Discovery  
T1135  
1

Virtualization/Sandbox...  
T1497  
2

Software Discovery  
T1518  
1

Malware Behavior Catalog Tree

+ Anti-Static Analysis OB0002

+ Defense Evasion OB0006

+ Execution OB0009