

# screenshot task 5 (hash sha256=4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a )

4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

61/70 security vendors flagged this file as malicious

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 vendor	Threat label	Vendor	Confidence
AhnLab-V3	Win-Trojan/Suspig16.Exp	Alibaba	Ransom:Win32/Kryptik.dab15db1
AliCloud	Ransomware:Win/Maze.PM8PHU	ALYac	Trojan.Ransom.ChaCha
Anty-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.nkjxl
BitDefender	Gen:Variant.Ursu.824481	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Ransomware.Packer-7473772-1	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	DL!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/Cl.A
Rising	Trojan.MalCert!l.C603 (CLASSIC)	Sangfor Engine Zero	Ransom:Win32.Maze.GGIMTB

Σ  4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a

The screenshot shows the VirusTotal analysis interface. At the top, there's a search bar with the file hash and a 'Sign in' button. Below the search bar is a table with two columns of analysis results for 21 different engines. The engines are listed in the first column, and their detection results are in the second column. A blue 'File Insight' button is at the bottom left, and a blue 'Feedback' icon is at the bottom right.

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.nkxl	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