

13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31

↑

?

Sign in

Sign up

63

/ 73

Community Score

-10

63/73 security vendors flagged this file as malicious

Reanalyze

Similar

More

13828b390d5f58b002e808c2c4f02fdd920e236cc8015480fa33b6c1a9300e31

Size

2.93 MB

Last Analysis Date

8 days ago

EXE

peexe

idle

direct-cpu-clock-access

detect-debug-environment

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

17+

Join our Community

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

Popular threat label

ransomware.blackcat/blackcatalphv

Threat categories

ransomware

trojan

Family labels

blackcat

blackcatalphv

encoder

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win.Generic.R476325	Alibaba	Ransom:Win32/BlackCat.80f4d7e7
AliCloud	RansomWare	ALYac	Trojan.Ransom.BlackCat
Antiy-AVL	Trojan/Win32.Filecoder	Arcabit	Trojan.Ransom.BlackCatALPHV.9
Avast	Win32:RansomX-gen [Ransom]	AVG	Win32:RansomX-gen [Ransom]
Avira (no cloud)	TR/YAV.Minerva.hegar	BitDefender	Gen:Variant.Ransom.BlackCatALPHV.9
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Ransomware.BlackCat-9934796-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.ransomware.blackcat
Cylance	Unsafe	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Encoder.34835
Elastic	Multi.Ransomware.BlackCat	Emsisoft	Gen:Variant.Ransom.BlackCatALPHV.9 (B)
eScan	Gen:Variant.Ransom.BlackCatALPHV.9	ESET-NOD32	A Variant Of Win32/Filecoder.BlackCat.A
Fortinet	W32/Filecoder.A!tr.ransom	GData	Gen:Variant.Ransom.BlackCatALPHV.9
Google	Detected	Gridinsoft (no cloud)	Ransom.Win32.AI.oa!s1
Huorong	Ransom/BTCware.b	Ikarus	Trojan-Ransom.BlackCat
Jiangmin	Trojan.Generic.helpw	K7AntiVirus	Ransomware ( 005ad4021 )
K7GW	Ransomware ( 005ad4021 )	Kaspersky	HEUR:Trojan-Ransom.Win32.Generic
Kingsoft	Win32.Trojan-Ransom.Generic.a	Lionic	Trojan.Win32.Encoder.U!c
Malwarebytes	Generic.Malware.AI.DDS	MaxSecure	Trojan.Malware.10307848.susgen

McAfee Scanner

Ti113828B390D5F

Microsoft

Ransom:Win32/BlackCat.MKIMTB

NANO-Antivirus

Trojan.Win32.Encoder.jruyqf

Palo Alto Networks

Generic.ml

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our [Privacy Notice](#).

Ok

Page 1 of 2

Sign inSign up

Rising	⚠ Ransom.BlackCat!1.DB0B (CLASSIC)	Sangfor Engine Zero	⚠ Ransom.Win32.Blackcat.V8qq
SecureAge	⚠ Malicious	SentinelOne (Static ML)	⚠ Static AI - Malicious PE
Skyhigh (SWG)	⚠ BehavesLike.Win32.RansomBlackCat.vh	Sophos	⚠ Troj/Ransom-GSD
Symantec	⚠ Ransom.Noberus	TACHYON	⚠ Ransom/W32.Agent.3073536.B
Tencent	⚠ Malware.Win32.Gencirc.10bc6df4	Trellix (ENS)	⚠ Ransom-BlackCat!C6901BC6720E
Trellix (HX)	⚠ Generic.mg.c6901bc6720e1e30	TrendMicro	⚠ Ransom.Win32.BLACKCAT.YXBL2Z
TrendMicro-HouseCall	⚠ Ransom.Win32.BLACKCAT.YXBL2Z	Varist	⚠ W32/Filecoder.CP.gen!Eldorado
VBA32	⚠ BScope.Trojan.Encoder	VIPRE	⚠ Gen:Variant.Ransom.BlackCatALPHV.9
ViRobot	⚠ Trojan.Win32.Z.Fragtor.3073536.C	Webroot	⚠ W32.Ransom.Blackcat
WithSecure	⚠ Trojan.TR/YAV.Minerva.hegar	Zillya	⚠ Trojan.Filecoder.Win32.21394
ZoneAlarm by Check Point	⚠ HEUR:Trojan-Ransom.Win32.Generic	Acronis (Static ML)	✅ Undetected
Baidu	✅ Undetected	CMC	✅ Undetected
SUPERAntiSpyware	✅ Undetected	TEHTRIS	✅ Undetected
Trapmine	✅ Undetected	VirIT	✅ Undetected
Xcitium	✅ Undetected	Yandex	✅ Undetected
Zoner	✅ Undetected	Avast-Mobile	🚫 Unable to process file type
BitDefenderFalx	🚫 Unable to process file type	Symantec Mobile Insight	🚫 Unable to process file type
Trustlook	🚫 Unable to process file type		

Our product	Community	Tools	Premium Services	Documentation
<a href="#">Contact Us</a>	<a href="#">Join Community</a>	<a href="#">API Scripts</a>	<a href="#">Get a demo</a>	<a href="#">Searching</a>
<a href="#">Get Support</a>	<a href="#">Vote and Comment</a>	<a href="#">YARA</a>	<a href="#">Intelligence</a>	<a href="#">Reports</a>
<a href="#">How It Works</a>	<a href="#">Contributors</a>	<a href="#">Desktop Apps</a>	<a href="#">Hunting</a>	<a href="#">API v3   v2</a>
<a href="#">ToS   Privacy Notice</a>	<a href="#">Top Users</a>	<a href="#">Browser Extensions</a>	<a href="#">Graph</a>	<a href="#">Use Cases</a>
<a href="#">Blog   Releases</a>	<a href="#">Community Buzz</a>	<a href="#">Mobile App</a>	<a href="#">API v3   v2</a>	