

15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc59a79fc222c7ed

↑

🗨

?

⚙

Sign in

Sign up

65

/ 72

Community Score

-1

⚠ 65/72 security vendors flagged this file as malicious

🔄 Reanalyze

🔗 Similar

More

15b57c1b68cd6ce3c161042e0f3be9f32d78151fe95461eedc...239908___a910ba1b-a35d-4955-8635-d4a2e9c37c4d.exe

Size

2.93 MB

Last Analysis Date

10 days ago

🔧🌙

EXE

peexe

idle

detect-debug-environment

direct-cpu-clock-access

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

16+

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

encode

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	⚠ Trojan/Win.Generic.R476325	Alibaba	⚠ Ransom:Win32/BlackCat.b238c162
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

⚠ Tl15B57C1B68CD

Microsoft

⚠ Ransom:Win32/BlackCat

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.Ve2o
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!C1DD3D5A3528
Trellix (HX)	Generic.mg.c1dd3d5a3528bf56	TrendMicro	Ransom.Win32.BLACKCAT.YXBLXZ
TrendMicro-HouseCall	Ransom.Win32.BLACKCAT.YXBLXZ	Varist	W32/Filecoder.CP.gen!Eldorado
VBA32	BScope.Trojan.Encoder	VIPRE	Gen:Variant.Ransom.BlackCatALPHV.9
ViRobot	Trojan.Win32.Z.Fragtor.3073536.A	Webroot	W32.Ransom.Blackcat
WithSecure	Trojan.TR/YAV.Minerva.hegar	Xcitium	Malware@#dl db6jjjz wfu
Yandex	Trojan.Filecoder!1pVHrfYo9JM	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	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
VirIT	—		

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](#)