

38283b775552da8981452941ea74191aa0d203edd3f61fb2dee7b0aea3514955

⬆

💬

?

☀

Sign in

Sign up

28

/ 63

Community Score

-9

⚠ 28/63 security vendors flagged this file as malicious

🔄 Reanalyze

🔗 Similar

More

38283b775552da8981452941ea74191aa0d203edd3f61fb2d...

Size

6.31 KB

Last Analysis Date

1 month ago

z.bat

bat

direct-cpu-clock-access

idle

calls-wmi

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY6

Join our Community

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

🌟 Code insights

The script you provided contains a number of commands that delete or stop various services and processes. These include services and processes for antivirus software, such as Trend Micro, Kaspersky, and Webroot. The script also contains a command to kill all processes with a PID greater than 1000, which could include legitimate processes as well as malicious processes.

Show more

Popular threat label

⚠ trojan.generickds/killav

Threat categories

trojan

Family labels

generickds

killav

battamper

Security vendors' analysis ⓘ

Do you want to automate checks?

ALYac	⚠ Trojan.GenericKDS.61002071	Arcabit	⚠ Trojan.GenericS.D3A2D157
Avast	⚠ Other:Malware-gen [Trj]	AVG	⚠ Other:Malware-gen [Trj]
BitDefender	⚠ Trojan.GenericKDS.61002071	CTX	⚠ Batch.trojan.killav
DrWeb	⚠ BAT.KillProc.26	Emsisoft	⚠ Trojan.GenericKDS.61002071 (B)
eScan	⚠ Trojan.GenericKDS.61002071	ESET-NOD32	⚠ BAT/KillAV.NGH
GData	⚠ Trojan.GenericKDS.61002071	Google	⚠ Detected
Huorong	⚠ Trojan/Generic!DFF170D0C22946CE	Ikarus	⚠ Trojan.Win32.BatTamper
Kaspersky	⚠ Trojan.BAT.KillAV.ri	Kingsoft	⚠ Win32.Troj.Undef.a
Lionic	⚠ Trojan.Script.GenericKDS.4!c	Microsoft	⚠ Trojan:Win32/BatTamper.A
QuickHeal	⚠ Script.Agent.45687	Sangfor Engine Zero	⚠ Suspicious.Win32.Save.a
Skyhigh (SWG)	⚠ Generic Trojan.ni	Sophos	⚠ Troj/KillAV-JF
Symantec	⚠ Trojan Horse	Tencent	⚠ Bat.Trojan.Killav.Gdhl
Trellix (ENS)	⚠ Generic .ni	Trellix (HX)	⚠ Trojan.GenericKDS.61002071
VIPRE	⚠ Trojan.GenericKDS.61002071	ZoneAlarm by Check Point	⚠ Trojan.BAT.KillAV.ri
Acronis (Static ML)	✔ Undetected	AhnLab-V3	✔ Undetected
Alibaba Cloud	✔ Undetected	Antiy-AVL	✔ Undetected
Avira (NO cloud)	✔ Undetected	Baidu	✔ Undetected

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

CMC		Undetected	CrowdStrike Falcon		Undetected
Cynet		Undetected	Fortinet		Undetected
Gridinsoft (no cloud)		Undetected	Jiangmin		Undetected
K7AntiVirus		Undetected	K7GW		Undetected
Malwarebytes		Undetected	MaxSecure		Undetected
NANO-Antivirus		Undetected	Panda		Undetected
Rising		Undetected	SUPERAntiSpyware		Undetected
TACHYON		Undetected	TEHTRIS		Undetected
TrendMicro		Undetected	TrendMicro-HouseCall		Undetected
Varist		Undetected	VBA32		Undetected
VirIT		Undetected	ViRobot		Undetected
WithSecure		Undetected	Xcitium		Undetected
Yandex		Undetected	Zillya		Undetected
Zoner		Undetected	Alibaba		Unable to process file type
Avast-Mobile		Unable to process file type	BitDefenderFalx		Unable to process file type
Cylance		Unable to process file type	DeepInstinct		Unable to process file type
Elastic		Unable to process file type	McAfee Scanner		Unable to process file type
Palo Alto Networks		Unable to process file type	SecureAge		Unable to process file type
SentinelOne (Static ML)		Unable to process file type	Symantec Mobile Insight		Unable to process file type
Trapmine		Unable to process file type	Trustlook		Unable to process file type
Webroot		Unable to process file type			

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