



SUMMARY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

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

Popular

threat ! trojan.swrort/cryptz

Threat categories tr

Family labels swrort














label

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	<span>!</span> Trojan/Win32.Shell.R1283
Alibaba	<span>!</span> Trojan:Win32/CobaltStrike.5c89
AliCloud	<span>!</span> Backdoor:Win/CobaltStrike.reverse.A
ALYac	<span>!</span> Trojan.CryptZ.Marte.1.Gen
Antiy-AVL	<span>!</span> Trojan/Win32.Rozena
Arcabit	<span>!</span> Trojan.CryptZ.Marte.1.Gen
Avast	<span>!</span> Win32:Meterpreter-C [Trj]
AVG	<span>!</span> Win32:Meterpreter-C [Trj]
Avira (no cloud)	<span>!</span> TR/Patched.Gen2
BitDefender	<span>!</span> Trojan.CryptZ.Marte.1.Gen
Bkav Pro	<span>!</span> W32.AIDetectMalware
ClamAV	<span>!</span> Win.Trojan.MSShellcode-7
CrowdStrike Falcon	<span>!</span> Win/malicious_confidence_100% (W)
CTX	<span>!</span> Exe.trojan.cryptz
Cylance	<span>!</span> Unsafe
Cynet	<span>!</span> Malicious (score: 100)
DeepInstinct	<span>!</span> MALICIOUS
DrWeb	<span>!</span> Trojan.Swrort.1
Elastic	<span>!</span> Windows.Trojan.Metasploit
Emsisoft	<span>!</span> Trojan.CryptZ.Marte.1.Gen (B)
eScan	<span>!</span> Trojan.CryptZ.Marte.1.Gen
Fortinet	<span>!</span> W32/Swrort.C!tr
GData	<span>!</span> Win32.Backdoor.Swrort.C
Google	<span>!</span> Detected

Huorong	⚠ Backdoor/Meterpreter.d
Ikarus	⚠ Trojan.Win32.Rozena
K7AntiVirus	⚠ Trojan ( 001172b51 )
K7GW	⚠ Trojan ( 001172b51 )
Kaspersky	⚠ HEUR:Trojan.Win32.Generic
Kingsoft	⚠ Malware.kb.a.1000
Lionic	⚠ Trojan.Win32.Swrort.4!c
Malwarebytes	⚠ Trojan.Rozena
MaxSecure	⚠ Trojan.Malware.7164915.susgen
McAfee Scanner	⚠ Real Protect-LS!DAAA5713109E
Microsoft	⚠ Trojan:Win32/Meterpreter.O!MTB
NANO-Antivirus	⚠ Trojan.Win32.Shellcode.ewfwj
Palo Alto Networks	⚠ Generic.ml
Panda	⚠ Trj/Genetic.gen
QuickHeal	⚠ Trojan.Swrort.A
Rising	⚠ HackTool.Swrort!1.6477 (CLASSIC)
Sangfor Engine Zero	⚠ Trojan.Win32.Save.a
SecureAge	⚠ Malicious
SentinelOne (Static ML)	⚠ Static AI - Suspicious PE
Skyhigh (SWG)	⚠ BehavesLike.Win32.Generic.lz
Sophos	⚠ Mal/EncPk-ACE
Symantec	⚠ Packed.Generic.347
Tencent	⚠ Trojan.Win32.Metasploit_heur.16000...
Trellix (ENS)	⚠ Swrort.d
Trellix (HX)	⚠ Generic.mg.daaa5713109e3a50
TrendMicro	⚠ BKDR_SWRORT.SM
TrendMicro-HouseCall	⚠ BKDR_SWRORT.SM
Varist	⚠ W32/Swrort.A.gen!Eldorado
VBA32	⚠ BScope.Trojan.Metasploit
VIPRE	⚠ Trojan.CryptZ.Marte.1.Gen
VirIT	⚠ Trojan.Win32.Rozena.AA
Webroot	⚠ W32.Malware.Gen
WithSecure	⚠ Trojan.TR/Patched.Gen2
Xcitium	⚠ TrojWare.Win32.Rozena.A@4jwdqr
Yandex	⚠ Trojan.Rosena.Gen.1
Zillya	⚠ Trojan.Rozena.Win32.226148
Acronis (Static ML)	✅ Undetected
Baidu	✅ Undetected
CMC	✅ Undetected

Gridinsoft (no cloud)	 Undetected
Jiangmin	 Undetected
SUPERAntiSpyware	 Undetected
TACHYON	 Undetected
TEHTRIS	 Undetected
Trapmine	 Undetected
ViRobot	 Undetected
Zoner	 Undetected
ESET-NOD32	 Timeout
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