66 / 73

Community Score -1

66/73 security vendors flagged this file as malicious

Reanalyze Similar More

5092b2672b4cb87a8dd1c2e6047b487b95995ad8ed5e9f…
5092b2672b4cb87a8dd1c2e6047b487b95995ad8ed5e9f…

Size 217.50 KB

Last Analysis Date 23 days ago

EXE

peexe direct-cpu-clock-access long-sleeps checks-network-adapters spreader runtime-modules malware cve-2015-3008 exploit

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 12

Popular threat label trojan.cobaltstrike/rozena **Threat categories** trojan virus **Family labels** cobaltstrike rozena cometer

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Unwanted/Win32.RL_Cobalt.R293669	Alibaba	Backdoor:Win32/Cometer.16b82d7f
AliCloud	Backdoor:Win/CobaltStrike.Artifact.3A4	ALYac	Trojan.CobaltStrike.FM
Antiy-AVL	GrayWare/Win32.Rozena.wz	Arcabit	Trojan.CobaltStrike.FM
Avast	Win32:MsfShell-J [Trj]	AVG	Win32:MsfShell-J [Trj]
Avira (no cloud)	TR/Crypt.XPACK.Gen	BitDefender	Trojan.CobaltStrike.FM
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.CobaltStrike-8091534-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.cobaltstrike
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	Trojan.Siggen6.51060
Elastic	Windows.Trojan.CobaltStrike	Emsisoft	Trojan.CobaltStrike.FM (B)
eScan	Trojan.CobaltStrike.FM	ESET-NOD32	A Variant Of Win32/CobaltStrike.Beacon…
Fortinet	W32/Rozena.WZ!tr	GData	Win32.Malware.Rozena.F
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.vb!s1
Huorong	HEUR:VirTool/Obfuscator.gen!B	Ikarus	Trojan.Win32.CobaltStrike
Jiangmin	Trojan.Cometer.od	K7AntiVirus	Virus (7000000b1)
K7GW	Virus (7000000b1)	Kaspersky	HEUR:Trojan.Win32.CobaltStrike.gen
Kingsoft	Malware.kb.a.1000	Lionic	Trojan.Win32.CobaltStrike.4!c
Malwarebytes	Generic.Malware.AI.DDS	MaxSecure	Trojan.Malware.73412758.susgen
McAfee Scanner	Real Protect-LSIBBEBA65CE171	Microsoft	Backdoor:Win32/CobaltStrike!pz
NANO-Antivirus	Virus.Win32.Gen-Crypt.ccnc	Palo Alto Networks	Generic.ml

Rising	Trojan.Swrort!1.BAB0 (CLASSIC)	Sangfor Engine Zero	HackTool.Win32.Artifact32_and_Resour…
SecureAge	Malicious	SentinelOne (Static ML)	Static AI - Malicious PE
Skyhigh (SWG)	BehavesLike.Win32.Generic.dh	Sophos	Mal/Generic-S
Symantec	Backdoor.Rozena	Tencent	Trojan.Win32.CobaltStrike.yb
Trapmine	Malicious.moderate.ml.score	Trellix (ENS)	GenericRXLP-MH!BBFBA65CE171
Trellix (HX)	Generic.mg.bbfba65ce17191fe	TrendMicro	Backdoor.Win32.COBEACON.SMC
TrendMicro-HouseCall	Backdoor.Win32.COBEACON.SMC	Varist	W32/Rozena.AD.gen!Eldorado
VBA32	Trojan.CobaltStrike	VIPRE	Trojan.CobaltStrike.FM
VirIT	Trojan.Win32.Crypt5.BLLV	ViRobot	Adware.Cobaltstrike.222720
WithSecure	Trojan.TR/Crypt.XPACK.Gen	Xcitium	TrojWare.Win32.Kryptik.BYGK@59ple7
Yandex	Trojan.GenAsa!zvVdoDjE9iw	Zillya	Trojan.CobaltStrike.Win32.7372
ZoneAlarm by Check Point	HEUR:Trojan.Win32.Cometer.gen	Zoner	Probably Heur.ExeHeaderL
Acronis (Static ML)	Undetected	Baidu	Undetected
CMC	Undetected	SUPERAntiSpyware	Undetected
TACHYON	Undetected	TEHTRIS	Undetected
Webroot	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		