54 / 72

Community Score

54/72 security vendors flagged this file as malicious

Reanalyze Similar More

5fcda49ee7f202559a6cbbb34edb65c33c9a1e0bde9fa2af…

Rubeus.exe

Size 193.50 KB

Last Analysis Date 18 days ago

EXE

peexe direct-cpu-clock-access runtime-modules assembly detect-debug-environment long-sleeps

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

Popular threat label trojan.rubeus/msil

Threat categories trojan hacktool pua

Family labels rubeus msil marte

Security vendors' analysis

Do you want to automate checks?

Alibaba	VirTool:MSIL/Rubeus.9248eef7	AliCloud	Hacktool:Win/Rubeus
ALYac	Misc.Riskware.Rubeus	Arcabit	Generic.Trojan.Rubbie.Marte.A.DE313EED
Avast	Win32:HacktoolX-gen [Trj]	AVG	Win32:HacktoolX-gen [Trj]
Avira (no cloud)	HEUR/AGEN.1307547	BitDefender	Generic.Trojan.Rubbie.Marte.A.DE313EED
Bkav Pro	W32.AIDetectMalware.CS	ClamAV	Win.Trojan.HackTool_MSIL_Rubeus_1-9…
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.marte
Cylance	Unsafe	DeepInstinct	MALICIOUS
DrWeb	Tool.RubeusNET.1	Elastic	Windows.Hacktool.Rubeus
Emsisoft	Generic.Trojan.Rubbie.Marte.A.DE313EE…	eScan	Generic.Trojan.Rubbie.Marte.A.DE313EED
ESET-NOD32	A Variant Of MSIL/Riskware.Rubeus.A	Fortinet	Riskware/Rubeus
GData	Generic.Trojan.Rubbie.Marte.A.DE313EED	Google	Detected
Huorong	HackTool/MSIL.Rubeus.a	Ikarus	Virus.Win32.Kekeo
Jiangmin	HackTool.MSIL.oye	K7AntiVirus	Trojan (00577e681)
K7GW	Trojan (00577e681)	Kaspersky	HEUR:HackTool.MSIL.Rubeus.gen
Lionic	Hacktool.Win32.Rubeus.3!c	Malwarebytes	Generic.Malware.AI.DDS
MaxSecure	Trojan.Malware.101416824.susgen	McAfee Scanner	Ti!5FCDA49EE7F2
Microsoft	VirTool:MSIL/Kekeo.NT!MTB	NANO-Antivirus	Trojan.Win32.Mlw.hyokus
QuickHeal	Trojan.YakbeexMSIL.ZZ4	Rising	Virus.Undefined!8.23 (CLOUD)
Sangfor Engine Zero	Hacktool.Win32.Kekeo.fireeye	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE	Skyhigh (SWG)	BehavesLike.Win32.AgentTesla.cm
Sophos	ATK/Rubeus-B	Symantec	Hacktool.Rebeus

Trellix (HX)	Generic.mg.5a40286e2a672b5c	TrendMicro	TROJ_FRS.0NA103LA20
TrendMicro-HouseCall	TROJ_FRS.0NA103LA20	Varist	W32/Rubeus.A.gen!Eldorado
VIPRE	Generic.Trojan.Rubbie.Marte.A.DE313EED	Webroot	W32.Trojan.Gen
WithSecure	Heuristic.HEUR/AGEN.1307547	Xcitium	Malware@#2zzojhyxygwtv
Zillya	Tool.Rubeus.Win32.54	ZoneAlarm by Check Point	HEUR:HackTool.MSIL.Rubeus.gen
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Antiy-AVL	Undetected	Baidu	Undetected
CMC	Undetected	Cynet	Undetected
Gridinsoft (no cloud)	Undetected	Kingsoft	Undetected
Palo Alto Networks	Undetected	Panda	Undetected
SUPERAntiSpyware	Undetected	TACHYON	Undetected
TEHTRIS	Undetected	Trapmine	Undetected
VBA32	Undetected	ViRobot	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
VirIT	—		