58d21840d915aaf4040ceb89522396124c82f325282f805d1085527e1e2ccfa1

Sign in | Sign up

27 / 60

Community Score

27/60 security vendors flagged this file as malicious

Reanalyze | Similar | More

58d21840d915aaf4040ceb89522396124c82f325282f805d108…

VirtualHost.vbs

Size 265 B

Last Analysis Date 7 months ago

vba | run-file | direct-cpu-clock-access | detect-debug-environment | create-ole | powershell | macro-powershell | exe-pattern | enum-windows | long-sleeps | runtime-modules

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 5

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Code insights

The code creates a WScript.Shell object and uses it to execute a command.
The command starts a hidden PowerShell window and runs a configuration file named "ngrok.yml" located in the user's AppData folder.
The purpose of this command is to start the ngrok tool, which is used for creating secure tunnels to expose local servers to the internet.

Popular threat label trojan.fhuk/runner | **Threat categories** trojan | **Family labels** fhuk | runner | starter

Security vendors' analysis | Do you want to automate checks?

AhnLab-V3	Trojan/VBS.Runner	ALYac	Trojan.VBS.Runner
Arcabit	Trojan.Agent.FHUK	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	BitDefender	Trojan.Agent.FHUK
ClamAV	Vbs.Loader.Empire-9860999-0	Emsisoft	Trojan.Agent.FHUK (B)
eScan	Trojan.Agent.FHUK	ESET-NOD32	VBS/Runner.NPU
GData	Trojan.Agent.FHUK	Google	Detected
Ikarus	Trojan.VBS.Runner	Kaspersky	Trojan.VBS.Starter.mo
MAX	Malware (ai Score=82)	Microsoft	Trojan:Script/Wacatac.B!ml
Rising	Trojan.Runner!8.93 (TOPIS:E0:tdbef30ra…	Skyhigh (SWG)	VBS/Agent.gs
Symantec	Trojan.Gen.NPE	Tencent	Vbs.Trojan.Starter.Ywhl
Trellix (ENS)	VBS/Agent.gs	Trellix (HX)	Trojan.Agent.FHUK
TrendMicro	TROJ_FRS.0NA103A324	TrendMicro-HouseCall	TROJ_FRS.0NA103A324
Varist	VBS/Agent.ADJ	VIPRE	Trojan.Agent.FHUK
ZoneAlarm by Check Point	Trojan.VBS.Starter.mo	Acronis (Static ML)	Undetected
Antiy-AVL	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected
CAT-QuickHeal	Undetected	CMC	Undetected

Fortinet	Undetected	Gridinsoft (no cloud)	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kingsoft	Undetected
Lionic	Undetected	Malwarebytes	Undetected
MaxSecure	Undetected	NANO-Antivirus	Undetected
Panda	Undetected	QuickHeal	Undetected
Sangfor Engine Zero	Undetected	Sophos	Undetected
SUPERAntiSpyware	Undetected	TACHYON	Undetected
VBA32	Undetected	VirIT	Undetected
ViRobot	Undetected	WithSecure	Undetected
Xcitium	Undetected	Yandex	Undetected
Zillya	Undetected	Zoner	Undetected
Alibaba	Unable to process file type	AliCloud	Unable to process file type
Avast-Mobile	Unable to process file type	BitDefenderFalx	Unable to process file type
CrowdStrike Falcon	Unable to process file type	Cybereason	Unable to process file type
Cylance	Unable to process file type	DeepInstinct	Unable to process file type
Elastic	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	TEHTRIS	Unable to process file type
Trapmine	Unable to process file type	Trustlook	Unable to process file type