60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3

Sign in Sign up

29 / 65

Community Score -56

29/65 security vendors flagged this file as malicious

Reanalyze Similar More

60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffc...

sdaidapguyeblhyhbbkd

Size 6.17 KB

Last Analysis Date 2 months ago

shell detect-debug-environment self-delete idle persistence malware direct-cpu-clock-access

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 8

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

Code insights

This script is designed to download and install a backdoor on a QNAP NAS device. The backdoor is a binary executable file named "apached". The script first checks if the file already exists, and if not, it downloads it from a remote server. The file is then moved to a directory named "/share/CACHEDEV3_DATA/.qnapd" and given the executable permissions.

Show more

Popular threat label trojan.gobrat/shell **Threat categories** trojan downloader **Family labels** gobrat shell

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Downloader/Shell.Agent.SC189011	AliCloud	DDoS
ALYac	Trojan.Downloader.Shell.Agent	Arcabit	Trojan.Linux.Generic.D48C9A
Avast	BV:GobRat-A [Drp]	AVG	BV:GobRat-A [Drp]
BitDefender	Trojan.Linux.Generic.298138	DrWeb	Linux.DownLoader.2212
Emsisoft	Trojan.Linux.Generic.298138 (B)	eScan	Trojan.Linux.Generic.298138
ESET-NOD32	Linux/GobRAT.A	Fortinet	BASH/GobRAT.6049!tr
GData	Trojan.Linux.Generic.298138	Google	Detected
Ikarus	Trojan.Linux.Gobrat	Kaspersky	HEUR:Trojan.Shell.Agent.bv
Lionic	Trojan.Script.GobRAT.4!c	MAX	Malware (ai Score=80)
Microsoft	Trojan:Linux/ShellAgnt!MTB	Sophos	Linux/GobRAT-A
Symantec	Downloader	Tencent	Win32.Trojan.Agent.Mgil
Trellix (HX)	Trojan.Linux.Generic.298138	TrendMicro	TROJ_FRS.0NA103FM23
TrendMicro-HouseCall	TROJ_FRS.0NA103FM23	Varist	ABRisk.PHAL-71
VIPRE	Trojan.Linux.Generic.298138	ViRobot	BIN.S.Agent.6319
ZoneAlarm by Check Point	HEUR:Trojan.Shell.Agent.bv	Acronis (Static ML)	Undetected
Antiy-AVL	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected

CMC	Undetected	CrowdStrike Falcon	Undetected
Cybereason	Undetected	Cynet	Undetected
Gridinsoft (no cloud)	Undetected	Huorong	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kingsoft	Undetected
Malwarebytes	Undetected	MaxSecure	Undetected
NANO-Antivirus	Undetected	Panda	Undetected
QuickHeal	Undetected	Rising	Undetected
Sangfor Engine Zero	Undetected	Skyhigh (SWG)	Undetected
SUPERAntiSpyware	Undetected	TACHYON	Undetected
TEHTRIS	Undetected	Trellix (ENS)	Undetected
VBA32	Undetected	VirIT	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		