# Indicator Removal: File Deletion, Sub-technique T1070.004 - Enterprise

Archived: 2026-04-05 14:20:17 UTC

C0028 2015 Ukraine Electric Power Attack

During the 2015 Ukraine Electric Power Attack, vba_macro.exe deletes itself after `FONTCACHE.DAT`, `rundll32.exe`, and the associated .lnk file is delivered. [2]

S1167 AcidPour

AcidPour includes a self-delete function where the malware deletes itself from disk after execution and program load into memory.[3]

S0045 ADVSTORESHELL

ADVSTORESHELL can delete files and directories.[4]

S0504 Anchor

Anchor can self delete its dropper after the malware is successfully deployed.[5]

S1133 Apostle

Apostle writes batch scripts to disk, such as `system.bat` and `remover.bat`, that perform various anti-analysis and anti-forensic tasks, before finally deleting themselves at the end of execution. Apostle attempts to delete itself after encryption or wiping operations are complete and before shutting down the victim machine.[6]

S0584 AppleJeus

AppleJeus has deleted the MSI file after installation.[7]

S0622 AppleSeed

AppleSeed can delete files from a compromised host after they are exfiltrated.[8]

G0026 APT18

APT18 actors deleted tools and batch files from victim systems.[9]

G0007 APT28

APT28 has intentionally deleted computer files to cover their tracks, including with use of the program CCleaner. [10]

G0016 APT29

APT29 has used SDelete to remove artifacts from victim networks.[11]

G0022 APT3

APT3 has a tool that can delete files.[12]

G0050 APT32

APT32's macOS backdoor can receive a "delete" command.[13]

G0082 APT38

APT38 has used a utility called CLOSESHAVE that can securely delete a file from the system. They have also removed malware, tools, or other non-native files used during the intrusion to reduce their footprint or as part of the post-intrusion cleanup process.[14][15]

G0087 APT39

APT39 has used malware to delete files after they are deployed on a compromised host.[16]

G0096 APT41

APT41 deleted files from the system.[17][18]

C0040 APT41 DUST

APT41 DUST deleted various artifacts from victim systems following use.[19]

G1023 APT5

APT5 has deleted scripts and web shells to evade detection.[20][21]

G0143 Aquatic Panda

Aquatic Panda has deleted malicious executables from compromised machines.[22][23]

C0046 ArcaneDoor

ArcaneDoor included multiple instances of file deletion or removal during execution and other adversary actions.[24][25]

S0456 Aria-body

Aria-body has the ability to delete files and directories on compromised hosts.[26]

S0438 Attor

Attor's plugin deletes the collected files and log files after exfiltration.[27]

S0347 AuditCred

AuditCred can delete files from the system.[28]

S0344 Azorult

Azorult can delete files from victim machines.[29]

S0414 BabyShark

BabyShark has cleaned up all files associated with the secondary payload execution.[30]

S0475 BackConfig

BackConfig has the ability to remove files and folders related to previous infections.[31]

S0093 Backdoor.Oldrea

Backdoor.Oldrea contains a cleanup module that removes traces of itself from the victim.[32]

S1081 BADHATCH

BADHATCH has the ability to delete PowerShell scripts from a compromised machine.[33]

S0234 Bandook

Bandook has a command to delete a file.[34]

S0239 Bankshot

Bankshot marks files to be deleted upon the next system reboot and uninstalls and removes itself from the system.[35]

S0534 Bazar

Bazar can delete its loader using a batch file in the Windows temporary folder.[36]

S0127 BBSRAT

BBSRAT can delete files and directories.[37]

S1246 BeaverTail

BeaverTail has deleted files from a compromised host after they were exfiltrated.[38]

S0268 Bisonal

Bisonal will delete its dropper and VBS scripts from the victim's machine.[39][40][41]

G1043 BlackByte

BlackByte deleted ransomware executables post-encryption.[42][43][44][45]

S1181 BlackByte 2.0 Ransomware

BlackByte 2.0 Ransomware deletes itself following device encryption.[44]

S0069 BLACKCOFFEE

BLACKCOFFEE has the capability to delete files.[46]

S0520 BLINDINGCAN

BLINDINGCAN has deleted itself and associated artifacts from victim machines.[47]

S0657 BLUELIGHT

BLUELIGHT can uninstall itself.[48]

S1184 BOLDMOVE

BOLDMOVE can remove files on victim systems.[49]

S1161 BPFDoor

After initial setup, BPFDoor's original execution process deletes the dropped binary and exits.[50]

G0060 BRONZE BUTLER

The BRONZE BUTLER uploader or malware the uploader uses `command` to delete the RAR archives after they have been exfiltrated.[51]

S1039 Bumblebee

Bumblebee can uninstall its loader through the use of a `Sdl` command.[52]

C0032 C0032

During the C0032 campaign, TEMP.Veles routinely deleted tools, logs, and other files after they were finished with them.[53]

S0274 Calisto

Calisto has the capability to use `rm -rf` to remove folders and files from the victim's machine.[54]

S0030 Carbanak

Carbanak has a command to delete files.[55]

S0348 Cardinal RAT

Cardinal RAT can uninstall itself, including deleting its executable.[56]

S0462 CARROTBAT

CARROTBAT has the ability to delete downloaded files from a compromised host.[57]

S1043 ccf32

ccf32 can delete files and folders from compromised machines.[58]

S0674 CharmPower

CharmPower can delete created files from a compromised system.[59]

S0107 Cherry Picker

Recent versions of Cherry Picker delete files and registry keys created by the malware.[60]

G0114 Chimera

Chimera has performed file deletion to evade detection.[61]

S0106 cmd

cmd can be used to delete files from the file system.[62]

S1105 COATHANGER

COATHANGER removes files from victim environments following use in multiple instances.[63]

G0080 Cobalt Group

Cobalt Group deleted the DLL dropper from the victim's machine to cover their tracks.[64]

G1052 Contagious Interview

Contagious Interview has configured malware to remove archives used in collection activities following successful exfiltration.[38]

S0115 Crimson

Crimson has the ability to delete files from a compromised host.[65][66][67]

S0498 Cryptoistic

Cryptoistic has the ability delete files from a compromised host.[68]

S0527 CSPY Downloader

CSPY Downloader has the ability to self delete.[69]

S0625 Cuba

Cuba can use the command `cmd.exe /c del` to delete its artifacts from the system.[70]

C0029 Cutting Edge

During Cutting Edge, threat actors deleted `/tmp/test1.txt` on compromised Ivanti Connect Secure VPNs which was used to hold stolen configuration and cache files.[71][72]

S1014 DanBot

DanBot can delete its configuration file after installation.[73]

S1111 DarkGate

DarkGate has deleted its staging directories.[74]

S0673 DarkWatchman

DarkWatchman has been observed deleting its original launcher after installation.[75]

S0354 Denis

Denis has a command to delete files from the victim's machine.[76][77]

S0021 Derusbi

Derusbi is capable of deleting files. It has been observed loading a Linux Kernel Module (LKM) and then deleting it from the hard disk as well as overwriting the data with null bytes.[78][79]

G0035 Dragonfly

Dragonfly has deleted many of its files used during operations as part of cleanup, including removing applications and deleting screenshots.[80]

S0502 Drovorub

Drovorub can delete specific files from a compromised host.[81]

S0567 Dtrack

Dtrack can remove its persistence and delete itself.[82]

S0062 DustySky

DustySky can delete files it creates from the infected system.[83]

S0593 ECCENTRICBANDWAGON

ECCENTRICBANDWAGON can delete log files generated from the malware stored at `C:\windows\temp\tmp0207` .[84]

S0081 Elise

Elise is capable of launching a remote shell on the host to delete itself.[85]

S1247 Embargo

Embargo has leveraged MDeployer to terminate the MS4Killer process, delete the decrypted payload files and a driver file dropped by MS4killer, and reboot the system.[86]

G1003 Ember Bear

Ember Bear deletes files related to lateral movement to avoid detection.[87]

S0091 Epic

Epic has a command to delete a file from the machine.[88]

S0396 EvilBunny

EvilBunny has deleted the initial dropper after running through the environment checks.[89]

G0120 Evilnum

Evilnum has deleted files used during infection.[90]

S0401 Exaramel for Linux

Exaramel for Linux can uninstall its persistence mechanism and delete its configuration file.[91]

S1179 Exbyte

Exbyte will self-delete if a hard-coded configuration file is not found.[44]

S0181 FALLCHILL

FALLCHILL can delete malware and associated artifacts from the victim.[92]

S0512 FatDuke

FatDuke can secure delete its DLL.[93]

S0267 FELIXROOT

FELIXROOT deletes the .LNK file from the startup directory as well as the dropper components.[94]

S0679 Ferocious

Ferocious can delete files from a compromised host.[95]

G0051 FIN10

FIN10 has used batch scripts and scheduled tasks to delete critical system files.[96]

G0053 FIN5

FIN5 uses SDelete to clean up the environment and attempt to prevent detection.[97]

G0037 FIN6

FIN6 has removed files from victim machines.[98]

G0061 FIN8

FIN8 has deleted tmp and prefetch files during post compromise cleanup activities. FIN8 has also deleted PowerShell scripts to evade detection on compromised machines.[99][100]

S0381 FlawedAmmyy

FlawedAmmyy can execute batch scripts to delete files.[101]

S0277 FruitFly

FruitFly will delete files on the system.[102]

S1044 FunnyDream

FunnyDream can delete files including its dropper component.[58]

S0410 Fysbis

Fysbis has the ability to delete files.[103]

G0047 Gamaredon Group

Gamaredon Group tools can delete files used during an operation.[104][105][106][107]

S0168 Gazer

Gazer has commands to delete files and persistence mechanisms from the victim.[108][109]

S0666 Gelsemium

Gelsemium can delete its dropper component from the targeted system.[110]

S0032 gh0st RAT

gh0st RAT has the capability to to delete files.[111][112]

S0249 Gold Dragon

Gold Dragon deletes one of its files, 2.hwp, from the endpoint after establishing persistence.[113]

S0493 GoldenSpy

GoldenSpy's uninstaller can delete registry entries, files and folders, and finally itself once these tasks have been completed.[114]

S1198 Gomir

Gomir deletes its original executable and terminates its original process after creating a systemd service.[115]

S0531 Grandoreiro

Grandoreiro can delete .LNK files created in the Startup folder.[116]

S0690 Green Lambert

Green Lambert can delete the original executable after initial installation in addition to unused functions.[117][118]

S0342 GreyEnergy

GreyEnergy can securely delete a file by hooking into the DeleteFileA and DeleteFileW functions in the Windows API.[119]

S0632 GrimAgent

GrimAgent can delete old binaries on a compromised host.[120]

G0043 Group5

Malware used by Group5 is capable of remotely deleting files from victims.[121]

S0561 GuLoader

GuLoader can delete its executable from the `AppData\Local\Temp` directory on the compromised host.[122]

S0151 HALFBAKED

HALFBAKED can delete a specified file.[123]

S0499 Hancitor

Hancitor has deleted files using the VBA `kill` function.[124]

S0391 HAWKBALL

HAWKBALL has the ability to delete files.[125]

S0697 HermeticWiper

HermeticWiper has the ability to overwrite its own file with random bites.[126][127]

S1027 Heyoka Backdoor

Heyoka Backdoor has the ability to delete folders and files from a targeted system.[128]

S0087 Hi-Zor

Hi-Zor deletes its RAT installer file as it executes its DLL payload file.[129]

S0601 Hildegard

Hildegard has deleted scripts after execution.[130]

S0431 HotCroissant

HotCroissant has the ability to clean up installed files, delete files, and delete itself from the victim's machine.[131]

S0070 HTTPBrowser

HTTPBrowser deletes its original installer file once installation is complete.[132]

S0203 Hydraq

Hydraq creates a backdoor through which remote attackers can delete files.[133][134]

S0398 HyperBro

HyperBro has the ability to delete a specified file.[135]

S1022 IceApple

IceApple can delete files and directories from targeted systems.[136]

S0434 Imminent Monitor

Imminent Monitor has deleted files related to its dynamic debugger feature.[137]

G1032 INC Ransom

INC Ransom has uninstalled tools from compromised endpoints after use.[138]

S0259 InnaputRAT

InnaputRAT has a command to delete files.[139]

S0260 InvisiMole

InvisiMole has deleted files and directories including XML and files successfully uploaded to C2 servers.[140][141]

S1132 IPsec Helper

IPsec Helper can delete itself when given the appropriate command.[6]

S0015 Ixeshe

Ixeshe has a command to delete a file from the machine.[142]

S0044 JHUHUGIT

The JHUHUGIT dropper can delete itself from the victim. Another JHUHUGIT variant has the capability to delete specified files.[143][144]

S0201 JPIN

JPIN's installer/uninstaller component deletes itself if it encounters a version of Windows earlier than Windows XP or identifies security-related processes running.[145]

S0283 jRAT

jRAT has a function to delete files from the victim's machine.[146]

S0265 Kazuar

Kazuar can delete files.[147]

S1020 Kevin

Kevin can delete files created on the victim's machine.[148]

S0271 KEYMARBLE

KEYMARBLE has the capability to delete files off the victim's machine.[149]

S0607 KillDisk

KillDisk has the ability to quit and delete itself.[150]

G0094 Kimsuky

Kimsuky has deleted the exfiltrated data on disk after transmission. Kimsuky has also used an instrumentor script to terminate browser processes running on an infected system and then delete the cookie files on disk.[151][152][153] Kimsuky has deleted files using the `Remove-Item` PowerShell commandlet to remove traces of executed payloads.[154]

S0437 Kivars

Kivars has the ability to uninstall malware from the infected host.[155]

S0162 Komplex

The Komplex trojan supports file deletion.[156]

S0356 KONNI

KONNI can delete files.[157]

C0035 KV Botnet Activity

KV Botnet Activity removes on-disk copies of tools and other artifacts after it the primary botnet payload has been loaded into memory on the victim device.[158]

S1160 Latrodectus

Latrodectus has the ability to delete itself.[159][160]

G0032 Lazarus Group

Lazarus Group malware has deleted files in various ways, including "suicide scripts" to delete malware binaries from the victim. Lazarus Group also uses secure file deletion to delete files from the victim.[161][162]

S0395 LightNeuron

LightNeuron has a function to delete files.[163]

S1188 Line Runner

Line Runner removes its initial ZIP delivery archive after processing the enclosed LUA script.[24]

S0211 Linfo

Linfo creates a backdoor through which remote attackers can delete files.[164]

S0513 LiteDuke

LiteDuke can securely delete files by first writing random data to the file.[93]

S1199 LockBit 2.0

LockBit 2.0 can delete itself from disk after execution.[165][166][167]

S1202 LockBit 3.0

LockBit 3.0 can delete itself from disk.[168][169]

S0372 LockerGoga

LockerGoga has been observed deleting its original launcher after execution.[170]

S0447 Lokibot

Lokibot will delete its dropped files after bypassing UAC.[171]

S0582 LookBack

LookBack removes itself after execution and can delete files on the system.[172]

S0451 LoudMiner

LoudMiner deleted installation files after completion.[173]

S1142 LunarMail

LunarMail can delete the previously used staging directory and files on subsequent rounds of exfiltration and replace it with a new one.[174]

S1141 LunarWeb

LunarWeb can self-delete from a compromised host if safety checks of C2 connectivity fail.[174]

S0409 Machete

Once a file is uploaded, Machete will delete it from the machine.[175]

S1016 MacMa

MacMa can delete itself from the compromised computer.[176]

S0282 MacSpy

MacSpy deletes any temporary files it creates[177]

G0059 Magic Hound

Magic Hound has deleted and overwrote files to cover tracks.[178][179][180]

S1182 MagicRAT

MagicRAT can delete files on victim systems, including itself.[181]

G1051 Medusa Group

Medusa Group has deleted previously installed tools.[182]

S1244 Medusa Ransomware

Medusa Ransomware has the ability to delete itself after execution.[183] Medusa Ransomware also has the ability to delete itself after execution through the command `cmd /c ping localhost -n 3 > nul & del` .[184][185]

G0045 menuPass

A menuPass macro deletes files after it has decoded and decompressed them.[186][187]

S0443 MESSAGETAP

Once loaded into memory, MESSAGETAP deletes the keyword_parm.txt and parm.txt configuration files from disk. [188]

G1013 Metador

Metador has quickly deleted `cbd.exe` from a compromised host following the successful deployment of their malware.[189]

S1059 metaMain

metaMain has deleted collected items after uploading the content to its C2 server.[189][190]

S0455 Metamorfo

Metamorfo has deleted itself from the system after execution.[191][192]

S0688 Meteor

Meteor will delete the folder containing malicious scripts if it detects the hostname as `PIS-APP` , `PIS-MOB` , `WSUSPROXY` , or `PIS-DB` .[193]

S1015 Milan

Milan can delete files via `C:\Windows\system32\cmd.exe /c ping 1.1.1.1 -n 1 -w 3000 > Nul & rmdir /s /q` . [73]

S0083 Misdat

Misdat is capable of deleting the backdoor file.[194]

S0149 MoonWind

MoonWind can delete itself or specified files.[195]

S0284 More_eggs

More_eggs can remove itself from a system.[64][196]

S1047 Mori

Mori can delete its DLL file and related files by Registry value.[197]

S0256 Mosquito

Mosquito deletes files using DeleteFileW API call.[198]

S1135 MultiLayer Wiper

MultiLayer Wiper uses a batch file, `remover.bat` to delete malware artifacts and the batch file itself during execution.[199]

S0233 MURKYTOP

MURKYTOP has the capability to delete local files.[79]

G0129 Mustang Panda

Mustang Panda will delete their tools and files, and kill processes after their objectives are reached.[200][201]

S0228 NanHaiShu

NanHaiShu launches a script to delete their original decoy file to cover tracks.[202]

S0630 Nebulae

Nebulae has the ability to delete files and directories.[203]

S1192 NICECURL

NICECURL has a function to remove artifacts.[204]

S1147 Nightdoor

Nightdoor can self-delete.[205]

S0385 njRAT

njRAT is capable of deleting files.[206][207]

S0353 NOKKI

NOKKI can delete files to cover tracks.[208]

S0346 OceanSalt

OceanSalt can delete files from the system.[209]

S1170 ODAgent

ODAgent can delete payloads and files used to pass C2 commands from remotely hosted cloud accounts.[210]

G0049 OilRig

OilRig has deleted files associated with their payload after execution.[211][212]

S0439 Okrum

Okrum's backdoor deletes files after they have been successfully uploaded to C2 servers.[213]

S0264 OopsIE

OopsIE has the capability to delete files and scripts from the victim's machine.[214]

C0022 Operation Dream Job

During Operation Dream Job, Lazarus Group removed all previously delivered files from a compromised computer.[215]

C0006 Operation Honeybee

During Operation Honeybee, the threat actors used batch files that reduced their fingerprint on a compromised system by deleting malware-related files.[216]

C0014 Operation Wocao

During Operation Wocao, the threat actors consistently removed traces of their activity by first overwriting a file using `/c cd /d c:\windows\temp\ & copy \\<IP ADDRESS>\c$\windows\system32\devmgr.dll \\<IP ADDRESS>\c$\windows\temp\LMAKSW.ps1 /y` and then deleting the overwritten file using `/c cd /d c:\windows\temp\ & del \\<IP ADDRESS>\c$\windows\temp\LMAKSW.ps1`.[217]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D has a command to delete a file from the system. OSX_OCEANLOTUS.D deletes the app bundle and dropper after execution.[218][219][220]

S1017 OutSteel

OutSteel can delete itself following the successful execution of a follow-on payload.[221]

S0598 P.A.S. Webshell

P.A.S. Webshell can delete scripts from a subdirectory of /tmp after they are run.[91]

S0208 Pasam

Pasam creates a backdoor through which remote attackers can delete files.[222]

G0040 Patchwork

Patchwork removed certain files and replaced them so they could not be retrieved.[223]

S0556 Pay2Key

Pay2Key can remove its log file from disk.[224]

S1050 PcShare

PcShare has deleted its files and components from a compromised host.[58]

S0587 Penquin

Penquin can delete downloaded executables after running them.[225]

S0517 Pillowmint

Pillowmint has deleted the filepath `%APPDATA%\Intel\devmonsrv.exe`.[226]

G1040 Play

Play has used tools including Wevtutil to remove malicious files from compromised hosts.[227]

S0435 PLEAD

PLEAD has the ability to delete files on the compromised host.[155]

S0013 PlugX

PlugX has the remove itself and other artifacts.[228][229]

S0067 pngdowner

pngdowner deletes content from C2 communications that was saved to the user's temporary directory.[230]

S0428 PoetRAT

PoetRAT has the ability to overwrite scripts and delete itself if a sandbox environment is detected.[231]

S0453 Pony

Pony has used scripts to delete itself after execution.[232]

S0139 PowerDuke

PowerDuke has a command to write random data across a file and delete it.[233]

S0441 PowerShower

PowerShower has the ability to remove all files created during the dropper process.[234]

S0223 POWERSTATS

POWERSTATS can delete all files on the C:\, D:\, E:\ and, F:\ drives using PowerShell Remove-Item commands.[235]

S0113 Prikormka

After encrypting its own log files, the log encryption module in Prikormka deletes the original, unencrypted files from the host.[236]

S0654 ProLock

ProLock can remove files containing its payload after they are executed.[237]

S0279 Proton

Proton removes all files in the /tmp directory.[102]

S0238 Proxysvc

Proxysvc can delete files indicated by the attacker and remove itself from disk using a batch file.[162]

S0147 Pteranodon

Pteranodon can delete files that may interfere with it executing. It also can delete temporary files and itself after the initial script executes.[238]

S0196 PUNCHBUGGY

PUNCHBUGGY can delete files written to disk.[99][239]

S1032 PyDCrypt

PyDCrypt will remove all created artifacts such as dropped executables.[240]

S0583 Pysa

Pysa has deleted batch files after execution. [241]

S0650 QakBot

QakBot can delete folders and files including overwriting its executable with legitimate programs.[242][243][244][237]

S1242 Qilin

Qilin can delete itself from infected hosts after execution.[245][246]

S0269 QUADAGENT

QUADAGENT has a command to delete its Registry key and scheduled task.[247]

S1148 Raccoon Stealer

Raccoon Stealer can remove files related to use and installation.[248]

S0629 RainyDay

RainyDay has the ability to uninstall itself by deleting its service and files.[203]

S1212 RansomHub

RansomHub has the ability to self-delete.[249]

S1130 Raspberry Robin

Raspberry Robin can delete its initial delivery script from disk during execution.[250]

S0662 RCSession

RCSession can remove files from a targeted system.[251]

S0495 RDAT

RDAT can issue SOAP requests to delete already processed C2 emails. RDAT can also delete itself from the infected system.[252]

S0416 RDFSNIFFER

RDFSNIFFER has the capability of deleting local files.[253]

S0172 Reaver

Reaver deletes the original dropped file from the victim.[254]

G1039 RedCurl

RedCurl has deleted files after execution.[255][256][257]

S0153 RedLeaves

RedLeaves can delete specified files.[258]

C0056 RedPenguin

During RedPenguin, UNC3886 used malware capaple of removing scripts after execution.[259]

S0125 Remsec

Remsec is capable of deleting files on the victim. It also securely removes itself after collecting and exfiltrating data.[260][261][262]

S0496 REvil

REvil can mark its binary code for deletion after reboot.[263]

S0448 Rising Sun

Rising Sun can delete files and artifacts it creates.[264]

S1150 ROADSWEEP

ROADSWEEP can use embedded scripts to remove itself from the infected host.[265][266]

G0106 Rocke

Rocke has deleted files on infected machines.[267]

S0240 ROKRAT

ROKRAT can request to delete files.[268]

S0148 RTM

RTM can delete all files created during its execution.[269][270]

S0253 RunningRAT

RunningRAT contains code to delete files from the victim’s machine.[113]

S0085 S-Type

S-Type has deleted files it has created on a compromised host.[194]

S1018 Saint Bot

Saint Bot can run a batch script named `del.bat` to remove any Saint Bot payload-linked files from a compromise system if anti-analysis or locale checks fail.[221]

S0074 Sakula

Some Sakula samples use cmd.exe to delete temporary files.[271]

S0370 SamSam

SamSam has been seen deleting its own files and payloads to make analysis of the attack more difficult.[272]

G0034 Sandworm Team

Sandworm Team has used backdoors that can delete files used in an attack from an infected system.[150][273][274]

S0461 SDBbot

SDBbot has the ability to delete files from a compromised host.[275]

S0195 SDelete

SDelete deletes data in a way that makes it unrecoverable.[1]

S0053 SeaDuke

SeaDuke can securely delete files, including deleting itself from the victim.[276]

S0345 Seasalt

Seasalt has a command to delete a specified file.[277]

S0382 ServHelper

ServHelper has a module to delete itself from the infected machine.[278][279]

S1019 Shark

Shark can delete files downloaded to the compromised host.[73]

S0444 ShimRat

ShimRat can uninstall itself from compromised hosts, as well create and modify directories, delete, move, copy, and rename files.[280]

S1178 ShrinkLocker

ShrinkLocker can delete itself depending on various checks performed during execution.[281]

S0589 Sibot

Sibot will delete itself if a certain server response is received.[282]

G0091 Silence

Silence has deleted artifacts, including scheduled tasks, communicates files from the C2 and other logs.[283][284]

S0692 SILENTTRINITY

SILENTTRINITY can remove files from the compromised host.[285]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has deleted itself and the 'index.dat' file on a compromised machine to remove recent Internet history from the system.[286]

S1166 Solar

Solar has the ability to delete staged files after they are uploaded to C2.[287]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 routinely removed their tools, including custom backdoors, once remote access was achieved.[288]

S0615 SombRAT

SombRAT has the ability to run `cancel` or `closeanddeletestorage` to remove all files from storage and delete the storage temp file on a compromised host.[289]

S0374 SpeakUp

SpeakUp deletes files to remove evidence on the machine. [290]

S0390 SQLRat

SQLRat has used been observed deleting scripts once used.[291]

S1200 StealBit

StealBit can self-delete its executable file from the compromised system.[292][165]

S0380 StoneDrill

StoneDrill has been observed deleting the temporary files once they fulfill their task.[293]

S1034 StrifeWater

StrifeWater can self delete to cover its tracks.[294]

S0491 StrongPity

StrongPity can delete previously exfiltrated files from the compromised host.[295][296]

S0603 Stuxnet

Stuxnet uses an RPC server that contains a routine for file deletion and also removes itself from the system through a DLL export by deleting specific files.[297]

S0559 SUNBURST

SUNBURST had a command to delete files.[288][298]

S0562 SUNSPOT

Following the successful injection of SUNBURST, SUNSPOT deleted a temporary file it created named `InventoryManager.bk` after restoring the original SolarWinds Orion source code to the software library.[299]

S0663 SysUpdate

SysUpdate can delete its configuration file from the targeted system.[300]

S0011 Taidoor

Taidoor can use `DeleteFileA` to remove files from infected hosts.[301]

S0586 TAINTEDSCRIBE

TAINTEDSCRIBE can delete files from a compromised host.[302]

S0164 TDTESS

TDTESS creates then deletes log files during installation of itself as a service.[303]

G0139 TeamTNT

TeamTNT has used a payload that removes itself after running. TeamTNT also has deleted locally staged files for collecting credentials or scan results for local IP addresses after exfiltrating them.[304][305]

G0089 The White Company

The White Company has the ability to delete its malware entirely from the target system.[306]

G0027 Threat Group-3390

Threat Group-3390 has deleted existing logs and exfiltrated file archives from a victim.[307][308]

S1239 TONESHELL

TONESHELL has deleted payload files received from the C2 server.[309]

S0094 Trojan.Karagany

Trojan.Karagany has used plugins with a self-delete capability.[310]

S1196 Troll Stealer

Troll Stealer creates and can execute a BAT script that will delete the malware.[311]

G0081 Tropic Trooper

Tropic Trooper has deleted dropper files on an infected system using command scripts.[312]

S0263 TYPEFRAME

TYPEFRAME can delete files off the system.[313]

G1048 UNC3886

UNC3886 has used the the esxcli command line to remove files created by malicious vSphere Installation Bundles from disk.[314][315]

S1164 UPSTYLE

UPSTYLE removes `bootstrap.min.css` after parsing command and control instructions, restoring the file to its original state.[316]

S0022 Uroburos

Uroburos can run a `Clear Agents Track` command on an infected machine to delete Uroburos-related logs.[317]

S0386 Ursnif

Ursnif has deleted data staged in tmp files after exfiltration.[318]

S0136 USBStealer

USBStealer has several commands to delete files associated with the malware from the victim.[319]

S0442 VBShower

VBShower has attempted to complicate forensic analysis by deleting all the files contained in `%APPDATA%..\Local\Temporary Internet Files\Content.Word` and `%APPDATA%..\Local Settings\Temporary Internet Files\Content.Word\`.[320]

S0257 VERMIN

VERMIN can delete files on the victim's machine.[321]

S1154 VersaMem

VersaMem deleted files related to initial installation such as temporary files related to the PID of the main web process.[322]

S0180 Volgmer

Volgmer can delete files and itself after infection to avoid analysis.[323]

G1017 Volt Typhoon

Volt Typhoon has run `rd /S` to delete their working directories and deleted systeminfo.dat from `C:\Users\Public\Documentsfiles`.[324][325]

S0689 WhisperGate

WhisperGate can delete tools from a compromised host after execution.[326]

S0155 WINDSHIELD

WINDSHIELD is capable of file deletion along with other file system interaction.[327]

S0466 WindTail

WindTail has the ability to receive and execute a self-delete command.[328]

S0176 Wingbird

Wingbird deletes its payload along with the payload's parent process after it finishes copying files.[329]

S0141 Winnti for Windows

Winnti for Windows can delete the DLLs for its various components from a compromised host.[330]

G0102 Wizard Spider

Wizard Spider has used file deletion to remove some modules and configurations from an infected host after use.[331]

S1065 Woody RAT

Woody RAT has the ability to delete itself from disk by creating a suspended notepad process and writing shellcode to delete a file into the suspended process using `NtWriteVirtualMemory`.[332]

S0161 XAgentOSX

XAgentOSX contains the deletFileFromPath function to delete a specified file using the NSFileManager:removeFileAtPath method.[333]

S1207 XLoader

XLoader can delete malicious executables from compromised machines.[334]

S0251 Zebrocy

Zebrocy has a command to delete files and directories.[335][336][337]

S1151 ZeroCleare

ZeroCleare has the ability to uninstall the RawDisk driver and delete the `rwdsk` file on disk.[265][338]

S0330 Zeus Panda

Zeus Panda has a command to delete a file. It also can uninstall scripts and delete files to cover its track.[339]

S0350 zwShell

zwShell has deleted itself after creating a service as well as deleted a temporary file when the system reboots.[340]

S0412 ZxShell

ZxShell can delete files from the system.[17][341]

---