Service Stop, Technique T1489 - Enterprise

Archived: 2026-04-05 12:51:16 UTC

S1194 Akira _v2

Akira _v2 can stop running virtual machines.[7][8][9]

S0640 Avaddon

Avaddon looks for and attempts to stop database processes.[10]

S1053 AvosLocker

AvosLocker has terminated specific processes before encryption.[11]

S0638 Babuk

Babuk can stop specific services related to backups.[12][13][14]

S1181 BlackByte 2.0 Ransomware

BlackByte 2.0 Ransomware can terminate running services.[15]

S1068 BlackCat

BlackCat has the ability to stop VM services on compromised networks.[16][17]

S1096 Cheerscrypt

Cheerscrypt has the ability to terminate VM processes on compromised hosts through execution of `esxcli vm process kill`.[18]

S0611 Clop

Clop can kill several processes and services related to backups and security solutions.[19][20]

S0575 Conti

Conti can stop up to 146 Windows services related to security, backup, database, and email solutions through the use of `net stop`.[21]

S0625 Cuba

Cuba has a hardcoded list of services and processes to terminate.[22]

S0659 Diavol

Diavol will terminate services using the Service Control Manager (SCM) API.[23]

S0605 EKANS

EKANS stops database, data backup solution, antivirus, and ICS-related processes.[24][25][26]

S1247 Embargo

Embargo has terminated active processes and services based on a hardcoded list using the `CloseServiceHandle()` function.[27] Embargo has also leveraged MS4Killer to terminate processes contained in an embedded list of security software process names that were XOR-encrypted.[28]

S1211 Hannotog

Hannotog can stop Windows services.[29]

S0697 HermeticWiper

HermeticWiper has the ability to stop the Volume Shadow Copy service.[30]

S0431 HotCroissant

HotCroissant has the ability to stop services on the infected host.[31]

S1139 INC Ransomware

INC Ransomware can issue a command to kill a process on compromised hosts.[32]

G0119 Indrik Spider

Indrik Spider has used PsExec to stop services prior to the execution of ransomware.[33]

S0604 Industroyer

Industroyer's data wiper module writes zeros into the registry keys in `SYSTEM\CurrentControlSet\Services` to render a system inoperable.[34]

S1245 InvisibleFerret

InvisibleFerret has terminated Chrome and Brave browsers using the `taskkill` command on Windows and the `killall` command on other systems such as Linux and macOS.[35] InvisibleFerret has also utilized it's `ssh_kill` command to terminate Chrome and Brave browser processes.[36]

S0607 KillDisk

KillDisk terminates various processes to get the user to reboot the victim machine.[37]

G1004 LAPSUS$

LAPSUS$ has shut down virtual machines from within a victim's on-premise VMware ESXi infrastructure.[38]

G0032 Lazarus Group

Lazarus Group has stopped the MSExchangeIS service to render Exchange contents inaccessible to users.[39]

S1199 LockBit 2.0

LockBit 2.0 can automatically terminate processes that may interfere with the encryption or file extraction processes.[40]

S1202 LockBit 3.0

LockBit 3.0 can terminate targeted processes and services related to security, backup, database management, and other applications that could stop or interfere with encryption.[41][42][43][44]

S0582 LookBack

LookBack can kill processes and delete services.[45]

S0449 Maze

Maze has stopped SQL services to ensure it can encrypt any database.[46]

G1051 Medusa Group

Medusa Group has terminated services related to backups, security, databases, communication, filesharing and websites.[47][48][49]

S1244 Medusa Ransomware

Medusa Ransomware has the capability to terminate services related to backups, security, databases, communication, filesharing and websites.[47][48][49] Medusa Ransomware has also utilized the `taskkill /F /IM <process> /T` command to stop targeted processes and `net stop <process>` command to stop designated services.[48][49]

S0576 MegaCortex

MegaCortex can stop and disable services on the system.[50]

S1191 Megazord

Megazord has the ability to terminate a list of services and processes.[9]

S0688 Meteor

Meteor can disconnect all network adapters on a compromised host using `powershell -Command "Get-WmiObject -class Win32_NetworkAdapter | ForEach { If ($.NetEnabled) { $.Disable() } }" > NUL`.[51]

S0457 Netwalker

Netwalker can terminate system processes and services, some of which relate to backup software.[52]

S0365 Olympic Destroyer

Olympic Destroyer uses the API call `ChangeServiceConfigW` to disable all services on the affected system.[1]

S0556 Pay2Key

Pay2Key can stop the MS SQL service at the end of the encryption process to release files locked by the service.[53]

S1058 Prestige

Prestige has attempted to stop the MSSQL Windows service to ensure successful encryption using `C:\Windows\System32\net.exe stop MSSQLSERVER`.[54]

S0583 Pysa

Pysa can stop services and processes.[55]

S1242 Qilin

Qilin can terminate specific services on compromised hosts.[56][57][58]

S0481 Ragnar Locker

Ragnar Locker has attempted to stop services associated with business applications and databases to release the lock on files used by these applications so they may be encrypted.[59]

S1212 RansomHub

RansomHub has the ability to terminate specified services.[60]

S0496 REvil

REvil has the capability to stop services and kill processes.[61][62]

S1150 ROADSWEEP

ROADSWEEP can disable critical services and processes.[63]

S0400 RobbinHood

RobbinHood stops 181 Windows services on the system before beginning the encryption process.[64]

S1073 Royal

Royal can use `RmShutDown` to kill applications and services using the resources that are targeted for encryption.[65]

S0446 Ryuk

Ryuk has called `kill.bat` for stopping services, disabling services and killing processes.[66]

G0034 Sandworm Team

Sandworm Team attempts to stop the MSSQL Windows service to ensure successful encryption of locked files.[54]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has the capability to stop processes and services.[67]

S1217 VIRTUALPITA

VIRTUALPITA can start and stop the `vmsyslogd` service.[68]

S0366 WannaCry

WannaCry attempts to kill processes associated with Exchange, Microsoft SQL Server, and MySQL to make it possible to encrypt their data stores.[69][3]

G0102 Wizard Spider

Wizard Spider has used taskkill.exe and net.exe to stop backup, catalog, cloud, and other services prior to network encryption.[70]
