Impair Defenses: Disable or Modify Tools, Sub-technique T1562.001 - Enterprise

Archived: 2026-04-05 13:45:49 UTC

C0028 2015 Ukraine Electric Power Attack

During the 2015 Ukraine Electric Power Attack, Sandworm Team modified in-registry internet settings to lower internet security. [15]

S0331 Agent Tesla

Agent Tesla has the capability to kill any running analysis processes and AV software.[16]

G1030 Agrius

Agrius used several mechanisms to try to disable security tools. Agrius attempted to modify EDR-related services to disable auto-start on system reboot. Agrius used a publicly available driver, `GMER64.sys` typically used for anti-rootkit functionality, to selectively stop and remove security software processes.[17]

G1024 Akira

Akira has disabled or modified security tools for defense evasion.[18]

G0082 APT38

APT38 has unhooked DLLs to disable endpoint detection and response (EDR) or anti-virus (AV) tools.[19]

G0143 Aquatic Panda

Aquatic Panda has attempted to stop endpoint detection and response (EDR) tools on compromised systems.[20]

C0046 ArcaneDoor

ArcaneDoor modified the Authentication, Authorization, and Accounting (AAA) function of targeted Cisco ASA appliances to allow the threat actor to bypass normal AAA operations.[21][22]

S0640 Avaddon

Avaddon looks for and attempts to stop anti-malware solutions.[23]

S0638 Babuk

Babuk can stop anti-virus services on a compromised host.[24]

S0534 Bazar

Bazar has manually loaded ntdll from disk in order to identity and remove API hooks set by security products.[25]

G1043 BlackByte

BlackByte disabled security tools such as Windows Defender and the Raccine anti-ransomware tool during operations.[26][27][28]

S1180 BlackByte Ransomware

BlackByte Ransomware adds .JS and .EXE extensions to the Microsoft Defender exclusion list. BlackByte Ransomware terminates and removes the Raccine anti-ransomware utility.[29]

S0252 Brave Prince

Brave Prince terminates antimalware processes.[30]

G0060 BRONZE BUTLER

BRONZE BUTLER has incorporated code into several tools that attempts to terminate anti-virus processes.[31]

S0482 Bundlore

Bundlore can change browser security settings to enable extensions to be installed. Bundlore uses the `pkill cfprefsd` command to prevent users from inspecting processes.[32][33]

S0484 Carberp

Carberp has attempted to disable security software by creating a suspended process for the security software and injecting code to delete antivirus core files when the process is resumed.[34]

S0144 ChChes

ChChes can alter the victim's proxy configuration.[35]

S0611 Clop

Clop can uninstall or disable security products.[36]

S0154 Cobalt Strike

Cobalt Strike has the ability to use Smart Applet attacks to disable the Java SecurityManager sandbox.[37][38]

S0608 Conficker

Conficker terminates various services related to system security and Windows.[39]

G1052 Contagious Interview

Contagious Interview has convinced victims to disable Docker and other container environments and run code on their machine natively in attempts to bypass container isolation and ensure device infection.[40]

C0029 Cutting Edge

During Cutting Edge, threat actors disabled logging and modified the `compcheckresult.cgi` component to edit the Ivanti Connect Secure built-in Integrity Checker exclusion list to evade detection.[41][42]

S0334 DarkComet

DarkComet can disable Security Center functions like anti-virus.[43][44]

S1111 DarkGate

DarkGate will terminate processes associated with several security software products if identified during execution.[45]

S0659 Diavol

Diavol can attempt to stop security software.[46]

S0695 Donut

Donut can patch Antimalware Scan Interface (AMSI), Windows Lockdown Policy (WLDP), as well as exit-related Native API functions to avoid process termination.[47]

S0377 Ebury

Ebury can disable SELinux Role-Based Access Control and deactivate PAM modules.[48]

S0554 Egregor

Egregor has disabled Windows Defender to evade protections.[49]

S0605 EKANS

EKANS stops processes related to security and management software.[50][51]

G1003 Ember Bear

Ember Bear uses the NirSoft AdvancedRun utility to disable Microsoft Defender Antivirus through stopping the WinDefend service on victim machines. Ember Bear disables Windows Defender via registry key changes.[52]

G0037 FIN6

FIN6 has deployed a utility script named `kill.bat` to disable anti-virus.[53]

G0047 Gamaredon Group

Gamaredon Group has delivered macros which can tamper with Microsoft Office security settings.[54][55]

S0249 Gold Dragon

Gold Dragon terminates anti-malware processes if they're found running on the system.[30]

S0477 Goopy

Goopy has the ability to disable Microsoft Outlook's security policies to disable macro warnings.[56]

G0078 Gorgon Group

Gorgon Group malware can attempt to disable security features in Microsoft Office and Windows Defender using the `taskkill` command.[57]

S0531 Grandoreiro

Grandoreiro can hook APIs, kill processes, break file system paths, and change ACLs to prevent security tools from running.[58]

S0132 H1N1

H1N1 kills and disables services for Windows Security Center, and Windows Defender.[59]

S0061 HDoor

HDoor kills anti-virus found on the victim.[60]

S0601 Hildegard

Hildegard has modified DNS resolvers to evade DNS monitoring tools.[61]

C0038 HomeLand Justice

During HomeLand Justice, threat actors modified and disabled components of endpoint detection and response (EDR) solutions including Microsoft Defender Antivirus.[62]

S0434 Imminent Monitor

Imminent Monitor has a feature to disable Windows Task Manager.[63]

G1032 INC Ransom

INC Ransom can use SystemSettingsAdminFlows.exe, a native Windows utility, to disable Windows Defender.[64]

G0119 Indrik Spider

Indrik Spider used PsExec to leverage Windows Defender to disable scanning of all downloaded files and to restrict real-time monitoring.[65] Indrik Spider has used `MpCmdRun` to revert the definitions in Microsoft Defender.

[66] Additionally, Indrik Spider has used WMI to stop or uninstall and reset anti-virus products and other defensive services.[66]

S0201 JPIN

JPIN can lower security settings by changing Registry keys.[67]

G0094 Kimsuky

Kimsuky has been observed turning off Windows Security Center and can hide the AV software window from the view of the infected user.[68][69]

S0669 KOCTOPUS

KOCTOPUS will attempt to delete or disable all Registry keys and scheduled tasks related to Microsoft Security Defender and Security Essentials.[70]

C0035 KV Botnet Activity

KV Botnet Activity used various scripts to remove or disable security tools, such as `http_watchdog` and `firewallsd`, as well as tools related to other botnet infections, such as `mips_ff`, on victim devices.[71]

G0032 Lazarus Group

Lazarus Group malware TangoDelta attempts to terminate various processes associated with McAfee. Additionally, Lazarus Group malware SHARPKNOT disables the Microsoft Windows System Event Notification and Alerter services.[72][73][74][75].

S1199 LockBit 2.0

LockBit 2.0 can disable firewall rules and anti-malware and monitoring software including Windows Defender.[76][77]

S1202 LockBit 3.0

LockBit 3.0 can disable security tools to evade detection including Windows Defender.[78][79][80]

S0372 LockerGoga

LockerGoga installation has been immediately preceded by a "task kill" command in order to disable anti-virus.[81]

S1213 Lumma Stealer

Lumma Stealer has attempted to bypass Windows Antimalware Scan Interface (AMSI) by removing the string "AmsiScanBuffer" from the "clr.dll" module in memory to prevent it from being called.[82]

S1048 macOS.OSAMiner

macOS.OSAMiner has searched for the Activity Monitor process in the System Events process list and kills the process if running. macOS.OSAMiner also searches the operating system's `install.log` for apps matching its hardcoded list, killing all matching process names.[83]

G0059 Magic Hound

Magic Hound has disabled antivirus services on targeted systems in order to upload malicious payloads.[84]

S1169 Mango

Mango contains an unused capability to block endpoint security solutions from loading user-mode code hooks via a DLL in a specified process by using the `UpdateProcThreadAttribute API` to set the `PROC_THREAD_ATTRIBUTE_MITIGATION_POLICY` to `PROCESS_CREATION_MITIGATION_POLICY_BLOCK_NON_MICROSOFT_BINARIES_ALWAYS_ON` for an identified process. [85]

S0449 Maze

Maze has disabled dynamic analysis and other security tools including IDA debugger, x32dbg, and OllyDbg.[86] It has also disabled Windows Defender's Real-Time Monitoring feature and attempted to disable endpoint protection services.[87]

G1051 Medusa Group

Medusa Group has terminated antivirus services utilizing the gaze.exe executable and utilizing `psexec.exe`.[88] [89][90] Medusa Group has also leveraged I/O control codes (IOCTLs) for terminating and deleting processes of identified security tools.[88]

S1244 Medusa Ransomware

Medusa Ransomware has terminated antivirus services utilizing the gaze.exe executable.[88] Medusa Ransomware has also terminated antivirus services utilizing PowerShell scripts.[88][91]

S0576 MegaCortex

MegaCortex was used to kill endpoint security processes.[92]

S0455 Metamorfo

Metamorfo has a function to kill processes associated with defenses and can prevent certain processes from launching.[93][94]

S0688 Meteor

Meteor can attempt to uninstall Kaspersky Antivirus or remove the Kaspersky license; it can also add all files and folders related to the attack to the Windows Defender exclusion list.[95]

G0069 MuddyWater

MuddyWater can disable the system's local proxy settings.[96]

S1135 MultiLayer Wiper

MultiLayer Wiper removes the Volume Shadow Copy (VSS) service from infected devices along with all present shadow copies.[17]

S0228 NanHaiShu

NanHaiShu can change Internet Explorer settings to reduce warnings about malware activity.[97]

S0336 NanoCore

NanoCore can modify the victim's anti-virus.[98][99]

S0457 Netwalker

Netwalker can detect and terminate active security software-related processes on infected systems.[100][101]

C0002 Night Dragon

During Night Dragon, threat actors disabled anti-virus and anti-spyware tools in some instances on the victim’s machines. The actors also disabled proxy settings to allow direct communication from victims to the Internet.[102]

G1040 Play

Play has used tools including GMER, IOBit, and PowerTool to disable antivirus software.[103][104]

S0223 POWERSTATS

POWERSTATS can disable Microsoft Office Protected View by changing Registry keys.[105]

S0279 Proton

Proton kills security tools like Wireshark that are running.[106]

G0024 Putter Panda

Malware used by Putter Panda attempts to terminate processes corresponding to two components of Sophos Anti-Virus (SAVAdminService.exe and SavService.exe).[107]

S0583 Pysa

Pysa has the capability to stop antivirus services and disable Windows Defender.[108]

S0650 QakBot

QakBot has the ability to modify the Registry to add its binaries to the Windows Defender exclusion list.[109]

S1242 Qilin

Qilin can terminate antivirus-related processes and services.[110][111][112][113]

C0055 Quad7 Activity

Quad7 Activity has disabled the TP-Link management interface for TP-Link by killing the `/usr/bin/httpd` process.[114][115][116]

S0481 Ragnar Locker

Ragnar Locker has attempted to terminate/stop processes and services associated with endpoint security products.[117]

S1130 Raspberry Robin

Raspberry Robin can add an exception to Microsoft Defender that excludes the entire main drive from anti-malware scanning to evade detection.[118]

S1240 RedLine Stealer

RedLine Stealer can disable security software and update services.[119]

S0496 REvil

REvil can connect to and disable the Symantec server on the victim's network.[120]

S0400 RobbinHood

RobbinHood will search for Windows services that are associated with antivirus software on the system and kill the process.[121]

G0106 Rocke

Rocke used scripts which detected and uninstalled antivirus software.[122][123]

S0253 RunningRAT

RunningRAT kills antimalware running process.[30]

S0446 Ryuk

Ryuk has stopped services related to anti-virus.[124]

G1031 Saint Bear

Saint Bear will modify registry entries and scheduled task objects associated with Windows Defender to disable its functionality.[125]

G1015 Scattered Spider

Scattered Spider has uninstalled and disabled security tools.[126]

C0058 SharePoint ToolShell Exploitation

During SharePoint ToolShell Exploitation, threat actors disabled Microsoft Defender through Registry settings and real-time monitoring via PowerShell.[127][128]

S1178 ShrinkLocker

ShrinkLocker disables protectors used to secure the BitLocker encryption key on victim systems.[129][130]

S0692 SILENTTRINITY

SILENTTRINITY's `amsiPatch.py` module can disable Antimalware Scan Interface (AMSI) functions.[131]

S0468 Skidmap

Skidmap has the ability to set SELinux to permissive mode.[132]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 used the service control manager on a remote system to disable services associated with security monitoring products.[133]

S1234 SplatCloak

SplatCloak has identified and disabled API callback features of Windows Defender and Kaspersky.[134]

S0058 SslMM

SslMM identifies and kills anti-malware processes.[60]

S0491 StrongPity

StrongPity can add directories used by the malware to the Windows Defender exclusions list to prevent detection.[135]

S0559 SUNBURST

SUNBURST attempted to disable software security services following checks against a FNV-1a + XOR hashed hardcoded blocklist.[136]

G1018 TA2541

TA2541 has attempted to disable built-in security protections such as Windows AMSI. [137]

G0092 TA505

TA505 has used malware to disable Windows Defender.[138]

G0139 TeamTNT

TeamTNT has disabled and uninstalled security tools such as Alibaba, Tencent, and BMC cloud monitoring agents on cloud-based infrastructure.[139][140]

S0595 ThiefQuest

ThiefQuest uses the function `kill_unwanted` to obtain a list of running processes and kills each process matching a list of security related processes.[141]

S0004 TinyZBot

TinyZBot can disable Avira anti-virus.[142]

S0266 TrickBot

TrickBot can disable Windows Defender.[143]

G0010 Turla

Turla has used a AMSI bypass, which patches the in-memory amsi.dll, in PowerShell scripts to bypass Windows antimalware products.[144]

G1048 UNC3886

UNC3886 has disabled OpenSSL digital signature verification of system files through corruption of boot files.[145]

S0130 Unknown Logger

Unknown Logger has functionality to disable security tools, including Kaspersky, BitDefender, and MalwareBytes.[146]

G1047 Velvet Ant

Velvet Ant attempted to disable local security tools and endpoint detection and response (EDR) software during operations.[147]

S0670 WarzoneRAT

WarzoneRAT can disarm Windows Defender during the UAC process to evade detection.[148]

S0689 WhisperGate

WhisperGate can download and execute AdvancedRun.exe to disable the Windows Defender Theat Protection service and set an exclusion path for the C:\ drive.[149][150][151]

G0102 Wizard Spider

Wizard Spider has shut down or uninstalled security applications on victim systems that might prevent ransomware from executing.[152][153][154][155]

S1207 XLoader

XLoader loads a copy of NTDLL to evade hooks from security monitoring tools on this library.[156] XLoader can add the path of its executable to the Microsoft Defender exclusion list.[157]

S1114 ZIPLINE

ZIPLINE can add itself to the exclusion list for the Ivanti Connect Secure Integrity Checker Tool if the `--exclude` parameter is passed by the `tar` process.[158]

S0412 ZxShell

ZxShell can kill AV products' processes.[159]
