Execution Guardrails, Technique T1480 - Enterprise

Archived: 2026-04-05 15:41:51 UTC

S1194 Akira _v2

Akira _v2 will fail to execute if the targeted `/vmfs/volumes/` path does not exist or is not defined.[4]

S0504 Anchor

Anchor can terminate itself if specific execution flags are not present.[5]

S1133 Apostle

Apostle's ransomware variant requires that a base64-encoded argument is passed when executed, that is used as the Public Key for subsequent encryption operations. If Apostle is executed without this argument, it automatically runs a self-delete function.[6]

S0570 BitPaymer

BitPaymer compares file names and paths to a list of excluded names and directory names during encryption.[7]

G1043 BlackByte

BlackByte stopped execution if identified language settings on victim machines was Russian or one of several language associated with former Soviet republics.[8] BlackByte has used ransomware variants requiring a key passed on the command line for the malware to execute.[9]

S1180 BlackByte Ransomware

BlackByte Ransomware creates a mutex value with a hard-coded name, and terminates if that mutex already exists on the victim system. BlackByte Ransomware checks the system language to see if it matches one of a list of hard-coded values; if a match is found, the malware will terminate.[10]

S1184 BOLDMOVE

BOLDMOVE verifies it is executing from a specific path during execution.[11]

S0635 BoomBox

BoomBox can check its current working directory and for the presence of a specific file and terminate if specific values are not found.[12]

S1161 BPFDoor

BPFDoor creates a zero byte PID file at `/var/run/haldrund.pid`. BPFDoor uses this file to determine if it is already running on a system to ensure only one instance is executing at a time.[13]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP can execute a task which leads to execution if it finds a process name containing "creensaver."[14]

G1052 Contagious Interview

Contagious Interview has configured C2 endpoints to review IP geolocation, request headers, victim environment details and runtime conditions prior to delivering payloads.[15]

S1111 DarkGate

DarkGate uses per-victim links for hosting malicious archives, such as ZIP files, in services such as SharePoint to prevent other entities from retrieving them.[16]

S1052 DEADEYE

DEADEYE can ensure it executes only on intended systems by identifying the victim's volume serial number, hostname, and/or DNS domain.[17]

S0634 EnvyScout

EnvyScout can call `window.location.pathname` to ensure that embedded files are being executed from the C: drive, and will terminate if they are not.[12]

S1179 Exbyte

Exbyte checks for the presence of a configuration file before completing execution.[18]

G0047 Gamaredon Group

Gamaredon Group has used geoblocking to limit downloads of the malicious file to specific geographic locations.[19][20]

S1185 LightSpy

On macOS, LightSpy checks the existence of a process identification number (PID) file, `/Users/Shared/irc.pid`, to verify if LightSpy is currently running.[21]

S1199 LockBit 2.0

LockBit 2.0 will not execute on hosts where the system language is set to a language spoken in the Commonwealth of Independent States region.[22][23]

S1202 LockBit 3.0

LockBit 3.0 can make execution dependent on specific parameters including a unique passphrase and the system language of the targeted host not being found on a set exclusion list. [24][25][26]

S1143 LunarLoader

LunarLoader can use the DNS domain name of a compromised host to create a decryption key to ensure a malicious payload can only execute against the intended targets.[27]

S0637 NativeZone

NativeZone can check for the presence of KM.EkeyAlmaz1C.dll and will halt execution unless it is in the same directory as the rest of the malware's components.[12][28]

S1242 Qilin

Qilin can require a specific password to be passed by command-line argument during execution which must match a pre-defined value in the configuration in order for it to continue execution.[29]

S1212 RansomHub

RansomHub will terminate without proceeding to encryption if the infected machine is on a list of allowlisted machines specified in its configuration.[30]

S1130 Raspberry Robin

Raspberry Robin will check for the presence of several security products on victim machines and will avoid UAC bypass mechanisms if they are identified.[31] Raspberry Robin can use specific cookie values in HTTP requests to command and control infrastructure to validate that requests for second stage payloads originate from the initial downloader script.[32]

C0047 RedDelta Modified PlugX Infection Chain Operations

Mustang Panda included the use of Cloudflare geofencing mechanisms to limit payload download activity during RedDelta Modified PlugX Infection Chain Operations.[33]

S1240 RedLine Stealer

RedLine Stealer has built in settings to not operate based on geolocation or country of the victim host.[34][35]

S1150 ROADSWEEP

ROADSWEEP requires four command line arguments to execute correctly, otherwise it will produce a message box and halt execution.[14][36][37]

S1210 Sagerunex

Sagerunex uses a "servicemain" function to verify its environment to ensure it can only be executed as a service, as well as the existence of a configuration file in a specified directory.[38]

S1178 ShrinkLocker

ShrinkLocker will exit its "main" function if the victim domain name does not match provided criteria.[39]

S1035 Small Sieve

Small Sieve can only execute correctly if the word `Platypus` is passed to it on the command line.[40]

S1200 StealBit

StealBit will execute an empty infinite loop if it detects it is being run in the context of a debugger.[41]

S1183 StrelaStealer

StrelaStealer variants only execute if the keyboard layout or language matches a set list of variables.[42][43]

S0603 Stuxnet

Stuxnet checks for specific operating systems on 32-bit machines, Registry keys, and dates for vulnerabilities, and will exit execution if the values are not met.[44]

S0562 SUNSPOT

SUNSPOT only replaces SolarWinds Orion source code if the MD5 checksums of both the original source code file and backdoored replacement source code match hardcoded values.[45]

S1239 TONESHELL

TONESHELL has an exception handler that executes when ESET antivirus applications `ekrn.exe` and `egui.exe` are not found and directly injects its code into waitfor.exe using Native Windows API including `WriteProcessMemory` and `CreateRemoteThreadEx`.[46]

S0678 Torisma

Torisma is only delivered to a compromised host if the victim's IP address is on an allow-list.[47]

S0636 VaporRage

VaporRage has the ability to check for the presence of a specific DLL and terminate if it is not found.[12]
