Application Window Discovery, Technique T1010 - Enterprise

Archived: 2026-04-02 12:49:04 UTC

S0456 Aria-body

Aria-body has the ability to identify the titles of running windows on a compromised host.[3]

S0438 Attor

Attor can obtain application window titles and then determines which windows to perform Screen Capture on.[4]

S0454 Cadelspy

Cadelspy has the ability to identify open windows on the compromised host.[5]

S0261 Catchamas

Catchamas obtains application windows titles and then determines which windows to perform Screen Capture on.[6]

S1111 DarkGate

DarkGate will search for cryptocurrency wallets by examining application window names for specific strings.[7] DarkGate extracts information collected via NirSoft tools from the hosting process's memory by first identifying the window through the `FindWindow` API function.[7]

S0673 DarkWatchman

DarkWatchman reports window names along with keylogger information to provide application context.[1]

S0038 Duqu

The discovery modules used with Duqu can collect information on open windows.[8]

S1159 DUSTTRAP

DUSTTRAP can enumerate running application windows.[9]

S0696 Flagpro

Flagpro can check the name of the window displayed on the system.[10]

S1044 FunnyDream

FunnyDream has the ability to discover application windows via execution of `EnumWindows`.[11]

S0531 Grandoreiro

Grandoreiro can identify installed security tools based on window names.[2]

G1001 HEXANE

HEXANE has used a PowerShell-based keylogging tool to capture the window title.[12]

S0431 HotCroissant

HotCroissant has the ability to list the names of all open windows on the infected host.[13]

S0260 InvisiMole

InvisiMole can enumerate windows and child windows on a compromised host.[14][15]

S0265 Kazuar

Kazuar gathers information about opened windows.[16]

G0032 Lazarus Group

Lazarus Group malware IndiaIndia obtains and sends to its C2 server the title of the window for each running process. The KilaAlfa keylogger also reports the title of the window in the foreground.[17][18][19]

S0409 Machete

Machete saves the window names.[20]

S0455 Metamorfo

Metamorfo can enumerate all windows on the victim's machine.[21][22]

S0033 NetTraveler

NetTraveler reports window names along with keylogger information to provide application context.[23]

S0198 NETWIRE

NETWIRE can discover and close windows on controlled systems.[24]

S1090 NightClub

NightClub can use `GetForegroundWindow` to enumerate the active window.[25]

S0385 njRAT

njRAT gathers information about opened windows during the initial infection.[26]

S1233 PAKLOG

PAKLOG has used `GetForegroundWindow` to access the foreground window. [27] PAKLOG has also captured text from the foreground windows.[27]

S0435 PLEAD

PLEAD has the ability to list open windows on the compromised host.[28][28]

S0012 PoisonIvy

PoisonIvy captures window titles.[29]

S0139 PowerDuke

PowerDuke has a command to get text of the current foreground window.[30]

S0650 QakBot

QakBot has the ability to enumerate windows on a compromised host.[31]

S0375 Remexi

Remexi has a command to capture active windows on the machine and retrieve window titles.[32]

S0240 ROKRAT

ROKRAT can use the `GetForegroundWindow` and `GetWindowText` APIs to discover where the user is typing.[33]

S0692 SILENTTRINITY

SILENTTRINITY can enumerate the active Window during keylogging through execution of `GetActiveWindowTitle`.[34]

S0157 SOUNDBITE

SOUNDBITE is capable of enumerating application windows.[35]

S1239 TONESHELL

TONESHELL has used `GetForegroundWindow` to detect virtualization or sandboxes by calling the API twice and comparing each window handle.[36]

S0094 Trojan.Karagany

Trojan.Karagany can monitor the titles of open windows to identify specific keywords.[37]

G1017 Volt Typhoon

Volt Typhoon has collected window title information from compromised systems.[38]

S0219 WINERACK

WINERACK can enumerate active windows.[39]
