Query Registry, Technique T1012 - Enterprise

Archived: 2026-04-05 14:48:12 UTC

S0045 ADVSTORESHELL

ADVSTORESHELL can enumerate registry keys.[2][3]

G0050 APT32

APT32's backdoor can query the Windows Registry to gather system information. [4]

G0087 APT39

APT39 has used various strains of malware to query the Registry.[5]

G0096 APT41

APT41 queried registry values to determine items such as configured RDP ports and network configurations.[6]

S0438 Attor

Attor has opened the registry and performed query searches.[7]

S0344 Azorult

Azorult can check for installed software on the system under the Registry key `Software\Microsoft\Windows\CurrentVersion\Uninstall`.[8]

S0414 BabyShark

BabyShark has executed the `reg query` command for `HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default`.[9]

S0031 BACKSPACE

BACKSPACE is capable of enumerating and making modifications to an infected system's Registry.[10]

S0239 Bankshot

Bankshot searches for certain Registry keys to be configured before executing the payload.[11]

S0534 Bazar

Bazar can query `Windows\CurrentVersion\Uninstall` for installed applications.[12][13]

S0574 BendyBear

BendyBear can query the host's Registry key at `HKEY_CURRENT_USER\Console\QuickEdit` to retrieve data.[14]

S0268 Bisonal

Bisonal has used the RegQueryValueExA function to retrieve proxy information in the Registry.[15]

S0570 BitPaymer

BitPaymer can use the RegEnumKeyW to iterate through Registry keys.[16]

G1043 BlackByte

BlackByte queried registry values to determine system language settings.[17]

S1180 BlackByte Ransomware

BlackByte Ransomware enumerates the Registry, specifically the `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options` key.[18]

S0252 Brave Prince

Brave Prince gathers information about the Registry.[19]

S1039 Bumblebee

Bumblebee can check the Registry for specific keys.[20]

S0030 Carbanak

Carbanak checks the Registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings` for proxy configurations information.[21]

S0484 Carberp

Carberp has searched the Image File Execution Options registry key for "Debugger" within every subkey.[22]

S0335 Carbon

Carbon enumerates values in the Registry.[23]

S0348 Cardinal RAT

Cardinal RAT contains watchdog functionality that periodically ensures `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load` is set to point to its executable.[24]

S0674 CharmPower

CharmPower has the ability to enumerate `Uninstall` registry values.[25]

G0114 Chimera

Chimera has queried Registry keys using `reg query \\HKU\\SOFTWARE\Microsoft\Terminal Server Client\Servers` and `reg query \\HKU\\Software\Microsoft\Windows\CurrentVersion\Internet Settings`.[26]

S0023 CHOPSTICK

CHOPSTICK provides access to the Windows Registry, which can be used to gather information.[27]

S0660 Clambling

Clambling has the ability to enumerate Registry keys, including `KEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt\strDataDir` to search for a bitcoin wallet.[28][29]

S0154 Cobalt Strike

Cobalt Strike can query `HKEY_CURRENT_USER\Software\Microsoft\Office\\Excel\Security\AccessVBOM\` to determine if the security setting for restricting default programmatic access is enabled.[30][31]

S0126 ComRAT

ComRAT can check the default browser by querying `HKCR\http\shell\open\command`.[32]

S0115 Crimson

Crimson can check the Registry for the presence of `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\last_edate` to determine how long it has been installed on a host.[33]

G1034 Daggerfly

Daggerfly used Reg to dump the Security Account Manager (SAM), System, and Security Windows registry hives from victim machines.[34]

S0673 DarkWatchman

DarkWatchman can query the Registry to determine if it has already been installed on the system.[35]

S0354 Denis

Denis queries the Registry for keys and values.[36]

S0021 Derusbi

Derusbi is capable of enumerating Registry keys and values.[37]

S0186 DownPaper

DownPaper searches and reads the value of the Windows Update Registry Run key.[38]

G0035 Dragonfly

Dragonfly has queried the Registry to identify victim information.[39]

S0567 Dtrack

Dtrack can collect the RegisteredOwner, RegisteredOrganization, and InstallDate registry values.[40]

S1159 DUSTTRAP

DUSTTRAP can enumerate Registry items.[41]

S0091 Epic

Epic uses the `rem reg query` command to obtain values from Registry keys.[42]

S0512 FatDuke

FatDuke can get user agent strings for the default browser from `HKCU\Software\Classes\http\shell\open\command`.[43]

S0267 FELIXROOT

FELIXROOT queries the Registry for specific keys for potential privilege escalation and proxy information. FELIXROOT has also used WMI to query the Windows Registry.[44][45]

S0182 FinFisher

FinFisher queries Registry values as part of its anti-sandbox checks.[46][47]

G0117 Fox Kitten

Fox Kitten has accessed Registry hives ntuser.dat and UserClass.dat.[48]

S1044 FunnyDream

FunnyDream can check `Software\Microsoft\Windows\CurrentVersion\Internet Settings` to extract the `ProxyServer` string.[49]

G0047 Gamaredon Group

Gamaredon Group has queried `HKEY_CURRENT_USER\\Console\\WindowsUpdates` to obtain the C2 addresses.[50]
Gamaredon Group has queried `HKEY_CURRENT_USER\\Console\\WindowsUpdates` to obtain the C2 addresses.[50]

S0666 Gelsemium

Gelsemium can open random files and Registry keys to obscure malware behavior from sandbox analysis.[51]

S0032 gh0st RAT

gh0st RAT has checked for the existence of a Service key to determine if it has already been installed on the system.[52]

S0249 Gold Dragon

Gold Dragon enumerates registry keys with the command `regkeyenum` and obtains information for the Registry key `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`.[19]

S0376 HOPLIGHT

A variant of HOPLIGHT hooks lsass.exe, and lsass.exe then checks the Registry for the data value 'rdpproto' under the key `SYSTEM\CurrentControlSet\Control\Lsa Name`.[53]

S0203 Hydraq

Hydraq creates a backdoor through which remote attackers can retrieve system information, such as CPU speed, from Registry keys.[54][55]

G0119 Indrik Spider

Indrik Spider has used a service account to extract copies of the `Security` Registry hive.[56]

S0604 Industroyer

Industroyer has a data wiper component that enumerates keys in the Registry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`.[57]

S0260 InvisiMole

InvisiMole can enumerate Registry values, keys, and data.[58]

S0201 JPIN

JPIN can enumerate Registry keys.[59]

S1190 Kapeka

Kapeka queries registry values for stored configuration information.[60]

G0094 Kimsuky

Kimsuky has obtained specific Registry keys and values on a compromised host.[61]

G0032 Lazarus Group

Lazarus Group malware IndiaIndia checks Registry keys within HKCU and HKLM to determine if certain applications are present, including SecureCRT, Terminal Services, RealVNC, TightVNC, UltraVNC, Radmin, mRemote, TeamViewer, FileZilla, pcAnyware, and Remote Desktop. Another Lazarus Group malware sample

checks for the presence of the following Registry key: `HKEY_CURRENT_USER\Software\Bitcoin\Bitcoin-Qt`.[62][63][64]

S0513 LiteDuke

LiteDuke can query the Registry to check for the presence of `HKCU\Software\KasperskyLab`.[43]

S0680 LitePower

LitePower can query the Registry for keys added to execute COM hijacking.[65]

G0030 Lotus Blossom

Lotus Blossom has run commands such as `reg query HKLM\SYSTEM\CurrentControlSet\Services\[service name]\Parameters` to verify if installed implants are running as a service.[66]

S0532 Lucifer

Lucifer can check for existing stratum cryptomining information in `HKLM\Software\Microsoft\Windows\CurrentVersion\spreadCpuXmr - %stratum info%`.[67]

S1060 Mafalda

Mafalda can enumerate Registry keys with all subkeys and values.[68]

S1015 Milan

Milan can query `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography MachineGuid` to retrieve the machine GUID.[69]

S1047 Mori

Mori can read data from the Registry including from `HKLM\Software\NFC\IPA` and `HKLM\Software\NFC\`.[70]

S0385 njRAT

njRAT can read specific registry values.[71]

G0049 OilRig

OilRig has used `reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default"` on a victim to query the Registry.[72]

C0014 Operation Wocao

During Operation Wocao, the threat actors executed `/c cd /d c:\windows\temp\ & reg query HKEY_CURRENT_USER\Software\<username>\PuTTY\Sessions\` to detect recent PuTTY sessions, likely to further

lateral movement.[73]

S0165 OSInfo

OSInfo queries the registry to look for information about Terminal Services.[74]

S1050 PcShare

PcShare can search the registry files of a compromised host.[49]

S0517 Pillowmint

Pillowmint has used shellcode which reads code stored in the registry keys `\REGISTRY\SOFTWARE\Microsoft\DRM` using the native Windows API as well as read `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces` as part of its C2.[75]

S0013 PlugX

PlugX can enumerate and query for information contained within the Windows Registry.[76][77][78]

S0145 POWERSOURCE

POWERSOURCE queries Registry keys in preparation for setting Run keys to achieve persistence.[79]

S0194 PowerSploit

PowerSploit contains a collection of Privesc-PowerUp modules that can query Registry keys for potential opportunities.[80][81]

S0184 POWRUNER

POWRUNER may query the Registry by running `reg query` on a victim.[82]

S0238 Proxysvc

Proxysvc gathers product names from the Registry key: `HKLM\Software\Microsoft\Windows NT\CurrentVersion ProductName` and the processor description from the Registry key `HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0 ProcessorNameString`.[83]

S1228 PUBLOAD

PUBLOAD has queried Registry values to identify software using `reg query`.[84]

S1242 Qilin

Qilin can check `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control SystemStartOptions` to determine if a machine is running in safe mode.[85]

S0269 QUADAGENT

QUADAGENT checks if a value exists within a Registry key in the HKCU hive whose name is the same as the scheduled task it has created.[86]

S1076 QUIETCANARY

QUIETCANARY has the ability to retrieve information from the Registry.[87]

S1148 Raccoon Stealer

Raccoon Stealer queries the Windows Registry to fingerprint the infected host via the `HKLM:\SOFTWARE\Microsoft\Cryptography\MachineGuid` key.[88][89]

S0241 RATANKBA

RATANKBA uses the command `reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\InternetSettings"` .[90]

S0172 Reaver

Reaver queries the Registry to determine the correct Startup path to use for persistence.[91]

S1240 RedLine Stealer

RedLine Stealer can query the Windows Registry.[92]

S0075 Reg

Reg may be used to gather details from the Windows Registry of a local or remote system at the command-line interface.[93]

S0496 REvil

REvil can query the Registry to get random file extensions to append to encrypted files.[94]

S0448 Rising Sun

Rising Sun has identified the OS product name from a compromised host by searching the registry for `SOFTWARE\MICROSOFT\Windows NT\ CurrentVersion | ProductName` .[95]

S0240 ROKRAT

ROKRAT can access the `HKLM\System\CurrentControlSet\Services\mssmbios\Data\SMBiosData` Registry key to obtain the System manufacturer value to identify the machine type.[96]

S1018 Saint Bot

Saint Bot has used `check_registry_keys` as part of its environmental checks.[97]

S1099 Samurai

Samurai can query `SOFTWARE\Microsoft\.NETFramework\policy\v2.0` for discovery.[98]

S0140 Shamoon

Shamoon queries several Registry keys to identify hard disk partitions to overwrite.[99]

S1019 Shark

Shark can query `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography MachineGuid` to retrieve the machine GUID.[69]

S0589 Sibot

Sibot has queried the registry for proxy server information.[100]

S0692 SILENTTRINITY

SILENTTRINITY can use the `GetRegValue` function to check Registry keys within `HKCU\Software\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated` and `HKLM\Software\Policies\Microsoft\Windows\Installer\AlwaysInstallElevated`. It also contains additional modules that can check software AutoRun values and use the Win32 namespace to get values from HKCU, HKLM, HKCR, and HKCC hives.[101]

S0627 SodaMaster

SodaMaster has the ability to query the Registry to detect a key specific to VMware.[102]

G0038 Stealth Falcon

Stealth Falcon malware attempts to determine the installed version of .NET by querying the Registry.[103]

S0380 StoneDrill

StoneDrill has looked in the registry to find the default browser path.[104]

S0603 Stuxnet

Stuxnet searches the Registry for indicators of security programs.[105]

S0559 SUNBURST

SUNBURST collected the registry value `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid` from compromised hosts.[106]

S1064 SVCReady

SVCReady can search for the `HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System` Registry key to gather system information.[107]

S0242 SynAck

SynAck enumerates Registry keys associated with event logs.[108]

S0011 Taidoor

Taidoor can query the Registry on compromised hosts using `RegQueryValueExA`.[109]

S0560 TEARDROP

TEARDROP checked that `HKU\SOFTWARE\Microsoft\CTF` existed before decoding its embedded payload.[106][110]

G0027 Threat Group-3390

A Threat Group-3390 tool can read and decrypt stored Registry values.[111]

S0668 TinyTurla

TinyTurla can query the Registry for its configuration information.[112]

S1201 TRANSLATEXT

TRANSLATEXT has queried the following registry key to check for installed Chrome extensions: `HKCU\Software\Policies\Google\Chrome\ExtensionInstallForcelist`.[113]

G0010 Turla

Turla surveys a system upon check-in to discover information in the Windows Registry with the `reg query` command.[42] Turla has also retrieved PowerShell payloads hidden in Registry keys as well as checking keys associated with null session named pipes .[114]

S0022 Uroburos

Uroburos can query the Registry, typically `HKLM:\SOFTWARE\Classes\.wav\OpenWithProgIds`, to find the key and path to decrypt and load its kernel driver and kernel driver loader.[115]

S0386 Ursnif

Ursnif has used Reg to query the Registry for installed programs.[116][117]

S0476 Valak

Valak can use the Registry for code updates and to collect credentials.[118]

S0180 Volgmer

Volgmer checks the system for certain Registry keys.[119]

G1017 Volt Typhoon

Volt Typhoon has queried the Registry on compromised systems, `reg query hklm\software\` , for information on installed software including PuTTY.[120][121]

S0612 WastedLocker

WastedLocker checks for specific registry keys related to the `UCOMIEnumConnections` and `IActiveScriptParseProcedure32` interfaces.[122]

S0579 Waterbear

Waterbear can query the Registry key `"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDTC\MTxOCI"` to see if the value `OracleOcilib` exists.[123]

S0155 WINDSHIELD

WINDSHIELD can gather Registry values.[124]

S1065 Woody RAT

Woody RAT can search registry keys to identify antivirus programs on an compromised host.[125]

S0251 Zebrocy

Zebrocy executes the `reg query` command to obtain information in the Registry.[126]

S0330 Zeus Panda

Zeus Panda checks for the existence of a Registry key and if it contains certain values.[127]

G0128 ZIRCONIUM

ZIRCONIUM has used a tool to query the Registry for proxy settings.[128]

S0412 ZxShell

ZxShell can query the netsvc group value data located in the svchost group Registry key.[129]

S1013 ZxxZ

ZxxZ can search the registry of a compromised host.[130]
