Software Discovery, Technique T1518 - Enterprise

Archived: 2026-04-05 17:26:48 UTC

S0534 Bazar

Bazar can query the Registry for installed applications.[1]

G0060 BRONZE BUTLER

BRONZE BUTLER has used tools to enumerate software installed on an infected host.[2]

S0482 Bundlore

Bundlore has the ability to enumerate what browser is being used as well as version information for Safari.[3]

S0674 CharmPower

CharmPower can list the installed applications on a compromised host.[4]

S0154 Cobalt Strike

The Cobalt Strike System Profiler can discover applications through the browser and identify the version of Java the target has.[5]

S0126 ComRAT

ComRAT can check the victim's default browser to determine which process to inject its communications module into.[6]

S1153 Cuckoo Stealer

Cuckoo Stealer has the ability to search systems for installed applications.[7]

S0472 down_new

down_new has the ability to gather information on installed applications.[2]

S0384 Dridex

Dridex has collected a list of installed software on the system.[8]

S0062 DustySky

DustySky lists all installed software for the infected machine.[9]

S0024 Dyre

Dyre has the ability to identify installed programs on a compromised host.[10]

G1001 HEXANE

HEXANE has enumerated programs installed on an infected machine.[11]

S0431 HotCroissant

HotCroissant can retrieve a list of applications from the `SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths` registry key.[12]

G0100 Inception

Inception has enumerated installed software on compromised systems.[13]

S1245 InvisibleFerret

InvisibleFerret has gathered installed programs and running processes.[14]

S0260 InvisiMole

InvisiMole can collect information about installed software used by specific users, software executed on user login, and software executed by each system.[15][16]

C0044 Juicy Mix

During Juicy Mix, OilRig used browser data dumper tools to create a list of users with Google Chrome installed.[17]

S0526 KGH_SPY

KGH_SPY can collect information on installed applications.[18]

S1185 LightSpy

If sent the command `16001`, LightSpy uses the `NSFileManger contentsOfDirectoryAtPath()` to enumerate the Applications folder to collect the bundle name, bundle identifier, and version information from each application's `info.plist` file. The results are then converted into a JSON blob for exfiltration.[19]

S1141 LunarWeb

LunarWeb can list installed software on compromised systems.[20]

S0652 MarkiRAT

MarkiRAT can check for the Telegram installation directory by enumerating the files on disk.[21]

S0455 Metamorfo

Metamorfo has searched the compromised system for banking applications.[22][23]

G0069 MuddyWater

MuddyWater has used a PowerShell backdoor to check for Skype connectivity on the target machine.[24]

G0129 Mustang Panda

Mustang Panda has searched the victim system for the `InstallUtil.exe` program and its version.[25]

C0016 Operation Dust Storm

During Operation Dust Storm, the threat actors deployed a file called `DeployJava.js` to fingerprint installed software on a victim system prior to exploit delivery.[26]

C0014 Operation Wocao

During Operation Wocao, threat actors collected a list of installed software on the infected system.[27]

S0229 Orz

Orz can gather the victim's Internet Explorer version.[28]

S0598 P.A.S. Webshell

P.A.S. Webshell can list PHP server configuration details.[29]

S1228 PUBLOAD

PUBLOAD has used several commands executed in sequence via `cmd` in a short interval to gather software versions including querying Registry keys.[30]

S0650 QakBot

QakBot can enumerate a list of installed programs.[31]

S1148 Raccoon Stealer

Raccoon Stealer is capable of identifying running software on victim machines.[32][33]

S1240 RedLine Stealer

RedLine Stealer can get a list of programs on the victim device.[34]

S0148 RTM

RTM can scan victim drives to look for specific banking software on the machine to determine next actions.[35]

S1099 Samurai

Samurai can check for the presence and version of the .NET framework.[36]

S0445 ShimRatReporter

ShimRatReporter gathered a list of installed software on the infected host.[37]

G1008 SideCopy

SideCopy has collected browser information from a compromised host.[38]

G0121 Sidewinder

Sidewinder has used tools to enumerate software installed on an infected host.[39][40]

S0623 Siloscape

Siloscape searches for the kubectl binary.[41]

S1124 SocGholish

SocGholish can identify the victim's browser in order to serve the correct fake update page.[42]

S0646 SpicyOmelette

SpicyOmelette can enumerate running software on a targeted system.[43]

S1183 StrelaStealer

StrelaStealer variants use COM objects to enumerate installed applications from the "AppsFolder" on victim machines.[44]

S1042 SUGARDUMP

SUGARDUMP can identify Chrome, Opera, Edge Chromium, and Firefox browsers, including version number, on a compromised host.[45]

S1064 SVCReady

SVCReady can collect a list of installed software from an infected host.[46]

S0467 TajMahal

TajMahal has the ability to identify the Internet Explorer (IE) version on an infected host.[47]

G0081 Tropic Trooper

Tropic Trooper's backdoor could list the infected system's installed software.[48]

G1017 Volt Typhoon

Volt Typhoon has queried the Registry on compromised systems for information on installed software.[49][50]

G0124 Windigo

Windigo has used a script to detect installed software on targeted systems.[51]

G0112 Windshift

Windshift has used malware to identify installed software.[52]

S1065 Woody RAT

Woody RAT can collect .NET, PowerShell, and Python information from an infected host.[53]

S0658 XCSSET

XCSSET uses `ps aux` with the `grep` command to enumerate common browsers and system processes potentially impacting XCSSET's exfiltration capabilities.[54]
