System Time Discovery, Technique T1124 - Enterprise

Archived: 2026-04-05 14:09:26 UTC

S0331 Agent Tesla

Agent Tesla can collect the timestamp from the victim’s machine.[13]

S0622 AppleSeed

AppleSeed can pull a timestamp from the victim's machine.[14]

S0373 Astaroth

Astaroth collects the timestamp from the infected machine. [15]

S1053 AvosLocker

AvosLocker has checked the system time before and after encryption.[16]

S0344 Azorult

Azorult can collect the time zone information from the system.[17][18]

S1081 BADHATCH

BADHATCH can obtain the `DATETIME` and `UPTIME` from a compromised machine.[19]

S0534 Bazar

Bazar can collect the time on the compromised host.[20][21]

S1246 BeaverTail

BeaverTail has obtained and sent the current timestamp associated with the victim device to C2.[22]

S0574 BendyBear

BendyBear has the ability to determine local time on a compromised host.[23]

S0017 BISCUIT

BISCUIT has a command to collect the system `UPTIME`.[24]

S0268 Bisonal

Bisonal can check the system time set on the infected host.[25]

S0657 BLUELIGHT

BLUELIGHT can collect the local time on a compromised host.[26]

G0060 BRONZE BUTLER

BRONZE BUTLER has used `net time` to check the local time on a target system.[27]

S0471 build_downer

build_downer has the ability to determine the local time to ensure malware installation only happens during the hours that the infected system is active.[28]

C0015 C0015

During C0015, the threat actors used the command `net view /all time` to gather the local time of a compromised network.[29]

S0351 Cannon

Cannon can collect the current time zone information from the victim's machine.[30]

S0335 Carbon

Carbon uses the command `net time \127.0.0.1` to get information the system's time.[31]

S1043 ccf32

ccf32 can determine the local time on targeted machines.[32]

G0114 Chimera

Chimera has used `time /t` and `net time \ip/hostname` for system time discovery.[33]

S0660 Clambling

Clambling can determine the current time.[34]

S0126 ComRAT

ComRAT has checked the victim system's date and time to perform tasks during business hours (9 to 5, Monday to Friday).[35]

S0608 Conficker

Conficker uses the current UTC victim system date for domain generation and connects to time servers to determine the current date.[36][37]

S0115 Crimson

Crimson has the ability to determine the date and time on a compromised host.[38]

G1012 CURIUM

CURIUM deployed mechanisms to check system time information following strategic website compromise attacks.[39]

S1111 DarkGate

DarkGate creates a log file for capturing keylogging, clipboard, and related data using the victim host's current date for the filename.[40] DarkGate queries victim system epoch time during execution.[40] DarkGate captures system time information as part of automated profiling on initial installation.[41]

G0012 Darkhotel

Darkhotel malware can obtain system time from a compromised host.[42]

S0673 DarkWatchman

DarkWatchman can collect time zone information and system `UPTIME`.[43]

S1033 DCSrv

DCSrv can compare the current time on an infected host with a configuration value to determine when to start the encryption process.[44]

S1134 DEADWOOD

DEADWOOD will set a timestamp value to determine when wiping functionality starts. When the timestamp is met on the system, a trigger file is created on the operating system allowing for execution to proceed. If the timestamp is in the past, the wiper will execute immediately.[45]

S0694 DRATzarus

DRATzarus can use the `GetTickCount` and `GetSystemTimeAsFileTime` API calls to inspect system time.[46]

S1159 DUSTTRAP

DUSTTRAP reads the infected system's current time and writes it to a log file during execution.[47]

S0554 Egregor

Egregor contains functionality to query the local/system time.[48]

S0091 Epic

Epic uses the `net time` command to get the system time from the machine and collect the current date and time zone information.[49]

S0396 EvilBunny

EvilBunny has used the API calls NtQuerySystemTime, GetSystemTimeAsFileTime, and GetTickCount to gather time metrics as part of its checks to see if the malware is running in a sandbox.[50]

S0267 FELIXROOT

FELIXROOT gathers the time zone information from the victim's machine.[51]

G0046 FIN7

FIN7 has used the PowerShell script 3CF9.ps1 to execute `net time`.[52]

S1044 FunnyDream

FunnyDream can check system time to help determine when changes were made to specified files.[32]

S0588 GoldMax

GoldMax can check the current date-time value of the compromised system, comparing it to the hardcoded execution trigger and can send the current timestamp to the C2 server.[53][54]

S0531 Grandoreiro

Grandoreiro can determine the time on the victim machine via IPinfo.[55]

S0237 GravityRAT

GravityRAT can obtain the date and time of a system.[56]

S0690 Green Lambert

Green Lambert can collect the date and time from a compromised host.[57][58]

S0417 GRIFFON

GRIFFON has used a reconnaissance module that can be used to retrieve the date and time of the system.[59]

G0126 Higaisa

Higaisa used a function to gather the current time.[60]

S0376 HOPLIGHT

HOPLIGHT has been observed collecting system time from victim machines.[61]

S0260 InvisiMole

InvisiMole gathers the local system time from the victim's machine.[62][63]

S1051 KEYPLUG

KEYPLUG can obtain the current tick count of an infected computer.[64]

G0032 Lazarus Group

A Destover-like implant used by Lazarus Group can obtain the current system time and send it to the C2 server.[65]

S1244 Medusa Ransomware

Medusa Ransomware has discovered device uptime through `GetTickCount()`.[66]

S0455 Metamorfo

Metamorfo uses JavaScript to get the system time.[67]

S0149 MoonWind

MoonWind obtains the victim's current time.[68]

S0039 Net

The `net time` command can be used in Net to determine the local or remote system time.[69]

S1147 Nightdoor

Nightdoor can identify the system local time information.[70]

S0353 NOKKI

NOKKI can collect the current timestamp of the victim's machine.[71]

S0439 Okrum

Okrum can obtain the date and time of the compromised system.[72]

S0264 OopsIE

OopsIE checks to see if the system is configured with "Daylight" time and checks for a specific region to be set for the timezone.[73]

C0012 Operation CuckooBees

During Operation CuckooBees, the threat actors used the `net time` command as part of their advanced reconnaissance.[74]

C0014 Operation Wocao

During Operation Wocao, threat actors used the `time` command to retrieve the current time of a compromised system.[75]

S1233 PAKLOG

PAKLOG has collected a timestamp to log the precise time a key was pressed, formatted as %Y-%m-%d %H:%M:%S.[76]

S0501 PipeMon

PipeMon can send time zone information from a compromised host to C2.[77]

S0013 PlugX

PlugX has identified system time through its GetSystemInfo command.[78]

S0139 PowerDuke

PowerDuke has commands to get the time the machine was built, the time, and the time zone.[79]

S0238 Proxysvc

As part of the data reconnaissance phase, Proxysvc grabs the system time to send back to the control server.[65]

S1228 PUBLOAD

PUBLOAD has collected the machine's tick count through the use of `GetTickCount`.[80]

S0650 QakBot

QakBot can identify the system time on a targeted host.[81]

S1148 Raccoon Stealer

Raccoon Stealer gathers victim machine timezone information.[82][83]

S0148 RTM

RTM can obtain the victim time zone.[84]

S0596 ShadowPad

ShadowPad has collected the current date and time of the victim system.[85]

S0140 Shamoon

Shamoon obtains the system time and will only activate if it is greater than a preset date.[86][87]

S0450 SHARPSTATS

SHARPSTATS has the ability to identify the current date and time on the compromised host.[88]

S1178 ShrinkLocker

ShrinkLocker retrieves a system timestamp that is used in generating an encryption key.[89]

G0121 Sidewinder

Sidewinder has used tools to obtain the current system time.[90]

S0692 SILENTTRINITY

SILENTTRINITY can collect start time information from a compromised host.[91]

S0615 SombRAT

SombRAT can execute `getinfo` to discover the current time on a compromised host.[92][93]

S1227 StarProxy

StarProxy has utilized the windows API call `GetLocalTime()` to retrieve a SystemTime structure to generate a seed value.[94]

S0380 StoneDrill

StoneDrill can obtain the current date and time of the victim machine.[95]

S1034 StrifeWater

StrifeWater can collect the time zone from the victim's machine.[96]

S0603 Stuxnet

Stuxnet collects the time and date of a system when it is infected.[97]

S0559 SUNBURST

SUNBURST collected device `UPTIME`.[98][99]

S1064 SVCReady

SVCReady can collect time zone information.[100]

S0098 T9000

T9000 gathers and beacons the system time during installation.[101]

S0011 Taidoor

Taidoor can use `GetLocalTime` and `GetSystemTime` to collect system time.[102]

S0586 TAINTEDSCRIBE

TAINTEDSCRIBE can execute `GetLocalTime` for time discovery.[103]

S0467 TajMahal

TajMahal has the ability to determine local time on a compromised host.[104]

G0089 The White Company

The White Company has checked the current date on the victim system.[105]

S0678 Torisma

Torisma can collect the current time on a victim machine.[106]

G0010 Turla

Turla surveys a system upon check-in to discover the system time by using the `net time` command.[49]

G1048 UNC3886

UNC3886 has used installation scripts to collect the system time on targeted ESXi hosts.[107]

S0275 UPPERCUT

UPPERCUT has the capability to obtain the time zone information and current timestamp of the victim’s machine.[108]

G1017 Volt Typhoon

Volt Typhoon has obtained the victim's system timezone.[109]

S0466 WindTail

WindTail has the ability to generate the current date and time.[110]

S0251 Zebrocy

Zebrocy gathers the current time zone and date information from the system.[111][112]

S0330 Zeus Panda

Zeus Panda collects the current system time (UTC) and sends it back to the C2 server.[113]

G0128 ZIRCONIUM

ZIRCONIUM has used a tool to capture the time on a compromised host in order to register it with C2.[114]

Source: https://attack.mitre.org/techniques/T1124