Indicator Removal: Timestomp, Sub-technique T1070.006 - Enterprise

Archived: 2026-04-05 17:40:08 UTC

S0066 3PARA RAT

3PARA RAT has a command to set certain attributes such as creation/modification timestamps on files.[7]

G0007 APT28

APT28 has performed timestomping on victim files.[8]

G0016 APT29

APT29 has used timestomping to alter the Standard Information timestamps on their web shells to match other files in the same directory.[9]

G0050 APT32

APT32 has used scheduled task raw XML with a backdated timestamp of June 2, 2016. The group has also set the creation time of the files dropped by the second stage of the exploit to match the creation time of kernel32.dll. Additionally, APT32 has used a random value to modify the timestamp of the file storing the clientID.[10][11][12]

G0082 APT38

APT38 has modified data timestamps to mimic files that are in the same folder on a compromised host.[13]

G1023 APT5

APT5 has modified file timestamps.[14]

S0438 Attor

Attor has manipulated the time of last access to files and registry keys after they have been created or modified.[15]

S0239 Bankshot

Bankshot modifies the time of a file as specified by the control server.[16]

S0570 BitPaymer

BitPaymer can modify the timestamp of an executable so that it can be identified and restored by the decryption tool.[17]

S1181 BlackByte 2.0 Ransomware

BlackByte 2.0 Ransomware can timestomp files for defense evasion and anti-forensics purposes.[18]

S0520 BLINDINGCAN

BLINDINGCAN has modified file and directory timestamps.[19][20]

S1226 BOOKWORM

BOOKWORM has modified file timestamps from the export address table (EAT) to make it difficult to discern when the module was created. [21]

S1161 BPFDoor

BPFDoor uses the `utimes()` function to change the executable's timestamp.[22]

C0032 C0032

During the C0032 campaign, TEMP.Veles used timestomping to modify the `$STANDARD_INFORMATION` attribute on tools.[23]

G0114 Chimera

Chimera has used a Windows version of the Linux `touch` command to modify the date and time stamp on DLLs. [24]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP can time stomp its executable, previously dating it between 2010 to 2021.[25]

S0020 China Chopper

China Chopper's server component can change the timestamp of files.[26][27][28]

S0154 Cobalt Strike

Cobalt Strike can timestomp any files or payloads placed on a target machine to help them blend in.[29][30]

C0029 Cutting Edge

During Cutting Edge, threat actors changed timestamps of multiple files on compromised Ivanti Secure Connect VPNs to conceal malicious activity.[31][32]

S0687 Cyclops Blink

Cyclops Blink has the ability to use the Linux API function `utime` to change the timestamps of modified firmware update images.[33]

S0021 Derusbi

The Derusbi malware supports timestomping.[34][35]

S0081 Elise

Elise performs timestomping of a CAB file it creates.[36]

S0363 Empire

Empire can timestomp any files or payloads placed on a target machine to help them blend in.[37]

S0568 EVILNUM

EVILNUM has changed the creation date of files.[38]

S0181 FALLCHILL

FALLCHILL can modify file or directory timestamps.[39]

S0168 Gazer

For early Gazer versions, the compilation timestamp was faked.[40]

S0666 Gelsemium

Gelsemium has the ability to perform timestomping of files on targeted systems.[41]

S0260 InvisiMole

InvisiMole samples were timestomped by the authors by setting the PE timestamps to all zero values. InvisiMole also has a built-in command to modify file times.[42]

S0387 KeyBoy

KeyBoy time-stomped its DLL in order to evade detection.[43]

G0094 Kimsuky

Kimsuky has manipulated timestamps for creation or compilation dates to defeat anti-forensics.[44]

S0641 Kobalos

Kobalos can modify timestamps of replaced files, such as `ssh` with the added credential stealer or `sshd` used to deploy Kobalos.[45]

G0032 Lazarus Group

Several Lazarus Group malware families use timestomping, including modifying the last write timestamp of a specified Registry key to a random date, as well as copying the timestamp for legitimate .exe files (such as

calc.exe or mspaint.exe) to its dropped files.[46][47][48][49]

S1016 MacMa

MacMa has the capability to create and modify file timestamps.[50]

S1059 metaMain

metaMain can change the `CreationTime`, `LastAccessTime`, and `LastWriteTime` file time attributes when executed with `SYSTEM` privileges.[51]

S0083 Misdat

Many Misdat samples were programmed using Borland Delphi, which will mangle the default PE compile timestamp of a file.[52]

S1135 MultiLayer Wiper

MultiLayer Wiper changes timestamps of overwritten files to either 1601.1.1 for NTFS filesystems, or 1980.1.1 for all other filesystems.[53]

G0129 Mustang Panda

Mustang Panda has modified file timestamps from the export address table (EAT) in malware to make it difficult to identify creation times.[21]

S1090 NightClub

NightClub can modify the Creation, Access, and Write timestamps for malicious DLLs to match those of the genuine Windows DLL user32.dll.[54]

S1100 Ninja

Ninja can change or create the last access or write times.[55]

S0352 OSX_OCEANLOTUS.D

OSX_OCEANLOTUS.D can use the `touch -t` command to change timestamps.[56][57]

S0072 OwaAuth

OwaAuth has a command to timestop a file or directory.[58]

S1031 PingPull

PingPull has the ability to timestomp a file.[59]

S0150 POSHSPY

POSHSPY modifies timestamps of all downloaded executables to match a randomly selected file created prior to 2013.[60]

S0393 PowerStallion

PowerStallion modifies the MAC times of its local log files to match that of the victim's desktop.ini file.[61]

S0078 Psylo

Psylo has a command to conduct timestomping by setting a specified file’s timestamps to match those of a system file in the System32 directory.[62]

G0106 Rocke

Rocke has changed the time stamp of certain files.[63]

S0185 SEASHARPEE

SEASHARPEE can timestomp files on victims using a Web shell.[64]

S0140 Shamoon

Shamoon can change the modified time for files to evade forensic detection.[65]

C0024 SolarWinds Compromise

During the SolarWinds Compromise, APT29 modified timestamps of backdoors to match legitimate Windows files.[66]

S0603 Stuxnet

Stuxnet extracts and writes driver files that match the times of other legitimate files.[67]

S0586 TAINTEDSCRIBE

TAINTEDSCRIBE can change the timestamp of specified filenames.[68]

S0164 TDTESS

After creating a new service for persistence, TDTESS sets the file creation time for the service to the creation time of the victim's legitimate svchost.exe file.[69]

G1048 UNC3886

UNC3886 has used scripts to timestomp ESXi hosts prior to installing malicious vSphere Installation Bundles (VIBs).[70]

S1164 UPSTYLE

UPSTYLE restores timestamps to original values following modification.[71]

S0136 USBStealer

USBStealer sets the timestamps of its dropper files to the last-access and last-write timestamps of a standard Windows library chosen on the system.[72]

S0141 Winnti for Windows

Winnti for Windows can set the timestamps for its worker and service components to match that of cmd.exe.[73]
