Clipboard Data, Technique T1115 - Enterprise

Archived: 2026-04-05 13:26:15 UTC

S0331 Agent Tesla

Agent Tesla can steal data from the victim's clipboard.[6][7][8][9]

G0082 APT38

APT38 used a Trojan called KEYLIME to collect data from the clipboard.[10]

G0087 APT39

APT39 has used tools capable of stealing contents of the clipboard.[11]

S0373 Astaroth

Astaroth collects information from the clipboard by using the OpenClipboard() and GetClipboardData() libraries.[12]

S0438 Attor

Attor has a plugin that collects data stored in the Windows clipboard by using the OpenClipboard and GetClipboardData APIs.[13]

S1226 BOOKWORM

BOOKWORM has used its KBLogger.dll module to steal data saved to the clipboard. [14]

S0454 Cadelspy

Cadelspy has the ability to steal data from the clipboard.[15]

S0261 Catchamas

Catchamas steals data stored in the clipboard.[16]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP can capture content from the clipboard.[17]

S0660 Clambling

Clambling has the ability to capture and store clipboard data.[18][19]

S0050 CosmicDuke

CosmicDuke copies and exfiltrates the clipboard contents every 30 seconds.[20]

S0334 DarkComet

DarkComet can steal data from the clipboard.[21]

S1111 DarkGate

DarkGate starts a thread on execution that captures clipboard data and logs it to a predefined log file.[22][23]

S1066 DarkTortilla

DarkTortilla can download a clipboard information stealer module.[24]

S0363 Empire

Empire can harvest clipboard data on both Windows and macOS systems.[25]

S0569 Explosive

Explosive has a function to use the OpenClipboard wrapper.[26]

S0381 FlawedAmmyy

FlawedAmmyy can collect clipboard data.[27]

S0531 Grandoreiro

Grandoreiro can capture clipboard data from a compromised host.[28]

S0170 Helminth

The executable version of Helminth has a module to log clipboard contents.[29]

S1245 InvisibleFerret

InvisibleFerret has stolen data from the clipboard using the Python project "pyperclip".[30][31][32] InvisibleFerret has also captured clipboard contents during copy and paste operations.[33]

S0044 JHUHUGIT

A JHUHUGIT variant accesses a screenshot saved in the clipboard and converts it to a JPG image.[34]

S0283 jRAT

jRAT can capture clipboard data.[35]

S0250 Koadic

Koadic can retrieve the current content of the user clipboard.[36]

S0356 KONNI

KONNI had a feature to steal data from the clipboard.[37]

S0409 Machete

Machete hijacks the clipboard data by creating an overlapped window that listens to keyboard events.[38][39]

S0282 MacSpy

MacSpy can steal clipboard contents.[40]

S0652 MarkiRAT

MarkiRAT can capture clipboard content.[41]

S0530 Melcoz

Melcoz can monitor content saved to the clipboard.[42]

S0455 Metamorfo

Metamorfo has a function to hijack data from the clipboard by monitoring the contents of the clipboard and replacing the cryptocurrency wallet with the attacker's.[43][44]

S1146 MgBot

MgBot can capture clipboard data.[45][46]

S1122 Mispadu

Mispadu has the ability to capture and replace Bitcoin wallet data in the clipboard on a compromised host.[47]

G0049 OilRig

OilRig has used infostealer tools to copy clipboard data.[48]

C0014 Operation Wocao

During Operation Wocao, threat actors collected clipboard data in plaintext.[49]

S1233 PAKLOG

PAKLOG has monitored and extracted clipboard contents.[50]

S0332 Remcos

Remcos steals and modifies data from the clipboard.[51]

S0375 Remexi

Remexi collects text from the clipboard.[52]

S0240 ROKRAT

ROKRAT can extract clipboard data from a compromised host.[53]

S0148 RTM

RTM collects data from the clipboard.[54][55]

S0253 RunningRAT

RunningRAT contains code to open and copy data from the clipboard.[56]

S0692 SILENTTRINITY

SILENTTRINITY can monitor Clipboard text and can use `System.Windows.Forms.Clipboard.GetText()` to collect data from the clipboard.[57]

S0467 TajMahal

TajMahal has the ability to steal data from the clipboard of an infected host.[58]

S0004 TinyZBot

TinyZBot contains functionality to collect information from the clipboard.[59]

S0257 VERMIN

VERMIN collects data stored in the clipboard.[60]

S1207 XLoader

XLoader can collect data stored in the victim's clipboard.[61][62]

S0330 Zeus Panda

Zeus Panda can hook GetClipboardData function to watch for clipboard pastes to collect.[63]
