Screen Capture, Technique T1113 - Enterprise

Archived: 2026-04-05 15:41:42 UTC

S0331 Agent Tesla

Agent Tesla can capture screenshots of the victim’s desktop.[3][4][5][6][7]

S0622 AppleSeed

AppleSeed can take screenshots on a compromised host by calling a series of APIs.[8][9]

G0007 APT28

APT28 has used tools to take screenshots from victims.[10][11][12][13]

G0087 APT39

APT39 has used a screen capture utility to take screenshots on a compromised host.[14][15]

G1044 APT42

APT42 has used malware, such as GHAMBAR and POWERPOST, to take screenshots.[16]

S0456 Aria-body

Aria-body has the ability to capture screenshots on compromised hosts.[17]

S1087 AsyncRAT

AsyncRAT has the ability to view the screen on compromised hosts.[18]

S0438 Attor

Attor's has a plugin that captures screenshots of the target applications.[19]

S0344 Azorult

Azorult can capture screenshots of the victim’s machines.[20]

S1081 BADHATCH

BADHATCH can take screenshots and send them to an actor-controlled C2 server.[21]

S0128 BADNEWS

BADNEWS has a command to take a screenshot and send it to the C2 server.[22][23]

S0337 BadPatch

BadPatch captures screenshots in .jpg format and then exfiltrates them.[24]

S0234 Bandook

Bandook is capable of taking an image of and uploading the current desktop.[25][26]

S0017 BISCUIT

BISCUIT has a command to periodically take screenshots of the system.[27]

S0089 BlackEnergy

BlackEnergy is capable of taking screenshots.[28]

S0657 BLUELIGHT

BLUELIGHT has captured a screenshot of the display every 30 seconds for the first 5 minutes after initiating a C2 loop, and then once every five minutes thereafter.[29]

G0060 BRONZE BUTLER

BRONZE BUTLER has used a tool to capture screenshots.[30][31]

S1063 Brute Ratel C4

Brute Ratel C4 can take screenshots on compromised hosts.[32]

S0454 Cadelspy

Cadelspy has the ability to capture screenshots and webcam photos.[33]

S0351 Cannon

Cannon can take a screenshot of the desktop.[34]

S0030 Carbanak

Carbanak performs desktop video recording and captures screenshots of the desktop and sends it to the C2 server.[35]

S0484 Carberp

Carberp can capture display screenshots with the screens_dll.dll plugin.[36]

S0348 Cardinal RAT

Cardinal RAT can capture screenshots.[37]

S0261 Catchamas

Catchamas captures screenshots based on specific keywords in the window's title.[38]

S0631 Chaes

Chaes can capture screenshots of the infected machine.[39]

S0674 CharmPower

CharmPower has the ability to capture screenshots.[40]

S1149 CHIMNEYSWEEP

CHIMNEYSWEEP can capture screenshots on targeted systems using a timer and either upload them or store them to disk.[41]

S0023 CHOPSTICK

CHOPSTICK has the capability to capture screenshots.[12]

S0667 Chrommme

Chrommme has the ability to capture screenshots.[42]

S0660 Clambling

Clambling has the ability to capture screenshots.[43]

S0154 Cobalt Strike

Cobalt Strike's Beacon payload is capable of capturing screenshots.[44][45][46]

S0338 Cobian RAT

Cobian RAT has a feature to perform screen capture.[47]

S0591 ConnectWise

ConnectWise can take screenshots on remote hosts.[48]

S0050 CosmicDuke

CosmicDuke takes periodic screenshots and exfiltrates them.[49]

S0115 Crimson

Crimson contains a command to perform screen captures.[50][51][52]

S0235 CrossRAT

CrossRAT is capable of taking screen captures.[25]

S1153 Cuckoo Stealer

Cuckoo Stealer can run `screencapture` to collect screenshots from compromised hosts. [53]

G0070 Dark Caracal

Dark Caracal took screenshots using their Windows malware.[25]

S0187 Daserf

Daserf can take screenshots.[54][30]

S0021 Derusbi

Derusbi is capable of performing screen captures.[55]

S0213 DOGCALL

DOGCALL is capable of capturing screenshots of the victim's machine.[56][57]

G0035 Dragonfly

Dragonfly has performed screen captures of victims, including by using a tool, scr.exe (which matched the hash of ScreenUtil).[58][59][60]

S1159 DUSTTRAP

DUSTTRAP can capture screenshots.[61]

S0062 DustySky

DustySky captures PNG screenshots of the main screen.[62]

S0593 ECCENTRICBANDWAGON

ECCENTRICBANDWAGON can capture screenshots and store them locally.[63]

S0363 Empire

Empire is capable of capturing screenshots on Windows and macOS systems.[64]

S0152 EvilGrab

EvilGrab has the capability to capture screenshots.[65]

G0046 FIN7

FIN7 captured screenshots and desktop video recordings.[66]

S0182 FinFisher

FinFisher takes a screenshot of the screen and displays it on top of all other windows for few seconds in an apparent attempt to hide some messages showed by the system during the setup process.[67][68]

S0143 Flame

Flame can take regular screenshots when certain applications are open that are sent to the command and control server.[69]

S0381 FlawedAmmyy

FlawedAmmyy can capture screenshots.[70]

S0277 FruitFly

FruitFly takes screenshots of the user's desktop.[71]

S1044 FunnyDream

The FunnyDream ScreenCap component can take screenshots on a compromised host.[72]

G0047 Gamaredon Group

Gamaredon Group's malware can take screenshots of the compromised computer every minute.[73][74][75]

S0032 gh0st RAT

gh0st RAT can capture the victim’s screen remotely.[76]

G0115 GOLD SOUTHFIELD

GOLD SOUTHFIELD has used the remote monitoring and management tool ConnectWise to obtain screen captures from victim's machines.[77]

S0417 GRIFFON

GRIFFON has used a screenshot module that can be used to take a screenshot of the remote system.[78]

G0043 Group5

Malware used by Group5 is capable of watching the victim's screen.[79]

S0151 HALFBAKED

HALFBAKED can obtain screenshots from the victim.[80]

S1229 Havoc

Havoc can capture screenshots.[81][82][83]

S0431 HotCroissant

HotCroissant has the ability to do real time screen viewing on an infected host.[84]

S0203 Hydraq

Hydraq includes a component based on the code of VNC that can stream a live feed of the desktop of an infected host.[85]

S0398 HyperBro

HyperBro has the ability to take screenshots.[86]

S0260 InvisiMole

InvisiMole can capture screenshots of not only the entire screen, but of each separate window open, in case they are overlapping.[87][88]

S0163 Janicab

Janicab captured screenshots and sent them out to a C2 server.[89][90]

S0044 JHUHUGIT

A JHUHUGIT variant takes screenshots by simulating the user pressing the "Take Screenshot" key (VK_SCREENSHOT), accessing the screenshot saved in the clipboard, and converting it to a JPG image.[91][92]

S0283 jRAT

jRAT has the capability to take screenshots of the victim’s machine.[93][94]

S0088 Kasidet

Kasidet has the ability to initiate keylogging and screen captures.[95]

S0265 Kazuar

Kazuar captures screenshots of the victim’s screen.[96]

S0387 KeyBoy

KeyBoy has a command to perform screen grabbing.[97]

S0271 KEYMARBLE

KEYMARBLE can capture screenshots of the victim’s machine.[98]

G0094 Kimsuky

Kimsuky has captured browser screenshots using TRANSLATEXT.[99]

S0437 Kivars

Kivars has the ability to capture screenshots on the infected host.[100]

S0356 KONNI

KONNI can take screenshots of the victim’s machine.[101]

S1185 LightSpy

LightSpy uses Apple's built-in AVFoundation Framework library to access the user's camera and screen. It uses the `AVCaptureStillImage` to take a picture using the user's camera and the `AVCaptureScreen` to take a screenshot or record the user's screen for a specified period of time.[102]

S0680 LitePower

LitePower can take system screenshots and save them to `%AppData%`.[103]

S0681 Lizar

Lizar can take JPEG screenshots of an infected system.[104][105] Lizar has also used a plugin to take a screenshot of the infected system.[105]

S0582 LookBack

LookBack can take desktop screenshots.[106]

S1213 Lumma Stealer

Lumma Stealer has taken screenshots of victim machines.[107]

S1142 LunarMail

LunarMail can capture screenshots from compromised hosts.[108]

S0409 Machete

Machete captures screenshots.[109][110][111][112]

S1016 MacMa

MacMa has used Apple’s Core Graphic APIs, such as `CGWindowListCreateImageFromArray`, to capture the user's screen and open windows.[113][114]

S0282 MacSpy

MacSpy can capture screenshots of the desktop over multiple monitors.[71]

S1060 Mafalda

Mafalda can take a screenshot of the target machine and save it to a file.[115]

G0059 Magic Hound

Magic Hound malware can take a screenshot and upload the file to its C2 server.[116]

S1156 Manjusaka

Manjusaka can take screenshots of the victim desktop.[117]

S0652 MarkiRAT

MarkiRAT can capture screenshots that are initially saved as ‘scr.jpg’.[118]

S0167 Matryoshka

Matryoshka is capable of performing screen captures.[119][120]

S1059 metaMain

metaMain can take and save screenshots.[115][121]

S0455 Metamorfo

Metamorfo can collect screenshots of the victim’s machine.[122][123]

S0339 Micropsia

Micropsia takes screenshots every 90 seconds by calling the Gdi32.BitBlt API.[124]

S1122 Mispadu

Mispadu has the ability to capture screenshots on compromised hosts.[125][126][127][128]

G1019 MoustachedBouncer

MoustachedBouncer has used plugins to take screenshots on targeted systems.[129]

G0069 MuddyWater

MuddyWater has used malware that can capture screenshots of the victim’s machine.[130]

S0198 NETWIRE

NETWIRE can capture the victim's screen.[131][132][133][134]

S1090 NightClub

NightClub can load a module to call `CreateCompatibleDC` and `GdipSaveImageToStream` for screen capture.[129]

S0385 njRAT

njRAT can capture screenshots of the victim's machines.[135]

S1107 NKAbuse

NKAbuse can take screenshots of the victim machine.[136]

S0644 ObliqueRAT

ObliqueRAT can capture a screenshot of the current screen.[137]

S0340 Octopus

Octopus can capture screenshots of the victims' machine.[138][139][140]

G0049 OilRig

OilRig has a tool called CANDYKING to capture a screenshot of user's desktop.[141]

S1050 PcShare

PcShare can take screen shots of a compromised machine.[72]

S0643 Peppy

Peppy can take screenshots on targeted systems.[50]

S0013 PlugX

PlugX allows the operator to capture screenshots.[142]

S0428 PoetRAT

PoetRAT has the ability to take screen captures.[143][144]

S0216 POORAIM

POORAIM can perform screen capturing.[56]

S0194 PowerSploit

PowerSploit's `Get-TimedScreenshot` Exfiltration module can take screenshots at regular intervals.[145][146]

S0223 POWERSTATS

POWERSTATS can retrieve screenshots from compromised hosts.[147][148]

S0184 POWRUNER

POWRUNER can capture a screenshot from a victim.[149]

S0113 Prikormka

Prikormka contains a module that captures screenshots of the victim's desktop.[150]

S0279 Proton

Proton captures the content of the desktop with the screencapture binary.[71]

S0147 Pteranodon

Pteranodon can capture screenshots at a configurable interval.[151][152]

S0192 Pupy

Pupy can drop a mouse-logger that will take small screenshots around at each click and then send back to the server.[153]

S1209 Quick Assist

Quick Assist allows for the remote administrator to take screenshots of the running system.[154]

S0686 QuietSieve

QuietSieve has taken screenshots every five minutes and saved them to the user's local Application Data folder under `Temp\SymbolSourceSymbols\icons` or `Temp\ModeAuto\icons`.[155]

S1148 Raccoon Stealer

Raccoon Stealer can capture screenshots from victim systems.[156][157]

S0629 RainyDay

RainyDay has the ability to capture screenshots.[158]

S0458 Ramsay

Ramsay can take screenshots every 30 seconds as well as when an external removable storage device is connected.[159]

S0662 RCSession

RCSession can capture screenshots from a compromised host.[160]

S0495 RDAT

RDAT can take a screenshot on the infected system.[161]

S0153 RedLeaves

RedLeaves can capture screenshots.[162][163]

S1240 RedLine Stealer

RedLine Stealer can capture screenshots on a compromised host.[164][165]

S0332 Remcos

Remcos takes automated screenshots of the infected machine.[166]

S0375 Remexi

Remexi takes screenshots of windows of interest.[167]

S0592 RemoteUtilities

RemoteUtilities can take screenshots on a compromised host.[168]

S0379 Revenge RAT

Revenge RAT has a plugin for screen capture.[169]

S0270 RogueRobin

RogueRobin has a command named `$screenshot` that may be responsible for taking screenshots of the victim machine.[170]

S0240 ROKRAT

ROKRAT can capture screenshots of the infected system using the `gdi32` library.[171][172][173][174][175]

S0090 Rover

Rover takes screenshots of the compromised system's desktop and saves them to `C:\system\screenshot.bmp` for exfiltration every 60 minutes.[176]

S0148 RTM

RTM can capture screenshots.[177][178]

S0546 SharpStage

SharpStage has the ability to capture the victim's screen.[179][180]

S0217 SHUTTERSPEED

SHUTTERSPEED can capture screenshots.[56]

G0091 Silence

Silence can capture victim screen activity.[181][182]

S0692 SILENTTRINITY

SILENTTRINITY can take a screenshot of the current desktop.[183]

S0633 Sliver

Sliver can take screenshots of the victim’s active display.[184]

S0533 SLOTHFULMEDIA

SLOTHFULMEDIA has taken a screenshot of a victim's desktop, named it "Filter3.jpg", and stored it in the local directory.[185]

S0649 SMOKEDHAM

SMOKEDHAM can capture screenshots of the victim’s desktop.[186][187]

S0273 Socksbot

Socksbot can take screenshots.[188]

S0380 StoneDrill

StoneDrill can take screenshots.[189]

S1034 StrifeWater

StrifeWater has the ability to take screen captures.[190]

S1064 SVCReady

SVCReady can take a screenshot from an infected host.[191]

S0663 SysUpdate

SysUpdate has the ability to capture screenshots.[192]

S0098 T9000

T9000 can take screenshots of the desktop and target application windows, saving them to user directories as one byte XOR encrypted .dat files.[193]

S0467 TajMahal

TajMahal has the ability to take screenshots on an infected host including capturing content from windows of instant messaging applications.[194]

S0004 TinyZBot

TinyZBot contains screen capture functionality.[195]

S1239 TONESHELL

TONESHELL has conducted screen capturing.[196]

S1201 TRANSLATEXT

TRANSLATEXT has the ability to capture screenshots of new browser tabs, based on the presence of the `Capture` flag.[99]

S0094 Trojan.Karagany

Trojan.Karagany can take a desktop screenshot and save the file into `\ProgramData\Mail\MailAg\shot.png`.[197][198]

S1196 Troll Stealer

Troll Stealer can capture screenshots from victim machines.[199][200]

S0647 Turian

Turian has the ability to take screenshots.[201]

S0199 TURNEDUP

TURNEDUP is capable of taking screenshots.[202]

S0275 UPPERCUT

UPPERCUT can capture desktop screenshots in the PNG format and send them to the C2 server.[203]

S0386 Ursnif

Ursnif has used hooked APIs to take screenshots.[204][205]

S0476 Valak

Valak has the ability to take screenshots on a compromised host.[206]

S0257 VERMIN

VERMIN can perform screen captures of the victim’s machine.[207]

G1017 Volt Typhoon

Volt Typhoon has obtained a screenshot of the victim's system using the gdi32.dll and gdiplus.dll libraries.[208]

G1035 Winter Vivern

Winter Vivern delivered PowerShell scripts capable of taking screenshots of victim machines.[209]

S1065 Woody RAT

Woody RAT has the ability to take a screenshot of the infected host desktop using Windows GDI+.[210]

S0161 XAgentOSX

XAgentOSX contains the takeScreenShot (along with startTakeScreenShot and stopTakeScreenShot) functions to take screenshots using the CGGetActiveDisplayList, CGDisplayCreateImage, and NSImage:initWithCGImage methods.[11]

S0658 XCSSET

XCSSET saves a screen capture of the victim's system with a numbered filename and `.jpg` extension. Screen captures are taken at specified intervals based on the system. [211]

S1207 XLoader

XLoader can capture screenshots on compromised hosts.[212][213]

S0248 yty

yty collects screenshots of the victim machine.[214]

S0251 Zebrocy

A variant of Zebrocy captures screenshots of the victim’s machine in JPEG and BMP format.[34][215][216][217][218][219]

S0330 Zeus Panda

Zeus Panda can take screenshots of the victim’s machine.[220]

S0086 ZLib

ZLib has the ability to obtain screenshots of the compromised system.[221]

S0412 ZxShell

ZxShell can capture screenshots.[222]

Source: https://attack.mitre.org/techniques/T1113