

T1113 - Screen Capture

Description from ATT&CK

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as CopyFromScreen , xwd , or screencapture .(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Atomic Tests

- Atomic Test #1 Screencapture
- Atomic Test #2 Screencapture (silent)
- Atomic Test #3 X Windows Capture
- Atomic Test #4 Capture Linux Desktop using Import Tool
- Atomic Test #5 Windows Screencapture
- Atomic Test #6 Windows Screen Capture (CopyFromScreen)

Atomic Test #1 - Screencapture

Use screencapture command to collect a full desktop screenshot

Supported Platforms: macOS

auto_generated_guid: 0f47ceb1-720f-4275-96b8-21f0562217ac

Inputs:

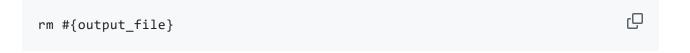
Name	Description	Туре	Default Value
output_file	Output file path	Path	/tmp/T1113_desktop.png

Attack Commands: Run with bash!

screencapture #{output_file}

Q

Cleanup Commands:



Atomic Test #2 - Screencapture (silent)

Use screencapture command to collect a full desktop screenshot

Supported Platforms: macOS

auto_generated_guid: deb7d358-5fbd-4dc4-aecc-ee0054d2d9a4

Inputs:

Name	Description	Туре	Default Value
output_file	Output file path	Path	/tmp/T1113_desktop.png

Attack Commands: Run with bash!

screencapture -x #{output_file}

Q

Cleanup Commands:

rm #{output_file}



Atomic Test #3 - X Windows Capture

Use xwd command to collect a full desktop screenshot and review file with xwud

Supported Platforms: Linux

auto_generated_guid: 8206dd0c-faf6-4d74-ba13-7fbe13dce6ac

Inputs:

Name	Description	Туре	Default Value
output_file	Output file path	Path	/tmp/T1113_desktop.xwd
package_checker	Package checking command for linux. Debian system command-dpkg -s x11-apps	String	rpm -q xorg-x11-apps
package_installer	Package installer command for linux. Debian system commandapt-get install x11-apps	String	yum install -y xorg-x11- apps

Attack Commands: Run with bash!

xwd -root -out #{output_file} xwud -in #{output_file}



Cleanup Commands:

rm #{output_file}

Dependencies: Run with bash!

Description: Package with XWD and XWUD must exist on device

Check Prereq Commands:

Q if #{package_checker} > /dev/null; then exit 0; else exit 1; fi

Get Prereq Commands:

sudo #{package_installer}



Atomic Test #4 - Capture Linux Desktop using Import Tool

Use import command from ImageMagick to collect a full desktop screenshot

Supported Platforms: Linux

auto_generated_guid: 9cd1cccb-91e4-4550-9139-e20a586fcea1

Inputs:

Name	Description	Туре	Default Value
output_file	Output file path	Path	/tmp/T1113_desktop.png

Attack Commands: Run with bash!

import -window root #{output_file}



Cleanup Commands:

rm #{output_file}



Dependencies: Run with bash!

Description: ImageMagick must be installed

Check Prereq Commands:

if import -help > /dev/null 2>&1; then exit 0; else exit 1; fi



Get Prereq Commands:

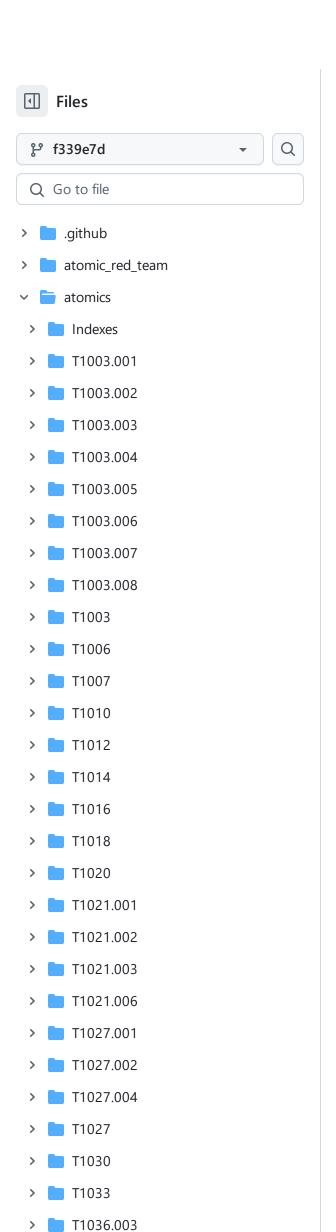
sudo apt install graphicsmagick-imagemagick-compat



Atomic Test #5 - Windows Screencapture

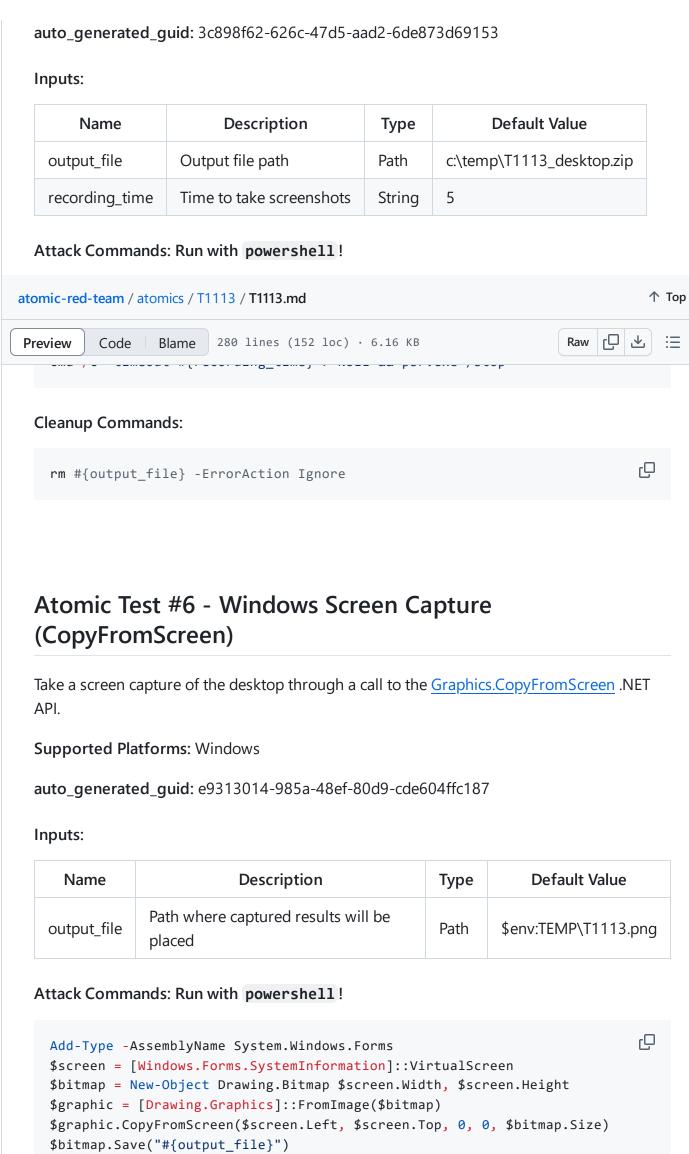
Use Psr.exe binary to collect screenshots of user display. Test will do left mouse click to simulate user behaviour

Supported Platforms: Windows



T1036.004

T1036.005



Q

Remove-Item #{output_file} -ErrorAction Ignore

Cleanup Commands: