

# 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:

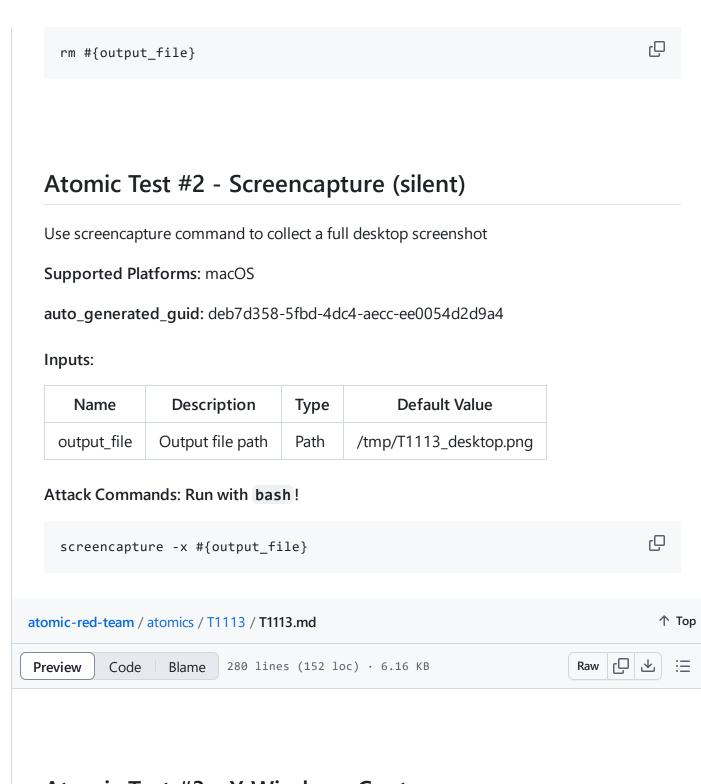
Name	Description	Туре	Default Value
output_file	Output file path	Path	/tmp/T1113_desktop.png

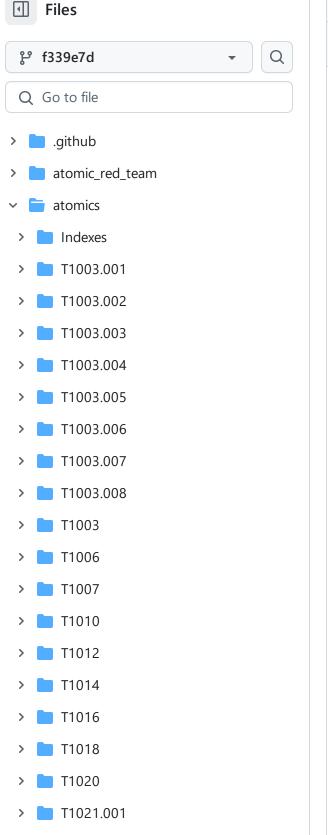
Attack Commands: Run with bash!

screencapture #{output\_file}

Q

**Cleanup Commands:** 





T1021.002

T1021.003

# 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}

Q

T1021.006 T1027.001 T1027.002 T1027.004 T1027 T1030 T1033 T1036.003 T1036.004 T1036.005 T1036.006 T1036 T1037.001 T1037.002 T1037.004 T1037.005 T1039

> T1040

Dependencies: Run with bash!

Description: Package with XWD and XWUD must exist on device

**Check Prereq Commands:** 

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

Q

**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

auto\_generated\_guid: 3c898f62-626c-47d5-aad2-6de873d69153

#### Inputs:

Name	Description	Туре	Default Value
output_file	Output file path	Path	c:\temp\T1113_desktop.zip
recording_time	Time to take screenshots	String	5

#### Attack Commands: Run with powershell!

```
cmd /c start /b psr.exe /start /output #{output_file} /sc 1 /gui 0 /stop
Add-Type -MemberDefinition '[DllImport("user32.dll")] public static exte
[W.U32]::mouse_event(0x02 -bor 0x04 -bor 0x01, 0, 0, 0, 0);
cmd /c "timeout #{recording_time} > NULL && psr.exe /stop"
```

#### **Cleanup Commands:**

```
rm #{output_file} -ErrorAction Ignore
```

# Atomic Test #6 - Windows Screen Capture (CopyFromScreen)

Take a screen capture of the desktop through a call to the <u>Graphics.CopyFromScreen</u> .NET API.

**Supported Platforms:** Windows

auto\_generated\_guid: e9313014-985a-48ef-80d9-cde604ffc187

#### Inputs:

Name	Description	Туре	Default Value
output_file	Path where captured results will be placed	Path	\$env:TEMP\T1113.png

#### Attack Commands: Run with powershell!

```
Add-Type -AssemblyName System.Windows.Forms

$screen = [Windows.Forms.SystemInformation]::VirtualScreen

$bitmap = New-Object Drawing.Bitmap $screen.Width, $screen.Height

$graphic = [Drawing.Graphics]::FromImage($bitmap)

$graphic.CopyFromScreen($screen.Left, $screen.Top, 0, 0, $bitmap.Size)

$bitmap.Save("#{output_file}")
```

#### Cleanup Commands:

```
Remove-Item #{output_file} -ErrorAction Ignore
```