

> T1037.001

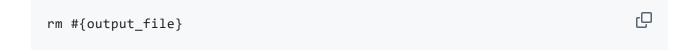
> T1037.002

> **T**1037.004

> T1037.005

> **T**1039

> T1040



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}

O

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:

Q 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

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
```