Hiding Malware in Plain Sight

gdatasoftware.com/blog/2021/06/36861-malware-hides-in-steam-profile-images

SteamHide abuses the gaming platform Steam to serve payloads for malware downloaders. Malware operators can also update already infected machines by adding new profile images to Steam. The developers seem to have a few more ambitious goals.

Suspicious steam profile images

Researcher @miltinhoc tweeted in May 2021 about new malware[1][2] that uses Steam profile images to hide itself inside them.

The low quality image (see picture below) shows three frames of the "white guy blinking" meme alongside the words January, a black screen, and September. The image content itself does not seem to make sense.

Common online EXIF tools don't show anything interesting about the image except for a warning that the length of the ICC profile data is not valid. That's because instead of an ICC profile the malware is placed in encrypted form inside the **PropertyTagICCProfile** value. The ICC profile's purpose is to map colors correctly for output devices like printers.


January
September

Here's the full data:

ExifTool

Warning	Bad length ICC_Profile (length 2986051446)

JFIF

JFIF Version	1.02
Resolution Unit	inches
X Resolution	0
Y Resolution	0

File — basic information derived from the file.

File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Encoding Process	Progressive DCT, Huffman coding
Bits Per Sample	8
Color Components	3
File Size	119 kB
Image Size	1,064 × 1,324
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

Implications and Affected Users

While hiding malware in an image file's metadata is not a new phenomenon, using a gaming platform such as Steam is previously unheard of. From attacker's point of view, this approach makes sense: Replacing the malware is as easy as just replacing a profile image file. There is also a huge number of legitimate accounts - and blocklisting the Steam platform outright would have many undesired side effects.

It should be noted that in order to become a target for this method, no installation of Steam - or any other game platform - is required. The Steam platform merely serves as a vehicle which hosts the malicious file. The heavy lifting in the shape of downloading, unpacking and executing the malicious payload is handled by an external component which just accesses the profile image on one Steam profile. This payload can be distributed by the usual means, from crafted emails to compromised websites.

The Steam profile image is neither infectious nor executable. It serves as carrier for the actual malware[2]. It needs a second malware[1] to be extracted. This second malware sample[1] is a downloader. It has the hardcoded password "**{PjID\\bzxS#;8@\\x.3JT&<4^MsTqE0**" and uses TripleDES to decrypt the payload from the image.

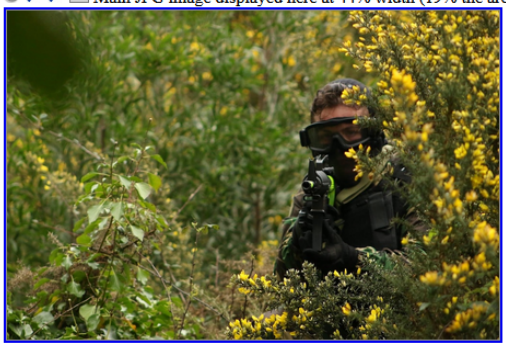
I found newer samples[3][4] of this malware via Virustotal retrohunt. The downloader uses a different Steam profile but the very same technique to hide malware in images. Below is the output of another online EXIF extraction tool.

Basic Image Information

Target file: camper.jpg

File:	**1,024** × **683** JPEG 217,626 bytes (213 kilobytes)
Color Encoding:	**WARNING:** Embedded color profile: "**(unrecognized embedded color profile 'c2')**" Some popular web browsers ignore embedded color profiles, meaning users of those browsers see the wrong colors for this image. Images for the web are most widely viewable when in the sRGB color space and with an embedded color profile. See my Introduction to Digital-Image Color Spaces for more information.

Main JPG image displayed here at 44% width (19% the area of the original)



Click image to isolate; click this text to show histogram

Payload Functionality

The sample first queries Win32_DiskDrive for VMWare and VBox and terminates if any of those exist.

It will then check if it has administrator rights and attempt privilege escalation via cmstp.exe

On the first run it copies itself to the LOCALAPPDATA folder using the name and extension specified in the configuration. In sample[2] the filename is **uNoFGmsEX.txt**

SteamHide persists itself by creating the following key in the registry:
\Software\Microsoft\Windows\CurrentVersion\Run**BroMal**

The mutex is named Global\<GUID> were GUID is the globally unique identifier for a certain class in the malware.

SteamHides initial command-and-control server IP is saved in a specific pastebin paste.

The malware can update itself via a given Steam profile. Just like the downloader it will extract the executable from the **PropertyTagICCProfile** data in an image of the Steam profile. The configuration allows to change the ID for the image property and the search string to find the correct image on Steam. That means other image properties might be used in the future to hide malware on Steam.

The future of SteamHide

SteamHide currently lacks functionality and seems to be in active development. There are a few code segments in the binary that aren't used by now.

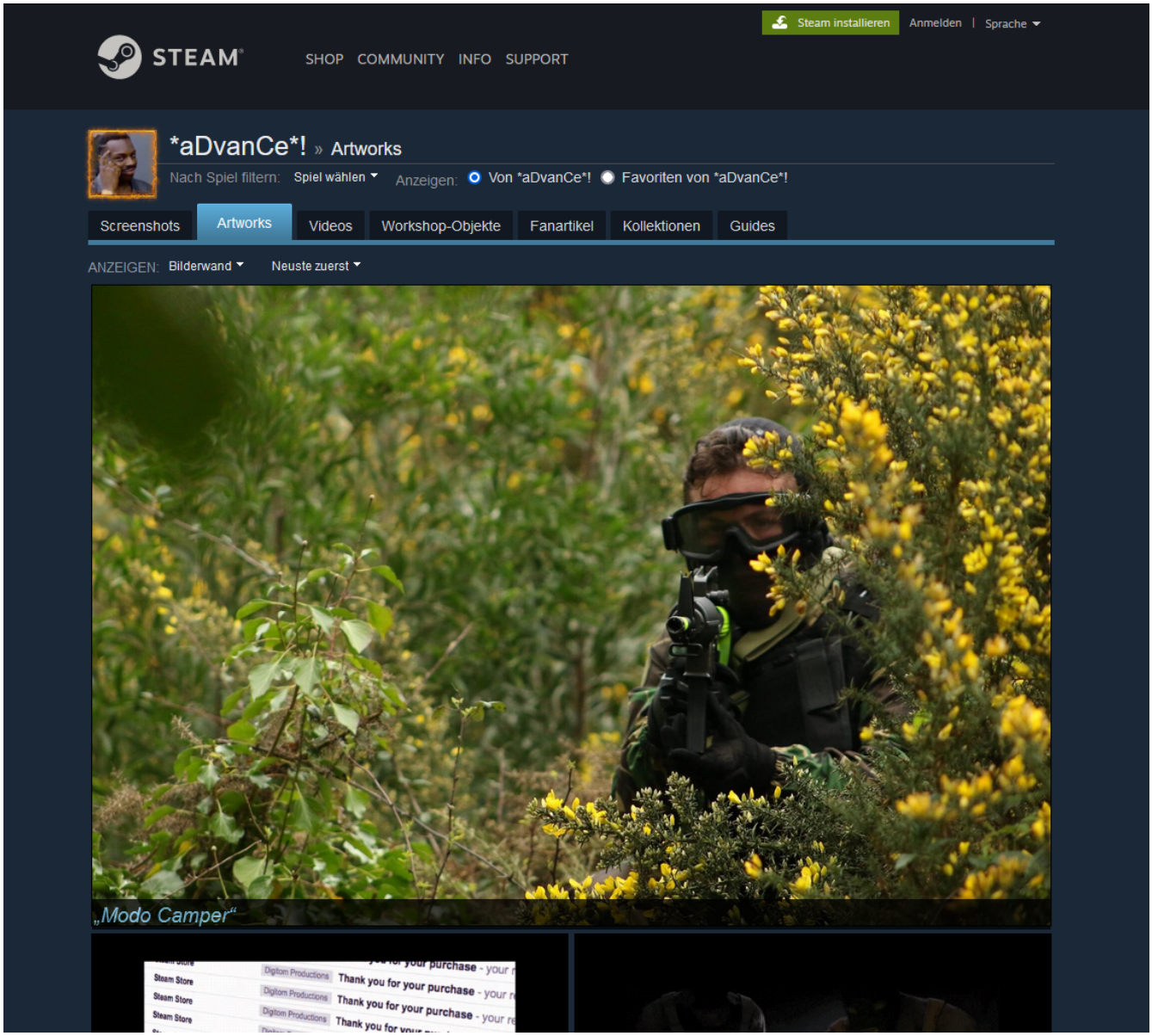
The malware checks if Teams is installed by looking for the existance of SquirrelTemp**SquirrelSetup.log,** but there isn't anything done with this information. The method is called **EnumerateVulnerable** and possibly serves to check installed applications on the infected system, so they can be abused for exploits.

There is a method stub named **ChangeHash()**, but it is not implemented yet. It seems the malware developer plans to include polymorphism in future versions.

It has a **CodePieceManager**, which can compile source code to MSIL assemblies. It might be used to add functionality on the fly or to apply metamorphism.

Futhermore there is a method that allows sending Twitter requests, which might in the future enable the malware to either receive commands via Twitter or to act as a Twitter bot.

I am confident that we will see this malware emerge soon in the wild just like it happened with other in-development families that we covered, e.g., StrRAT, SectopRAT



Steam profile containing images with SteamHide malware

Hash listing

Description	Filename	SHA256
[1] Steam profile downloader, downloads [2]	Hide binary inside image.exe	148914b6c64c51130a42159e4100e6eb670852901418d88c1c0383bf0cd1e339
[2] SteamHide backdoor	FinalMalware.exe	b41868a6a32a7e1167f4e76e2f3cf565b6c0875924f9d809d889eae9cb56a6ae

[3] Steam profile downloader, downloads [4]	Hide binary inside image.exe	368c97aef6c41b83d06c0ebb1f52679ff96a9aea35499a1caa8c3115cd16880b
[4] SteamHide backdoor	FinalMalware.exe	194c18dc8bc923887ff6b6f2acacd00b54890ca1c52233581c7802fd176dc056

Update: Clearing Up Some Confusion

June 14, 2021

Since this article was published, a number of users have contacted us asking whether they are at an increased risk of infection if they have Steam installed.
Therefore we would like to clarify that **Steam users are NOT at an increased risk** in this case. The Steam platform - specifically the profile pictures - are just serving as a download platform. This method of malware distribution also is **not a bug in the Steam ecosystem itself**. As mentioned in this article, the payload is hidden in the metadata of the image file in question.
Those profile pictures need to be specially crafted in order to contain malware. Even **opening such a modified image with an image viewing application will not result in an infected system**.
A profile picture that contains malware has to be deliberately placed on a profile on the Steam platform by a malicious user. The profile in question of course needs to be under the control of the malicious actor, too.
The type of payload implanted in the image file is at the discretion of the actor.
This may consist of any type of malware. **The malware is inactive unless it is unpacked and decrypted by a separate malware downloader that accesses the image file.** The downloader may be hidden in email attachments or on a manipulated website. **Those do not necessarily have any association with Steam or gaming in general.**

Hosting malicious file on a third party platform is a common practice among malware authors. Typically, compromised web servers are abused for this.
Other than abusing the Steam platform for hosting the malicious file, there is nothing worth noting about the implanted malware itself.

It should also be pointed out that so far, **this method appears to be under developmentand has not yet seen active use** on a broader scale.

Karsten Hahn
Malware Analyst