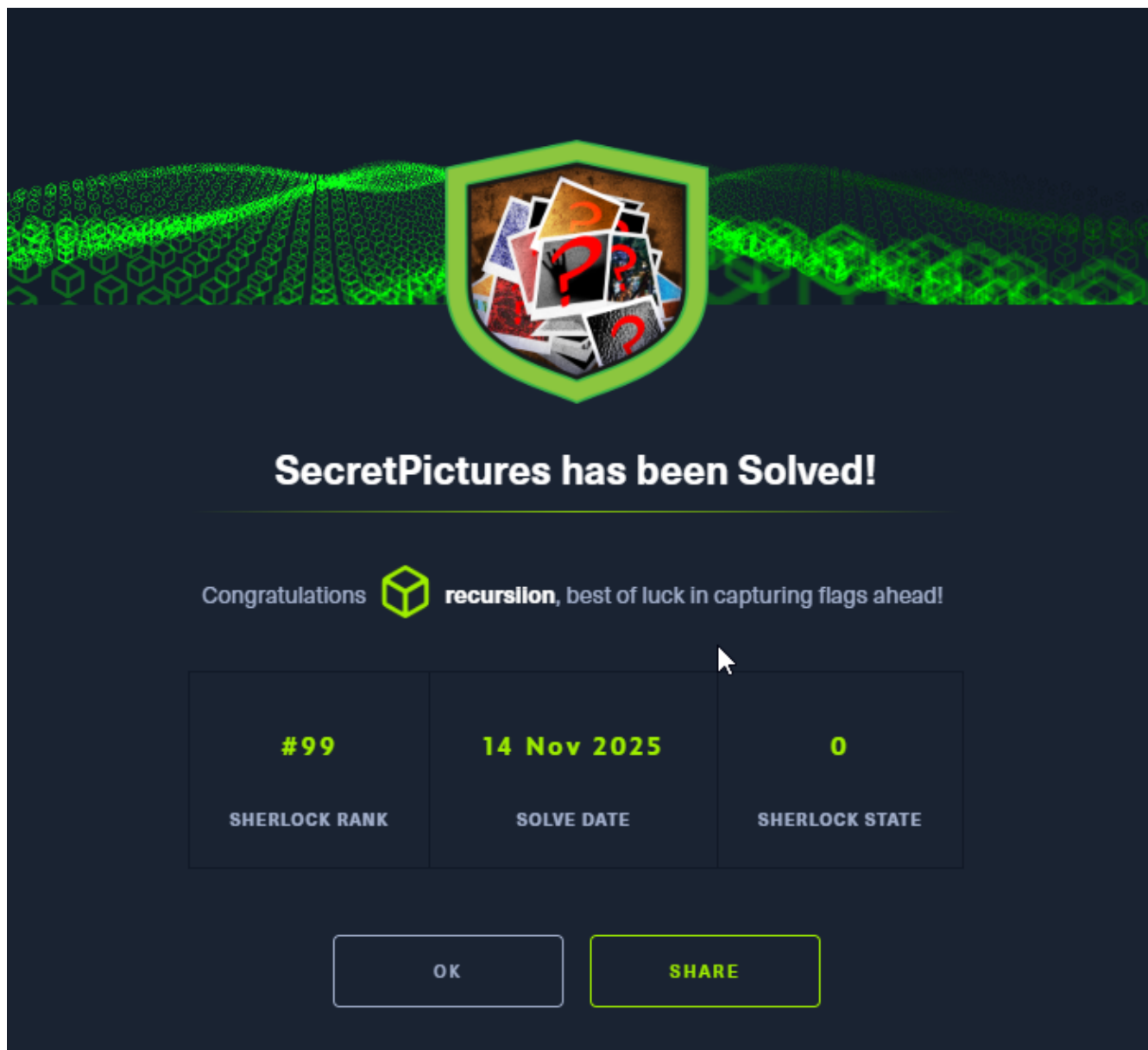


# SecretPictures - HackTheBox Sherlock

## "Easy"



## Overview

This writeup details the analysis of SecretPictures, a Go-based malware that spreads via USB drives, establishes persistence through registry modifications, and communicates with a command-and-control server to exfiltrate system information and credentials.

# Sherlock - Secret Pictures

| Header 1    | Header 2         |
|-------------|------------------|
| Category    | Malware Analysis |
| Rating      | 5 ☆              |
| User Solves | 97               |

## Sherlock Scenario

The university's IT team began receiving reports of strange activity on library computers. Students noticed hidden files appearing on their USB drives and disappearing moments later. An investigation revealed a single suspicious file named "SecretPictures." When opened, it vanished instantly without leaving a trace, and no antivirus tool could identify it. The IT team isolated the file and provided it for your analysis. As a cybersecurity analyst, your task is to determine what this malware does, how it spreads, and how to stop it before it affects more systems.

## Lab Questions

1. What is the MD5 hash of the malware?
2. What programming language is used to write the malware?
3. What is the name of the folder the malware copies itself to after the initial run?
4. What registry key does the malware modify to achieve persistence?
5. What FQDN does the malware attempt to connect to?
6. Which Windows API function does the malware call to check drive types?
7. Which Go standard library function does the malware use to schedule periodic execution?
8. What encoding does the malware use to decode server responses?
9. The malware communicates with a backend server via a POST request. What are the names of the fields in the request body, separated by commas and listed alphabetically?

## Files Provided

```
SecretPictures.zip
└─ secretPictures.exe
```

## Analysis

Unzipping the file from the zip, we can obtain the md5hash and utilize VirusTotal to gain more information on the malware.

```
└─[x]-[user@parrot]-[~/labs/htb/sherlocks/secretpictures]
└─ $md5sum secretPictures.exe
[REDACTED] secretPictures.exe
```

via [VirusTotal](#) we can see that the file is indeed a malicious executable, which appears to be compiled in Go.

The screenshot shows the VirusTotal interface for the file `secretPictures.exe`. The file's MD5 hash is `80e82415a26ac7c0124bbaa2133192dadd51cbc5ed22b202ebb24f6dddf8c8ab`. The file size is 5.23 MB, and it was last analyzed 1 day ago. The interface indicates that 35 out of 71 security vendors flagged this file as malicious. The file is identified as a Win32 executable (PE32+) compiled with Go (1.15.0-X.XXX). The basic properties section lists various hashes (MD5, SHA-1, SHA-256, Vhash, Authentihash, Imphash, SSDEEP, TLSH) and file details (File type, Magic, TrID, DetectItEasy, Magika, File size). The history section shows the first submission on 2025-11-06 and the last submission on 2025-11-13.

| Property     | Value                                                                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MD5          | fd46d178474f32f96641f0f7bb337e                                                                                                                                          |
| SHA-1        | 8dd9495545bc121b3aa490d358da15e7590086cf                                                                                                                                |
| SHA-256      | 80e82415a26ac7c0124bbaa2133192dadd51cbc5ed22b202ebb24f6dddf8c8ab                                                                                                        |
| Vhash        | 05608665d55551d15541az2elz                                                                                                                                              |
| Authentihash | d619fc594c3ccc6ba5c2db13e66e08707196b1e1bbb1e46f32b8f06744952b2e                                                                                                        |
| Imphash      | d42595b695fc008e7c56aabd8ef6d8e                                                                                                                                         |
| SSDEEP       | 49152:025yWbYfIcKdoDA4qc2wvhkUx6woe05+EOas8GOju5ErVqILAbopG2s:0CKW8vhkSEoIac                                                                                            |
| TLSH         | T1B346A07FCD545E8C0AED235C6669253BA71BC48583523D72B60F7282FB6BD0AA79340                                                                                                 |
| File type    | Win32 EXE executable (console) x86-64, for MS Windows                                                                                                                   |
| Magic        | PE32+ executable (generic) x86-64, for MS Windows                                                                                                                       |
| TrID         | Win64 Executable (generic) (44.4%)   Win16 NE executable (generic) (21.3%)   Windows Icons Library (generic) (8.7%)   OS/2 Executable (generic) (8.5%)   Generic Win... |
| DetectItEasy | PE64   Compiler: Go (1.15.0-X.XXX)                                                                                                                                      |
| Magika       | PEBIN                                                                                                                                                                   |
| File size    | 5.23 MB (5487104 bytes)                                                                                                                                                 |

| History          | Value                   |
|------------------|-------------------------|
| First Submission | 2025-11-06 19:01:28 UTC |
| Last Submission  | 2025-11-13 18:19:13 UTC |

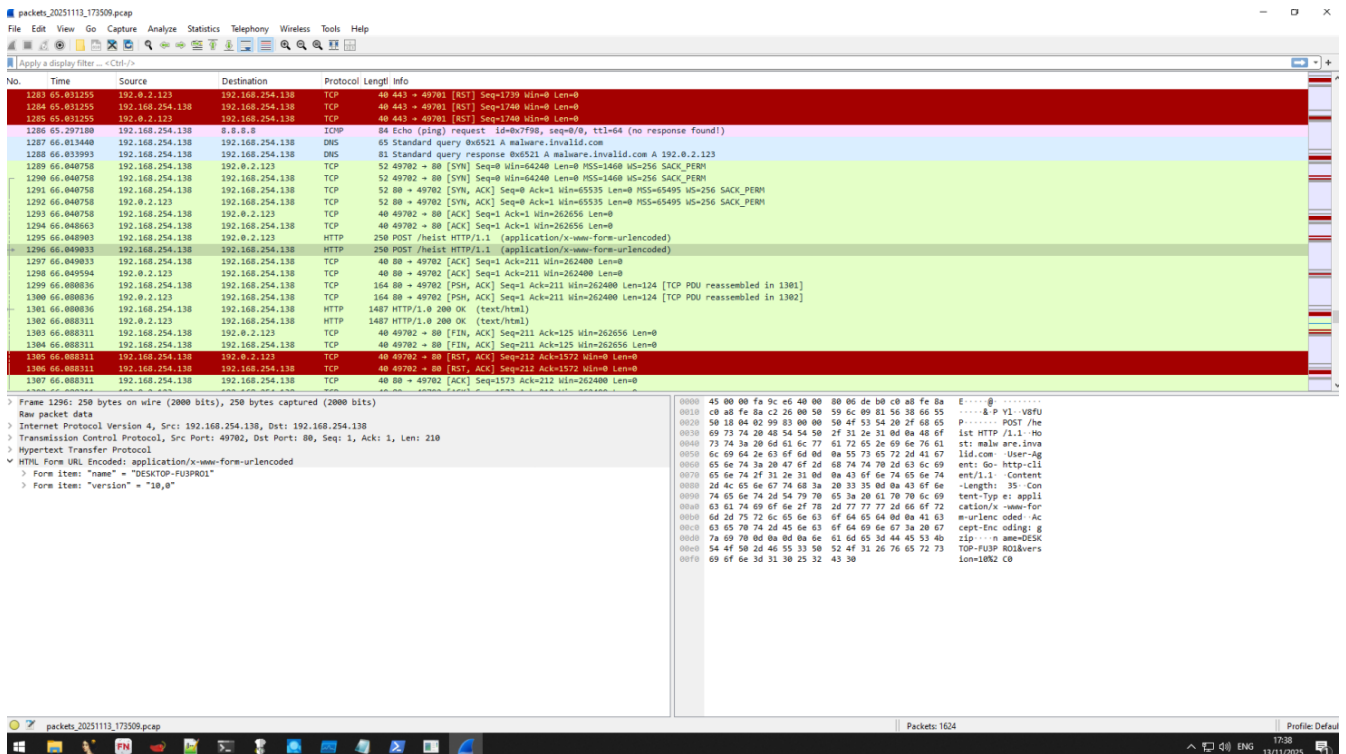
The malware copies itself after the initial run to `C:\SystemLogs\` and edits the `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\HealthCheck` registry key to achieve persistence.

The `secretpictures.exe` malware attempts a connection to `malware.invalid.com` and makes a Windows API

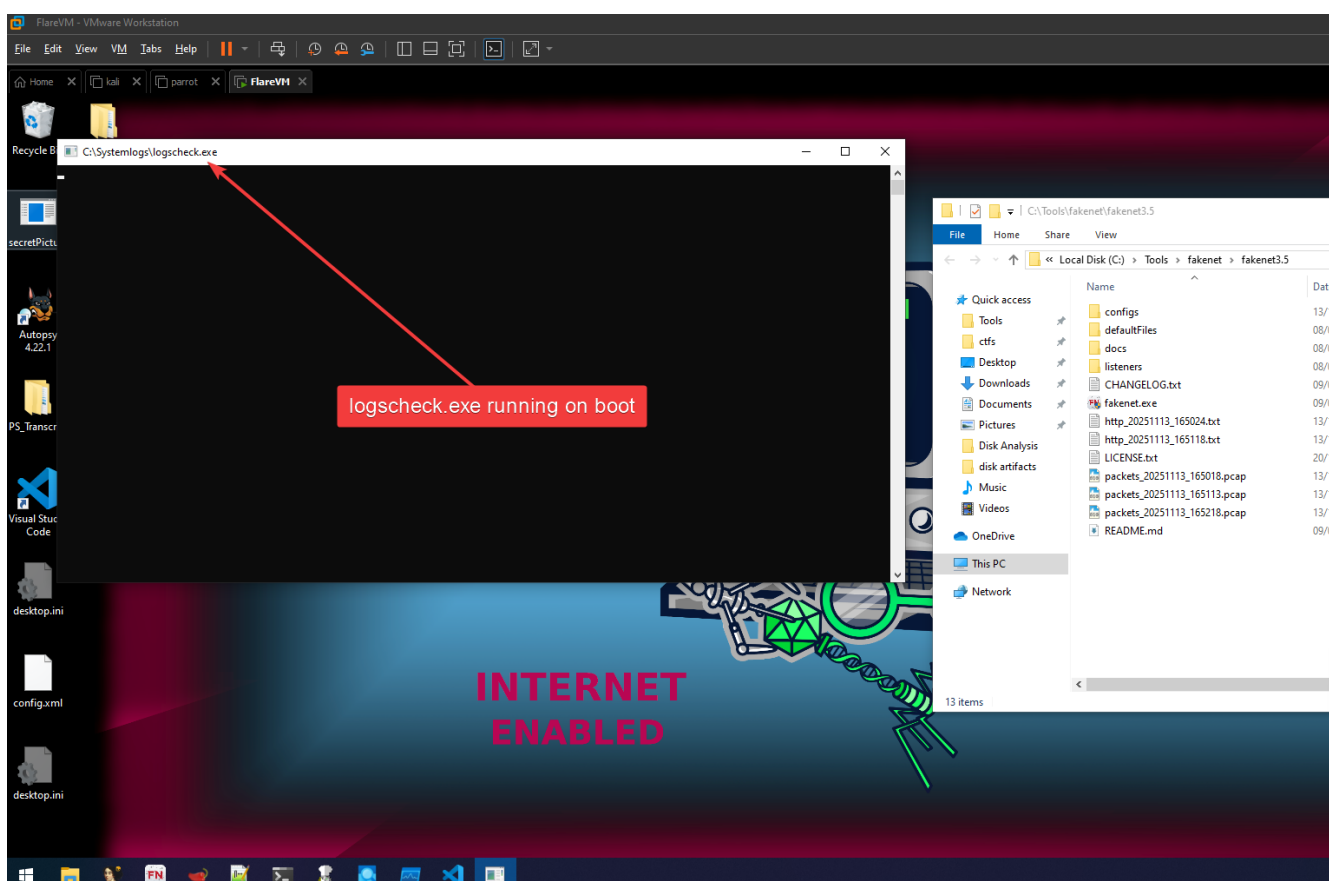
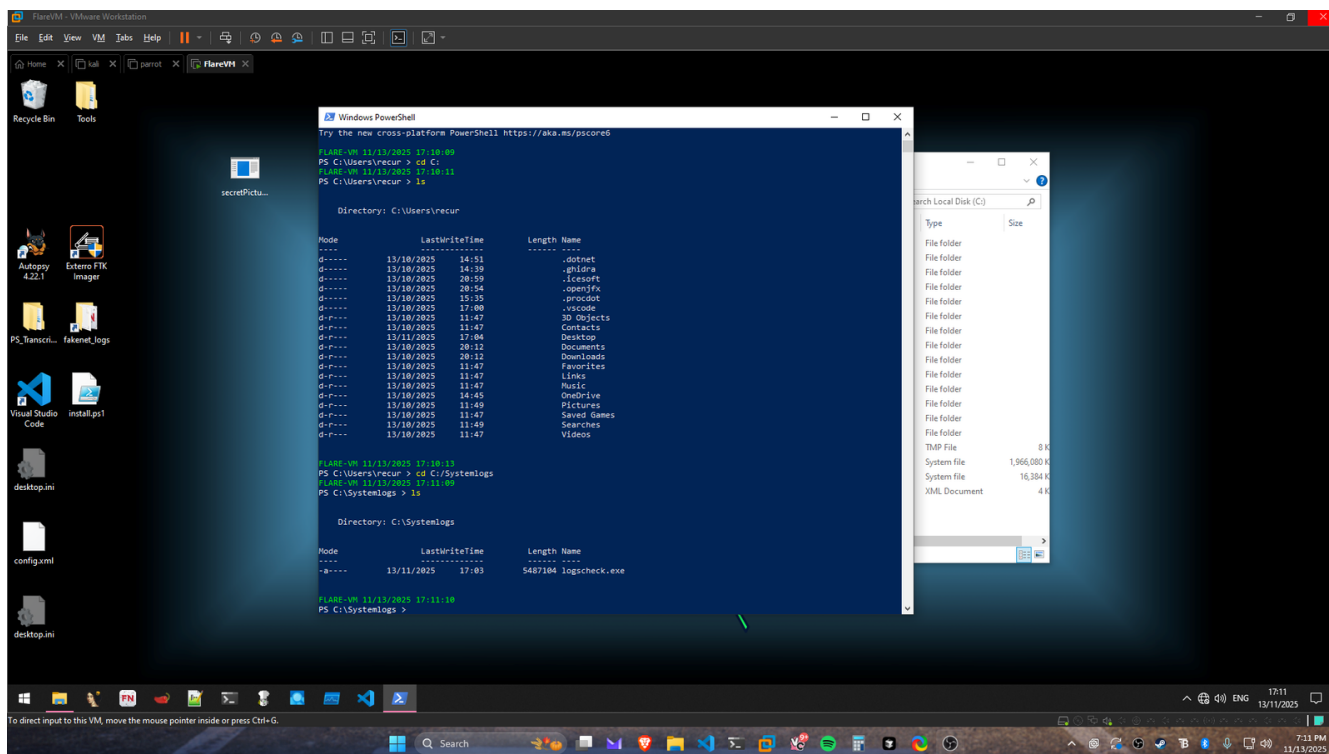
call to `GetDriveType` via PowerShell to check the drive types.

The malware utilizes the [NewTicker](#) Go library function to schedule periodic execution and decode server responses through base64.

Once the executable is run, the malware makes a POST request to `malware.invalid.com/heist` capturing the workstation name, and device version.



As mentioned previously, after the initial run of the malware, the malware reproduces itself into `C:\SystemLogs\` and runs on boot via the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\HealtCheck` edited.



There was also some POST requests of credentials being uploaded, and based on the data in the request, it looks to be credentials added onto the workstation for a new user is my assumption, possibly to elevate privileges or move laterally.

## Closing Thoughts

This was a lot of fun, being able to gain intel on the malware through VirusTotal and then go straight into Malware Analysis for the last flag was very fun, I got stuck on the last flag, and was able to use fakenet-NG to simulate legitimate network services while intercepting all network traffic and logging it.



**hunts.dev**

Originally published on hunts.dev

<https://hunts.dev/blog/secretpictures/>