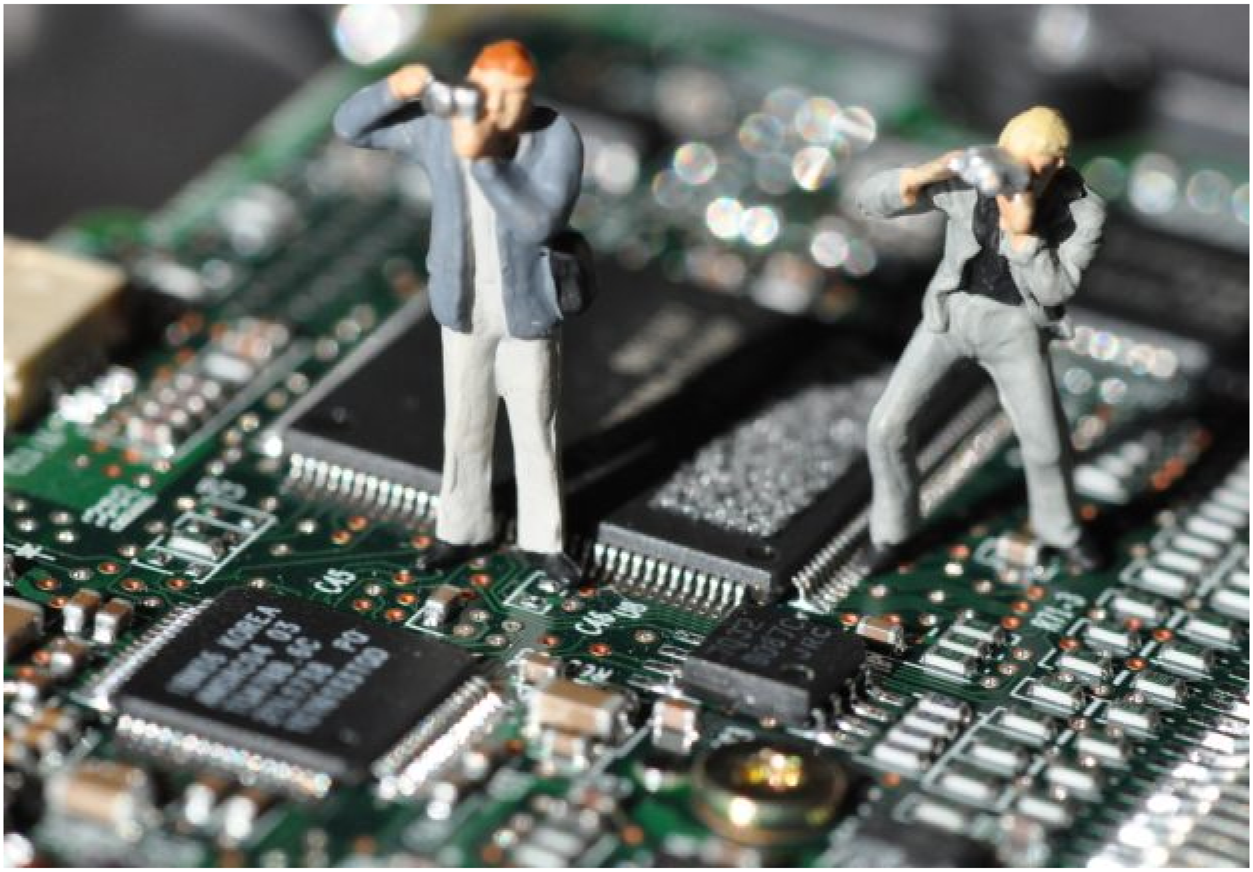
StrongPity2 spyware replaces FinFisher in MitM campaign – ISP involved?

welivesecurity.com/2017/12/08/strongpity-like-spyware-replaces-finfisher/

December 8, 2017



As we reported in September, in campaigns we detected in two different countries, man-in-the-middle attacks had been used to spread FinFisher, with the "man" in both cases most likely operating at the ISP level.

Filip Kafka
8 Dec 2017 - 02:58PM

As we reported in September, in campaigns we detected in two different countries, man-in-the-middle attacks had been used to spread FinFisher, with the “man” in both cases most likely operating at the ISP level.

Continuing our research into FinFisher – the infamous spyware known also as FinSpy and sold to governments and their agencies worldwide – we noticed that the FinFisher malware in our previously-documented campaign, which had strong indicators of internet service provider (ISP) involvement, had been replaced by different spyware. Detected by ESET as Win32/StrongPity2, this spyware notably resembles one that was attributed to the group called StrongPity. As well as detecting and blocking this threat, all ESET products – including the free ESET Online Scanner – thoroughly clean systems compromised by StrongPity2.

As we reported in September, in campaigns we detected in two different countries, Man-in-the-Middle (MitM) attacks had been used to spread FinFisher, with the “man” in both cases most likely operating at the ISP level. According to our telemetry, those campaigns were terminated on 21 September 2017 – the very day we published our research.

On 8 October 2017, the same campaign resurfaced in one of those two countries, using the same (and very uncommon) structure of HTTP redirects to achieve “on-the-fly” browser redirection, only this time distributing Win32/StrongPity2 instead of FinFisher. We analyzed the new spyware and immediately noticed several similarities to malware allegedly operated by the StrongPity group in the past.

The first similarity is the attack scenario – users trying to download a software installation package were being redirected to a fake website serving a trojanized version of the expected installation package. The StrongPity group was observed performing such watering hole attacks in the summer of 2016, targeting mostly Italian and Belgian users of encryption software.

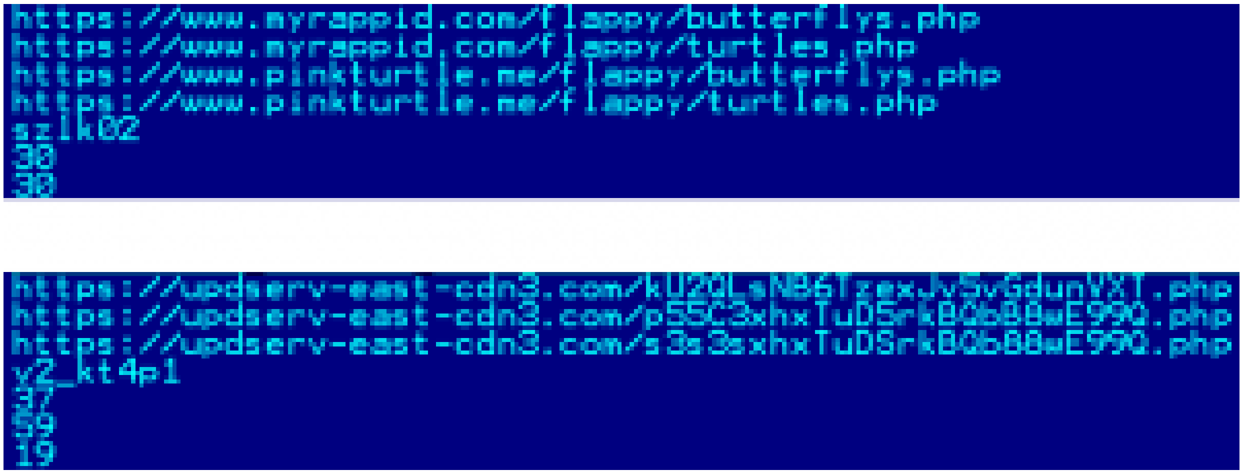
During our research, we found several different software packages trojanized with Win32/StrongPity2:

- CCleaner v 5.34
- Driver Booster
- The Opera Browser
- Skype
- The VLC Media Player v2.2.6 (32bit)
- WinRAR 5.50

Since the beginning of the campaign, our systems have recorded more than one hundred detections of this malware.

We found a number of other similarities between StrongPity-operated malware, and the way in which Win32/StrongPity2 is implemented:

- Some parts of the code are exactly the same
- The (not exactly common) structures of their configuration files share some notable similarities, as shown in Figure 1:



```
https://www.myrappid.com/flappy/butterflys.php
https://www.myrappid.com/flappy/turtles.php
https://www.pinkturtle.me/flappy/butterflys.php
https://www.pinkturtle.me/flappy/turtles.php
szlk02
30
30
```

```
https://updserv-east-cdn3.com/kU2QLsNB6TzexJvSvGdunVXT.php
https://updserv-east-cdn3.com/p55C3xhxTuD5rkBQbB8wE99Q.php
https://updserv-east-cdn3.com/s3s3sxhxTuDSrkBQbB8wE99Q.php
y2_kt4p1
37
59
19
```

Figure 1: Configuration file samples (top: StrongPity, bottom: StrongPity2)

- Both use the same obfuscation algorithm (a very uncommon Byte ^= ((Byte & 0xF0) >> 4)
- Both use the same (quite old) libcurl version 7.45
- Both exfiltrate files in the same way (the main payload handles exfiltration of files previously collected and saved by a dedicated module)

Speaking of stealing data, Win32/StrongPity2 has several file types with the following extensions in its crosshairs:

- .ppt
- .pptx
- .xls
- .xlsx
- .txt
- .doc
- .docx
- .pdf
- .rtf

While searching for these files, it avoids the following folders:

- %Windows%
- %Windows.old%
- %AppData%
- %Program Files%

- %Program Files (x86)%
- %ProgramData%

In addition to data exfiltration, Win32/StrongPity2 is able to download and execute virtually any other (malicious) software of the attacker’s choice, with the privileges held by the compromised account.

How to check your system for compromise, how to clean it and how to stay protected

To determine whether a system is infected with Win32/StrongPity2, the system can be scanned using the free ESET Online Scanner. If Win32/StrongPity2 is detected this tool is able to remove it.

It is also possible to check the system manually by verifying the existence of the folder %temp%\lang_be29c9f3-83we, which the malware creates to stores its components, with the file wmpsvn32.exe being the main one. Another easy-to-check indicator of compromise is the presence of Registry string value located in the path HKCU\Software\Microsoft\Windows\CurrentVersion\Run, named Help Manager with the string
%temp%\lang_be29c9f3-83we\wmpsvn32.exe in its data field:

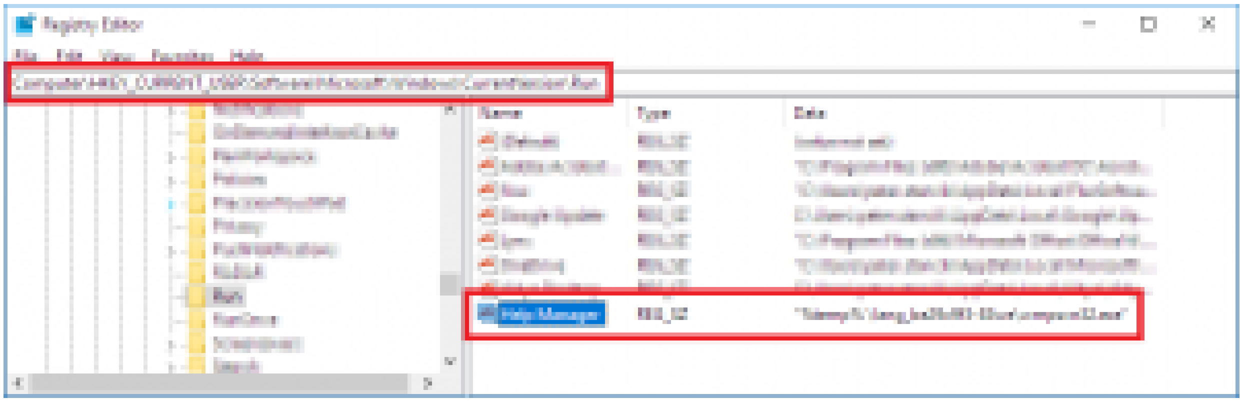

Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Run
Name
Type
Data
Help Manager
REG_SZ

Figure 2: Registry entry used by the malware to gain persistence

Manual clean-up of an infected system includes the following steps:

1. Killing the main component’s process, wmpsvn32.exe
2. Deleting the folder %temp%\lang_be29c9f3-83we and all its contents
3. Deleting the ‘Help Manager’ value in the above-mentioned Registry entry

It is important to note that for real-time, continuous protection we recommend using a reputable multi-layered internet security suite.

Special thanks to Ivan Besina for his help with the research for this article.

IoCs

Hashes of analyzed samples:
4ad3ecc01d3aa73b97f53e317e3441244cf60cbd
8b33b11991e1e94b7a1b03d6fb20541c012be0e3
49c2bcae30a537454ad0b9344b38a04a0465a0b5
e17b5e71d26b2518871c73e8b1459e85fb922814
76fc68607a608018277afa74ee09d5053623ff36
87a38a8c357f549b695541d603de30073035043d
9f2d9d2131eff6220abaf97e2acd1bbb5c66f4e0
f8009ef802a28c2e21bce76b31094ed4a16e70d6
a0437a2c8c50b8748ca3344c38bc80279779add7

Domain serving the software packages trojanized by Win32/StrongPity2

hxxps://downloading.internetdownloading.co

URLs used to exfiltrate stolen data

hxxps://updserv-east-cdn3.com/s3s3sxhxTuDSrkBQb88wE99Q.php

hxxps://updserv-east-cdn3.com/kU2QLsNB6TzexJv5vGdunVXT.php

hxxps://updserv-east-cdn3.com/p55C3xhxTuD5rkBQbB8wE99Q.php

Folder created by the malware to store its components

%temp%\lang_be29c9f3-83we

8 Dec 2017 - 02:58PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion