New FinFisher surveillance campaigns: Internet providers involved?

welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/

September 21, 2017

FinFisher has extensive spying capabilities, such as live surveillance through webcams and microphones, keylogging, and exfiltration of files. What sets FinFisher apart from other surveillance tools, however, are the controversies around its deployments.

Filip Kafka

21 Sep 2017 - 03:30PM

FinFisher has extensive spying capabilities, such as live surveillance through webcams and microphones, keylogging, and exfiltration of files. What sets FinFisher apart from other surveillance tools, however, are the controversies around its deployments.

New surveillance campaigns utilizing FinFisher, infamous spyware known also as FinSpy and sold to governments and their agencies worldwide, are in the wild. Besides featuring technical improvements, some of these variants have been using a cunning, previously-unseen infection vector with strong indicators of major internet service provider (ISP) involvement.

FinFisher has extensive spying capabilities, such as live surveillance through webcams and microphones, keylogging, and exfiltration of files. What sets FinFisher apart from other surveillance tools, however, are the controversies around its deployments. FinFisher is marketed as a law enforcement tool and is believed to have been used also by oppressive regimes.

We discovered these latest FinFisher variants in seven countries; unfortunately, we cannot name them so as not to put anyone in danger.

Infecting the targets

FinFisher campaigns are known to have used various infection mechanisms, including spearphishing, manual installations with physical access to devices, 0-day exploits, and so-called watering hole attacks – poisoning websites the targets are expected to visit (which we observed to serve a mobile version of FinFisher, for example).

What's new – and most troubling – about the new campaigns in terms of distribution is the attackers' use of a man-in-the-middle attack with the "man" in the middle most likely operating at the ISP level. We have seen this vector being used in two of the countries in which ESET systems detected the latest FinFisher spyware (in the five remaining countries, the campaigns have relied on traditional infection vectors).

When the user – the target of surveillance – is about to download one of several popular (and legitimate) applications, they are redirected to a version of that application infected with FinFisher.

The applications we have seen being misused to spread FinFisher are WhatsApp, Skype, Avast, WinRAR, VLC Player and some others. It is important to note that virtually any application could be misused in this way.

The attack starts with the user searching for one of the affected applications on legitimate websites. After the user clicks on the download link, their browser is served a modified link and thus redirected to a trojanized installation package hosted on the attacker's server.

When downloaded and executed, it installs not only the intended legitimate application, but also the FinFisher spyware bundled with it.

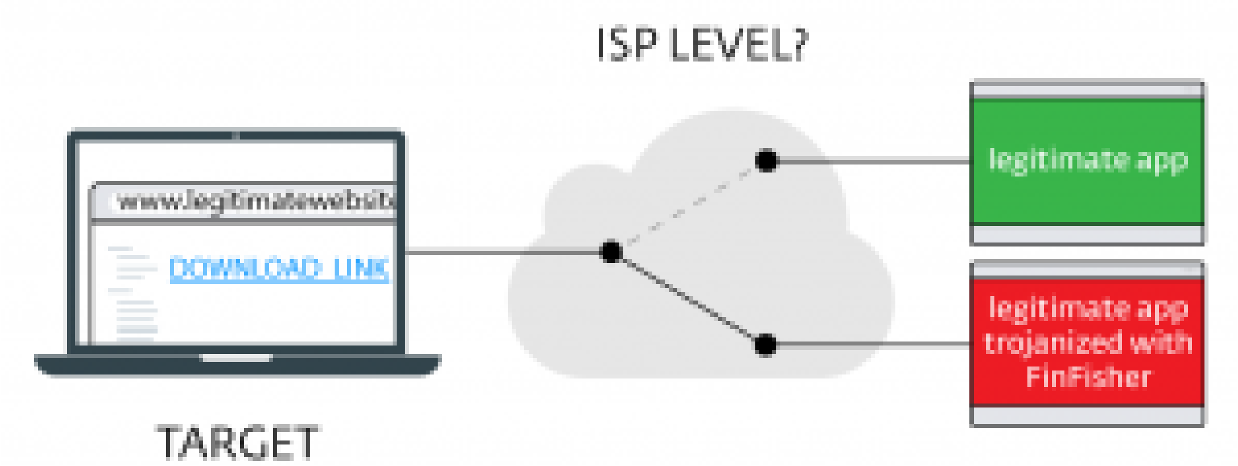

Figure 1: Infection mechanism of latest FinFisher variants

The redirection is achieved by the legitimate download link being replaced by a malicious one. The malicious link is delivered to the user’s browser via an HTTP 307 Temporary Redirect status response code indicating that the requested content has been temporarily moved to a new URL. The whole redirection process occurs without the user’s knowledge and is invisible to the naked eye.

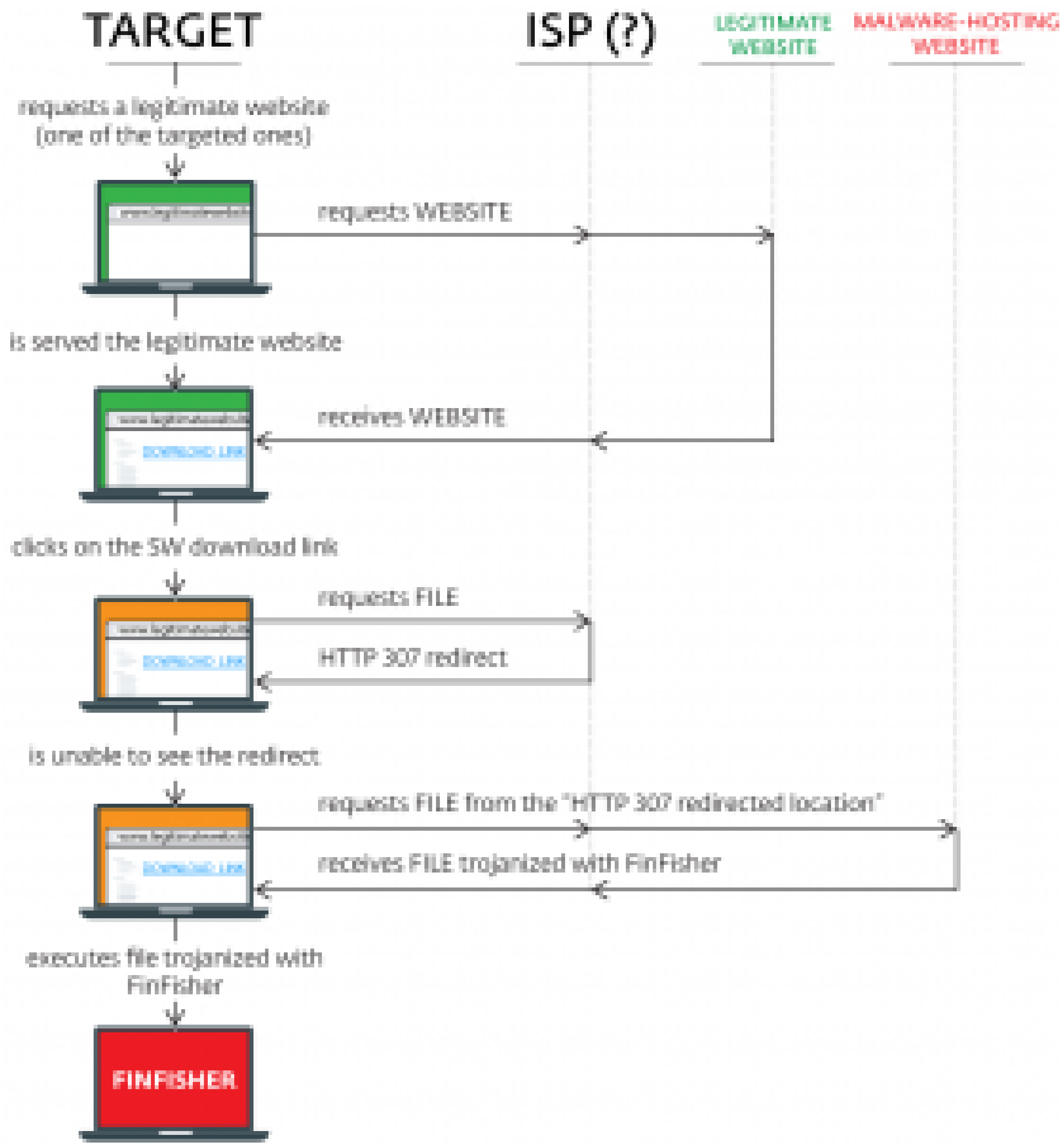
TARGET
ISP (?)
LEGITIMATE WEBSITE
MALWARE-HOSTING WEBSITE
requests a legitimate website (one of the targeted ones)
requests WEBSITE
is served the legitimate website
receives WEBSITE
DOWNLOAD LINK
clicks on the SW download link
requests FILE
HTTP 307 redirect
is unable to see the redirect
requests FILE from the "HTTP 307 redirected location"
receives FILE trojanized with FinFisher
executes file trojanized with FinFisher
FINFISHER

Figure 2: Detailed infection mechanism of latest FinFisher variants

FinFisher: All about flying under the radar

The latest version of FinFisher has also received technical improvements, its authors putting even greater focus on stealth. The spyware uses custom code virtualization to protect the majority of its components, including the kernel-mode driver. In addition, the entire code is filled with anti-disassembly tricks. We found numerous anti-sandboxing, anti-debugging, anti-virtualization and anti-emulation tricks in the spyware. All this makes the analysis more complicated.

After overcoming the first level of protection (anti-disassembly), the next level – code virtualization – awaits. The virtual machine dispatcher has 34 handlers; the spyware is executed almost entirely within an interpreter, which adds another layer to be dealt with during the analysis.

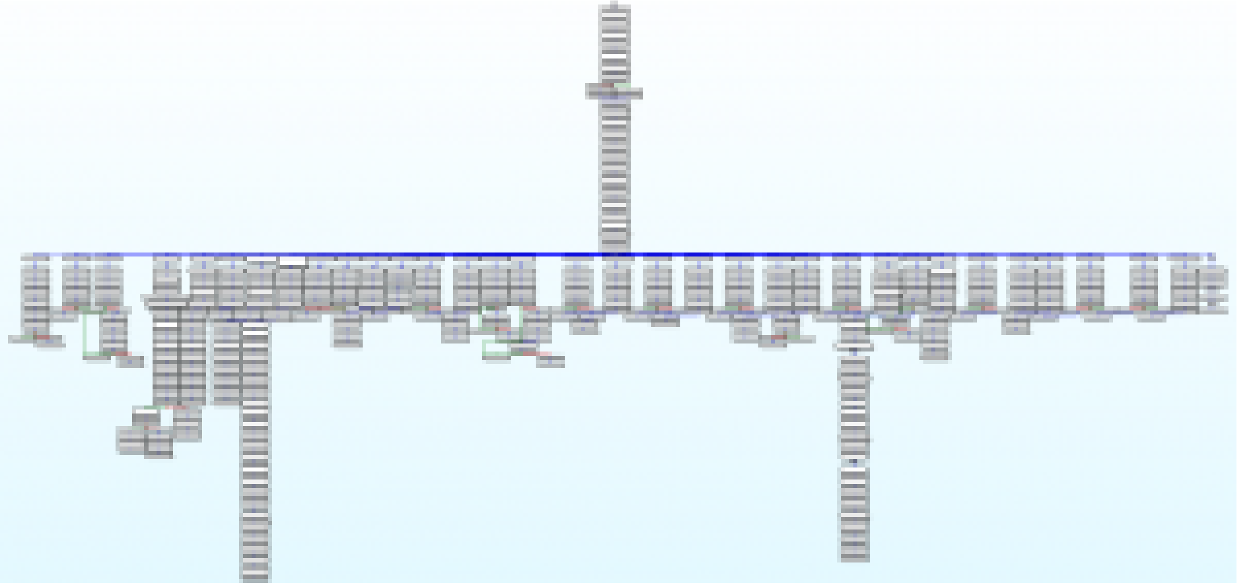

Figure 3: Visualization of the many virtual machine handlers that complicate code analysis

We have also released a whitepaper to help malware analysts and security researchers overcome FinFisher's advanced anti-disassembly and virtualization features.

Special treatment for privacy-concerned users

While analyzing the recent campaigns, we discovered an interesting sample: FinFisher spyware masqueraded as an executable file named "Threema". Such a file could be used to target privacy-concerned users, as the legitimate Threema application provides secure instant messaging with end-to-end encryption. Ironically, getting tricked into downloading and running the infected file would result in the privacy-seeking user being spied upon.

This special focus on users seeking encryption software is not limited solely to end-to-end communicators, apparently. During our research, we have also found an installation file of TrueCrypt – the once-very-popular disk encryption software – trojanized with FinFisher.

Who is the "man" in the middle?

It would be technically possible for the "man" in these man-in-the-middle attacks to be situated at various positions along the route from the target's computer to the legitimate server (e.g. compromised Wi-Fi hotspots). However, the geographical dispersion of ESET's detections of latest FinFisher variants suggests the MitM attack is happening at a higher level – an ISP arises as the most probable option.

This assumption is supported by a number of facts: First, according to leaked internal materials that have been published by WikiLeaks, the FinFisher maker offered a solution called “FinFly ISP” to be deployed on ISP networks with capabilities matching those necessary for performing such a MitM attack. Second, the infection technique (using the HTTP 307 redirect) is implemented in the very same way in both of the affected countries, which is very unlikely unless it was developed and/or provided by the same source. Third, all affected targets within a country are using the same ISP. Finally, the very same redirection method and format have been used for internet content filtering by internet service providers in at least one of the affected countries.

The deployment of the ISP-level MitM attack technique mentioned in the leaked documents has never been revealed – until now. If confirmed, these FinFisher campaigns would represent a sophisticated and stealthy surveillance project unprecedented in its combination of methods and reach.

Has my computer been infected? / Am I being spied on?

All ESET products detect and block this threat as Win32/FinSpy.AA and Win32/FinSpy.AB. Using ESET’s Free Online Scanner, you can check your computer for its presence and remove it if detected. ESET customers are protected automatically.

IoCs

ESET detection names:
Win32/FinSpy.AA
Win32/FinSpy.AB

Redirect:
HTTP/1.1 307 Temporary Redirect\r\nLocation:**URL**\r\nConnection: close\r\n\r\n

*List of **URL**’s we found during our investigation:*
hxxp://108.61.165.27/setup/TrueCrypt-7.2.rar
hxxp://download.downloading.shop/pcdownload.php?a=dad2f8ed616d2bfe2e9320a821f0ee39
hxxp://download.downloading.shop/pcdownload.php?a=84619b1b3dc8266bc8878d2478168baa
hxxp://download.downloading.shop/pcdownload.php?a=ddba855c17da36d61bcab45b042884be

IoCs
hxxp://download.downloading.shop/pcdownload.php?a=d16ef6194a95d4c8324c2e6673be7352
hxxp://download.downloading.shop/pcdownload.php?a=95207e8f706510116847d39c32415d98
hxxp://download.downloading.shop/pcdownload.php?a=43f02726664a3b30e20e39eb866fb1f8
hxxp://download.downloading.shop/pcdownload.php?a=cb858365d08ebfb029083d9e4dcf57c2
hxxp://download.downloading.shop/pcdownload.php?a=8f8383592ba080b81e45a8913a360b27
hxxp://download.downloading.shop/pcdownload.php?a=e916ba5c43e3dd6adb0d835947576123
hxxp://download.downloading.shop/pcdownload.php?a=96362220acc8190dcd5323437d513215
hxxp://download.downloading.shop/pcdownload.php?a=84162502fa8a838943bd82dc936f1459
hxxp://download.downloading.shop/pcdownload.php?a=974b73ee3c206283b6ee4e170551d1f7
hxxp://download.downloading.shop/pcdownload.php?a=cd32a3477c67defde88ce8929014573d
hxxp://download.downloading.shop/pcdownload.php?a=36a5c94ffd487ccd60c9b0db4ae822cf
hxxp://download.downloading.shop/pcdownload.php?a=0ebb764617253fab56d2dd49b0830914
hxxp://download.downloading.shop/pcdownload.php?a=f35e058c83bc0ae6e6c4dffa82f5f7e7
hxxp://download.downloading.shop/pcdownload.php?a=64f09230fd56149307b35e9665c6fe4c
hxxp://download.downloading.shop/pcdownload.php?a=b3cc01341cb00d91bcc7d2b38cedc064
hxxp://download.downloading.shop/pcdownload.php?a=5fc0440e395125bd9d4c318935a6b2b0
hxxp://download.downloading.shop/pcdownload.php?a=5ca93ad295c9bce5e083faab2e2ac97a

IoCs
hxxp://download.downloading.shop/pcdownload.php?a=f761984bb5803640aff60b9bc2e53db7
hxxp://download.downloading.shop/pcdownload.php?a=5ca93ad295c9bce5e083faab2e2ac97a
hxxp://download.downloading.shop/pcdownload.php?a=514893fa5f3f4e899d2e89e1c59096f3
hxxp://download.downloading.shop/pcdownload.php?a=a700af6b8a49f0e1a91c48508894a47c
hxxp://download.downloading.shop/pcdownload.php?a=36a5c94ffd487ccd60c9b0db4ae822cf
hxxp://download.downloading.shop/pcdownload.php?a=a700af6b8a49f0e1a91c48508894a47c
hxxp://download.downloading.shop/pcdownload.php?a=395ce676d1ebc1048004daad855fb3c4
hxxp://download.downloading.shop/pcdownload.php?a=cd32a3477c67defde88ce8929014573d
hxxp://download.downloading.shop/pcdownload.php?a=49d6d828308e99fede1f79f82df797e9
hxxp://download.downloading.shop/pcdownload.php?a=d16ef6194a95d4c8324c2e6673be7352
Samples (SHA-1)
ca08793c08b1344ca67dc339a0fb45e06bdf3e2f
417072b246af74647897978902f7d903562e0f6f
c4d1fb784fcd252d13058dbb947645a902fc8935
e3f183e67c818f4e693b69748962eecda53f7f88
d9294b86b3976ddf89b66b8051ccf98cfae2e312
a6d14b104744188f80c6c6b368b589e0bd361607
417072b246af74647897978902f7d903562e0f6f
f82d18656341793c0a6b9204a68605232f0c39e7
df76eda3c1f9005fb392a637381db39cceb2e6a8

IoCs
5f51084a4b81b40a8fcf485b0808f97ba3b0f6af
4b41f36da7e5bc1353d4077c3b7ef945ddd09130
1098ba4f3da4795f25715ce74c556e3f9dac61fc
d3c65377d39e97ab019f7f00458036ee0c7509a7
c0ad9c242c533effd50b51e94874514a5b9f2219
a16ef7d96a72a24e2a645d5e3758c7d8e6469a55
c33fe4c286845a175ee0d83db6d234fe24dd2864
cfa8fb7c9c3737a8a525562853659b1e0b4d1ba8
9fc71853d3e6ac843bd36ce9297e398507e5b2bd
66eccea3e8901f6d5151b49bca53c126f086e437
400e4f843ff93df95145554b2d574a9abf24653f
fb4a4143d4f32b0af4c2f6f59c8d91504d670b41
f326479a4aacc2aaf86b364b78ed5b1b0def1fbe
275e76fc462b865fe1af32f5f15b41a37496dd97
df4b8c4b485d916c3cadd963f91f7fa9f509723f
220a8eacd212ecc5a55d538cb964e742acf039c6
3d90630ff6c151fc2659a579de8d204d1c2f841a

21 Sep 2017 - 03:30PM

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

Newsletter

Discussion