Prince of Persia: The Sands of Foudre

By Jay Rosenberg

Published: 2018-08-17 · Archived: 2026-04-05 18:19:37 UTC

Introduction

In the past couple years, Palo Alto Networks reported on the “Prince of Persia” malware campaign which is believed to be of Iranian origin and ongoing for more than 10 years. The original research, published in 2016, called the malware Infy and their second report, published in 2017, named the upgraded malware Foudre. The name “Foudre” comes from a string in the binary used to check if the computer is already infected. At the time of their blog post, Palo Alto Networks stated the version of Foudre they observed were versions 1 and 2. We have found new evidence of the Prince of Persia campaign active by finding a new version of the Foudre malware, version 8.

In this blog post, we are only going to focus on the new, unique, interesting features of the new version of Foudre, and its related campaign

(Internal version name of Foudre v8)

No to The Forced Hijab

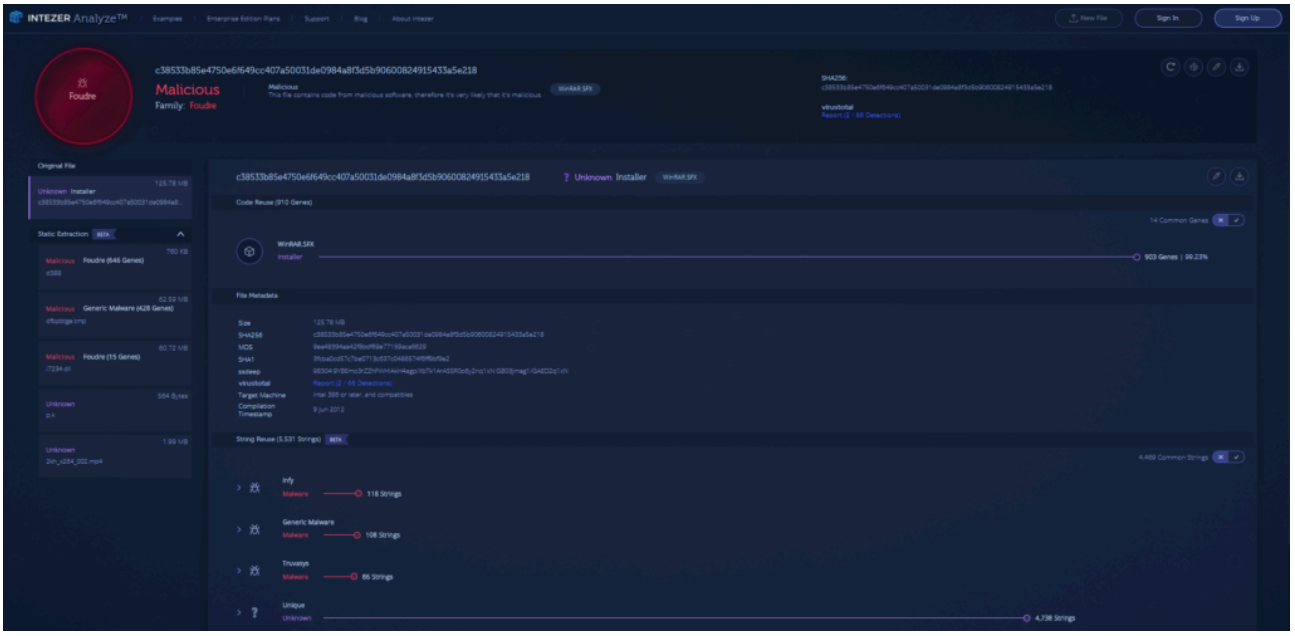
Similarly to the samples noted in previous reports, this new malware also comes packaged in a WinRAR SFX archive including multiple malicious binaries and a media file. The media file in this case is a video in the MP4 format showing a woman in Iran walking around and at the end pulling off her hijab. In the video, there is text written in Farsi with a hashtag, #بنه به حجاب اجباری, literally translating to “no to the forced hijab.” This hashtag is in reference to protesters in Iran who are protesting the mandatory use of the hijab for women and the video is meant to distract the victim while the Foudre malware gets installed in the background.

(Screenshot from the video bundled in the malware)

Foudre is a remote access tool and has the ability to remotely execute commands, steal information about the infected target (such as keystrokes, process information, etc), and auto-update itself. Most of the code and functionality from the previous versions of Foudre and Infy was reused and can be read about in the reports linked above, so we are only going to focus on the new, unique, interesting features and the linkage of code reuse from previous versions.

Code Reuse

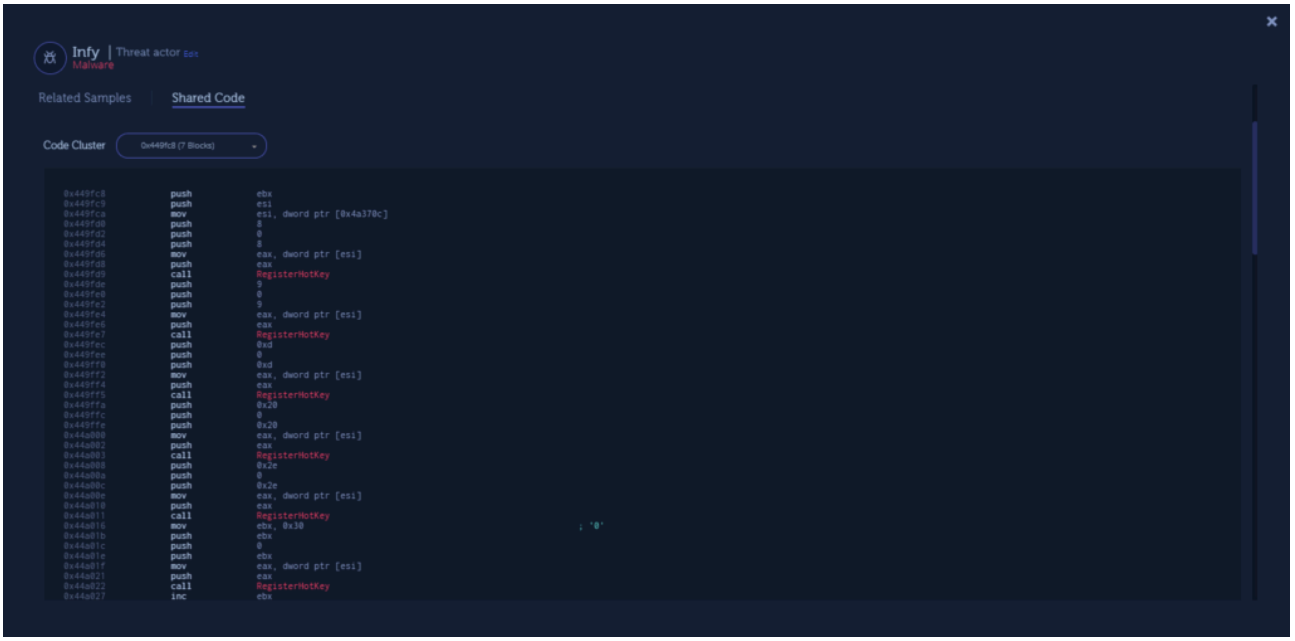
After uploading the WinRAR SFX to Intezer Analyze™, the files inside were statically extracted which reveals 3 binaries, a lockbox3 signature, and the video mentioned above.



(https://analyze.intezer.com/#/analyses/115debab-ca0a-423a-983a-c40c7d751109)

Using our new Show Code feature, we can see code overlapping with Foudre and Infy.

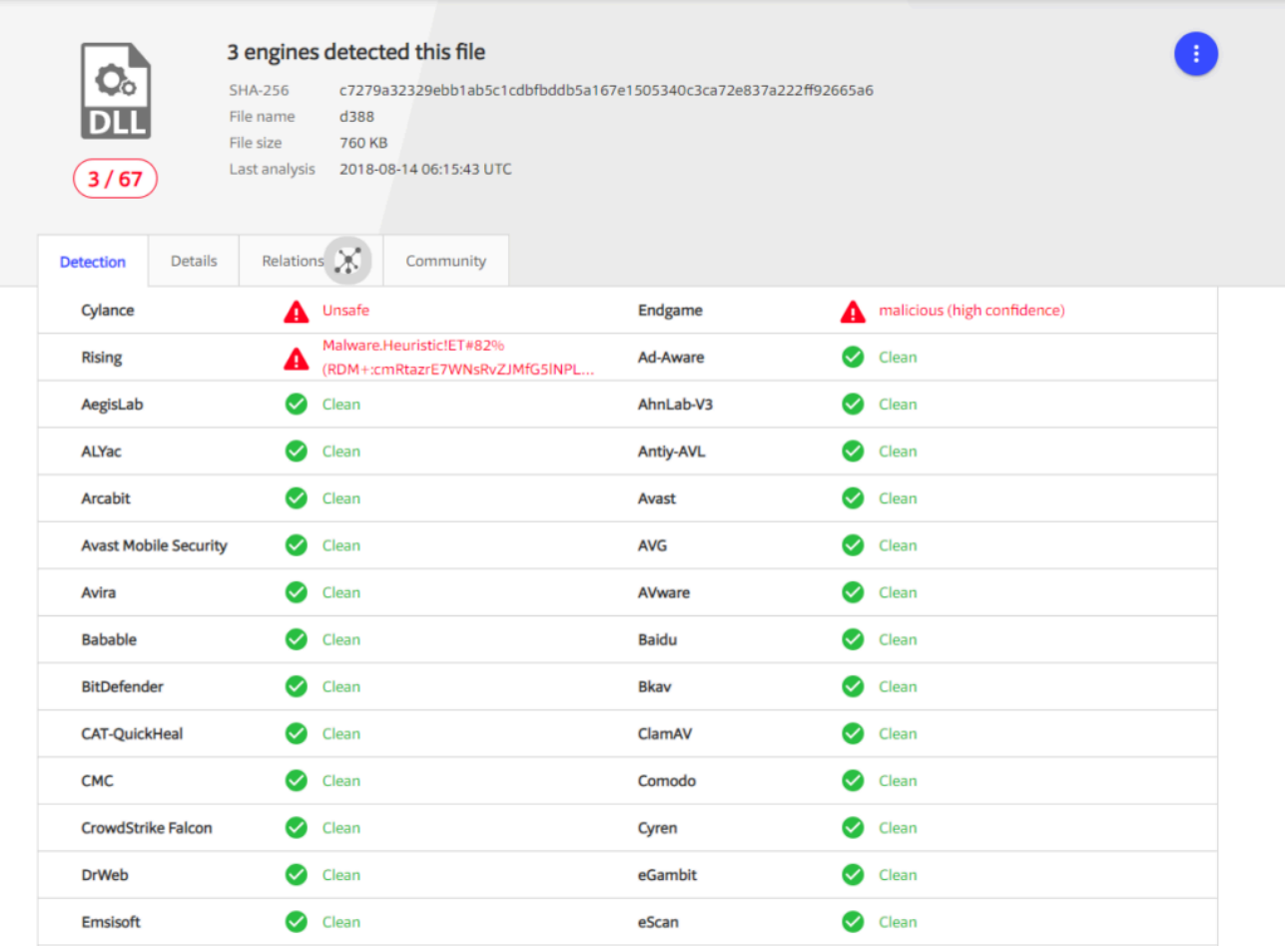
(Code overlap with Foudre)



(Code overlap with Infy)

New Features/Changes

First of all, the main binary of the upgraded Foudre malware is mostly undetected on VirusTotal with only 3/67 detections.



(VirusTotal)

In the latest version of Foudre, there are 2 modules. One of the modules (i7234.dll) has the export “D1” and the other module (d388) exports “D2” as a function. We are going to refer to the different binaries based on their exports, D1 and D2. The third binary never gets launched and is still under investigation. We will release more details about it on a further date. The WinRAR SFX and D1 module only get executed once. The following features/changes are spread across the WinRAR SFX, D1, and D2:

WinRAR SFX Dropper

1. WinRAR SFX has icon of girl with hijab from video
2. Extracts files
3. Launches D1 (i7234.dll) with rundll32 and executes export D1

D1

1. D1 executes the mp4 file
2. Checks if finds a window “TNRRDPKE2” means it’s already running
3. Copies D2 and key to %APPDATA% with filenames a.n and p.k and creates a shortcut in the folder named “an.lnk” C:WINDOWSsystem32rundll32.exe a.n D2 838238125
4. Deletes these files from TEMP folder
5. Stores name of D2 (a.n) in HKEY_CURRENT_USERSoftwaretemp in key called “ran2”

6. Checks HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun for SnailDriver
7. Creates autorun for an.lnk
8. Checks for %PROGRAMFILES%Kaspersky Lab
9. Launches D2 with rundll32 “C:WINDOWSsystem32rundll32.exe a.n D2 838238125”

D2 has mostly the same features as reported in the older versions of Foudre but this table shows the main changes:

Foudre	Version 2	Version 8
Browser Stealer Support	Microsoft Edge, Internet Explorer, Mozilla Firefox and, Google Chrome	Opera, Microsoft Edge, Internet Explorer, Mozilla Firefox and, Google Chrome
Domain Generation Algorithm	Yes	Yes, different (see below)
VirusTotal Detections	41/66	3/67
String Encryption	Yes	No
Already Running Detection String	TNRRDPKE	TNRRDPKE2

Domain Generation Algorithm (DGA)

The DGA used by version 8 of Foudre has only changed slightly from the previous versions.

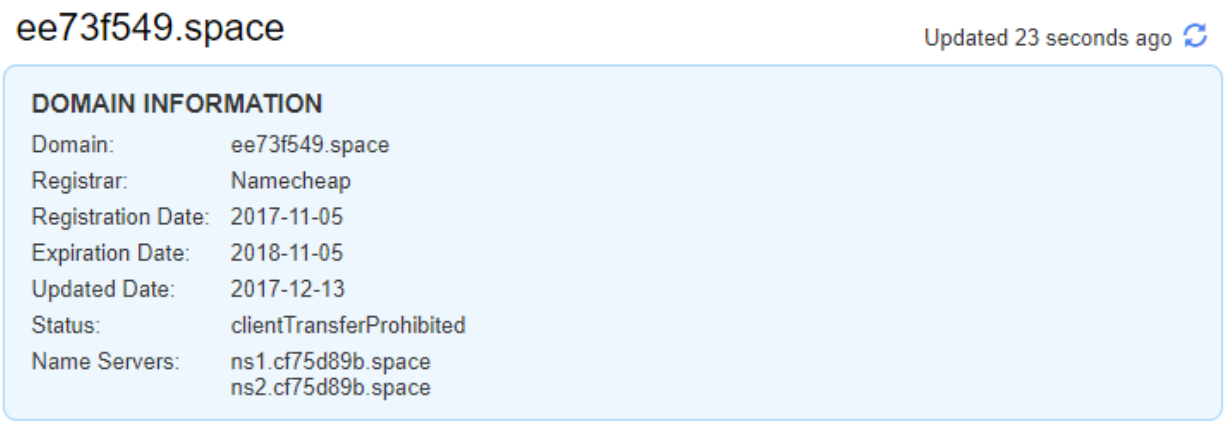
In the previous versions, the DGA algorithm was calculated by the following algorithm (credit to Esmid Idrizovic):

ToHex(CRC32(“NRV1” + year + month + week_number)) + (“.space”|”.net”|”.top”)

There are two minor differences now when calculating the C2. NRV1 was replaced with NRTV1 and .dynu.net was added as suffix to the domain making the algorithm now:

ToHex(CRC32(“NRTV1” + year + month + week_number)) + (“.space”|”.net”|”.top”|”.dynu.net”)

A few of the calculated domains were added to the bottom of the report in the IoCs section. The domains up to week of September 9, 2018 (week 35) have been registered in Panama and resolve to the same IP address 185[.]61[.]154[.]26. The oldest domain using this algorithm we could find that was registered was registered for the week of November 5, 2017.



Conclusion

Due to the content of the video and the information from the reports on previous versions of Foudre, we believe the targets are mostly Iranian citizens. We have registered some of the future generated domains to prevent the attack, and will update the post with information in regards to the infected victims.

IoCs

Files:

WinRAR SFX c38533b85e4750e6f649cc407a50031de0984a8f3d5b90600824915433a5e218

D1 DLL a02ce6768662ef250d248c158f26129dd4dfab30845d07962fbfe7aa19b16db9

D2 DLL c7279a32329ebb1ab5c1cdbfbddb5a167e1505340c3ca72e837a222ff92665a6

Unknown Binary cef161a220e019acc9ae79924a477c64aac2d6cc04126bb3f4a9f8452515f40f

MP4 dbed2ca2e9c53dd72c3ed3ce60e603c6c91c80152f924d97d8514781e6d9e26f

lockbox3 signature d2645d16e869addd099727c3c58438c2f6935d92c00f9e4b237ef498de1dad87

C&Cs:

185[.]61[.]154.26

ns1[.]cf75d89b[.]space

ns2[.]cf75d89b[.]space

Week 32 (Aug 5) – fe19f97f[.]space

Week 33 (Aug 12) – 891ec9e9[.]space

Week 34 (Sept 2) – 177a5c4a[.]space

Week 35 (Sept 9) – 607d6cdc[.]space

Week 36 (Sept 16) – f8b65751[.]space

Week 37 (Sept 23) – 8fb167c7[.]space

Week 38 (Sept 30) – 1f0e7a56[.]space

Week 39 (Oct 7) – 68094ac0[.]space

Week 40 (Oct 14) – 1d8bfc20[.]space
