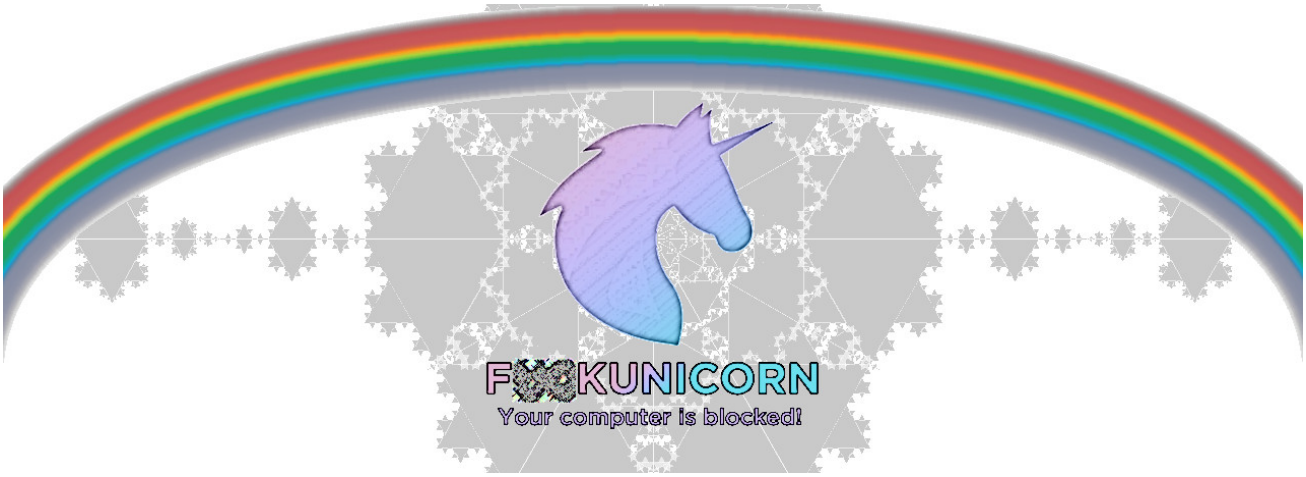
New [F]Unicorn ransomware hits Italy via fake COVID-19 infection map

bleepingcomputer.com/news/security/new-f-unicorn-ransomware-hits-italy-via-fake-covid-19-infection-map/

Ionut Ilascu

By
Ionut Ilascu

- May 26, 2020
- 12:23 PM
- 0



A new ransomware threat called [F]Unicorn has been encrypting computers in Italy by tricking victims into downloading a fake contact tracing app that promises to bring real-time updates for COVID-19 infections.

The attacker used convincing social engineering that made it look like the malicious executable was delivered by the Italian Pharmacist Federation (FOFI).

Powerful social engineering

On Monday, the Computer Emergency Response Team (CERT) from the Agency for Digital Italy (AgID) released an advisory about an indigenous ransomware threat called [F]Unicorn that spreads through the country.

It lands on the victim system under the guise of the contact tracing app Immuni for mobile devices, which the Italian government announced would be released at the end of the month.

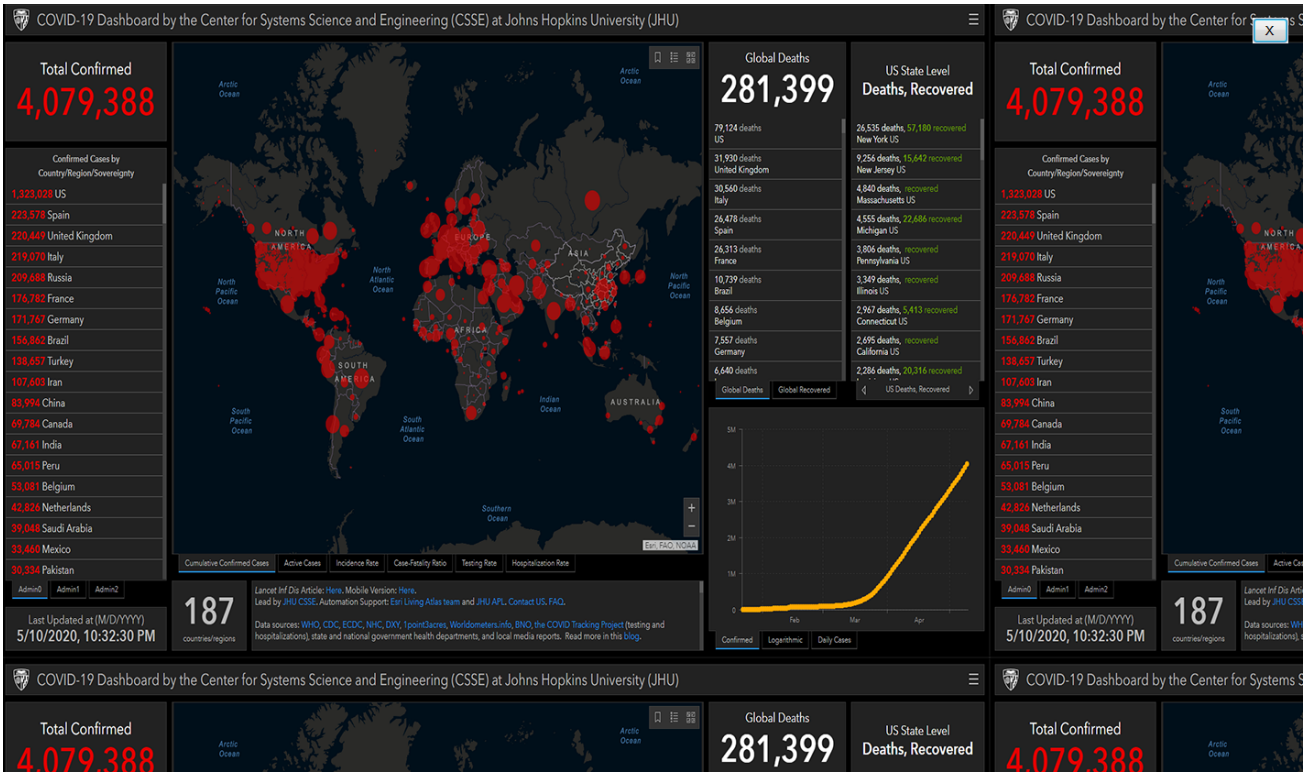
CERT-AgID received a sample of the malware from security researcher JamesWT_MHT and analyzed it along with the social engineering technique that deceive users into downloading and installing the ransomware.

Users are lured with an email in Italian informing that a beta release of Immuni for PC is available to fight the spread of COVID-19. From the text of the message, the targets are pharmacies, universities, doctors, and other entities fighting the new coronavirus contagion.

The attacker also cloned the FOFI website and registered a domain name similar to the original. However, they used “fofl.it,“ with a lowercase ”L“ as the last character that is easily confused with the lowercase ‘i’ used in the legitimate domain name.

An email sample from tech consultant Dottor Marc, shows that the message ends with download links and contact information that combines email addresses from the attacker and FOFI.

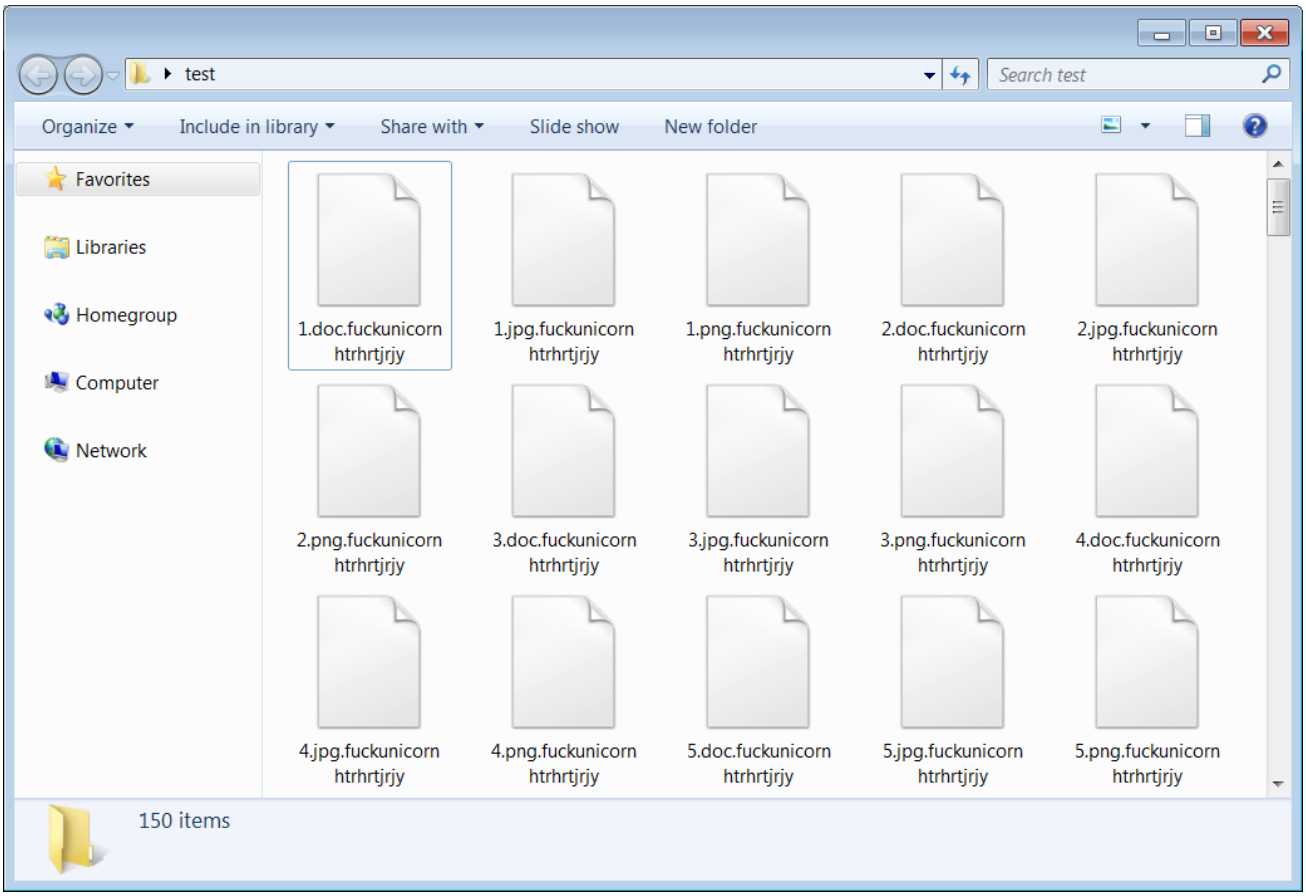
When executed, the malware shows a fake dashboard with COVID-19 information allegedly from the Center for Systems Science and Engineering at Johns Hopkins University.



While users are watching the map, the [F]Unicorn starts encrypting data on the system. According to analysis published by CERT AgID, the malware scans /Desktop, /Links, /Contacts, /Documents, /Downloads, /Pictures, /Music, /OneDrive, /Saved Games, /Favorites, /Searches, and /Videos for the following file types:

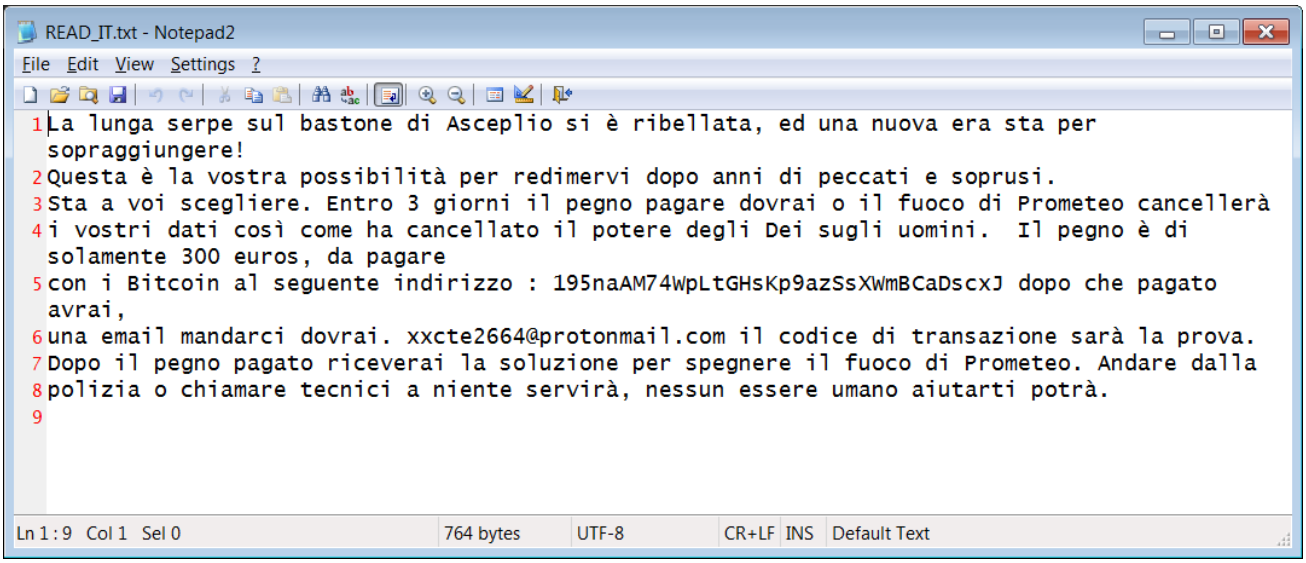
```
.Txt, .jar, .exe, .dat, .contact, .settings, .doc, .docx, .xls, .xlsx, .ppt, .pptx,
.odt, .jpg, .png, .csv,. py, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .htm, .xml,
.psd, .pdf, .dll, .c, .cs, .mp3, .mp4, .f3d, .dwg, .cpp, .zip, .rar, .mov, .rtf,
.bmp, .mkv, .avi, .apk, .lnk, .iso, .7-zip, .ace, .arj, .bz2, .cab, .gzip, .lzh,
.tar, .uue, .xz, .z, .001, .mpeg, .mp3, .mpg, .core, .crproj, .pdb, .ico, .pas ,
.db, .torrent "
```

Files encrypted with [F]Unicorn get a new extension as seen in the image below:



Users learn that their files have been locked from a ransom note written in Italian, which indicates an Italian author. The oddity of the message aside, the ransom note asks victims to pay EUR 300 in three days or the data would be lost.

A bitcoin address is provided along with an email address to contact the attacker with the proof of the payment. There are no transactions recorded for the given wallet.



Translated, the ransom note reads this:

```
The long snake on Asceplio's staff has rebelled, and a new era is about to come!
This is your chance to redeem yourself after years of sins and abuses.
It's up to you to choose. Within 3 days the pledge to pay you will have to or the
fire of Prometheus will cancel your data just as it has wiped out the power of Gods
over men. The pledge is only 300 euros, to be paid with Bitcoins at the following
address: 195naAM74WpLtGHsKp9azSsXWmBCaDscxJ after you have paid, an email to send us
you will. xxcte2664@protonmail.com the transaction code will be the proof.
After the paid pledge you will receive the solution to put out Prometheus' fire. Go
from
police or calling technicians will be of no use, no human being can help you.
```

According to CERT-AgID, the password for encrypting the files is sent in clear text to the attacker, so it can be retrieved from the network traffic logs.

Dottor Marc says that [F]Unicorn is the work of a novice attacker with little technical knowledge, who used the code from a previously seen ransomware.

Their analysis also shows that the email address in the ransom note is invalid so there is no possibility to send the attacker the payment proof. This is another reason for victims not to pay.

Security researcher MalwareHunterTeam told BleepingComputer that it is heavily based on Hidden Tear. The author made some changes here and there, one component being the panel, where CSS and HTML code was modified.

Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

- [F]Unicorn
- Coronavirus
- COVID-19
- Italy
- Ransomware

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: