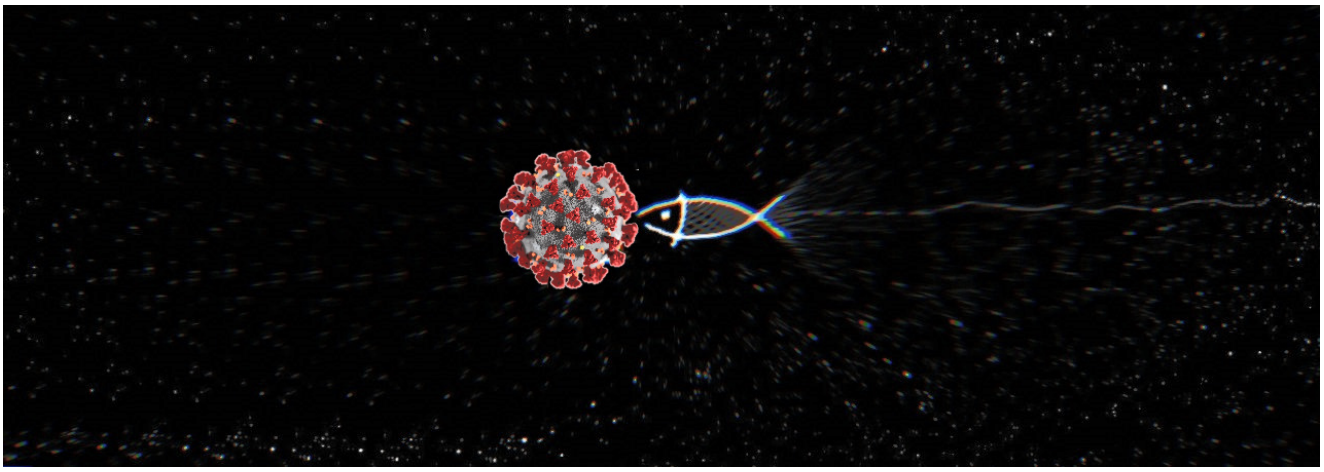
RedLine Info-Stealing Malware Spread by Folding@home Phishing

bleepingcomputer.com/news/security/redline-info-stealing-malware-spread-by-folding-home-phishing/

Lawrence Abrams

By
Lawrence Abrams

- March 19, 2020
- 11:25 AM
- 3



A new phishing email is trying to take advantage of the Coronavirus pandemic and the race to develop medications by promoting a fake Folding@home app that installs an information-stealing malware.

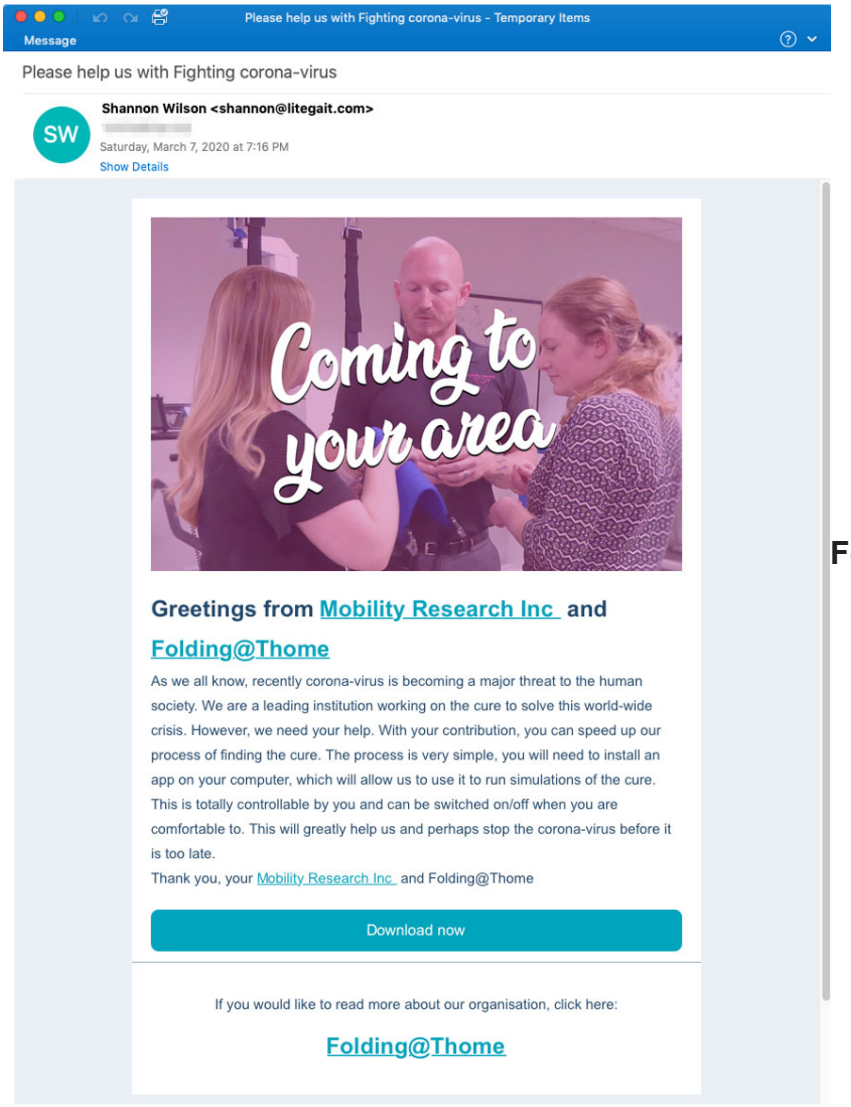
Folding@home is a well-known distributed computing project that allows users to download software that uses CPU and GPU cycles to research new drug opportunities against diseases and a greater understanding of various diseases.

As the COVID-19 epidemic spreads throughout the world, Folding@home has added over 20 new projects focusing on coronavirus research and has seen a huge increase in usage by people all over the world.

Scammers take advantage of a good thing

With the rise in popularity of Folding@home, security researchers at ProofPoint have discovered a new phishing campaign that pretends to be from a company developing a cure for Coronavirus.

These emails have a subject of "Please help us with Fighting corona-virus" and state that they want you to help "speed up our process of finding the cure" by downloading and installing the Folding@home client.



Folding@home Phishing email

Click to see full size

The text of this email reads:

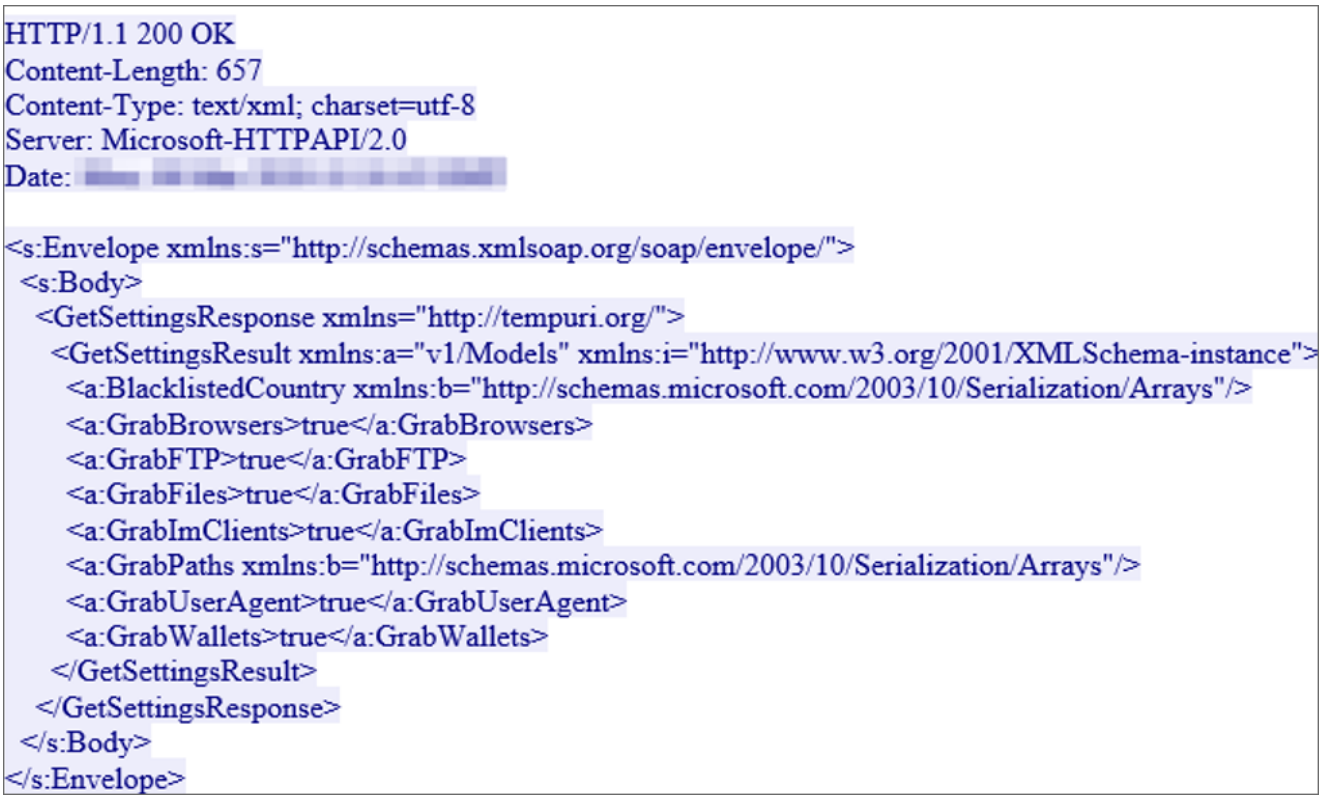
```
Greetings from Mobility Research Inc and Folding@Thome
As we all know, recently corona-virus is becoming a major threat to the human
society. We are a leading institution working on the cure to solve this world-wide
crisis. However, we need your help. With your contribution, you can speed up our
process of finding the cure. The process is very simple, you will need to install an
app on your computer, which will allow us to use it to run simulations of the cure.
```

Embedded in the phishing email is a "Download now" button that when clicked will download a file called foldingathomeapp.exe, which is the Redline information-stealing Trojan.

"RedLine Stealer is new malware available for sale on Russian underground forums with several pricing options: $150 lite version; $200 pro version; $100 / month subscription option. It steals information from browsers such as login, autocomplete, passwords, and

credit cards. It also collects information about the user and their system such as the username, their location, hardware configuration, and installed security software. A recent update to RedLine Stealer also added the ability to steal cryptocurrency cold wallets," ProofPoint states in their report.

Once installed, the malware will connect to a remote site to receive commands as to what types of data should be stolen from the victim. These instructions are sent using the SOAP messaging protocol as seen by the image below.



RedLine getting instructions

This malware can steal saved login credentials, credit cards, cookies, and autocomplete fields from browsers. It can also collect data from FTP and IM clients, steal files, download files, execute commands, and send information back about the computer.

You can see an example of this malware in action in an Any.run session performed by security researcher James.

As this malware can steal a large amount of information, anyone who has fallen victim to this scam should immediately perform a scan using antivirus software.

They should also change the passwords at any online accounts that they frequent as they may now be in the possession of the attackers. This should be done from another computer until they are sure their infected computer has been cleaned.

It should also be noted that Folding@home is a terrific project and just because people are performing scams in their name, does not mean it should be avoided.

Just be sure to download the Folding@home client only from the legitimate site.

Related Articles:

German automakers targeted in year-long malware campaign

New Meta information stealer distributed in malspam campaign

PDF smuggles Microsoft Word doc to drop Snake Keylogger malware

Eternity malware kit offers stealer, miner, worm, ransomware tools

Historic Hotel Stay, Complementary Emotet Exposure included

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.