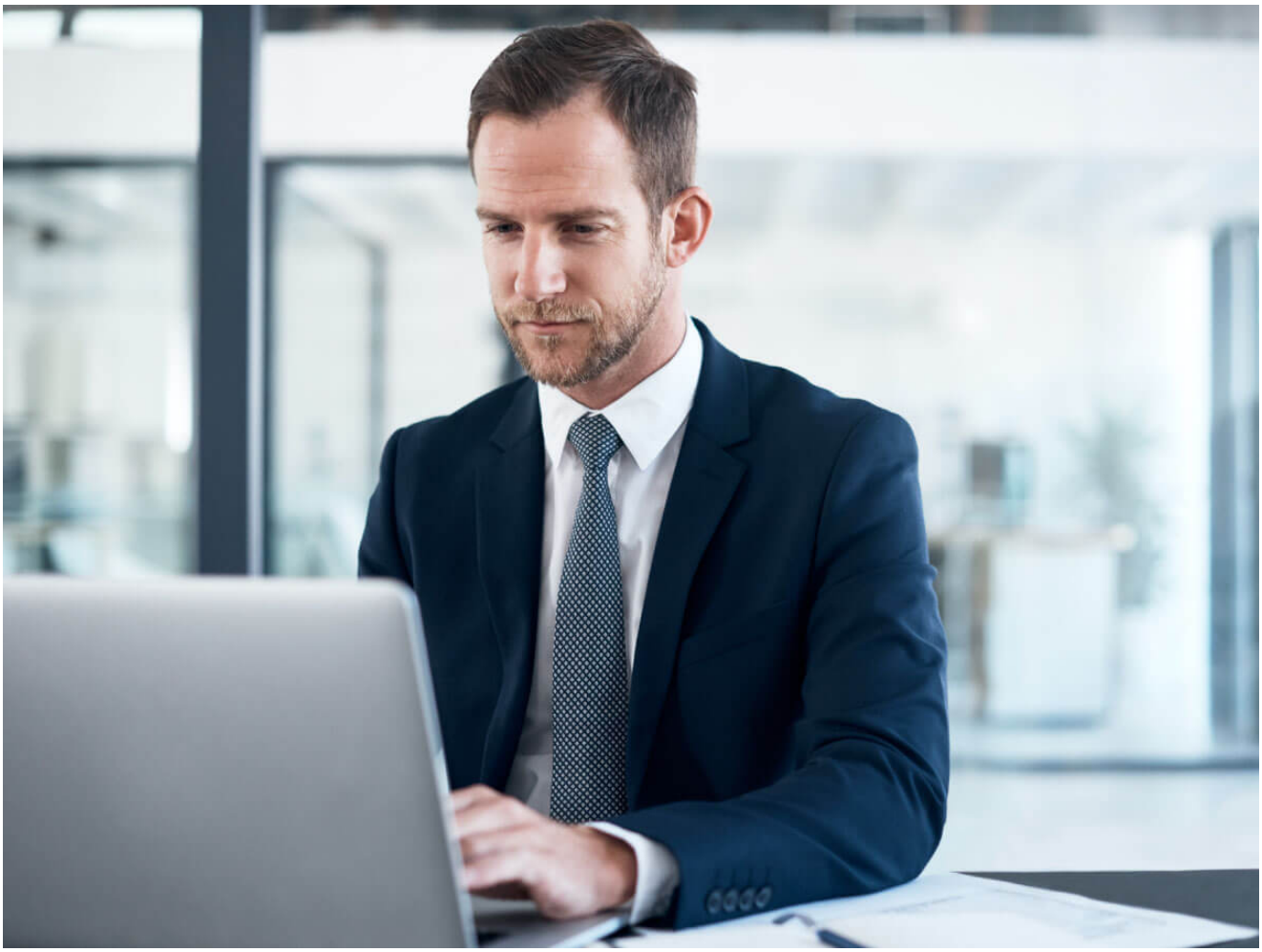
To Joke or Not to Joke: COVID-22 Brings Disaster to MBR

fortinet.com/blog/threat-research/to-joke-or-not-to-joke-covid-22-brings-disaster-to-mbr

November 11, 2021



FortiGuard Labs Threat Research Report

Affected platforms: Microsoft Windows
Impacted parties: Windows Users
Impact: Unable to boot the machine
Severity level: Medium

Even now, almost two years after the COVID-19 pandemic started, there is no sign that cybercriminals will stop taking advantage of the situation as an attack vector. This time, however, this attacker uses a COVID pandemic that has not yet happened as bait. FortiGuard Labs recently discovered a new malware posing as a mysterious COVID22 installer. While containing many of the features of "joke" malware, it is also destructive, causing infected machines to fail to boot. Because it has no features for encrypting data

demanding a ransom to undo the damage it inflicts, it is instead a new destructive malware variant designed to render affected systems inoperable. This blog explains how this malware works.

Covid-22 in Action

The malware file is named Covid22. For those unfamiliar with the naming scheme, COVID-19 is a short form of **Co**rona**v**irus**d**isease, and **19** represents the year the outbreak was first identified. The file name Covid22 plays off the current Coronavirus disease but applies that same image of fear and destruction to computers, potentially creating a cyber-pandemic in 2022. While we don't know how exactly the malware was distributed, the malware author has tried to weaponize fear as bait to lure victims into opening the file.

While the malware itself is not sophisticated, it does take several actions designed to put fear into the victim before inducing true panic. But before that, when first manually running the file, it asks whether the potential victim wants to install Covid-22 on their machine, as if it were an application.

Figure 1. Installer screen that asks the victim for permission to install

Once the victim proceeds with the installation, the malware drops several malicious files before forcefully rebooting the machine. Dropped files have file names that are simple and self-described for their actions. They are listed below in sequence of execution.

- Covid22Server.exe executes the commands in the dropped script.txt
- lol.vbs creates an endless loop of a MessageBox with "Your PC has been infected by Covid-22 Corona Virus! Enjoy the death of your pc!"

Figure 2. Image of the pop-up message “Your PC has been infected by Covid-22 Corona Virus! Enjoy the death of your pc!”

- speakwh.vbs uses the computer's speaker to say "coronavirus" in a loop
- CoronaPopup.exe displays a pop-up with the title "Covid-22 has infected your pc!" and an image of the actual coronavirus

Figure 3. Image of the virus

- ClutterScreen.exe clutters the screen by constantly moving blocks of pixels
- x.vbs displays the pop-up message, "Corona Virus!" 50 times

Figure 4. Image of the pop-up message “Corona Virus!”

noescapes.vbs displays the pop-up message "THERE IS NO ESCAPE" 10 times

Figure 5. Image of the pop-up message “THERE IS NO ESCAPE”

icons.exe fills the screen with red Xs

Figure 6. Image of the user's screen filled with red Xs

final.vbs displays a pop-up message "Bye!"

Figure 7. Image of the pop-up message "BYE!!!"

These are the classic actions of joke programs usually intended to annoy or make fun of users. But the next activity is not laughable at all. The malware drops and executes the malicious WipeMBR.exe wiper malware that destroys the Master Boot Record (MBR) by overwriting its first 512 bytes with zeros. The malware then forces a machine reboot after displaying the following pop-up message:

Figure 8. Final pop-up message before forcefully rebooting the compromised machine

Because MBR has information about the partitions of the hard drive and acts as a loader for the operating system (OS), the compromised machine will not be able to load the OS upon reboot. The good news for the users is that the malware does not destroy nor steal any files on the compromised device, meaning the victim can still recover user files from the hard drive. The malware also does not demand ransom.

While the result is almost identical to another MBR wiper that Sonicwall posted a blog about in April 2020, our analysis did not show any resemblance in their wiper codes. This newer variant simply overwrites the MBR with zeroes.

How to Repair a Damaged MBR

Fixing an MBR is relatively easy in modern Windows. After the affected machine reboots (sometimes it requires a few reboots), the system enters automatic repair mode. First, choose Advanced Options, Troubleshoot. Another Advanced Option should then let you use the Command Prompt. From the Command Prompt, type and run "bootrec.exe /fixmbr".

An alternative and more straightforward option would be to choose Startup Repair on the screen to run the Command Prompt. The downside of selecting Startup Repair is that it will take longer to complete the job.

If the automatic repair mode does not kick in for some reason, you'll need to boot the system off a recovery disk or drive. Note that you'll need to change your BIOS settings to ensure the system boots from the recovery media first, or else the system will try to boot using the overwritten MBR leading to a boot error. Once the system boots from recovery media, you should be able to choose to run the command prompt, whereby the user can run the command "bootrec.exe /fixmbr".

It is also vital to remind system administrators of the importance of backing up your data on external storage in case any of your files are ever damaged, encrypted, or destroyed. You will also want to create recovery media beforehand, or else you will need to use a working machine, which can be difficult for home users after the damage is done.

Conclusion on COVID-22 Brings Disaster to MBR

What looks to be a mere joke program is designed to bring destruction to impacted systems. This time, luck was on the victim's side as the malware did not touch any user data, but the user may not be so lucky next time. Imagine if the files on the compromised machine had been encrypted or destroyed and could not be recovered. Always be mindful of executing unknown files received from the internet.

Fortinet Protections

Fortinet customers are already protected from this malware by the FortiGuard Labs AntiVirus Service as used by FortiGate, FortiClient and FortiMail, and by FortiEDR as follows:

W32/Ursu.558C!tr
Malicious_Behavior.SB
VBS/BadJoke.8A6B!tr
VBS/BadJoke.7182!tr
VBS/BadJoke.84AB!tr
VBS/BadJoke.0C12!tr
VBS/BadJoke.DF52!tr
W32/BadJoke.DCAB!tr

FortiEDR detects the downloaded executable file as malicious based on its behavior.

IOCs

Sample SHA-256:
[Covid22.exe]
79f3b39797f0e85d9e537397a6f8966bc288d1b83ae1c313c825fbd17698879e
[ClutterScreen.exe]
726DC8D52C9CF794412941BFBD27AF8F6FA27E72154A63F5C81A42BA40BD972D
[CoronaPopup.exe]
80C9F65617386940153CC4D42E1097DEB79B4F9C98C67E6025BDC1CA03AD8FB7
[icons.exe]
496CABBD18530780A3CB75340BDDD7F74A71E84C83DF4D185CFC6EC71D14C41E
[WipeMBR.exe]
5FC9080177A096DE2B717F2F2196867B6966900E129E5BC4E412D5DCA7ED9E60
[final.vbs]
EA2EF4196586BF851D4DC422A04D51AD2CB552BF5AAE2DF361D1ED2D4842B4BA

[lol.vbs]
C88D3022B25EF86CD19CE99815AD26A1F9A201F69974577DA93E08328E047410
[noescapez.vbs]
3D519FC10BC2B6CAA5A27069DA55B1614CC97C1DFD4BCDC1DD7F36E686D913F1
[x.vbs]
E22F004CF9E7C4C7B52BDA59DB2B57816992CB01FDBEF6675760FDD7BCD29728
[speakwh.vbs]
4624876389F6DDFB111FBBF3473D7C6B5555ED8A0F31C37E822A6FFEF5E27DE0
[Covid22Server.exe]
0C6DFAA12A98FB17058B79D283E96A3E34549D0AD2BE58F505AC8ABDE858D8A6

Learn more about Fortinet's FortiGuard Labs threat research and intelligence organization and the FortiGuard Security Subscriptions and Services portfolio.

Learn more about Fortinet's free cybersecurity training, an initiative of Fortinet's Training Advancement Agenda (TAA), or about the Fortinet Network Security Expert program, Security Academy program, and Veterans program. Learn more about FortiGuard Labs global threat intelligence and research and the FortiGuard Security Subscriptions and Services portfolio.