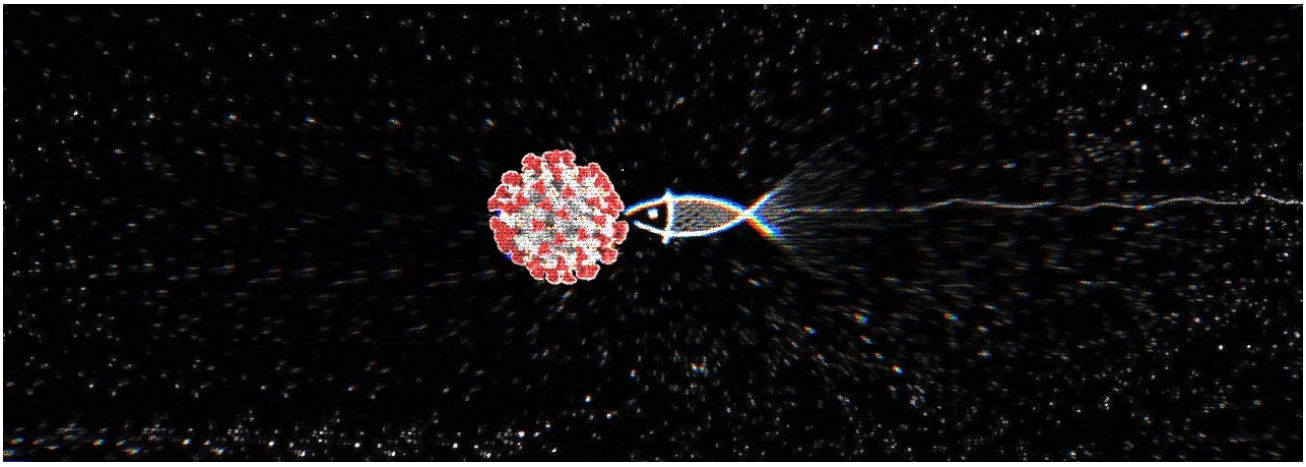
Netwalker Ransomware Infecting Users via Coronavirus Phishing

bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/

Lawrence Abrams

By
Lawrence Abrams

- March 21, 2020
- 12:06 PM
- 0

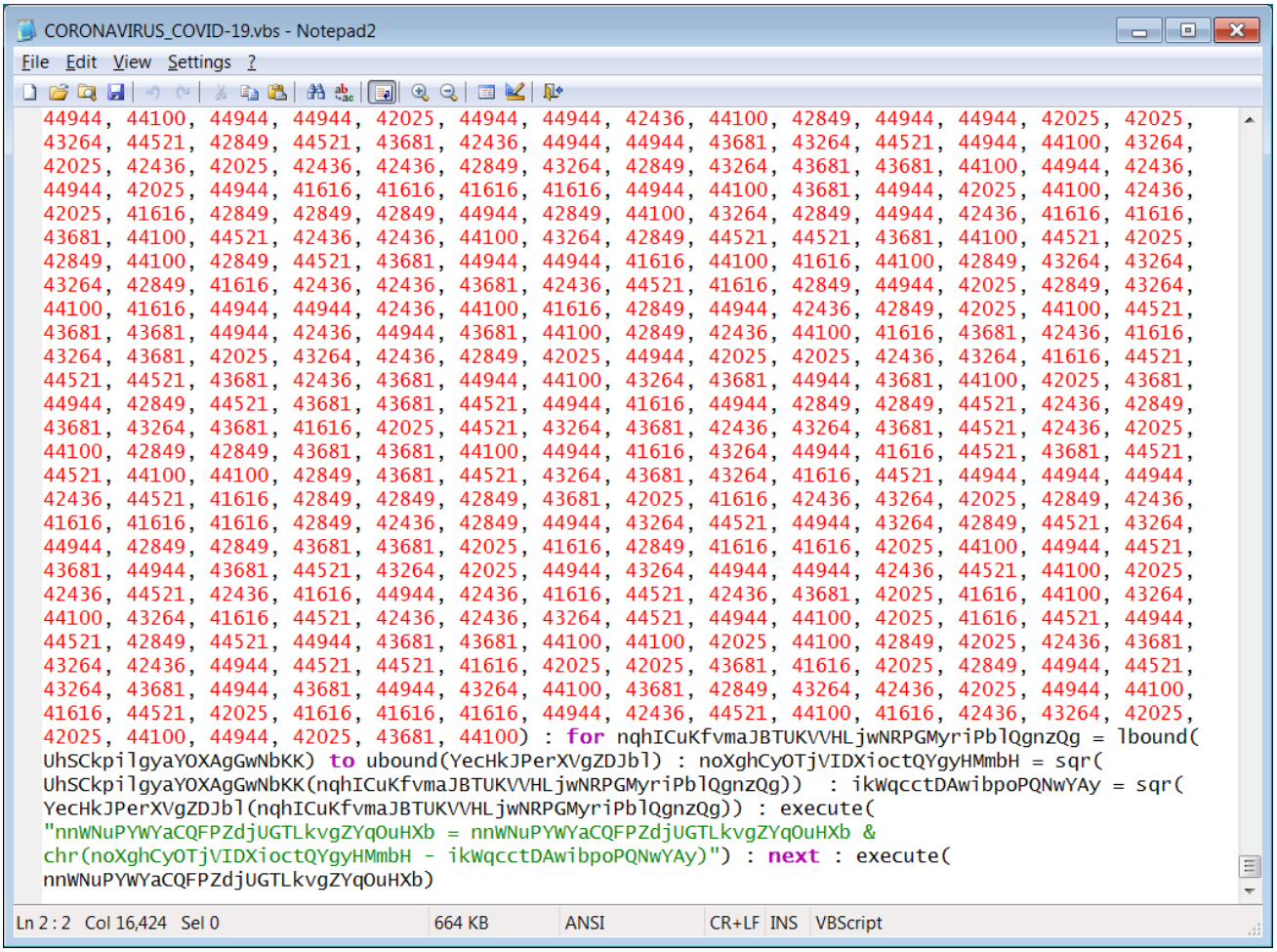


As if people did not have enough to worry about, attackers are now targeting them with Coronavirus (COVID-19) phishing emails that install ransomware.

While we do not have access to the actual phishing email being sent, MalwareHunterTeam was able to find an attachment used in a new Coronavirus phishing campaign that installs the Netwalker Ransomware.

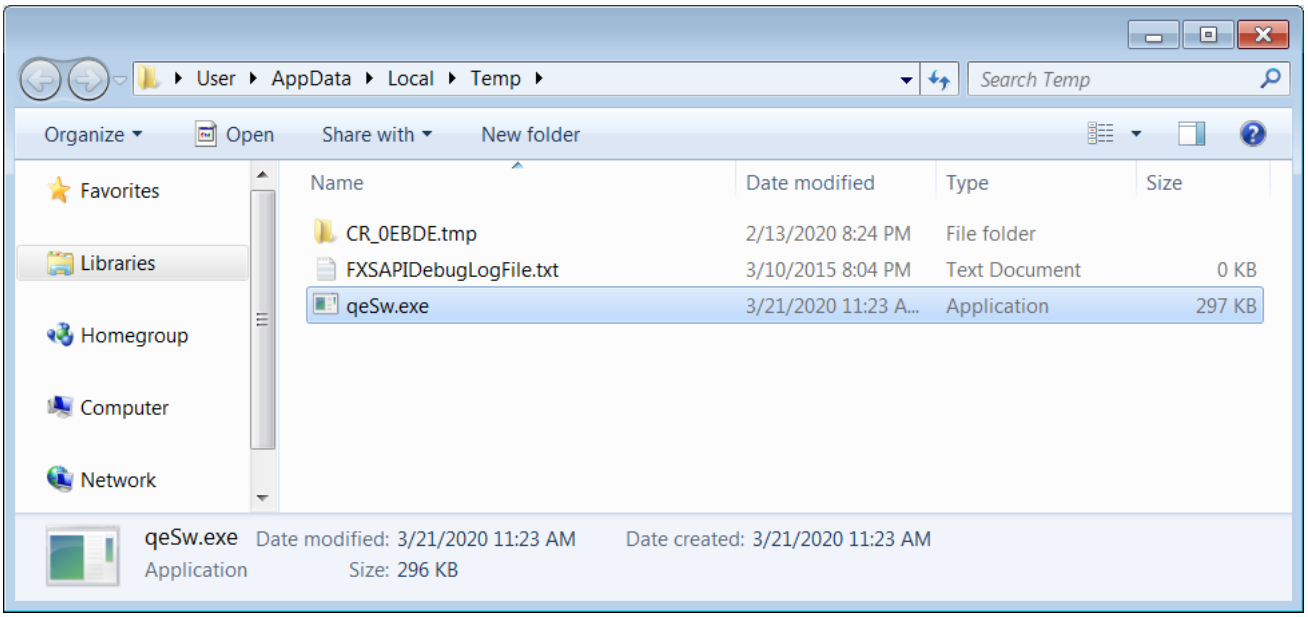
Netwalker is a ransomware formerly called Mailto that has become active recently as it targets the enterprise and government agencies. Two widely reported attacks related to Netwalker are the ones on the Toll Group and the Champaign Urbana Public Health District (CHUPD) in Illinois.

The new Netwalker phishing campaign is using an attachment named "CORONAVIRUS_COVID-19.vbs" that contains an embedded Netwalker Ransomware executable and obfuscated code to extract and launch it on the computer.



VBS Attachment

When the script is executed, the executable will be saved to **%Temp%\qeSw.exe** and launched.



Netwalker Executable

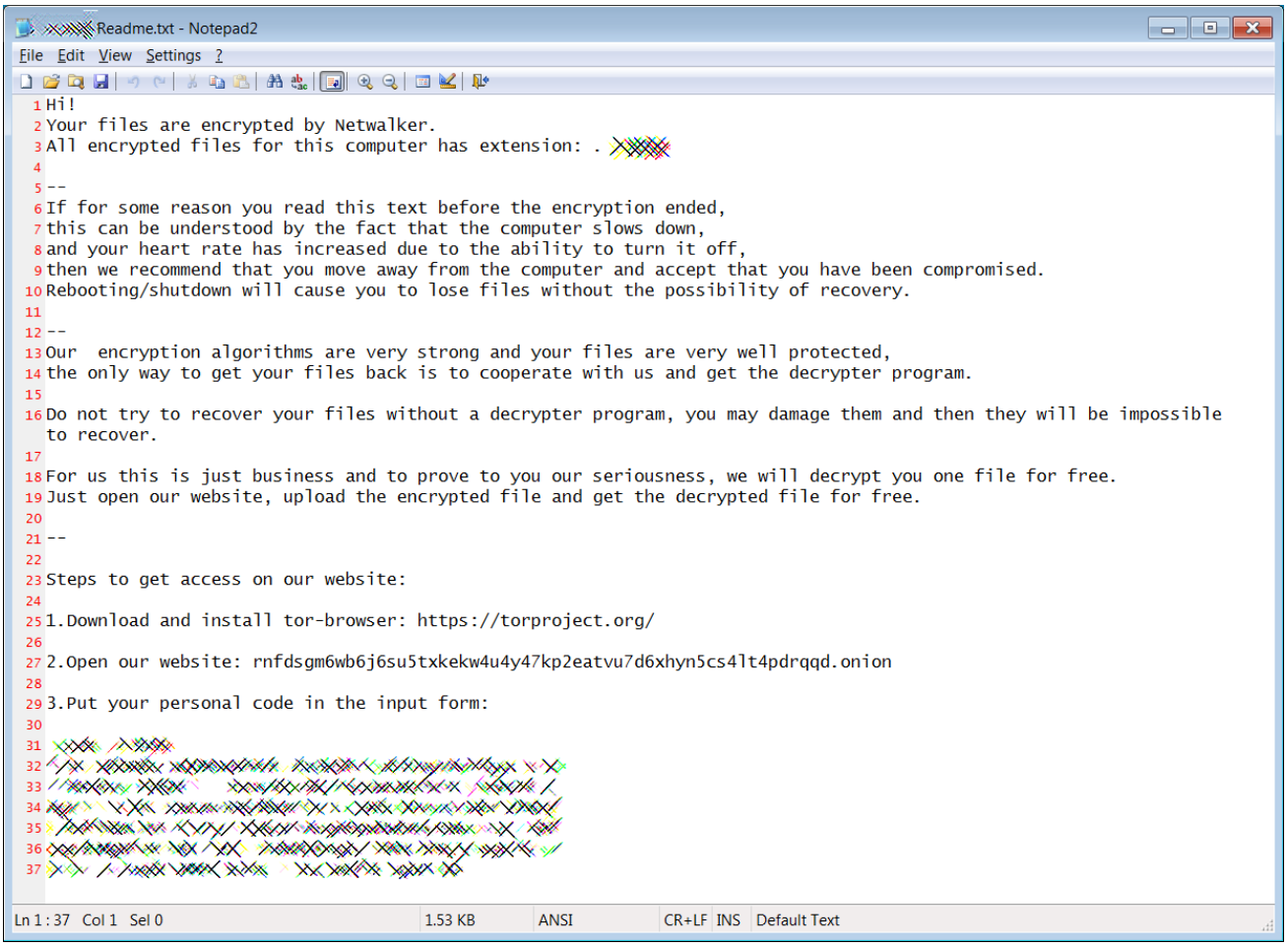
Once executed, the ransomware will encrypt the files on the computer and append a random extension to encrypted file names.

Head of SentinelLabs Vitali Kremez, the research division of SentinelOne, told BleepingComputer that this version of the ransomware specifically avoids terminating the Fortinet endpoint protection client.

When asked why they would do that, Kremez stated it may be to avoid detection.

"I suppose it might be because they have already disabled the anti-virus functionality directly from the customer admin panel; however, they do not want to trip an alarm by terminating the clients," Kremez told BleepingComputer.

When done, victims will find a ransom note named [extension]-Readme.txt that contains instructions on how to access the ransomware's Tor payment site to pay the ransom demand.



Netwalker Ransom Note

Unfortunately, at this time there is no known weakness in the ransomware that would allow victims to decrypt their files for free.

Instead, victims will need to either restore from backup or recreate the missing files.

Coronavirus attacks have become common

Due to the ongoing Coronavirus pandemic, threat actors have actively started using the outbreak as a theme for their phishing campaigns and malware.

We have seen the TrickBot trojan using text from Coronavirus related news stories to evade detection, a ransomware called CoronaVirus, the data-stealing FormBook malware spread through phishing campaigns, and even an email extortion campaign threatening to infect your family with Coronavirus.

This has led to the US Cybersecurity and Infrastructure Security Agency (CISA) to issue warnings about the rise of Coronavirus-themed scams and the World Health Organization (WHO) to release warnings of phishing scams impersonating their organization.

As threat actors commonly take advantage of topics that spread anxiety and fear, everyone must be more diligent than ever against suspicious emails and the promotion of programs from unknown sources.

Related Articles:

New Bumblebee malware replaces Conti's BazarLoader in cyberattacks

Intuit warns of QuickBooks phishing threatening to suspend accounts

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

- Coronavirus
- COVID-19
- Netwalker
- Phishing
- Ransomware

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.

- Previous Article
- Next Article

You may also like: