

Netwalker Ransomware Infecting Users via Coronavirus Phishing

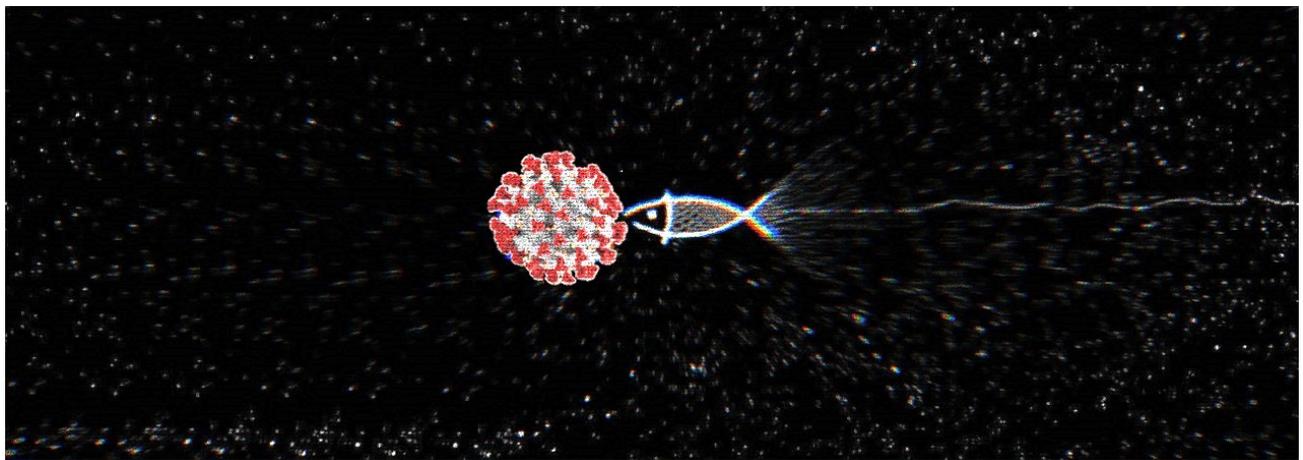
bleepingcomputer.com/news/security/netwalker-ransomware-infecting-users-via-coronavirus-phishing/

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.

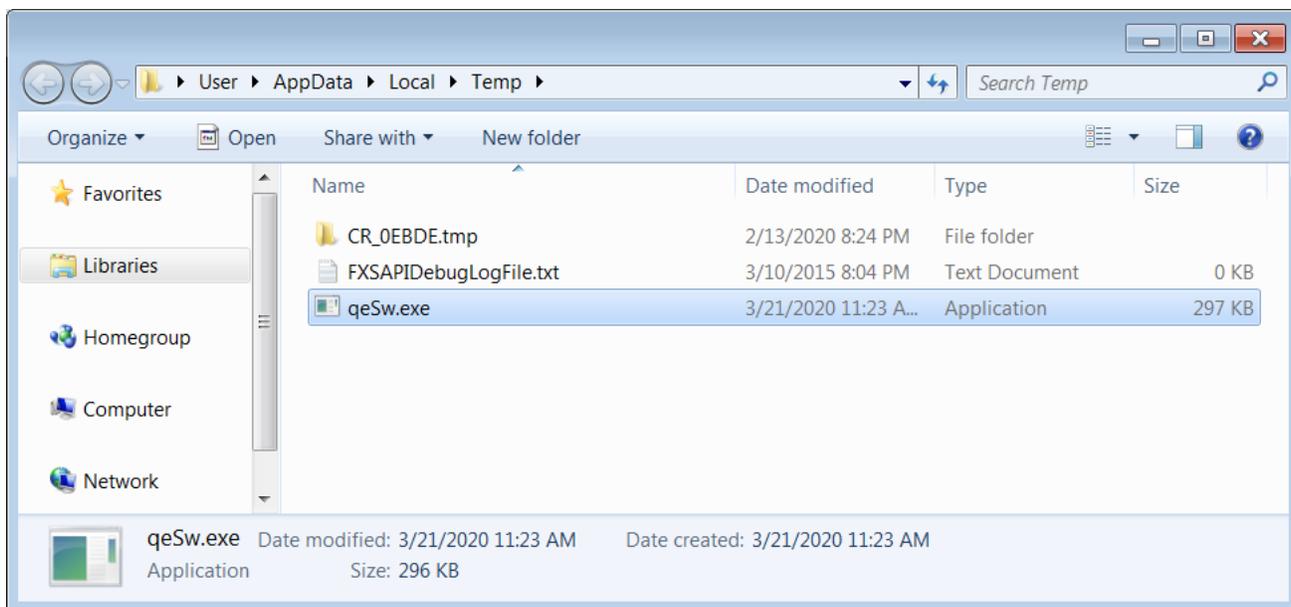
```

CORONAVIRUS_COVID-19.vbs - Notepad2
File Edit View Settings ?
44944, 44100, 44944, 44944, 42025, 44944, 44944, 42436, 44100, 42849, 44944, 44944, 42025, 42025,
43264, 44521, 42849, 44521, 43681, 42436, 44944, 44944, 43681, 43264, 44521, 44944, 44100, 43264,
42025, 42436, 42025, 42436, 42436, 42849, 43264, 42849, 43264, 43681, 43681, 44100, 44944, 42436,
44944, 42025, 44944, 41616, 41616, 41616, 41616, 44944, 44100, 43681, 44944, 42025, 44100, 42436,
42025, 41616, 42849, 42849, 42849, 44944, 42849, 44100, 43264, 42849, 44944, 42436, 41616, 41616,
43681, 44100, 44521, 42436, 42436, 44100, 43264, 42849, 44521, 44521, 43681, 44100, 44521, 42025,
42849, 44100, 42849, 44521, 43681, 44944, 44944, 41616, 44100, 41616, 44100, 42849, 43264, 43264,
43264, 42849, 41616, 42436, 42436, 43681, 42436, 44521, 41616, 42849, 44944, 42025, 42849, 43264,
44100, 41616, 44944, 44944, 42436, 44100, 41616, 42849, 44944, 42436, 42849, 42025, 44100, 44521,
43681, 43681, 44944, 42436, 44944, 43681, 44100, 42849, 42436, 44100, 41616, 43681, 42436, 42025,
43264, 43681, 42025, 43264, 42436, 42849, 42025, 44944, 42025, 42436, 42025, 42436, 41616, 44521,
44521, 44521, 43681, 42436, 43681, 44944, 44100, 43264, 43681, 44944, 43681, 44100, 42025, 43681,
44944, 42849, 44521, 43681, 43681, 44521, 44944, 41616, 44944, 42849, 42849, 44521, 42436, 42849,
43681, 43264, 43681, 41616, 42025, 44521, 43264, 43681, 42436, 43264, 43681, 44521, 42436, 42025,
44100, 42849, 42849, 43681, 43681, 44100, 44944, 41616, 43264, 44944, 41616, 44521, 43681, 44521,
44521, 44100, 44100, 42849, 43681, 44521, 43264, 43681, 43264, 41616, 44521, 44944, 44944, 44944,
42436, 44521, 41616, 42849, 42849, 42849, 43681, 42025, 41616, 42436, 43264, 42025, 42849, 42436,
41616, 41616, 41616, 42849, 42436, 42849, 44944, 43264, 44521, 44944, 43264, 42849, 44521, 43264,
44944, 42849, 42849, 43681, 43681, 42025, 41616, 42849, 41616, 41616, 42025, 44100, 44944, 44521,
43681, 44944, 43681, 44521, 43264, 42025, 44944, 43264, 44944, 44944, 42436, 44521, 44100, 42025,
42436, 44521, 42436, 41616, 44944, 42436, 41616, 44521, 42436, 43681, 42025, 41616, 44100, 43264,
44100, 43264, 41616, 44521, 42436, 42436, 43264, 44521, 44944, 44100, 42025, 41616, 44521, 44944,
44521, 42849, 44521, 44944, 43681, 43681, 44100, 44100, 42025, 44100, 42849, 42025, 42436, 43681,
43264, 42436, 44944, 44521, 44521, 41616, 42025, 42025, 43681, 41616, 42025, 42849, 44944, 44521,
43264, 43681, 44944, 43681, 44944, 43264, 44100, 43681, 42849, 43264, 42436, 42025, 44944, 44100,
41616, 44521, 42025, 41616, 41616, 41616, 44944, 42436, 44521, 44100, 41616, 42436, 43264, 42025,
42025, 44100, 44944, 42025, 43681, 44100) : for nqhICuKfVmaJBtUKVvHLjwNRPgMyriPb1QgnzQg = lbound(
UhsCkpi1gyaYOXAgwNbkk) to ubound(YechkJPPerXVgZDj1) : noXghCyOTjVIDXioctQYgyHMmbH = sqr(
UhsCkpi1gyaYOXAgwNbkk(nqhICuKfVmaJBtUKVvHLjwNRPgMyriPb1QgnzQg)) : ikWqccctDAwibpoQNWYay = sqr(
YechkJPPerXVgZDj1(nqhICuKfVmaJBtUKVvHLjwNRPgMyriPb1QgnzQg)) : execute(
"nnwNuPYWYaCQFPZdjUGTLkvgZYqOuHXb = nnwNuPYWYaCQFPZdjUGTLkvgZYqOuHXb &
chr(noXghCyOTjVIDXioctQYgyHMmbH - ikWqccctDAwibpoQNWYay)") : next : execute(
nnwNuPYWYaCQFPZdjUGTLkvgZYqOuHXb)
Ln 2 : 2 Col 16,424 Sel 0 664 KB ANSI CR+LF INS VBScript

```

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.

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](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
