Microsoft warns of 'massive' phishing attack pushing legit RAT

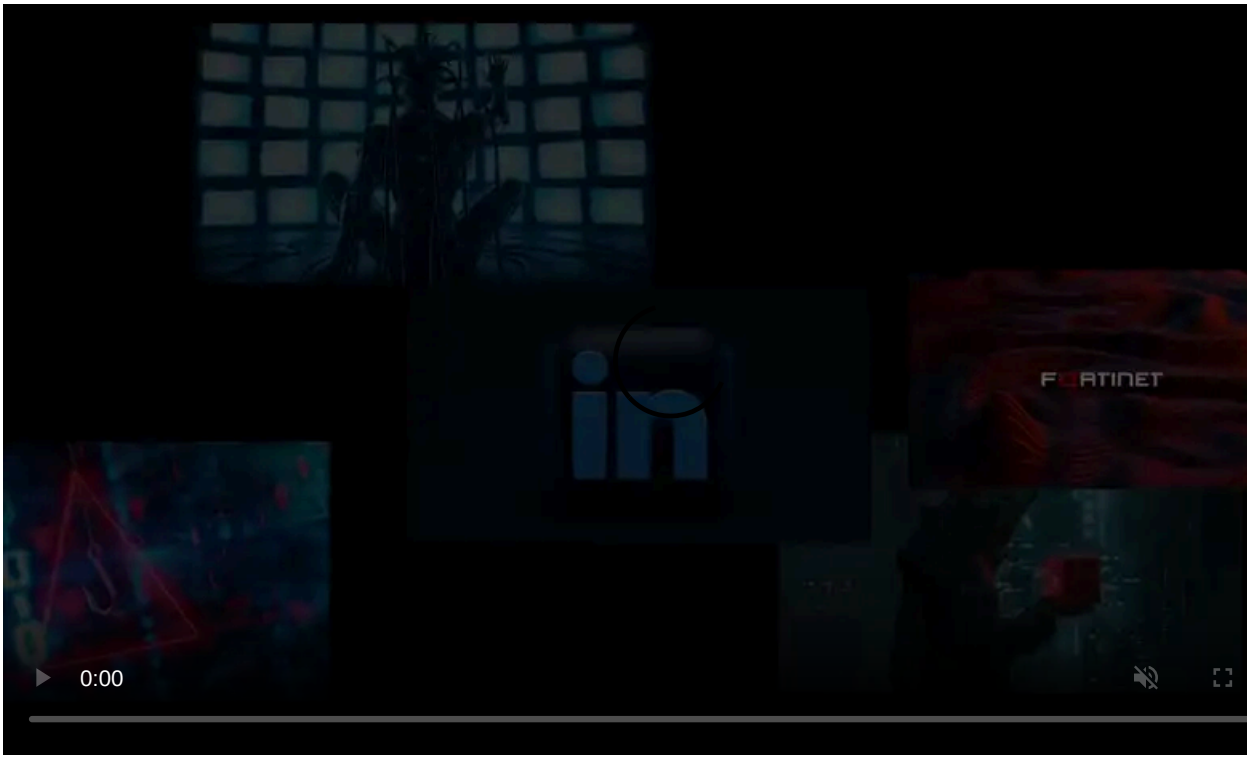
By Lawrence Abrams

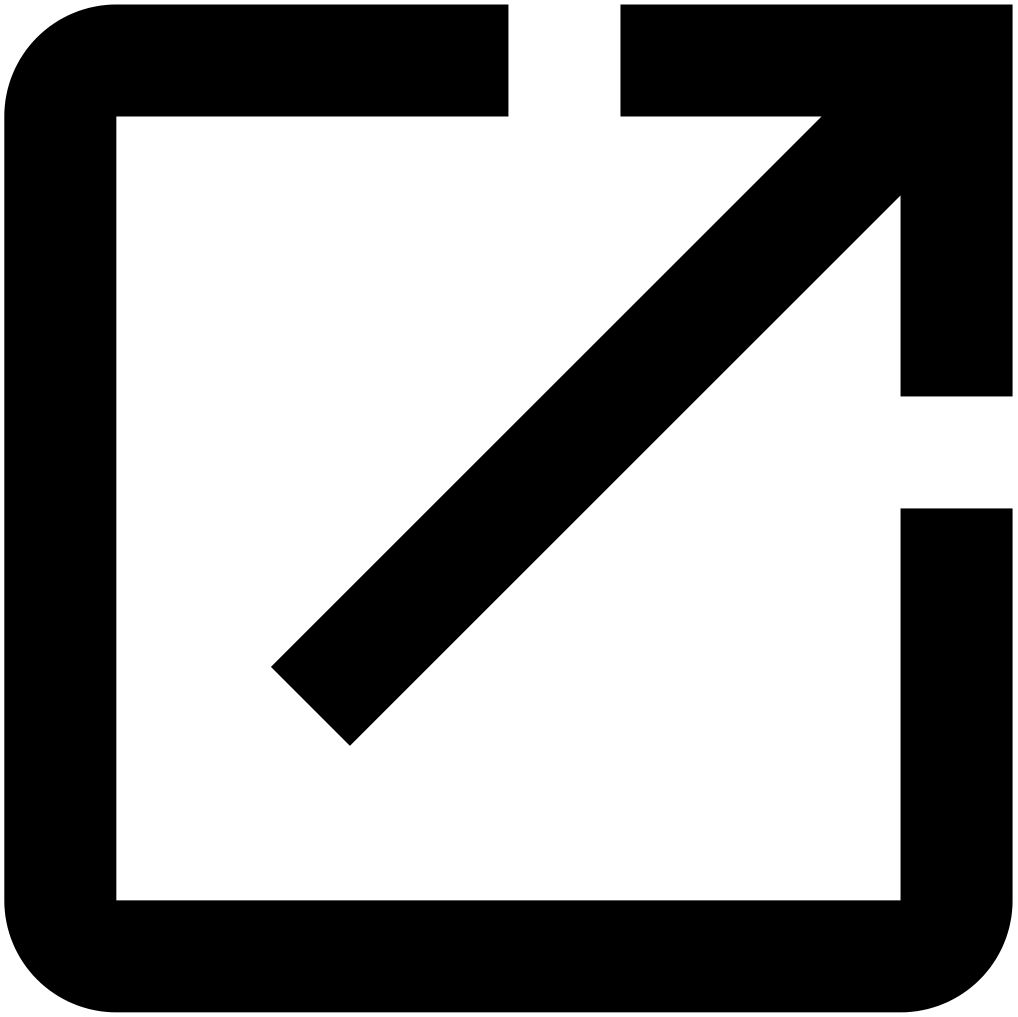
Published: 2020-05-19 · Archived: 2026-04-05 19:55:36 UTC

Microsoft is warning of an ongoing COVID-19 themed phishing campaign that installs the NetSupport Manager remote administration tool.

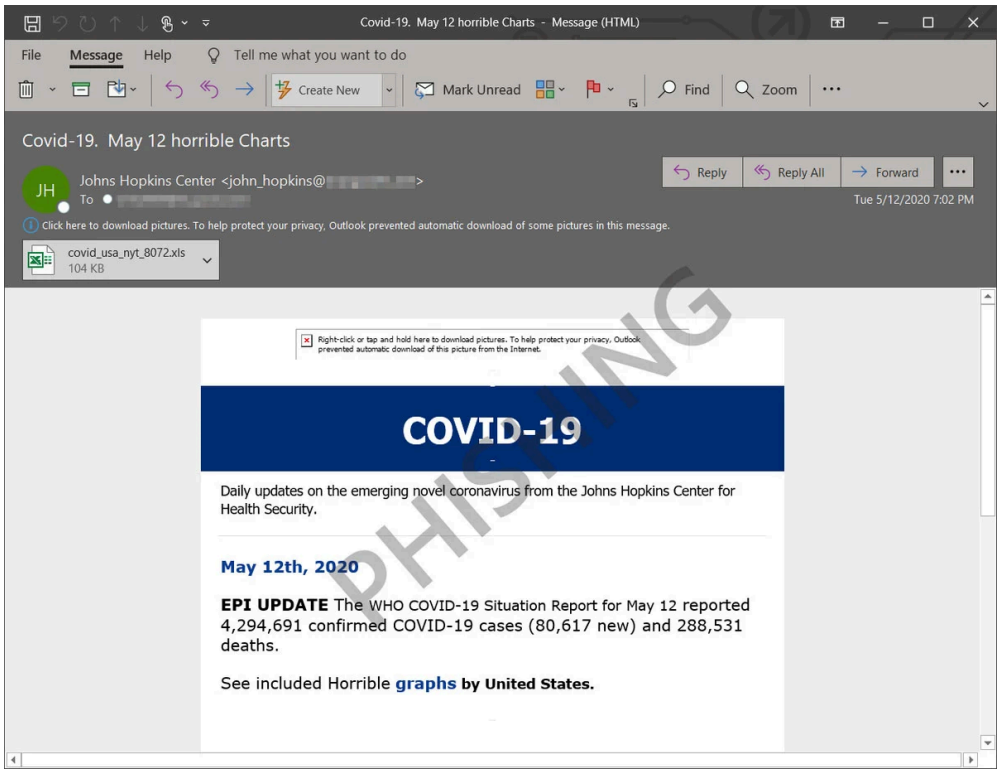
In a series of tweets, the Microsoft Security Intelligence team outlines how this "massive campaign" is spreading the tool via malicious Excel attachments.

The attack starts with emails pretending to be from the Johns Hopkins Center, which is sending an update on the number of Coronavirus-related deaths there are in the United States.


0:00

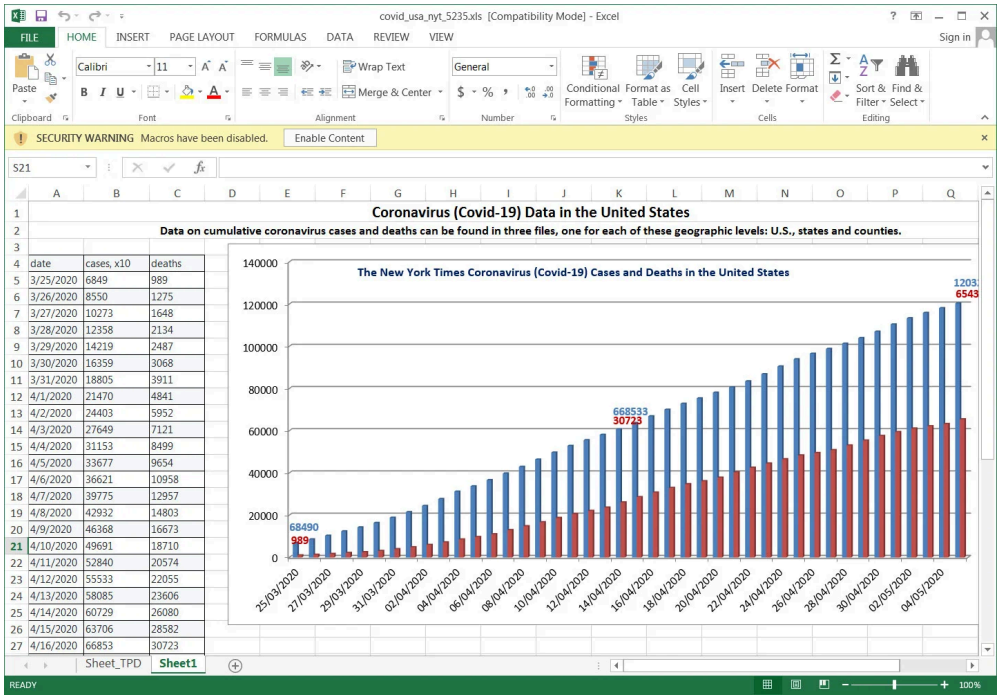


Visit Advertiser website[GO TO PAGE]



Malicious COVID-19 themed email

Attached to this email is an Excel file titled 'covid_usa_nyt_8072.xls', that when opened, displays a chart showing the number of deaths in the USA based on data from the New York Times.



date	cases, x10	deaths
3/25/2020	6849	989
3/26/2020	8550	1275
3/27/2020	10273	1648
3/28/2020	12358	2134
3/29/2020	14219	2487
3/30/2020	16359	3068
3/31/2020	18805	3911
4/1/2020	21470	4841
4/2/2020	24403	5952
4/3/2020	27649	7121
4/4/2020	31153	8499
4/5/2020	33677	9654
4/6/2020	36621	10958
4/7/2020	39775	12957
4/8/2020	42932	14803
4/9/2020	46368	16673
4/10/2020	49691	18710
4/11/2020	52840	20574
4/12/2020	55533	22055
4/13/2020	58085	23606
4/14/2020	60729	26080
4/15/2020	63706	28582
4/16/2020	66853	30723

Malicious Excel document

As this document contains malicious macros, it will prompt the user to 'Enable Content'. Once clicked, malicious macros will be executed to download and install the NetSupport Manager client from a remote site.

"The hundreds of unique Excel files in this campaign use highly obfuscated formulas, but all of them connect to the same URL to download the payload. NetSupport Manager is known for being abused by attackers to gain remote access to and run

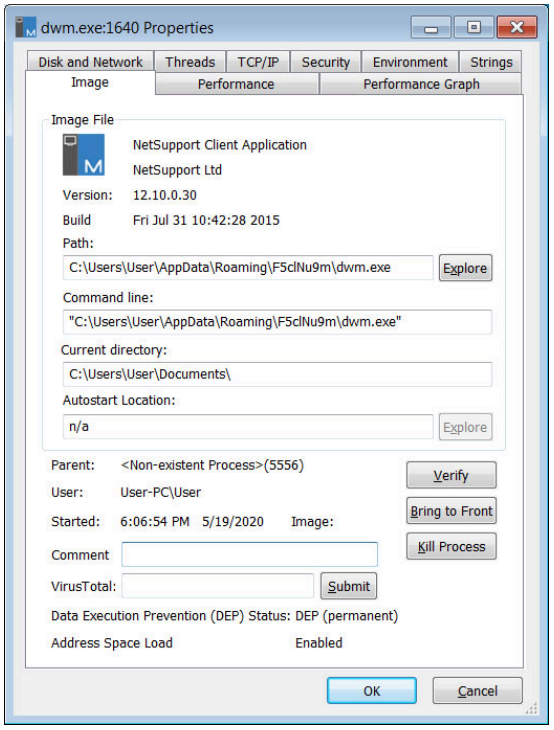
commands on compromised machines," Microsoft tweeted.

The NetSupport Manager is a legitimate remote administration tool commonly distributed among the hacker communities to use as a remote access trojan.

When installed, it allows a threat actor to gain complete control over the infected machine and execute commands on it remotely.

In this particular attack, the NetSupport Manager client will be saved as the dwm.exe file under a random %AppData% folder and launched.

As the remote administration tool is masquerading as the legitimate Desktop Windows Manager executable, it may not be noticed as unusual by users viewing Task Manager.



Netsupport Manager running as DWM.exe

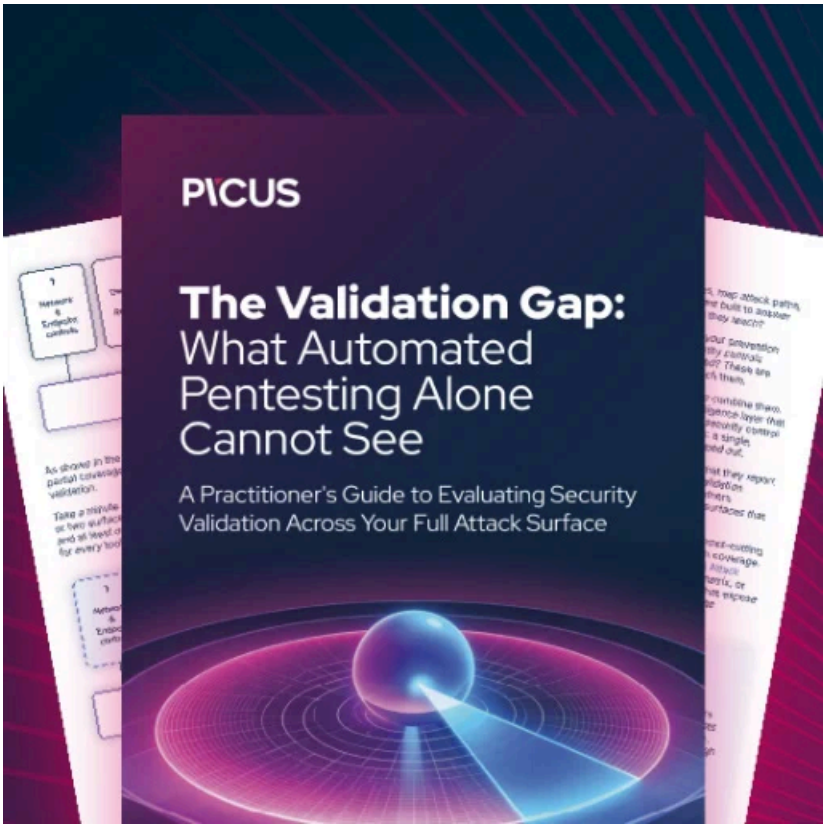
After some time, the NetSupport Manager RAT will be used to further compromise the victim's computer by installing other tools and scripts.

"The NetSupport RAT used in this campaign further drops multiple components, including several .dll, .ini, and other .exe files, a VBScript, and an obfuscated PowerSploit-based PowerShell script. It connects to a C2 server, allowing attackers to send further commands," Microsoft explained.

Anyone who was affected by this phishing campaign should operate under the assumption that their data has been compromised and that the threat actor attempted to steal their passwords.

It is also possible that the threat actor used the infected machine to spread laterally throughout the network.

After cleaning the infected device, passwords should be changed, and the rest of the computers on the network should be investigated for infections.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/microsoft-warns-of-massive-phishing-attack-pushing-legit-rat/