


TA505 Malware Threat Insights

 proofpoint.com/us/threat-insight/post/ta505-and-others-launch-new-coronavirus-campaigns-now-largest-collection-attack

March 16, 2020





[Blog](#)
[Threat Insight](#)
TA505 Malware Threat Insights



March 16, 2020 Sherrod DeGrip

Proofpoint researchers are continuing to monitor malicious threat actor activity surrounding COVID-19. To date, the cumulative volume of coronavirus-related email lures now represents the greatest collection of attack types united by a single theme that our team has seen in years, if not ever. We've observed credential phishing, malicious attachments, malicious links, business email compromise (BEC), fake landing pages, downloaders, spam, and malware, among others, all leveraging coronavirus lures.

Over the past week, the team observed a campaign from TA505, the group behind Locky ransomware and the Dridex banking Trojan, that uses a coronavirus lure as part of a downloader campaign targeting the U.S. healthcare, manufacturing, and pharmaceuticals industries.

The team also found a separate coronavirus-themed campaign that uses a downloader, targets the healthcare industry, and demands Bitcoin payment. Indicating a potential future shift in the attack landscape, the downloaders used in the above two campaigns are sometimes seen as a first stage payload before ransomware is later downloaded and installed on a victim's machine. Ransomware is typically delivered as either second or later stage payload.

We've additionally seen TA564 using coronavirus emails to target Canadian users by spoofing the Public Health Agency of Canada in an attempt to deliver Ursnif.

New TA505 Malware and Campaign Examples

As everyone around the world continues to search online for the latest developments and news around coronavirus, Proofpoint researchers have observed TA505, the group behind the Locky ransomware, using a coronavirus lure in an attempt to deliver a downloader to a victim's computer. Once delivered, attackers can then download additional types of malware including banking Trojans and ransomware. TA505 is known as one of the most significant financially motivated threat actors due to the extraordinary volumes of messages they send.

Figure one below shows an email from one of the attempted TA505 Coronavirus attacks purporting to contain information to help protect users' friends from the virus, urging readers to click the link provided.

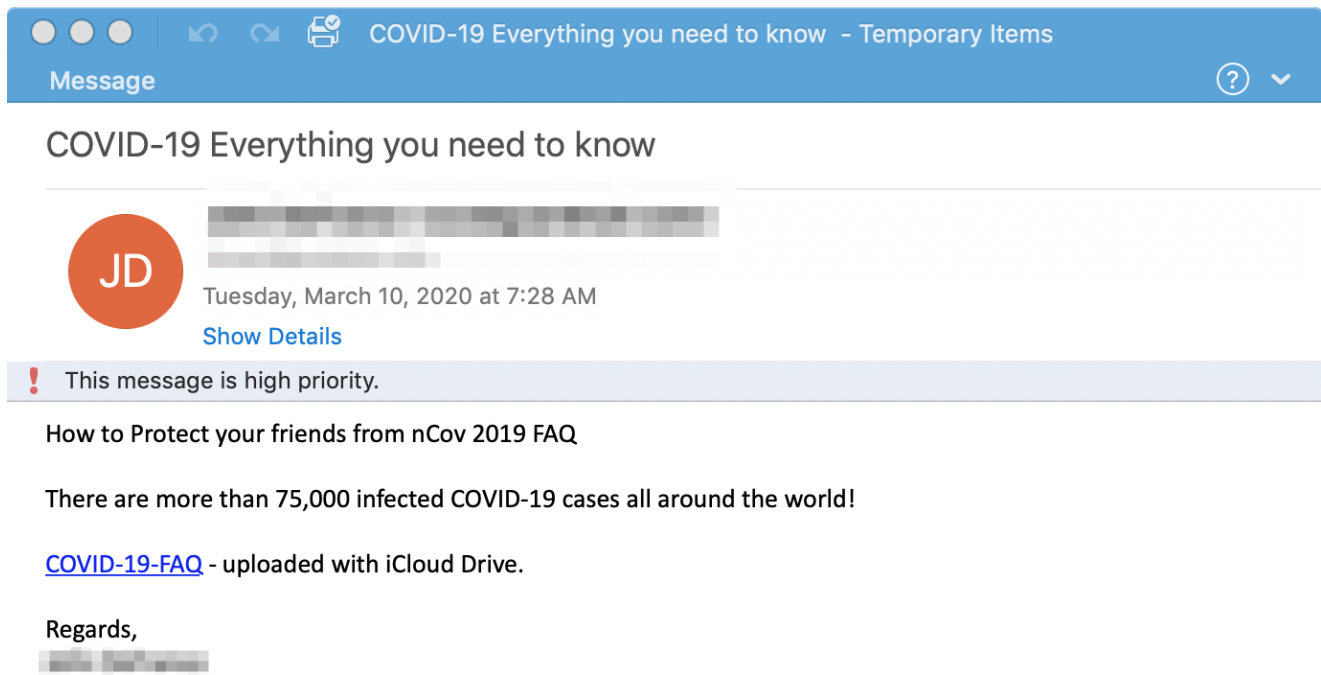


Figure 1 TA505 Coronavirus FAQ Lure

We have also separately seen coronavirus-themed emails with downloaders targeting healthcare organizations that request Bitcoin payments. Figure 2 below shows an email offering coronavirus remedies in exchange for Bitcoin.

From [REDACTED] ☆
Subject Remedies On Corona-Virus 23/02/2020 à 15:00
Reply to [REDACTED]

Reply Reply All Forward More


Dear Reader,

A group of Corona-Virus Specialist is here in our own direct contact clinical attachedl for an antiviral called remdesivir.

Attached is step one 10\$ to connect with [REDACTED] on Skype

Skype: live:.cid.e63ddc29b41078e7

Note: If you have an active email then your reply is needed. PLEASE PAY THE BTC URGENTLY! IF OUR SYSTEM DOES NOT RECEIVE YOUR PAYMENT WITHIN 7 DAYS. ALL DATA FOR THE SPECIFIC METHOD WILL BE TERMINATED PERMANENTLY FOR YOUR DOWNLOAD.

 1Kw5qE92mSehKJ9AHjXRh44q2u2wgxZ86Z

[log in to your account](#) | [get support](#)



>  1 attachment: REMEDIES ON CORONA-VIRUS.pdf 20,6 KB  Save

Figure 2 Coronavirus Campaign Requesting Bitcoin for Remedy

We've also seen TA564 using coronavirus emails targeting Canadian users by spoofing the Public Health Agency of Canada in an attempt to deliver Ursnif. Ursnif is a common banking Trojan that can steal stored data, including passwords, from banking websites via web injections, proxies, and VNC connections.

Figure 3 below shows an email addressing "parents and guardians," with a reported update from the Public Health Agency of Canada's Medical Officer of Health, listing the individual's correct name.

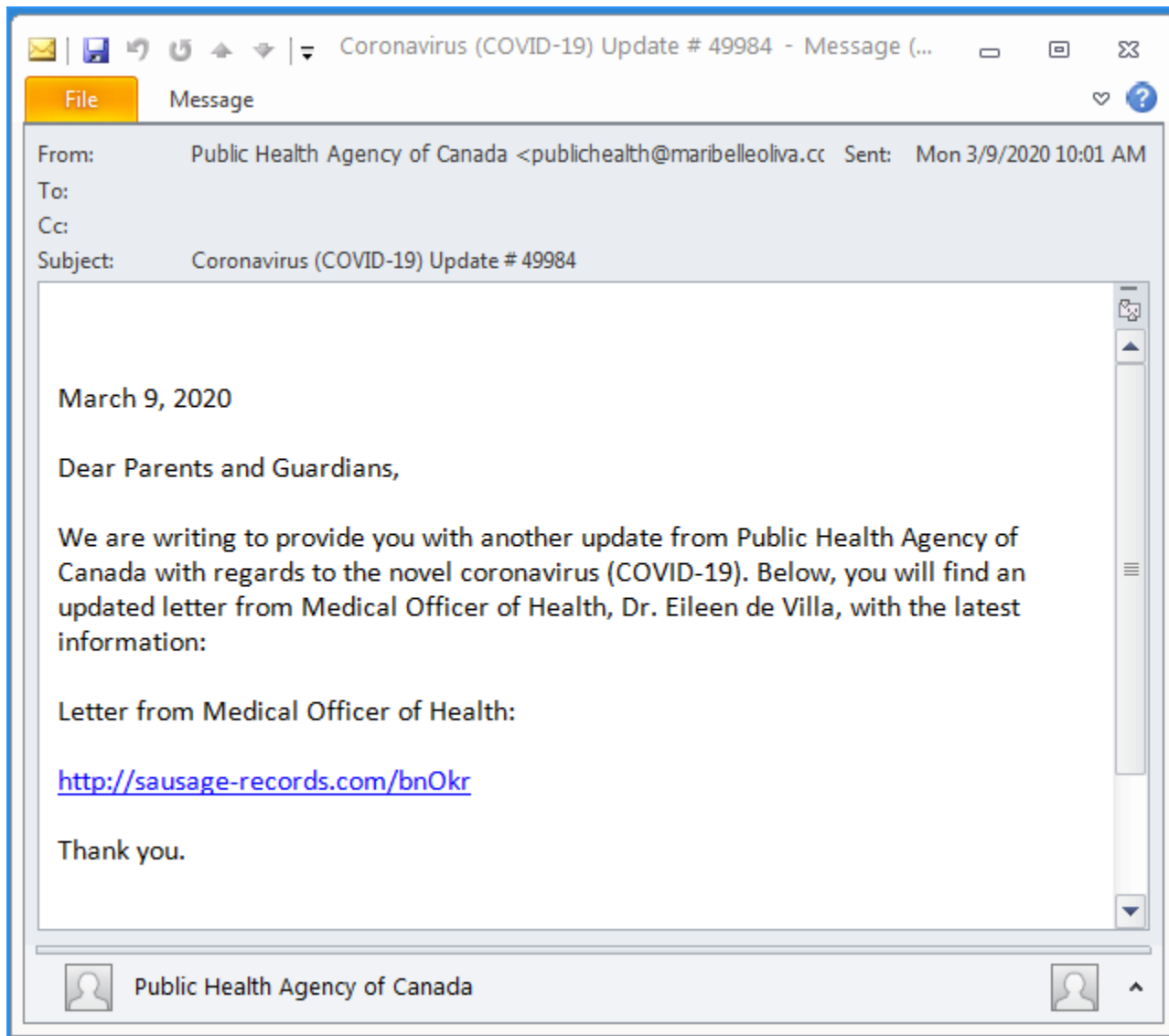


Figure 3 Fake Public Health Agency of Canada Lure

Summary of TA505 Coronavirus Attacks

We anticipate TA505 malware attackers will continue to leverage COVID-19 (as detailed in our new Redline Stealer Threat Insight blog) as it develops further worldwide and will also likely pursue potential targets who are now being asked to work from home. Stay vigilant for malicious emails regarding remote access and fake corporate websites, all aimed at ensnaring teleworkers. When working remotely, be sure to use a secure Wi-Fi connection, protect your VPN log-in, use strong passwords, think twice about clicking on links, and confirm all transactions are authentic.

We'll continue posting future TA505 attack news as well as coronavirus campaigns and insights on our threat research Twitter account: <https://twitter.com/threatinsight>. You can also review additional coronavirus-themed campaign examples on [conspiracy theories](#) and [global shipping concerns](#) in our previous posts.

Subscribe to the Proofpoint Blog