National Computer Board

CERT-MU

# CERT-MU Security Alert

# COVID-19: Malware Scams


**Issue Date: 30 March 2020**

**Description:**

Unscrupulous marketers and cyber-criminals have seized upon concerns over the emergence of the COVID-19 global pandemic as bait for not only spam and phishing attacks but also malware. Sadly, they are also exploiting this situation and there has been a significant rise in Coronavirus-themed malicious websites, with more than 16,000 new coronavirus-related domains registered since January 2020. From ten domains a day in February, there are now thousands of new domains popping up daily, containing terms like coronavirus, covid, pandemic, virus, or vaccine.

**How you can recognize covid-19 related malware?**

Malicious emails using subjects containing COVID-19 and related keywords carrying Remote Administration Tools (RATs) such as NetWire, NanoCore, and LokiBot, as well as other malware have been identified.

Below are some of the examples of the email subjects:

- "CORONAVIRUS (COVID-19) UPDATE // BUSINESS CONTINUITY PLAN ANNOUNCEMENT STARTING MARCH 2020."
- "Latest corona-virus updates"
- "UNICEF COVID-19 TIPS APP"
- "POEA HEALTH ADVISORY re-2020 Novel Corona Virus."
- "WARNING! CORONA VIRUS"

Examples of file attachment names include:

- "AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_pdf.exe"
- "Coronavirus COVID-19 upadte.xlsx"
- "CORONA VIRUS1.uue"
- "CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm"
- "covid19.ZIP"

**Mobile users are being targeted as well**

The coronavirus malware and scam campaigns are not only targeting desktop users. With the entire world moving to a lockdown, including Mauritius, cyber-criminals are capitalizing on people's habit of relying on mobile apps for information on Covid-19 (Coronavirus).

Malicious applications that claim to offer information about the virus allow the attacker to spy on you through your devices, or encrypt your device and hold it for ransom.

**How to avoid installing fake applications on your mobile**

- Android users should not install applications from untrusted sources (stick to the Google Play store)

- iPhone users should refrain from jailbreaking their phones and install apps from third-party sources (stick to the App Store).

**Sale of malware through COVID-19 discount codes on the darknet**

It is worth noting that hackers are also selling malware and hacking tools through COVID-19 discount codes on the darknet, many of which are aimed at accessing corporate data from home-workers' laptops, which may not be as secure as within an office environment.

**Best practices for working from home/remotely**

The following steps can be helpful in ensuring a more secure and stable remote working:

- Increase the number of simultaneous VPN connections to accommodate all remote employees.
- Set up and support conferencing software that ensures both a stable voice and video connection.
- Ensure all employees have valid credentials that do not expire within less than 30 days as in the case of Windows Operating Systems, changing expired Active Directory credentials can be challenging when remote.
- Send out rules and guidelines regarding accepted applications and collaborative platforms so employees are aware of what is sanctioned and supported and what is not.
- Have gradual rollout procedures for deploying updates, as delivering them all at once to VPN-connected employees could create bandwidth congestions and affect inbound and outbound traffic.
- Enable disk encryption for all endpoints to reduce the risk of data loss on compromised devices.
- And last but not the least, be vigilant at all times!