Coronavirus Cyber Campaigns

FEBRUARY

Feb. 01

Emotet

Coronavirus themed email-based malware campaign targeting Japanese victims with malicious .docm files.
Source: IBM X-Force Exchange

Feb. 02

Various Trojans & Worms

Malicious pdf, mp4 and docx files disguised as documents relating to Coronavirus.
Source: Kaspersky

Feb. 05

Patchwork APT Group

Uses Coronavirus-named malicious .xlsm and .docx files as lure , targeting Chinese victims.
Source: @blackorbird

Feb. 11

Parallax RAT

Downloaded through sample named "new infected CORONAVIRUS sky 03.02.2020.pif.", likely delivered as an attachment to an email.
Source: @malwrhunterteam

Feb. 13

Nanocore RAT

"Coronavirus update" emails spread the RAT utilizing ZIP attachments with a PIF executable downloader.
Source: Cisco Talos Blog

MARCH

Mar. 07

Formbook

Email campaign supposedly delivering Coronavirus information from the WHO delivers Formbook stealer.
Source: Bleeping Computer

Mar. 09

AZORult

AZORult threat actors weaponize Coronavirus map applications with the information stealer.
Source: Reason Security

Mar. 09

Scam Websites

Websites claiming to give COVID-19 news and mask information while scamming victims.
Source: ThreatConnect

Mar. 11

Hancitor Resurfaces

After a few quiet weeks, Hancitor returns with Coronavirus-themed malspam.
Source: @mesa_matt

MARCH

Mar. 12

Vicious Panda Campaign

Coronavirus-themed campaign targeting the Mongolian public sector, using malicous RTF email attachments to deliver a custom RAT.
Source: Checkpoint

Mar. 12

CoronaVirus Ransomware & Kpot

Fake WiseCleaner site distributes a malware cocktail of CoronaVirus ransomware and Kpot password-stealing trojan.
Source: Bleeping Computer

Mar. 12

Transparent Tribe Campaign

Malicious "Health Advisory of Coronavirus" document pretending to be from the Indian Government delivers Crimson RAT.
Source: @RedDrip7

Mar. 13

CovidLock Android Ransomware

An Android app posing as a "Coronavirus map tracker" downloads CovidLock ransomware on to victim mobile devices.
Source: Domaintools

MARCH

Mar. 16

RedLine Stealer

Malicious emails asking recipients to "help find a Coronavirus cure" by running simulators downloads RedLine.
Source: Proofpoint

Mar. 16

APT36 Delivers Crimson RAT

AZORult threat actors weaponize Coronavirus map applications with the information stealer.
Source: Malwarebytes

Mar. 17

Cerberus

The Android banking trojan targets Vodafone customers using a fake Coronavirus website.
Source: @1ZRR4H

Mar. 17

Chinoxy

In a campaign targeting Kyrgyzstan, malicious Coronavirus-themed documents are distributed to infect with Chinoxy.
Source: @Sebdraven

Mar. 18

Google Squatting Campaign

A phishing campaign uses google typosquatting domains with Coronavirus themes, luring victims into giving away their credentials.
Source: IBM X-Force

MARCH

Mar. 23

BlackNET RAT

Fake Coronavirus Antivirus claiming to use "Harvard University AI" actually downloads BlackNET RAT.
Source: Malwarebytes

Mar. 29

Bank & Government Phishing

Phishing pages posing as the Bank of Ireland, Government of Canada and Gov.UK use Coronavirus themed domains.
Source: @jorgemieres

Mar. 31

Coronavirus Wiper Trojan

An MBR-wiping trojan is distributed, using many Coronavirus-related file names in its infection process.
Source: SonicWall