This page identifies the open source intelligence collection and analysis by the Cyber Threat Intelligence community over the past two months.

- Researchers at Proofpoint observed a COVID-19-themed phishing campaign targeting the manufacturing, industrial, finance, transportation, pharmaceutical and cosmetics industries. These attacks involved emails that contained Microsoft Office document attachments designed to lure victims and exploit a Microsoft Office vulnerability, tracked as CVE-2017-11882. The malicious documents contained what is purported to be an advisory on the impact of the virus on the shipping industry. Once the malicious document is opened, it installs the information-stealing malware "**AZORult**." The **AZORult** strain observed in the campaign did not download ransomware, as it has done in previous attacks. According to researchers at Proofpoint, the malicious emails are originating from groups in Russia and Eastern Europe.

- Back in January 2020, IBM X-Force observed cybercriminals using coronavirus as a phishing lure to distribute **EMOTET** in a campaign primarily targeting Japan. The phishing emails claimed that the attached Microsoft Word documents contained health information and updates, but in reality contained a malicious VBA macro that installs a PowerShell script, which then downloads the **EMOTET** trojan.

- Kaspersky published an article about phishing emails that emulated the CDC, in particular from emails containing the domains **cdc-gov[.]org** and **cdcgov[.]org**. In one instance, the URL contained within a phishing email led to a fake Microsoft Outlook login page that was designed to convince victims to input their credentials. In another instance, victims were asked to donate Bitcoin to aid in the pursuit of a vaccine.

- Phishing emails primarily targeting Italian email addresses contained malicious Microsoft Office documents with embedded VBA macros that were used to drop **TRICKBOT**. The **TRICKBOT** banking trojan can be used to steal victims' confidential information, as well as to drop additional malware. The email subject line used in this campaign was "Coronavirus: informazioni importanti su precauzioni," and to bolster the credibility of the attached lure, the supposed author was "Dr. Penelope Marchetti," an employee of the WHO in Italy.

- The security firm Cofense identified a similar, though more sophisticated, phishing campaign using the subject line "COVID-19 — Now Airborne, Increased Community Transmission" that appears to originate from the address **CDC-Covid19[@]cdc[.]gov**. When victims click on the embedded link, they are redirected to a Microsoft Outlook login page, and upon entering their legitimate credentials are further redirected to a legitimate website of the CDC. While these phishing emails appear to come from a legitimate address on the CDC domain, this is due to the threat actor purposefully disguising the true origin of the email.

- Cofense also identified a phishing campaign using the subject line "Attention: List Of Companies Affected With Coronavirus March 02, 2020." that contained a malicious attachment that dropped **AGENT TESLA** Keylogger. This attachment used the icon of a Microsoft Excel file to masquerade as a legitimate Office document and was reported to be titled "SAFETY PRECAUTIONS," with an .exe file extension.
- The security research team @issuemakerslab observed a malicious Microsoft Word document dropping the North Korean **BABYSHARK** malware that claimed to contain information on South Korea's response to the COVID-19 virus.
- The security research team @reddrip7 identified a malicious Word document attachment called "Коронавірусна інфекція COVID-19.doc" that contained a C# backdoor. Researchers suspect this malware is related to the Hades APT. Due to the presence of the string "TrickyMouse" in the malware, the campaign has been dubbed TrickyMouse by the researchers. The document uses the branding and trademark of the WHO and the Public Health Center of the Ministry of Health of Ukraine as a decoy and was used to target Ukraine.
- @reddrip7 also identified a COVID-19-themed phishing campaign that used a decoy document containing **NANOCORE** RAT targeting the South Korean chemicals manufacturing company Dongwoo Fine-Chem Corporation.
- Another campaign used the FedEx trademark in a phishing attack, claiming to provide victims with information on global FedEx operations while the COVID-19 outbreak continues. It contained an attachment titled "Customer Advisory.PDF.exe" that, when opened, infected the victim with the **LOKIBOT** malware.
- **LOKIBOT** was additionally distributed in a phishing campaign that used COVID-19 as a lure, claiming to be sent by the Ministry of Health in the People's Republic of China. The emails claimed to contain information about emergency regulations surrounding the virus with the subject line "Emergency Regulation Ordiance" (sic), and had a Windows RAR file attachment with the extension .arj. Once opened, the malicious attachment infects the victim with **LOKIBOT**, immediately contacting a malicious IP address and exfiltrating user credentials.
- The **GRANDOREIRO** banking trojan was observed being distributed via malicious sites that use the ongoing coronavirus pandemic as a lure. Twitter user @JAMESWT_MHT shared an instance of the trojan used as part of this campaign. The websites show information about the coronavirus with an embedded video player, and once the user clicks the player, the **GRANDOREIRO** executable is downloaded. According to Twitter user @ESETresearch, the malware is currently targeting users in Brazil, Mexico and Spain.

Even during a pandemic, cybersecurity threats show no signs of slowing down. Visit ey.com/ca/cyber to find out how EY can help you mitigate threats and protect your business.