Commonwealth Fusion Center (CFC)
Massachusetts
(978) 451-3700 | (508) 820-2233

MCP
Massachusetts Cybersecurity Program

(U/FOUO) CFC Massachusetts Cybersecurity Program (MCP) Bulletin: Coronavirus Cyber Attacks
February 19, 2020

(U) Overview of Coronavirus Cyber Attacks

(U) Today's cyber criminals are taking advantage of fears surrounding the coronavirus. The virus, which has caused thousands of deaths worldwide, has been a highly publicized story across all media outlets. The CFC Massachusetts Cybersecurity Program (MCP) has developed this bulletin for situational awareness purposes. Cyber criminals regularly use global events and stories to launch cyber-attacks. There are multiple known variations of cyber-attacks and scams involving coronavirus. The goals of these scams are either to plant malicious software (malware) or to trick the victim into relinquishing personal or financial information (phishing).

Source: QuickHeal

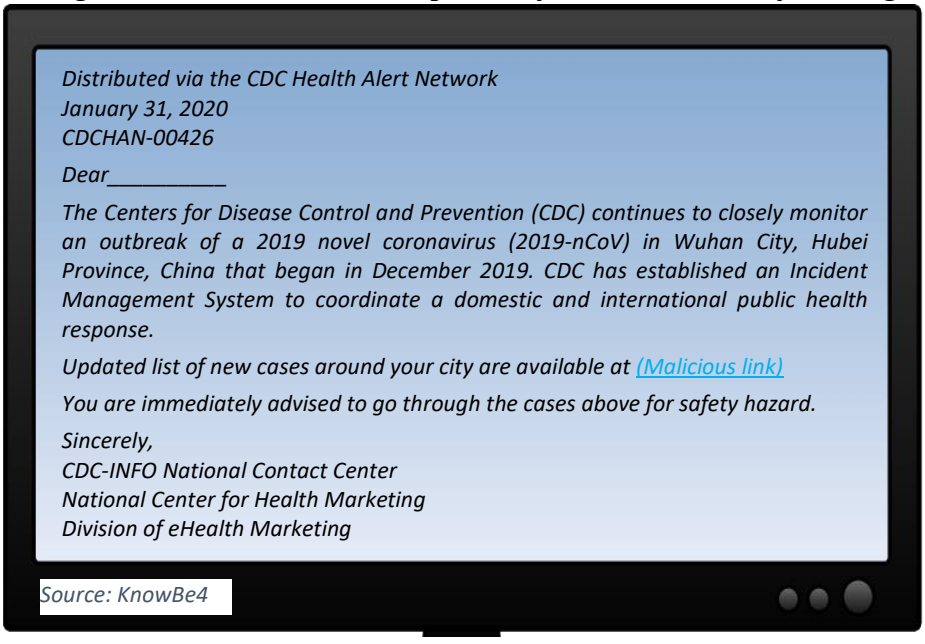
Phishing – Phishing is a cyber crime in which the unsuspecting victim willingly gives sensitive information (personal, financial, business) to who they believe is an official/legitimate institution in which they have a preconceived relationship with.

Malware – Malware is software that is specifically designed to gain access to or damage a computer, usually without the knowledge of the owner.

(U) Coronavirus Cyber-Attack Variations

(U) One type of reported scam is the creation of fake coronavirus donation websites. In this type of scam, cyber criminals play on the generosity of people looking to donate to individuals impacted by the coronavirus by stealing their money and financial information. As these websites appear legitimate, victims may send money directly to cyber criminals or provide financial information that could lead to further exploitation.

(U) Cyber criminals have also created fraudulent posts, notifications, and emails (example shown to the right) that appear to be promoting awareness and prevention tips about coronavirus. They advertise a link that claims to display the number of coronavirus cases in the viewer's area. The goal is to trick the user into clicking the malicious link that will then download a string of malware


Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear_____

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (Malicious link)

You are immediately advised to go through the cases above for safety hazard.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing

Source: KnowBe4

onto the victim's machine. The malware could lead to the theft or destruction of the victims' files. Another form of malware that could be downloaded is ransomware, which prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

(U) Recommendations and Tips

- Do not click links from untrusted sources.
- Be aware of potential malicious emails being disguised as emails from legitimate organizations.
- Be cautious of online offers for vaccinations.
- If uneasy about using certain websites for charitable donations, try searching for online ratings and reviews. Victims of fraudulent or improper sites may leave reviews to warn off others. Check for customer ratings and satisfaction before purchasing or sending money.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) has observed an increase in the registration of domain names containing the phrase "coronavirus." The domains include combinations of the words "help," "relief," "victims," and "recover." Of these domains, MS-ISAC noted that some seem malicious and the domains themselves appear suspect and should be viewed with caution.

(U) OUTLOOK

(U) The Commonwealth Fusion Center (CFC) Massachusetts Cybersecurity Program (MCP) is providing this information for situational awareness purposes only. At this time, the CFC has no intelligence indicating a specific or credible threat to the Commonwealth of Massachusetts.

(U) Please report any suspicious activity to your police department of jurisdiction and the Commonwealth Fusion Center at 978-451-3700.

For additional information or to be added to the MCP distribution list, please contact the MCP by email: MCPPOL@pol.state.ma.us.

This report addresses HSEC SINs: 1.1, 1.3, 1.8, 6
This report addresses CFC SINs: 1E, 1F MSPC1989/MSPC1977

Sources:

"Cyber Threat Actors Expected to Leverage Coronavirus Outbreak," CIS Security, Accessed 14 February 2020
"Coronavirus: Scammers follow the headlines," Federal Trade Commission, 10 February 2020
"FTC Warns of Ongoing Scams Using Coronavirus Bait," Bleeping Computer, 11 February 2020
"Coronavirus Phishing Attack Infects US, UK Inboxes," Dark Reading, 3 February 2020
"Coronavirus Attacks Aim to Spread Malware Infection," Info Security, 5 February 2020
"Hackers are riding on the global panic pertaining to the deadly Coronavirus," 10 February 2020