United States Secret Service [INFO]

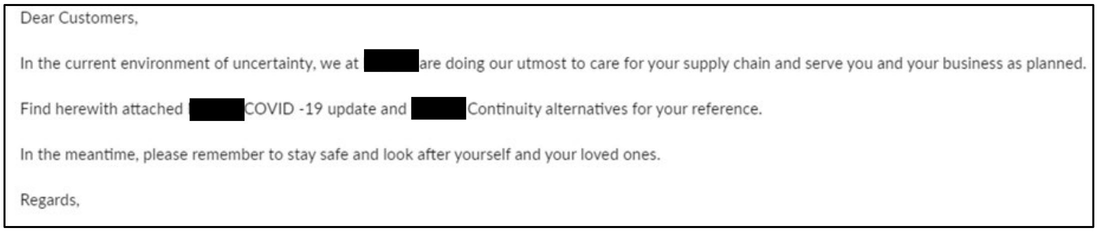
April 1, 2020

[INFO] Information Only Alert – GIOC Reference #20-006-I
TLP Green

Fraudulent COVID-19 Emails with Malicious Attachments

During the coronavirus outbreak, many companies and organizations have sent emails containing COVID-19 updates to their customers to make them aware of their current response and status. As these types of emails have now become increasingly frequent, criminals have started to use this familiarity to their advantage. The USSS is aware of fraudulent emails, framed as a corporate COVID-19 response, which contain malicious attachments and are targeting individual consumers and corporations alike.

In the attempted attacks we are aware of, the malicious attachment would allow the attackers to remotely install malware on the infected system to potentially harvest credentials, install keyloggers, or lockdown the system with ransomware. The impact of these type of attacks may not be immediately felt by the victim but may result in a BEC or other fraud in the future. The email attachment is frequently a Microsoft Office or WordPad file type, as so far, the attacks have utilized a now patched exploit of Microsoft Office. However, it is always possible that different variations exist, or the attack vectors will evolve. Corporations should be aware they are being targeted, with the attackers potentially posing as a vendor, member of the supply chain, or other familiar entities that would not seem out of place.



Dear Customers,

In the current environment of uncertainty, we at [redacted] are doing our utmost to care for your supply chain and serve you and your business as planned.

Find herewith attached [redacted] COVID -19 update and [redacted] Continuity alternatives for your reference.

In the meantime, please remember to stay safe and look after yourself and your loved ones.

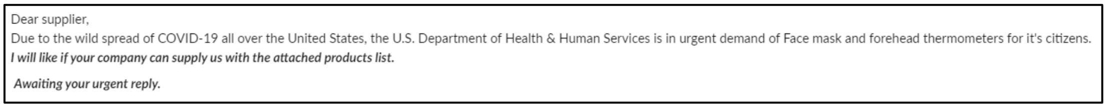
Regards,

The U.S. Secret Service has also received information regarding individuals receiving emails disguised as coming from a hospital that inform the recipient they may have come in contact with an individual who tested positive for COVID-19. The email instructs the recipient to download an attached Excel file, complete a form, and bring it to the nearest emergency clinic to be tested. As in the previous example, once the attachment is downloaded, the malware has been activated and the attackers may be able to:

- Steal log-in credentials for sites you have visited
- Look for open shares on the network and view all documents and folders
- Receive your IP address
- Discover and steal cryptocurrency wallet information

/RJ/

Another variation of this attack is an email purportedly from the U.S. Department of Health and Human Services. The email is targeting potential supplier companies by requesting they provide any medical protective equipment from an included product list with the attachment containing malware:



Dear supplier,
Due to the wild spread of COVID-19 all over the United States, the U.S. Department of Health & Human Services is in urgent demand of Face mask and forehead thermometers for it's citizens.
I will like if your company can supply us with the attached products list.

Awaiting your urgent reply.

In most instances referenced above, the email signature blocks used the identity of a legitimate employee. Keep in mind that typically, legitimate COVID-19 response emails have a message only in the body of the email and do not contain attachments.

The U.S. Secret Service is working with domestic and foreign law enforcement partners, along with the private sector, to disrupt and dismantle COVID-19 related fraud schemes. If anyone has any information related to this alert, the GIOC can be contacted at GIOC@usss.dhs.gov.

/RJ/