(U) VFC Highlight #20-27

Date: April 23, 2020; Tracked by: HSEC 1.8

(U) Title: Indicators of Fraud or Malware in Emails Marketing Medical Equipment or Personal Protective Equipment (PPE)

(U) Key Points

- (U) Cybercriminals are taking advantage of the current COVID-19 pandemic to circulate phishing emails to perpetuate scams and distribute malware.
- (U) Recent malicious emails center on the sale or provisioning of medical equipment or Personal Protective Equipment (PPE).
- (U) Emails may attempt to capitalize on human emotions related to fear and need. Messages observed have contained links or attachments that contain malware or redirect recipients to malicious websites.
- (U) Emails may be from third parties representing overseas companies, claiming to have appropriate, official scientific validation of their products.

(U) Possible Indicators of Concern Related to Fraudulent/Scam Emails Observed by VFC

- (U) Email of sender may be from a personal account that does not contain an organizational or commercial company domain (i.e. john.doe@gmail.com vs. john.doe@ourcompanyname.com)
- (U) The geographic address used in signature line is a residential instead of commercial location.
- (U) The sender of the email and the company they claim to represent has a minimal on-line footprint. Additionally, the company may have a recently established website.
- (U) The email may highlight a referral from a well-known public figure or authoritative individual.
- (U) Such emails may be sent to executive level personnel because they have publicly available contact information and they are in a position of authority to take action on the request contained within the email.

(U) Methods to Identify Potential Fraud or Malicious Emails

- (U) Utilize an internet search engine to research information contained in the email before clicking on links or attachments. This information can include email and physical addresses, company name, and telephone numbers.
- (U) If the sender claims to have been referred by a known government official or public entity, independently contact that official or entity for verification, using contact information obtained independently, not by what is provided in the email solicitation.
- (U) Check company domain names (i.e. yourcompanyname.com) through domain analysis tools such as urlscan.io.
- (U) Identify characteristics or factors that one would expect to be present for legitimate business interests in your industry (i.e. professional or business licenses). Consider having a process requiring solicitors to provide documentation consistent with the identified characteristics or factors associated with businesses in your industry. Many cyber criminals will not respond to these requests or be able to provide requested documentation.

(U) Additional Resources

- (U) COVID-19 Exploited by Malicious Cyber Actors—Cybersecurity & Infrastructure Security Agency (CISA)
- (U) FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic
- (U) Combating COVID-19 FRAUD—U.S. Department of Justice
- (U) PPE, COVID-19 Medical Supplies Targeted by BEC Scams— Threatpost

(U) Please report COVID-19 email scams to the VFC at vfc@vfc.vsp.virginia.gov.