FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 APRIL 2020

Alert Number

MI-000122-MW

WE NEED YOUR HELP!

If you find any of these indicators on your networks, or have related information, please contact **FBI CYWATCH immediately**.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals. This FLASH was coordinated with DHS-CISA.

This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

COVID-19 Email Phishing Against US Healthcare Providers

Summary

Following a global increase in malicious cyber activity exploiting fear derived from the COVID-19 pandemic, the FBI was notified of targeted email phishing attempts against US-based medical providers. These attempts leveraged email subject lines and content related to COVID-19 to distribute malicious attachments, which exploited Microsoft Word Document files, 7-zip compressed files, Microsoft Visual Basic Script, Java, and Microsoft Executables. The FBI is providing indicators of compromise related to these phishing attempts to assist network defenders in protecting their environments. Additionally, the FBI is providing the attached list of hashes related to additional COVID-19 phishing.

Technical Details

On 18 March 2020, network perimeter cyber security tools associated with US-based medical providers identified email phishing attempts from domestic and international IP addresses. The emails contained subjects related to the COVID-19 pandemic and included malicious files as attachments. These attachments were in the form of Microsoft Word Document files, 7-zip compressed files, Microsoft Visual Basic Script, Java, and Microsoft Executables. The capabilities of these malicious attachments are unknown, but they would have likely

created an initial intrusion vector to enable follow-on system exploitation, persistence, and exfiltration.

Indicators

Email Sender	Email Subject	Attachment Filename	Hash
srmanager@combytellc.com	PURCHASE ORDER PVT	Doc35 Covid Business Form.doc	babc60d43781c5f7e415e2354cf32a6a24badc96b971a3617714e5dd2d4a14de
srmanager@combytellc.com	PURCHASE ORDER PVT	Doc35 Covid Business Form.doc	babc60d43781c5f7e415e2354cf32a6a24badc96b971a3617714e5dd2d4a14de
srmanager@combytellc.com	Returned mail: see transcript for details	Covid-19_UPDATE_PDF.7z	de85ca5725308913782d63d00a22da480fcd4ea92d1bde7ac74558d5566c5f44
srmanager@combytellc.com	COVID-19 UPDATE !!	Covid-19_UPDATE_PDF.7z	de85ca5725308913782d63d00a22da480fcd4ea92d1bde7ac74558d5566c5f44
admin@pahostage.xyz	Information about COVID-19 in the United States	covid50_form.vbs	d231d81538b16728c2e31c3f9e0f3f2e700d122119599b052b9081c2c80ecd5c
help@pahofinity.xyz	Coronavirus (COVID-19)	covid27_form.vbs	d231d81538b16728c2e31c3f9e0f3f2e700d122119599b052b9081c2c80ecd5c
monique@bonnienkim.us	Business Contingency alert - COVID 19	COVID-19 Circular.jar	eacc253fd7eb477afe56b8e76de0f873259d124ca63a9af1e444bfd575d9aaae
info@mohap.gov.ae	Todays Update on COVID-19	Todays Update on COVID-19.exe	7fd2e950fab147ba39fff59bf4dcac9ad63bbcdfbd9aadc9f3bb6511e313fc9c
erecruit@who.int	World Health Organization/ Let,Äôs fight Corona Virus together	COVID-19 WHO RECOMENDED V.exe	d150feb631d6e9050b7fb76db57504e6dcc2715fe03e45db095f50d56a9495a5

erecruit@who.int	World Health Organization/ Let,Äôs fight Corona Virus together	COVID-19 WHO RECOMENDED V.exe	d150feb631d6e9050b7fb76db57504e6dcc2715fe03e45db095f50d56a9495a5
erecruit@who.int	World Health Organization/ Let,Äôs fight Corona Virus together	COVID-19 WHO RECOMENDED V.exe	d150feb631d6e9050b7fb76db57504e6dcc2715fe03e45db095f50d56a9495a5

Information Requested:

If you or your company are targeted by a phishing campaign, please provide the FBI with a copy of the email with the full email header and a copy of any attachments. Please do not open the attachment if you or your organization does not have the capability to examine the attachment in a controlled and safe manner. Additionally, if you or your company is a victim of a cyber intrusion related to email phishing, please retain any logs, image(s) of infected device(s), and memory capture of all affected equipment, if possible, to assist in the response by the FBI.

Recommended Mitigations

- Be wary of unsolicited attachments, even from people you know. Cyber actors can "spoof" the return address, making it look like the message came from a trusted associate.
- Keep software up to date. Install software patches so that attackers can't take advantage of known problems or vulnerabilities.
- If an email or email attachment seems suspicious, don't open it, even if your antivirus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the antivirus software might not have the signature.
- Save and scan any attachments before opening them.
- Turn off the option to automatically download attachments. To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and disable it.

- Consider creating separate accounts on your computer. Most operating systems give you the option of creating multiple user accounts with different privileges. Consider reading your email on an account with restricted privileges. Some viruses need "administrator" privileges to infect a computer.
- Apply additional security practices. You may be able to filter certain types of attachments through your email software or a firewall.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.