FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

4 May 2020

Alert Number

MI-000124-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 actors. 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 Phishing Email Indicators

Summary

The FBI uncovered targeted email phishing attempts to harvest user credentials and compromise targets' computer systems by exploiting fear derived from the COVID-19 pandemic. Through investigations, the FBI continues to identify multiple COVID-19 email phishing campaigns with malicious file attachments and URLs. The following associated indicators of compromise (IOCs) are being provided to assist in network defense.

Technical Details

Cybercriminal and advanced persistent threat (APT) groups are leveraging COVID-19 themed health, informational, and warning notice emails in an attempt to obtain online service credentials, e.g., Microsoft O365 accounts. These emails direct targets to click links by purporting to be online services requiring authentication. Malicious actors use these links to capture victim credentials and then redirect victims to the World Health Organization's (WHO) Coronavirus notice. Additionally, cybercriminals and APT groups have attached archive files that contain malicious portable executables (PE) or JAVA.jar files to their phishing emails, outlined in the table below.

Indicators

COVID-19 Themed Malware	
Filename:	AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_zip.jar
MD5:	bac2f22d53c6f2b43eba6adbb0f2ea9a
SHA-256:	f7b0d6d95f2644e32c22eb3e681e33387ac27d71dd73eee3ff37ce77985ab177
Magic:	Zip archive data
File Size:	685140 bytes
File Contents:	Filename: AWARENESS NOTICE ON CORONAVIRUS COVID-19 DOCUMENT_pdf.exe MD5: 9498ba71b33e9e9e19c352579e0d1b0a SHA-256: da26ba1e13ce4702bd5154789ce1a699ba206c12021d9823380febd795f5b002 File type: Win32 EXE Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit

Filename:	Covid-19_zip.bin
MD5:	08dd5ee67ee69ddfa11cb55562baef58
SHA-256:	3e1fb4ff54112a78d8bdccbe596c119201f079010c4f69cdf2c99385e7aee3dc
Magic:	Zip archive data
File Size:	998017 bytes
File Contents:	Filename: 1Original_document_exe.bin MD5: e7351df51633435293ddc09de7fdc57c SHA-256: 7b98cd3800dede6537cf78e7b61eeeda71d251dc97c70cb7c2135c6aa310ab7f File type: Win32 EXE Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit

Filename:	COVID-19.rar
MD5:	c49856a3df308e8b1739b357832c8e9b
SHA-256:	15e029c3834435150c76741e714540fcb799662db8cc2c61ba4ef192a781727b
Magic:	RAR archive data
File Size:	430116 bytes
File Contents:	Filename: Γενική ειδοποίηση χρονοδιαγράμματος εργασίας στο COVID-19 MD5: 62f9618752fffbd4ff7d52fdc39ec5fb SHA-256: f681c1f8c12956a20c27beb9be1112374fefc7651884d7dd92010b40db1e7bee File type: Win32 EXE Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit

Filename:	Attachments-Fwd_ Proforma for COVID-19.zip
MD5:	5da446b5f22bfa77a51b654762583a28
SHA-256:	47f1570e770d236836c0d3cb50755b6dd91e1be58a0d3e61507c7baacfd27784
Magic:	Zip archive data
File Size:	58332 bytes
File Contents:	Filename: Persons_status_details_list.xlsx MD5: 61d50cbcdc5c52588bd79736ac7dd5e0 SHA-256: d56bb81d0f8e4de24dc12a7d963ed95eec36291c71a29d6b434e72f098cc1131 File type: Office Open XML Spreadsheet Magic: Zip archive data

Filename:	COVID-19 WHO RECOMENDED V.gz
MD5:	378bbb172ccae5e28549a003e4e84bce
SHA-256:	43670ae43df9e361fa15f09f611da32db104ee207ed5af3e7e7f098ad82a68e0
Magic:	Zip archive data
File Size:	368339 bytes
File Contents:	Filenames: COVID-19 WHO RECOMENDED V.exe / YkZeIEiv.exe MD5: 1179a7989031fc4b6331505b388dcb12 SHA-256: d150feb631d6e9050b7fb76db57504e6dcc2715fe03e45db095f50d56a9495a5 File type: Win32 EXE Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly

Filename:	Covid 19 Immunity Tips (2).zip
MD5:	51b7f0213cb2945d42b88996761ce74b
SHA-256:	2c464648ff97fd39dab054d0c3e1bd249e244fcc975b697e312796669c7763f1
Magic:	Zip archive data
File Size:	377236 bytes
File Contents:	Filenames: Covid 19 Immunity Tips.exe MD5: 76fffeef410bd6b633c09c0f6529891d SHA-256: e4e5c3a6c15beff4e17117075e2c0bd65f176d81e6885134d2b4d97c20d4773a File type: Win32 EXE Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit Mono/.Net assembly

Filename:	zbetcheckin_tracker_COVID-19.jar
MD5:	e8973e617a743a5597b63ce268986761
SHA-256:	5b0ba8d58a64630cb5fcb80e72520bd2ef6f322003fa2588d4d594620e6685ae
Magic:	Zip archive data
File Size:	402345 bytes

COVID-19 Themed Phishing Campaign and Associated MD5 Hash Values	
e8973e617a743a5597b63ce268986761	51b7f0213cb2945d42b88996761ce74b
76fffeef410bd6b633c09c0f6529891d	378bbb172ccae5e28549a003e4e84bce
1179a7989031fc4b6331505b388dcb12	5da446b5f22bfa77a51b654762583a28
61d50cbcdc5c52588bd79736ac7dd5e0	c49856a3df308e8b1739b357832c8e9b
62f9618752fffbd4ff7d52fdc39ec5fb	e7351df51633435293ddc09de7fdc57c
08dd5ee67ee69ddfa11cb55562baef58	9498ba71b33e9e9e19c352579e0d1b0a
bac2f22d53c6f2b43eba6adbb0f2ea9a	

COVID-19 Themed Phishing Campaign and Associated URLs	
Date	URL
2020-02-21	https://soikeobongdahomnay[.]com/Ham/index.php
2020-02-26	https://cscic.fundashonaltonpaas[.]org/cm/index.php
2020-02-28	https://sportscambo[.]com/sisa/index.php
2020-03-09	https://tokoonlinebaru[.]com/co/index.php
2020-03-17	https://printlogz[.]com/ee/index.php
2020-03-18	http://printlogz[.]com/ee
2020-03-18	http://feenixlanguage[.]com/jog/index.php
2020-03-18	http://printlogz[.]com/ee/index.php
2020-03-18	https://feenixlanguage[.]com/han/index.php
2020-03-18	https://feenixlanguage[.]com/jog/index.php
2020-03-18	https://hpindl[.]com/fe/index.php
2020-03-18	http://hpindl[.]com/fe

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

- Scrutinize attachments and Website hyperlinks contained in e-mails, and do not open attachments included in unsolicited e-mails.
- 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.
- 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.
- 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.
- Implement application whitelisting to block the execution of malware, or at least block execution of files from TEMP directories, from which most phishing malware attempts to execute.
- Install and regularly update anti-virus or anti-malware software on hosts.
- Implement an update and patch management cycle. Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers.
- Implement an incident management system and prepare an incident response plan for rapid deployment in case of a cyber intrusion.
- Audit and increase security controls and password requirements for all network protocols, which could be used to move laterally or gain access to a network, specifically: file-sharing protocols, such as SMB, and remote network protocols, such as RDP, SSH, VPN, Telnet, and VNC.
- Limit and audit accessible files via SMB shares. Recommend limiting SMB accessibility through Active Directory Group Policies.
- Audit privileged accounts and implement principle of least privilege, especially for administrator accounts. Routinely audit administrator and business critical user accounts.
- Monitor for SSL or TLS traffic over non-standard ports.

- Require strong password requirements for local administrators to inhibit lateral movement across workstations.
- Upgrade PowerShell to new versions with enhanced logging features and centralize logs to detect use of commonly used malware-related PowerShell commands.
- Implement a data backup and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks and should not be updated in real time.

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.