TLP: GREEN

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21MAY2020

Alert Number

AC-000128 -LD

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the Reporting Notice section of this message.

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 in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), 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 in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Nation State Cyber Actors Target US Organizations Conducting COVID-19 Research

Summary

Nation-state cyber actors are targeting many domestic universities, research institutes, and private companies conducting COVID-19-related research. The FBI has observed malicious cyber actors conducting vulnerability scanning, reconnaissance activity, and attempted data exfiltration from entities involved in COVID-19 research and associated clinical trials. The potential compromise and theft of this information jeopardizes the delivery of secure, effective, and efficient treatment options and the United States' efforts to respond to the ongoing crisis.

Threat

US medical and pharmaceutical research has long been a target of state-sponsored cyber espionage. Similar to past public health crises, nation states are demonstrating increased targeting of this research for information gathering and data exfiltration in support of their domestic response operations and industry development. In the wake of the COVID-19 outbreak, multiple public and private sector research organizations conducting COVID-19 vaccine and treatment research and clinical trials have experienced increased reconnaissance and attempted data theft by nation-state cyber actors.

The following indicators of compromise (IOCs) were observed being used in the attempted attacks against organizations involved in COVID-19 vaccine, treatment, and testing programs:

IP Addresses:				
154.223.175.62	154.48.238.124	156.255.2.118	92.63.192.0/24	47.240.0.0/14
161.117.177.248	161.117.249.236	182.162.136.235	147.139.128.0/17	47.246.0.0/16
185.45.193.13	185.82.202.142	45.138.209.91	207.148.224.0/19	47.244.0.0/15
47.254.75.210	47.90.214.83	47.91.92.53	80.249.144.0/24	47.254.0.0/17
60.250.18.188	5.61.32.0/20	8.208.0.0/16	47.74.0.0/18	47.245.0.0/18
8.209.64.0/18	23.192.0.0/11	94.103.81.0/24	47.75.0.0/16	47.252.0.0/17
161.117.128.0/17	139.28.222.0/24	193.56.28.0/24	49.51.0.0/16	47.56.0.0/15
47.90.128.0/17	47.236.0.0/14	47.235.0.0/16	47.91.64.0/19	

Domains:			
0hpwca2c.on7kvm9y.site	8hh3aktk.kasprsky.info	airbus.mircosoft.site	restupdate1.xyz
api-asia-190.xyz	api-oberon-i.info	api-test10.xyz	salmonellen-entstehung.icu
api-test11.xyz	api-upload-i.info	api1800-i.xyz	statistics-ad.best
army17.com	army18.org	b1umby40.com	theone.jobsearchindex.com
b3d3fn9n.kasprsky.info	barbeyo.xyz	bertaysag.best	tworestupdate2.xyz
bsyu.dnslookup.services	c632bynt.xloli.xyz	ce1com.club	usstatupdate.org
chtoesli.info	ciliophora1.icu	ciliophora2.icu	wechatgifservice.com
cleanerpc.info	data.wechatgifservice.com	dnslookup.services	restupdate2.xyz
ecrm.ce1com.club	eduing.everywebsite.us	eulegion-update1.xyz	salmonellen.icu
eulegion-update2.xyz	eustatupdate.org	everywebsite.us	statistics-pro.best
fasters01.top	fasters02.top	fasters03.top	trade-softsinn.icu
fasters04.top	fasters05.top	geostatistics.org	uenoeakd.site
hootsulte.com	hotinstalls.com	installcensus.info	uuptimes.xloli.xyz
installneva.org	installtrades.me	jobsearchindex.com	xloli.xyz
juv0cumdo3.kasprsky.info	kasprsky.info	legion-update1.xyz	salmonella-symptome.icu
legion-update2.xyz	legion17.net	legion17.top	snowfall.icu

lmogv.dnslookup.services	minorr01.top	minorr02.top	tg9f6zwkx.icu
minorr03.top	minorr04.top	mircosoft.site	tworestupdate1.xyz
mplsvpn.everywebsite.us	myneva.net	myneva.org	ur1lwzh2qp.kasprsky.info
mynevainstall.org	nevainstall.org	nevainstalls.org	vt.mircosoft.site
ntusjneo3a.tg9f6zwkx.icu	oberon-a.org	oberon-t.org	perdator.xyz
oberon-trade-client.org	oberon-trade.com	oberon-trade.org	predwar.org
oberonapps.org	on7kvm9y.site	oneinstalls.com	predatorwar.org
orruucsl.xyz	pandastat.info	pjb.mircosoft.site	

The Common Vulnerabilities and Exposures (CVEs) used by malicious cyber actors to gain or attempt to gain access to US COVID-19 research include but are not limited to:

- Microsoft Exchange Server vulnerability CVE-2020-0688
- Citrix Vulnerability related to CVE-2019-19781
- Apache vulnerability related to CVE-2020-1938
- Secure VPN vulnerability CVE-2019-11510

To help reduce the overall risk from these exploitation attempts, the FBI recommends immediate installation of patches and implementation of corrective measures released by the vendors.

Recommendations

In addition to the recommendations provided below, please see the attached document for guidance on how to detect the illicit use of legitimate credentials.

- Assume that a press announcement affiliating your company or organization with COVID-19 related research will lead to increased interest and activity by nation-state cyber actors and cyber criminals on your network.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected servers for known vulnerabilities and software processing Internet data, such as web browsers, browser plugins, and document readers.
- Actively scan and monitor web applications for unauthorized access, modification, and anomalous activities.
- Strengthen credential requirements and implement multi-factor authentication to protect individual accounts, particularly for webmail and VPN access and for accounts that access critical systems. Change passwords and do not reuse passwords for multiple accounts.

- Recommend developing a network baseline to allow for the identification of anomalous account activity. Identify and suspend access of users exhibiting unusual activity (see attachment for guidance).
- Network device management interfaces, such as Telnet, SSH, Winbox, and HTTP, should be turned off for WAN interfaces and secured with strong passwords and encryption when enabled.
- Identify and suspend access of users exhibiting unusual activity.
- When possible, segment critical information on air-gapped systems. Use strict access control measures for critical data.
- Be mindful of new and existing cyber infrastructure for work and bioscience collaborations.

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 e-mail 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:GREEN. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.

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