TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

12 June 2020

PIN Number

20200612-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

Unattributed Cyber Actors Register Domains Spoofing Legitimate Airport Websites as a Possible Precursor to Future Operational Activity

Summary

The FBI has observed unattributed cyber actors registering numerous domains spoofing legitimate US-based airport websites, indicating the potential for future operational activity. Spoofed domains mimic legitimate domains by either altering character(s) within the domain or associating another domain with similar characteristics to the legitimate domain, such as “m1crosoft.com” or “microsoft-software.biz.” Spoofed domains are increasingly used by cyber criminal and state-sponsored groups to propagate the spread of malware, which can lead to further compromise and financial losses. As a result, this activity poses an increased risk not only to US airports but also to the greater US Aviation Sector and its myriad stakeholders.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

US airports are an attractive target for cyber actors due to a rich environment of business and personal information, wide use of information technology and operational technology systems, and numerous entities operating within the same environment. Cyber actors can capitalize on this complicated ecosystem by creating spoofed domains, which can trick both passengers and airport operators into interacting with malicious websites or e-mails. The initial attack vector, typically in the form of a website waterhole attack or a phishing e-mail, can lead to the collection of personally identifiable information (PII) and legitimate credentials, or plant malware on a system. As a result, cyber actors could potentially conduct a ransomware attack, sell customer and employee information on the dark web, exfiltrate sensitive business information, conduct money mule schemes, or alter existing routing numbers and bank accounts in order to divert vendor payments. Moreover, cyber actors can use this information and access to move laterally throughout a network, identifying additional systems of interest for further compromise or to conduct the targeting of an outside entity using trusted credentials. The following examples illustrate targeting of US airports observed by the FBI since March 2020.

- As of 5 March 2020, unknown actor(s) registered the domain www.phl-airport.com which closely mirrors that of the legitimate Philadelphia International Airport website (philadelphia.airport.com). The use of “phl” in the domain directly mirrors the airport’s International Air Transport Association code “PHL”. The actor(s) registered the domain using WhoisGuard, a privacy protection services, to anonymize the registration information. Images were used of the airport from publicly available Internet image searches.

- In late March 2020, unknown actor(s) registered multiple domains possessing the term “Greensboro airport” possibly in an effort to confuse flyers and/or customers. The Piedmont Triad International Airport serves the Greensboro, North Carolina, area.

- From March through May 2020, unknown actor(s) registered multiple domains possessing the term “webmail” likely in an effort to spoof legitimate airport email landing pages. For instance, these actors registered the domain “webmail.newark-airport.info.”

Recommended Mitigations

- Devise a continuity of operations plan for a potential cyber attack; prioritize the systems most important to continued operations.

- Use e-mail authentication protocols such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-Based Message Authentication Reporting and Conformance (DMARC), and Sender ID Framework (SIDF).

- Establish a training mechanism to inform end users on proper email and web usage, highlighting current information and analysis, and including common indicators of phishing. End users should have clear instructions on how to report unusual or suspicious emails.
- Regularly patch operating systems, software, and firmware.
- Update anti-malware and anti-virus software and conduct regular network scans.
- Use multi-factor authentication where possible.
- Audit networks and systems for unauthorized remote communication.
- Disable or remove unneeded software, protocols, macros, and portals.

Appendix A: Registered Domains

The Internet protocol (IP) address associated with the following 450 domains is identified as, 46.249.38.241. This IP address is assigned to Hostkey B.v. located in the Netherlands.

ns2.airphost.com	webmail.westchester-airport.com
ns1.airphost.com	whm.tampa-airport.net
mail.greensboro-airport.com	webdisk.westchester-airport.com
greensboro-airport.com	webmail.saipan-airport.com
webmail.greensboro-airport.com	webmail.st-louis-airport.com
webdisk.greensboro-airport.com	webdisk.saipan-airport.com
www.greensboro-airport.com	st-louis-airport.com
whm.greensboro-airport.com	www.san-antonio-airport.info
www.greensboro-airport.airphost.com	cpanel.tampa-airport.net
cpanel.greensboro-airport.com	www.westchester-airport.com
greensboro-airport.airphost.com	mail.san-antonio-airport.info
www.orlando-sanford-airport.com	webdisk.st-louis-airport.com
mail.orlando-sanford-airport.com	webmail.washingtondc-airport.com
webmail.newark-airport.info	mail.washingtondc-airport.com
orlando-sanford-airport.com	mail.pie-airport.com
webmail.orlando-sanford-airport.com	pie-airport.airphost.com
mail.newark-airport.info	www.pie-airport.airphost.com
www.mht-airport.com	cpanel.san-antonio-airport.info
cpanel.panamacity-airport.com	webdisk.missoula-airport.com

niagara-falls-airport.com	mail.tampa-airport.net
www.sju-airport.com	pie-airport.com
whm.orlando-sanford-airport.com	mail.missoula-airport.com
cpanel.orlando-sanford-airport.com	whm.missoula-airport.com
newark-airport.info	cpanel.westchester-airport.com
webmail.sju-airport.com	www.st-louis-airport.airphost.com
whm.newark-airport.info	washingtondc-airport.com
mail.mht-airport.com	webdisk.washingtondc-airport.com
orlando-sanford-airport.airphost.com	saipan-airport.com
webdisk.orlando-sanford-airport.com	whm.saipan-airport.com
www.sju-airport.airphost.com	webdisk.ict-airport.com
www.newark-airport.info	www.tampa-airport.net
webdisk.niagara-falls-airport.com	www.st-louis-airport.com
cpanel.newark-airport.info	cpanel.tri-cities-airport.com
webdisk.newark-airport.info	www.missoula-airport.com
msp-airport.com	webmail.san-antonio-airport.info
www.niagara-falls-airport.com	www.saipan-airport.airphost.com
www.orlando-sanford-airport.airphost.com	whm.ict-airport.com
webmail.pbi-airport.com	webmail.tampa-airport.net
cpanel.niagara-falls-airport.com	tampa-airport.net
webdisk.sju-airport.com	webmail.ict-airport.com
www.newark-airport.info	www.dca-airport.info
webdisk.niagara-falls-airport.com	whm.medford-oregon-airport.com
cpanel.newark-airport.info	mail.ict-airport.com
webdisk.newark-airport.info	mail.tri-cities-airport.com
msp-airport.com	webmail.dca-airport.info
www.niagara-falls-airport.com	cpanel.ict-airport.com
www.orlando-sanford-airport.airphost.com	medford-oregon-airport.airphost.com
webmail.pbi-airport.com	webdisk.tri-cities-airport.com
cpanel.niagara-falls-airport.com	webdisk.dca-airport.info
webdisk.sju-airport.com	cpanel.dca-airport.info
mht-airport.com	mail.dca-airport.info
whm.mht-airport.com	www.tri-cities-airport.com
sju-airport.airphost.com	mail.university-park-airport.com
mail.panamacity-airport.com	dca-airport.airphost.com
www.minot-airport.com	www.university-park-airport.com
www.msp-airport.com	medford-oregon-airport.com

webmail.panamacity-airport.com	webdisk.university-park-airport.com
mail.pbi-airport.com	whm.university-park-airport.com
panamacity-airport.com	whm.fortmyers-airport.com
www.mht-airport.airphost.com	webmail.medford-oregon-airport.com
webdisk.msp-airport.com	www.medford-oregon-airport.com
sju-airport.com	www.medford-oregon-airport.airphost.com
cpanel.sju-airport.com	webdisk.medford-oregon-airport.com
whm.niagara-falls-airport.com	webdisk.fortmyers-airport.com
whm.msp-airport.com	mail.medford-oregon-airport.com
webmail.msp-airport.com	cpanel.university-park-airport.com
webdisk.panamacity-airport.com	dca-airport.info
msp-airport.airphost.com	fortmyers-airport.com
cpanel.mht-airport.com	whm.dca-airport.info
mail.niagara-falls-airport.com	www.amarillo-airport.airphost.com
webdisk.pbi-airport.com	amarillo-airport.airphost.com
mht-airport.airphost.com	www.dca-airport.airphost.com
cpanel.msp-airport.com	university-park-airport.com
webmail.niagara-falls-airport.com	mail.fortmyers-airport.com
mail.msp-airport.com	www.fortmyers-airport.airphost.com
webdisk.mht-airport.com	cpanel.fortmyers-airport.com
webmail.mht-airport.com	www.fortmyers-airport.com
whm.panamacity-airport.com	webmail.fortmyers-airport.com
www.panamacity-airport.com	fortmyers-airport.airphost.com
www.msp-airport.airphost.com	little-rock-airport.info
mail.sju-airport.com	cpanel.tucson-airport.info
minot-airport.airphost.com	webmail.myrtlebeach-airport.com
webdisk.minot-airport.com	webmail.mem-airport.com
webmail.minot-airport.com	webmail.manchester-airport.net
cpanel.pbi-airport.com	cpanel.rdu-airport.com
whm.sju-airport.com	rdu-airport.com
whm.pbi-airport.com	tucson-airport.info
www.minot-airport.airphost.com	mail.phl-airport.com
www.pbi-airport.com	yeager-airport.airphost.com
mail.minot-airport.com	webmail.phl-airport.com
minot-airport.com	whm.myrtlebeach-airport.com
pbi-airport.com	www.yeager-airport.com
cpanel.minot-airport.com	webdisk.phl-airport.com

whm.minot-airport.com	whm.sanfrancisco-airport.com
www.bna-airport.com	webmail.rdu-airport.com
webmail.bna-airport.com	whm.reno-airport.net
whm.bna-airport.com	savannah-airport.airphost.com
mke-airport.com	sjc-airport.airphost.com
www.oak-airport.com	pit-airport.com
mercedita-airport.com	mail.tucson-airport.info
mail.mlb-airport.com	cpanel.ogg-airport.com
cpanel.mlb-airport.com	mail.pit-airport.com
www.mlb-airport.com	whm.manchester-airport.net
bna-airport.com	webdisk.manchester-airport.net
mail.bna-airport.com	www.oma-airport.com
webdisk.mlb-airport.com	webdisk.sjc-airport.com
cpanel.oak-airport.com	mail.little-rock-airport.info
whm.mlb-airport.com	cpanel.ric-airport.com
webmail.mlb-airport.com	mail.ogg-airport.com
oak-airport.com	mail.salt-lake-airport.com
mlb-airport.com	whm.pit-airport.com
www.mercedita-airport.com	cpanel.salt-lake-airport.com
cpanel.bna-airport.com	www.ric-airport.com
webdisk.bna-airport.com	whm.savannah-airport.com
mail.mercedita-airport.com	webdisk.salt-lake-airport.com
mke-airport.airphost.com	www.sanfrancisco-airport.airphost.com
webmail.oak-airport.com	whm.salt-lake-airport.com
mail.oak-airport.com	mail.sandiego-airport.com
webmail.mercedita-airport.com	mail.mem-airport.com
www.mke-airport.airphost.com	whm.little-rock-airport.info
webdisk.mercedita-airport.com	mail.seattle-tacoma-airport.com
webmail.mke-airport.com	whm.ric-airport.com
www.mke-airport.com	webmail.ogg-airport.com
whm.mke-airport.com	mem-airport.com
cpanel.mercedita-airport.com	www.tampa-airport.airphost.com
mail.mke-airport.com	ogg-airport.com
whm.mercedita-airport.com	whm.yeager-airport.com
webdisk.oak-airport.com	mail.rdu-airport.com
cpanel.mke-airport.com	mail.manchester-airport.net
mercedita-airport.airphost.com	webdisk.mem-airport.com

www.mercedita-airport.airphost.com	www.pit-airport.com
whm.oak-airport.com	www.pvd-airport.com
webdisk.mke-airport.com	mail.yeager-airport.com
www.amarillo-airport.com	webdisk.myrtlebeach-airport.com
www.phoenix-sky-harbor.com	manchester-airport.net
whm.moline-airport.com	phl-airport.com
mail.phoenix-sky-harbor.com	rdu-airport.airphost.com
cpanel.amarillo-airport.com	www.reno-airport.net
cpanel.plattsburgh-airport.com	webmail.sjc-airport.com
webdisk.amarillo-airport.com	tri-cities-airport.airphost.com
mail.amarillo-airport.com	pvd-airport.com
whm.amarillo-airport.com	www.savannah-airport.com
webmail.amarillo-airport.com	mail.oma-airport.com
plattsburgh-airport.com	www.rdu-airport.com
webdisk.plattsburgh-airport.com	mail.myrtlebeach-airport.com
www.niagara-falls-airport.airphost.com	webdisk.yeager-airport.com
mail.plattsburgh-airport.com	whm.rdu-airport.com
whm.plattsburgh-airport.com	www.yeager-airport.airphost.com
plattsburgh-airport.airphost.com	whm.oma-airport.com
www.plattsburgh-airport.airphost.com	www.myrtlebeach-airport.com
niagara-falls-airport.airphost.com	webmail.oma-airport.com
webmail.plattsburgh-airport.com	webdisk.rdu-airport.com
amarillo-airport.com	www.tri-cities-airport.airphost.com
www.plattsburgh-airport.com	webmail.savannah-airport.com
www.newark-airport.airphost.com	www.rdu-airport.airphost.com
webmail.phoenix-sky-harbor.com	mail.sjc-airport.com
phoenix-sky-harbor.airphost.com	www.sandiego-airport.airphost.com
newark-airport.airphost.com	salt-lake-airport.com
cpanel.moline-airport.com	pit-airport.airphost.com
www.mlb-airport.airphost.com	tampa-airport.airphost.com
phoenix-sky-harbor.com	cpanel.sanfrancisco-airport.com
webdisk.palmsprings-airport.com	cpanel.myrtlebeach-airport.com
panamacity-airport.airphost.com	myrtlebeach-airport.com
whm.phoenix-sky-harbor.com	www.manchester-airport.net
webmail.moline-airport.com	webmail.yeager-airport.com
mail.moline-airport.com	www.phl-airport.airphost.com
www.pbi-airport.airphost.com	whm.phl-airport.com

www.panamacity-airport.airphost.com	cpanel.phl-airport.com
www.moline-airport.com	ric-airport.airphost.com
pbi-airport.airphost.com	www.phl-airport.com
cpanel.palmsprings-airport.com	webmail.little-rock-airport.info
whm.palmsprings-airport.com	phl-airport.airphost.com
www.phoenix-sky-harbor.airphost.com	whm.pvd-airport.com
www.oak-airport.airphost.com	cpanel.mem-airport.com
webdisk.phoenix-sky-harbor.com	webmail.pvd-airport.com
palmsprings-airport.airphost.com	yeager-airport.com
mail.palmsprings-airport.com	mail.sanfrancisco-airport.com
cpanel.phoenix-sky-harbor.com	www.pvd-airport.airphost.com
palmsprings-airport.com	www.tucson-airport.info
mlb-airport.airphost.com	cpanel.manchester-airport.net
www.bna-airport.airphost.com	mail.pvd-airport.com
webdisk.moline-airport.com	webmail.sanfrancisco-airport.com
www.palmsprings-airport.com	cpanel.yeager-airport.com
www.palmsprings-airport.airphost.com	webdisk.sanfrancisco-airport.com
moline-airport.com	www.missoula-airport.airphost.com
oak-airport.airphost.com	www.sjc-airport.airphost.com
webmail.palmsprings-airport.com	webmail.pit-airport.com
bna-airport.airphost.com	cpanel.pvd-airport.com
san-antonio-airport.info	whm.sjc-airport.com
cpanel.saipan-airport.com	webdisk.pit-airport.com
cpanel.missoula-airport.com	webdisk.pvd-airport.com
westchester-airport.com	cpanel.sjc-airport.com
mail.saipan-airport.com	missoula-airport.airphost.com
missoula-airport.com	webmail.salt-lake-airport.com
cpanel.st-louis-airport.com	www.sjc-airport.com
tri-cities-airport.com	seattle-tacoma-airport.airphost.com
webmail.tri-cities-airport.com	sanfrancisco-airport.airphost.com
webmail.missoula-airport.com	salt-lake-airport.airphost.com
www.san-antonio-airport.airphost.com	sanfrancisco-airport.com
www.saipan-airport.com	webmail.seattle-tacoma-airport.com
mail.westchester-airport.com	www.pit-airport.airphost.com
webmail.pie-airport.com	cpanel.little-rock-airport.info
webdisk.pie-airport.com	www.sanfrancisco-airport.com
san-antonio-airport.airphost.com	webdisk.oma-airport.com

whm.pie-airport.com	whm.mem-airport.com
webdisk.tampa-airport.net	tucson-airport.airphost.com
whm.westchester-airport.com	www.mem-airport.com
st-louis-airport.airphost.com	mail.savannah-airport.com
mail.st-louis-airport.com	sjc-airport.com
www.ict-airport.com	www.university-park-airport.airphost.com
www.pie-airport.com	webdisk.sandiego-airport.com
moline-airport.airphost.com	cpanel.oma-airport.com
www.moline-airport.airphost.com	pvd-airport.airphost.com
ict-airport.com	whm.tucson-airport.info
cpanel.washingtondc-airport.com	cpanel.savannah-airport.com
www.washingtondc-airport.com	cpanel.sandiego-airport.com
cpanel.medford-oregon-airport.com	webdisk.ric-airport.com
whm.tri-cities-airport.com	www.salt-lake-airport.com
saipan-airport.airphost.com	webdisk.little-rock-airport.info
whm.san-antonio-airport.info	cpanel.pit-airport.com
whm.washingtondc-airport.com	webdisk.tucson-airport.info
webmail.university-park-airport.com	www.reno-airport.airphost.com
whm.st-louis-airport.com	webmail.ric-airport.com
webdisk.san-antonio-airport.info	whm.seattle-tacoma-airport.com
cpanel.pie-airport.com	ric-airport.com

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@ic.fbi.gov or (202) 324-3691.

Administrative Note

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

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.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey