Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

09 January 2020

PIN Number

20200109-001

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

Email:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients 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 PIN has been released **TLP:WHITE** Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Notice on Iranian Cyber Tactics and Techniques

Summary

The FBI assesses foreign cyber actors operating in the Islamic Republic of Iran, one of two nation-states known to have conducted destructive cyber attacks inside the United States, could potentially use a range of Computer Network Operations (CNO) against US-based networks in retaliation for last week's strikes against Iranian military leadership. The FBI has observed an increase in Iranian cyber reconnaissance activity since last week's strike. Among the most common and effective methods Iranian cyber actors use to conduct CNO are spear-phishing, virtual private network (VPN) vulnerability targeting, and password spray attacks, which enable remote access and allow Iran to gather information to counter perceived threats to their regime. Businesses and individuals in the United States whom this activity may target include those involved in industries of interest to Iran, including academia, government, cleared defense contractors, and non-governmental organizations focusing on Iranian issues.

Malicious activity and reconnaissance may not necessarily occur from Iranian Internet Protocol space, as actors may utilize midpoint infrastructure in other countries. As such, traffic from Iranian IP addresses may not be indicative of malicious activity.

Details

The FBI has identified several high-level tactics and techniques employed by Iranian cyber actors to gain access to targeted systems and individual accounts. The FBI is providing information concerning these tactics and techniques to ensure situational awareness and proper network defense postures.

Spear-phishing

The FBI assesses Iranian cyber actors use spear-phishing to capture credentials of targeted individuals, including usernames, passwords, and multi-factor authentication (MFA) codes. The FBI has observed spear-phishing emails imitating legitimate correspondence from popular email and other well-known online services, such as file sharing or job-seeking services. The objective of these spear-phishing efforts is to trick the target into believing the actors' message is actually from the legitimate service, enticing the user to click on a link provided in the message. Unbeknownst to the user, the link directs the user to a spoofed login page crafted by the malicious actors and not to a legitimate login page. When the user enters his or her username and password into the spoofed page, the malicious actors capture these credentials. The actors are then able to confirm the captured username and password by using them on the individual's legitimate login page to complete the sign-in. The process appears seamless to the user, who remains unsuspicious and unaware their credentials have been stolen. The FBI further warns that this could be done even if users have MFA enabled, as the malicious actors can tailor a spoofed login page to capture any MFA code provided by the user, in addition to the username and password. Successfully compromising user accounts provides malicious actors with access to a wealth of information, including personally identifiable information, financial information, personal and professional contacts (including family and friends), travel plans, private correspondence, etc. Malicious actors can then leverage this information in various ways, which pose additional dangers to compromised victims.

Virtual Private Network Vulnerability Targeting

Separately, the FBI has information indicating Iranian cyber actors have attempted to exploit Common Vulnerability and Exposures (CVEs) 2019-11510 and 2018-13379, pertaining to VPNs. The FBI assesses this targeting, which has occurred since late 2019, is broadly scoped and has affected numerous sectors in the United States and other countries. The FBI has observed actors using information acquired from exploiting these vulnerabilities to further access targeted networks, and establish other footholds even after the victim patched the vulnerability. The FBI further warns that entities which may not be of interest to the Government of Iran could be follow-on targets for cyber-criminal activity on the part of the actors. The FBI advises this activity may not necessarily occur directly from Iranian IP address space, and entities deploying these VPN products are advised to investigate to see if any suspicious activity occurred over the past few months – especially if these vulnerabilities were not patched at the time.

For mitigation, the FBI recommends reviewing the information and recommendations provided in National Security Agency Cybersecurity Advisory: Mitigating VPN Vulnerabilities. (Release No: PA-010-19, 7 October 2019)

Password Spray Attack Activity

In March 2018, the FBI disseminated the FLASH message “Malicious Cyber Activity of Iran-based Mabna Institute” (Alert Number ME-000092-TT). The FLASH detailed coordinated and broadly targeted password spray attacks against organizations in the United States and abroad. Victims of the attacks often lack multi-factor authentication (MFA), lack preventative network activity alerts, and allow easy-to-guess passwords (e.g., “Winter2018”, “Password123!”). The FBI recommends reviewing the information and mitigation recommendations provided in the FLASH, as it assesses these techniques continue to be used with success.

Defense

- Be aware of unsolicited contact on social media from any individual you do not know personally.
- Be aware of attempts to pass links or files via social media from anyone whom you do not know.
- Be aware of unsolicited requests to share a file via online services.

- Be aware of email messages conveying suspicious alerts or other online accounts, including login notifications from foreign countries or other alerts indicating attempted unauthorized access to your accounts.
- Be suspicious of emails purporting to be from legitimate online services. (e.g. the images in the email appear to be slightly pixelated and/or grainy, language in the email seems off, messages originate from an IP not attributable to that provider/company, etc.).
- Be suspicious of unsolicited email messages that contain shortened links (i.e. via tinyurl, bit.ly, etc.).
- Use security features provided by social media platforms, use strong passwords, change passwords frequently, and use a different password for each social media account.
- Patch CVEs 2019-11510 and 2018-13379 if you are deploying products affected by these vulnerabilities.

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.

Administrative Note

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

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