Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

22 May 2018

PIN Number
20180522-001

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

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: 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.

Advisory: Continued Iranian Cyber Threats to US Private Industry

Summary

The FBI assesses foreign cyber actors operating in the Islamic Republic of Iran could potentially use a range of Computer Network Operations (CNO)—from scanning networks for potential vulnerabilities to data deletion attacks—against US-based networks in response to the US Government's withdrawal from the Joint Comprehensive Plan of Action (JCPOA). Iranian cyber actors have previously launched cyber attacks against symbolic targets in the United States in retaliation for perceived slights against the regime. The FBI assesses Iranian cyber actors could view the JCPOA withdrawal as justification for increased malicious cyber activity directed against US-based networks.

Between December 2011 and August 2013, two organizations with ties to the Government of Iran launched Distributed Denial of Service (DDoS) attacks targeting US financial institutions' forward-facing Web sites, likely in response to sanctions affecting the Iranian economy.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

In 2014, Iranian cyber actors launched a data deletion attack against the network of a US-based casino. This attack was likely in response to public comments made by the CEO regarding the Iranian regime.

From 2016 to 2017, malicious Iranian cyber actors conducted coordinated and broadly targeted intrusion campaigns against US companies, academic institutions, and government entities. The FBI encourages US companies to report suspicious network activities to local FBI offices or FBI CyWatch.

Threat

To increase awareness of this potential threat, the FBI is providing the following table outlining Iran's recent cyber targets, TTPs, and related results.

Target/Victim	TTPs	Result
Academic Sector	- Spear-phishing - Password Spray	- Spear-phishing and Password spray allowed actors to access networks and escalate privileges without triggering account lockout. - Confidential and proprietary information was compromised. (FBI FLASH ME-000092-TT)
Commercial Sector	- Spear-phishing - Data deletion malware	- Spear-phishing allowed unauthorized access to networks, and gave the actors the access to wipe hard drives connected to the network.
Financial Sector	- DDoS	- Distributed Denial of Service attacks prevented customers from accessing financial websites, disrupting normal business activity. (FBI PIN 160324-001)

Government Sector	- Spear-phishing - Password Spray	- Spear-phishing and Password spray attacks allowed actors to access networks and escalate privileges without triggering account lockout. - Confidential and proprietary information was compromised. (FBI FLASH ME-000092-TT)

Measures to deter unauthorized access to a company network:

• Educate personnel on appropriate preventative and reactive actions to known criminal schemes and social engineering threats, including how employees should respond in their respective positions and environments.

• Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.

• Disable macros. Be careful of pop-ups from attachments that require users to enable them.

• Only download software—especially free software—from known and trusted sites.

• Create a centralized Information Technology e-mail account for employees to report suspicious e-mails.

• Change network default passwords, configurations, and encryption keys. Use strong passwords.

• Recommend your company's IT professional(s) review, test, and certify the need/compatibility of a patch or update prior to installing it onto the operating system or software.

• Monitor employee logins that occur outside of normal business hours.

• Restrict access to the Internet on systems handling sensitive information.

• Install and regularly update anti-malware solutions, software, operating systems, remote management applications, and hardware.

- Do not use the same login and password for multiple platforms, servers, or networks.
- Monitor unusual traffic, especially over non-standard ports. Close unused ports.
- Monitor outgoing data, and be willing to block unknown IP addresses.
- Isolate sensitive information within the network.
- Only allow required processes to run on systems handling sensitive information.
- Implement two-factor authentication for access to sensitive systems.
- Ensure proper firewall rules are in place.
- Conduct searches using multiple search engines on multiple Internet domains of company names, Web addresses, key personnel, and projects to determine if there is an accidental weak point in the network security. Conduct infrastructure look-ups in the public domains to ensure additional information is not inadvertently advertised.

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.

Administrative Note

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