ACTIVITY ALERT

AA18-305 NUMBER

November 1, 2018 DATE

IRANIAN CYBER THREATS TO U.S. PRIVATE INDUSTRY

CONTENTS

SUMMARY

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and the Federal Bureau of Investigation (FBI) assess Iran may seek to launch retaliatory cyberattacks against the United States in response to resumed sanctions against Iran's energy, financial, and shipping sectors. These sanctions will be re-imposed on November 5, 2018, due to the U.S. withdrawal from the Joint Comprehensive Plan of Action (JCPOA). NCCIC and FBI recommend organizations remain vigilant and aware of potential malicious cyber activity ahead of the renewed economic sanctions against Iran.

Malicious cyber actors operating in Iran could potentially use a variety of Computer Network Operations to launch attacks against U.S.-based networks in response to the U.S. Government's withdrawal from the JCPOA. Iran has previously conducted retaliatory and intelligence gathering cyber operations against U.S. organizations in order to protect the regime, including distributed denial of service (DDoS) attacks, data deletion attacks, and intellectual property theft. NCCIC and FBI would like to note the following historic Iran-nexus cyber activity:

- Between December 2011 and May 2013, Iranian cyber actors conducted DDoS attacks against U.S. financial institutions in response to U.S. sanctions against the Iranian banking system. Activity was sporadic between December 2011 and August 2012. However, between September 2012 and May 2013, approximately 46 financial institutions across the United States were affected by persistent DDoS activity, resulting in tens of millions of dollars in remediation costs.

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise. This document is distributed as TLP:GREEN: Limited disclosure, restricted to the community. 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. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp.

NCCIC

Federal Bureau of Investigation

- In 2014, Iranian cyber actors launched a data deletion attack against a U.S.-based casino's network. The attack was likely retaliation for political remarks the casino's chief executive officer made against Iran.
- Between 2013 and 2017, Iranian cyber actors conducted targeted spear-phishing operations against U.S. universities and companies, resulting in billions of dollars of intellectual property theft.

MITIGATIONS

The following are recommended defensive techniques and programs, which are further detailed in the reports linked in the Resources section below:

Securing Network Infrastructure Devices

- Segment and segregate networks and functions.
- Limit unnecessary lateral communications.
- Harden network devices.
- Secure access to infrastructure devices.
- Perform Out-of-Band network management.
- Validate integrity of hardware and software.

Brute Force Attack Mitigations

- Enable multi-factor authentication (MFA) and review MFA settings to ensure coverage over all active, internet-facing protocols.
- Review password policies to ensure they align with the latest NIST guidelines and deter the use of easy-to-guess passwords.
- Review IT helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts. IT helpdesk password procedures may not align to company policy, creating an exploitable security gap.
- Offer additional assistance and tools that can help detect and prevent password spray attacks, such as the Microsoft blog released on March 5, 2018.

DDoS Attack Mitigations

- Enroll in a denial of service (DoS) protection service that will detect abnormal traffic flows and redirect traffic away from your network. The DoS traffic is then filtered out, while clean traffic is passed on to your network.
- Create a disaster recovery plan to ensure successful and efficient communication, mitigation, and recovery in the event of an attack.
- Install and maintain antivirus software.
- Install a firewall and configure it to restrict traffic coming into and leaving your computer.
- Evaluate security settings and follow good security practices in order to minimalize the access other people have to your information and to manage unwanted traffic.

Avoiding Social Engineering Attacks

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information or follow links provided in a suspicious email.
- Do not send sensitive information over the internet before checking a website's security.
- Pay attention to the uniform resource locator (URL) of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group.
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your email client and web browser.

Best Practices

- Implement a vulnerability assessment and remediation program.
- Encrypt all sensitive data in transit and at rest.
- Create an insider threat program.
- Assign additional personnel to review logging and alerting data.
- Complete independent security (not compliance) audits.
- Create an information sharing program.
- Complete and maintain network and system documentation to aid in timely incident response, including network diagrams, asset owners, type of asset, and an up-to-date incident response plan.

RESOURCES

- DDoS: https://www.us-cert.gov/ncas/tips/ST04-015
- Social Engineering: https://www.us-cert.gov/ncas/tips/ST04-014
- Brute Force: https://www.us-cert.gov/ncas/alerts/TA18-086A
- Securing Network Infrastructure Devices: https://www.us-cert.gov/ncas/tips/ST18-001
- NIST Password Guidance: https://pages.nist.gov/800-63-3/
- Microsoft. Azure AD and ADFS best practices: Defending against password spray attacks: https://cloudblogs.microsoft.com/enterprisemobility/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/

The United States Government provides these resources for informational purposes only. The United States Government does not endorse the author or content of any non-federal resources linked above.

CONTACT INFORMATION

To report an intrusion and request resources for incident response or technical assistance, contact NCCIC at (NCCICCustomerService@hq.dhs.gov or 888-282-0870), FBI through a local field office, or the FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937)

FEEDBACK

NCCIC continuously strives to improve its products and services. You can help by answering a few short questions about this product at the following URL: https://www.us-cert.gov/forms/feedback