Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

20 October 2022

PIN Number

20221020-001

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False-Flag Personas

Summary

The FBI is providing information concerning ongoing hack-and-leak cyber operations conducted by Iranian cyber group Emennet Pasargad. According to FBI information, since at least 2020, Emennet targeted entities primarily in Israel with cyber-enabled information operations that included an initial intrusion, theft and subsequent leak of data, followed by amplification through social media and online forums, and in some cases the deployment of destructive encryption malware. To avoid attribution, Emennet executed false-flag campaigns under the guise of multiple personas like hacktivist or cyber-criminal groups. Although Emennet's latest attacks have primarily targeted Israel, the FBI judges these techniques may be used to target US entities as seen during Emennet's cyber-enabled information operation that targeted the 2020 US Presidential election[1]. Within the past year, the FBI has identified a destructive cyber attack against a US organization – indicating the group remains a cyber threat to the United States.

[1] For previous FBI reporting on Emennet Pasargad's cyber-enabled information operation targeting the 2020 US Presidential election and additional context, please see FBI advisories *Indicators of Compromise Pertaining to Iranian Interference in the 2020 US Presidential Election* (ME-000138-TT https://www.ic3.gov/Media/News/2020/201030.pdf), and *Context and Recommendations to Protect Against*

Threat

According to FBI information the Iranian cyber threat group Emennet Pasargad has been conducting hack-and-leak operations against organizations primarily in Israel. The FBI assesses the purpose of these operations is to undermine public confidence in the security of the victim's network and data, as well as embarrass victim companies and targeted countries. These hack-and-leak campaigns involve a combination of hacking/theft of data and information operations that impact victims via financial losses and reputational damage. Similar to the Emennet campaign against the 2020 US Presidential election, the FBI judges the group's campaigns include a mix of computer intrusion activity and exaggerated or fictitious claims of access to victim networks or stolen data to enhance the psychological impact of their operations.

In early 2022, Emennet conducted a cyber attack against a US-based organization as a means to target the Iranian opposition group The People's Mujahedin (aka MEK). As a part of this operation, Emennet leaked information concerning personally identifiable information (PII) they presumably obtained via their compromise of the organization's network. Emennet's activity resulted in destructive effects on victim infrastructure. The FBI warns that organizations, which Iran perceives as affiliated with the MEK, are at an elevated risk of cyber exploitation or attack activities.

Although Emennet personas may exaggerate their level of access to a victim network or the volume of victim data stolen, the FBI judges that each of these campaigns likely start with some level of cyber intrusion. Historically, the actors choose victims by conducting online research into leading businesses across several sectors. Emennet cyber actors typically demonstrate a preference for websites running PHP code or those with externally accessible myssql databases. In most cases, these actors then use open source penetration testing tools such as SQLmap and Acunetix. In addition to Emennet's hack-and-leak operations, these actors have used website defacements and destructive encryption malware to cause further harm to victims' networks. Emennet is likely more opportunistic in choosing victims rather than targeting specific entities. However, victim trends appear to show their preference for companies with significant traffic and a large customer base.

In furtherance of Emennet's information operations, the group often amplifies and promotes the theft and leaking of victim data on their own dedicated leak websites, Telegram, and online hacking and illicit access trading forums. The actors typically create social media accounts for each false-flag persona to generate additional attention to their activity. The FBI has also observed Emennet amplifying information operations through techniques such as contacting

Malicious Activity by Iranian Cyber Group Emennet Pasargad (PIN-20220126-001 – https://www.ic3.gov/Media/News/2022/220126.pdf).

news media organizations and using email-marketing services. This is a tactic previously observed during their campaign against the 2020 US Presidential election.

The FBI previously disseminated a Private Industry Notification on Emennet Pasargad on 26 January 2022. In this product, the FBI identified numerous Tactics, Techniques, and Procedures used by this cyber threat actor. The FBI is re-emphasizing Emennet's focus on the below techniques to highlight how the group enables access to target websites. Emennet will leverage their access to edit content on victim websites in an effort to further their information operations. The FBI further assesses Emennet will likely conduct research for newly identified vulnerabilities pertaining to the below:

- Commonly used Content Management Systems, including specifically Drupal and Wordpress
- Ckeditor

The FBI along with multiple US and foreign partners disseminated a Joint Cybersecurity Advisory on 22 December 2021. The advisory provided mitigation guidance related to vulnerabilities in Apache's Log4j software library. Emennet exploited a Log4j vulnerability CVE-2021-44228 for at least one US-based organization that allowed the actors to access the organization's web server. Emennet cyber actors used destructive capabilities to take down the organization's web server and associated websites.

Observed Emennet Pasargad Personas

The FBI attributes the below false-flag personas to Emennet Pasargad. Attribution was achieved through analysis of FBI acquired information.

Hackers of Savior

Pro-Palestinian Hacktivist Group Persona – Active between 2020 and 2022

Emennet used the false-flag hacking group persona 'Hackers of Savior' at several points between May 2020 and April 2022. During that timeframe, Emennet conducted four cyber campaigns that targeted entities across multiple sectors in Israel. The campaigns, most of which occurred around Qods Day, involved hack-and-leak activity and website defacements. Their latest actions, which occurred in April 2022, involved a blended campaign of hacking and psychological operations for the purpose of promoting a political narrative.

Deus

Cyber-Criminal Persona – Active in 2021

Emennet operated under the cyber-criminal persona of Deus while conducting a lock-and-leak operation targeting an Israeli call service center. According to reports, Emennet cyber actors encrypted victim computers and leaked company data. Emennet then offered to sell the data

on public forums, and used a Deus Telegram channel to amplify their messaging regarding the intrusion and leaked documents.

Recommendations

The FBI recommends our partners remain vigilant and if the behaviors outlined in this notification are observed, to contact their local FBI 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. The FBI recommends the following mitigation efforts:

- If a member of your organization receives messages threatening the release of stolen PII or other data, please contact your local FBI office or CyWatch.

- Immediately identify, mitigate, and update affected products that use Log4j to the latest patched version.

    - For environments using Java 8 or later, upgrade to Log4j version 2.17.0 (released December 17, 2021) or newer.
    - For environments using Java 7, upgrade to Log4j version 2.12.3 (released December 21, 2021). Note: Java 7 is currently end of life and organizations should upgrade to Java 8.

- The actors consistently use Virtual Private Network services such as NordVPN, Private Internet Access, and TorGuard VPN. The FBI believes operational infrastructure will almost exclusively be created from and accessed by VPN exit nodes of these services.

- Disable Content Management Systems features if they are not needed, and configure them to:
    - Disable remote file editing
    - Restrict file execution to specific directories
    - Limit login attempts

- Consider reputable hosting services for websites and content management systems (CMS), if you need assistance in configuring and maintaining your external facing applications.

- The FBI provided common vulnerabilities exploited by Emennet in a January 2022 Pin titled *Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad.* Please ensure, if applicable to your network, these

vulnerabilities are remediated. The PIN may be found here - https://www.ic3.gov/Media/News/2022/220126.pdf.

- Consider employing a Web Application Firewall (WAF) to block inbound malicious traffic.
- Review the logs generated by security devices for signs that your organization's external networks are being scanned for vulnerabilities.
- Employ regular updates to applications and the host operating system to ensure protection against known vulnerabilities.
- Establish, and backup offline, a "known good" version of the relevant server and a regular change management policy to enable monitoring for alterations to servable content with a file integrity system.
- Employ user input validation to restrict local and remote file inclusion vulnerabilities.
- Implement a least-privileges policy on the Webserver to:
    - Reduce adversaries' ability to escalate privileges or pivot laterally to other hosts.
    - Control creation and execution of files in particular directories.
- If not already present, consider deploying a demilitarized zone (DMZ) between the Web-facing systems and corporate network. Limiting the interaction and logging traffic between the two provides a method to identify possible malicious activity.
- Ensure a secure configuration of Webservers. All unnecessary services and ports should be disabled or blocked. All necessary services and ports should be restricted where feasible. This can include whitelisting or blocking external access to administration panels and not using default login credentials.
- Use a reverse proxy or alternative service to restrict accessible URL paths to known legitimate ones.
- Conduct regular system and application vulnerability scans to establish areas of risk. While this method does not protect against zero day attacks, it will highlight possible areas of concern.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. 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

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