- Risk Management
- Compliance
- Privacy
- Supply Chain
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Cyberwarfare

FBI Warns of Hacker Attacks Conducted by Iranian Cyber Firm

By Eduard Kovacs on January 28, 2022

Share Tweet 推荐 0 RSS

The FBI this week issued a private industry notification to warn organizations about the malicious activities conducted by an Iranian cyber company named Emennet Pasargad.

The agency has described their tactics, techniques and procedures (TTPs) and it has shared several recommendations for preventing and detecting attacks.

In November 2021, the U.S Treasury Department announced sanctions against six Iranian nationals and a company involved in a campaign whose goal was to influence the 2020 presidential election.

The company in question is Emennet Pasargad, previously known as Eeleyanet Gostar and Net Peygard Samavat — the company has regularly rebranded to evade U.S. sanctions. Emennet has provided cybersecurity services within Iran, including to government organizations.

On the day the Treasury announced the sanctions, the Justice Department announced charges against two of Emennet’s employees, who were allegedly responsible for hacking and misinformation activities related to the presidential election.

In the alert issued this week, the FBI noted that in addition to its election-focused operation, the Emennet threat actor conducted “traditional cyber exploitation activity,” targeting sectors such as news, shipping, travel, oil and petrochemical, telecoms, and financial. They targeted the United States, Europe and the Middle East.

The hackers leveraged various VPNs to hide their location, and used several open source and commercial tools in their operations, including SQLmap, Acunetix, DefenseCode, Wappalyzer, Dnsdumpster, Netsparker, wpscan, and Shodan.

In the reconnaissance phase of their hacking operations, the threat actor chose potential victims by searching the web for major organizations representing various sectors. They would then try to find vulnerabilities in their software for initial access.

“In some instances, the objective may have been to exploit a large number of networks/websites in a particular sector as opposed to a specific organization target. In other situations, Emennet would also attempt to identify hosting/shared hosting services,” the FBI said.

The hackers were also observed targeting popular content management systems such as WordPress and Drupal, as well as exposed databases. In many cases they attempted to use default passwords to gain access to a targeted system.

“FBI information indicates the group has attempted to leverage cyber intrusions conducted by other actors for their own benefit. This includes searching for data hacked and leaked by other actors, and attempting to identify webshells that may have been placed or used by other cyber actors,” the FBI said.

Related: U.S., U.K. and Australia Warn of Iranian APTs Targeting Fortinet, Microsoft Exchange Flaws

Related: U.S. Imposes Sanctions on 'APT39' Iranian Hackers

Related: Twitter Removes Iran-Linked Accounts Aimed at Disrupting U.S. Presidential Debate

Share Tweet 推荐 0 RSS

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia’ s security news reporter. Eduard holds a bachelor’ s degree in industrial informatics and a master’ s degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

Network Security Firm Portnox Raises $22 Million in Series A Funding
Vulnerabilities in Swiss E-Voting System Earn Researchers Big Bounties
FBI Warns of Hacker Attacks Conducted by Iranian Cyber Firm
French Ministry of Justice Targeted in Ransomware Attack
Microsoft Saw Record-Breaking DDoS Attacks Exceeding 3 Tbps

Tags: