LIFARS
your digital world, **secured**

The Threat of Iranian Hackers

The Threat of Iranian Hackers

Based on the current tense situation in the world- U.S elimination of the Iranian general associated with terrorist attacks- there is a present threat of cyberattacks against U.S. and allied targets. Iran's long history of cyberattacks against Western infrastructures and strong cyber presence make it highly likely threat actors, more or less affiliated with Iran, will engage in cyberattacks. Iranian threat actors are known to be able to disrupt critical infrastructure, target government organizations and officials, as well as to compromise large corporate networks thus disrupting operations for days or weeks.

APT groups considered to be affiliated with Iran, including state sponsored groups, are known to target critical infrastructures, specifically utility (energy and transportation) and financial sectors. It is probable that these groups will target other sectors in the U.S. as well.

The purposes of these attacks are to cause disruption, to steal information, to create fear by posting threatening messages on defaced websites, to perform espionage activities, and to hit targets with ransomware attacks.

Known Iranian APT groups include:

- APT33:
  - Interests in aviation and energy sectors
- APT39
  - Interests in telecommunications and travel industries
- Charming Kitten
  - Interests in public personalities including media, research and activists
- Cleaver
  - Interests in aviation, educations, chemical, transportation, military sectors
- CopyKittens
  - Interests against multiple targets such as Israel, Turkey, and the U.S
- Group5
  - Interests to Syrian opposition groups and other focus in the Middle East
- LeafMiner
  - Interests in government and business organizations in the Middle East
- Magic Hound
  - Interest against multiple targets in the Middle East

- Muddy water
  - Interest in telecommunications and oil sectors
- OilRig
  - Interests in the financial, government, energy, chemical, and telecommunications sectors

Analysis of TTPs (tools, techniques, and procedures) in the past have shown that attacks are initiated with user or perimeter attacks.

This includes:

User Attacks:

- Use of spear phishing emails:
  - Users received emails with a link with infected HTML Applications (hta files) or infected attachment
- Use of Fake LinkedIn and Facebook profile to the entice user to click on infected email/ attachment
- Use of watering hole attacks
  - A particular set of users are observed and targeted

Perimeter Attacks:

- Password spraying (especially against Outlook on Web)
  - Attackers attempt to access accounts by submitting a large number of usernames with a few common passwords.
- Leaked credentials use
  - Attackers use credentials acquired in previous attacks and compromises to login into accounts of interest.

After compromising the endpoints, attackers can play out the following tasks:

- Credential dumping (endpoints and domain) – Mimikatz, Lazagne, GPP passwords, used for lateral movement into the network and to access restricted data.
- Keystroke and screen capture of users.

- Use of DarkComet, Remexi, PowerShell Empire, NanoCore, Pupy and njRAT remote access tools (RAT) to spy and create a backdoor on the network, eventually taking control of compromised computers
- Use of DownPaper Trojan, a backdoor trojan, that is used to run the second stage of malware.
- Creation of scheduled tasks on a victim's computers to run executables or malware at a certain date and time.
- Use of RDP, SSH,psexec, Cobalt strike and custom payloads for lateral movement into networks.
- Use of webshells such as ANTAK or ASPXSPY to remotely control Internet facing web servers.
- Use of malware digitally signed with stolen certificates to avoid detection by antivirus software.
- Creation of new users on compromised machines to gain further control of endpoints and networks.
- Use of javaScript, vbscript or powershell code to execute malicious scripts.
- Exfiltration of emails, databases and files of interests

Known exploited vulnerabilities

- CVE-2018-20250: A WinRAR vulnerability which manipulates ACE files to allow remote code execution.
- CVE-2017-0213: A Windows COM privilege escalation vulnerability that is used to elevate privileges within a network.

LIFARS Incident Response and Digital Forensics Team Recommendations

LIFARS recommends organizations implement the following protections:

User credentials authentication protection:

- Ensure password complexity (at least 10 characters long, including lowercase, uppercase, and special characters).
- Train users for security awareness; educate users on corporate policies/procedures and increase awareness of security risks.
- Perform phishing and spear phishing social engineering tests.
- Minimize privileges of all users, input access control where necessary and only grant access where needed.

Perimeter Infrastructure Protection:

- Patch all publicly facing technologies (web portals, databases, and other services) with the most recent version.
- Ensure high complexity of passwords for all users; force reset of passwords every six months.
- Disable access to administrative interfaces from the Internet; consider restricting access to these interfaces only from a few IP addresses assigned to the operational staff.

- Implement two-factor authentication to limit the impact of stolen or guessed credentials.
- Protect all publicly available machines with Intrusion Prevention Systems (IPS) and firewalls to monitor malicious activity and incoming traffic.
- Perform external penetration tests; remediate the findings from such tests.

Endpoint Protection:

- Implement an up-to-date, centrally managed antimalware solution.
- Implement strong and monitored 24/7 EDR solution wherever possible.
- Ensure that OS, applications and all installed software are up-to-date and use supported version, and/or compensating controls are implemented on system, which are not possible to upgrade to supported version
- Implement endpoint isolation on user segments by implementing Private Virtual Local Area Network (PVLAN)
- Implement application whitelisting where possible to ensure that only business accepted applications can run.
- Harden all endpoints to at least CIS level 1, which ensures basic security requirements are met.
- Perform vulnerability scans and internal penetration tests; implement the recommendations prioritizing based on findings criticality and severity.

Organization Protection:

- Harden windows domain by implementing strong domain policy based on industry standards, such as Microsoft Guidelines on AD Security.
- Ensure that the organization is capable of monitoring perimeter, endpoints and network, from Level 1 to Level 3, and if needed, Level 3 is reinforced by an external detection and response provider.
- Verify the incident management processes are in place up to the most recent version of incident playbooks, and Incident Response Tabletop exercises are conducted on a quarterly basis.

Conclusion:

The heightened tensions between Iran and the U.S. present a real concern of elevated cyber-attacks on the U.S. and its allies. APT groups, more or less affiliated with Iran, such as APT33 and Muddy Water, target critical infrastructure sectors such as energy and oil in an attempt to cause mass disruptions. Protecting your organization following LIFARS Incident Response and Digital Forensics Team's recommendations can alleviate the risk of attack by threat actors.

Worried about Attacks Against Your Organization?
For Incident Response and Threat Intelligence consultancy Contact LIFARS Today
Email:contact@lifars.com | **Call us at**:(212) 222-7061