



Emennet Pasarged Iranian Threat Group

CRITICALITY



17/11/2022

Recommendations



Prevention



Detection



Remediation



Response



MITRE ATT&CK

Summary

Emennet Pasarged is a private Iranian threat group conducting hack-and-leak cyber operations against United States, Israel, Europe, and Middle East.



Threat Details

Emennet Pasarged (aka Eeleyanet Gostar) is a private Iranian threat group conducting hack-and-leak cyber operations against the United States, Israel, Europe, and the Middle East. The main purposes of their campaigns are to embarrass the victims and support the political aims of the Iranian government.

The Emennet threat actors are known for their cybercrimes during the 2020 presidential election in the US. As reported by the FBI, they hacked voting records, ran disinformation campaigns, and directly targeted US government officials. Moreover, they sent threatening emails to intimidate voters and crafted and disseminated disinformation about the election and election security. Besides, an online operation was executed to intimidate and influence American voters, undermine voter confidence, and sow discord by impersonating the far-right extremist group The Proud Boys in an email threatening thousands of prospective voters in Florida.

As observed, Emennet Pasarged's behaviour is based on hack-and-leak operations, social media manipulation, and false-flag personas. For example, creating fake social media accounts, impersonating accounts, contacting news media organizations, and using email-marketing services to exaggerate the group's operations (this is a tactic previously observed during their campaign against the 2020 US Presidential election). They also promote victims' data on their own dedicated leak websites, Telegram, and online hacking and illicit access trading forums.

Further analysis of Emennet's Tactics, Techniques, and Procedures (TTPs) indicate that they exploit known vulnerabilities and software applications including WordPress (revslider and layerslider plugins), Drupal, Apache Tomcat, Ckeditor and FCKeditor (exploitation of Roxy Fileman). Also, targeting webpages running PHP code and identifying externally accessible MySQL databases (in particular, phpMyAdmin). For Virtual Private Networks (VPN), they used TorGuard, CyberGhost, NordVPN, and Private Internet Access. For penetration testing, they depend on open-source tool SQLmap and the commercial tool Acunetix during operational activity. Other tools including DefenseCode Web Security Scanner, Wappalyzer, Dnsdumpster, Tiny mce scanner, Netsparker, Wordpress security scanner (wpscan), and Shodan.



Recommendations



Prevention

- **Appendix A** contains the recommendations to prevent such attacks.



Detection

- **Appendix B** contains a sample of Indicators of compromise of this threat the full list is in the attached file.

References

FBI. (2020, October 29). *Indicators of Compromise Pertaining to Iranian*. Retrieved from FBI FLASH:
<https://www.ic3.gov/Media/News/2020/201030.pdf>

FBI. (2022, October 20). *Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False-Flag Personas*. Retrieved from Private Industry Notification:
<https://www.ic3.gov/Media/News/2022/221020.pdf>



Contact Us

Bahrain National CERT - National Cyber Security Center "NCSC"

Email: CERT@ncsc.gov.bh



Appendix A – Prevention

The National Cyber Security Center recommends all the entities to follow the below steps:

- Ensure that all your systems have endpoint protection software installed and up to date.
- Regularly run vulnerability assessments on your internet facing systems.
- Regularly review your systems, especially internet facing systems, for misconfigurations
 - Make sure that accounts do not use the default password.
 - Ensure that all server components are up to date.
 - Ensure that the admin page is not accessible to the public.
 - Ensure that directory traversal is not allowed.
 - Ensure that services are running using service accounts. Never run services using administrator accounts.
- For WordPress:
 - Make sure WordPress, plugins, and themes are up to date.
 - Only install trustable WordPress plugins and themes.
- Ensure backup of important data.
- Ensure that all your systems are up to date.
- Make sure to follow OWASP's top 10 to secure web applications.
- Remove the default admin user.
- Use strong passwords and Two Factor Authentication (2FA).
- Periodically review users' permissions.
- Limit login attempts to prevent a Brute Force attack.



Appendix B – Indicators of Compromise

Indicators of Compromise

Domains

- hxxp[:]//eeleyanet[.]ir – 5[.]144[.]130[.]40

IP Addresses

- 93.119.208[.]86
- 92.223.89[.]X
- 92.223.89[.]224
- 92.223.89[.]212
- 88.202.178[.]104
- 70.32.0[.]107
- 64.44.81[.]36
- 45.131.211[.]246
- 37.235.103[.]27
- 212.102.45[.]X
- 212.102.45[.]23
- 212.102.45[.]13
- 185.191.207[.]X
- 185.191.207[.]164
- 184.170.241[.]13
- 156.46.54[.]X
- 156.146.55[.]X
- 156.146.55[.]195
- 156.146.54[.]X
- 156.146.54[.]58
- 156.146.54[.]45
- 154.3.251[.]56
- 145.239.110[.]112
- 104.237.232[.]153



- 103.205.140[.]X
- 185.183.32[.]177
- 92.223.89[.]191
- 92.223.89[.]187
- 92.223.89[.]172
- 212.102.45[.]63
- 185.191.207[.]179
- 128.90.56[.]147
- 104.140.54[.]91
- 91.239.206[.]181
- 91.223.106[.]201
- 91.223.106[.]148
- 89.165.43[.]244
- 5.160.253[.]152
- 46.45.138[.]100
- 185.191.207[.]36
- 185.191.207[.]184
- 176.53.23[.]252
- 103.205.140[.]30
- 103.205.140[.]177

Detected Emails

- sidafin[@]mihanmail[.]ir
- safary.mansoor[@]gmail[.]com
- support[@]yahoolinkexchange[.]com
- faranakbehjati[@]yahoo[.]com
- amirhaghighi2014[@]yahoo[.]com
- h.boloukat[@]gmail[.]com
- Rahimi[@]Live[.]com



Appendix C – Best Practices

Bahrain National CERT team recommends organizations to implement the following best security practices.

- Backup daily important new/changed data, software and configuration settings, store disconnected data retained for at least three months. Test restoration initially, annually, and when IT infrastructure changes.
- Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- Restrict administrative privileges to operating systems and applications based on user role. Regularly reassess the need for privileges. Don't use privileged accounts to read emails or to browse the web.
- Configure Microsoft Office macro settings to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
[http://www.asd.gov.au/publications/protect/Microsoft Office Macro Security.pdf](http://www.asd.gov.au/publications/protect/Microsoft%20Office%20Macro%20Security.pdf)
- Whitelist applications of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- Harden user application. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- Activate multi-factor authentication for VPNs, Outlook Web Access (OWA), RDP, SSH and other remote access for all users when they perform a privileged action or access an important (sensitive or high-availability) data repository.
- Implement CIS Critical Security Controls while prioritizing the implementation of the top 5 CIS Controls. (<https://www.cisecurity.org/critical-controls.cfm>)
- Implement strategies to mitigate cyber security incidents. (<http://www.asd.gov.au/infosec/mitigationstrategies.htm>)

CERT.bh recommends organizations to implement the following strategies to detect and respond to cyber security incidents:

- Use network-based intrusion detection/prevention system using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
- Use The host-based intrusion detection/prevention system to identify anomalous behaviour during program execution e.g. process injection, keystroke logging, driver loading and persistence mechanisms.
- Use endpoint detection and response software on all computers to centrally log systems' behaviour and facilitate incident response. Microsoft's free Symon tool is an entry level option.
- Enhance visibility through PowerShell logging to provide investigators a detection mechanism for malicious activity and a historical record of how PowerShell was used on systems.
https://www.fireeye.com/blog/threat-research/2016/02/greater_visibility.html
- Hunt to discover incidents using threat intelligence consisting of analyzed threat data with indicators of compromise and mitigating threats based on behaviour patterns.



-
- Capture network traffic to and from internal systems that store important data or are considered critical assets, and network traffic traversing the network perimeter, to assist with incident detection and analysis.
 - Detect and response to incidents continuously with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access, network activity.
 - Refer to MITRE Corporation which provides a public repository that includes a model and framework for describing the actions attackers may take while operating within an enterprise network. These details can aid organizations in detecting attacker activities.
 - https://attack.mitre.org/wiki/Main_Page
 - https://car.mitre.org/wiki/Full_Analytic_List
 - <https://car.mitre.org/caret/#/>



Appendix D – TLP Definitions

RED

For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that **TLP:AMBER+STRICT** restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

GREEN

Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction