FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

29 OCT 2020

Alert Number

ME-000138-TT

**Note: This information is being provided by the FBI to assist cyber security specialists protect against the persistent malicious actions of cyber criminals. The information is provided without any guaranty or warranty and is for use at the sole discretion of the recipients.*

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals. This FLASH was coordinated with DHS/CISA.

This FLASH has been released **TLP:WHITE**: Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Indicators of Compromise Pertaining to Iranian Interference in the 2020 US Presidential Election

Summary

On 22 October 2020, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) published a joint Cybersecurity Advisory (Alert AA20-296B) warning that Iranian advanced persistent threat (APT) actors are likely intent on influencing and interfering with the US elections to sow discord among voters and undermine public confidence in the US electoral process. APT actors are creating fictitious media sites and spoofing legitimate media sites to spread anti-American propaganda and misinformation about voter suppression.

The Cybersecurity Advisory followed a joint press conference from the Director of National Intelligence (DNI) and FBI Director on election security, alerting the American public that Iran had taken specific actions to influence public opinion relating to the 2020 US Presidential Election.

The FBI is now providing a list of indicators of compromise (IOCs) pertaining to a threat group, assessed to be located in Iran, conducting operations aimed at influencing and interfering in the 2020 US Presidential Election.

Technical Details

The FBI is providing the below list of identified IP addresses previously used as part of an Iran-based campaign to conduct operations aimed at impacting the 2020 US Presidential Election, to include voter intimidation emails and dissemination of US election-related propaganda. The FBI has high confidence these IP addresses were used by the Iranian group on the corresponding dates. Please note many of these IP addresses likely correspond to Virtual Private Network (VPN) services which can be used by individuals all over the world. While this creates the potential for false positives, any activity on the below would likely warrant further investigation.

This group has been linked to efforts to disseminate a propaganda video concerning voter fraud and hacking of US voter information. The FBI advises this video is almost certainly intended to make US voter information and the voting process appear insecure and susceptible to fraud. The FBI advises that certain demonstrational activity in the video [e.g., a purported Structured Query Language (SQL) injection to obtain US voter information] may have been fabricated by the actors for psychological effect.

The video shows actors using the SQLmap tool. While the video alone does not necessarily validate whether the actors successfully conducted a SQL injection against US election infrastructure and/or obtained voter information, it should be assumed that this group is familiar with traditional TTPs such as SQL injection and other exploitation methods referenced in AA20-296B. While there is reason to doubt the veracity of the activity portrayed in the video, the FBI advises this group is likely capable of exploiting US Web sites with common vulnerabilities.

The below IOC list includes several Class C ranges (e.g., 212.102.45.X). This is based on the expectation that the group may have used, or may use in the future, IPs in those ranges based on known VPN service usage. Many VPN service IPs linked to the group are from the NordVPN service, and these IPs may not necessarily correspond to VPN services via IP address lookup services. The VPN service IPs may correspond to providers such as:

- Provider name variants including “CDN77”
- Provider name variants including “HQSERV”
- Provider name variants including “M247”

IP address	Timeframe
93.119.208.86	13 October 2020
92.223.89.X (range)	August - September 2020
92.223.89.224	12 September 2020
92.223.89.212	6 September 2020
88.202.178.104	20 October 2020
70.32.0.107	21 October 2020
64.44.81.36	12 September 2020
45.131.211.246	21 October 2020
37.235.103.27	16 October 2020 – 17 October 2020
212.102.45.X (range)	October 2020
212.102.45.23	21 October 2020
212.102.45.13	12 October 2020
185.191.207.X (range)	February - September 2020
185.191.207.164	19 September 2020
184.170.241.13	17 October 2020 - 19 October 2020
156.46.54.X (range)	October 2020
156.146.55.X (range)	October 2020
156.146.55.195	15 October 2020
156.146.54.X (range)	October 2020
156.146.54.58	20 October 2020

IP address	Timeframe
156.146.54.45	18 October 2020
154.3.251.56	16 October 2020 - 21 October 2020
145.239.110.112	20 October 2020
104.237.232.153	13 October 2020 – 19 October 2020
103.205.140.X (range)	October 2020
185.183.32.177	October 2020
92.223.89.191	19 August 2020 - 25 August 2020
92.223.89.187	26 August 2020
92.223.89.172	26 August 2020
212.102.45.63	24 August 2020
185.191.207.179	29 July 2020
128.90.56.147	23 June 2020
104.140.54.91	23 August 2020
91.239.206.181	23 April 2019
91.223.106.201	10 March 2020
91.223.106.148	22 February 2020
89.165.43.244	24 February 2020
5.160.253.152	24 February 2020
46.45.138.100	3 May 2020
185.191.207.36	17 September 2019

IP address	Timeframe
185.191.207.184	18 February 2020
176.53.23.252	31 May 2020
103.205.140.30	11 March 2020
103.205.140.177	10 March 2020

Best Practices for Network Security and Defense:

- 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.
- Deploy a Web application firewall and conduct regular virus signature checks, application fuzzing, code reviews, and server network analysis.

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 https://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, **TLP:WHITE** information may be distributed without restriction.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:
https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only. Reporting of technical information regarding FLASH reports must be submitted through FBI CYWATCH.