FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

21 January 2020

Alert Number

ML-000115-TT

WE NEED YOUR HELP!

If you identify any suspicious activity within your enterprise or have related information, please contact **FBI CYWATCH** immediately with respect to the procedures outlined in the **Reporting Notice** section of this message.

Email:

cywatch@fbi.gov

Phone:

1-855-292-3937

**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 has been released **TLP: GREEN**: The information in this product is useful for the awareness of all participating organizations within their sector or community, but should not be shared via publicly accessible channels.

Additional Website Defacement Activity Indicators of Compromise and Techniques Used to Disseminate Pro-Iranian Messages

Summary:

On 10 January 2020, the FBI disseminated the FLASH message "**Website Defacement Activity Indicators of Compromise and Techniques Used to Disseminate Pro-Iranian Messages**" (ML-000114-TT) after the FBI observed increased reporting of website defacements disseminating pro-Iranian messages. FLASH message ML-000114-TT provided indicators of compromise (IOCs), and tactics, techniques, and procedures (TTPs) associated with the reported pro-Iranian website defacement activity.

The FBI is disseminating this follow-on FLASH message based on the identification of additional IOCs and TTPs. The FBI advises organizations and people concerned with Iranian cyber activity review FLASH message ML-000114-TT and Private Industry Notification (PIN) "**Notice on Iranian Cyber Tactics and Techniques**" (20200109-001, 9 January 2020).

Technical Details:

The FBI identified the below strings and link in file "iran.php," which was used in a website defacement:

Filename	String
iran.php	Hacked By Liosion_team, Defacer, Hacker, Hacked, Hacked By, Mrb3hz4d
	Hacked By Iranian_Hackers
	Hacked BY Mrb3hz4d & MR_Liosion & H43ER & T4arik[J3N] & NikbinHK & ImanGorji & EbRaHiM-VaKeR & Perilous Man & BigNorouzi
	Official Teams: Liosion Team & Storm Security Team
	TelegramID==> @Mrb3hz4d
	Warning: This game will have a tough end.
	Down With USA
	http://s7.picofile[.]com/file/8383747492/5271925.jpg

The FBI identified the following files and MD5 hash values associated with website defacement activity:

Filename	MD5
3.php	301b7bb7e44a589e7dd2265ea62464e6
iran.php	596daf9a5610ea0834e186583225cf5d
wp-gdipt.php	85cd14f3c4d2e52e4004a9a692874a5f
wp-muen.php	02b9ba379a469fabe9e93e5af674e638
wp-updatee.php	60a7e9a733a6ad5dbfa507338774d0f7

FBI Comment: The FBI notes file "wp-muen.php" was base64 encoded.

The FBI identified file "jsspwned.php" was associated with website defacement activity. The below IP addresses interacted with "jsspwned.php." The FBI believes these IP addresses are associated with the actor responsible for some defacement activity:

Filename	IP Address
jsspwned.php	195.181.168[.]138
	195.181.168[.]142

Separately, the FBI identified the below IP address associated with website defacement activity. This defacement activity was likely the result of a Structured Query Language injection attack:

IP Address
45.227.255[.]58

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.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Administrative Note:

This product is marked **TLP: GREEN**. Recipients may share **TLP: GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

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.