FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

10 January 2020

Alert Number

ML-000114-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.

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

Summary:

Following last week's US airstrikes against Iranian military leadership, the FBI observed increased reporting of website defacement activity disseminating Pro-Iranian messages. The FBI believes several of the website defacements were the result of cyber actors exploiting known vulnerabilities in content management systems (CMSs) to upload defacement files. The FBI advises organizations and people concerned with Iranian cyber targeting be familiar with the indicators, tactics, and techniques provided in this FLASH, as well as tactics and techniques provided in recently disseminated Private Industry Notification "Notice on Iranian Cyber Tactics and Techniques" (20200109-001, 9 January 2020).

Technical Details:

The FBI identified malicious actors leveraging known vulnerabilities in CMSs to upload defacement images onto victim websites. The FBI believes one actor leveraged known vulnerabilities allowing remote execution via cookie and remote installation. The FBI also identified that one of the files used in a defacement was posted to a website where the server hosting the

compromised website was configured so external users could conduct HTTP POSTs. The FBI observed the use of an HTTP PUT command to upload a defacement file to a victim server.

The FBI notes different actors conducted website defacement activity with pro-Iranian messages. As such, the IP addresses and techniques used will vary. The FBI identified the below groupings of defacement activity.

One set of defacement activity used the below file:

Filename	MD5
Default.aspx	87b3b80bb214c0f5cfa20771dd6625f2

The following links, contact information, and strings were included in a defacement file:

https://anonymousfiles[.]io/f/photo_2020-01-03_04-42-19_6777572386023010304.jpg
http://uupload[.]ir/files/5h2a_15112.jpg
http://yon[.]ir/6YL2X
https://t[.]me/ZetaTech_iR2
https://instagram[.]com/Mrb3hz4d
hackedbymrb3hz4d(at)gmail[.]com

The following IP addresses are associated with the actor linked to the defacement activity with the above referenced links, contact information, and strings:

IP Address
83.123.83[.]61
196.64.50[.]13

A second set of defacement activity was identified using the below file:

Filename
hardrevenge11.html

The FBI notes the above defacement image was uploaded via an HTTP PUT command. The following IP address is associated with the actor linked to this set of defacement activity:

IP Address
2.182.188[.]39

A third set of defacement activity was identified using the below IP address:

IP Address
212.92.114[.]228

The FBI notes for this defacement activity, the actor was able to conduct an HTTP POST of a file used in a defacement.

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.

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.