WE NEED YOUR HELP!
If you find any of these indicators on your networks, or have related information, please contact FBI CYWATCH immediately.
Email: cywatch@ic.fbi.gov
Phone: 1-855-292-3937

*Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.

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 to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This FLASH has been released TLP:AMBER: Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.

IP Addresses and Domains Used by Likely Iran-Based Cyber Actors to Attack Victims Worldwide

Summary
The FBI assesses a group of malicious cyber actors—likely located in Iran—use Virtual Private Server infrastructure hosted in the United States to compromise government, corporate, and academic computer networks based in the Middle East, Europe and the United States. This infrastructure is used in conjunction with identified malicious domains to support a broad cyber campaign which likely includes the use of e-mail spear phishing, social engineering, and malicious Web sites (“watering hole attack”). These cyber actors almost certainly have been involved in this activity since at least early-2015.

Through a combination of FBI and private sector analysis, it is likely the actors involved with this activity are located in Iran. At least some victim information from this cyber activity transits US-based infrastructure to IP addresses located in Iran. At least one identified malicious domain was registered by a presumed Iranian national connected to a physical address in Tehran, Iran. The majority of the victims were located in Middle Eastern countries known to be traditional adversaries of the Iranian regime.
Technical Details
Attached to this FLASH is a list of 87 IP addresses and 136 domain names associated with this cyber activity. Activity related to these IPs and domains detected on a network should be considered an indication of compromise requiring mitigation.

Recommended Mitigations
Precautionary measures to mitigate this activity are:
- Prepare an incident response plan to be rapidly implemented in case of a cyber intrusion.
- Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected servers and software that processes Internet data such as Web browsers, browser plugins, and document readers.
- Scrutinize links contained in e-mails, and do not open attachments included in unsolicited e-mails.
- Implement application whitelisting to block execution of malware, or at least block execution of files from TEMP directories where most malware attempts to execute from.

Reporting Notice
The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI’s 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@ic.fbi.gov. 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. Press inquiries should be directed to the FBI’s National Press Office at npo@ic.fbi.gov or (202) 324-3691.
Administrative Note
This product is marked TLP:AMBER. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
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.