Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

26 January 2022

PIN Number

PIN-20220126-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients 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 actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:WHITE**

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad

Summary

This Private Industry Notice provides a historical overview of Iran-based cyber company Emennet Pasargad's tactics, techniques, and procedures (TTPs) to enable recipients to identify and defend against the group's malicious cyber activities. On 20 October 2021, a grand jury in the US District Court for the Southern District of New York indicted two Iranian nationals employed by Emennet Pasargad (formerly known as Eeleyanet Gostar) for computer intrusion, computer fraud, voter intimidation, interstate threats, and conspiracy offenses for their alleged participation in a multi-faceted campaign aimed at influencing and interfering with the 2020 US Presidential Election. In addition, the Department of the Treasury Office of Foreign Assets Control designated Emennet along with four members of the company's management and the two indicted employees for attempting to influence the same election. The Department of State's Rewards for Justice Program also offered up to $10 million for information on the two indicted actors.

Threat

Starting in August 2020, Emennet Pasargad actors conducted a multi-faceted campaign to interfere in the 2020 US presidential election. As part of this campaign, the actors obtained confidential U.S. voter information from at least one state election website; sent threatening email messages to intimidate voters; created and disseminated a video containing disinformation pertaining to purported but non-existent voting vulnerabilities; attempted to access, without authorization, several states' voting-related websites; and successfully gained unauthorized access to a U.S. media company's computer network. During the 2020 election interference campaign, the actors claimed affiliation with the Proud Boys in the voter intimidation and disinformation aspects of the campaign.

In addition to the 2020 U.S. election-focused operation in which the actors masqueraded as members of the Proud Boys, Emennet previously conducted cyber-enabled information operations, including operations that used a false-flag persona. According to FBI information, in late 2018, the group masqueraded as the "Yemen Cyber Army" and crafted messaging critical of Saudi Arabia. Emennet also demonstrated interest in leveraging bulk SMS services, likely as a means to mass-disseminate propaganda or other messaging.

FBI information indicates Emennet poses a broader cybersecurity threat outside of information operations. Since 2018, Emennet has conducted traditional cyber exploitation activity targeting several sectors, including news, shipping, travel (hotels and airlines), oil and petrochemical, financial, and telecommunications, in the United States, Europe, and the Middle East.

Tactics, Techniques, and Procedures

The FBI is providing a summary of the group's past TTPs to recipients so they can better understand and defend against the group's future malicious activity.

Emennet is known to use Virtual Private Network (VPN) services to obfuscate the origin of their activity. The group likely uses VPN services including TorGuard, CyberGhost, NordVPN, and Private Internet Access.

Over the past three years, Emennet conducted reconnaissance and chose potential victims by performing web searches for leading businesses in various sectors such as "top American news sites." Emennet would then use these results to scan websites for vulnerable software that could be exploited to establish persistent access. In some instances, the objective may have been to exploit a large number of networks/websites in a particular sector as opposed to a specific organization target. In other situations, Emennet would also attempt to identify hosting/shared hosting services.

After the initial reconnaissance phase, Emennet typically researched how to exploit specific software, including identifying open source available tools. In particular, Emennet demonstrated interest in identifying webpages running PHP code and identifying externally accessible mysql databases (in particular, phpMyAdmin). Emennet also demonstrated an interest in exploiting the below software applications:

- Wordpress (in particular the revslider and layerslider plugins)
- Drupal
- Apache Tomcat
- Ckeditor and Fckeditor (including the exploitation of Roxy Fileman)

Emennet also expressed interest in numerous specific vulnerabilities, outlined in Appendix A.

When conducting research, Emennet attempted to identify default passwords for particular applications a target may be using, and tried to identify admin and/or login pages associated with those same targeted websites. It should be assumed Emennet may attempt common plaintext passwords for any login sites they identify.

Emennet is known to use the open source penetration testing tools SQLmap and the commercially available tool Acunetix during operational activity. They also likely use the below tools or resources:

- DefenseCode Web Security Scanner
- Wappalyzer
- Dnsdumpster
- Tiny mce scanner
- Netsparker
- Wordpress security scanner (wpscan)
- Shodan

FBI information indicates the group has attempted to leverage cyber intrusions conducted by other actors for their own benefit. This includes searching for data hacked and leaked by other actors, and attempting to identify webshells that may have been placed or used by other cyber actors.

Recommendations

- Ensure anti-virus and anti-malware software is enabled and signature definitions are updated regularly in a timely manner. Well-maintained anti-virus software may prevent use of commonly deployed attacker tools that are delivered via spear-phishing.

- Adopt threat reputation services at the network device, operating system, application, and email service levels. Reputation services can be used to detect or prevent low-reputation email addresses, files, URLs, and IP addresses used in spear-phishing attacks.

- If your organization's information was previously compromised, the FBI recommends considering how any data exfiltrated could be leveraged to conduct further malicious activity against your network, and take appropriate measures to ensure security mechanisms are in place.

- If your organization is employing certain types of software and appliances referenced in the aforementioned CVEs, the FBI recommends patching for those vulnerabilities.

- Review the Tactics, Techniques, and Procedures in the referenced table and take steps to ensure you can identify and defend against malicious activity by this actor.

- Consider reputable hosting services for websites and content management systems (CMS), if you need assistance in configuring and maintaining your external facing applications.

- Consider employing a Web Application Firewall (WAF) to block inbound malicious traffic.

- Disable Content Management Systems features if they are not needed, and configure them to:
  - Disable remote file editing
  - Restrict file execution to specific directories
  - Limit login attempts

- Review the logs generated by security devices for signs that your organizations external networks are being scanned for vulnerabilities.

Reporting Notice

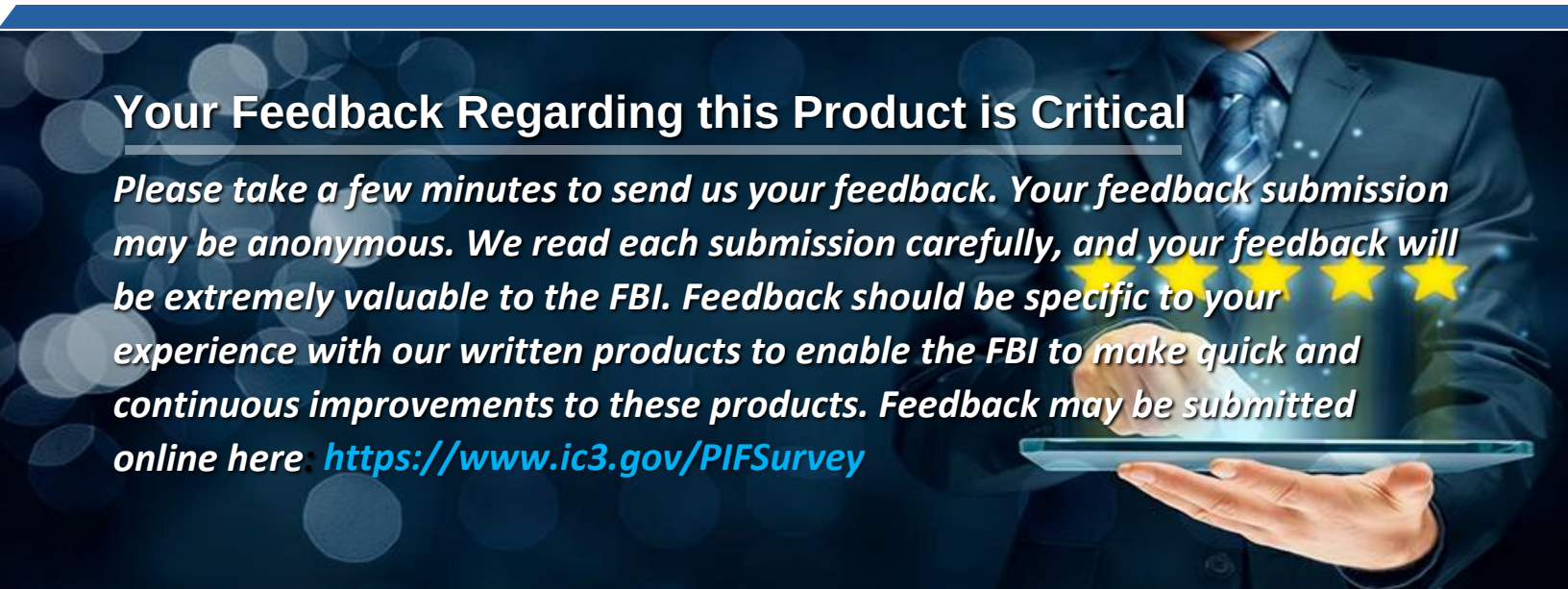
The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, 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.

The FBI also notes the Department of State's Rewards for Justice Program is offering up to $10 million for information leading to the identification or location of Emennet-associated cyber actors Seyyed Mohammad Hosein Musa Kazemi and Sajjad Kashian:

- https://rewardsforjustice.net/terrorist-rewards/seyyed-kazemi/
- https://rewardsforjustice.net/terrorist-rewards/sajjad-kashian/

Administrative Note

This product is marked TLP:WHITE. Subject to standard copyright rules, the information in this product may be shared without restriction.



Appendix A

CVE	Description
CVE-2019-0232	When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disabled by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behavior, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).
CVE-2017-5963	An issue was discovered in caddy (for TYPO3) before 7.2.10. The vulnerability exists due to insufficient filtration of user-supplied data in the "paymillToken" HTTP POST parameter passed to the "caddy/Resources/Public/JavaScript/e-payment/paymill/api/php/payment.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.
CVE-2018-7600	Drupal before 7.58, 8.x before 8.3.9, 8.4.x before 8.4.6, and 8.5.x before 8.5.1 allows remote attackers to execute arbitrary code because of an issue affecting multiple subsystems with default or common module configurations.
CVE-2018-1000001	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
CVE-2014-0160	The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.
CVE 2019-9546	SolarWinds Orion Platform before 2018.4 Hotfix 2 allows privlege escalation through the RabbitMQ service.
CVE-2016-10033	The mailSend function in the isMail transport in PHPMailer before 5.2.18 might allow remote attackers to pass extra parameters to the mail command and consequently execute arbitrary code via a \" (backslash double quote) in a crafted Sender property.
CVE-2009-1151	Static code injection vulnerability in setup.php in phpMyAdmin 2.11.x before 2.11.9.5 and 3.x before 3.1.3.1 allows remote attackers to inject arbitrary PHP code into a configuration file via the save action.

CVE	Description
CVE-2017-5930	The AliasHandler component in PostfixAdmin before 3.0.2 allows remote authenticated domain admins to delete protected aliases via the delete parameter to delete.php, involving a missing permission check.
CVE-2019-0708	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specifically crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability".
CVE-2017-0213	Windows COM Aggregate Marshaler in Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allows an elevation privilege vulnerability when an attacker runs a specially crafted application, aka "Windows COM Elevation of Privilege Vulnerability". This CVE ID is unique from CVE-2017-0214.
CVE-2018-8639	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8641.
CVE-2017-14723	Before version 4.8.2, WordPress mishandled % characters and additional placeholder values in $wpdb-> prepare, and thus did not properly address the possibility of plugins and themes enabling SQL injection attacks.
CVE-2017-8295	WordPress through 4.7.4 relies on the Host HTTP header for a password-reset e-mail message, which makes it easier for remote attackers to reset arbitrary passwords by making a crafted wp-login.php?action=lostpassword request and then arranging for this message to bounce or be resent, leading to transmission of the reset key to a mailbox on an attacker-controlled SMTP server. This is related to problematic use of the SERVER_NAME variable in wp-includes/pluggable.php in conjunction with the PHP mail function. Exploitation is not achievable in all cases because it requires at least one of the following: (1) the attacker can prevent the victim from receiving any e-mail messages for an extended period of time (such as 5 days), (2) the victim's e-mail system sends an autoresponse containing the original message, or (3) the victim manually composes a reply containing the original message.
CVE-2017-14726	Before version 4.8.2, WordPress was vulnerable to a cross-site scripting attack via shortcodes in the TinyMCE visual editor.
CVE-2017-5611	SQL injection vulnerability in wp-includes/class-wp-query.php in WP_Query in WordPress before 4.7.2 allows remote attackers to execute arbitrary SQL commands by leveraging the presence of an affected plugin or theme that mishandles a crafted post type name.

CVE	Description
CVE-2019-0044	Receipt of a specific packet on the out-of-band management interface fxp0 may cause the system to crash and restart (vmcore). By continuously sending a specifically crafted packet to the fxp0 interface, an attacker can repetitively crash the rpd process causing prolonged Denial of Service (DoS). Affected releases are Juniper Networks SRX5000 Series: 12.1.X46 versions prior to 12.1X46-D82; 12.3X48 versions prior to 12.3X48-D80; 15.1.X49 versions prior to 15.1.X49-D160.
CVE-2019-9621	Zimbra Collaboration Suite before 8.6 patch 13, 8.7.x before 8.7.11 patch 10, and 8.8.x before 8.8.10 patch 7 or 8.8.x before 8.8.11 patch 3 allows SSRF via the ProxyServelet componet.

Source: National Vulnerability Database (nvd.nist.gov)