FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 MAR 2018

Alert Number

ME-000092-TT

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 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: White** Subject to standard copyright rules, **TLP: White** information may be distributed without restriction.

Malicious cyber activity of Iran-based Mabna Institute

Summary

According to information derived from an FBI investigation, a group of malicious cyber actors working for the Iran-based Mabna Institute (Mabna) have been conducting coordinated and broadly targeted password spray attacks against organizations in the United States and abroad. Victims of Mabna often lack multi-factor authentication (MFA), lack preventative network activity alerts, and allow easy-to-guess passwords (e.g., “Winter2018”, “Password123!”).

Nine Mabna Institute actors were indicted by the Department of Justice in the Southern District of New York in February 2018, for computer intrusion offenses related to the activity described in this report. The techniques and activity described herein, while characteristic of Mabna actors, are not solely used by this group.

Mabna targets companies using single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols. While many SSO and cloud-based applications offer federated authentication protocols, Mabna has focused their efforts on victims hosted on Microsoft Office 365 (O365). After successfully compromising victims, Mabna actors likely utilize inbox synchronization to obtain unauthorized access to the organization's email directly from the cloud which subsequently allows for the download of user mail to locally stored email

files (.PST). In addition, Mabna often surreptitiously implements inbox rules for the forwarding of sent and received messages through the use of synchronization functionality in email clients like Microsoft Outlook.

Technical Details

During a password spray attack, a malicious actor attempts a single password against a population of accounts before moving on to attempt a second password against the accounts, and so on. This technique allows the actor to remain undetected by avoiding account lockouts. Traditional Tactics, Techniques, and Procedures (TTP's) for conducting the password-spray attacks are as follows:

- Perform online research (i.e., Google search, LinkedIn, etc.) to identify target organizations and specific user accounts for initial password spray
- Using easy-to-guess passwords (e.g., "Winter2018", "Password123!") and publicly available tools, execute a password spray attack against targeted accounts by utilizing the identified SSO or web-based application and federated authentication method
- Leveraging the initial group of compromised accounts, download the Global Address List (GAL) from a target's email client, and perform a larger password spray against legitimate accounts
- Using the compromised access, malicious actors attempt to expand laterally (e.g., via Remote Desktop Protocol) within the network, and perform mass data exfiltration using File Transfer Protocol tools such as FileZilla

Indicators of a password spray attack include:

- A massive spike in attempted logons against the enterprise SSO Portal or web-based application. Using automated tools, malicious actors attempt thousands of logons, in rapid succession,

against multiple user accounts at a victim enterprise, originating from a single IP address and computer (e.g., a common User Agent String). Attacks have been seen to run for over two hours

- Employee logons from IP addresses resolving to locations inconsistent with their normal locations

Mabna Intrusion Activity

The FBI notes that Mabna has conducted password spray attacks and malicious activity from hundreds of IP addresses. Additionally, Mabna is known to mask their true location through the use of various VPN providers including, but not limited to, IPVanish.

The FBI also notes that Mabna may have compromised organizations with MFA in place. An attacker can perform a password spray attack against an MFA-protected protocol, confirm a legitimate user ID and password combination, but generally is unable to defeat the secondary authentication protocol. However, the attacker can then take a verified user ID and password combination, search for other lesser used protocols that may not have MFA covering them, and attempt to gain unauthorized access.

Mabna targets SSO and web-based applications because the single point-of-compromise typically yields access to large amounts of intellectual property. Specifically targeting SSO and web-based applications utilizing the federated authentication method, Mabna actively identifies companies lacking the following common security settings:

a) Absent specific configuration by the customer, event logging available to the customer can be limited for post-incident response and investigation

b) Absent specific additional technology, the authentication software, most commonly Active Directory Federated Services (ADFS), has limited capability to defend against various brute force-style attacks, such as password spray attacks

c) Absent specific configuration by the customer, most commonly the IP address captured by ADFS would be the SSO or web-based application IP address and not the source IP address of the malicious actor

Typical Victim Environment

While Mabna has been seen to target different environments, the vast majority of known victims share the following similar profile:

- Use O365 or Outlook with the federated authentication method, and lack MFA protocol
- Allow easy-to-guess passwords (e.g., “Winter2018”, “Password123!”)
- Use inbox synchronization allowing email to be pulled from the Microsoft cloud to a remote device
- Allow email forwarding to be setup at the user level
- Limited logging setup with Microsoft, creating difficulty during post-event investigations

Recommended Mitigations

To help deter this style of attack, the following steps should be taken:

- Enable MFA and review MFA settings to ensure coverage over all active, internet facing protocols
- Review password policies to ensure they align with the latest NIST guidelines and deter the use of easy-to-guess passwords
- Review IT Helpdesk password management related to initial passwords, password resets for user lockouts, and shared accounts. IT Helpdesk password procedures may not align to company policy, creating a security gap Mabna can exploit

On March 5, 2018, Microsoft released an article highlighting the dangers of password spray attacks, along with the tools they currently offer or will offer in 2018, to defend against this style of attack. The FBI has included the article to allow Microsoft customers the opportunity to review and consider implementing the available tools to better detect and prevent password spray attacks:

https://cloudblogs.microsoft.com/enterprisemobility/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/

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: 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.