Crossing the Digital Divide (v105)
"Nag"
By Joseph Feigon
For the Observer

Not to sound like a broken record (some of you might remember those vinyl platters we'd place onto a turn-table for playback recorded music), but you need to do this today: create better passwords and establish 2-Factor Authentication wherever you create online accounts. Briefly, two-factor authentication means "a strong password and a means to prove you're the password owner, e.g., a text to your cellphone, an automated phone call to your home phone, etc."

TA18-086A: Brute Force Attacks Conducted by Cyber Actors

03/27/2018 06:00 PM EDT

Original release date: March 27, 2018

Systems Affected

Networked systems

Overview

According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad.

On February 2018, the Department of Justice in the Southern District of New York, indicted nine Iranian nationals who were associated with the Mabna Institute for computer intrusion offenses related to activity described in this report. The techniques and activity described herein, while characteristic of Mabna actors, are not limited solely to use by this group.

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are releasing this Alert to provide further information on this activity.

Description

In a traditional brute-force attack, a malicious actor attempts to gain unauthorized access to a single account by guessing the password. This can quickly result in a targeted account getting locked-out, as commonly used account-lockout policies allow 3-to-5 bad attempts during a set period of time. During a password-spray attack (also known as the "low-and-slow" method), the malicious actor attempts a single password against many accounts before moving on to attempt a second password, and so on. This technique allows the actor to remain undetected by avoiding rapid or frequent account lockouts.

Password spray campaigns typically target single sign-on (SSO) and cloud-based applications utilizing federated authentication protocols. An actor may target this specific protocol because federated authentication can help mask malicious traffic. Additionally, by targeting SSO

applications, malicious actors hope to maximize access to intellectual property during a successful compromise.

Email applications are also a target. In those instances, malicious actors would have the ability to utilize inbox synchronization to (1) obtain unauthorized access to the organization's email directly from the cloud, (2) subsequently download user mail to locally stored email files, (3) identify the entire company’s email address list, and/or (4) surreptitiously implements inbox rules for the forwarding of sent and received messages.

The bad guys will continue their efforts to take over our wallets, don’t let them get to yours!

Control those things you can, and keep the surprises to a minimum!