On July 11, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to multiple vulnerabilities in Mozilla Firefox and Microsoft products.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

19 July 2019

In The News This Week

Microsoft Launches Public Preview of Security Key Support: Password-Free Life Creeps Closer. - With over 551 million real world passwords exposed in data breaches and the growing ease with which they can be brute-forced, dumping the password makes a lot of sense…

Microsoft says enterprises can now roll out the use of security keys at scale, as it launches a public preview of FIDO2 security key support in Azure Active Directory (AD). The move is a major step towards a passwordless enterprise environment. (Azure AD is Microsoft's identity and access management platform). Security keys are available in a range of form factors, but commonly come as small USB key fob that creates a public and private key when registered. The private key can only be unlocked using a local gesture such as a biometric or PIN. Users have the option to either sign in directly via biometric recognition—such as fingerprint scan, facial recognition, or iris scan—or with a PIN that's locked and secured.

The move will be welcomed by many businesses concerned at the growing ease with which passwords can be brute forced, or otherwise compromised: that is if they have not been stolen in a data breach already. An estimated 81 percent of successful cyberattacks begin with a compromised username/password and there is no shortage of those in the wild. The site https://haveibeenpwned.com lists 551,509,767 real world passwords previously exposed in data breaches.

Alex Simons, a VP in Microsoft's Identity and Security department, said the company has also "turned on a new set of admin capabilities in the Azure AD portal that enable you to manage authentication factors for users and groups in your organization."

This currently lets admins use either security keys or Microsoft's Authenticator application for authentication. (The latter is a Microsoft app that lets employees augment a password with a one-time passcode or push notification; instead of using a password, users confirm their identity using mobile phone through fingerprint scan, facial or iris recognition, or PIN for authentication.) Simons added: "You'll see us add the ability to manage all our traditional authentication factors (Multi-Factor Authentication, OATH Tokens, phone number sign in, etc.). Our goal is to enable you to use this one tool to manage all your authentication factors." on the device. Read the full story here: CBR-News

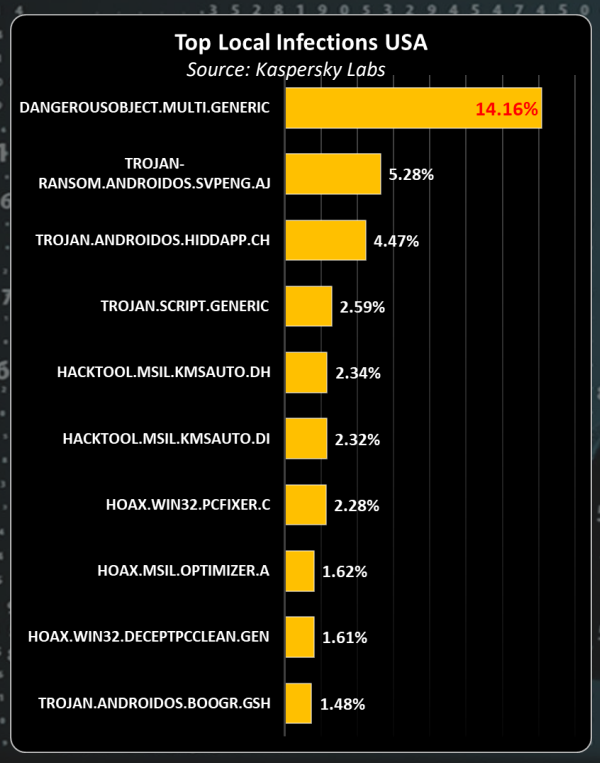
Microsoft has warned 10,000 people that nation-state hackers are targeting them.

Microsoft has warned nearly 10,000 people that nation-state hackers have targeted or breached their accounts in the past year. The software giant revealed that around 84 percent of these attacks are aimed at businesses, while the remaining 16 percent are targeted at personal email accounts. The statistics reveal the extent of nation-state attacks, and that as many as 1,600 personal Microsoft Accounts have been affected by these hackers recently.

Most of these attacks originate from hackers in Iran, North Korea, and Russia according to Microsoft. "We have seen extensive activity from the actors we call Holmium and Mercury operating from Iran, Thallium operating from North Korea, and two actors operating from Russia we call Yttrium and Strontium," explains Tom Burt, corporate vice president for customer security and trust at Microsoft.

At least one of these groups, that Microsoft identifies as Strontium, is the Russian Fancy Bear collective that have previously been involved in the 2016 hacks of the Democratic National Committee and the NotPetya attacks against Ukranian banks and infrastructure in June 2017.

Read the full story here: TheVerge



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

According to Meg Prater on HupSpot Google processes approximately **70,000** search queries every second, translating to **5.8 billion** searches per day and approximately **2 trillion** global searches per year.

PASSWORDLESS AUTHENTICATION

Passwordless authentication is any method of verifying the identity of a user that does not require the user to provide a password. Instead of passwords, proof of identity can be done based on possession of something that uniquely identifies the user (e.g. a one-time password generator, a registered mobile device, or a hardware token) or the user's biometric signature (e.g. fingerprint, face, retina, etc.).

What are the benefits of Passwordless Authentication?

- Improved User Experience: It means that the user doesn't have remember or mange a gazillion password anymore
- Better Security: User controlled passwords are a major vulnerability, users reuse passwords, are able to share them with others. Passwords are the biggest attack vector and are responsible for 81% of breaches.
- Reduction in Total Cost of Ownership (TCO): Passwords are expensive, it require constant maintenance from IT staff.
- IT Gains Control and Visibility: Phishing, reuse, and sharing are common issues when relying on passwords, with passwordless authentication IT reclaims its purpose of having complete visibility over identity and access management.

The security of passwordless authentication systems depends on how proof of identity is acquired in lieu of passwords and the implementation of the method. For example, using secure push notifications to the account holder's mobile device is generally considered more secure than passwords. SMS codes to the account holder's mobile device can be considered less secure because SMS is an insecure communication channel and open to attacks.

What does Passwordless Authentication Prevent?

Password spraying - Password spraying is an attack that attempts to access a large number of accounts (usernames) with a few commonly used passwords.

Credentials stuffing - Credential stuffing is a type of cyberattack where stolen account credentials, typically consisting of lists of usernames and/or email addresses and their corresponding passwords are used to gain unauthorized access to user accounts. Using a program called an 'account checker', hackers activate large-scale automated login requests directed against a slew of web applications.

Spear Phishing - Phishing hacks are a form of cyberattacks designed with the aim of getting a user to divulge compromising information. As its name would imply, Spear Phishing is a targeted attack against a particular user or set of users, based on their unique profile. Spear phishing messages are tailored to the targets in an effort to convince them the communications are legit. This is usually done by acquiring personal details on the victim such as their friends, hometown, employer, locations they frequently visit, or what they have recently bought online. The attackers then disguise themselves as a trustworthy friend or entity and attempt to extract sensitive information, typically through email or other online messaging. To date, Spear phishing is the most successful form of acquiring credentials and other sensitive data via the internet, accounting for 91% of all attacks.

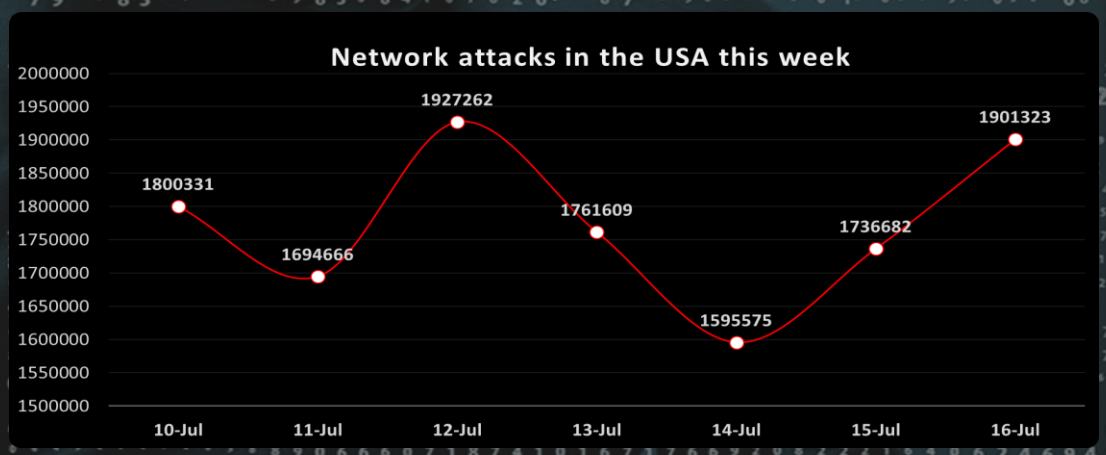
Brute Force Attack - Brute force attacks involve repeated login attempts using every possible letter, number, and character combination to guess a password. An attacker using brute force is typically trying to guess a user, or an administrator password or a password hash key. Guessing a short password can be relatively simple, but that isn't necessarily the case for longer passwords or encryption keys—the difficulty of brute force attacks grows exponentially the longer the password or key is.

Offline Password Cracking - Offline Password Cracking is an attempt to extract one or more passwords from a password storage file that has been recovered from a target system. Typically, this form of cracking will require that an attacker has already attained a high level of access to a system, in order to gain access to the necessary file. Once the hackers gain access to the stored passwords, they are able to move freely through a wide range of network accounts.

Rainbow table attacks - A Rainbow Table attack is designed to recover passwords from their cryptographic hashes. They are basically huge sets of precomputed tables filled with hash values that are pre-matched to possible plaintext passwords. The proper application of a Rainbow Table can allow a hacker to break passwords with relatively high complexity.

Social Engineering - Social engineering covers a very broad range of attacks by which cybercriminals manipulate individuals into divulging login credentials. Social media platforms often provide the perfect venue for hackers to reach out to potential victims under a guise and extract information. Some social engineering methods don't even require attackers to engage directly with victims. Criminals can go directly to a user's service provider such as a cell phone or internet company and deceive a representative into delivering new passwords to the phone or device of their choice.

Adapted from multiple resources found on the net



Author: Chris Bester
chris.bester@yahoo.com