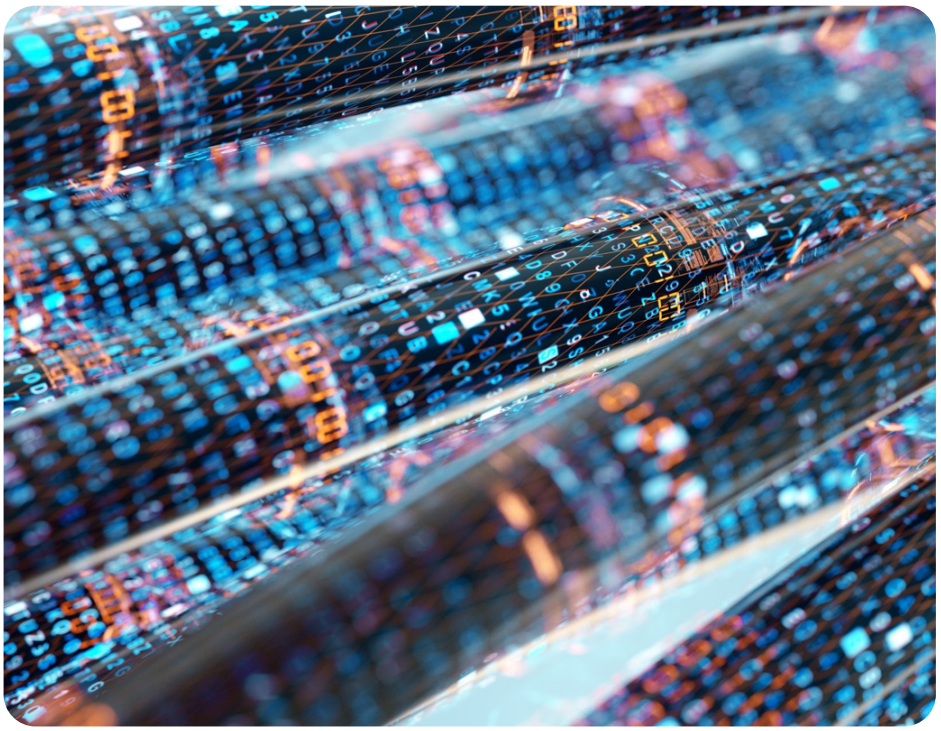
beazley

Article

The Threat of Stolen Credentials: What Organisations Need to Know

Jad Nehmé • January 18, 2023



Organisations and websites are suffering cybersecurity incidents on a daily basis, some of them leading to the compromise of customers' data. Compromised data frequently include lists of usernames and passwords, which allow the bad actors who possess them to access online resources such as websites and mobile applications. These passwords are then traded and sold on the internet, mostly on dark web marketplaces, but also on publicly accessible websites. Some of these password lists can be bought for as little as $5. Moreover, nowadays, passwords can be easily mis-shared or guessed, especially when users still use weak passwords (ex. "password" or "123456") and with the abundance of personal information available on the Internet.

A CLOSER LOOK AT PASSWORDS.

Passwords can be big business: according to several studies, an average person can have more than 150 different online accounts. Due to insufficient security awareness, most people use the same password for several accounts, and may even utilize the same password for personal accounts, sensitive business applications that are accessible from the Internet, or for remote connections into their company's network (like a VPN or Citrix). Thus, a compromised personal account password, even from a site hosting non-sensitive data such as dailyquizz.me, can provide threat actors with valid credentials for accessing an organisation's systems remotely.

It is relatively easy and cheap for threat actors to perform credential stuffing attacks, which are large-scale automated login requests using stolen credentials (one authentication request per user). These attacks are often difficult to detect by IT security teams, as the threat actor is actually using valid usernames and credentials rather than brute force attacks.

The impact of such an attack depends on the type of data or access of the compromised accounts. It can vary from accessing a magazine subscription, to remotely accessing an organisation's information systems using privileged access. Fortunately, there are several ways your organisation can protect against this risk.

THE MOST IMPORTANT THING THAT YOUR ORGANISATION CAN DO IS TO ENABLE MULTI-FACTOR AUTHENTICATION, OR MFA.

The concept behind multifactor authentication (MFA) is not a new one. Before keys were invented (over 6,000 years ago), you needed to identify yourself with a secret message before getting access to an important meeting room. Years later, and as humans discovered how easy it was to find or guess a secret message, keys were invented. The advent of the key represented the first version of 2-FA (two-factor authentication): something you knew (the location of the door), and something you had (a physical key).

We can apply the same concept to secure access IT nowadays: the part that you "know" (username and password or PIN) can also be known by multiple threat actors, so you need the second factor, which is the part that you "have": this can include a mobile phone with a SIM card, a code generated on a physical token or software installed on your mobile device, an enterprise enrolled device, etc.

MFA is a very efficient way to protect your account from the above mentioned opportunistic attacks. Even if a threat actor gets access to a valid password, the second factor of your MFA would prevent them from using it to connect to your online accounts.

EXAMPLES OF MFA BEING BYPASSED

Recently, threat actors have developed tools to bypass some MFA implementations, and some of these tools were made public (ex. EvilProxy).
There have been two major incidents during which MFA was recently bypassed:

The first was an Uber hack, for which the attacker first gained access to company systems by targeting an individual employee's account (whose password was previously compromised) and repeatedly sending them MFA push notifications. After more than an hour, the threat actor contacted the same employee on WhatsApp pretending to be an Uber IT support employee and saying that the MFA notifications would stop once the target approved the login. The employee approved and the threat actor obtained access immediately.

The second was a Twilio hack incident, in which employees were redirected to fake login pages via SMS. This allowed the threat actor to retrieve the MFA tokens and use them to connect remotely (here's an example of how MFA is being bypassed).

Not all MFA solutions offer the same level of security. In most cases, MFA-bypass incidents exploit weak configuration practices that can be fixed by changing the default configuration (ex. blocking legacy authentication). Thus, weaker MFA solutions can be made more secure with proper security configuration (check out Microsoft's recommendations)

SECURITY AWARENESS & SECURE PASSWORD HYGIENE ARE ALSO ESSENTIAL.

Security awareness remains key for helping individuals adopt best practices when handling passwords. Best practices include using unique, long and/or complex passwords that cannot be guessed based on information that can be found on the Internet like a user's first name, last name, company name, or address. A personal password manager (such as Bitwarden, which is free and open source) provides an individual with an easy way to generate and store a unique and complex password for each of their online accounts. Training employees to identify fake or spoofed domain names is also key in protecting against recent MFA bypass techniques.

Organisations that do not expect employees or customers to connect from specific locations can control remote connections coming from other countries, regions or continents by implementing geo-location restrictions. Based on the location and the time of the connection, an organisation can decide whether to block a connection or to require additional verifications using a third factor such as a link sent by email, a question with a pre-configured secret answer, a phone call, or a notification on a mobile device.

LEAKED CREDENTIALS

Monitoring leaked credentials is another way that companies and individuals alike can practice secure password hygiene. Some organisations that have suffered a data breach take the effort to notify customers and employees who were impacted by the incident, however others don't. Knowing when your data or passwords are leaked can be useful as it allows you to take appropriate action when needed, for example changing a password that is used for several accounts, enabling MFA if not enabled or alerting your bank if your credit card number has been stolen. There are several websites that allow individuals to know if their data has been disclosed in publicly known breaches (Like haveibeenpwned.com).

Password managers (including Bitwarden and Google Chrome’s password manager) offer functionalities that allow users to know if their passwords are found in a disclosed password leak, and these are often offered for free. Furthermore, specialized service providers offer services that notify organisations when their data is found on the dark web, sometimes even before the breach is publicly disclosed. This service is often called “Dark Web Monitoring.”

As bad actors continue to prey on easy victims, security techniques like implementing secure MFA and practicing secure password hygiene are essential risk management components for every organisation. Educating yourself and your colleagues about the latest risks and taking steps to mitigate them is well worth the time and effort.

Jad Nehmé

Client Experience Manager

Jad Nehmé is a cyber services manager with Beazley’s cyber services team — international. He is based in France and supports Beazley’s clients during a cybersecurity incident or a data breach. He also assists clients with privacy and cybersecurity risk management as well as preventive controls. Prior to joining Beazley, Jad held roles at Alcatel-Lucent and KPMG covering both the technical and organisational aspects of cyber security.
Opinions expressed here are the author’s own.

beazley