Beazley Logo

Video

Footnote 7 - Video The Threat of Stolen Credentials: What Organisations Need to Know 3333

Troy Long Name Example Dehman edit

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.

2022

2022

2022

2022

2022

2022

2022

2022

2022

2022

Where is this offered?

This is the title for the Article Highlighted Text edited - FULL WIDTH VERSION

Providing some of the most innovative insurance products on the market, we combine risk management, financial indemnity and tailored incident response services, to ensure that, when the worst happens, our clients can get back to doing what they do best, as quickly as possible. Providing some of the most innovative insurance products on the market, we combine risk management, financial indemnity and tailored incident response services, to ensure that, when the worst happens, our clients can get back to doing what they do best, as quickly as possible.

This is new paragraph...

2022

Troy Long Name Example Dehman edit

Business Manager

[1] footnote text

2022

2022

2022

2022

2022

2022

2022

2022

2022

2022

[1]

[2] https://www.bain.com/insights/covid-19-accelerates-the-adoption-of-telemedicine-in-asia-pacific-countries/

[3] In Weekend Outage test, Diabetes Monitors Fail to Send Crucial Alerts, New York Times (20:

[4] JAMA Dermatology 2017: https://jamanetwork.com/journals/jamadermatology/article-abstract/2588699

[5] This is an internal link: https://bmal01mstre8wy9inte.dxcloud.episerver.net/en/qa-test-pages/full-width-page/