INSIGHTS

One Brightly Cyber

WHAT IS CREDENTIAL STUFFING?

BY JAY BORDEN

We and others have always told people never to use the same password or a variant on different websites. We also say to use long, complex passwords that are harder to guess and crack.

Why? One reason is credential stuffing. What is that? It's a cybercriminal technique that if they get one of your passwords, and they will, they try it on lots of popular sites. If you used the same password on other sites, then ta-da they are in.

Credential stuffing has been a tool of attackers for years because despite all the warnings, people still use the same password for multiple services and sites.

Hackers have found credential stuffing to be successful enough that they continue to use it. Cybercriminals are like anyone else, they will stop doing what doesn't work and continue doing what does work. If it is successful enough, they may well expand their use of it.

Expansion of credential stuffing is happening now because AI, Artificial Intelligence, has put credential stuffing on steroids.

Why would attackers want to use AI for credential stuffing? Recent investigations have discovered the use of an AI tool called Atlantis AIO that enables the testing of millions of stolen credentials in succession on 140 platforms or sites. The ones you most probably use.

In case you think your password is safe, there are 10s of millions or even billions of username / password combinations for sale on the Dark Web that have already been stolen. Attackers buy them very inexpensively and will use them in credential stuffing and other types of attacks.

WHAT IS CREDENTIAL STUFFING?

CONTINUED

Now with AIO, the rate at which they can test stolen credentials on other sites is significantly faster. This means they will find the ones that work more quickly and move on to the next platform or set of credentials if they don't work.

The sellers of the AIO tool claim to test against popular sites and services including email providers like Yahoo, Hotmail. GMX, AOL, and e-commerce sites, streaming services, VPNs, banks and other financial services companies, and even food delivery services.

You can see they have a good chance of finding other services you use. When they find one that works, they have a choice. They can use it to steal more of your information such as a credit card or personal information for identity theft, they can sell what they have found to other attackers, or use the accounts to send out phishing messages.

I'm sure you receive phishing emails. It's not the real owner of that account sending the phishing emails. It's a cybercriminal who got access to that email account. The real owner probably doesn't even know their account is being used for this.

This is why we recommend using a unique password for each and every site or service you access. By unique we don't mean a slight variation on a password such as Chocolate for one site and Chocolate2 for another one. Hackers will break that in under a second. The passwords should be completely unique. If possible, use a recognized password manager to create long, complex, and unique passwords for every site and service.

We also strongly recommend using phish resistant MFA, Multi-Factor Authentication. That can stop someone who has stolen your credentials. Be sure it is phish resistant MFA or it won't protect you.

Even phish resistant MFA may not protect forever, or always, but it helps keep you safer.

Visit our website onebrightlycyber.com or call (888) 873-1920 to learn all the ways we help keep you safer.