National Cyber Security Centre
a part of GCHQ

Advisory: Use of credential stuffing tools

19 November 2018

Introduction

The NCSC is aware of recent cases of credential stuffing. This advisory gives information about this method of attack and advice on how to protect your organisation against it.

Credential stuffing takes advantage of people reusing username and password combinations. Attackers fraudulently obtain valid combinations for one site and then use them across others to try and gain access to accounts.

Details

Credential stuffing has been seen in use across a range of different industry sectors as a method to gain unauthorised access to accounts. It works in a similar way to a brute force attack, by attempting to gain unauthorised access to user accounts on a site or service via multiple login attempts. However, instead of randomly generating multiple password guesses against a service (as in a brute force attack), credential stuffing exploits people's tendency to reuse username and password combinations. Here attackers fraudulently obtain valid combinations for one site and then use them across other sites to try and gain access to accounts. Any website that requires an online login is potentially vulnerable.

The attacks are automated and often large scale. One data breach can put many other accounts and organisations at risk. As credential stuffing enables an attacker to gain access to an account using legitimate credentials, it can cause a data breach without penetrating a company's infrastructure or systems.

The primary motivation for these types of attacks is financial gain but also includes the theft of Personally Identifiable Information (PII) such as credit card details which can lead to identity theft.

NCSC information indicates that the retail and gambling sectors have been repeatedly targeted. Cybercriminals have even used credential stuffing against points-based loyalty schemes, to steal accumulated points and successfully redeem their monetary value.

Credential stuffing tools

This attack method is facilitated by a range of off-the-shelf tools which are easily available, making it unsophisticated and relatively straightforward.

Commonly used tools include Sentry MBA, Account Hitman, Vertex and Apex. To launch an attack, an attacker simply needs their tool of choice, a configuration file for the website to be attacked and a list of username/password combinations to test against the site. Log in attempts are typically directed through one or more proxies to hide the source of the attack. The software is set up to automatically insert the credentials from the username/password list into the corresponding fields contained within the GET or POST requests.

Detection

There may be indicators that a website or service is victim of a credential stuffing attack, or other brute force attack. They include:

- Multiple failed attempted logins across multiple accounts. The tools can be configured to use a new IP address each time a set of credentials is attempted against a user account. Previous credential stuffing attacks indicate a considerable variation in the number of different IPs used to launch an attack – from one up to tens of thousands.
- Higher than usual volumes of foreign IPs, or anomalies in browser activity.
- Patterns in log in attempts which indicate use of automation (this could be authentication attempts to an API or log ins to a website portal).

Mitigation

The NCSC recommends putting in place enhanced measures to detect the use of compromised credentials:

- Model normal user login patterns and set up alert systems to spot the unusual activity as described in the 'Detection' section (e.g. high volumes of traffic, browser or IP anomalies).
- Proactively identify vulnerable accounts on your site, by aggregating breach sets and confirming hits in your own users' credentials, and by using online services such as https://haveibeenpwned.com/. If an account's credentials are found to be leaked, force a password change.
- Many credential stuffing tools require site-specific configuration files, which can be rendered neutral by making small changes in the login pages once detected (although be aware that attackers may work across different tools with varying configuration files, making detection based on tools alone inadvisable).
- Add a metric at the system backend to monitor unsuccessful login attempts across accounts – this will flag instances where an attacker isn't rate-limiting the number of guesses.

Reduce the impact of password compromise:

- Enforce multi-factor (or two-factor) authentication where possible. See NCSC guidance: www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services.
- Use device and/or browser fingerprinting to enforce additional checks – request more information from users in the event of multiple password failure or if login is from an unknown device.
- Use advanced analytics such as historical logging to help assess if a login is legitimate. Information such as location, IP address and browser can all be checked against the last successful login attempt, to make a credibility judgement of a log in request.

The NCSC also recommends carrying out additional checks on authentication attempts from a TOR node.