THREAT BULLETINS

Proxies and Configurations Used for Credential Stuffing Attacks on Online Customer Accounts

TLP:WHITE

Aug 19, 2022

The FBI is highlighting significant details about proxies and configurations used by cyber criminals to mask and automate credential stuffing attacks on US companies, resulting in financial losses associated with fraudulent purchases, customer notifications, system downtime and remediation, as well as reputational damage. Credential stuffing attacks, commonly referred to as account cracking, apply valid username and password combinations, also known as user credentials or “combo lists”, from previously compromised online resources or data leaks. Malicious actors utilizing valid user credentials have the potential to access numerous accounts and services across multiple industries – to include media companies, retail, healthcare, restaurant groups and food delivery – to fraudulently obtain goods, services and access other online resources such as financial accounts at the expense of legitimate account holders. The FBI acknowledges the Australian Federal Police for their assistance collecting the information included in this Private Industry Notification.

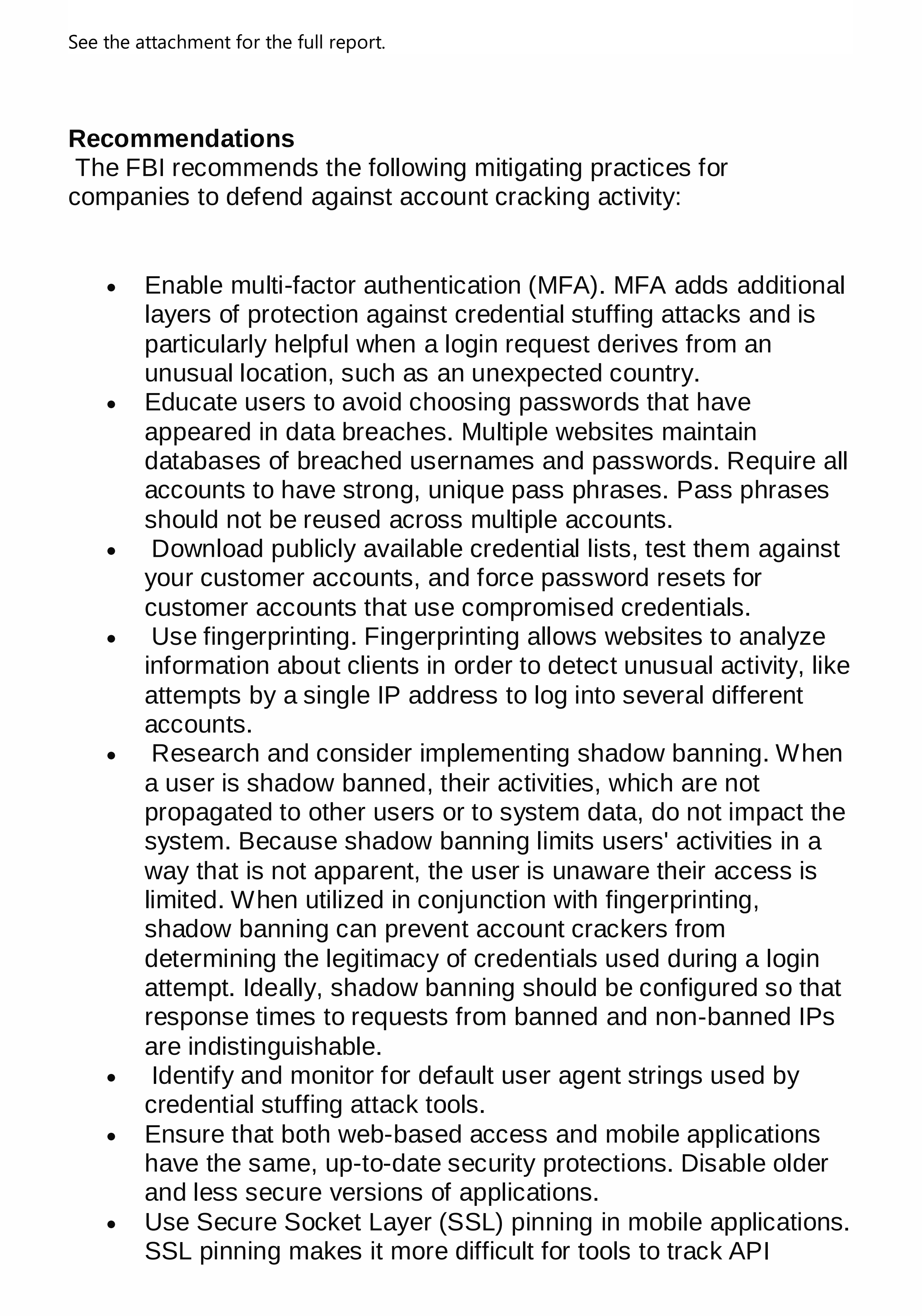
Cyber criminals leverage proxies and configurations to mask and automate credential stuffing attacks on online customer accounts of US companies. Credential stuffing, a type of brute force attack that exploits leaked user credentials from a website breach or purchased on dark web credential selling websites, takes advantage of the fact that many users reuse usernames and passwords across multiple accounts and services. Leveraging proxies and configurations automates the process of attempting logins across various sites and facilitates exploitation of online accounts. In particular, media companies and restaurant groups are considered lucrative targets for credential stuffing attacks due to the number of customer accounts, the general demand for their services, and the relative lack of importance users place on these types of accounts.

Numerous publicly accessible websites offer for sale compromised account credentials from popular online services. Two such websites investigated by the FBI and the Australian Federal Police were found to contain over 300,000 unique sets of credentials obtained via credential stuffing. The websites had over 175,000 registered customers and over 400,000 USD in sales. In addition to "combo lists" purchased from cyber criminal forums and websites dedicated to account cracking, cyber criminals can acquire configurations or "configs", which facilitate attacks by customizing credential stuffing tools to gain access to a particular target website. The config may include the website address to target, how to form the HTTP request, how to differentiate between a successful vs unsuccessful login attempt, whether proxies are needed, etc. In addition, cracking tutorial videos available via social media platforms and hacker forums make it relatively easy to learn how to crack accounts using credential stuffing and other techniques.

Actors may opt to use proxies purchased from proxy services, including legitimate proxy service providers, to facilitate bypassing a website's defenses by obfuscating the actual IP addresses, which may be individually blocked or originate from certain geographic regions. In executing successful credential stuffing attacks, cyber criminals have relied extensively on the use of residential proxies, which are connected to residential internet connections and therefore are less likely to be identified as abnormal. Existing security protocols do not block or flag residential proxies as often as proxies associated with data centers. In some instances, actors conduct credential stuffing attacks without the use of proxies, requiring less time and financial resources to execute. Some cracking tools, including one of the most popular automated attack tools, allow actors to run the software without proxies.

Cyber criminals may also target a company's mobile applications as well as the website. Mobile applications, which often have weaker security protocols than traditional web applications, frequently permit a higher rate of login attempts, known as checks per minute (CPMs), facilitating faster account validation. Cyber criminals leverage packet capture software, such as Wireshark, Burp Suite, or Fiddler to record and gain an understanding of the authentication mechanism employed by the targeted website and/or mobile application. This allows the cyber criminal to craft a custom configuration for credential stuffing activities. Other cyber criminals buy configurations created by others or obtain them from hacking forums. Cyber criminals have employed dedicated, hosted servers to execute credential stuffing attacks.

For additional information, see Private Industry Notification 20200910-001 TLP: WHITE Cyber Actors Conduct Credential Stuffing Attacks Against US Financial Sector, and I-112321-PSA Cyber Criminals Likely Developing and Selling Scamming Tools to Harvest Credentials of Brand-Name Consumers.



See the attachment for the full report.

Recommendations

The FBI recommends the following mitigating practices for companies to defend against account cracking activity:

- Enable multi-factor authentication (MFA). MFA adds additional layers of protection against credential stuffing attacks and is particularly helpful when a login request derives from an unusual location, such as an unexpected country.
- Educate users to avoid choosing passwords that have appeared in data breaches. Multiple websites maintain databases of breached usernames and passwords. Require all accounts to have strong, unique pass phrases. Pass phrases should not be reused across multiple accounts.
- Download publicly available credential lists, test them against your customer accounts, and force password resets for customer accounts that use compromised credentials.
- Use fingerprinting. Fingerprinting allows websites to analyze information about clients in order to detect unusual activity, like attempts by a single IP address to log into several different accounts.
- Research and consider implementing shadow banning. When a user is shadow banned, their activities, which are not propagated to other users or to system data, do not impact the system. Because shadow banning limits users' activities in a way that is not apparent, the user is unaware their access is limited. When utilized in conjunction with fingerprinting, shadow banning can prevent account crackers from determining the legitimacy of credentials used during a login attempt. Ideally, shadow banning should be configured so that response times to requests from banned and non-banned IPs are indistinguishable.
- Identify and monitor for default user agent strings used by credential stuffing attack tools.
- Ensure that both web-based access and mobile applications have the same, up-to-date security protections. Disable older and less secure versions of applications.
- Use Secure Socket Layer (SSL) pinning in mobile applications. SSL pinning makes it more difficult for tools to track API

requests, and applications that use it are generally more difficult to crack.

- Search online for account cracking configurations tailored to your company’s website, then make changes to that website to prevent the configurations from working.
- Employ cloud protection services (also known as content delivery networks, or CDNs), some of which can detect and block suspicious traffic.
- Do not rely solely on CAPTCHA to defend against credential stuffing and other automated attacks. CAPTCHAs may help deter account cracking but can also be easily defeated using CAPTCHA solving services.

Alert ID 10146bef

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags credential stuffing techniques, Proxies, Configurations, FBI

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Turn off Categories For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC’s Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**