Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

18 August 2022

PIN Number

20220818-001

Please contact the FBI with any questions related to this Private Industry Notification via your local Cyber Squad.

www.fbi.gov/contact-us/field-offices

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

Summary

The FBI is highlighting significant details about proxies[1] and configurations[2] 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

[1] A proxy is an intermediary between an end user (a client) and an online resource (a server). In the context of credential stuffing, proxies are used to mask the true source of a credential stuffing attack, making it appear to the target that the requests are coming from the proxies and not the computer executing the attack.

[2] Configurations, also known as "configs," refer to a file containing instructions or configuration options used by a credential stuffing tool to customize an attack against a particular target.

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.

Threat

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[3], Burp Suite[4], or Fiddler[5] 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.

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.

[3] Wireshark, a free open-source packet analyzer, is a network analysis tool used for network troubleshooting, analysis, software and communications protocol development, and education.
[4] Burp Suite is a set of tools used to perform security testing of web applications.
[5] Fiddler is a web proxy server tool used to debug web applications by capturing network traffic between the internet and test computers.

- 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[6] 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[7] 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.

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*.

[6] SSL pinning is a process of associating a host with its certificate or public key. This security measure pins the identity of trustworthy certificates on mobile applications and blocks unknown documents from the suspicious servers. SSL pinning is used as an additional security layer for application traffic.
[7] CAPTCHA stands for Completely Automated Public Turing test to tell Computers and Humans Apart.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.