Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

10 September 2020

PIN Number

20200910-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

Cyber Actors Conduct Credential Stuffing Attacks Against US Financial Sector

This notification was created jointly by the FBI and the National Cyber Investigative Joint Task Force (NCIJTF).

Summary

Since 2017, the FBI has received numerous reports on credential stuffing attacks[a] against US financial institutions, collectively detailing nearly 50,000 account compromises. The victims included banks, financial services providers, insurance companies, and investment firms. During this timeframe, the FBI noted many reports on attacks targeting application programming interfaces (APIs), which are less likely to require multi-factor authentication (MFA). The attackers masqueraded as legitimate account holders and bank employees to submit fraudulent transactions, including money transfers, bill payments, and credit card reward points purchases. Credential stuffing also caused losses from business costs associated with customer notification, system downtime, and remediation.

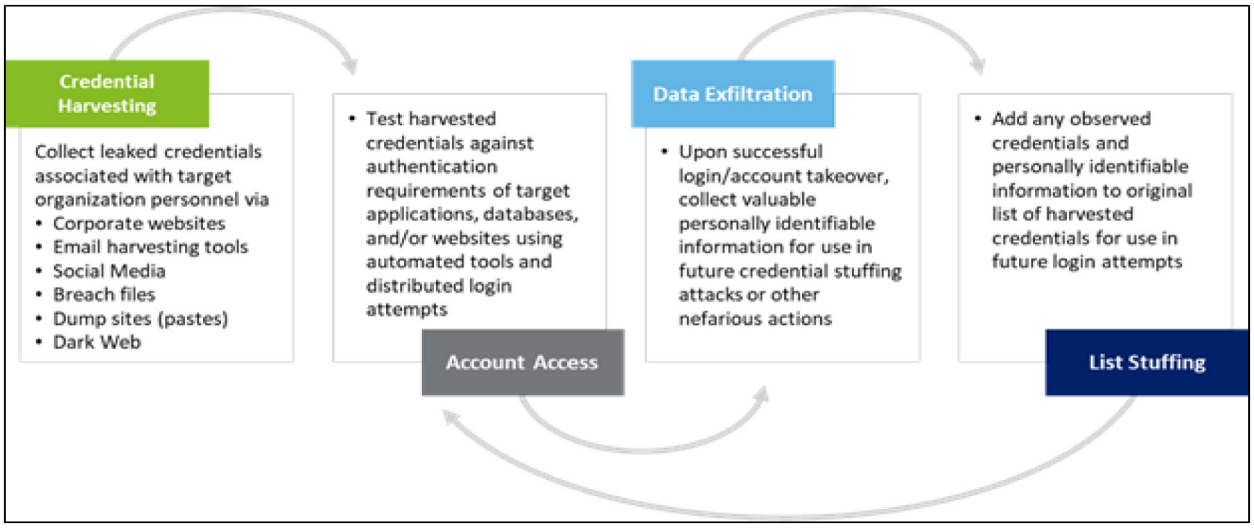
[a] Credential stuffing is a technique using automated tools and botnets to attempt authentication across online platforms with stolen credentials.

Threat Overview

Credential stuffing attacks accounted for the greatest volume of security incidents against the financial sector at 41 percent of total incidents from 2017 through 2019, according to a 2020 cybersecurity firm report. Affected companies experienced downtime, loss of customers, and reputational damage as well as losses associated with customer notification and system remediation costs, according to a 2019 data analytics firm study. Credential stuffing attacks cost an affected business an average of $6 million per year, which excludes costs associated with fraud, according to a 2019 international study conducted by a US-based research center.

When customers and employees use the same email and password combinations across multiple online accounts, cyber criminals can exploit the opportunity to use stolen credentials to attempt logins across various sites. According to a 2020 survey conducted by a data analytics firm, nearly 60 percent of respondents reported using one or more passwords across multiple accounts. When the attackers successfully compromise accounts, they monetize their access by abusing credit card or loyalty programs, committing identity fraud, or submitting fraudulent transactions such as transfers and bill payments.

Figure 1 Credential Stuffing Process



Source: NCIJTF

The increasing prevalence of credential stuffing attacks since 2017 correlates with an increase in leaked credentials available on the dark web, which are expected to number in the billions, according to a 2020 cybersecurity firm report and open-source reporting. Many of the reports received by the FBI indicated the use of botnet credential stuffing. Although most credential stuffing attacks have low success rates, cyber actors' use of botnets to conduct a massive scale of automated login attempts in a short timeframe enabled them to discover multiple valid credential pairs. In addition, the FBI noted a significant level of targeting against APIs. Between May and September 2019, as much as 75 percent of credential stuffing attacks against the financial industry targeted APIs, according to a 2020 cybersecurity firm report.

- In July 2020, a mid-sized US financial institution reported its Internet banking platform had experienced a "constant barrage" of login attempts with various credential pairs, which it believed was indicative of the use of bots. Between January and August 2020, unidentified actors used aggregation software to link actor-controlled accounts to client accounts belonging to the same institution, resulting in more than $3.5 million in fraudulent check withdrawals and ACH transfers. However, reporting does not indicate whether the increased logins and fraudulent transactions could be attributed to the same actor(s).

- Between June 2019 and January 2020, a NY-based investment firm and an international money transfer platform experienced credential stuffing attacks against their mobile APIs, according to a credible financial source. Although neither entity reported any fraud, one of the attacks resulted in an extended system outage that prevented the collection of nearly $2 million in revenue.

- Between June and November 2019, a small group of cyber criminals targeted a financial services institution and three of its clients, resulting in the compromise of more than 4,000 online banking accounts, according to a credible financial source. The cyber criminals then used bill payment services to submit fraudulent payments—about $40,000 in total—to themselves, which they then wired to foreign banking accounts. According to a 2020 case study on one of the firms, security researchers identified more than 1,500 email addresses and 6,000 passwords exposed in more than 80 data breaches. Some of the credentials belonged to company leadership, system administrators, and other employees with privileged access.

Identification

Between 2017 and 2020, credential stuffing attacks and DDoS attacks accounted for most security incidents against the financial sector, according to a cybersecurity firm. The attacks can also be difficult to tell apart as both can slow or crash networks. However, while a DDoS attack is intended to take a system offline by flooding it with more traffic than it is designed to process, a credential stuffing attack is intended to gain system access using a high volume of login attempts to ultimately monetize access. Two indicators specific to a credential stuffing attack are:

- an unusually high number of failed logins, possibly in the millions, from a diverse range of IP addresses via the online account portal;
- a higher than usual lockout rate and/or an influx of customer calls regarding account lockouts.

Recommended Mitigations

The FBI recommends taking the following precautionary measures to mitigate the threat and protect against exploitation, which would best be applied in combination and not individually.

- Alert customers and employees to this scheme and actively monitor accounts for unauthorized access, modification, and anomalous activities.
- Advise customers and employees to use unique passwords they are not using for any other accounts and to change their passwords regularly.
- Direct customers to change their usernames and passwords upon identification of account compromise or fraud.
- Validate customer credential pairs against databases of known leaked usernames/passwords.
- Modify Internet banking login page responses to remove indicators that reveal the validity of credential pairs by issuing the same error message and response time when both username and password are incorrect or only the password is incorrect.

- Establish company policies to contact the owner of an account to verify any changes to existing account information.

- Establish MFA for creating and updating account information, especially for bank, insurance, and trading accounts, as well as for providing initial account access to financial aggregator services.

- Use anomaly detection tools that identify an unusual increase in traffic and failed authentication attempts.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts can be identified at www.fbi.gov/contact-us/field. CyWatch can be contacted by phone at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Administrative Note

This PIN has been released **TLP:WHITE:** Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction**.**

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey