2021

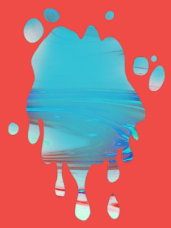
EXECUTIVE SUMMARY

CREDENTIAL STUFFING REPORT

2018 THROUGH 2020
SHAPE SECURITY & F5 LABS

F5 LABS

SHAPE
Part of F5



EXECUTIVE SUMMARY

It is February 2021. The tech industry is reeling from the twin shocks of the theft of FireEye's red team tools and the SolarWinds Orion supply chain attack. Based on what we presently know, these campaigns were state-sponsored attacks against public and private institutions of strategic importance to the United States. However, it was also an opportunity for attackers to achieve persistence in the environments of thousands of organizations. We anticipate that 2021 will have many more announcements and unwelcome discoveries surrounding credential spills. In the meantime, what we already know makes it clear that credential stuffing will remain an enormous risk to organizations of all types.

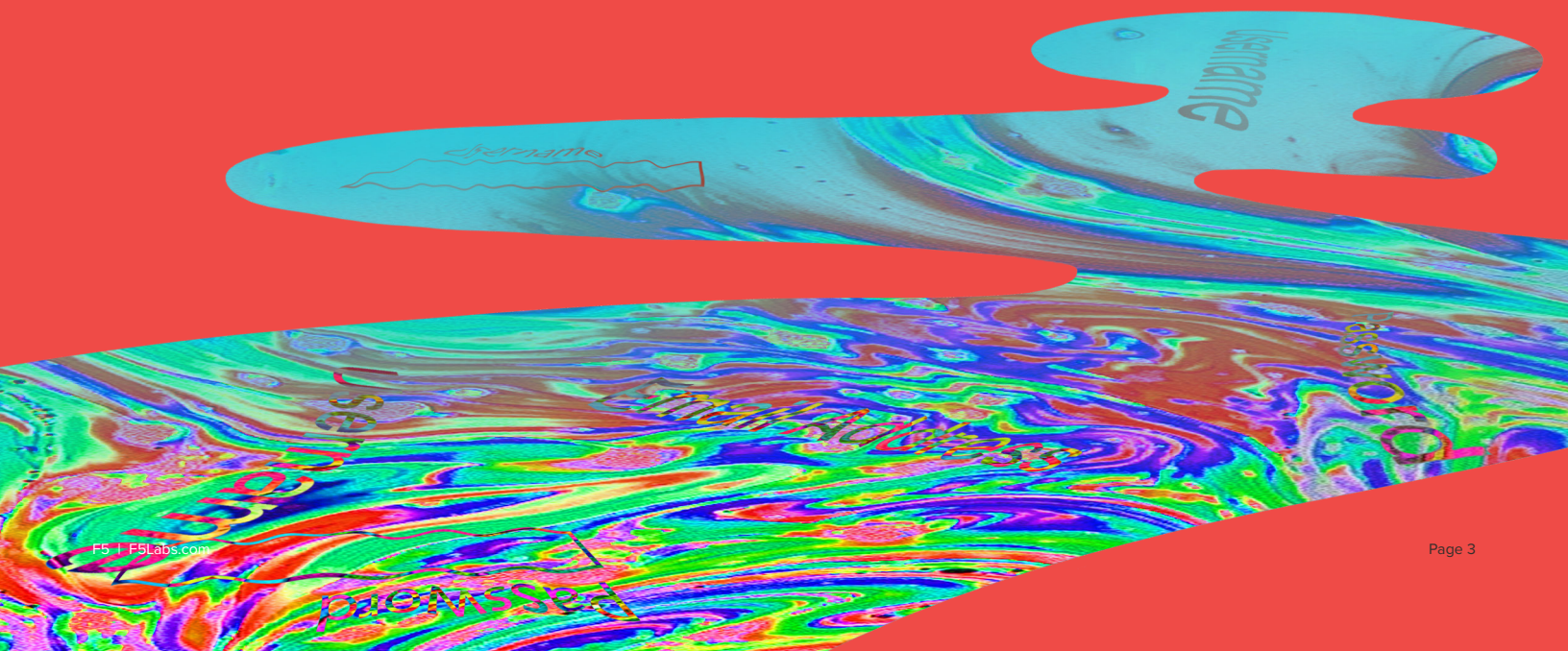
We collected the data in this report to gain a sense of the relationship between three aspects of the ecosystem surrounding stolen credentials: theft, sale, and fraud use. Over the last few years, security researchers at F5 and elsewhere have identified credential stuffing as one of the foremost threats. In 2018 and 2019, the combined threats of phishing and credential stuffing made up roughly half of all publicly disclosed breaches in the United States. In other words, stolen credentials are so valuable that demand for them remains enormous, creating a vicious circle in which organizations suffer both network intrusions in pursuit of credentials and credential stuffing in pursuit of profits. Understanding the supply and demand sides of the market for stolen credentials is, therefore, key to contextualizing and understanding the enormity of the risk that cybercriminals present to organizations today.

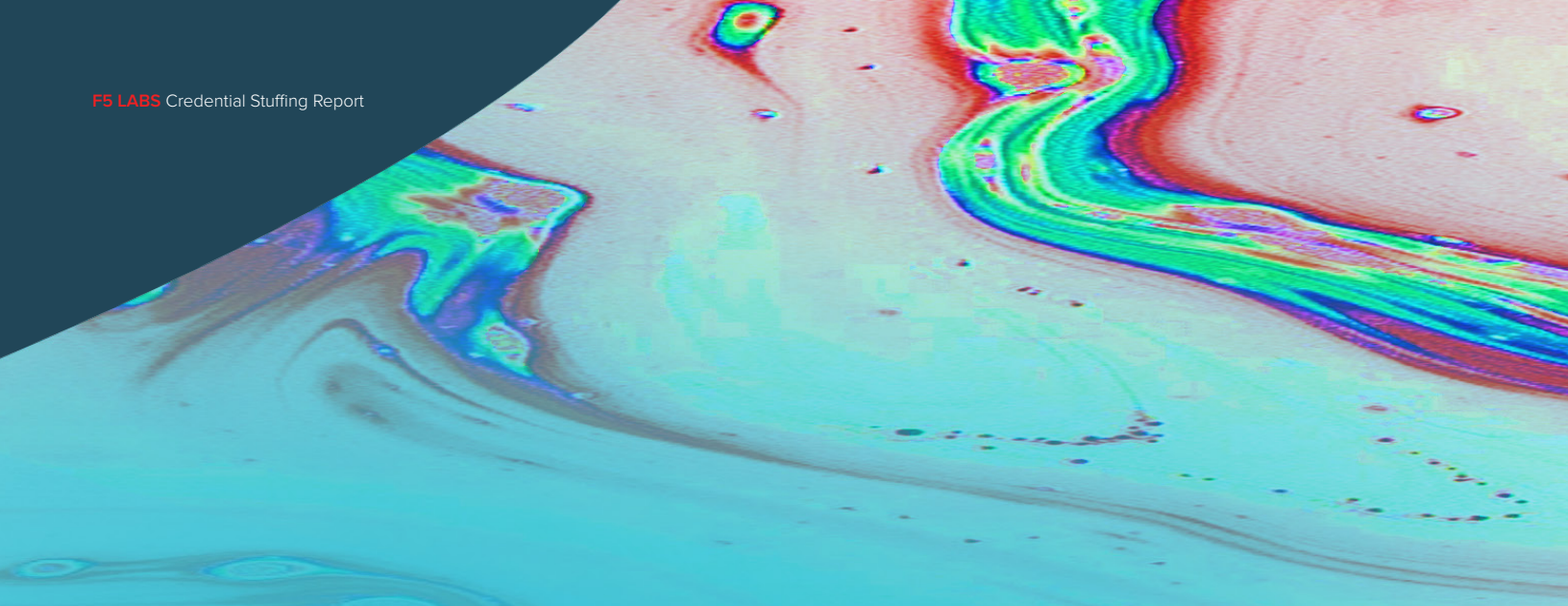
That is why, for 2021, we have renamed this the Credential Stuffing Report (prior versions of this report were titled the Credential Spill Report, published by Shape Security, now part of F5), in order to understand the entire lifecycle of credential abuse, and why we have dedicated so much time and effort to not just quantifying the trends around credential theft but to understanding the steps that cybercriminals take to adapt to and surmount enterprise defenses.

KEY FINDINGS

- The number of annual credential spill incidents nearly doubled between 2016 and 2020.
- The annual volume of spilled credentials has mostly declined between 2016 and 2020.
- The average spill size declined from 63 million records in 2016 to 17 million records in 2020.
- Breach sizes appear to be stabilizing and becoming more consistent over time.
- Despite consensus about best practices, industry behaviors around password storage remain poor. Plaintext storage of passwords is responsible for the greatest number of spilled credentials by far, and the widely discredited hashing algorithm MD5 remains surprisingly prevalent.
- Organizations remain weak at detecting and discovering intrusions and data exfiltration. Median time to discovering a credential spill between 2018 and 2020 was 120 days; the average time to discovery was 327 days. Often spills are discovered on the dark web before organizations detect or disclose a breach.
- Tracing stolen credentials through their theft, sale, and use across Shape customers revealed nearly 33% of logins used credentials compromised in Collection X, a massive set of spilled credentials that appeared for sale on a hacking forum in early 2019. However, the stolen credentials in Collection X also showed up in legitimate human transactions, most frequently at banks.

- There are five distinct phases of credential abuse, corresponding to their initial use and subsequent dissemination among other threat actors:
    - **Stage 1: Slow and Quiet.** Sophisticated attackers use compromised credentials in stealth mode. This phase usually lasts until attackers start sharing their credentials within their community.
    - **Stage 2: Ramp-Up.** As credentials begin to circulate on the dark web, more attackers use them in attacks. The increase in pace means that this period only lasts about a month before the credentials are discovered, so the rate of attack goes up sharply.
    - **Stage 3: Blitz.** Once the word is out and users start changing passwords, script kiddies and other amateurs race to use the compromised credentials across the biggest web properties they know.
    - **Stage 4: Drop-Off.** Credentials no longer have premium value but are still used at a higher rate than in Stage 1.
    - **Stage 5: Reincarnation.** Attackers repackage spilled credentials hoping for a continued lifecycle.
- The majority of "fuzzing" attacks occur prior to the public release of the compromised credentials, lending credence to our understanding that fuzzing is more common among sophisticated attackers.
- A rich and growing ecosystem of attack tools—many of which are shared with security professionals—enables credential stuffing attacks and threatens the efficacy of existing controls.
- Attackers continue to adapt to fraud-protection techniques, creating a need and opportunity for adaptive, next-generation controls around credential stuffing and fraud.





READ THE FULL REPORT ON F5LABS

https://www.f5.com/labs/articles/threat-intelligence/2021-credential-stuffing-report

CONCLUSION: MINIMIZING THE THREAT OF CREDENTIAL STUFFING

A common truism in the security industry says that there are two types of companies—those that have been breached, and those that just don't know it yet. As of 2021, we should be updating that to something like "There are two types of companies—those that acknowledge the threat of credential stuffing and those that will be its victims." In the F5 Labs 2019 Application Protection Report, we found that access-related attacks, which comprise phishing and credential stuffing in its various forms, made up roughly half of the publicly disclosed data breaches in the United States over 2018 and 2019, which was a far greater proportion than any other cause (Figure 35).

Figure 35. U.S. breaches, 2018-2019, by cause (%).

Credential stuffing will be a threat so long as we require users to log in to accounts online. The most comprehensive way to prevent credential stuffing is to use an anti-automation platform. In addition, follow these 10 best practices for minimizing the threat of credential stuffing—from ways an organization can shrink its attack surface to tips for employees:

1. **Promote unique passwords.** Every year, articles are published on the most common passwords used, and year after year, very little changes.[8] Clearly, consumers continue to use them. Why not share that top 10 list when users are creating a password on your site, encouraging them to choose a different password? Furthermore, when users are creating accounts or resetting passwords, use language to encourage them to choose a unique password they haven't used elsewhere. Now, 70% of users will likely tweak an old password, which still leaves them vulnerable to fuzzing attacks, but it will weed out the bottom of the barrel.[9]

2. **Give users options for passwords.** Do not set requirements on the number or type of characters customers and employees must use when creating a password. While these parameters prevent users from choosing one of the absolute worst passwords (123456, password, 111111, etc.), they actually reduce the set of possible passwords, thereby increasing the likelihood an attacker can brute force their way in. Instead, encourage users to choose a password optimized for length.

3. **Prevent users and employees from using known compromised credentials.** All organizations should routinely cross-reference their users' and employees' credentials against an "allow list" of username and password combinations that have already been compromised. One way is to use a "dark web" service as an intermediary to discover spilled credentials that have been shared on dark web marketplaces. However, because the dark web is, by design, unsearchable, it is impossible to ascertain whether one of these services has combed 10, 30, or 50% of all posted credentials.

   Furthermore, as discussed in "The Lifecycle of Spilled Credentials," it takes on average 10 months for credentials to be posted on dark web forums. Thus, organizations may want to use technology that detects compromised credentials as soon as attackers weaponize them, months before they hit the dark web.

4. **Reduce feedback.** As we mentioned in "The Lifecycle of Spilled Credentials," time is an extremely precious resource for an attacker. One way to increase the time it takes for an attacker to launch a successful credential stuffing campaign is to reduce the feedback attackers receive from unsuccessful attempts. As an example, when a user enters incorrect login credentials, do not disclose which element of the credential, the username or password, was incorrect. Instead, the error message should read "login failed," or the verbose yet accurate, "that combination of username and password does not exist in our system."

5. **Look for a diurnal pattern.** One of the things that distinguishes humans from bots is sleep. Legitimate consumers are going to wake up in the morning, conduct transactions during the day, and then power down at night. So organizations should monitor three functions—login, password reset, and account creation—to ensure a consistent diurnal pattern that reflects their customers' business hours. If not, it is likely the organization is under substantial credential stuffing attacks.

6. **Monitor key metrics.** While blocking based on diurnal patterns will deter elementary attackers, advanced attackers time their attacks to mirror normal business hours. So just because traffic appears relatively diurnal and normal does not mean attacks are not occurring. Thus, security teams should monitor two key metrics:

   - Login success rate. Normal human login success rates are 60 to 80%, depending on the industry.[10] Financial institutions have higher success rates because customers tend to value and therefore remember their online banking credentials over, say, their password for one of many ecommerce sites they visit. If a website or mobile app's login success rate suddenly drops by 10 to 15%, that suggests the application is under attack by criminals testing nonexistent credentials.

   - Password reset request rate. An uptick in reset requests may indicate reconnaissance for a credential stuffing attack.

7. **Connect security and fraud with marketing.** False positives are a huge issue for security teams fighting fraud. Not only do they impact revenue, but they run the risk of alienating both the customer and colleagues at the organization. In order to reduce this risk, it is important to be in touch with teams

at the organization whose activities might affect legitimate human traffic. To use a recent real-world example, a siloed security team might think that a spike in transactions from the UK represented an attack on their site. In fact, these weren't credential stuffers targeting the company, they were actual customers acting slightly out of the norm. The digital marketing team had emailed out a two-for-one flight deal that morning to all of its UK customers, causing an abnormal spike in traffic. Had the security or fraud teams not had a heads-up, the company might have lost tens of thousands of dollars in revenue.

8. **Train marketing.** The relationship between security teams and marketing departments should be a two-way street. In many organizations, digital marketing teams have a dominant say in managing the website. They need to be taught how to best keep the website and their customers safe.

   For example, one practice might be having the security team verify that any plug-ins and code snippets are acceptably low risk before they are added to the website. In other words, a customer-facing site should go through the same change control process as any other aspect of an application. Several breaches have occurred in the last few years due to the addition of malicious code to the website that masqueraded as a Google Analytics script.[11]

   Another practice marketing teams should embrace is storing data only when necessary. Data-driven marketing is all the rage, but each piece of data collected poses an additional risk for end customers. For example, does your particular company require a unique account registration system? Or would it be possible to outsource identity management to a known secure solution such as Google or Okta? Educating marketing teams about the risks that accompany the rewards of collecting customer data can save a lot of pain down the line.

9. **Extend signal collection beyond a single organization.** Companies should adopt methods to leverage each other's data points (in compliance with data privacy laws), allowing them to better secure users and prevent fraud from account takeovers. For example, if a user known to make purchases of $25 to $50 on a certain retail site suddenly made a $500 purchase, that wouldn't necessarily raise any alarms (nor should it). But if that user also made an unusually large purchase on another retail site and also converts all of their credit card reward points into gift cards that week, then it's possible the user's accounts have been compromised.

   Similarly, it would be reasonable for an American user to log in to their frequent flyer account from Japan, as they might be traveling. The airline would not want to block users' transactions simply due to a change in location. What would be unusual, and a sign of account takeover fraud, would be if that same "user" had logged in to their bank account that same day from Brazil.

10. **Work with law enforcement.** Another area for potential collaboration is between the private sector and law enforcement. In 2018, we witnessed the first major conviction of a credential stuffer.[12] The FBI managed to track down the attacker after he forgot to use his VPN when stealing data from Disqus (a spill reported in 2017).

    Furthermore, while credential stuffing is by and large a financially motivated attack, we have seen nation-states engage in credential stuffing. The lines will likely continue to blur between nation-state activities and financially motivated crimes, in which case it is especially prudent for companies to begin collaborating with law enforcement, if they haven't already.