# SHAPE

2018
Credential
Spill Report

2018 Credential Spill Report

Second Annual Edition

About Shape Security

The world's leading financial, retail and travel companies and government agencies rely on Shape Security as their primary line of defense against fraud and attacks on their web and mobile applications. The Shape platform, covered by 55 patents, was designed to stop the most dangerous application attacks enabled by cybercriminal fraud tools, including credential stuffing (account takeover), product scraping, unauthorized aggregation, and other threats. Shape has prevented over $1 billion in fraud losses for its customers and protects more than 20% of the world's in-store mobile payments. Shape is headed by industry leaders from Google, Cisco, IBM, Raytheon, Palo Alto Networks, and the Pentagon.
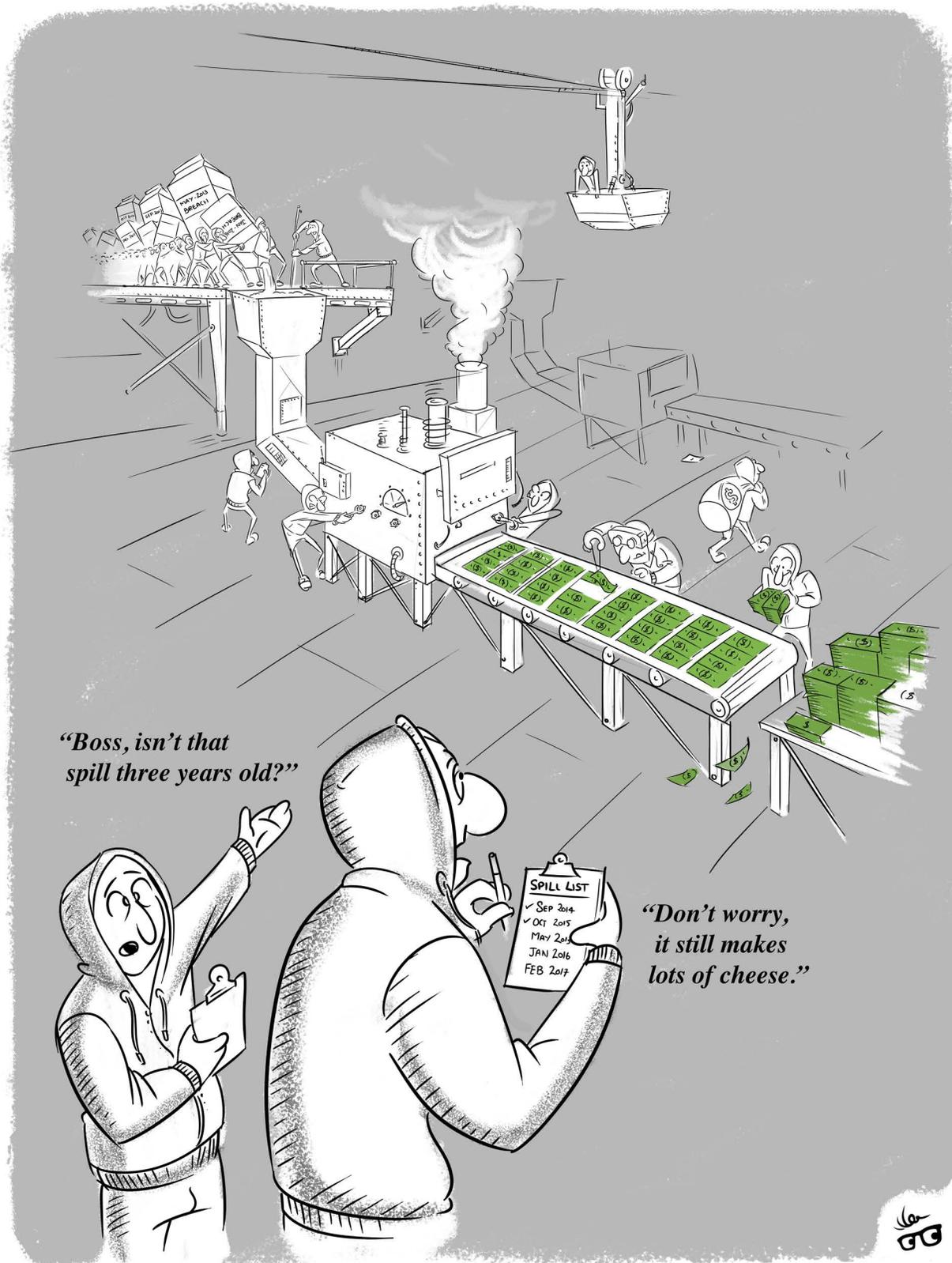
Table of Contents

Figures and Tables

Key Findings

2017 Credential Spills

2.3 Billion
Credentials reported spilled in 2017

The frequency of credential spills has remained extremely consistent for two years, but the average size of spills in 2017 was lower than in 2016.

13 Spills
13 of the 51 credential spills were from breaches of web forums

Web forums were the most frequent targets for credential spills in 2017, but organizations providing online services contributed the largest number of compromised credentials (over 2 billion).

15 Months
Between spill and announcement

On average, there was a 15-month delay between the day credentials were compromised and the day the spill was reported.

2017 Credential Stuffing Analysis

80-90%
Credential stuffing attacks make up, on average, 80-90% of an online retailer's login traffic

Online retailers face the highest proportion of credential stuffing as attackers exploit retailers' desire for a frictionless customer experience.

$50 Million
The US consumer banking industry faces nearly $50 Million per day in potential losses due to credential stuffing attacks

Consumer banks face the highest potential losses from credential stuffing due to the high volume of attacks, as well as the high cost of account takeovers.

Introduction

Everyone knows there's no such thing as a free lunch, but that doesn't stop us from salivating over a deal that's too good to be true. Roundtrip business class flights from LAX-LHR for the cost of a one-way from SFO-JFK. A $100 gift card for $50. Even a wheel of fancy French cheese at American single prices.

Such Internet offers might sound benign, or silly at worst, but they're in fact the consequence of a criminal enterprise that costs US businesses more than $5 billion each year.

It all starts with the keys to the internet kingdom: credentials. These are the username-password combinations that we use every day.

Criminals harvest credentials from data breaches and then test them on every website and mobile app imaginable. A small subset of those credentials unlock accounts because most consumers reuse passwords across multiple sites. The criminals then drain those accounts of value to commit all manner of fraud, from unauthorized bank transfers to illicit purchases of Camembert. Some of us unintentionally help perpetuate the fraud cycle when we snap up those deals that are indeed, too good to be true.

Last year, over 2.3 billion credentials from 51 different organizations were reported compromised. In our 2018 Credential Spill Report, we delve into how criminals stole, weaponized and resold those credentials and how they turn compromised account into profits. We also drill down into the costs of credential stuffing attacks on companies in various industries that attackers routinely target.

Shape Security's perspective on the credential stuffing ecosystem is unparalleled. We protect more than 1.6 billion online accounts from credential stuffing on behalf of our customers. Our customer network represents huge swaths of US industries, including 60% of airlines, 40% of hotels, and 40% of consumer banking. On a periodic basis we aggregate our data on credential stuffing attacks across all industries, which provides the world's most comprehensive picture of how attackers are operating and evolving.

Last year, we published the first Credential Spill Report to raise awareness of the issue of credential stuffing. Our second edition shines light on a crucial piece of the credential-stuffing problem: the length of time between credential spill & discovery.

The longer the period between a credential spill and its discovery, the more time criminals have to carry out attacks using credentials that have not yet been identified as compromised. **In 2017, it took on average 15 months for a credential spill to be discovered and reported.** Why do discovery and reporting take so long? How can the gap be shortened? Our chapter "The Life Cycle of Stolen Credentials," seeks to explain what exactly is happening during that gap and how attackers keep credential spills under wraps.

2017 Reported Credential Spills

We define credential spill as an incident in which a set of usernames and passwords from an organization become compromised. For this first chapter, we aggregated and analyzed all of the credential spills that were reported by breached organizations or by the media in 2017.

By the Numbers

Table 1: 2017 Reported Credential Spill Statistics

		Change from 2016 to 2017
Total Credentials Reported Spilled	**2,328,576,631**	⬇
Total Reported Credential Spills	51	⬌
Average Number of Credentials Compromised Per Spill	47,521,972	⬇
Median Number of Credentials Compromised Per Spill	996,000	⬇
Largest Reported Credential Spill	2,000,000,000	⬆

Note, there were two spills reported in 2017 - HipChat and Cash Converters - that were included in the total number of spills but not included in any additional analysis because we do not know the number of credentials included in each compromise. HipChat's compromise affected all users, but HipChat has declined to report their total number of users.[1] The breach at Cash Converters affected an unknown number of customers in Australia and the UK.[2]

[1] https://www.engadget.com/2017/04/24/hipchat-resets-all-passwords-after-hackers-break-in/
[2] https://teiss.co.uk/news/cash-converters-data-breach/

2016 vs. 2017 Credential Spills

The number and frequency of spills has remained remarkably consistent over two years. In 2016, there were 52 reported spills; in 2017, there were 51. As depicted by the figures below, there doesn't appear to be a relationship between time of year and size of spill. Additionally, over the course of two years, spills have been reported on a very regular basis; in 2017, the longest gap between reports was 31 days.

Credential Spills over Time
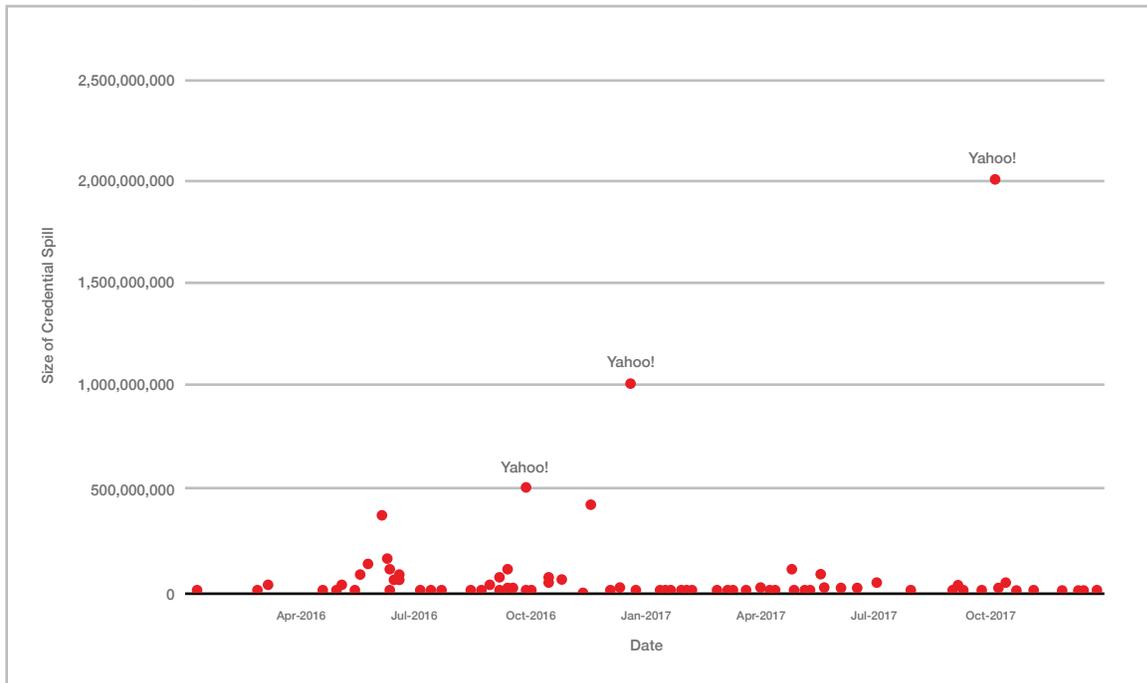
Figure 1: Credential Spills Over Time 2016-2017

Credential Spills over Time (excluding Yahoo! spills)
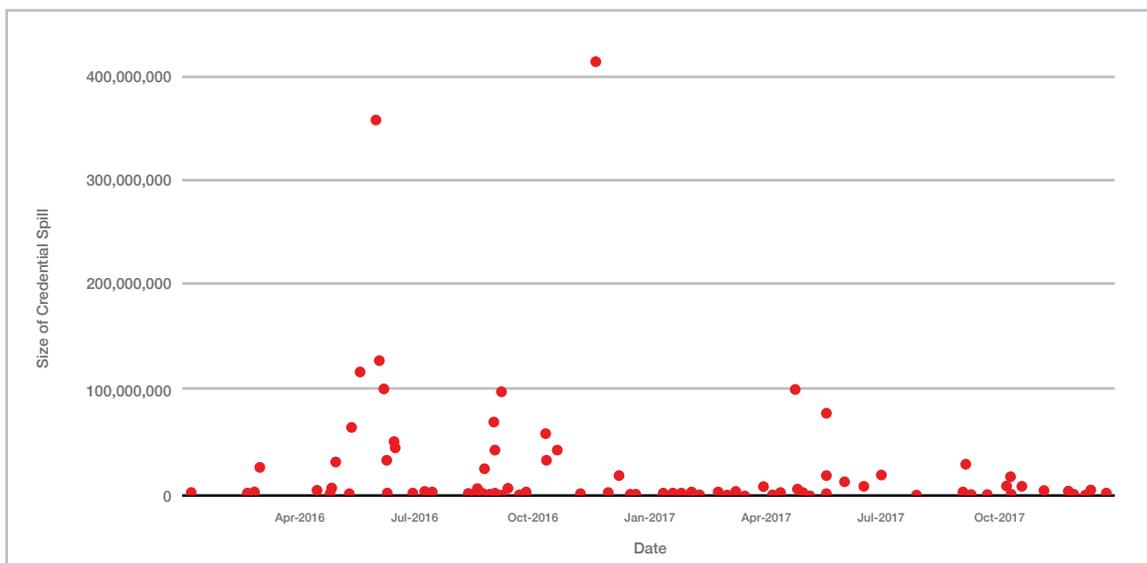
Figure 2: Credential Spills Over Time (Excluding Yahoo Spills) 2016-2017

5 Largest Spills in 2016 vs. 2017

Social media sites were typically responsible for the largest spills. This makes sense because those organizations rely on a network effect to succeed, so they are likely to have the largest user bases.
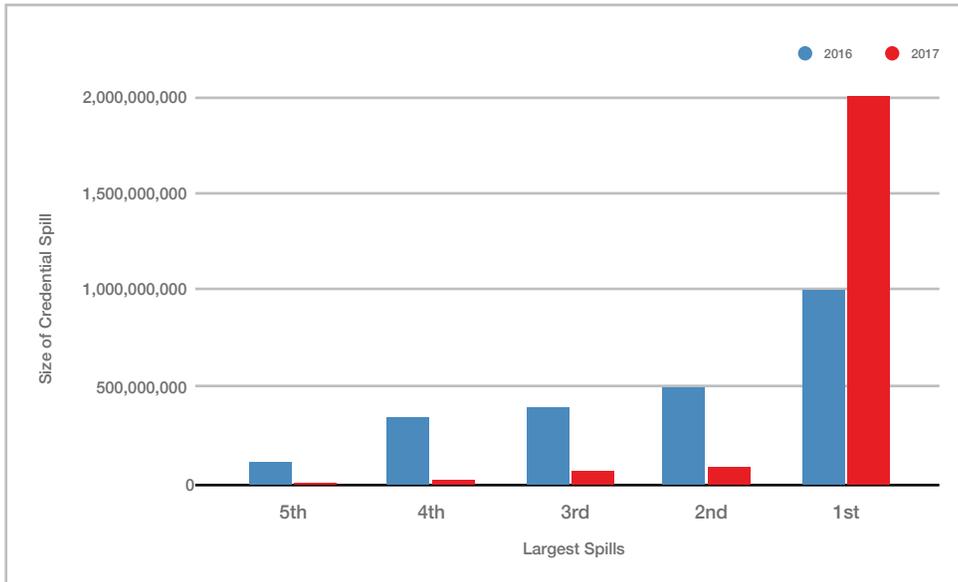
Figure 3: Five Largest Spills in 2016 vs. 2017

While the number of spills reported remained consistent, the size of spills reported was smaller in 2017. The median spill size in 2016 was 2.8 million while it was just under 1 million in 2017. However, as shown in Figure 3, 2017 did break the record for the largest spill.

Yahoo!

In 2016, Yahoo made records for both being the only organization with two reported spills (September and December 2016) and for having the largest single credential spill (1 billion). The next year, Yahoo unfortunately beat its own record of having the largest recorded credential spill in history. In October 2017, Yahoo announced that its previously reported 2013 breach had actually affected all users, meaning an additional two billion credentials had been included in the spill.

While Yahoo made up a considerable number of the credentials reported compromised in 2017, even without its spill, there were on average nearly 1 million credentials exposed to criminals every single day. That's the equivalent of **every San Francisco resident** having one of their online accounts exposed every single day.

Origins of 2017 Credentials

We categorized each spill by organization type to explore the different sources of compromised credentials. All types of organizations fell victim to credential spills in 2017, from the online service[3] Ancestry.com to Lady Gaga fan forum[4] Little Monsters.

As demonstrated by Figure 4, while web forums were the most frequent targets, they weren't the contributor of the same proportion of spilled credentials. This is likely due to the nature of web forums themselves. Forums serve as hyper-specialized communities of online users, so their overall membership is likely to be low, making them a small provider of credentials. However, they are easy targets for credential spills because many are volunteer-run and lack a corporate security or IT function. For example, the forum MrExcel reported a credential spill in January 2017. The website is dedicated to sharing information about Microsoft Excel and features an online forum for users to post and answer questions. The site appears to be run largely by the sole owner, Bill Jelen. Fewer than 400,000 credentials were compromised in a breach due to an old, known vulnerability in the web forum's software.

Not All Spills are Created Equal:
Most frequent targets are not responsible for the largest spills
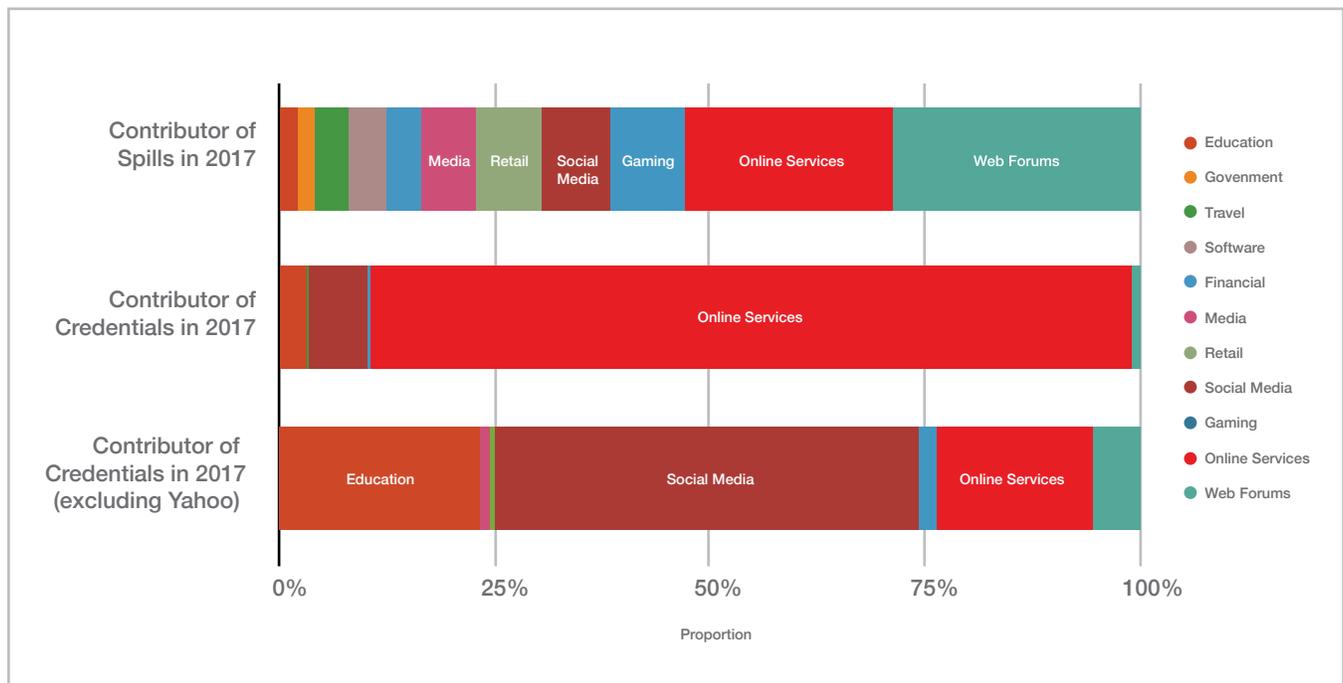
Figure 4: 2017 Proportion of Credential Spills and Spilled Credentials by Organization Type

When comparing credential spills by organization type in 2016 and 2017 (Figure 5), a key difference comes to light. In 2016, adult and dating sites were frequent targets for breaches resulting in spills, yet in 2017, not a single adult site reported a credential spill.

[3] Online services are defined as communications or productivity services that can only be consumed via the internet.
[4] Web forums are categorized here as topic-based online user groups.

Spills by Organization Type
2016 vs 2017
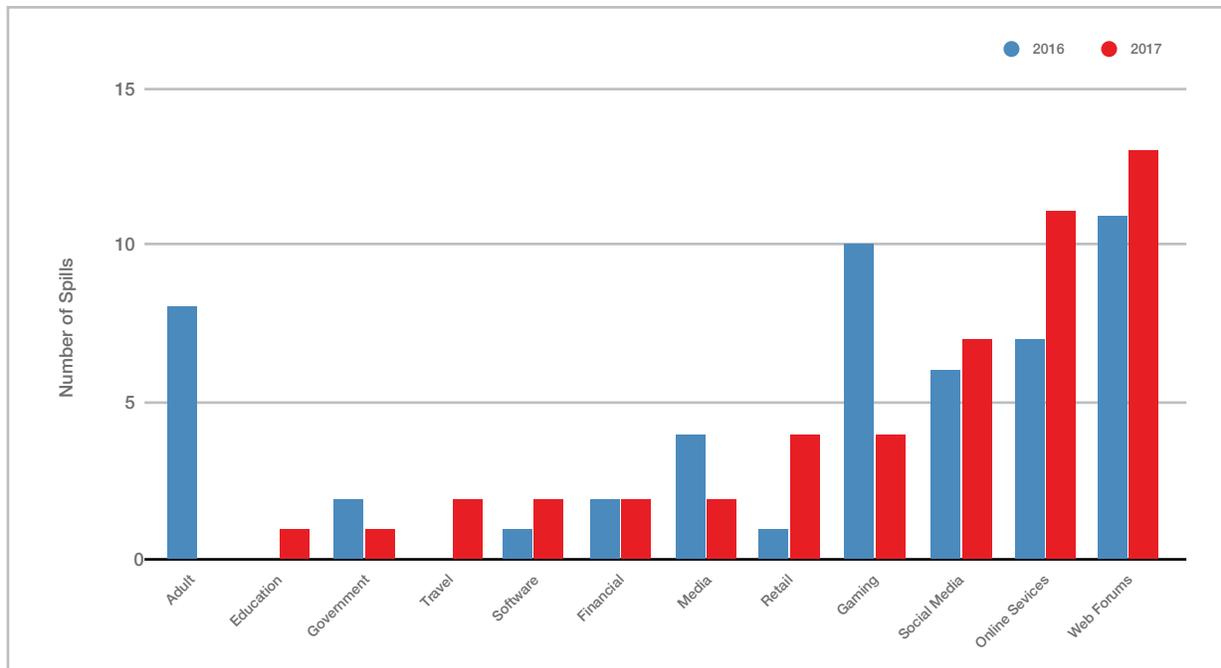
Figure 5: Credential Spills by Organization Type 2016 vs. 2017

Another point that will become even clearer in a later chapter is that the organizations that criminals source credentials from are very different from the ones that they use those credentials against. Attackers primarily source credentials from the easiest targets - for example, free websites that make their revenue off of ads - and then weaponize them against the highest-value targets, e.g., financial, retail, travel, and telecom companies.

Spills by Method of Attack

Sometimes an organization is either unwilling or unable to share exactly how credentials came to be compromised. Of the 51 reported spills in 2017, we only know the cause of compromise for 30 of them. Interestingly, those 30 disproportionately represent the smaller spills. For example, of the five largest spills in 2017, we only know the cause of the fifth largest (8Tracks, 18 million credentials compromised via an employee's GitHub account). Still, of the spills where the method of attack is known, three key themes emerge:

9 spills
13.8M credentials

VBulletin is still a VBig problem: Why Web Forums were the Most Frequent Target

VBulletin is a popular software used to create online forums. In 2015, the creators announced the existence of SQL injection vulnerabilities,[5] and they subsequently released a patch. Unfortunately, many forum owners did not update their software and continue to run older versions. Attackers know this, so an easy source of credentials in 2017 was to probe internet forums for the vulnerability.

9 spills
9.1M credentials

Locked Doors but Open Windows: Misconfigured Database or Server

Attackers don't need to be very skilled hackers if the organization does the work for them. Organizations across almost all industries were guilty of misconfiguring their databases or database servers, leaving them exposed to the public.

3 spills
2.5M credentials

Go Directly to the Source: Users

The benefit of acquiring credentials via malware or phishing campaigns is that the attacker knows that the credentials are likely to be fresher than from a database, which may contain old, outdated records. Note, phishing and malware campaigns are very prevalent and are likely under-reported.

Beyond the big three, other reasons for credential spills in 2017 included software vulnerabilities, a third-party web server breach, and SQL-injection attacks.

---

[5] A SQL injection vulnerability occurs when software poorly sanitizes user-submitted data before sending commands to run on a database. Specially formatted values can enable attackers to write unapproved commands that are run directly on a database, often with privileged data access.

The Life Cycle of Spilled Credentials

New to this year's report, we studied how long it took between the time credentials were originally compromised and the time the spill became publicly known.

Why does this length of time matter? **Because the length of time between the day credentials are stolen and the day spills finally become public increases the cost and negative consequences of the spill.** The longer an attack group can keep secret the fact that they have stolen credentials, the more value they can extract by weaponizing the credentials against many other organizations beyond the source. Users, unaware of the spill, will typically continue using the compromised credentials at the original organization, as well as five other key online accounts.[6]

In the previous chapter, we discussed the difficulty in identifying the root cause of a credential spill. Similarly, it is not always possible to determine when credentials are originally compromised. Roughly

two-thirds of the organizations that reported spills in 2017 were able to trace back the original date of compromise, and the data does not paint a pretty picture.

Half of all credential spills were discovered and reported within the first four months of the compromise. However, because some spills take years to discover, it took an average of 15 months between the day that an attacker accessed the credentials to the day the spill was reported in 2017.

15 months
average time for credential spills
to be discovered and reported in 2017

Most organizations in 2017 reported a credential spill soon after they discovered it themselves, but that discovery can take years. CafeMom, a now-defunct

The Four Stages of Spilled Credentials

### Access to Stolen Credentials Increases, Value Decreases Over Time
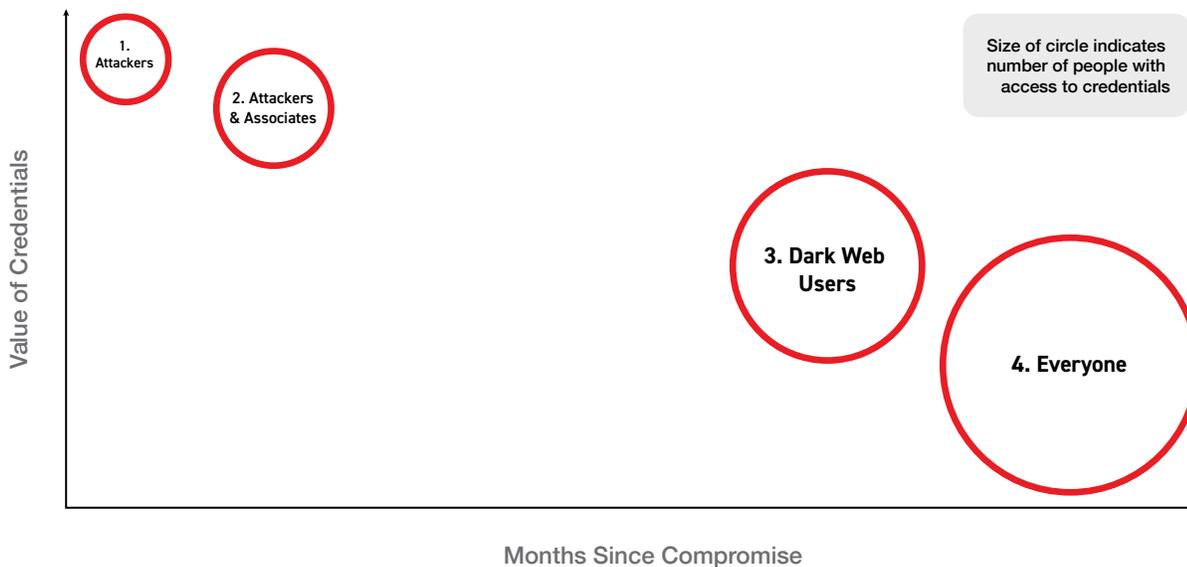
Figure 6: The Life Cycle of Spilled Credentials in Four Stages

[6] An Experian poll found that the average consumer uses just five passwords across 26 online accounts.
http://www.theregister.co.uk/2012/07/20/password_reuse_survey/

social network for mothers, took **nearly seven years** to discover and report that the credentials of 2.5 million users had been compromised.

The biggest offender in 2017 in terms of reporting time was Avon. The cosmetics company had been alerted by external security researches about a database vulnerability in May 2016 that had exposed over 600,000 customers' credentials to attackers. The company ultimately took the database offline in early 2017 but did not ever alert their customers of the spill. The spill was reported in April 2017 only because the security researchers publicized their discovery.[7]

When attackers initially steal credentials, they try to extract the maximum value from the information (stage 1). If willing and able, they may conduct credential stuffing attacks themselves. Otherwise, or afterwards, the attacker will sell the credentials directly to known associates (stage 2). Selling directly means the attacker will share the credentials only with his criminal network and not post them for public sale on dark web marketplaces or forums. Keeping stolen credentials secret drives up the price and lessens the likelihood that the credential spill will be discovered by the organization or security researchers. After the attacker and/or associates have sufficiently leveraged the credentials they will post the credentials on the dark web (stage 3).[8]

If a credential stuffing attacker is new to the game, however, he may not have direct contacts or access to private forums where he can sell the credentials. He would then have to post the credentials on a public forum or marketplace. Because there are so many credentials available on the dark web and because a new attacker lacks credibility, he may have to price them below market rates in order to attract a buyer. In some cases, the attacker may even publish a subset of the stolen credentials for free on the dark web or on an open site like Pastebin.com as an advertisement (stage 4). This option allows other criminals to validate the credentials, gaining the original poster credibility. Once a criminal has gained credibility, he will be invited to specialized forums, allowing him to extract further value the next time he has spilled credentials to trade.

The length of time between when an attacker steals credentials and when they are posted on the dark web (if at all) varies wildly. CafeMom which, as mentioned above, discovered its breach nearly seven years after the fact, likely discovered the spill only because its users' passwords were finally posted on a dark web forum. Online pawnbroker Cash Converters, on the other hand, announced its data breach just two months after it originally occurred, but no major dark web credential collector has received those credentials yet.

Credential Stuffing Attacks During Early Stage of Life Cycle

Shape has seen instances of credential stuffing attacks occuring at each stage of the credential life cycle. For example, over the course of two months, we observed a criminal actor or group of actors, "Actor Prime," performing attacks across four separate customers in the Shape Network - a North American financial services provider, two retailers, and a global dating platform. Based on Actor Prime's extreme technical sophistication, selection of high-profile targets, and login success rate, we can assume these attacks were in stage 1 or stage 2 of the life cycle.

Shape identified that all of these credential stuffing attacks originated from the same source based on the technical specifications of the attack and shared infrastructure used.

Attack Method

Actor Prime used an iOS platform, which is extremely rare due to the steep technical and architectural obstacles faced by would-be iOS attackers. In Shape's prior five years of defending companies from credential stuffing attacks, we had seen the iOS platform used as an attack vector only once before; and even in that case, the attacker was never able to correctly produce any iOS-specific signals. Every other mobile API attack observed across Shape's entire network used only Android platforms.

---

[7] https://www.ibtimes.co.uk/avon-left-more-620000-brazil-customer-details-exposed-hackers-months-1616732

[8] If they are posted at all. The three billion Yahoo credentials that were compromised in 2013 have yet to be posted on HaveIBeenPwned, which is one of the largest collectors of dark web credentials.

Inconsistencies and behavioral clues enabled Shape to accurately distinguish the attack traffic from legitimate iOS visitors and ultimately mitigate Actor Prime's attack.

Infrastructure

Besides technical skill, Actor Prime had ample financial resources. Actor Prime had access to a seemingly unlimited number of IP addresses from a wide variety of ASNs (Autonomous System Numbers). Their attack on one of the retailers started off with IP addresses from over 30 countries, and they only expanded their global reach when retooling, i.e., attempting to tweak their attack in order to circumvent Shape's defense.

Geographic Distribution of Original Attack & Retooled Attack

The key takeaway from the charts below is that IP-based rate limiting is wildly ineffective when facing sophisticated attackers
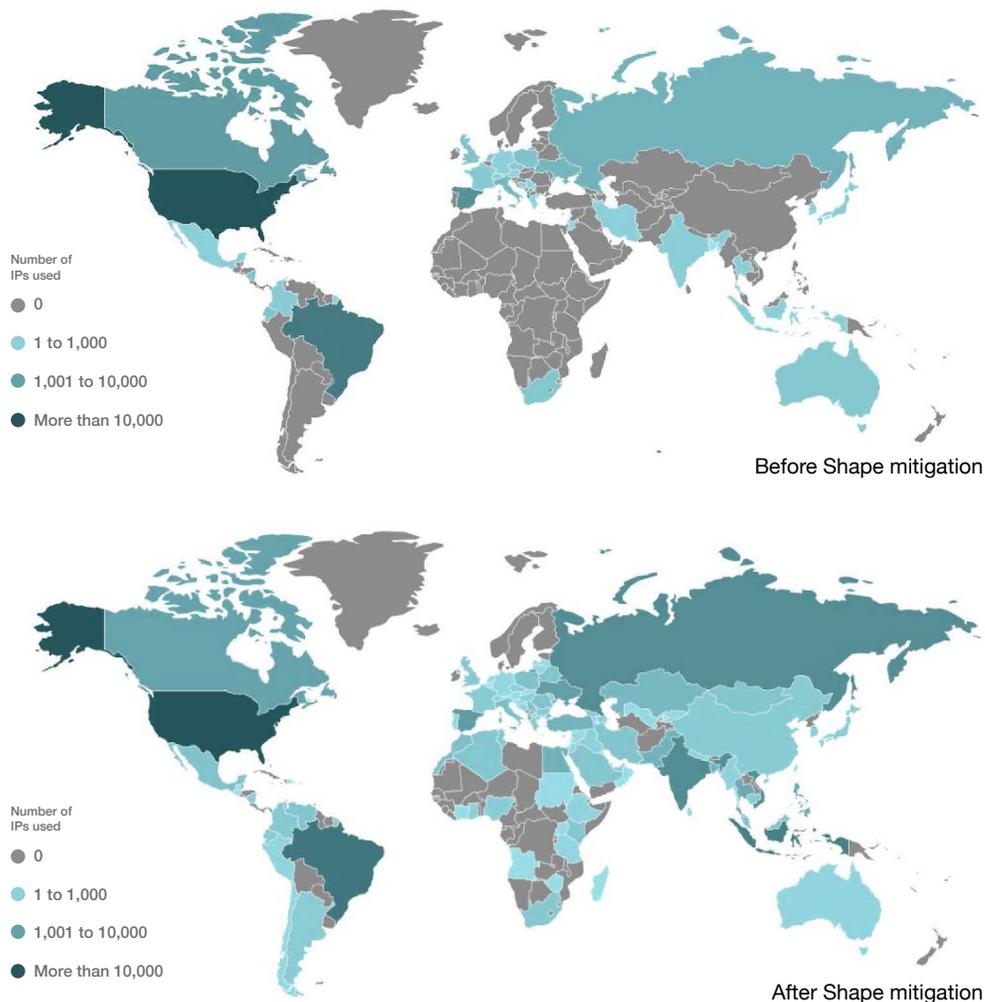
Figure 7: The Geographic Distribution of an Attack Before and After Shape Mitigation

While Actor Prime was too sophisticated to reuse IP addresses when attacking a single target, lest they be stopped by IP-rate limiting, they didn't think they would be caught recycling IPs across their target set. Shape observed credential stuffing attacks using the iOS platform originating **from the same IP hit the two retailers and the financial services company within a minute of each other,** strongly suggesting these attacks were orchestrated by the same source.

Credential Stuffing Attacks Occur During All Stages of Life Cycle Simultaneously

At any given moment, an enterprise will be under attack from multiple groups that are weaponizing separate credentials spills. For example, Shape observed five separate attack groups performing credential stuffing attacks on a Top 5 US Bank's mobile app over the course of two weeks.
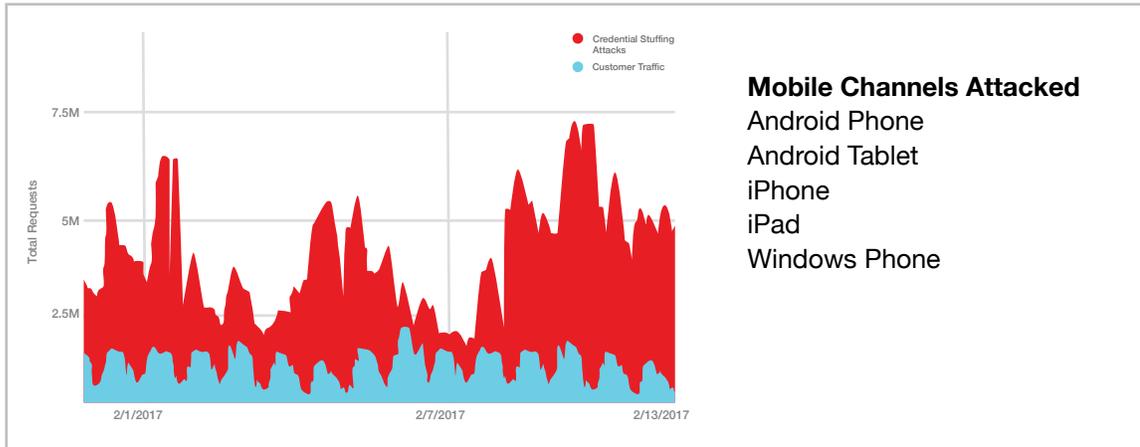
Figure 8: Credential Stuffing Attacks on a Top 5 US Bank

In aggregate, the attackers targeted 363,000 bank accounts, or about 4,000 accounts per day. Since each represented a separate criminal network, they each operated using a different set of credentials, so we analyzed how much overlap there was amongst their different sets.

5 Different Attack Groups Used Mostly Unique Credential Lists
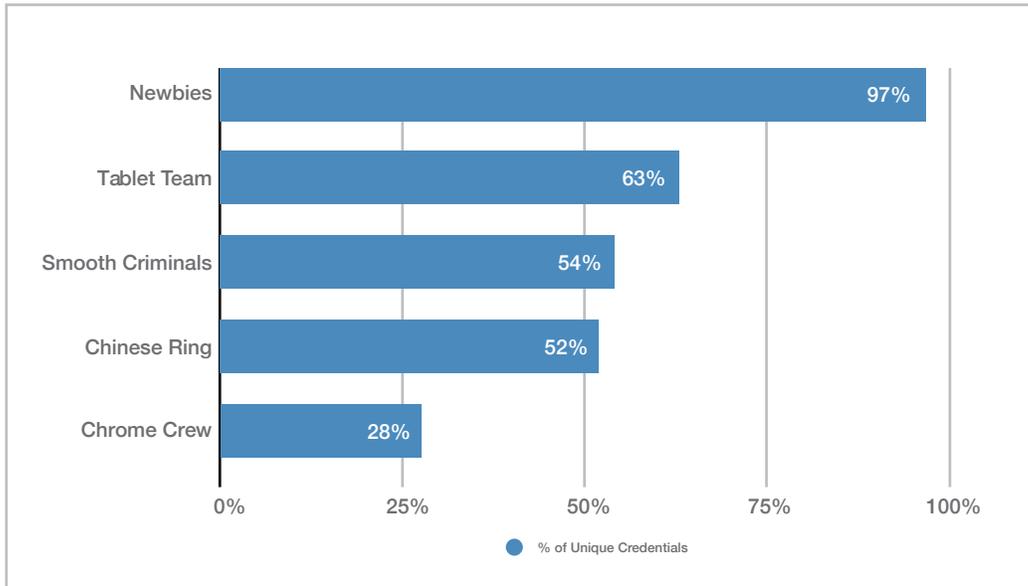
Figure 9: The Proportion of Credentials Unique to Various Credential Stuffing Attack Groups

Of all five groups, the "Newbies" had the largest, as well as most differentiated, list. Ninety-seven percent of the credentials used, or about 92,000, were unique to their group. On the other end of the spectrum, only about a quarter of the 8,000 credentials tested by the Chrome Crew were unique.

However "unique" does not necessarily mean fresh or good; it could be that the Newbies were using older credentials from irrelevant sources.[9] Indeed, the group only had a 0.02 percent login success rate, meaning after two weeks they successfully hijacked just 19 accounts.

What's in a Name?

Each attack group observed by Shape is named based on a unique characteristic or behavior:

Newbies:
This group was likely new to credential stuffing based on their extremely low login success rate.

Tablet Team:
These actors were the only ones to target the bank's Android tablet application.

Smooth Criminals:
These actors were clearly experienced based on their high login success rate and ability to target multiple applications across both Android and iOS platforms.

Chinese Ring:
The only group originating from China.

Chrome Crew:
While this group used almost 50,000 different user agents throughout their campaign, they heavily favored a user agent string associated with Chrome 30.

Judge a Credential List by its Login Success Rate

As shown in Figure 10, only half of the Smooth Criminals' credential list was unique to them, but they also had the highest login success rate, at nearly 1 percent. This suggests that the Smooth Criminals had access to fresher, more relevant credentials.
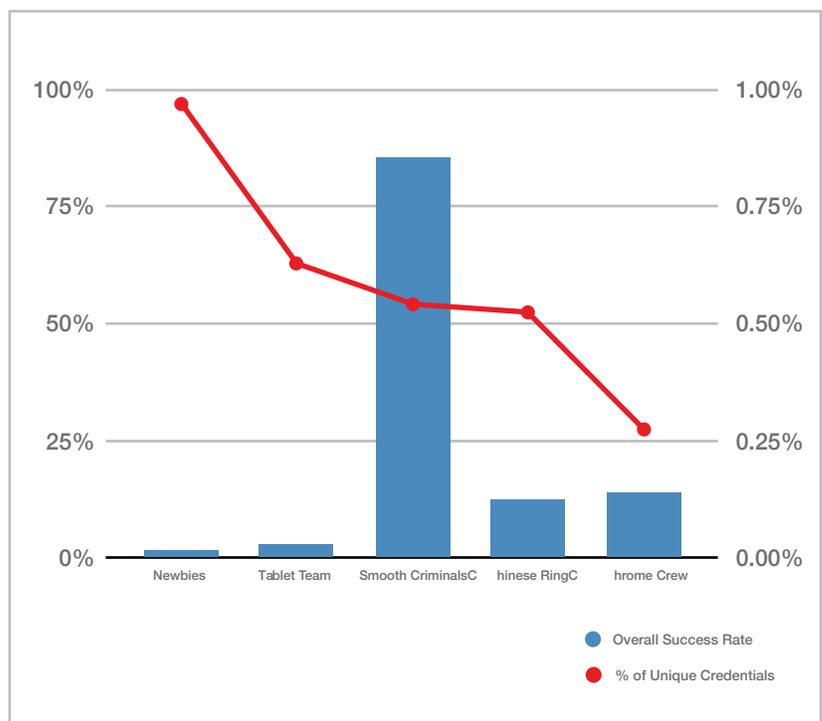
Figure 10: Comparison of Attackers' Credential Lists and Login Success Rates

[9] Consumers tend to be more careful about reusing passwords for their banking accounts, so if the Newbies were using credentials stolen from other types of services (such as web forums or gaming sites), they likely had a lower match rate.

The Steps to a Credential Stuffing Attack

Ultimately, all credentials that are spilled will be used to fuel credential stuffing attacks against other organizations. There are many ways for an attacker to carry out a credential stuffing campaign; the exact method will depend on the attacker's skill level.

**The Method of Credential Stuffing Depends on an Attacker's Skill Level**

Advanced Attacker	Acquire Credentials	Develop Attack	Test Attack	Distribute Attack	Take Over Accounts
Script Kiddie	Acquire Credentials	Choose Attack Tool		Distribute Attack	Take Over Accounts
Faudster N00b	Acquire Credentials	Choose Account Checker Service			Take Over Accounts
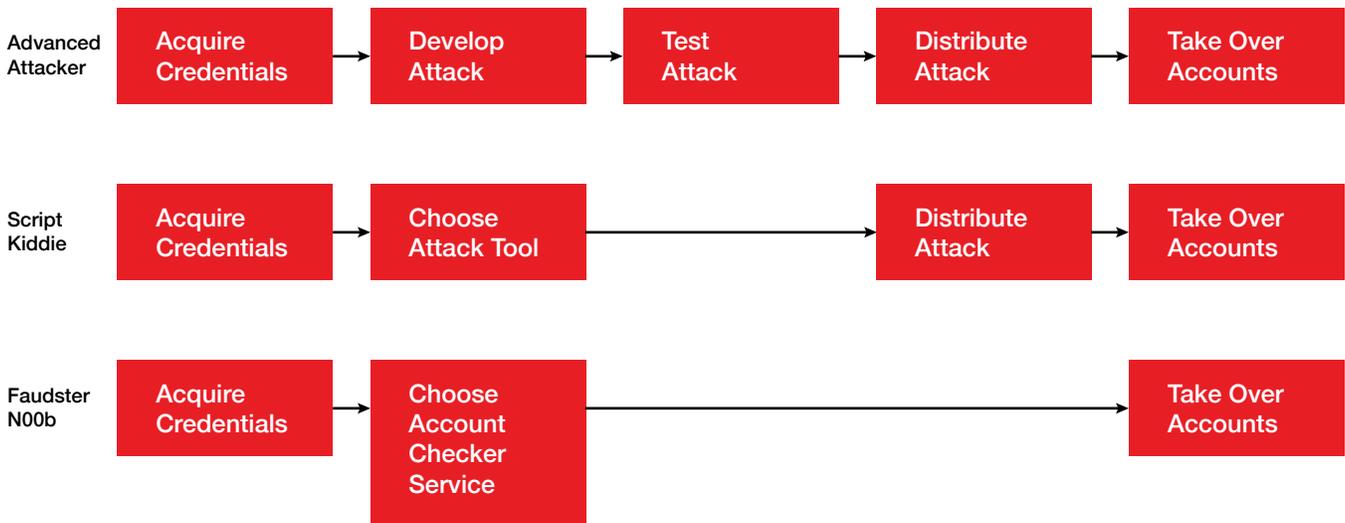
Figure 11: Credential Stuffing Methods Based on Skill Level

Advanced Attacker

If fairly sophisticated, an attacker will write his own attack script or even develop his own tool that he may share with his network. While this may be a more time-consuming task, the benefit of a custom script is that it can be made more difficult to detect than a cookie-cutter tool like SentryMBA, which is fairly easy to detect.

Script Kiddie

If the attacker has less experience or specializes in the monetization of account takeover, as opposed to the credential stuffing attack itself, he may opt for a pre-configured tool. This method still requires an attacker to disguise their traffic via proxies, so the attacker must still understand the basics of networking and HTTP.

Fraudster N00b

Lastly, even a criminal who doesn't understand the difference between a GET and a POST[10] can still defraud a Fortune 500 company of millions of dollars by using an account checker service. Technically-skilled criminals have developed these white-glove services to enable their less adept brethren to enter the cybercriminal industry.

Below we go into detail on individual steps:

---

[10] GET requests are repeatable in order to retrieve the same information (e.g. a web search, a product page). POSTs initiate a one-time action on the server side (e.g. a login, a purchase, an image upload).

SH=PE
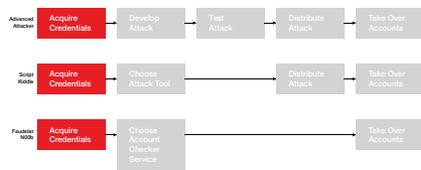
Acquire Credentials

As discussed in the "Life Cycle of Stolen Credentials," attackers may steal credentials themselves, acquire them from another attacker in their network, or purchase them via a dark web marketplace or forum.

Marketplace vs. Forum

While marketplaces and forums are both used to trade goods, services, and knowledge on the dark web, they each have slightly different use cases. A marketplace is a more legitimate channel, so, to participate, sellers must have already built a reputation. Forums will allow anyone to post goods, but the transfer of money is not as clean as in a marketplace. Forum owners engage in the practice of "escrow," requiring both buyer and seller to wire funds matching the desired price of goods to the forum owners as a guarantee. Once the seller provides the buyer with the goods, the forum owner will transfer the escrow funds to the seller, less a commission, which is usually a higher percentage than one would find on marketplaces. Marketplaces are fairly public, however, so many sophisticated criminals frequent specialized forums that are only open to the dark web elite.

The cost of credentials can range anywhere from free to tens of dollars, depending on source, freshness, and an attacker's reputation. Because there are so many credentials available to potential buyers, sellers compete with one another not only on price, but also on the integrity of the credentials being traded. For example, during a two-week observation period of dark web marketplace PaySell, Shape found that certain sellers verified a subset of their posted financial credentials every 24 hours. By doing so, their listings rose to the top of the page everyday as the "freshest" accounts available.
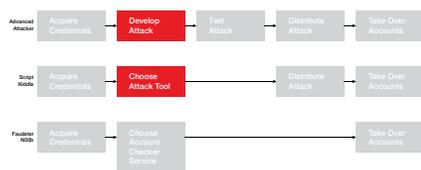
Develop or Decide on an Attack Toolkit

Attackers of all skill levels may leverage toolkits in their attack. Examples of toolkits include "bruters," which are generalized software to perform credential stuffing attacks, and "checkers," which can be added to the end of a script to automatically provide information about valid accounts, such as account balances, gift card balances, associated credit cards, etc.

Just like credentials, toolkits also have a life cycle that affects their price and availability:

Even Criminals Have a Sense of Community:

On the forum Hack-Tool.org, a developer posted a credential stuffing toolkit. A savvy forum member asked the developer to provide evidence that the toolkit was malware-free, which the developer dutifully provided. All appeared well until another forum member down thread realized that the developer had posted the VirusTotal[11] results from a *different* piece of software. This good Dark samaritan then shared the true VirusTotal assessment of the posted toolkit, revealing malware-ridden software.

Life Cycle of a Toolkit

1. Developer posts toolkit offering on specialized forums. In some cases, the seller limits the number of copies of the software so he can: a) ensure that he can offer customer support to the buyers, and/or b) lower the likelihood that the software will be detected and blocked by an easy signal, such as browser fingerprint or user agent.

2. After the first round of buyers extract the maximum value from the toolkit, i.e., they have exhausted their databases of stolen credentials, the developer re-sells the software on a second market via re-registration.

3. At the end of the life cycle, when the toolkit is almost completely useless software, a criminal may try to use it for phishing or other exploits against other criminals by injecting the software with malware and then redistributing it on forums and marketplaces for script kiddies to unwittingly download.
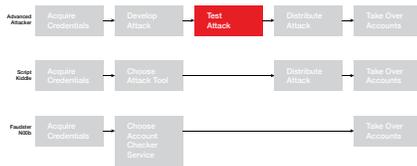
Test the Attack

Before expending resources on a full-blown credential stuffing campaign, an attacker will want to first test their software on the target site. Attackers often use fake accounts that they created on the target site earlier to check if their attack method works. If the fake account credentials yield an "unsuccessful login" message, the attacker will know the script isn't properly evading anti-automation defenses.

Attackers also advance in their ability to conduct reconnaissance of an application's anti-automation defenses. An inexperienced attacker may have no idea why a credential stuffing script doesn't work on a target site. If determined and slightly skilled, the attacker may attempt fuzzing, the technical term for trial and error or tweaking the script until stumbling onto something that works. If fuzzing brings no luck, an advanced attacker may reverse engineer any JavaScript involved in detecting the automation. If the attacker succeeds, he will be able to incorporate that knowledge into his own automation, creating new payloads that fool the JavaScript detection mechanism.
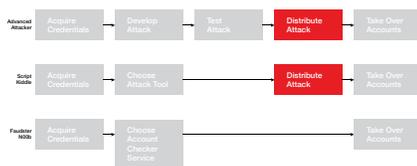
Distribute the Attack

Attackers route their traffic through proxy servers in order to avoid detection. There are three main ways criminals access proxy servers. The most common way is to find free, open proxy servers, which are just a Google search away. The downside is that these servers are overused so they are likely to be slow and already blacklisted by the target enterprises.

---

[11] VirusTotal is a website designed for security professionals that checks submitted files and URLs for viruses.

The second most common way to access proxy servers is to pay up. There are multiple sites that sell access to proxy servers that were originally developed for people in countries that impose internet restrictions on citizens. Unfortunately, attackers will often abuse these services to such an extent that many enterprises have blocked access from those servers.

The next level of sophistication is to visit a dark web marketplace in search of sellers who offer access to their own proxy servers. These proxy servers that are for sale are a byproduct of another criminal industry, botnets.

No matter what method of proxying traffic an attacker chooses, it will be cheap (<$50) and allow the attacker to launch attacks from countless IP addresses.
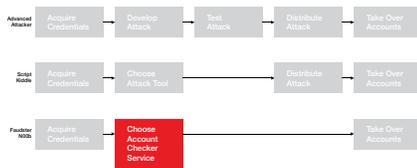
Account Checker Services

An account checker can be thought of as credential stuffing-as-a-service. An attacker provides a list of compromised credentials, and then the software will perform the credential stuffing attack itself, returning the attacker with a list of validated credentials. The attacker is only charged for each "success" at a rate of about 2 cents per validated credential.

Account checker services are custom-made to target a single organization, so they tend to only exist for sites which have hundreds of millions of accounts. Many of these account checker services are accessible on the clear web and can be found by searching for "Target Company" and "account checker." Developers will also sometimes publish tutorials or video demos to promote their attack service. Figure 12 is an example of a demo found on YouTube advertising a criminal's account checker service for a financial institution.
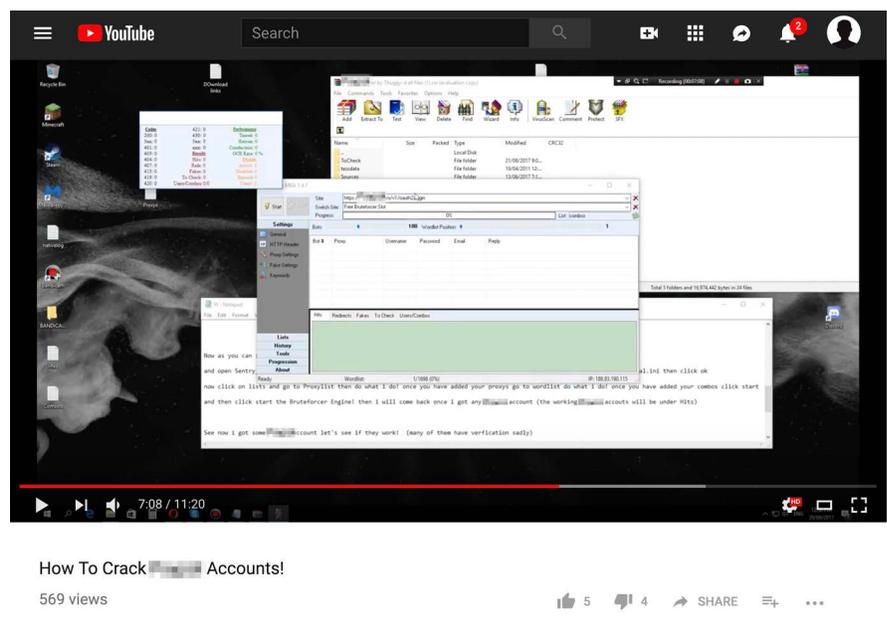
Figure 12: Account Checker Service Demo on YouTube
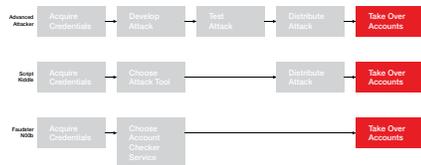
Take Over Accounts

Once an attacker establishes valid credentials, they will typically do one of four things:

1. Steal the stored value or abuse the stored credit card information.

2. Exploit the personally identifiable information within the account

3. Leverage the positive reputation associated with the account to commit another type of fraud, e.g., apply for credit cards in the victim's name.

4. Sell the list of valid credentials for another criminal to leverage. One of the ways the secondary criminal may monetize the original credential spill is by performing credential stuffing attacks, and then reselling the subset of credentials that were valid for each site. That's likely the case for a Playstation credential listing on a dark web marketplace posted in March 2017.[12] The attacker acknowledged that the credentials were not stolen directly from a Playstation database and only had a relatively small subset of accounts (640,000) compared to the overall number of Playstation users (over 100 million).

Which monetization scheme an attacker chooses depends on the attacker's specialty as well as the type of organization that was attacked. We discuss how each monetization scheme plays out in particular industries in the next chapter.

---

[12] https://www.hackread.com/640000-decrypted-playstation-accounts-sold-darkweb/

Credential Stuffing Threat by Industry

Proportion of Login Traffic that is Credential Stuffing Attacks by Industry (Global)
Averages derived from customers' login traffic before Shape Enterprise Defense was deployed on login applications.
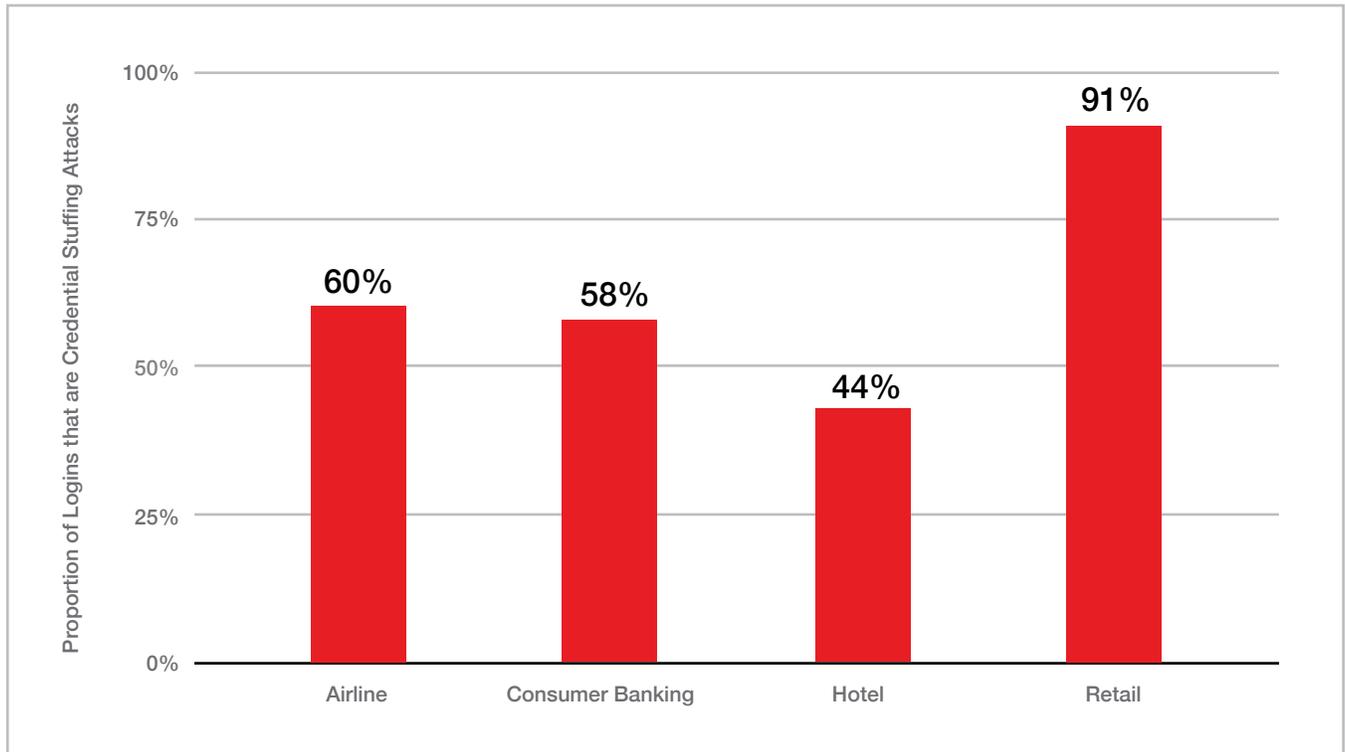
Figure 13: Credential Stuffing as a Proportion of Login Traffic by Industry (Global)

Of four of the most prominent industries targeted by credential stuffing attacks, retail has the highest proportion of traffic that is fraudulent.

Where does this data come from?

In this chapter, we rely on data from the Shape Network. Across the US, Shape's customers represent:

59%
of the Airline Industry
(by revenue passenger miles)

15%
of the Hotel Industry
(by revenue)

41%
of the Consumer Banking Industry
(by assets)

40%
of Mobile Retail
(by in-store payments)

Number of Credential Stuffing Attacks Per Day in US by Industry

Figure 14: Daily Volume of Credential Stuffing Attacks by Industry (US)
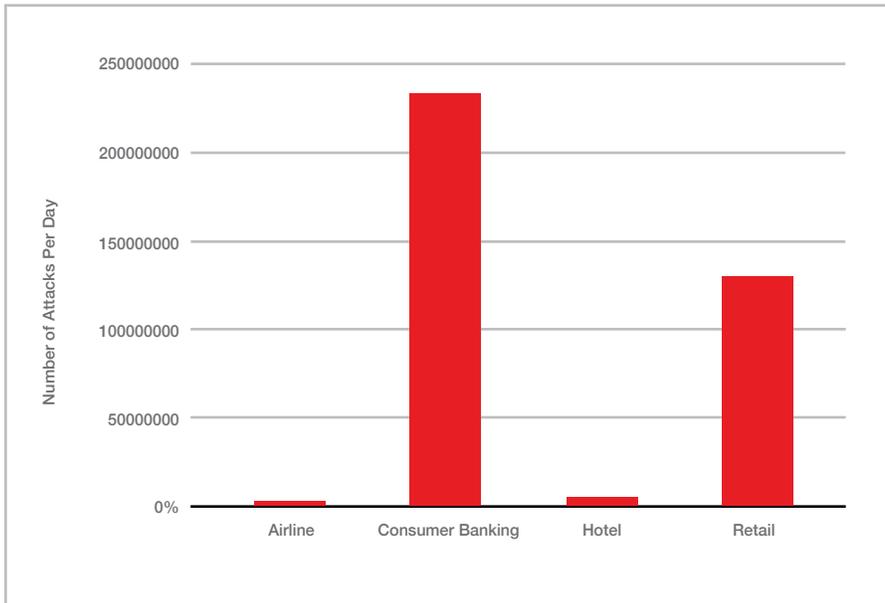
We estimated the number of credential stuffing attacks using the total number of credential stuffing attacks observed on Shape's US customers and the total proportion of the US industry our customers represent.

The discrepancies between proportion of traffic (Figure 13) and attack volume (Figure 14) are due to differences in login frequency for normal, good users. For example, a typical online banking customer may log in to their banking mobile app a few times per week. Yet an airline's frequent flyer customer may only log in to their own account a few times a year.

Using the analysis above, we estimated the daily cost of credential stuffing for the four industries as follows in terms of losses from account takeover and resulting fraud:

Table 2: Total Cost of Credential Stuffing Per Day by Industry (in millions)

	Consumer Banking	Hotel	Airline	Retail
Potential Losses from Credential Stuffing (per day)	$46.4	$4.3	$3.6	$32.9
Actual Losses from Credential Stuffing (per day)	$4.6	$1.1	$0.9	$16.5
Actual Losses Per Year	$1,700	$400	$300	$6,000

Below we will explore the threat of credential stuffing for individual industries to discuss how credential stuffing transpires, unique insights, and ways in which attackers cash out after taking over accounts.

Retail

Retailers face relentless credential stuffing attacks, typically comprising **80-90 percent of their traffic**. In fact, one luxury retailer experienced 99 percent attack traffic on their login page in 2017. Credential stuffing against retail web properties is very lucrative for cybercriminals for two key reasons.

First, retail websites are designed to cause as little friction as possible for customers. Due to the emphasis on user experience, retailers are reluctant to impose any security measure that could lead a customer to abandon their cart, whether it be two-factor authentication or email confirmations required for account changes.

Second, credential stuffing attackers have benefited from the rise in omnichannel services. One of the biggest opportunities for fraud is the gap between online and offline retail created by omnichannel services. Fraudsters can use hijacked online accounts to more easily monetize previously stolen merchandise from physical storefronts, as well as purchase merchandise online which they then monetize in stores.

Table 3: Cost of Credential Stuffing in Retail

TOTAL COST OF CREDENTIAL STUFFING PER DAY	**$16,450,000**	A3*B*C
TOTAL COST PER MONTH	$493,500,000	
TOTAL COST PER YEAR	$6,004,250,000	
A1) Total number of attacks per day across US Industry	131,455,382	The average number of malicious login attempts per day
A2) Average Credential Stuffing Success Rate	0.50%	The proportion of credential stuffing attacks that result in a successful login, i.e., the attacker used credentials that were valid on the target site.
A3) Average # of ATOs (Account Takeovers) Per Day	657,277	A1*A2
B) Average Cost of Fraudulently Purchased Merchandise	$50	There are a number of ways for fraudsters to monetize a retail ATO. For this analysis, we assumed that the fraudster used stored value in the account to fraudulently purchase merchandise.
C) Percentage of Fraud Success	50%	The estimated proportion of fraudulent purchases that are not detected by internal fraud resources. Third party research finds that typical fraud success rates range between 20% to 67%

Monetization of Credential Stuffing

Ultimately, in almost all scenarios, an attacker wants to obtain merchandise that can be resold or used to commit return fraud. To purchase goods, a cybercriminal needs a hijacked retail account to contain a form of currency, e.g., a credit card on file, a balance from a previous return of goods, or a deposited gift card. Once the criminal obtains the goods, they will resell the merchandise to either unsuspecting consumers on third-party marketplaces or other wrongdoers on the dark web.

In the age of Amazon, customers expect absolute convenience from their retailers. Unfortunately, each act of convenience to customers has been an act of convenience for criminals, allowing them to more easily monetize account takeovers.

The Underground Cheese Market

The majority of credential stuffing and account takeover attacks are conducted by professional criminal rings that are financially motivated. These criminal organizations purchase and traffic goods for which there is consistent, high demand. We have mentioned that retail gift cards and electronics are always safe bets. Another product that has become a go-to for credential stuffers: cheese.

The restaurant industry has notoriously low profit margins, so owners and chefs are always on the lookout for good deals on expensive ingredients. Fancy cheeses are a staple across many cuisines but can be pricey - Wyke Farms Cheddar retails for about $200 per pound. Criminals have caught on and are targeting grocery chains with credential stuffing attacks. After taking over customers' accounts, they will load up their shopping carts with wheels of Jersey Blue, which they then resell on the grey market.

Mobile In-Store Payments

Many retailers have developed, or are in the process of developing, their own mobile apps with a payment function to enable a faster check-out experience in physical stores. All types of retailers, from CVS to Kohls to Chipotle, already allow customers to pay in-store with just a tap or swipe of their phone. Consequently, if an attacker takes over a customer's account for one of those companies, they can log in to the victim's account on their mobile phone and then go on an in-person shopping spree. Purchasing items in stores allows attackers to obtain physical items immediately and with low-risk, as opposed to the shipping time and higher risk associated with online purchases.

Buy Online, Pick Up in Store (BOPIS)

If an attacker wants to make a physical purchase, a BOPIS channel is another good option. BOPIS allows a fraudster to take over a victim's account, make a purchase, and then, instead of shipping the item, choose "pick up in store." This retail channel is a fraudster's dream because there is a fast turnaround time between the transaction, often just a few hours. While the store associate is typically supposed to prevent fraud by requesting identification during pick-up, oftentimes an attacker can just flash the barcode on the receipt and be given the merchandise. Depending on the checkout flow, the attacker may need to first change the email address associated with the account before placing the order, so that he receives the pick-up receipt with the barcode.

Add New Payment Method

Sometimes we see attackers taking over accounts to test and use credit cards stolen from elsewhere. The advantage to taking over accounts (as opposed to creating fake accounts) is the attacker can leverage good behavior history associated with the hijacked account, so the transaction is more likely to go through.

Return Without a Receipt

This scheme involves purchasing items online using a victim's account and then returning the items in-store, leveraging retailers' generous "no receipt required" return policies.

Intermediaries

To monetize account takeovers from the comfort of their own home, many attackers purchase digital assets such as e-gift cards or video games that are available immediately. The attacker then does not need to worry about the fraud being discovered, as they receive the product instantly, which they can then resell.

However, some criminal rings specialize in the purchase and resale of specific items, such as luxury handbags. In these cases, a network of intermediaries may be used to help disguise the fraud. For example, a "remailer" may be used when ordering products online from hijacked accounts. A remailer receives fraudulently-purchased goods and then re-ships them to the attacker for a small fee, making it more difficult for the retailer to follow the money trail.

Airlines

Airlines are popular targets for credential stuffing. Frequent flyer miles are highly monetizable and valuable assets that are often not protected with the sophisticated security measures of financial services. A typical consumer is an infrequent traveler who logs into his/her frequent flyer account far less often than he/she logs in to other online accounts. Due to this infrequency, it often takes much longer for an airline customer to discover theft from account takeover, than, say, a banking customer.

Sixty-percent to 65 percent of logins against airlines are credential stuffing attacks when typical username/ password credentials are required for authentication. Some airlines employ a unique customer number that can lower the number of credential stuffing attacks. However, this unique ID introduces customer friction by requiring users to remember a username just for that site.

The reason the cost of credential stuffing is relatively low compared to other industries is that there are far fewer airlines than retailers, banks, or even hotel chains in the US. One top 5 US airline executive reported to Shape that **$7 million** is spent each year reinstating stolen miles alone. So, per company, airlines suffer significantly from credential stuffing.

Table 4: Cost of Credential Stuffing for Airline Industry

TOTAL COST OF CREDENTIAL STUFFING PER DAY	**$900,000**	**A3*B*C**
TOTAL COST PER MONTH	$27,000,000	
TOTAL COST PER YEAR	$328,500,000	
A1) Total number of attacks per day across US Industry	1,437,645	The average number of malicious login attempts per day
A2) Average Success Rate	1.0%	The proportion of credential stuffing attacks that result in a successful login, i.e., the attacker used credentials that were valid on the target site.
A3) Average # of ATOs Per Day	**14,376**	**A1*A2**
B) Average Amount of Stored Value	$250	Based off of third-party estimates of total number of frequent flyer accounts and unused miles.
C) Percentage of Fraud Success	25%	The estimated proportion of fraudulent purchases that are not detected by internal fraud resources.

Monetization of Credential Stuffing

The theft and sale of miles is very different from the theft and sale of gift cards. The span between when an account is compromised and when the assets in the account are monetized is a key factor to an attacker. Attackers want this time frame to be as short as possible.

Miles are difficult to monetize quickly on an individual scale due to the specificity of the sale and the time it could take to find an appropriate buyer. Thus, credential stuffing in the airline and other travel industries has fueled the grey market of mileage brokers.

Attackers want to shorten this time span as much as possible

Figure 15: Credential Stuffing Steps Including Monetization
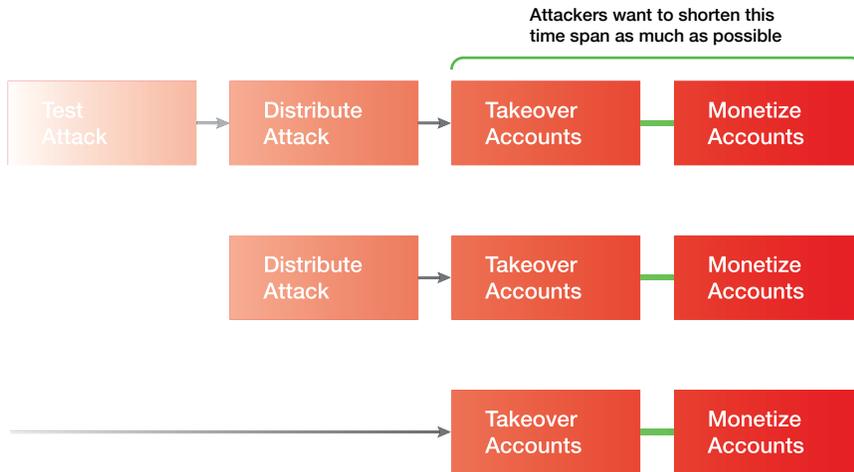
Mileage brokers are individuals or companies that specialize in buying airline miles, hotel points and other award program points. This activity of selling award program points is not illegal, but is often strictly prohibited by the service provider's term of service. Suspicion or discovery of a sale of award program points can result in an audit, cancellation of a ticket, or even the revoking of an account. This is a rather risky offering for a legitimate consumer, but not a problem for an attacker who is looking for a quick way to get paid with little regard for the future validity of the account.

The credential stuffing attacker sells the miles to a broker by providing the broker the account credentials. The broker logs in, confirms the account has miles, and then pays the attacker, often via PayPal. Rates vary depending on the broker and the number and type of miles being sold. One organization, The Miles Broker, claims on its website to pay up to 1.5 cents per mile. The attacker has now "cashed out," but the miles typically remain in the victim's account until the broker needs to use them, as that shortens the window of time in which the fraud can be detected.

The broker monetizes purchased miles in one of two ways. First, the broker may create a two-way marketplace, selling back those miles to everyday consumers looking for a deal. The second more common option is for the mileage broker to act as or in partnership with another grey market group - discount travel agencies. These travel agencies specialize in selling first class and business class airfare at up to a 70 percent discount.
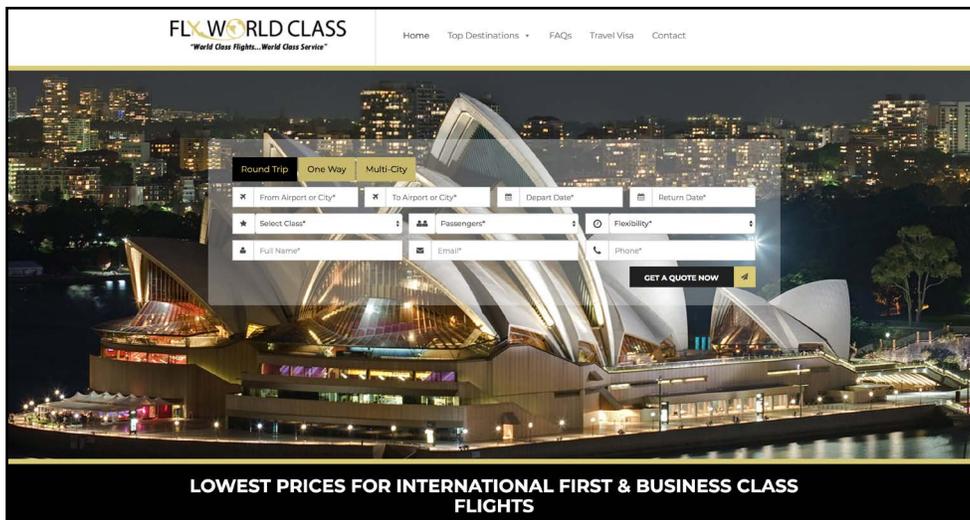
Figure 16: Homepage of discounted travel agency "Fly World Class"

While the agencies do not specify how they get such discounted rates, Shape has reason to suspect that they purchase miles from the brokers (or are co-operated by mileage brokers) and use those miles to secure airfare. Having this two-step process in the supply chain (first mileage brokers then discounted travel agencies) would create a smokescreen, making it more difficult for an airline to prove fraud.

Hotels

Just like airlines, hotel chains offer client accounts with loyalty points and consolidated reservations.

An estimated 82 percent of login requests for the hotel and hospitality industry can be attributed to credential stuffing. These high rates are due to the attractiveness of loyalty points to criminals as well as the fact that most customers do not log in to their hotel loyalty account as often as they would other online accounts. Therefore, most daily login traffic is from attackers.

Example of a Credential Stuffing Attack Against a Hotel

Attack Volume Grew to **15X** Normal Customer Traffic

Figure 17: Credential Stuffing Attack Against a Hotel
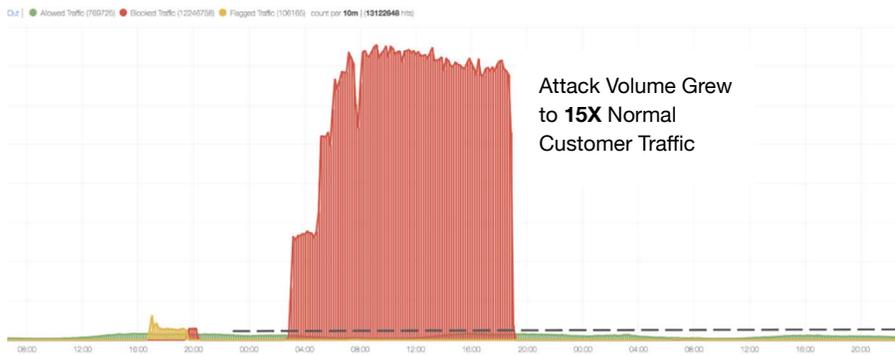
Figure 17 shows an example of a large-scale credential stuffing attack against a Top 3 Hotel that took place over 16+ hours. The attack is attempting to take over guest accounts to withdraw loyalty points. Human traffic is in green (1000 requests/min). Automated traffic is in red and was blocked by Shape (15,000 requests per minute).

In recent years, in order to provide better experiences to customers and to stand out in a competitive market, more hotels are offering mobile apps for elevated experiences such as skipping check-in lines, instant room reservation, the addition of a payment method for room charges, and the utilization of phones as room keys. These mobile apps have significantly increased the credential stuffing attack surface.

Table 5: Cost of Credential Stuffing for Hotel Industry

TOTAL COST OF CREDENTIAL STUFFING PER DAY	**$1,075,000**	**A3*B*C**
TOTAL COST PER MONTH	$32,250,000	
TOTAL COST PER YEAR	$392,375,000	
A1) Total number of attacks per day across US Industry	4,290,260	The average number of malicious login attempts per day
A2) Average Success Rate	1.0%	The proportion of credential stuffing attacks that result in a successful login, i.e., the attacker used credentials that were valid on the target site.
A3) Average # of ATOs Per Day	42,903	**A1*A2**
A4) Average Stored Value in an Account	$100	Assuming the average hotel loyalty account holds 10,000 points and 1 point is worth 1
C) Percentage of Fraud Success	25%	The estimated proportion of fraudulent purchases that are not detected by internal fraud resources.

The above model estimates hard costs for a hotel, but brand loyalty is critical in a competitive market and loyalty point fraud directly impacts performance and revenue of a hotel. Customers who participate in loyalty programs and engage via mobile apps or online accounts are typically the most loyal and high-spending visitors. So if one of those customers has his accounts compromised, the hotel may lose that customer permanently, resulting in substantial revenue loss over the long run.

Monetization of Credential Stuffing

There are three key ways that attackers can monetize hotel loyalty accounts:

1. **Redeem points for non-hotel goods**
   Attackers make use of a hotel's reward redemption options to convert stolen points into goods offered by the hotel's partners. This is one of the lowest-risk options as many of the goods purchased are available immediately, such as e-gift cards.

2. **Sell points to a mileage broker**
   Mileage brokers (as discussed in the Airline section) also accept hotel loyalty points, so the process for selling is nearly identical to selling airline miles.
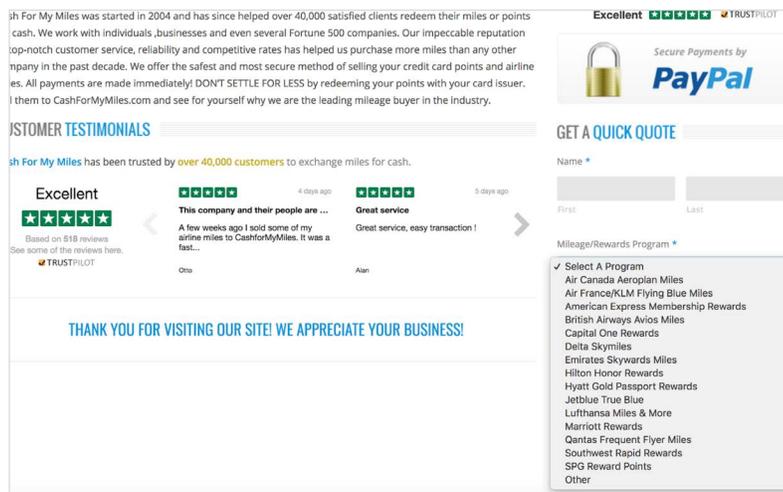
Cash For My Miles, which is one of the most heavily advertised mileage brokers, readily accepts Hilton Honor Rewards, Marriott Rewards and SPG Reward Points and accepts other hotel loyalty points on a case by case basis.

Figure 18: Mileage Broker "Cash For My Miles"

3. **Redeem points for hotel stay**
   We discussed earlier that it was difficult for attackers to redeem airline miles for flights on an individual basis as the fraud was easily tracked. Up until recently, the same challenge existed for monetizing hotel reward points; however, two recent innovations have made it easier to monetize individual account takeovers: mobile check-in and digital room keys.

   Earlier, the issue was that if an attacker made a reservation using a hijacked account, they would have to still check-in at the front desk, which requires presenting identification. So a fraudster would have to risk using their own name or present fraudulent identification. With the introduction of digital check-in, attackers can now takeover the account, book the room under the victim's name, check in online, and use their mobile app as their digital room key, all without having to interact with any hotel staff or present identification.

   Many hotel apps do not send email notifications when actions like digital check-in are taken, reducing the risk for the fraudster. At most, the fraudster may need to change notification settings after taking over a victim's account, so that the true account owner is not alerted of activity.

   Shape has not yet received direct reports of this type of fraud occurring, but as more hotel chains continue to enable digital room keys across their properties, their mobile apps may become a target.

Consumer Banking

As one might imagine, online banking applications are the most lucrative target for cybercriminals. The median US savings or checking account holds between $3,000-$5,000, which is substantially higher than a typical rewards account. Because banks are such attractive targets, Shape has observed attackers taking extreme measures to bypass banks' application defenses.

Exploitation of Aggregators for Credential Stuffing
Financial aggregators are companies like Intuit, Yodlee and Plaid that allow users to have a consolidated view of their finances. The aggregator receives users' login credentials for multiple financial services providers and logs in to various accounts on the users' behalf to give them a single view of all the data on the aggregator's platform.

Aggregators have trusted relationships with financial institutions and are usually whitelisted. This means that traffic coming from aggregators is not as heavily scrutinized and bypasses typical anti-automation control. Criminals have become aware of this loophole and have started exploiting the relationship to perform credential stuffing attacks.

The attacker, instead of going directly to the financial institution's website to test credentials, goes to the aggregator's website and signs up for accounts using the stolen credentials. The aggregator then attempts to log in to the financial institution's website using those credentials. The aggregator then will provide the attacker feedback as to whether those credentials were valid or not. At the end of this third-party credential stuffing attack, an attacker will have a list of validated banking credentials that can be used for manual account takeover on the banking site.

Key Indicator of a Credential Stuffing Attack is a Change in Login Success Rate
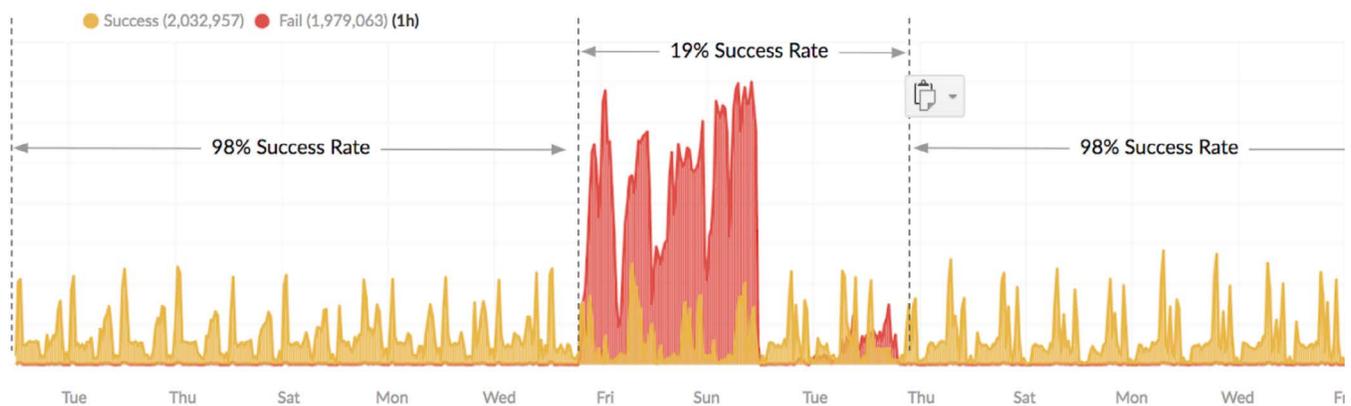
Figure 19: Credential Stuffing Attack on a Bank via a Financial Aggregator

Figure 19 above shows an example of one such attack leveraging a banking aggregator. The graph shows four weeks of aggregator traffic split into successful logins (yellow) and failed logins (red).

During a five-day period in April, the aggregator was exploited by a bad actor to perform credential stuffing. The spike in failed logins around that period is evidence of this crime. Over that time period, the average sign in success rate was 19 percent, which is much lower than the aggregator's usual 98 percent sign in success rate. Another indicator of a credential stuffing attack is the accounts accessed by an aggregator. Aggregators usually sign into the same known accounts over and over, i.e., their customer base. However, during that five-day period, 69 percent of this aggregator's attempted logins were to accounts it had never before accessed.

Bypassing 2FA via Credential Stuffing on Telecom Companies

One of the key ways banks have attempted to combat credential stuffing and account takeover is through the rollout of multi-factor authentication (MFA). Most banking customers that choose to enable 2-factor authentication use their mobile device as the second authentication mechanism.

While many believe this would stymie credential stuffing attackers, Shape has seen evidence of attackers targeting **cell phone carriers'** login applications in order to bypass banking security. If an attacker has successfully broken into a customer's mobile account, then the attacker can circumvent 2-factor authentication, taking over the victim's bank account.

After performing a credential stuffing attack on a cell phone carrier's website, an attacker will have access to victims' account details. The attacker can then call customer service, impersonate the victim, and ask for a new SIM card to be associated with the phone number attached to the account.

The attacker will then be able to intercept all phone and SMS-based communication directed at the victim's phone number, including codes sent for authentication purposes.

For this reason, and other fraud schemes involving telecom account takeover, one telecom customer faced **nearly 7 million credential stuffing attacks per day.**

Credential Stuffing Attackers Target Telecom in Order to Bypass 2FA
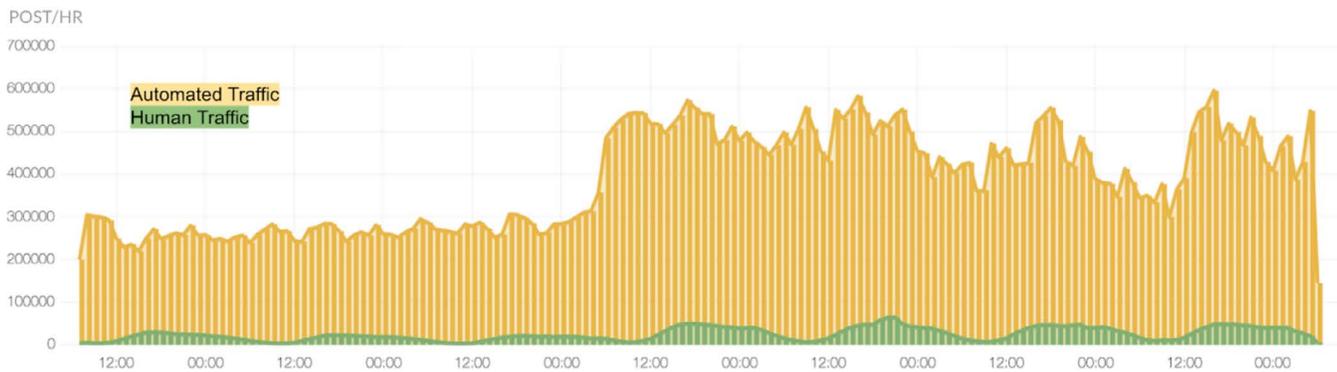
Figure 20: A Top 3 Telecom Company's Login Traffic

Manual Methods Once Automation is Blocked

Shape has observed extremely persistent attackers resort to manual methods after a bank has deployed comprehensive anti-automation defenses. Attackers scale manual credential stuffing by employing an army of people in geographies with low labor costs. These "employees" can be thought of as a credential stuffing equivalent to click farm workers - they are given a list of username and password combinations which they copy and paste into given login applications, recording which credentials result in successful logins.

● Failed login

● Successful login

Note, the actual rate of the manual credential stuffing campaign is extremely low, averaging about 10 attempts per hour. However, because all automated credential stuffing attacks had been blocked, Shape was able to identify even this low-volume manual attack.
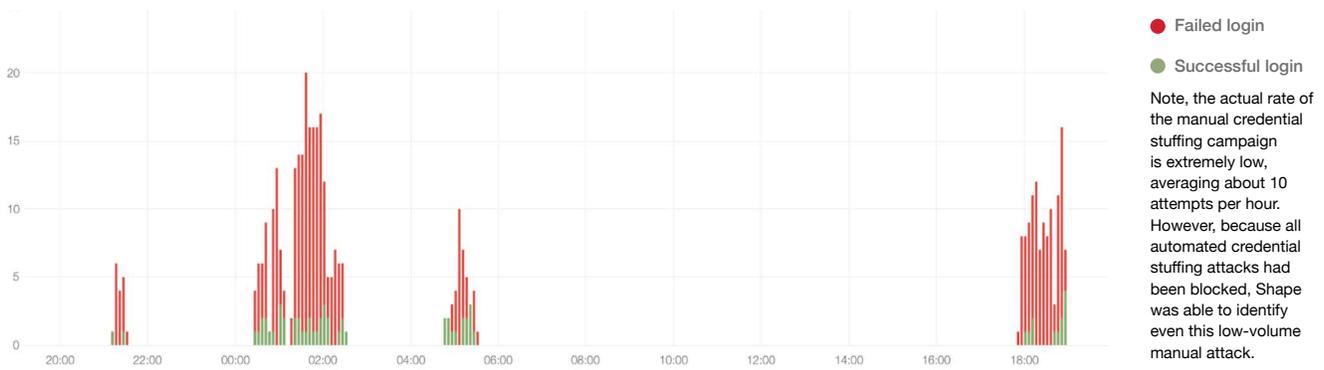
Figure 21: Manual Credential Stuffing Attack on a Top 5 US Bank

Table 6: Cost of Credential Stuffing for Consumer Banking Industry

|		
TOTAL COST OF CREDENTIAL STUFFING PER DAY	**$4,640,000**	**A3*B*C**
TOTAL COST PER MONTH	$139,200,000	
TOTAL COST PER YEAR	$1,693,600,000	
A1) Total number of attacks per day across US Industry	232,212,683	The average number of malicious login attempts per day
A2) Average Credential Stuffing Success Rate	0.05%	The proportion of credential stuffing attacks that result in a successful login, i.e., the attacker used credentials that were valid on the target site.
A3) Average # of ATOs Per Day	116,106	**A1*A2**
B) Average Amount Stolen from an Account	$400	The median US bank account holds between $3000-$5000. We assumed an attacker may take 10% (or $400).
C) Percentage of Fraud Success	10%	The estimated proportion of fraudulent purchases that are not detected by internal fraud resources. Banks tend to have more fraud resources and procedures than other industries, so they are likely to prevent more ATO fraud.

Monetization of Credential Stuffing

Figure 22 summarizes the methods by which an attacker can monetize a bank account once it is taken over. The vertical axis is the amount of value the attacker is able to extract and the horizontal axis is the level of risk and difficulty associated with that monetization method.

1. **Sell Personally Identifiable Information (PII):** This is the most basic level of monetization. The attacker harvests personally identifiable information (PII) such as names, date of birth, phone numbers, etc. This information has market value and can be aggregated into fullz (fraudster term for a "full identity") that are used for identity theft and more sophisticated fraud. The market value of a single fullz record is between $30-$100.

2. **Buy goods and services:** The attacker uses the hijacked account to make purchases. The most commonly purchased items using these accounts are high-value, portable, and easy to sell, such as smartphones, gift cards and luxury watches.
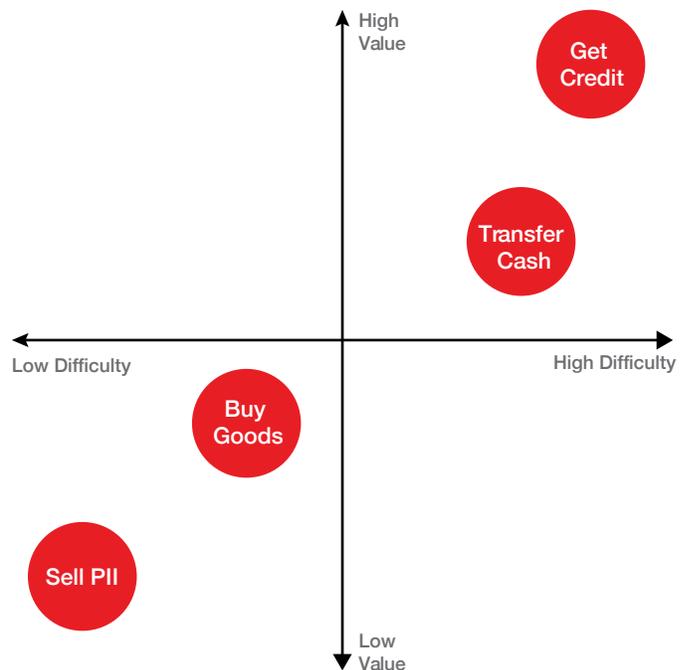

Figure 22: Banking Monetization Schemes Plotted by Difficulty and Value to Attacker

The problem with this type of scheme is that the fraudster usually cannot get the full value of the item that they purchased. They usually have to try and resell the item at a discount. To get around this, some attackers create a fake merchant account on a marketplace like Upwork or eBay. They then use the hijacked financial account to pay for fake contract work on Upwork or make purchases from the eBay storefront.

3. **Transfer Cash:** At the end of the day, fraudsters want cold, hard cash. Direct transfers from a hijacked account to an account the attacker controls are risky because the money can be traced directly back to the attacker. To avoid detection, credential stuffing attackers employ various tactics, including:
   - Digital currencies - This allows the fraudster to buy quasi-anonymous digital currencies like Bitcoin off an exchange using an accomplice, a victim account or anonymous crypto-exchanges like Coinchimp. Once the transaction is processed there is no way to recover the money or to track who received the money.
   - Peer-to-peer payment apps like PayPal, Zelle, and Venmo - The attacker can use these apps to send money from one account to another, making it difficult to trace the money. These peer-to-peer payment apps usually only require a phone number or an email address to send cash. Attackers can therefore open multiple accounts and use them to obfuscate their identity and the destination of the stolen cash.

4. **Get Credit**: Unlike transferring cash from a stolen account, which is limited only to the funds available in the account, the ability to apply for credit using the hijacked account will give the fraudster access to even more money. Though the potential payout is large, the complexity and risk involved is much higher. The fraudster will use the stolen PII in conjunction with other compromised information available to apply for credit from another financial institution. It is uncommon for the fraudster to try and apply for credit from the same bank or institution where they hijacked the account. This is because the fraudster will need to supply different contact information and physical address for the delivery of the card to what is already in the bank's database and this may draw unnecessary attention to the fraudster's credit application.

Regulators & Standard Bearers Addressing Credential Stuffing

With the increased frequency of spilled credentials and successful account takeover attacks, regulatory, compliance, and industry standards groups are starting to recognize this impact and provide guidance paving the roadmap for future requirements and solutions against this problem. Four key organizations have taken measures since the 2017 Credential Spill Report that, in part, addressed the issues of credential spills and credential stuffing.

NIST: Government Agencies Should Reduce Rate of Success of Credential Stuffing

The National Institute of Standards and Technology (NIST) published new digital identity guidelines (SP 800-63) in June 2017, focusing on the security of authentication processes in volume 63B, Digital Identity Guidelines: Authentication and Lifecycle Management. In this volume, NIST advised organizations that, when allowing users to create a new password, they should "compare the prospective secrets [passwords] against a list that contains values known to be commonly-used, expected, or compromised." In this way, agencies can prevent the likely success of credential stuffing. All US federal agencies were directed to comply with NIST's guidelines by June 2018.[13]

While NIST's guidelines are written primarily for US government agencies, the organization is well respected within the security community, and many private sector organizations adopt NIST standards as guidance or best practices.

FTC: Financial Institutions Must Adequately Prevent Credential Stuffing Attacks

In August 2017, the Federal Trade Commission (FTC) brought its first-ever enforcement case regarding credential stuffing when it investigated TaxSlayer LLC, a tax preparation company. TaxSlayer offers consumers tax preparation and filing services that are both web-based and available through the company's app. For a two-month period in 2015, TaxSlayer was subject to a credential stuffing attack, which allowed remote attackers to access the accounts for about 8,800 TaxSlayer users.

In the FTC's view, companies holding sensitive consumer information should be safeguarding the data from internal and external threats. The FTC complaint stated that TaxSlayer violated the Privacy Rule and Reg P under the Gramm-Leach-Bliley Act by failing to provide customers the privacy notices they were due. What's more, TaxSlayer violated the Safeguards Rule by failing to have a written information security program, failing to conduct the necessary risk assessment, and failing to put safeguards in place to control those risks – specifically, the risk that remote attackers would use stolen credentials to take over consumers' TaxSlayer accounts and commit tax identity theft. This case sets a precedent that failure to protect sensitive customer information from credential stuffing due to third-party credential spills could result in any financial services institution being in violation of the Gramm-Leach-Bliley Act, putting the companies at risk fines or prosecution.

OWASP: Practitioners Should Protect Web Applications Against Credential Stuffing

The Open Web Application Security Project (OWASP) is a nonprofit organization dedicated to defining, promoting, and training on application security. One of OWASP's most recognized contributions to the field is the Top 10 Project, which outlines the 10 most critical web application vulnerabilities that practitioners should prevent when developing applications. Most companies align their application security to defend

---

[13] Federal agencies have 12 months to comply with a new publication per Office of Management and Budget (OMB) Circular A-130.

against the OWASP Top 10 threats as part of internal policies.

In November 2017, OWASP formally updated the Top 10 Project, with specific language regarding credential stuffing included in A2: Broken Authentication. OWASP states that an application is weak if it "permits automated attacks such as credential stuffing" and recommends practitioners take proactive measures "such as testing new or changed passwords against a list of the top 10,000 worst passwords."

W3C: The Internet Should Stop Using Passwords

In April 2018, The World Wide Web Consortium (W3C), in conjunction with the FIDO Alliance, released a new standards milestone, WebAuthn, to more easily allow for password-less authentication. WebAuthn defines a standard web API that can be incorporated into browsers and related web platform infrastructure and gives users new methods to securely authenticate on the web, in the browser, and across sites and devices. The standard moves users away from passwords and towards more secure login methods such as biometrics and USB tokens in order to reduce account takeovers stemming from password reuse. However, replacing passwords with a physical device that acts as a key still maintains one-point authentication which attackers can eventually overcome by emulating the device.

Conclusion

We hope this report has helped dissect the complex problem of credential spills, credential stuffing, and account takeover fraud. But what makes this criminal enterprise so hard to conquer?

There are two main obstacles.

First, at an organizational level, there is no owner of the problem. Credential stuffing attacks burden an IT, security, fraud, and customer service department in different ways. IT teams have to support excess traffic while fraud analysts are forced to review hundreds, even thousands of additional cases of account takeover fraud every day. Yet when something is everybody's problem, it's no one's problem.

Second, at an industry level, we distract ourselves with the concept of passwords. Many people's proposed solution to credential stuffing is to augment or replace passwords with a different authentication system, such as introducing two-factor authentication. As detailed in the retail chapter, however, companies with high competition are loathe to introduce additional friction into their experience in the form of MFA, lest they lose out on potential revenue. Furthermore, as described in the Consumer Banking chapter, attackers are already motivated enough to figure out ways to bypass 2FA, such as by performing credential stuffing attacks against wireless providers.

Others think biometrics like fingerprints would be an apt solution. As we've already seen after Apple unveiled their iPhone 5s four years ago, attackers were able to defeat the fingerprint sensor in just two days by creating false fingerprints using high resolution images. In the age of oversharing on social networks combined with machine learning, it's not a stretch to imagine attackers will be able to do this automatically and cheaply if the value is there. This is, of course, not at all accounting for the fact that, once biometrics are required, they end up being stored and susceptible to breaches just like anything else.

The first obstacle is manageable. Once something becomes an expensive enough problem, a CEO or Board, or even customers, will demand a solution, so an owner will be found.

At that point, the second obstacle must be overcome. Simply augmenting or replacing passwords with another form of authentication is a distraction because the challenge isn't picking the right piece(s) of information to use to determine that a user is who they say they are. It's using hundred, or maybe even thousands, of other signals to ascertain exactly who is using that information.

It may be impossible for any one company to collect enough information about its users to make the right call every single time. But if every company shared their data on users (and attackers), then they would be able to create a very realistic, composite view of the user.

That is what Shape strives to enable: a collective defense.

Appendix

2017 Reported Spills

Target	# of Credentials	Date of Announcement	Organization Type
TwoPlusTwo	400,000	Jan-9	Web Forum
MrExcel	366,140	Jan-14	Web Forum
SuperCell	1,100,000	Jan-17	Web Forum
The Candid Board	178,201	Jan-24	Web Forum
XBOX360 ISO	1,296,959	Jan-29	Gaming
PSP ISO	1,274,070	Jan-29	Web Forum
PoliceOne	715,000	Feb-3	Web Forum
Coachella	950,000	Feb-22	Web Forum
Funimation	2,491,103	Feb-24	Media
CloudPets	821,296	Feb-27	Gaming
vBulletin Forums	819,977	Feb-28	Web Forum
Little Monsters	996,000	Mar-7	Web Forum
Instagram	1,500,000	Mar-9	Social Media
Association of British Travel Agents (ABTA)	43,650	Mar-16	Travel
Soundwave	130,705	Mar-17	Online Services
Dueling Network	6,500,000	Mar-29	Web Forum
Scottrade Bank	20,000	Apr-5	Financial
Avon	629,295	Apr-11	Retail
Fashion Fantasy Game	2,400,000	Apr-20	Gaming
Youku	100,759,591	Apr-23	Social Media
HipChat	N/A	Apr-24	Online Services
R2Games	1,023,466	Apr-25	Web Forum
Retina-X	71,153	Apr-27	Software
GoogleDocs	1,000,000	May-3	Online Services
Gannett	18,000	May-6	Media
Edmodo	77,000,000	May-17	Education
DaFont	699,464	May-18	Online Services
Zomato	17,000,000	May-18	Online Services
OneLogin	12,000,000	May-31	Online Services
CashCrate	6,800,000	Jun-14	Online Services

2018 Credential Spill Report

8Tracks	18,000,000	Jun-29	Social Media
XPG	890,341	Jul-2	Gaming
Virgin America	3,120	Jul-27	Travel
Mall.cz	735,000	Aug-27	Retail
CeX	2,000,000	Aug-30	Retail
Taringa	28,722,877	Sep-4	Social Media
Equifax	14,961	Sep-7	Financial
SVR Tracking	540,000	Sep-21	Software
Yahoo	2,000,000,000	Oct-3	Online Services
Disqus	6,000,000	Oct-6	Online Services
Jobstreet	17,000,000	Oct-9	Online Services
Accenture	40,000	Oct-10	Online Services
We Heart It	8,000,000	Oct-17	Social Media
Australian Government	48,270	Nov-2	Government
Verticalscope	2,700,000	Nov-3	Web Forum
CafeMom	2,628,148	Nov-6	Social Media
Cash Converts	N/A	Nov-17	Retail
Imgur	1,700,000	Nov-24	Social Media
The TVDB	181,871	Nov-25	Web Forum
Dvd-Shop	67,973	Dec-7	Retail
Ancestry.com	300000	Dec-23	Online Services