2017 CREDENTIAL SPILL REPORT

January 2017

Table of Contents

Figures and Tables

Executive Summary

More than three billion credentials were reported stolen worldwide in 2016.

Over the past twelve months the number of reported stolen credentials has set an all-time record, with Yahoo in particular being responsible for the first and second-largest reported credential spills in history.

Shape Security has a unique view into this activity. Since our technology protects the online applications of the world's largest corporations in financial services, retail, travel, and other industries, as well as some of the largest government agencies in the world, the Shape network is able to observe the use of stolen credentials globally.

Shape has identified millions of instances of credentials from reported breaches being used in credential stuffing attacks on other websites, with up to a 2% success rate in taking over accounts on systems that did not report public data breaches. As a result, automated fraud losses from credential stuffing is in the billions of dollars worldwide, based on the value of accounts taken over. The most commonly targeted account systems include bank accounts, retail gift card accounts, and airline and hotel loyalty programs.

The theft of user credentials and their use in attacking other sites is now so widespread that it prompted the National Institute of Standards and Technology in December to recommend, in the Draft NIST Special Publication 800-63B Digital Identity Guidelines, that online account systems check their users' passwords against known spilled credential lists, as companies such as Facebook are already doing. If the password chosen by a user appears on the list, NIST recommends that the user be informed that they should choose a different password since their chosen password is not considered secure.

Credential theft has now reached the point that every organization operating a publicly accessible web or mobile application should be aware of the implications to their business and investigate how to effectively protect their company and their users.

This report includes key findings from the credential spills reported in 2016 and presents data from the Shape network to provide insight into the scale of credential theft and how stolen credentials are used in credential stuffing attacks worldwide.

Key Findings

>3B Credentials Reported Stolen in 2016

3,301,824,415	Total # of Credentials Reported Spilled in 2016
275,152,035	Average # Credentials Spilled per Month
9,046,094	Average # Credentials Spilled per Day
376,920	Average # Credentials Spilled per Hour
6,282	Average # Credentials Spilled per Minute

Company with Most Spilled Credentials 2016
Yahoo 1.5B Credentials*

* Yahoo reported two separate spills of 1B and 500M credentials with some overlap in affected accounts.

Industry with Most Spilled Credentials 2016
Technology 1.75B Credentials

Industry with Greatest Number of Credential Spills 2016
Gaming 11 Companies Reporting Spills

Shape Network Data

- Shape observes credential stuffing attacks (testing stolen credentials) generating more than 90% of login traffic on many of the world's largest websites and mobile applications.
- Shape typically observes success rates of 0.1% to 2% when stolen credentials from one site are used by cybercriminals to log in to and take over accounts on other sites.
- Credential stuffing is now the single largest source of account takeover and automated fraud on most large online services.
- One of the world's largest retailers experienced a credential stuffing attack with over 10,000 login attempts in one day coming from the attack tool Sentry MBA.
- Shape regularly detects Sentry MBA in particular being used for attacks against nearly every customer in every industry.
- Shape analyzed more than 15.5M account login attempts for one customer during a 4 month period, discovering that over 500K accounts were on publicly spilled credential lists.

Introduction

In 2011, while serving as Deputy Assistant Secretary of Defense at the Pentagon, Shape co-founder Sumit Agarwal observed a rising trend in the volume and complexity of automated attacks on web and mobile applications. At that time he coined the term "credential stuffing" to describe the use of automation to test usernames and passwords stolen from one site on other sites with the intent of taking over a large set of accounts en masse. This new type of threat exploited not an accidental vulnerability in an application, but rather its correctly implemented functionality: the login form where anyone could enter the right credentials to access an account and its data and privileges. Protecting online services from this threat was the impetus for starting Shape Security with co-founders Derek Smith and Justin Call.

Today, Shape protects the web and mobile applications of the world's largest companies in financial services, retail, airline, hotels, government, and other industries. Analyzing more than one billion high value transactions per week—primarily login requests—to detect and protect against against credential stuffing and other attacks, Shape has been able to observe the automated use of stolen credentials by cybercriminals across the world.

In 2016, 51 organizations reported that their users' credential data had been stolen, totalling more than three billion credentials reported spilled over the course of the year. By far the biggest spills were from Yahoo, who had the dubious honor of being both first and second on the list of largest credential spills reported, not only in 2016, but in history. Given the ongoing and widespread theft of user credentials, organizations need to consider how to protect their users from account takeover attempts enabled by the use of spilled credentials. While the initial data breaches and credential spills in 2016 made headlines, the bigger issue for 2017 and beyond is the increasing level of credential stuffing attacks that are expected in their wake. This report provides insights into the scale of credential theft and explains how stolen credentials are used in credential stuffing attacks.

A credential spill occurs when user credential data, such as usernames and passwords, are stolen from an organization or its users. "Spill" refers to the fact that stolen credentials do not just affect the company who was originally hacked or breached, but are now available for use in attacking any other website or mobile application. Stolen credentials that make their way onto the dark web, either by being posted on online forums or being offered for sale, become accessible to more cybercriminals for use in automated attacks aimed at large-scale account takeover. Widespread password reuse by users makes it possible to use credentials stolen from one site to gain access to many of those same users' accounts on other sites.

Online credentials have been stolen and compromised for almost as long as the Internet has existed. However, over the past decade, the frequency of credential theft has increased and the tools and techniques used by cybercriminals have evolved. In the early and mid-2000s, there were few reports of leaked credentials, and they were mostly due to stolen or lost laptops or phishing scams. Credential thefts were mostly opportunistic and not necessarily the end goal. It is only in the past couple of years that theft of user credentials has ramped up significantly. This is likely due to the newfound versatility and value of online credentials, the

proliferation of online accounts held by most people, and the tendency of users to reuse the same usernames and passwords across those systems. This last issue has been exacerbated by the widespread use of primary email addresses as the default or required username across major online systems.

Today, usernames and passwords act as keys to online services that are vital to many aspects of peoples' lives, and include their retail, banking, travel, and insurance accounts. And yet, those accounts are less secure than they have ever been, due to the scale and scope of data breaches on unrelated sites.

2016 Reported Credential Spills

In 2016, 51 organizations contributed to the total of more than three billion spilled credentials. Figure 1 shows the cumulative number of credentials reported stolen in 2016.

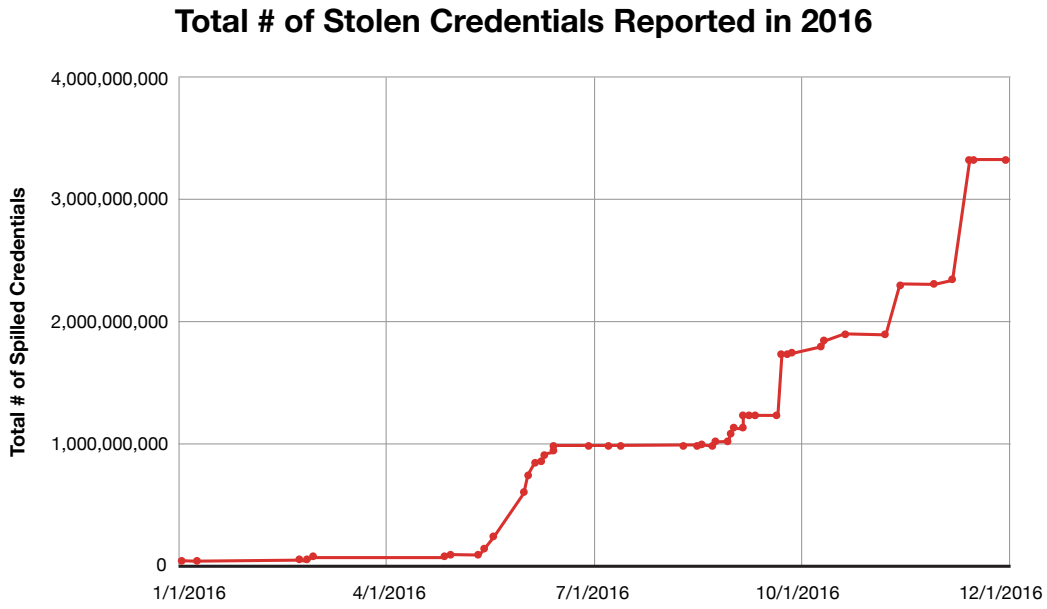

Figure 1: Total # of Stolen Credentials Reported in 2016

>3B Credentials Reported Stolen in 2016

3,301,824,415	Total # of Credentials Reported Spilled in 2016
275,152,035	Average # Credentials Spilled per Month
9,046,094	Average # Credentials Spilled per Day
376,920	Average # Credentials Spilled per Hour
6,282	Average # Credentials Spilled per Minute

# of Credentials Spilled per Incident

Mean 63,496,623 Credentials per Spill (36,036,488*)

Median 2,750,000 Credentials per Spill (2,168,260*)

* Excluding Yahoo spills.

Figure 2 shows the relative size of the ten largest spills of 2016, with the three largest spills all reported in the last four months of the year.

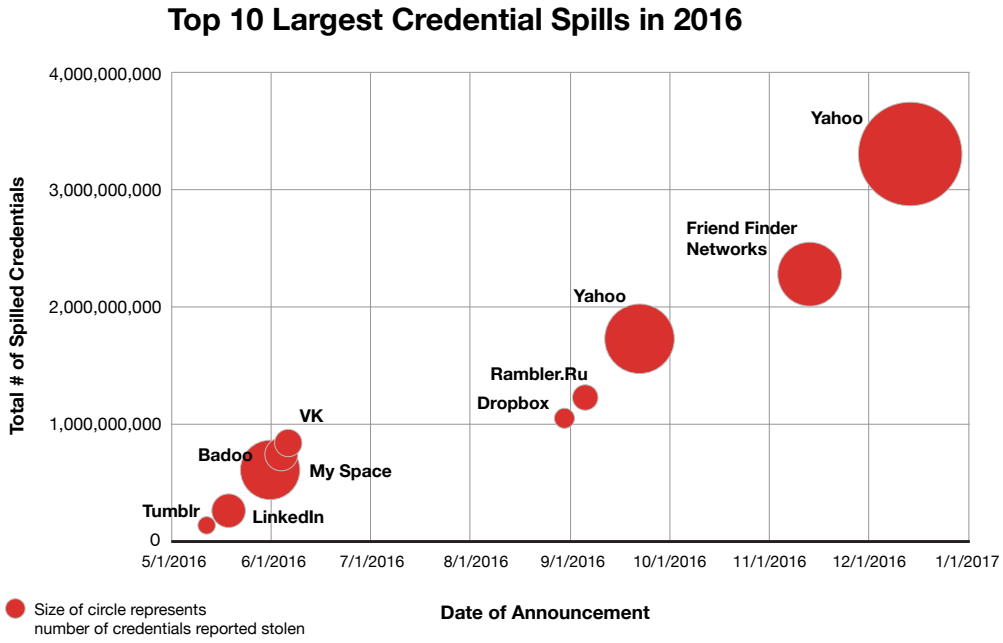

Figure 2: Top 10 Largest Reported Credential Spills in 2016

Table 1: Top 10 Credential Spills Reported in 2016

Company	# Spilled Credentials Reported	Announcement Date
Yahoo	1,000,000,000	12/14/2016
Yahoo	500,000,000	9/22/2016
Friend Finder	412,214,295	11/13/2016
MySpace	359,420,698	5/31/2016
Badoo	127,343,437	6/2/2016
LinkedIn	117,000,000	5/18/2016
VK	100,544,934	6/5/2016
Rambler.Ru	98,167,935	9/5/2016
Dropbox	68,680,741	8/30/2016
Tumblr	65,469,298	5/12/2016

A complete list of all 2016 reported spilled credentials is provided in Appendix A.

Company with Most Spilled Credentials 2016

Yahoo 1.5B Credentials*

* Yahoo reported two separate spills of 1B and 500M credentials with some overlap in affected accounts.

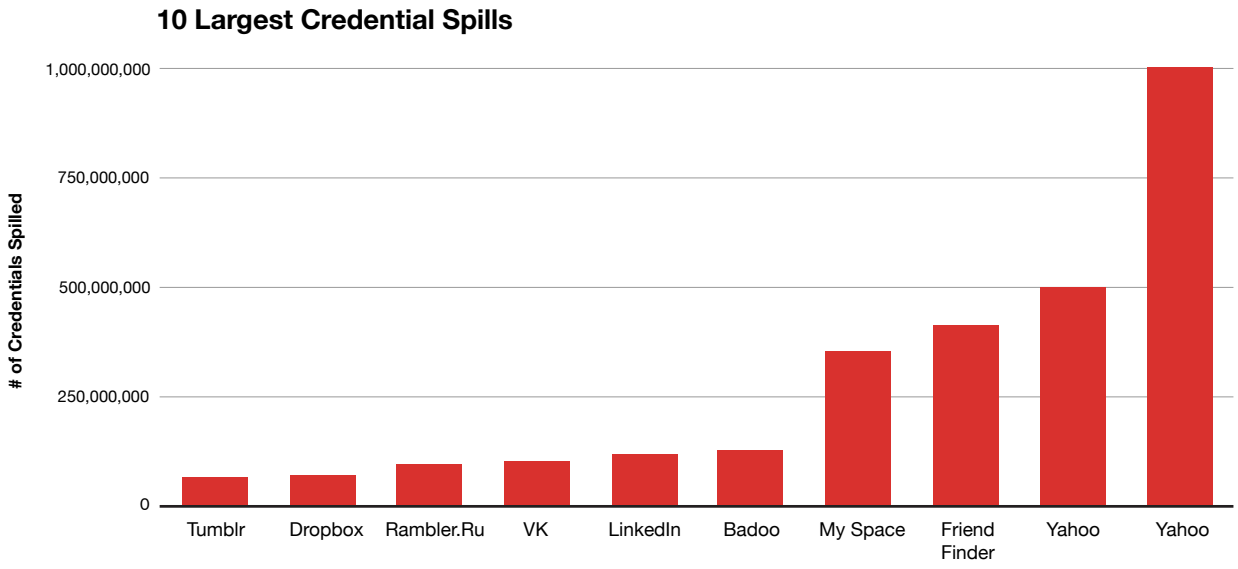

Figure 3: Companies With Most Reported Stolen Credentials in 2016

Industry with Most Spilled Credentials 2016
Technology 1.75B Credentials

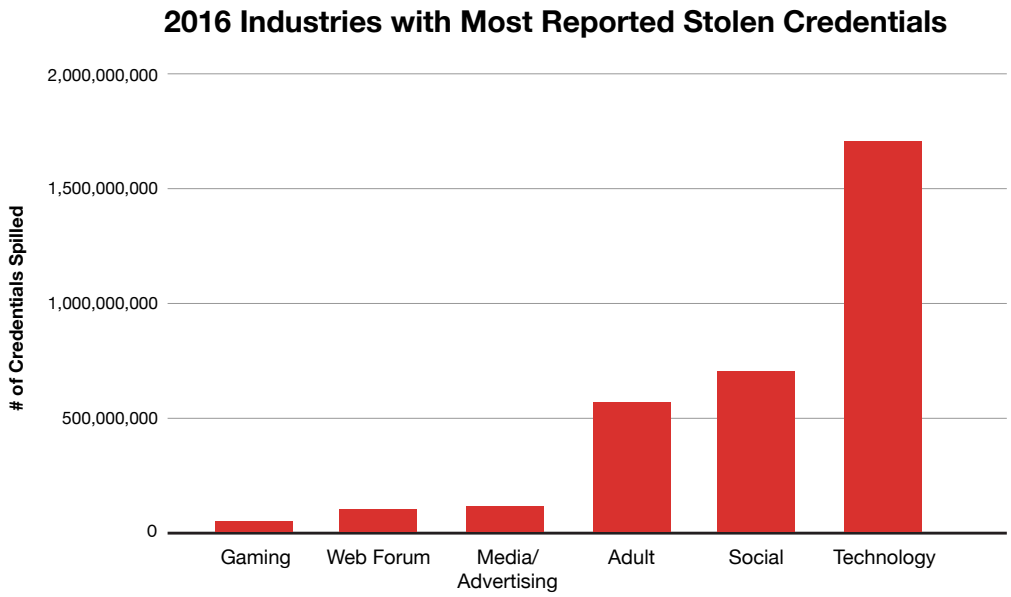

Figure 4: Industries With Most Reported Stolen Credentials in 2016

Industry with Greatest Number of Credential Spills 2016

Gaming 11 Companies Reporting Spills

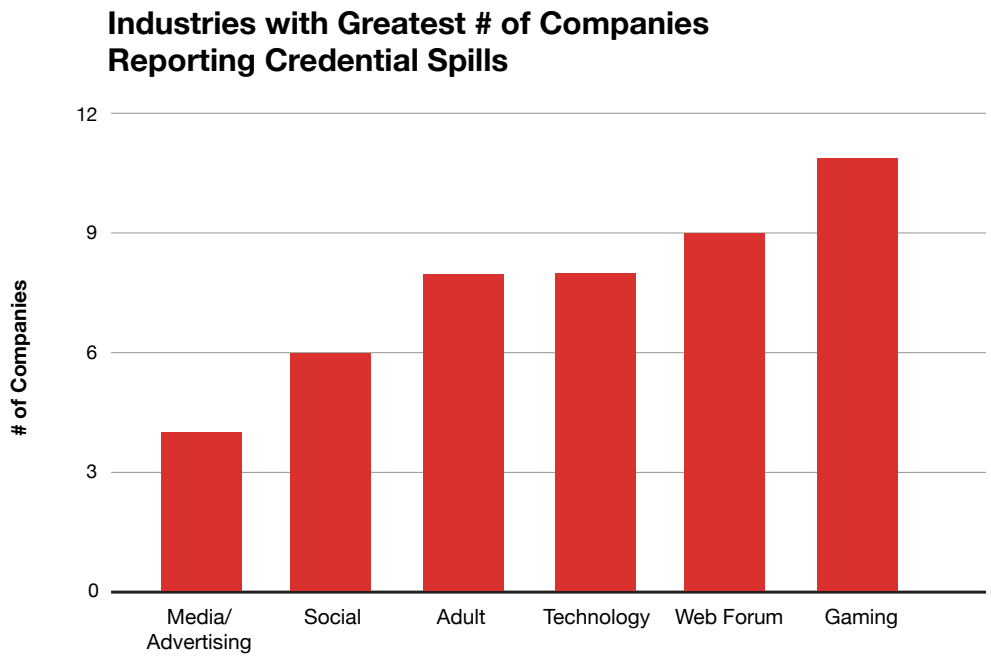

Figure 5: Industries with Greatest # of Companies Reporting Stolen Credentials in 2016

Table 2: Top Industries Reporting Stolen Credentials in 2016

Industry	# Spilled Credentials Reported	# Companies Reporting Spills
Technology	1,735,192,762	8
Social	705,323,230	6
Adult	573,713,306	8
Media/Advertising	109,360,535	4
Web Forum	103,962,899	9
Gaming	54,741,744	11

Shape Network Data

Use of Spilled Credentials by Industry

In working with customers in retail, finance, travel, and government, Shape has seen millions of instances of credentials from reported breaches being used in credential stuffing attacks. These industries are among the top targets for credential stuffing attacks. It is notable that the industries with the most credential spills, such as gaming, are not the same as the industries that are targeted the most for credential stuffing attacks. That is not to say that industries such as gaming are not facing credential stuffing attacks (they are) but instead illustrates the extent to which a company's own lack of a major data breach is not related to its vulnerability to credential stuffing from someone else's spill. This is also consistent with the pattern of other types of attacks, such as phishing, where the most common targets are the world's largest companies and biggest brands.

Login Traffic from Spilled Credentials

Most companies have no visibility into, or are unaware of, the volume of automated login traffic they are experiencing from credential stuffing attacks. They are frequently shocked when they see these metrics. One of the reasons for the inability to measure this traffic is that these type of attacks appear as legitimate requests to the security controls in place on most applications. Since real user credentials are being used to attempt log in to an application, these types of attacks do not need to use brute force techniques to attempt to guess passwords, but instead just need to "behave" the way a legitimate user providing their own credentials would. When the simulation of this behavior is fully automated, credential stuffing attacks can achieve great scale and efficiency. This often results in the vast majority of traffic to a login application actually coming from cybercriminals testing stolen credentials rather than from the site's legitimate users accessing their accounts.

Shape Network Data:

Shape observes over **90%** of login requests on many of the world's largest web and mobile applications coming from credential stuffing.

Figure 6 shows actual incoming login traffic for one of Shape's Fortune 100 customers. More than 92% of the incoming login traffic for this customer was from automated credential stuffing. The credential stuffing login attempts are shown in orange and red while the real human logins are shown in green.

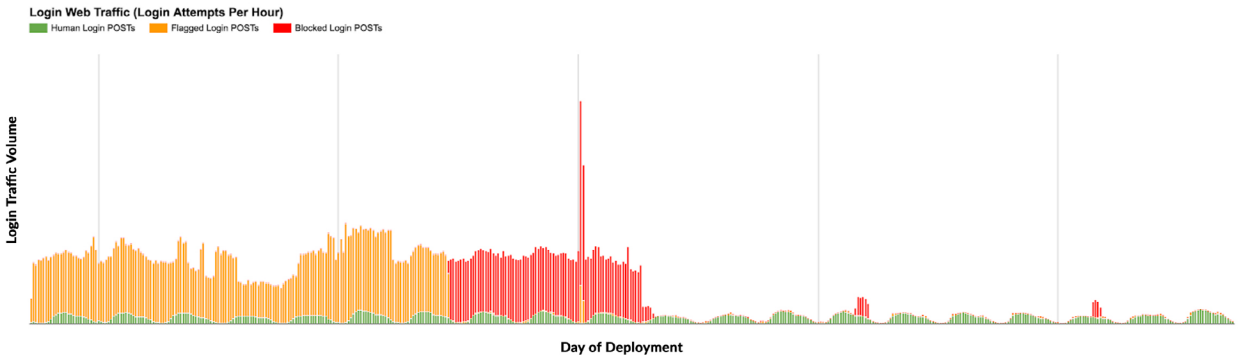

Figure 6: Incoming Automated and Legitimate Customer Login Traffic for Shape Customer

In the first several days, Shape was able to distinguish between real human user traffic (green) and automated credential stuffing traffic (orange). Once Shape went into blocking mode, the automated traffic was blocked (red) and was no longer successful at login, and after a few more days, the cybercriminals moved on to other targets. For this customer more than 92% of their incoming login traffic was from credential stuffing attacks which bypassed their industry standard security controls. This also illustrates the heavy load that automated traffic places on major websites, taxing infrastructure and adding login latency for real users.

Login Success Rates for Spilled Credentials

Using automation, cybercriminals can rapidly test stolen credentials for successful logins. If one million stolen credentials are stolen from site A and used in a credential stuffing attack on site B, the cybercriminal will typically be able to take over tens of thousands of accounts within a matter of hours or days. The same stolen credentials can then be reused in another attack on site C, and so on, attacking every major online service in turn. The greater the number of credentials used, the greater the number of accounts that can be taken over.

Shape Network Data:

Shape typically sees success rates of **0.1% to 2%** in the use of stolen credentials to access accounts on other sites.

Observing more than 15.5 million account login attempts during a 4 month period for a major retailer, Shape identified that over 500,000 accounts were on spilled credential lists.

Furthermore, Shape analyzed a sample of six billion login and search page submissions over a one month period and found the following:

- In one week, cybercriminals made over five million login attempts at a Fortune 100 B2C website using multiple attack groups and hundreds of thousands of proxies located throughout the world.
- In two days, a large retailer saw two major attacks with over 20,000 total login attempts.
- During one day, a large retailer witnessed over 10,000 login attempts from over 1,000 IPs.
- Two attacks highlight how cybercriminals are turning their attention to mobile APIs. The first attack focused on the target's traditional web application and made over 30,000 login attempts using proxies located in eastern Europe. The second attack focused on the target's mobile API and made over 10,000 login attempts on a daily basis. Both attacks shared hundreds of IP addresses and other characteristics, indicating the same actors may have been responsible.

Background on Credential Spills

How Are Credentials Stolen?

There are a variety of ways that credentials are stolen, however the source of the greatest volume of stolen credentials is the direct compromise and theft of a database of login credentials and passwords. This was the case in the infrastructure hack of LinkedIn in 2012, that resulted in 117 million stolen LinkedIn credentials spilling onto the dark web in 2016 and later being offered for sale.

Phishing attacks also yield stolen credentials, although in a much smaller volume than the breach of an account database. In phishing attacks, users are targeted with email spam containing phishing links. While the volume of stolen credentials produced from phishing attacks is much smaller, these attacks do directly yield non-hashed cleartext passwords.

Another technique used to steal credentials is the use of botnets and browser injectors. When a user inserts account information or credit card information into a browser, this information is captured by the bot client software. Also in the case of an infected computer, botnet software scans the computer for different artifacts, and grabs information about email accounts, including credentials.

What Happens with Stolen Credentials?

There are two main factors that influence what happens to stolen credentials after the original breach: the motive of the attacker and the timing of when the victim discovers the breach. These factors influence the below scenarios, which are not mutually exclusive.

Credentials stolen to be sold for a profit on the dark web
When the primary motive for credential theft is resale profit, stolen credentials are quickly sold on the dark web, and broadly resold and exploited. In some instances, not unlike drug dealers who add cutting agents to drugs, sellers may first increase the size of the credential list by adding fabricated entries. Unlike drugs, however, where the cutting agents can be determined and measured with some effort, it is not possible for buyers to differentiate the fabricated credentials from the real credentials in a credential list. From the buyer's perspective, the fabricated entries are indistinguishable from real credentials that are simply no longer valid. This practice does, however, negatively impact the ratio of good to bad credentials in the credential list, which can and does influence the seller's reputation on the dark web. Those reputations are often given a published score by the participants of underground forums, similar to seller reputation systems in legitimate marketplaces.

Even if the victim did not detect the original breach, monitoring of the dark web can sometimes identify stolen credentials before they are broadly exploited. However, because people reuse passwords, every company with a customer login form is vulnerable as a result of a credential spill, not just the original victim. In order to mitigate this risk, not just the victim, but also every company with a login form would need to continuously monitor the dark web for spilled

credentials and check against all of the company's registered users. And while that would help, it would not provide full protection, since there are many stolen credentials that would be used in credential stuffing attacks that would not be available on the dark web, at least at that point.

> *"A breach anywhere is a breach everywhere."*
>
> Shuman Ghosemajumder,
> CTO, Shape Security,
> QCon New York Keynote, 2016

The sooner a victim company is able to identify the breach and notify its customers and the public, the more quickly the stolen credential list becomes stale and less effective. Unfortunately, it is more common that attackers steal credentials, not to sell them for a quick profit on the dark web, but to advance their own illicit activities. This can conceal the original breach for months or even years.

Credentials stolen to advance other illicit activities

When the primary motive for stealing credentials is to directly advance illicit activities, the attackers behind the original breach will use the stolen credentials directly for credential stuffing, fake account creation, extortion, or money laundering. The attacker will *not* immediately sell the credentials on the dark web so the victim will not be able to discover such a breach by monitoring dark web activities. Unless, or until, the victim detects the original breach, they will have no way of knowing the breach even occurred, and consequently, will have no reason to notify customers or the public. In this scenario, no one knows to take remedial action, and the scope of the breach, even if discovered, is difficult to ascertain.

In addition, in this scenario attackers will only sell the stolen credentials after months or even years of criminal conduct, after the stolen credentials have become stale and less effective. The timing for this decision is made just like any legitimate business concerned with its bottom line—the stolen credentials are sold only when the anticipated profits from selling the credentials exceed those that are being realized from the illicit activities. Like any business, cybercriminals seek to maximize profits.

There is another similarity between criminal organizations and legitimate businesses: just as legitimate businesses sometimes have employees who steal proprietary information for personal profit, criminal organizations have "employees" who steal lists of stolen credentials and sell them on the dark web for personal profit. When this happens, the list of stolen credentials reaches the dark web more quickly and is much more broadly exploited.

This scenario played out in the summer of 2016 when there was a spike in reported spills from technology companies, including Tumblr, MySpace, and LinkedIn. As reported in the *Wired* article "An Interview With the Hacker Probably Selling Your Password Right Now," a team of criminals had originally stolen the credentials for their own purposes. When a former team member began selling some of the stolen credentials, an attacker who goes by the username of "Peace" or "Peace_of_mind" decided he didn't want to miss out on a similar opportunity to make money, and began listing the credentials for sale on the dark web.

Currently, Shape estimates that there are billions of stolen credentials available for free and for purchase on the dark web, with millions of new spilled credentials being added daily.

What Does the Market for Stolen Credentials Look Like?

The market for stolen credentials has two main components: offers of free lists of stolen credentials and lists of credentials for sale.

Free offers of stolen credentials on community forums

One portion of the market comprises people who hack companies and crack accounts for "fun" and share the information they steal, for free, with other members of the underground community on online forums. Free lists of stolen credentials are usually offered on a first-come-first-served basis. In many cases this is done to make connections and support the underground community. In some cases people do this to make a name for themselves inside the cybercriminal community. There are several forums where stolen credentials are offered for free, including:

- **Cracking.org**
- **Crackingking.org**
- **Crackingseal.io**

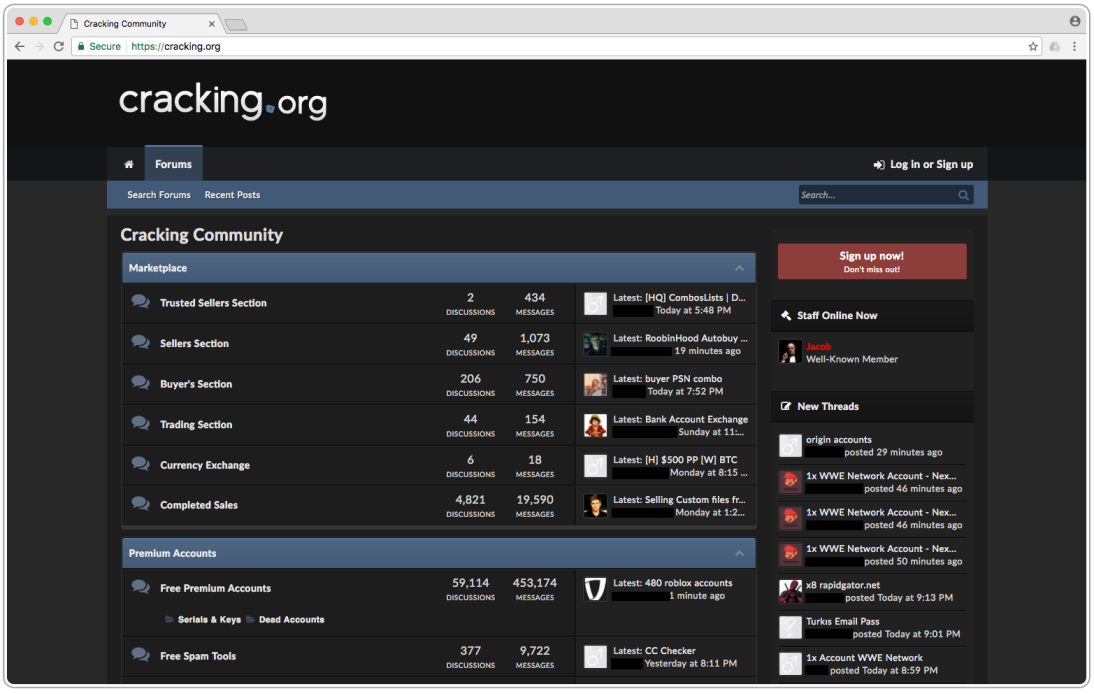

Figure 7: Spilled Credentials Shared on cracking.org

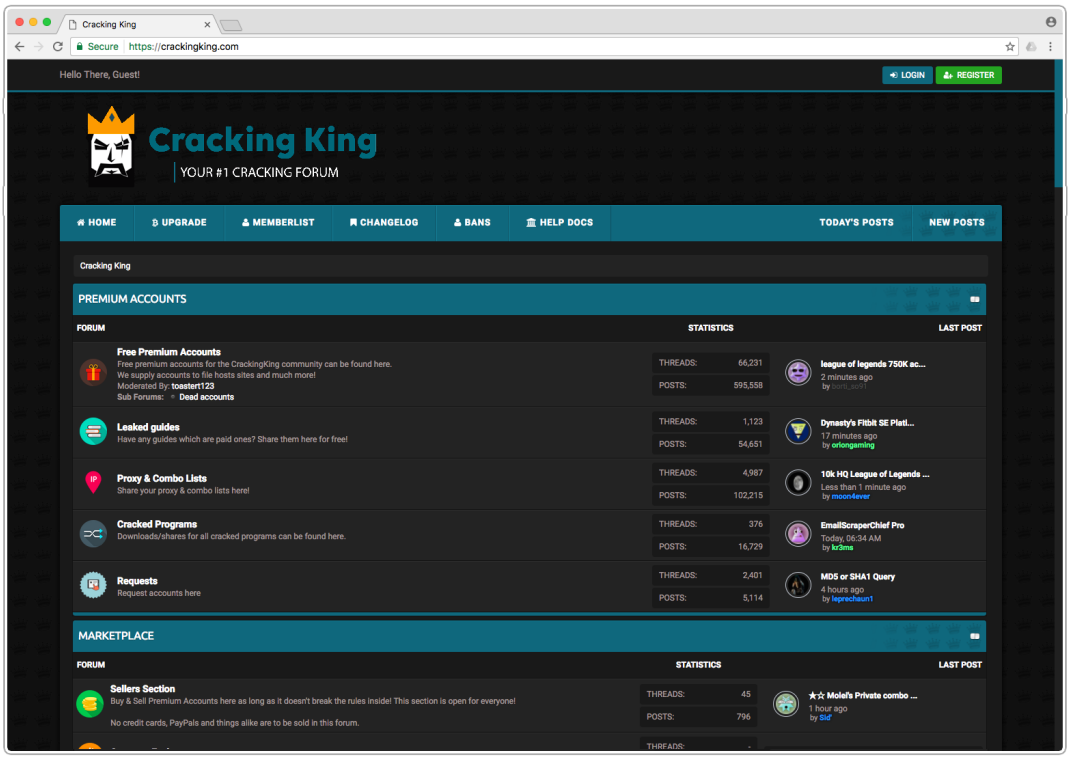

Figure 8: Spilled Credentials Shared on crackingking.org

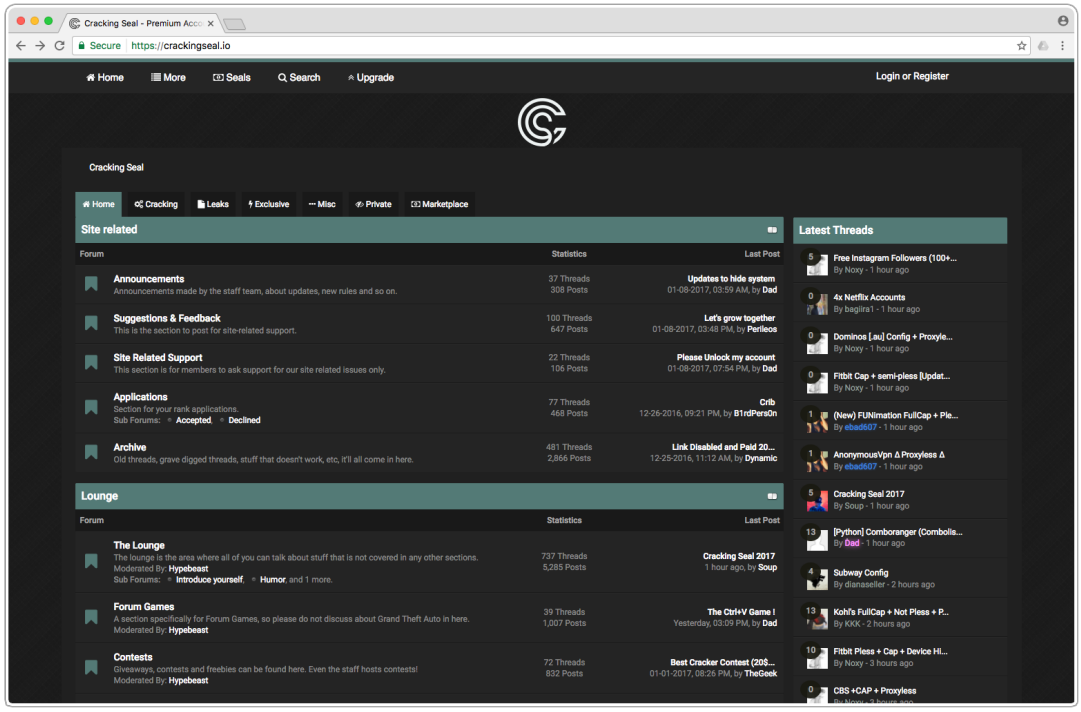

Figure 9: Spilled Credentials Shared on crackingseal.io

For-Profit Sale of Stolen Credentials

The other part of the market for stolen credentials is driven by cybercriminals who offer stolen credentials for profit. The for-profit portion of the stolen credential market includes people who sell stolen credentials in smaller or bigger chunks, and chunks pre-selected and filtered. Access to underground marketplaces is very limited. Any new potential sellers or buyers of stolen credentials will have difficulty gaining access to these marketplaces. Users need to have not only the money to pay for the credential lists, but also need to gain reputation to even be given access into some parts of the sensitive content in the forum/marketplace messages. This is one of the reasons why potential cybercriminals publish lists of stolen credentials for free—to build their reputation.

Marketplaces where stolen credentials are offered for sale include Internet forums such as Leakforums.net and Crackingweb.org, and the deep web resource called the AlphaBay Market. The following figures show credentials for O2 and LinkedIn being offered for sale on AlphaBay at the time of this report.

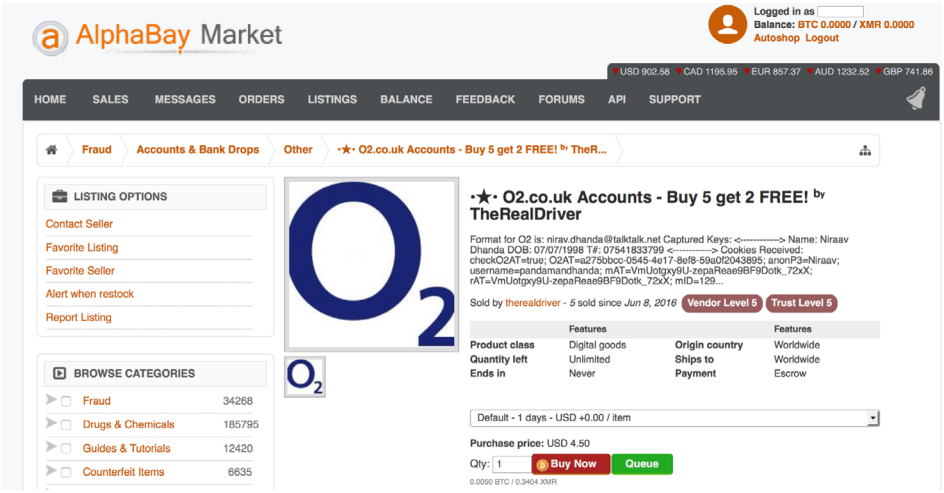

Figure 10: O2 Credentials for Sale on AlphaBay Market

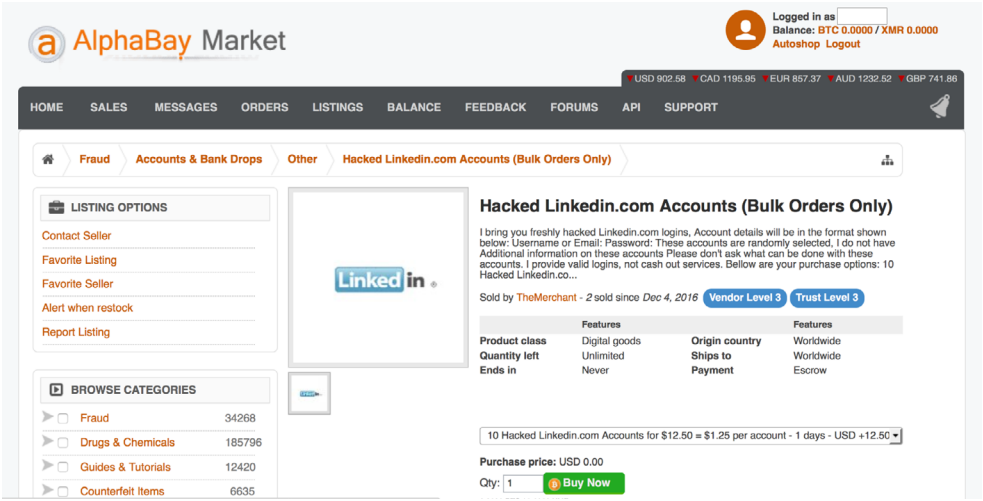

Figure 11: LinkedIn Credentials (Bulk Orders) for Sale on AlphaBay Market

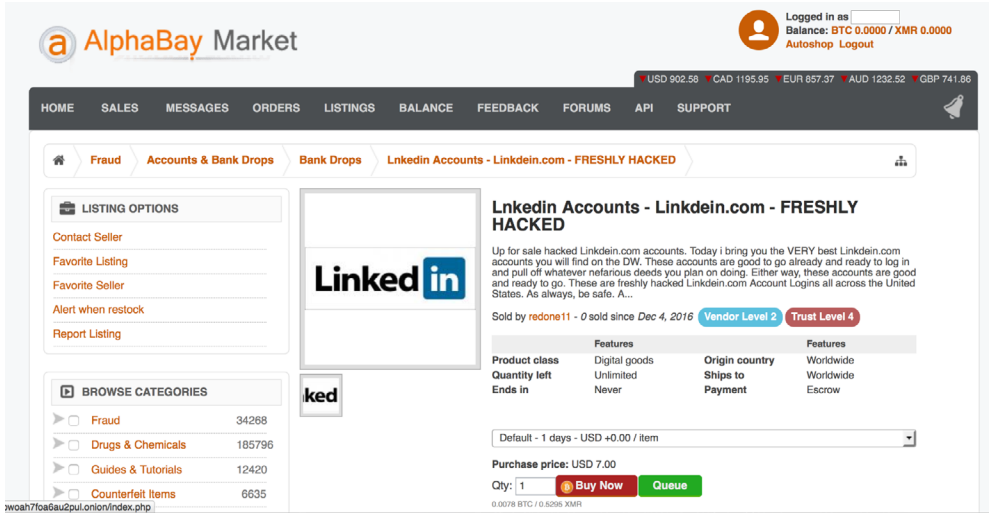

Figure 12: LinkedIn Credentials (Freshly Hacked) for Sale on AlphaBay Market

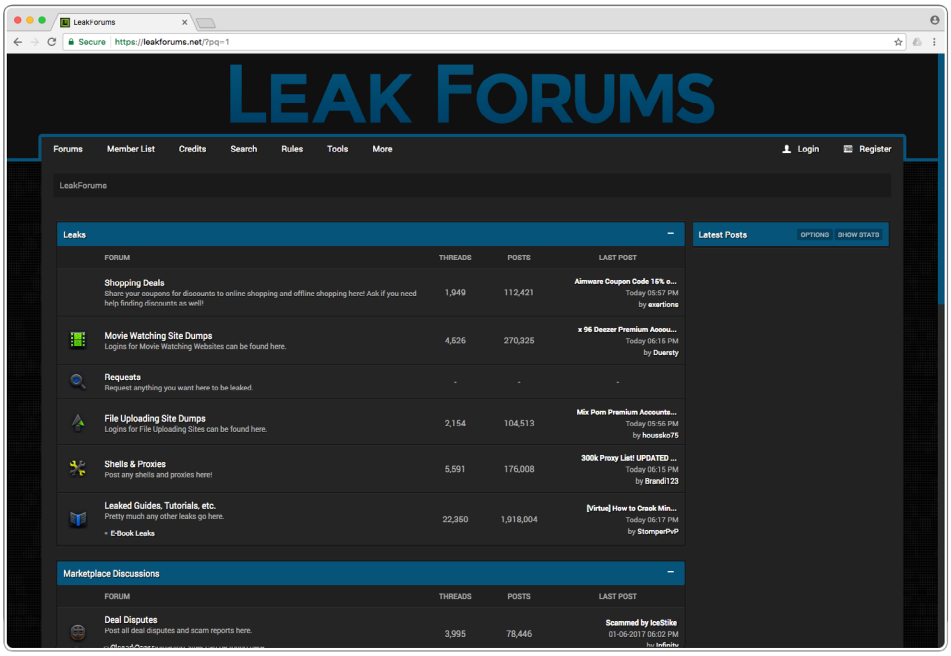

Figure 13: Spilled Credentials Shared on leakforums.net

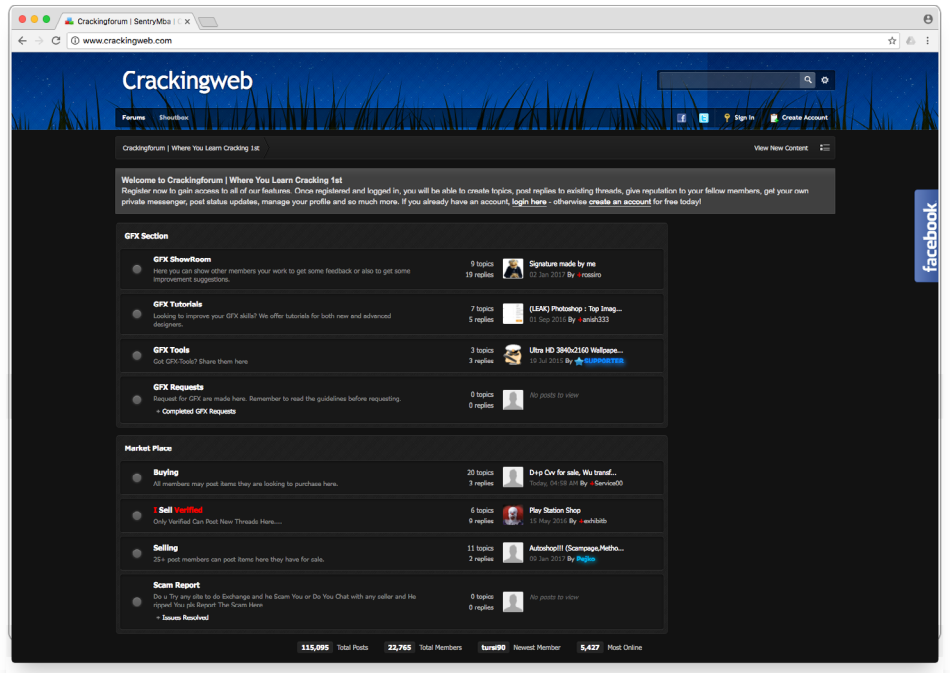

Figure 14: Spilled Credentials Shared on crackingweb.com

Time Between Credential Spill and Subsequent Credential Stuffing Attack

The Yahoo credential breaches (both of them) reported in 2016 are by far the largest credential thefts on record. Was it bad luck, poor security, or just being a prime target that led to these thefts? While the flaws that led to the Yahoo breach are still being investigated, it's important to note that these breaches actually happened back in 2012 and 2013, which means that while they were reported in 2016, the credentials have been compromised for over two years.

> *"This breach makes the job of cybercriminals that much easier. Credential spills are one of the most widespread, yet misunderstood, security breaches. Most stories will focus on users' Yahoo accounts, but the damage affecting those appears to have been done over two years ago, and Yahoo will now simply encourage those users to reset their passwords."*
>
> Shuman Ghosemajumder,
> CTO, Shape Security,
> Fox News, December 2016

While there are no direct news reports to date linking other website breaches with the Yahoo spills, the sheer scale of the credential theft and the prevalence of Yahoo users' accounts in the Internet ecosystem suggests that these stolen credentials have been benefiting cybercriminals over the past few years. Just as it took Yahoo more than two years to identify and report their credential spills, it may take other companies time to detect and also identify any resulting follow-on breaches they have suffered.

One credential spill from 2013 that finally surfaced publicly in 2016 was related to Xsplit and O2. In November 2013, Xsplit, a live streaming and recording platform for gaming, reported a data breach, with an estimated 3 million user credentials stolen. In their notification to users they recommended users reset their passwords. Fast forward to May 2016, when the BBC reported that O2 accounts had been breached via a credential stuffing attack using credentials stolen from Xsplit. In this case, the user credentials from the breached O2 accounts were subsequently put up for sale on the dark web.

Scale of Credential Stuffing Worldwide

Cybercriminals are economically motivated and look for items of value to steal. Credential stuffing attacks are not only widespread now, but continue to grow in popularity, since with as high as a 2% successful login rate for stolen credentials, attackers are able to rapidly steal millions of dollars of value, either in the form of directly stolen funds or goods, or by stealing gift cards and other intermediary vehicles that can be sold on secondary markets to unsuspecting buyers. The scale of automated fraud from credential stuffing across every major service in every industry in Shape's network indicates that these attacks are present on every large user account system in the world, often in volumes that can account for the vast majority of login traffic. In 2016 alone, Shape has already identified and protected its customers against $1 billion in attempted fraud from credential stuffing attacks.

Is a Credential Stuffing Attack Considered a Security Breach?

Credential stuffing is a different type of attack than most traditional security breaches, since it exploits the correctly implemented login functionality of a website or mobile application service in an unintended way, as opposed to exploiting an accidental application vulnerability introduced by a design or coding error. This means that there isn't a simple "defect" to fix, or patch to issue, to ameliorate the problem. Instead, the defense of a login application against automation and reuse of spilled credentials is a much more difficult and complex challenge, extending into user behavior (password reuse) and poor security practices at third-party sites.

As a result, when credential stuffing attacks are revealed to the public, some websites seek to reaffirm that they have not been "breached" or "hacked", but that is somewhat beside the point. Regardless of how credential stuffing attacks are formally classified, they are the single largest source of account takeover and automated fraud on most large online services, resulting in millions of users' funds, personal information, and identities being stolen. This has not only similar types of implications as traditional security breaches, but the aspects of automation and scale achieved by these attacks makes the damage to users generally much larger and more widespread than most traditional security breaches.

Shape Network Data:

Credential stuffing is the single largest source of account takeover and automated fraud on most large online services.

The Steps to a Credential Stuffing Attack

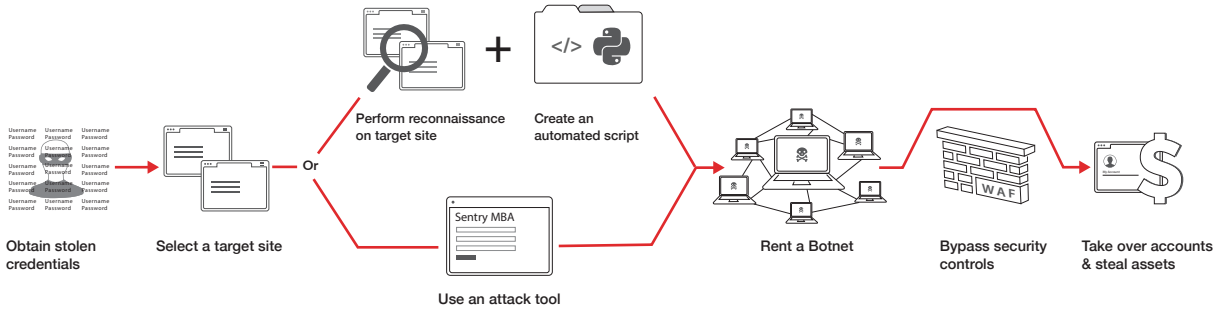

Figure 15: Typical Steps for a Credential Stuffing Attack

How has credential stuffing become so widespread? The reason is that it is now possible for even unsophisticated cybercriminals without programming ability to create and launch automated attacks to rapidly test user credentials against any target site, with the purpose of account takeover and fraud. Attack tools such as Sentry MBA make it easy for cybercriminals to test millions of username and password combinations with very little manual effort.

Credential stuffing attacks follow a sequence of easily repeatable steps. The first step is the acquisition of stolen credentials. Next, an attacker with programming skills may survey the target site and create an automation script, or any attacker can use credential stuffing software which can be configured to work with any website login form or mobile login API. These tools, plus a botnet or list of proxy IPs, allow attackers to bypass standard security controls. The final steps are simply launching the attack, taking over accounts, and stealing assets.

I. **Obtain list of stolen credentials.** Stolen credentials make their way onto the dark web from cybercriminals posting them on underground forums or public websites specifically created for the purpose of selling or distributing stolen credentials. Some of these websites even advertise the expected success rates of their credential lists (i.e., the likelihood of login success on a particular site). While many credentials can be found for free, premium lists typically have prices that vary based on characteristics of the list.

II. **Select a target site.** Cybercriminals focus their credential stuffing attacks on websites where there are assets to steal or other resources needed to advance a broader criminal scheme, such as accounts used to launder illicit proceeds. For this reason, the most attacked sites are in the banking, retail, airline, and travel industries, where there are either cash deposits, cash in gift card accounts, or loyalty points which can be effectively converted into cash through a sequence of additional steps. Cybercriminals typically start by targeting industry leaders, since they offer the biggest potential rewards, and then reuse their attack infrastructure on other sites.

IIIa. Perform reconnaissance on target site. Every website has a unique login sequence and process. In order to create a working attack script, the attacker needs to know the login page address (URI), field names for the required login parameters (such as username and password), and the required authentication steps.

Create an automation script. The automation script, which could be written in any language, such as Python, systematically works through a list of stolen credentials to verify whether each credential achieves a successful login or fails on the target site. To disguise their attempts, sophisticated attackers often use headless browsers. Headless browsers were developed to help in automating the testing of web applications for legitimate purposes. They are typically open source tools and are used by QA and test engineering groups in most companies. However, the power of these tools makes them perfect for emulating real browser functionality for fraudulent purposes as well. The use of a headless browser allows an attacker to make their login requests appear as though they are coming from real browsers, not just from a simple script, but without the overhead and friction of actually running and marionetting a full browser. The requests from headless browsers simply purport to be from real browsers, such as Firefox or Chrome. *Note: the most popular headless browser, PhantomJS, was created in 2011 by Dr. Ariya Hidayat, now VP of Engineering at Shape. The team at Shape have published insights on how to detect PhantomJS requests which may be disguised by attackers.*

-or-

IIIb. Use a configurable credential stuffing tool. As an alternative to the steps in IIIa, for cybercriminals who do not have any programming ability, or simply do not want to expend the effort in performing reconnaissance and creating custom automation scripts, there are now out-of-the-box software applications that can be configured to attack any website or mobile API. The most popular credential stuffing tool, Sentry MBA, uses "config" files for target websites that contain all the login sequence logic needed to automate login attempts. There are literally thousands of Sentry MBA configs available for free or for sale on the dark web or in underground forums to allow the tool to attack any major site. *Note: an overview of Sentry MBA and its ecosystem is given by Dr. Xinran Wang, Chief Security Scientist at Shape, in "A Look at Sentry MBA."*

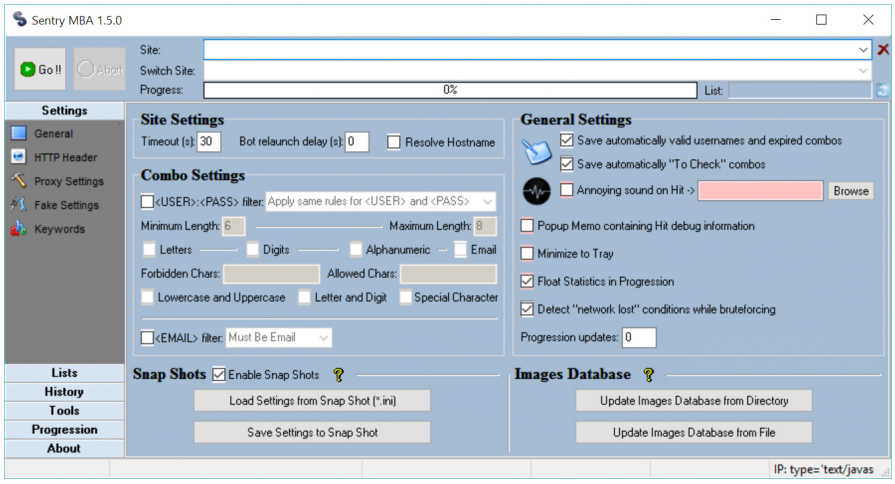

Figure 16: Sentry MBA (Windows Application for Credential Stuffing)

IV. Rent a botnet/list of proxy IPs. Botnets are networks of computing devices that have had malware installed so that they can be controlled by a criminal third party. For credential stuffing attacks, the use of a botnet enables cybercriminals to simulate the network distribution of a population of real users so that the login attempts do not appear to be coming from the same computer or IP address. In the past, botnets required a considerable amount of time, money, and expertise to assemble, but the proliferation of IoT devices has made botnet creation much easier. Once created, they are easy to rent out on the dark web. Because of the large number of devices available for infection, there are many competing botnets available for rent for any purpose, with rates as low as $2 an hour for access to 1,000 machines.

V. Bypass security controls such as Web Application Firewalls (WAF) or CAPTCHA. Sentry MBA has built-in Optical Character Recognition (OCR) technology to solve CAPTCHA challenges, the still ubiquitous obfuscated-text-based defenses which attempt to validate that a user is human. There are also third-party services which will defeat any and every CAPTCHA system in the world for low rates, often less than $1.50 for 1000 CAPTCHA solutions. In the event that the login application being attacked has these types of defenses in place, attackers program their script or configure their attack tool to solve the challenges presented. WAFs operate by detecting specific attack signatures. Cybercriminals merely change the behavior of their automation script or attack tool to generate a different signature, thereby bypassing the WAF. As a result of these techniques, CAPTCHA systems and WAFs, despite still being in widespread use, have not been effective against credential stuffing attacks for many years.

VII. Take over accounts and steal assets. By combining a list of stolen credentials with an automated script or attack tool, a rented botnet, and a way to bypass security controls, a credential stuffing attack can be quickly launched against a target site. Working systematically through a list of stolen credentials to attempt logins on the target site, cybercriminals collect credentials that yield successful logins. Those credentials are then used to take over user accounts and steal assets, either directly or indirectly.

Conclusions

Credential spills will continue and may increase in frequency

With over three billion stolen credentials reported in the last twelve months, 2016 was the year of the credential spill. Credential spills will continue as cybercriminals continue to exploit security vulnerabilities to steal credentials and sell them on the dark web. Furthermore, as additional cybercriminals discover how easy both the theft of credentials and the execution of credential stuffing attacks are, it increases both supply and demand for stolen credentials and makes it likely that the pace of credential spills will increase in the coming years.

During the past year, companies and users have been introduced to the consequences of credential spills and in particular the lesson that "a breach anywhere is a breach everywhere". This has helped improve and evolve the public's understanding of what end users should do in response to such announcements. After the first reported credential spill in 2016, at Time Warner Cable (TWC), public commentary suggested that the spill was only dangerous if users had sensitive data in their TWC email messages. In contrast, by the time of the final spills of 2016, it was common to see articles explaining that users' accounts on completely unrelated systems were also at risk. In particular, as a result of the magnitude of the Yahoo spills, many companies started proactively contacting their users to inform them that their accounts could be at risk and that they should change their passwords.

Credential stuffing is the real threat for 2017 and onwards

The theft of credentials is on the rise and credential stuffing attacks on web and mobile applications are now widespread. Unlike issues such as password selection and reuse, which are the responsibilities of users themselves, the onus is on online services to protect their users' accounts against credential stuffing attacks.

There are a variety of measures which can help, such as investing significantly in scaling up specialized security and fraud teams, arming them with advanced tools to detect automated fraud, and requiring all user accounts to enable two-factor authentication. But it is a complex problem, and there are drawbacks or limitations to each of these options.

The Open Web Application Security Project (OWASP) provides a starting point for learning about credential stuffing and other automated attacks, in their list of OWASP Automated Threats To Web Applications.

Going forward in 2017, Shape is committed to helping protect companies from the threat of credential stuffing attacks, by detecting and stopping automated logins and other fraud, and making it economically unattractive for cybercriminals to continue their attacks. In addition, Shape actively supports increasing user awareness of the role of credentials in protecting access to online services, and preventing account takeover and theft of online assets.

About Shape Security

Shape Security protects the world's largest banks, retailers, insurance companies, airlines, hotel chains, and government agencies against automated fraud and other advanced automated attacks, including credential stuffing, application-specific denial of service, and database and inventory scraping.

Recognized by CNBC as one of the top 50 most disruptive companies in the world, Shape changes the economics of cyberattacks by constantly increasing the cost and difficulty for cybercriminals to attack web applications and mobile APIs, rendering their fraud schemes unscalable and unviable.

Shape's research and development efforts have focused exclusively on creating the most sophisticated technology platform to identify and stop automated cybercriminal attacks against web and mobile application services. With more than 120 patents filed and 33 patents granted, Shape's technology has proven to be uniquely effective at defending against the complex cyberattacks faced by leading global brands.

Today, Shape's technology protects over 20% of in-store mobile payments worldwide and defends more than 500 million user accounts on behalf of its customers. In 2016, Shape prevented more than $1 billion in automated fraud losses.

Contact Information
Website www.shapesecurity.com
General Inquiries info@shapesecurity.com
Sales Inquiries sales@shapesecurity.com
Press Inquiries press@shapesecurity.com
Phone +1 650 399 0400

Appendix A

Table A1: Credential Spill Data for 2016

Company	# Reported Spilled Credentials 2016	Announcement Date
Time Warner Cable	320,000	2016-01-07
Linux Mint	71,000	2016-02-21
TruckersMP	84,000	2016-02-25
Mate1	27,000,000	2016-02-29
Naughty America	3,800,000	2016-04-14
Qatar National Bank	100,000	2016-04-25
Minecraft Lifeboat	7,000,000	2016-04-26
17	30,000,000	2016-04-29
Rosebutt Board	107,303	2016-05-10
Tumblr	65,469,298	2016-05-12
LinkedIn	117,000,000	2016-05-18
MySpace	359,420,698	2016-05-31
Badoo	127,343,437	2016-06-02
VK	100,544,934	2016-06-05
BitTorrent	34,235	2016-06-08
uTorrent	388,000	2016-06-08
Twitter	32,888,300	2016-06-08
iMesh	51,310,759	2016-06-13
VerticalScope	45,000,000	2016-06-14
Muslim Match	149,830	2016-06-29
Penton Technology	1,442,602	2016-07-08
Shadi.com	2,035,020	2016-07-13
Dota2	1,500,000	2016-08-10
Social Blade	273,086	2016-08-16
Steam	3,300,000	2016-08-18
Leet	6,084,276	2016-08-18

Epic Games	808,000	2016-08-22
Grand Theft Auto	197,184	2016-08-23
Mail.ru	25,000,000	2016-08-24
Minecraft World Map	71,000	2016-08-30
Dropbox	68,680,741	2016-08-30
Last.fm	43,570,999	2016-09-01
BTC-e	568,335	2016-09-02
Brazzers	790,724	2016-09-05
Rambler.Ru	98,167,935	2016-09-05
Flash Flash Revolution	1,771,845	2016-09-08
ClixSense	6,606,008	2016-09-11
MoDaCo	880,000	2016-09-20
Yahoo!	500,000,000	2016-09-22
gPotato	2,136,520	2016-09-24
iDressup	2,200,000	2016-09-26
Modern Business Solutions	58,843,488	2016-10-10
Evony	34,345,472	2016-10-11
Weebly	43,430,316	2016-10-20
Sam’s Club	14,600	2016-11-07
Heroes of Gaia	179,967	2016-11-07
FriendFinder Networks	412,214,295	2016-11-13
xHamster	380,000	2016-11-28
DailyMotion	18,300,000	2016-12-06
Yahoo!	1,000,000,000	2016-12-14
US Election Assistance Commission	100	2016-12-15
LA County	108	2016-12-16

2017
CREDENTIAL SPILL REPORT

SHAPE

www.shapesecurity.com