SpyCloud

October 2017

THE RISING THREAT OF ACCOUNT TAKEOVER

Exploring the Burgeoning Underground Market for Account Takeover Attacks

OVERVIEW

As technology advances to make our lives easier, so too, do the capabilities of criminals seeking to exploit its weaknesses. Today, it seems we're bombarded with a litany of data breach headlines on a near-daily basis. So many, in fact, that the clear majority of the population has become seemingly numb to the news. Larger breaches, such as the ones we've heard about at Target, Yahoo, and Home Depot, draw our attention back in—but the smaller breaches are so commonplace, they often go unnoticed.

At SpyCloud, we notice. Utilizing proprietary tradecraft, we recover stolen and breached data from private sources at exceedingly high volumes. Eighty percent of the data we acquire is privately held, as it cannot be found by scanners, scrapers or web crawlers. Unfortunately, it is also often in the hands of malicious threat actors. This enables even unsophisticated threat actors to compromise a number of customer or employee-facing accounts with little to no knowledge of traditional hacking techniques.

Because of widespread password reuse, Account Takeover (ATO) attacks have become an extremely lucrative business for cybercriminals. Organized crime rings are performing ATO attacks at a massive scale by leveraging botnet-infected armies to attempt credential-stuffing attacks against various web and mobile applications. Cyber criminals exploit compromised accounts for financial gain by pilfering financial or personally identifiable information (PII) directly or by selling access to these accounts on underground markets.

Based on the number of data breaches that took place in 2016 alone, it's likely that these stolen credentials will continue to be used heavily in ATO attacks in 2017 and beyond.

Experts have observed a

40%

INCREASE IN

U.S. data breaches over the all-time high of 780 breaches reported in 2015.

Recently, SpyCloud's research group analyzed the wealth of breach data that we have collected thus far in 2017. Through this research, we have discovered some alarming trends:

The Underground Economy is Thriving

The online underground market for identities, credentials, and personally identifiable information (PII) is growing exponentially. Anyone with a computer,

A STAGGERING

81%

OF CONFIRMED DATA BREACHES LAST YEAR INVOLVED LEVERAGING WEAK OR STOLEN PASSWORDS.

a bitcoin wallet and internet access can easily buy (or sell) access to stolen credentials and PII. It's not uncommon to see threat actors making the rounds on underground sites trying to sell data shortly after a target site or commercial web application has been breached.

Often referred to as "fullz" in threat-actor communities, this stolen information can sometimes include full "packages" of information that can be used to empty a victim's bank account or be leveraged in credit card fraud operations. Fullz usually include physical addresses, credit information, dates of birth, social security numbers and additional sensitive information belonging to the victim. Part of the sales process involves offering "proof of access" by sharing a sample of hacked account logins (oftentimes, thousands of them) to prospective buyers. In short, credential harvesting is lucrative—and business is booming.

We're also seeing emerging secondary markets dedicated exclusively to selling actual user account access. Once a threat actor has successfully compromised an online account, he can usually get a decent return on his investment. Hacked accounts that have cash account balances, linked credit cards, or travel/gift points typically demand respectively higher prices in underground markets.

Why Credential Stuffing is so Effective

The proliferation of stolen or leaked-breach databases has given rise to "credential stuffing." This is a considerably simple technique in which criminals load lists of stolen credentials into automated brute-forcing tools. These tools then test stolen passwords against thousands of commercial web or mobile applications and sites.

The use of stolen credentials to break into sites is not particularly new or sophisticated--but it works.

This is exactly what happened to Dropbox when an employee used the same password to access the enterprise networks of both LinkedIn and Dropbox[1].

After the 2012 LinkedIn data breach, threat actors were able to reuse the Dropbox employee's LinkedIn password to infiltrate the corporate network and, eventually, steal 60 million Dropbox credentials. Shortly thereafter, a criminal

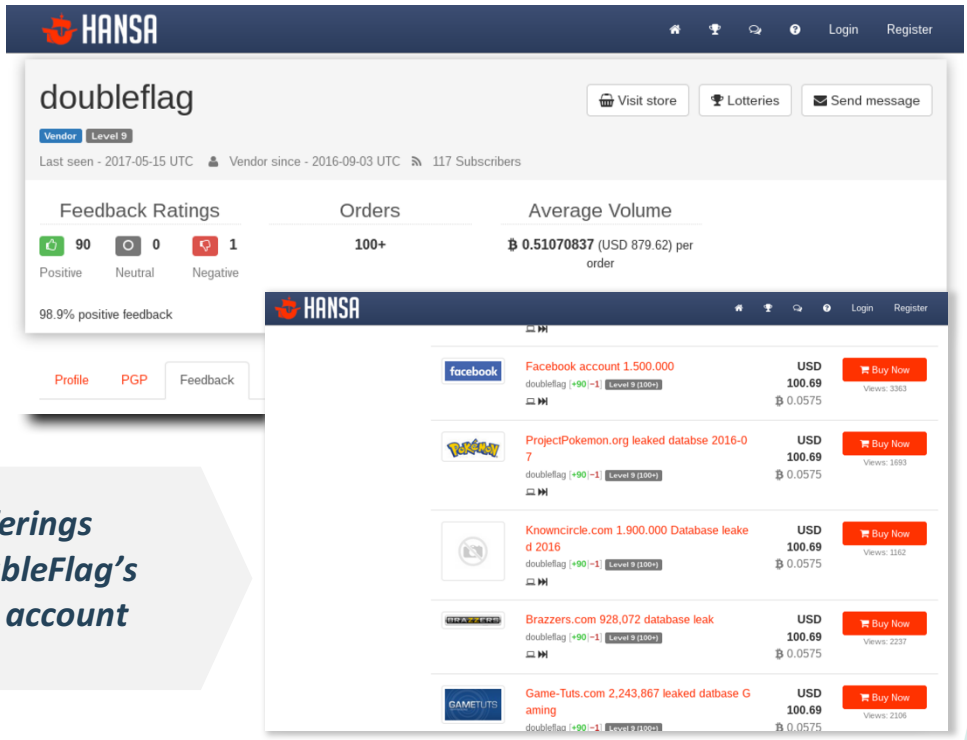
[1] https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/

using the alias “DoubleFlag” was found on the popular dark web market “TheRealDeal,” where he was selling the Dropbox data dump for 2 BTC (roughly $1200 USD at the time).

One reused password was all it took to jeopardize millions of customer accounts.

“DoubleFlag”—and other actors taking a similar approach—were active on the “TheRealDeal,” as well as some of the most popular and easily-accessed dark web marketplaces like “The AlphaBay Market,” and the “Hansa Market” before those sites were taken down in 2017. Unlike other dark net markets, these markets were not “invite only.” Anyone who has internet access and utilizes the TOR browser can register free buyer accounts on these markets without special invitations or access to trusted groups. Though vendors on these markets may not be the most technically savvy or operationally sophisticated, the items they sell benefit from an extremely large customer base. On the AlphaBay Market Forum alone, over 170,000 members were registered. This is good news for vendors—who see the procurement novice customers and opportunistic criminals as “easy money.”

SPYCLOUD RESEARCHERS HAD FOUND DOUBLEFLAG’S ACCOUNTS ON THE ALPHABAY MARKET AND HANSA MARKET WHEN THOSE SITES WERE STILL ACTIVE.



The offerings on DoubleFlag’s vendor account

If you're a large enterprise, your business can likely weather the storm and recover. But for the average company, a data breach can cause irreparable damage. One study found that as many as 60% of hacked small- and medium-sized businesses go under within 6 months of a data breach[2].

Clearly, credential stuffing puts your own organization at risk—even if your business is completely unrelated to the compromised site. Criminals leverage the resulting successful logins on other sites to hijack accounts (mostly for financially-motivated gains).

BY REUSING PASSWORDS ACROSS MULTIPLE SERVICES, USERS MAKE IS EASIER FOR CYBERCRIMINALS TO BREACH ALL THEIR ACCOUNTS, NOT TO MENTION COMPANY DATABASES.

On average, attackers are seeing up to a 2% success rate for gaining access to these other accounts simply due to password reuse.[3]

This may sound like a relatively insignificant proportion, but it equivocates to billions of dollars worldwide in automated fraud losses.

It's actually surprising that the success rate of credential stuffing isn't higher. A recent password-use study of roughly 1 billion leaked user accounts concluded that 20% of users were reusing passwords and 27% of users used a password that was nearly identical with other account passwords[3].

Because password reuse is so rampant across all industries, threat actors can usually expect a decent return on their investments when purchasing fresh credential dumps on the black market.

---

[2] https://www.paychex.com/articles/human-resources/creating-cyber-security-culture

[3] http://www.ghacks.net/2016/12/09/password-use-study-massive-reuse-of-passwords/

KEY FINDINGS–EXPOSED CREDENTIALS IN THE GLOBAL FORTUNE 500

At SpyCloud, our seasoned team of researchers discovers and recovers stolen credentials and other assets primarily through human intelligence collection and analysis. Each month, we acquire hundreds of millions of records from the dark corners of the internet. These records impact individuals and organizations globally. We validate and ingest these records into a central database, then analyze and match which assets correspond to items in our customers' watchlists. When we find a match, we notify our customers immediately so that they can react and mitigate further damage as soon as possible.

Our research team has compiled a list of all companies and their subsidiaries in the Global Fortune 500[4], and matched them against the breached records we've collected in the underground so far in 2017.

Key highlights of our research, spanning January – Sept 2017, include:

1519

# of breached databases recovered so far by SpyCloud in 2017
1288 private (85%) 291 public (15%)

1.1B

Total number of unique leaked credentials recovered by SpyCloud

[4] http://www.fortune.com/global500

5,877,052	**Total number of leaked records in 2017 affecting Global Fortune 500 companies and their subsidiaries**
499	**Total number of Global Fortune 500 companies exposed to leaked credentials in 2017**
1306 per mo.	**Average number of new exposed credentials per month per Global Fortune 500 company in 2017**
235 So far this year	**Assuming a 2% credential stuffing success rate, average number of hackable employee accounts per company** **26 new hackable employee accounts per month**
519 mil	**Number of total exposed credentials in 2017 with weak or no encryption. (69%)**
Fortune 500 Industries with most 3rd-party leaked records	**Technology:** 1,416,140 records (24%) **Financial Services:** 1,140,285 records (19%) **Telecommunications:** 960,446 records (16%)
$1.93	**Average underground market price per hacked online account access (depending on cash or points balance)**

2017 Fortune Global 500 Breach Exposure Stats

Sector	Total Leaked 3rd Party Records	Percent total	Leaked Records in Jan – Sept 2017	Percent in 2017	Average Per Company/mo in 2017
Technology	2,819,132	23.95%	1,416,140	24.10%	4,768
Telecommunications	2,466,271	20.95%	960,446	16.34%	6,277
Financial Services	1,975,179	16.78%	1,140,285	19.40%	1,111
Industrials	725,763	6.17%	319,326	5.43%	1,690
Health Care	813,619	6.91%	488,743	8.32%	2,263
Energy	554,539	4.71%	261,465	4.45%	330
Automotive	338,869	2.88%	155,977	2.65%	510
Aerospace & Defense	347,661	2.95%	189,461	3.22%	1,403
Transportation	280,078	2.38%	157,225	2.68%	873
Household Products	148,246	1.26%	64,924	1.10%	2,405
Food & Beverages	142,733	1.21%	63,302	1.08%	440
Retail	494,625	4.20%	252,382	4.29%	1,558
Materials	108,936	0.93%	64,709	1.10%	399
Chemicals	93,255	0.79%	45,095	0.77%	716
Wholesalers	133,777	1.14%	88,252	1.50%	363
Media & Entertainment	102,955	0.87%	49,246	0.84%	1,824
Food & Drug Stores	156,245	1.33%	129,011	2.20%	717
Apparel	27,136	0.23%	12,120	0.21%	449
Hotels & Restaurants	23,805	0.20%	11,049	0.19%	409
Business Services	12,572	0.11%	5,339	0.09%	198
Engineering & Construction	4,943	0.04%	2,555	0.04%	22
Total	**11,770,339**		**5,877,052**		

INTELLIGENCE AND TRADECRAFT NOTES

- Our match rate against Fortune 500 domains doesn't take into account that an employee's personal email is likely used for many professional services (e.g. Github, Dropbox, LinkedIn, etc.)[5].
- Our analysis of Fortune 500 company subsidiaries is based on public reverse WhoIs data and public corporate subsidiary data.
- For service providers in the Fortune 500, we did not include affected customers and subscribers (e.g. gmail.com, att.net, etc.).
- It's important to note that this data only represents data that SpyCloud has been mining since the *beginning of 2017*. Given this, it's likely that the metrics shown may underestimate the severity of account takeover across various industries; leaked credentials from the LinkedIn breach from 2012 are still quite effective today in credential stuffing attacks.

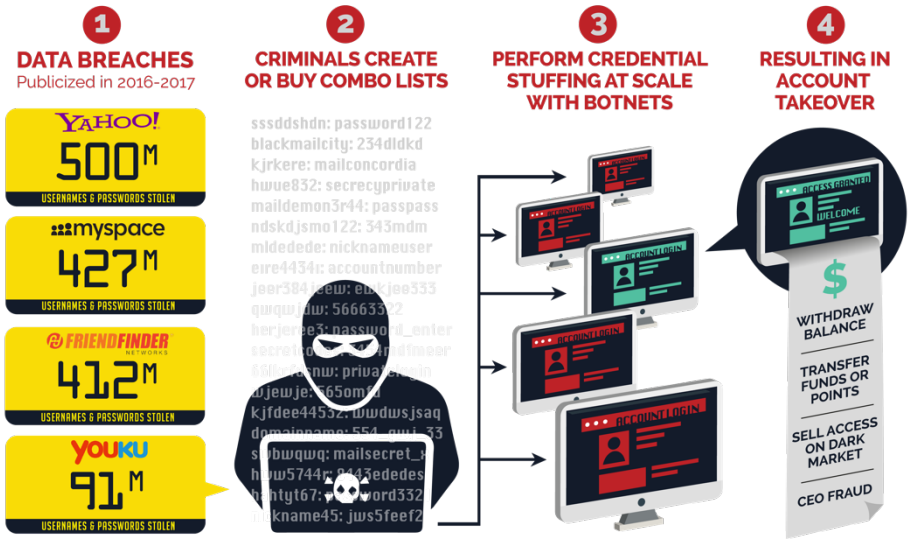
[5] https://techcrunch.com/2016/06/16/github-accounts-targeted-in-password-reuse-attack/

ANATOMY OF AN ACCOUNT TAKEOVER ATTACK

For the company that suffers a data breach, the financial, reputational, and cleanup costs can be immense. However, the collateral damage that occurs to their users and employees can be even worse.

The sequence of events that occurs following a breach has become fairly predictable.

The following chart illustrates the chain of events that often leads to secondary mass-account compromises on a variety of other sites:



1. A breach occurs or a site is compromised in some other manner.

2. The threat actor acquires leaked credentials directly from the breach or by purchasing a pre-assembled lists of username/password pairs (combo lists) from an underground market. Some underground websites even advertise the expected success rates of their combo lists[6].

3. The actor loads his combo list in an automated credential stuffing tool, and with the help of botnets, tests the stolen credentials against many other sites at once (for instance banking, gift card, or online marketplace sites). One such credential stuffing tool that has gained in popularity for its ease-of-use is Sentry MBA[7].

[6] https://blog.shapesecurity.com/2017/01/17/2017-credential-spill-report/

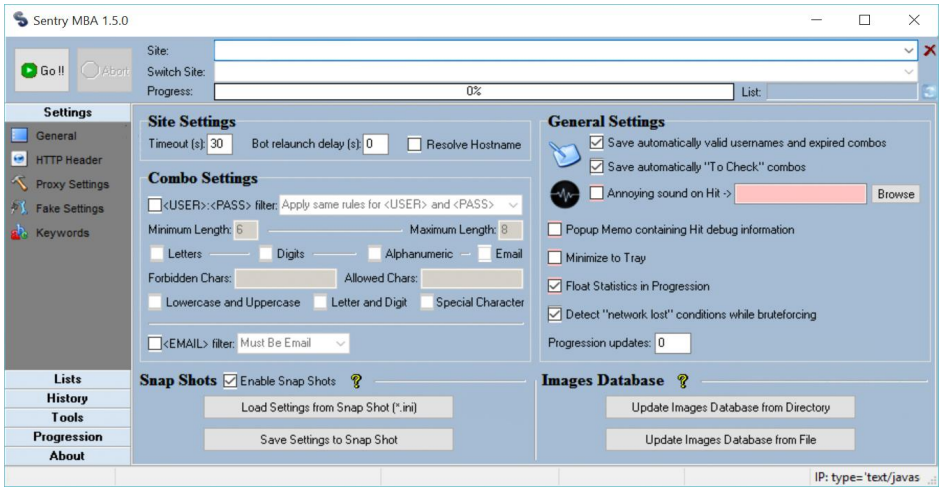
[7] http://engineering.shapesecurity.com/2016/03/a-look-at-sentry-mba.html

What is Sentry MBA?

The act of credential stuffing can be automated by certain tools, many of which are considerably easy to use. The use of these tools increases the likelihood that even less-sophisticated threat actors can hijack at least some accounts. One such tool is called Sentry MBA, which is a windows application requiring the following inputs to run against a targeted interface or application:

- **Config file:** Helps Sentry MBA navigate the unique characteristics of the site being targeted; the URL for the targeted website's login page, for example, is specified in the config (configuration) file. There are several dark web and clearnet sites dedicated to the sale and trade of custom config files for many popular commercial services.
- **Proxy file:** A list of IP addresses (usually compromised endpoints and botnets) to route traffic through, so that the set of login attempts appears to be coming from a large variety of sources (resembling organic traffic) rather than from a single attacker.
- **Combo list:** A database of username/password pairs to be tested against the target site; these lists are typically obtained from the breaches on other websites that can also be sold or traded on certain markets.

Sentry MBA has a number of additional features to assist the attacker further, including built-in OCR capabilities for bypassing CAPTCHA challenges and functionality to spoof various browser characteristics, such as the user agent and referrer strings.



Successful logins (up to 2% of the total login attempts[1]) allow the attacker to take over several accounts matching the stolen credentials.

There are countless underground forums on both the dark web and clearnet dedicated to the sale and trade of Sentry MBA config files, combo lists and proxy files (although sometimes config files are marketed as "proxyless"). Some of these forums, which often advertise themselves as "cracking" forums or communities in the "cracking scene" use a reputation system among its members. Rather than acting as marketplaces, these forums allow members to manufacture, test, and post access to combo lists for free for each contributing in these communities. Members who take and paste config files (which are often pasted as text files) without giving back to the community are often banned for "leeching." This honor system has helped create self-sustaining micromarkets for the creation and trade of Sentry MBA config files and combo lists on cracking forums. There are also marketplaces, many on the dark web, dedicated solely to Sentry MBA inputs. These often require use of a bitcoin wallet to purchase inputs such as config files and combo lists, which tend to be of a higher quality than those posted in the types of communities described above.

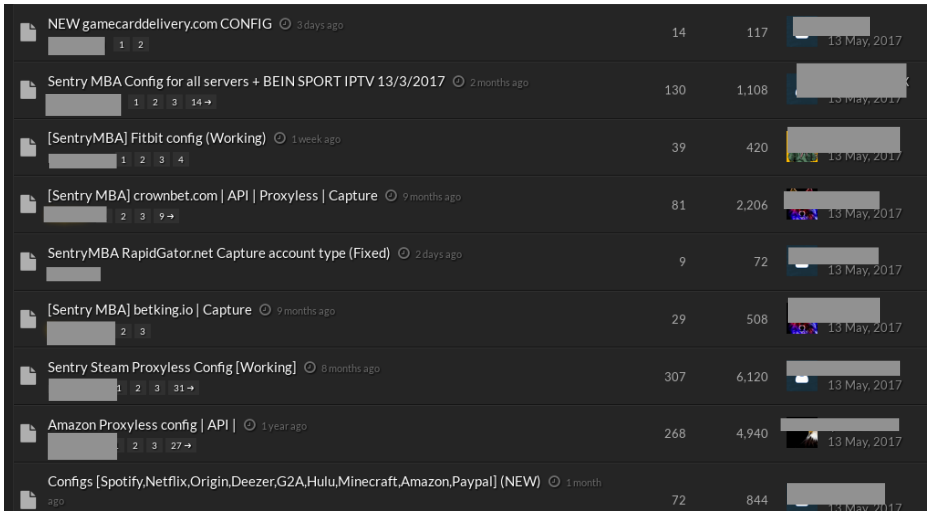
The screenshot below shows some recent threads on one such cracking forum dedicated to the trade of Sentry MBA config files. As shown, many of these custom config files are designed by members for popular services such as Spotify, Amazon, Netflix, Hulu, Minecraft, PayPal, Steam, FitBit, and others. Fresh config files for new and existing services are often added to these forums daily. And as services adjust their web applications to prevent Sentry MBA attacks, so too do the "crackers" seeking to break them. Sentry MBA inputs are often tweaked, tested, and reposted until they are proved to be effective.

The price per hacked account varies depending on the affected site, and the cash/points balance in it, but averages around

$1 - $5

per account.

Threads advertising custom-designed Sentry MBA config files for a variety of services on a popular cracking forum.



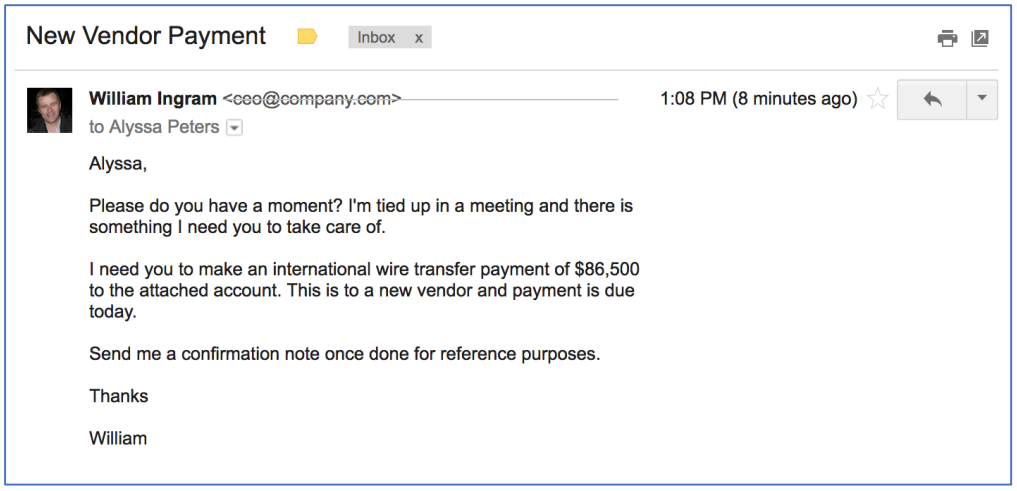
4. Even more lucrative than selling credential lists, is the sale of actual accounts which have been previously accessed and taken over (thanks to tools like Sentry MBA). The attacker either sells access to the account on a dark market, or cashes the accounts out himself of stored balance, credit card numbers, and other PII. Cybercriminals are often after accounts with cash or points balances. Instead of leveraging the account for himself, an attacker may sell access to these accounts on other underground forums. These types of account demand high prices, and take out the leg work of cracking applications and sites that are particularly well-guarded against tools like Sentry MBA.

See prices for hacked accounts from underground markets as of May 2017 in Appendix A.

The attacker may also further leverage the accounts he cashes out in other types of fraud operations. An example from 2017 involved attackers using credential stuffing to break into Amazon merchant accounts to steal up to tens of thousands of dollars. Attackers also used the same technique to hack into the Amazon accounts of inactive sellers to post sales of nonexistent merchandise, at steep discounts, in an attempt to pocket the cash[8].

[8] http://www.foxbusiness.com/markets/2017/04/10/amazon-coms-third-party-sellers-hit-by-hackers.html

The attacker may use the account for launching targeted spear-phishing or social engineering campaigns[9]—also known as "CEO Fraud" or "Business Email Compromise" (BEC). These are highly-effective e-mail scams in which the attacker spoofs a message from a C-level exec and tricks someone at the organization into wiring funds to the fraudsters[10],[11].


New Vendor Payment

Inbox x

William Ingram <ceo@company.com> 1:08 PM (8 minutes ago)

to Alyssa Peters

Alyssa,

Please do you have a moment? I'm tied up in a meeting and there is something I need you to take care of.

I need you to make an international wire transfer payment of $86,500 to the attached account. This is to a new vendor and payment is due today.

Send me a confirmation note once done for reference purposes.

Thanks

William

[9] https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams

[10] https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/

[11] https://www.trustwave.com/Resources/SpiderLabs-Blog/CEO-Fraud-Scams-and-How-to-Deal-With-Them-at-the-Email-Gateway/

We highly recommend enforcing the use of a password manager inside your organization

REMEDIATION AND FINAL THOUGHTS

Third-party breaches have impacted the most sophisticated users of top technology companies due to simple password reuse. Credential leaks will likely continue in frequency and volume, therefore, exacerbating the problem.

We highly recommend enforcing the use of a password manager inside your organization so all employees' passwords are unique to them and easily managed. Additionally, we also recommend that you enable two-factor authentication (2FA) for all internal and third-party accounts.

An increasingly large number of organizations are also obtaining breached third-party data to better protect their own employee and customer accounts from credential stuffing. This data allows them to proactively reset and monitor high-profile executives' and board members' online assets[12].

[12] https://www.troyhunt.com/random-thoughts-on-the-use-of-breach-data/

ABOUT SPYCLOUD

SpyCloud is a Breach Discovery & Alerting company headquartered in Austin, TX. SpyCloud was founded by information security experts who recognized a clear security gap resulting from the rise of data breaches and their impact on organizations of all sizes.

Our founders have worked in DoD, NSA, MIT, HP, iDefense, TippingPoint and other security firms with over 50 years of collective cyber security experience. Utilizing proprietary tradecraft, we recover stolen and breached data from private sources at very high volumes. 80% of the data that we acquire is unique, cannot be found by scanners, scrapers or web crawlers, and is currently in the hands of active threat actors.

Our platform alerts exposed customers through email or API well before normal breach notification timelines, improving their ability to mitigate harm against their most valued online assets.

Contact Information

Web: https://spycloud.com

Phone: +1 (800) 513-2502

Sales Inquiries: **sales@spycloud.com**

Press: press@spycloud.com

Appendix A: Underground Prices for Online Accounts

Industry	Hacked Account Site	Price per account Sold on the Dark Web
Social Media	FACEBOOK.COM	$2.00
	INSTAGRAM.COM	$1.00
	LINKEDIN.COM	$0.80
	PINTEREST.COM	$0.40
	TAGGED.COM	$1.00
	TWITTER.COM	$0.80
Shipping	DHL.COM	$2.00
	FEDEX.COM	$2.00
	UPS.COM	$2.00
	USPS.COM	$2.00
Dating Sites	CHEMISTRY.COM	$1.50
	EHARMONY.COM	$1.00
	FABSWINGERS.COM	$1.00
	MATCH.COM	$4.00
	MEETME.COM	$1.00
	OKCUPID.COM	$0.40
	OURTIME.COM	$1.00
	SENIORPEOPLEMEET.COM	$1.50
	TINDER.COM	$2.50
	ZOOSK.COM	$1.00
Finance/Ecommerce	BANKOFAMERICA.COM	Balance-dependent.
	HRSACCOUNT.COM	$5.00
	HUNTINGTON.COM	$2.50
	LENDINGCLUB.COM	$5.00
	MONEYGRAM.COM	$10.00
	SCHWAB.COM	$10.00
	SKRILL.COM	$3.00
	TDBANK.COM	$2.50
	BILL.COM	$2.50. With CC or Bank - $5.00
	DISCOVER.COM	$2.50
	ESSOEXTRA.COM	$3+0.1$ for each 100points
	ICSCARDS.NL	$2.50
	SQUAREUP.COM	$5.00
	VENMO.COM	$0.50
	WESTERNUNION.COM	unverified - $5. Verified - $15
	WORLDREMIT.COM	$2.50
	XOOM.COM	$0.50. + $2.50 with bank account
	PAYPAL.COM	$2.50
	WELLSFARGO.COM	$7.00
Hosting/Web Services	AWS.AMAZON.COM	With a cc - $4.50
	CLOUDFLARE.COM	$1.50
	DIGITALOCEAN.COM	no cc - $1.20. With a cc - $3.00
	OPENCART.COM	$1.00
	SHOPIFY.COM	$1.50
	TEMPLATEMONSTER.COM	$2.00
	WORDPRESS.COM	$1.50
Wireless/Email	ATT.COM	$4.50 with Wireless. $2.00 without Wireless. $9.00 with mail access
	BLACKBERRY.COM	$1.00

	COMCAST.NET	$1.00
	CRICKETWIRELESS.COM	$2.50
	H2OWIRELESSNOW.COM	$2.50
	PAGEPLUSCELLULAR.COM	$2.50
	PUMA.COM	$1.50
	ROGERS.COM	$1.50
	SPRINT.COM	$1.00
	T-MOBILE.COM	$2.50. With upgrade - $4.50
	TELUS.COM	$2.00
	TEXTNOW.COM	$1.00
	TRACFONE.COM	$2.00
	USCELLULAR.COM	$3.00
	VERIZONWIRELESS.COM	with upgrade - $4.50. With secret answer - $15.0
Travel / Points	AEROPLAN.COM	$0.50 below 5000 Balance. Higher: $0.00017391304 * Balance
	AIRBNB.COM	$1.50
	AIRMILES.CA	$2.00 + Balance * $0.031578947
	AIRMILESME.COM	$2.00 + $1.00 per 1000 miles
	ALASKAAIR.COM	no cc - $0.80. With a cc - $2.50. + $1 for 1000 miles
	ATLASCHOICE.COM	$2.50
	BOOKING.COM	$1.00
	BRITISHAIRWAYS.COM	$1.50. + $1.00 per 1000 mile
	CHEAPAIR.COM	no cc - $1.00. With a cc - $2.00
	CHEAPTICKETS.COM	$1.20
	EASYJET.COM	$0.80
	EXPEDIA.COM	$0.40. + 15% of points (3500 points = 25$)
	FLYSAS.COM	$0.20. + $0.50 for 1000 mile
	GWR.COM	no cc - $1.00. With a cc - $1.80
	HOUSETRIP.COM	$1.20
	INTERVALWORLD.COM	no cc - $0.80. With a cc - $2.50
	JETBLUE.COM	$1.50 + 0.5$ for each 1000 points
	KLM.COM	$1.00
	LUFTHANSA.COM	$0.50 for empty accounts or $0.00139130432 * Points
	MILES-AND-MORE.COM	$0.20. + $0.50 for 1000 miles
	ORBITZ.COM	$1.00
	SOUTHWEST.COM	$1.50
	STARWOODHOTELS.COM	$0.80 updated account
	TICKETNETWORK.COM	$1.50
	TRENITALIA.COM	$1.00. + 15% of points balance (1000 points = 5€)
	TRIPADVISOR.COM	$0.80
	VIRGIN-ATLANTIC.COM	$1.50. + $1 for 1500 miles
	VIRGINTRAINSEASTCOAST.COM	$1.50
	WESTJET.COM	$0.50. +10% of Balance
	WORLDSHOP.EU	$1.00. + 10% of miles (10000 Miles = 30$)
Retail	1STCHOICE.CO.UK	$1.50
	ACADEMY.COM	$1.50
	ACER.COM	$1.20
	ACETOOLONLINE.COM	$1.50
	ACMETOOLS.COM	$2.50
	ADORAMA.COM	no cc - $0.20. With a cc - $2.50
	ADVANCEAUTOPARTS.COM	$1.50
	AE.COM	$2.00
	AEROPOSTALE.COM	$1.50
	ALBEEBABY.COM	$1.50. + 10% of points (500 points = 5$)
	ALDOSHOES.COM	$1.50
	ALLMODERN.COM	$1.00
	ALLPOSTERS.COM	$1.50
	ALTERNATE.DE	$1.80
	AMERICANAPPAREL.NET	$1.50
	ANTHROPOLOGIE.COM	no cc - $0.80. With a cc - $2.00

	APPLE.COM	no cc - $0.20. With a cc - $2.50
	ARGOS.CO.UK	$1.50
	ARKTIS.DE	$1.80
	ARLT.COM	$1.80
	ASOS.COM	$1.50
	ASUS.COM	$1.00
	AUTOZONE.COM	$1.00
	BACKCOUNTRY.COM	$1.50
	BARNESANDNOBLE.COM	no cc - $1.00. With a cc - $2.00
	BARNEYS.COM	$1.80
	BASSPRO.COM	$1.50. + 10% of points (500 points = 10$)
	BEAUTY.COM	$1.50
	BEDBATHANDBEYOND.COM	$1.00
	BERGDORFGOODMAN.COM	$2.50
	BESTBUY.CA	no CC - $0.50. With a CC - $2.50
	BESTBUY.COM	no CC - $0.20. With a CC - $2.50. + 20% of Balance (Certificates). +
	BIKEBANDIT.COM	$1.50
	BJS.COM	$1.50
	BLOOMINGDALES.COM	no cc - $0.40. With a cc - $2.50. + 15% of Rewards balance
	BLUEFLY.COM	no cc - $0.80. With a cc - $2.50
	BODYBUILDING.COM	$1.50
	BOL.COM	no cc - $0.80. With a cc - $2.50
	BOOTS.COM	$1.50
	BREUNIGER.COM	$1.50
	BROOKSTONE.COM	$1.50
	BUILD.COM	$1.50
	BURBERRY.COM	$1.50
	BUYCOSTUMES.COM	$1.50
	BUYDIG.COM	$1.50
	C21STORES.COM	$1.50
	CABELAS.COM	no cc - 1.00. With a cc - 1.50. + 15% of cards (Points Available)
	CALVINKLEIN.COM	$1.50
	CAMPINGWORLD.COM	$1.50
	CAMPSAVER.COM	$1.50
	CANADIANTIRE.CA	$1.00. + 15% of Balance
	CANON.COM	with orders - $2.50; no orders - $4.00
	CARID.COM	$1.50
	CARS.COM	$1.50
	CARTERS.COM	no cc - $0.80. With a cc - $2.00
	CDISCOUNT.COM	$1.50
	CHAMPSSPORTS.COM	$1.50
	CHECKOUT51.COM	$1.00
	CHICOS.COM	$1.50
	CHILDRENSPLACE.COM	$1.50
	COLEHAAN.COM	no cc - $0.80. With a cc - $2.50
	COLUMBIA.COM	no cc - $0.80. With a cc - $2.50. + 10% of points (1000 points = 5$)
	COMPUTERUNIVERSE.NET	$1.80
	COMTECH.DE	$1.80
	COSTCO.CO.UK	$1.50
	COSTCO.COM	$1.00
	CRUTCHFIELD.COM	no cc - $0.20. With a cc - 2.50 ; + 15% of Points balance ; + 15% of
	CSL-COMPUTER.COM	$1.80
	CURRYS.CO.UK	$1.50
	DABS.COM	$1.50
	DAILYSTEALS.COM	$2.00
	DAVIDSBRIDAL.COM	$1.50
	DEBIJENKORF.NL	$1.50
	DELL.COM	no cc - $0.50. With a cc - $2.50
	DIAPERS.COM	$1.50

	DICKSSPORTINGGODS.COM	$1.50
	DINODIRECT.COM	$2.00. + 15% of balance
	DISNEYSTORE.COM	$1.50
	DRJAYS.COM	$1.50
	DRUCKERZUBEHOER.DE	$1.80
	DRUGSTORE.COM	$1.20
	DSW.COM	$1.50
	DYSON.COM	$1.50
	E-TEC.AT	$2.00
	EASTBAY.COM	$1.50
	EBAGS.COM	$1.50
	EBUYER.COM	$1.50
	ECSTUNING.COM	$1.50
	EDDIEBAUER.COM	$1.50
	ELV.DE	$1.80
	EPSON.DE	$1.80
	EREPLACEMENTPARTS.COM	$1.50
	ETSY.COM	$1.50
	EVINE.COM	no cc - $0.80. With a cc - $2.50
	EVO.COM	$1.50
	FAB.COM	$2.00. + 15% of balance (Available Credits)
	FANATICS.COM	$1.50
	FARFETCH.COM	$1.50. + 10% of balance
	FINGERHUT.COM	$1.50
	FOREVER21.COM	$1.50
	FRAGRANCENET.COM	$1.50
	FRAGRANCEX.COM	$1.50
	FRYS.COM	$1.50
	FULLCOMPASS.COM	$1.50
	GAMESTOP_RESET_PASS	with password reset - $0.10
	GAMESTOP.COM	no cc - $0.20. With a cc - $2.50 ; + 15% of Current Points balance ; + 15%
	GAP.COM	no cc - $0.80. With a cc - $2.50
	GARMIN.COM	$1.50
	GETDIGITAL.DE	$1.80
	GILT.COM	no cc - $0.80. With a cc - $2.00 ; + 15% of Balanc
	GNC.COM	$1.50
	GOPRO.COM	$1.50
	GRAVIS.DE	$1.80
	GUITARCENTER.COM	$1.50
	GYMBOREE.COM	$1.50
	HANNAANDERSSON.COM	$1.50
	HAUTELOOK.COM	$1.50. + 10% of balance
	HAYNEEDLE.COM	no cc - $0.80. With a cc - $2.50
	HELZBERG.COM	$1.50
	HM.COM	$1.5 no cc/$3 with cc
	HOMEDEPOT.COM	$1.50
	HOUSEOFFRASER.CO.UK	$1.50
	HOUZZ.COM	$1.50
	HP.COM	$0.40
	HSN.COM	$1.50
	HUGOBOSS.COM	$1.50
	IHERB.COM	$1.50
	INDIGO.CA	$0.20. + $0.00022222222 * Points
	INTERNATIONALTOOL.COM	$1.00
	IROBOT.COM	$1.50
	JARED.COM	$2.00
	JCREW.COM	$1.50
	JCWHITNEY.COM	$1.50
	JDSPORTS.CO.UK	$1.50

	JEGS.COM	$1.50
	JOESNEWBALANCEOUTLET.COM	$1.50
	JOMASHOP.COM	$1.50
	JOSBANK.COM	$1.50
	KAY.COM	$2.00
	KIJIJI.CA	$0.40
	KITHNYC.COM	$1.50
	KOHLS.COM	$1.50. + 10% of Balance
	LACOSTE.COM	$1.50
	LAMPENWELT.DE	$1.80
	LANDSEND.COM	no cc - $0.80. With a cc - $2.50
	LASTCALL.COM	$1.50
	LCBO.COM	$2.00; with AIR MILES NUMBER - $5.00
	LENOVO.COM	$1.50
	LLBEAN.COM	$1.50
	LOCCITANE.COM	no cc - $0.80. With a cc - $2.50
	LOFT.COM	$1.50
	LOGITECH.COM	$1.50
	LOUISVUITTON.COM	$1.50
	LOWES.COM	no cc - $0.20. With a cc - $2.50
	LUCKYVITAMIN.COM	$1.50
	LULULEMON.COM	$1.50
	MACCOSMETICS.COM	$1.50
	MACMALL.COM	$1.50
	MACYS.COM	$0.80
	MANGO.COM	$1.50
	MASSIMODUTTI.COM	$1.50
	MICHAELKORS.COM	no cc - $0.80. With a cc - $2.50
	MINDFACTORY.DE	$1.80
	MINIINTHEBOX.COM	$0.80
	MMOGA.COM	$2.00
	MOLESKINE.COM	$1.50
	MOOSEJAW.COM	$1.50
	MORRISONS.COM	$1.50
	MOTORCYCLE-	no cc - $0.80. With a cc - $2.50
	MOTOSPORT.COM	$1.50
	MRPORTER.COM	$1.50
	MUSICIANSFRIEND.COM	$1.50
	MUSIK-PRODUKTIV.DE	$1.80
	NEIMANMARCUS.COM	$1.00
	NET-A-PORTER.COM	$2.00
	NEWEGG.COM	$0.40
	NEXT.CO.UK	$1.50
	NFM.COM	$1.50
	NIKE.COM	$2 no cc/$5 with cc
	NIKONUSA.COM	$1.50
	NORDSTORM.COM	$2.00
	OCADO.COM	$1.50
	OFFICEDEPOT.COM	$0.40 all ; + 15% of Current Points balance ; + 15% of all Certificates
	ONLINESHOES.COM	$1.50
	OPTICSPLANET.COM	$1.50
	OSHKOSH.COM	no cc - $0.80. With a cc - $2.50
	OVERSTOCK.COM	$1.50
	PARTYCITY.COM	no cc - $0.80. With a cc - $2.50
	PATAGONIA.COM	$1.50
	PCM.COM	$1.50
	PCPLUS.CA	$0.50 below 5000 Balance. Higher: $0.00008695652 * Balance
	PCWORLD.CO.UK	$1.80
	PIZZAEXPRESS.COM	$1.50

	POTTERYBARN.COM	no cc - $0.80. With a cc - $2.50
	POTTERYBARNKIDS.COM	no cc - $0.80. With a cc - $2.50
	PSYCHOBUNNY.COM	no cc - $1.20. With a cc - $2.50
	PUBLICMOBILE.CA	$3+(points/10)
	PURITAN.COM	$1.50
	QUIKSILVER.COM	$1.50
	QUILL.COM	no cc - $0.80. With a cc - $2.50
	QVC.COM	no cc - $1.00. With a cc - $2.50
	QVCUK.COM	$1.50
	RAKUTEN.COM	$1.50. + 15% of points balance (1000 points = 10$)
	RALPHLAUREN.COM	$1.5 no cc/$3 with cc
	RAZERZONE.COM	$1.50
	REEBOK.COM	$1.50
	RESTORATIONHARDWARE.COM	no cc - $0.80. With a cc - $2.50
	REVOLVECLOTHING.COM	$1.50
	REVZILLA.COM	$1.50
	SAKSFIFTHAVENUE.COM	no cc - $1.00. With a cc - $2.00
	SAMSCLUB.COM	no cc - $1.00. With a cc - $2.00. + 15% of Balanc
	SAMSUNG.COM	$1.50
	SELFRIDGES.COM	no cc - $1.00. With a cc - $2.00
	SEPHORA.COM	$2.00 + 1$ for each 100point
	SHELLSMART.COM	$1.00. + 10% of Points (5000 Points = 25$)
	SHOEBUY.COM	$1.50
	SHOPRUNNER.COM	no cc - $0.50. With a cc - $2.00
	SHOPYOURWAY.COM	$1.50. + 10% of Points
	SKECHERS.COM	$1.50
	SOAP.COM	$1.50
	SOCCER.COM	no cc - $0.80. With a cc - $2.50
	SPORTSAUTHORITY.COM	$1.50
	SPORTSMANSGUIDE.COM	$1.50
	STAPLES.COM	no cc - $0.80. With a cc - $2.50
	SWANSONVITAMINS.COM	$1.50
	SWAROVSKI.COM	no cc - $1.50
	SWEETWATER.COM	$1.50
	TALBOTS.COM	no cc - $0.80. With a cc - $2.50
	TANGA.COM	$1.50
	TARGET.COM	no cc - $0.20. With a cc - $2.50. + 15% of Gift cards
	TENNIS-WAREHOUSE.COM	$1.50
	TESCO.COM	$1.00. + 15% of points balance (1000 points = 10£)
	TIGERDIRECT.COM	$0.40
	TOMS.COM	$1.50
	TOOLS-PLUS.COM	$1.50
	TOPCASHBACK.CO.UK	$1.00
	TOPSHOP.COM	$1.50
	TORRID.COM	no cc - $1.00. With a cc - $2.50
	TOWERHOBBIES.COM	$1.50
	TOYSRUS.COM	$1.50
	TUMI.COM	$1.50
	VENUS.COM	$1.50
	VICTORIASSECRET.COM	$2.00
	VISTAPRINT.COM	$0.50
	VITACOST.COM	$1.50
	VITAMINSHOPPE.COM	$1.50
	VITAMIX.COM	$1.50
	WALMART.COM	no cc - $0.20. With a cc - $2.50. + 15% of Gift cards. + 15% of Rewards
	WALMART.CA	no cc - $0.20. With a cc - $2.50
	WAYFAIR.COM	$1.50
	WILLIAMS-SONOMA.COM	$1.00
	WISH.COM	$1.00

	WORLDMARKET.COM	$1.50
	ZAPPOS.COM	$1.50
	ZARA.COM	$1.00
	ZULILY.COM	$0.80
	ZUMIEZ.COM	$1.50
Email Marketing	BENCHMARKEMAIL.COM	$5.00
	CONSTANTCONTACT.COM	$5.00
	DATA.COM	$1.80
	GMX.COM	$0.80
	ICONTACT.COM	$1.50
	MAILCHIMP.COM	$5.00
	MAILGUN.COM	$5.00
	MANDRILLAPP.COM	$10.00
	SENDGRID.COM	$5.00
	ZOOMINFO.COM	$1.50
Entertainment	CBSSPORTS.COM	$1.50
	CRUNCHYROLL.COM	$1.00
	DAILYMOTION.COM	$1.50
	FILMON.COM	$1.50
	HULU.COM	$4.00
	MLB.COM	$1.00
	NBA.COM	$1.50
	NETFLIX.COM	no cc - $1.50. With a cc - $3.00
	NHL.COM	$1.50
	TALKTALKTVSTORE.CO.UK	$1.50
	WWE.COM	$1.50