New and Old Techniques in the Fight Against Credential Stuffing

Forkbombus Labs
reports@forkbomb.us
August 2017

Abstract

Credential theft is a known issue, and it is compounded by credential stuffing - that is, automatically compromising accounts by utilizing credentials that have been reused between services. Existing techniques for detection and prevention have been shown to have multiple weaknesses. They can be circumvented, and although they can disrupt attack chains, these disruptions are temporary rather than conclusive. In this paper we will describe credential stuffing, list common methodologies to combat it, and introduce a better means to detect, prevent, and respond to it. As threats become more sophisticated, teams must become aware of emerging approaches to thwart them. This new technique combines existing technologies with attribution, so as to better tie together all stages of the threat.

1. Introduction

One of the greatest threats to consumers and corporations alike is the use of stolen user credentials. The commoditization of cyber-crime has dramatically increased the demand for access to stolen accounts. Public breaches of ubiquitous services like Yahoo!, Myspace, Tumblr, and Dropbox have made compromised accounts more accessible than ever.

Attack motivations such as spam, theft, fraud, espionage, and business email compromise all benefit from the apparent legitimacy provided by a compromised identity.[1] From online gaming accounts and on-demand video streaming, to finances and health care, hackers have found a way to monetize nearly every form of online identity. The increase in market demand and the ease of accessibility have made credential stuffing attacks more prevalent and costly than ever before.

While traditional reactive defenses perform well at identifying and preventing technical exploitation techniques, they often struggle to identify credential-stuffing attacks which masquerade as legitimate traffic. This shift in the attack landscape demands new defensive techniques and strategies.

In this paper, we discuss the life cycle of credential stuffing, including the acquisition, verification, sale, and use of stolen credentials. We then cover traditional defenses used against credential-stuffing attacks. Lastly, we explore how defenders can employ deception technologies and attribution methodologies to combat credential-stuffing attacks.

2. What is Credential Stuffing?

Credentials are sets of information - including but not limited to usernames, passwords, tokens, and personal identification numbers - that are used to authenticate someone's or something's identity. “Credential stuffing” is the automated injection of credentials which are known to be, or are suspected to have been, valid with some service X, against another service Y, in **an** attempt to identify accounts

[1] http://www.computerworld.com/article/2874207/attacks-using-stolen-credentials-are-on-the-rise.html

which use the same credentials; these services include, but are not limited to, social media, entertainment, healthcare, and financial services.[2] Ultimately, credential stuffing is enabled by password reuse, which has been a known issue for some time.[3] Unfortunately, this is a social vulnerability, not a technical one, and thus has no easy solution. Even the technically inclined are not immune to this vulnerability (as highlighted by the 2012 Dropbox credential spill).[4]

With new credential lists beings leaked daily, plentiful open proxies, VPNs and botnets for hire,[5] and simple tools for automating attacks, credential stuffing is nearly effortless, with minimal cost of entry and high reward. The trend towards commoditizing cyber crime ensures these credentials are often sold online for a fraction of their true value. The market in stolen credentials is growing every year, and proves to be a costly threat to organizations and their users.[6] From tarnished reputations, to the cost of incident response and consumer identity protection, credential theft proves to be one of the most costly attacks an organization may face.[7]

[2] https://www.owasp.org/index.php/Credential_stuffing

[3] https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/

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

[5] https://krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet/

[6] https://threatpost.com/password-breaches-fueling-booming-credential-stuffing-business/125900/

[7] http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

2.1 Where do the credentials come from?

Credentials used in credential stuffing attacks are acquired from sources where they are known to be valid, or suspected to once have been. Most commonly, this is achieved by attacking services and pilfering their users' credentials. Alternatively, attackers may purchase the already-plundered information from other attackers. They may also use credential lists found posted on forums and pastebins by people hoping for credence within hacking communities (or, sometimes, for revenge).

2.2 How are credential-stuffing targets chosen?

With credentials for accounts in financial verticals demanding the highest price tags, lower-priced credentials for accounts in verticals such as entertainment still yield a decent payoff. Attackers must take into consideration the levels of security which different services and verticals implement, and calculate cost/reward ratios. When there are defenses against credential stuffing, this prolongs the operation and increases the initial cost of performing the attack, thereby reducing an attacker's return on investment of both time and money.

2.3 How are credential-stuffing attacks performed?

The heart of a credential stuffing attack lies in the tools used to facilitate the automated logins. While many tools, such as Sentry MBA or Vertex can be used "off the shelf" and offer community support and configurations, some attackers still choose to write their own tools. Attackers must also hide the fact that their authentication attempts are not sourced legitimately. For this, they often use proxies.

Proxies can be public and free, commercially available via subscription (e.g., VPNs), or illegal (e.g., botnets). Attackers must weigh the proxy's reputation versus the target's security posture. Hosts listed as public proxies are obvious risks even to the most immature security teams, while hosts within the target's service area can go unnoticed by even the most sophisticated defenses. Residential and small business hosts - a treasured resource - are increasingly accessible to attackers. This is in part thanks to the popularization of Internet of Things devices - which are riddled with default passwords and trivial vulnerabilities.

Regardless of which path an attacker chooses, the process is the same: start with a list of credentials suspected to be legitimate elsewhere, attempt to validate them on the target, and output a list containing only those which have been successfully validated. These plentiful proxies, combined with tools like Sentry MBA and Vertex, make credential stuffing easier, more common, and more potent, than ever before.

2.4 Why is credential stuffing performed?

There are numerous motivations behind credential-stuffing attacks. Perpetrators may sell the discovered credentials, or use them directly. Some examples of how stolen accounts may be used are:

- Theft of funds from users of financial services
- Laundering of funds through marketplace services
- Higher-reputation spam sent through personal email accounts or social media
- Gaining initial - or deeper - access to an organization
- Cheap access to on-demand media or online games

Regardless of the type of service a credential is valid for, it's critical that the sold credentials are actually valid. For resellers of stolen credentials, having an impressive reputation is paramount. Selling invalid credentials creates distrust from the purchasers and the greater community, directly impacting the amount they can charge per credentials. Invalid credentials also result in more work for sellers, who must re-engage with mistrustful purchasers; as well, their ROI is directly impacted, because they must invest increased human capital.

2.5 Global impact of attacks

Market demand has made compromised credential lists more accessible, and the tools which facilitate credential stuffing attacks are lowering the cost of entry. This availability increases the risk to consumers and corporations alike. To defend against credential stuffing, areas which contain an authentication mechanism now must distinguish between legitimate login events, and those masquerading as such. The types of defenses employed to detect these anomalies are much costlier than the standard detection-and-prevention techniques of technical exploits, and require constant upkeep to maintain.

Detection and prevention of attacks are costly, and so is remediation. In 2016, online backup provider Carbonite, in response to mass credential-stuffing attacks, forced a password reset for its >1.5 million users.[8] This response may not be considered costly in

[8] https://www.databreaches.net/carbonite-forces-password-reset-after-password-reuse-attack/

terms of direct labor by Carbonite, but it hindered their business continuity, and severely frustrated their users. Aggravating though it might be to require all users to reset their passwords, the repercussions of falling victim to credential stuffing can be worse. In 2012, attackers gained the credentials of a Dropbox employee, entered the corporate database, and stole the credentials of over 60 million users.[9]

Credential stuffing is an attack which primarily targets the end user accounts of a victim organization, and depending on laws may require public disclosure.[10] Despite the expenses of responding to a data breach (e.g., remediation, and consumer identity protections), perhaps the greatest cost to an organization is the potential loss of public trust.[11]

End users themselves also face troubles and costs from accounts taken over by credential stuffing. One scheme saw attackers taking over Amazon merchant accounts and replacing sellers' bank routing information with their own, allowing attackers to have the funds of sales deposited directly into their accounts.[12] In another, attackers compromised Apple iCloud and email credentials, and held the end users' personal data for ransom.[13]

3. Traditional Defenses Against Credential Stuffing

As credential stuffing attacks become more sophisticated and accessible, traditional reactive detection-and-prevention methodologies are failing to meet the demands of determining if authentication attempts are legitimate or simply masquerading as such. With business continuity as a top consideration, organizations are rightfully concerned with implementing even stricter prevention methodologies, especially when safeguarding areas of high user traffic. As the traditional response of blocking suspicious activity has become a last resort, new defenses which target all layers of an attack are required to protect organizations and their users.

3.1 Credential Enforcement

The core vulnerability which credential stuffing exploits is password reuse: the fact that many users will use the same credentials across multiple services. In 2010, Trusteer found that more than 73% of online banking users also used the same passwords on non-financial related services. Furthermore, 47% used both the same user identifiers as well as passwords elsewhere.[14] This bad habit can directly be combatted by educating users. Informing users of the risk and dangers associated with password reuse, and equipping them with the appropriate practices and tools can directly lead to securer environment.[15] Another way to directly defend against password reuse is to *use* credential enforcement standards,

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

10 https://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/databreach.html

11 http://investors.fireeye.com/releasedetail.cfm?ReleaseID=970718

12 https://www.infosecurity-magazine.com/news/hackers-count-on-password-reuse-in/

13 https://www.the-parallax.com/2017/04/07/apple-ransom-credential-stuffing/

14 https://www.trusteer.com/en/news/press-release/trusteer-finds-two-thirds-internet-users-reuse-their-online-banking-credentials

15 https://securityintelligence.com/its-time-for-users-to-pony-up-and-quit-reusing-passwords/

such as password lifetimes, requiring users to choose new distinct passwords at each change, and ensuring a user's chosen passwords are not well known.

Implementing password lifetimes helps to ensure passwords across services have less of a chance of overlapping. If the credentials obtained from a compromised website were last updated years ago, while those credentials of a targeted service were recently changed, there's less of a chance of password reuse having occurred. This is especially true when services enforce new password policies, ensuring that when a new password is chosen, it doesn't match one previously used. Services which implement these new password requirement policies may even serve to condition users to adopt these habits elsewhere.

3.2 CAPTCHAs

A fairly common defence most users are familiar with is the use of CAPTCHAs are challenges presented to users which are intended to be reasonably easy for humans to solve, while being expensive for computer algorithms.[16] CAPTCHAs have seen wide adoption by services which wish to distinguish between automated connection attempts, and those which represent users. Services have adopted this defense not only alongside user authentication attempts, but also for functionalities like search or access to semi-confidential data (e.g., organizational contact details).

While largely effective when first introduced, numerous attacks have since been developed against CAPTCHAs. These attacks include 'click farms' (cheap laborers - often in the third world - being presented with the CAPTCHAs to solve), advances in computer vision, and - for audio CAPTCHAs designed for the visually impaired - speech recognition software.[17] [18] Some automated credential-stuffing tools include CAPTCHA solvers built in.

3.3 Multi-Factor Authentication

Multi-Factor Authentication (MFA) is authentication via multiple pieces of proof of identity. Pieces of proof supplied for authentication typically fall under one of three categories.

A. Something the user *knows* (e.g., Usernames, Passwords, PIN)
B. Something the user *possesses* (e.g., Security Tokens, Identity/Key Cards)
C. Something the user *is* (e.g., Fingerprints, Retina, Finger Veins[19])

Most commonly today, MFA implementations are known as Two-Factor Authentication (2FA). The first factor is something that the user knows, and the second factor is typically something in the user's possession (e.g., an RSA SecurID token[20], a phone app authenticator[21], or a shared secret sent via e-mail or SMS).

While MFA may stop attacks that could penetrate a single layer of protection, it is too commonly implemented in ways which may lead to the

16 https://www.cylab.cmu.edu/partners/success-stories/recaptcha.html

17 https://www.blackhat.com/docs/asia-16/materials/asia-16-Sivakorn-Im-Not-a-Human-Breaking-the-Google-reCAPTCHA-wp.pdf

18 http://www.zdnet.com/article/inside-indias-captcha-solving-economy/

19 https://www.google.com/patents/US7526111

20 https://www.rsa.com/en-us/products/rsa-securid-suite

21 https://techcrunch.com/2010/09/20/google-secure-password/

disclosure of whether the first factor succeeded or failed. For instance, many sites only display the next layer of authentication if the first layer has been successfully passed. Disclosure of the first factor's validity may be enough for an attacker to target the user directly via (for example) spear-phishing techniques.[22] [23]

3.4 Credential Monitoring

At the core of every credential stuffing attack is a list of credentials that an attacker uses in attempts to authenticate with services. While attackers are constantly seeking new credential lists to use, defenders can use those same lists as part of monitoring and enforcement. By acquiring credential lists, defenders can compare the found credentials to those of their users, and require affected users to update their accounts with new identifiers (e.g., passwords).

Credential monitoring requires substantial involvement from defenders, who must constantly watch for new breaches and proactively work to obtain the credentials lists before they can be used maliciously. There are a great many sources to monitor, with many requiring that participants first be vetted and/or undergo initiation. Even with access, new credentials lists are typically only sold to a limited number of buyers -- not to mention the issues of liability, risk, and knowingly purchasing stolen goods.

Defenders must then run tests of the discovered credentials against their users' information. This testing may not be entirely straightforward, as credential dumps may contain encrypted or obfuscated data, making it more difficult for defenders to compare it against their own users' information. Furthermore, defenders must proceed cautiously in taking defensive action based on discovered credentials, as repeatedly requiring users to update their information may introduce unnecessary frustrations and disrupt business continuity.

3.5 Credential Canaries

Credential Canaries are invented credentials which are placed in lists, or otherwise disseminated, specifically to track their usage. Because a credential canary will never come from a legitimate user, its presence is a true positive indicator of a credential stuffing attack, regardless of how else the attack may be disguised.

Canaries can be introduced into credential sources in various ways. Known credential lists can have canaries added to them, and then be reintroduced into public and private sources (pastebins, web forums). Canaries may be supplied to specific individuals with the intent that they will either resell them or use them directly. Canaries can also be placed on 'honeypots' - systems which have been deliberately configured to be vulnerable to attack. Such canaries can be tied to specific incidents, providing further insight into attacks and offering the ability to track specific attackers beyond individual incidents.

The use of canaries has multiple disadvantages. Firstly, canaries must be distributed and tracked. This is a very involved process which requires a large

---

22 https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/

23 https://twitter.com/maccaw/status/739232334541524992/photo/1

amount of effort, and which is difficult to automate, making it very expensive. Defenders need to identify the locations where their canaries are likely to be used against them. And even once the locations are identified, nothing will happen if the attacker does not trust the canaries blindly but instead researches their provenance. This is especially true when canaries have been added into publicly-available lists of which canaryless versions still exist. In such cases, it is trivial for attackers to cross-reference known sources and identify the user who introduced the canary.

3.6 Detecting proxies and Virtual Private Networks

Proxies and Virtual Private Networks (VPN) allow attackers to spread their digital footprint across many hosts, masking their true source. In credential stuffing, attackers often use many proxies and/or VPNs to hide the fact a single entity may be responsible for the large number of login attempts involved in an attack. Proxies and VPNs are widely available on the internet, both free and subscription. They can also be installed and configured on compromised devices, providing private connections.

Proxies and VPNs are often easily identified by publicly visible information, such as hostnames, whois information, service identifiers, or open ports. That said, it is important to note that proxies and VPNs have numerous legitimate uses; their presence is not necessarily an indicator of malice. Individuals may use them for privacy reasons, and organizations may use them for caching or security monitoring. As such, defenders may find it more trouble than it's worth to block proxy-sourced activity. Even when a given proxy is identified as the source of malicious activity, it may simultaneously be in use by legitimate users.

If one disregards concerns of business continuity, then defenders who have identified a proxy or VPN can simply block its Internet Protocol (IP) address and/or domain name. However, as illustrated by the Pyramid of Pain, a blocked IP Address is one of the easiest blocked resources for an attacker to overcome.[24] This may disrupt an attack, but not terminate it. In fact, it can be more work for a defender to block an IP address or domain name than for an attacker to switch to a new one. Moreover, blocking the address or domain name can tip off the attacker that they have been detected, which may cause them to adjust more variables than just their IP address or domain name, and ultimately make them harder to spot next time.

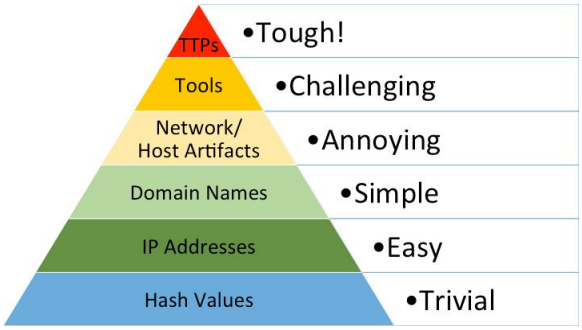

Figure A. The Pyramid of Pain [24]

3.7 Botnet Tracking

Botnets allow an attacker to spread their footprint across many hosts, like proxies and VPNs. However, botnets tend to be harder to discern from legitimate connections. Proxies and VPNs, by their very nature, must accept remote connections and then pass along traffic from those connections; typically there is some

[24] https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

form of identifier. Botnet-infected machines typically connect outwards to a central location, making them hard to discern from the basic reconnaissance defenders will perform. By monitoring botnets, defenders can gain great insight into credential-stuffing attacks, sometimes even before they engage the intended target.

Botnet tracking involves monitoring the command and control (C&C) traffic which controls the bots. This grants insight into what the botnet is being used for, who it is attacking and how, and multiple other aspects. There are several ways to monitor botnet C&C traffic, depending on the communications protocol it employs; for instance, one can reverse-engineer the botnet malware, and then create software to connect to the C&C and passively observe the commands. An easier way, however, involves infecting a machine while monitoring its network activity; this removes the overhead of having to reverse-engineer the malware and build compatible observers. As well, by controlling the network in which the infected machine resides, defenders can redirect attack traffic away from intended targets and into deceptive targets, and thereby control the flow of information which the attacker receives. Once the attack's heuristics have been ascertained, the intended targets can be alerted, allowing them to employ appropriate defenses, and thereby block the connections with a higher degree of confidence that they are illegitimate.

Tracking botnets is complex, and does not always produce the desired results. They may be used for various reasons, and the only way to tell which reason is being used is to observe it. To observe a botnet's activity, defenders must first observe the propagation of the infectious malware. The botnet must then be observed at all times, in order to identify attacks as they occur. Defenders must also hide their presence from attackers, who may exclude them from the nets. This quickly becomes cumbersome for even the most resourceful defenders, and the return on investment is often considered too little for organizations which are only concerned with their own standings.

4. Combining Deception and Attribution

Traditionally, defenses against cyber crime have extremely technical solutions. In response, attackers have begun attacking the undefended human element; defenders have just recently begun to leverage the attackers' own human element. In Forkbombus Labs’ research, employing deception against attackers has been a valuable asset in the collection phase of the threat intelligence lifecycle. Several of the defenses outlined in section three contain a deceptive component; some beneficial outcomes of these defenses are outlined below. Deception can increase confidence in attack alerting and attribution, while allowing defenders to control the flow of information.

Attribution is key when defending against cyber attacks, and is sought by defenders. However, it is not easy to accomplish, especially in environments with a reactive security posture. Threat intelligence is vital when pursuing attribution, and little information is gleaned when attacks go according to the attackers' plan.

Attackers succeed by manipulating environments out of their operational guidelines, while defenders

succeed by manipulating attackers out of theirs. Deceptive defenses enable defenders to manipulate the environment with which an attacker is engaging, ultimately controlling both the flow of information to the attacker, and the attack itself. When attackers lose control of their attack, they begin to behave in ways that they had not planned, disregarding their own operational security, and often divulging more information about themselves. This information directly leads to stronger and higher confidence attribution, and enables root cause mitigation.

In the arms race that is cyber security, new attacks and new defenses are created every day. However, it's much easier for an attacker to figure out how to circumvent a new defense, than it is for defenders to research, develop, and employ one.[25] Instead of continuing the seemingly perpetual fight in the cyber domain, attribution brings the fight into the physical domain. By bridging the physical and cyber domains, the possibility of Root Cause Mitigation is introduced, preventing today's threats from becoming tomorrow's.

4.1 Key Benefits

Proactive deception tactics and attack attribution offer several benefits over traditional reactive detection-and-prevention methodologies. Ultimately, whoever controls the flow of information, controls the attack. Deception introduces the ability to directly alter the information an attacker receives, giving defenders many new opportunities and advantages.

Using deception to defend against credential stuffing attacks, defenders can directly affect an attacker's ability to perform. By deceiving attackers, supplying them with false information, and tricking them into believing their attacks are successful, defenders ultimately raise the cost for a successful attack. Providing attackers with falsified information causes them to distrust their own capabilities, causing frustration. When this falsified information is introduced to third parties, such as the purchasers of stolen credentials, those third parties begin to distrust the attacker. This distrust directly affects an attacker's ability to profit from these attacks, and hinders their reputation within their communities.

Traditional methods of detection and prevention are highly visible to attackers, allowing them to adjust, compensate, and continue attacking. Depending on the adjustments that an attacker makes, defenders may completely lose track of the attack. Deception defenses allow defenders to covertly control the attacks, so that attackers believe everything is going as planned even though their attack has been rendered useless.

Defenders may also benefit from the increased intelligence acquired through the observation of an attack; this can also provide defenders with deeper insight into how attacks are being performed, and potentially allow them to devise new defenses against uncovered resources and capabilities. This intelligence can also be used to perform attribution - that is, relating attacks together to track how an attacker's capabilities, motives, and resources have evolved over time (and, on occasion, personally identifying attackers). Deceiving attackers into divulging this intelligence directly enables root cause mitigation, removing their access to the resources they require to commit their crimes.

25 https://threatpost.com/defenders-adapt-offensive-techniques-continue-evolve-041113/77722/

4.2 Disrupting the Chain

While traditional reactive defenses may block attacks as they occur, they seldom discourage the attackers from continuing with their endeavors. Proactive deception tactics enable defenders to mitigate attacks as they occur, and discourage attackers from continuing. Deception tactics help defenders to expose an attacker's resources and capabilities. This allows defenders to identify distinct defensive opportunities, such as working with service providers or law enforcement to remove an attacker's access to specific resources.

Deception also gives defenders the opportunity to end the attack prematurely, by persuading the attackers that the mission is complete. Attackers who believe that they've succeeded may move on to something else.

4.3 Root Cause Mitigation

Traditional reactive detection-and-prevention methodologies allow attackers to identify the weak points of their attacks (i.e., those points which defenders leverage), make the necessary changes, and try again later. Root Cause Mitigation is the practice of disrupting attacks as close to the source as possible by limiting an attacker's access to a resource, such as servers, domain names, botnets, or even the internet as a whole.

Deceptive tactics assist in the attribution of attackers, and attribution assists in root cause mitigation. The Cyber Security industry today largely focuses on the cyber component of cyber crime, but ignores that the actions are themselves criminal. Attribution directly enables the global law enforcement community to formally accuse, arrest, try, and convict identified attackers. While attackers can overcome the obstacles introduced by removing access to their resources, a formal accusation and conviction is the only method proven to stop attackers definitively, ensuring they don't return to attack again.

4.4 Use Case

A common deception tactic to employ as a defense to credential stuffing is the controlled affirmation of credentials which are actually invalid. When attackers believe invalid credentials to be valid, credential stuffers are severely inconvenienced. These invalid credentials enable many new possibilities for defenders; for instance, they can be used as credential canaries, to be tracked for attribution, and for further defensive actions. Additionally, providing attackers with false positive credentials damages their morale and customer relationships.

Purchasers of such invalid credentials will often try to dispute the transaction, and sellers will suffer from tarnished reputations. To sellers on illicit markets, reputation is everything,[26] bad reviews directly harm their ability to profit from their attacks, as lower-reputation sellers are not able to demand higher prices for their illegally-obtained data.[27]

Another defensive maneuver, and one which is hidden from the attacker's view, is a deceptive login portal which facilitates the false affirmation of spurious credentials. When attackers believe their efforts are progressing normally, any false positive

[26] https://motherboard.vice.com/en_us/article/gvy5b9/what-ive-learned-as-an-internet-drug-dealer

[27] https://arxiv.org/pdf/1703.01937.pdf

response directly increases their cost to perform the attack successfully. With increased costs to perform credential stuffing, and decreased revenues from selling false positive credentials, attackers' return on investment is minimized - and as the return on investment dwindles, and reputations are tarnished, credential stuffing attacks become less worthwhile an endeavor for attackers.

5. Conclusion

Credential stuffing is a costly and growing threat which affects organizations and end users alike. Since credential stuffing is predicated on the social vulnerability of password reuse, defending against it can prove difficult, time-consuming, and costly. The traditional detection-and-prevention methodologies used in the defense of technical vulnerability have little effect on credential stuffing. While some of these defenses have better results than others, they are often time-consuming and resource-intensive; ultimately, they keep attackers informed of defensive maneuvers, which allows them to stay one step ahead of the defenders.

Whoever controls the flow of information controls an attack. By utilizing deception, defenders are able to control the information their attackers are receiving and acting upon. This enables defenders to fight credential stuffing in new ways, reducing their own costs while directly increasing those of the attacker, and ultimately having a negative impact on the viability of credential-stuffing attacks.

There is one constant behind every cyber attack: the human element. No computer performs an attack without first being instructed by a human to do so. Deception enables defenders to manipulate attacks and control attackers. This gives defenders the opportunity to learn more about the attackers, by observing how they react to specific situations. Defenders can use this level of control to encourage attackers to divulge intimate information, lowering the costs of attribution (of an attack to specific attackers, of attackers to resources, and even of attackers to personal identities). This level of attribution directly enables root cause mitigation, the ultimate defensive action. Attribution-enabled defenses allow defenders to gain the deep intimate intelligence to defend against attacks as they occur, while enabling law enforcement to conclusively stop the responsible parties from committing these crimes.

5.1 Hivemind

The Hivemind Platform contains the world's first Learning Dynamic Deception Honeynet. Hivemind sensors communicate with one another to learn attackers' motivations and capabilities, dynamically altering their appearance to offer the most enticing target for those attackers. In addition to client-sponsored sensors, Forkbombus Labs maintains a global network of Hivemind sensors which are constantly disrupting attacks and deceiving attackers into divulging their most intimate details, including their methodologies, motivations, and even identities.

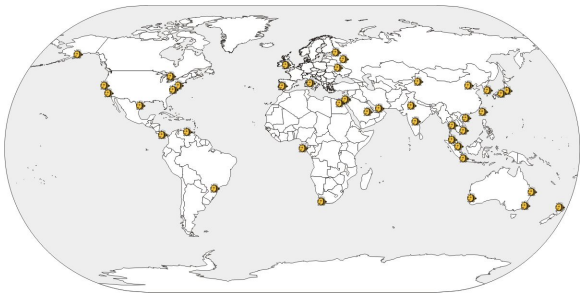

Figure B. Map Indicating Several Hivemind Sensor Locations

Hivemind sensors actively detect and respond to numerous attack classifications, including but not limited to proxy identification and botnet propagation. With sensors across the globe, Hivemind has extended awareness of attacks affecting a plethora of locations and market verticals (Figure B). Hivemind sensors perform long-term incubation of observed malware, gaining visibility into the inner workings of botnets and their controllers. By inserting themselves as bots, Hivemind sensors are capable of redirecting intended attack traffic to their own dynamic deception engines, enabling an unparalleled deceptive depth. In the case of credential stuffing, Hivemind sensors are able to dynamically emulate the intended target and begin introducing fraudulent successes to the attackers, tainting their results and hindering their efforts. Hivemind provides the best defense in the industry against credential stuffing.

6. References and Further Reading

1. http://www.computerworld.com/article/2874207/attacks-using-stolen-credentials-are-on-the-rise.html
2. https://www.owasp.org/index.php/Credential_stuffing
3. https://www.troyhunt.com/password-reuse-credential-stuffing-and-another-1-billion-records-in-have-i-been-pwned/
4. https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/
5. https://krebsonsecurity.com/2011/09/rent-a-bot-networks-tied-to-tdss-botnet/
6. https://threatpost.com/password-breaches-fueling-booming-credential-stuffing-business/125900/
7. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf
8. https://www.databreaches.net/carbonite-forces-password-reset-after-password-reuse-attack/
9. https://techcrunch.com/2016/08/30/dropbox-employees-password-reuse-led-to-theft-of-60m-user-credentials/
10. https://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/databreach.html
11. http://investors.fireeye.com/releasedetail.cfm?ReleaseID=970718
12. https://www.infosecurity-magazine.com/news/hackers-count-on-password-reuse-in/
13. https://www.the-parallax.com/2017/04/07/apple-ransom-credential-stuffing/
14. https://www.trusteer.com/en/news/press-release/trusteer-finds-two-thirds-internet-users-reuse-their-online-banking-credentials
15. https://securityintelligence.com/its-time-for-users-to-pony-up-and-quit-reusing-passwords/
16. https://www.cylab.cmu.edu/partners/success-stories/recaptcha.html
17. https://www.blackhat.com/docs/asia-16/materials/asia-16-Sivakorn-Im-Not-a-Human-Breaking-the-Google-reCAPTCHA-wp.pdf
18. http://www.zdnet.com/article/inside-indias-captcha-solving-economy/
19. https://www.google.com/patents/US7526111
20. https://www.rsa.com/en-us/products/rsa-securid-suite
21. https://techcrunch.com/2010/09/20/google-secure-password/
22. https://www.wired.com/2016/06/hey-stop-using-texts-two-factor-authentication/
23. https://twitter.com/maccaw/status/739232334541524992/photo/1
24. https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
25. https://threatpost.com/defenders-adapt-offensive-techniques-continue-evolve-041113/77722/
26. https://motherboard.vice.com/en_us/article/gvy5b9/what-ive-learned-as-an-internet-drug-dealer
27. https://arxiv.org/pdf/1703.01937.pdf