Exploring the use of Stolen Credentials in Digital Forensics

Leonard Melnik
Pat Velez
Shantoye Reid
Kai Xiang Lin
Anna Huang

I. Introduction

A. What is digital forensics and what are stolen credentials.

Digital forensics is the branch of forensic science that identifies, acquires, processes, analyzes, and finally reports on digital information (Interpol) . Digital forensics can be used to analyze data to determine actions that were taken on a device as well as any intention and sometimes the identity of the individual responsible for the actions.

Before we discuss stolen credentials, let us discuss credentials. Normally credentials are something like an accomplishment, such as a degree etc, if someone has credentials for a given topic it “proves” that they know the topic. Knowing is one of the most used methods of authentication, in our case though what we know is a unique set of identifiers like a username, email, and password which gives us authority to act. Everyone who uses the internet has credentials, you have them for your computer, for your internet access, and for every account on every website.

Stolen credentials are when those unique identifiers are in the hands of someone not authorized by the initial party. They can be stolen in a multitude of ways. Once they are obtained they can be used to access an individual's accounts (bank, email, social media) and get access to further information. These credentials can be used to carry out fraudulent activity which we will discuss later.

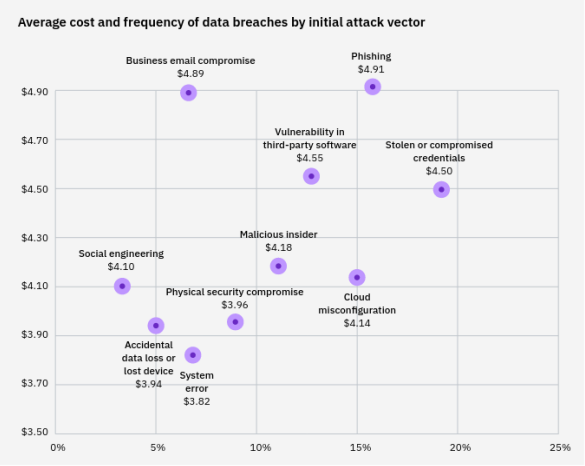


Figure 11: Measured in USD millions

As you can see from the graph to the left, stolen or compromised credentials were the most frequent

attack vector to breach a company (“Cost of a data breach 2022”). Which can indicate to a digital forensics investigator to look into if stolen credentials were the primary attack vector.

B. What are the methods that stolen credentials are initially acquired

1. Database breaches

A breach occurs when a central trusted party (such as a service or website) is hacked in some way or another, this often results in the hackers accessing customer data and credentials. It used to be the case that companies would store users' passwords in cleartext, but these days that is less and less common as the passwords are stored as hashes. Even though the hashes are not reversible, hackers can use various methods (rainbow tables, dictionary attacks, etc…) to de-hash (in a sense) the passwords.

2. Remote Access Trojans/ other stealer malware

Viruses are installed on computers manually or by accident, usually starting with a phishing attack and manipulating victims into downloading malware or trojan viruses. These viruses can then grab all the stored passwords from web browsers.

3. Phishing attacks

A fake email or website is set up where the victim thinks it is a legitimate source. They then enter their PII or credentials onto the site.

C. What are the methods that digital forensics and law enforcement can acquire these credentials

There are many forums and marketplaces where hackers and malicious actors trade and sell stolen credentials and other data. Many times the compromised data is free to download if an account is made and the account is active on the forums. Digital forensics investigators and law

enforcement can create accounts and just monitor the forums for when new data is released. By keeping up to date, they can also be aware of where the information was hacked from, potentially allowing for prevention by notifying the victims as soon as the data becomes public. While this process is manual it can be automated to a certain extent using web scrapers and other tools to minimize the effort and increase data ingestion.

Since stolen credentials are so prevalent, there are also services and companies that compile the data and allow searching (such as Dehashed). While the ethics of this is questionable, it is within the law and this service is used by companies and governments worldwide.

Both when creating accounts for forums and for private group chats, it is important to create a sockpuppet so that the identity of the investigator is not known. Additionally a sockpuppet can be helpful because it indicates history which leads to forums and hackers trusting more.

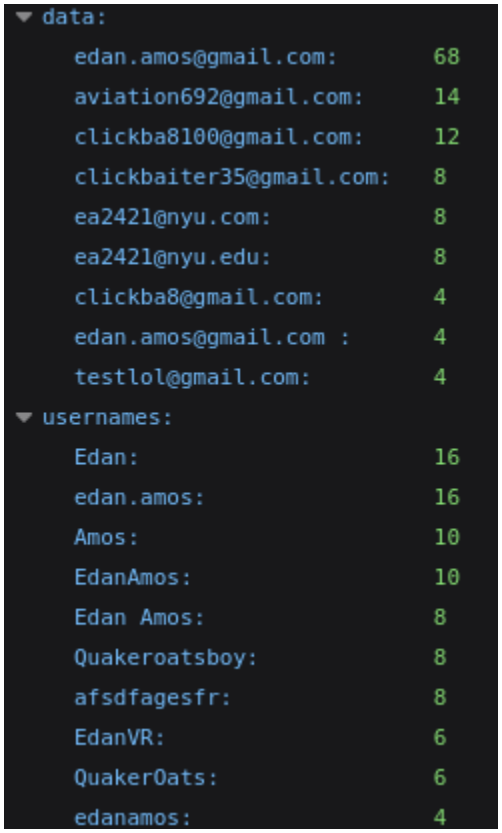
II. Benefits of Credentials in Digital forensics

A. Gathering Stage

51% of people use the same password for work and personal accounts. 78% of Gen-Z users use the same password for several online accounts. (“Save Your Data with These Empowering Password Statistics”). What this indicates is that if we are able to identify one password a person used, it is highly probable that they re-used this password at least once. Digital forensics investigators can use this as an opportunity to see any other stolen credential

pairs where the password has also been used, revealing other emails or aliases that were used by the target.

To show an example, we acquired data from a compilation of RAT logs posted on the now defunct Breached.vc. This compilation contained approximately 121 million records. After analyzing it, we were able to find a lot of alternate accounts used by individuals due to their unique passwords. To show an example we reached out to one of the victims and asked for their permission to demonstrate in this paper.



Just with one password, we were able to reverse search and find many alternate emails and usernames that the victim used. This same method can be used to understand what data to get and from where when investigating a target.

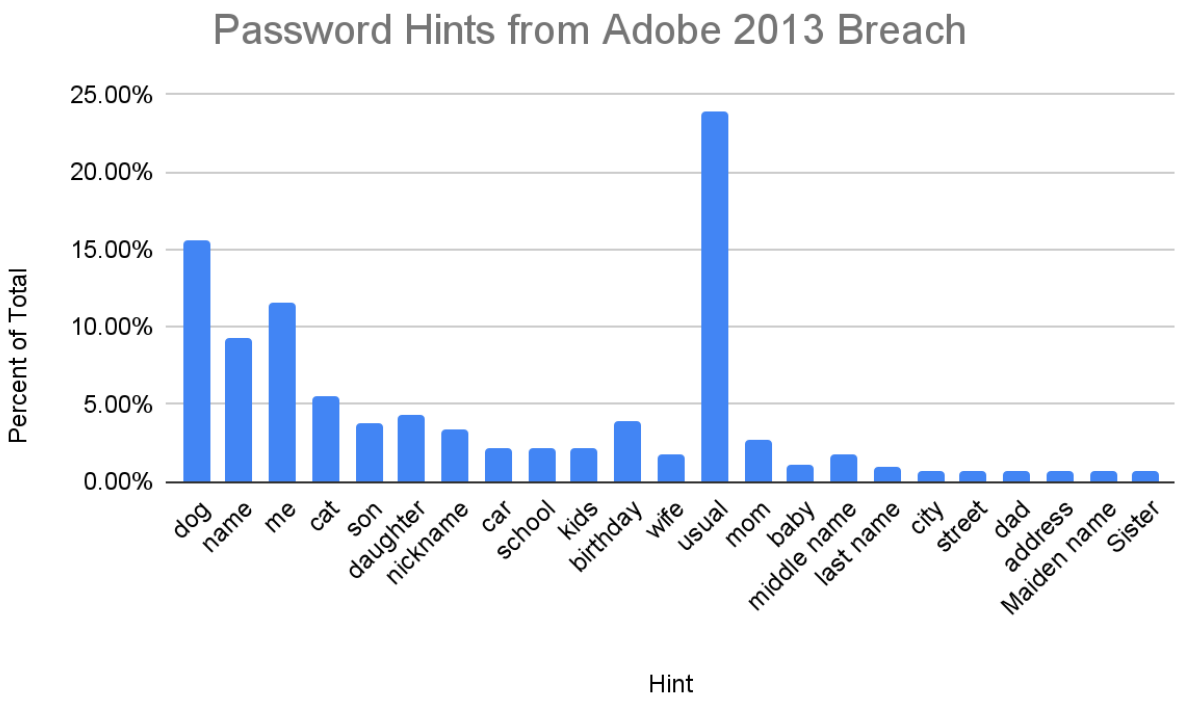
As it is necessary to obtain a warrant to access non-public data, digital investigators need to know where to get a warrant to. Stolen credentials often come paired with the site or resource they are used to access, such as social media, messaging software, and more allowing the investigators to narrow down their search.

When a warrant is acquired, stolen credentials can help investigators archive and access resources that would otherwise be encrypted and locked, such as booting up a pc and unlocking it to get a live image.

B. Preservation

In digital forensics, it's exceedingly important to preserve evidence, and credentials can be used to ensure this is done. Credentials play an enormous role in the preservation stage of the digital investigation process as they enable investigators to access and copy data from systems that would otherwise be inaccessible. By acquiring the right credentials, digital investigators can access accounts and systems that could contain valuable information relating to the investigation. When investigators gain access to the password protected information, they can copy it and create a cold forensic image of all potential evidence. With this forensic image, investigators can freely analyze the data while ensuring the original evidence will not be altered or deleted. In doing this, investigators can guarantee their evidence will be admissible in court while simultaneously allowing for a more thorough analysis of the data, alleviating the risk of altering the original evidence. Access to a live system blocked by credentials is also exceptionally important for investigators. Digital investigators can utilize the live system to identify running processes, network connections, and mounted file systems [6]. By using the live image accessed with credentials, investigators can preserve the processes meant to be killed upon log-off. In a digital investigation, credentials must be acquired legally, ensuring evidence gathered from these credentials are admissible in court. The best way for an investigator to obtain credentials legally is with a warrant or subpoena, as their actions will be legally backed by a judge. Investigators can also acquire credentials through social engineering or through password cracking techniques,

however they must have explicit legal permission to do this. It is extremely important for digital investigators to acquire credentials legally, as illegally acquired evidence is inadmissible in court. Without legal acquisition, the evidence can not be preserved. Overall, the access to accounts and devices that can be obtained through the use of a suspect's credentials is vital to preserving original evidence and guaranteeing the integrity of this evidence.



In the analysis stage of a digital investigation, credentials can prove immensely valuable. Specifically, credentials can potentially provide access to encrypted files that were previously unreadable by investigators. In unlocking these files, investigators can learn more about the actions of the suspect as well as uncover any information that the suspect tried to obfuscate. Investigators can also find a suspect's motives and plans within these encrypted files. Additionally, the credentials themselves can provide valuable insight into the life of the suspect. Usernames and passwords can reveal personal information such as the suspect's date of birth,

their family name, home or business addresses, and significant dates. For example, Ross Ulbricht, the creator of the infamous Silk Road, was caught due to his username relating to a personal account. The Silk Road was a darknet drug market, used worldwide by individuals attempting to anonymously and safely acquire illegal drugs. Through a simple Google search, IRS agent Gary Alford was able to connect Ulbricht's Silk Road username to his personal gmail account, implicating his involvement with the creation and management of this illegal drug market [7]. Information hiding within usernames and passwords can provide an insightful look into suspect behavior and their intentions. Using this information, investigators have a better chance of associating a cyber crime to an individual as it can identify potential suspects or even corroborate information already uncovered by investigators. Forensic investigators can also use credentials to identify the scope of their investigation. By utilizing a suspect's credentials, investigators can find out how many users and devices are associated with the system, giving investigators a clearer picture on the scope of their investigation. Along with identifying the scope, investigators can figure out what information is most relevant and focus on that thanks to their unchallenged access to the system.

C. Interpretation

Through digital forensics techniques, credentials can help provide important inferences to investigators. By examining how they were used, investigators can draw inferences on the implications of why those specific credentials were chosen. This can then be related back to the intentions of the perpetrator when utilizing them. There are various situations in which stolen credentials can be indicative in the motives of the individuals responsible.

Where stolen credentials are used is a potential source of evidence for investigators to determine the interests to which criminals were aiming for. The content and sites that attackers were engaging with can be linked with one another and then analyzed to determine what their connections are. Through careful observations based on the behavior exhibited, a system can be devised to categorize the malicious activities (Onaolapo etc, 2016). Investigators can then proceed to identify which actions were done by illegitimate access and have a better understanding of the cybercriminals. The motivations of each credential used is interconnected back to what activities are performed. By monitoring the user activities, a comprehensive analysis can be done to discern variations in intent and behavioral patterns.

Through the analysis of other data such as browsing history in conjunction with stolen credentials, investigators can piece together a more detailed picture on the crime based on the perpetrator's digital footprint. According to Cross and Layt, the digital footprint and online presence of a person proves to be a necessity in navigating a person's interests (Cross & Layt, 2022). This information is useful in the context of stolen credentials for social media platforms in that investigators can narrow the scope of interactions that criminals have left their traces on. From there, it can be further assessed as to why they had chosen these specific individuals to hack into. On the other hand, with credentials regarding financial data, investigators can determine the interests of the perpetrators to be based on monetary gain. For example, phishing tricks a user into sharing personal information so that the attackers can access banking accounts or credit cards (Ludl, 2007). In this scenario, the motive for stolen credentials is relatively straightforward. Law enforcement will affirm that the criminals want to achieve an economic profit in an illegal manner.

III. Methods that Stolen Credentials can interfere with a digital forensics investigation

A. Impersonation

According to Codepath.com, Credential theft is the most common security breach among other security breaches. Over 80% of hacking-related breaches leveraged either stolen and/or weak passwords (Bank of North Dakota). Crowdstrike.com describes credential theft as Credential stuffing which is a cyberattack where cybercriminals use stolen login credentials from one system to attempt to access an unrelated system. The principle behind it is that individuals frequently utilize the same username and password for various accounts making their accounts more susceptible to attacks.

This type of attack is particularly dangerous in the context of remote work, where employees, contractors, and third-party suppliers may all have access to sensitive information. Without the protections offered by traditional cybersecurity defense measures such as firewalls and antivirus software, detecting a credential stuffing attack can be extremely challenging. It is essential that organizations take steps to protect their login credentials and monitor for signs of unauthorized access to prevent data breaches and other security incidents. It is often difficult to pinpoint how the credentials were initially compromised and depending on the nature of the attack it may be difficult for a Digital Forensics Investigator to detect important elements of the attack.

Digital impersonation is a type of identity theft that typically occurs when a person's login credentials are compromised. This form of identity theft involves an individual assuming the identity of another person to gain unauthorized access to resources such as credit cards and other personal property. A digital impersonator can commit fraud using the victim's identity and

reputation. This can have serious consequences for the victim, including damage to their credit score and financial reputation. Digital impersonation can come in the form of fake celebrity profiles, these cases have risen with the age of social media, attackers use fake profiles to generate user engagement and sometimes financial fraud as well as other more heinous crimes (Cyber Crime Chambers).

Data breaches are often initiated by stolen login credentials, which can be easily obtained through lists available for purchase on dark web marketplaces. A crowdstrike.com article claims that for as low as $50 USD, anyone with a computer can buy a compromised account on the dark web to launch a credential stuffing attack. Reported by Security Magazine as of June 2022 there are over 24 billion usernames and passwords available on the dark web (Staff). Organizations can implement policies requiring strong passwords for all users, Multi-Factor Authentication to deter attackers and Biometric Authentication, when possible, can be more secure and tailored to security controls. They can sometimes be costly upfront but much less than the cost of an organization disruption due to compromised credentials.

Rapid7, a company that provides cyber security solutions highlights three must-have components that can help identifying unusual user activity using User Behavior Analytics to differentiate a users' normal activity from the suspicious, the automated deception technology to identify unwanted user behavior missing from logs, and the endpoint visibility to reveal lateral movement behavior which would be highly unlikely for any legitimate user (Hathaway).

B. Altered Evidence

With stolen credentials, attackers are gaining unauthorized access to numerous systems, accounts, and devices, which can negatively impact an investigation in various ways. Firstly, this

access information can be tampered through fabrication or alterations. These include the metadata of the file system and directories that would be retrieved in an investigation, ranging from timestamps to log files (Buchholz, 2004). Attackers with unauthorized access can delete log files or modify timestamps that indicate the devices have been compromised. Investigators will find it difficult to refine their timeframe of the criminal activity. In addition, with stolen credentials, attackers can integrate manipulated data with information that has not been altered. This falsified evidence disrupts the flow of the investigation as more resources have to be spent on determining which data and information retrieved are factual. Modified or deleted data will undermine the integrity of the forensics analysis and consequently, the investigation overall.

At the same time, data manipulation resulting from stolen credentials can make it challenging for investigators to determine the original state of the compromised systems or devices. With the necessary credentials to make changes to a configuration of a system or file, attackers possess the capabilities to alter various attributes. This could be based on their motivation to conceal their actions, or to make it a problematic situation where investigators cannot ascertain any information about the systems. It is necessary to determine the initial operational status and original setup so that differences between the present state can be found. However, because attackers have the credentials required to change information as they'd like, it once again raises the concern of integrity of any documentation retrieved.

C. Multiple Attackers

One of the most significant challenges in a digital forensics' investigation is determining the source and responsible parties of an attack. This challenge becomes even more difficult when multiple attackers are involved, and stolen credentials are used. This is because the use of shared

credentials can complicate the investigation making it harder to identify which attacker is responsible for certain attacks.

The use of shared credentials makes it difficult for investigators to link specific actions to the parties responsible. This can lead to confusion and errors in the investigation process. For example, if two attackers have access to the same credentials, they can both perform different actions using those same credentials, making it challenging to determine who carried out specific actions. In such cases, investigators may need to conduct a more extensive investigation to identify the methods and tools used in the attack and to determine who is responsible for what.

Another challenge that investigators face when multiple attackers are involved is the compounding effect of different attack methods. With multiple attackers, each may use different methods and tools to carry out their attacks. This can make it difficult to identify a single point of entry or a common modus operandi. As a result, the investigators will need to conduct a more extensive investigation to identify the methods and tools used in the attack.

Furthermore, the use of shared credentials can make it difficult for investigators to understand the scope and nature of the attack. Multiple attackers may have different motives for their attacks, making it difficult for investigators to identify potential and future threats. For example, if multiple attackers are using the same set of credentials to access a system, one attacker may be trying to steal data, while the other may be trying to plant malware onto the devices. Without a thorough investigation on the motives of each attacker, it will be difficult to determine the scope and nature of the attack and identify potential threats.

D. Use of RAT and Remote Access Tools

The use of RATs or Remote Access Tools can interfere with digital forensics investigations in many ways. RATs are software tools that allow the users to control another device remotely over the network. They are commonly used by attackers to gain unauthorized access to other devices.

When a device has been taken over by a RAT, it can be difficult for a digital forensics investigator to determine the extent of the intrusion since the attacker may have full access to the system and may be able to modify or remove evidence. A skilled attacker may also utilize a RAT to cover their tracks, such as deleting logs and modifying system timestamps.

On top of that, RATs can provide attackers with ongoing access to a compromised system, allowing them to continue their attacks even after the initial breach has been detected and remediated. This will make it more challenging for investigators to fully remove the attacker from the system and prevent further damages.

Overall, the use of RATs may hinder digital forensics investigations and make them more complex, making it more challenging for investigators to determine the scope of an attack and identify the parties responsible. Therefore, it is important for organizations to take action to stop RATs based attacks, such as using network segmentation, strong access controls, and regular security awareness training for employees.

Conclusion

The theft of credentials is a growing concern in the digital age, and digital forensics plays a critical role in identifying and mitigating the impact of such incidents. The use of advanced technologies and lack of education on particular credential hygiene and security pose significant challenges for digital forensics investigators. However, with the right tools, techniques, and training, forensic investigators can successfully identify the source of the attack, recover stolen credentials, and prevent future attacks.

Stolen credentials play a critical role in digital forensics investigations. They provide valuable information to identify suspects, access encrypted files, and help determine the scope of a given investigation. With analyzing the usage patterns and targeted platforms, investigators can infer the motives and intentions of perpetrators. However, stolen credentials can interfere with investigations through impersonation, altered evidence, and multiple attackers. The significance of stolen credentials is essential for effective investigations and ensuring the integrity of evidence obtained.

References

Buchholz, Florian, and Eugene Spafford. "On the role of file system metadata in digital forensics." *Digital investigation* 1.4 (2004): 298-309.

"Credential Theft." *Credential Theft | CodePath Cliffnotes*, https://guides.codepath.com/websecurity/Credential-Theft.

Bank of North Dakota. "81% Of Company Data Breaches Due to Poor Passwords." *Bank of North Dakota*, 15 Oct. 2018, https://bnd.nd.gov/81-of-company-data-breaches-due-to-poor-passwords/.

Cyber Crime Chambers. "Investigating Digital Impersonation." *Investigating Digital Impersonation*, https://www.cybercrimechambers.com/investigating-digital-impersonation.php.

"What Is Credential Stuffing? - Crowdstrike." *Crowdstrike.com*, Crowdstrike, 6 Mar. 2023, https://www.crowdstrike.com/cybersecurity-101/credential-stuffing/.

Staff, S. (2022) *24 billion usernames, passwords available on the dark web*, *Security Magazine RSS*. Available at: https://www.securitymagazine.com/articles/97825-24-billion-usernames-passwords-available-on-the-dark-web (Accessed: 15 May 2023).

Cross, Cassandra, and Rebecca Layt. "“I Suspect That the Pictures Are Stolen”: Romance Fraud, Identity Crime, and Responding to Suspicions of Inauthentic Identities." *Social Science Computer Review* 40.4 (2022): 955-973.

Hathaway, Matt. “Detecting Stolen Credentials Requires Endpoint Monitoring: Rapid7 Blog.” *Rapid7*, Rapid7 Blog, 28 Oct. 2019, https://www.rapid7.com/blog/post/2016/05/23/detecting-stolen-credentials-requires-endpoint-monitoring/.

31. IJCSIT- live vs dead computer forensic image acquisition. (n.d.). Retrieved May 6, 2023, from https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080331.pdf

Jackson, J. (2015, January 26). *Simple google search outed alleged Silk Road founder*. Computerworld. Retrieved May 6, 2023, from https://www.computerworld.com/article/2875655/simple-google-search-outed-alleged-silk-road-founder.html

Ludl, Christian, et al. "On the effectiveness of techniques to detect phishing sites." *Detection of Intrusions and Malware, and Vulnerability Assessment: 4th International Conference, DIMVA 2007 Lucerne, Switzerland, July 12-13, 2007 Proceedings 4*. Springer Berlin Heidelberg, 2007.

Onaolapo, Jeremiah, Enrico Mariconti, and Gianluca Stringhini. "What happens after you are pwnd: Understanding the use of leaked webmail credentials in the wild." *Proceedings of the 2016 Internet Measurement Conference*. 2016.

Cost of a data breach 2022. (n.d.). IBM. Retrieved May 5, 2023, from

https://www.ibm.com/reports/data-breach

Interpol. (n.d.). *Digital forensics*. Interpol. Retrieved May 5, 2023, from https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics

Save Your Data with These Empowering Password Statistics. (2023, April 24). DataProt. Retrieved May 6, 2023, from https://dataprot.net/statistics/password-statistics/