Understanding the credential theft lifecycle

Jose Miguel Esparza, Blueliv

Jose Miguel Esparza

Credential theft is a serious driver of cybercrime today. The world over, different kinds of credentials are used by billions daily to authenticate themselves in their physical and digital lives. From physical keys, to tokens and cards, to digital private keys, session cookies, digital certificates, crypto-currency wallets, login and password combinations, all of these types of credentials are vulnerable to attack.

All industries are impacted by credential theft and for any organisation a single stolen credential can be the beginning of a nightmare. Stolen corporate credentials are used to breach organisations and steal sensitive information, with the 2017 Verizon Data Breach Investigations Report (DBIR) revealing that 81% of hacking-related breaches leverage either stolen or weak passwords.[1]

From blackmail to ransom, from selling sensitive information to committing fraud, the end goal of credential theft is normally for the cyber criminal to gain some sort of profit. The market for compromised credentials is extremely broad, with high potential depending on the credentials being traded.

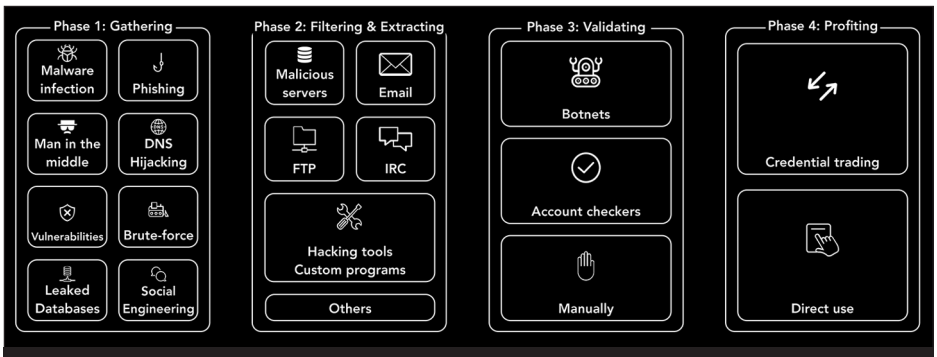
The cost of bank account credentials, for example, varies significantly, depending on where they are sold and the balance the accounts contain. An account sold on TOR markets can go from $10 when the balance is lower than $1,000, to more than $300 when the balance is higher than $10,000. Accounts advertised with a balance of $500,000 would cost $25,000.

Credential theft lifecycle

The most widely used stolen credentials are banking and social network logins, followed by email and web service providers and credentials used for retailers and e-commerce, according to a recent report.[2] The advent of the General Data Protection Regulation (GDPR) last May also means that personally identifiable information (PII) will become more attractive to cyber criminals, as the ramifications of the legislation mean that they can demand higher ransom amounts.

Cyber criminals steal these credentials using a wide range of tactics, from blackmail to ransom to malware that extracts credentials – so-called stealers.

Once credentials are captured, they can be used in a variety of ways, depending on type. One of the most common ways is to facilitate a data breach, leveraging corporate accounts and using these to perpetrate serious intrusions. Further ways include VIP impersonation on social media or email to damage the company's reputation or instruct fraudulent transactions; account compromise and identity theft, impersonating real customers to steal goods and services; and executing fraudulent transactions in financial institutions.



The credential theft lifecycle. Source: Blueliv.

"Stolen credentials are rarely ever used in real time, unless they're compromised in highly targeted attacks; cyber criminals require time to analyse the data they capture, filter out the 'prime' credentials, and sell or exploit the data"

Understanding the lifecycle of a stolen credential is key to protecting your organisation from being damaged by such a theft. In terms of value, the 'freshness' of corporate credentials (how recently they have been compromised) is key. The best-case scenario for a cyber criminal is if the credential has been harvested without alerting the affected user. Stolen credentials are rarely ever used in real time, unless they're compromised in highly targeted attacks; cyber criminals require time to analyse the data they capture, filter out the 'prime' credentials, and sell or exploit the data. This means that the faster an organisation can detect stolen credentials, the better – as this can hugely minimise the risk of an attack, or at least limit the damage.

Left are the different phases of the credential theft lifecycle, showing the various ways that cyber criminals can steal credentials and what they do with them afterwards: from the moment they are stolen, until they are used by the cyber criminals for financial gain.

Gathering

There are many ways cyber criminals steal credentials and their choice often depends on their skillset and resources. One of the easiest ways to collect credentials from their victims is phishing, which is normally accessible to a wide range of criminals and does not require a great deal of resources. Other methods include DNS hijacking, 'man in the middle' attacks, brute force, taking advantage of existing vulnerabilities, leaked databases or social engineering.

Stealer malware is a particularly common threat. The most common 'tool' is malware such as LokiPWS. Also known as LokiBot, this can act both as a loader for other malware as well as a password and crypto-wallet stealer. Currently, it is available from a variety of underground markets as a modular product (stealer, wallet stealer and loader) with prices ranging between $250-$500, depending on the desired functionality.

Its functionalities as a stealer include extracting credentials and private information from browsers, FTP/VNC clients, email and IM clients, poker games and 'sticky' note clients. It also aims to steal crypto-currency wallets, including Bitcoin and Litecoin. LokiPWS is still widely distributed through malicious email campaigns containing malicious PDFs or Office documents with macros, which at execution download and launch the malware. In the past year there has been an increase in the number of LokiPWS samples detected, suggesting that its popularity among cyber criminals is increasing. The most active stealer families are currently Pony Loader, KeyBase, AZORult, LokiPWS, ISR Stealer, Usteal, Agent Tesla and HawkEye, though many more exist in the wild.

On the cheaper side, criminals can buy inexpensive malware kits or use source code leaks in order to achieve their objective. More advanced attackers are able to infect machines and move laterally in an organisation's network, which allows them to exfiltrate thousands or even millions of credentials at once.

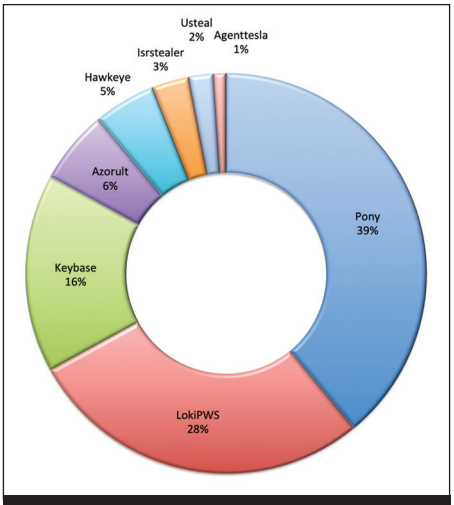
Filtering, extracting and validating

So what happens next? All these credentials are stored by the cyber criminals in databases, email accounts or files and now it's time to use them. First of all, they need to be extracted and/or filtered, depending on the objective. After the extraction phase, the criminals might need to double-check that the stolen passwords are still valid. This can be done using credential checkers or even bots to automate the task. Additionally, over the past few years control panels have improved in sophistication and functionality, so that the panels themselves can be used to mine the recovered credentials, extracting specific ones to target specific companies.

"More advanced attackers may look for credentials belonging to specific organisations to perform more targeted attacks, which can have a massive financial and reputational impact on the affected companies"

Depending on the objective, it's possible that the criminals create batches and try to sell them in underground markets, or they search for specific credential types to perform additional attacks. More advanced attackers may look for credentials belonging to specific organisations to perform more targeted attacks which can have a massive financial and reputational impact on the affected companies. This is one of the most worrisome risks when it comes to credential theft – a door left open to breach an organisation.

Depending on the source of the credentials, the validation step can sometimes be omitted, for example, in the event that the cyber criminal knows the information is fresh and quite likely to be valid. However, where criminals source the credentials from other criminals online or use leaked databases, this step is necessary to avoid wasting time and resources. Credential validation can be performed in different ways, but it is usually automatic when a large number of credentials is involved.



The most active credential stealer malware families, logged over a six month period. Source: Blueliv.

Profiting

In this final phase, cyber criminals try to make a profit from the stolen credentials. There are different ways of monetising the credentials.

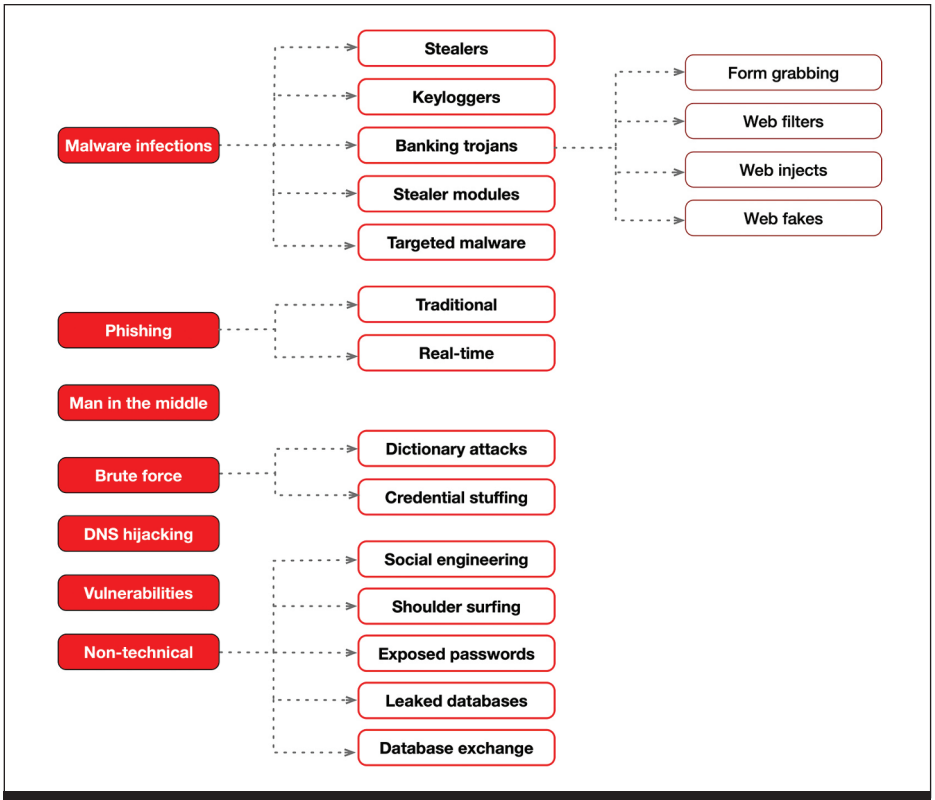
In the first case, criminals try to sell stolen accounts in underground forums or markets, offering their use to a third party. This also occurs with credential sharing between criminal groups. It is a known fact that cyber criminal groups with fewer resources share credentials with more professional groups who can perform more advanced and targeted attacks against the compromised organisations.

If the hackers are using the credentials themselves, they might access the user accounts directly and steal PII or use them as a 'tool' to perform additional targeted attacks such as CEO fraud (commonly known as business email compromise, BEC), or massive website compromises to inject JavaScript code, etc.

There are a number of markets, forums and websites where people sell and buy credentials. Some of these sites are hidden on the dark web, but others are on the

visible part of the Internet (or 'clearnet'). In these markets, there are three types of credentials on sale, depending on the public to which they are addressed:

- Services accounts: The trading of accounts such as Netflix, Spotify, HBO, pornography, sport streaming services and gaming accounts is very popular currently. These types of credentials are focused on the general public who want to use these services but pay less.
- Hosting accounts: Credentials on hosting sites are used by criminals who want the sites to perform their illegal activities.
- Corporate accounts: These types of credentials are rarely found in markets. Usually trade is conducted through personal relationships via private messages in forums, where people can directly contact a 'specialist' to buy the information or hire him to attack a specific corporation. It is easy to find leads in markets where people sell contact information of different corporations.



Methods used for stealing credentials. Source: Blueliv.

Protecting your organisation

As with many aspects of cyber security, education is key to mitigating credential theft. The ability to recognise when credentials might be compromised can save a huge amount of pain and financial loss. In the case of credential theft, the responsibility ultimately rests on the user rather than the technology. This makes the end user both the weakest and strongest link in the chain. Do all employees know how to recognise a phishing email, for example? It may sound extreme but generally any request for credentials should be treated as guilty until proven innocent, and employees should be trained accordingly.

However, you cannot rely on user education alone, so technology must also play a part in any organisation's cyber security strategy. Investing in security software is crucial and can prevent many types of cybercrime. Using threat intelligence services can significantly reduce the damage caused by credential theft, and more targeted modules can also work to prevent attacks. There are also counter-intelligence modules that combat phishing attempts by proactively detecting campaigns before they can have a significant impact. Analysis and reporting on these potential attacks can then be shared with employees to ensure that they, and your organisation, do not become victims.

Cyber hygiene

The key to all of these strategies is continuous 'cyber hygiene'. This can help prevent attacks, as well as mitigate their impact if, and when, one happens. Cyber hygiene involves setting the appropriate alerts to detect attacks, as well as an ongoing process of penetration testing and patching, password protection, additional authentication mechanisms and designating people within your organisation to consistently challenge your security protocols. Cyber criminals are constantly testing new ways to exploit your infrastructure, so remaining static when it comes to your security protocols is a sure-fire way to get breached.

In the event of a breach or suspected breach, the first thing to do is also the most obvious: change your credentials! As mentioned above, this should be done regularly regardless. Credential theft is a multi-million pound industry for cyber criminals. The impact of such theft on organisations, and the individuals within them, can be profound, especially in the wake of the GDPR, which means that not protecting user data correctly can lead to financial loss and reputational damage that it could be difficult to recover from. This is why corporate accounts must be protected and both organisations and individuals must remain vigilant to potential threats.

Ultimately, the most effective deep defence against attackers is collaboration. If businesses and security professionals work together in providing a collaborative approach, it is infinitely better than siloing ourselves. Socialising cyber security means encouraging parity and fighting cybercrime collaboratively and more effectively – such as through participation in threat exchange networks.[3]

About the author

Jose Miguel Esparza is head of threat intelligence at Blueliv, responsible for advanced

research and gathering threat intelligence about botnets, malware and threat actors. He is a security researcher who has been analysing cyberthreats since 2007 when he started his career at S21sec e-crime. Formerly leading the Threat InTELL team at Fox-IT, Esparza joined Blueliv in 2017. He is the author of the security tool peepdf and periodically writes on eternal-todo.com about security and cyberthreats. He is a regular speaker and trainer on the conference circuit, often present at the likes of RootedCon, Cyber Security Summer BootCamp, Source, Black Hat, Troopers and Botconf, among others.

References

1. 'Data Breach Investigations Report 2017'. Verizon, 2017. Accessed Jan 2019. www.verizondigitalmedia.com/blog/2017/07/2017-verizon-data-breach-investigations-report/.
2. 'The Credential Theft Ecosystem'. Blueliv. Accessed Jan 2019. www.blueliv.com/the-credential-theft-ecosystem/.
3. Blueliv Threat Exchange Network, home page. Accessed Jan 2019. https://community.blueliv.com/#!/discover.

Three ways in which GDPR impacts authentication

Brett McDowell

Brett McDowell, FIDO Alliance

The General Data Protection Regulation (GDPR) has been enforced across the European Union (EU) since late May, and is widely considered the single most significant change to data protection law in two decades, impacting a countless number of organisations across the globe that collect and process information from EU citizens.[1] This very much includes those in charge of online authentication, given the sensitive nature of the data being protected by those authentication systems, and the regulatory consequences of providing inadequate protections for that data.

Unlike previous EU data protection rules, the GDPR may apply to any processing of the personal data of an EU resident (or 'data subject'), even if the firm does not have an office or employees in the EU. Non-compliance is also more costly than before, as the EU Data Protection Authorities (DPAs) now have the right to levy hefty fines. Fundamental violations of the GDPR could lead to fines of up to €20m or up to 4% of global turnover (or revenue), whichever is higher. Fines for secondary violations, related to obligations such as privacy by design and children's consent, could be €10m or up to 2% of global turnover – again, whichever is higher.

While the GDPR pertains to all members of the EU alike, there will also be a supervisory authority established in every EU Member State to enforce the regulations – meaning that firms doing business in Europe may now have to deal with 28 different supervisory authorities all at once.

Online authentication

The focus of compliance teams within organisations subject to the GDPR has primarily been informed consent and all that entails. But the new law is equally relevant to how your company protects that data after consent has been given.

While there is a general understanding of what the GDPR means for privacy, it is important for these compliance teams to dig deeper into the specific articles pertaining to their business operations – and there are plenty. The articles can roughly be placed into three categories: data security; consent and individual rights; and biometrics.

Data security

There are a few articles in the regulation pertaining to data security that directly impact online authentication: articles 5, 25, 32, 33 and 34.

First of all, article 5 lays out the core principles relating to the processing of personal data, including that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (known as 'data minimisation') and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Companies also need to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 25 of the GDPR calls for data protection by design and default – or, more specifically, for entities to implement appropriate technical and organisational measures that are designed to implement data protection principles, such as data minimisation. Appropriate technical and organisational measures also need to be taken to ensure that only personal data which is necessary for each specific purpose of the processing is processed by default.

Through article 32, the GDPR directs entities to implement technical and organisational measures to ensure appropriate security relative to state of the art, cost of implementation and risks.