The Economy of Credential Stuffing Attacks

By Insikt Group
This report covers the current threat landscape of credential stuffing attacks. It reviews the most popular tools used by cybercriminals to initiate credential stuffing and describes some of the most popular marketplaces that sell compromised credentials. This report contains information gathered using the Recorded Future® Platform, as well as additional open source, dark web, and underground forum research, and will be of most interest to analysts protecting e-commerce, telecommunications, and financial organizations from credential stuffing attacks, as well as those looking for investigative leads on threat actors performing such attacks.

Executive Summary

The rapid proliferation of automated marketplaces on the dark web, fueled by the widespread availability of support infrastructure such as account-checking software, email and password combo lists, and proxy service providers, has created the perfect attack landscape for the abuse of thousands of popular web services such as e-commerce, financial services, travel websites, and telecommunications companies. It is safe to assume that almost every large organization with an online retail presence has had their users exposed to credential stuffing attacks in the past few years, with some companies having upwards of millions of exposed login credentials available for purchase on the dark web at any given moment.

Key Judgments

- The first widespread credential stuffing attacks were observed in late 2014, coinciding with the proliferation of automated underground marketplaces. When selling accounts, attackers offered the quick and easy monetization of compromised account credentials. Some actors who engaged in credential stuffing attacks remain active today.
- With an investment of as little as $550, criminals could expect to earn at least 20 times the profit on the sale of compromised login credentials.
- The overall supply of compromised login credentials across several large marketplaces exceeds tens of millions of accounts.
- Insikt Group identified at least six popular variants of account-checking software used by cybercriminals; however, dozens of lesser-known variants can be found on the dark web.
• While some companies may choose to implement multi-factor authentication (MFA), which blocks the credential stuffing attack vector, organizations may not be prepared to choose security over convenience.

**Background**

Around late 2014 and in the beginning of 2015, we observed the widespread adoption of new dark web business models specifically tailored to facilitate a high volume of trades in a fully automated manner. Designed to emulate legitimate retail platforms such as eBay and Amazon, these so-called “automated shops” allow even low-level criminals to become vendors of stolen data, such as compromised login credentials, without having to worry about maintaining their own infrastructure or marketing campaigns. By and large, the adoption of account marketplaces was made possible primarily by the proliferation of account-checking software, or simply “checkers,” used as the main tool in credential stuffing attacks.

**Threat Analysis**

Compromised account credentials were always a valuable commodity in the dark web — the number of transactions was relatively small, and they were primarily conducted either on a peer-to-peer basis or via semi-automated markets such as AlphaBay, Silk Road, and Hansa Market. In older models, buyers received their wares only after the seller manually approved the deal and delivered the purchased data. Moreover, sellers had to maintain the listings and communicate with the buyers personally.

However, with the advent of automated shops, the need for manual engagement was eliminated and the business of compromised accounts fully transitioned from peer-to-peer dealings to a much more democratized, open-to-everyone enterprise.
For a nominal 10 to 15 percent commission deducted from the amount of each sale, members can upload any number of validated compromised accounts, which in addition to email and password, often include data such as the account holder’s city or state of residency, transaction history, and/or account balance. All of this is valuable data to fraudsters seeking to buy accounts tailored to their specific needs. The vendor’s main focus is replenishing the stock, while all customer support, remittances, and dispute resolutions are handled by the shop’s support team.

At first, only a handful of select vendors became the primary suppliers of stolen data, but as the tradecraft was shared among members of the criminal underground, the business of stolen credentials has grown exponentially.

Since regular internet users tend to reuse the same passwords across multiple websites, threat actors quickly learned that instead of attempting to obtain access to an individual account, which may take a very long time, they should instead focus on hacking multiple random accounts, reducing their efforts.
A combination of several elements made the hacking of various online services accounts not just effortless, but also incredibly lucrative. To launch account brute-forcing, also known as credential stuffing attacks, an attacker only needed brute-forcing software, a database of random email and password combinations, and access to a pool of proxies.
The Economics

Early versions of checkers were made to target a single company and were sold for between $50 and $250, depending on the tool's capabilities. These tools would attempt to log in to a website using an email and password combination obtained from a random database often obtained on the dark web. If a combination worked, it would be marked as valid. If not, the software would simply pick another combination from the list and attempt to log in again. For valid logins, more expensive and complex checkers would also collect additional information from the compromised account, such as linked banking and payment card information, account balances, the owner's address, and even transaction history. Until this day, the ingenuity of the method truly lies in the economy of scale, allowing criminals to process hundreds of thousands of combinations in a very short period of time.

Eventually, several dominant players such as STORM, Black Bullet, and Sentry MBA entered the market with more robust tools, supporting an unlimited number of custom plugins, also called “configs,” which essentially offered hackers the capability to target almost any company with an online retail presence.

What had initially started as several hundred or several thousand compromised accounts quickly ballooned to hundreds of thousands, or even millions, of accounts. Some of the most prominent account shops have tens of millions of compromised accounts for sale at any given moment.

Although the competition quickly brought the average price of a single compromised account from over $10 down to a mere $1 to $2, the overall profitability of credential stuffing attacks increased significantly through sheer volume.

According to underground chatter observed over time, the average success rate for credential stuffing is anywhere between one to three percent. Hence, for every one million random combinations of emails and passwords, attackers can potentially compromise between 10,000 and 30,000 accounts. Moreover, the same database could then be reused over and over again to hack dozens of different websites, yielding even higher profits.
Based on a conservative success rate of one percent per 100,000 compromised emails and passwords, the economics behind credential stuffing attacks reveals at least 20 times higher profit levels.

<table>
<thead>
<tr>
<th>Victim</th>
<th>Average Price</th>
<th>Max. Potential Profit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>$2.00</td>
<td>$2,000</td>
</tr>
<tr>
<td>PayPal</td>
<td>$1.00</td>
<td>$1,000</td>
</tr>
<tr>
<td>eBay</td>
<td>$3.50</td>
<td>$3,500</td>
</tr>
<tr>
<td>Expedia</td>
<td>$0.50</td>
<td>$500</td>
</tr>
<tr>
<td>Airbnb</td>
<td>$1.50</td>
<td>$1,500</td>
</tr>
<tr>
<td>FedEx</td>
<td>$1.50</td>
<td>$1,500</td>
</tr>
<tr>
<td>Credit Karma</td>
<td>$2.00</td>
<td>$2,000</td>
</tr>
<tr>
<td>Online Video Service</td>
<td>$1.40</td>
<td>$1,400</td>
</tr>
<tr>
<td>Xfinity</td>
<td>$3.50</td>
<td>$3,500</td>
</tr>
</tbody>
</table>

Gross Profit Margin | 97.5%  | Gross Profit $19,150

2.5%  | Direct Cost $550

Max. Selling Price $19,700

Gross Price $550
Technical Analysis

Below are the most prominent variants of account-checking software used by cybercriminals in credential stuffing campaigns. It is important to note that lesser-known solutions, which are often built to target a single company, are also available for purchase. However, such one-off tools rarely gain significant market presence and tend to disappear quickly, as the developers cease product support due to slow adoption.

STORM

STORM is marketed across several English-speaking forums, and unlike other account-checking tools, is available free of charge. However, users are encouraged to make donations. The exact identity of the developer is unknown; however, according to underground forum chatter, the software was allegedly created by the actor mrviper. STORM was first launched in January 2018, and according to the description found on dark web advertisements, it is characterized as a free “cracking” program designed to perform website security testing. STORM is written in C language and was developed in close cooperation with members of the Cracked forum. The tool has the following technical features:

- Supports FTP cracking
- Simultaneous FTP and HTTP attacks
- Concurrent sessions
- Debug functionality for activity analysis
- Supports combo lists of up to 20 million email:password records
- Supports HTTP/HTTPS
- Supports SOCKS4 and SOCKS5
- Proxy auto update with automated harvesting from public sources
- Keywords capture (collection of premium account details)
- JavaScript redirect
Black Bullet

Black Bullet first appeared on the dark web in early 2018 and likely was created by the actor Ruri, who operates the official www.bullet[.]black website; however, according to the information found on the main page, the community no longer accepts new members. Several members of the dark web, including daltonbean8 and Doberman, were observed distributing the tool.

In contrast to other account-checking tools, BlackBullet does not offer multi-threaded capabilities, and only allows a single company at a time to be attacked. The tool also comes with a brute-forcing feature that can perform dictionary attacks when run against specific accounts.

- Captchas bypass
- Configuration files: ~ 530; however, users have an option to modify and create new configurations themselves
- Selenium Webdriver support
- Price: Between $30 and $50
**Private Keeper**

Private Keeper was developed by the actor deival909. According to the description provided by the actor, the tool is based on in-line technology. Private Keeper is by far the most popular account-checking software in the Russian-speaking underground.

- Price: From 49 Russian rubles (approximately $0.80)
- Concurrent sessions
- Utility software to aid in automated connection to the private or publicly available proxy services
- Official online store: www.deival909[.]ru
- Latest version: 7.9.3.34
SNIPR was sold and publicly shared on multiple underground forums. The threat actor PRAGMA is the developer of the malware. SNIPR is a configurable account-checking software, written in C language that supports both online credential stuffing and offline brute-forcing dictionary attacks. Although the tool was advertised by multiple threat actors, this account checker has its own website with a forum and a marketplace www.snipr[.]gg. The website allows third party developers to share custom-made configuration files.

- Configuration files: More than 100 are part of the official package
- Concurrent attacks: Up to four targets
- Price: $20
Sentry MBA

Sentry MBA, with over 1,000 configuration files available, is one of the most prominent and readily available examples of account-checking software on the dark web. Several criminal forums maintain ongoing discussion threads dedicated to Sentry MBA. As of December 2018, the registration at https://sentry[.]mba, the official Sentry MBA marketplace and discussion board, is closed and available by invitation only. Insikt Group identified that the tool has been actively advertised on the dark web since late 2014. However, the official Twitter account was launched in July 2013. The tool was allegedly developed by an actor using the alias “Sentinel” and later modified by another actor, “Astaris.” Sentry MBA uses OCR (optical character recognition) functionality to bypass captcha. However, Sentry MBA doesn't support Javascript anti-bot challenges. Sentry MBA can be configured to recognize specific keywords associated with a website’s responses to successful and unsuccessful login attempts.

- Available Configs: More than 1000
- Official Website: https://sentry[.]mba
- Price: Between $5 and $20 per configuration file
- Supports HTTP/HTTPS
- Supports SOCKS4 and SOCKS5
WOXY

Unlike a typical account-checking software, the WOXY email checker allows criminals to verify the validity of email accounts, scan email content for valuable information (like gift card codes or online subscriptions to streaming services, travel websites, and financial institutions), and hijack valid accounts by resetting login passwords automatically. According to the conducted analysis, WOXY was developed by the actors Dreamzje and Deos, who operated the currently defunct website www.keepit[.]online. The original price of the WOXY checker was $40; however, in September 2018, actors Crank and Yuki shared the cracked version of WOXY on the dark web, which now can be easily obtained free of charge.
Mitigation

- Criminals will often use paid proxy services aside from using publicly available free proxies to further obfuscate attacks. However, our analysis shows that such services often use geo-spoofing techniques to create a wide pool of IPs. Such domains will have the same IP addresses, but they will use different subnets. Monitoring for web traffic activity from such IPs offers additional mitigation capabilities.

- The introduction of multi-factor authentication has proven to be a highly effective mitigation practice for many organizations that historically experienced a high level of credential stuffing attacks.

- Monitoring criminal underground communities for the availability of new configuration files targeting your organization, acquisition, and the thorough analysis of such files for additional attack indicators.

- End users can reduce the risk of being victimized by a credential stuffing attack by using a password manager and setting a unique strong password for each online account.
Appendix A — Most Targeted Industries

- Financial
- E-commerce
- Social Media and Entertainment
- Information Technology and Telecommunications
- Restaurants and Retail
- Transportation
## Appendix B — MITRE ATT&CK Techniques

<table>
<thead>
<tr>
<th>MITRE ATT&amp;CK Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial Access</strong></td>
</tr>
<tr>
<td>Bypass auditor</td>
</tr>
<tr>
<td><strong>Horizontal Transfers</strong></td>
</tr>
<tr>
<td><strong>Serverless Link</strong></td>
</tr>
<tr>
<td><strong>Data Processing</strong></td>
</tr>
<tr>
<td><strong>Data-Flow</strong></td>
</tr>
<tr>
<td><strong>Data-Flow</strong></td>
</tr>
</tbody>
</table>

### Valid Answer

- **Mitigation:** Defend against Command and Control channels.
- **Prevention:** Implement multi-factor authentication for access controls.
- **Detection:** Monitor for anomalous network traffic.
- **Response:** Isolate affected systems and contain the threat.

**Legend:**
- **Initial Access:** Techniques used to gain access to the environment.
- **Execution:** Techniques used to execute malicious code.
- **Persistence:** Techniques used to maintain access.
- **Privilege Escalation:** Techniques used to increase privilege.
- **Defense Evasion:** Techniques used to evade detection.
- **Credential Access:** Techniques used to steal credentials.
- **Discovery:** Techniques used to discover the environment.
- **Command and Control:** Techniques used to communicate with the attacker.
About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.