Hidden in Plain Sight: The Tools and Resources Used in Credential Abuse Attacks

Authors:
Luis Raga Hines & Danny Wasserman
# Table of Contents

Executive Summary ............................................ 3

Overview ......................................................... 5
  Introduction .................................................. 5
  Finding Credentials .......................................... 6
  Proxies and Credential Abuse Attacks .................. 8
  The Tools and the Lab Environment ...................... 9

Credential Abuse Tools ....................................... 10
  Cr3d0v3r ....................................................... 10
    Installation ................................................ 10
    Weaponization ............................................. 12
  Sentry MBA .................................................. 12
    Installation ................................................ 12
    Usage & Modules ......................................... 13
  SNIPR .......................................................... 17
    Installation ................................................ 18
    Community and Support .................................. 18
    Usage ....................................................... 18
    Proxy Features .......................................... 19
    Configuration Files ..................................... 20

Akamai Detection Capabilities ............................ 22

Protection Recommendations ............................... 24
Executive Summary

In this white paper, we analyze different methods and tools used by malicious actors when launching credential abuse attacks against web applications on the Internet. The purpose of this paper is to raise awareness about some popular and public tools used by attackers and the capabilities of these tools so online businesses can better protect their assets and those of their customers.

Credential abuse attacks are on the rise worldwide, according to recent Akamai research that shows Akamai detected approximately 3.2 billion malicious logins against customer websites per month from January through April 2018, and over 8.3 billion malicious login attempts from bots in May and June 2018 — a monthly average increase of 30%. In total, from the beginning of November 2017 through the end of June 2018, Akamai researcher analysis shows more than 30 billion malicious login attempts during the eight-month period.

Credential stuffing can cost organizations millions of dollars in fraud losses annually, according to Ponemon Institute’s “The Cost of Credential Stuffing” report. One financial institution reported that the cost of an account takeover, resulting from credential stuffing, can range from $1,500 to $2,000 per account. This is a very lucrative business for hackers — and there is a thriving market for tools, support services and info, and rewards reaped from a successful attack.

Key Takeaways

• Finding lists of leaked usernames and passwords to use in credential stuffing attacks is easy and inexpensive; a simple Google search can reveal a large number of credentials available on text storage sites and hacking forums, in addition to the trove available on the Dark Web.

• Popular and easy-to-use account checking tools like Cr3d0v3r, Sentry MBA, and SNIPR enable threat actors with minimal technical expertise to launch brute-force login attacks against many websites using configurations shared and maintained by the credential abuse community.

• Akamai customers should review the repositories of SNIPR configurations to see if their websites are included and take measures to mitigate further abuse.

• Akamai’s Bot Manager Premier proved successful in detecting sample malicious activity generated by these three tools against a testing environment. This malicious activity can be mitigated at the edge of the Internet by leveraging Behavioral Anomaly controls in Deny mode.

• For website owners, the best defenses involve reducing or eliminating the attack surface. Some effective methods include eliminating the use of email addresses as the unique identifier for usernames and adding a third element (in addition to a username and password) to login pages, such as last name or customer ID. Implementing multi-factor authentication also helps immensely.

• End users can protect themselves and reduce the risk of being victims of credential abuse-related fraud by avoiding password reuse. Using a password manager to handle and generate strong and unique passwords and enabling multi-factor authentication wherever possible are critical.
Overview

Introduction

The Open Web Application Security Project (OWASP) defines credential stuffing (also known as password stuffing, account checking, or credential abuse) as “the automated injection of breached username/password pairs in order to fraudulently gain access to user accounts. This is a subset of the brute-force attack category: Large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.”2 Akamai CSO Andy Ellis recently explained this threat in a short video. Credential abuse may be carried out by cybercriminals for financial gain, by hacktivists to further their cause, or by nation-state actors to steal data or support cyber operations.

Credential abuse from a typical botnet requires three factors to be successful: 1) a list of usernames and passwords to attempt login, 2) a legion of open proxies or bots to do the dirty work of checking the credentials, and 3) the technical knowledge about how and where to target the web application. Attackers must gather some credentials for the login attempts, either by purchasing lists of leaked username and password pairs inexpensively on the Dark Web or by downloading the lists freely on the web. Getting a list of working proxies is usually easier, as there are many sites that maintain an index of open proxies or tools to help build a working list. The technical knowledge about the targeted site is usually the most complicated and most expensive aspect to acquire, yet some tools already supply this information.

The result of a successful credential stuffing attack is usually account takeover, where the stolen, but valid, credentials may be sold to other threat actors, used to drain the account of stored value, or used to steal data. Credential abuse attacks are usually done automatically by bots, whereas account takeover attacks may be carefully executed manually by threat actors.

Figure 1: Overview of credential abuse and account takeover attacks

2 https://www.owasp.org/index.php/Credential_stuffing
Finding Credentials

Nearly every week, there are news reports about a company being breached or a sensitive database exposed. The results of these leaks may be compiled and offered for sale or shared freely, such as the recent dump of 42 million emails, passwords, and partial credit card data that was uploaded to a free and public file hosting service. Breached data can include sensitive information such as usernames, email addresses, mailing addresses, telephone numbers, Social Security numbers, and in many cases, cleartext passwords. This leaked data is also collected and shared on credential abuse forums, on anonymous text storage sites like Pastebin, or on the Dark Web. The Dark Web offers a vast set of hacker resources, and in some cases, archives have been found with compilation lists of over 1.4 billion credentials from various breaches.

Finding leaked credentials is easy and inexpensive. A simple Google search with the right keywords reveals an astonishing number of credentials available in paste sites and forums without even having to look on the Dark Web. In many cases, a snippet of thousands of credentials is offered as a sample of a much larger set that can be bought for around $20. However, lists of leaked credentials can often be obtained for free. Data intended for use in credential abuse attacks is usually in the text format of username:password and is referred to as a “combo list,” which is a list containing a combination of usernames and their associated passwords. Email addresses are the most popular form of usernames.

Because credential reuse is so rampant on the Internet, oftentimes these combinations will work on many different websites. A data breach can therefore have a cascading effect and cause collateral damage on seemingly unrelated websites. The use of strong, unique passwords for every website and enabling multi-factor authentication (whenever possible) drastically reduces impact of these breaches.

Figure 2: Sample data from a recent “combo list” dump, retrieved from Bleeping Computer
Hidden in Plain Sight: The Tools and Resources Used in Credential Abuse Attacks

Figure 3: Pastebin credentials offer

Figure 4: Cracking forum with credentials for sale
Proxies and Credential Abuse Attacks

A proxy allows one to “hide” their IP address by routing traffic from their computer through the proxy to the targeted site, causing the target site to see the connecting IP of the proxy instead of the end user. An open or public proxy is one that does not require authentication to be used and thus is lucrative for abuse by criminals. In credential abuse attacks, the use of many proxies and bots is usually crucial to success since web applications may have security controls in place to detect and limit excessive requests from individual IP addresses. Proxies typically include HTTP headers such as X-Forwarded-For or similar information to identify the client IP that originated the request. An anonymous proxy strips this identifying information and may also not retain logs of activity on the proxy system in order to protect the privacy of its users. Threat actors prefer using anonymous proxies over transparent proxies that may leak potentially identifying information (like their source IP address) and cause them to get caught by law enforcement.

A threat actor with good operational security techniques runs their attack tools from a dedicated/hosted server and connects to that server using a Virtual Private Network (VPN), further obfuscating the true source of their traffic. Attackers may also use proxies to bypass geo blocking restrictions in place for web applications by utilizing a proxy in an allowed geographical location. The use of proxies may cause a credential abuse attack to appear to be coming from a botnet, yet further investigation could reveal the source IPs as misconfigured open proxy servers instead of malware-infected devices. Another benefit to attackers of utilizing proxy servers is distributing the workload of checking the credentials against the target site(s).

![Free Proxy List](https://freeproxy-list.net)

**Figure 5:** Free-proxy-list-net, one of many sites that offer free proxy lists for use
The Tools and the Lab Environment

As part of this research, we analyzed three common tools that are used for credential abuse and account checking. The purpose of our analysis is to provide intelligence on the capabilities of popular tools used by attackers so businesses can better protect their assets and those of their customers. The following tools are included in our analysis: Cr3d0v3r, Sentry MBA, and SNIPR. Publicly available tools like these may be used by less sophisticated cybercriminals, “script kiddies,” and hacktivists. However, these tools can be quite effective in credential abuse attacks, despite their low threshold to use. Sophisticated groups and nation-state actors often develop their own tools for the specific target or task.

We ran these tools against a lab environment WordPress login page protected by Akamai using a set of fake credentials. Three valid user/password combinations were intentionally included as part of the credentials used.

Success and Failure Keywords

Credential abuse tools rely on success and failure keywords to separate valid credentials from invalid ones. These keywords can be part of the response HTML such as “Welcome, User X” or “Please enter a valid password”, as part of a response header such as “Set-Cookie: wordpress_logged_in_abc123”, or as part of a response code like a “200 OK” versus a “302 with Location:/user/profile.php” response.

For this exercise, we used the following keywords as part of our success and failure scenarios:

- **Success Keyword:** “Howdy,”
- **Failure Keyword:** “ERROR,”

The following screenshot shows the result of logging in with user@fakemail.com and a correct password.
Credential Abuse Tools

Cr3d0v3r

The first tool we analyzed was Cr3d0v3r. The author describes it as “your best friend in credential reuse attacks,” and this simple tool has two main functions:

When provided an email address, it searches for public leaks where the email was exposed and then it tries to obtain the plaintext passwords from leaked information.

When provided a username/password, it checks the credentials against 14 popular websites like Facebook, Twitter, and LinkedIn, and reports if the credentials are valid.

We know that people often use the same password for more than one website or application on the Internet and choose insecure passwords. This only contributes to the credential abuse problem as exposed passwords from third-party breaches are valid on totally different websites and applications, causing collateral damage.

How does it work?

Cr3d0v3r is a Python script that leverages Troy Hunt’s popular HaveIBeenPwned? service to see if an email address was compromised and found in a data breach. If a result is found, the tool checks the GhostProject to determine if cleartext passwords are available in the data leak(s), displaying any positive results.

By supplying credentials to Cr3d0v3r, it can check if they are valid on popular websites, such as eBay, GitHub, and Wikipedia. It also gives users the option to use the passwords found by the tool or to provide a password. The list of sites to check is customizable and there is a guide available with instructions on how to modify the tool to include additional websites.

Installation

The installation is straightforward, and the download is available from GitHub. For Windows users, the author provides a zip file with all the required resources. Linux users can use Git to download the required files, then use “pip,” the Python Package Manager, to download additional requirements. There is a Docker container available for Docker users.

Usage

Cr3d0v3r is executed as a command line program, requiring the user to supply an email address to check. If the email address is found in a public leak and plaintext passwords are available, the user can direct Cr3d0v3r to attempt to log in to well-known websites with the credentials and report back the results. If the email address is not found in a public leak, the user can enter a password to check the login against the default list of websites.
Additional Features

Cr3d0v3r depends on login forms to check if the login is successful or not, without the need to search for specific strings. To find the username and password fields within the login page, Cr3d0v3r uses CSS selectors. The only requirement is that these fields should be unique and should not change if credentials are invalid.

The list of websites against which Cr3d0v3r will attempt to log in is customizable and the user can add or delete websites as needed. There is a guide on GitHub with instructions on how to modify the tool to include additional websites. The following is a snippet of the code used to add a new website:

```javascript
1 2 3 4 5 6 7
example = {
  "url":"",  #The url of the login page
  "form":"",  #The login form CSS Selector
  "e_form":"",  #The email input name
  "p_form":""  #The password input name
}
```

Figure 8: Cr3d0v3r execution

Figure 9: Cr3d0v3r new website template
Weaponization

Even though Cr3d0v3r is designed to be used with a single email address and for “educational purpose,” it only takes a few lines of code to enable this Python script to check a list of email addresses instead of just one. Email addresses that have passwords leaked in cleartext can be used later against the list of sites or against any other website. Attackers can modify the tool to check more websites than the default 14.

Sentry MBA

Sentry MBA is one of the most common tools used for credential abuse attacks. For a while, it was the favorite credential abuse tool among cracking forums. It was originally developed by a user called “Sentinel,” and it came with a disclaimer that users must only run it against their own sites. Sentry was later updated by a member of the underground cracking community, “Astaris,” who added MBA (Modded by Astaris) to the title, along with their enhancements. The free tool is still popular among cracking forums even though it hasn’t been officially updated since 2012. Other cracking community members have released modified versions with their own bug fixes and enhancements, similar to what Astaris did.

The tool is free to download and run, and is available for Microsoft Windows operating systems. It comes with detailed readme files and release notes that include a log of all the versions, bug fixes, and new features. The program has a user-friendly graphical user interface and UI help available for several of its settings.

As per the release notes, some of the tool’s features include:

- OCR Support (Optical Character Recognition)
- Configurable Keywords Capture
- Fixed Captcha OCR Sites
- Form Redirects
- HTTPS
- Special Keywords Matching Functions
- Socks 4a/5
- Proxy Analyzer

Installation

Sentry MBA can be freely downloaded as a zip file, which includes the Windows executable and all the required DLLs, configurations, and documentation files. The program is a standalone executable and requires no further installation after unzipping the contents of the zip archive.
Usage & Modules
Sentry MBA's GUI is divided into six modules:

- Settings
- Lists
- History
- Tools
- Progression
- About

Settings Module
This module allows the user to configure the settings specific to the website to be attacked. It also allows for header manipulation. The user can choose from a default list of predefined user-agents or add their own to the list. Other HTTP headers such as Referer, Accept-Encoding, and Connection can be added or modified.

By default, Sentry MBA uses the following hard-coded and outdated HTTP user-agents:

- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
- Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en) AppleWebKit/522.11.3 (KHTML, like Gecko) Version/3.0 Safari/522.11.3
- Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.0 Version/10.00
Different request methods can be used to check credentials against the site. By default, the tool uses GET requests, but can be configured to use the HEAD or POST request methods. POST settings have a dedicated window where the user can either input the POST parameters to use or let the tool’s “Master Wizard” feature analyze the login page to automatically populate the parameters, along with other settings like Session Cookies.

Other sections in this module include Proxy Settings, which allows the user to configure different thresholds to determine if a proxy is still available; Fake Settings, which allows the user to configure additional validation; and HTTP Settings. The Keywords module uses configurable keywords to differentiate a successful login from an unsuccessful one and can be used in different parts of the HTTP response, such as the source HTML or response headers such as cookies, redirect locations, or response codes.

Figure 12: Sentry MBA keyword settings
Lists Module

The Lists module allows the user to upload a list of username:password combinations or separate lists of users and passwords. It also enables the user to upload a list of proxies to use. One interesting feature: Proxies that are no longer responding or appear to be blocked (HTTP 403 response code) are banned and thus removed from the algorithm.

History, Progression, and Tools Modules

The Progression tab allows the user to understand progress made with a particular set of credentials and change the number of bots (concurrent jobs) being used. Valid credentials are saved to the History tab for future reference. The Tools tab includes some additional features such as an HTTP debugger and a proxy analyzer to check if the proxies used are still working.
Configuration Files

Sentry MBA allows the user to save or import settings from a snapshot or configuration file. This enables users to create and share configuration files with the rest of the community.
Similar to the findings with credentials “combo lists,” these configuration files are shared on sites such as Pastebin and on cracking forums. A quick Google search for “Sentry MBA Config” reveals a little over 300 configuration files on Pastebin. However, there is definitely a market for skilled individuals to create working configs, and people will pay $20 or more for these services.

**Figure 17: Sentry MBA configuration files available on a cracking forum**

### SNIPR

The final tool we will analyze, SNIPR, is the most advanced. Akamai wrote about SNIPR in March 2018 and was perhaps the first to publish information about the tool. SNIPR claims to be the first C# implementation of a configurable combo list checker and an “all-in-one toolkit” for account and email checking. Similar to Cr3d0v3r and Sentry MBA, this tool easily enables users to check credentials against several popular websites, but it comes with more features and is regularly updated.

Developed and maintained by a threat actor under the alias “PRAGMA,” SNIPR is free to download. However, it requires a one-time payment of $20 for a license key, which the user can pay in certain cryptocurrencies or by purchasing an Amazon U.K. gift card. The tool has been receiving frequent updates and support since April 2017, and has an active and robust user community.

According to its website, SNIPR has several features:

- **Live-Chat Support** provides instant and real time support to customers.
- **Modern UI** is designed with ease of use as a priority.
- **Library of Configurations**: The tool comes loaded with over 100 target website configurations out of the box that are maintained by the author.
- **Public-Repo Support**: Any activated SNIPR user can upload target site configurations to the public repository, which contains configurations maintained by the community.
- **Concurrent Checking**: You can check up to four target site configurations at once.
- **Unlimited Combo-Size Support**: Load any combo list, regardless of how big it is.
- **Config-Editor GUI** allows you to create and edit SNIPR configurations.
- **Config-Encryption** allows you to save and encrypt configs to avoid viewing or editing.
Installation

Installation of SNIPR is simple and straightforward. The tool is developed for 32-bit or 64-bit Microsoft Windows operating systems. A free download with a zip archive is provided with all the required files; however, the tool cannot be used unless an activation key is entered. The activation key costs $20, and according to PRAGMA (SNIPR creator), access will be provided within 24 hours of payment. “Cracked” versions of the tool that don’t require a key are available in underground forums, but the cracked software is often bundled with malware. The program is a standalone executable and requires no further installation after unzipping the contents of the downloaded archive.

Community and Support

One of SNIPR’s key features is its community and support. The author provides live support via chat using Chatra and via a community forum on the tool’s website. There used to be a SNIPR subreddit, but they migrated to the current community forum. There is a FAQ on the website and a very active community that continuously contributes with new public configurations, credential leaks, proxy lists, bug reports, and suggestions (enhancement requests), among other topics. There are even several tutorial videos on YouTube by community members showing how to download, install, and run SNIPR against different websites.

Usage

As described on the SNIPR website, the tool’s UI is easy to use. SNIPR comes preloaded with over 100 target website configurations that are presented to the user after launching the tool. Configurations marked in blue require the use of active proxies while those marked in green are considered “proxyless.”

Once the user has selected the site(s) to be attacked (up to 4 sites concurrently), the next step is to load the credential combo list, and optionally a list of open proxies, to carry the traffic.
Proxy Features

SNIPR supports uploading a user-supplied list of proxies to route traffic through to the target web application. In case the user does not already have a list of open proxies to use, another useful feature of SNIPR is an open proxy list generator that grabs open proxies from many open proxy sites and indexes available on the web.

Besides the proxy list generator feature, the tool allows the user to check if the proxies on the list are still working or “alive.” The list of proxies to check could be a custom list uploaded by the user or an automatically generated list created by the proxy grabbing feature.
Configuration Files

The last critical piece required for a successful credential abuse attack is the configuration for how and where on the targeted website to pass credentials from the combo list. At the time of writing, SNIPR comes preloaded with 115 “official” configuration files and a community-maintained repository of 157 “public” configuration files. The “official” repository for configuration files is maintained and updated by the tool developer on a regular basis. These configuration files cover websites in different industry verticals, ranging from Retail, Gaming, and Travel to Pornography and Gambling.

Both configuration repositories can be found at the following links on the SNIPR website:

- hxxp://repo.snipr.gg/official/configs/
- hxxp://repo.snipr.gg/public/configs/

The configuration files are JSON-based and contain information about the URL(s) to test, request parameters, HTTP headers to be included, success and failure indication keys, and other data that can be captured as part of a successful login (such as gift card/loyalty program/customer account balances and/or points). **We strongly suggest Akamai customers review both SNIPR configuration repositories to see if their websites are included and then take measures to avoid further abuse.**

Once the tool is loaded with username and password combinations, a list of proxies to use, and a target site selected, the only thing left to do is hit the “Play” button and wait. The tool will display valid credentials and results as it finds them, without waiting for the entire combo list to be checked.
For our testing, we created a new configuration and started an attack against our test site. We also used a custom proxy list that we manually uploaded. The configuration file looked like this:

```json
*
"General": {
  "name": "MyWordPressLab",
  "proxyType": "Proxyless",
  "comboType": "Email",
  "note": "Created for testing purposes"
},

"Requests": {
  
  "actionUrl": "http://example.net/wp-login.php",
  "method": "GET",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0",
  "accept": "text/html,application/xhtml+xml,application/xml;q=0.9,"*,
  "referer": "http://example.net",
  "successKeys": []
  "Back to AAR LAB"
},

"session": {
  "session": "https://example.net/wp-login.php",
  "method": "POST",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:61.0) Gecko/20100101 Firefox/61.0",
  "cookie": "wordpress_logged_in_cookie=RF=Cookie+check",
  "postData": "log=USER&pwd=PASS&submit=Log+In&redirect_to=http%3A%2F%2Fexample.net%2Fwp-admin%2Ffitestcookie1",
  "successKeys": []
},

"failureKeys": {
  "ERROR": "Invalid email address."
},
```

Figure 22: SNIPR valid credentials found on test environment website

Figure 23: SNIPR custom site configuration file
Akamai Detection Capabilities

We ran these three tools against our WordPress lab login page that is protected by Akamai’s Bot Manager Premier cloud security solution, and in all three cases the Behavior Anomaly Detections caught the malicious activity.

Bot Manager Premier introduces new behavior anomaly analysis capabilities proven to be successful in detecting many of the most sophisticated bots currently in evidence. It is able to detect bot activity disguised as human interactions even if the bots continually modify information in an attempt to evade detection.

For more information about Bot Manager Premier and its configuration, reach out to your Akamai Account Manager or Professional Services contact.

![Figure 24: Bot Manager detected activity; Bot Categories](image)

**Note:** The user-agents shown for Sentry MBA and Cr3d0v3r are the default user-agents, yet they can be modified based on the user’s preferences. SNIPR’s user-agent is set per configuration file, which means that different configuration files would result in different user-agents observed. The user-agent shown below for SNIPR was manually configured as part of our custom website settings. See Figure 23 above for more info about the lab configuration details.
Hidden in Plain Sight: The Tools and Resources Used in Credential Abuse Attacks

Figure 25: Bot Manager detected activity; user-agent
Protection Recommendations

As a website owner or defender:

- A recommended additional layer of protection against credential abuse attacks is for the web application to have strong authentication (especially multi-factor) and identity and access management.

- Organizations should not use email addresses as usernames for authentication. Many leaked credential lists contain email address/password pairs and thus are easy to validate across many websites, especially when users reuse the same password on multiple websites.

- Users should be required to create a unique user ID specific to the website and provide a second factor of authentication such as a one-time code in addition to their user ID and password when logging in.

- This can also help protect both the user and the organization from ripple effects due to third-party data breaches.

- Adding a third informational proof element to login pages, such customer ID or last name, has proven to be very effective for several companies in the Hotel & Travel industry.

- Customers of Bot Manager Premier can leverage Behavioral Controls in Deny Mode to protect sensitive transactional URLs such as login, account creation, and gift card checking to block this malicious activity at the edge of the Internet.

- Akamai strongly suggests customers review the SNIPR configuration repositories listed above to see if their websites are included as potential targets for SNIPR users, and take measures to avoid further abuse.

As an end user:

End users can reduce the risk of being victims of account takeover attacks by enabling multi-factor authentication where possible and by avoiding password reuse with the help of a password manager. Use a password manager such as LastPass or 1Password to generate strong unique passwords for every website that requires authentication. Never use the same password twice and never on more than one website or application.