Cyberint
Protection Beyond the Perimeter

Threat Brief

Account Checkers & Credential Stuffing

www.cyberint.com

Cyberint
Protection Beyond the Perimeter

Contents

Introduction

Cyberint has observed increased use and availability of 'account checker' tools that allow threat actors to bulk test credentials, typically obtained from data breaches or leaks, against a variety of online retailers and services. These 'credential stuffing' attacks allow threat actors to identify customers that have reused the same credentials across multiple sites and, when a successful combination of credentials has been found, automatically extract pertinent account information such as details of any credit balance or subscription status.

Once a list of valid credentials for an online retailer or service has been identified through the use of an account checker, their value can be determined at a glance (Figure 1) and subsequently traded on underground marketplaces and forums, if not directly abused by the threat actor.

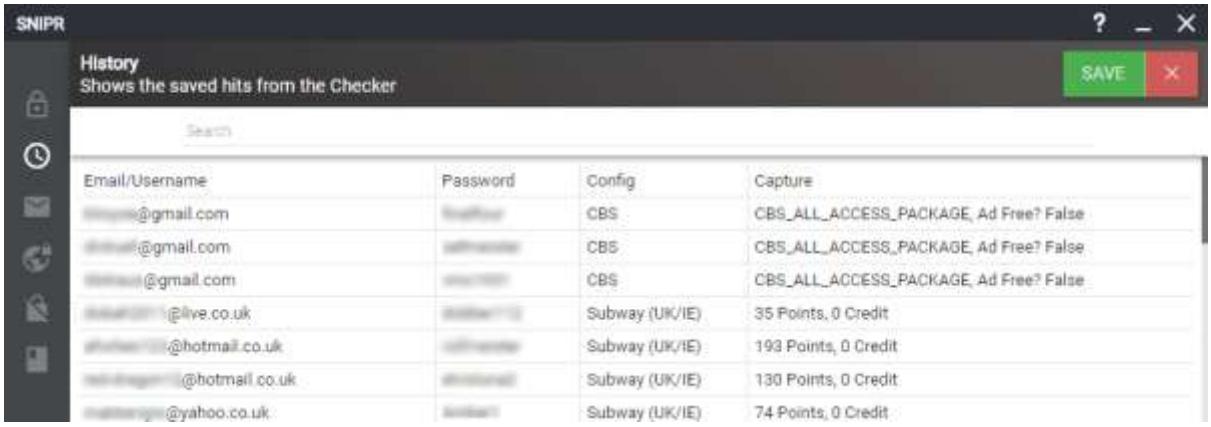

Figure 1 - Account checker with additional details (SNIPR)

Subsequent abuse of compromised accounts can include the extraction of payment card data, if not properly secured by the retailer, theft of credit or gift card balances, and the fraudulent acquisition of goods and services.

In the last case of fraudulent transactions involving digital goods, such as the purchasing of gift cards, subscription codes or digital download codes, the act itself requires little sophistication on behalf of the threat actor. Digital purchases can typically be completed by a threat actor from anywhere in the world and will be easy to resell or trade. Conversely, transactions involving physical goods will likely require a threat actor to be located in the same region as the retailer as well as need a 'drop' address to receive the goods so that the fraud is not directly linked to him.

Whilst numerous site- and service-specific account checkers exist (Figure 2) as both online tools and downloadable executables, this report focuses on two extensible tools that are readily available, well-supported and popular amongst threat actors wishing to target a variety of online retailers and services, i.e. 'Sentry MBA' and 'SNIPR'.

Figure 2 - Example site/service-specific account checkers

'Combo' Preparation

Before using the account checker tool, the threat actor will first need to obtain and compile a list of 'combos', that being a text file containing a combination of potential usernames or email addresses as well as passwords (Figure 3).

```
[redacted]@gmail.com:aaaa
[redacted]@[redacted].com:88888888
[redacted]@[redacted].net:kindness
[redacted]@hotmail.com:borg
[redacted]@[redacted].net:hello23
```

Figure 3 - Example 'combos' list in the format <email address>:<password>

In addition to commonly being traded on underground forums and marketplaces (Figure 4), many threat actors may seek to download or build their own 'combos' from leaked credential dumps often posted to text-sharing websites.

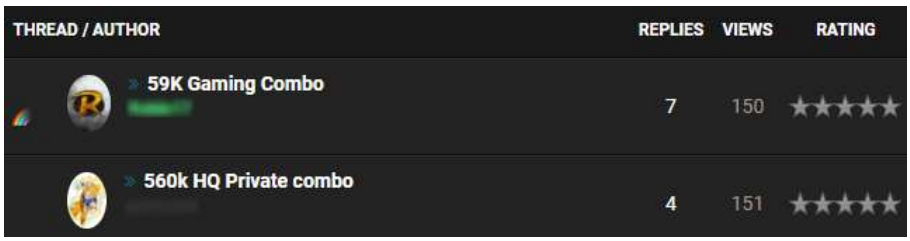

Figure 4 – Example trade of 'Combos'

While a few advanced threat actors may compromise hosts to gather their own sets of credentials, the most common users of these tools will be less capable and therefore reliant on combos obtained from other sources.

Furthermore, threat actors experienced in the use of account checkers may seek to increase the tool's efficacy by compiling targeted lists of credentials, for example, building a list containing only '.co.uk' based credentials to target a UK-based organisation.

Considering that over five-million data records are reportedly lost or stolen every day[1] and that numerous studies and surveys have indicated that sometimes up to 80% of users reuse passwords across multiple sites, the potential return on investment for threat actors is incredibly high. The off-the-shelf nature of these tools, credential sets and site-specific configurations, allow unsophisticated threat actors to be relatively successful when using high volumes of lost or stolen credentials given the high proportion of users with poor security practices.

Anonymisation

Once the credential set has been prepared, both Sentry MBA and SNIPR tools support the use of proxies in order to anonymise and mask the threat actor's account checking activity. Both tools support the loading of a pre-prepared proxy list from a text file; that said, SNIPR also features a 'Proxy-Leecher', automatically scraping IP addresses and ports from various proxy listing websites (Figure 5).

IP Address	Port	Code	Anonymity	Https
191.101.	80	US	anonymous	yes
207.246.	8080	US	elite proxy	yes

Figure 5 - Example proxy listing website

This scraping feature further simplifies the process for the threat actor and potentially increases the number of IP addresses from which account checking activity would originate, increasing the difficulty for site owners to detect and mitigate.

[1] http://breachlevelindex.com/

Sentry MBA

Originally developed by an individual using the alias 'Sentinel', potentially as a legitimate security tool for web security testing, the source code was apparently released leading to the current 'MBA' versions that include a number of additions and features contributed by an individual using the alias 'Astaris' (Figure 6) amongst others.

```
1   DISCLAIMER
2   This program is intended ONLY for testing your own sites.
3   Any other use of this program is forbidden.
4   The Author does not take responsibility for any improper use of the program.
5
6   ABOUT MBA
7   This version of Sentry is labeled Sentry MBA,  i.e. Sentry 2.0 modded by Astaris.
8   My thanks go to Sentinel for making this wonderful program and for giving away for free the source code.
```

Figure 6 - Sentry MBA 'ReadMe.txt'

Widely traded and available for free on various underground forums, numerous versions of the tool exist and are often modified to include a particular group's name in the title bar. Of these, the 'Sentry MBA' forum[2] claims to be the official repository of Sentry MBA, offering version 1.4.1 (Figure 7) for free when registering a new account to the forum.

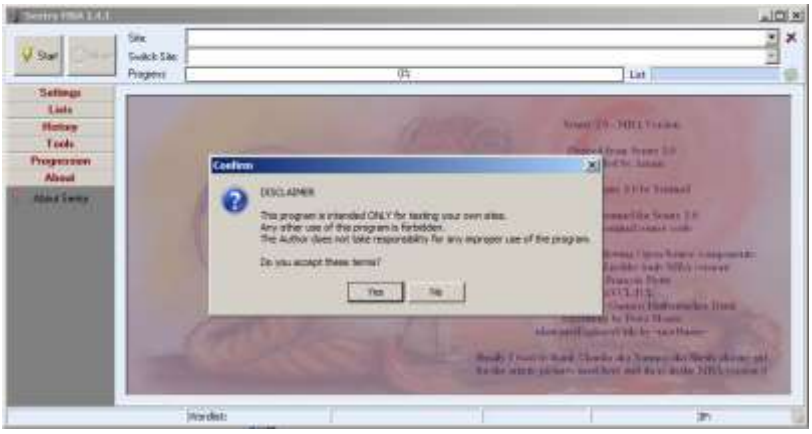

Figure 7 - Sentry MBA 1.4.1 (Initial dialog)

Functionality amongst the currently available releases appears to be somewhat consistent and includes 'teseract', a CAPTCHA[3] cracking capability which uses an optical character recognition (OCR) component that can be updated to defeat new CAPTCHA methods (Figure 8), as well as support for Ajax, HTTPS, SOCKS 4a/5 proxies, keyword capture and JavaScript/form redirects.

[2] hxxps://sentry.mba
[3] https://en.wikipedia.org/wiki/CAPTCHA

Figure 8 - Sentry MBA 1.4.1 'Settings', including OCR 'Images Database' configuration

Additionally, a proxy analyser can determine the status of imported proxies and remove/filter those that fail to handle requests correctly.

Whilst Sentry MBA allows a threat actor to configure his own attacks using the debug utility and other features within the tool, the true value of Sentry MBA comes from its ability to load pre-defined configuration files for specific sites (Figure 9).

```
8   [Settings]
9   SiteURL=https://www.[redacted].com/ap/signin?openid.ns=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0&pageId=[redacted]&open
    id.identity=http%3A%2F%2Fspecs.openid.net%2Fauth%2F2.0%2Fidentifier_select&openid.claimed_id=http%3A%2F%2Fspecs.openid.
    net%2Fauth%2F2.0%2Fidentifier_select&openid.mode=checkid_setup&marketPlaceId=[redacted]&openid.assoc_handle=[redacted]
    ents&openid.return_to=https%3A%2F%2Fpayments.[redacted].com%3A443%2Foverview&openid.pape.max_auth_age=0&openid.pape.preferr
    ed_auth_policies=http%3A%2F%2Fschemas.[redacted].com%2Fpape%2Fpolicies%2
    F2010%2F05%2Fsingle-factor-strong&ld=[redacted]
```

Figure 9 – Example Sentry MBA site configuration (site URL)

These configuration files, which typically target online retailers, streaming services and video game sites, are readily available on underground forums and marketplaces, and provide site-specific parameters such as the target webpage for 'credential stuffing.' The files also specify strings that, when matched, determine the success or failure of each tested credential combination (Figure 10).

```
85   SourceSuccess=Sign Out;seen you using this device before. To help protect your account
86   SourceBan=
87   SourceFail=There was an error with your E-Mail/Password combination. Please try again.
```

Figure 10 – Example Sentry MBA site configuration (success/failure parameters)

Furthermore, HTTP headers, POST data and user-agents are often specified in the configuration files and as such, may provide an opportunity to detect the use of the tool based on unexpected duplication of typically unique or anomalous values.

Finally, parameters to parse the content of the authenticated page (Figure 11) can be defined to automatically extract data of interest to the threat actor, for example, account balances or subscription status.

```
115   ParsingCode=
116   FormRedirectUrl=https://www.[redacted].com/gp/css/gc/balance?ie=UTF8&ref_=ya_view_gc
117   RedPostData=
118   RedKeys=<Source>||Sign Out
119   DataDesc=Gift Card Balance&Total Orders
120   CaptureParsingCode=<span>|<|#00|RedURL|0|#00|#00|0&-orders">|  |#00|AddURL|0|#00|#00|0
```

Figure 11 – Example Sentry MBA site configuration (account detail parser)

Upon execution of the tool, the threat actor will load his target site configuration file, import a pre-prepared list of proxies and finally import the credential 'combo' for testing. Subsequently clicking on 'Start' will commence the credential stuffing process, attempting to authenticate to the target site using each set of credentials whilst cycling through the list of proxy servers in an attempt to make the access attempts appear legitimate and therefore unsuspicious (Figure 12).

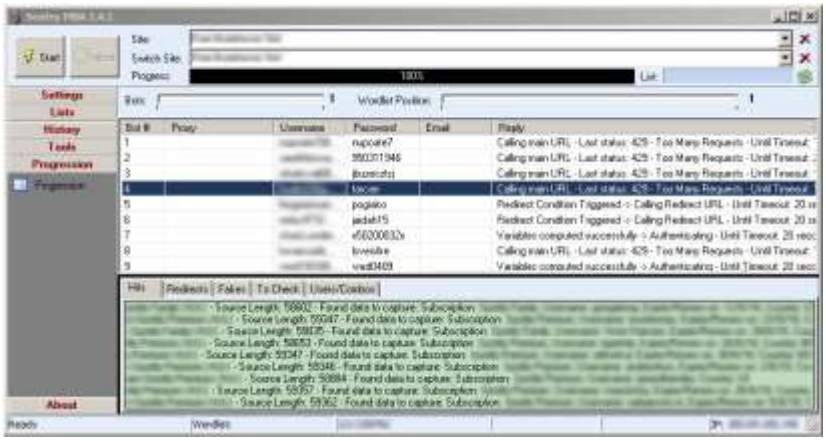

Figure 12 – Sentry MBA 'credential stuffing' progress

During and upon completion of the process the threat actor is presented with a list of 'Hits', i.e. successfully authenticated credentials that can be directly abused or resold, as well as lists of 'Redirects' and 'Fakes' that have failed to authenticate or are invalid.

SNIPR

Similar in function to Sentry MBA, SNIPR (aka SNIPEthemHITS) has been developed by an individual using the alias 'PRAGMA' and is available to download and purchase from its official

webpage[4]. The executable is freely downloadable; however, the program cannot be used without first purchasing a license key for USD15, using cryptocurrency, or a GBP15 Amazon.co.uk gift card, potentially suggesting that the author of this program is UK-based (Figure 13).

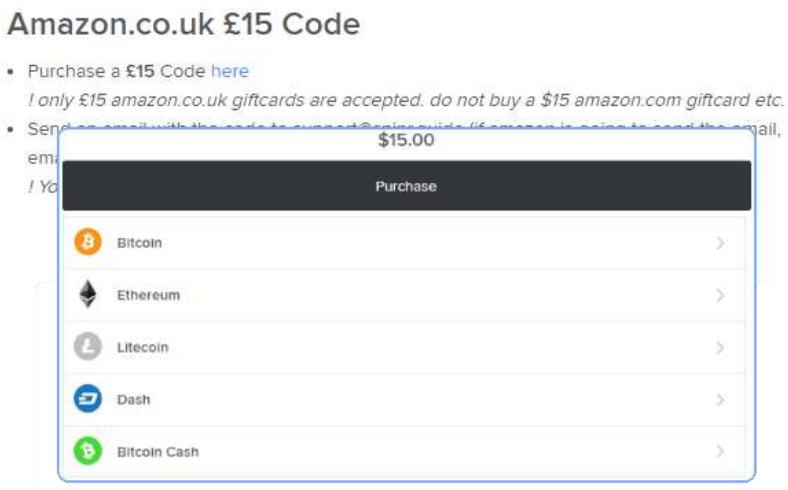

Figure 13 – SNIPR Key purchase

Whilst the current release version is 3.3.x, unsurprisingly 'cracked' versions (v2.x) are available on some underground forums and negate the need to purchase a key.

Upon loading the tool, a number of 'official' configurations are displayed which, unlike Sentry MBA, allow a threat actor to target a variety of sites and services 'out-of-the-box' (Figure 14) for online retailers, streaming services and video game sites. Notably, the interface also supports multiple languages (currently Albanian, English, French, German and Italian).

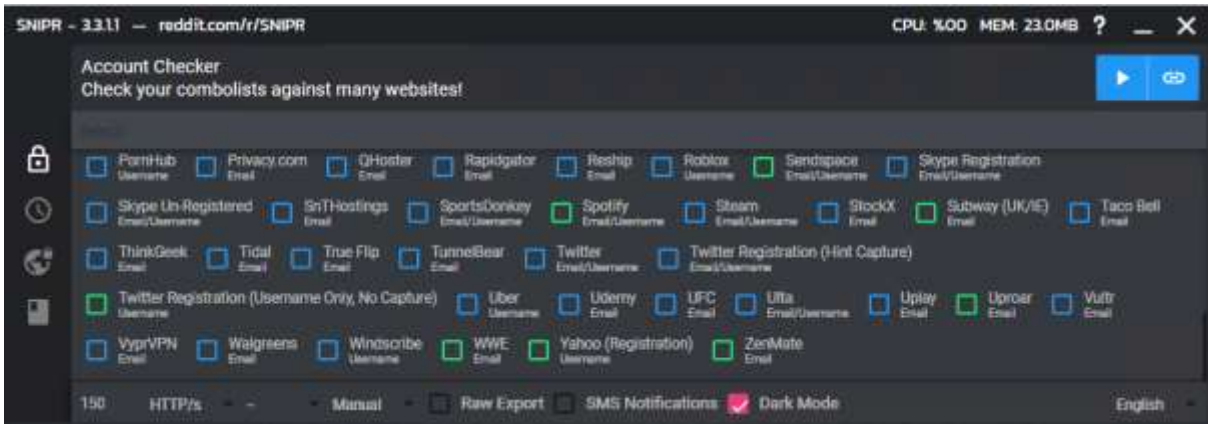

Figure 14 – SNIPR 'out-of-the-box' official configurations

[4] hxxps://snipr.guide

Given the nature of the tools, the core functionality of SNIPR and Sentry MBA is understandably similar. That said, the simplicity of SNIPR and the inclusion of both 'official' configurations as well as the 'Proxy-Leecher' (Figure 15), used to parse public proxy websites rather than manually preparing a proxy list, will appeal to less-experienced threat actors.

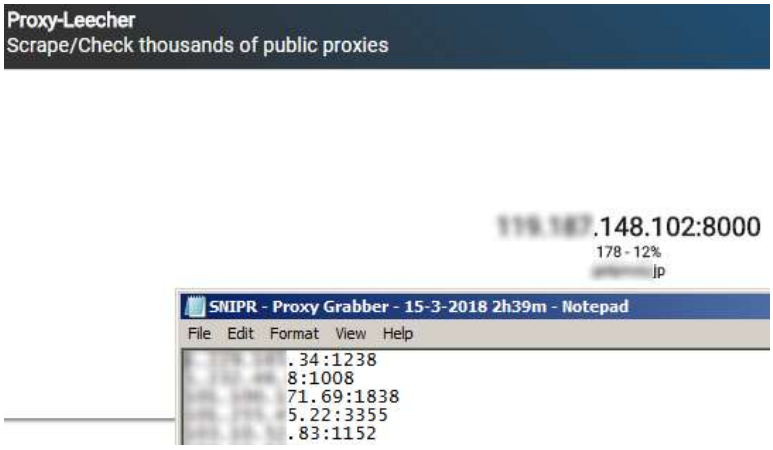

Figure 15 – SNIPR 'Proxy-Leecher' feature

Furthermore, not all target site configurations require the use of a proxy and this is indicated by the colour of the tick box displayed in the main interface: green configurations are 'proxyless' whilst blue configurations require the use of a 'proxy'. Given this, inexperienced threat actors may attempt to utilise the tool without taking additional steps to protect their identity, such as the use of VPN's or anonymisation networks.

Site and service configurations are similar in logic to Sentry MBA's 'ini' files, albeit appearing to be JSON, and the credential stuffing target URL can be identified along with other hard-coded 'request' parameters (Figure 16).

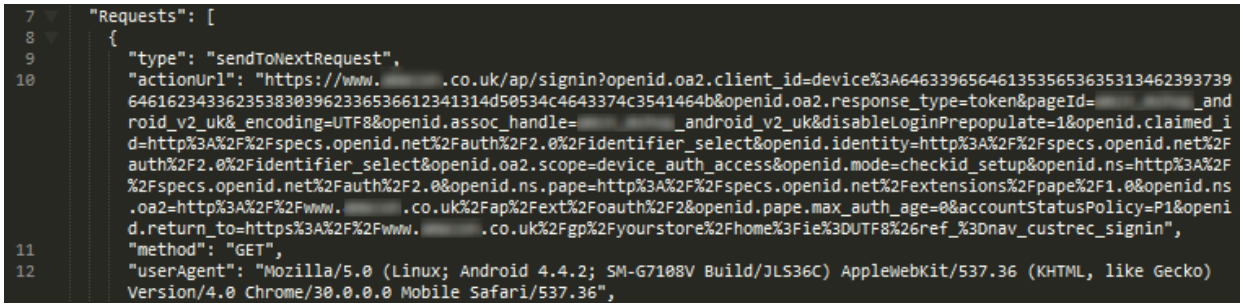

Figure 16 – Example SNIPR configuration file (site URL)

Similarly, the configuration file specifies the strings that, when matched, determine the success or failure of each tested credential combination, as well as extract useful information such as account balances or subscription statuses from authenticated accounts (Figure 17).

```
169         "failureKeys": [
170           "Your password is incorrect",
171           "For your security, we need you to reset the password on your account",
172           "Your account has been locked for security purposes."
173         ]
174       },
175       {
176         "type": "CaptureProcessing",
177         "actionUrl": "https://www.[redacted].co.uk/gp/css/gc/balance?ie=UTF8&ref_=ya_view_gc",
178         "method": "GET",
179         "userAgent": "Mozilla/5.0 (Linux; Android 4.4.2; SM-G7108V Build/JLS36C) AppleWebKit/537.36 (KHTML, like Gecko)
          Version/4.0 Chrome/30.0.0.0 Mobile Safari/537.36",
180         "contentType": "",
181         "accept": "",
182         "referer": "",
183         "headers": [
184           {
185             "name": "X-Requested-With",
186             "value": "com.[redacted].android.shopping"
187           }
188         ],
189         "successKeys": [
190           "<title>Current Balance</title>"
191         ],
192         "captureParse": {
193           "patterns": [
194             {
195               "pattern": 'Current Balance:\\s*<span>([^<]*)',
196               "returnString": "+1+ Gift Card Balance"
```

Figure 17 – Example SNIPR configuration file (Success string, line 190; Failure string, lines 170-172; Data extraction, line 195)

Notably, the configuration files seemingly include a number of hard-coded values such as user-agent strings and cookie values which may provide further opportunities for detection.

Having selected or loaded a site configuration, imported or 'leeched' a proxy list and loaded a 'combo' list, starting the account checker process will result in the credentials being tested (Figure 18) against the target site as it cycles through the proxy list (when applicable). Additionally, up to four configurations can be 'checked' during the same process, further streamlining the activity and increasing the effectiveness of the credential stuffing operation.

Figure 18 – SNIPR 'credential stuffing' progress

Similar to Sentry MBA, during and upon completion of the process, the threat actor is presented with a list of 'Hits', those being successfully authenticated credentials along with any 'capture' data, as well as a count of invalid accounts and those awaiting retry.

Mitigations

Multi-factor Authentication

The implementation of multi-factor authentication (MFA) provides the best defence against credential stuffing attacks, such as those performed by these account checking tools. as Without the code obtained from something in the possession of the customer, be that a SMS code or hard/software token, the credentials are useless and the threat actor cannot proceed with the purchase. If MFA has already been implemented, customers should be educated on its security benefits, and steps should be taken to both encourage its use and prevent it from being disabled without additional authentication steps.

IP Address Monitoring/Blacklists

Whilst more experienced threat actors may take further steps to anonymise their connection when using these tools, for example tunnelling their activity via a virtual private network (VPN) or Tor, both of the discussed account checker/credential stuffing tools provide support for proxies in order to hide the threat actor's true IP address and to mask the successive account login activity that is originating from the same source.

Given this, specifically monitoring for activity originating from suspicious networks or hosts, such as open proxies, Tor exit nodes or known VPN providers, may identify potentially malicious or nefarious activity that can be restricted or blocked accordingly (Figure 19).

Figure 19 - Example 'Access Denied' message when accessing a retailer's website via Tor

Behavioural Analysis

The monitoring and analysis of 'normal' customer connection behaviour, including device fingerprinting, access times and geolocation, can also be used to determine abnormalities, such as account compromise, and used to either restrict account activity or prompt for an additional layer of authentication. For example, if a user typically connects to the site or service using a Windows-based device from an IP address based within the United Kingdom between the hours of 0800 and 2200hrs GMT, a connection from a Linux-based device on a Canadian IP address at 0330hrs GMT could be suspicious.

Additionally, attempts to access multiple accounts from the same IP address should be met with the same suspicion, and therefore implementing access restrictions or blocks may be considered.

Threat Intelligence

Analysis of common tools and their configurations can provide potential indicators such as hard-coded parameters that are unusual for legitimate customers. For example, reuse of unique identifiers, parameters or cookie values may be unexpected, and therefore indicative of a hard-coded value that can be filtered. Also,legacy user-agent strings such as for end-of-life operating systems or web browsers could be redirected or restricted to prevent abuse (Figure 20).

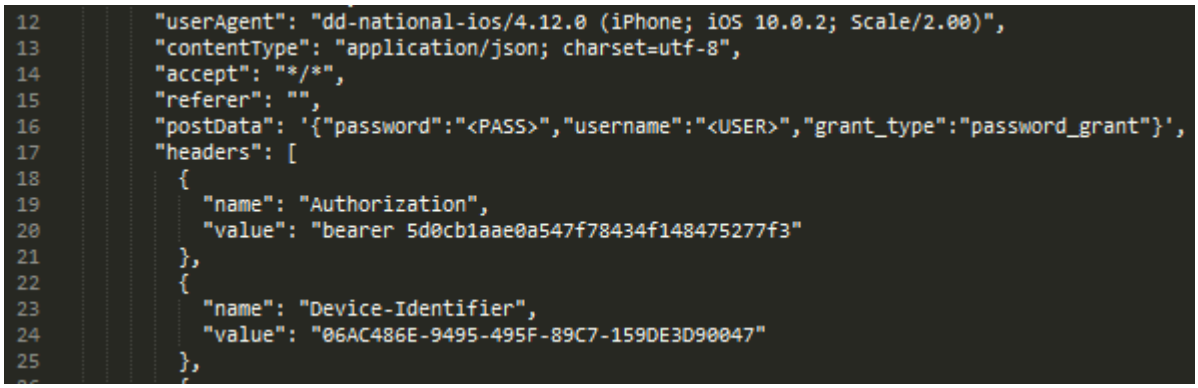

Figure 20 - Example SNIPR configuration showing potential hard-coded values (lines 12, 20 and 24)

Credential Dump Monitoring

The early detection of dumped credentials and subsequent auditing of customer accounts for password reuse allow for a proactive defence before leaked or stolen data may be abused in

credential stuffing attacks. In the event that a user's credentials are being reused, customer accounts should be restricted and practical advice can be shared to educate them of the risks of credential reuse, in addition to advising them of the potential breach and remediation steps (Figure 21).

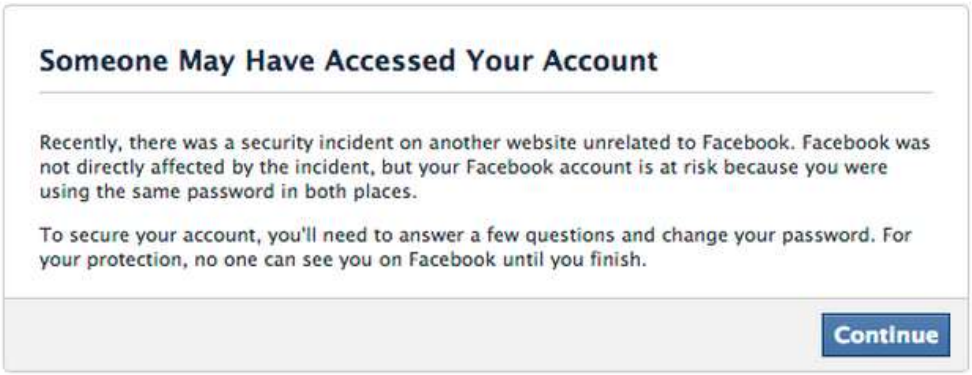

Figure 21 – Facebook 'password reuse' alert