Sentry MBA

A Tale of the Most Widely Used Credential Stuffing Attack Tool

Report by Danna Thee
CyberInt Threat Intelligence Researcher

Table of Contents

Introduction

Every so often security breaches and compromised accounts are reported in the news. Some data breaches are disclosed to the public long after the act; others are not even reported. Large data breaches generally are focused on very large organizations, which have become targets for threat actors. However, organizations of all sizes are affected by data breaches. **But how can organizations better prepare for and mitigate against such events?**

Compromised credentials are not a new phenomenon, but the frequency of such instances has increased. The number of compromised credentials available online is staggering, providing a goldmine for attackers. Of confirmed data breaches, 63% involve weak, default or stolen passwords.[1] At all times, users' credentials are being sold, traded and shared online across the Internet: hacking forums, online marketplaces, paste sites, and of course, on the Dark Web.

This report describes the Sentry MBA, a credential stuffing attack tool, which has become the most popular cracking tool among threat actors in recent months. Among the reasons for its popularity, the Sentry MBA hacking tool is freely and publicly available, extremely effective, and easy to operate.

In a credential stuffing attack, large numbers of stolen credentials are automatically tested against a web application's authentication mechanism until a match with an existing account is found. The attack technique relies on weak passwords and password reuse as it uses previously leaked credential combinations as part of its attacks.

It is important to note that not all industries are affected in the same way by this type of attack. The top three industries affected are technology, entertainment and financial services. This report seeks to help organizations understand where they are exposed, how threat actors are using this information, and what they can do to prepare for and mitigate such events.

This report describes the Sentry MBA, a credential stuffing attack tool, which has become the most popular cracking tool among threat actors in recent months

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

What is Cracking?

In the security industry, the term cracking refers to the malicious act of obtaining unauthorized access into someone's computer system without his permission and knowledge. Contrary to the widespread terminology, cracking does not usually involve extensive hacking knowledge and capabilities, but rather persistence and dogged repetition of handful tricks that exploit common weaknesses in the targeted system.

Hackers conceive crackers as less educated hackers, and refer to them as "script kiddies" or "newbies", because they do not create their own attack tools, but instead they steal or purchase cracking tools for malicious intent or personal gain. Although the number of crackers is numerous, they are generally easier to stop and identify. Sentry MBA is an example of a very popular tool among crackers because it is free and considered to be very effective.

Figure 1 below shows a discussion on an underground Dark Web forum about the essence of cracking. A threat actor identifies himself as "MysticRabbit1" was in search after cracking lessons or tips. In reply, one threat actor identifies as "v4grant" refers to cracking as an action focusing on obtaining users credentials. Another threat actor that calls himself "panic" refers to sentry MBA as a cracking tool by claiming that cracking takes advantage of the fact that people commonly reuse their passwords on multiple websites, and that the tool tests username/password combinations against other websites.

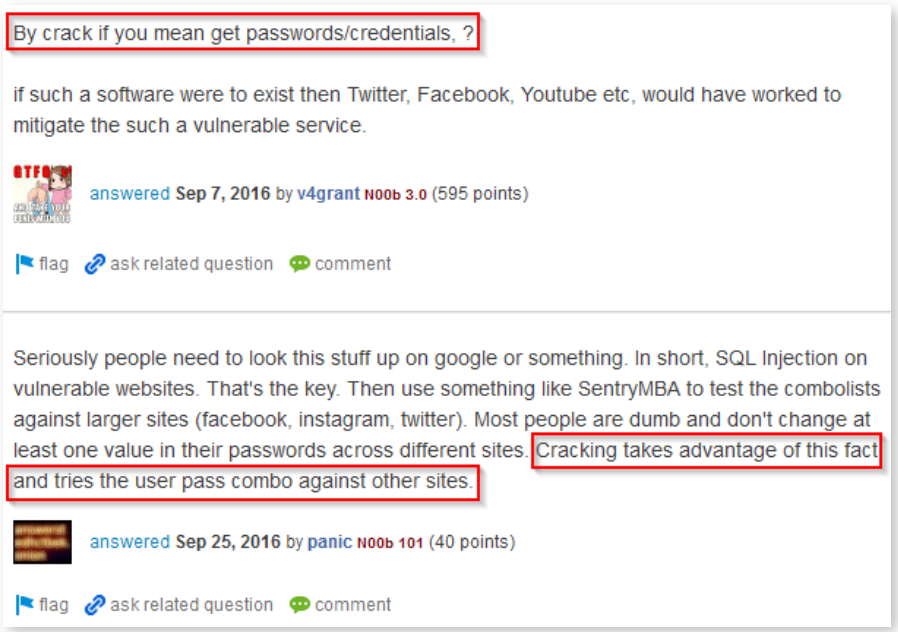

Figure 1: Dark web discussion about the essence of cracking.

Credential stuffing attack

Credential stuffing (OWASP OAT-008) is the automated injection of compromised username and password pairs in order to accomplish account take-overs. Large numbers of stolen credentials are automatically tested against a web application's authentication mechanism until a match with an existing account is found. Then the attacker can hijack the account for diverse purposes: drain the account of funds, steal personal identifiable information, spread spam and phishing, or install C2 malware or keyloggers.

Although the credential stuffing technique is referred to as a type of brute-force attack, the attacker does not guess at values; Attackers using the credential stuffing technique instead rely on weak passwords and password reuse and uses previously leaked credential combinations. These credentials pairs, known among threat actors as "Combos" or "Combo List", are regularly obtained from breaches on other websites that are sold on underground forums or marketplaces or may be available on public sites like Pastebin.

Sentry MBA exploits the improper control of interaction frequency and the improper enforcement of a single, unique action, meaning Sentry MBA is relying on the lack of restrictions against automated attacks such as credentials stuffing. This vulnerability is also known as Insufficient Anti-Automation Vulnerability, which occurs when a web application permits the attacker to automate a process that was originally designated only for manual users.

According to OWASP, credential stuffing is an emerging threat as it is one of the most common attacks on web and mobile applications today and is capable of breaching sites that do not have what are considered to be traditional security vulnerabilities. These attacks will put at risk both consumers, as the compromised account owners, and organizations, as the web application provider.

Credential stuffing technique relies on weak passwords and password reuse and uses previously leaked credential combinations that are automatically tested against a web application's authentication mechanism until a match with an existing account is found

Sentry MBA Cracking Tool

There are many credential stuffing tools, though in recent months Sentry MBA has emerged to become the most popular. Among the reasons for its popularity, Sentry MBA is a freely and publicly available modular software with a nice user interface. Additionally, the tool is extremely effective because it's common for people to use the same credentials on multiple applications.

Even though Sentry MBA is commonly used and has high success rates (usually 0.1%-0.2% of the total login attempts), our customers were generally not aware of its existence. Not only were they not familiar with the attack technique and the tool used to execute it, they were not able to differentiate attacks from regular login activities.

Below, Figure 2 shows a screenshot of the main interface of the Sentry MBA tool, which is a standalone Windows application.

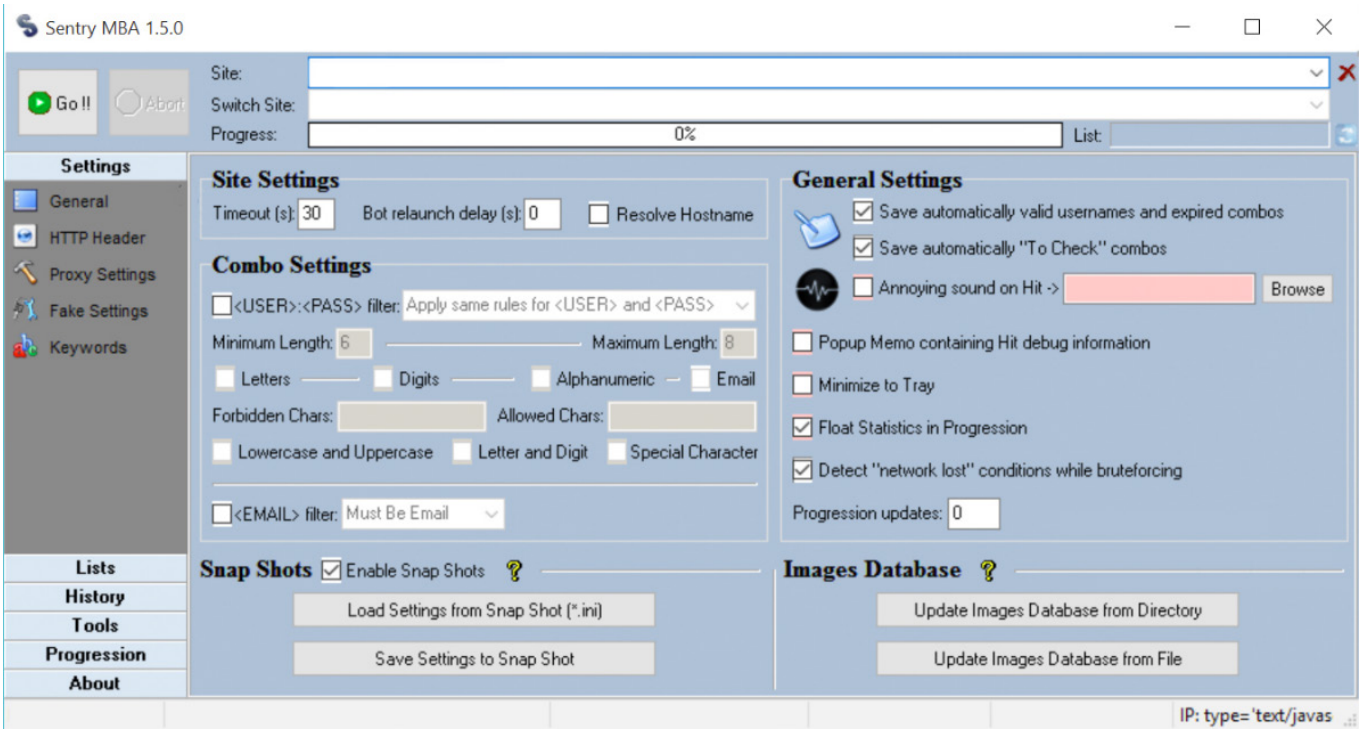

Figure 2: Sentry MBA main interface.

Three vital components are needed to execute a credential stuffing attack using the Sentry MBA tool:

- **The configuration file**, also known as "Config file", enables Sentry MBA to properly navigate in the targeted online login portal by defining the unique parameters of each web page.

- **Proxy file** is a list of compromised hosts (usually compromised endpoints or bots) that Sentry MBA uses during the attack. Proxies help the attacker evade website defenses by spreading login attempts across many sources.

- **Combos list** contains numerous username/password combinations from previous leaks that will be tested against the target's authentication mechanism.

Cracking communities offer a wide range of these sentry MBA components for various websites.

Sentry MBA has functions to mitigate traditional online login form security controls, such as IP rate limits and blacklists, as well as the capability to bypass third-party security controls that a targeted website might use. For example, if a site has a CAPTCHA mechanism implemented, Sentry MBA attempts to bypass it by using Optical Character Recognition (OCR) software, like Death by Captcha API, so that it can read and solve CAPTCHA challenges.

In most cases, threat actors are using Sentry MBA for a credential stuffing attack. But in some cases, attackers use the Sentry MBA in DDoS attacks when run at a high rate. [2]

https://lp.incapsula.com/rs/804-TEY-921/images/2015-16%20DDoS%20Threat%20Landscape%20Report.pdf

Anatomy of Credential Stuffing Attack Executed by Sentry MBA

Figure 3 is a visual representation of what happens during a Sentry MBA attack. An attacker takes the following steps to make an attack using Sentry MBA:

- The threat actor obtains dumps of leaked credential combinations from paste sites, file-sharing sites or underground marketplaces.
- The threat actor uses the Sentry MBA tool to test the credential combinations against the target's online login web page.
- Successful logins allow the attacker to take over the account matching the stolen credentials.
- The threat actor drains stolen accounts of stored value, credit card numbers, and other personal identifiable information.
- The threat actor can then either make a profit by selling the stolen account information or use it for other malicious intentions.

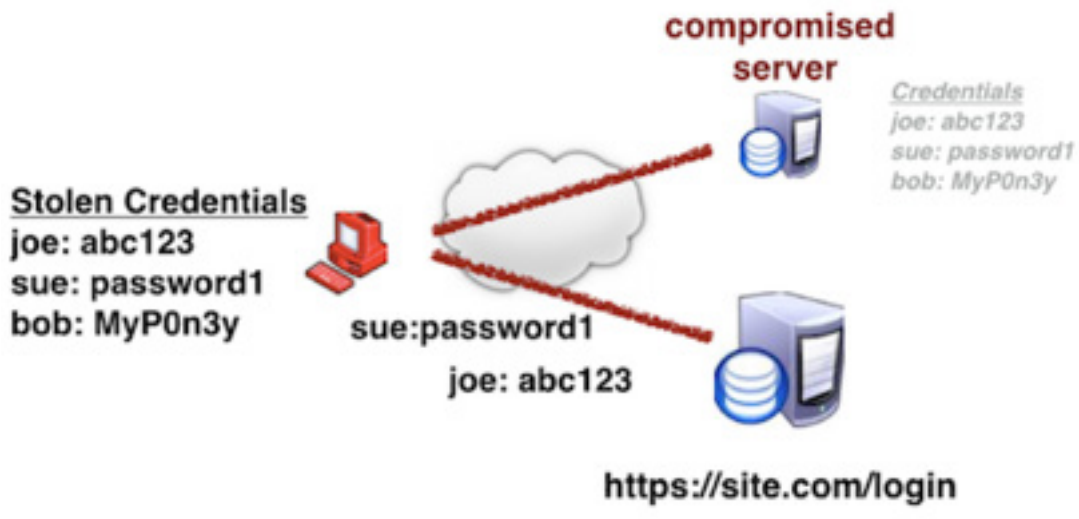

Figure 3: Credential Stuffing attack diagram by OWASP.[3]

https://www.owasp.org/index.php/Credential_stuffing

Sentry MBA Credential Stuffing Attack Detection

By default, Sentry MBA uses the following user agent strings:

- 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

If you find these user agent strings in your web logs, it's likely you have been compromised by a credential stuffing attack. The OWASP Automated Threat handbook notes that you should observe a high authentication failure rate when a credential stuffing attack is taking place. The term "high" is left to interpretation, but it's fair to say that any authentication failure rate that is multiple standard deviations beyond the mean for your website qualifies as "high".

If you decide to blacklist these User Agent strings, you should recognize that these strings can be changed by an attacker to bypass such a control. Before you take any action, we recommend you consider the associated game theory.

Suggested Mitigation Steps

Secure your system to mitigate credential stuffing attacks:

- Monitor the system for systematical attempts to query the database from the same HTTP client (based on IP, User Agent, device, fingerprint, patterns in HTTP headers, etc).
- Implement an anti-automation mechanism, such as CAPTCHA or two-factor authentication, on vulnerable requests: login, registration, password reset, etc.
- Limit the number of accounts that can be registered from one IP address in a certain period of time.
- Limit the number of login attempts per HTTP client.
- Document and monitor all user login actions.
- Define the measures that would be taken in the event that a credential stuffing attack occurs.
- Use threat intelligence services to detect potential or real-time credential stuffing attacks.
- Restricting automated process by one of the following:
  - Fingerprinting
  - Reputable methods such as geo-location and/or IP address block lists

Hacking in the Age of Social Media

We are accustomed to threat actors using social networking sites as a tool to target organizations or people for the means of getting vital information and data about the targets. But threat actors also take advantage of direct communication between individuals and easy access to the wisdom of the crowd. They use social networks to gain knowledge on attack techniques and tools and also to share data leakages, brag on their successes and share their experiences.

While we used to think that hacker activity goes under the radar in underground forums, marketplaces or the Dark Web, in the age of social media hacking and cracking communities are thriving out in the open, sometimes by using a fake identity, but often with their real names.

Thus, information on how to use Sentry MBA is not hidden in an underground Dark Web community. In fact, a simple search on YouTube will show dozens of how-to videos, and a quick search on Twitter or Facebook will reveal threat actors sharing their Sentry MBA "config" files or a dump of stolen credentials. Figures 4-10 show real examples, taken from online sources, of how threat actors interact online and share information regarding Sentry MBA and compromised credentials.

1. Open Sentry Mba
2. Put The Configs in Setting Tab.....Follow me.....
3. Now Put The Combos And Proxy In The List Tab.....Follow me.....
4. Open The Progression Tab
5. Start and Wait xDDDDDD
6. Now Copy the Hits and Paste in Text Document.....
7. xDDDD Done.....U can check those Hitsss and Enjoy.....

Figure 4: Screenshot from an online Sentry MBA tutorial on YouTube.

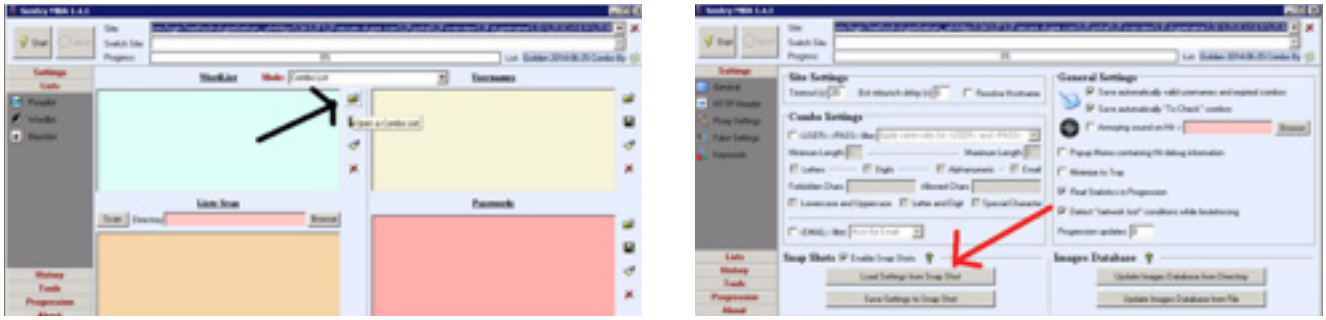

Figure 5: Screenshot from a threat actor guide on how to use Sentry MBA interface.

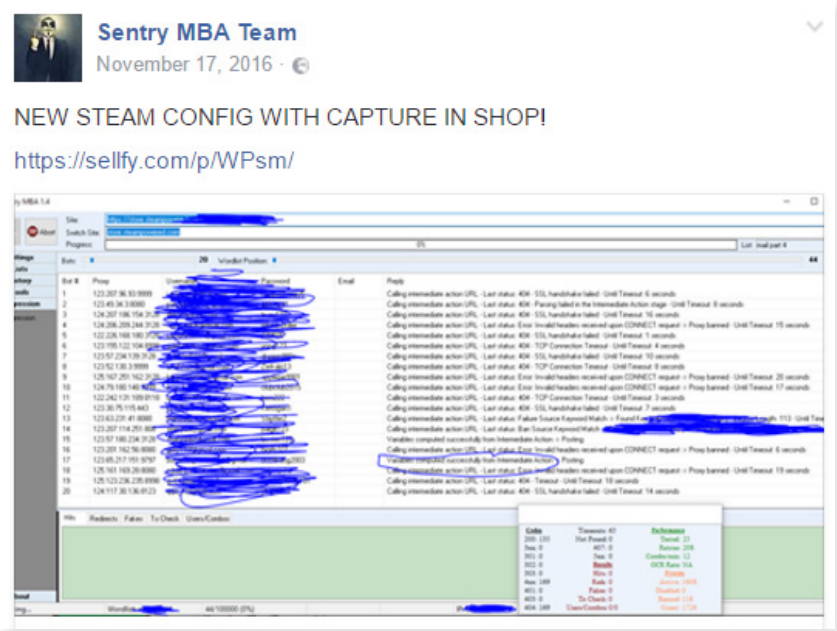

Figure 6: "Sentry MBA Team" crackers group offering Steam config file for sale on Facebook.

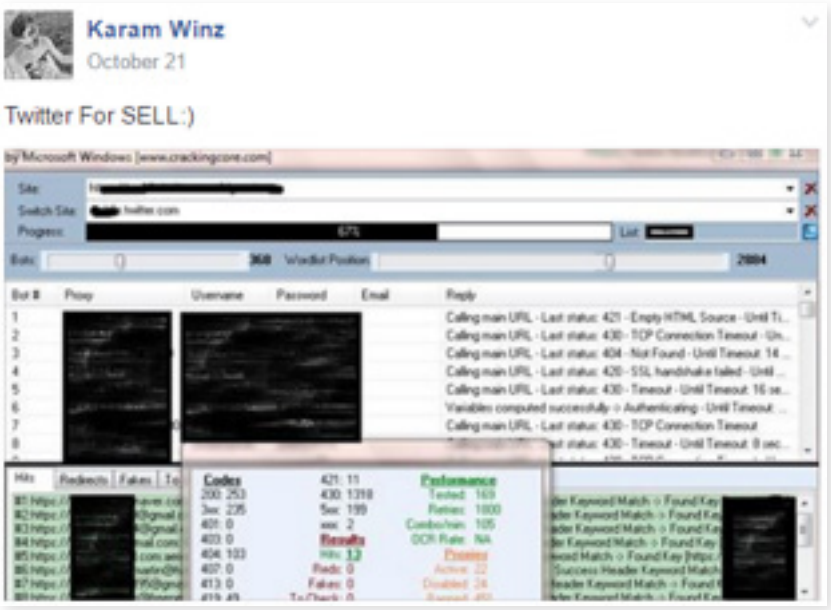

Figure 7: Twitter config file for Sentry MBA is offered for sale on Facebook.

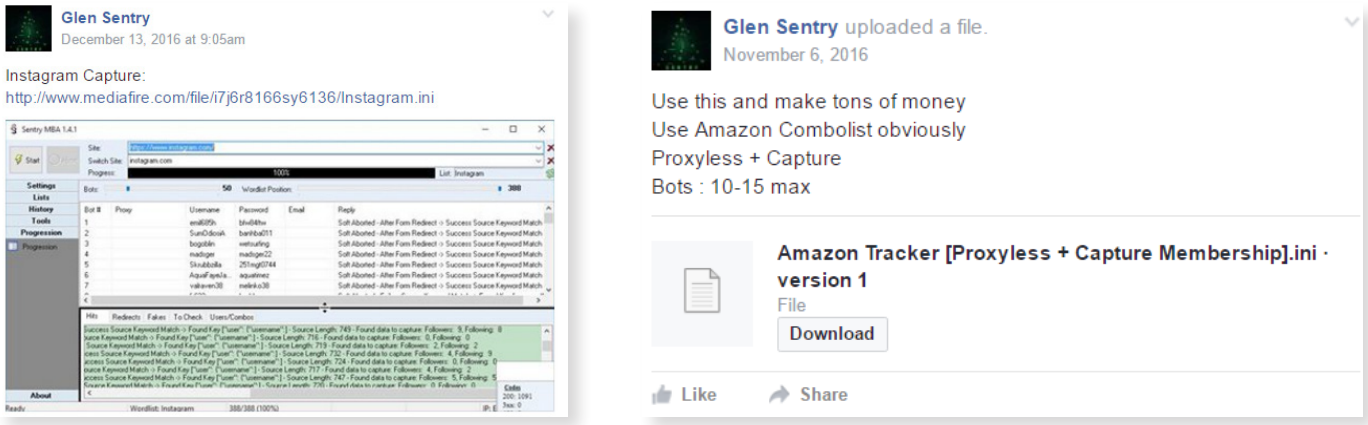

Figure 8: Threat actor identified as “Glen Sentry” shared Instagram and Amazon config files for Sentry MBA on Facebook.

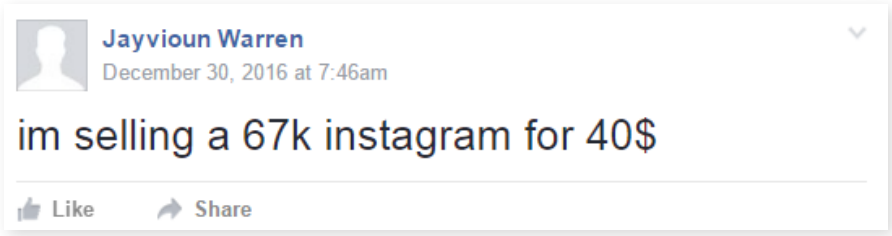

Figure 9: A threat actor identifies as "Jayvioun Warren" offers a combolist of 67,000 Instagram users for sale for $40 on a Facebook group.

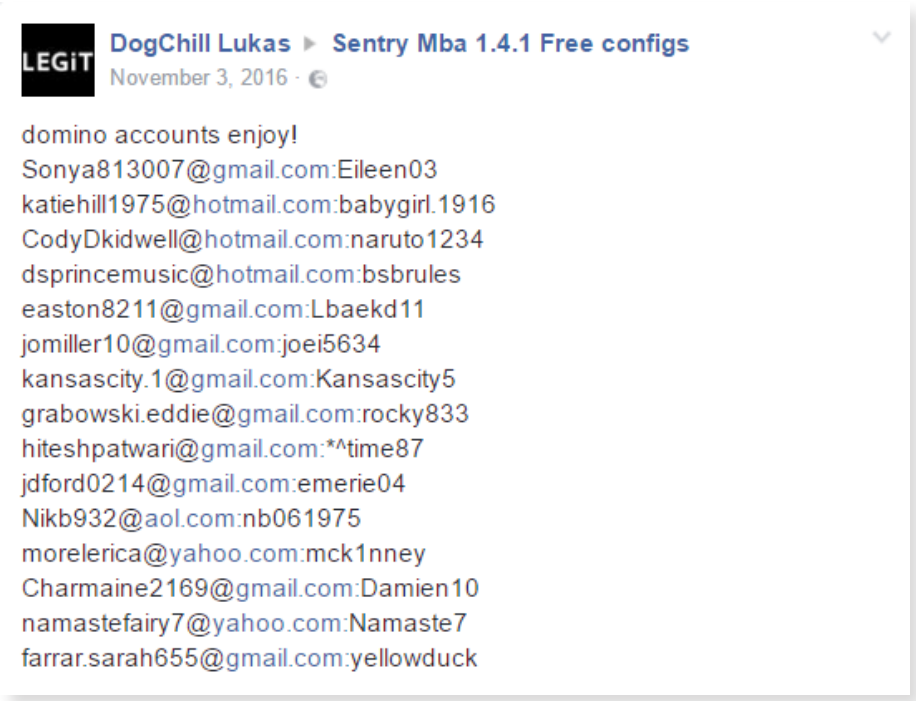

Figure 10: Threat actor posted a dump of 15 username/password pairs.

Cyberint
Protection Beyond the Perimeter

United Kingdom
Tel: +442035141515
sales@cyberint.com
25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA
Tel: +972-3-7286-777
sales@cyberint.com
3 Columbus Circle | NY 10019 | New York | USA

Israel
Tel:+972-3-7286777 Fax:+972-3-7286777
sales@cyberint.com
Ha-Mefalsim 17 St | 4951447 | Kiriat Arie Petah Tikva | Israel

SINGAPORE
Tel: +65-3163-5760
sales@cyberint.com
10 Anson Road | #33-04A International Plaza 079903 | Singapore