SCTE•ISBE CABLE-TEC EXPO® VIRTUAL EXPERIENCE » OCTOBER 12-15 2020

2020 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS®

Credential Fraud Detection And Remediation In Media Consumption Services

A Technical Paper prepared for SCTE•ISBE by

Steven Epstein
Distinguished Engineer
Synamedia

054-566-4116
sepstein@synamedia.com

Table of Contents

List of Figures

List of Tables

1. Introduction

Accessing another's credentials has always been a major goal of hackers or pirates. Typically, pirates would perform phishing or even spear phishing attacks on naïve or unsuspecting targeted individuals. In these attacks, the hacker would send a user a link to some embellished website mimicking a known banking, credit card or other financial site. It would request the unsuspecting user to enter their personal credentials. Once the credentials were entered and transferred to the pirate, the pirate could now perform bank transfers, embezzle money or even take over the victim's account. These attacks were very costly to financial institutions and other highly secure websites, but not highly effective or scaleable. That's because in order to be successful, phishing sites required much intelligence to send the proper link to the appropriate users and even so most users did not take the bait.

In the last five years however, a new more scaleable and effective method of accessing another's credentials has become increasingly popular. This form of piracy, known as credential stuffing, is based on two historical realities:

1. In the past 10 years, thousands of identity databases belonging to large websites, have been breached leading to the identity theft of tens of billions of credentials.
2. Most people reuse the same credentials (username and password) on multiple sites as a convenient way of remembering them.

Given these two facts, new credential stuffing tools were created to enable a set of bots over proxies or VPNs to discover active breached credentials from a set of popular websites. The diagram below illustrates how credential stuffing attacks are performed.

A pirate purchases millions of username/password combinations (combos) extracted from breached websites, and configures a set of bots, proxies, desired websites and scripts describing login navigation details of each of these desired sites. The pirate then inputs all these artifacts into credential stuffing tools. The tool then assigns bots to try all of these combos on each of the popular websites, using navigation instructions within scripts, and connect to them via separate proxies or VPNs. In order to go undetected, different IP addresses are used for each malicious attempt! The tool returns a subset of the list of credentials that are still active on each popular site. This attack is effective because most users tend to employ the same username/password combination across most of their websites.

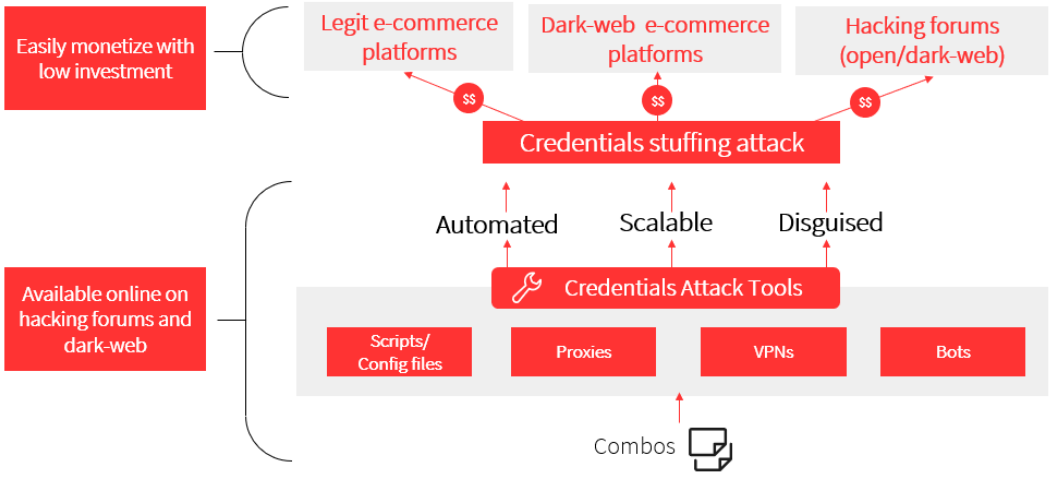


Figure 1 - Credential Stuffing Attack

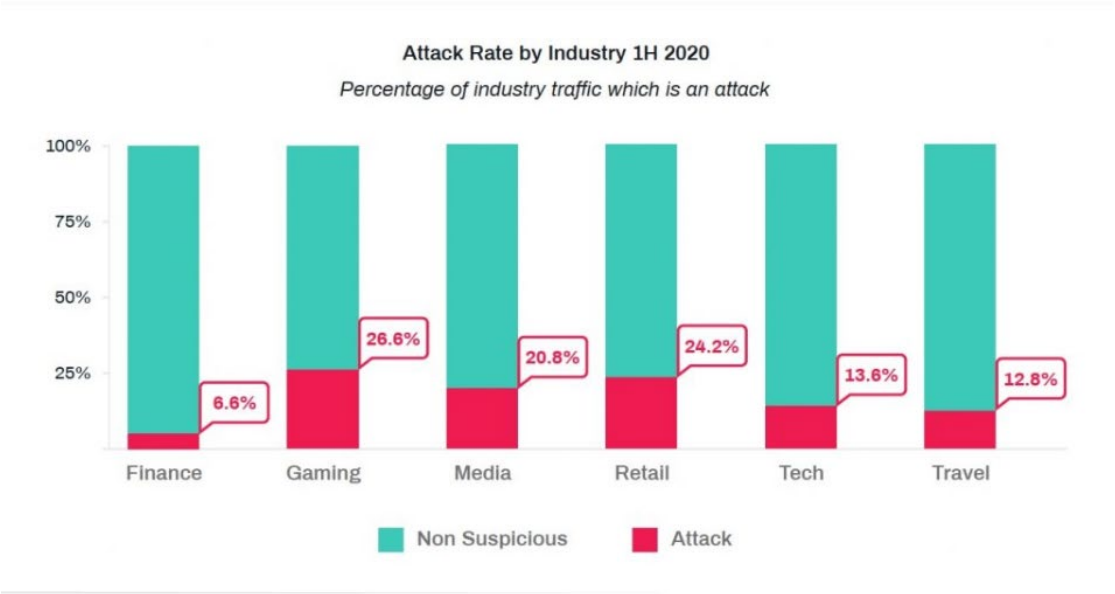
Once any login attempt succeeds, the stolen credentials become marketable and can enable access to another's account. The accounts which are typically accessed via credential stuffing are not only banking sites but also streaming media sites, where the purpose of the attack is not to pilfer money, but to sell access to someone else's account and enable a buyer to enjoy content made available by another's monthly subscription. As a result of these credential stuffing attacks, access to media sites such as streaming video, music, audio book, books etc. are sold over telegram groups, forums, websites on the open Internet and especially the dark web.

Unlike phishing or spear phishing attacks, where the victim realizes the credential theft and resulting fraud fairly early and immediately alerts authorities, credential stuffing attacks on media sites tend to go undetected for a very long time. That's because the pirate or purchaser of the credentials desires to receive a free media service and hence does whatever it takes to remain unnoticed by the real owner.

2. The prevalence of fraudulent password usage in media services

Credential stuffing is growing dramatically, especially in media services. According to Forbes, 4.1 billion credentials were breached in the beginning of 2019 alone. The HaveIBeenPwned website has a database of over 10 billion breached credentials. According to Shape Security, between 0.5 and 2% of these credentials will be valid on any targeted website or mobile app.

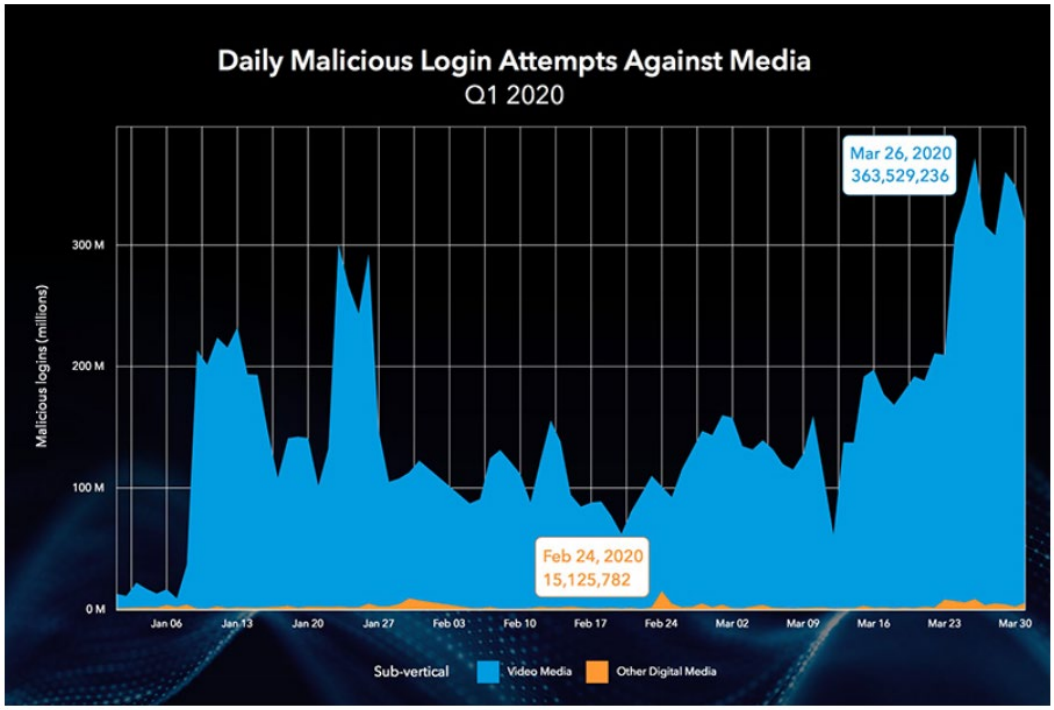
Between the beginning of May and the end of June this year, Akamai collected data on 8.35 billion credential stuffing attempts across the globe across all industries. They estimate that in Q1, credential stuffing attacks increased by 1,450%, compared with about 200% in 2019 (compared with 2018). One European broadcaster was even hit with peaks of malicious credential stuffing attempts that ranged into the billions. However, as mentioned above, unlike phishing attacks which typically target financial institutions, a good percentage of credential stuffing attacks are focused on media. The graph below by Arkose Labs shows that over 20% of all online traffic to media sites are credential stuffing attacks.



Data source: Arkose Labs

Figure 2 - Credential Stuffing Attack Rate by Industry

These attacks against media sites continue to grow significantly. The graph below by Akamai exhibits the steep rise in malicious credential stuffing login attempts against media, exacerbated by the period of COVID-19, where a 300% increase was observed.



Daily malicious login attempts during Q1 2020. Source: Akamai

Figure 3 - Daily Malicious Login Attempts Against media

But even before COVID-19, between 2018 and 2019 there was a 63% increase in credential stuffing attacks against video media sites as shown by the Akamai graph below.

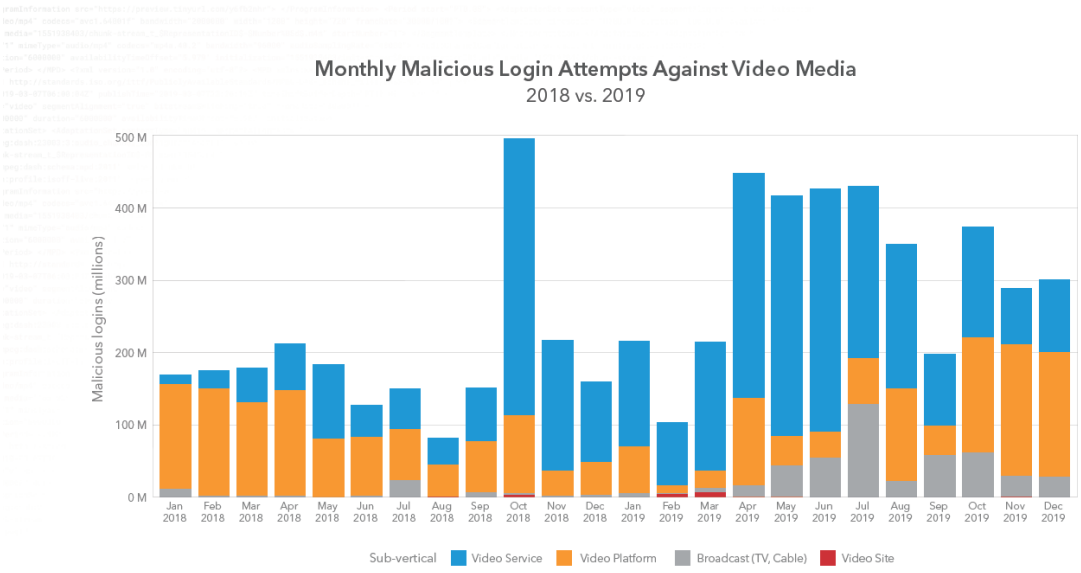


Figure 4 - Monthly Malicious Login Attemts Against Video Media

Akamai researchers watching the credential stuffing space in Q1 2020, noted that video media accounts were trading for about $1 to $5 on the criminal market early on. Some packaged offers (those that include multiple services per order) were even being sold for $10 to $45. Toward the end of Q1 2020, those prices fell as the credential stuffing market became flush with new accounts and lists of recycled credentials.

Based on the statistics above, it is clear that the criminal economy is a chained instance, where everything is somehow connected, and no piece of information is without worth. Criminals pre-package compromised accounts, selling them based on interest, location, and volume, and people are willing to pay. This only fuels the criminals' actions and keeps them hyper-focused on evading detection and mitigation.

3. Why credential fraud detection is so difficult: Sharing vs Fraud

As mentioned above, credential stuffing discovers marketable credentials that are active on various media sites. These credentials are then typically sold on either the dark web, telegram groups, forums or open Internet websites. Below is an example of a site selling various subscriptions to streaming services for one time payments under $15.

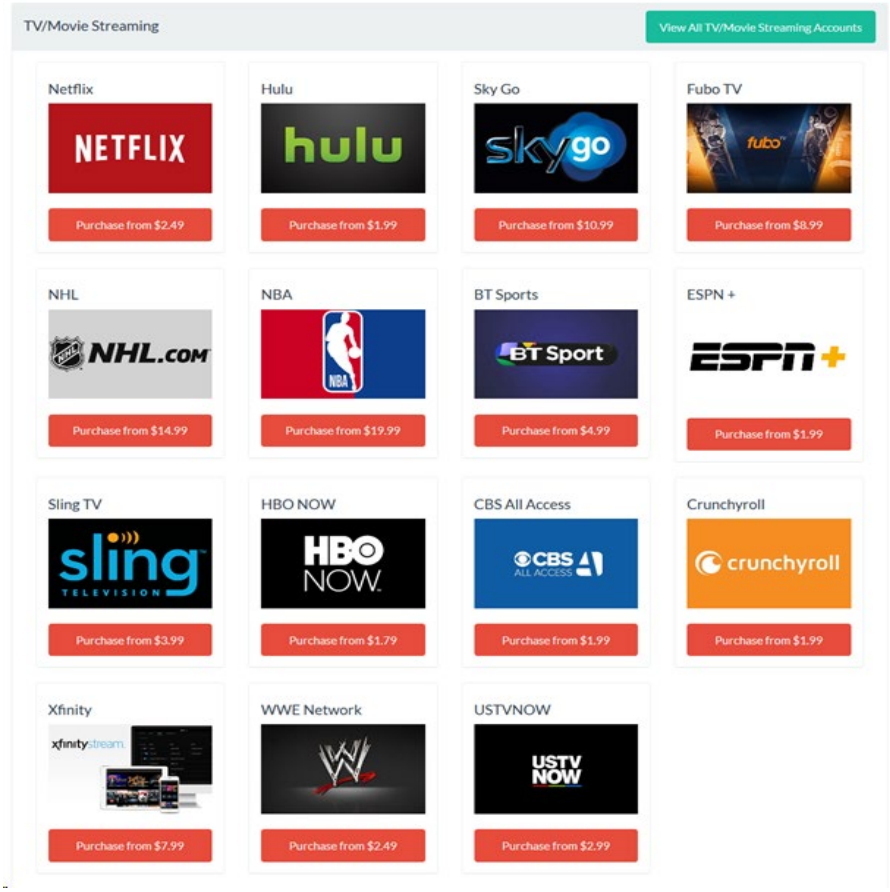


Figure 5 - Online Sales of Fraudulent Subscription Services

The motive of those purchasing these credentials is not malicious. They aren't looking to takeover and control the account. Nor are they looking to purchase goods on the account owner's credit card. They simply want to enjoy a popular streaming subscription service for a low one-time cost.

In other words, those who purchase another person's credentials to a popular video media site is unable to find another account owner who is willing to casually share their credentials with them. Hence they need to rely on purchasing the credentials from a stranger in order to receive a free subscription to this media service.

The goal of the user who purchases credentials from a credential stuffing fraudster is to enjoy this service that he purchased for a low one-time fee for as long as possible without being noticed and without the account owner changing his password out of suspicion. Hence, the behavior of the fraudster will by definition mimic that of the sharer, one who benefits from casual sharing, or even the account owner.

Based on this new reality, it becomes challenging by scrutinizing the data alone to differentiate between the account owner and the fraudster and even more difficult to differentiate between the fraudster and the casual sharer. If you scrutinize which devices within any given account constantly view video from out-of-home locations and IP addresses, you cannot distinguish between the fraudster, the person who purchased the fraudulent credentials or the casual sharer.

While most service providers are willing to tolerate some level of casual sharing, the same is not the case when it comes to credential fraud. Given concerns over privacy and other liabilities, detecting the fraudster and differentiating them from the sharer is critical to the well-being of a video service.

Which begs the question: How does one differentiate between casual credential sharing and credential fraud?

4. Credential Fraud indicators and Solution Enablement

Synamedia has created a novel solution to detect credential fraud in media services resulting from credential stuffing attacks based on machine learning. In this solution, credentials sold online to any particular media service are purchased by our own intelligence group. The credentials are then used to train a supervised machine learning model to detect a fraudulent account using various indicators. Indicators of fraud in the model are based on some of the following principles:

1. Landscape of how credentials are sold on the various marketplaces and various trends on the frequency of usage of a stolen credential once put up for sale
2. Assumption that there is less correlation between the viewing preferences, behaviors and habits of the fraudster and the account owner versus those of the sharer and the account owner
3. Other anomalous, suspicious and unexpected activity in the account

Once this supervised model is built, it can be applied to locate other, as yet undiscovered fraudulent accounts. Once all fraudulent accounts are classified, a second model is built which can differentiate between the devices of the sharer and account owner and that of the fraudster within each classified fraudulent account. This algorithm is semi-supervised but is based on many of the same indicators described.

Finally, fraudulent devices are graded according to the likelihood that they will perform real malicious activity, such as an online purchase of goods and/or new services in the name the account owner or even an account takeover. The activity diagram describing this algorithm is shown below.

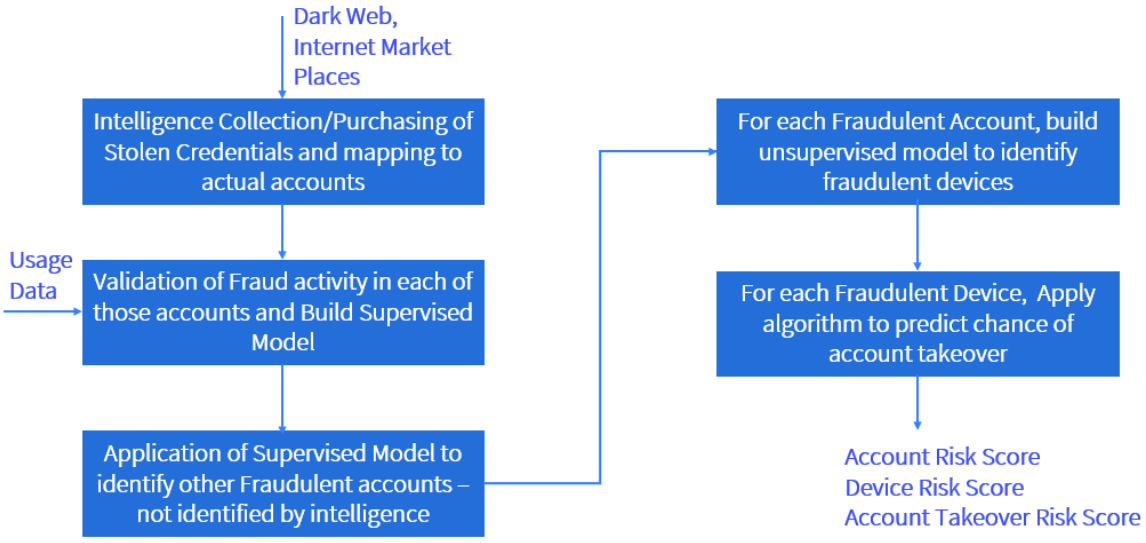


Figure 6 - Synamedia Anti-Fraud Algorithm

5. Trusted Identity as a Service

By creating such an algorithm, Synamedia provides a service to validate the trusted identity of media accounts and devices within each account. Upon receiving near real-time data streams from a media provider, Synamedia supports an API where it can return:

1. Likelihood that a specific account is fraudulent
2. Likelihood of fraud in each device within that fraudulent account
3. Risk of account takeover or other malicious activity of each fraudulent device in that fraudulent account

An example of this service is shown in the diagram below

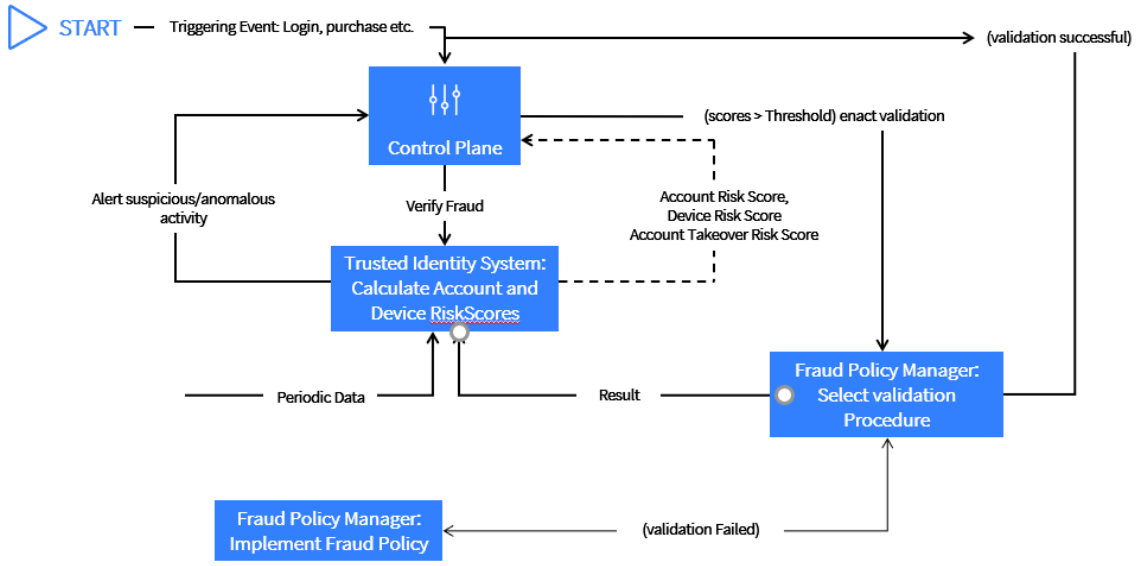


Figure 7 - Anti-Fraud Detection and Resulting Policy

This trusted identity service enables a media provider to both perform adaptive authentication and enforce adaptive remediation policies, where the authentication and the resulting policy are compliant to the risk of fraud of every device in every account. As a result, the service provider can create an adaptive policy table as a function of the sensitivity of the trigger (login, TVOD purchase, change of address etc.) which caused the trusted identity API to be called.

Many verification and remediation policies, such as password change and answering security questions, are effective against fraudsters as opposed to sharers because we assume no social connection nor passing of information between the account owner and the fraudster!

An example of an adaptive policy table is shown below.

Table 1 - Fraud Policy Table

Trigger Sensitivity Score	Account Risk Score	Device Risk Score	Account Takeover Risk Score	Fraud Verification Policy	Fraud Remediation Policy if verification Fails	Fraud Remediation Policy if verification Succeeds
<30	All	ALL	All	None	N/A	N/A
>30 <60	<50	<30	N/A	None	N/A	N/A
>30 <60	>50	<30	N/A	Provide Password	Suspend Account	Change Password
>30 <60	>50	>30	<20	Answer 1 or more Security Questions	Blacklist Device	Change Password
>30 <60	>50	>30	>20	Biometric / MFA	Suspend Account	Change Password
>60	<50	<30	N/A	Provide Password	Suspend Account	Change Password
>60	>50	<30	N/A	Answer 1 or more Security Questions	Blacklist Device	Change Password
>60	>50	>30	<20	Answer 1 or more Security Questions	Suspend Account	Change Password
>60	>50	>30	>20	None	Suspend Account and Blacklist Device	Change Password

6. Conclusion

Credential stuffing is a new piracy attack that has become prevalent in the past several years. This is due to the vast increase in the quantity of breached credentials in the marketplace and also based on the fact that few users change their credentials between accounts.

Credential stuffing, as opposed to other credential discovery techniques such as phishing, is prevalent not only on financial sites but also on media sites where the primary objective of the fraudster is to benefit from a low one-time payment to a subscription service. Hence, fraudulent use based on credential stuffing is extremely difficult to detect and disrupt!

Using advanced machine learning techniques, Synamedia has managed to build new fraud detection algorithms that can detect fraudulent usage of devices within accounts based on credential stuffing attacks. The results of this algorithm enable very effective adaptive authentication and remediation techniques to combat those passwords that were stolen and purchased based on credential stuffing!

Abbreviations

API	Application programmable Interface
CSA	Credential Stuffing Attack
TVOD	Transactional Video On Demand
VPN	Virtual Private Network
SCTE	Society of Cable Telecommunications Engineers

Bibliography & References

https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

https://piracymonitor.org/fraudulent-logins-q2-2020-arkose-labs/?utm_source=Piracy+Monitor&utm_campaign=3e0dea891d-PM-E-Newsletter-2019-1223_COPY_01&utm_medium=email&utm_term=0_baec17a8d9-3e0dea891d-364275657

https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-credential-stuffing-in-the-media-industry-report-2020.pdf

https://haveibeenpwned.com/

