[state of the internet] / security

Volume 5, Special Media Edition

Credential Stuffing: Attacks and Economies

Intelligent Security Starts at the Edge

Introduction

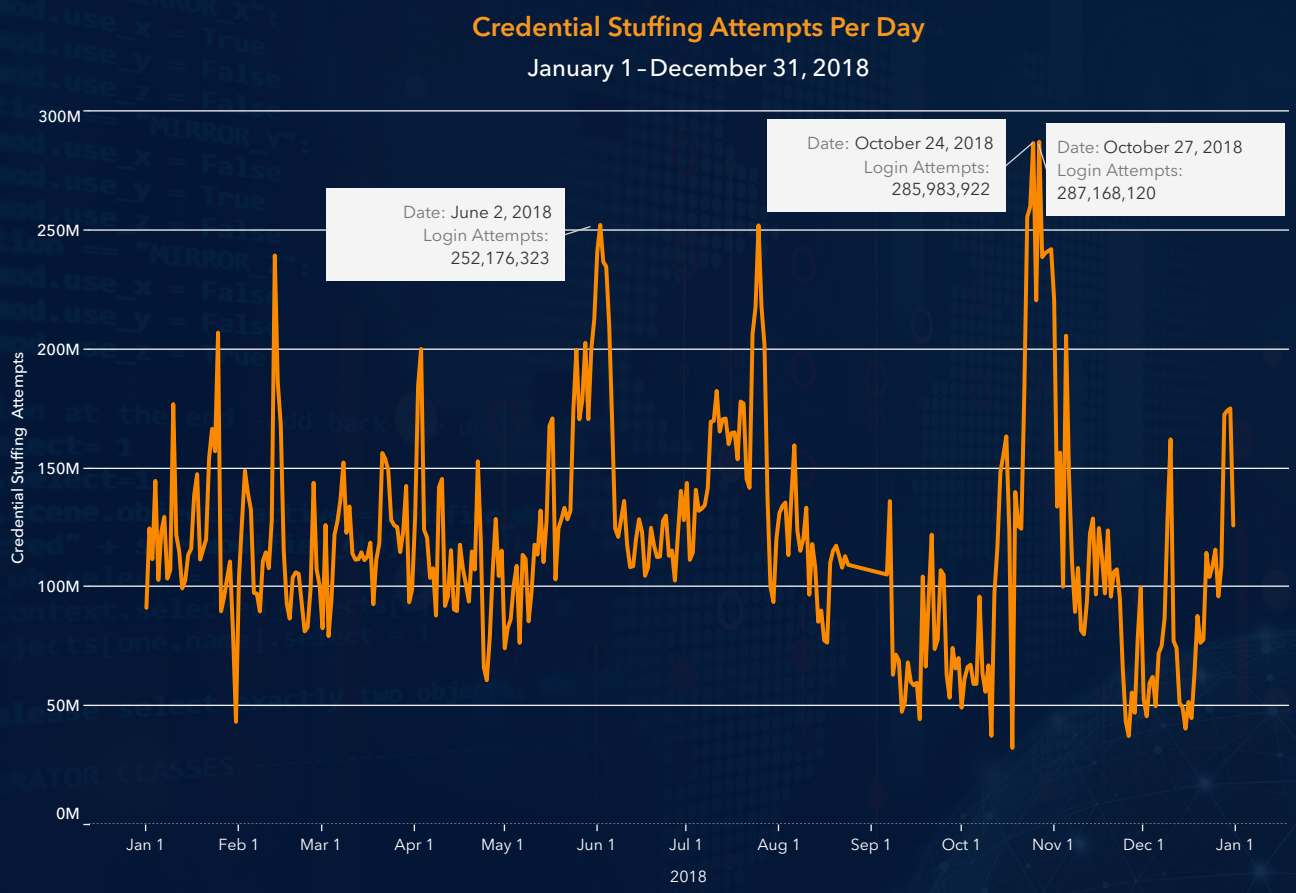
Akamai recorded nearly 30 billion credential stuffing attacks in 2018. Each attack represented an attempt by a person or computer to log in to an account with a stolen or generated username and password. The vast majority of these attacks were performed by botnets or all-in-one applications.

Botnets are groups of computers tasked with various commands. They can be instructed to find accounts that are vulnerable to being accessed by someone other than the account owner; these are called account takeover (ATO) attacks. AIO applications allow an individual to automate the login or ATO process, and they are key tools for account takeovers and data harvesting.

What does this have to do with media organizations, gaming companies, and the entertainment industry? A lot. These organizations are among the biggest targets of credential stuffing attacks. The people behind these attacks realize the value of an account, whether it's to a streaming site, a game, or someone's social media account. And they're willing to do whatever it takes to steal them.

In this report, we're going to give you an overview of the credential stuffing attacks in 2018 against the aforementioned sectors and look at the risks these attacks pose. We'll also explore some of the ways adversaries conduct these attacks.

Media organizations, gaming companies, and the entertainment industry are among the biggest targets of credential stuffing attacks.



Attacks Per Day

In 2018, Akamai observed hundreds of millions of credential stuffing attacks each day. These attacks targeted a range of sectors, from media and entertainment to retail and gaming. As seen in Figure 1, there were three days that peaked at more than 250 million attempts. Credential stuffing attacks are becoming a favorite for criminals at all skill levels. While previous "State of the Internet" (SOTI) reports have examined their impact on retail, this edition examines the media and entertainment sectors.

Criminals target large video and entertainment brands, because access to verified accounts can be sold or traded in underground marketplaces. If you've ever streamed a song, movie, or TV show online, you may already be familiar with some of the accounts most criminals favor. The information associated with these accounts also has value.

Figure 1

Three of the largest attacks observed in 2018 are highlighted, including two that occurred within days of each other

Largest Attacks

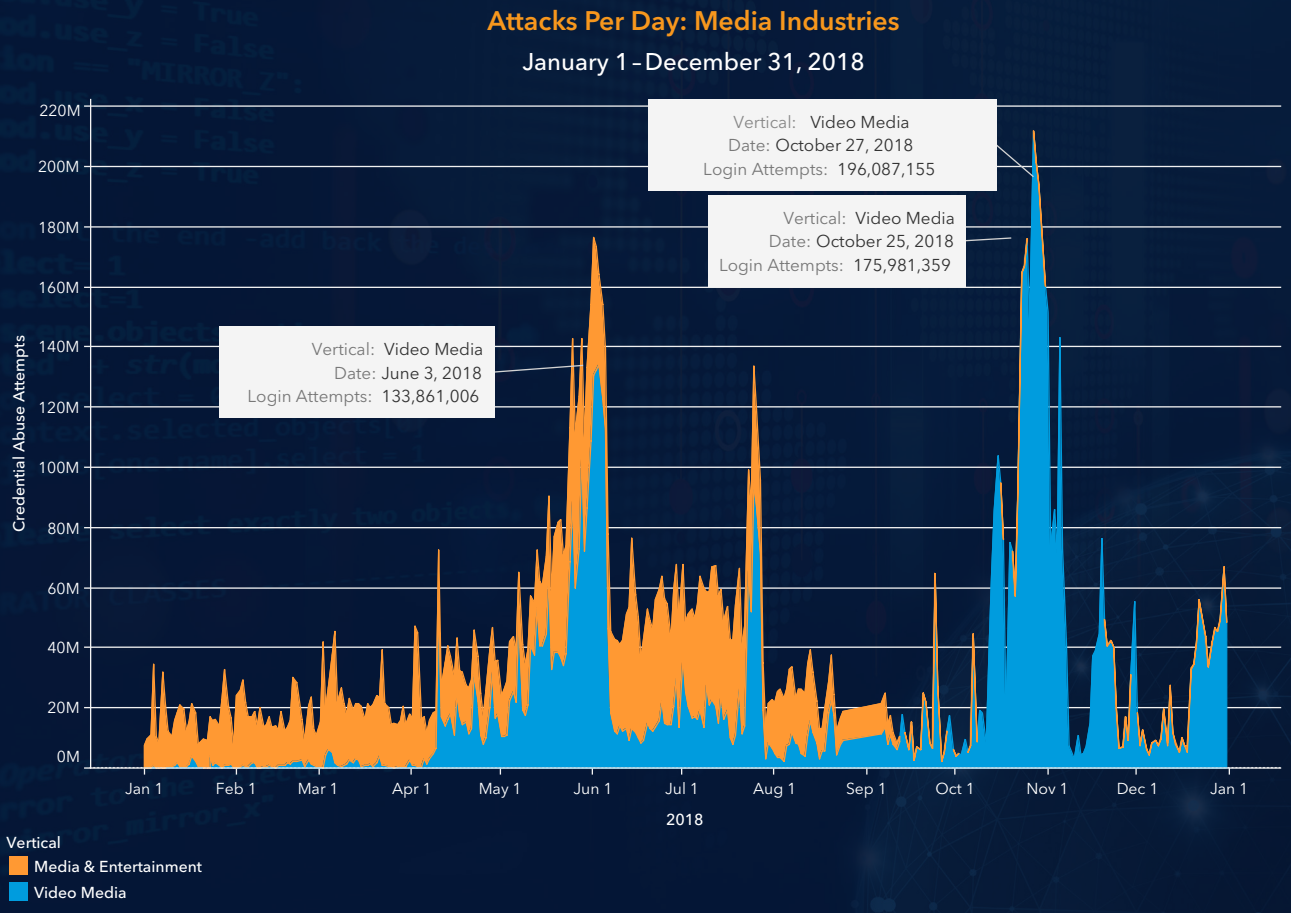
In the video media sector alone, three of the largest credential stuffing attacks in 2018 jumped up from 133 million to nearly 200 million attempts. This is significant, because the dates of the attacks sync with known data breaches: The sellers may have been testing the credentials before they were to be sold. In early February 2019, some 620 million usernames, passwords, and other records – taken from 16 organizations with disclosed data breaches – were offered for sale on the darknet.

Credential Stuffing

At the start of 2019, you may have heard the news that an anonymous individual released a collection of email addresses and passwords, here referred to as "releases 1–5," for credential stuffing.

Figure 2

Three of the largest credential stuffing attacks against the video media sector during 2018 ramped up from 133 million to nearly 200 million attempts



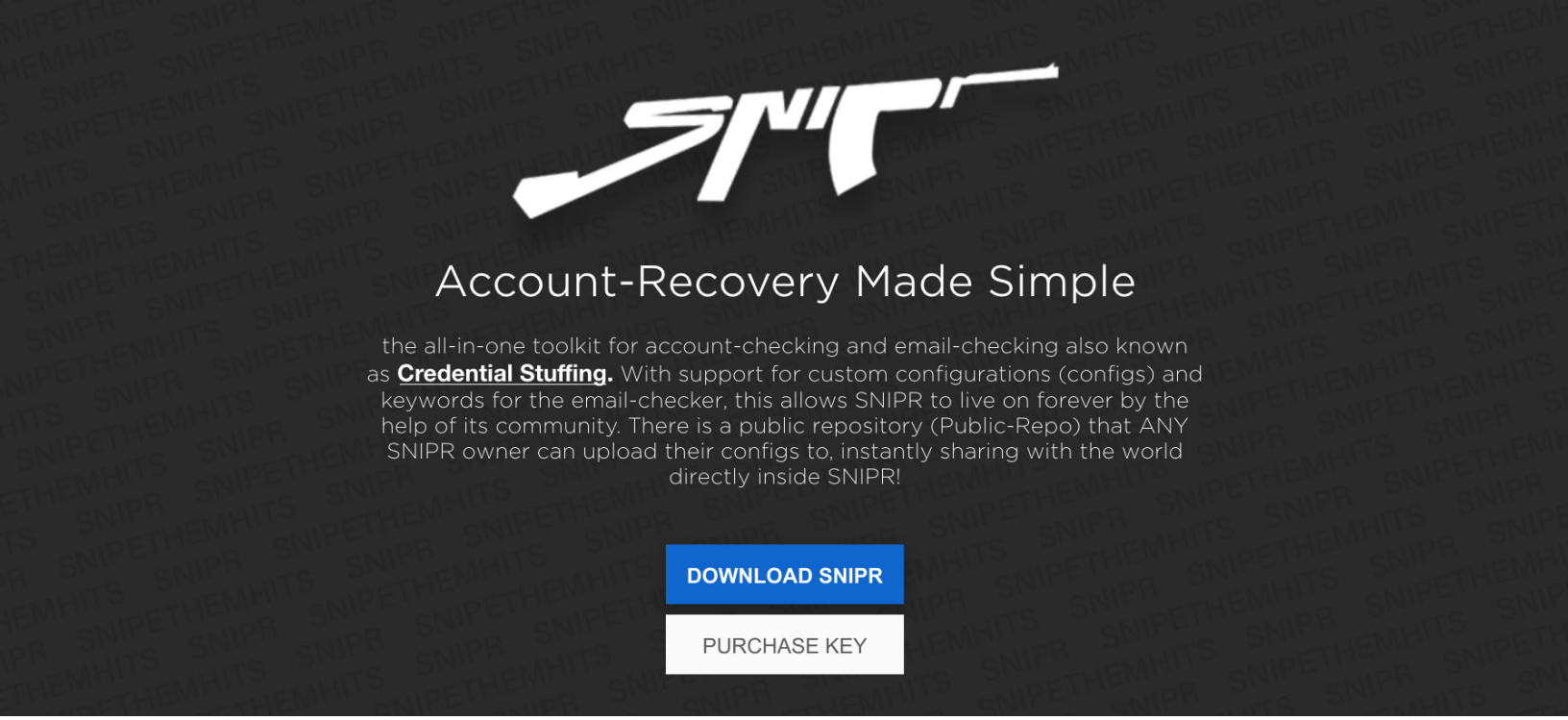


Figure 3

SNIPR is a low-cost AIO used for credential stuffing; it retails for $20 USD

Across these five collections, this anonymous person published nearly 1 TB of data, amounting to more than 25 billion email address and password combinations. Once the duplicates and unusable entries were removed, there were still billions of combinations available in various places online at the time this report was written.

Releases 1–5 are just basic collections of usernames and passwords, although they represent the largest collection ever released in a single instance. Such a massive collection is the exception and not the norm. But collections like this are created by merging combination lists from other data breaches, including highly notable ones.

Credential stuffing attacks are a major risk to online businesses, so having a pool of more than 1 billion potential combinations to pull from lowers the bar of entry significantly for any would-be criminal looking to cash in on the credential stuffing trend. However, lists like these are not the only way criminals collect the data they need to perform credential stuffing attacks.

In a YouTube video watched by Akamai researchers, an individual walked viewers step-by-step through a tutorial on how to create combination lists to use against the popular online battle royale game.

The tutorial started by teaching the concept of "Google Dorking," which uses Google's search engine operators to locate websites that are potentially vulnerable to SQL injection. Once the websites were located, the tutorial then moved on to teach viewers how to exploit these vulnerable domains using a common SQL injection tool. This tool then downloads email addresses and passwords, cracks passwords if needed, generates a valid combination list, and then follows up with a "checker" program with proxies to test its newly minted lists for validity.

These checker programs, or All-in-One applications (AIOs), allow the attacker to validate stolen or generated credentials. Depending on the application, AIOs can target login forms directly, or APIs — or both, if the situation calls for it.

Once the accounts are confirmed as valid, they can be sold, traded, or harvested for various types of personal information. Depending on the situation, it isn't uncommon for all three things to happen.

There are scores of AIOs online. Some are sold openly, and others are sold or traded underground. One of them, an application called SNIPR, is favored as an entry-level tool by those looking to target games, social media, and streaming media.

Another AIO called STORM uses detailed configuration settings that are sold or traded in their own right. At the time of writing this report, one seller on the darknet was promoting STORM configurations for use against one of the largest streaming platforms online at a cost of $52 USD.

The same seller is also selling gift card codes for the previously mentioned platform at a discount — offering cards with a value of $30 for as little as $7.80 USD. These codes are sometimes generated, but more often than not they're purchased with stolen credit cards, so any money collected is pure profit for the criminal.

This same retailer also does a steady business in selling credential stuffing combination lists. One listing is a batch of 5 billion random email addresses and passwords for $5.20 USD. Another is a customized list of 50,000 email addresses and passwords for the same price. The customized option allows the purchaser to choose format (email:pass or user:pass), provider, location, and more.

SNIPR Training Videos on YouTube

While researching facts and data for this report, Akamai researchers came across a number of related YouTube videos dealing with credential stuffing and associated attacks. We were able to confirm that at least 89,000 people have watched demonstration and tutorial videos on the AIO known as SNIPR.

There are dozens of videos, spanning across several SNIPR versions, detailing how to use the application, as well as how to get the most return on resource investment. Since SNIPR is an entry-level tool, such tutorials are often requested by the tool's users, which are then created by the developers or other users.

A Booming Economy

The market for stolen media and entertainment accounts is thriving.

The media, gaming, and entertainment industries are prized targets for criminals who are looking to trade in stolen information and access. The accounts are sold in bulk, and the goal for the criminals is to move their goods by volume, rather than single account sales.

Many accounts compromised via credential stuffing will sell for as little as $3.25 USD. These accounts come with a warranty: If the credentials don't work once sold, they can be replaced at no cost, which is a service sellers offer to encourage repeat purchases. The reason this service exists is that brands have become increasingly quick to detect compromised accounts and deactivate them.

So how do credential stuffing attacks translate into stolen accounts that are later sold on a criminal marketplace? Short answer: password sharing.

Credential stuffing attempts can advance to full-blown account takeovers and compromises because people tend to use the same password across multiple websites — or the passwords they are using are easily guessed, and they generated credentials.

Top Attack Sources

SOURCE COUNTRY	ATO HEUR.LOGINS
United States	4,016,181,582
Russia	2,509,810,095
Canada	1,498,554,065
Vietnam	626,028,826
India	625,476,485
Brazil	585,805,408
Malaysia	369,345,043
Indonesia	367,090,420
Germany	354,489,922
China	308,827,351

Figure 4

Top attack sources sorted by country; the United States remains the top source for credential stuffing

Top Attack Destinations

DESTINATION COUNTRY	ATO HEUR.LOGINS
United States	12,522,943,520
India	1,208,749,669
Canada	1,025,445,535
Germany	760,722,969
Australia	104,655,154
Korea	37,112,529
China	26,173,541
Gibraltar	6,559,360
Netherlands	4,991,790
Japan	3,424,334
Italy	2,601,632
France	1,864,733
Hong Kong	1,305,262

Figure 5

Top attack destinations sorted by country; the United States remains the top destination for credential stuffing attacks

So a data breach at one website, or a massive release of known combinations of usernames and passwords (such as releases 1–5), can translate into one person having their entire digital life exposed. Once that happens, every bit of information associated with said individual can be packaged and sold.

As expected, the United States topped the source country list for credential stuffing attacks. This is because most of the common credential stuffing tools are developed there. Russia hits a close second, with Canada in third place. Also, the United States is the number one spot for attack destinations, because many of the most popular targets are based there.

India and Canada are a close second and third for attack destinations, but are greatly overshadowed in volume compared with the United States.

> *"The United States is the number one spot for attack destinations."*

Looking Forward

The impact that credential stuffing criminals can have on businesses is wide reaching – combination lists like the ones anonymously released earlier this year are just the tip of the iceberg. When a credential stuffing attack is successful, the brand takes a hit to its reputation (even if it isn't their fault), and faces increased operational costs as incident response, payroll, crisis communications, and other associated expenses start to mount.

> *"When a credential stuffing attack is successful, the brand takes a hit to its reputation (even if it isn't their fault)…"*

In February 2019, a well-known online tax service issued breach notifications to some customers. The notification letter clearly explained how the attack itself was credential stuffing, as all of the accounts at risk were using passwords exposed by data breaches elsewhere. The tax service reset passwords to prevent further access and warned customers. While the incident clearly wasn't the tax service provider's fault, customers felt otherwise, and the public reaction to the news was less than positive.

Partnering with a solid solutions provider to help detect and stop credential stuffing attacks is the obvious option to defend against such things. But addressing the credential stuffing threat isn't a simple situation. An organization needs to ensure a defensive solution is tailored to the business, as criminals will adjust their attacks accordingly to evade out-of-the-box configurations and basic mitigations.

And yet there is more to fixing the problem than a single vendor or set of products. Users need to be educated about credential stuffing attacks, phishing, and other risks that put their account information in jeopardy. Brands should stress the use of unique passwords and password managers to customers and highlight the value of multi-factor authentication. When discussing ATOs and AIO scripts, criminals often complain about the use of multi-factor authentication, which is a particularly effective method of stopping most of their attacks.

Constant reinforcement of these solutions, managed the same way any awareness program would, has worked for organizations in the financial and gaming industries.

Methodologies

For purposes of this report, credential stuffing attempts are defined as unsuccessful login attempts for accounts using an email address as a username. To identify abuse attempts, as opposed to real users who can't type, two different algorithms are used. The first is a simple volumetric rule that counts the number of login errors to a specific address. This differs from what a single organization might be able to detect because Akamai is correlating data across hundreds of organizations.

The second algorithm uses data from our bot detection services to identify credential stuffing from known botnets and tools. A well-configured botnet can avoid volumetric detection by spreading its traffic among many targets, by using a large number of systems in its scan or spreading the traffic out over time, just to mention a few countermeasures.

Research into the tools and tactics of credential stuffing botnets was done by hand, using a wide variety of web searches and human intelligence.

Credits

State of the Internet / Security Contributors

Shane Keats, Director of Global Industry Marketing, Media and Entertainment – YouTube research

Steve Ragan, Researcher, Sr. Technical Writer – Darknet market research

Martin McKeay, Editorial Director – Credential stuffing attack data and analysis

Editorial Staff

Martin McKeay, Editorial Director

Amanda Fakhreddine, Sr. Technical Writer, Managing Editor

Steve Ragan, Sr. Technical Writer, Editor

Program Management

Georgina Morales Hampe, Project Manager – Creative

Murali Venukumar, Program Manager – Marketing

Akamai secures and delivers digital experiences for the world's largest companies. Akamai's intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai's portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world's top brands trust Akamai, visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 04/19.