Protecting Media Logins from Credential Stuffing

How to build your defense
Introduction

Credential stuffing is on the rise. Akamai observed 55 billion attacks during a recent 17-month period (November 2017 through the end of March 2019) and we are not alone in observing this epidemic. What is new is that attackers have shifted their target. Media companies – OTT providers, newspapers, game publishers, etc. – have become the number one target. Video game companies alone accounted for one out of every five attacks Akamai logged.

The reasons for this surge are simple: Media companies now capture and store an enormous amount of data that has value on the dark web, but media companies are also complex – the device and login landscapes they must use to serve their customers lend themselves to attack. In the inevitable arms race that has resulted, media companies find themselves in need of more advanced tools to fight back.

This primer offers data that you can use to help you make the case for devoting additional resources to your company’s credential stuffing defenses, as well as suggestions for tools and approaches that can help.
The Extent of Credential Stuffing

The Many Names of Credential Stuffing

- Credential Abuse
- Password List Attack (PLA)
- Account Takeover (ATO)
- Account Hijack
- Login Abuse
- Account Checking
- Password Checking
- Password Spraying
- Password Guessing
- Etc.

Credential stuffing is known by many names. No matter what the activity is called, however, this form of attack has been increasing. In 2018, for example, we observed five days with more than 200 million attacks and three days on which fraudulent login requests exceeded 250 million. Video game companies were often the primary target.

The Cost of Credential Stuffing

Successful credential stuffing attacks have a significant impact on company costs. Obviously, IT and security teams spend time monitoring, detecting, fighting, and logging these attacks. But there are other, less obvious costs: Fraud teams and customer support resources devote scarce time dealing with account resets all day; and legitimate viewers, players, and readers are forced to change passwords, adding friction to the customer experience and leading to reduced customer satisfaction and increased churn.

Akamai sought to quantify these costs by commissioning the Ponemon Institute to research the financial impact of credential stuffing. Ponemon analysis determined that the average annual cost to a large video programmer was $6 million.
Protecting Media Logins from Credential Stuffing

Additionally, some companies consider large-scale successful credential stuffing campaigns to be data breaches reportable under law and regulations such as the GDPR.

Table 1 presents the cost for a security team to deal with this type of attack.

### Annualized Cost Estimates for a Large Video Programmer

- **Customer churn:** $2.7 million
- **Application downtime:** $1.7 million
- **IT security resources:** $1.6 million

The total annualized cost of credential stuffing, excluding fraud, can average more than $6 million.

<table>
<thead>
<tr>
<th>COST OF CUSTOMER CHURN</th>
<th>CALCULUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>A = Average value of customer</td>
<td>$1,494</td>
</tr>
<tr>
<td>B = Percentage of customers who churn as a result of a credential stuffing attack</td>
<td>7.56%</td>
</tr>
<tr>
<td>C = Average number of user accounts that are typically targeted</td>
<td>1,252</td>
</tr>
<tr>
<td>D = Percentage of successful credential stuffing attacks</td>
<td>12.40%</td>
</tr>
<tr>
<td>E = Average number of credential stuffing attacks per month</td>
<td>12.72</td>
</tr>
<tr>
<td>F = (A x B x C x D x E)</td>
<td>$222,804</td>
</tr>
<tr>
<td>G = F x 12</td>
<td>$2,673,648</td>
</tr>
</tbody>
</table>

Source: [Ponemon Institute, 2017](#)

Additionally, some companies consider large-scale successful credential stuffing campaigns to be data breaches reportable under law and regulations such as the GDPR.
Credential Stuffing Ecosystem Basics

Although the media industry has become the number one target for these attacks, the overall basics are the same no matter what the industry. Because most people reuse usernames and passwords across multiple sites and services, stealing the login of one service often provides access to all. Attackers know and exploit this.

Combolists

Credential stuffing is enabled by data breaches and phishing attacks. Lists of these stolen usernames and passwords are added to a "combolist," which is then offered for share, trade, and sale in underground forums.

Automated Account Checkers

Combolists can run to hundreds or even millions of entries. To extract the full value of the list, the attacker needs to use a tool to automate the process of checking each account. These tools, sometimes called account checkers, test each login against a target service or site. The more advanced versions, called All-In-Ones (AIOs), support plugins for multiple target services and sites, as well as the ability to relay traffic through a large set of proxies to evade detection.
Attack Monetization

Once an account is compromised, the attacker has several options for making money out of the account details:

- Resell the account
- Steal in-game virtual items
- Evade digital rights management (DRM), antipiracy controls, and per-user download limits
- Steal download tokens to use in DRM-free players
- Create spam or leave harassing comments on articles
- Buy and resell real-world merchandise and prepaid gift cards
- Bypass paywalls

For example, in 2019, Akamai research found that compromised video game accounts can sell for as little as $1.30. The price depends on volume (number of accounts purchased), account type, and what the account includes (skins, weapons, currency, etc.). Darknet marketplaces include accounts for popular titles such as Fortnite, Minecraft, Clash of Clans, Runescape, CS:GO, NBA 2019, League of Legends, Hearthstone, Dota 2, PlayerUnknown’s Battlegrounds (PUBG), and Apex Legends, as well as the Steam and Origin platforms.
These findings are similar to those of security software provider Irdeto. They, monitored 15 dark web marketplaces during April 2018 and found 69 unique sellers of data, and the average price for a single stolen account was $8.71.

Taken together, these tools and ecosystem have made it easier than ever for even novice hackers to commit a profitable credential stuffing attack. Akamai has discovered that there are even tutorials on short-form video sites, many with thousands of views, that teach viewers how to download and use account checkers and AIOs.

Challenges with Identifying Credential Stuffing Bots

In the early days of bot management solutions, website defenders used rudimentary tools such as IP address and user-agent blocking. Over time, bot developers evolved their tools to look more like legitimate clients. This forced defenders to use more of the request context data, as well as web browser client characteristics, such as session token, operating system and browser versions, language encodings, etc.

When customers of a service use a standard web browser for login, defenders can successfully use this data to identify and manage bots. However, the majority of logins for broadcast, OTT, gaming, and publishing sites happen via applications running on mobile devices, streaming media players (SMPs), and gaming consoles. This has several implications for the identification of bots.
Applications typically access services via API, and APIs normally receive requests with little contextual data about the human operating the application.

API request templates are easy to capture and replay.

APIs sometimes use nonstandard ports and protocols instead of the typical web-centric HTTP and HTTPS on TCP ports 80 and 443.

As a result, media companies that want to protect login and reduce account takeover need additional tools.

Four recommendations for protecting your customers’ identities

Akamai has worked with media companies large and small, across the globe, to tackle this challenge. That work has yielded a lot of best practices. Here are our top recommendations.

1. **Code your login page/API with OWASP**
   - Write secure code according to the OWASP best practices and do a penetration test on your login endpoints.

2. **Use anti-DDoS protection**
   - Using anti-DDoS protection can help you prevent volumetric botnets from reaching your infrastructure and overwhelm your assets.

3. **Use a bot management solution**
   - Using a bot management solution can help with sophisticated credential abuse attacks by verifying user behavior and device telemetry.

4. **Use an identity as a service provider**
   - Use an identity as a service (CIAM) provider that will manage your identities for you in a secure and reliable manner.

Serving today’s viewers, readers, and players requires media companies to meet them on their terms, on the devices they use. But that then requires companies to step up their defensive game if they want to better protect their crown jewel: their customers.

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 akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 3/20.