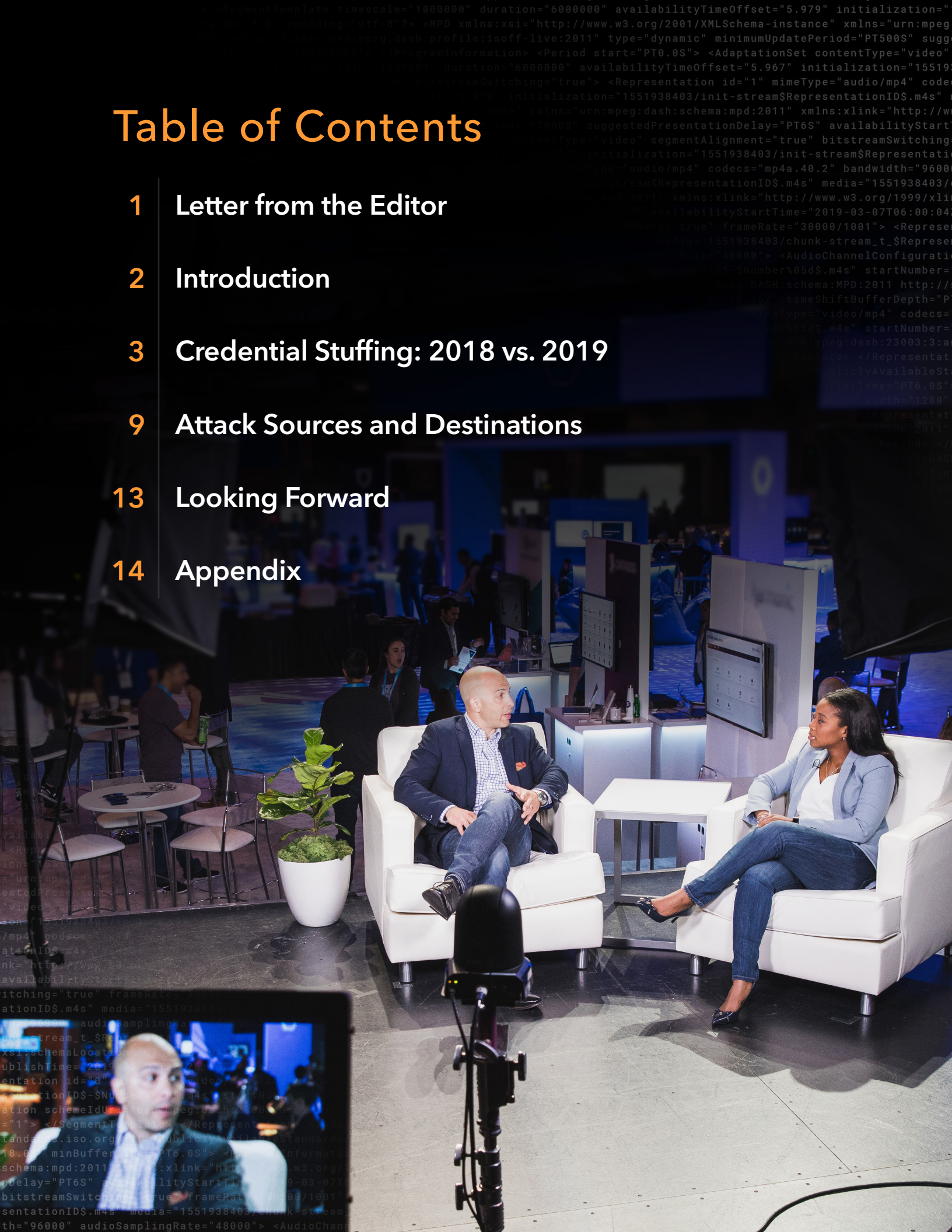


Credential Stuffing in the Media Industry

Table of Contents

- 1 Letter from the Editor
- 2 Introduction
- 3 Credential Stuffing: 2018 vs. 2019
- 9 Attack Sources and Destinations
- 13 Looking Forward
- 14 Appendix



Sometimes you make plans. Sometimes those plans get pushed to the side, turn up, and thrown into the wind.

That's what happened with this issue of our report. current events. These sections help give you the

This State of the Internet / Security Report was originally scheduled to be a brief document, focusing on the media industry. It was meant to be published shortly before a large media conference.

When the conference was cancelled because of the COVID-19 pandemic, we took a step back to reflect on our course of action. Should we publish what we had at that point, ignoring the effects of COVID-19? Should we scrap it and wait to see how COVID-19 influences the media industry? Or was there a third option?

When this team, Akamai, and almost every other company in the world started to transition to a work-from-home/school-from-home/live-at-home setup, we knew we had to acknowledge the changes that were happening around us. It's been a high stress time. While our research shows the internet is unlikely to break, it has become an even more vital part of how businesses operate and how people communicate.

We must continue to be aware that criminals are utilizing all the tools at their disposal to make money. Keeping your important information safe by practicing good credential hygiene is now more important than ever. In other words, don't reuse passwords.

Come to think of it, good hygiene is extremely important these days, whether we're talking about

This report is like a mini time capsule – the original report remains intact. We dive deep into the data from January 1, 2018, to December 31, 2019, and keep the original analysis of how credential stuffing has impacted media companies. When we look just at the media sector during this period, we can see that Akamai recorded 17 billion credential stuffing attacks during that 24-month period.

During the first quarter of 2020, there were changes to the attack landscape worldwide and an increase in our own visibility. The team was quick to pivot, and we were able to include new data from current events. These sections help give you the most current information we're able to share.

While we navigate these historic times together, we must continue to be aware that criminals are utilizing all the tools at their disposal to make money.

While we navigate these historic times together, we must continue to be aware that criminals are utilizing all the tools at their disposal to make money. Keeping your important information safe by practicing good credential hygiene is now more important than ever. In other words, don't reuse passwords.

Come to think of it, good hygiene is extremely important these days, whether we're talking about the digital world or the physical one.

So, on behalf of the entire State of the Internet / Security team – be healthy, be safe, and we are happy to share our latest analysis with you.

Amanda Goedde
Managing Editor, SOTI

Introduction

Between January 1, 2018, and December 31, 2019, Akamai recorded more than 88 billion credential stuffing attacks across all industries. When we look specifically at the media sector, which includes streaming media, television networks, cable networks, broadcasting, and even digital publishing and advertising, that number is about 17 billion, or about 20% of all attacks.

In our previous media report, we wrote that media organizations were among the biggest targets of credential stuffing, and here we see continuing support of this observation. In large part, the public visibility of media companies makes them the target of attacks more frequently than most other verticals.

Year over year, there was a 63% increase in credential stuffing attacks in the video media sector when we examine data for 2018 and 2019. Some of this growth is due to new visibility. With more customers and customer assets (i.e., hostnames) being added to the fold, it shows that even with a vast amount of visibility, we're only scratching the surface when it comes to the attacks we're seeing.

Criminals realize the resale value of accounts in the media industry and that the personal data those accounts contain is useful, too. That data can be collected and resold as a sort of "value-add" proposition to the compromised media assets.

For example, a compromised pizza account with reward points (enabling free food delivery) is combined with a compromised streaming media account in the same location and sold to people in those areas, often at a markup.

These "date-night" offers are pre-packaged and leverage a number of data points, all of which come from examining the compromised source.

The same thing happens with money laundering. Criminals will take a person's identity, match it to compromised financial accounts, and verify their location and other data points by looking at what's in their streaming media profiles. If the media platform's data (address, name, and access locations) matches the compromised personal information, as well as the records on their financial accounts, then the criminal has all the information needed to acquire proxy services or remote desktop access in the general geographic region. Doing so enables them to slip past some of the more basic defenses and is a key element to many account takeover scams.

Data for 2018 and 2019 shows a 63% year-over-year increase in credential stuffing attacks against the video media sector.

In this report, we examine the attack trends in the media sector over a 24-month period, as well as what organizations are seeing on a continual basis. The data shows that credential stuffing attacks and account takeover activity in the media industry continue to grow at a steady pace, without any signs of slowing in the near future.

Credential Stuffing: 2018 vs. 2019

Daily Malicious Login Attempts Against Media 2018 vs. 2019

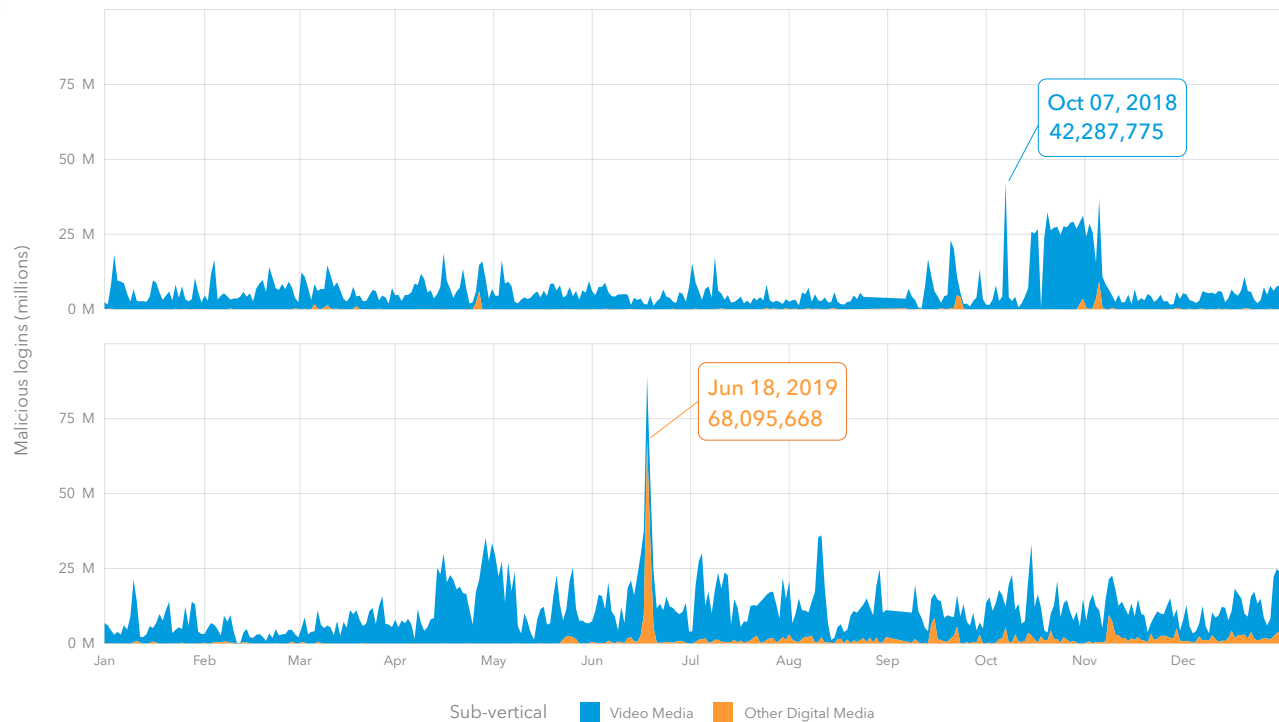


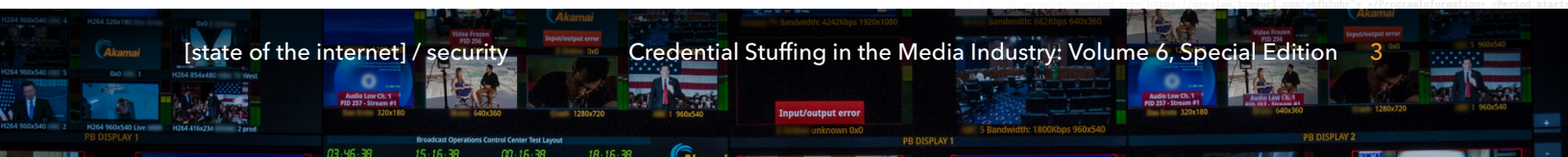
Fig. 1 – There was a consistent stream of credential stuffing attacks across the media industry over the past 24 months

Akamai detects tens of millions of attacks each day against the media industry. As you can see in Figure 1, we have also split the industry into two – video media and other digital media. The standout element in these graphics is the consistent nature of the attacks, with peaks in the summer and late fall.

Such time-based attacks are often attributed to what security professionals call the “kids are home” effect, where low-level, easily detected attacks are presumably conducted by unsophisticated actors, or script kiddies. Filled with the hype of easy money, the script kiddies start using tools and free credential

lists shared on criminal forums in an attempt to compromise accounts of all kinds, including those in the media industry. Their goal is typically to resell access at a markup.

In addition to summer and late fall, these attack peaks are also observable during holidays and periods associated with academic breaks, such as spring break in the United States. Make no mistake, though – just because the actors responsible lack technical acumen and a high degree of sophistication, low-level attacks are effective and can be linked to several high-profile data breaches.



Daily Malicious Login Attempts Against Media Q1 2020

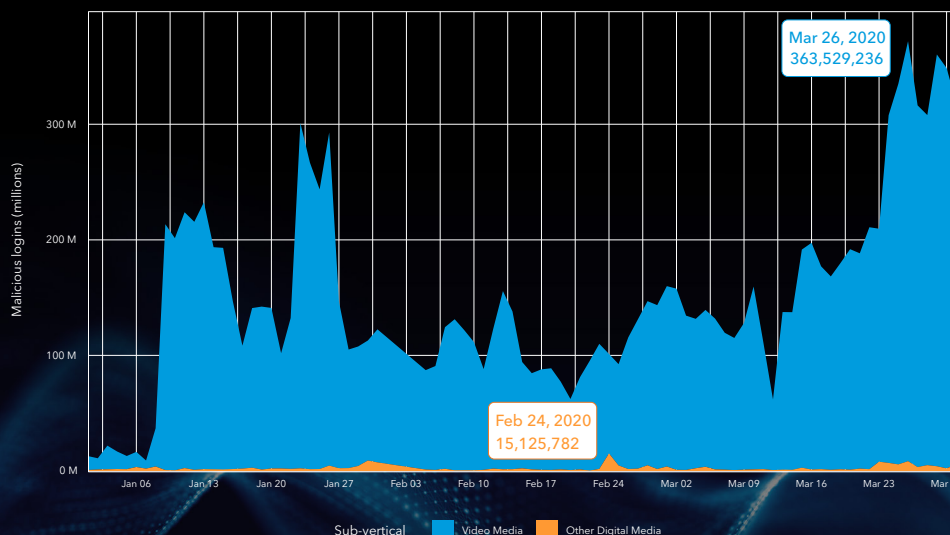


Fig. 1a - The apparent fourfold increase in attacks (compare the y-axis here with Figure 1) is partly attributable to the enhanced visibility into the threat landscape

Visibility, when writing reports such as this, or when defending an enterprise, is critical. You need to see the attacks in order to stop them or track them. After this report was written, it was delayed by COVID-19. In the weeks and months that followed, there were changes to the attack landscape worldwide and an increase in Akamai's visibility.

Figure 1a is similar to Figure 1, but with a focus on Q1 2020 and additional visibility from our Cloud Security Intelligence (CSI) tool. CSI is an internal tool for storage and analysis of security events detected on the Akamai Intelligent Edge Platform, which comprises more than 290,000 servers in thousands of networks around the globe. Our security teams use this data – measured in petabytes per month – to research attacks, flag malicious behavior, and feed additional intelligence into Akamai's solutions.

Clearly there has been a large spike in malicious login attempts. Notice that the scale for the y-axis of the updated plot is about four times larger than the original. While the spike happened during the

COVID-19 lockdown in Europe, there is no way to conclusively prove that the global pandemic was the sole cause. However, there are some interesting observations in the data.

On March 26, 2020, a video media service in Europe experienced a strong spike in attacks, reaching 348,050,675 malicious login attempts in 24 hours, accounting for 96% of all malicious login attempts against the video media sub-vertical during the same period. This service provider was one of several that were targeted, as credential stuffing attacks reached peaks in the hundreds of millions daily during Europe's lockdown.

Throughout Q1 2020, criminals merged old combination lists with newer lists and trained their collections on some of the world's largest streaming media providers to generate freshly verified accounts that could be sold on the open market. Akamai's increased global visibility allowed us to gain better insight into these attacks and the massive scale on which they occurred.

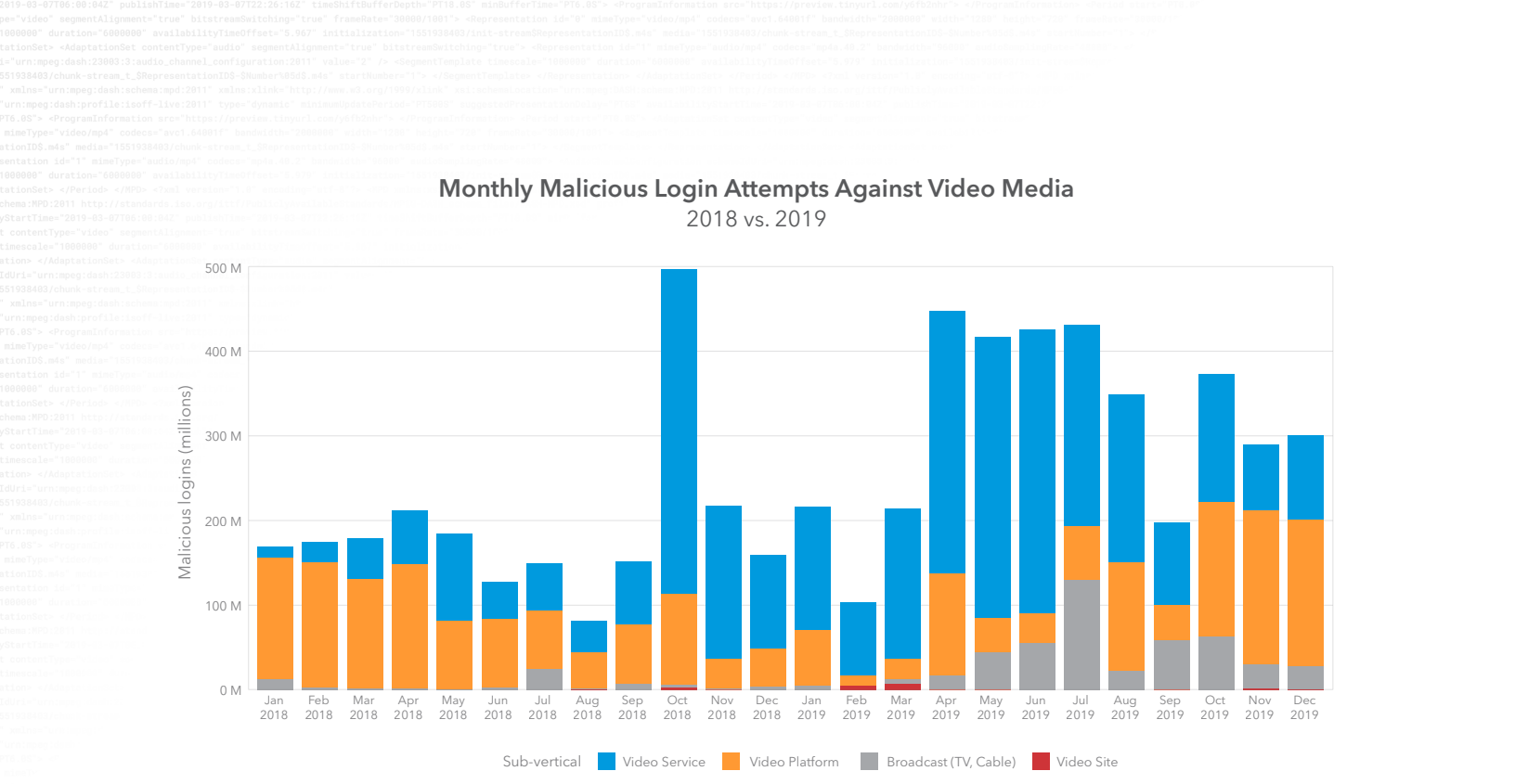
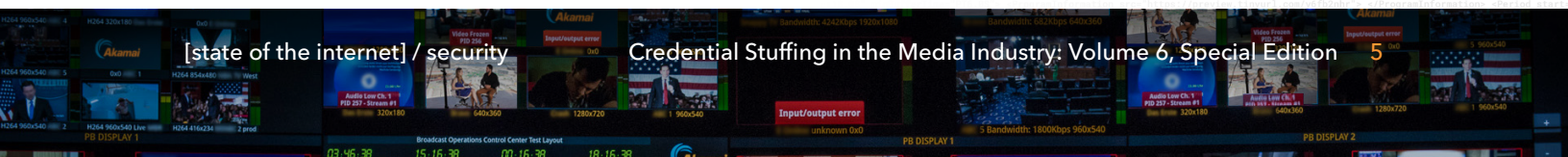


Fig. 2 - Video websites and broadcast television became hot targets for criminals in 2019, but video services remained their primary focus

In Figure 2, we see a breakdown of sub-verticals, where video services and video platforms are the top two targets. These two sub-verticals are natural targets, as access to streaming platforms and services is in hot demand for criminals. Again, criminals who conduct these attacks desire not only the commercial assets (new-release movies, original programming, television), but also the ancillary data on the account, such as personal and geographical information.

There was a 98% year-over-year increase in the level of attacks against video services, with a 5% drop in attacks against video platforms. However, the standout change can be seen with broadcast television and video websites, which experienced 630% and 208% increases, respectively.

It's all about access. Broadcast television and video websites align well with the criminal goals observed when targeting video services and platforms. In 2019, the world saw an explosion of on-demand media, especially in the broadcast space. Also, two popular new video websites were introduced to consumers via several promotions, including free access to those who are customers of a related ISP. Websites that provide on-demand access to local television, sporting events, and educational entertainment were all hot targets from the middle of 2019 until the end of the year.



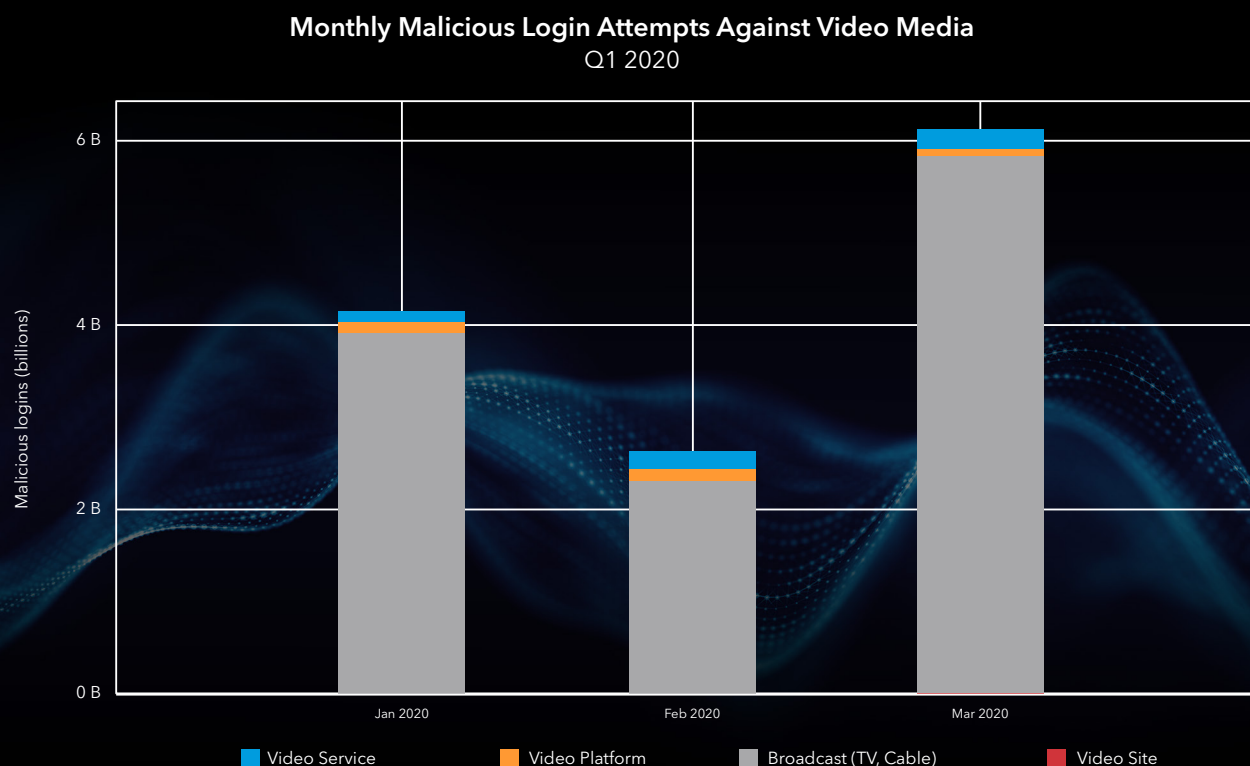


Fig. 2a - Most of the huge spike in broadcast media attacks were against one customer

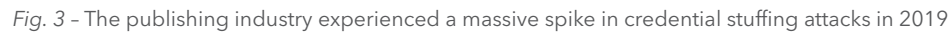
As previously mentioned, video websites and broadcast television became hot targets in 2019. We can see in Figure 2a that this is still the case. Yet it is important to note that the massive spike in attacks against broadcast television can be sourced to a single customer.

This customer has massive reach in Europe due to various partnerships with media service providers. The brand recognition, as well as this particular provider's reach, made it a top target for credential stuffing early on in Q1 2020, hitting attack peaks ranging in the billions each month of the quarter. As with Figures 1 and 1a, take note of the change in the y-axis scale when comparing the updated and original plots. The original

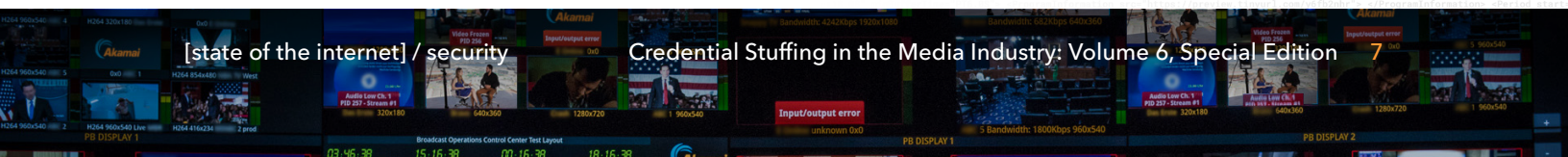
plot shows October 2018 with the highest total for a single month during the two-year period, with just less than half a billion attacks. That peak is a mere bump now, when compared with the 6 billion malicious login attempts observed during March 2020.

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.

Monthly Malicious Login Attempts Against Other Digital Media



When criminals conduct credential stuffing attacks, they start with a set of usernames and passwords, and then use bots or automated tools in an effort to access assets. They usually focus on financial services and streaming media first; however, criminals will eventually target everything they can. This means that academic publishing, online news portals, region-locked broadcasts, e-book services, and so forth are all – in the criminals' eyes – fair game.



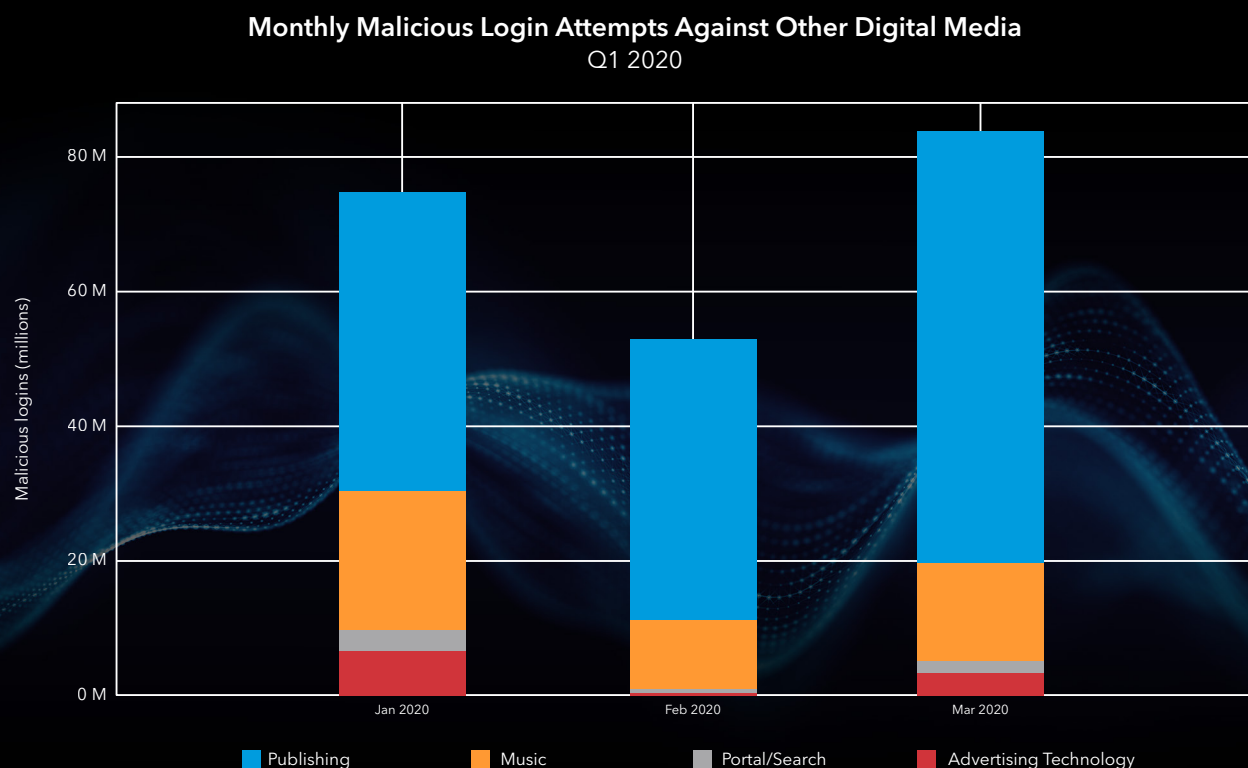


Fig. 3a – Along with a continuation of trends that started in 2019, Q1 2020 saw an uptick in attacks against advertising technology

In Q1 2020, the trend of credential stuffing attacks against publishing continued, with slight increases in the streaming/on-demand music industry as well (see Figure 3a). There is no way to conclusively prove these spikes are related to COVID-19, but as in the video media sector, criminals were actively selling and trading access to various music and publishing platforms in February and March, as well as circulating combination lists in order to target new accounts.

Particularly of interest were the number of criminals who shared free access to various newspaper accounts to boost their own personal brand and reputations. Criminals often give away working username and password combinations to various services as a means of self-promotion and branding. However, to obtain these freebies, credential stuffing campaigns must be initiated. There were several of them in Q1 2020, revealing credentials for various publications, advertising platforms, and music services.

Attack Sources and Destinations

Top Source Areas of 2019 – Malicious Logins Against Media

SOURCE AREA	2019 TOTAL	YOY CHANGE 2018 TO 2019
United States	1,106,075,259	162%
France	393,053,557	407%
Russia	242,801,831	67%
Netherlands	215,858,077	217%
Germany	181,107,515	128%
Brazil	152,389,083	71%
India	150,954,578	-37%
Singapore	137,037,227	142%
United Kingdom	131,931,328	42%
Indonesia	97,448,973	234%

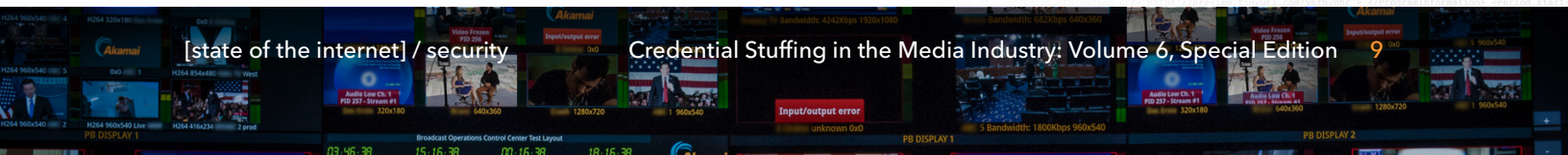
Fig. 4 – The United States remained the top source of credential stuffing attacks, but there were noticeable year-over-year (YOY) spikes in France, the Netherlands, Singapore, and Indonesia

The source areas of credential stuffing attacks are the locations where the attacks originated, though the criminals driving the attacks could be anywhere, as Akamai can only see the “final hop” of the attack. When we look at the 2019 numbers and compare them year over year, as in Figure 4, several notable increases appear. While seeing the United States at the top of the list isn’t shocking, as criminals find easy proxy access there, the uptick in France, the Netherlands, Singapore, and Indonesia is a bit of a surprise.

It isn’t immediately clear why these countries had such a year-over-year spike. Examining the targets being hit from these locations indicates that the victims are scattered. Some are video platforms and video services, while others

represent broadcast television, publishing, and social media. A common thread across each of the countries with a significant spike, which is more speculation than fact, is that all of them had credentials leaked at various stages over 2019, and proxy services in those locations were cheaper than other locations. In some cases, proxy fees could dip as low as 49 cents an hour, with top tier offers only reaching 99 cents an hour, with locations in the European Union, the United States, and Canada.

Criminals are not picky about location when it comes to launching an attack. As long as they can hide themselves and leverage proxy services for their bots, they’re going to use whatever is available.



Top Sources Areas of Q1 2020 – Malicious Logins Against Media

SOURCE AREA	MEDIA	ALL VERTICALS
United States	1,911,335,476	7,417,823,520
France	1,019,358,941	1,617,205,897
Brazil	649,022,806	1,121,054,851
Poland	632,344,358	679,589,056
Indonesia	523,598,887	931,841,370
Russia	510,798,702	871,467,745
Netherlands	480,689,352	896,971,365
Germany	448,044,870	1,137,856,581
Thailand	395,099,677	873,507,956
China	394,848,730	1,730,368,258

Fig. 4a - Q1 2020 saw a shuffling of leading attack source areas

There has been a clear increase in numbers during Q1 2020, and several rankings in the top five positions have shifted (see Figure 4a). The United States and France are still the top two source areas, but Russia was replaced by Brazil, the Netherlands was replaced by Poland, and Germany fell toward the bottom of the list after being replaced by Indonesia.

It isn't clear why there was such a shift in geographic ranking. Each of the top five countries have well-known and established brands that criminals target. They also have established proxy services up for sale, which could account for some of the change in recent months, as more people are home and using proxies for both legitimate and illegitimate reasons. However, we simply don't have enough data to make a conclusive determination.

Top Target Areas of Q1 2020 – Malicious Logins Against Media

TARGET AREA	MEDIA	ALL VERTICALS
France	12,010,942,083	12,235,691,613
India	682,804,616	958,303,704
United States	345,764,310	10,765,342,972
Italy	27,551,548	80,840,601
United Kingdom	18,071,667	272,181,435
Germany	14,982,744	460,800,209
Australia	14,867,093	78,312,783
Finland	2,154,271	2,462,277
Switzerland	584,838	2,130,302
Canada	349,018	659,927,969

Fig. 5a – Some of the shuffling of top target areas in Q1 2020 correlate with effects of the pandemic lockdowns in various parts of the world

As we saw in Figure 5, the United Kingdom and the European Union experienced serious year-over-year attack growth, and the Q1 2020 data in Figure 5a shows that this continues to be the case. The significant growth in Europe is due to Akamai's expanded visibility into attack traffic, so this was an expected change. China completely disappeared from the top 10 because of a drop in attacks, while Canada made its entrance in the first quarter of the year. As previously mentioned, the nations listed here represent the billing locations for the organizations being targeted.

While none of these changes can be definitively connected to COVID-19, there are some curious indications that can't be ignored. Italy moved up to the top five and had consistent attack traffic during the country's mandated pandemic lockdown. It isn't clear if that was because criminals were stuck at home, too, or if outsiders were targeting companies based there.

Appendix



Supplemental Data

Top Source Areas – Malicious Logins

MEDIA VERTICALS				ALL VERTICALS		
Source Area	2018	2019	YoY Change	2018	2019	YoY Change
United States	422,483,545	1,106,075,259	162%	14,359,304,968	14,886,361,909	4%
France	77,581,134	393,053,557	407%	823,078,544	1,661,385,937	102%
Russia	145,809,672	242,801,831	67%	4,261,652,136	1,765,456,425	-59%
Netherlands	68,067,234	215,858,077	217%	1,047,784,566	830,924,341	-21%
Germany	79,305,093	181,107,515	128%	894,003,476	1,430,819,154	60%
Brazil	89,034,848	152,389,083	71%	1,948,034,815	2,073,066,375	6%
India	241,114,285	150,954,578	-37%	1,313,967,923	1,878,279,277	43%
Singapore	56,627,940	137,037,227	142%	552,662,315	1,213,497,779	120%
United Kingdom	92,682,256	131,931,328	42%	803,067,972	970,719,134	21%
Indonesia	29,185,095	97,448,973	234%	922,233,454	1,774,834,686	92%

Top Target Areas – Malicious Logins

MEDIA VERTICALS				ALL VERTICALS		
Target Area	2018	2019	YoY Change	2018	2019	YoY Change
India	1,119,140,037	2,394,309,395	114%	1,320,840,577	5,563,333,116	321%
United States	1,161,578,140	1,421,345,721	22%	34,343,633,488	32,133,407,450	-6.44%
United Kingdom	252,151	124,273,711	49,185%	287,026,423	875,673,215	205.08%
France	1,864,733	75,797,079	3,965%	24,973,561	264,869,149	960.60%
Germany	10,119,511	66,864,153	561%	828,017,738	764,955,305	-7.62%
Italy	1,287,890	38,248,972	2,870%	75,034,794	171,175,121	128.13%
Australia	33,294,168	29,949,976	-10%	148,489,698	113,763,464	-23.39%
Finland	928,999	6,557,245	606%	1,311,570	6,603,047	403.45%
Switzerland	866,350	2,268,087	162%	76,538,312	106,311,356	38.90%
China	26,376,170	1,248,276	95%	2,329,983,440	3,058,416,048	31.26%

Credits

State of the Internet / Security Contributors

Omri Hering

Senior Data Analyst –
Credential Abuse

Lydia LaSeur

Data Scientist –
Credential Abuse

Editorial Staff

Martin McKeay

Editorial Director

Amanda Goedde

Senior Technical Writer, Managing Editor

Steve Ragan

Senior Technical Writer, Editor

Lydia LaSeur

Data Scientist

Marketing

Georgina Morales Hampe

Project Management, Creative

Murali Venukumar

Program Management, Marketing

More State of the Internet / Security

Read back issues and watch for upcoming releases of Akamai's acclaimed State of the Internet / Security reports. akamai.com/soti

More Akamai Threat Research

Stay updated with the latest threat intelligence analyses, security reports, and cybersecurity research. akamai.com/threatresearch

Access Data from This Report

View high-quality versions of the graphs and charts referenced in this report. These images are free to use and reference, provided Akamai is duly credited as a source and the Akamai logo is retained.

akamai.com/sotidata



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 07/20.