Volume 5, Special Edition

Media Under Assault

Akamai Intelligent Security Starts at the Edge

Table of Contents

Overview

From January 2018 through June 2019, Akamai recorded more than 61 billion credential stuffing attempts and more than 4 billion web application attacks. In this special edition of the State of the Internet / Security Report, we're focusing on data within the high tech, video media, and entertainment sectors – collectively named Media & Technology.

These three industries accounted for nearly 35% of all credential stuffing attacks, and almost 17% of the web application attacks seen by Akamai during the 18-month reporting period. Our analysis indicates these three verticals are a stable and consistent attack source for two reasons: personal and corporate data. The targeted brands are household names, and criminals are looking to capitalize on that familiarity.

By attacking directly via web application attacks, criminals hope to expose customer records and financial data or leverage a vulnerable server to spread malicious code – also a common motive driving criminals to attack the retail sector. Credential stuffing abuses the brands targeted, as well as their customers, enabling the criminals to target personal information and corporate assets, such as media or digital products.

Web Attacks by the Numbers
January 2018 – June 2019

Total Number of Web Application Attacks: 4,068,741,948

- *High Tech: 609,117,260*
- *Video Media: 143,308,490*
- *Entertainment: 51,464,909*

Attack Types:

- *SQL Injection (SQLi): 69.7%*
- *Local File Inclusion (LFI): 21.6%*
- *Cross-Site Scripting (XSS): 3.5%*

Same Attacks, Different Risks, Global Impacts

Jaspal Jandu

Group CISO

DAZN

When it comes to the fundamental attack methodologies criminals use to compromise organisations, broadcasters and the media industry as a whole suffer from the same attack methods that many other industry verticals see every day. It's the risks that these attacks pose to media organisations that set our concerns apart.

When most broadcasters were only linear, and you had to be in front of a television at a pre-scheduled time to watch the show, the risks posed by technology were relatively simple in comparison to what affects us today. If anything interrupted a live transmission, the fault would likely be physical – either a cable issue or hardware failure. With today's shift to IP-based television (IP TV) and Over-the-Top (OTT) streaming, the risks are both dramatically increased and more complex to manage.

Supply-chain risk is a good example of how things have become increasingly complex. In today's world, traditional broadcast suppliers are now evolving into software companies. Cloud delivery mechanisms, such as Infrastructure as a Service (IaaS), have made this transition easier in some cases. But this approach also introduces considerably more third- and fourth-party risk that broadcasters now have to manage. This is a vastly different proposition than a decade ago, when most of the broadcast chain was delivered by tried-and-tested broadcast infrastructure fully in their control.

One of the biggest fears that broadcasters have is "black to air" – the moment when all the viewer sees is an empty screen. From a security point of view, Internet-based attacks such as Distributed Denial of Service (DDoS) are risks that broadcasters now have to think about across the supply chain. These are risks that have been around for decades in industries such as financial services. The new world of live IP TV, where much of the world's media is consumed, means that any attack on availability could result in subscriber retention issues, hit ad revenue, and reduce the chances of future successful bids for rights. There aren't second chances in live TV. Viewers don't care if it's a supplier issue – it's the broadcaster's reputation that takes the hit.

The media industry also has to deal with a great deal of cultural change on the regulatory front. Incorporating more data is now at the heart of many broadcasters' strategic ambitions. The drive is to not only to grow share of viewing, but also to look at where other opportunities exist to offer viewers a more tailored and relevant experience. There is a very fine line between legitimate business use of consumer data and exceeding the bounds of acceptable usage – a limit that isn't always apparent. The challenge for media is balancing the need to innovate and be agile against the risks that regulation creates in an environment where users demand constant innovation and cutting-edge entertainment opportunities.

Also following the cultural change, there's a skills shortage facing every business that needs to secure its digital assets. The challenge is finding skilled security professionals who understand the need to balance business opportunities against the risks of a rapidly changing world. Many security professionals have backgrounds in industries with strong compliance environments, like banking and government, and have difficulty adapting to more fluid environments. It's much easier to point to a regulation than to articulate the risks a particular decision might pose to a creative business.

There is one very structural risk unique to the media industry, with deep, complex societal ramifications: fake news. Broadcasters and social media have a significant impact on public views and opinions. While there can be debates about what is or isn't fake news, truly fake news and the ability to create "deep fakes" that are indistinguishable from real, trusted content pose a significant threat to the industry. These tools have the power to influence electoral outcomes and can give traction to toxic, divisive messages on a truly global scale. This attacks the very heart of trust and how we have come to learn about the world around us.

Nation-states are now paying much closer attention to broadcasters and media outlets as they realise they can reach a ready-made audience of millions. This is not just through compromising broadcast platforms, but also through the social media presence that many broadcasters and media outlets use. There have been at least two well-known cases of nation-state attacks on the media industry in the past five years.

Trust is vital to the future of the media industry. Maintaining consumer trust is not only threatened by the speed at which we address well-known risks, but also by how we respond to those risks that are unique to us, many of which simply didn't exist a decade ago. We do know that there is a significant cultural shift needed to deal with the threats, and there aren't enough of the right skills to go around. Things aren't about to change anytime soon; for now at least, we will continue to face a challenging road ahead, and the risks we now face could impact us more than we ever imagined.

Jaspal is a senior security professional with more that 20 years of experience. He has spent the last decade primarily focused on the media sector. He brings incredible insights into the risks faced by media organizations, having dealt with some of the most high-profile attacks against the sector.

The views expressed in this essay are the views of the author and do not necessarily reflect the views of Akamai.

Web Application Attacks

Attacks against the high tech sector, which includes equipment and software manufacturing, in addition to technology and service providers (such as cloud, mobile, telecom, and cable operators), accounted for the bulk of the attacks observed across Media & Technology, as shown in Figure 1.

In contrast, attacks against entertainment, which includes organizations like content providers, broadcasters, post-production, content development, research, and analytics, remained steady, with one very significant spike on September 22, 2018. The video media vertical, which includes distribution and delivery, as well as the film industry, likewise had a steady stream of attacks, which increased over time, culminating in a few peaks during the second quarter of 2019.

The consistent volume shows Media & Technology is an attractive target for the criminal economy. Personal information can be sold or traded once compromised, while corporate data can be leveraged in additional attacks. That same data can also be used by attackers to steal media streams, which is common during sporting events.

Equally damaging, criminals look to steal original content in order to release it before the intended broadcast date or sell it on various criminal markets. This is common with pre-release software and games (called *warez* in some circles), while music and movies are traded.

The attack peak in September 2018 was against a well-known international brand, and consisted only of SQL Injection (SQLi) attacks. It isn't clear what the criminals were after during this attack, but SQLi tends to be a straightforward attack against credentials and other data. It is unusual, but not unheard of, for a site to receive a brute-force SQLi attack of this intensity.

The second attack peak against high tech in November 2018, is a more interesting case. This attack was against another well-known brand – something of a high-value target, all things considered. The criminals were targeting the sensitive information held by this company. This attack consisted of Local File Inclusion (LFI) (82.3%), PHP Injection (9.3%), Command Injection (7.6%), and SQLi (0.7%) attempts.

Daily Web Application Attacks Targeting Media Verticals
January 2018 – July 2019

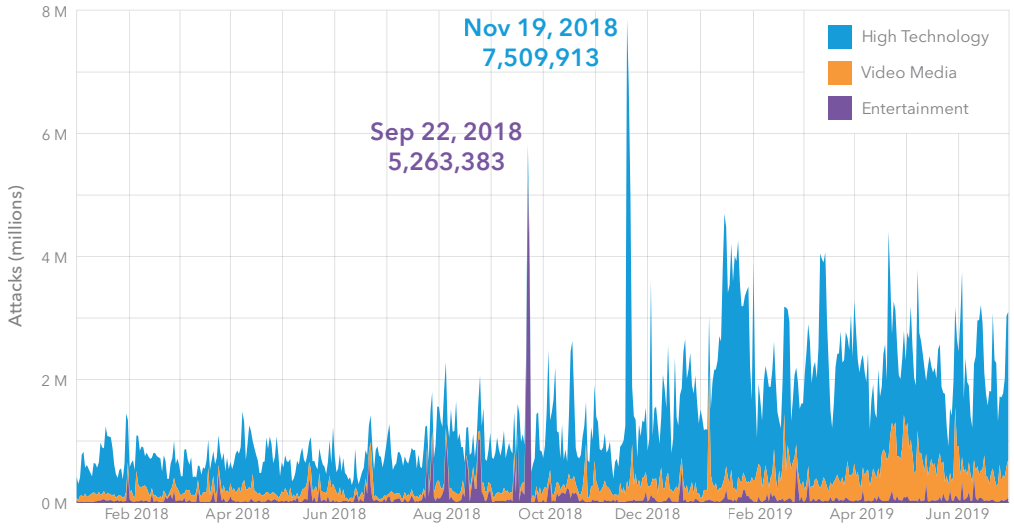


Fig. 1 – Application attacks have experienced noticeable growth since the second half of 2018 – a trend we expect to continue

SQLi remained the top attack vector during the 18-month window, with more than 70% of attacks, followed by Local File Inclusion (LFI) at 19.3%, Cross-Site Scripting (XSS) at 3.9%, PHP Injection at 3.3%, and Remote File Inclusion (RFI) at less than 1%.

SQLi attacks are the go-to attack method for criminals looking to acquire credentials, financial records, or anything else that a company might store in their database. However, injection attacks as a whole, as seen in Figure 2, accounted for more than 98% of the attacks against Media & Technology.

Code injection attack, which includes SQLi, LFI, RFI, and XSS, is a general term for attack types that enable an attacker to insert malicious code into an application that is then interpreted or otherwise executed. This differs from command injection attacks, because criminals use their own code.

In contrast, in command injection attacks, the adversary is limited to the default functions of the application or service.

The key aspect of any injection attack centers on poor data validation and handling. Such vulnerabilities have been discovered in platforms ranging from .NET, PHP, Java, JavaScript, and Ruby on Rails.

Code injection vulnerabilities can be leveraged in groups or individually (as observed in the two days highlighted in Figure 1), and the skills required to seek out and exploit such flaws are almost nonexistent. There are several tools on the Internet that automate scanning for code injection vulnerabilities and, in some cases, these tools will automate exploitation and exfiltration too.

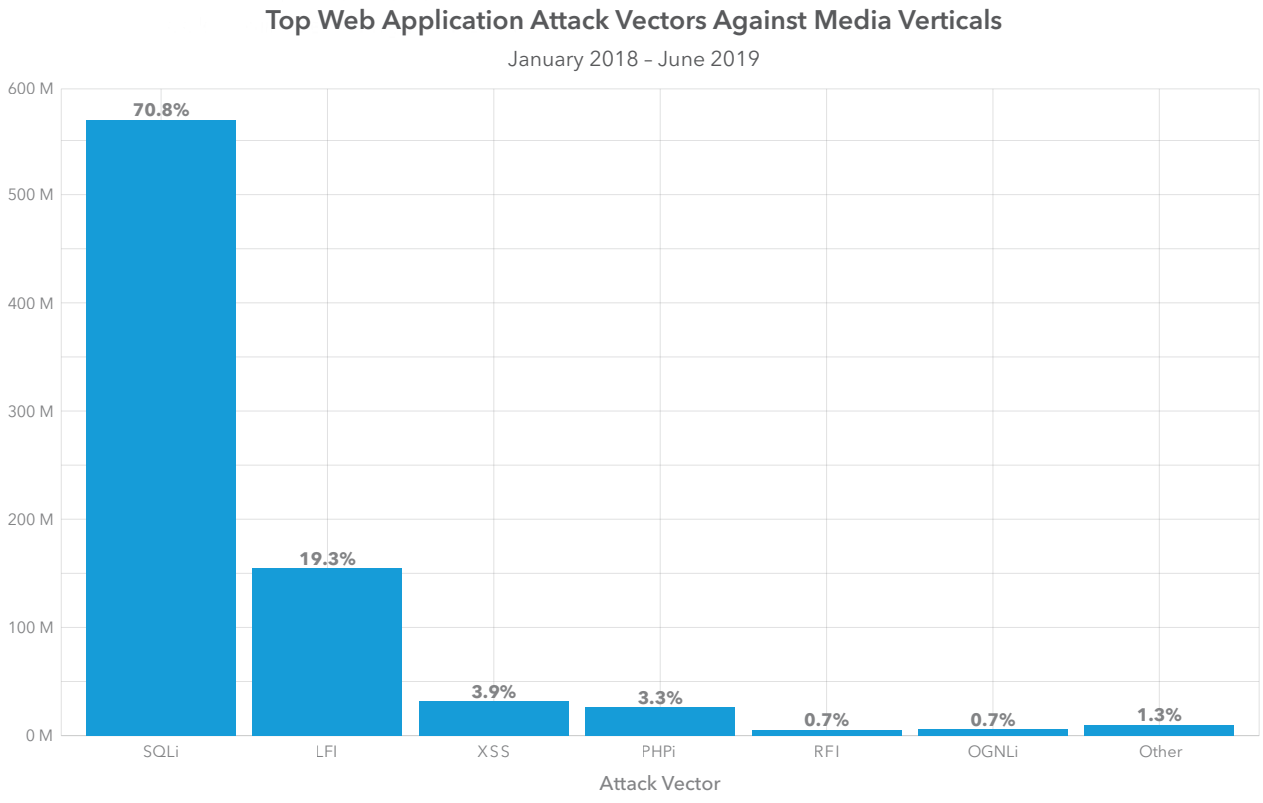


Fig. 2 – Injection attacks as a whole accounted for more than 98% of the attacks against the Media & Technology sectors

It's worth noting that most criminals aren't using sophisticated or specialized tools. They generally use the same legitimate programs widely available in numerous security offerings, including Metasploit and Kali Linux. Criminals with the skills to create bespoke tools are rarely noisy enough to show up in volume-based metrics, but they do exist.

Successful injection attacks can lead to compromised data and corporate assets — such as customer records, internal communications, business development plans, usernames, and passwords. Activists from the group LulzSec leveraged XSS, RFI, LFI, and SQLi in 2010 to launch a series of attacks that compromised dozens of websites and organizations. But injection attacks can also be an entry-level event, and set the stage for larger problems, such as what happened to Heartland Payment Systems in 2009.

So why do criminals leverage injection-based attacks? First, they provide a low entry barrier for criminals lacking advanced skills, thanks to tooled automation. The second reason these attacks are heavily favored is because they work.

When considering the global view for source of web attacks, the United States maintained the top spot globally across all verticals, followed by the United Kingdom and Germany. The top target for Media & Technology attacks was also the United States, with France placing second. In fact, as seen in Figure 3, 18.63% of all attacks seen by Akamai targeting the US were against Media & Technology during the 18-month window.

It's interesting to note that no other North American country resides in the top 10 targets when considering the Media & Technology vertical. France (34.78%), Japan (22.96%), Germany (11.09%), and India (10.55%) round out the top five. Korea is an interesting outlier to this data set, with 64% of all the attacks against organizations in Korea targeting media organizations.

Application Attacks - Top Targets

TARGETED AREAS	MEDIA VERTICALS	ALL VERTICALS	GLOBAL RANK IN ALL VERTICALS
United States	636,551,596	3,416,411,545	1
France	27,995,960	80,501,396	8
Japan	25,417,099	110,691,972	6
Germany	16,896,288	152,341,265	3
India	15,116,167	143,323,371	4
Netherlands	12,968,664	52,918,175	11
Korea	11,007,413	17,307,359	18
Australia	10,837,898	61,597,371	10
United Kingdom	7,662,747	243,559,654	2
Hong Kong SAR	6,503,057	27,502,462	15

Fig. 3 – Nearly 20% of all the attacks targeting the United States were in the Media & Technology vertical

The United States is again in the top spot when considering the source countries and attacks in just the Media & Technology verticals (Figure 4). The Netherlands (31.23%) came in at a distant second.

However, the biggest surprise is Belize, which comes in at third during the reporting period. Not only is Belize the 11th-largest source of attacks overall, 68% of those attacks targeted Media & Technology. After some additional research, the high rank appears connected to compromised ISP routers and services in Q1 2019. During those months, criminals compromised customer equipment and abused services in order to host botnet command and control servers (C2). Those servers were then used to launch attacks.

The recent *Botnet Threat Report* from Spamhaus listed ISPs in Belize in the top 20 for botnet C2 hosting, compromised servers, and compromised websites. The dates covered by the Spamhaus report matched the spikes in malicious traffic observed by Akamai in Belize, which is what supports our conclusion.

Application Attacks - Top Sources

SOURCE AREA	MEDIA VERTICALS	ALL VERTICALS	GLOBAL RANK IN ALL VERTICALS
United States	177,678,990	1,041,639,431	1
Netherlands	90,602,359	290,096,974	3
Belize	71,054,852	103,372,849	11
Russia	54,058,380	822,468,109	2
China	51,751,691	240,602,133	4
India	40,352,673	173,637,873	7
Germany	28,651,918	147,644,005	8
Ireland	28,172,199	82,245,577	13
Ukraine	19,804,493	181,211,429	6
France	16,400,882	128,396,046	9

Fig. 4 – Due to an increase of bot-related activity in Belize, the country jumped to third on the source list, and 11th overall, when it comes to web attacks

Credential Stuffing by the Numbers
January 2018 – June 2019

Total Malicious Login Attempts: 61,192,394,742

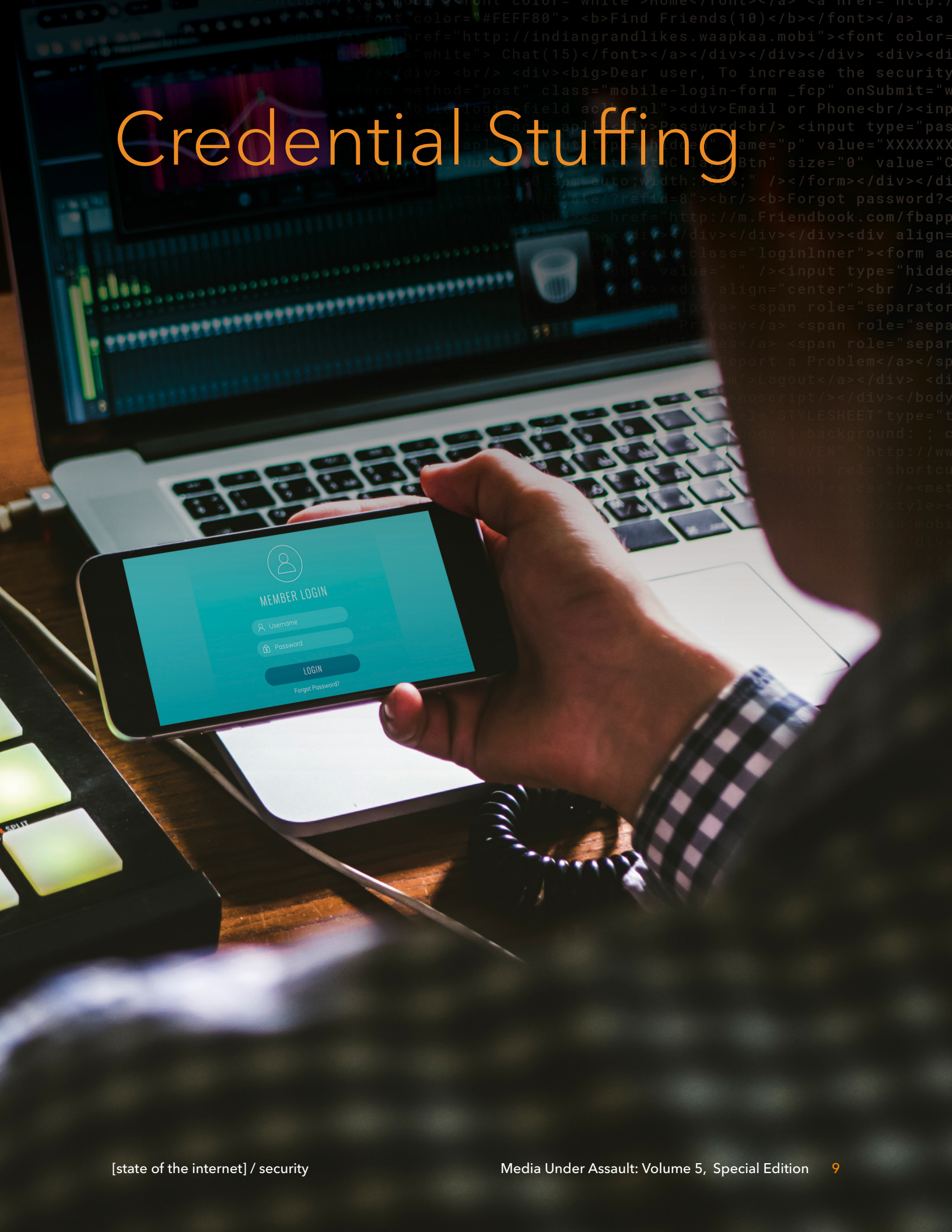
- *Video Media: 13,760,213,425*
- *High Tech: 7,533,980,169*
- *Entertainment: 77,292,308*

Average Malicious Logins Per Unique Host:

- *SQL Injection (SQLi): 69.7%*
- *Local File Inclusion (LFI): 21.6%*
- *Cross-Site Scripting (XSS): 3.5%*

Media & Technology account for nearly 35% of all malicious logins

Credential Stuffing



Credential abuse, or credential stuffing as it is commonly known, is a type of attack that has gotten a lot of attention lately. The reason for the attention isn't because credential stuffing is new, but because the volume of attacks in this area has risen exponentially over the last few years.

Akamai has covered credential stuffing extensively this year and, for this report, we look at how these attacks impact Media & Technology.

Background

Credential stuffing works by taking a list of usernames and passwords, which can be freely shared, sold, or traded, and attempting each combination against a target's authentication platform. More often than not, the criminals target authentication APIs, but there are some that will target login forms directly. While most combination lists are freely downloaded, other lists, such as those geared toward a particular service or geography, can sell for about $5 for 50,000 usernames and passwords.

Fig. 5 – The STORM AIO software is easy to use and free, making it a popular choice for criminals conducting credential stuffing attacks

Almost completely automated, credential stuffing attacks are driven by All-in-One (AIO) applications with names such as SNIPR or STORM. Some AIO programs are free, while others require an upfront registration fee. One of the more popular programs, SNIPR, will retail for about $20, while STORM (shown in Figure 5) is freely available online.

AIO platforms like STORM and SNIPR operate using configuration files, which enable them to target various services (such as those in Media & Technology) without much concern for rate limits or other security restrictions. The configuration files are sometimes just given away free of charge, but other more customized configurations can sell for more than $50.

These applications are developed to mimic the actions of a normal user, so defending against them requires planning and the ability to quickly identify attacks. Most AIOs come with pre-built evasion techniques for many default defensive measures, so custom solutions geared toward the business's needs are mandatory. Moreover, any defensive plan has to include awareness training for end users, since criminals take advantage of shared account access and recycled or weak and easily guessed passwords.

Once the criminals have their configuration files and combination lists loaded into the AIO, they will thread connections via proxy to the target's website and attempt to log in. Successful entries are recorded, and the access to the account is either traded or sold. Compromised accounts in the Media & Technology verticals can sell for as little as $5, but some accounts can sell for as much as $15 depending on what they are. Broadcasting and content development are key targets for credential stuffing, and accounts in that space sell for a premium.

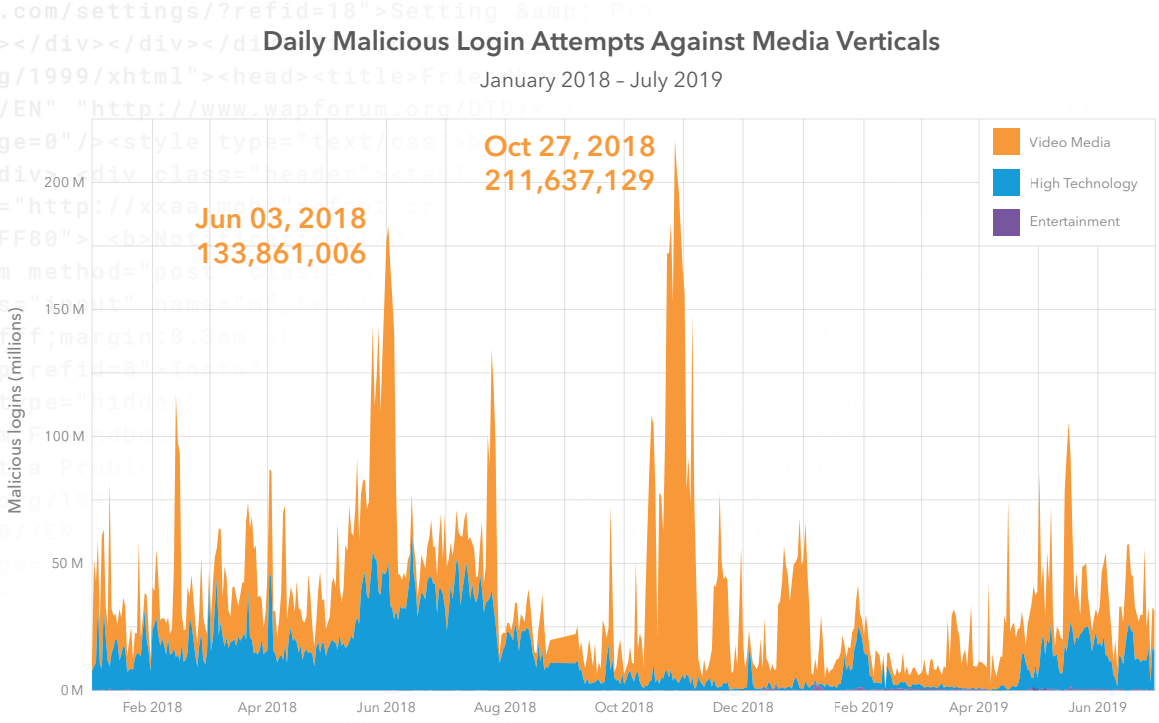


Fig. 6 – Two attacks in 2018 accounted for more than 340 million credential stuffing attempts

In Figure 6, using the same 18-month time frame, you can clearly see the overwhelming majority of attacks are focused on video media and high tech. The entertainment vertical is present, but barely noticeable in the chart when compared with the other two industries. As mentioned, accounts in these two areas are prime targets and can be resold quickly for a profit.

We've singled out two months, June 2018 and October 2018, as both were interesting from an attack standpoint.

In June, attackers targeted seven different organizations, and 14 unique hosts. The goal was seemingly to obtain access to data and content-rich accounts, which would later be resold. Considering the customers targeted, the criminals were looking to resell accounts in the video media sector and obtain new credentials and other data that can be resold from the high tech sector. In October, attackers hit 18 different organizations and 28 unique hosts. Once more, the goals were apparently the same.

In both instances, the top source of attacks was tracked back to Russia. This is likely due to the high-number of proxy services in that country. When considering attacks against everything in the Media & Technology verticals, Russia was followed by Canada, Brazil, Malaysia, and China. Each of those locations are known for proxy services, piracy, as well as account reselling and trading.

Average Malicious Logins by Vertical

VERTICAL	MALICIOUS LOGINS	AVERAGE MALICIOUS LOGINS PER UNIQUE TARGET
Retail	24,245,971,895	26,556,377
Video Media	13,760,213,425	151,211,137
High Technology	7,533,980,169	35,537,642
Hotel & Travel	4,860,206,037	23,941,902
Financial Services	3,900,240,393	27,466,482
Manufacturing	2,615,438,681	74,726,819
Consumer Goods	1,560,726,138	18,803,929
Social Media	1,079,139,624	37,211,711
Gaming	645,181,719	25,807,269
Other Digital Media	331,455,583	5,815,010
Consumer Services	311,243,282	14,147,422
Automotive	97,816,354	13,973,765
Media & Entertainment	77,292,308	4,294,017
Public Sector	75,116,539	4,694,784
Business Services	35,908,816	1,158,349

Fig. 7 – The average attacks per host in video media coming out far ahead of any other vertical

In Figure 7, we examine the number of malicious logins per unique victim. Based on the data, we can see that while retail is the top vertical, video media and high tech dominate, meaning they are getting hit harder on average. In fact, the rate of attacks per host against video media is close to five times the rate of attacks against the others when considering all verticals.

Another thing that stands out in Figure 6 is the consistent level of attacks. In the summer months, when new releases come out on various platforms, the attacks spike – it's the same with the months in the fall too – but all year long, there are millions and millions of credential stuffing attacks happening all across the web. Clearly, this problem isn't going to phase out; it's here to stay.

Top targets for credential stuffing attacks during the 18-month window, as noted in Figure 8, were the United States, India, Canada, Singapore, and Australia. The companies tied to these locations include some of the world's top brands in the Media & Technology space. The accounts and data the companies in these spaces maintain are valuable, and can be easily traded or sold for a profit. The criminals are chasing the money.

The top sources for credential stuffing attacks included the United States, Russia, Canada, Germany, and India. The reason for Russia and India landing so high on the list is proxy services that make hiding the true origin of attacks easy. Akamai only sees the last system used in an attack and does no further attribution.

Malicious Login Attempts - Top Targets

TARGETED AREA	MEDIA VERTICALS	ALL VERTICALS	GLOBAL RANK IN ALL VERTICALS
United States	17,554,816,847	46,897,833,276	1
India	2,455,628,895	3,702,332,247	3
Canada	1,156,597,318	1,487,337,095	4
Singapore	47,008,228	55,117,432	18
Australia	42,773,334	198,379,421	9
Czech Republic	36,139,380	36,139,380	19
Netherlands	15,614,129	15,770,397	22
China	15,105,040	4,58,443,883	2
Germany	12,683,512	1,280,565,528	5
Italy	7,532,004	106,015,785	14

Fig. 8 – The United States and India were top targets for credential stuffing attacks

Just because an attacker's IP address is in Russia, it doesn't mean the attacker is there too. Criminals conducting credential stuffing attacks rely on proxy settings not only to evade security defenses, but to also offer a layer of masking as to their identity.

During our research, we found one proxy service offering access with prices ranging from $30 per week to $200 per week. The cost depends on the proxy server's location and account limitations. The cheapest option, which is located in Australia, has a limit of 50 concurrent connections (threads), and boasted more than 200 servers available for connections (called a pool). China offered one of the more expensive options: a thread limit of 500 and more than 20,000 servers in the pool.

Malicious Login Attempts - Top Sources

SOURCE AREA	MEDIA VERTICALS	ALL VERTICALS	GLOBAL RANK IN ALL VERTICALS
United States	5,978,803,240	19,946,636,280	1
Russia	2,811,700,327	5,080,433,712	2
Canada	1,767,056,222	2,423,776,410	4
Germany	883,080,860	1,727,582,602	8
India	790,854,971	2,167,920,536	5
Vietnam	750,780,050	1,618,414,860	10
Brazil	692,183,261	2,834,964,769	3
France	518,293,553	1,358,495,125	13
Netherlands	448,213,143	1,386,280,155	12
United Kingdom	424,914,180	1,140,233,591	14

Fig. 9 – The United States and Russia were still major sources of credential stuffing attacks online, during the 18-month reporting period

Conclusion

It can't be overstated: Web attacks and credential stuffing are real, long-term threats. They are both part of a larger criminal economy, which is fueled by their symbiotic relationship. When it comes to developing combination lists for credential stuffing, one of the most common methods is to download the data from a freshly compromised database. As such, an SQLi attack can shift into a credential stuffing attack in a matter of moments. But dealing with these threats isn't easy. It requires organizations to partner with their security vendors and customers to address the root causes of these attacks.

Methodologies

Web Attacks

The Akamai Intelligent Edge Platform is a network of more than 240,000 servers in thousands of networks around the world. The Kona WAF is used to protect this traffic, and the information about the attacks is fed into an internal tool called Cloud Security Intelligence (CSI). This data, measured in petabytes per month, is used to research attacks, understand trends, and feed additional intelligence into Akamai's solutions. This data represents millions of daily application layer alerts, but these alerts do not indicate a successful compromise.

The plots and tables provided in this section were limited to records between January 2018 and June 2019.

Credential Abuse

The data for this section was also drawn from the CSI repository. Credential abuse attempts were identified as unsuccessful login attempts for accounts using an email address as a username. In order 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 abuse from known botnets and tools. A well-configured botnet can avoid volumetric detection by distributing its traffic among many targets, using a large number of systems in its scan, or spreading out the traffic over time, just to name a few.

These records were collected between January 2018 and June 2019.

Credits

State of the Internet / Security Contributors

Omri Hering
Data Analyst Senior –
Credential Abuse

Lydia LaSeur
Data Scientist –
Credential Abuse, Web Attacks

Editorial Staff

Martin McKeay
Editorial Director

Amanda Fakhreddine
Sr. Technical Writer, Managing Editor

Steve Ragan
Sr. 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 at akamai.com/soti

More Akamai Threat Research

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

Akamai

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 09/19.


Akamai
Intelligent Security
Starts at the Edge