

Web Attacks and Gaming Abuse

Letter From the Editor

Whether we're discussing security in the physical **or** digital world, criminals **go** where the money is. This is just as true for businesses; however, criminals are looking for less wholesome ways to make that money. Lack of competition often **makes** the edge cases and **other** untapped opportunities **the** easiest path to riches.

It's our job, as security **professionals**, to understand and identify these edge cases as quickly as possible in order to **prevent** attacks and fraud before **they** affect the business. We're always participating in **a** cat-and-mouse **game**, doing our best to catch up with the new trends that **are** being exploited.

We've been looking at credential abuse and related attacks since summer 2018, and **we** think this is one of the key areas the **attackers** are increasingly **transitioning** into. The vast majority of users and businesses are aware that login attempts are an issue, since credential abuse-related attacks **have** been around in some **form** since the first days of the Internet. We have **found** that many organizations are simply **not** aware of either the scope or the complexity of the problem, especially as attackers move in and focus their resources on escaping detection.

We chose to focus on the **gaming** industry, because it has spawned **one** of the most active and rapidly evolving underground economies fueled by credential abuse. It's important to note that there are also other styles of attacks, from phishing to malware aimed directly at gaming accounts. These accounts can have significant value, so it's **unlikely** we'll see a decrease in attacks soon.

We have heard feedback that some **organizations** think they're **not** targets of credential abuse, and neither are similar businesses. While it's true that some verticals are less targeted than others, each time we **look** at the data, we can clearly see that **no** industry is **truly** immune. Some businesses might be more likely to be part of a random spray of login attempts, but **every** organization with a page that's asking for a username and password is going to see attempts to compromise this process.

Attackers see credential abuse as a low-risk **venture** with potential for a high payout, at least for now. These types of attacks are more **likely** to increase for the foreseeable future. As with many other types of attacks, the **important** thing is for you, the reader, to be aware that the attacks are happening so you can find ways to **defend** your enterprise from them.



Table of Contents

01 | Overview

02 | Guest Author: Monique Bonner

05 | Akamai Research

06 | The Big Picture of Web Attacks

10 | Credential Abuse and Gaming

19 | Looking Forward

21 | Appendix

22 | Methodologies

23 | Supplemental Data

26 | Credits

Overview

This installment of State of the Internet / Security examines credential stuffing and web application attack trends over the last 17 months, with a focus on the gaming industry. One reason gaming is so lucrative is the trend of adding easily commoditized items for gamers to consume, such as cosmetic enhancements, special weapons, or other related items. Gamers are also a niche demographic known for spending money, so their financial status makes them tempting targets. We began collecting credential abuse data at the beginning of November 2017 and chose to use the same period with our application attack data to make direct comparisons between plots easier for readers.

Credential abuse is nothing new for the gaming industry, where virtually any gamer can share an anecdote about an account that has been taken over due to credential stuffing attacks. Over the

17-month period, Akamai witnessed 55 billion credential stuffing attacks – showing that no industry is immune to them. The gaming industry alone saw 12 billion of those attacks, marking it as a growing target for criminals looking to make a quick buck. For now, attackers see credential abuse as a low-risk venture with potential for a high payout, and these types of attacks are likely to increase for the foreseeable future.

We didn't forget about web attack data. When we look at web attack data historically observed by Akamai, 89.9% of the attacks fall into one of two categories: SQL Injections (SQLi) and Local File Inclusion (LFI) attacks. The data over this same 17-month period shows that SQLi have continued to grow at an alarming rate as an attack vector. While we can see that the attacks escalated with the holiday shopping season, they never returned to their previous levels.

TL;DR

- Akamai observed 55 billion credential stuffing attacks over 17 months; 12 billion of those attacks targeted the gaming industry
- United States is still the top source for credential stuffing attacks, followed by Russia; however, when we look at the source countries for credential stuffing attacks against the gaming industry only, Russia takes the top spot
- In our 17-month data set, SQL Injections now represent nearly two-thirds of all web application attacks

Three Lessons Learned as a Security CMO

Guest Author

Monique Bonner

Executive Vice President & Chief Marketing Officer at Akamai

It's been three years since I became the Chief Marketing Officer (CMO) at Akamai, after having been at a tech hardware vendor for more than 15 years. While I thought I knew a bit about security – the prior company had some SaaS security offerings – I realize now that I still had a lot to learn about the industry. Security is a very different space, with unique motivations and dynamics.

We've been on a journey at Akamai, growing our security portfolio and setting our sights on becoming a \$1B security business by 2020. This has required significant changes to our marketing, our products, and how we communicate with our customers. We've evolved a lot over the past three years, and I think it's worth sharing our three biggest lessons learned.

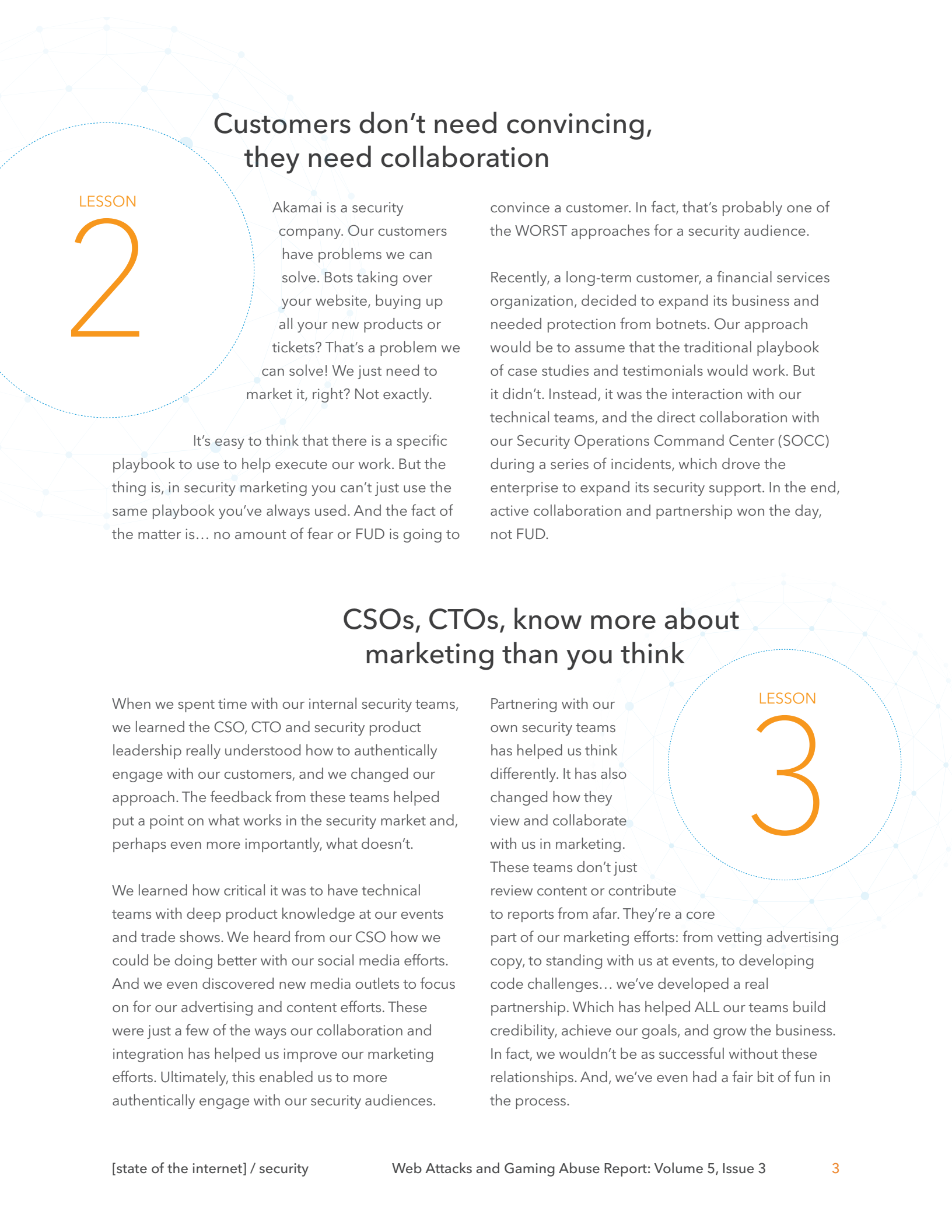
LESSON

1

Security is a passion, not a product

I used to believe our security product and research teams were like any other in the tech space: Innovation focused, improvement oriented, all while keeping an eye on costs and ROI. And what I've learned is that, while those things are certainly part of what our security teams do, it's not what drives them. It's not what keeps them curious. It's not what keeps them awake for 24 hours straight to help defend a customers' website during a DDoS attack.

What drives security professionals is passion. Passion and unbridled energy for doing what is right for the customers that entrust them to protect their businesses. And it even goes beyond this passion for serving customers. What also makes them unique is their incredible dedication to the security community at large. I think this commitment to the industry, this service to something greater than themselves is what's unique to security. The work. It matters.



Customers don't need convincing, they need collaboration

LESSON

2

Akamai is a security company. Our customers have problems we can solve. Bots taking over your website, buying up all your new products or tickets? That's a problem we can solve! We just need to market it, right? Not exactly.

It's easy to think that there is a specific playbook to use to help execute our work. But the thing is, in security marketing you can't just use the same playbook you've always used. And the fact of the matter is... no amount of fear or FUD is going to

convince a customer. In fact, that's probably one of the WORST approaches for a security audience.

Recently, a long-term customer, a financial services organization, decided to expand its business and needed protection from botnets. Our approach would be to assume that the traditional playbook of case studies and testimonials would work. But it didn't. Instead, it was the interaction with our technical teams, and the direct collaboration with our Security Operations Command Center (SOCC) during a series of incidents, which drove the enterprise to expand its security support. In the end, active collaboration and partnership won the day, not FUD.

CSOs, CTOs, know more about marketing than you think

When we spent time with our internal security teams, we learned the CSO, CTO and security product leadership really understood how to authentically engage with our customers, and we changed our approach. The feedback from these teams helped put a point on what works in the security market and, perhaps even more importantly, what doesn't.

We learned how critical it was to have technical teams with deep product knowledge at our events and trade shows. We heard from our CSO how we could be doing better with our social media efforts. And we even discovered new media outlets to focus on for our advertising and content efforts. These were just a few of the ways our collaboration and integration has helped us improve our marketing efforts. Ultimately, this enabled us to more authentically engage with our security audiences.

Partnering with our own security teams has helped us think differently. It has also changed how they view and collaborate with us in marketing. These teams don't just review content or contribute to reports from afar. They're a core part of our marketing efforts: from vetting advertising copy, to standing with us at events, to developing code challenges... we've developed a real partnership. Which has helped ALL our teams build credibility, achieve our goals, and grow the business. In fact, we wouldn't be as successful without these relationships. And, we've even had a fair bit of fun in the process.

LESSON

3



Monique Bonner is a global marketing executive who is passionate about building brands, customer-centric marketing, driving strategic transformations, and motivating teams to exceptional performance. Ms. Bonner is Executive Vice President & Chief Marketing Officer at Akamai, where she is dually focused on driving growth and operational excellence. She leads Akamai's marketing efforts globally including brand, communications, field and digital marketing, as well as the company's sales and services training and enablement programs.

Prior to Akamai, Ms. Bonner spent 16 years at Dell Technologies in a variety of roles including sales, operations, strategy, and marketing. She led the company's first global brand strategy work and designed and developed our digital innovation roadmap for marketing. She was also based in Europe for seven years.

Ms. Bonner serves on the Boards of Directors for 8x8, the Akamai Foundation, and the Lake Champlain Maritime Museum. She earned a Bachelor of Arts from Middlebury College and Master of Business from the University of Michigan. On behalf of the hard work and efforts of the entire Marketing team at Akamai she was honored to accept the 2018 Massachusetts Technology Leadership Council CMO of the Year. When she's not championing change, she can be often be found refinishing furniture, skiing, or cheering on the New England Patriots with her two sons and husband.

05 | Akamai Research



The Big Picture of Web Attacks

We'd like to say that web application attacks are a diverse ecosystem, but that's not true once we look at the data. The vast majority these attacks fall into just two categories, SQL injection (SQLi) and Local File Inclusion (LFI), which account for 89.8% of the application layer attacks, as shown in Figure 1. Cross-site scripting (XSS), PHP Injection (PHPi), and Remote File Inclusion (RFI) account for another 8.4%, with all other types of attacks accounting for only 1.8% of the alerts seen by Akamai's Kona Web Application Firewall (WAF). It does suggest that the security industry should be paying more attention to fighting SQLi, which has been a known issue for more than a decade.

In this section of the State of the Internet / Security report, we're looking at a 17-month period across our graphs and tables in order to keep them in line with the data we've collected on credential abuse. While a 12- or 24-month period might be more common, we wanted to examine a unified timeframe, using the most recent data available to us for this report. In the future, as we collect additional credential abuse data, we plan on standardizing on a rolling two-year time frame. Akamai saw slightly fewer than 4 billion (3.993 billion) WAF alerts in this period, and 1.2 billion alerts in the first quarter of 2019 alone.

Top Web Attack Vectors November 2017 - March 2019

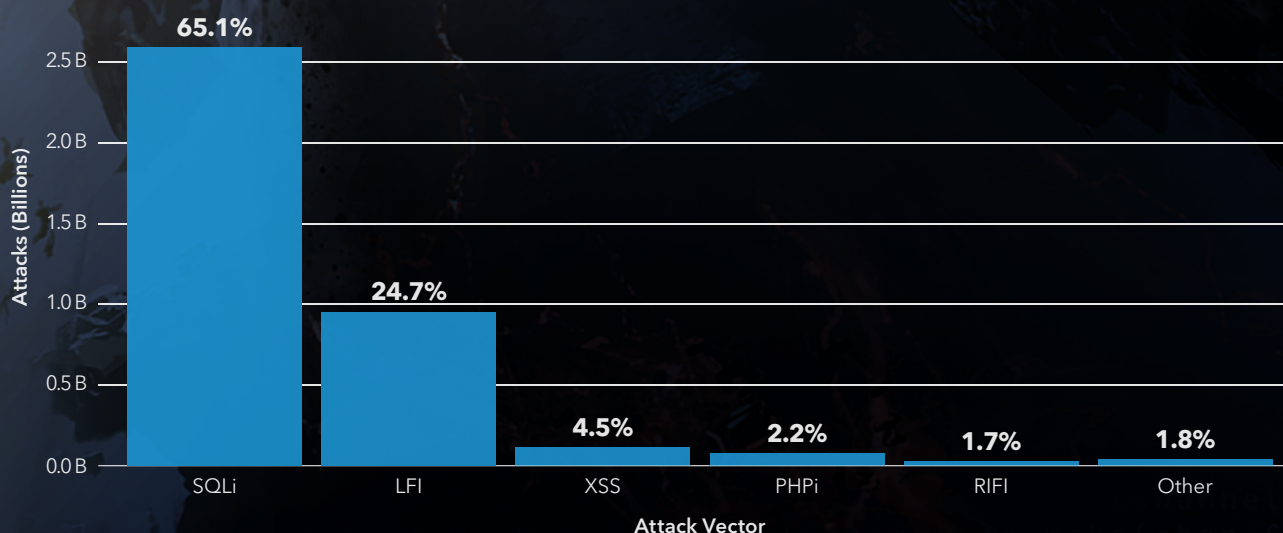


Fig. 1 - SQLi now represents nearly two-thirds of all web application attacks

Daily Web Attacks by Vector November 2017 – March 2019

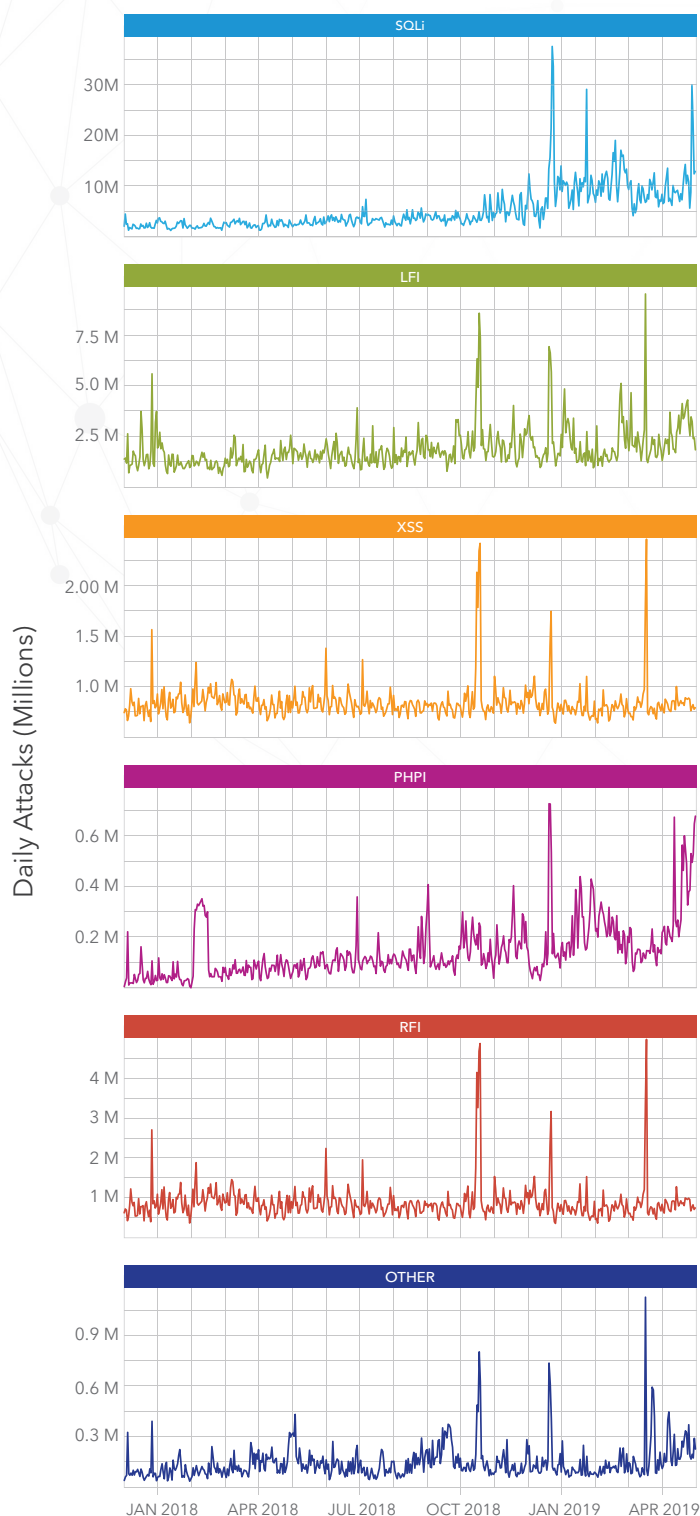


Fig. 2 – Spikes across multiple attack vectors often represent a single botnet or attacker

SQL Injection Growth

The growth of SQLi as an attack vector over the last two years should concern website owners. In the first quarter of 2017, SQLi accounted for 44% of application layer attacks. This actually represented a rather large drop from the previous baseline, which was historically slightly over 50%. As shown in Figure 2, while every application attack vector is stable or growing, none are growing as quickly as SQLi. As you read this figure, please keep in mind that each vector uses a scale determined by the number of attacks seen by Akamai. If not for the difference in scale, only LFI would be visible in comparison to the SQLi attacks in our plots.

In late November 2018, our customers experienced a spike of SQLi alerts (more than 35 million attacks), which also carried over to multiple other types of web application attacks. The timing was most likely tied to the start of the holiday shopping season. However, it's also important to note that there's been a continuing elevated trend since that time. Database attacks are appealing to criminals because they work often enough to be profitable.

The United States has long been the main target for application layer attacks, experiencing 2.7 billion attacks over 17 months. It's unlikely that this key position will be challenged in the foreseeable future, as the United States has held this dubious honor for as long as we've been tracking web application attacks. The other target countries listed in Figure 3 are also familiar members of the list, though Australia and Italy have not been consistently in the top spots in the past.

When we look at where application attacks originate, the traffic is much more evenly distributed around the globe. The United States maintains an unhealthy lead as the biggest source of these attacks, but Russia, the Netherlands, and China all show significant amounts of alerts originating from their countries. It should be noted that “source country” designates where the traffic is coming from and does not necessarily indicate where the actual attacker is located. Smart attackers take significant steps to hide where they’re coming from, and are also unlikely to show up in Top 10 lists, as their attack patterns tend to be much quieter.

Top 10 Target Countries

November 2017 – March 2019

COUNTRY	TOTAL ATTACKS	GLOBAL RANK
United States	2,666,156,401	01
United Kingdom	210,109,563	02
Germany	135,061,575	03
Brazil	118,418,554	04
India	113,280,600	05
Japan	95,550,352	06
Canada	84,443,615	07
Australia	54,187,181	08
Italy	47,784,870	09
Netherlands	47,390,611	10

Top 10 Source Countries - All Verticals

November 2017 – March 2019

COUNTRY	TOTAL ATTACKS	GLOBAL RANK
United States	967,577,579	01
Russia	608,655,963	02
Netherlands	280,775,553	03
China	218,015,784	04
Brazil	155,603,585	05
Ukraine	154,887,375	06
India	142,621,086	07
France	121,691,941	08
Germany	113,233,187	09
United Kingdom	102,531,816	10

Fig. 3 – Nearly 67% of application layer attacks target organizations based in the United States

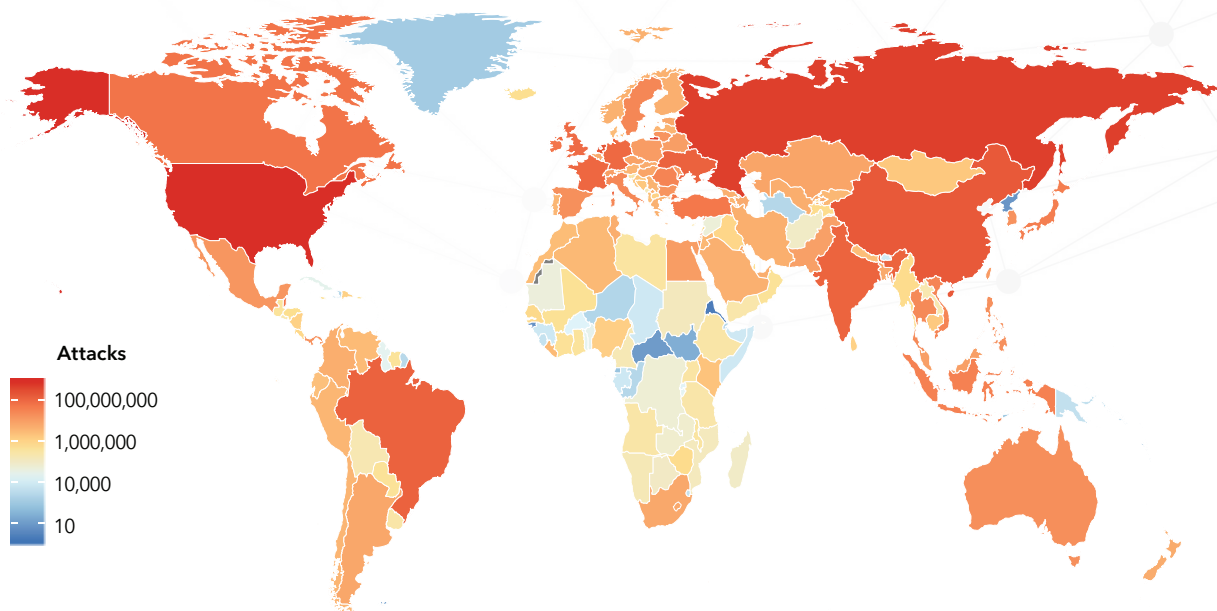


Fig. 4 – Russia has become firmly entrenched as the second largest source of application attacks

As a precursor to our research on the gaming industry, we focused on the source of application attacks against these sites. The rankings in Figure 5 are generally similar to the overall trends we see, with the exception of the United Kingdom making a significant rise in the charts, and Ireland making its first appearance in the report. It should be noted that most of the attacks in our report are against the websites of game companies, not the applications that run the games. Most games are being driven by APIs and custom applications that do not lend themselves to standard WAF rules.

Top 10 Source Countries - Gaming

COUNTRY	TOTAL ATTACKS	GLOBAL RANK
United States	43,411,879	01
Russia	15,114,894	02
China	13,062,873	04
Netherlands	11,187,344	03
United Kingdom	7,871,201	10
France	7,760,629	08
India	5,859,202	07
Ukraine	5,339,086	06
Ireland	5,209,188	12
Germany	5,016,555	09

Web Application Attack Sources - Gaming
November 2017 - March 2019

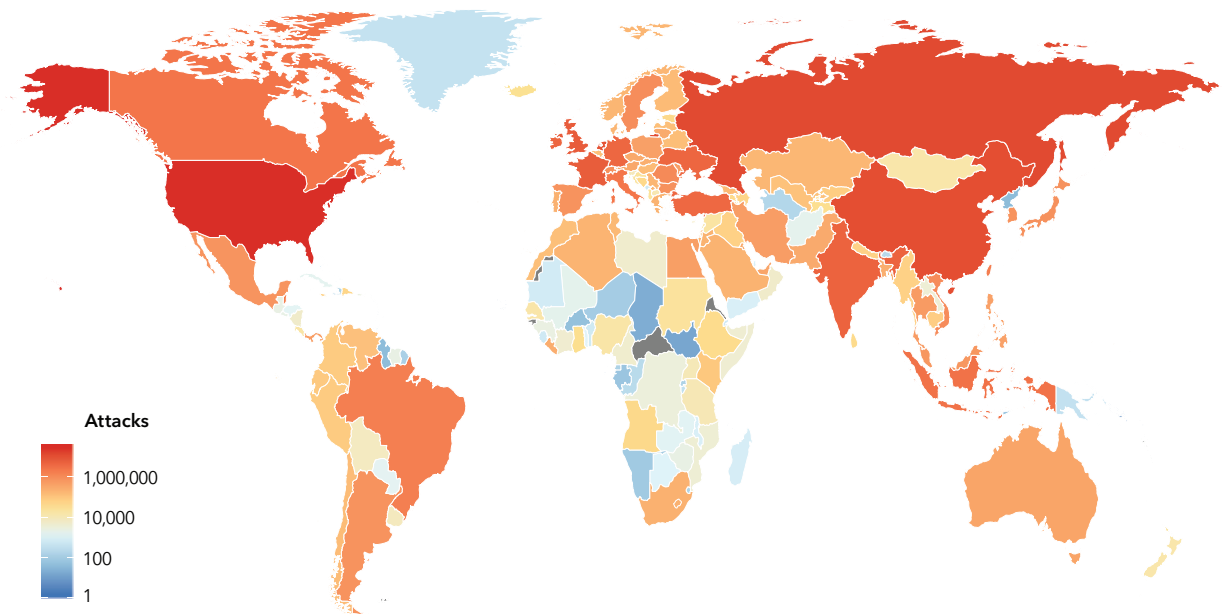
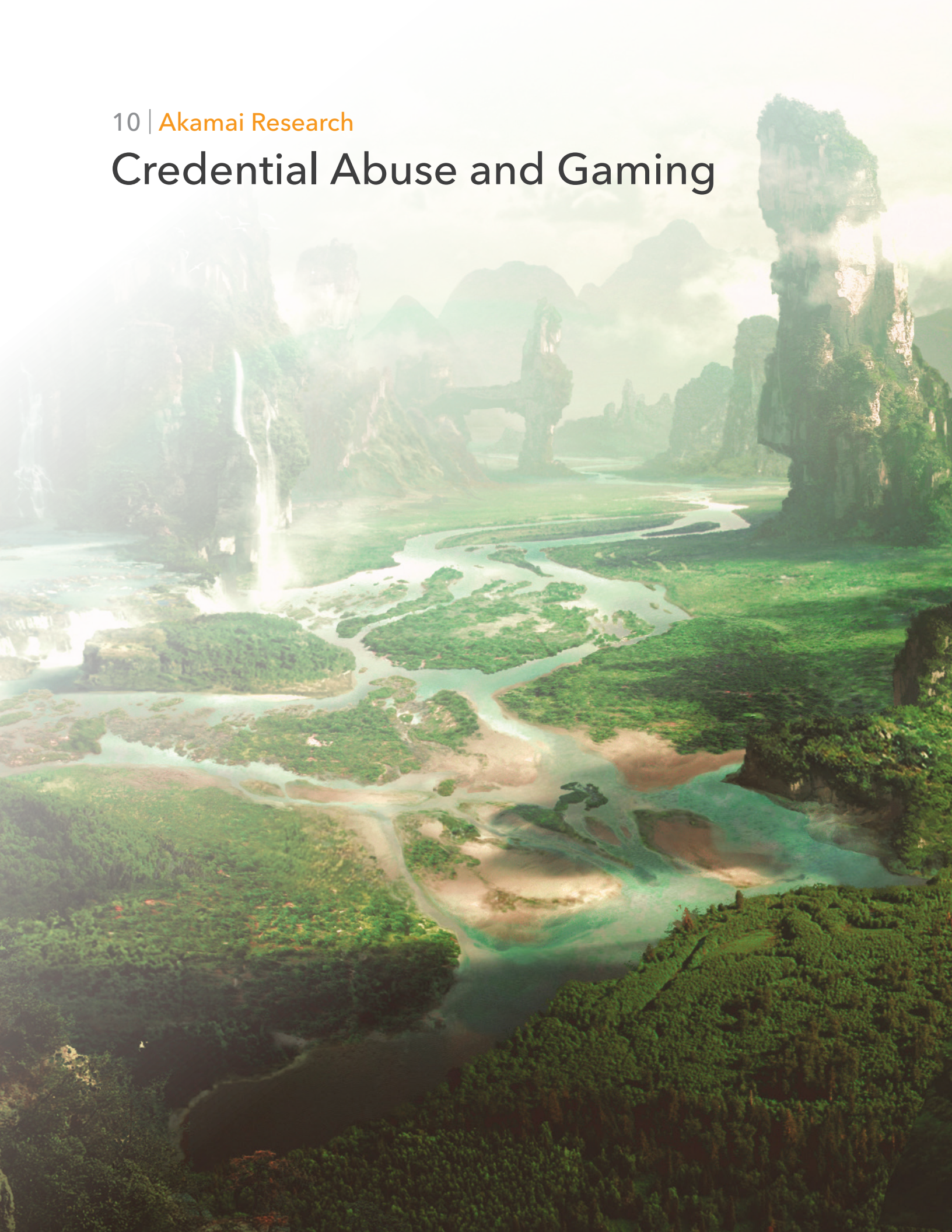


Fig. 5 - Attackers in Brazil don't appear to consider gaming to be a major target for their efforts

Credential Abuse and Gaming



[illegible]

“Criminal
exist so
login cr

While some organizations have taken advantage of expanded authentication options – including multi-factor authentication (MFA), open authorization (OAuth), and hardware-based authenticator tokens – not everyone has jumped on the bandwagon. Moreover, unless multi-factor options are required, it is left up to the user to enable and use them, creating a classic trade-off between security and usability. Criminals are targeting these gaps and compromising dozens, if not hundreds, of accounts each day.

“Criminals are essentially creating mini-botnets that exist solely to focus on validating massive lists of login credentials.”





Background

We've covered credential stuffing in two previous State of the Internet / Security reports this year, focusing on the retail sector and the media and entertainment industry.

As mentioned in the Letter From the Editor, criminals are going to follow the money. Retail targets are selected due to the large and influential secondary market, where limited run or special edition goods are re-sold. This is also why the media and entertainment sectors are so popular. Streaming media services are packaged together and sold once the accounts are compromised. Often those accounts are warrantied, meaning if they stop working, the seller will replace the account at no cost.

In our State of the Internet / Security: Retail, we reported more than 115 million credential stuffing attacks per day between May and December 2018. During this seven-month window, the retail sector received the bulk of those attacks. Direct commerce and department stores were the top two subsectors

(1.4 billion respectively), followed by office supply stores (1.3 billion).

Expanding the attack window to cover all of 2018, our State of the Internet / Security: Special Media Edition noted that credential stuffing attacks against video, media, and entertainment sectors jumped from 133 million to more than 200 million in 2018.

In fact, 2018 was a busy year overall for credential stuffing. On three different days last year, one in June and two in October, credential stuffing attacks spiked considerably, with the attacks in October nearly hitting 300 million.

When it comes to credential stuffing, no industry is immune. Each vertical has something to offer an enterprising criminal looking to monetize access and information. In this report, we're expanding the data set further to 17 months and taking a look at one of the fastest growing segments for credential stuffing – gaming.

A Growing Market

As an industry, gaming is a large, unregulated market of in-game purchases and rare items. Gaming sites saw 12 billion attacks out of the total 55 billion in our data. Accordingly, the gaming marketplace is quickly becoming a lucrative target for criminals looking to make a quick buck.

Part of the reason why gaming is so lucrative is the trend of adding easily commoditized items for gamers to consume, such as cosmetic enhancements, special weapons, or other related items. Furthermore, gamers are a niche demographic known for spending money, so their financial status is also a tempting target.

For example, criminals target popular games like Fortnite and Counter-Strike: Global Offensive (CS:GO), looking for valid accounts and unique skins. Once a player's account is successfully compromised, it can then be traded or sold.

Most compromised accounts sold in gaming marketplaces are used to avoid bans, but others are purchased for the novelty of playing with a rare skin or unique item. Sometimes, the items in the compromised account are traded away or later sold.

If the hijacked profiles are connected to a valid credit card or PayPal account, they're considered more valuable, since the criminal can purchase additional items (e.g., account upgrades, game currency, or other loot) and then trade or sell the account at a markup.

According to a BBC report published in December 2018, some people – including children as young as 14 years old – are making thousands of dollars per week selling or trading compromised gaming accounts. Once a criminal obtains access, any money made from the attack is pure profit.

Credential Abuse by Day

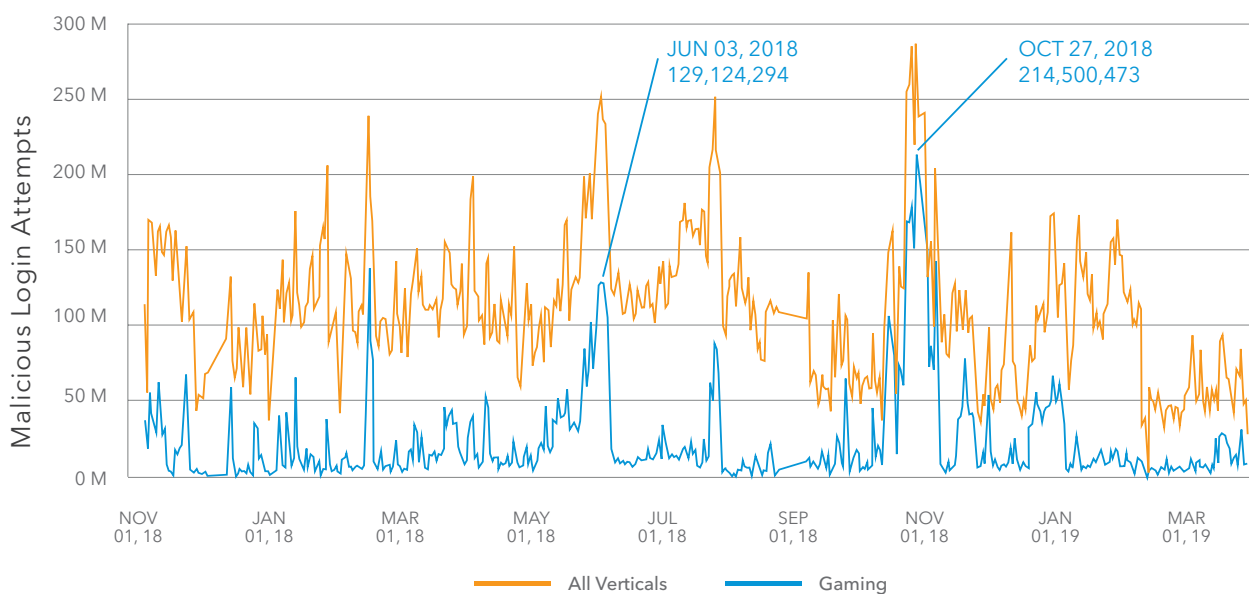


Fig. 6 - Credential stuffing attacks by day during the reporting period

Development Lifecycles

Credential stuffing attacks target login forms, APIs, or both, depending on the organization. The tools used during these attacks are advanced and regularly maintained.

Using a regular development lifecycle, AIOs such as SNIPR – an entry-level AIO that retails for approximately \$20 USD – have regular releases that address bugs, security issues, UI improvements, and functionality.

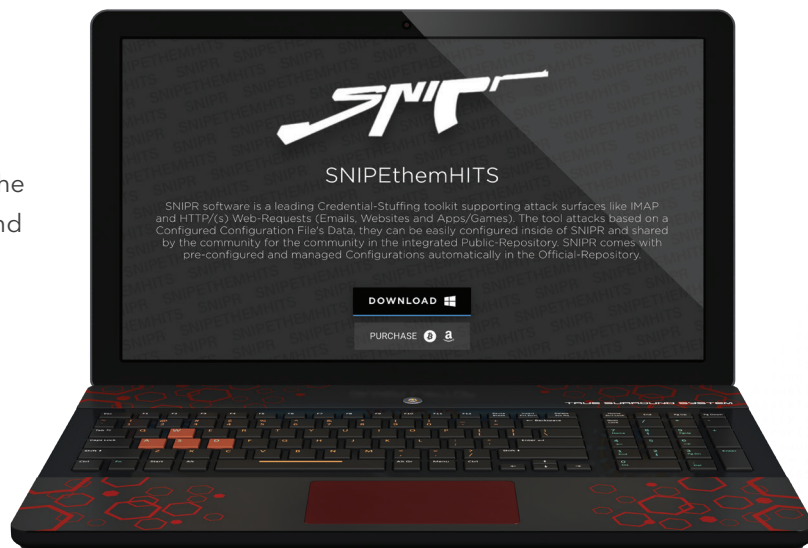


Fig. 7 – A screenshot of the SNIPR product page

Combination Lists

In February 2018, Epic Games warned gamers about the rise of credential stuffing attacks against Fortnite accounts, stating that a number of accounts had been compromised due to “well-known hacking techniques.”

Specifically, Epic urged Fortnite players to avoid password reuse across multiple websites, warning that it was a “dangerous practice” to be avoided. In addition, Epic’s warning also discussed phishing and other related scams. In fact, password reuse is a primary reason why credential stuffing attacks are so successful. After reuse, the second most common reason such attacks succeed is easily guessed passwords.

Credential stuffing attacks start with a combination list, or a collection of usernames and passwords that can be tested against a number of platforms. The attacker will load the lists into an AIO application, and after tuning a configuration file, run the passwords against the organization one right after another until they get a positive result.

The combination lists themselves are sourced from data breach sets published publicly, or they can be purchased from darknet sellers who deal in bulk. Those selling combination lists often tailor them to the customers’ needs. One darknet seller recently offered a split deal, which included one of the following: A batch of 5 billion random email addresses and passwords, or a customized list of 50,000 where the purchaser can dictate the format (email:pass or user:pass), provider, location, and more. Either option costs a total of \$5.20.

Some sellers are more daring with their list creation, turning to actual hacking in order to get a fresh list of credentials. Earlier this year, a YouTube video viewed by researchers at Akamai promoted the functionality of an AIO application and demonstrated how to generate combination lists by performing SQLi attacks on vulnerable websites.

Another method by which combination lists are created is via phishing. Phishing attacks targeting popular games generate instant results. The compromised credentials can then be tested against other services, potentially turning a single compromised account into dozens.

In some cases, as seen in Figure 8, phishing attacks against gamers will try and take advantage of various login methods. In this example, the phishing kit is looking for a Battlenet username and password, but it's also able to collect Google and Facebook credentials, too.



Fig. 8 - A phishing kit targeting Google, Facebook, and Battlenet credentials

Many gaming platforms offer the option to authenticate via Facebook or Google, which can be helpful as long as those passwords are kept safe. But again, the problem credential stuffing capitalizes on is password sharing among multiple websites. So if a Google or Facebook account's credentials are compromised, any services where they can be used are at risk as well.

Gamers also have to contend with in-game phishing, such as a request sent via private message to verify account credentials, or alleged contests where prizes need to be claimed.

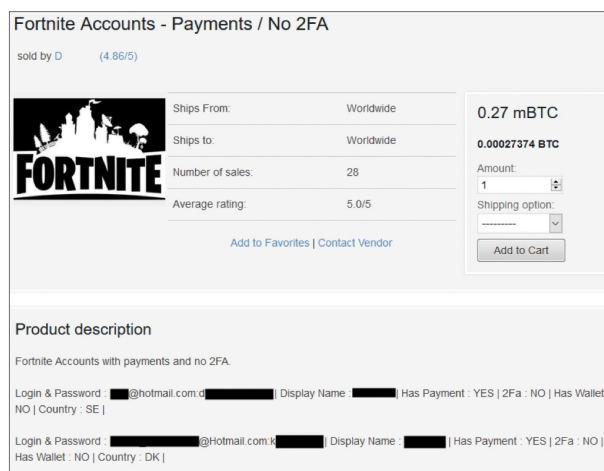


Fig. 9 – Verified Fortnite accounts with viable payment methods are sold on a darknet marketplace

The Marketplace

Once an account is compromised, it's likely going to be quickly sold or traded. Some of the transactions dealing with the sale or trading of gaming accounts take place in public view, on easily accessible websites or forums, or social services like Discord.

Other transactions happen in more exclusive areas, such as private forums or markets on the darknet. Some of the public forums exist on the premise that the account owners themselves are the people offering the gaming account for sale, but there is little verification to prove and confirm ownership. In their warning to gamers about credential stuffing, Epic Games singled out purchasing and selling accounts as a risky endeavor, urging players not to do either.

On the darknet, as shown in Figure 9, compromised accounts can sell for as little as \$1.30 USD. The price depends on volume (number of accounts purchased), account type, and what the account includes (skins, weapons, currency, etc.).

In Figure 10, we see that Fortnite is just one title out of dozens being sold or traded online. Other games, such as Minecraft, Clash of Clans, Runescape, CS:GO, NBA 2019, League of Legends, Hearthstone, DOTA 2, PlayerUnknown's Battlegrounds (PUBG), and Apex Legends, are also prized targets. Even platform accounts, such as Steam or Origin, can be acquired.

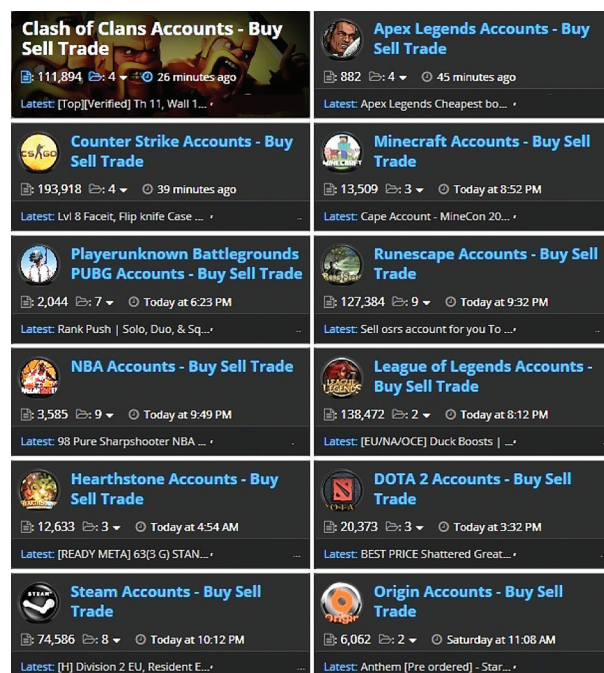


Fig. 10 – A sample of the types of games where accounts can be purchased



Location Breakdown

In Figure 11, we see that the United States is still the top source for credential stuffing attacks, followed by Russia. Since we are looking at attacks across all verticals, this isn't too surprising. However, when you drill down into gaming alone, something changes.

When we take a look at the source countries for credential stuffing attacks against the gaming industry only, Russia takes the top spot. There could be a number of reasons for this, but the most commonly accepted one is the growth of Russian-based proxy services and bot farms where accounts are compromised at scale, before being packaged up and sold on various forums and markets.

Top Source Countries - All Verticals

SOURCE COUNTRY	MALICIOUS LOGINS	GLOBAL RANK
United States	17,908,767,171	01
Russia	5,258,924,742	02
Brazil	3,042,890,769	03
Canada	2,313,304,317	04
China	2,008,074,469	05

Fig. 11 - Top credential stuffing source countries across all vertical markets

Top Source Countries - Gaming

SOURCE COUNTRY	MALICIOUS LOGINS	GLOBAL RANK*
Russia	2,674,783,777	02
Canada	1,486,753,732	04
United States	1,435,752,015	01
Vietnam	617,097,561	09
India	599,317,123	06

*All Verticals

Fig. 12 - Top gaming-focused credential stuffing source countries

“

The common factor in each successful attack is a shared password or a password that is easily guessed.”

Conclusion

No organization is immune from credential stuffing. In the gaming industry, credential stuffing is a known threat to organizations, and while they've leveraged a number of security measures to protect accounts, the common factor in each successful attack is a shared password or a password that is easily guessed.

Many gaming companies, such as Epic Games, will hunt down password dumps from data breaches or combination lists once they are leaked online. They then proactively reset the passwords of players whose accounts are discovered in the lists.

While this proactive approach is a solid layer of defense, Epic still advises players to leverage MFA, as do two other large gaming giants, Valve and Blizzard. In fact, both Valve and Blizzard have created authentication applications to help guard their customers from account theft. And yet, while you can lead a horse to water, as the saying goes, it is up to the players themselves to enable and consistently use added security layers.

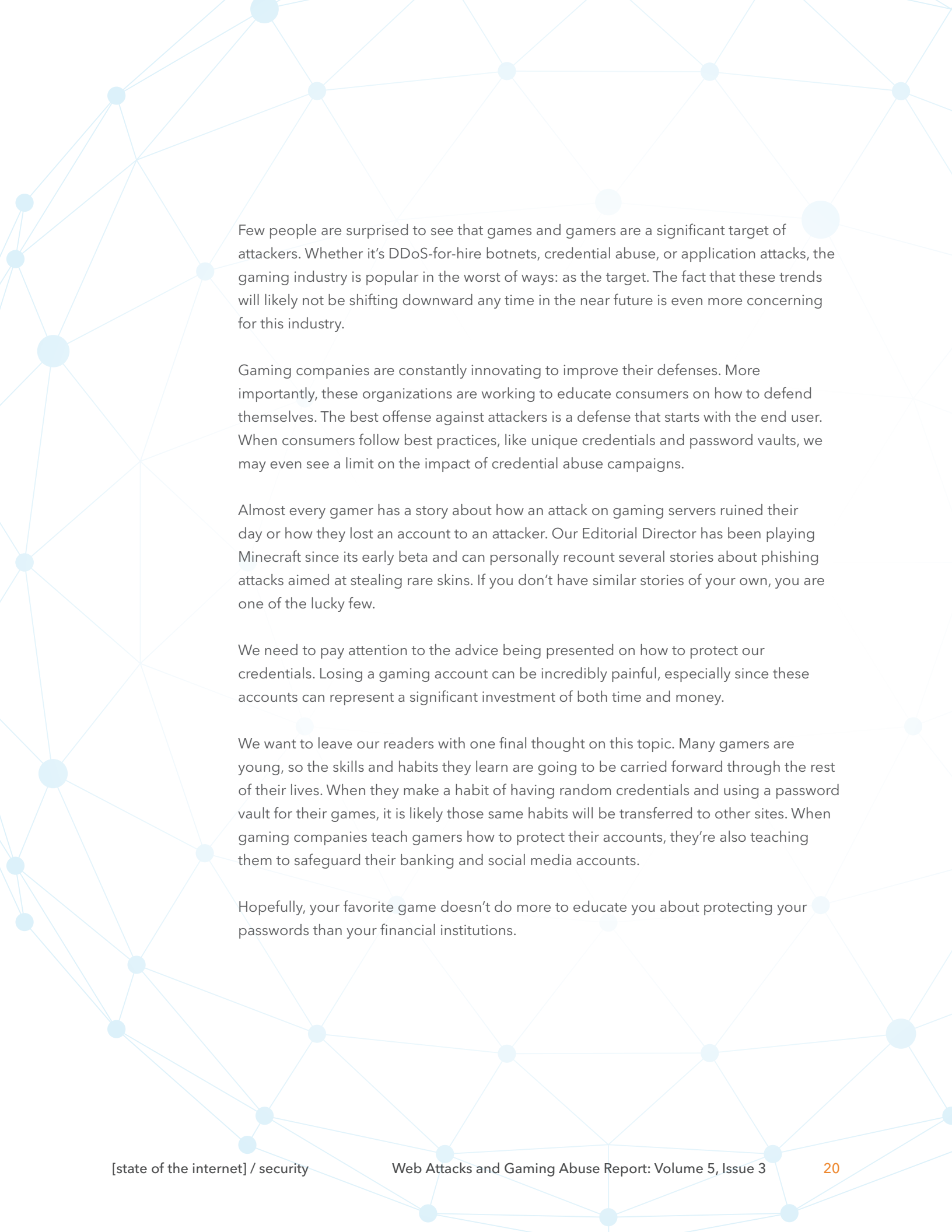
Another facet of gaming theft happens outside the gaming company's control. Criminals often target a gamer's email account or social media first, which is a key enabler for password changes and access. This is another reason why multi-factor authentication is so important.

Credential stuffing isn't going anywhere. Since it can't be stopped outright, the goal should be making the process of obtaining credentials as difficult as possible. Weak passwords and password reuse are the bane of account security; it doesn't matter if we're talking about gaming, retail, media and entertainment, or any other industry. If a password is weak or reused across multiple accounts, it will eventually be compromised.

Awareness around these facts needs to increase, as does the promotion of password managers and multi-factor authentication.

19 | Looking Forward





Few people are surprised to see that games and gamers are a significant target of attackers. Whether it's DDoS-for-hire botnets, credential abuse, or application attacks, the gaming industry is popular in the worst of ways: as the target. The fact that these trends will likely not be shifting downward any time in the near future is even more concerning for this industry.

Gaming companies are constantly innovating to improve their defenses. More importantly, these organizations are working to educate consumers on how to defend themselves. The best offense against attackers is a defense that starts with the end user. When consumers follow best practices, like unique credentials and password vaults, we may even see a limit on the impact of credential abuse campaigns.

Almost every gamer has a story about how an attack on gaming servers ruined their day or how they lost an account to an attacker. Our Editorial Director has been playing Minecraft since its early beta and can personally recount several stories about phishing attacks aimed at stealing rare skins. If you don't have similar stories of your own, you are one of the lucky few.

We need to pay attention to the advice being presented on how to protect our credentials. Losing a gaming account can be incredibly painful, especially since these accounts can represent a significant investment of both time and money.

We want to leave our readers with one final thought on this topic. Many gamers are young, so the skills and habits they learn are going to be carried forward through the rest of their lives. When they make a habit of having random credentials and using a password vault for their games, it is likely those same habits will be transferred to other sites. When gaming companies teach gamers how to protect their accounts, they're also teaching them to safeguard their banking and social media accounts.

Hopefully, your favorite game doesn't do more to educate you about protecting your passwords than your financial institutions.

21 | Appendix



{Appendix A: Methodologies}

<General Notes>

The team that creates the State of the Internet / Security report does the best we can to make our data as clear and accurate as we can, but some issues escape even our attention. In reviewing the data for this report, we discovered a field for one customer had been reclassified during the reporting period. Our review of the data and how we'd used it in previous reports determined that none of the statistics or plots we have reported on were affected by the change in classification. The

difference between the first draft of the images in this report and what we're publishing was significant, however.

Although these changes had no effect on previous reports and it was possible to proceed without bringing these issues to light, it is counter to the philosophy of the State of the Internet / Security team to hide errors.

<The Big Picture of Web Attacks>

The Akamai Intelligent Platform is a network of more than 230,000 servers in thousands of networks around the globe. In March 2019, this network delivered an average daily peak in excess of 60 terabits per second (Tbps). In March, multiple patch and gaming releases drove a peak of more than 82 Tbps of traffic over Akamai's network.

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 November 1, 2017, and March 31, 2019, to be in line with the available credential abuse data.

<Credential Abuse and Gaming>

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 spreading its traffic among many targets, using a large number of systems in its scan, or spreading the traffic out over time, just to name a few.

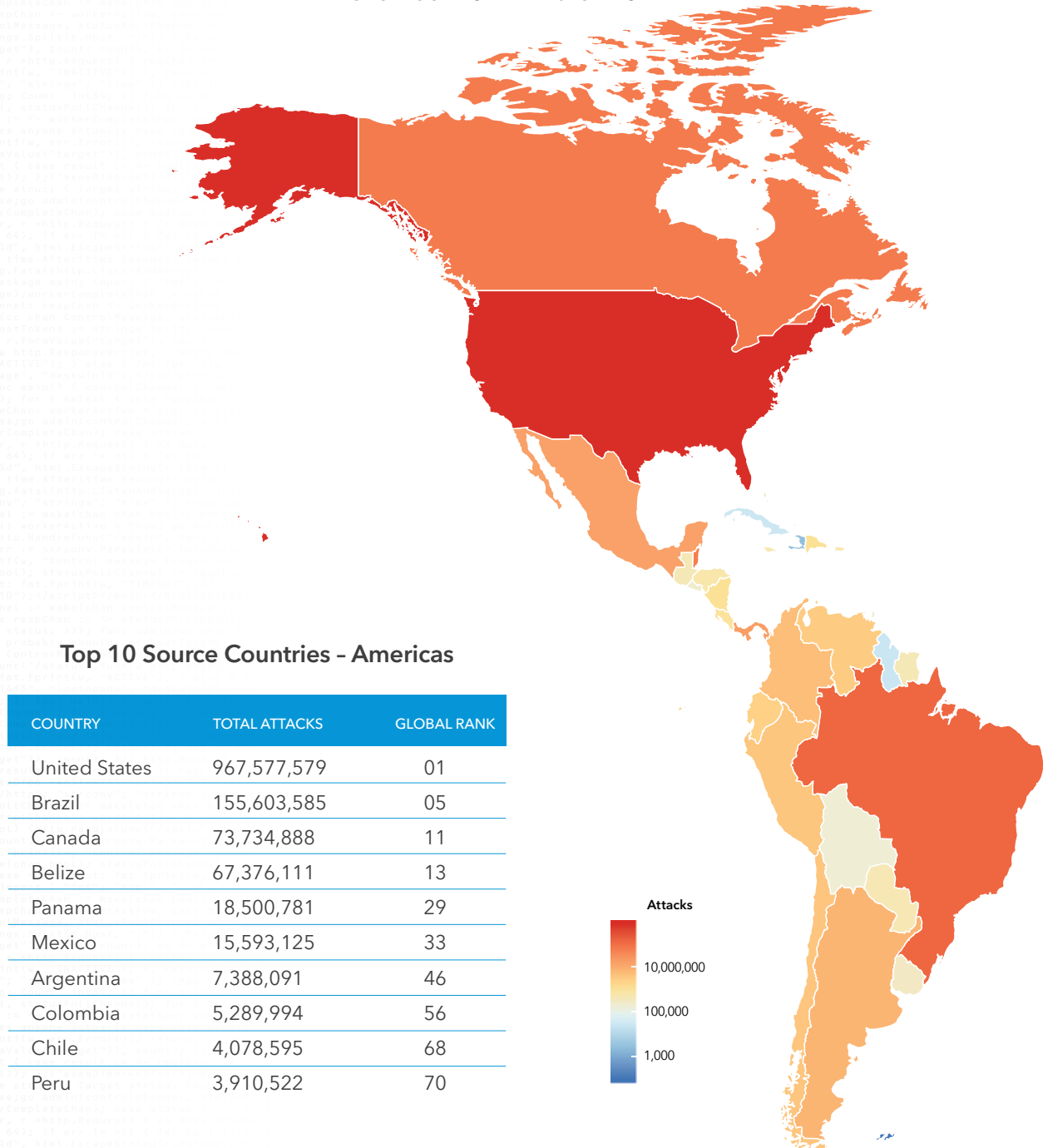
These records were collected between November 1, 2017, and March 31, 2019. As additional data is collected, future reporting will target a rolling two-year time frame.

{Appendix B: Supplemental Data}

The following plots are provided to show the regional differences in some of the plots used in the main body of the State of the Internet / Security report. They are roughly divided into the Americas, the Asia Pacific (APAC) region, and the Europe, Middle East, and Africa (EMEA) region. Our goal was to show the top representatives in each region and do not include the entirety of our data sets.

Web Application Attack Sources - Americas

November 2017 - March 2019

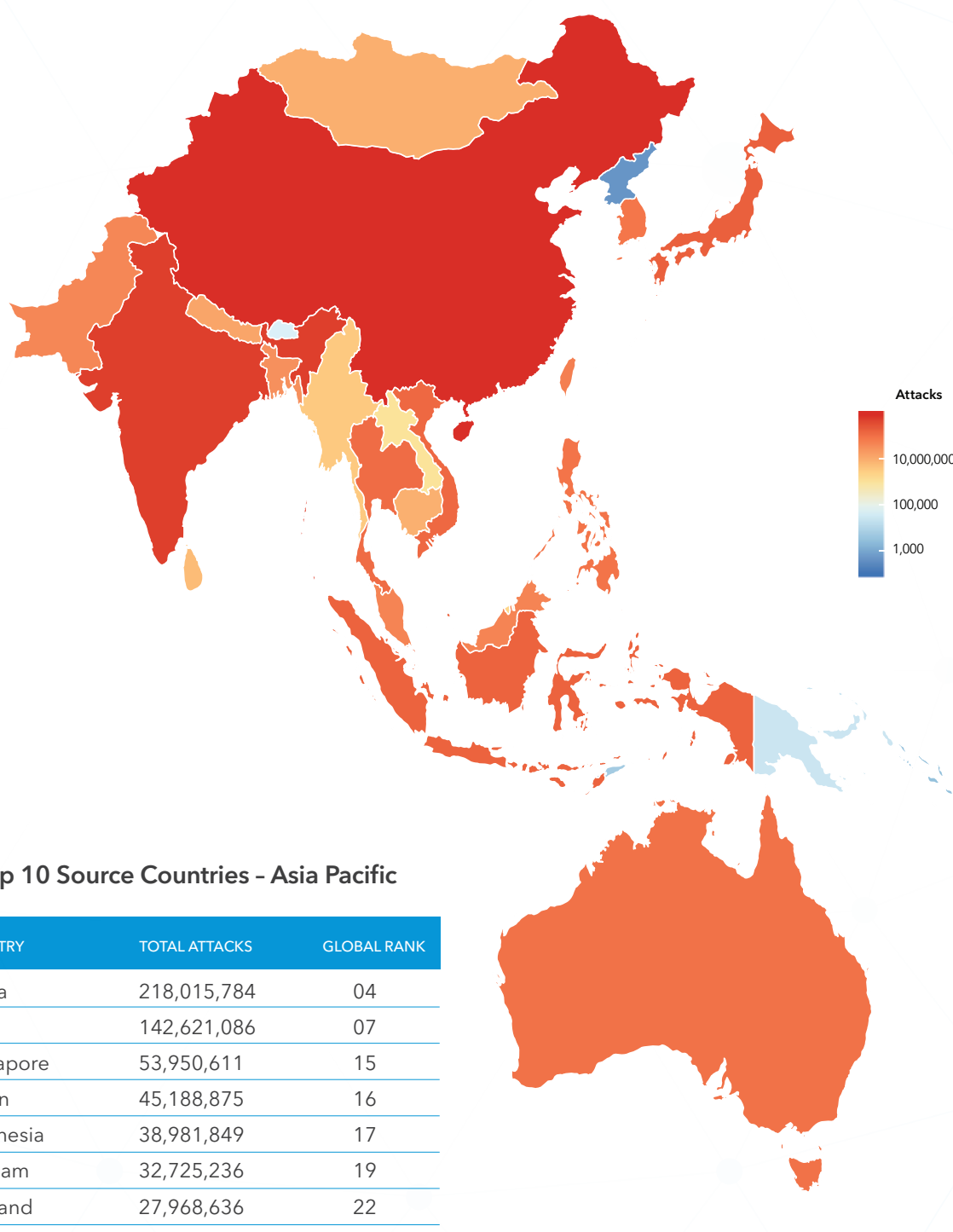


Top 10 Source Countries - Americas

COUNTRY	TOTAL ATTACKS	GLOBAL RANK
United States	967,577,579	01
Brazil	155,603,585	05
Canada	73,734,888	11
Belize	67,376,111	13
Panama	18,500,781	29
Mexico	15,593,125	33
Argentina	7,388,091	46
Colombia	5,289,994	56
Chile	4,078,595	68
Peru	3,910,522	70

Web Application Attack Sources - Asia Pacific

November 2017 - March 2019

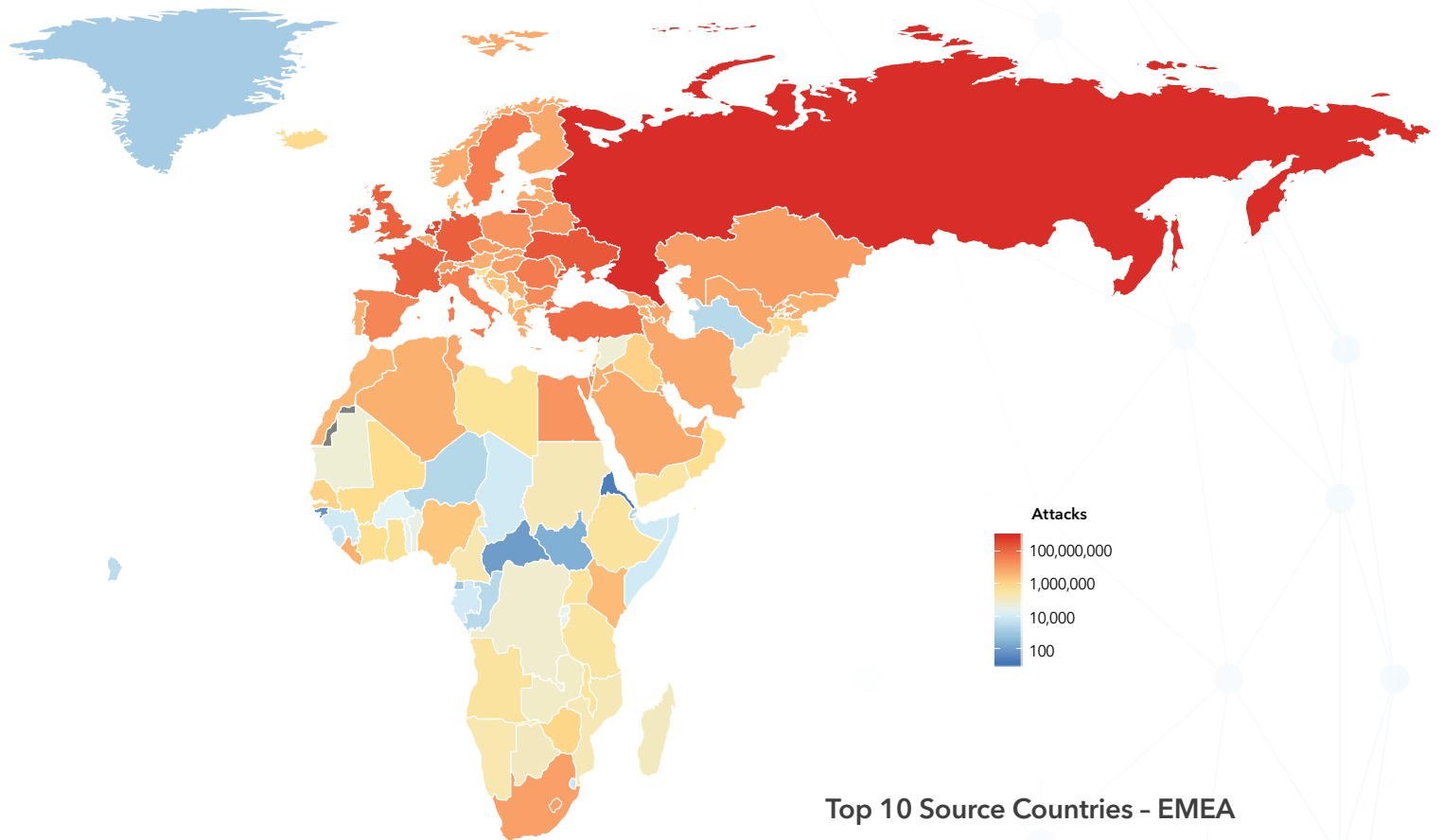


Top 10 Source Countries - Asia Pacific

COUNTRY	TOTAL ATTACKS	GLOBAL RANK
China	218,015,784	04
India	142,621,086	07
Singapore	53,950,611	15
Japan	45,188,875	16
Indonesia	38,981,849	17
Vietnam	32,725,236	19
Thailand	27,968,636	22
Hong Kong	27,733,134	23
Australia	21,669,279	25
Philippines	19,903,684	27

Web Application Attack Sources - EMEA

November 2017 - March 2019



Top 10 Source Countries - EMEA

COUNTRY	TOTAL ATTACKS	GLOBAL RANKS
Russia	608,655,963	02
Netherlands	280,775,553	03
Ukraine	154,887,375	06
France	121,691,941	08
Germany	113,233,187	09
United Kingdom	102,531,816	10
Ireland	68,870,633	12
Turkey	60,851,894	14
Romania	35,196,535	18
Sweden	31,273,168	20

Credits

State of the Internet / Security Contributors

Elad Shuster

Senior Lead Security Researcher

– Credential Abuse and The Big Picture of Web Attacks

Martin McKeay

Editorial Director

– The Big Picture of Web Attacks

Steve Ragan

Senior Technical Writer

– Editor, Cipher Work – Likes Books

Editorial Staff

Martin McKeay

Editorial Director

Steve Ragan

Senior Technical Writer, Editor

Marketing

Georgina Morales Hampe

Project Management, Creative

Lydia LaSeur

Data Scientist

– Credential Abuse and The Big Picture of Web Attacks

Tim April

Principal Architect

– Cipher Work – Photography

Amanda Fakhreddine

Senior Technical Writer, Managing Editor

Lydia LaSeur

Data Scientist

Murali Venukumar

Program Management, 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](http://www.akamai.com), blogs.akamai.com, or [@Akamai](https://twitter.com/Akamai) on Twitter. You can find our global contact information at www.akamai.com/locations. Published 06/19.



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

