Volume 6, Issue 2

GAMING_

You Can't Solo Security

Photo: DreamHack

Table of Contents

Photo: DreamHack/Joe Chuang

Letter from the Editor — Gaming

We're gamers too.

Whether it's digging for diamonds in a virtual sandbox, playing the role of a hero in a massively multiplayer online role-playing game (MMORPG), or looking for the perfect place to set up an ambush in a first-person shooter (FPS), gaming is how many of us let off a little bit of steam at the end of the day. Or maybe in the middle of the day when there's a dead space in the calendar, now that we're all working from home. Don't tell my boss.

So when a game server goes down, or a gaming company's network has increased latency due to a Distributed Denial-of-Service (DDoS) attack, or an account is compromised and digital goods are stolen, we feel the pain both as professionals and as gamers. Much of the data we work with is generated by the teams directly protecting many gaming companies from these attacks. Which means that we have a pretty decent idea of the stress some of these organizations are under.

For this issue of the State of the Internet / Security report, Akamai is highlighting a survey of gamers about their thoughts on security in partnership with the esports production and broadcasting organization DreamHack. More than 1,200 gamers from across Europe responded, and the results are, as you'll see, very interesting. While surveys aren't the type of data we usually deal with in our reporting, understanding how gamers picture security and how that relates to the types of attacks game companies see on a daily basis made for some very thought-provoking discussions within our team.

The team enjoyed having a chance to research the topic of gaming from so many different angles. We know how we feel when our favorite games are under attack. We understand the pressure defenders are under to keep these systems online and running despite the attackers' best efforts. What we hadn't examined before was how gamers themselves feel about the security of their games and their gaming accounts.

If you take nothing else from this issue of the State of the Internet / Security report, please, please, please, remember not to reuse passwords, and take advantage of the tools gaming companies make available to secure your accounts. Now, if you'll excuse me, I need to go order a two-factor authentication (2FA) token or two.

Martin McKeay
Editorial Director

Straight from the Gamers

We asked gamers who responded to the DreamHack & Akamai survey who they thought should be responsible for security and what their personal experiences have been. Here are just a few of their responses:

"…[Security] must be a joint effort. The gaming companies must provide a secure solution, but I need to live up to them and use them…"

– Frequent player who has had their account hijacked in the past

"Everyone has an equal responsibility, and should always, to the best of their ability, ensure everyone is safe and protected online."

– Frequent player who has not been hacked

"Everyone is responsible for managing the security correctly…I should make a strong and secure password, [and] the gaming companies should [offer] two-step verification and similar added security…"

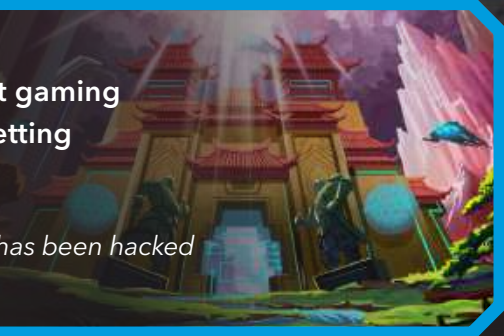
– Frequent player who has not been hacked

"You shouldn't share any information, or use the same passwords. The gaming company should always have [2FA] and make sure everything is safe…"

– Frequent player who has not been hacked

"Everyone is responsible for upholding the needed security. [Players] should always try NOT to be the weakest link since it's there the attackers look."

– Frequent player who has not been hacked



"I would say that I am responsible for my end. But gaming companies are responsible for their games not getting used as a back door."

– Non-frequent player (plays a few times per week) who has been hacked

"…One attempt through my business email got me, and I had my Twitch, Twitter, Instagram, and most likely Steam login leaked. Login attempts were made, but luckily my 2FA saved most of them…"

– Professional streamer who was hacked

Introduction

Between July 2018 and June 2020, Akamai observed more than 10 billion web application attacks across all customers, including 152 million in the gaming industry. Moreover, between July 2019 and June 2020, Akamai observed 3,072 distinct DDoS attacks in the gaming industry, making it the largest DDoS target across our customer base.

From July 2018 through June 2020, Akamai observed 100 billion credential stuffing attacks across all industries. Within the gaming sector alone, there were nearly 10 billion attacks recorded.

Gaming was a $159 billion industry in 2019, and it will reach $200 billion by 2023, according to NewZoo. The market analytics house also noted the COVID-19 pandemic, and subsequent lockdowns, led to increases in engagement and revenue all across the gaming industry.

During the COVID-19 lockdowns, everyone (especially gamers) looked for alternative ways to socialize, since PC cafes, gaming houses, bars/pubs, and other social gathering points were all closed during the early months of 2020. The availability of cross-platform gameplay, as well as gaming-friendly social platforms (e.g., Discord), enabled a common element of interaction.

In April, Steam reported a record-setting day, shortly after the previous record was set in March. On April 4, 2020, 24 million players were online, with 8 million of them in-game at the time the record was set. In fact, if you look at the Steam metrics in Figure 1, you can see that Q1 2020 – when most of the pandemic-based lockdowns took place – included steady increases in gamer interaction and consistent play times.

Steam Charts for Everyday

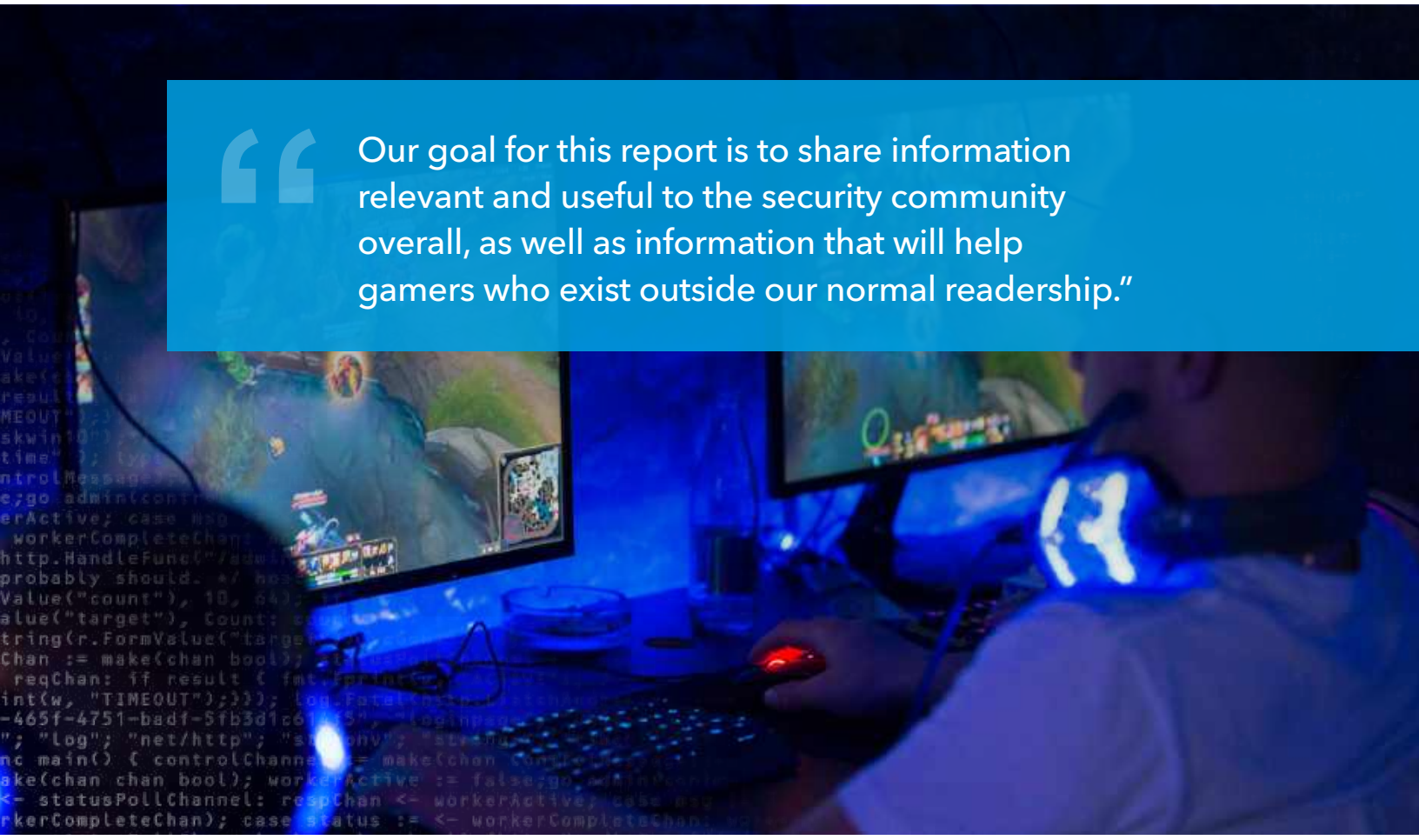
Fig. 1 – Metrics released by Steam show steady growth in Q1 2020, followed by a record setting day on April 4, 2020 (Source: SteamDB.info)

The reason we're starting this report by talking about industry metrics is simple: last year, we told you that the gaming industry was quickly becoming a lucrative target for criminals. Now, with 24 months of data, we can positively state that gamers are a prime target, and so are their online existences. COVID-19 changed gaming, and criminals who were under the same pandemic lockdown as the rest of us wasted no time targeting gamers across the globe.

Our goal for this report is to share information that is relevant and useful to the security community overall, as well as information that will help gamers who exist outside of our normal readership. One way to do that is to speak directly to gamers.

In the spring of 2020, working with esports company DreamHack, Akamai sent a survey to gamers to gather their insights on security as it relates to their gaming experience. The initial survey results include 1,253 responses from European gamers, followed by a second set of questions and answers from 369 of the original respondents. In addition, Akamai interviewed two American gamers: one who works inside the security industry, and thus resides in the security echo chamber, and one who has no connections to the industry whatsoever.

It is our hope that adding gamer perspectives to our collected data allows us to offer a more rounded picture when it comes to the state of security in the gaming industry.



> "Our goal for this report is to share information relevant and useful to the security community overall, as well as information that will help gamers who exist outside our normal readership."

Protecting the Servers

Photo: DreamHack/Kim Ventura

Gamers love their games, and their hobby often requires a certain level of commitment as they grind out levels or gear. It's no surprise to see them playing daily or several times a day. Yet all of that interaction means that the gaming companies responsible for the various platforms and servers need to keep these assets online. As such, they constantly need to fend off web-based attacks targeting their infrastructure.

Between July 2018 and June 2020, Akamai observed 10,628,755,494 web application attacks across all customers and 152,256,924 in the gaming industry alone. Looking at the attack landscape, SQL Injection (SQLi) is still the number one attack vector, with 76% of attacks across all customers taking this format (58% in gaming). SQLi is followed by Local File Inclusion (LFI) attacks, with 16% of attacks across all customers and 31% in the gaming industry alone.

81% of respondents say they play games every day or several times a day

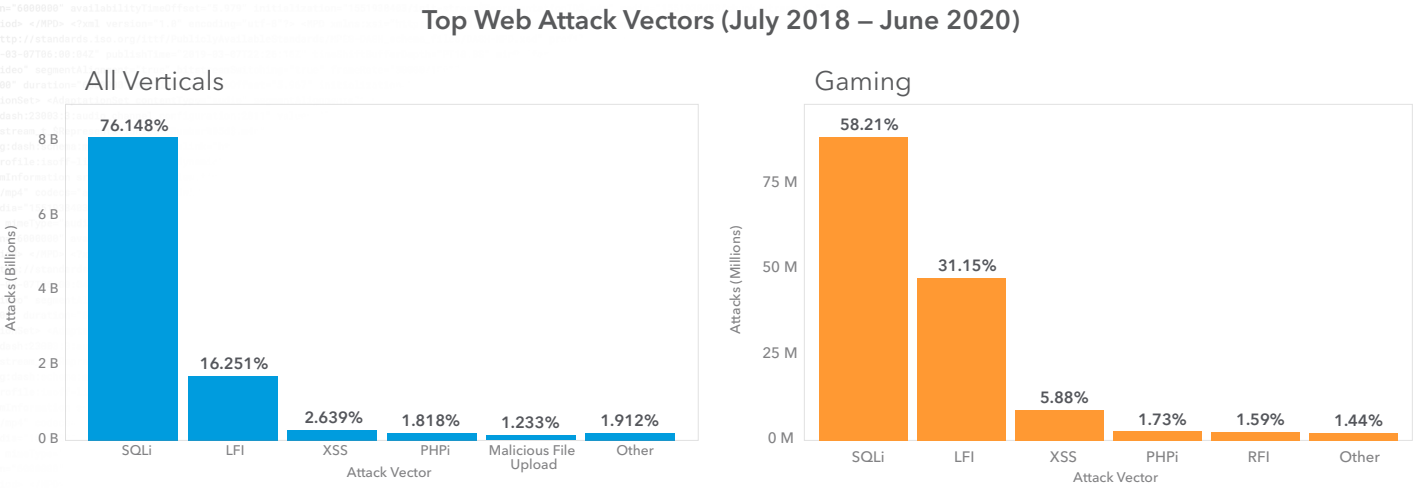


Fig. 2 – Web application attacks against the gaming industry are mostly dominated by SQLi and LFI

When it comes to SQLi and LFI attacks, criminals are looking for a few things. SQLi attacks could yield login credentials, personal information, or anything else stored in the targeted server's database. For example, researchers at Akamai have seen training videos shared by criminals, where SQLi attacks are used as a way to source login data, which is then used as part of a credential stuffing attack.

LFI attacks look to exploit scripts running on the servers. However, criminals have been known to target LFI flaws that exist in ASP, JSP, and other web technologies. LFI attacks usually result in information disclosure, such as server configuration files (which can be used to compromise the server and all the accounts on it). In the case of gaming, LFI can be used to target stored data. The stored data being targeted could include files housing player and game details, which can be used for exploiting or cheating.

Mobile games and web-based games are big SQLi and LFI targets, because criminals who successfully pull off attacks against these platforms will gain access to usernames and passwords, account information, and anything game related that is stored on the server.

There are entire markets dedicated to selling boosted accounts, or accounts that have been compromised and taken over. If exploited, these flaws can also be used by criminals running resource farming operations, where bots (automated accounts that act like a player) grind out resources or in-game items that can be traded or sold.

Examining the daily sources, a pattern of steady web attacks unfolds over the recorded period, with consistent streams across all types, from SQLi and LFI, to Cross-Site Scripting (XSS), PHP Injection (PHPi), malicious file uploads, etc.

Fig. 3 – Daily views of web attacks during the observation period show a consistent stream of attacks against the gaming industry across multiple attack types

Some attacks, including LFI, show strong spikes at certain times of the year, such as summer months in the United States, or on global holidays. Others, such as malicious file uploads, PHPi, and XSS, show steady and consistent attack spread. Notably, each one spiked in May of 2020, along with LFI, but there does not appear to be any definitive cause – only an observed period of high activity. What the charts in Figure 3 show is that criminals are consistent and relentless when it comes to targeting the gaming industry.

In addition to web-based attacks on servers and applications, gaming companies also need to contend with DDoS attacks. Gamers are familiar with DDoS attacks, because at one point or another they've played a game that has been knocked offline due to criminals, or angry kids with an axe to grind.

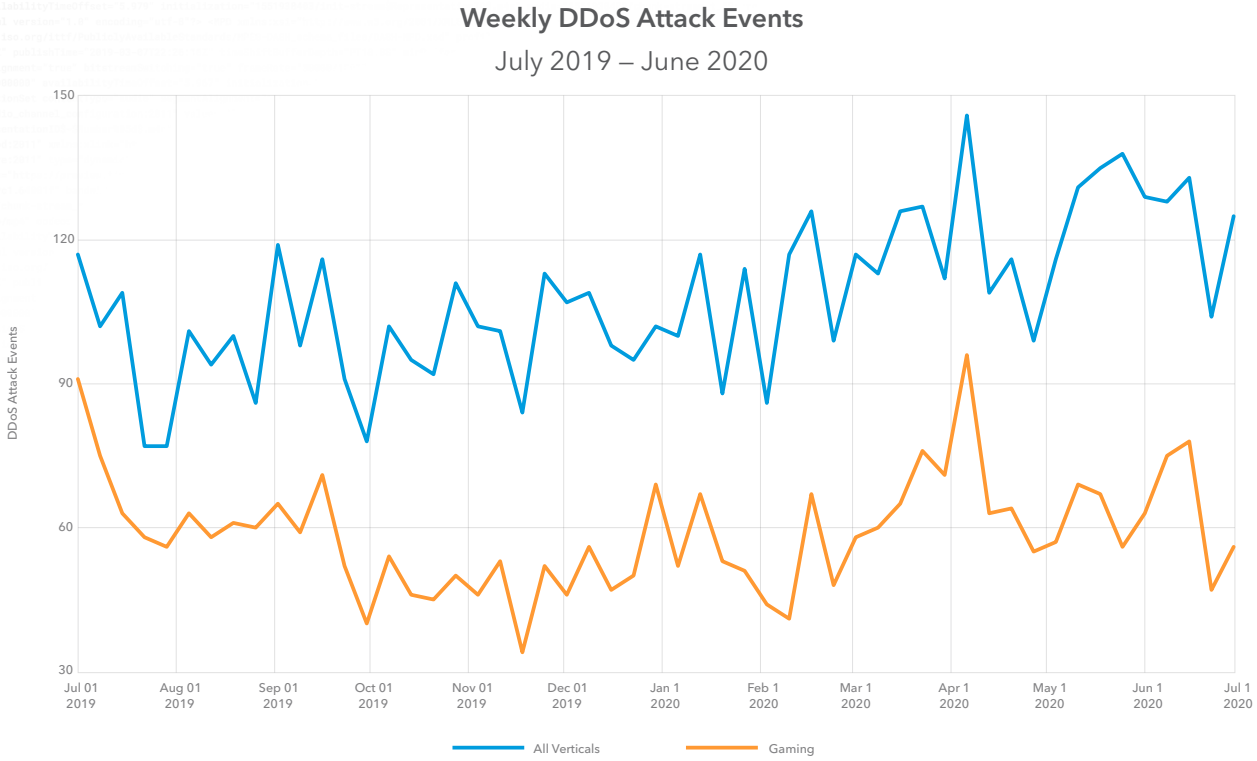


Fig. 4 – DDoS attacks are constant, and the majority of them target the gaming industry, followed by the high tech and financial services sectors

In 2016, the Mirai botnet was responsible for a series of DDoS attacks that wreaked havoc on the internet. Yet this botnet wasn't the work of some massive cabal of criminals attempting world domination. Instead, this destructive botnet originated with three college kids looking to take down Minecraft servers for fun and profit. Their goal was simple – DDoS the competition and get their customers to switch hosts, once the slow or nonexistent server connections frustrated them to the point of leaving.

Between July 2019 and June 2020, Akamai observed 3,072 distinct DDoS attacks in the gaming industry, making it the largest DDoS target across our customer base, followed by the high tech and financial services sectors. There were 5,624 DDoS attacks across all verticals during the same period.

As you can see in Figure 4, DDoS attacks are consistent, occurring daily across all industries, particularly in gaming. Moreover, these attacks spike during holiday periods, as well as during the summer and spring seasons. This is usually an indicator that the ones responsible are home from school.

Photo: BLIZZARD/StarCraft II 10th Anniversary

Did You Know?

Contrary to popular belief, a lag switch isn't a DDoS attack. A lag switch cuts off outgoing data when activated, and really only works well on peer-to-peer (P2P) games. During a first-person shooter game, for example, a switch will cause the opposing player to appear frozen on your screen. The person using the switch, however, can move and shoot on their screen as normal. Once the switch is released, and the data syncs up again, the person using the lag switch will appear to move at rapid speed and will often score kills before you can act.

On consoles and PCs, lag switches are starting to make a comeback, at least where blame is concerned. Cross-play gaming and the emergence of new P2P games, as well as wide implementation of lag compensation, have led to claims of lag switching increasing among players of several popular multiplayer titles. The reality isn't as clever as a switch on a controller, though. More often than not, it isn't a lag switch causing problems – it's just bad network connections and overloaded servers.

Top Target Areas for Web Application Attacks – Gaming

July 2018 – June 2020

TARGET AREA	ATTACK TOTAL	GLOBAL RANK
United States	147,034,562	1
Hong Kong SAR	1,683,439	16
United Kingdom	1,068,738	2
Singapore	891,319	15
Japan	753,653	6
China	386,584	9
South Korea	352,368	17
Canada	57,333	7
Germany	15,044	4
Taiwan	13,882	18

Fig. 5 – Three of the top five targets in the gaming industry have strong mobile gaming presences, proving that criminals target mobile games just as frequently as they target other platforms

When it comes to targets, the majority of them are in the United States, followed by gaming firms in Hong Kong SAR, the United Kingdom, Singapore, and Japan. Within the top five, as shown in Figure 5, it is worth mentioning that the Asian market has a strong mobile gaming presence. Criminals often single out mobile gaming for DDoS, account trading, and takeovers, as well as resource farming. Such actions sometimes translate into real-world currency losses to both the players and the gaming developers.

***Note:** Please see the Methodologies section for details about how we came up with the area rankings for attack targets and attack sources. Source does not imply attribution of an attacker to the country referenced.*

> Criminals often single out mobile gaming for DDoS, account trading, and takeovers, as well as resource farming.

Photo: PUBG Corporation/PUBG Stadia

Top Source Areas for Web Application Attacks – Gaming

July 2018 – June 2020

SOURCE AREA	ATTACK TOTAL	GLOBAL RANK
United States	68,039,746	1
Russia	9,913,447	2
Turkey	5,735,990	21
Netherlands	5,101,199	3
Indonesia	4,568,904	17
United Kingdom	4,474,914	13
China	4,326,990	4
Germany	4,318,502	8
France	4,162,498	14
Hong Kong SAR	3,710,690	22

Fig. 6 – When looking at the source of the attacks, the United States remains at the top but is followed by countries known for botting and credential stuffing

As for the source of the attacks, shown in Figure 6, Akamai can only talk about the final hop in the attack chain, as there is no real way to track a given hostile actor beyond what we can see coming into our network. However, we can see the United States at the top of the source list, followed by Russia, Turkey, the Netherlands, and Indonesia. Three of these countries have strong presences in underground forums known for DDoS services, credential stuffing, and botting, which is used for targeting gaming via account takeover or resource farming.

***Note:** In this instance, when we talk about resource farming and botting, we're talking about bots that are used to automate play in a given game in order to collect in-game items. For example, a farming bot could be used to collect gems or rare items, which are then traded, or the account with all of these rewards could be sold. Hacked accounts are often used for farming, so if they're suspended or shut down, the criminal behind the operation doesn't lose their own accounts.*

Photo: STARCRAFT/Legacy Of The Void

Playing the Game

We've talked about the attacks against gaming platforms and services, but now we're going to talk about attacks against gamers themselves.

Criminals target gamers directly via two different paths. The first is phishing. When a criminal creates a legitimate-looking website related to a game or gaming platform, with the goal of tricking gamers into revealing their login credentials, it's called phishing. An example of a phishing attack against users on Steam can be seen in Figure 7.

In the image, the inset is what the phishing kit displays once the Add Friend link is clicked. Anyone who entered their credentials would have had their account compromised. Attacks like this often originate via random messages offering a rare item, or trade, on the platform. They're designed to target those with little to no awareness about such scams.

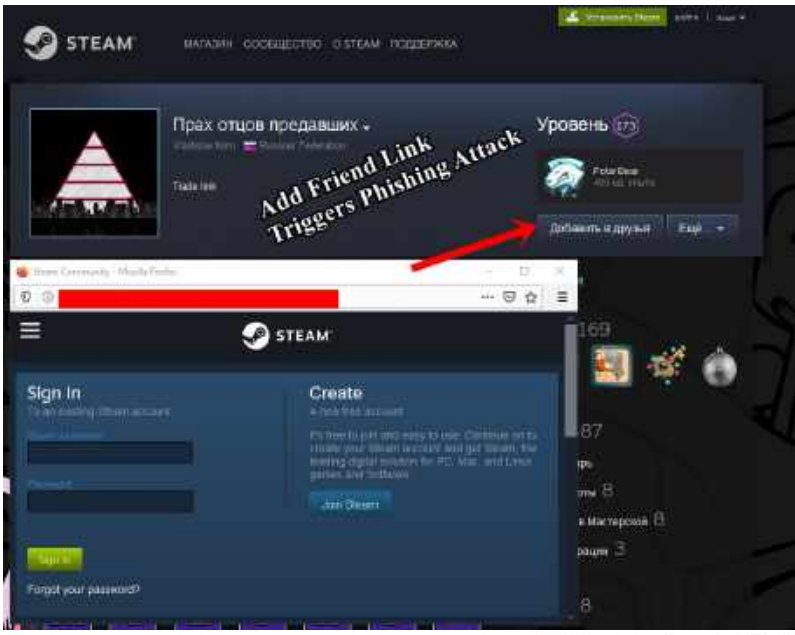


Fig. 7 – A Steam phishing page targeting login credentials

The second most common way criminals target gamers is through credential stuffing. This is when a criminal takes a list of usernames and passwords, and attempts to access a game or gaming service using each item on the list. Every successful login means a gamer's account has been compromised.

To streamline the credential stuffing process, vendors on various marketplaces offer collections of targeted lists. Figure 8 is an example of one such list that targets the gaming industry. The seller is pushing lists in bulk, with a going rate of $5 per million records. The reference to "private" means that the usernames and passwords being sold are not part of any of the publicly traded gaming lists; they are fresh at the time the sale was posted.

There are a lot of credential stuffing attacks happening. From July 2018 until June 2020, Akamai observed 100,195,620,436 credential stuffing attacks across all industries. Within the gaming sector alone, there were 9,831,295,227 attacks recorded.

Fig. 8 – Targeted credential stuffing lists are created for a number of markets and sectors, including the gaming industry

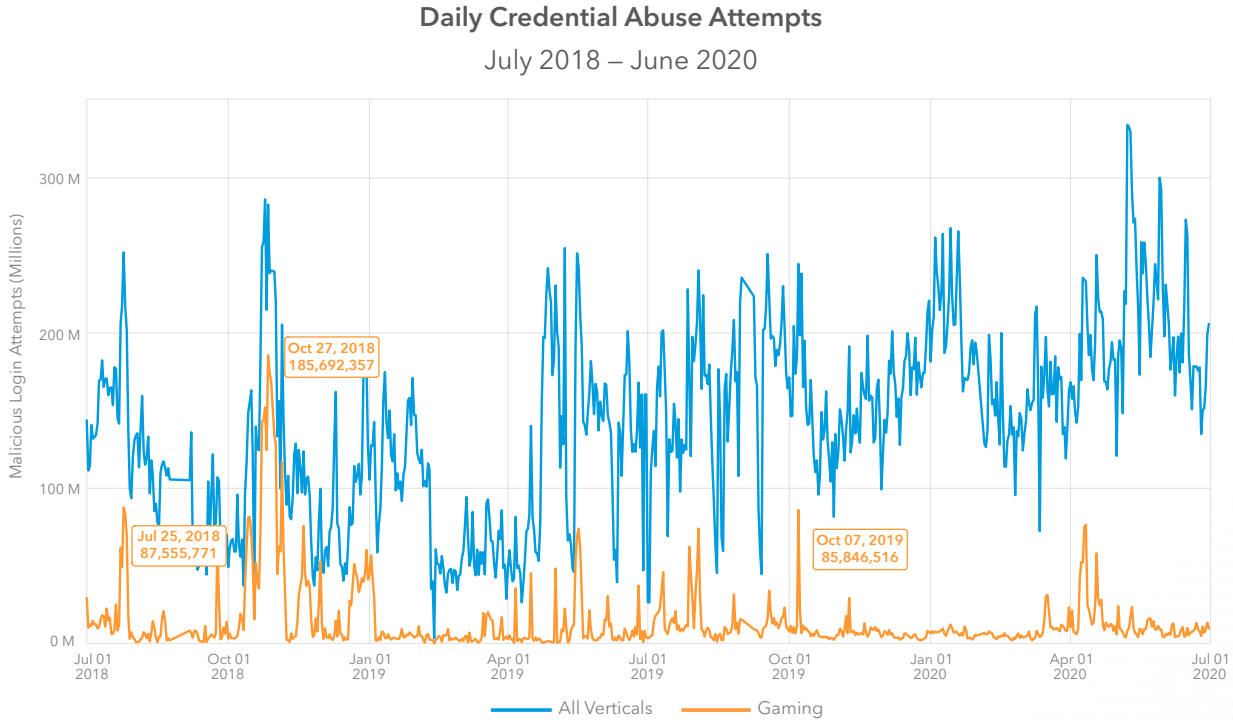


Fig. 9 – Credential stuffing attacks in gaming remained a constant threat over the past two years and spiked in the first quarter of 2020

In Figure 9, we've plotted out the credential stuffing attacks over time, but we've removed one non-gaming customer from the data set because its attack volume generated significant traffic, essentially pushing gaming down to a barely visible line when it was included. In addition, it was removed because only six months of data were available at the time this report was being developed.

As you can see, credential stuffing attacks against the gaming industry occur consistently, much like the web attacks we discussed earlier. However, as the COVID-19 lockdowns started in Q1 2020, there was a noticeable spike in credential stuffing activity. This was due to a number of factors, including a push by criminals to test the credentials exposed during older data breaches to see if there were new accounts to compromise.

A highly publicized example of this were the attacks on Zoom. While not a gaming channel, the same tactics used against the popular communications tool (including scanning and account verification, as well as direct credential stuffing) were also used against gaming and other entertainment platforms.

As mentioned earlier in this report, many people turned to gaming as a means of social interaction during the lockdowns. Criminals wasted no time directly targeting them. The offer seen in Figure 8 is just one example of how the retesting of old data and new SQLi attacks resulted in a fresh batch of credentials targeting gamers. Other examples, including the ads for Steam, Minecraft, Epic Games, and uPlay accounts in Figure 10, represent more focused listings, aimed at people looking for particular games.

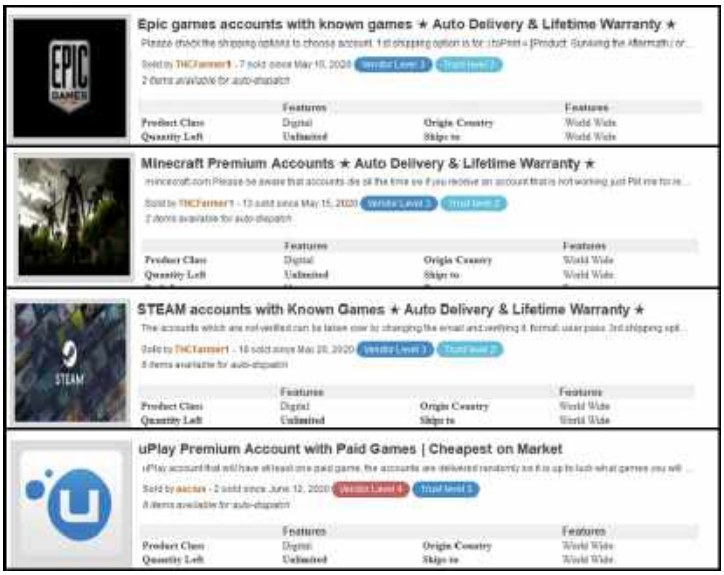
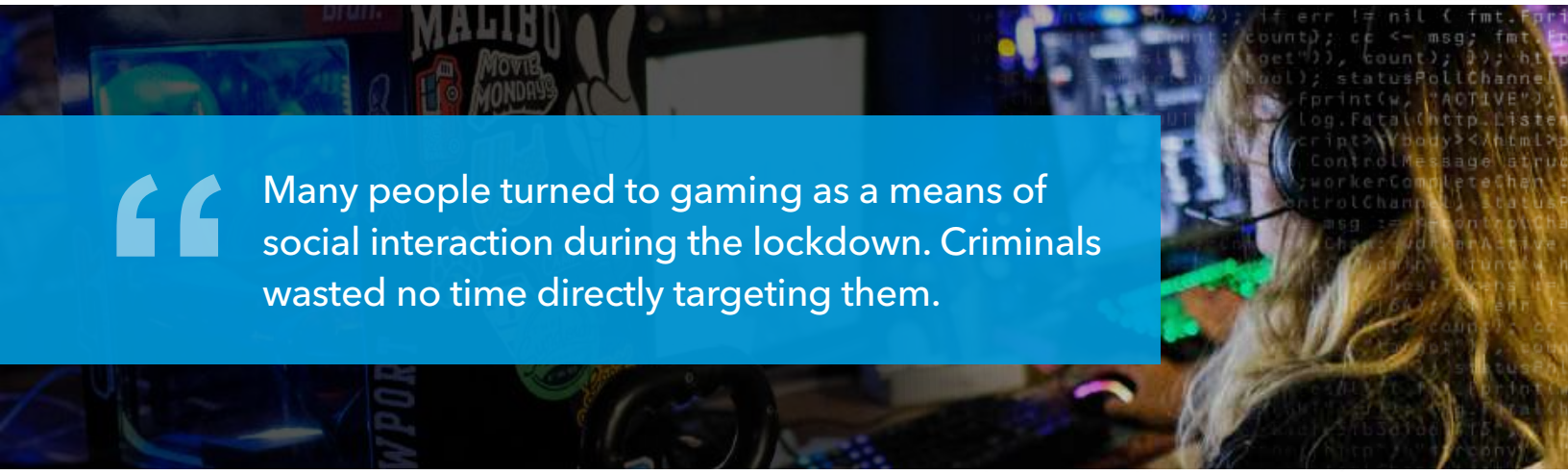


Fig. 10 – Offers on the darknet include targeted sales based on gaming platform or title



> Many people turned to gaming as a means of social interaction during the lockdown. Criminals wasted no time directly targeting them.

Perfectly Balanced

Photo: DreamHack/Kim Ventura

At its core, the most vulnerable and the most targeted elements of the gaming industry are its players. The human element is always the hardest to control and secure, so this revelation isn't a surprise.

A good example of this difficult balance comes from our survey. More than half of the frequent players said they've had their accounts compromised, but only one-fifth of them were worried about such things. Why the disconnect?

It could be that the gamers themselves don't see the value in the associated data tied to their gaming accounts. It could be that their gaming experience doesn't change even if an account is compromised. Humans deal with risk in different ways, and gamers are no exception.

20% of frequent players say they're worried or very worried about having their gaming accounts compromised (hacked or hijacked)

55% of frequent players said they've had one of their accounts compromised in the past

The fact remains, gamers are highly targeted, because they have several qualities that criminals look for. They're engaged and active in social communities. For the most part, they have disposable income, and they tend to spend it on their gaming accounts and gaming experiences. When these factors are combined, criminals see the gaming industry as a target-rich environment.

54% of the survey participants who have been hacked say that security is the shared responsibility of the gamer and the game developer/company

So, who is responsible for protecting the gamers? Are the players themselves responsible for their own protection? Does this responsibility fall to the game developer, or gaming company? Is it a mix of both?

"In my opinion, any and all security measures should be looked at by the gaming companies themselves. We [the gamers] purchase games, services, etc. under the understanding that we are supposed to be able to play it comfortably and without hassle," commented Nate Collard, a gamer who makes a living off streaming on Twitch. His thoughts are similar to many other gamers, who often just want to play and not worry about fending off attacks on their own.

He continued, "However, in doing so, for most games anyway, you have to apply your personal information, financial accounts, etc. to even play them. I feel this just opens people up to even more risk."

On the other end of that spectrum, a gamer who works in the security industry, Chris Hawkins, reminds us that security is everyone's responsibility.

"When it comes to securing accounts and transactions, companies should be the first line of defense in protecting users and their online experience. This can also be in the form of protecting users from themselves by having minimum requirements in place such as password length and complexity as well as multi-factor authentication," he explained.

"Security and awareness within this industry is more essential today than it has ever been. Gaming has gone beyond simple consumption, as esports and game streaming have gained greater legitimacy and presence. More individuals and companies have a financial stake in the overall success of the industry, and there won't be any success if accounts are compromised and trust is eroded."

The gaming industry agrees with both of them, to a degree, especially when it comes to security awareness and taking control over account protection mechanisms.

What participants would be concerned about if their accounts were hacked:

49% credit card information

48% account access

43% in-game assets (skins, special weapons, etc.)

Multiple answers allowed

When criminals use credential stuffing, the goal is account takeover, which is exactly what the participants in the DreamHack/Akamai survey are worried about. Criminals are looking for in-game assets that can be traded or sold, account details and personal information (which can be traded or sold), and financial information, which can be compromised and used for financial theft. Moreover, criminals are also looking for accounts that have a large number of games associated with them, or accounts that have access to whatever the hot game is at the moment.

Criminals obtain the usernames and passwords needed for credential stuffing from a number of places. As mentioned earlier, criminals will conduct SQLi attacks to harvest login details. In the past, criminals have targeted forums related to gaming discussions using this method. These places are an environment full of known gamers, making them an ideal target.

On one criminal marketplace, a collection of gaming databases has been on sale since 2019, targeting fans of popular titles such as Battlefield, Minecraft, Counter-Strike: Global Offensive (CS:GO), and Witcher, as well as gaming companies such as Ubisoft and Bandai Namco.

Some of these databases are collections of older data breaches, but there were a few newer releases mixed into the sale. All of the databases sold in this collection are available individually and are still used today in credential stuffing attacks.

Old Data. New Attacks.

The reason older data breach collections are used by criminals is due largely to password recycling and reuse. Thus, a data breach on a movie forum could lead to a compromised gaming account if the victim used the same password in both places. This is why it is so important to never share or recycle passwords and why password managers are an essential security tool online.

Gaming giants, such as Ubisoft, Epic Games, Valve, and Blizzard, encourage multi-factor authentication usage, adding an additional layer of protection. In some cases, they even offer authenticator applications. However, unless these protections are actually used by the players, they can't help protect their accounts.

Top Source Areas for Credential Abuse – All Verticals

July 2018 – June 2020

SOURCE AREA	MALICIOUS LOGIN ATTEMPTS	GLOBAL RANK
United States	34,935,239,915	1
China	4,871,373,517	2
Russia	4,057,633,311	3
Brazil	4,047,223,074	4
Thailand	3,647,391,930	5

Fig. 11 – The United States remains the top source for credential stuffing attacks across all industries

Across all industries, the United States was the top source for credential stuffing, followed by China and Russia (Figure 11).

When you consider just the gaming industry alone (Figure 12), the first position is the same, but China drops to fourth place, and is replaced by Canada. Last year, the United States was the third-largest source area for credential stuffing against gaming, but moved up this year to replace Russia as the primary source of attack traffic.

The cause of this shift is unknown, but it could be related to a number of factors, including the increased number of people at home during the pandemic lockdowns, or the number of remote desktop protocol and proxy services located in the United States that have gone up for sale in the past year or so. Attack source and attack target data are constantly in a state of flux, and it is difficult to determine a single source or cause of movement within the vast pool of sampled data.

Top Source Areas for Credential Abuse – Gaming

July 2018 – June 2020

SOURCE AREA	MALICIOUS LOGIN ATTEMPTS	GLOBAL RANK
United States	1,521,791,715	1
Russia	1,074,537,783	3
Canada	1,045,782,596	10
China	671,047,993	2
Germany	536,160,008	8

Fig. 12 – The United States has moved up two spots since 2019 to replace Russia as the top source of credential stuffing attacks in the gaming industry

Dealing with Attacks

So, we've talked about phishing and credential stuffing, but what can you – as a gamer and a customer – do about these attacks?

The first thing to remember is this: Most gaming platforms have several security features, but you need to activate them in order to use them. This opt-in approach is called a security tradeoff.

Sometimes security can be a bit of a hassle. Gaming companies want to make your experience as painless as possible. It isn't feasible in many cases to impose several layers of defense if those protections make playing the game – the whole reason you're there in the first place – difficult or near impossible. When done right, security should be seamless, and for many of the larger AAA gaming companies, that's exactly what it is.

So, in a sense, when Nate Collard said that "any and all security measures should be looked at by the gaming companies themselves," he was completely correct. The gaming companies acknowledge this and dedicate vast sums of resources and people toward delivering security to their players.

But, as Chris Hawkins said, security is everyone's responsibility. This means you'll need to do your part to keep the security chain strong.

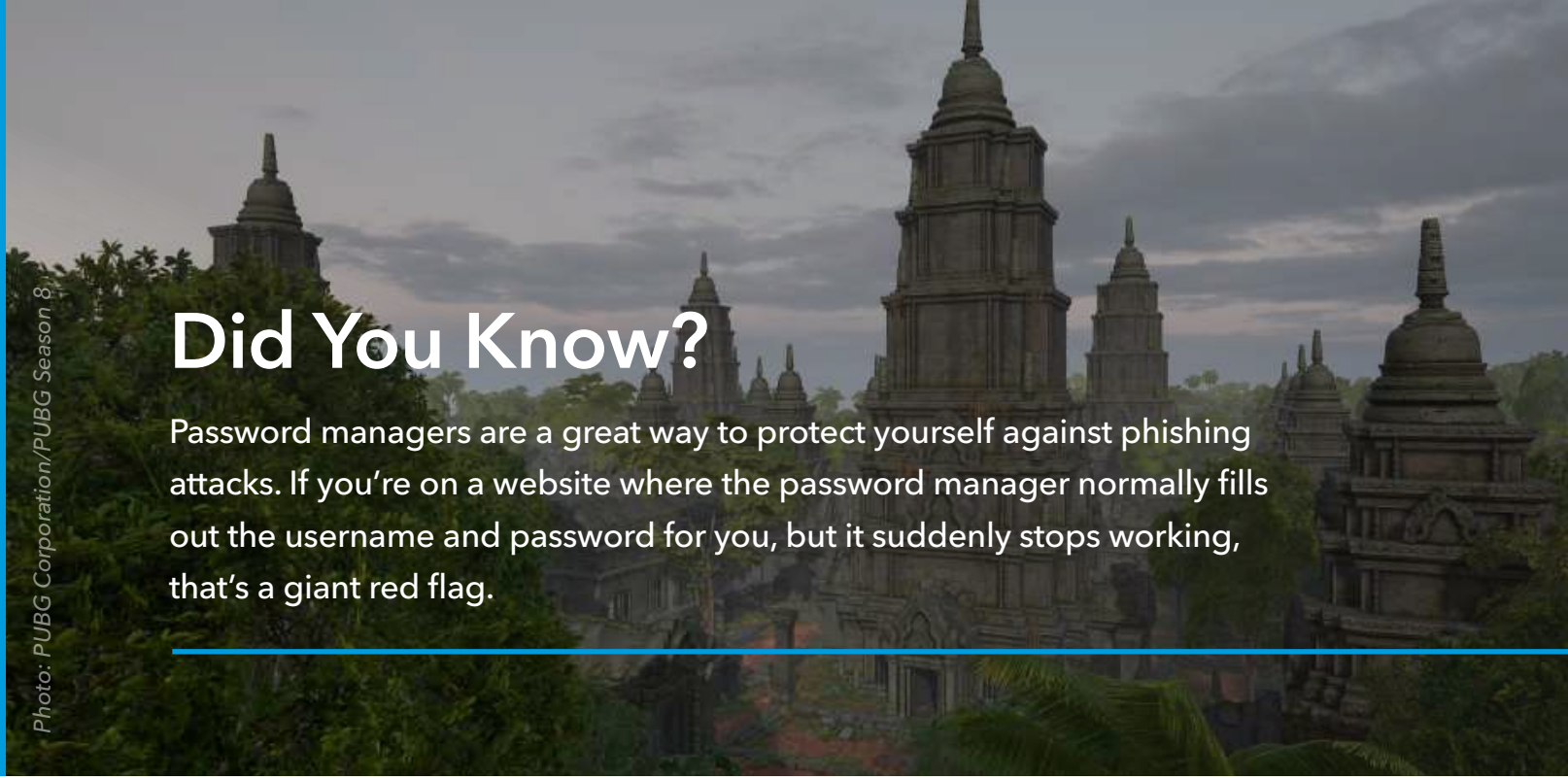


Photo: PUBG Corporation/PUBG Season 8

Did You Know?

Password managers are a great way to protect yourself against phishing attacks. If you're on a website where the password manager normally fills out the username and password for you, but it suddenly stops working, that's a giant red flag.

Password Managers – It doesn't matter which password manager you use, as long as you use one. Pick the manager that works best for you. The goal is to make sure that each password you have is unique and not shared across multiple websites and services. Why is this so important? Because if you recycle/reuse the same password across multiple websites or services, then a single compromised account (via a phishing attack, for example) could lead to multiple compromised accounts. This, in a nutshell, is essentially how credential stuffing works when such attacks are successful. The single most important defense against credential stuffing attacks is a lengthy, unique password for each account you have, gaming or otherwise.

Two-Factor Authentication (2FA) – 2FA is a subset of multi-factor authentication, requiring two different factors when confirming identity. In many cases, this is something you know (your password) and something you have (your phone). A phone is the most common item in this process, as authenticator apps and SMS messages deliver the code needed to verify you are who you claim to be when presenting your account password. If either of these are missing, the authentication fails and you can't log in to your account.

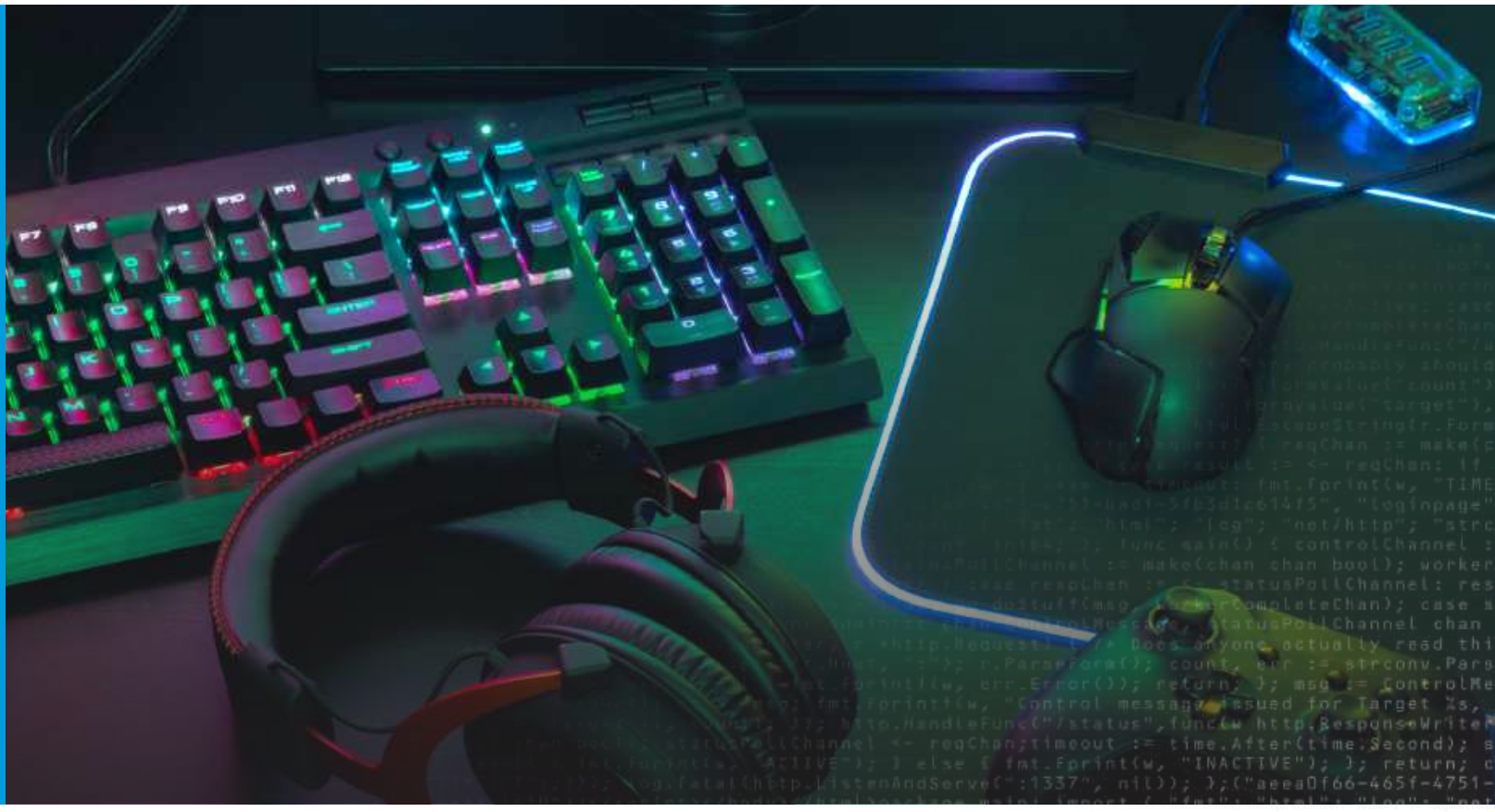
Microsoft, Blizzard, and Steam have their own authenticator apps, but others, including Ubisoft and Nintendo, will allow you to use third-party authenticator apps like Google Authenticator. When an authenticator isn't an option, most gaming companies, like Sony, will use two-step verification, delivering a one-time passcode to the phone via SMS.

Using SMS as part of a security process, such as two-step verification, comes with some risk. This risk mainly centers on the phone, as the SIM card can be cloned or the device directly compromised, which sidesteps the security aspect of using "something you have." When it comes to phishing, SMS 2FA cannot prevent phishing. There have been several examples in the news where SMS verification has been exploited by criminals to gain access to accounts, such as attackers who cloned SIM cards or used phishing kits that have SMS 2FA implemented.

Despite these potential vulnerabilities, if SMS is available, you should use it unless a stronger verification method exists. Something is better than nothing. However, if there is a choice between SMS 2FA and an authenticator app, opt to use the app, as you'll want the strongest protections available. Layered protections during the authentication process are essential and do a lot to lessen the severity of credential stuffing and phishing attacks.

Other things you can do to protect your account include making sure to log in through official apps and services, not through third parties. For example, use the Store or Community page on Steam. If you're asked to log in to Steam after you've given your account username and password to a third party, that's a positive indicator that you've been phished.

Finally, remember that the customer support or official corporate staff for any game you play will never — ever — randomly reach out and ask for personal information, financial information, or passwords in order for you to keep your game or your account. Nor would these staffers ask for authenticator codes (Steam) or your authenticator restore code (Blizzard). To be blunt, anyone asking for any of these pieces of data is almost certainly an attacker, and you are the target.



Additional Resources

The following resources might be of assistance for securing your accounts on some of the most popular platforms and services.

Microsoft

How to Use Two-Step Verification with Your Microsoft Account

Xbox One Online Safety and Privacy Settings for Parents and Kids

Blizzard

Securing a Blizzard Account

Account Hacked with Authenticator

Received a Suspicious Email from Blizzard (Phishing)

Steam

Account Security Recommendations

Common Scam Types

Ubisoft

Securing Your Account with 2-Step Verification (Mobile App)

Recognizing Legitimate Ubisoft Communication

Sony

How to Activate 2-Step Verification on PS4

How to Keep Your Account on PlayStation Network Safe

Nintendo

How to Set Up 2-Step Verification for a Nintendo Account

Closing Thoughts

Web attacks are constant. Credential stuffing attacks can turn data breaches from the days of old (meaning last week) into new incidents that impact thousands (sometimes millions) of people and organizations of all sizes. DDoS attacks disrupt the world of instant communication and connection.

These are problems that gamers, consumers, and business leaders face on a daily basis. This year, these issues have only gotten worse, and the stress caused by them was compounded by an invisible deadly threat known as COVID-19.

This report was planned and mostly written during the COVID-19 lockdown, and if there is one thing that's kept our team sane, it is constant social interaction and the knowledge that we're not alone in our anxieties and concerns. For two of us, that social interaction involved gaming.

But the world isn't all dark, and when it comes to the security space, companies are increasingly focusing their energies on protecting their players. Gamers themselves are starting to realize the strength of security controls and are leveraging them on a regular basis. In the DreamHack/Akamai survey, those who participated acknowledged their willingness and active use of additional protections such as password managers and 2FA. This is a good thing.

If you're interested in helping, especially if you're a gamer, share this report with those outside of the security and technology space, and help them protect themselves. A little awareness and preparedness goes a long way toward thwarting an attack.

Keep in mind, this isn't just about protecting gaming accounts. Some victims were targeted long before their gaming profiles were compromised. Criminals will target everything, including email and social media, and use those trust networks and expected safe spaces as a launching pad toward other targets and new attacks.

We all have a part to play when it comes to protecting the gaming community and the broader internet community. Awareness of the problem, as well as a willingness to use the tools available to protect yourself and others, is key.

Stay safe!

Photo: DreramHack/Emma Andersson

Methodologies

General Notes

The data used for all sections was limited to the same 24-month period – July 1, 2018, to June 30, 2020 – unless stated otherwise below.

Attack "Source" and "Target" Areas

For requests flagged as an application attack or credential abuse attempt, the source area is determined using the source IP address that connected to one of Akamai's edge servers and our in-house geolocation service, Edgescape. Akamai leverages its massive network and high visibility to verify and maintain the geolocation data, which is 99% accurate at the country level.

The source of traffic should not be confused with attribution of attacker location. Attribution implies a determination of the location of the person or organization controlling the attack. It's relatively easy to say where the traffic came from, while it's extremely difficult to determine who caused the traffic to be generated in the first place without a dedicated team of researchers. Even then, it's nearly impossible at this scale.

Given our definition for source area, one may assume that target area is determined by the IP address that received the malicious request, but that's not the case. If it were, the top target list would likely look pretty similar since Akamai edge servers are deployed in most countries. Instead, the target area of an attack is defined as the primary location of the customer that was targeted. Many organizations have a widely distributed network and services environment, and gathering data based on where it is being served from would be problematic on multiple levels.

Protecting the Servers

Web Application Attacks

This data describes application-layer alerts generated by Kona Site Defender and Web Application Protector. The products trigger these alerts when they detect a malicious payload within a request to a protected website or application. The alerts do not indicate a successful compromise. While these products allow a high level of customization, we collected the data presented here in a manner that does not consider custom configurations of the protected properties.

The data was drawn from Cloud Security Intelligence (CSI), an internal tool for storage and analysis of security events detected on the Akamai Intelligent Edge Platform. This is a network of approximately 300,000 servers in 4,000 locations on 1,400 networks in 135 countries. 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.

DDoS

Prolexic Routed defends organizations against DDoS attacks by redirecting network traffic through Akamai scrubbing centers and only allowing the clean traffic forward. Experts in the Akamai Security Operations Command Center (SOCC) tailor proactive mitigation controls to detect and stop attacks instantly, and conduct live analysis of the remaining traffic to determine further mitigation as needed. DDoS attack events are detected either by the SOCC or the targeted organization itself, depending on the chosen deployment model – always-on or on-demand – but the SOCC records data for all attacks mitigated. Similar to web application traffic, the source is determined by the source of the IP traffic prior to Akamai's network.

This data covered a 12-month period – July 1, 2019, to June 30, 2020.

Playing the Game

Credential Abuse

Credential abuse attempts were identified as unsuccessful login attempts for accounts using an email address as a username. We use two algorithms to distinguish between abuse attempts and real users who can't type. 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 evasion examples.

This data was also drawn from the CSI repository.

DreamHack Survey

Surveys are tricky; they are a request for opinions on a topic, and the plural of opinion is not data. When designing a survey, one must be mindful of how the design and execution might bias the response data. Recognizing the biases inherent in your questions is crucial when targeting a specific population, like gamers.

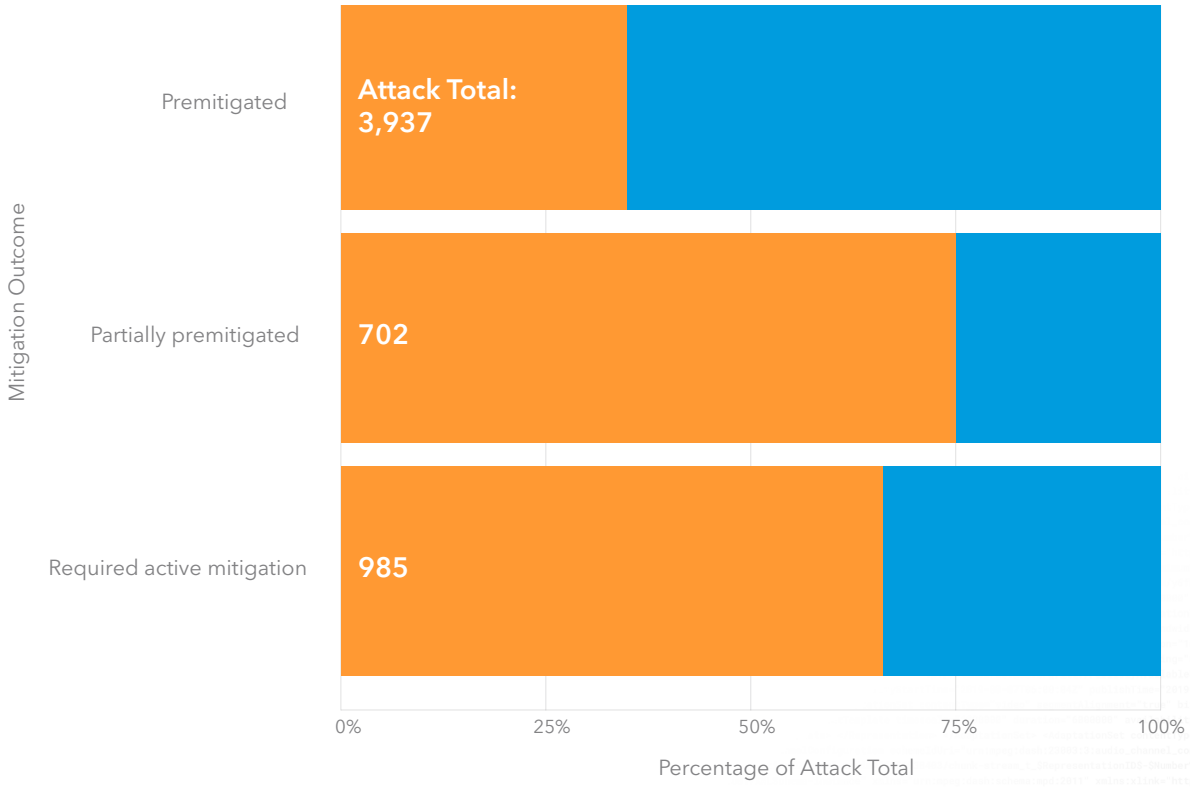
The DreamHack/Akamai survey targeted gamers by promoting it on their social media and offering respondents a chance to win a 1,000 Swedish kronor (SEK) Steam gift card. While the survey was open to anyone with the proper link, those in Sweden were more likely to be motivated by the incentive and are assumed to account for the majority of the respondents. More than 1,200 gamers responded to the survey, and although we do not believe this accurately represents all gamers, it is a good snapshot of a significant sample of gamers.

The survey was available from April 16 to May 31, 2020.

Appendix

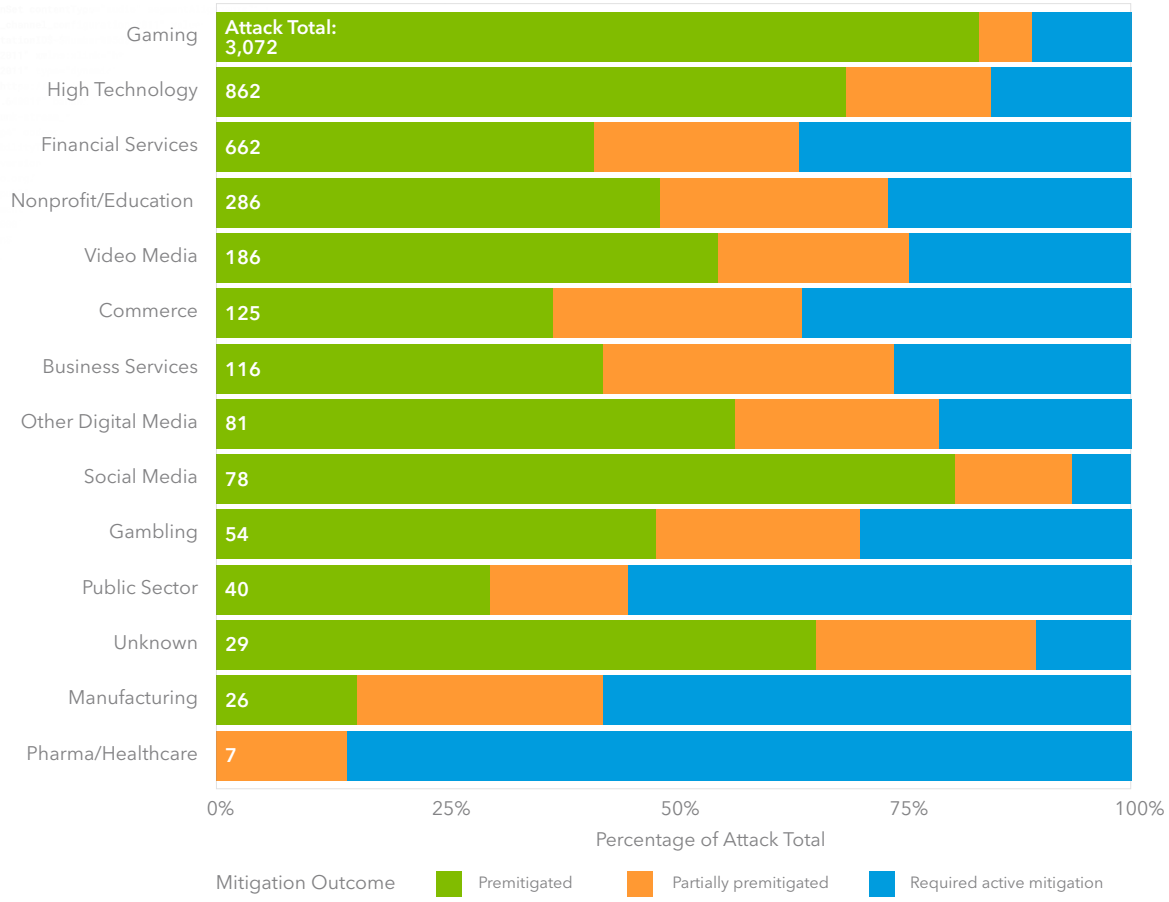
DDoS Attacks Events by Mitigation Outcome, Gaming vs. Other

July 2019 – June 2020



DDoS Attacks Events by Vertical and Mitigation Outcome

July 2019 – June 2020



Top Source Areas for Web Application Attacks Against All Verticals – Asia Pacific

July 2018 – June 2020

SOURCE AREA	ATTACK TOTAL	GLOBAL RANK
China	460,914,627	4
India	356,046,674	6
Thailand	177,934,268	12
Singapore	143,436,266	16
Indonesia	134,356,852	17
Japan	109,610,415	19
Hong Kong SAR	90,727,016	22
Vietnam	88,634,484	23
Taiwan	84,014,121	24
South Korea	58,412,763	28

Top Source Areas for Web Application Attacks Against All Verticals – Americas

July 2018 – June 2020

SOURCE AREA	ATTACK TOTAL	GLOBAL RANK
United States	2,435,701,993	1
Belize	302,937,328	7
Brazil	260,210,075	9
Panama	210,844,120	11
Canada	144,807,266	15
Mexico	37,856,641	36
Argentina	36,564,348	37
Colombia	24,291,358	45
Venezuela	23,304,334	46
Chile	14,918,952	55

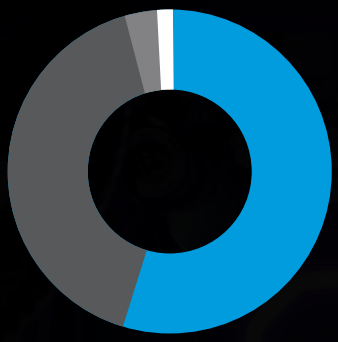
Top Source Areas for Web Application Attacks Against All Verticals – EMEA

July 2018 – June 2020

SOURCE AREA	ATTACK TOTAL	GLOBAL RANK
Russia	1,611,382,489	2
Netherlands	999,514,976	3
Ukraine	362,284,152	5
Germany	273,444,936	8
Ireland	257,264,198	10
United Kingdom	169,171,768	13
France	163,122,139	14
Romania	114,689,010	18
Turkey	105,874,601	21
Israel	64,392,342	26

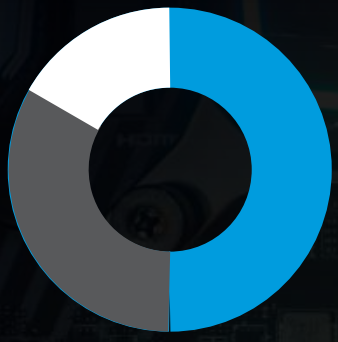
Survey Responses

Have you had any of your gaming accounts hacked/hijacked?



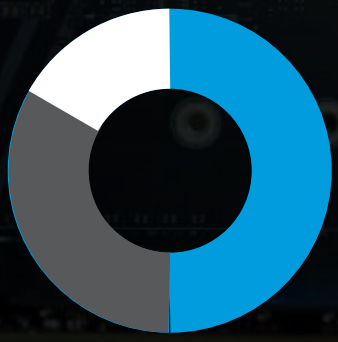
- **Yes:** 51.8 % (649 respondents)
- **No:** 41.7 % (522 resp.)
- **Maybe, but I don't know:** 5.8% (72 resp.)
- **I don't know:** 0.7% (9 resp.)

How worried are the players about accounts being hijacked?



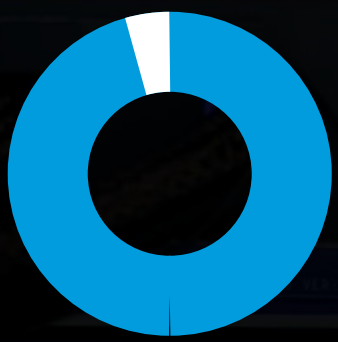
All players

- **Not thought about it / not worried:** 50% (632)
- **Neutral:** 32% (398)
- **Worried / very worried:** 18% (222)



Frequent players (daily + several times a day – 1,018 people)

- **Not thought about it / not worried:** 48% (485)
- **Neutral:** 32% (330)
- **Worried / very worried:** 20% (203)

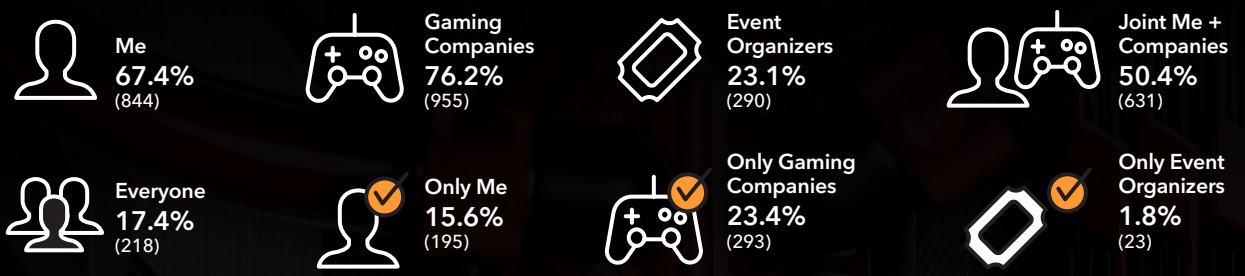


Non-frequent players

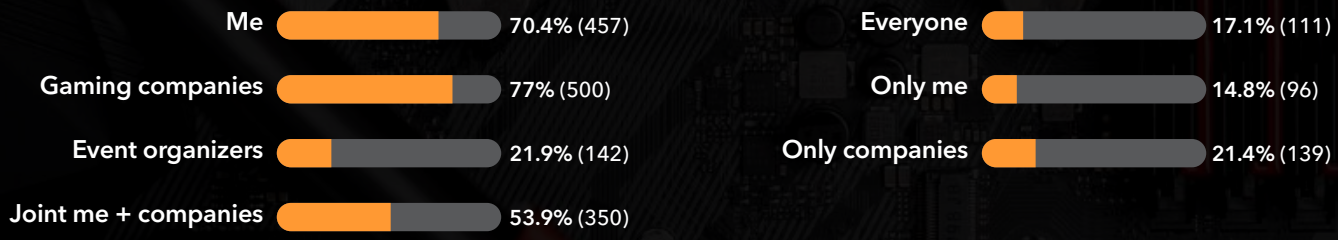
- **Not worried / neutral:** 92%
- **Worried / very worried:** 8%

What are you most worried about losing if your account is hacked?

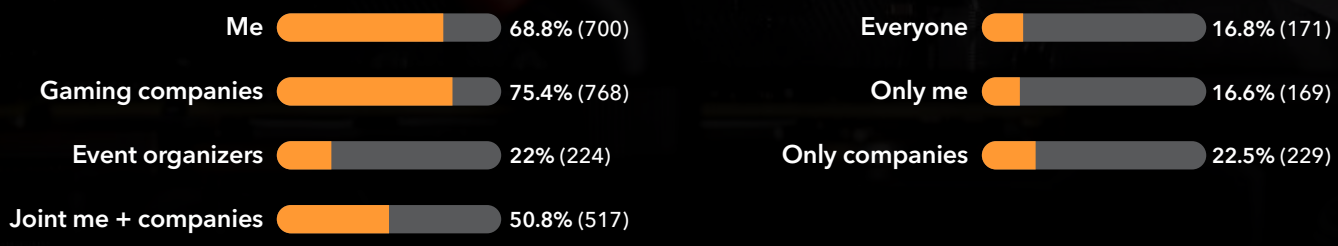
Who should be responsible for cybersecurity in gaming?



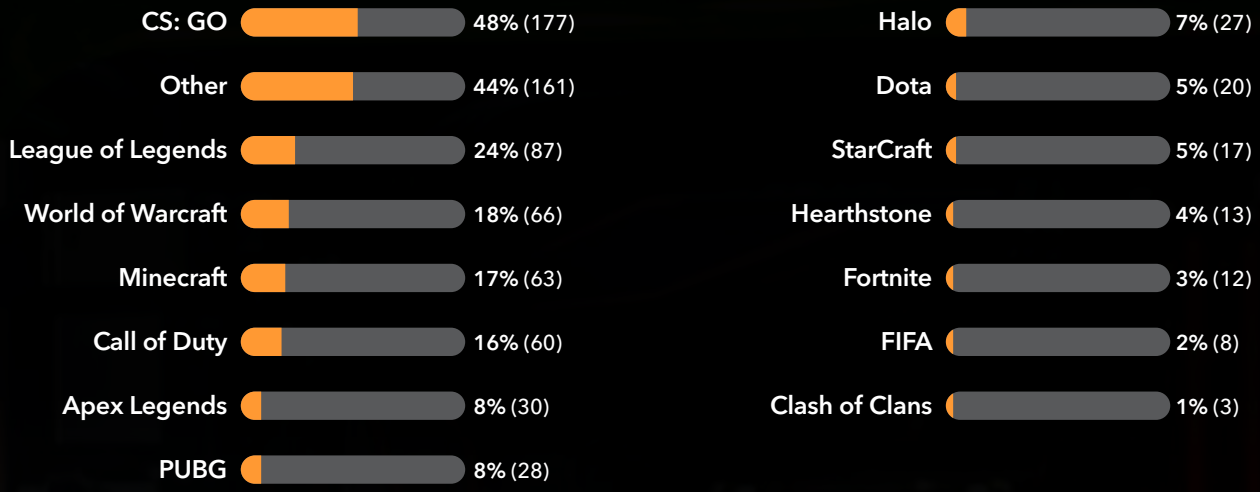
Among those who have been hacked in the past...(649)



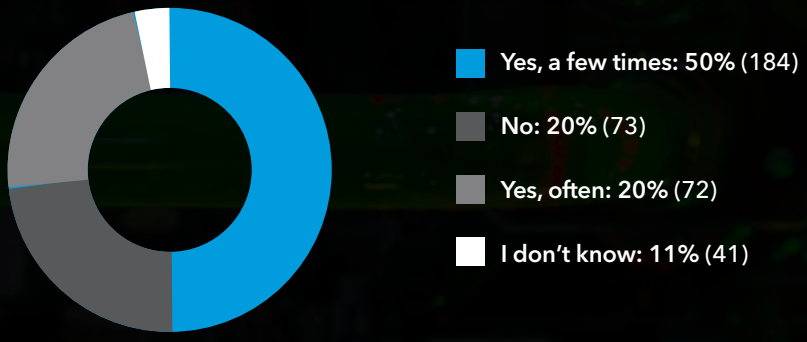
Among frequent players...(1,018)



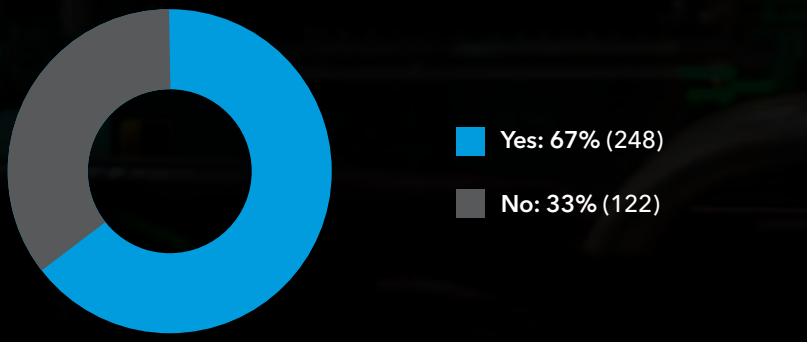
What is your favorite game?



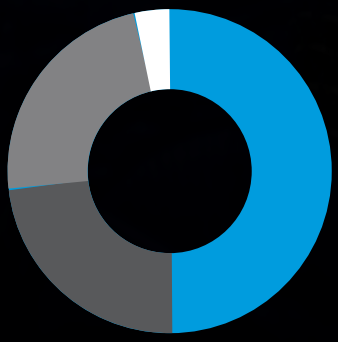
Have you come across hacked accounts / in-game assets being sold or traded online?



Have you experienced in-game phishing attempts (e.g., private message requests for credential verification)



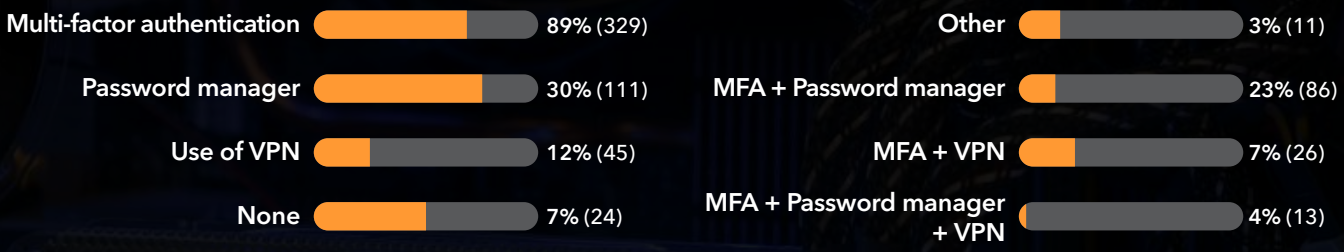
What is your opinion on hacked accounts and assets being sold on the black market? (scale 1–5)



- ① **I don't care:** 2% (8)
- ② 2% (8)
- ③ 5% (19)
- ④ 20% (73)
- ⑤ **Horrible—it should be stopped:** 71% (262)

91% of respondents think hacked accounts and assets being sold on the black market is bad, and 71% think it should be stopped

What measures do you take to keep your gaming accounts secure? (multiple answer)



Credits

State of the Internet / Security Contributors

Editorial Staff

Martin McKeay
Editorial Director

Amanda Goedde
Senior Technical Writer, Managing Editor

Steve Ragan
Senior Technical Writer, Editor

Lydia LaSeur
Data Scientist

Chelsea Tuttle
Data Scientist

Marketing

Georgina Morales Hampe
Project Management, Creative

Murali Venukumar
Program Management, Marketing

Special Thanks

Elisabeth Bitsch-Christensen
Field Marketing Manager

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 09/20.