

Gaming Respawned

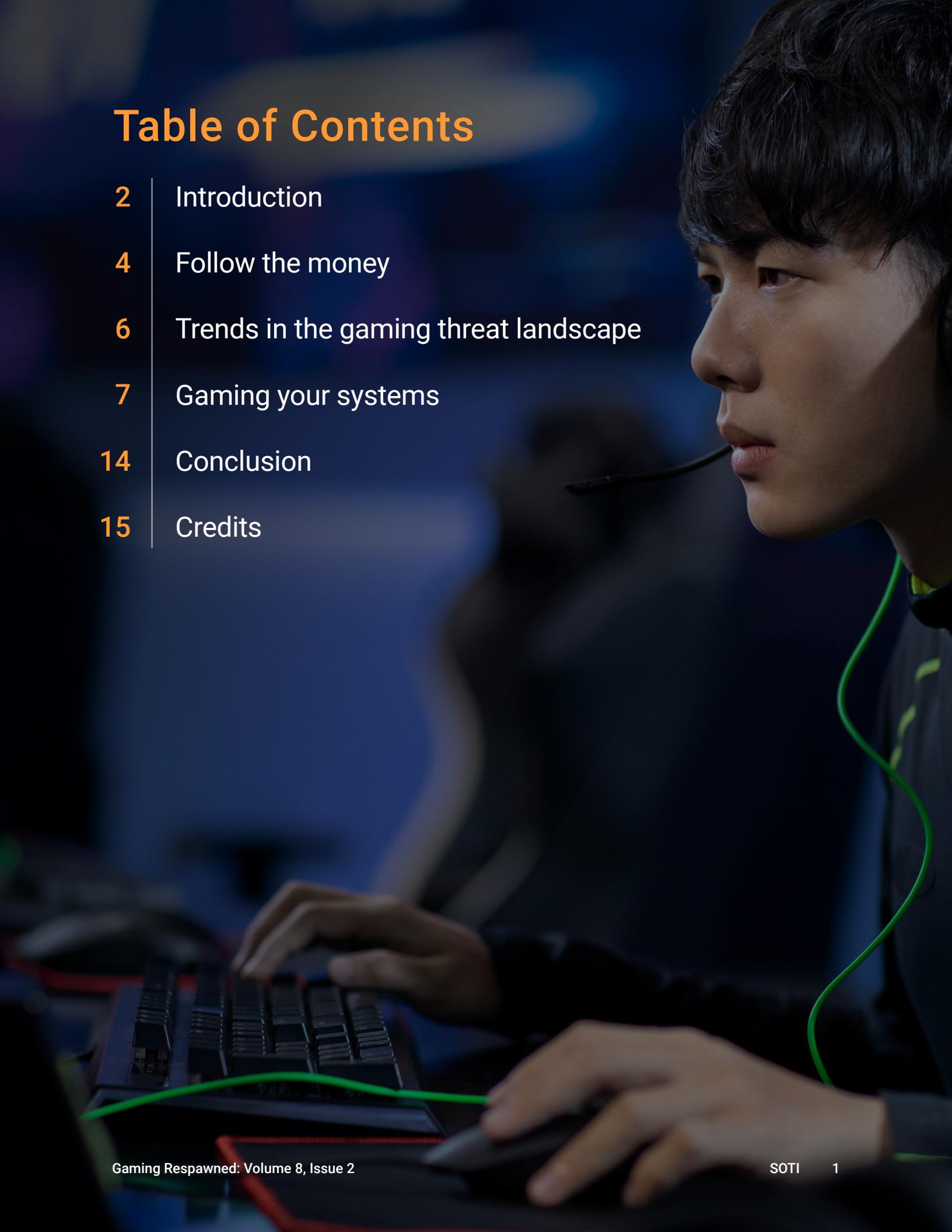
Cyberattacks on Players and Gaming Companies Rise Again

Volume 8, Issue 2

[State of the Internet]



Table of Contents

- 
- A close-up, low-angle shot of a young man's face and hands as he plays a video game. He is wearing a black headset with a microphone. His hands are on a black keyboard and a black mouse. A green cable from the mouse is visible in the foreground. The background is dark and out of focus.
- 2 Introduction
 - 4 Follow the money
 - 6 Trends in the gaming threat landscape
 - 7 Gaming your systems
 - 14 Conclusion
 - 15 Credits

Introduction

Welcome to the State of the Internet – Gaming Respawned. In a previous edition, we looked at attacks and trends in the gaming industry during 2020, the first year of lockdowns during the global COVID-19 outbreak. As isolation due to government mandates – as well as commonsense worries about catching the virus – deprived many people of creative outlets and ways to maintain human connections, gaming helped to fill the gap. According to a [study](#) by Streamlabs and Stream Hatchet, Twitch – the world's leading live-streaming platform for gamers – saw an 83% year-on-year increase in viewership when the pandemic hit. Many gaming companies adapted to the increased demand, and thanks to improvements in cloud-based gaming, their players can now stream games on TVs, PCs, and phones, something that was only wishful thinking 15 to 20 years ago. This cross-platform progression means people are playing more games on more devices.

The gaming industry has attracted cybercriminals almost since its inception. And the sudden boom in gaming during the pandemic was not lost on global threat actors. In 2021, attacks on the gaming industry more than doubled over the prior year.

Our previous State of the Internet (SOTI) report, [Gaming in a Pandemic](#), also detailed cybercriminals' preferred attack methods and looked at the rise in phishing-as-a-service kits, which attempt to dupe gamers out of their money or confidential information. Many of those tools remain top threats in gaming today. As Gartner recently explained in a report about the overall [2022 threat landscape](#), bad actors targeting all verticals continue to rely on tried-and-true exploits, such as phishing and ransomware.

So, as the world attempts to return to normal, or perhaps to some new normal, this SOTI report looks at the current state of online gaming. It also examines the most pervasive threats coming from online criminals. And to fully explore the topic of attacks on gaming, we dig deeper into the data around web application and API attacks, Distributed Denial of Service (DDoS) trends, the overarching goals of attackers, and more. This report also explores the threat landscape that has grown out of the pandemic in the gaming industry. And, of course, it looks at the impact of cyberattacks on gaming companies.

TL;DR

-  As detailed in the previous SOTI gaming report, COVID-related lockdowns and social distancing resulted in a major increase in gaming.
-  Now, as many countries emerge from the pandemic, the data shows no sign of this trend slowing – e.g., Akamai managed a peak traffic record of 250 Tbps in April 2022, with game downloads being one of the primary traffic drivers.
-  After refining the technology over many years, gaming companies are growing their investment in cloud-based gaming, which will represent an expansion of gaming companies' attack surfaces.
-  Concurrently, cyberattacks on player accounts and gaming companies increased dramatically in the past year, with web application attacks growing by 167%.

 The value in games continues to grow and to attract cybercriminals, cheaters, money launderers, and other bad actors.

 In the second year of the pandemic, web application and API attacks represented the largest category of attacks overall, and they have increased in volume.

 The top three web application attacks were LFI (38%), SQLi (34%), and XSS (24%).

 DDoS attacks against the gaming industry remain a major threat, and have grown by 5% since the previous year.

 Gaming remains the industry most hit by DDoS attacks, accounting for 37% of all DDoS traffic observed globally, nearly twice that of the second-most DDoS-attacked vertical – financial services.

Follow the money

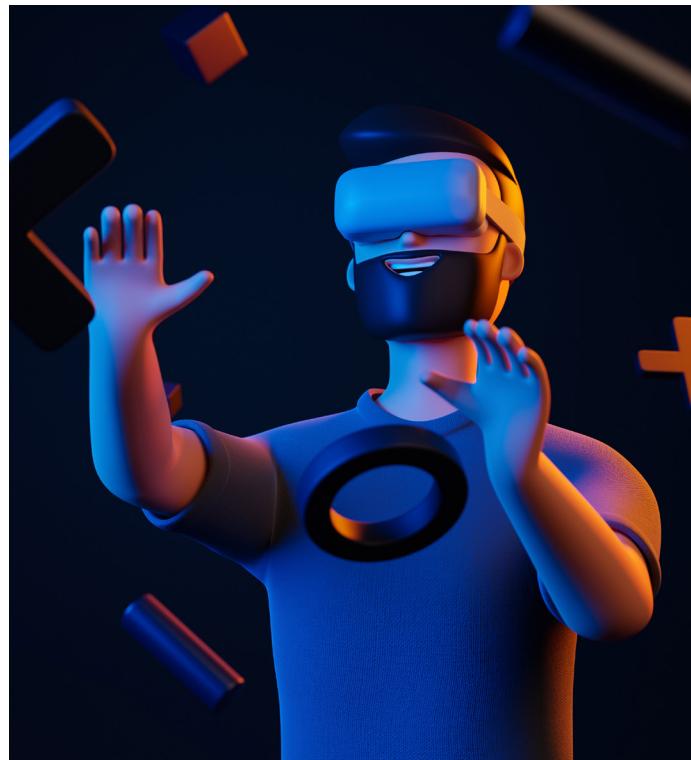
Whether the pandemic has ended is a subject of debate, but cybercriminals have not ended their focus on gaming platforms, players, and organizations. This comes as no surprise since gamers tend to stay connected online to one another and with the world at large. More important, criminals target gamers because they're inclined to spend money on the things that they love.

As the saying goes, if you want to know who online criminals target: "Follow the money."

For example, in addition to the cost of the games themselves, gamers spend liberally on things like tool and character upgrades. This is the highly lucrative world of microtransactions. Between July and September 2020, Activision Blizzard, for example, raked in \$1.5 billion from microtransactions alone. And the growth of gamers' spending on virtual stuff shows no sign of abating. According to a [report](#) from The Business Research Company, the online microtransaction market is expected to reach \$106.02 billion in 2026 at a CAGR of 11.9%.

Another sign of gamers' spending power is the support that they provide to other gamers, developers, and charities. For instance, in 2021, Awesome Games Done Quick raised \$2.7 million for a cancer charity, followed by another \$3.4 million for the same charity in 2022. And this represents just the money raised via one event; it does not include the money raised for various causes by individual gamers, streamers, or participants in local and regional events.

To an attacker, gamers represent value. If they can hack into user accounts, bad actors can steal everything from in-game currencies and assets to account information, and then sell the loot on the dark web. Or, they can steal a whole account, along with the time a gamer had invested in creating a game experience. Then, they can rename the account and sell it. Additionally, if hackers can breach a gaming company, they can wreak all sorts of havoc – from stealing the source code and engineering cheats that make the game unfair to extorting companies by encrypting systems or publicly exposing exfiltrated data.



Governments have also become concerned with a growing illicit use of the huge flows of real and fiat funds in gaming: putting dirty money in and getting clean money out. The fungible nature of in-game virtual currencies and assets attracts criminals of all sorts – from international drug gangs to human traffickers – who need to launder their ill-gotten gains. ACAMS, the largest international organization for anti-financial crime professionals, recently reported on [how it works](#). Criminals sign up for a game, create a profile, and then use the proceeds of their illegal activities or stolen credit cards to purchase as much in-game currency or as many accessories as they can, and then sell their account at a discounted rate to a second actor/victim, receiving clean money in return.

Microtransactions [further attract criminals](#) because many small transactions can more easily fly under the radar of the Internal Revenue Service and the U.S. Treasury by not triggering dollar-amount [thresholds](#) (generally \$10,000).

The growth of other digital assets, such as cryptocurrencies, and their abuse by criminals or terrorist groups who need to launder funds has put this type of activity on the front burners of regulators around the world. The current dramatic increase in anti-money laundering (AML) compliance scrutiny and hefty sanctions tends to focus on online gambling and cryptocurrency trading. Nonetheless, governments and the Paris-based [Financial Action Task Force](#) (FATF), often referred to by its French name, Groupe d'action financière (GAFI) , which sets global standards for AML, also have virtual worlds in their sights. The fines levied by regulators – such the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) and the U.S Justice Department's Financial Action Task Force – for noncompliance with AML laws can reach as much as \$100,000 per day.

Therefore, it would seem prudent for gaming companies to keep the risks of allowing their products to be used for money laundering on their radar.

Trends in the gaming threat landscape

In this report, we also look at some major trends impacting the online gaming threat landscape. First, the beginning of the end of the pandemic does not seem to have spelled an end of the boom in gaming. Since the start of the pandemic, Akamai has recorded an increase of 150% in traffic peaks, culminating in April of this year when we experienced 250 Tbps of traffic related to gaming downloads. The influx of new users, as well as existing users who continue to spend money on games, makes the gaming industry an even more lucrative target for cybercriminals. Second, as gaming moves to new streaming models and devices, the overall attack surface increases, which also means new cybersecurity risks for gaming companies and players. For example, Akamai research found that in the past year web application and API attacks on gaming companies spiked dramatically.

Will criminals find a silver lining in cloud gaming?

In the past several years, and certainly during the pandemic, gaming companies have grown their cloud-based gaming infrastructure. Cloud gaming generally offers an affordable alternative for consumers because it does away with the need to purchase physical consoles or PCs powerful enough to play games. In fact, earlier this year, Samsung announced it has partnered with Microsoft to bring cloud gaming to Samsung 2022 smart TVs.

Numbers from industry analysts further reveal this rush to the cloud. According to [Allied Market Research](#), the cloud gaming market reached \$244 million in 2020 and is expected to reach nearly \$21.54 billion by 2030.

For consumers, the lure of the cloud includes the ability to pick from a wide range of titles. For one low monthly fee, they can access these games from the cloud and play them virtually anywhere. The success of cloud gaming is evidenced by the growing number of gaming companies offering “pass” systems. This model allows users to play several titles on consoles or PCs – without worrying about device limitations or the rush to buy the latest generation of hardware.

In fact, [research from Newzoo](#) shows that, as many of the world's most well-known platforms and developers shift to this emerging dynamic, the cloud gaming ecosystem is quickly exploding. This growing popularity of the cloud reinforces the fact that today's gamers want to be mobile, have choices and options, and enjoy resiliency.

What all this means for security is an expanded attack surface for threat actors to exploit by using everything from DDoS to SQL Injection (SQLi) attacks.

Gaming your systems: Bad actors have been busy since the pandemic shutdowns

Now, as we begin to exit an unprecedented environment caused by an historic public health crisis, let's look at the ramifications of more spend and an expanded attack surface for gaming. The gaming industry now finds itself faced with a major bump in cyberattacks. Mostly, these comprise the same laundry list of attacks as those impacting other enterprises: web application and API, ransomware, and DDoS.

Among web application and API attacks, from the massive amounts of threat data Akamai collects every day, we are observing three [major patterns](#):

- 1 Long-running attack campaigns** – This describes the pattern when organizations get attacked often and consistently.
- 2 Short-burst attack campaigns** – These involve bursts of activity in which the daily attack volumes run 10 to 30 times above their 2022 average and tend to cluster over a few days. These bursts are difficult to predict; i.e., they seem to come out of nowhere and go away as quickly as they came.
- 3 One-time attack campaigns** – These comprise the big booms in which volumes of web application and API attack activity go way beyond – more than 30 times – what we normally see.

Web application attacks: When the game is the end game

Across industries, web application attacks are the 800-pound gorilla in the security operations center, accounting for more than [half of all data breaches](#). And in the past year (May 2021 – April 2022), web application and API attacks on the gaming industry have grown by 167% compared with the year prior. Gaming companies are by no means immune to these exploits. With its global threat detection network, Akamai sees millions of web applications attacks every day. During the period between May 2021 and April 2022, Akamai tracked 821,648,208 web application attacks in the gaming industry (Figure 1).

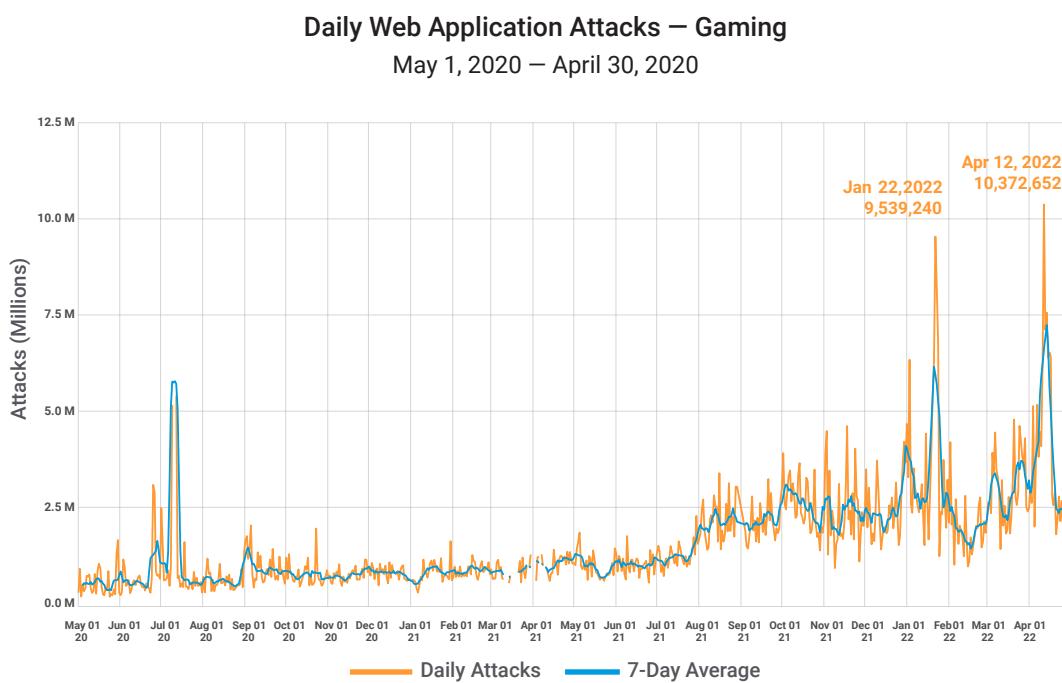


Fig. 1: Daily web application attacks targeting gaming

Whether hackers want to access gems in user accounts or the crown jewels of game companies themselves, web application and API attacks represent the main threat vector. For example, cybercriminals use exploits such as SQLi to penetrate back-end databases. Once inside, they can, for example, steal source code and use it to engineer cheats. Local File Inclusion (LFI) attacks look to exploit scripts running on the servers to attack stored data. This includes player and game details, which can be used for exploiting or cheating. Hackers can use the access gained from these types of attacks to manipulate in-game economies to beat the odds in real-money gaming scenarios.

Akamai researchers have analyzed web application and API attacks over the past year and have seen a threefold uptick in Q1 2022 versus Q1 2021. In particular, LFI attacks have seen a massive increase, making them the most prevalent web attack vector. Since January 2021, the top three web application attack vectors targeting gaming were, in order, LFI at 38%, SQLi at 34%, and Cross-Site Scripting (XSS) at 24% (Figure 2).

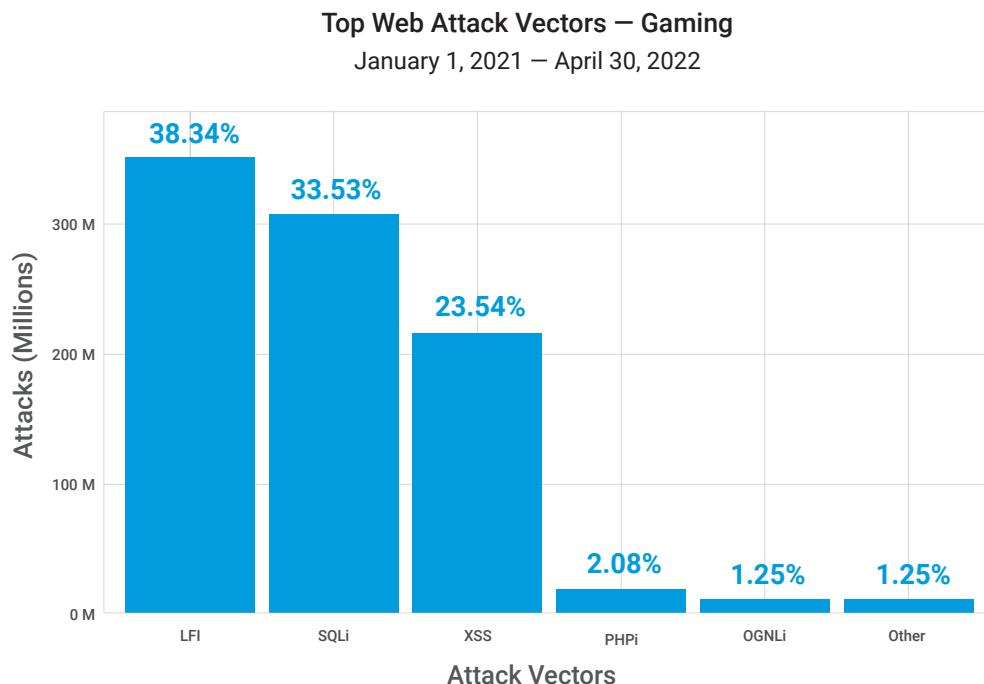


Fig. 2: The top web application attack vectors targeting gaming

Akamai data shows the frequency of web application attacks grew dramatically, essentially doubling, as countries began to emerge from the pandemic. The unusual rise of these attacks, we believe, betrays a massive increase in organized criminal activity. But what does this mean for the games business? 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. So, this represents another way for criminals to control player accounts. Training videos on how to hack video game accounts – in which SQLi attacks are used to source login data, which is then used as part of a credential stuffing attack – are commonly shared by criminals.

LFI attacks attempt to exploit scripts running on servers to attack stored data. This can include player and game details, which criminals can use for exploiting or cheating. Given the right access, they might also be able to use this type of attack to gain further access into the networks of gaming companies.

Mobile games and web-based games represent major 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 resides on the server.

Finally, according to our data, attacks focus on companies in the United States, Switzerland, India, Japan, and the United Kingdom. This comes as no surprise as many countries on this list are home to some of the largest gaming communities in the world.



Top Target Areas for Web Application Attacks – Gaming (May 1, 2021–April 30, 2022)

- | | |
|------------------|-------------------|
| 1. United States | 5. United Kingdom |
| 2. Switzerland | 6. Poland |
| 3. India | 7. Singapore |
| 4. Japan | 8. South Korea |



DDoS attacks

The majority of gaming security professionals are well familiar with DDoS attacks. Attackers use bot armies or other automated techniques to overwhelm servers with requests. They can completely knock infrastructure offline or make web infrastructure slow to a crawl, impacting business operations and game performance. They raise customer support costs and reduce customer satisfaction when it ruins gameplay. DDoS attacks increased by nearly 5% in 2021. DDoS attacks against the gaming industry accounted for 37% of the DDoS traffic observed across all verticals (Figure 3).

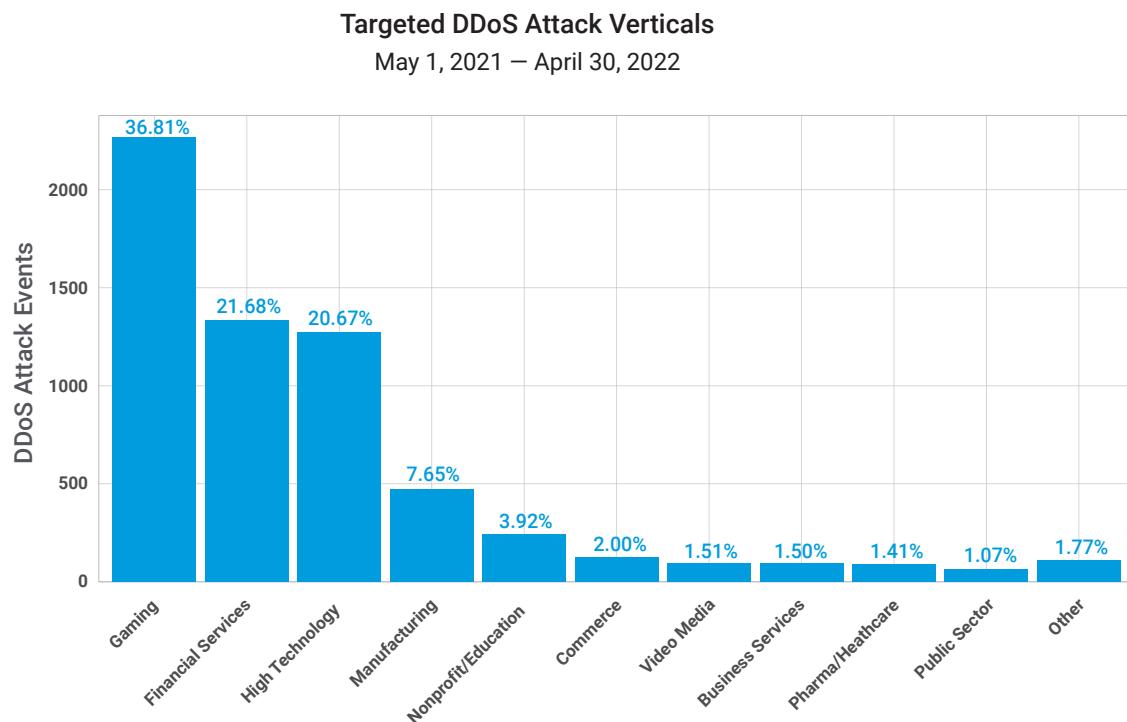


Fig. 3: Targeted DDoS attack verticals

What's more, over the past year, DDoS attacks have become larger and more sophisticated, and the gaming industry is a prime target (Figure 4). Volumetric attacks, for instance, can take games offline and affect thousands of players in a matter of seconds. Or they can be more targeted, increasing latency just enough to give one player an advantage over others. Game companies cannot afford to ignore this threat because it can have enormous impacts on the business.

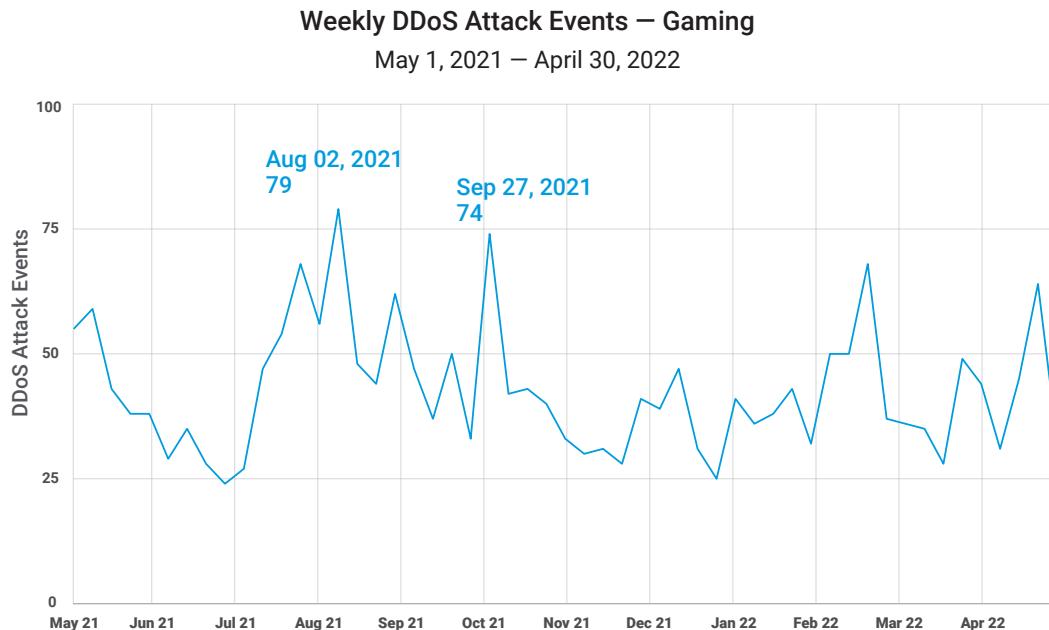


Fig. 4: Weekly DDoS attacks targeting gaming

DDoS attacks also come in several forms, and attackers often use more than one type to wreak havoc on their targets. The three key types are volumetric, protocol, and [application-layer attacks](#). The goal of all three involves severely slowing down or stopping legitimate traffic from reaching its intended destination. By making game resources unavailable or diminishing performance, DDoS can cause a gaming company's business to grind to a halt or, at minimum, increase support costs.

Ransomware

Although this report does not include data on ransomware attacks specifically in the gaming industry, ransomware has the potential to cause devastating business disruption across industries. According to Gartner's latest [Emerging Risks Report](#), the threat of "new ransomware models" ranked as the top concern faced by executives toward the end of last year.

Sophisticated new types of ransomware can even steal backups. And as more companies have opted to rebuild systems from backup as an alternative to paying ransom, criminals have devised new techniques, such as double extortion attacks. Basically, the malware exfiltrates data before encrypting it so attackers can demand ransom for not publishing the stolen data publicly. Imagine if a cyberextortionist published your gamers' financial data or one of your game's source code.

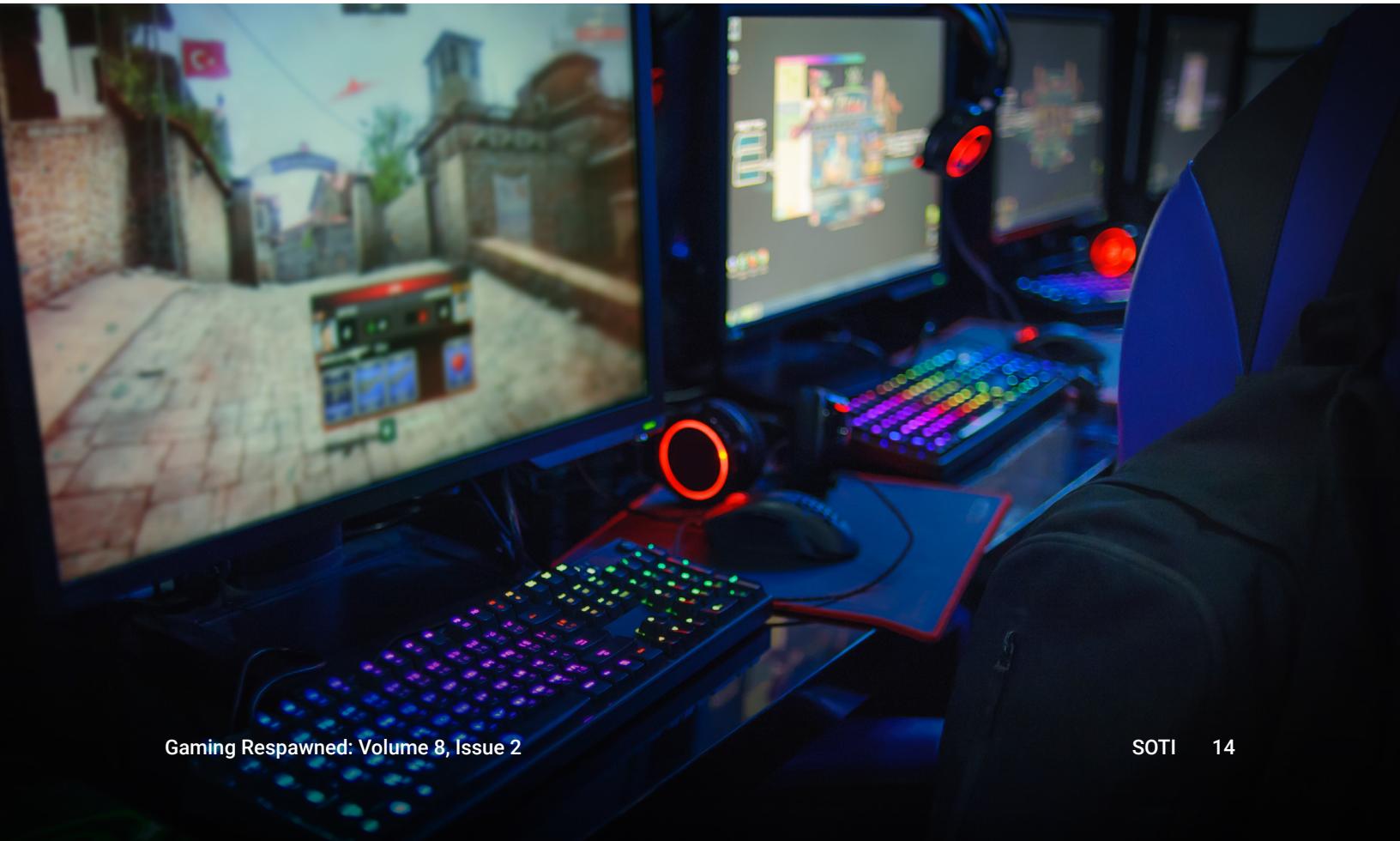
Akamai recommends game companies mitigate this risk by following best practices for preventing ransomware attacks, such as having a good backup strategy and educating users about phishing (a common way ransomware is dropped into networks). You should also consider deploying microsegmentation, which ringfences individual systems and thus helps prevent the malware from spreading laterally from one system to the next across your infrastructure.



Conclusion

Since our last report on threats in the gaming industry – and since what is hopefully the beginning of the end of the pandemic – Akamai threat researchers have observed some key trends. First, the lucrative gaming industry shows no signs of slowing down from the boost that shutdowns and social distancing gave to gaming. Second, cybercriminals have shown no sign of slowing their attacks on gamers and game platforms. Web application attacks have more than doubled over the last year, and the attacks comprise three key attack vectors: LFI, SQLi, and XSS. DDoS and ransomware also remain major threats.

On top of this, while the growth of cloud gaming seems to have a bright future, its expansion will also increase the game industry's overall attack surface. Plus, the growth of other lucrative aspects of the gaming industry will continue to attract bad actors. Microtransactions, for example, represent a huge draw for criminals who can capitalize on the spending power of gamers and the fungible nature of virtual assets. Basically, cybercriminals know there is value in gaming, and they will continue to invent ways of getting it or exploiting the flow of virtual funds.



Credits

Writing

Kevin Mitchell

Data analysis

Chelsea Tuttle

Subject matter experts

Eliad Kimhy Jonathan Singer

Tony Lauro

Production

Georgina Morales Hampe Shivangi Sahu

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/security-research

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 powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences – helping billions of people live, work, and play every day. With the world's most distributed compute platform – from cloud to edge – we make it easy for customers to develop and run applications, while we keep experiences closer to users and threats farther away. Learn more about Akamai's security, compute, and delivery solutions at akamai.com, and akamai.com/blog, or follow Akamai Technologies on [Twitter](#) and [LinkedIn](#). Published 08/22.