intertrust®

White Paper

ExpressPlay

The new perspective on securing eSports

Part 1

Surging success of eSports intensifies need for robust, affordable security

Contents

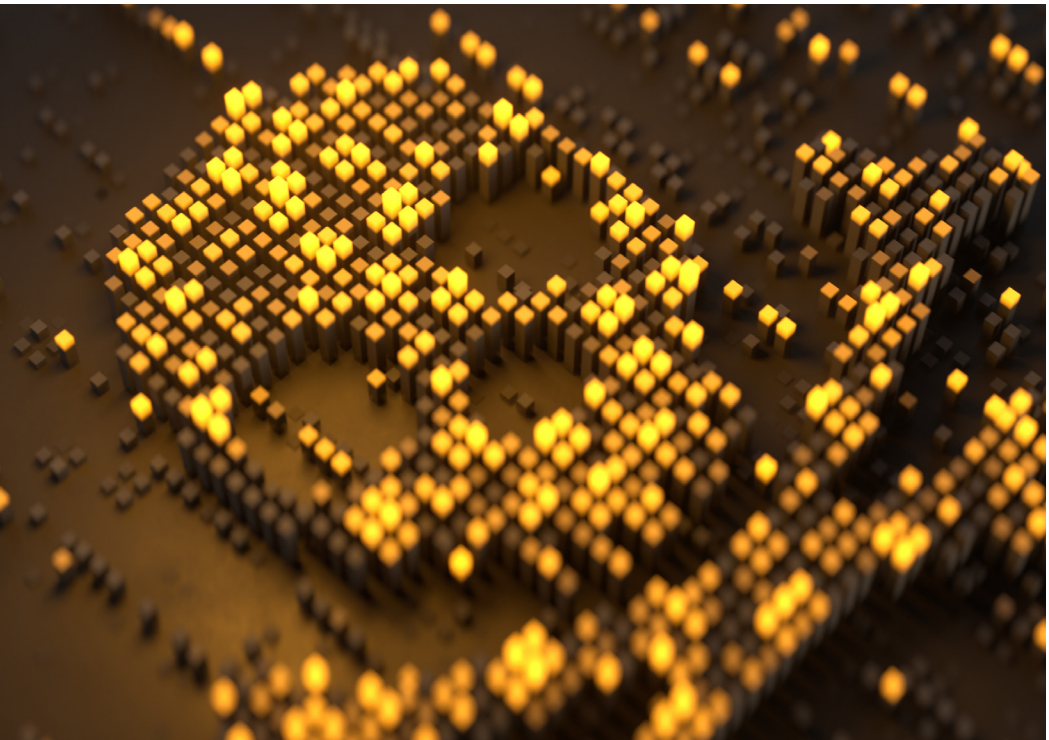
Introduction

The rapid rise of live-streamed eSports has triggered an equally rapid rise in the threats against business stability posed by hackers worldwide, leaving service providers no choice but to fight back.

With a fan base approaching a billion viewers across the globe, producers of eSports streaming services face the same security challenges confronting their counterparts in traditional online sports streaming. When live-streamed content gets to this level of popularity, strategists must take into account everything from the rampant professional and amateur modes of theft now siphoning billions of dollars out of live event revenue streams, to an onslaught of hackers exploiting app vulnerabilities for a vast array of nefarious ends.

Fortunately, eSports service providers, or anyone else mounting live streaming services, no longer must deal with the heavy lifting once required to meet these challenges. This is true whether the goal is to thwart the revenue-stealing activities of professional pirates, or to shield service apps against a multitude of attack vectors.

Part 1 of this two-part white paper series provides a comprehensive look at why security threats have risen to become a far greater challenge to the eSports industry than was once the case. In Part 2 readers will learn about the solutions that have emerged to make it easier to deal with these threats and with greater effectiveness than ever before.



The first half of this paper reviews the trends that are reshaping the eSports industry at warp speed and, in the process, raising its profile as a field of great interest to wrongdoers. Accelerating rates of consumer engagement, event virtualization, localized competition, diversity in monetization strategies, and rollouts of betting options and new eSports categories over the past two years have completely transformed these market dynamics.

In the second half, we begin by asking what all this means when it comes to judging the seriousness of security threats. First, we explore the scope and tactics employed in theft of live content and what these trends imply for the eSports sector. As shall be seen, there are many bases to cover relating not only to how pirates profit from offering stolen subscription-based content but also to how they benefit from garnering ad support for bundling free content into their service portfolios. Then, we look at the other side of the coin, namely, the threat to business models and users posed by exploitation of app vulnerabilities. Hackers leverage reverse-engineering and tampering techniques against service apps to steal intellectual property, fraudulently redirect payments, and hijack personal data for malicious purposes.

We also examine the threat posed to business models by inadvertent errors in production. As with any software component where thousands or millions of lines of code are involved, producers must be able to quickly identify and correct the inevitable errors that can wreak havoc on the performance of an eSports service app.

With a fan base approaching a billion viewers across the globe, producers of eSports streaming services face the same security challenges confronting their counterparts in traditional online sports streaming.

The new market dynamics in eSports

Like most sports, eSports is benefitting from the fact that people who love to play, love to watch competition among the best players.

According to a report on the global gaming market issued by Nielsen's SuperData group, 62% of viewers find it important to watch games they personally play, which bodes well for the eSports market as the overall gaming market continues to surge.[1]

In fact, as measured by revenue growth, the eSports market is exceeding the annual growth rate in revenues generated by game and console sales by a considerable margin, according to a comparison of statistics from several researchers (see Figure 1). Juniper Research predicts the global eSports audience will top 800 million by YE 2021 on its way to 1 billion by 2024.[2] No wonder Netflix has characterized eSports as a bigger competitor for viewership than any of its SVOD rivals.[3]

This is a passionate audience. In the U.S., 25% of gamers who watch eSports events tune in for more than four hours a week, according to Deloitte. Forbes reports that U.S. consumers in the 18-25 age group who play video games spend 77% more time watching others playing games than they do watching traditional sports.[9]

But eSports viewing isn't just a Gen Z/ Millennial, male-dominated phenomenon. Deloitte's report notes that more than 40% of U.S. Gen X gamers and nearly 30% of female gamers watch eSports weekly.

Figure 1
Comparing eSports growth to overall game market growth

Global Gaming Market			
2019	2020	2021	CAGR
$148.8B	$159.3B	$189.3B	8.36%

3 Global eSports Projections		CAGR
2018-2023[5]	$660M-$1.8B	18.3%
2018-2025[6]	$915.3M-$2.977B	18.35%
2021-2025[6]	$2.1B-$3.6B	10.76%

Source: Newzoo[4], PWC[5], Verified Market Research[6], Juniper Research[7]

The sea change in publisher strategies

It all adds up to the fact that a new entertainment sector built around current cultural realities is taking shape. Game producers and third-party distributors are tapping advanced networking, cloud resources, and sophisticated production technologies to blend game-playing, eSports fandom, the virtualization of social engagement, new approaches to monetization, and, in some cases, more traditional entertainment content in myriad ways that have yet to be fully defined.

Developments across multiple categories of entities seeking to capitalize on the eSports opportunity will determine where things go from here, driving increasingly dynamic trends in the staging, frequency and types of events and modes of monetization. Many of these developments have a direct bearing on the security questions under discussion here.

Game publishers, the linchpin to all this activity, began staging big eSports events as a way to boost and extend the popularity of their core products. But, with the massive success of eSports, many publishers now view that aspect of their businesses in a broader light where opportunities abound to create new revenue streams as well as to build ongoing gamer enthusiasm through regional and local amateur leagues, development of new types of content and features, and partnerships with traditional sports networks and leagues.

Shifting distribution agendas

So far, the eSports success of game publishers has been closely aligned with the surging fortunes of game streaming platform providers like Twitch, YouTube Gaming, and Facebook Gaming, who comprise the other big group of stakeholders in the evolving scenario. By alleviating the publishers of the distribution headaches, they became the primary go-to centers for viewers to find and stream eSports competitions of every description.

During Q1 2020, viewing time on Amazon's Twitch, the market leading platform, grew by 17% over the previous quarter to a record 3.1 billion hours with a 33% increase in the number of unique hosted channels, according to a StreamLabs report.[10] YouTube Gaming and Facebook Gaming, the second and third ranking platforms, also registered strong growth.

But publishers are beginning to look at these marriages of convenience with distributors as a lost revenue opportunity. As the streaming platforms continually add chat and other features along with ancillary content to make themselves ever more indispensable in this booming market, they're inspiring license holders to leverage their intellectual property to greater advantage by taking more control of the business and its monetization potential with instantiations of their own content distribution and streaming platforms.

Virtualization and regionalization of game play

The success of virtual competitions implemented out of necessity during the Covid-19 pandemic has become a game changer in eSports strategies. Rather than gathering in one place to compete and produce games, players and production personnel have been connected across vast regions via specialized streaming platforms that support interactions with close to real-time latencies at 200 milliseconds or less.

A key to this transition has been maturation of production platforms designed specifically to accommodate the unprecedented complexities of producing eSports. For example, whereas the Super Bowl, one of the biggest traditional sports productions, requires anywhere from 70 to 90 cameras, one live *Fortnite* competition involving 100 players can require more than 300 camera feeds that must be orchestrated second by second to keep online viewers abreast of the most significant player action.[11]

Now all this is done virtually via cloud orchestration of the input from cameras tracking dispersed players' actions.

While publishers are scheduling a return to venue-based competitions for big audiences wherever circumstances allow, the success of virtual events during the pandemic has led to adoption of hybrid approaches with live competitions interspersed among a steady flow of virtual events.

At the same time, the volume of live events is sure to increase with the likelihood that the more frequent regional play impelled by the pandemic "could well become a fixture," according to Newzoo. In fact, the researcher says, the shift by big game ecosystems away from major international events may also endure.

With the emergence of amateur leagues, publishers are rapidly building migration paths players can follow to reach the top pro tiers, mirroring the way traditional sports are organized. Following the trail blazed in 2018 by the launches of Activision Blizzard's Overwatch sports league and Riot Games' North American League Championship Series, ever more publishers are franchising their eSports brands to foster localized teams and venues for hierarchies of competition culminating in professional championships.

The success of virtual competitions implemented out of necessity during the Covid 19 pandemic has become a game changer in eSports strategies.

Major sports brands capitalize on eSports popularity

The expanding scope of eSports competition also includes virtual competitions tied to traditional professional sports brands. For example, simulated car races (sim racing), long a fixture in video gaming, began drawing millions of viewers when cancellation of traditional NASCAR and Formula 1 competitions brought top-ranked drivers into events like Formula 1's Virtual Grand Prix and the eNascar iRacing Pro Invitational Series.

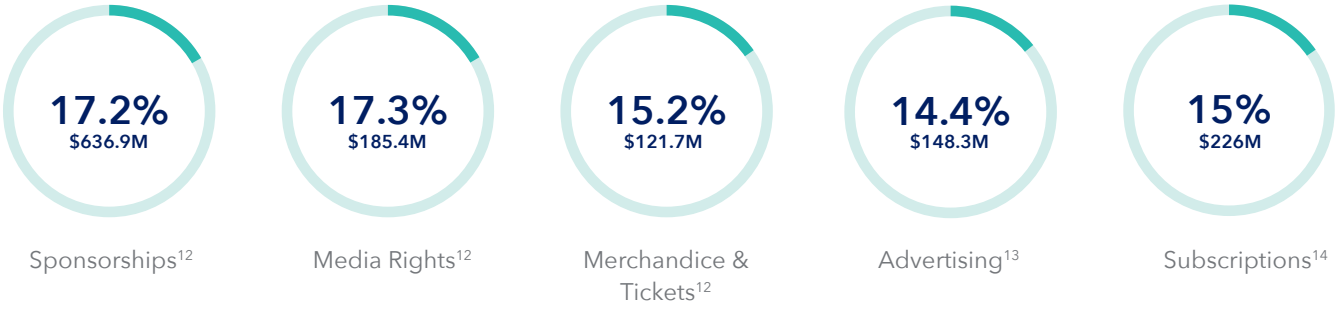
The 16-team NBA 2K20 eSports competition drew participation of NBA stars like Kevin Durant and Donovan Mitchell in 2020. Former NFL quarterback Michael Vick and other NFL pros joined in an eight-player Madden NFL20 tournament, marking another boost to the profile of eSports. Soccer, too, has been fueling the popularity of eSports competitions with participation of big-name players.

These developments have contributed to another phenomenon transforming the eSports market, which is coverage of game playing by major TV sports networks. Many of those high-profile competitions involving traditional sports stars were carried on TV, along with many other high-profile competitions from eSports leagues.

TV eSports programming, which began over 20 years ago in South Korea and spread worldwide over the past decade, continues to expand with gaming carried by networks like TBS, CBS, ABC, Fox Sports, NBC Sports Network, Disney XD, and ESPN in the U.S. and many others elsewhere. For example, in late 2020, German broadcaster Sport1 launched the pan-European eSports channel eSportsOne. It remains to be seen how eSports programming will impact TV lineups, but the expanding coverage makes clear the category is on big media's radar.

TV eSports programming, which began over 20 years ago in South Korea and spread worldwide over the past decade, continues to expand with gaming carried by networks like TBS, CBS, ABC, Fox Sports, NBC Sports Network, Disney XD, and ESPN in the U.S.

Figure 2
eSports revenue trends/ 2020 totals/YoY increase
Source: Newzoo[12], eMarketer[13], PWC[14]



New patterns in monetization

These strategic shifts in the eSports ecosystem are accompanied by changes in monetization patterns. By all accounts, sponsorship and media rights fees will remain the two largest pieces of the eSports revenue pie, but other categories will take increasingly larger shares as the overall revenue total continues to increase.

Researchers vary in their descriptions of eSports revenue categories. Figure 2 lists the 2020 revenue totals in the five major categories as reflected by disparate findings by three researchers, none of whom individually distinguish all five in their tabulations. Significantly, when it comes to developments bearing on eSports security requirements, Juniper Research, without publicly disclosing amounts, predicts subscription fees and advertising revenues will be the two biggest contributors to the 10.76% revenue CAGR it projects for 2021-2025, as shown in Figure 1.

By the measures reflected in Figure 2, advertising and subscription revenues constituted 28% of the combined $1.3 billion in 2020 revenue. There's nothing surprising about expectations that in the years ahead the ad total will track with the general growth of advertising in all types of streaming services. Digital TV Research predicts ad revenue generated by all types of OTT video services worldwide will grow 120% from 2019 to reach $43.2 billion by 2025.[15]

Of course, OTT subscription revenues, with a bigger share of the OTT total, are on the rise as well, albeit at a slower 103% increase to $97.5 billion by 2025, according to Digital TV Research. But a sharp rise in eSports subscription revenues marks a break with past trends when publishers were largely focused on sponsorships to fund live events while their distribution partners mostly relied on advertising.

Now, it seems, publishers' search for new returns on their investments in their own streaming platforms will inevitably lead to at least minimal subscription fee levels, often for premium versions of their services. After all, as noted by Deloitte, gamers, who increasingly rely on fee-based cloud services rather than hard copy purchases to access games, are already well adapted to paying for streaming services[16]. Indeed, as of 2019, 53% of millennials were paying for video gaming subscriptions while only 51% were subscribing to pay TV, which was a sudden reversal from the year before when the shares were 44% and 52%, respectively.

However, when it comes to the role of user payments in game playing and eSports, attempting straight-forward comparisons with traditional streaming service subscription fees can be misleading. For example, many of the most popular multiplayer action games are offered online at no cost but generate millions of dollars in revenue through sale of skins, weapons and other virtual artifacts used in the games.

While eSports offered on Twitch and other streaming platforms are free, channels devoted to specific streamers may not be. Streamer channel subscription fees, along with ad revenue sharing, have long been a component of service revenues generated through partner programs with Twitch and other eSports streaming platforms.

Twitch supports three tiers of pricing for such subscriptions, starting at $4.99 monthly (or less in low-income regions of the world), 50% of which goes to the streamer. Viewers are more than willing to pay such fees. Top-tier pro streamers putting in 40-hour weeks on their channels make $3,000-$5,000 monthly from subscription payments, according to a CNBC report.[17] They also take in about $250 per 100 subscribers from their share of monthly ad revenues.

Subscribers to a channel also get Twitch-supplied special perks as an incentive to subscribe. And while Twitch itself doesn't charge a basic service subscription fee, it does offer Twitch Turbo at $8.99 monthly, which allows users ad-free access, with some exceptions, to any channel on the platform, including music, video and gaming as well as eSports channels.[18]

Publishers can be expected to follow similarly complex pricing patterns as they introduce subscription fees. For example, Riot Games, publisher of League of Legends and producer of the game's eSports league competitions worldwide, introduced a $15 Pro View pass in 2019, since lowered to $9.99 in response to the pandemic. Pro View allows users to access personalized experiences, including unique camera views on individual players, which they can trigger through an on-screen timeline that allows them to skip around current and past action across the field of competition while eavesdropping on players' in-game chat messages.[19] Riot's strategy points to the types of bells and whistles like multi-camera views that publishers can implement as value-adds through management of their own streaming platforms.

The emerging security threat landscape in eSports

Any assessment of the security requirements that attend eSports' emergence as a major networked entertainment category must take into account a broader scope of vulnerabilities than once was the case.

eSports producers now face the same spectrum of threats that are menacing every other high-value segment of the streaming ecosystem. Moreover, the long-standing cheating threat unique to eSports has grown far more serious at both the professional and amateur levels of competition.

The lines of assault on eSports broadly divide into two realms of illegal activity: professional pirates' efforts to generate illicit revenues through unauthorized streaming of eSports content, and hackers' disruptions of business and the wellbeing of players and users through exploitation of vulnerabilities in service apps. Of course, all entities who depend on the internet no matter what business they're in face the scourge of denial-of-service (DDoS) attacks, credential stuffing, ransomware, SQL injection, malicious botnets, and other tactics roiling cyberspace. That said, here our focus is on the attack vectors and remedies that are more specific to the streaming media space generally, and eSports in particular.

Streaming piracy—a fast-growing threat to eSports providers

Online video service piracy is often associated with theft of premium subscription content. Pirates employ a variety of approaches to making money, including free offerings supported by advertising; packaged service bundles mimicking legitimate services at cut-rate prices; cheap pay-per-view options, and sales of illegal hardware modules typically using open-source Kodi software to stream stolen content to TV sets and other devices.

Advertisers have the tools to identify and act against these placements but typically choose not to, because they're getting exposure to a lot of viewers they otherwise wouldn't reach.

Pirates also benefit from malware embedded with streamed content. According to research conducted by KU Leuven University in Belgium and Stony Brook University in New York, most live sports content streamed by pirates is infected by malware, some of it aimed at defeating ad blocks to ensure they can collect from ad network placements.[20] Other malware elements are used to copy graphics and other features from legal sites.

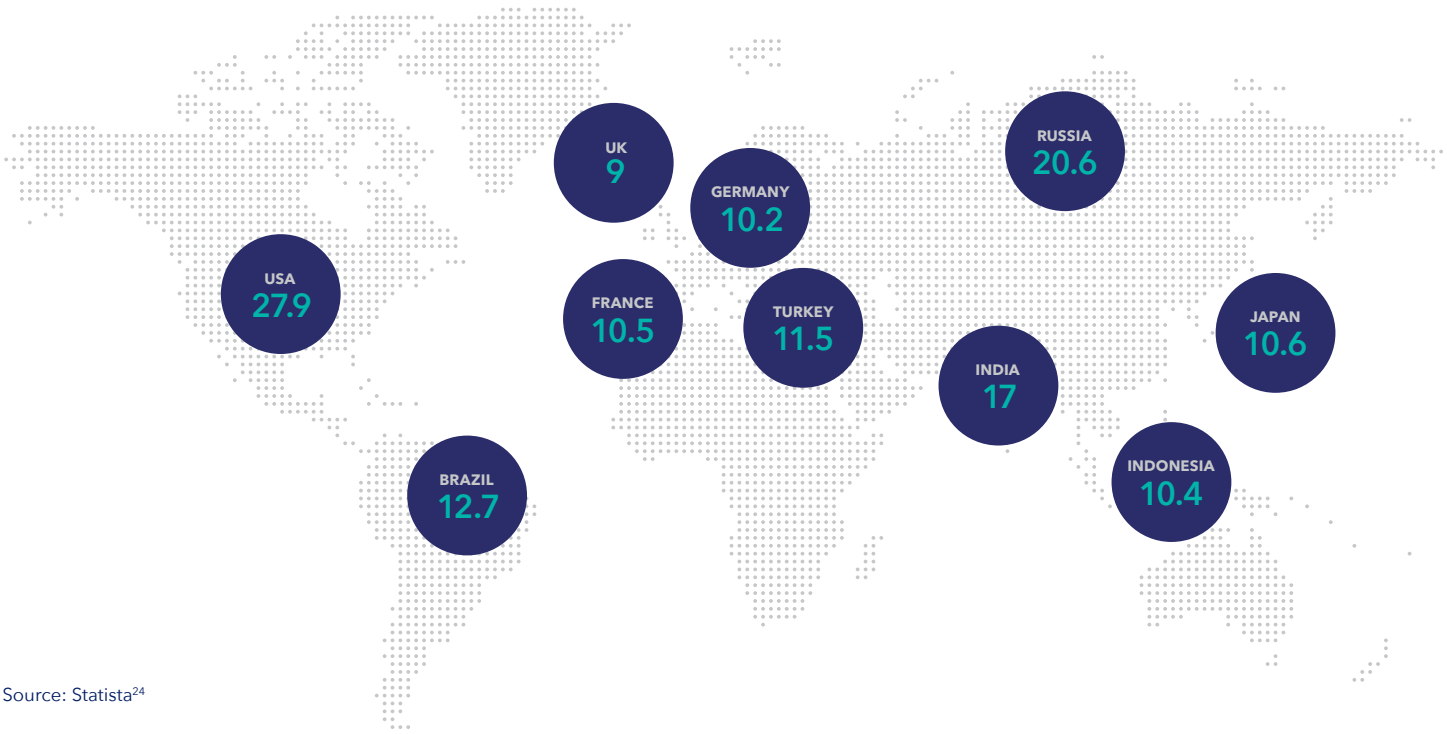
Certainly, as eSports providers introduce subscription fees to drive revenues as discussed in Chapter 1, the popularity of those services will make them as susceptible to piracy as other types of high-value services. But pirates also steal free advertising-supported services, restreaming them from their sites where little is done by advertisers to thwart their ad placements with stolen content.

White Bullet Solutions, a provider of illicit ad detection services, has found that advertising promoting legitimate and often well-known brands comprises 96% of all advertising on illegal sports streaming sites[21]. Advertisers have the tools to identify and act against these placements but typically choose not to, because they're getting exposure to a lot of viewers they otherwise wouldn't reach.

User complicity

Of course, there would be no piracy without consumers willing to view stolen content. As detailed in Figure 3, there's a ready audience throughout the world for any live-streamed content that comes through the pirate channels people rely on to find programming at little or no cost. In a 10-country survey of over 6,000 sports fans, Ampere Analysis recently found that over 51% are watching content from pirate services at least once a month[22]. In the U.S. 20% of broadband households report they use a piracy device, app or website, according to Parks Associates.

Figure 3
Media piracy site visits by country/ billions of visits in 2018



Source: Statista[24]

A good reference point for the impact piracy could have on the eSports business is the toll illicit streaming is taking on live-streamed sports. According to another Ampere Analysis study, illegal OTT sports streaming worldwide is costing legitimate service providers $5.4 billion annually.[25]

As with live sports streaming, combatting eSports streaming piracy poses a unique challenge compared to content streamed on demand. In these cases, the peak value of the content is reached during the event, which means the effectiveness of counter actions as discussed in Part 3 depends on speed of execution.

The rising pace of piracy in eSports

So far, eSports piracy is happening below many producers' radar as viewers of traditional distribution platforms, knowingly or not, tune into pirate channels that are streaming the content to capitalize on the advertising opportunities. One unpublicized study conducted for a major eSports producer uncovered nearly 400 channels that were streaming one of its events on platforms like Twitch, Facebook and YouTube.[26] Twitch is an obvious choice for illicit eSports streaming, given how popular it has become for accessing illegal live sports streams. In an article titled "Twitch Has Become a Haven for Live Sports Piracy," Wired cited several documented instances of illicit restreaming of high-profile sports events on the platform's channels.[27] For example, three channels streaming a FIFA World Cup match in December 2019 were in the top 10 of the most viewed Twitch channels that day.

Piracy also benefits from ad hoc marketing assistance when regular users of their services pass out links to illicit services on social media. Many of these people are also gamers and avid eSports fans. Wired noted that users on Discord's gaming chat site "distribute links to soccer live streams like handfuls of pigeon feed at the park."

Pirates have gotten good at offering services that offer many of the same features available from legitimate sources. As Wired reported, some of the illicit services on Twitch offer live chats that utilize the Twitch chats code.

Disruptions to eSports business resulting from app vulnerabilities

As in the case of the streaming piracy threat, the success of eSports has significantly elevated the threat of disruptions to their business models posed by hackers exploiting app vulnerabilities. Here again the magnitude of the threat can be seen in developments impacting the entire streaming media sector.

These threats stem from app vulnerabilities to reverse engineering of code governing core functionality and to various modes of tampering and other techniques that allow hackers to execute nefarious actions. The degree to which developers harden apps against tampering in the development process varies, but virtually all follow the practice of enabling reverse engineering of their apps as a legitimate means of allowing other developers to break down an application to understand its architecture and code.

Repackaging of apps via cloning in order to gain access to the data of users who mistake the clones for the real thing was found to be the modus operandi in 86% of malware samples studied by a North Carolina State University team.

This serves to foster innovation and broader engagement across the developer community as well as to make it easier to execute app upgrades. But for this practice to work as intended, developers and the entities that make use of their output must take steps to prevent unauthorized players from engaging in reverse engineering for illegitimate ends. surprising about expectations that in the years ahead the ad total will track with the general growth of advertising in all types

How hackers are exploiting app vulnerabilities

Any doubts about the urgent need to shield eSports apps are easily dispelled by well-documented intrusions that are disrupting all types of streaming operations worldwide. What follows is just a small sampling of the intensity of attacks on inadequately shielded streaming apps in various media categories, and the damage they're causing to businesses and participants.

App closing and malware distribution

Repackaging of apps via cloning in order to gain access to the data of users who mistake the clones for the real thing was found to be the modus operandi in 86% of malware samples studied by a North Carolina State University team. Another approach to malware distribution is illustrated by Check Point Research's recent revelation that Google Play store has been host to nine malicious apps that employ a malware-as-a-service model to deliver malware fetched by a "dropper" that penetrates vulnerable smartphones. The malware initially steals victims' financial information and eventually takes over their phones.

Still another well-publicized recent incident on Google Play involved malware disguised as a Netflix app. The infection was spread on WhatsApp promising 60 days free access to Netflix Premium via a fake Netflix site that phished for credentials and credit card information from unwitting victims.

Of course, there's an abundance of examples where hacks having nothing to do with Google Play-hosted apps, but have resulted in significant damage from malware distribution. One notorious case occurred in 2017 when hackers got into the E-Sports Entertainment Association League database via ESEA's karma game-playing rating module to steal the personal account information of over 1.5 million users.

Flaws in eSports apps exploited for fraudulent purposes

As noted above, not every fraudulent activity is predicated on app hacks. Perhaps the most widely publicized eSports scandal involving exploitation of an inadvertent app flaw occurred with the so-called "spectator bug" associated with Counter-Strike: Global Offensive, one of the most popular eSports titles in the world, with championship prize money that can top $2 million.

An investigation by the eSports Integrity Commission, the industry's self-policing organization, concluded 37 team coaches, now banned from the game, had been abusing the bug over a multi-year period, throwing many outcomes into doubt and badly damaging the reputation of Valve, the event producer. The coaches used the bug to get an unrestricted view of certain parts of the game's maps during gameplay, which allowed them to pass along information that gave their players game-tipping advantages.

Reverse engineering in support of eSports cheating

So far, the greatest damage to eSports stemming from reverse engineering of apps has been the destruction of gaming integrity through cheating. Nothing better illustrates the seriousness of the cheating issue than the eSports industry's backing for the Esports Integrity Commission (ESIC), whose investigations are regularly triggering suspensions of individual players and whole teams worldwide.

The distribution of cheats for myriad games developed through penetration of coding algorithms has morphed into a global business generating tens, if not hundreds of millions of dollars through sales to professionals in high-profile competitions with big prizes at stake, and to amateurs who cheat for bragging rights about their gaming prowess.

According to the BBC, findings from one large survey suggested about a third of gamers use cheating apps. In March 2021, Chinese police arrested what they called the world's largest video-game cheating operation, which netted $76 million selling cheat software to gamers worldwide. The situation has deteriorated to the point that big-name players have begun to abandon participation in the games they are known for. One case in point involved a gamer with seven million followers on his YouTube channel who announced he was quitting Activision's Call of Duty: Warzone. This came right after Activision reported a nefarious escalation in cheating apps that promise unlimited ammunition, extra speed and improved targeting, but which actually contain malware designed to take over a computer's camera or microphone, record keystrokes or steal banking information.

Conclusion

eSports' emergence as a mainstream live-streamed entertainment category opens service providers to all the threats plaguing live-streamed sports. At the same time, intensifying competition for big purses and social prestige has raised the cheating threat to unprecedented levels across the ranks of professional and amateur players.

Already, piracy aimed at stealing ad revenue from free ad-based eSports services is cutting into producers' and distributors' revenues. The losses are sure to mount as the global eSports fan base soars past the one-billion mark, especially as it becomes possible for pirates to capitalize on eSports providers' move to subscription services by offering stolen services at cut-rate prices to augment ad revenues.

Beyond the piracy threat to bottom lines, eSports providers face a plague of app hackers who are exploiting vulnerabilities in pursuit of myriad nefarious ends. Employing reverse engineering and other modes of app tampering, hackers are stealing personal data, inserting malware, duplicating code to create fake apps, breaking authentication codes, and doing much else to disrupt businesses and the lives of consumers. On top of that, they're making a lot of money selling "cheats" to players looking for an unfair advantage. Clearly, eSports providers have too much at stake to leave these threats unaddressed or to apply anything less than the most rigorous protections against them. Part 2 will explore in depth the remedies now at hand that not only deliver the comprehensive protection eSports providers need, but do so in ways that they will discover are far less manually intensive and costly than they might otherwise have assumed.

With smart TV penetration approaching saturation levels, broadcasters can proceed with confidence that, when they want to make the move to all-IP TV operations, they'll have the big-screen reach they need to facilitate that transition.

Footnotes

1 Venture Beat, SuperData:Games Hit $120.1 Billion in 2019, January 2020

2 Telecom.com, 1 Billion People Will Be Watching eSports by 2025, March 2021

3 CNBC, Netflix Says It's More Scared of Fortnight and YouTube than Disney and Amazon, January 2019

4 Newzoo, Trends to Watch in 2021, February 2021

5 PWC, Monetizing eSports via Multiple Revenue Streams, January 2020

6 TVerified Market Research, eSports Market Size and Forecast, January 2019

7 Ibid. Telecom.com

8 Deloitte, Digital Media Trends Report, March 2019

9 Forbes, eSports Is Filling the Programming Void, April 2020

10 StreamLabs, Streamlabs & Stream Hatchet Q1 2020 Live Streaming Industry Report, April 2020

11 DLA Piper, Media and Sport: Anti-Piracy eSports and Gambling Webinar, December 2020

12 Newzoo, Global eSports Market Report, February 2020

13 Business Insider, eSports Ecosystem Report, January 2021

14 Ibid. PWC

15 Media Post, OTT Revenue Now Projected to Double by 2025, May 2020

16 Deloitte, Digital Media Trends: Video Gaming Goes Mainstream, June 2019

17 CNBC, Watch Me Play Video Games! May 2016

18 Twitch, Twitch Turbo: What's Included, May 2021

19 Dot eSports, League Pro View Returns with Lower Price and New Features, January 2020

20 Softpedia, Half of the Ads in Sports Live Streaming Are Malicious, July 2016

21 The Drum, How Ads Fund Football Piracy, October 2020

22 Streaming Media, SVOD Services Correlate with Lower Rates of Piracy, July 2019

23 Digital TV Europe, Piracy to Exceed $67 Billion by 2023, January 2020

24 Statista, Number of Media Piracy Site Visits Worldwide 2018, May 2019

25 Advanced Television, Report: $28bn Anti-Piracy Sports Rights Bonus, March 2021

26 Smart Protection, Explosive Growth Signals Need for eSports Copyright Protection, July 2020

27 Wired, Twitch Has Become a Haven for Live Sports Piracy, January 2020

28 North Carolina State U., Dissecting Android Malware: Characterization & Evolution, February 2021

29 Check Point, Dangerous Malware Dropper Found in 9 Utility Apps on Google Play, March 2021

30 Threat Post, Fake Netflix App on Google Play Spreads Malware via WhatsApp, April 2021

31 European Gaming, The Role of Cybersecurity in eSports, February 2019

32 TalkeSport, What Is the Spectator Bug in CSGO?, September 2020

33 BBC, The Cheat Hackers Ruining Gaming for Others, September 2019

34 BBC, Police Bust World's Biggest Video Game Cheat Operation, March 2021

35 BBC, Gamer Vikkstar Quits Call of Duty: Warzone over Cheating, February 2021

36 Activision, Cheating Cheaters: Malware Delivered as Call of Duty Cheats, February 2021

intertrust®

Building trust for the connected world.

Learn more at: expressplay.com/products
Contact us at: +1 408 616 1600 | onestopshop@expressplay.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035