verimatrix
cybersecurity

Ensuring Mobile Gaming Security

Cyber Quest: Combating IP Theft,
In-Game Fraud and Cheating

CHAPTER 1

Online Gaming Draws Cyber Threats

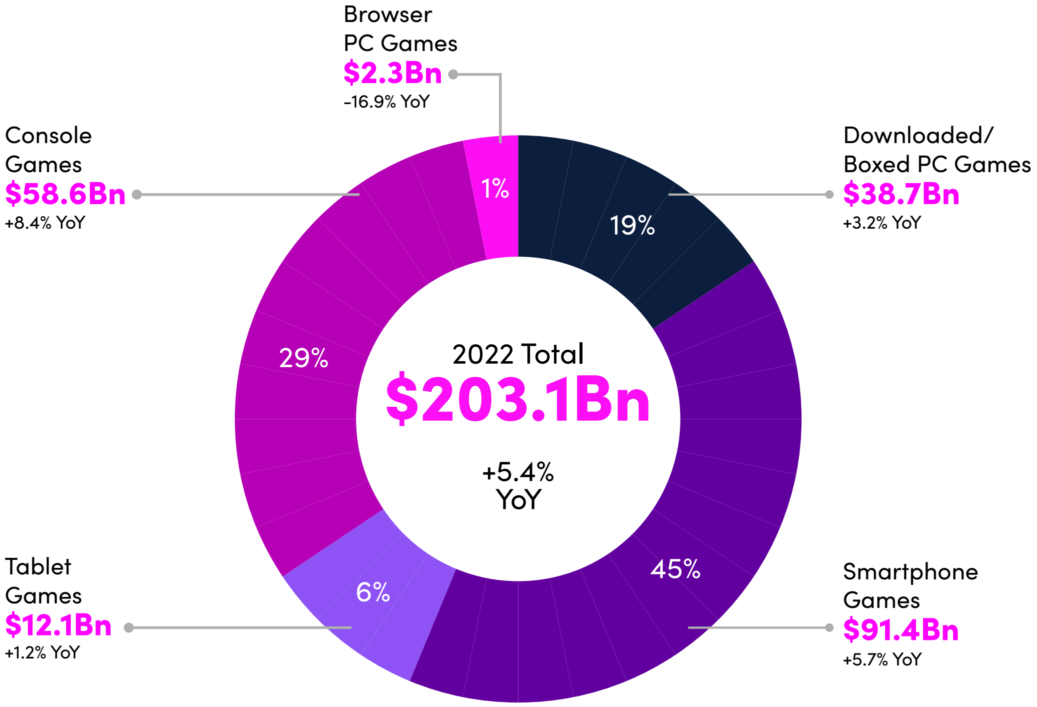
The online gaming business is booming. Video games have long been popular, but the 2020 pandemic lockdown drove millions of people worldwide to pursue online entertainment as a form of social engagement—and gaming companies happily obliged. The breadth of games to choose from and the ability to play on your own device (not an expensive console) now make cloud gaming especially attractive to many gamers. Allied Market Research reported that the cloud gaming market value in 2020 was US$244 million but is expected to grow to a whopping $21.95 billion by 2030.

Participating in online gaming requires users to provide their gaming platform of choice with sensitive personal information, such as name, address, player profile data and rank, messages, contacts, and even credit card numbers. That data, combined with the skyrocketing number of players and their devices, increases the cyberattack surface, putting gamers at continual risk. Gaming companies are also in jeopardy. Cyberattackers may target game developers and third parties in the supply chain or try to steal source code, development kits, or sensitive personal data of users and staff.

Among the many attack vectors cybercriminals exploit, one of the most accessible is the increasingly popular gaming apps that customers use to play games on their mobile devices. That makes securing those mobile apps critical for protecting gamers and gaming companies alike.

2022 Global Games Market

Per Segment With Year-on-Year Growth Rates



Source: Global Games Market 2022

CHAPTER 2

Common Cyber Threats to Online Gaming

The influx of less savvy (and likely less cautious) players, the abundance of online games, the emotional draw of wanting to have fun, so letting your guard down—all of these factors and more, combined with the growing sophistication of cyberattackers—have created myriad attack vectors. Bad actors excel at exploiting them through a breadth of threat techniques. Among the most common are:

- **Malware.** This harmful and disruptive type of software is often used to steal gamers' personal information. It is frequently downloaded from untrusted sites that distribute cheap or free games (often illicit versions of popular games). Players may also use cheat codes sourced from third parties, and cyberattackers can use fake cheat software as a means to spread malware and steal players' data.

- **Identity theft.** Cybercriminals use personally identifiable information (PII) to build profiles of players that they may target. Attackers may "chat" with random players in a game as a way to elicit sensitive PII from those who engage. Attackers may eventually collect enough information through chat and other means to achieve the theft of a player's identity.

- **Phishing.** Attackers may use malicious emails or links distributed through in-game chat to get gamers to reveal PII or to download malicious code. While phishing messages may look legitimate, they direct unsuspecting gamers to other legitimate-looking but malicious sites promising treats like fake prizes or bonus content.

- **Character Theft.** Phishing can also lead to character theft, with attackers helping themselves to characters that players have spent considerable time and effort building up. The account and associated progress in a game may be renamed and sold.

- **Account takeover.** Using the same username and (simple or predictable) password for multiple games puts players at risk. If that data gets stolen once, it can be used across all platforms where it's registered. Hackers may also try to break into gaming accounts using credentials they've stolen elsewhere in what's known as brute force attacks.

- **Swatting and doxing.** Doxing involves publishing personal information online with the goal of intimidating, punishing, or humiliating a victim. Swatting involves criminals sending law enforcement to a victim's address under fake pretenses as another attempt at intimidation. These are more reasons to guard personal information carefully!

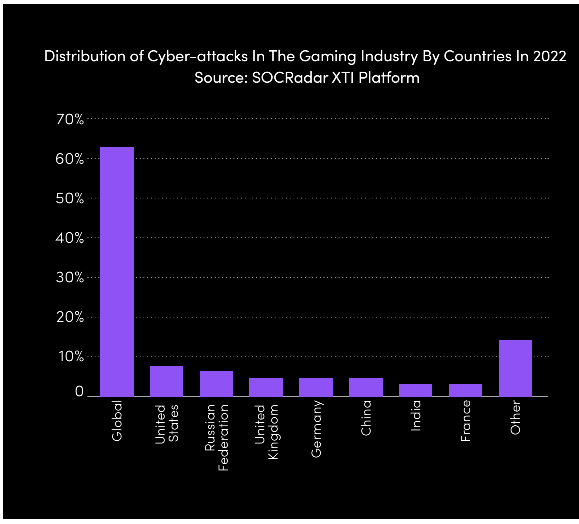
- **Cross-site scripting.** This type of attack involves inserting some malicious code (often JavaScript) into a webpage, where it captures customers' information in real-time while they are performing an action. The customer information is redirected to a server controlled by the attacker. Older gaming platforms that may still be using unsecure methods for processing users' login credentials are especially vulnerable to this kind of attack. In 2022, cross-site scripting was the most common attack on the gaming industry (32.2%)![1]

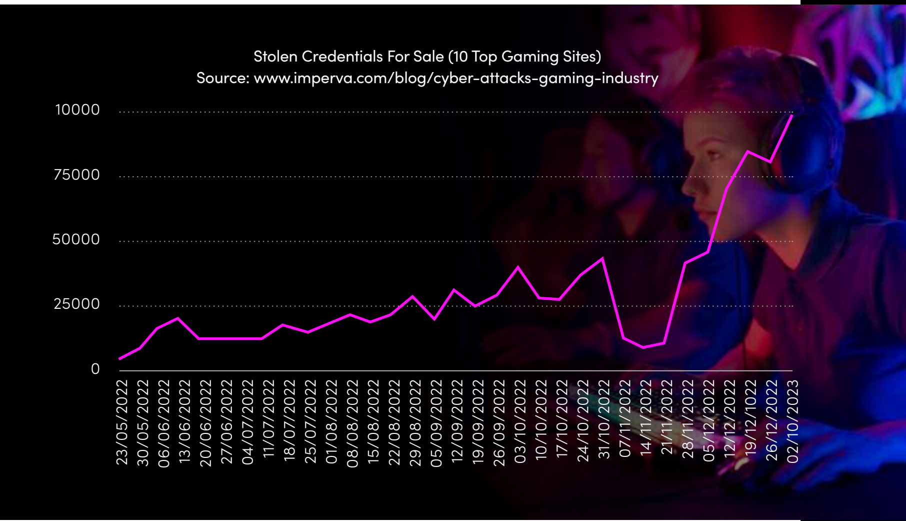
While phishing messages may look legitimate, they direct unsuspecting gamers to other legitimate-looking but malicious sites promising treats like fake prizes or bonus content.

[1] Imperva Threat Research, Why Attackers Target the Gaming Industry

- **Distributed Denial of Service (DDoS)**. Bad actors may attempt to dominate a gaming platform by flooding a game site with traffic to degrade performance, shut out other users, or make the platform unavailable. That's usually done by interrupting the hosting server. DDoS attacks impact play, result in game downtime, and impose recovery steps on the game's provider. For an industry that depends entirely on a stable internet, especially for multi-player games and the loading of high-quality content, this can be especially harmful. These types of attack capabilities in a user-friendly format can even be rented or bought, enabling almost anyone to launch an attack and force other players offline. It's been reported that DDoS attacks targeting the gaming industry cover 37% of all DDoS attacks.[2]

- **Shadow APIs.** Game developers regularly use application programming interfaces (APIs) to connect a game's code with other apps and plug-ins that enrich the game experience and provide game-related services. APIs make gaming companies a vulnerable cyber target for attackers that want to access users' credentials and financial information. For instance, they may direct data to undocumented "shadow" APIs that are not maintained by normal IT management and security, offering hackers entry to the gaming company's wider network. In 2022, 28% of all API traffic in gaming went to API endpoints flagged as a shadow API.


Distribution of Cyber-attacks In The Gaming Industry By Countries In 2022
Source: SOCRadar XTI Platform


Stolen Credentials For Sale (10 Top Gaming Sites)
Source: www.imperva.com/blog/cyber-attacks-gaming-industry

- **Bad Bots.** Automated bots are a growing mechanism for attacking online gambling sites. These automated software programs perform malicious tasks that enable attackers to steal user data, take over accounts, disrupt a gambling service, or otherwise manipulate the in-game environment. 55% of bot attacks in 2022 came from "simple" bots that, like DDoS attack codes, can be bought online.[3]

- **Ransomware.** Hackers may trick users into clicking on malicious links or downloading malicious code, which then renders their data, or entire mobile device or computer, inaccessible until a ransom is paid. That will prevent gamers from continuing to play. Attackers may also use extortion demands, threatening to reveal users' sensitive information or the gaming company's source code. Similar attacks may be made against gaming companies' employees, whether on their laptops or mobile devices. Clicking on the wrong link can impact the user's device or even the company's other networked systems.

- **Money Laundering.** Bad actors may open up a game account, create a profile, and then use stolen funds or credit card information to purchase in-game currency and accessories. Selling the account to an unsuspecting buyer then leaves them 'clean'.

[2] Gaming Respawned Report, https://www.akamai.com/resources/state-of-the-internet/soti-security-gaming-respawned
[3] Imperva Threat Research, Why Attackers Target the Gaming Industry

CHAPTER 3

Common Cyber Threats to the Mobile Gaming Sector

The incredible growth of the mobile gaming sector in recent years has unfortunately attracted cybercriminals looking to exploit vulnerabilities within the mobile gaming ecosystem. As the mobile gaming industry evolves and expands, so do the cyber threats. IP theft, in-game fraud, and cheating are three of the most prominent.

IP Theft

Intellectual property (IP) theft in the gaming industry involves the unauthorized reproduction, distribution, or use of copyrighted game assets, including game code, characters, artwork, music, and storylines. It encompasses various techniques:

- **Reverse Engineering:** Attackers reverse engineer a game's code to replicate its mechanics or create derivative works.
- **Repackaging:** Copycats take the stolen assets and create a near-identical game, often with only minor modifications.
- **Cloning:** Some developers or individuals create games that closely mimic the original without directly copying code or assets, but still infringe on the original game's IP.
- **Distribution of Stolen Assets:** Stolen game assets can be distributed on illegal platforms, undermining the original game's revenue stream.

IP theft can have severe consequences for the gaming industry. The most significant is financial loss because game developers invest significant resources in creating unique gaming experiences. When their IP is stolen, they lose potential revenue to copycat games. IP theft can also stifle innovation, as developers may become hesitant to invest in creating new games or innovative features if they fear their work will be quickly copied.

Of course, when players encounter multiple cloned or low-quality copycat games, it can erode your company's reputation and their trust in the gaming industry as a whole, leading to a decline in player engagement and consumer confidence. Additionally, game developers often need to allocate resources to pursue legal action against IP thieves, diverting funds and time away from game development and improvement.

Verimatrix's cybersecurity solutions play a crucial role in delaying and reducing the effectiveness of IP theft attempts. By implementing advanced techniques that safeguard apps against reverse engineering and repackaging, Verimatrix makes it significantly more challenging for malicious actors to clone a game successfully.

Our sophisticated app protection mechanisms also make it arduous for attackers to reverse engineer games merely by playing them. This multi-faceted approach not only safeguards the original game but also extends its competitive advantage by delaying the entry of copy-cat games into the market.

In-Game Fraud

Deceptive activities within a video game's ecosystem may aim to exploit the game's virtual economy or the real-world financial transactions associated with it. This type of fraud can take various forms, such as:

- **Unauthorized Purchases:** Players or attackers might manipulate the game to make unauthorized in-game purchases using real money, which can lead to financial losses for both players and game developers.
- **Fake Virtual Goods:** Fraudsters can create counterfeit virtual items or currency, which they might sell to unsuspecting players or use to undermine the in-game economy.
- **Account Hijacking:** In-game fraudsters may steal players' accounts, gaining access to their virtual assets, characters, or progress. They can then use or sell these stolen accounts for profit.
- **Scams and Phishing:** Some fraudsters employ deceptive tactics such as phishing emails, fake websites, or social engineering to trick players into divulging their account credentials or personal information.

These fraud schemes pose significant challenges for the gaming industry. As with IP theft, financial loss is a real possibility. Game developers rely heavily on in-game purchases and microtransactions for revenue. Fraudulent and illegitimate purchases drain revenue streams, and players might become wary of making legitimate transactions.
High-profile instances of in-game fraud can also tarnish a game developer's reputation, eroding player trust and leading to a loss of player base.

Fraudulent and illegitimate purchases drain revenue streams, and players might become wary of making legitimate transactions.

Players who feel cheated or scammed are less likely to continue playing or spending money on a game. Fraud can also distort the in-game economy by disrupting balance and fairness, negatively impacting the player experience. Inflation caused by the creation of fake virtual goods can devalue legitimate in-game items, making it harder for players to progress or achieve in-game goals. Finally, there are increased operational costs for combating in-game fraud—investment in more security measures, moderation teams, and customer support.

Verimatrix offers comprehensive protection against in-game fraud by preventing unauthorized access to and manipulation of game assets. Through safeguarding the integrity of the game code, Verimatrix ensures that attackers cannot reverse engineer or modify it to add virtual currency to their accounts. This, in turn, preserves the fairness and competitiveness of the gaming environment while safeguarding the revenue generation machine for gaming companies.

Cheating

Video game cheating involves using unfair or unauthorized means to gain an advantage over other players or manipulate a game's mechanics. Cheaters use a variety of approaches, including:

- **Aim Bots and Wallhacks:** Cheaters use software that enhances aiming accuracy or reveals hidden information like the location of opponents through walls.
- **Speed Hacks:** Players can manipulate their character's movement speed, giving them an unfair advantage in races or competitive scenarios.
- **Exploits and Glitches:** Some cheaters exploit bugs or glitches in the game to gain unintended advantages, such as clipping through walls or duplicating valuable items.
- **Emulators and Third-Party Software:** Cheaters may use emulators on more powerful PCs to run mobile games, enabling them to manipulate the game's code more easily.

Cheating has several adverse effects on the gaming industry. It creates an uneven playing field where honest players are at a disadvantage. This can lead to frustration, loss of interest, and ultimately, a decline in player engagement or even attrition. Cheating can also deter players from spending money on in-game items or subscriptions, as they may perceive the game as unfair or unenjoyable.

The bottom line is that cheating undermines the integrity of the game, reducing its appeal and credibility. This can impact the game's long-term success and the developer's brand image.

Verimatrix addresses cheating by protecting mobile games from static and dynamic analysis as well as tampering attempts. Through implementing comprehensive security measures, Verimatrix ensures that attackers cannot reverse engineer and manipulate a game to gain an unfair advantage. We help ensure a level playing field for all players, regardless of their gaming platform or device.

Cheating can also deter players from spending money on in-game items or subscriptions, as they may perceive the game as unfair or unenjoyable.

Verimatrix addresses cheating by protecting mobile games from static and dynamic analysis as well as tampering attempts.

CHAPTER 4

Key Impact of Cyberattacks on Online Gaming Businesses

While technology is dramatically extending the reach of gaming enterprises, the widespread adoption of online gaming, especially involving mobile devices and apps, can have significant impacts on gaming businesses and their customers. Depending on the severity and number of customers and assets involved, it may take weeks, months, or longer to overcome the potential impacts of a successful cyberattack.

Interruptions in a game's online services and network infrastructure resulting from a cyberattack can cause reputational losses for a gaming company. Industry expert Jonathan Shroyer holds that gamers' loyalty depends on trust, credibility, and predictability. If gaming companies are lax in their security, their games won't succeed.[4] Of course, that translates to the financial impacts of lost customers.

Cyberattacks can also impose other potential costs from interruptions of normal operations. Repairs to affected systems and networks may be needed, as well as a re-design of systems for collecting, processing, and storing customer data to keep it more secure. There can even be the expensive loss of intellectual property and trade secrets, which is especially harmful in this highly competitive industry.

User impacts are also a huge concern. Identity theft and theft of personal funds are harmful to customers personally. But cyberattackers may also go further with malicious actions like using unauthorized customer device access to launch phishing or business email compromise attacks against the user's contacts or others.

Another somewhat less obvious impact is the disruption to philanthropy that is a generous characteristic of gaming communities. Gamers donated $145 million to charity between 2011 and 2019, including $42 million in 2019 alone.[5]

70%

of regular gamers think hacking is a big problem in the gaming world.

63%

say their accounts aren't safe enough from attacks.

33%

report that their accounts have been hacked in the last two years.

89%

of gamers said they want game developers to pay more attention to cybersecurity issues.

Source: Kaspersky

[4] Dark Reading, For Gaming Companies, Cybersecurity Has Become a Major Value Proposition

[5] Direct Relief, Gamers Raised Millions for Charity in 2019: Meet Three Leading the Way

A Lot of 'Skin' in the Game

In-game microtransactions are big business. Gamers regularly purchase tools, character skins, and character upgrades using virtual money. They may also swap real money for virtual items. Business Research Company forecasts the online micro-transaction market will be worth $106.02 billion by 2026. Payment is usually linked to a player's account – an attractive target for cyberattackers.

CHAPTER 5

The Changing Role of Regulations in the Online Gaming Industry

Compared with other sectors, the gaming industry has historically been subject to fewer regulations. Most notable have been copyright and intellectual property laws, voluntary assignment of age, and content ratings assigned by the Entertainment Software Rating Board (ESRB) for games in the United States and Canada. There are no regulations as of yet for user-generated or interactional content, which is becoming more popular as more gamers move beyond consoles to cloud-based games.

With the growing popularity of online gaming, more regulations are now coming into play. For example, any game currencies that have real-world value may be subject to financial regulations, such as those from the US Treasury Department of the Treasury.

Also, more than 200 countries and jurisdictions implement international standards set by the Financial Action Task Force (FATF). This organization works to prevent global money laundering and terrorist financing through illegal activities.

Of course, any US business that accepts online credit card payments is subject to the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS is a long-standing security standard for ensuring that all companies that accept, process, store, or transmit credit card information maintain a secure environment for that data.

The European Union (EU), known for its strict information technology laws, is working towards making the online gaming industry subject to its general regulations for online platforms that provide hosting services. The European Regulation Digital Services Act (DSA), enacted in late 2022, will also quickly impact the online gaming industry with new requirements, such as suspending accounts of repeat offenders who publish illegal content and promptly informing authorities of any serious criminal offense they identify.

Gaming platforms that collect and store players' PII are subject to a plethora of data breach laws that exist around the world, depending on where they transact. For example, the EU General Data Protection Regulation (GDPR) mandates protections for the personal data and privacy of European Economic Area (EEA) citizens. It applies to online gaming companies that sell to any of these citizens, regardless of where those companies are located worldwide.

The GDPR sets firm rules for collecting, processing, and storing personal data of online gaming companies, and the EU is known to be quite strict on enforcement. In fact, GDPR is considered by many to be the world's strictest data protection law.

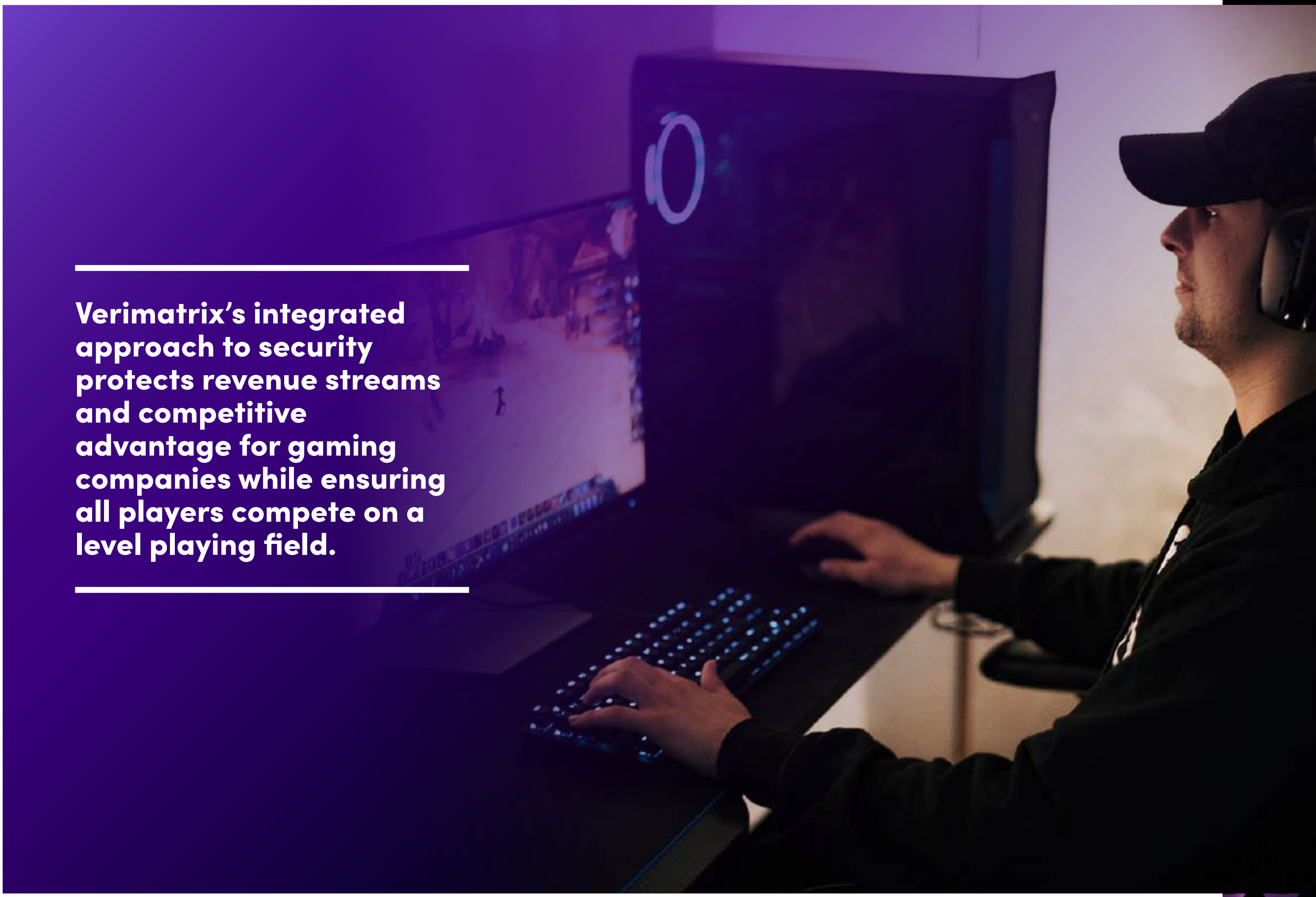
As the online gaming business continues to grow, it is quite likely we will see more regulations coming from more countries. Gaming companies should pay careful attention to these developments and start strengthening protections for the applications and devices that are increasingly central to the gaming experience.

The GDPR sets firm rules for collecting, processing, and storing personal data of online gaming companies, and the EU is known to be quite strict on enforcement.

CHAPTER 6

How Verimatrix Protects Online Gaming Apps

As mentioned in Chapter 3, Verimatrix provides comprehensive cybersecurity solutions that safeguard mobile games through multi-layered protection against reverse engineering, hacking, and manipulation attempts.



Verimatrix's integrated approach to security protects revenue streams and competitive advantage for gaming companies while ensuring all players compete on a level playing field.

By implementing robust app shielding, code integrity checks, and cheat detection, Verimatrix makes it extremely difficult for attackers to steal IP, defraud in-game economies, or gain an unfair advantage over other players. This delays the entry of cloned games while preserving the integrity and fairness of the gaming environment. Verimatrix's integrated approach to security protects revenue streams and competitive advantage for gaming companies while ensuring all players compete on a level playing field.

Let's delve into some of the Verimatrix protective measures in more detail.

Code Obfuscation

Verimatrix's code obfuscation techniques make it extremely challenging for attackers to reverse engineer game code. By transforming the source code into a complex and unintelligible form, obfuscation ensures that malicious actors encounter significant obstacles when attempting to analyze and manipulate a game. This deters IP theft, in-game fraud, and cheating by raising the bar for attackers.

Encryption

Encryption is a fundamental component of Verimatrix's cybersecurity solutions. It secures sensitive data like in-game transactions and player information from prying eyes. By encrypting communication between the game and the server, Verimatrix protects against data interception and manipulation, safeguarding the integrity and confidentiality of in-game interactions.

Runtime Application Self-Protection (RASP)

RASP is central to Verimatrix's cybersecurity arsenal, providing real-time monitoring and protection against dynamic attacks. By continuously analyzing game behavior during runtime, RASP identifies and thwarts tampering attempts, ensuring game integrity remains intact. By detecting and responding to threats as they occur, this proactive approach is essential to countering cheating and in-game fraud.

Tamper Detection and Response

Verimatrix' solutions include tamper detection mechanisms that actively monitor a gaming app's environment for signs of manipulation or unauthorized access. When tampering is detected, Verimatrix's system can respond in real-time, either by blocking the offending user or alerting administrators to take appropriate action. The rapid response capability is crucial to maintaining the fairness and security of the gaming environment.

Protecting Your Mobile Gaming Business

The mobile gaming sector faces myriad threats that not only jeopardize the intellectual property and financial stability of your business but also disrupt the gaming experience for legitimate players. Verimatrix cybersecurity solutions provide a comprehensive defense against these threats by safeguarding the integrity of mobile games and the connected app ecosystem.

Verimatrix's commitment to protecting mobile games and their ecosystems demonstrates its dedication to ensuring a secure and enjoyable gaming experience for players worldwide. In an era where cyber threats are ever-present, Verimatrix's cybersecurity solutions serve as a beacon of security and reliability for the mobile gaming sector.

Encryption is a fundamental component of Verimatrix's cybersecurity solutions. It secures sensitive data like in-game transactions and player information from prying eyes.

Verimatrix' solutions include tamper detection mechanisms that actively monitor a gaming app's environment for signs of manipulation or unauthorized access.

CHAPTER 7

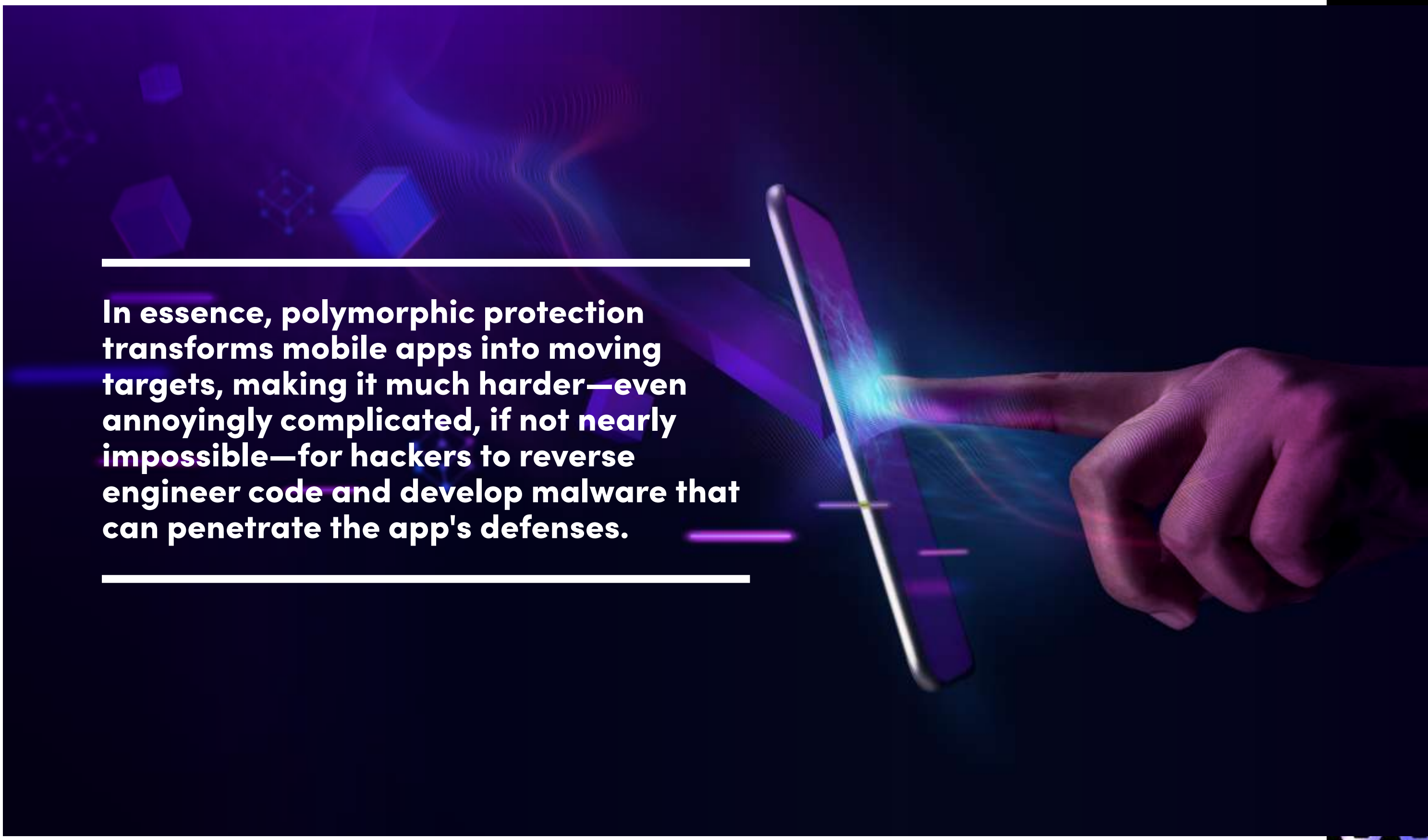
Polymorphic Protection: An Important App Security Attribute

An effective XTD platform should include polymorphic protective capabilities. This innovative approach involves constantly changing an application's code and structure to make it more challenging to hack. It's a bit like changing the password of your online accounts every so often to reduce your cyber vulnerability. Some savvy online gaming companies are already protecting their mobile apps with polymorphic protection.

Developers can use various techniques to make an app's code and structure more resistant to attack. One approach is to use obfuscation, which involves modifying the source, byte, or machine code so that it becomes significantly more difficult for hackers to read and understand. In essence, polymorphic protection transforms mobile apps into moving targets, making it much harder—even annoyingly complicated, if not nearly impossible—for hackers to reverse engineer code and develop malware that can penetrate the app's defenses.

That way, the code cannot be used to potentially reveal an app's inner workings or any exploitable vulnerabilities that may be found within it. Obfuscated code is also far less susceptible to tampering. Given the online gaming sector's particular vulnerability to cyberattacks, this approach is crucial for protecting customer information.

To implement polymorphic protection, online gaming businesses must invest in tools that not only shield mobile apps but also provide threat detection and response capabilities.



In essence, polymorphic protection transforms mobile apps into moving targets, making it much harder—even annoyingly complicated, if not nearly impossible—for hackers to reverse engineer code and develop malware that can penetrate the app's defenses.

CHAPTER 8

The Verimatrix XTD Approach

Verimatrix XTD offers an affordable and user-friendly solution that utilizes cutting-edge technology to secure mobile apps. With its ability to detect and respond to attacks promptly, Verimatrix XTD ensures the safety of mobile applications and prevents potential damage. Our military-grade, multi-layered security is very difficult for hackers to penetrate. We also help customers monitor the fastest-growing attack surface: consumer endpoints. By analyzing extensive data, Verimatrix XTD can predict future attacks and provide proactive protection.

Covering a Wider Attack Surface with Zero-Code Protection

Verimatrix XTD offers a truly distinct differentiator. Unlike those solutions that necessitate agent installation, Verimatrix XTD offers an agentless, zero-code approach. This capability enables the rich protection, attack detection, and response capabilities to be quickly and easily deployed without cumbersome development or coding—making speed-to-market a reality. This is especially valuable for the mobile-transacting environment, where consumer devices with various levels of protection are always in play.

Detecting and Responding to Active Attacks

Verimatrix XTD's proactive defense strategy involves the swift detection of active attacks and an immediate response to neutralize potential damage. By leveraging advanced threat detection techniques, Verimatrix XTD identifies attacks in real-time, enabling security professionals to disconnect compromised devices promptly. This decisive action safeguards sensitive data and prevents malicious actors from exploiting vulnerabilities.

Proactive Protection through Predictive Analytics

One of the standout features of Verimatrix XTD is its capability to analyze vast amounts of data to predict potential attacks. By employing predictive analytics, the solution can anticipate threats even before they occur. This proactive approach empowers online gaming businesses to stay one step ahead of attackers, ensuring enhanced security for their mobile applications and connected infrastructure.

Understanding Risks and Empowering Security Professionals

Verimatrix XTD is dedicated to helping security professionals comprehend the risks associated with mobile applications and their connections. Highlighting the existence of blind spots by assigning a risk score to every threat found, Verimatrix XTD prompts online gaming businesses to acknowledge and address potential vulnerabilities. XTD provides security professionals with a meticulously designed Software-as-a-Service (SaaS) offering. There is also an optional service incorporating the services of human data scientists to review your account and take response actions on your behalf, adding an extra layer of expert assistance to combat evolving app threats effectively.

Verimatrix XTD offers a truly distinct differentiator. Unlike those solutions that necessitate agent installation, Verimatrix XTD offers an agentless, zero-code approach.

By leveraging advanced threat detection techniques, Verimatrix XTD identifies attacks in real-time, enabling security professionals to disconnect compromised devices promptly.

Fight Back with Verimatrix XTD!

As the online gaming sector grows, so does the need for robust cybersecurity measures. Verimatrix XTD is an exceptional solution, providing affordable and user-friendly mobile app protection. With its agentless, zero-code approach, it allows for easy and painless deployment, allowing customers to monitor a wider attack surface, including unmanaged consumer devices.

Verimatrix XTD effectively detects active attacks and responds promptly, minimizing the potential for damage. By analyzing data and predicting attacks, it enables organizations to proactively protect their mobile applications. Armed with Verimatrix XTD's comprehensive security offerings and expert support, security professionals can effectively mitigate the risks associated with online gaming app vulnerabilities and secure their digital assets

Verimatrix — Award-winning Cybersecurity

Verimatrix helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world.

We are proud of the market recognition our innovative solutions have earned:

2023 Global Infosec Award for Hot Company in Mobile App Security – Cyber Defense Magazine

2023 Cybersecurity Excellence Awards – Gold Winner for Artificial Intelligence Security and Biggest Brand Growth

2023 Product of the Year, AI and Machine Learning – National Association of Broadcasters (NAB)

2022 Gartner® Hype Cycle™ for Application Security

Get A Demo of the Verimatrix XTD cloud-native platform, deployed in minutes to protect your apps!

Sources

https://www.alliedmarketresearch.com/press-release/cloud-gaming-market.html

https://usa.kaspersky.com/resource-center/threats/top-10-online-gaming-risks

https://www.reliablesite.net/hosting-news/cybersecurity-threats-for-gamers/

https://socradar.io/increasing-cyberattacks-targeting-the-gaming-industry-in-2022/

https://securityintelligence.com/news/cyberattacks-against-gamers-increase-167-percent/

https://www.enterpriseappstoday.com/news/online-gaming-market-to-hit-usd-163-0-bn-globally-by-2032-at-10-2-cagr.html#:~:text=The%20global%20online%20gaming%20market,at%20a%20CAGR%20of%2010.2%25

https://tremau.com/regulating-online-gaming-challenges-and-future-landscape

https://www.imperva.com/blog/cyber-attacks-gaming-industry/

https://www.darkreading.com/threat-intelligence/cybersecurity-major-game-company-value-proposition

https://threatpost.com/critical-steam-flaws-crash-opponents-computers/162100/

https://www.kaspersky.com/blog/gamers-report-2022/

https://tremau.com/regulating-online-gaming-challenges-and-future-landscape

https://www.directrelief.org/2019/12/gamers-raised-millions-for-charity-in-2019-meet-three-leading-the-way/#:~:text=other%20corporate%20sources.-,As%20reported%20by%20Direct%20Relief%20earlier%20this%20year%2C%20on%20Twitch,from%20the%20Amazon%2Downed%20company

https://sanctionscanner.com/blog/online-video-games-and-money-laundering-183