
# Industry Landscape Report

## iGaming/Betting

SOCRadar®
Your Eyes Beyond

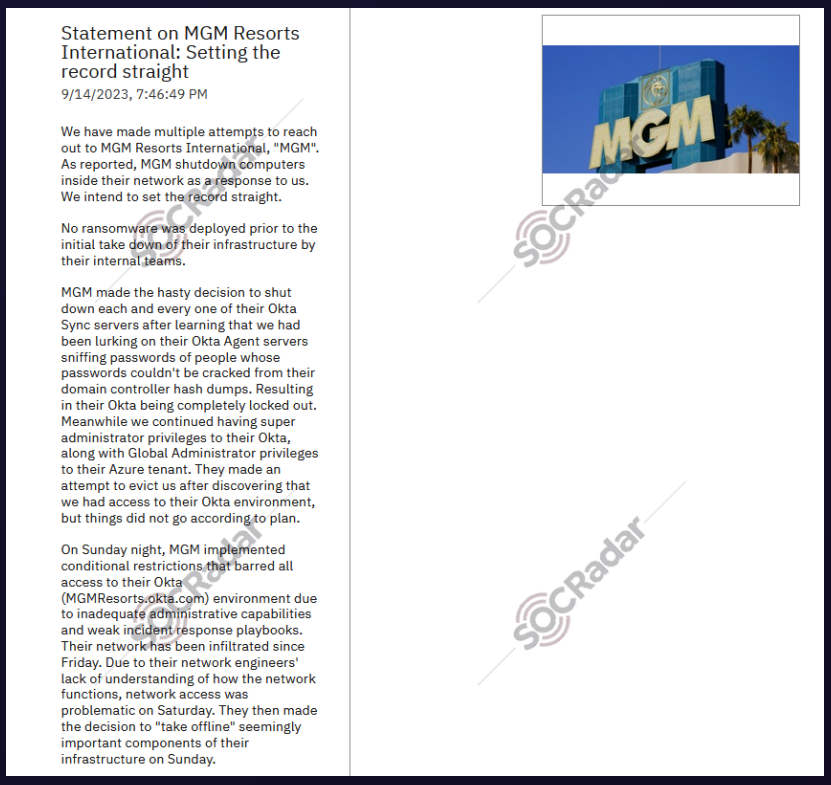
# Table of Contents

After the data breach at Caesars Entertainment, where over 41,000 Maine residents had the company undertook decisive steps for damage control and customer reassurance. The initial ransom demand by the attackers was a staggering $30 million, but negotiations brought it down to $15 million. While Caesars has not officially confirmed the payment, industry insiders widely believe that the company complied with this revised demand to mitigate the consequences of the breach.

To address customer concerns, Caesars Entertainment dispatched a detailed security breach notification letter, outlining the offer of complimentary identity theft protection services for a period of two years, provided by IDX. This package included critical services such as credit and Dark Web monitoring, a substantial $1,000,000 insurance reimbursement policy, and comprehensive managed identity restoration services. These measures were aimed at alleviating customer apprehensions and safeguarding them against potential repercussions of identity theft.

The breach and Caesars' response garnered significant attention from regulatory bodies and the public. This incident came to light in a Securities and Exchange Commission (SEC) filing by Caesars in September.

## 1.2 - MGM Resorts International




*In the AlphVM / Blackcat ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as MGM Resorts International.*

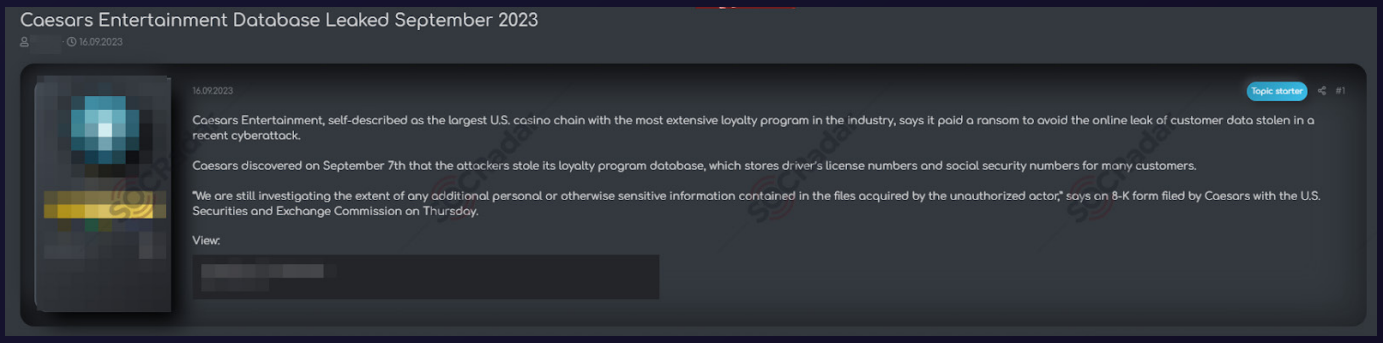
# Escalating Cyber Risks in the Gambling and Online Gaming Industry

The Gambling and Online Gaming industry, a sector that intricately intertwines large financial transactions and sensitive customer data, stands as a prominent target for cybercriminals. The value and accessibility of this data make it a goldmine for malicious actors. The recent surge in cyberattacks on casinos and online gambling platforms brings to light the industry's urgent need for reinforced cybersecurity defenses.

## 1 - Persistent Cyber Threats to Physical Casinos

Casinos, both land-based and online, are experiencing an alarming increase in sophisticated cyberattacks.

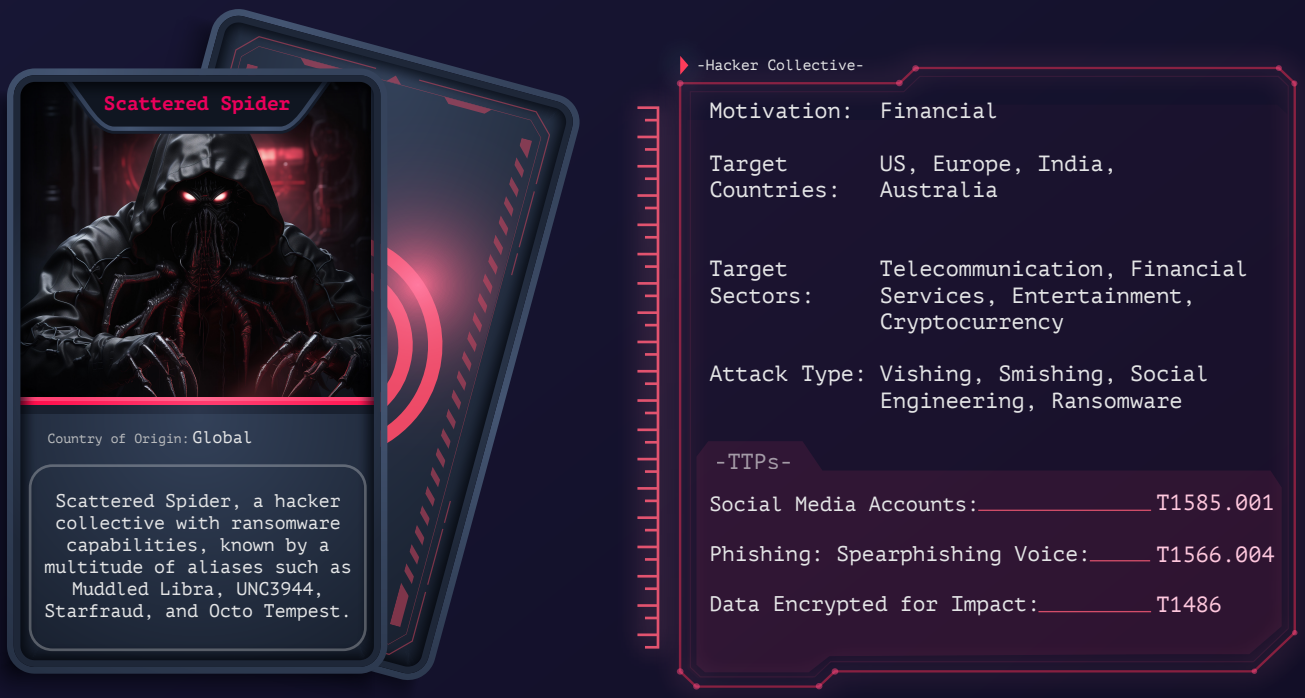
### 1.1 - Caesars Entertainment




*In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Caesars Entertainment.*

In a notable incident in August 2023, Caesars Entertainment, the owner of Caesars Palace, reported a significant breach. Over 41,000 Maine residents had their personal information, including names and driver's license numbers, stolen by a ransomware gang. The attack, which involved social engineering tactics on an IT support vendor, resulted in unauthorized network access and data exfiltration. This led to a ransom negotiation, where Caesars reportedly agreed to pay $15 million to retrieve the stolen data. The cybersecurity professionals attributed the attack to a hacking group known as "Scattered Spider."

The cyberattack on MGM Resorts International, another major incident in the casino and hospitality sector, unfolded with a distinct set of circumstances and responses. This incident also involved the notorious cybercrime group Scattered Spider, which had simultaneously targeted other major players in the industry.




*Threat actor card of Scattered Spider.*

In the MGM Resorts case, the attackers managed to infiltrate the company's IT systems, leading to the theft of customer data. The exact nature of the data stolen included names, contact information, date of birth, and driver's license numbers, along with a limited number of customers' social security numbers, passport numbers, or both. Importantly, MGM Resorts confirmed that critical financial details like passwords, bank account numbers, or card details were not compromised in the breach.

The attack's fallout was significant, affecting several of MGM's hotels and casinos and causing substantial operational disruptions. The incident was so severe that it led to system shutdowns, leaving many guests, including notable figures such as FTC chair Lina Kahn, stranded and unable to check into their rooms. This event occurred during Kahn's visit to Las Vegas for meetings about a merger between Kroger and Albertsons, illustrating the widespread impact of the attack.

Unlike Caesars Entertainment, MGM Resorts chose a different path in responding to the ransomware attackers. The company decided not to pay the ransom demanded by the hackers. MGM's CEO, Bill Hornbuckle, cited the timely detection and immediate response to the attack as key reasons for this decision. By the time the ransom note was received, MGM had already begun rebuilding its systems from backups and saw no merit in engaging with the attackers' demands.

Despite not paying the ransom, the attack had substantial financial implications for MGM Resorts. The company incurred expenses under $10 million for technology consulting services, legal fees, and other third-party advisor expenses related to the attack. However, the total expected loss was projected to be around $100 million. This figure underscores the significant cost implications of cyberattacks, even when a ransom is not paid.

In terms of customer response, MGM Resorts notified affected customers via email and offered free credit monitoring and identity theft protection services. The company set up a dedicated call center and a webpage to provide additional information and support to those impacted.

### 1.3 - Gateway Casinos and Entertainment

In April 2023, Gateway Casinos and Entertainment, a prominent operator in the Canadian gaming and entertainment sector, experienced a significant cyberattack. This attack led to the temporary closure of their Ontario locations, including a notable site at the Western Fair District in London, Ontario. While the Casino Rama Resort's Hotel and restaurants in Orillia remained open, the company's gaming and virtual operations were notably disrupted.

The cyberattack, described as a "system-wide malfunction" initially, was later confirmed as a cybersecurity incident. Despite the operational disruptions, Gateway reported that there was no evidence suggesting personal information had been compromised. However, the impact on their services was substantial, highlighting the vulnerabilities and potential consequences of cyber threats in the gaming and entertainment industry.

Unifor Local 1090, representing employees at some of Gateway's locations, expressed concerns about the potential compromise of sensitive employee information. In response, Gateway assured proactive measures to protect their staff in the event of any data compromise.

## 2 - Increasing Attacks on Online Gambling Platforms

The online gambling space is equally targeted by cybercriminals, with several high-profile attacks causing significant financial and reputational damage.

### 2.1 - Stake.com Hack

Stake.com, an online gambling platform, was hacked for $40 million by North Korea's Lazarus Group. This state-sponsored group is known for targeting financial platforms, demonstrating the advanced capabilities and persistence of cyber attackers in this sector (Casino.org, Sep 8, 2023).

The Lazarus Group has been implicated in multiple attacks on various financial platforms, including Alphapo, Coinspaid, and Atomic Wallet, leading to significant financial losses. The Ronin Network attack, linked to the Lazarus Group, resulted in a staggering $622 million loss (Casino.org, Sep 8, 2023). These incidents underscore the severe threat posed by state-sponsored groups in the online gambling industry.

## 3 - Why the Gambling Industry is a Prime Target

The gambling industry, both traditional and online, presents a lucrative opportunity for cybercriminals for several reasons:

1. **Financially Motivated:** The industry's handling of large financial transactions makes it an attractive target.
2. **Sensitive Data:** Casinos and online platforms possess vast amounts of personal data, including financial information, making them prime targets for data theft and ransomware attacks.
3. **High Impact, Quick Payoff:** The operational disruption caused by cyberattacks can lead to significant financial losses, pressuring companies to pay ransoms.
4. **Vulnerabilities in Digital Infrastructure:** Often, the digital infrastructure of these platforms, especially legacy systems in traditional casinos, may have vulnerabilities that cybercriminals can exploit.

### 4 - The Urgent Need for Advanced Cybersecurity in the Gambling Sector

The increasing sophistication of cyberattacks on the gambling and online gaming industry necessitates an urgent shift to more advanced cybersecurity measures. This includes not only technological solutions but also awareness and training to mitigate social engineering attacks. Proactive defense strategies, robust incident response plans, and continuous monitoring are essential to safeguard against these evolving cyber threats and to protect the industry's integrity and customer trust.

## The Expanding Cyber Risk Landscape in Online Gaming

The online gaming industry, marked by an ever-growing economy and player base, presents a vast and lucrative target for cybercriminals. The COVID-19 pandemic catalyzed this growth, attracting more players and, consequently, more cybercriminals.

As of 2023, gaming revenue globally stands at an estimated about $240 billion globally, with projections to more than double by 2030. With around three billion individuals engaged in gaming worldwide, the sector not only offers a broad attack surface but also a diverse range of vulnerabilities for cyber attackers to exploit.

Recent research by Kaspersky found more than four million infection attempts targeting the global gaming community between July 2022 and July 2023, exploiting vulnerabilities through DDoS attacks, cryptocurrency mining, complex Trojan or phishing campaigns, and using web vulnerabilities.

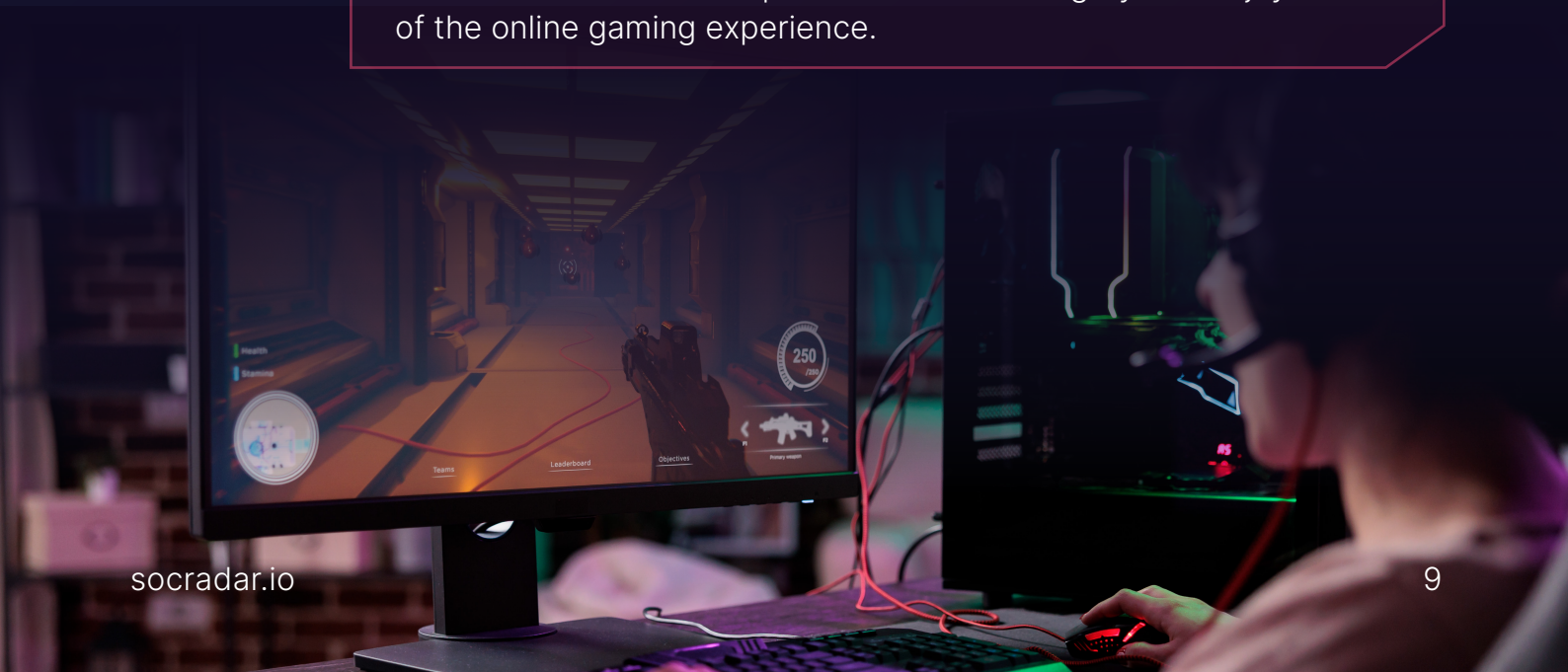
## 1 - Why Players are Targets in Online Gaming

Players in the online gaming world are attractive targets for cybercriminals for multiple reasons:

1. **Economic Transactions:** The gaming industry is not just about entertainment; it involves substantial financial micro-transactions through in-game purchases and trades.
2. **Valuable Personal Data:** Players often provide sensitive personal and financial data to gaming platforms.
3. **Inexperienced User Base:** A significant portion of the gaming community comprises individuals who may lack cybersecurity awareness.
4. **High Engagement:** The engaging nature of games can lead to a lowered guard among players, making them more susceptible to cyber threats.

## 2 - Types of Cyber Attacks in Online Gaming

As the online gaming industry continues to flourish, attracting millions of players worldwide, it also becomes a magnet for various sophisticated cyber threats. These threats range from phishing scams exploiting players' trust to highly disruptive DDoS attacks targeting both individual gamers and entire gaming platforms. Malware, often disguised as game modifications or cheats, and data breaches, which compromise sensitive player information, add to the spectrum of cyber risks. This evolving landscape of cyber threats not only poses significant risks to players' personal and financial data but also impacts the overall integrity and enjoyment of the online gaming experience.



## 1 - Phishing

Phishing and scams in the gaming industry have become increasingly sophisticated and prevalent, exploiting the vast and engaged user base of online gaming platforms. In 2023, platforms with large audiences such as Facebook, Instagram, YouTube, Twitter, Steam, Roblox, and Twitch have become prime targets for phishing campaigns. These platforms are attractive to scammers not only due to their large user bases but also because they often contain valuable digital assets and credit card information.

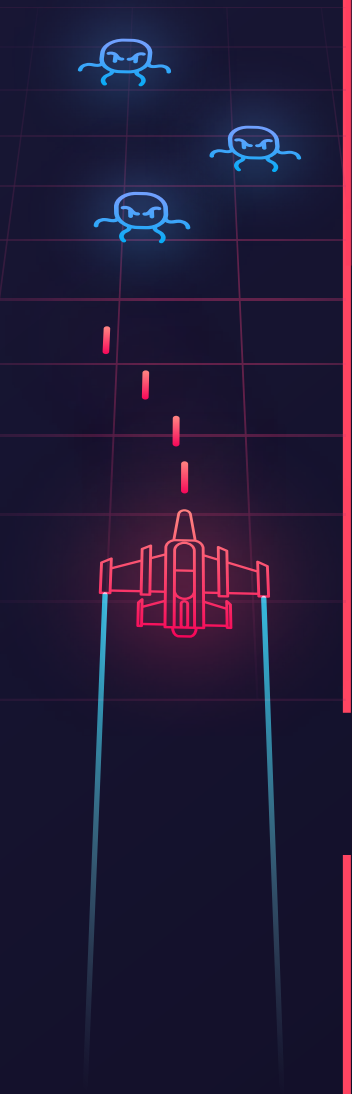
The nature of gaming and social platforms, which are designed to drive user engagement, makes them particularly susceptible to phishing attacks. Gamers are often in a mindset that primes them to share personal information and respond to calls-to-action, which scammers exploit to their advantage.

One specific example includes scams targeting Roblox users, where attackers used YouTube videos to entice children into clicking links for free in-game currency (Robux), leading them to phishing sites where their login information could be harvested. Phishers have also hijacked Roblox accounts using fake in-game ads.

Phishing scams targeting gamers worldwide have become increasingly effective. Phony emails attributed to Steam constitute the most common attacks, followed by scams involving Roblox, which is particularly popular among users under the age of 16. Another platform frequently targeted by scammers is Garena, a free gaming platform based in Singapore.

One innovative phishing method that emerged in 2022 involves "voting scams" used to steal Steam accounts. In these scams, attackers send messages in Steam or Discord channels, appearing to come from a friend and asking victims to follow a link to vote for their team. This link then directs them to a phishing page, leading to account compromise.

Phishing scams are rampant in the gaming industry. Attackers also create counterfeit websites or send deceptive emails mimicking legitimate gaming platforms to steal login credentials and financial information. In some cases, malicious software is disguised as popular games and distributed through third-party websites offering pirated versions, tricking users into downloading harmful files.



## 2 - DDoS Attacks

DDoS (Distributed Denial of Service) attacks in the gaming industry are increasingly becoming a significant threat. These attacks aim to overload servers, causing them to slow down significantly or crash entirely, thus disrupting the gaming experience. This can be particularly detrimental in competitive gaming scenarios, where a stable connection is crucial for fair play.

DDoS attacks have evolved to target not only large gaming platforms but also individual gamers' personal computers and networks. These attacks make the gaming session extremely slow and unplayable, giving attackers a substantial advantage. This is achieved by knowing the gamer's IP address, often obtained through malware, and using a network of computers (botnet) to send repeated requests to the target's network.

Significant DDoS attacks have targeted major online gaming platforms like the PlayStation Network and Xbox Live, rendering them unusable for extended periods. One of the most notable examples is the 2014 Christmas DDoS attack on both Sony's PlayStation Network and Xbox Live, affecting almost 160 million gamers. More recently, top-ranked Apex Legends players used DDoS attacks to gain an advantage in the game. Similarly, the Mirai botnet, initially feared as a tool for election disruption, was actually used by students to gain an advantage in Minecraft, targeting private servers and their protection tools.

## 3 - Malware and Info-Stealing Software

The use of malware in the gaming community is on the rise. Cybercriminals often target popular games like Minecraft and Roblox, using them as bait to distribute malware. These attacks often take the form of game mods or cheats, enticing players to download harmful software. For instance, Minecraft was responsible for triggering 70.29% of all cyber threat alerts of the research mentioned above, affecting 130,619 players globally during the reporting period.

Cybercriminals exploit vulnerabilities in gamers' interactions with digital content, using deceptive tactics like enticing in-game offers and fake cheat codes. These strategies lure gamers into inadvertently running malicious payloads, particularly those associated with info-stealing malware. The severity of this threat is escalating, causing growing concern within the gaming and cybersecurity communities.

In July 2023, an incident occurred where French gaming influencers were the targets of a cyberattack. They received Discord messages that falsely offered exclusive access to a game. This was part of a larger scheme where the cybercriminals used these messages to spread malware. The company Shadow, which provides cloud gaming services, had to alert its users about a security breach stemming from a fake game advertised on Discord. In these types of attacks, cybercriminals often use compromised accounts to send messages, aiming to influence specific individuals. The messages contain links that, when clicked, lead to downloading malware or redirect to deceptive websites. This strategy is employed to distribute malicious software discreetly.


*A new alleged Doenerium Stealer share has been detected in a hacker forum, under the surveillance of SOCRadar.*

Info-stealer families such as Doenerium and Epsilon Stealer have been identified in these campaigns. These malware strains operate with low antivirus detection rates, making them particularly elusive. To combat these threats, security experts recommend downloading software exclusively from official and trustworthy sources. Post-infection steps, including computer resets and password changes, are advised for those affected by such attacks.

## 3 - Exploitation of Mobile Gamers

The exploitation of mobile gamers has become a significant concern in 2023, with the mobile gaming sector encompassing nearly 40% of the global population, or over three billion individuals. This widespread use and accessibility make it a prime target for cybercriminal attacks.

Kaspersky recorded 436,786 attempts at infecting mobile devices, impacting 84,539 users between July 2022 and July 2023. Minecraft was the most targeted game, accounting for 90.37% of these attacks, affecting 80,128 users. For instance, in Indonesia, the Trojan.AndroidOS.Pootel.a was used to exploit Minecraft gamers, directing them to a fake marketplace page that initiated a stealthy process of subscribing them to premium services without their knowledge. This exploitation was achieved using the Google Phone Number Hint API to acquire phone numbers for subscription activation.

Additionally, the SpyNote Trojan on the Android platform targeted Roblox players, exhibiting spyware capabilities like keylogging, phone camera manipulation, and fake Google or Facebook application interfaces. This demonstrates the advanced techniques employed by cybercriminals to infiltrate and exploit user privacy and data.

These incidents highlight the dangers of phishing schemes and counterfeit distribution sites that often attract gamers by posing as legitimate sources for downloading popular games. However, these sites ultimately serve as fronts for distributing malware or irrelevant content, which bears no resemblance to the promised game files.

## 4 - Money Laundering Through In-Game Currencies

Online game currencies are also exploited for money laundering schemes. Criminals use stolen funds to purchase in-game currency and accessories, which are then sold to launder the money.

A prime example is the use of "V-bucks," the virtual currency in the popular game Fortnite, to launder proceeds from stolen credit cards. Investigations have revealed that discounted V-bucks are being sold on the Dark Web in large quantities. These illegally obtained gains are also being distributed on the open web, albeit on a smaller scale, through advertisements on social media platforms.

This practice has been recognized for years as an attractive method for money laundering. A 2013 report for the United Nations Office on Drugs and Crime highlighted that online games were increasingly becoming venues for criminals to launder money. The process typically involves the opening of numerous accounts across various online games to move money. One common method involves the transfer of in-game currency to associates in other countries, who then exchange it for real-world fiat currency.

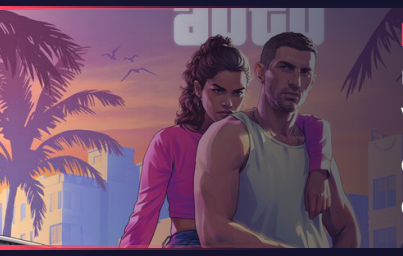
This method of money laundering through in-game currencies underscores the evolving challenges in regulating and monitoring online gaming platforms, particularly as they become increasingly intertwined with real-world financial transactions. The ability to transfer virtual currencies across borders with relative ease presents a significant loophole for illicit financial activities, necessitating more robust monitoring and regulatory measures in the online gaming sector.

## 5 - Data Breaches

Data breaches are a significant concern in the online gaming industry. For example, Roblox, an online gaming platform, experienced a data breach impacting almost 4,000 developer accounts due to a third-party security issue. However, recent years have seen other significant data breaches in the gaming industry, impacting major players such as Activision, Riot Games, and Rockstar Games.

**Activision Data Breach (December, 2022):** Unknown hackers stole internal data from Activision, including information on the planned content for "Call of Duty." The breach, which occurred on December 4, was a result of successful phishing of a privileged user on the network. The hackers obtained employee details like full names, emails, phone numbers, salaries, and addresses.

**Riot Games Data Breach:** In January, Riot Games disclosed a breach where hackers accessed the company's development environment. This allowed them to steal the source code for popular games "League of Legends" and "Teamfight Tactics," as well as the company's legacy anti-cheat system.



**Rockstar Games Data Breach:** In September, hackers published unreleased footage from the highly anticipated "Grand Theft Auto VI." Rockstar Games confirmed that the hackers had accessed confidential information from their systems, including early development footage for the game.

**Roblox Data Breaches:** An incident became public on July 18, 2023, impacting around 4,000 accounts of individuals who attended the Roblox Developer Conference between 2017 and 2020. The breach exposed personally identifiable information of Roblox developers, including names, phone numbers, usernames, IP and email addresses, dates of birth, physical addresses, and even T-shirt sizes. However, it did not expose financial information, account passwords, or social security numbers. This breach posed a risk of targeted phishing attacks for the affected individuals.

The platform addressed the breach on July 20, 2023, attributing it to a third-party security issue. Roblox engaged independent experts to support their investigation and communicated with the impacted individuals about the steps being taken to support them.

Roblox has a history of data breaches. In July 2022, a breach exposed 4GB of data, including identification documents and information about Roblox developers. In 2020, a hacker reportedly bribed a Roblox employee to access over 100 million users' information, disabling two-factor authentication, banning users, and eventually stealing in-game items.

**Widespread Targeting by 0ktapus (Scattered Spider):**
Throughout 2022, a hacking group known as 0ktapus (or Scattered Spider) targeted at least 130 companies, including several game makers like Riot Games and Epic Games. This group gained notoriety for hacking Twilio, a cloud communications company that provides services such as automated text messaging.


These incidents highlight the vulnerability of gaming companies to cyberattacks and the importance of robust cybersecurity measures to protect sensitive data and intellectual property.

## 6 - Necessity of Robust Cybersecurity in Online Gaming

Given the diverse nature of cyber threats in the online gaming sphere, players, gaming companies, and parents must adopt comprehensive cybersecurity measures. This includes using strong, unique passwords, enabling two-factor authentication, downloading games from official sources, and being vigilant against phishing campaigns. Additionally, the use of VPNs can provide an added layer of security, especially against DDoS attacks. As the gaming industry continues to expand, staying informed and vigilant against cyber threats becomes increasingly crucial for a safe and enjoyable gaming experience.

# Caught on the Radar:
# **The Scattered Spider in the Gaming and Gambling Sectors**


"Scattered Spider" is a name given to a specific threat actor or group of cyber attackers known for targeting various sectors, including the gaming, and gambling industries. This group is typically characterized by its sophisticated methods and strategic approach to cyberattacks.

**Social Engineering Expertise:** Scattered Spider is recognized for its proficiency in social engineering, employing a range of techniques such as phishing, push bombing, and Subscriber Identity Module (SIM) swapping attacks. These methods are used to obtain credentials, install remote access tools, and bypass multi-factor authentication (MFA) systems. Their social engineering skills have been particularly effective against large companies and their IT help desks, often with the goal of data theft for extortion purposes.

**High-Profile Casino Attacks:** The group gained significant notoriety following attacks on high-profile casinos such as Caesars and MGM Resorts International. These attacks caused prolonged disruptions and substantial financial losses. For instance, the attack on MGM Resorts resulted in a setback of $100 million. Despite the FBI's identification of some group members, Scattered Spider remains active and largely at large, continuing to pose a significant threat to the gambling industry.

**Shift to Ransomware Tactics:** Recently, Scattered Spider has begun deploying ransomware in victims' environments. This shift in strategy marks an evolution in their extortion attacks. In one notable incident involving MGM Resorts, the group claimed to have encrypted over 100 ESXi hypervisors. Scattered Spider is also believed to be an affiliate of ALPHV, a known ransomware group. This affiliation suggests a shared methodology or collaborative efforts in ransomware attacks, possibly sharing resources, tools, or intelligence. This evolution in tactics indicates a growing sophistication and threat level posed by Scattered Spider.

To combat the threat posed by Scattered Spider, companies in the gaming and gambling industries have to adopt a proactive cybersecurity posture. This includes regular security audits, employee training on cybersecurity practices, implementation of advanced security technologies, and collaboration with law enforcement and cybersecurity experts for threat intelligence and response strategies.

The activities of Scattered Spider show the continuous need for robust cybersecurity measures in the gaming and gambling industries. These sectors, due to the sensitive and financial data they handle, are particularly attractive targets for sophisticated cybercriminals like Scattered Spider. Their advanced social engineering skills, combined with a shift towards more destructive ransomware attacks, present a formidable challenge to cybersecurity defenses in these industries.

# Dark Web Trends in Online Entertainment and Gambling

The Dark Web, a hidden part of the internet associated with anonymity and illicit activity, is a barometer for trends in cyber threats and illegal trade. SOCRadar's Dark Web News channel, through advanced crawling techniques, machine learning, and AI, offers insights into the undercurrents of online activities. These findings are crucial for understanding the movements in the gaming, arts, and recreation sectors, along with the gambling industry.

## Monthly Analysis of Dark Web Activity in Entertainment and Gambling


*Monthly Comparison of Dark Web Discussions on Online Entertainment and Gambling in 2023, Highlighting Seasonal Peaks and Industry Trends.*

The bar chart presents a comparison of Dark Web chatter related to online entertainment, encompassing gaming, arts, and recreation websites, against gambling throughout the year. A noticeable peak in discussions about online entertainment occurs in September, possibly indicating a seasonal trend or the release of highly anticipated games or entertainment content. Conversely, the gambling chatter remains relatively consistent throughout the year, with a slight uptick in November and December, perhaps related to end-of-year festivities and associated gambling activities. This data suggests that while both sectors are subjects of Dark Web interest, online entertainment, particularly gaming, commands more attention and discussion, possibly due to its broader appeal and user base.

## Geographical Distribution of Dark Web Discourse in Entertainment and Gambling

**Top Countries Mentioned in Dark Web**

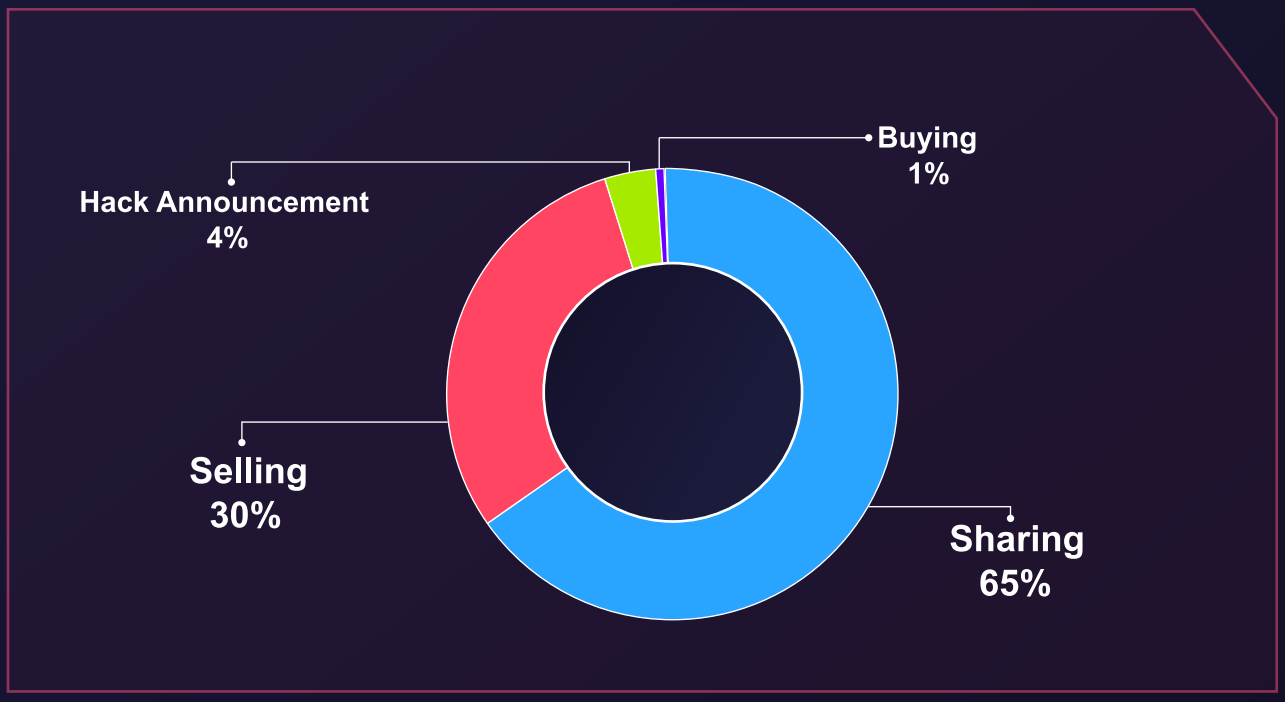
| | |
|---|---|
| **Entertainment** | |
| United States | 19,24% |
| Russian Federation | 4,42% |
| United Kingdom | 3,82% |
| **Gambling** | |
| United States | 13,26% |
| Turkey | 6,08% |
| China | 3,87% |

*Breakdown of Dark Web Mentions by Country for Online Entertainment and Gambling in 2023, Reflecting Dominant U.S. Presence and Global Engagement.*

The table above delineates the leading countries mentioned in Dark Web discussions related to online entertainment and gambling for the year 2023. In the realm of entertainment, the United States leads with a significant margin, accounting for 19.24% of the chatter, which may reflect its large digital content market and the presence of major entertainment companies. The Russian Federation and the United Kingdom follow, suggesting a substantial interest or targeted activity in these regions.

For gambling, the United States remains at the forefront but with a smaller percentage (13.26%), indicative of the country's active online betting scene. Turkey and China follow, highlighting the global reach of online gambling discussions and possibly correlating with the legal status and enforcement of gambling regulations in these countries.

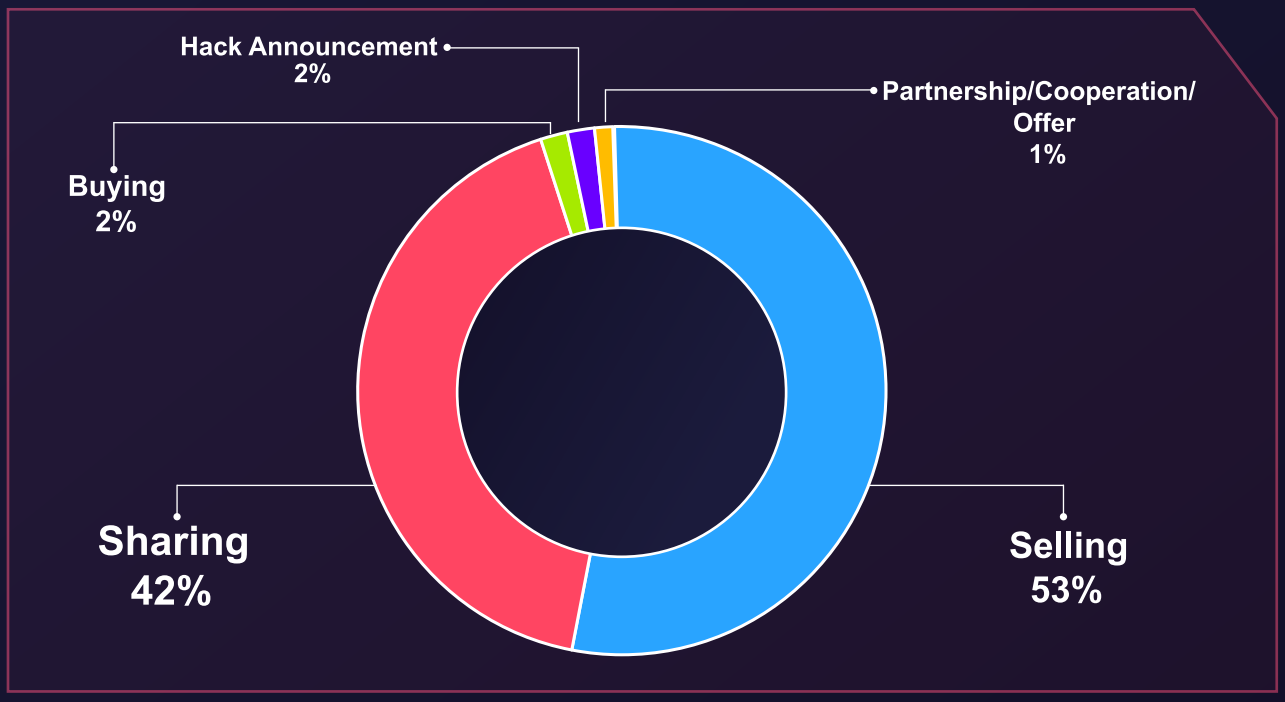
## Content Focus in Dark Web Entertainment and Gambling Discussions




*Dark Web Entertainment Discussions Dominated by Content Sharing and Sales in 2023.*

The pie chart for the online entertainment sector on the Dark Web shows a predominant focus on 'Sharing,' which makes up 65% of the discussions, indicative of a high level of content exchange or leaks within the community. 'Selling' constitutes 30% of the conversation, pointing towards a significant market for illicitly obtained or counterfeit digital entertainment goods. 'Hack Announcements' at 4% suggest that the disclosure of successful breaches is also a topic of interest, albeit to a lesser extent.

## Content Focus in Dark Web Entertainment and Gambling Discussions




*Trade and Information Exchange Lead Dark Web Gambling Discussions in 2023.*

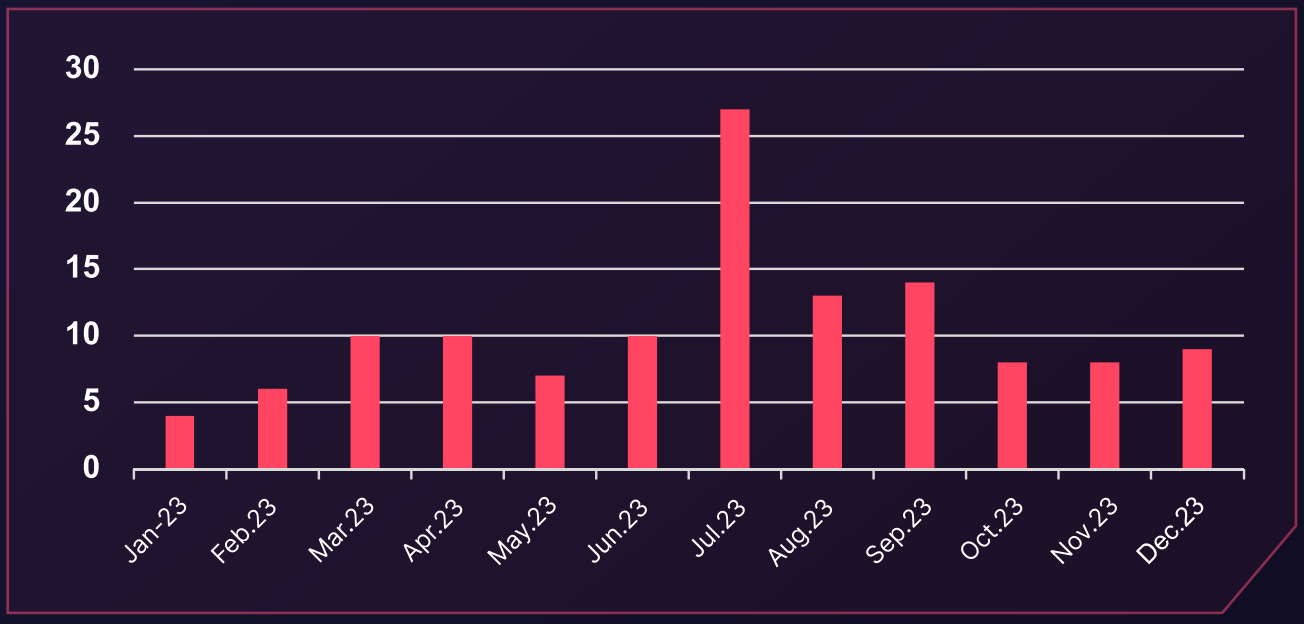
In the gambling sector, 'Selling' leads with 53% of the Dark Web discussions, possibly reflecting the trade of hacked accounts or insider information. 'Sharing' at 42% indicates that there is also a robust exchange of information, which could include tips, betting odds, and potentially compromised data. 'Hack Announcements,' 'Buying,' and 'Partnership/Cooperation' represent a smaller fraction of the discussions, hinting at less frequent but still present activities such as the announcement of new breaches or collaborations for illicit gambling operations.

In the online entertainment discussions on the Dark Web, 'Sharing' significantly outweighs 'Selling,' accounting for 65% of the conversations compared to 30% for selling. This disparity suggests a dominant culture of content dissemination, possibly including the sharing of pirated media, game mods, or leaks within the community. Conversely, in the gambling sector, 'Selling' surpasses 'Sharing,' with 53% of the discussions focused on sales versus 42% on sharing. This indicates a more transactional nature within the Dark Web's gambling circles, where the sale of potentially illicit services, such as betting tips, hacked account details, or access to gambling platforms, is more prevalent than the mere exchange of information. The comparison reveals that while both sectors have active markets for selling and sharing, their proportions differ, reflecting the underlying dynamics and intentions of the Dark Web communities involved in entertainment and gambling.

# Ransomware Trends in Online Entertainment

In the colorful digital world of entertainment, encompassing gaming, gambling, and various leisure websites, the threat of ransomware casts a significant shadow. SOCRadar harnesses the power of expert analysis, machine learning, and artificial intelligence to meticulously monitor ransomware blog sites, leak sites, and Telegram channels. This vigilant oversight is key to uncovering the prevalence and trends of ransomware incursions across these internet domains.

## Monthly Ransomware Attack Incidents in Online Entertainment




*July 2023 Witnesses a Surge in Ransomware Attacks in Online Entertainment, Amidst a Year of Varied Attack Frequencies.*

The bar chart illustrates the number of ransomware attack incidents reported each month in the online entertainment sector for 2023. Notably, July stands out with a peak of 27 incidents, suggesting a possible seasonal surge in cyberattacks or a successful campaign by threat actors during that month. The rest of the year shows variability but no other month approaches the high of July, with consistent activity seen in March, April, and September. These fluctuations may correlate with the release cycles of popular games or high-activity periods in online recreation and gambling.

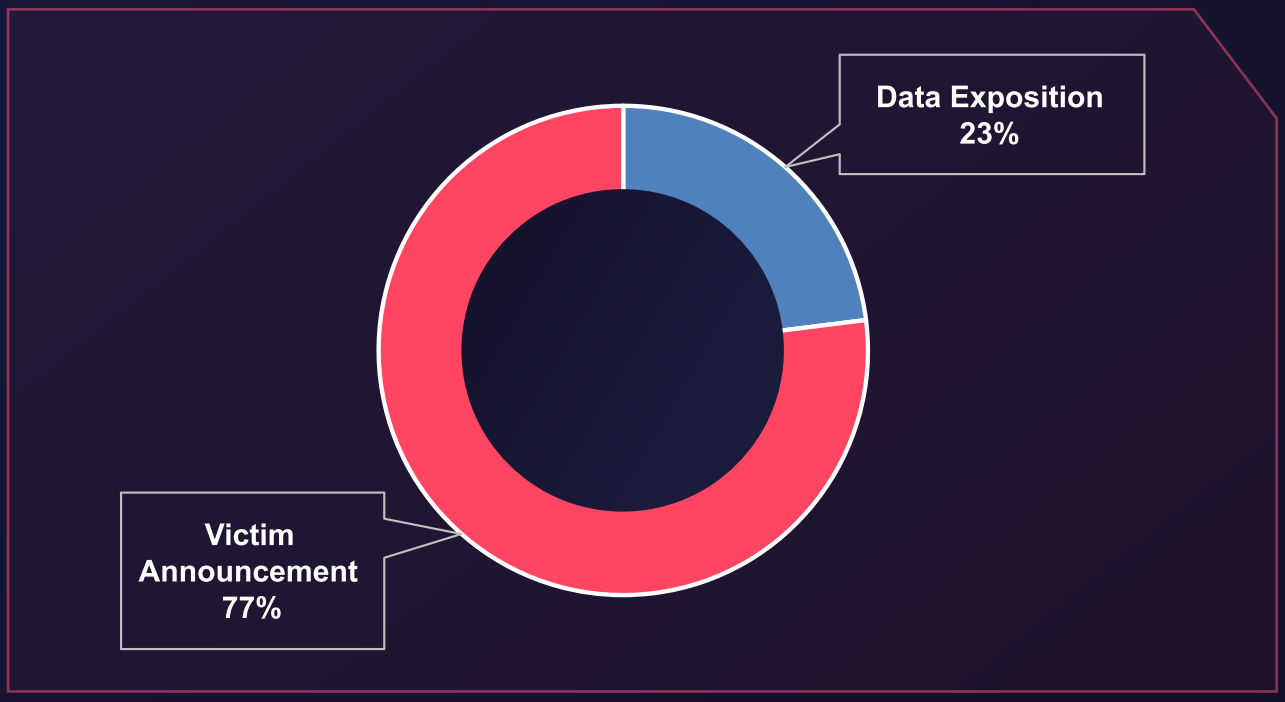
## Predominant Ransomware Groups in 2023's Cyber Landscape

| Activity Ranking of Top Ransomware Groups | |
|---|---|
| LockBit 3.0 | 22,22% |
| Play | 10,32% |
| 8base | 8,73% |
| Cl0p | 8,73% |
| Black Basta | 7,14% |

*LockBit 3.0 Dominates as the Most Active Ransomware Group in 2023.*

The table above ranks the top five most active ransomware groups in 2023, with LockBit 3.0 leading the pack, responsible for 28 incidents, which translates to 22.22% of the total ransomware attacks monitored. This is followed by 'Play' with 13 incidents, and both '8base' and 'Cl0p' tied at 11 incidents each. 'Black Basta' rounds out the list with 9 incidents, accounting for 7.14% of the attacks. This data illustrates not only the prevalence of these ransomware groups but also the potential threat they pose to cybersecurity infrastructures across various industries.

## Dissecting Ransomware Groups' Communication Strategies




*Victim Announcements Predominate in Ransomware Groups' Communications, Outnumbering Data Exposition Posts.*

The pie chart depicts the distribution of post types related to ransomware activity on the Dark Web. A significant 77% of the posts are categorized as 'Victim Announcement,' which suggests that the majority of communication from these groups is aimed at publicizing their successful attacks to exert pressure on victims and possibly enhance their notoriety. In contrast, 'Data Exposition' posts, which involve the publication of stolen data as proof of a successful breach or as a means to force victim compliance or punishment for noncompliance, make up 23% of the posts. This indicates that while data exposition is an integral part of ransomware strategy, the initial announcement to claim responsibility and potentially shame the victim into paying the ransom is more prevalent.

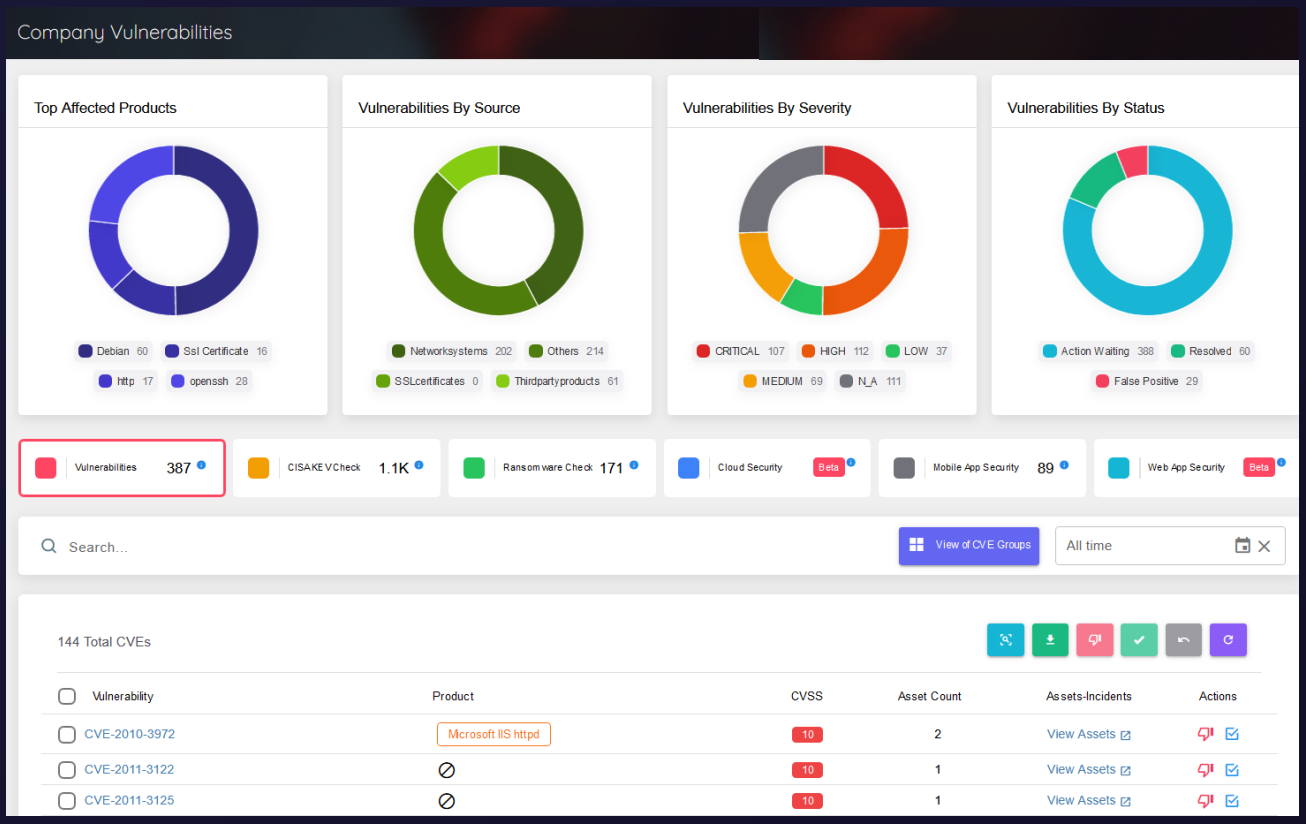
## Ransomware Impact by Country in 2023

| Ransomware Incidence Rates | |
|---|---|
| United States | 44,44% |
| United Kingdom | 7,14% |
| Germany | 6,35% |
| Canada | 5,56% |
| Spain | 3,97% |

*The United States Leads as the Most Ransomware-Affected Country in 2023.*

The table presents a stark view of the ransomware landscape in 2023, with the United States suffering the brunt of the attacks, experiencing 44.44% of incidents. This high percentage, which translates to 56 incidents, reflects the large target presented by the U.S. due to its vast digital infrastructure and valuable data reservoirs. The United Kingdom follows with 7.14% (9 incidents), then Germany with 6.35% (8 incidents), Canada at 5.56% (7 incidents), and Spain at 3.97% (5 incidents). The data showcases not only the global reach of ransomware but also highlights the particular vulnerability of certain nations, potentially due to economic, technological, and cyber-defense factors.

# Conclusion




*SOCRadar External Attack Surface module monitors your company's digital footprint and vulnerabilities for superior security insights.*

In conclusion, the data and trends presented in this report illustrate the critical importance of staying ahead of the curve in understanding and anticipating the movements within the Dark Web, especially in the context of the gaming and gambling sectors. The insights into the Dark Web discussions, ransomware attack patterns, and the countries most affected by these nefarious activities highlight the sophisticated and ever-evolving threat landscape that businesses in the entertainment and gambling industries face.

As an extended threat intelligence company, SOCRadar offers crucial capabilities to these sectors, providing them with the necessary tools and insights to proactively monitor these hidden cyber threats. By leveraging SOCRadar's comprehensive intelligence gathering and analysis, entities within the gaming and gambling spheres can better safeguard their digital assets, protect their customer's data, and maintain the integrity of their operations against the backdrop of an increasingly hostile cyber environment.

# Who is SOCRadar®?

Your Eyes Beyond

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

**21.000+**
**Free Users**

**Dark Web Monitoring:** SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

**Protecting Customers' PII:** Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

**Credit Card Monitoring:** Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

**360-Degree Visibility:** Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

**GET ACCESS FOR FREE**

## MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store

GET IT ON Google Play


Gartner Peer Insights™ 4.9/5


**SOCRadar HQ**
HQ Office: 254 Chapman Rd, Ste 208 Newark, Delaware 19702 USA

**Call**
+1 (571) 249-4598

**Email**
info@socradar.io

socradar.io

Virtual Addresses

**London, UK**
167 City Road Old Street, London EC1V 1AW

**Dubai, UAE**
8W building 5th Floor, DAFZA, Dubai

**São Paulo, Brasil**
7th & 8th Floors Torre Joao Salem, Av. Paulista 1079 São Paulo

**Bangalore, India**
The Estate, 8th Floor Dickenson Road 560042 Bangalore Karnataka