Picture credit: Riot Games

Riot's League of Legends was hit with a $10-million ransomware attack, which the company refused to pay

# GAME ON

**Holly Hagene** *reveals why online gaming is fast becoming the next frontier for cyber crime*

**The popularity of online gaming has driven prolific industries sustained by companies in betting services, casinos and more interactive MMORPGs and online multiplayer games. Unfortunately, with their growing popularity amongst the general public comes the prying eyes of cyber criminals looking for a multitude of ways to exploit the system. One of the most common tools used by these nefarious groups is ransomware or malicious software intended to either steal data or bar a company's access to important files with the hopes of collecting a ransom.**

The use of ransomware has one purpose: to make the affected company pay, whether it's to prevent a leak of sensitive information or regain access to crucial documents. Gaming developers like Riot Games, have been the victim of ransomware attacks. Riot's January 2023 incident involved the theft of source code for it online multiplayer League of Legends and came with a $10 million price tag that the company refused to pay. This ransomware attack came just four months after Rockstar Games, the creators behind Grand Theft Auto, confirmed that source code for the unreleased Grand Theft Auto 6 had leaked online. In neither instance was user data at risk, but transactional data, which can include user information, is at risk.

Additionally, the user can suffer if the attack results in a loss of service within the game. In March 2020, SBTech, a provider of online sports betting solutions, suffered an attack on its network. The incident resulted in a shutdown of its data centres, which affected partners that used the company's iGaming tech and the public trying to place bets.

When a website is forced to shut down or an online game has to pause servers because of a ransomware attack, that company not only risks losing revenue, but also long-term trust and loyalty. If customers can't access a website, especially one meant to provide entertainment, they're likely to go elsewhere. A company's reputation can be damaged and they are more prone to losing business as a result of a ransomware attack.

Unfortunately, when a company or video game developer feels compelled to pay the ransom, there's no guarantee the actor will follow through with their end of the promise. In fact, it's common for another sum of money to be requested and for the cycle to continue. In Riot Games' case, the ransom was not paid. Instead, Riot alerted League of Legends players of the breach and how it could impact the game's ongoing development of new content.

But how do these attacks occur? When a new online game or gambling site is released, it's not intentionally left vulnerable to attack. On the contrary, measures are taken to ensure maximum security. However, loopholes and gaps in security are not uncommon in the gaming industry, and it's here that actors find their way in.

THREATS NEED TO BE CLEARER FOR PLAYERS AS ONLINE GAMING BECOMES MORE POPULAR

How ransomware works may vary from one variant to the next, but there is typically one thing in common. When the malware is embedded in the target system and launches, it encrypts files at that destination, locking them away from the company. The process starts with the infection of a system, often achieved through email scams including links to the malware.

When the ransomware is in the system, it begins the encryption process. To prevent a system failure and instability that would alert to an attack, many variants of this malware are careful in what they encrypt. Some will even delete backups or shadow copies of files to complicate recovery without a decryption key.

The question still remains: how is the gaming industry left vulnerable to these attacks? To answer that, let's consider the backend of an online casino. One of the most important components of an online casino or any digital better is the network. There must be an open source for this data and information to flow. Since it's all transactional, it includes sensitive user information that requires a high degree of security to keep safe.

However, that very same network is a point of entry for any malware, and it only takes one user to open a floodgate. One well-worded email to a contact list of hundreds if not thousands of employees has a higher opportunity to be enacted on and if just one employee clicks a random link requesting to set a time for a call, they can infect their network-connected computer, and cause a trickling effect across all associated servers.

Much of the gaming industry is perpetually online, whether it's offering betting on the latest football game or sending players on epic quests together in the latest MMORPG. There is always a network or a server that can be compromised, and mission-critical employees are linked to these networks, giving inadvertent access to actors. It's because of this that there needs to be ongoing network visibility, meaning a set of eyes constantly scanning for vulnerabilities, security gaps and active cyber attacks.

Network visibility is still lacking in much of the gaming industry, which increases not only the threat of an attack but the potential severity. If an actor is able to grab source code or complete shutdown operations for a period of time, they have the ability to greatly impact the survivability of that game or website.

Security information and event management (SIEM) is a rather simple concept that can have a great impact on the overall security of a game developer's network and servers. SIEM is an internal protocol for real-time analysis of data logs to determine if there are active threats or the potential for security breaches. SIEM ensures that the company is in compliance with all data storage requirements, further guaranteeing that user data won't be compromised by ransomware attacks.

The gaming industry is light on centralised SIEM, meaning IT and security teams are either manually combing through datasets looking for concerns or not verifying the security of the data. In both instances, actors have a greater opportunity of infecting the network with ransomware.

## SECURITY ENDS WITH GAMERS

The focus on a more secure industry may start with the creators and website owners, but it eventually becomes the responsibility of the user. While a gamer won't be responsible for preventing ransomware attacks on a developer's network, they themselves are susceptible to individual attacks.

The very same schemes used to trap creators and site owners can be implemented at the user level. An email under the guise of an official password change request or some sort of in-game giveaway can include a link to unknowingly download ransomware. Once ransomware is on a computer, any other PC connected to the same network can be at risk.

While gaming companies have to look to more advanced tactics to prevent malware attacks, individual users simply need to practice safe surfing. When browsing the internet, checking emails or scrolling through social media, click only verifiable, trusted links. A link from unknown parties shouldn't be clicked until its origins can be determined. As online gaming lounges become more and more prominent, it becomes more and more important for these threats to be communicated to players.

Companies that run any form of online game, be it an MMORPG or gambling site, should frequently communicate potential risks to their players. Though they may not contract the ransomware directly from their game, actors can use the online game as a front to distribute threats by posing as an official representative and offering exclusive deals or new content. If players start to believe that a certain game is unsafe, they will move on to a competitor that may have more stringent security measures.

The gaming industry is under constant threat from these attacks, and it's no secret why. In 2021, the global video game market was valued at $195.65-billion by Grand View Research. At the time of the analysis by Grand View Research, 2022 to 2023 was expected to see a compound annual growth rate of 12.9 percent. As more money flows through the industry, more bad actors are going to emerge looking for ways to exploit the current systems.

Unfortunately, minimal security is never something any online gaming outlet will have the luxury of enjoying. In fact, actors are only more likely to produce more advanced threats against security, forcing creators to invest more in the protection of their core data. When it only takes one employee working on the network to open a link in the wrong email, detection and prevention of active threats becomes critical to the longevity of a service.

Online gaming isn't a new concept, but the push for more Games as a Service requires a greater focus on security. Even as more games enter the Web 3.0 space, how game developers and creators look at security will need to change. What worked at the onset of services like Xbox Live and PlayStation Network are antiquated concepts that won't protect against modern ransomware, and what works today won't stop ransomware developed five years from now.

Just as online gaming is ever-evolving, so too are the security threats that creators and developers need to be wary of. The purpose of ransomware may never really change, but how it's used to disrupt services can and will. Only through enhanced network visibility, a centralised SIEM and better security training for all employees will the gaming industry be able to combat bad actors ●

**Holly Hagene** is the Director of Go-To Market for NetWitness.

**The source code to Rockstar Games' Grand Theft Auto 6 was leaked online by cyber criminals before the game's official release**

Picture credit: Rockstar Games