Solution Brief

Ransomware Attacks on the Gaming Industry

Introduction

The gaming industry is experiencing a surge in cyber attacks because of its vast reservoirs of sensitive customer information, financial transactions, and interconnected operations. Zscaler's ThreatLabz threat research team reported earlier this year that ransomware attacks had grown 37% overall year-over-year, with the average cost of an attack reaching a whopping $5.3M. The Department of Homeland Security recently released a report stating that ransomware groups are on pace for their second most profitable year ever, driven largely by 'big game hunting' attacks against large organizations.

In light of the recent ransomware attacks and the growing trend of attacks against the gaming industries, we want to offer a broader analysis of ransomware attacks and trends affecting the gaming industry and give practitioners an informed perspective for how they can safeguard customer trust and data.

Key Takeaways

- The gaming industry is a treasure trove of customer data and transaction details. The nature of the gaming industry requires companies to handle high volumes of customer data and transaction details.
- Social engineering tactics played a prominent role in the most recent gaming cyberattacks. Recent cyberattacks continue to exploit social engineering techniques, but with a notable shift toward phone-based communication instead of email. This approach has proven effective due to lack of awareness and training when compared to email-based spam attacks, which are more familiar and often require education by organizations.
- International law enforcement agencies shut down two of the largest initial access brokers, Emotet and Qakbot, that should potentially reduce ransomware activity worldwide in the near term. The fall of Emotet and Qakbot reduced primary infection vectors that leveraged malicious email attachments and links. However, threat actors are turning to alternative techniques to carry out attacks.
- Minimizing external attack surface, preventing initial compromise, stopping compromised users & insider threats by eliminating lateral movement, and preventing data loss are the four core zero trust tenets for ransomware prevention.
- UNC3944, an affiliate of the BlackCat ransomware threat group, is believed to be responsible for the recent cyber attacks on the gaming industry.
- Ransomware attacks all follow a similar attack sequence. Understanding this attack sequence and employing security controls and strategies leveraging zero trust architecture is the key to an effective defense.

Attack Vectors and TTPs

Ransomware attacks have long been conducted using a variety of techniques including phishing and spam email, brute force attacks, and the exploitation of vulnerabilities.

The use of phishing and spam email has long been a primary infection vector for ransomware threat actors and/or initial access brokers. However, two of the largest sources of spam email, Emotet and Qakbot, were disrupted by law enforcement operations. Qakbot in particular was a major player as an initial access broker for ransomware operations including BlackBasta. In recent weeks, ThreatLabz has observed a significant decline in BlackBasta ransomware activity corresponding to the demise of Qakbot. As a result, many ransomware initial access brokers are likely to use alternative techniques and recent attacks on the gaming industry demonstrate how these attacks (at least in the short term) are likely to be carried out. Interestingly, the attacks still continue to leverage social engineering, but rely on speaking over the phone rather than through email. This tactic has been used in prior attacks and appears to be increasingly effective because there is a lack of education, in contrast to spam, which is better understood and often requires mandatory training at many organizations.

Although spam was not used in some recent attacks, the end goal is the same: to compromise a target environment, perform lateral movement to obtain access to an administrator's account, exfiltrate sensitive information, and (optionally) deploy ransomware. ThreatLabz has observed the latter being used less frequently in attacks in so-called encryption-less extortion attacks. Many of the extortion-less attacks have been targeted at multi-billion dollar companies with the intent to reduce the impact and disruption associated with file encryption. In May 2023, the Clop ransomware group leveraged a supply-chain style attack targeting a zero-day vulnerability in the MOVEit Transfer application enabling the group to access and steal sensitive information from hundreds of organizations. That information was then leveraged to extort victims into paying a ransom.

At the present time, public companies in the United States are not required by law to disclose breaches, and therefore, encryption-less extortion attacks may enable companies to avoid public disclosure. However, the Securities and Exchange Commission (SEC) has adopted a rule that will require public companies to disclose material cybersecurity incidents within four days that will become effective in December 2023. This change will likely have an impact on ransomware negotiations and lead to a significant reduction in the number of companies that today pay ransoms to avoid public disclosure of a breach and the corresponding release of stolen information. To learn more about the SEC's cybersecurity ruling and how it impacts public companies, visit The Impact of the SEC's New Cybersecurity Policies.

Suspected Threat Actors

UNC3944 has taken over ransomware news headlines with multiple high-profile attacks against casinos.

A financially-motivated threat group that has been active since May 2022, UNC3944 (a.k.a. Scattered Spider, Muddled Libra, Oktapus, and Scatter Swine). According to a Reuters report, UNC3944 is believed to be composed primarily of young adults from the United States and United Kingdom[1]. Their early attacks were waged against telecommunications organizations using techniques such as SIM swap scams, multi-factor authentication fatigue attacks, and SMS phishing.

More recently, UNC3944 has become an affiliate group for BlackCat/ALPHV ransomware—a notorious malware family called out as one of the top 5 ransomware families in our 2023 ThreatLabz State of Ransomware Report.

BlackCat was the second most prolific ransomware group performing double extortion attacks of the past year; only LockBit

[1] Source: https://www.reuters.com/technology/moodys-says-breach-mgm-is-credit-negative-disruption-lingers-2023-09-13/

was responsible for more data leaks. The BlackCat group is a sophisticated RaaS operation that has been active since November 2021 (after previously being branded as DarkSide and BlackMatter), and is known to leverage affiliates that use a variety of methods to infiltrate victim networks, including exploiting known vulnerabilities, phishing attacks, and social engineering. Once inside a network, BlackCat operators typically use a combination of tools and techniques to move laterally, escalate privileges, and exfiltrate data. The group then deploys its ransomware payload, which encrypts the victim's files.

Hackers Leverage Multiple Trending Techniques

The UNC3944 attacks underscore three major trends that ThreatLabz has reported in our research:

Ransomware-as-a-service: Many of the most popular and damaging ransomware families of the last year are able to scale their profits and operations using a Ransomware-as-a-Service (RaaS) model. In this model, ransomware groups outsource the infiltration, lateral movement, data theft, and ultimate deployment of their ransomware payload in exchange for a commission.

Double extortion: In double extortion ransomware attacks, threat actors not only encrypt data on the victims' systems, but also exfiltrate it and threaten to publish it if ransoms are not paid. In 2021, ThreatLabz observed 19 ransomware families that adopted double or multi-extortion approaches to their cyberattacks. This has since grown to 44 ransomware families observed. The data extortion component of the attack has become so profitable that many threat families are now waging encryption-less ransomware attacks in which they do not even bother to encrypt data, but instead focus entirely on stealing data. These encryption-less ransomware attacks have the side benefit of attracting less attention from authorities because they do not disrupt business operations, yet are still extremely effective at generating ransom payments.

Social engineering as a method of compromise: UNC3944 frequently leverages social engineering tactics in order to compromise systems. Many of their recent attacks began with phishing that enabled them to steal credentials and gain access to systems without triggering security controls.

Ransomware Best Practices and Mitigation

Guarding against ransomware attacks requires a comprehensive approach that tackles every stage of the threat, minimizing potential harm.

The Zscaler Zero Trust Exchange offers comprehensive ransomware protection across this entire attack sequence, with best-in-class security controls that are all delivered inline and at the edge. By adopting the following guidelines, you can effectively reduce the risk of falling victim to a ransomware attack.

- **Prevent initial compromise:** Employ consistent security policies that ensure uncompromising security starting at your source code. By implementing extensive SSL inspection capabilities, browser isolation, inline sandboxing, and policy-driven access control, you can thwart access to malicious websites, block channels of initial compromise and detect unknown threats from reaching your users.
- **Stop compromised users and insider threats:** Combining inline application inspection and Identity Threat Detection & Response (ITDR) with integrated deception capabilities empowers you to detect, deceive, and effectively stop potential attackers, whether they are external threats or insiders with malicious intent.
- **Minimize external attack surface and eliminate lateral movement:** Prevent hackers from maneuvering within your network by disconnecting applications from the internet and embracing a zero trust network access (ZTNA) architecture. Directly connecting users to applications, and applications to applications, rather than the network itself, significantly restricts the potential reach of an attack.
- **Prevent data loss:** Implement inline data loss prevention measures with full TLS inspection and thoroughly inspect data both while in transit and at rest, to effectively stop data theft attempts. Stay one step ahead of threat actors by regularly updating software and providing comprehensive security training.
- **Perform frequent audits:** Regular cybersecurity audits play a crucial role in enhancing best practices and mitigation tactics. Audits can assess compliance adherence, which is pivotal when refining a cybersecurity strategy for the gaming industry, especially as compliance & regulations change – like the SECs new ruling on cybersecurity. In addition, regular audits can help you identify knowledge gaps in your user training and employee awareness.
- **Educate and train your employees regularly:** Once knowledge gaps are identified, targeted and custom cybersecurity training programs can be put into place to empower and inform employees. This boosts employee awareness, and teaches them to recognize and respond to threats effectively.

zscaler™ | **Experience your world, secured.™**

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.