Your Casino Has Been Hacked by Ransomware!

by Andrew Cardno

The Indian gaming industry has officially been hacked. This has been a good year for cyber hackers with a number of tribal properties having been subjected to devastating cyber attacks. These hacks have resulted in property closures, in addition to closures for COVID-19.

The success of these attacks on tribal nations expose the industry to further attacks by emboldened hackers. These attackers have now gained experience in how tribal gaming operators run their facilities. Armed with this knowledge, they can now make more organized and effective attacks, threatening the livelihood of the gaming industry.

A recently hacked tribal nation stated, "While our investigation is ongoing, we have confirmed the cause was an external attack on our computer network." Now consider for a moment that this occurred at one of the most sophisticated operations in the U.S. with a large, well-resourced IT department.

The Cost

If you are still wondering if this requires any attention answer these simple questions:

1) What will it cost for you to close your operation for four weeks while you rebuild all of your systems to allow your gaming operation to restart?

2) Are you going to have to pay the ransomware attack fees rather than suffer the impacts of the cyber hack. If so, are you going to notify regulators that you have done this?

3) What could cyber hackers do with your customers private information?

Soft Underbelly: Systems

Ten years ago, knowledge of your gaming systems was hard to find and these systems were generally isolated from the outside world. In today's world, cyber criminals have specific knowledge of gaming systems, and furthermore they have a vast array of new systems to direct their attacks at. Each one is a potential point of weakness.

Today, the gaming industry is dependent on systems to operate. It is likely that your operations are running on systems that were designed 25-35 years ago. The fundamental communication protocols and methods in your older systems were never designed to handle cyber-attack, they were instead designed to operate as stand-alone systems isolated from the outside world. To further complicate the system's challenges, there are now enormous pressures to move gaming data into the cloud for everything from analytics to customer relationship management. This cloud move requires that your operation open communication pipelines (normally bi-directional) permanently.

The Incentive: Cash

Gaming systems handle vast amounts of cash and there is substantial potential benefit for hackers should they gain entry into your gaming environment. These cyber-attacks can range from hybrid money laundering attacks, to straight ransomware, to threats of publication of sensitive gaming data. At the center of this is the fundamental truth that the industry handles vast amounts of cash, and this cash presents creative criminals with a large set of potential attack vectors.

In addition to the risk associated with the cash you handle, your customer data is loaded with extremely sensitive information. For example, your customer database holds the behavioral and spending patterns of high net worth individuals. Criminals having this data potentially opens your customers up to cyber-attacks.

Example Threat Analysis: Multi-Factor Authentication

Your security team might say, multifactor authentication will secure everything. While it is true that multifactor authentication provides for substantial enhancement in your security there are now well-known attack methods. To illustrate the vulnerability, look at two stories as presented from the FBI in a Private Industry Notification (PIN).

Live Demonstration of Hacking

FBI reporting identified several methods cyber actors use to circumvent popular multi-factor authentication techniques in order to obtain the one-time passcode and access protected accounts. The primary methods are social engineering attacks which attack the users and technical attacks which target web code.

In February 2019 a cyber security expert at the RSA Conference in San Francisco, demonstrated a large variety of schemes and attacks cyber actors could use to circumvent multi-factor authentication. The security expert presented real-time examples of how cyber actors could use man-in-the-

middle attacks and session hijacking to intercept the traffic between a user and a website to conduct these attacks and maintain access for as long as possible. He also demonstrated social engineering attacks, including phishing schemes or fraudulent text messages purporting to be a bank or other service to cause a user to log into a fake website and give up their private information.

At the June 2019 Hack-in-the-Box conference in Amsterdam, cyber security experts demonstrated a pair of tools – Muraena and NecroBrowser – which worked in tandem to automate a phishing scheme against users of multi-factor authentication. The Muraena tool intercepts traffic between a user and a target website where they are requested to enter login credentials and a token code as usual. Once authenticated, NecroBrowser stores the data for the victims of this attack and hijacks the session cookie, allowing cyber actors to log into these private accounts, take them over, and change user passwords.

Cyber Security Action Plan

The following is a checklist for your gaming operation, including some areas for consideration. This list is not exhaustive, but should get you started on building your personalized action plan based on your current situation.

Take this seriously: First, take this seriously. These attackers are not timid, they are well equipped, well trained, and now have experience in gaming.

Build Your Ransomware Action Plan: Your business needs an immediate cyber security action plan. Plan out what you are prepared to pay for ransoms (not recommended), who will be called on, how you can go about a complex set of system rebuilds, if you can operate while isolated from systems housed in the cloud.

Appoint a Head of Cyber Security: They need to be experienced in cyber security and ready to engage in a plan to take on criminal activity. The challenge with this role is that the better the person is at their job, the less likely it is that you will be hacked. This can counterintuitively make their requests for resources potentially harder to justify due to the apparent lack of any security danger that results from them doing their job so well.

Recognize Gaming is Different: Your tribal gaming industry operates with older systems and in very specialized regulatory environments. These regulatory environments need to be part of your cyber plan. For example, do you have a plan to manage the relationship with regulators following a cyber-attack?

Build Contingency Plans: A backup gaming system that is clean and ready to go should be in place in the event of a cyber hack. This gaming system could be from a low-cost provider that provides only minimal functionality, but enough to keep the business running.

Buy Insurance: Cyber insurance is a powerful way of establishing the cost of fighting cyber criminals as this insurance covers the cost of a skilled response team. This response team can cover services from diagnosis of attack points to handling of public relations fallout.

Isolate Key Systems: There is no substitute for physical separation of systems. You could, for example, have the ability to run your core systems in an environment that is completely cut off from the outside world, or run it behind incredibly strong firewalls. Your response plan could include isolation of systems. As an example, your business continuity does not require your internal email system to be on the same physical network as your pit management system.

Control Cloud Connectivity: The cloud is a part of our technology world and in many cases it is cost-effective and convenient. Have you thought through the regulatory impacts on your business of cyber criminals gaining access to systems that are governed by state law?

Protect Your Data: If you close due to cyber-attack you are going to need data to get going again. Having your data in a strong data vault gives you options for recovery if you are hacked.

Monitor Vendors: Your vendors need access, especially in the world of COVID where it is not practical to physically visit. Are you recording all activities of the vendors? Are you subjecting them and all of their employees working on your systems to careful background screenings? What legal jurisdiction are your vendors' employees operating from? Is the system of law in this jurisdiction one that provides sufficient legal protection?

Implement Training and Awareness: In doing your cyber security threat analysis, the biggest difficulty you likely face is your team. They must be trained properly in cyber security and kept up to date on their skills. Human points of contact are much easier for criminal hackers to exploit, because tricking a human is almost universally easier than tricking a computer. Cyber security is an ongoing war, and if your team's training stagnates, it leaves them open to new avenues of attack the cyber criminals

"Ransomware and other cyber-attacks are now a reality in the tribal gaming world. There are two optimal times to implement your cyber security strategy, the first was about 10 years ago; the second is today."

will develop in the future. For example, is your team aware of the likely methods that cyber criminals will use to bypass multifactor authentication? If they are not, they should be, and the next time an inventive criminal comes up with a way to try to break into your systems, your team needs to be trained in defense about that, too.

Engage Expert Support: There are experts out there and their cyber security horror stories are going to scare you. It is much more cost effective to engage experts while you are still operating, than waiting until you are wondering if you should pay the ransomware fees so you can stay open.

Ransomware and other cyber-attacks are now a reality in the tribal gaming world. There are two optimal times to implement your cyber security strategy, the first was about 10 years ago; the second is today. If you are a leader in cyber security space, share your knowledge so everybody benefits. If you are not, take action today to become a leader. ♣

Andrew Cardno is CEO & Founder of Innovation Gaming Group. He can be reached by calling (858) 254-0412 or email andrew.cardno@innovationgaminggroup.com.