Ransomware and Why it Matters

by Andrew Cardno

Malicious actors are targeting casinos around the world, and it is likely that your operation is subjected to thousands of cyber attack attempts each month. These attacks come in many forms – one of the most difficult to handle is the ransomware attack. In short, the ransomware attacker locks up your files and systems, then extorts you for payment in order to unlock said files.

Technically, ransomware is a kind of computer virus, or malware, that infects your computer, and then all computers on the same network – encrypting files and making computers unusable until such time as you make a payment to the hackers. Cybersecurity is the means by which you can protect yourself from such attacks. To illustrate how detrimental such cyber-attacks can be, let's consider a hypothetical example of one such attack, and then examine ways it could have been prevented.

An employee is sitting at their desk, sifting through a day's worth of emails. It's all routine – replying to coworkers, sending documents, and communicating with patrons. Hidden among the mundanity of these everyday emails is a single message that is just a little bit wrong. Though not all people would have the wherewithal to notice, this one message, purporting to be from the employee's manager, is actually a cleverly hidden email from a hacker.

It is terrifyingly easy for anybody to go online and find a website that will send a message with a fake email address. If they wanted to, a hacker could send you a message from Bill Gates, inviting you to dinner. While something like that would be pretty suspicious from the get-go, this also means that a message from your direct superior can be faked just as easily. What reason would you have to be suspicious of an email from somebody you work with directly? As soon as you download the innocuous attachment in the email, the cyberattack begins, and all it takes is a single mistake from a single person inside your organization.

After opening the ransomware email, your computer stops responding as all its files are locked behind powerful encryption software. Due to your connection to the internal network, every computer in the building is soon infected with this virus. You cannot work, interact with patrons, make transactions, or do anything else with the computer. The only thing you can see on every screen in the building is a message stating that every computer will be wiped of its data if you don't make a payment of $100,000 worth of bitcoin to a specific web address within a week. While such a payment may not be considered much of an issue to you or other companies, the time and revenue lost while the issue is resolved would likely be worth much more. The hit to your organization's reputation could also be sizable if customer information is lost or leaked. On top of that, some hackers may not send you the decryption key even if the payment is received, and ceding to their demands encourages hackers to engage in more illegal behavior. Due to these considerations, meeting hackers' demands is generally regarded as a bad idea by the intelligence community. You should contact the FBI when a ransomware or other cyberattack occur. They have well established response programs. Not only can an investigation be launched to catch the perpetrators, but government agencies have their own computer experts that can work to extract data from your companies' computers without paying the hackers' ransom.

This all sounds like an enormous hassle, and if you could avoid going through all of this in the first place, your time could be used much more efficiently. Luckily, there are ways to protect your network from hackers. The most important consideration is for the users. People are the easiest facet of a networks security to exploit. No matter how good your firewall is, if somebody clicks on a malicious link, that firewall means nothing. Holding seminars to teach your employees the proper measures and precautions to take while on the internet makes it infinitely harder for hackers to gain entry into your network. Make sure your employees know to double check the spelling of email addresses, especially if there is a link attached that they intend to download. Teach them not to click on links at all unless they are from trusted sites, to avoid clicking on pop-ups, even the little x's that seem to be the means by which such things would be closed. These and many more strategies for safe internet usage can be taught to your employees in order to protect against ransomware attacks.

An equally important facet of cybersecurity for you is backing up data. If you store a recent copy of files from necessary computers off-network in some manner, then even a "successful" cyberattack is made much less effective. Instead of yielding to the hackers' demands, your computers can simply be wiped of all data, and then have the backup information loaded in. It's a fairly simple thing for IT professionals, whom you either hire or employ, to install a means of backing up data for your company.

Mere months ago, a major cyberattack was carried out on a prominent tribe's computer network. Though the encrypted documents were ultimately recovered, many hours of time and money were lost as a result of the attack, and some of the computers themselves are still inoperable. This example shows two notable facts: (1) cyberattacks can be combated by means other than complying with hackers' demands; and (2) regardless of how the attack is handled, it becomes a significant loss of time and money for the affected party. In any circumstance involving cybersecurity, prevention is a much better option than dealing with the repercussions of a lacking cybersecurity system. As the age old adage goes, "Better safe than sorry." ♣

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