# NIGC Tech Alert

## Tribal Gaming Operation attacked by “Cuba” ransomware

The threat of attacks on IT systems is always present and one of the many reasons for the need for strong Information Technology system controls and security measures. One of the most common and persistent types of attacks used in recent years both inside and outside of the gaming industry is that of malicious software known as ransomware.

Ransomware is a term for a family of malicious software that acts like a Trojan horse. The software runs quietly in the background of an infected system and searches for and encrypts key files such as players club databases and casino management systems. The files become locked and unusable to the victim until a decryption key is applied. Once the encryption process is complete, the attacker notifies the victim and demands a ransom.

The majority of ransomware tends to spread and propagate by way of emails with malicious attachments. The victim is persuaded to open or execute an attached file that infects the system and can spread to other systems on the same network. Due to the sheer volume of these emails, an attacker only needs a small percentage of would be victims to fall to the deception. The infected email attachment can be an Excel spreadsheet, an Adobe Acrobat document, a compressed Zip file, or one of many other types of files. Other popular attack vectors include fake software updates and pirated copies of popular applications.

Recently, a tribal gaming operation was the victim of such an attack. There are many families of ransomware available to criminals and more being crafted every day. In this particular case the ransomware “Cuba” was used. This particular ransomware appends ".cuba" to infected files and requires the victim to email the threat actor for the decryption key. (e.g., Important_spreadsheet.xls becomes -> Important_spreadsheet.xls.cuba) A ransom note tells the victim that databases and the contents of the ftp and file servers were stolen before the files were encrypted. Cuba uses RSA-2048 encryption and targets the Microsoft Windows operating system. Therefore, the importance of strong antivirus and intrusion detection systems and user education cannot be overemphasized.

The FBI advises against paying ransom fees. Doing so rewards these criminals’ illegal actions and provides no guarantee that the files will be decrypted after payment. NIGC recommends strong IT controls be put in place at tribal regulatory agencies and gaming operations to mitigate these threat actors.

Should assistance be necessary regarding the types of systems and controls to put in place to reduce the risk of ransomware or other such IT vector attacks, please don’t hesitate to reach out to the NIGC. The NIGC offers technical assistance, training courses, IT audits, and other tools and resources to help identify potential weak areas and improve security and IT controls.

Please find our recent posting on cybersecurity at
https://www.nigc.gov/images/uploads/Tribal_Cybersecurity_Readiness.pdf

Please review the FBI recommendation on ransoms
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

September 11, 2020

Division of Technology