NIGC Tech Alert

“Avaddon” Ransomware infiltrates Tribal Gaming Operations

The threat of attacks on Information Technology (IT) systems is always present and emphasizes the need for strong IT system controls and security measures. Recently, a tribal operation was the victim of the Avaddon ransomware attack.

Avaddon is offered as a Ransomware-as-a-Service (RaaS) or lease ransomware model, enabling cybercriminals to utilize it as desired, provided they return a percentage of profits to Avaddon developers as commission. An additional threat presented by the ransomware operators of Avaddon is the threat of public posting of the victim’s encrypted data on the dark web and performing Distributed Denial of Service (DDoS) attacks against the victim’s network. The extortion/data leak process typically (1) provides a leak warning (2) leak 5% of data if ransom isn’t paid in 3 to 5 days (3) full leak if ransom is not paid after 5% leak. The exfiltrated data is delivered in compressed zip files to dark web leak websites.

In recent news, the Avaddon ransomware group has announced they are shutting the operation down and giving thousands of victims a decryption tool for free. The internet community forum, “Bleeping computer” was sent an anonymous email with a password and link to a zip file named “Decryption Keys Ransomware Avaddon”. The file included over 2,900 victims of Avaddon ransomware. The files were verified and a free tool has been created for Avaddon victims to use to decrypt their files.

The FBI advises against paying ransom fees. Doing so rewards illegal actions of criminals 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.

The NIGC offers technical assistance, training, IT audits, and other tools and resources to help identify potential vulnerable areas and improve security and IT controls. For additional information, please email itsupport@nigc.gov

Resources

Reporting Internet Crime to the FBI:
https://www.ic3.gov/

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

Additional information regarding how to remove Avaddon from PCRisk:
https://www.pcrisk.com/removal-guides/18039-avaddon-ransomware

Bleeping Computer: Avaddon ransomware shuts down and releases decryption:
https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

Malwarebytes Labs blog post on Avaddon:
https://blog.malwarebytes.com/ransomware/2021/05/avaddon-ransomware-campaign-prompts-warnings-from-fbi-acsc/

June 16, 2021

National Indian Gaming Commission

Division of Technology