NIGC Tech Alert

2024: Ransomware Trends

Ransomware affected 66% of organizations in 2023, according to Sophos' "The State of Ransomware 2023" report. This trend is expected to continue in 2024 as cyber criminals continuously find new methods for pressuring victims to pay a ransom. Solely encrypting data and demanding financial payment is rapidly becoming a tactic of the past. The evolution of Ransomware-as-a-Service (RaaS) makes the threats more prolific and facilitates a phenomenon called 'Triple Extortion'. Bad actors can take ownership of sensitive data, leave it unencrypted for use, but threaten disclosure if unpaid. Affiliates of the same RaaS gang can simultaneously attack an organization and compete for the ransom. One affiliate could focus on " low and slow data exfiltration in hopes of a large data extortion payout, while the other affiliate came with a more "smash-and-grab" operation that helped to expose the first" (SCMagazine, 2024).

Mobile ransomware attack is another trend to be on the lookout for in 2024. Employees can be lured into downloading mobile ransomware through social networking platforms while thinking that they are accessing innocuous content or software. As stated by Shridhar Mittal Zimperium , "The explosive growth in mobile device and app usage has created an ever-growing attack surface. Mobile devices are integral to the way we work, communicate, navigate, bank, and stay informed – creating new opportunities for malware" (Zimperium, 2024). Understanding mobile risk is a crucial first step in securing mobile device management.

Supply chain attacks where third party and legitimate system tools are leveraged to launch ransomware attacks is another evolving trend. Since July 2023, the Federal Bureau of Investigation (FBI) had been observing the trend where ransomware actors exploit vulnerabilities in vendor-controlled remote access to casino servers, and companies are victimized through legitimate system management tools with elevated network permissions. The FBI released a Private Industry Notification in November 2023 to draw attention to the trend and encourage organizations to implement specific recommendations for reducing the likelihood and impact of ransomware incidents.

Generative AI and deepfake capabilities present serious challenges. While AI can be used to protect against ransomware spreading by detecting, isolating, and deleting infected files. Machine learning can be employed to create AI models that are trained by data sets to recognize the difference between clean and malicious files. Unfortunately, AI can also allow bad actors to conduct more targeted attacks. In the future, AI may be employed to fuel ransomware attacks. Malwarebytes and Barracuda Networks predicts ransomware with AI won't be seen in the wild for another one to three years (Venturebeat, 2024).

These ransomware threats relevant to Indian Country along with several others reinforce the need for extra vigilance in securing the infrastructure, educating users, and mitigating vulnerabilities expeditiously. The NIGC offers technical assistance, training courses, IT audits, along with other tools and resources to help the tribal community be proactive in combating cybersecurity threats.

To preview additional information on the FBI's Private Industry Notification, go to **https://www.ic3.gov/Media/News/2023/231108.pdf**

Review Cybersecurity and Infrastructure Security Agency (CISA) Stop Ransomware Facts Sheet at **https://www.cisa.gov/stopransomware/fact-sheets-information**