Prestige and Other Ransomware Attacks Highlight Need to Update Cyber Security

On October 11, a Russian-based threat group known as IRIDIUM carried out a series of coordinated attacks. Victims included organizations that provide or transport military and humanitarian assistance to Ukraine. Recent ransomware attacks such as this Prestige attack serve as an indicator of ransomware trends and a reminder of the need for improved security.

Recent Ransomware Attacks Suggest Cybercrime Patterns

The ransomware landscape has evolved quickly in recent years as technology and cyber security awareness continue to advance. On the one hand, as organizations implement tamper-resistant backups and more sophisticated malware detection, they significantly reduce the risk of data loss. On the other, attackers continually adjust their attack methods.

An overview of several key ransomware attacks in 2022 illustrates some of the current trends.

- Prestige – The Prestige attack mentioned above presents an example of a state-sponsored cyber-attack. In this case, Russia launched a targeted attack as an apparent warfare tactic focused on disrupting infrastructure. We have seen numerous such attacks around the world in recent years.
- Nvidia – Early in 2022 a ransomware attack hit Nvidia, the world's biggest semiconductor chip manufacturer. While Nvidia responded quickly to the attack, the event highlights the fact that even companies with strong security experience attacks.

- Daixin ransomware group – The Daixin group attacked AirAsia this month, acquiring personal data for all the airline's employees and five million passengers. According to the FBI, the group has been actively attacking U.S. businesses for some time, specifically targeting healthcare organizations.
- CommonSpirit Health – Last month, threat actors launched a ransomware attack against CommonSpirit Health, a system that operates over 1000 healthcare facilities nationwide. As a result of the attack, system outages in multiple locations caused troublesome delays in medical procedures.

In addition to cyber terrorism, increasingly sophisticated methods, and a focus on healthcare and infrastructure, other patterns have emerged. For instance, attackers frequently attack small vendors, disrupting the supply chain for bigger fish. Double extortion attacks have also increased, in which hackers steal sensitive data from the victim to use as additional leverage.

Credential Hygiene is Critical to Prevent Ransomware Attacks

Most successful ransomware attacks share a common feature. That is, successful attackers were able to compromise one or more highly privileged user accounts. In some cases, hackers gained access to a domain-wide administrator account. In other cases, multiple local administrator accounts shared the same password.

To guard against compromise of privileged accounts, organizations need to implement several best practices for credentials. For instance, the principle of least privilege mandates that users should be granted the minimum amount of access necessary. Tools like Microsoft Entra provide the analytics necessary to ensure that users do not have excessive or unused permissions.

Additionally, zero trust policies protect the system by requiring authentication every time a user or device attempts to access the network. Modern authentication systems such as multi-factor authentication (MFA) and randomized administrator passwords also provide critical security.

Configure Security Tools Properly

In some cases, organizations have security tools at their disposal but have not configured them properly. At the basic level, simply changing default passwords makes it more difficult for hackers to enter the system. But available tools provide many additional protections.

For example, Microsoft offers a suite of security tools in the Microsoft Defender family of products. Even small businesses can take advantage of enterprise-grade endpoint protection by deploying Microsoft Defender for Business.

These tools and others can play a critical role in reducing the risk of ransomware and other cyber-attacks. However, they can be difficult to configure, particularly for organizations with limited cyber security expertise. A cyber security consultant can provide crucial assistance in determining the right tools and settings to use.

Cyber Security Investment Delivers Results

Improving your cyber security posture requires an investment. However, companies that invest the time and resources required see important returns in mitigating the risk of a successful attack.

The cyber security consultants at eMazzanti offer the expertise necessary to ensure that you have the security you need. They will help you choose and configure the tools you need, including access management, email protection, data encryption and continuous network monitoring.