Health Information Compliance Alert

Ransomware: Thwart Zeppelin Ransomware Risks With Knowledge and Management

Hint: Feds offer a plethora of tools and tips to combat cyberattacks.

During the pandemic, cyber crime, particularly in healthcare, multiplied exponentially. And with ransomware attacks on the rise, you need to protect your organization from the professional and fiscal threats of a data breach.

Details: The Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency (CISA) have released a joint alert about the Zeppelin ransomware. Malicious actors have used the ransomware for the past three years to target several businesses and infrastructure organizations, "especially organizations in the healthcare and medical industries," the alert says. Initial ransom payment requests ranged from several thousand dollars to over a million dollars, and the actors have been known to request ransom payments in Bitcoin.

By exploiting SonicWall firewall vulnerabilities, taking advantage of remote desktop protocol (RDP) exploitation, and employing phishing attempts, Zeppelin threat actors are able to gain access to targeted networks. However, for about one to two weeks before unleashing the attack, they survey the targeted victim network "to identify data enclaves, including cloud storage and network backups," the alert explains.

The FBI and CISA have also issued recommended mitigations to help reduce the risk of a Zeppelin ransomware infection. Some of the recommendations include:

- Creating and implementing a recovery plan.
- Requiring password logins meet National Institute for Standards and Technology (NIST) standards for managing

and developing password policies.
- Requiring multifactor authentication (MFA) for accounts, virtual private networks (VPNs), email, and other connections to critical systems.
- Segmenting networks to help stem the spread of the ransomware.

The last recommendation is critical in your network's protection against this specific strain of ransomware. The FBI has seen situations where threat actors "executed their malware multiple times within a victim's network, resulting in the creation of different IDs or file extensions, for each instance of an attack," the joint alert says. As a result, the victim would need multiple decryption keys.

That fact is "particularly alarming," observes attorney **Linn Freedman** with law firm Robinson & Cole in Providence, Rhode Island, in online analysis of the alert.

And that's not all. Prior to encrypting the files, the criminals "exfiltrate sensitive company data files to sell or publish in the event the victim refuses to pay the ransom," the alert says.

In other words: "Along with encrypting files, this gang is engaging in the 'double layered' data extortion method," explains **John Riggi**, American Hospital Association national advisor for cybersecurity and risk, in a post on the AHA's website. "It appears this gang is stealing and threatening to publicly release sensitive information such as patient information, payroll, human resources and non-disclosure protected information. Thus, even if a victim organization can independently restore encrypted files from backup, they face the dilemma of potential public release of stolen information in the possession of the criminals," Riggi continues.

By the way: "The AHA, along with the federal government, strongly discourages the payment of ransom," Riggi emphasizes. "This alert along with the comprehensive #stopransomware site provide extensive guidance on how to protect your systems from ransomware and avoid the ethical and legal dilemma of 'pay, not pay.'"

Resource: The alert is at www.cisa.gov/uscert/ncas/alerts/aa22-223a.