CANNABIS NEWS YOU CAN USE
CANNABIS RISK MANAGER

Everest Ransomware Targets Cannabis Industry, Experts Warn

Everest Ransomware Group Targets Cannabis Industry, Raises Alarm for Cybersecurity Risks

The growing concern around cybersecurity in the cannabis industry has escalated with the recent emergence of Everest ransomware group, which has been targeting cannabis operators. According to the Cannabis Information Sharing & Analysis Organization (Cannabis ISAO), the group has started to make its presence felt in the marijuana sector.

Ransomware Attacks in the Cannabis Sector

This week, Everest ransomware group claimed responsibility for another attack on a cannabis operator, marking the second time in just one week that a marijuana business has appeared on Everest's dark-web blog. The second victim, according to the reports, is connected to the first victim through a software-as-a-service (SaaS) vendor. This link highlights an important issue: third-party vendor risks. With the cannabis industry's reliance on SaaS platforms and other service providers, there is an increasing concern about the expanding scope of cyber threats. The ongoing attacks by Everest point to the possibility of this group continuing to target the cannabis sector, raising alarms among operators.

The Dark Web Tactics: Data-Leak Sites and Cyber Threats

Ransomware groups like Everest often use data-leak sites, commonly referred to as "name and shame" blogs, to pressure victims into paying ransoms. These blogs, hosted on the dark web, publicly release stolen data in an effort to damage the reputations of organizations and force them into negotiating for the return of their data. While not all businesses featured on these sites have necessarily had their networks breached, the frequency of cannabis operators being listed in a short span suggests the sector is indeed facing a significant threat.

The U.S. Department of Health and Human Services (HHS) has already issued a Threat Actor Profile for Everest, highlighting the group's recent uptick in targeting healthcare organizations. Everest has evolved into an "initial access broker," a role where they gain unauthorized access to a victim's network before selling this access to other ransomware gangs. These gangs then execute the ransomware attack.

Understanding the Growing Cybersecurity Threat

As the cannabis industry continues to grow, so does the cyber risk. The increasing complexity of third-party vendors, coupled with a lack of mature cybersecurity practices, has made cannabis businesses vulnerable to such attacks. Organizations are encouraged to stay vigilant and maintain situational awareness to anticipate potential risks and safeguard their networks.

The Cannabis ISAO recommends that cannabis businesses regularly assess their cybersecurity practices to improve defenses. This approach includes updating software, implementing patches, and participating in threat-sharing practices. Collective defense is critical, as organizations can share critical information across sectors to mitigate cybersecurity risks. With the rapidly changing cyber threat landscape, staying proactive and connected within the industry can help defend against potential attacks.

Third-Party Risk Management and Ransomware Preparedness

Third-party risk refers to vulnerabilities introduced by external entities within an organization's ecosystem or supply chain. In the cannabis industry, these risks have been highlighted by previous incidents, such as the cyberattack on the Ontario Cannabis Store's logistics partner in 2022. This breach affected product delivery to retailers and demonstrated how a single vendor's vulnerabilities could affect the entire industry.

Chris Clai, Director of Information Security at Green Thumb Industries, emphasized that many cannabis vendors are still early in their cybersecurity development. This discrepancy in cybersecurity maturity between cannabis operators and their vendors makes it crucial for businesses to actively manage third-party risk. This could involve offering cybersecurity expertise to vendors or even helping vendors implement better security measures.

In the broader business world, ransomware incidents have led to a push for better preparation. Experts suggest that practicing responses through tabletop exercises, where businesses simulate a ransomware attack to test their incident-response plans, is essential. Organizations should also focus on training employees in cybersecurity best practices and building a solid cyber hygiene culture from the start.

Defending Against Everest: How to Strengthen Cyber Defenses

Given Everest's role as an initial access broker, cannabis operators should be aware of specific indicators of compromise (IOCs) related to this threat group. The HHS Threat Actor Profile highlights several files and URLs that could be associated with Everest's activities. For cannabis organizations, staying vigilant against these IOCs is crucial for early detection and prevention.

Cannabis organizations are urged to collaborate with their internal cybersecurity teams or managed security service providers (MSSPs) to scan for these indicators and fortify their defenses. Preventive measures include monitoring for suspicious network activity and using advanced detection tools to uncover early signs of compromise.

Building Cybersecurity Resilience in the Cannabis Industry

As the cannabis sector matures, so too must its cybersecurity practices. With cybercriminal groups like Everest actively targeting the industry, cannabis operators must remain proactive in their defense strategies. This includes improving third-party risk management, implementing robust incident-response plans, and educating employees about cyber hygiene. By strengthening defenses and collaborating with other businesses in the sector, cannabis organizations can reduce their risk of falling victim to ransomware attacks and ensure the continued growth and resilience of the industry.

In conclusion, while the rise of ransomware threats in the cannabis industry is concerning, businesses have the tools and strategies at their disposal to combat these risks. Staying informed, prepared, and connected to the larger cybersecurity community will be key to successfully navigating this evolving landscape.

Email: info@cannabisriskmanager.com | Phone: +415-226-4060