Published on *The National Law Review* https://natlawreview.com

Ransomware Hitting U.S. Companies at Increasing Rate

Article By:

Linn F. Freedman

Unfortunately, according to Unit 42 of Palo Alto's recently published "Ransomware and Extortion Report," ransomware groups had a good year in 2022. They found that threat actors are using multi-extortion tactics to get paid by victims, including data exfiltration. In addition, there was "a 49% increase in victims reported by ransomware leak sites, with a total of 3,998 posts from various ransomware groups."

Twenty-five new ransomware groups attacked companies in 2023, though the most successful continued to be some well-known groups, including BlackCat, CL0P, and Lockbit.

According to its analysis of leak site data, the manufacturing sector was the hardest hit in 2023, "signaling significant vulnerabilities in this sector." Unit 42 surmises this is because the manufacturing sector is using old software that makes patching difficult. Further, based on leak data, U.S.-based organizations were most severely affected by ransomware, a whopping 42 percent of leaks in 2022.

Threat actors are increasing their usage of harassment techniques, including communicating with C-Suite executives to apply pressure to pay.

Unit 42's experts have predictions for what to expect from extortion groups in 2024 and it is not pretty. **The predictions include:**

- "2024 will be the year we see a large cloud ransomware compromise.
- A rise in extortion related to insider threats.
- A rise in politically motivated extortion attempts.
- The use of ransomware and extortion to distract from attacks aimed to infect the supply chain or source code."

Unfortunately, ransomware is still dominating security incidents and will continue to cause chaos for U.S. companies. Conducting a tabletop exercise on a ransomware attack is imperative to prepare for the attack. Schedule one now before you get hit.

National Law Review, Volumess XIV, Number 39