Pay Ransom?

Expect to Pay Again

As we know, ransomware attacks are on the rise and the ransoms are getting higher. In the first half of this year, there were more than 226.3M attacks. Of course, the real number is unknown and companies and insurance companies go to great lengths to avoid report of the breach.

Ransomware criminals are now, not only attempting to extract money from their victims, but coming back a second time to extort more. Yonatan Striem-Amit, CTO and co-founder of Cybereason, explains, “Ransomware cybercriminals are constantly innovating on better ways to get companies to pay more. We’ve seen a shift as ransomware groups adopting nation-state and APT-style technologies to encrypt whole networks, employing both zero-day and lateral movement techniques. And we’ve seen that evolve even further into double extortion.” And, companies that pay find that much of the data they recover is corrupted.

Yonatan Streim-Amit

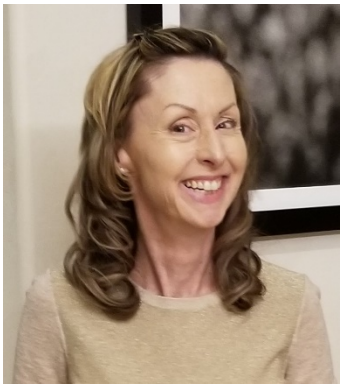
cybereason®

FBI Director Christopher Wray says the cyber threat "is increasing almost exponentially." The FBI director added that the federal government is currently investigating "100 different ransomware variants, and each of those 100 has dozens, if not hundreds of victims."

Cybereason conducted a global study of nearly 1,300 security professionals and found more than half of organizations had been the victim of a ransomware attack, and 80% of businesses that paid the ransom demand suffered a second ransomware attack — often at the hands of the same criminals. At least one report forecasts the cyber insurance market value will hit $24.19 million by 2025. But, if you buy it, don’t advertise it because that, too, invites attacks. Cybercriminals prefer a victim with deep pockets.

The Ransomware Task Force is a private-sector led, 60-member organization that includes dozens of private companies along with the FBI, U.S. Cybersecurity and Infrastructure Security Agency (CISA), and other law-enforcement groups. The Task Force provides a 48 step framework to avoid cyber attacks with four priority goals: 1) to deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; 2) to disrupt the

ransomware business model and decrease criminal profits; 3) to help organizations better prepare for ransomware attacks; and 4) to respond to ransomware attacks more effectively. Cisco is a founding member. Their Talos Intelligence group participates in cyber attack panels to advise companies and their insurance providers during an attack.



Karen Heumann

G2M Communications