www.techrepublic.com /article/traditional-security-fails-to-protect-against-ransomware/

How traditional security tools fail to protect companies against ransomware

Lance Whitney ⁝ 6-7 minutes ⁝ 7/1/2022

Most organizations surveyed by Titaniam have existing security prevention and backup tools, but almost 40% have still been hit by ransomware attacks in the last year.

Credit: Adobe

Traditional cybersecurity products were once enough to protect organizations against viruses and hacking attempts. But today's cyber threats are more prevalent, more sophisticated and more destructive, requiring more robust security defenses. A report released Thursday by cybersecurity firm Titaniam looks at the inability of traditional security products to protect against ransomware in particular.

SEE: How to become a cybersecurity pro: A cheat sheet **(TechRepublic)**

For its State of Data Exfiltration & Extortion Report, Titaniam commissioned CensusWide to survey 107 IT security professionals in the U.S. about their experiences with cybersecurity and ransomware. Among the respondents, more than 75% said they had tools in place for data protection, prevention and detection, and data backup and recovery. To protect their data, the professionals surveyed pointed to such technologies as encryption, including encryption at rest and encryption in transit; data masking; and tokenization.

Data exfiltration thwarts traditional security efforts

However, the defenses in place didn't protect the organizations against ransomware attacks. Almost 40% of them have been hit by ransomware attacks in the last year, while more than 70% have seen such an attack against them over the past five years.

One tactic increasingly favored by many ransomware gangs is double extortion. In this type of incident, the compromised data is not just encrypted but exfiltrated by the attacker. Unless the ransom is paid, the criminals vow to not only keep the hacked data encrypted but to release it publicly. This means that a data backup alone isn't sufficient to thwart the ransom demand.

With data exfiltration attempts up more than 100% from five years ago, 65% of the respondents who were hit by a ransomware attack also experienced data theft or exfiltration. Among those victims, 60% said the attackers used the stolen files to extort them further by threatening to leak the data. As a result, 59% of them felt they had no choice but to pay the ransom.

Understanding the different stages of ransomware attacks

With data exfiltration and double extortion tactics in play, how can organizations better protect themselves from ransomware attacks? Titaniam CEO and founder Arti Raman offers several pieces of advice.

"You cannot secure yourself against something you do not properly understand, so the first thing organizations need to do is to break down the how and why of ransomware attacks and examine those in light of their own organization," Raman said. "Specifically, ransomware attacks involve three distinct stages: infiltration, data exfiltration, and system lockup via encryption.

"Success on any of these stages results in a win for attackers, as they now have additional leverage to extort the victim."

The different stages work as follows:

1. Infiltration: Once they've infiltrated a network, attackers can monitor victims' behaviors and install backdoors. This type of exploitation can be sold as information or as access to other criminals.
2. Data Exfiltration: This may be the most profitable stage, as attackers can use the stolen information to demand ransom from victims, their customers, their partners, their board members and even their employees.
3. System Lockup: Attackers can prevent the victim from accessing their own systems, especially damaging if the organization lacks the proper backup and recovery methods.

“Once you understand these three distinctly, it becomes clear that each must be accounted for separately in your ransomware and extortion defense strategy,” Raman explained.

SEE: Ransomware: How executives should prepare given the current threat landscape **(TechRepublic)**

Network defense against the stages of ransomware attacks

First of all, organizations must invest in prevention and detection systems to mitigate infiltration. However, this is only the start, as attackers can still take advantage of stolen credentials to bypass these types of tools.

To prevent data exfiltration, organizations must invest in all three types of encryption, namely encryption at rest, encryption in transit and most importantly encryption in use. The newest type of protection available, encryption in use secures both structured and unstructured data while it’s actively being used. With this level of encryption, attackers using stolen credentials can’t access data even with privileged access. Nor can they grab data dumped from memory or by querying databases. As a result, encryption in use is a solid defense against data-related aspects of ransomware attacks.

In the event an attacker is able to infiltrate a network, organizations can guard against system lockout by investing in backup and recovery solutions.

“Focusing on just one or two … is certainly not sufficient, as evidenced by thousands of successful ransomware attacks that have already taken place this year,” Raman said. “A complete ransomware defense strategy should include all three.”

However, ransomware gangs are increasingly apt to focus more on data exfiltration and less on system lockup, according to Raman. For attackers, it may seem easier to simply steal data and threaten to expose it rather than risk getting caught while taking the time to encrypt files and deal with decryption technology.

Therefore, according to Raman, it is better for companies to focus on developing strategies that mitigate data exfiltration along with reducing infiltration and system lockup attempts.