SHARDSECURE

THE TANGLED WEB OF RANSOMWARE

Ransomware has been an ever-present threat for years, and its impact is only growing. An attack is attempted every 11 seconds, and the average cost of an incident exceeds $4 million. But ransomware has also grown more complex, making it increasingly difficult to prevent. Below, we illustrate some of its most challenging aspects and suggest solutions to mitigate its impact.

1 Ransomware as a service

One of the biggest developments in ransomware has been the rise of ransomware as a service (RaaS), which allows attackers to pay for malicious software on a subscription basis. The RaaS model has led to an increase in ransomware incidents worldwide, as it allows cybercriminals with no coding or technical skills to execute attacks. However, RaaS can still be mitigated like other forms of ransomware: with robust data security solutions, access controls, and backups.

2 Encryption-less variants

Another major development is the rise of encryption-less ransomware. While most ransomware operates by encrypting vital data and withholding the decryption key, new variants are skipping the encryption step altogether. Instead, attackers exfiltrate sensitive data and threaten to sell or publish it. Like double extortion attacks, encryption-less ransomware can be mitigated with data privacy technologies that render sensitive data unintelligible to unauthorized users.

3 Vulnerable targets

Ransomware attackers often target sectors that provide critical services, store significant amounts of sensitive data, and/or employ legacy technologies. These sectors — including healthcare, manufacturing, finance, and agriculture — often have inadequate cybersecurity measures, making them a key target for ransomware attackers. Keeping systems patched and updated is crucial, as are regular backups and strong access controls.

4 Double extortion and data breaches

Double extortion attacks are a one-two punch, working to encrypt and exfiltrate sensitive data. This method gives attackers more leverage over their victims, who face both the loss of their critical data and the exposure of that data online. With the average cost of data breaches hitting $4.45 million this year, companies must work to secure their sensitive materials so they can avoid data exposure, regulatory fines, and legal consequences.

5 Compromised backups

As ransomware evolves, it's increasingly able to evade detection for weeks or months at a time, allowing it to spread through systems and encrypt backups. This tactic all but guarantees that victims have no alternative but to pay the ransom, since their backups will be rendered useless for data recovery. The solution is to employ next-gen cloud backup solutions and sophisticated threat detection systems (including AI-assisted tools) so that critical data is never lost.

6 Cost of downtime

One of the costliest aspects of ransomware attacks is downtime. If businesses cannot restore critical systems and data quickly, they stand to lose revenue, productivity, and customer trust. In sectors like manufacturing, the expenses can exceed six figures an hour. To minimize downtime from ransomware attacks, organizations should invest in a robust data resilience solution.

The ShardSecure platform mitigates ransomware for organizations of all sizes, safeguarding sensitive data and mitigating top cyberthreats. To learn more, take a look at our ransomware white paper or book a demo today.