OVERVIEW

Targeted vs Opportunistic

Ransomware attacks are most commonly accomplished by installing malware which encrypts key parts of a server's filesystem, rendering it mostly unusable except to display a ransom note.

There are two main categories: opportunistic attacks, and targeted ones. Opportunistic attacks lean much more heavily on automation by the attacker and tend to affect fewer devices, so the ransoms tend to be lower. Targeted attacks involve more investment by the attacker; their actions may resemble those that happen during a data breach, such as reconnaissance, tailored lateral movement, and hunting for critical servers or data. As such, the ransoms are much higher.

One notable example of a targeted attack is the Travelex attack on or about New Years Day of 2020, believed to be carried out by the REvil/Sodinokibi group. Although the final ransom amount (or whether it was paid) remains undisclosed, at one point it ballooned to $6 Million. In addition to locking data and systems, the attackers threatened to release customer data in order to coax Travelex into paying the ransom. They also claimed they had infiltrated Travelex's systems at least 6 months prior to the ransomware attack.

BEST PRACTICE

Ransomware

Resilience's Cyber Meteorology Framework models cyber risk trends and helps companies stay up-to-date with current best practices and mitigation guidance. Resilience's targeted and opportunistic ransomware models recommend that organizations do the following to prevent and mitigate these attacks:

1. Employ Multi Factor Authentication, most critically for the organization's primary domain or hosting platform such as Office365 or GSuite
2. Reduce and scan externally exposed ports and network services
3. Employ an Email Gateway and conduct periodic phishing awareness tests
4. Use endpoint detection and response (EDR) products
5. Keep and practice restoring from backups

INSURANCE

Cyber Extortion

Cyber insurance policies should offer dedicated cyber extortion coverage and have experts at the ready to resolve your ransomware event on best terms. The end goal should focus on how to get your operations back up and running as fast as possible. Speak to your broker to learn more.

Example Claim

Health care provider suffers a ransomware attack that encrypted key computer

systems, rendering them inoperable and forcing offices to close and patients to be rerouted. In cases of life and death, incident responders need ransomware experience to evaluate and determine whether and how to negotiate.