8 STAGES OF TARGETED RANSOMWARE ATTACKS

1 RECONNAISSANCE

Threat actors research their targets in advance to determine the likelihood of ransom payment. Exploitable vulnerabilities or access points are often identified utilizing scanning and analysis tools.

2 GAINING ACCESS

Access points are identified and access is attained by brute-forcing passwords, using default passwords, obtaining credentials through phishing, exploiting misconfigured access points, or by purchasing access to systems on the dark web.

3 MAINTAINING ACCESS

One or several backdoors (malware) are typically installed to ensure persistent access to the environment.

4 DESTROYING OR ENCRYPTING BACKUPS

Threat actors attempt to move laterally throughout the network to gain access to additional systems and backups.

5 STEALING DATA

Criminals increasingly exfiltrate sensitive information from compromised networks to use as additional leverage to force the victim organization to pay a ransom by threatening to disclose the stolen data publicly if the ransom is not paid.

6 ENCRYPTING FILES

Threat actors encrypt as many files and systems as possible across the target network to effectively hinder the organization's system access and operations.

7 RANSOM NEGOTIATION AND PAYMENT

A ransom will be requested in order to release encrypted files. If a victim organization chooses to pay the ransom as a last resort, experienced incident response firms are commonly engaged by victim organizations to assist with the negotiation of the ransom demand and to facilitate a cryptocurrency payment.

8 RECOVERY

If a ransom is paid, receipt of decryption key(s), system decryption and data recovery occur. If a ransom isn't paid, the victim organization must either recover the files from a clean backup or rebuild the files and systems from scratch. Neither option is instantaneous and may take days, weeks or months.

Visit **TheHartford.com/cyber**

THE HARTFORD