Anatomy of a Ransomware Attack

Ransomware can remain undetected for days, weeks or even months, dramatically increasing the business impact. Understanding the lifecycle of a ransomware attack can help organizations beef up their defenses and detect and thwart the attack at various stages.

1. PAYLOAD

Ransomware is commonly delivered when a user clicks on a malicious link or attachment in a phishing email.

2. EXECUTION

The malicious code is downloaded to the victim's machine and begins to execute.

3. PHONE HOME

The malware connects to a command-and-control server and awaits an encryption key and other instructions.

4. LATERAL MOVEMENT

The malware moves laterally through the network, stealing credentials to access more systems.

5. SEARCH

The malware searches for files to encrypt on all the systems it has accessed.

6. ENCRYPTION/ EXFILTRATION

The malware begins encrypting and in some cases exfiltrating all the files it has discovered.

7. DEMAND

The attacker demands payment of a ransom in exchange for the decryption key.

What Are the Risks?

676 **Security Breaches Involved Ransomware in 2020, Double the Number in 2019.**

"2020 Year End Report," RiskBased Security, 2021

19 **Average Days of Downtime from Ransomware in Q3 2020 up 19% from Q2 2020.**

"Quarterly Ransomware Report," Coveware, Q3 2020

$20 billion

Predicted Global Ransomware Damages in 2021, a 5,697% increase since 2015.

"The Evolution of Ransomware," CrowdStrike, 2020

$233,817 **Average Ransomware Payment in Q3 2020, up 31% from Q2 2020.**

"Quarterly Ransomware Report," Coveware, Q3 2020

$730,000 **Average Cost of Recovering from a Ransomware Attack, not Including the Ransom.**

"The State of Ransomware 2020," Sophos, 2020