cybereason

Ransomware Gold Rush

305 MILLION RANSOMWARE ATTACKS IN THE FIRST HALF OF 2021

151% YEAR-OVER YEAR INCREASE

$500+ million AMOUNT GANGS HAVE EARNED IN 2021

What's driving the ransomware rush?

1. Organizations are more reliant on digital infrastructure
2. Ransomware-as-a-Service (RaaS) has lowered the technical bar
3. Cryptocurrency providing pseudo-anonymity
4. Lines blurred between nation-state = cybercrime threat actors
5. Ransomware gangs functioning like legitimate companies

8 Stages

TO A TYPICAL RANSOMWARE ATTACK SEQUENCE

1. Reconnaissance and Target Selection
2. Initial Access
3. Command & Control
4. Credential Theft & Privilege Escalation
5. Data Exfiltration
6. Encryption
7. Negotiation
8. Ransom payment

Common Targeted Data Categories

1. PROTECTED HEALTH INFORMATION
2. PERSONALLY IDENTIFIABLE INFORMATION
3. ACCOUNT CREDENTIALS
4. INTELLECTUAL PROPERTY

3 Reasons NOT To Pay

- NO GUARANTEES
- LEGAL IMPLICATIONS
- INCENTIVIZING RANSOMWARE ATTACKS

80% of those who paid were hit AGAIN

How to Protect Yourself

- IDENTIFY RANSOMWARE ATTACKS EARLY IN THE KILL CHAIN
- USE BEHAVIORAL DETECTIONS TO PREVENT ACCOUNT COMPROMISE
- UNCOVER THE ROOT CAUSE TO MITIGATE AGAINST FUTURE ATTACKS
- UTILIZE XDR SOLUTIONS TO EXPOSE THE ENTIRE MALICIOUS OPERATION