SaaS, Meet RaaS

What Is Ransomware?

Ransomware is malware that:

- Infects a user's system
- Encrypts its contents
- Demands payment for a decrypt or that will release the files

What Is Ransomware-as-a-Service (RaaS)?

Developers create a complete ransomware attack toolkit, including:

- Product development and support
- Service Level Agreements
- Helpdesk
- Ransom negotiators

Lease the product to "affiliates," who:

- Locate and compromise targets
- Collect the ransom

Share the proceeds

- 40%-60%
- 30%-70%

Why Does RaaS Exist?

Ransomware developers have monetized malware using a modified software-as-a-service model:

It is too risky to:

- Locate and compromise targets
- Launch attacks
- Wait to get paid
- Getting caught = Game Over

How Do Affiliates Use RaaS?

1. Automated target identification
2. Install ransomware and other malware
3. Eliminate log data
4. Extortion via unencrypted data

Decryption fails or is not provided in most ransomware attacks, even when the victim pays the ransom. On average, only 65% of compromised data are recovered.

The Most Common RaaS Targets

UNITED STATES

- Defense
- Emergency Services
- Food and Agriculture
- Government
- Information Technology

AUSTRALIA

- Health care
- Financial Services
- Higher education
- Research
- Energy

UK

- Higher Education

Anatomy Of a Ransomware Attack

Encryption is one of the last things a ransomware attacker does

- Ransomware is designed to evade detection
- Ransomware target is typically compromised for an average of 22 days before the malware encrypts user files

Most Common Successful Attack Techniques

- Phishing
- Microsoft Remote Desktop Protocol (RDP)
- Brute-force password attacks

New Ransomware Attack Trends

Ransomware attack trends:

- Cloud infrastructure
- Managed Service Providers
- Industrial Process
- Software supply chains
- Weekend and holiday attacks
- Smaller targets
- Information sharing
- Multiple extortions

Avoiding Ransomware

- Maintain A/V, anti-malware on Internet-facing systems
- Multi-factor authentication, strong passwords, least privilege, time-limited authorization, password management systems
- Network monitoring tools, segregating log data
- Duplicate, segregated backup strategies
- End-to-end encryption, cloud data encryption
- Patching
- Training
- Segregating network segments
- Third-party threat assessments

If You're Attacked...

- Immediately disconnect network from the Internet
- Locate and remove the ransomware
- Locate and remove additional malware, backdoors, rootkits
- Document the attack
- Seek third-party assistance when necessary
- Notify authorities and report the incident
- Conduct a post-incident analysis to avoid future intrusions