

Ransomware-as-a-Service (RaaS)
**A Rapidly-Growing Business Model for
Cybersecurity Attacks**
Frederick S. Lane

The CISO Summit
Accra, Ghana
22 March 2023



1

Cybertraps & Cyberethics



The Center for
CYBERETHICS

The Cybertraps Newsletter

2

10 Books



3

The Evolution of Malware

- **Experiments Gone Wrong**
 - The Morris Worm (1988)
- **Vandalism**
 - Michelangelo Virus (1992)
- **Zombie Networks (DDoS Attacks)**
 - MyDoom (2004)
- **Data Theft / Exfiltration**
 - Rise of Identity Theft and Fraud
- **Encryption of Mission-Critical Files**
 - The Era of Ransomware

4

Electric Company of Ghana

- Late September 2022
- Customers Lost Power or Were Unable to Purchase It
- Ransomware
 - Changed Source Code
 - Took Control of Parts of Server
- ECG Designated “Critical Infrastructure”

5

The Rise of Ransomware

- Kidnapped Data ➔ Ransom Demands
- Increased Use of Double-Extortion
- Exponential Growth in Attacks
- Multiple Sectors Targeted
 - Government (Including Infrastructure)
 - Finance
 - Healthcare
 - Education
 - Supply Chains

6

A Growth Industry

- **Reminder: Attack & Payment Data Is Incomplete**
- Ransomware Grew an Estimated 150% Between 2019 and 2020
- Approximately 65% of Attacks in 2020 Stemmed from RaaS
- Amount of Ransom Payments per Incident Nearly Doubled
- Remote Work Has Increased Risks
- Cybersecurity firm Trend Micro logged 146 billion cyber threats in 2022

7

RaaS Business Model

- Developer Creates Ransomware
 - Regular Updates and Enhancements
 - Create and Maintain Deployment Infrastructure (C&C, Payment, *etc.*)
 - Customer Support
- Affiliates Sign Up and Deploy Ransomware
- Subscription-Based or Revenue-Sharing
- Increases the Number of Potential Targets
- Hampers Efforts by Law Enforcement

8

The Economics of RaaS

- **Subscriptions**
 - Monthly/Yearly (\$\$ - \$\$\$\$)
 - Different Tiers Offer Additional Features/Support
- **Revenue-Sharing**
 - Affiliate Pays Percentage of Ransom Payments
 - Percentage Based on Level of Service
- **Tiered Commissions**
 - Commission Rate Based on Attack Success and Revenues
 - Higher Commissions Incentivize Number of Attacks, Penetration Techniques, and Ransom Techniques
- **Hybrid Systems**
 - Upfront Fee for Access, Revenue-Sharing on Ransoms
 - Guaranteed Revenue for Developer, Lower Commissions for Affiliate

9

Common Attack Vectors

- Phishing Emails and Messages
- Social Engineering
- Malvertising
- Compromised Web Sites
- Unpatched Software
- Remote Desktop Protocol (RDP) Attacks
- Physical Intrusion (USB/Unprotected Terminals)

10

Preventing Ransomware Attacks

- A Culture of Cybersafety (National, Local, Organizational)
- Employee Training and Awareness
- Software Updates and Patches
- Backup and Recovery Strategy (3-2-1, Verified Regularly)
- Network Segmentation and Access Controls
- Advanced Threat Detection
- Security Audits and Risk Assessments
- Incident Response Plan
- “Who Ya Gonna Call?”

11

The Future of RaaS

- Big Game Hunting (Targeted Attacks)
- Expansion and Diversification of RaaS Ecosystem
- Increased Attacks on IoT and OT
- More Sophisticated Evasion and Anti-Analysis Techniques
- Increased Collaboration among RaaS Providers (Cartels?)
- Integration of AI, Machine Learning, and Chatbots

12

Ransomware-as-a-Service (RaaS)
**A Rapidly-Growing Business Model for
Cybersecurity Attacks**
Frederick S. Lane

The CISO Summit
Accra, Ghana
22 March 2023



13