SANS DFIR

Ransomware and Cyber Extortion

POSTER

digital-forensics.sans.org

[illegible]

Overview: Ransomware and Cyber Extortion

The term "ransomware" was originally used to reference the malware itself. We now call this the "payload" or "encryptor." The general term "ransomware" is now used to reference the overall attack campaign, which includes all stages of the attack. Some ransomware attacks include the deployment of a payload/encryptor, whereas others do not. These latter attacks may alternatively be referred to as "cyber extortion."

RaaS Business Model – Roles and Participation

Each role is critical to the success of the ransomware campaign.

Initial Access Broker

- Obtains initial access to organizations
- Monetizes networks by selling them to any actor

Ransomware Affiliate

- Carries out the core attack:
  - Execution/persistence
  - Privilege escalation
  - Defense evasion
  - Discovery/lateral movement
  - Collection/exfil
  - Ransomware deployment

Data Manager

- Supplies data exfiltration infrastructure and software
- Sorts and organizes exfiltrated data
- Publishes exfiltrated data if applicable

Ransomware Operator

- Supplies ransomware infrastructure and software

Negotiator

- Negotiates with victim organization

Chaser

- Puts pressure on victim organizations by threatening with continuous attacks and leaking of stolen data

Accountant

- Launders ransom payment

IN | THROUGH | OUT

[illegible]

Types of Extortion

- **Data Encryption**—The act of encrypting data, often thereby disabling network services due to encrypted servers not being able to function correctly. Decryption is offered in return for a ransom payment.
- **Data Exfiltration**—The act of exfiltrating data from a victim organization during an attack and then using the threat of releasing that data for ransom purposes.
- **Multi-Extortion**—Additional extortion methods include, but are not limited to:
  - Carrying out DDoS attacks on victim networks
  - Contacting suppliers/partners
  - Contacting regulatory bodies
  - Contacting board members, VIPs, investors, etc.

Ransomware Actor Communications

Data Leak Sites (DLSs) exist to advertise that a breach has occurred and to incentivize the company to pay the ransom. Ransomware actors can choose to release victim's data or sell it.

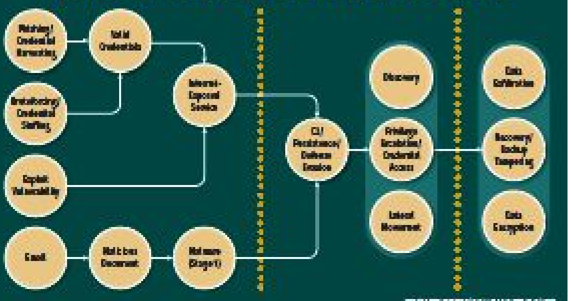
These sites typically include which company the data was taken from, the type of data available, as well as some sample data from the breach. Some DLSs also provide granular searching capabilities.

Online forums, including those on the darknet, are often used to facilitate communications, including by threat intelligence analysts and IR professionals. Many of these can be joined anonymously.

Top darknet forums include XSS.is, Exploit.in, Ransom Anon Market Place (RAMP), Hack Forums, and CryptBB.

Messaging systems like Tox, Telegram and RocketChat may be used by ransomware actors to communicate with victims.

Ransomware Incident Lifecycle



Phishing/ Credential Harvesting

Valid Credentials

Bruteforcing/ Credential Stuffing

Internet-Exposed Service

Exploit Vulnerability

Email

Malicious Document

Malware (Stager)

C2/ Persistence/ Defense Evasion

Discovery

Privilege Escalation/ Credential Access

Lateral Movement

Data Exfiltration

Recovery/ Backup Tampering

Data Encryption

[illegible]

Initial Access

3 MOST COMMON VECTORS

Remote Desktop Protocol | software exploitation | phishing

Remote Desktop Protocol (RDP) as an Infection Vector

[illegible]

Software Exploitation as an Infection Vector

[illegible]

Phishing as an Infection Vector

[illegible]

Tracking RDP Activity

[illegible]

Artifacts to Collect

collect data | parse/process data | analyze data

[illegible]