RansomHub Overview

RansomHub is an emerging ransomware threat, initially linked to the ALPHV (BlackCat) ransomware group, but later splitting off due to internal disputes among affiliates. Its first notable attack targeted Change Healthcare, marking its rise in the cybersecurity landscape. In 2024, it also targeted prominent organizations like Christie's Auction House and Rite Aid.

Ransomware-as-a-Service (RaaS) Model

RansomHub operates as a Ransomware-as-a-Service (RaaS) affiliate program, providing cybercriminals with the tools and infrastructure needed to carry out ransomware attacks. The RaaS model allows less-skilled attackers to rent out ransomware capabilities, leading to a broader distribution of attacks.

EDRKillShifter – RansomHub's Advanced Tool

A notable development in RansomHub's operations is the integration of EDRKillShifter, a sophisticated tool used to neutralize Endpoint Detection and Response (EDR) solutions. This tool:

- **Exploits vulnerable drivers** to disable EDR mechanisms.
- **Evades detection** by disrupting security monitoring in real-time.
- **Adapts dynamically** to the evolving security landscape, ensuring persistence even after initial threats are discovered and mitigated.

This level of sophistication places RansomHub in line with other notable ransomware groups like FIN7 and Black Basta, which have also adopted EDR-disabling tools. EDRKillShifter's integration ensures that all attack phases benefit from its capabilities, making traditional security measures less effective and forcing organizations to consider more adaptive defenses

How RansomHub Works

1. **Initial Infection (Entry Point)**: RansomHub primarily gains access to systems via phishing emails, which trick users into clicking malicious links or downloading attachments. These emails are often disguised as legitimate communications. Once opened, the ransomware installs, giving attackers a foothold in the network.
2. **Exploitation of Vulnerabilities**: RansomHub takes advantage of known software vulnerabilities, specifically targeting outdated or unpatched systems. By using tools linked to groups like **ALPHV**, it becomes harder to detect and prevent the attack.

3. **File Encryption**: After successfully infiltrating a system, RansomHub encrypts critical files on the victim's devices using strong cryptographic algorithms. This makes it impossible to access the files without the unique decryption key held by the attackers.
4. **Ransom Demand**: Following encryption, the ransomware presents a ransom note, demanding payment (typically in cryptocurrency) for the decryption key. Additionally, there are threats to leak or sell sensitive data if the ransom is not paid, increasing the pressure on victims.
5. **Data Exfiltration**: Alongside encryption, RansomHub also steals sensitive data from the victim's systems. If the ransom is not paid, this data is either published or sold on dark web forums, further harming the victim.
6. **Affiliates and Extensibility**: RansomHub's RaaS model enables a large network of affiliates to carry out attacks. This model scales ransomware campaigns and allows even low-skilled attackers to launch sophisticated operations using RansomHub's infrastructure.