cybereason | WHITEPAPER

INSIDE COMPLEX
RANSOMWARE OPERATIONS

RansomOps

Introduction

The recent surge in ransomware attacks has created a gold rush in the cybercrime world. A significant portion of the illicit funds generated are invested right back into attackers' operations, enhancing their sophistication, and lowering the barrier to entry for other would-be hackers.

Now generative AI has arrived, and it enables these groups to improve and scale their attacks like never before, giving them greater access and stealth.

These complex ransomware operations, or RansomOps™, involve highly targeted, "low and slow" attack sequences that remain clandestine and spread through as much of the target network as possible before the ransomware payload is delivered and a demand is issued.

Even data backups aren't enough to reject the ransom. They enable the organization to recover their encrypted information, but they cannot stop attackers from leaking stolen data online, where other threat actors can find and use it. It's just another way to ensure that victims pay up.

But that's not the solution either. Those who pay the ransom don't get all of their systems and data back uncorrupted. Many find that the attackers have leaked stolen data anyway. And most are hacked again shortly afterwards.

PAYING THE RANSOM IS NO GUARANTEE THAT YOUR DATA IS SAFE

Paying the ransom to get your data back is one thing, but preventing copies of that data from being used elsewhere is another. Here are the common data types that are used for double extortion:

- **Protected Health Information (PHI):** Medical records, diagnosis details, and patient medical insurance data. PHI is sometimes leveraged for blackmail.
- **Personally Identifiable Information (PII):** Birth dates, physical addresses, and social security numbers. Attackers monetize the information and sell it on the Dark Web for identity theft, fraud, or spear-phishing attacks.
- **Account Credentials:** Usernames, passwords and account credentials are valuable to attackers who use them to move laterally across the network, encrypting even more data and devices to demand a larger ransom amount.
- **Intellectual Property (IP):** New product releases and/or details that are integral to an organization's line of business. Attackers can monetize a victim's IP on the Dark Web or hand it over to a state-sponsored threat actor to be leveraged for economic advantage.

UNDERSTANDING COMMON RANSOMOPS ATTACK VECTORS

Researchers found that unsecured Microsoft Remote Desktop Protocol (RDP) connections accounted for over half of all ransomware attacks, followed by phishing emails and exploitation of software vulnerabilities. Here's how these common delivery vectors can enable a ransomware attack:

- **Unsecured RDP:** A proprietary protocol developed by Microsoft, RDP enables users to remotely connect to other computers over a network connection. When organizations leave their RDP ports exposed online, threat actors use brute-force attacks to establish persistence on a target network.
- **Phishing emails:** A typical attack attempt begins when a user receives an email that instructs them to click on a malicious link that delivers ransomware or an exploit kit as a payload, or instructs the recipient to open a tainted PDF, ZIP archive, or Microsoft Office file with enabled macros that downloads ransomware or initiates command and control for lateral movement on the network.
- **Exploitation of vulnerabilities:** Exploit kits can evaluate web browsers, operating systems, and other software for exploitable vulnerabilities to activate exploit code and install ransomware on the victim's machine or initiate command and control for lateral movement.

It is worth noting that ransomware gangs typically also have access to multiple zero-day vulnerabilities they can leverage in attacks, and a good deal of their R&D efforts go into finding new zero-days to exploit, keeping them well ahead of defenders.

UNDERSTANDING A RANSOMOPS ATTACK SEQUENCE

'Spray-and-pray' ransomware attacks typically begin with mass spam email campaigns or drive-by attacks leveraging malicious websites. Unwitting targets open malicious documents or click on malicious links which execute the ransomware on the target device. At that point, the ransomware encrypts the victim's files and a ransom note is displayed, usually demanding payment of hundreds of thousands to millions of dollars. Once they've received the ransom payment, the attackers may send a decryption utility to the victim, may make additional demands, or may do nothing in response.

RansomOps follows a similar progression but often involves a level of sophistication in target selection, infection, and network penetration that are more similar to complex nation-state operations to gain persistence, move laterally on the target network, exfiltrate sensitive information from the victim for double extortion, and more.

RansomOps also typically include several threat actors working in unison: a ransomware developer making their malicious code available on the black market, affiliates using an infection vector to launch an attack on a target using the Ransomware as a Service (RaaS)-supplied infrastructure, then sharing a portion of the ransom proceeds with the RaaS provider, the negotiator, the crypto exchange, and so on.

The typical RansomOps attack sequence includes the following stages:

1

Reconnaissance and target selection: Threat actors typically seek to target organizations of consequence to compel swift payment of the ransom demand, such as healthcare and critical infrastructure.

2

Initial access: RansomOps attackers typically gain an initial foothold on the targeted network through phishing attacks or the exploitation of a vulnerable component. Once persistence is established on the targeted network, the initial threat actor may opt to sell access to the network to another attacker or group.

3

Command and control: The attackers begin communications with the Command and Control (C2) server to import additional tools or commence abuse of legitimate tools already available on the network to spread laterally and escalate privileges.

4

Credential theft and privilege escalation: The abuse of user identities through credential theft allows the attackers to further spread through the targeted network and escalate privileges.

5

Data exfiltration: Sensitive data is exfiltrated for use in double extortion or to be monetized for sale on the dark web.

6

Encryption: The ransomware payload is delivered and the compromised systems and data are encrypted. They become inaccessible and a ransom demand is levied.

7

Negotiation: After the network assets are encrypted and the ransom demand issued, the negotiation stage begins to determine the final ransom amount and process for decryption.

8

Ransom payment: Victims can opt to pay the ransom with the expectation that a decryption key will be provided, but there are no guarantees the key will work or that no data will be corrupted in the process. Victims can also opt to not pay the ransom and restore systems from backups, but any exfiltrated data is still at risk of exposure. Either option is labor-intensive and costly.

TO PAY OR NOT TO PAY?

After falling prey to a ransomware attack, organizations must decide whether to pay the ransom demand. **Here are four reasons why it does not always pay to pay:**

NO GUARANTEES

Paying the ransom doesn't mean that you will regain access to your encrypted data. The decryption utilities provided by those responsible for the attack sometimes simply don't work properly.

YOU ARE LIKELY TO BE ATTACKED AGAIN

Our research found that most organizations who paid the ransom were breached shortly afterwards, either by the same attacker, or a new one who may have obtained their data on the dark web.

LEGAL IMPLICATIONS

Organizations could inadvertently incur penalties for paying ransomware actors who may reside or operate out of countries that are subject to sanctions.

INCENTIVIZING RANSOMWARE ATTACKS

Organizations who pay ransomware attackers are sending the message that extortion schemes work—a message that can only fuel continued ransomware attacks and extortion schemes.

RANSOMWARE: THE TRUE COST TO BUSINESS 2024 REPORT

It (still) doesn't pay to pay. We surveyed over 1,000 cybersecurity professionals whose organizations had been held to ransom over the last 24 months. The results—including the true cost of an attack—are surprising.

Read the 2024 report

DEFENDING AGAINST RANSOMOPS

It is possible for organizations to defend themselves at each stage of a ransomware attack. What's important to understand about RansomOps is that before the delivery of the ransomware payload, the attackers have often engaged in weeks or even months of detectable activity on the target network. This is where understanding RansomOps and strategies to detect and disrupt them early in the kill chain can turn what would have been a potentially devastating ransomware attack into a less consequential intrusion or data exfiltration attempt.

The cybersecurity advisory report published by CISA provides a detailed list of controls and policies to implement to better defend against ransomware attacks, as well as steps to take when initiating incident response following a ransomware attack.

Defenders can also use behavioral detections to prevent account compromise and credential theft attempts, flag attempts to gain access to other network resources, discover attempts to exfiltrate data as well as encrypt files, block the execution of malicious code prior to encryption of systems, and so on. Unfortunately, until recently, the task of correlating attack telemetry across the disparate and distributed assets was a difficult and resource-heavy task that was impossible to scale.

THE POWER OF XDR

The advent of Extended Detection and Response (XDR) solutions, when used alongside other solutions including endpoint and mobile threat defense, allows organizations to identify not only what systems were hit with ransomware, but also what business applications, user identities, and cloud deployments may have been involved.

XDR solutions also reveal the full impact of the compromise and whether the attackers pivoted into other systems, cloud infrastructure or into ICS systems. Its ability to surface the full attack sequence from reconnaissance to initial intrusion to data exfiltration allows defenders to quickly understand the full scope of the attack, which in turn helps them improve their overall security posture for the future.

There are clearly multiple opportunities to detect RansomOps prior to the final ransomware payload delivery but organizations must embrace an operation-centric approach if they are to visualize a MalOp™ (malicious operation) in its entirety.

XDR uses AI and machine learning to surface the full attack sequence from reconnaissance to initial intrusion to data exfiltration, allowing defenders to quickly understand the full scope of the attack.

ABOUT CYBEREASON

Cybereason is the XDR company, partnering with defenders to end attacks at the endpoint, in the cloud and across the entire enterprise ecosystem. Only the Cybereason AI-Driven XDR Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalO™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in La Jolla, California, with customers in more than 40 countries.