Analysing Ransomware as a Service (RaaS) Campaigns Using MITRE ATT&CK Framework

Introduction

Ransomware as a Service (RaaS) has transformed the cyber threat landscape, making powerful attack tools available to non tech savvy criminals. The affiliate driven business model makes it possible for developers to lease out their ransomware to attackers, or affiliates, in exchange for a commission on successful ransom payments. Analogous to traditional Software as a Service, RaaS platforms provide affiliates with complete toolsets, infrastructure, and support at lower barriers for cybercrime. This has caused a sharp rise in the occurrence and magnitude of ransomware attacks globally. MITRE ATT&CK is an open source repository of adversary tactics, techniques, and procedures derived from observed adversary behavior. It provides a structured taxonomy of adversary behavior across the attack lifecycle so that cybersecurity professionals can understand, analyse, and neutralise threats. Its utility to Cyber Threat Intelligence is of prime relevance, enabling defenders to attribute cyberattacks to specific tactics and techniques, enabling greater insight into the intentions and procedures of adversaries. Security processes and tools can be aligned by organisations with the framework in order to concentrate on defense against relevant threats, improve detection, prevention, and response mechanisms, raise risk assessments, and implement CTI for actionable intelligence.

Chapter 2: Mapping RaaS TTPs to MITRE ATT&CK

MITRE ATT&CK Phase	RaaS Technique	Real-World Example
Initial Access	Phishing (T1566), Exploiting Public-Facing Apps (T1190)	LockBit's use of phishing emails with malicious PDFs.
Execution	Command-Line Interface (T1059), User Execution (T1204)	BlackCat's use of PowerShell scripts to deploy payloads.
Lateral Movement	Pass the Hash (T1550), Exploitation of Remote Services (T1210)	Fog ransomware moving through compromised VPN services.
Exfiltration	Data Compressed (T1560.001)	Storm-0501's use of Rclone to exfiltrate data to cloud storage.
Impact	Data Encrypted for Impact (T1486)	Double extortion (encrypt + leak data) by LockBit.

Initial Access

Phishing tactics (T1566) are frequently employed by RaaS operators to gain initial access to target systems. LockBit, for instance, has been known to distribute malicious PDF attachments through phishing emails. The emails are usually presented as legitimate business email and mislead users into opening infected attachments or tapping on malicious links. In addition, RaaS operators exploit vulnerabilities in publicly accessible apps (T1190), such as VPN service or web server, to establish a first foothold in the target network. As outlined in Chapter 4, LockBit employs phishing (T1566) and VPN exploitation (T1190) as a first access method.

Execution

Once they have accessed the network, RaaS affiliates employ various execution techniques to deploy their payloads. The use of command-line interfaces (T1059), notably PowerShell, is common among ransomware actors like BlackCat. Scripts employed for this function commonly download and execute the main ransomware payload, making it more difficult to identify. User execution (T1204) is another common technique, whereby cyber attackers employ social engineering techniques to trick users into running malicious files or scripts, typically presented as legitimate software updates or documents.

Lateral Movement

Lateral movement is essential in RaaS attacks to have a maximum impact. Pass the hash (T1550) attacks are most commonly used to move around the network without any necessity to decrypt the passwords themselves. Fog ransomware, for example, has been reported to exploit stolen VPN credentials to move laterally across networks. Remote service exploitation (T1210) such as Remote Desktop Protocol (RDP) is another commonly used attack employed by ransomware actors to expand operations within the targeted system. Lateral mobility is highly critical for the success of RaaS attacks. Fog ransomware uses pass the hash (T1550) attacks and compromised VPN credentials for lateral movement without password cracking. Exploitation of remote services (T1210),Remote Desktop Protocol (RDP), is another common technique utilised by ransomware operators to further their presence within the affected ecosystem.

Exfiltration

Before encrypting, the majority of RaaS operators currently exfiltrate sensitive information to use in double extortion campaigns. Data compression (T1560.001) is often employed to reduce the volume of data being transmitted, which allows the exfiltration process to be faster and less detectable. Storm-0501, a RaaS operation, has been observed using tools like Rclone to efficiently exfiltrate data to cloud storage services before initiating the encryption process. Most RaaS operations exfiltrate sensitive information before encrypting it, which is subsequently used for double extortion attacks. Data compression (T1560.001) is also being used in the process to reduce the volume of data being transferred and hence enable faster and more covert exfiltration. Storm-0501 RaaS has also employed the usage of tools like Rclone to exfiltrate successfully to cloud storage providers even before the encryption process has begun.

Impact

The primary impact of RaaS attacks is data encryption for impact (T1486), which is the hallmark of ransomware attacks. LockBit clever and other advanced RaaS gangs have adopted double extortion tactics, whereby they cleverly encrypt the victim data as well as make threats to leak it in the event of ransom non-payment. This practice significantly increases pressure on victims to pay, since the reputational and legal consequences of data leakage can be severe. RaaS operators utilise a hybrid encryption technique, where both symmetric and asymmetric algorithms are used for security and efficiency.

Chapter 3: Case Study – LockBit 3.0

LockBit 3.0 has been the most visible Ransomware as a Service operation, accounting for approximately 30% of overall ransomware attacks in 2023. Such dominance in the ransomware landscape makes LockBit an ideal subject for a case study of the evolving tactics of sophisticated RaaS actors. The group's success even led to cross pollination between RaaS operations where LockBit welcomed BlackCat actors to conduct their operations on their platform at the end of 2023.

LockBit 3.0: Evolution and Impact

LockBit has developed significantly since it first emerged in late 2019. Initially known for its speed and efficiency, LockBit quickly gained notoriety for targeting a wide range of organisations across numerous sectors. LockBit 2.0 included the development of a more sophisticated affiliate program, which attracted a larger number of cybercriminals and expanded the group's reach. The release of LockBit 3.0, also known as LockBit Black, was a significant revamp with enhanced evasion techniques and a modular framework, allowing greater customisation and flexibility. The impact of LockBit on the ransomware landscape has been significant. The group has been linked to several high-profile attacks, causing enormous financial loss and reputational damage to targeted organizations.

Notable Campaigns and Attacks

The Continental Attack (2022): LockBit claimed responsibility for a massive attack against Continental, a major auto parts manufacturer. The group stole a vast amount of sensitive data and threatened to release it unless the ransom was paid.

Royal Mail Attack (2023): LockBit targeted Royal Mail, shutting down international mail services and causing significant delays. The attack showed the potential impact of ransomware on essential infrastructure.

Multi-Healthcare Attacks: LockBit has launched repeated attacks against healthcare organisations, disrupting patient care and compromising sensitive medical data.

Distinguishing TTPs

LockBit differs from other RaaS operations through the use of several distinguishing TTPs:

Aggressive Recruitment: LockBit actively recruits affiliates from dark web forums with assurances of high returns and a high level of autonomy.

Configurable Ransomware: LockBit's modular design allows affiliates to customise the ransomware payload to more successfully target victims and evade detection.

Data Leak Site: LockBit also has a dedicated data leak site on which it publishes stolen data of non paying victims, thus further incentivising ransom payments.

Primary TTPs of LockBit 3.0

Initial Access

LockBit actors utilise various techniques to achieve initial access to the victim networks. Publicly exploited application vulnerability (T1190), with a particular focus on VPN services, is one of their top techniques. LockBit actors were observed in 2023 exploiting VPN vulnerabilities in well known VPN software in order to gain access to corporate networks.Besides that, LockBit threat actors like to utilise phishing campaigns (T1566) as their way of gaining the initial entry point. Phishing emails contain PDF attachments or links that, when opened, initiate the infection chain.

Lateral Movement

Once they have access to a network, LockBit affiliates use sophisticated lateral movement and network propagation tools. Among the key tools in their toolkit is Cobalt Strike (T1588.002), a commercial penetration testing tool. LockBit leverages it for post exploitation. LockBit threat actors have introduced new techniques to deliver Cobalt Strike beacons, including exploitation of Windows Defender command line tool "MpCmdRun.exe" for side loading malicious DLLs. The technique allows them to evade security tool detection while gaining persistence in the victim system.

LockBit affiliates also use remote desktop tools like Splashtop (T1021.001) for lateral movement and to gain remote access to infected systems.

Impact

LockBit 3.0 has also changed its tactics to exert maximum pressure on the victims. The gang uses a triple extortion multi-faceted strategy:

Data Encryption (T1486): The primary ransomware payload encrypts critical data on compromised systems.

Data Exfiltration: LockBit exfiltrates sensitive data using StealBit and other tools before encryption.

DDoS Threats: LockBit threatens victims with Distributed Denial of Service attacks if the ransom is not paid.

This triple extortion method places a tremendous amount of pressure on the victims to pay, not only will they lose access to their data but also sensitive data will be leaked and business will be disrupted by DDoS attacks.

Indicators of Compromise for LockBit 3.0

- File Hashes:
- 80e8defa5377018b093b5b90de0f2957f7062144c83a09a56bba1fe4eda932ce
- 506f3b12853375a1fbbf85c82ddf13341cf941c5acd4a39a51d6addf145a7a51
- a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db
- ea6d4dedd8c85e4a6bb60408a0dc1d56def1f4ad4f069c730dc5431b1c23da37

- IP Addresses:
- **194.26.29.13**
- **212.102.39.138**
- **194.32.122.35**
- **178.175.129.35**

- Domains:lockbit3753ekiocyo5epmpy6klmejchjtzddoekjlnt6mu3qh4de2id.onion
- lockbit3g3ohd3katajf6zaehxz4h4cnhmz5t735zpltywhwpc6oy3id.onion
- lockbit3olp7oetlc4tl5zydnoluphh7fvdt5oa6arcp2757r7xkutid.onion

- Registry Keys:

- `HKLM\System\CurrentControlSet\Services\WinDefend\Start`
- `HKCU\Control Panel\Desktop\WallPaper`
- `HKR<Malware Extension>\DefaultIcon`
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*`

Chapter 4: MITRE ATT&CK Mapping

MITRE ATT&CK Technique	Sub-Technique	Description	Example
Exploit Public-Facing Application (T1190)		Exploitation of vulnerabilities in public-facing applications to gain initial access.	LockBit affiliates exploited a vulnerability in a VPN appliance to gain access to a corporate network.
Phishing (T1566)	Spear Phishing Attachment (T1566.001)	Use of spear phishing emails with malicious attachments to deliver the ransomware payload.	LockBit affiliates sent spear phishing emails disguised as invoices, containing malicious PDF attachments that installed the ransomware.
Obtain Capabilities (T1588)	Tool (T1588.002)	Use of commercial, open-source, or custom tools to perform post-exploitation activities.	LockBit affiliates leverage Cobalt Strike, a commercial penetration testing tool, for lateral movement and command and control.
Data Encrypted for Impact (T1486)		Encryption of data on victim systems to disrupt business operations.	LockBit encrypts files with a strong encryption algorithm, rendering them inaccessible without the decryption key.
Data Exfiltration (T1041)		Exfiltration of sensitive data prior to encryption for double extortion.	LockBit exfiltrates sensitive data using tools like StealBit before encrypting the victim's files, threatening to

			release the data if the ransom is not paid.

Chapter 5: Sources of Threat Intelligence

Gathering detailed threat intelligence on RaaS gangs like LockBit 3.0 must be multi-faceted, drawing from varied sources:

Malware Analysis Platforms: Malware analysis platforms like VirusTotal and Any.Run allow for the analysis of LockBit 3.0 samples and provide information on their behavior, code organization, and communication protocols.

Dark Web Monitoring: Monitoring of dark web forums and marketplaces can provide early indications of LockBit 3.0 campaigns, affiliate recruitment programs, and victim data breaches.

Information Sharing Platforms: Membership of industry information sharing platforms like the Cyber Threat Alliance and Information Sharing and Analysis Centers allows threat intelligence to be shared with other parties.

Incident Response Reports: An analysis of incident response reports from cybersecurity firms and government organisations is a useful reference regarding LockBit 3.0's techniques, tactics, and procedures.

Vendor Threat Intelligence Feeds: Commercial threat feeds from reputable security vendors offer screened and actionable threat intelligence on RaaS threats like LockBit 3.0.

Chapter 6: Mitigation Strategies Using ATT&CK

The MITRE ATT&CK framework provides actionable intelligence for ransomware threat mitigation by mapping adversary tactics, techniques, and procedures (TTPs) into defensive actions. Below are significant mitigation approaches based on specific ATT&CK techniques employed by RaaS operators on a regular basis.

MITRE ATT&CK Phase	Technique	Mitigation Strategy	Explanation
Initial Access	Phishing (T1566)	Enforce multi-factor authentication	MFA reduces the risk of credential

		(MFA) and block macro-enabled emails.	theft, while disabling macros prevents execution of malicious payloads embedded in phishing emails.
Initial Access	Exploiting Public-Facing Applications (T1190)	Regularly patch vulnerabilities and conduct penetration testing.	Keeping software updated and testing for exploitable weaknesses minimizes attack surfaces for RaaS affiliates targeting VPNs or web applications.
Lateral Movement	Exploitation of Remote Services (T1210)	Patch RDP vulnerabilities and implement network segmentation.	Securing RDP and segmenting networks limits attackers' ability to move laterally within the environment.
Lateral Movement	Pass the Hash (T1550.002)	Use strong password policies and disable NTLM authentication where possible	Enforcing complex passwords and disabling outdated protocols like NTLM reduces the effectiveness of credential theft techniques.
impact	Data Encrypted for Impact (T1486)	Maintain offline backups and use advanced monitoring tools to detect data exfiltration.	Offline backups ensure data recovery after encryption, while monitoring tools help identify exfiltration attempts before impact.

Proactive Defense Programs

To counter effectively against ransomware threat actors, organisations must focus on catching early stage TTPs such as credential dumping or phishing. Proactive efforts include applying behavior analysis to detect normal user behavior anomalies and threat hunting automation on the basis of ATT&CK techniques such as privilege escalation or lateral movement. Red teaming exercises can simulate actual attacks in order to qualify defenses against established techniques. Preemptive defense must utilise platforms like Greynoise to detect RaaS affiliate scanning and Recorded Future to flag industry directed phishing campaigns.

Leveraging a proactive posture and fusing defenses with MITRE ATT&CK, organizations can reduce their exposure to risk by a large degree and improve detection, response, and recovery to ransomware attacks.

Conclusion

Ransomware as a Service has become an increasing threat to the world of cybersecurity employing existing tools and model tactics, techniques, and procedures . The MITRE ATT&CK framework is now a vital resource to understand and combat these continually evolving threats. CTI teams become crucial in leveraging the MITRE ATT&CK framework to create an organisation's security posture. The CTI teams need to be directed towards constant collection and analysis of threat intelligence, linking adversary behavior to such frameworks as ATT&CK in order to stay ahead of newly emerging RaaS campaigns. Playing an active part in mapping new and emerging methods to the ATT&CK framework will become increasingly important to staying ahead of the threat actors. By ongoing examination and extension, organisations can build a stronger defense and respond more favorably to the constantly evolving threat of ransomware.