The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

"Ransomware as a Service: Trends, Threat Actors, and Impact on Businesses"

ABSTRACT

The problem of ransomware is becoming more critical as businesses start depending more on their IT infrastructure. A wide range of institutions have been attacked, including government, financial, medical, and academic ones. Businesses have suffered greatly from ransomware, and a new variant known as ransomware as a service (RaaS) has emerged. Hackers can rent ransomware tools to carry out attacks through RaaS, which operates on a subscription basis. Ransomware assaults have increased dramatically since the start of the COVID-19 outbreak. Although there could be several explanations for the sudden rise in attacks, working remotely from home in less secure settings than typical institutional networks seem to be one of them. Cybercriminals are always developing new ways to propagate ransomware, such as social engineering tactics or phishing attacks. The purpose of this research study is to present an in-depth analysis of the growing threat actors connected to ransomware as a service (RaaS), the impact it has on businesses, and the trend itself. From being a weapon only used by highly skilled hackers, ransomware has developed into a service on the dark web that enables even inexperienced attackers to initiate ransomware operations. This study examines the many features and workings of RaaS, such as its affordability, accessibility, and user-friendly interfaces.

INTRODUCTION

A malicious adaptation of the software as a service (SaaS) business model is known as ransomware as a service or RaaS. It is a subscription-based business model that allows users,

known as ransomware affiliates, to purchase or rent pre-made ransomware tools for use in ransomware attacks[1].

Threat actors had to have some programming or code-accessing experience before the introduction of the RaaS model to conduct a ransomware attack. Although many ransomwares as a service (RaaS) organizations are selective about who has access, these attacks are now accessible to criminals without any prior coding experience. Under this method, users act as affiliates, spreading the malware and collecting ransom payments, while developers produce and distribute ransomware tools. This approach has made ransomware attacks more accessible and widespread, posing a significant threat to individuals and organizations worldwide. Some well-known organizations even do background checks and digital footprint analyses on prospective affiliates. Through the provision of sophisticated software for file encryption and decryption, together with round-the-clock software support, the RaaS operations model facilitates the execution of ransomware campaigns by anyone. It is the affiliates' responsibility to successfully launch an attack via phishing or software exploits once they gain access to the ransomware. Recent instances, such the attacks on Kaseya by the REvil ransomware group and Colonial Pipeline by the Darkside ransomware group.[2]

How Does the Ransomware as a Service (RaaS) Business Model Work?

The Ransomware as a Service (RaaS) business model works by enabling hackers to distribute and profit from ransomware attacks without the requirement for technical competence or generating their own virus. This is how it usually works:

- Development of Ransomware: A skilled hacker or gang produces the malware that locks down victims' data using encryption techniques.
- RaaS Platform Creation: To enable potential clients to access and utilise the service, the developer creates an intuitive dashboard, user interface, and infrastructure for the RaaS platform.

[1] 'What is Ransomware as a Service (RaaS)?' (Paloalto Network) < https://www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service> accessed 30 March 2024.

[2] Kurt Baker, 'RANSOMWARE AS A SERVICE (RAAS) EXPLAINED HOW IT WORKS & EXAMPLES'[2023]< https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>
accessed 30 March 2024.

- Affiliate Recruitment: The RaaS operator invites or uses underground forums to find affiliates. Affiliates can be aspiring or experienced hackers who want to launch ransomware attacks but don't have the infrastructure or skills to do so.
- Customization and Setup: By choosing the ransom amount, deadline, and target requirements, affiliates can personalize the ransomware. They can also write ransom notes, customized messages, and virtual currencies that can be used as payment methods.
- Distribution and Infection: Affiliates employ a variety of strategies, including social engineering, exploit kits, phishing emails, and fraudulent advertising, to spread the ransomware. After the victims' systems are breached, the ransom demand is sent to them, and their files are encrypted.
- Revenue Sharing: Because the affiliate is in charge of spreading the virus and convincing victims to pay, they usually receive a greater share of the ransom payments, between 60 and 90 percent, from the RaaS operator.
- Technical Support: To guarantee the ransomware runs smoothly and increase the likelihood that the ransom will be paid, the RaaS operator offers updates, bug fixes, and encryption keys to affiliates.
- Payment and Decryption: The operator transfers the affiliate's portion and gives them the decryption keys required to unlock the encrypted files after victims pay the ransom in Bitcoin.
- Reports and analytics: RaaS platforms frequently give affiliates access to real-time tracking and analytics of infections, payments, and successful attacks. This enables affiliates to assess their own performance and earnings.
- Ongoing Development: In order to avoid detection by antivirus software, improve encryption techniques, and guarantee the ransomware's profitability, the RaaS developer changes the programme on a regular basis. All the while, the developer keeps the affiliate programme viable.

All things considered, the RaaS model gives hackers access to pre-built infrastructure and support, enabling them to use ransomware attacks without requiring a great deal of technical expertise or money.[3]

[3] 'What is Ransomware as a Service (RaaS)?' (Paloalto Network)
< https://www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service> accessed 30 March 2024.

What Are the RaaS Revenue Models?

On the dark web, payments take place, and several cryptocurrencies are used for payment. Although the precise payment terms differ based on the RaaS business model, affiliates typically receive a sizable portion of the ransom—roughly 70–80%. There are four possible ways to divide profits:[4]

- **Affiliate RaaS**: In the event of success, a tiny portion of earnings supports the inventor of RaaS, enabling them to operate a more effective business and coordinate their ransomware assaults.
- **Subscription-based RaaS**: In order to access the ransomware, users must pay a certain monthly cost.
- **Lifetime licence:** After a single payment, users are granted unrestricted access. If they are successful, they are not required to split the profits with the RaaS group. This also means that, as demonstrated by Dharma and Phobos, ransomware operators can purchase source code and alter it to suit their requirements.
- **RaaS partnerships:** When an affiliate obtains access to the ransomware, the profit split is determined. Payment is made solely in the event that an assault is successful, but this split is greater than the affiliate model.

Ransomware as a Service (RaaS) is a growing threat in the cybersecurity landscape.

In the landscape of cybersecurity, ransomware as a service, or RaaS, has become a serious and expanding concern. With the use of this malicious model, hackers can buy or lease ransomware tools and services from developers in return for a portion of the money that the victims are forced to pay in ransom. RaaS has made it easier for cybercriminals to get started, making ransomware assaults possible even for people with little technological expertise. The RaaS model gives hackers access to sophisticated spyware, payment processing systems, and technical assistance, as well as a ready-made infrastructure. As a result, there are now more ransomware attacks that target individuals, companies, governmental institutions, and healthcare facilities. Cybercriminals are now employing social engineering techniques,

[4] Amos K. Kibet and others, 'RANSOMWARE: RANSOMWARE AS A SERVICE (RaaS), METHODS TO DETECTS, PREVENT, MITIGATE AND FUTURE DIRECTION'[2022] <https://www.researchgate.net/publication/365349176_RANSOMWARE_RANSOMWARE_AS_A_SERVICE_RaaS_METHODS_TO_DETECTS_PREVENT_MITIGATE_AND_FUTURE_DIRECTION> accessed 30 March 2024.

phishing emails, and exploit kits in addition to other more advanced methods to breach networks and encrypt sensitive data.

The destructive effects of ransomware on businesses of all sizes have been brought to light by recent, high-profile attacks by RaaS groups like REvil, DarkSide, and Conti. These attacks have caused serious financial losses, harm to one's reputation, and interruptions of vital services. In many instances, victims have been compelled to cover enormous ransom demands to have their encrypted data back. Organizations must put strong cybersecurity measures in place to guard against the growing threat of RaaS. These measures include frequent data backups, network segmentation, cybersecurity best practices training for staff members, and the usage of endpoint security solutions. To minimize the impact on their operations, organizations should also create an incident response plan that outlines how they will quickly detect and address ransomware assaults.

Organizations must maintain awareness and proactivity in their cybersecurity efforts to safeguard their data and networks from ransomware threats as ransomware attacks increase and RaaS continues to change. To properly counter this expanding threat, cooperation between law enforcement organizations, cybersecurity professionals, and industry stakeholders is also necessary.[5]

IMPACT OF RAAS ON BUSINESSES

In recent times, ransomware as a service, or RaaS, has become one of the biggest online risks facing businesses. RaaS is a term used to describe a particular kind of cybercrime business model in which hackers or creators of ransomware offer their services and tools to other users, or affiliates, who then execute the actual assaults in return for a cut of the earnings. Because of this paradigm, ransomware assaults have grown more accessible, and even non-technical people may now become hackers and carry out complex attacks.[6]

---

[5] Kurt Baker, 'RANSOMWARE AS A SERVICE (RAAS) EXPLAINED HOW IT WORKS & EXAMPLES'[2023]< https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>
accessed 31 March 2024.

[6] 'Ransomware Attack – What is it and How Does it Work?' (Check Point) < https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/#:~:text=Ransomware%20as%20a%20Service%20(RaaS,payments%20with%20the%20ransomware%20developers> accessed 31 March 2024.

RaaS's effects on businesses have been devastating. Here are a few significant ways that it has impacted organizations:

- Financial Loss: Businesses may suffer large financial losses as a result of ransomware attacks. Large quantities of money are frequently demanded by attackers as ransom to unlock systems or data that is encrypted. There is no assurance that the attackers will keep their word and grant access back, even if the ransom is paid. Businesses may also have to pay for incident response, system restoration, legal fees, and reputational harm in addition to the ransom.
- Operations disruption: Ransomware attacks have the potential to cause downtime and lost productivity in businesses. Organisations may be unable to do their daily tasks when vital systems and data are held captive, which could lead to missed deadlines, postponed projects, and unhappy clients. It could take days, weeks, or even months to fully recover and resume regular operations, depending on how severe the attack happened.
- Data Loss and Breach: Ransomware attacks may occasionally result in permanent data loss or breaches. If the ransom is not paid, attackers frequently threaten to sell or release stolen data, which can have disastrous effects on businesses. A data breach or loss can lead to contractual penalties, fines from regulatory bodies, and a loss of customer trust, all of which can have a lasting negative impact on the reputation of the company.
- Reputational Damage: A company's reputation may be damaged by ransomware attacks, particularly if client data is compromised or services are interrupted for a long time. When an attack that works is reported, word gets out rapidly, raising doubts about the organization's dependability and security procedures among prospective clients and partners. It might take some time and effort to rebuild confidence, which would affect both present and future commercial prospects.
- Higher Security Costs: Businesses must spend more money on strong security measures to protect themselves from ransomware attacks. Regular security audits, employee education initiatives, cutting-edge endpoint security, backup systems, and incident response strategies are all included in this. Budgets may be strained and resources allotted for other business endeavors may be reduced as a result of these increased security expenses.

EXAMPLES OF RAAS

Ransomware as a Service (RaaS) has become a major cybersecurity problem due to recent high-profile attacks by groups like REvil, DarkSide, Hiva, Dharma, LockBit, and so forth. These organizations have been the victim of some of the most significant and destructive ransomware attacks in recent years, which have affected organizations in a variety of industries, including government agencies, essential infrastructure, and the healthcare industry.

Revil

The attack on the massive meat processing company JBS in May 2021, which forced the closure of several plants in North America and Australia, was one of REvil's most prominent occurrences. The ransomware attack caused operational problems, raising concerns about possible disruptions to the food supply system and demonstrating the pervasive effect of ransomware on vital services.

One of the highest ransoms demands ever recorded, $10 million, was traced back to the ransomware known as REvil, also known as Sodinokibi. The criminal organization PINCHY SPIDER is the one selling it. They use the affiliate model to sell RaaS and usually take 40% of the sales.

Like TWISTED SPIDER's early leaks, PINCHY SPIDER notifies victims of a planned data breach before releasing the majority of the data after a predetermined period, typically through a blog post on their DLS that includes sample data as evidence (see below). In the ransom message, REvil will also provide a link to the blog article. The impacted victim can view the leak through the link before it is made public. When you click the link, a countdown timer will start, and after the allotted period of time has passed, the leak will be released.[7]

DarkSide

One of the biggest fuel pipelines in the US, the Colonial Pipeline, was attacked by DarkSide in May 2021, earning them fame. Fuel shortages and price increases occurred along the East Coast as a result of the pipeline operator being forced to shut down due to a ransomware attack. The incident demonstrated the vulnerability of vital infrastructure to cyberattacks and the potentially disastrous effects of ransomware attacks.

[7] Kurt Baker, 'RANSOMWARE AS A SERVICE (RAAS) EXPLAINED HOW IT WORKS & EXAMPLES'[2023]< https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/>
accessed 31 March 2024.

RaaS operation DarkSide is connected to the eCrime gang known by CrowdStrike as CARBON SPIDER. DarkSide operators have recently branched out into Linux, focusing on enterprise setups running unpatched VMware ESXi hypervisors or stealing vCenter credentials. Traditionally, they have concentrated on Windows workstations. The FBI revealed in public on May 10 that the DarkSide ransomware was used in the Colonial Pipeline attack. Later, it was revealed that Colonial Pipeline had paid a DarkSide affiliate around $5 million USD in exchange for about 100GB of data that had been taken from their network.[8]

LockBit

This ransomware, which first surfaced in June 2021, uses PowerShell and SMB to propagate infection throughout a vulnerable network. It says it has the quickest encryption on the market and has hacked more than 50 companies in various industries.

Dharma

Attacks using the Dharma ransomware have been linked to an Iranian threat cell with financial motivations. Since 2016, this RaaS has been accessible on the dark web, primarily linked to attacks using the remote desktop protocol (RDP). Attackers typically seek one to five bitcoins from their targets, which are in a variety of businesses.

Dharma differs from REvil and other RaaS kits in that it is not centralised.

Variants of Dharma can be found everywhere, and the majority of cases where CrowdStrike detected Dharma showed almost a perfect match between sample files. The only customizations available through a RaaS interface were the encryption keys, contact email, and a few other items. Threat hunters are unable to gain much insight into the identity and methods of Dharma attackers from an occurrence because these attacks are essentially the same.[9]

BlackCat

BlackCat, also called ALPHV, is a programming language that is written in Rust and is simple to build for various operating systems. Because it is so easy to customize and so customizable, this malware is hazardous.

[8] *Ibid*

[9] *Ibid*

The advanced methods used by RaaS groups and their capacity to seriously disrupt targeted organizations and create financial losses have come to be regarded as a result of these high-profile attacks. The employment of encryption methods to secure important data, along with demands for ransom payments, has turned ransomware operations into a profitable venture for hackers.

RaaS has made it possible for threat actors to expand and operate more effectively by giving them access to sophisticated malware tools and infrastructure. Because of this, fraudsters now have a reduced entrance hurdle, making it possible for even unskilled people to carry out ransomware attacks with disastrous results. Businesses are urged to strengthen their cybersecurity defenses, put in place comprehensive incident response plans, and work with law enforcement agencies and cybersecurity experts to reduce the risk of ransomware attacks in response to the growing threat posed by RaaS groups like REvil and DarkSide. The seriousness of these high-profile events that have occurred recently serves as a clear reminder of how crucial proactive cybersecurity measures are in thwarting emerging cyber threats like RaaS.

PREVENTIVE MEASURES FOR RaaS ATTACKS

Since recovering from a ransomware attack is challenging and expensive, it is preferable to avoid them completely. Since RaaS is merely ransomware packaged to make it easier for anyone with malicious intent to use, the steps to avoid a RaaS attack are the same as preventing any other ransomware attack:

- Install reliable, cutting-edge endpoint security that operates continuously in the background using sophisticated algorithms.
- Make frequent and regular backups. A week's worth of work product could be lost in a ransomware assault if backups are only made on the weekends.
- Create several backups and keep them on several devices in various places.
- To make sure backups can be recovered, test them frequently.
- Keep up a strict patching regimen to guard against known and new vulnerabilities.
- Divide the network into segments to prevent spread among the surroundings.
- Put in place cutting-edge anti-phishing safeguards.

- Invest in user education and foster a security-conscious culture.[10]

CONCLUSION

Ransomware as a service, which makes it simple for even non-technical people to launch ransomware attacks, has become a serious danger in the field of cybersecurity. This model has increased the frequency and complexity of ransomware attacks, putting companies of all sizes at danger. Effective defence against such assaults has become increasingly difficult for organisations because to the cooperation between threat actors and service providers. In order to lessen the effects of ransomware as a service and safeguard their priceless data and assets, organisations must prioritise cybersecurity measures, such as frequent backups, staff training, and strong security solutions.

[10] 'What is ransomware-as-a-service (RaaS)?'(IBM)< https://www.ibm.com/topics/ransomware-as-a-service#:~:text=Ransomware%2Das%2Da%2Dservice%20(RaaS)%20is%20a,out%20their%20own%20ransomware%20attacks> accessed 31 March 2024.