**Understanding Ransomware as a Service (RaaS)**

Ransomware proves a persistent and serious threat in today’s threat landscape, and threat actors are unfortunately seeking to disrupt all the services that any individual can see as essential. Attacks against healthcare providers, government systems, and alcohol systems are some of the common places that are being targeted by cybercriminals. On this note, it must be remembered that with each passing day, traditional methods are falling increasingly short. Attack tools that are sophisticated are now widely available for rent on the dark web in what is known as Ransomware-as-a-service.

**What is its meaning?**

Ransome as a service, commonly known as RaaS, is a business model that is based on subscription malware. It is created to extract encrypted or stolen data, which is known as Ransomware. The one who created ransomware made the software accessible to users, known as affiliates who used a bit of technical skills in order to hold people’s data. RaaS enables these users to enter into an environment of extraction that completely belonged to authors earlier.

**History of RaaS**

Back in 2016, it was terrifying for the security teams to witness and find out that ransomware could be rented by any individual in exchange for a small amount of money. This Ransomware which was popularly known as Stampado and brought a lifetime subscription of approximately 39 dollars. This Stampado had actually a lot of similarities with the jigsaw Ransomware and just like a jigsaw, it could slowly delete files if the victim failed to pay. But just as one might buy a knock-off designer bag for the fraction of the price, Stampado was in fact, an extremely cheaper replica that was widely accessible to rent on the dark web. And since Stampado, the RaaS business model has skyrocketed. Stampado was so successful that its developers, the Rainmakers labs decided to launch a deluxe version which was known as Philadelphia. Philadelphia cost around $400 and came with a customer interface, reviews, discounts, and feature updates which was just like a legitimate software business.

Like any industry, crime-as-a-service is subject to the law of supply and demand. As the market began to grow and there was a hike in demand prices rose, but prices fluctuate depending on competitors and the quality of the product. For example, some Ransomware products can cost up to four thousand dollars approximately.

**How does it work?**

RaaS provides ransomware in a software-as-a-service or SaaS model. RaaS operator is situated in the organization’s topmost hierarchy that develops the payload for data encryption. It also operates the back-end infrastructure for smooth running. This involves a code, a portal for the sign-up process of potential users, and customer service. RaaS operators that are full-time service based also handle the payments which are primarily through any kind of cryptocurrency like Bitcoin. Additionally, it also advertises on several forums across the dark web.

SaaS models RaaS to potential audiences either through a monthly subscription or on a one-time payment basis.

**Prevention of Ransomware as a service attack**

There are several risks which are associated with the use of Ransomware. However, there are solutions through which the risk can be minimized. Some of them are as follows.

1. The first and most important step towards mitigating the risk of attack is to ensure a proper data backup and a backup plan for recovery well in advance. Data encryption is done by Ransomware and thus it makes the data inaccessible to the users. Thus the effect of data breaching can be minimized if there is a proper data backup available.

2. Ransomware is attacked in a number of ways, one of the popular ones being email phishing. Therefore, a proper phishing protection tool must be used.

3. Muti-step authentication process must be incorporated as this prevents dependency on a single password and gives an additional layer of protection.

4. Software must be updated frequently to prevent data exploitation through operating systems of applications.

**References**

1.<https://www.techtarget.com/whatis/definition/ransomware-as-a-service-RaaS>

2.<https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/#:~:text=What%20is%20Ransomware%20as%20a,service%20(SaaS)%20business%20model>.

3.<https://www.upguard.com/blog/what-is-ransomware-as-a-service>

4.<https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas>

5.<https://www.techopedia.com/definition/32410/ransomware-as-a-service-raas>

6.<https://www.varonis.com/blog/ransomware-as-a-service>

7.<https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>