Ransomware as a Service: Behind the Scenes

outpost24.com/blog/Ransomware-as-a-service-behind-the-scenes

Ransomware as a Service: Behind the Scenes

08.Jul.2022

Jose Miguel Esparza, Head of Threat Intelligence

Threat Intelligence

Ransomware attack is growing at an alarming rate thanks to Ransomware as a Service (RaaS) operations. Read this blog and learn what is RaaS and how the threat actors operate these attacks to help you understand why ransomware attribution is an industry problem, and the preemptive measures you need to take to protect your organization.

Introduction

We, as an industry, are continuously tracking how ransomware groups attack, and who the newest victims are. We do this by monitoring their leak sites, documenting the way they perform the attacks (Tactics, Techniques and Procedures – aka TTPs), and analyzing their toolsets. However, we sometimes forget to look at how all these groups work behind the scenes, what kind of resources they use before and after an attack, from affiliate services to “client support” platforms.

During the recent Rootedcon conference in Spain, we delivered a talk about this subject, and this blog post serves as a commentary of the insights presented about Ransomware as a Service (RaaS): how it really works; how the threat actors operate these attacks; and how organizations can analyze the attacks and take preemptive measures in the event of future attacks.

Presentation: “Ransomeware Groups: Behind the Scenes” | Download

We also took a deep dive into the activities of a particularly nefarious RaaS group called Hive (sometimes known as The Hive Gang); the in depth report will be published shortly so watch this space.

Targeted ransomware

As we mentioned in the history of ransomware blog post, the ransomware ecosystem has evolved enormously in the past years. Operating a banking botnet used to be the most popular way to get rich in the cybercriminal world, until CryptoLocker was taken down in 2014 and Slavik’s earnings were published. Cybercriminals realized ransomware was a profitable business, and so the ransomware boom began.

Since then, threat actors have been adapting their toolset, techniques, and underground services offering to better support and launch targeted ransomware attacks. Advanced attackers methodically penetrate corporate networks and move laterally to study the system(s). The malware is then deployed in a calculated manner designed to cause the biggest obstruction to business operations possible thereby maximising the chances of being paid.

With this in mind, the targets of ransomware operations have adjusted and are no longer domestic users but big corporations who can pay substantially higher amounts in ransom. This change started with a few ransomware families like BitPaymer back in 2017, but targeted ransomware is widespread today.

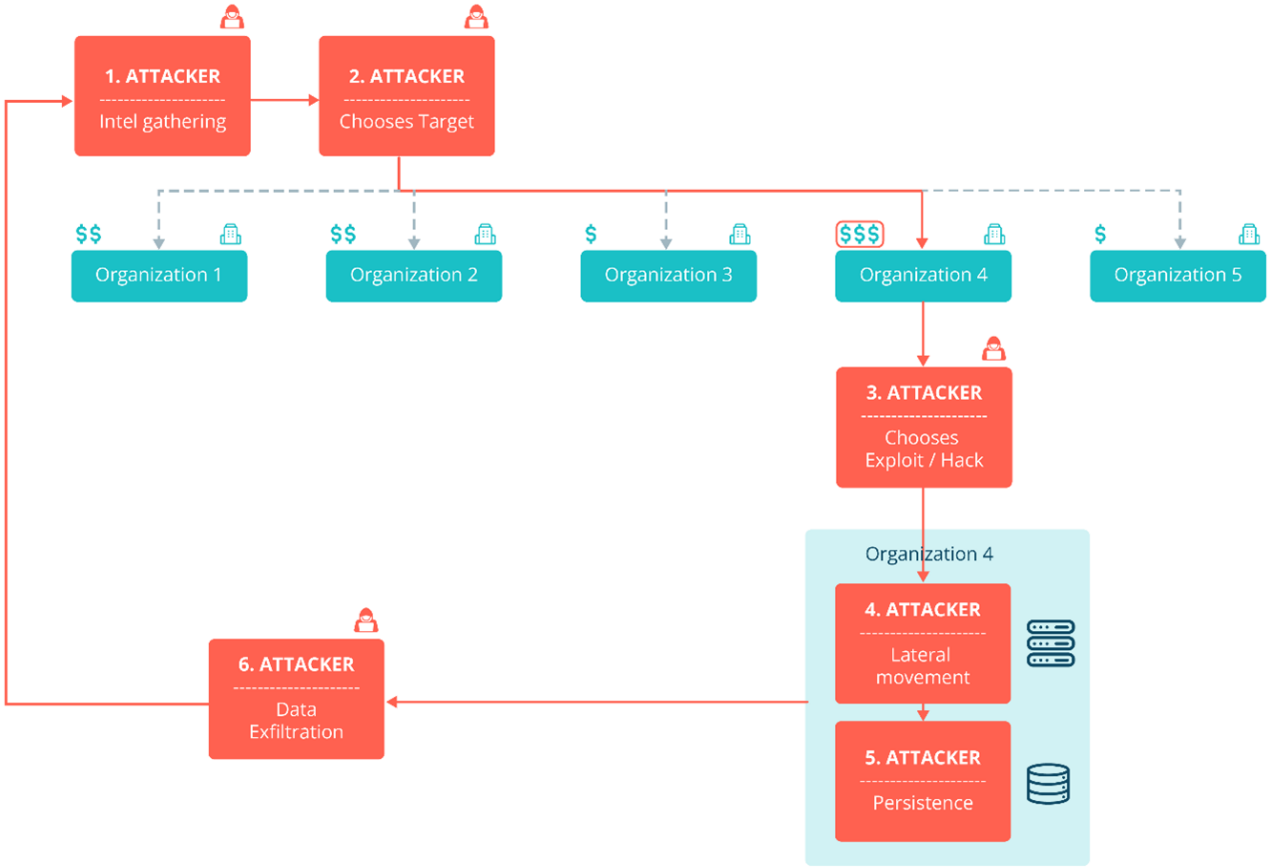

Image 1. Graphic showing the attack flow of a targeted ransomware attack

Advanced attackers would often use their own unique ransomware families. However, this lead to perpetrators being easily attributed as the source. In 2019, the FBI announced sanctions against Evil Corp, a Russia based group, after it was identified as the culprit of the extensive use of DRIDEX-based malware attacks.

In a bid to better cover their tracks and avoid further sanctions, the group tried a new strategy: continuously using different malware families. This included BitPaymer, WastedLocker, Hades, Phoenix Locker, PayloadBIN and Macaw Locker malwares.

Mandiant recently uncovered multiple Lockbit intrusions, an RaaS offering, which they connected with Evil Corp. While this is uncharacteristic of the group, it highlights another potential shift in strategy for the group as an attempt to distance themselves further from the risk of sanction.

Excluding Evil Corp, the majority of threat actors performing targeted attacks today make use of Ransomware as a Service (RaaS) offerings to get their hands on the ransomware binary. RaaS is now by far the most popular business model, allowing cybercriminals to swiftly set up their attack operations.

Ransomware as a Service

Ransomware as a Service (RaaS) is a more specialized version of the old Malware as a Service (MaaS) model, where a provider supplies a client with the malware binary, access to the backend to manage the botnet, and, in some cases, other additional services. When talking about RaaS the only difference is that the provided malware is exclusively a ransomware family.

There are different actors involved in the RaaS model, as can be seen in the following graphic:

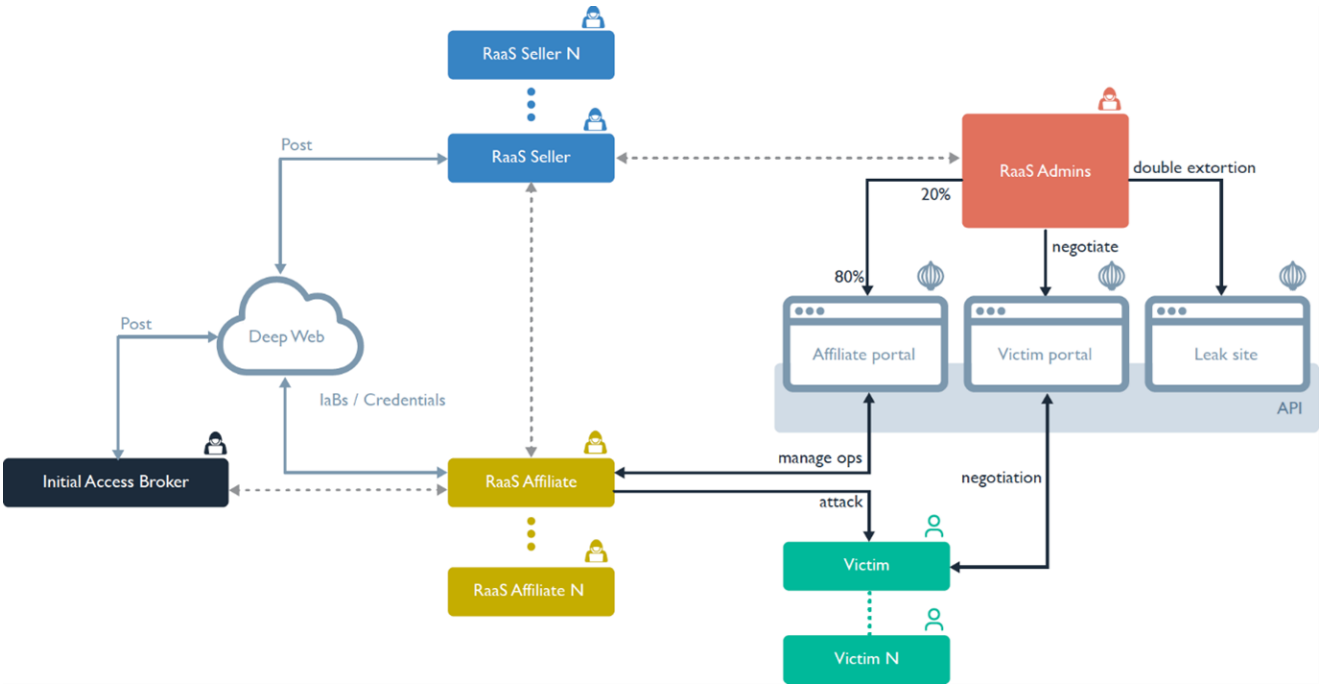

Image 2. Graphic showing the Ransomware as a Service (RaaS) model

Administrators

(Image 2 in orange)

The Administrators provide the affiliates with access to the malware, the infrastructure and sometimes even support in negotiations with the victims. Depending on the group, the infrastructure might be different, but it might include a leak site where victim information can be published, an affiliate portal where the affiliate will manage victims and generate malware binaries, the victim portal where victims will access to communicate with the cybercriminals, and, sometimes, even some internal servers for internal communication (internal IM, for instance).

The Administrators will get a cut from the affiliates' operations (80-20 is quite common), but they will not attack directly any victims.

Sellers

(Image 2 in blue)

If the RaaS offering is private, negotiations will be handled through private messages in forums or IM chats, and only accessible to certain cybercriminals with a particular reputation. The rest of RaaS offerings need to be advertised to potential "clients" and this is where the sellers and resellers are

useful. Those actors will be in charge of managing the sales side of the operation and obtaining new affiliates, and this will be achieved advertising the RaaS in underground forums.

In this context, it is important to highlight that ransomware conversations were banned from popular underground forums, like Exploit or XSS, in May 2021. This was mainly due to political/law enforcement pressure into ransomware operators and the fear of a shutdown of the forums. Other reasons were more philosophical. For instance, the administrator of XSS argued that the RaaS model is hurting the innovation in the cybercriminal community and that this was a good reason for the ban too.

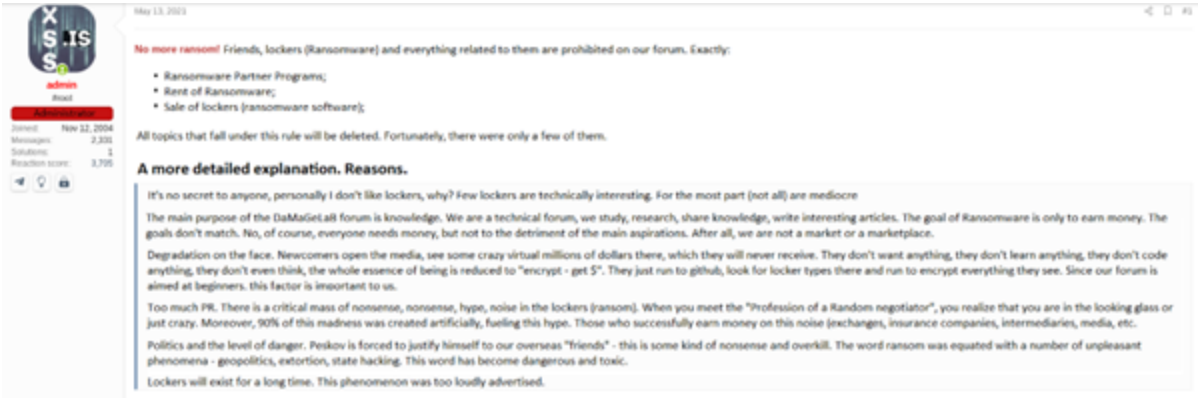

Image 3. XSS administrator announcing the ban and giving explanations

As it is normal in the underground ecosystem, when a service or forum disappears a new one appears the next day. This is what happened with the ban of ransomware conversations. In July 2021 a new forum called RAMP appeared where ransomware offering advertisements were more than welcome.

Affiliates

(Image 2 in gold)

The affiliates are the real attackers in a targeted ransomware operation. They will manage to get access to the targeted organization, by their own means or using Initial Access Brokers, and deploy the ransomware provided by the RaaS. They need to have enough experience to move laterally between systems, avoid detections, exfiltrate stolen information and deploy the ransomware in several systems at the same time.

Depending on the RaaS program, the affiliates will need to register their victims, including information about the victim and the operation, upload the stolen information to the leak site and communicate with the victims.

Initial Access Brokers

(Image 2 in black)

Initial Access Brokers (IABs) are financially motivated threat actors that profit through the sale of remote access to corporate networks in underground forums, like Exploit, or XSS. The types of access tools offered are mostly Remote Desktop Protocol (RDP), Virtual Private Network (VPN), web shells, and remote access software tools offered by companies such Citrix, Pulse Secure, Zoho, or

VMware. However, threat actors are also selling information and tools to perform intrusions into companies through SQL injections, remote code execution (RCE) exploits, and other vulnerabilities.

Image 4. Initial Access Broker offering access to a relevant Spanish company

Read more on how ransomware groups use IABs

Affiliates of RaaS offerings might use IABs services in order to facilitate and streamline the targeted ransomware operations, so they just need to focus on the intrusion, as the initial access and the malware were already given to them. IAB advertisements detail the industry

sector, location and revenue of the targets so affiliates can easily choose among them.

Victims

(Image 2 in green)

No person or organization wants to be the target of any malware attack, but of course they do not get a choice, they are a critical part of it. Without these victims, or “clients” as the ransomware operators call them, this business model would not work. The RaaS model exists because victims pay: there is no other option for them if they want a chance of surviving the attack. And for some companies, even if they pay, they are not guaranteed access to their systems and data. Regardless if they get access back or not, they are still at significant risk of bankruptcy. It’s not just the cost of the ransom, consider additional damages like the cost of downtime, business reputation and more.

RaaS and attribution problems

Threat attribution is crucial. Digging into the exact who, what, where, when and how of the attack provides valuable insights to better prevent attacks in the future.

As we have laid out above, different actors have different parts to play in the RaaS model. The nature of this business model, where actions are spread across different and separate actors, makes

life much more difficult for analysts and researchers who try to accurately put the pieces of the attack together and tie it to a group. Of course, we can attribute Indicators of Compromise (IOCs) and TTPs to the RaaS offering itself, as most of us do, but we should probably not call that accurate attribution.

In most of the cases, RaaS administrators will not attack victims directly, they will provide affiliates with the needed elements to perform the targeted attack. Meaning that the attribution should point to the affiliate and not to the RaaS provider.

However, an affiliate might have used the help of an IAB to access the targeted organization. This means that the IAB has probably scanned the organization looking for security weaknesses and maybe even exploiting a specific vulnerability. In this case, this scanning/exploiting activity should be attributed to the IAB, but not to the affiliate.

Let’s break down this example flow of an attack:

- Actor A breaches the company and sells access to Actor B, an affiliate of Lockbit

- Actor B requests a new payload to deploy and infect the company with ransomware
- The company contacts Lockbit about the infection
- Lockbit provides support and oversees the transaction

Some questions that will need answered:

- Given the IoCs that were retrieves from the infection, which belong to whom?
- Is the IP shown in the firewall logs to be associated with Actor A or Actor B?
- Does the payload belong to Lockbit or Actor B?

Ideally, an analyst wants to be able to differentiate between all these behaviors and IOCs, and correctly assign them to the corresponding actor.

Attribution of ransomware attacks is extremely tricky because we don't have enough information to accurately trace all the elements of an attack, tending to connect all indicators and attacking behavior to the RaaS itself, causing probably even more confusion for future analysis.

Conclusions

Knowing your enemy is key to effectively organize your defenses. Targeted ransomware operations are here to stay and they will continue threatening businesses indiscriminately.

Understanding how these groups operate behind the scenes, how the RaaS model works with its different actors, and how they negotiate is information that every potential ransomware target should be aware of. Threat intelligence services and insights are crucial to know more about the attackers that might target an organization in the future, helping to mitigate as much as possible the impact of an attack.

The RaaS model makes even harder the attribution of attacks, as IOCs and TTPs can be attributed to the wrong actors in the RaaS scheme. There is no vendor with 100% of visibility into threats, and that's why industry collaboration is extremely important to fill the gaps and win together the fight against ransomware.