Ransomware-as-a-Service, Rogue Affiliates, and What's Next

digitalshadows.com/blog-and-research/ransomware-as-a-service-rogue-affiliates-and-whats-next/

May 20, 2021

Generating a chain of unforeseen events, the Colonial Pipeline ransomware attack has drastically altered the broader cyber threat landscape as we speak. As you are probably all well aware now, law enforcement agencies identified the culprit of that malicious operation in DarkSide. This sophisticated cybercriminal group has traditionally operated professionally and with their own distinct flavor.

When we first wrote about DarkSide, we identified this operation as the latest example of a growing professionalization trend within the ransomware field. First observed around August 2020, DarkSide was a Ransomware-as-a-Service (RaaS) operation that used press releases to communicate with victims and press, and were also among the first cybercriminal operations to announce a ban on attacks on organizations in healthcare and education. DarkSide became the ultimate product of some key developments that we had observed emerging in previous months in the ransomware arena.

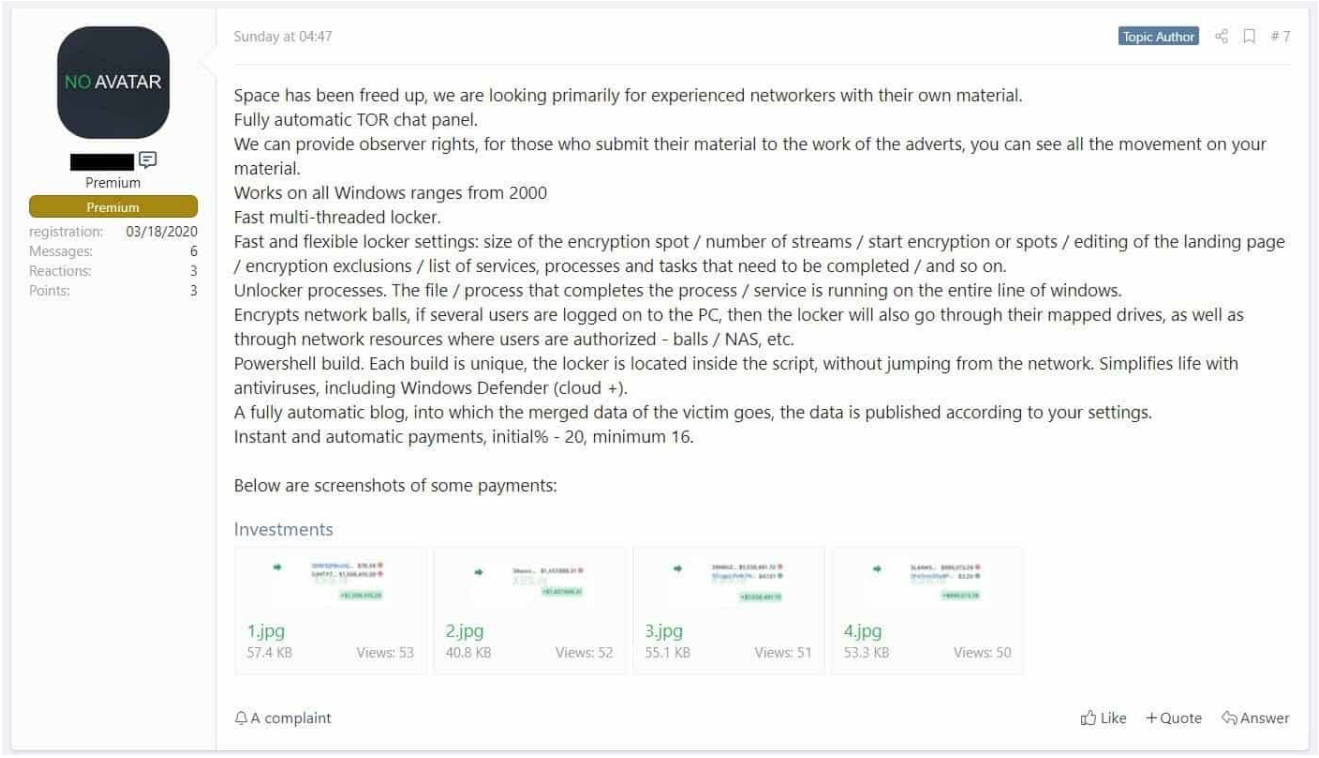
As a consequence of the attack on Colonial Pipeline, DarkSide claimed to have shut down its operations last week following increasing pressure from law enforcement agencies. Additionally, cybercriminal forums have begun banning all things ransomware from their platforms to dissociate themselves from a threat that had become too "dangerous and toxic", in the words of one forum administrator. Given the recent developments in the Ransomware-as-a-Service field, it will be interesting to see how this threat actor business model will adapt to this rapidly changing environment. This blog will analyze RaaS and try to answer some of the questions that our team of threat intelligence nerds raised in the past few days.

What is the Ransomware-as-a-Service (RaaS) Model?

In the past couple of years, the Ransomware-as-a-Service business models imposed itself as the best method for organized ransomware operators to operate a scalable business model by reducing the pressure on the malware developers. Ransomware became increasingly successful and profitable for cybercriminals and its developers started experimenting with different tactics to increase their revenues. Consequently, this model was increasingly adopted by several cybercriminal gangs attempting to outsource some of the activities associated with the encryption and extortion tactics to other affiliates.

Nowadays, the RaaS model can be summarized by three principal figures: operators, affiliates, and Initial Access Brokers (IABs).

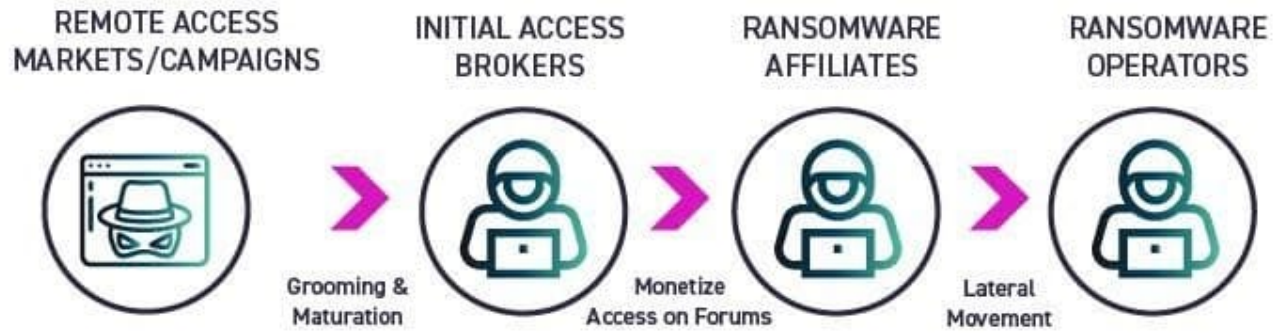
In the RaaS model, the ransomware operators own the malware source code and distribute it to the affiliates after vetting their technical skills and their country of origin (usually native English speakers are forbidden from participating). Other tasks typically involve negotiating with the victims the amount and payment of the ransom and improving the ransomware product.



Ransomware operator actively recruiting new affiliates on cybercriminal forum

Affiliates are typically offered a large share of the paid ransom, with percentage splits being reported between 65 and 90 percent for the affiliates. Wannabe affiliates must prove their technical skills before joining ransomware programs and are also required to find appropriate victims.

This is where Initial Access Brokers (IABs) come into action. These figures provide affiliates with a seemingly infinite pool of potential victims belonging to different geographies and sectors. Affiliates typically buy corporate access from IABs for cheap and then infect those networks with a ransomware product previously obtained by the operators. The rise of these threat actors in addition to the growing importance of RaaS models in the threat landscape indicates an expanding professionalization of cybercriminality. IABs allow this business model to continuously feed on new victims cheaply and efficiently, thus making ransomware work increasingly as a corporation rather than a criminal organization.



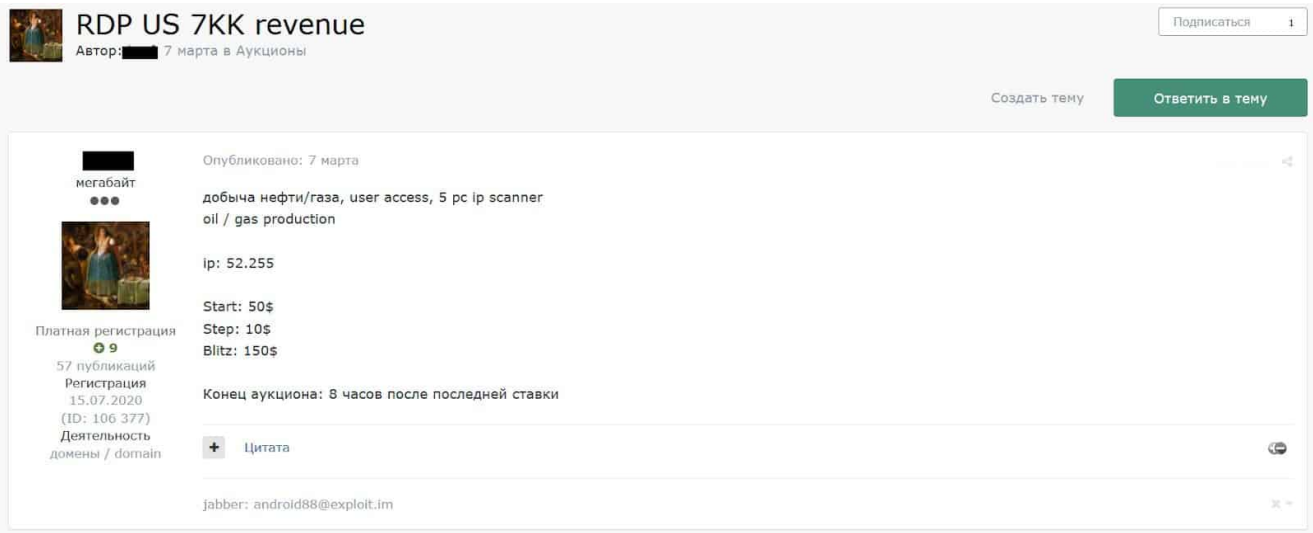
Going from Initial Access Brokers to Ransomware Operators

A RaaS Case Study: DarkSide

For the past couple of years, the model outlined above has worked just fine and has provided cybercriminals with a constant stream of money into their crypto wallets. However, the aftermath of the Colonial Pipeline incident highlighted some critical flaws in the RaaS model that now threaten to significantly affect the broader threat landscape.

Why would DarkSide target US Critical National Infrastructure (CNI)? Given the chaos ensuing from the attack on Colonial Pipeline, it is likely that that operation was conducted by a rogue affiliate that hadn't realized the potential consequences of targeting CNI. The massive international media coverage and law enforcement attention stemming from this attack later forced DarkSide to shut down its operations— something that I'm sure its operators weren't keen on doing before this attack.

Suppose we apply the RaaS model described above to this operation. In that case, it is realistic that the DarkSide affiliate that conducted the attack had previously bought remote access from an IAB without realizing they were describing a critical company or CNI for the US. In fact, IABs typically avoid naming the targeted company they're selling access to avoid giving out too much information to security researchers and law enforcement agencies. DarkSide affiliates may have bought remote access to a general company in the oil and energy industry with high revenue without realizing the critical importance of that infrastructure for the US. On the other hand, it is also possible that DarkSide knew the damage they would create but simply miscalculated the cost-risk-benefit analysis before the attack.

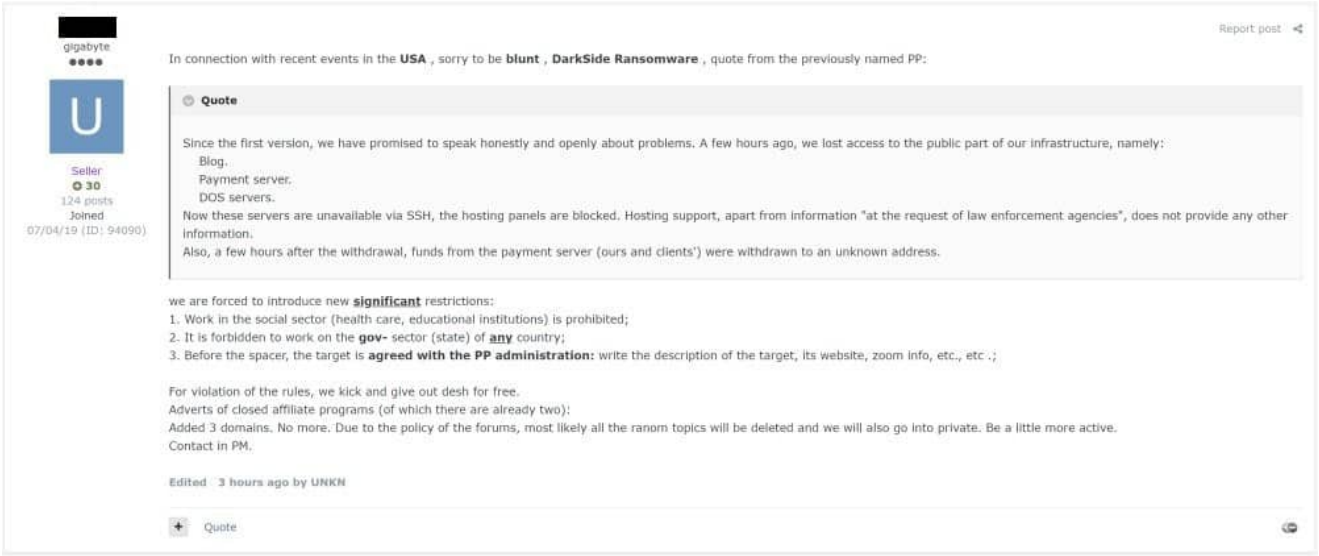


IAB advertising Remote Desktop Protocol (RDP) access to a US "oil/gas production" company with a revenue of 7 million (no currency unit given) that was sold on 07 Mar 2021

How other Ransomware gangs are adapting their RaaS

Ransomware is an attack vector in continuous evolution and expansion, and what we're observing today may not stand the test of time as tactics change. However, analyzing how these loose groups of operators function, where they get their revenues from, and what risks these groups themselves face is key to understanding the threats they pose and mitigating accordingly.

The analysis of the Colonial Pipeline ransomware attack and its aftermath highlighted that the existing Ransomware-as-a-Service model, albeit highly successful in past months, may not be well suited for the current situation of hyperawareness from security researchers and law enforcement agencies. For this reason, different threat groups associated with ransomware operations have started a review process to adapt RaaS to the changing environment and grant operators greater control over the potential affiliates' targets to avoid a second Colonial Pipeline-like incident.



Ransomware REvil operators publishing new, stricter guidelines for their affiliates' operations

For example, the REvil operators published new guidelines following DarkSide's attack against Colonial Pipeline. In one of the last posts published by ransomware operators in cybercriminal forums, REvil announced that the group will begin approving or denying encryption of any companies the group's affiliates want to target to avoid future social consequences. Additionally, REvil operators restricted attacks against organizations in the social sector and government institutions belonging to any country. Violating these rules would result in expulsion from the affiliate program and handling a decryption key to the victim for free.

Following the ransomware ban from most cybercriminal arenas, including both surface and dark web forums, it is likely that these loosely affiliated criminal groups will go on and conduct their business in private messaging channels and smaller ad hoc forums. Additionally, that ban could cause a bump in the road for ransomware gangs as they've often used those platforms to recruit more affiliates in their program. Ultimately, although some of these groups may wait to quiet things down a bit before going back to full operations, it is unlikely that DarkSide and Co. will simply stop engaging in criminal behavior without seizure of their infrastructure and arrest of their leaders by law enforcement.

At the end of the day, it is essential to follow one topical principle to understand how ransomware groups will evolve: these cybercriminals want to get rich quick and under the radar. This observation is crucial to understanding their behavior and should always be kept in mind when analyzing their actions.

If ransomware is a threat not already on your radar, or if you are interested in learning more, we recommend a 7-day free trial of Threat Intelligence with SearchLight. SearchLight clients receive real-time, actionable intelligence updates regarding ransomware activity, including analysis from our team of global analysts and intelligence on new posts to ransomware data leak sites across open and closed sources.