REvil Vanishes From Underground - Infrastructure Down

advanced-intel.com/post/revil-vanishes-from-underground-infrastructure-down-support-staff-adverts-silent

AdvIntel July 13, 2021

By Yelisey Boguslavskiy & AdvIntel Security & Development Team

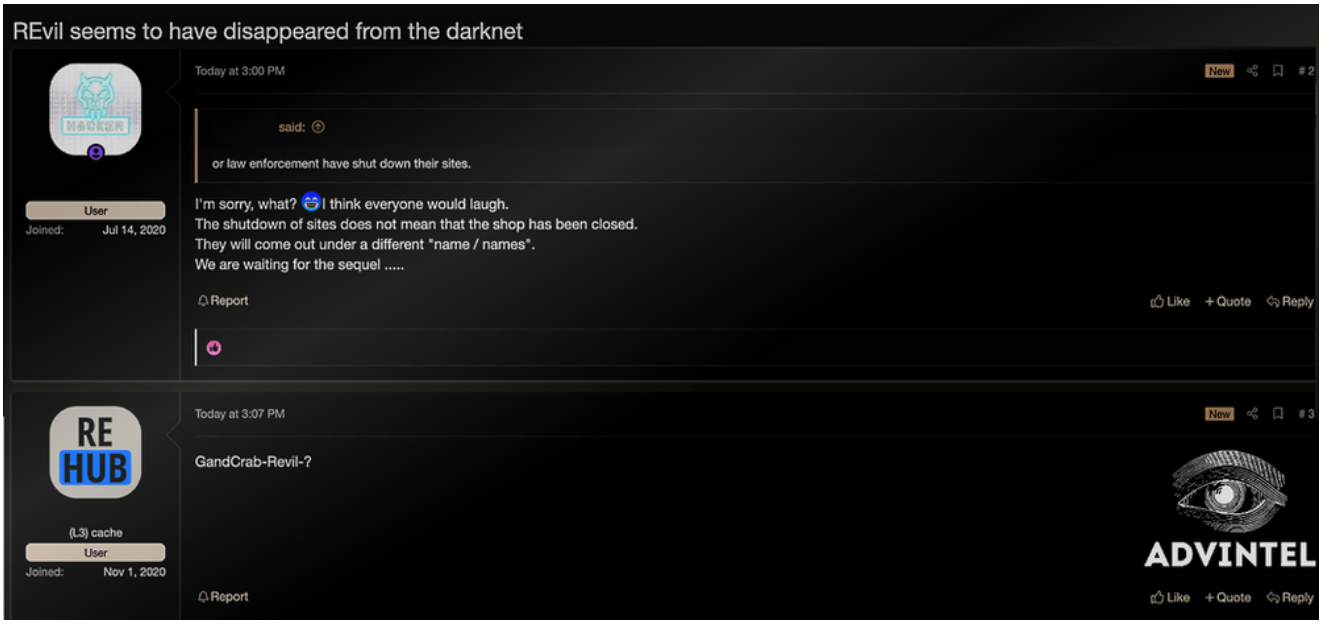
Background

On July 12 and July 13, 2021, DarkWeb and underground blogs, as well as other infrastructural elements associated with the Russian-speaking ransomware group, REvil, were reported shut down.

Attempting to access REvil's Happy Blog DarkWeb site leads to the page "not found." In the past weeks, REvil has attacked multiple large companies by targeting several MSPs.

Previously, Russian-speaking underground forums have restricted the promotion of ransomware groups such as REvil and have cracked down on deleting and banning forum members who attempt to post related topics. However, REvil still attempted to continue their interactions with the community.

On July 13, multiple forums held discussions on REvil's disappearance. Members discussed if the servers were actually down, and what was the likely cause of it. Some cybercriminals believed this could be due to law enforcement intervention, but others mocked this assertion by stating that the disappearance of REvil's blogs in no way implied the disappearance of their operations. Overall, underground leaders agreed that REvil will return, possibly under a new name, and continue their cyberattacks.



DarkWeb forum discussion on REvil's disappearance - Threat actors suggest REvil disappearance is temporary

On June 17, 2021, United States President, Joe Biden, met with Russian President, Vladimir Putin, at Geneva where Biden pushed for Russia to crack down on cyber-crime and ransomware groups. As stated, DarkWeb forums members do not believe that US law enforcement had a hand in the REvil's infrastructural shutdowns, however, they hinted at a possibility of the shutdown caused by a Russian law enforcement operation. AdvIntel analysts have analyzed several possible scenarios for the possible reasons for REvil's disappearance.

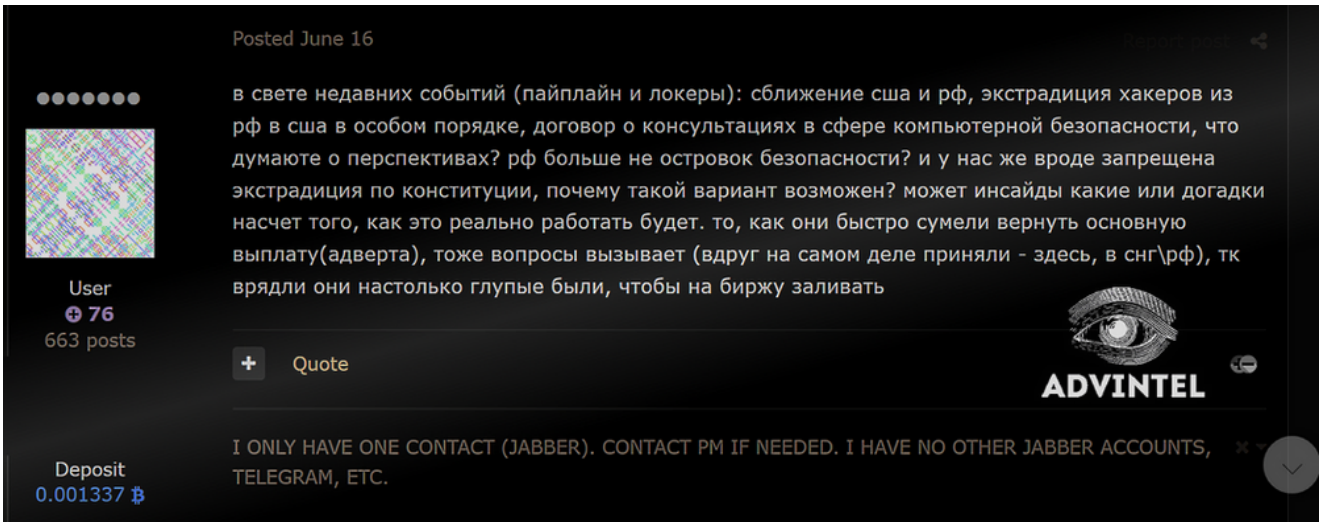
Scenario Analysis

Scenario 1 - International / US Law Enforcement (LE) operation

This is the clearest assumption due to Biden's push on cyberattacks from Russia at the Geneva convention, however, Putin does not seem bothered by it. It is more likely that the Biden administration hopes to take credit. Except for President Biden's statement that it would make sense for the United States to attack computer servers used by ransomware groups, there is currently no evidence proving that this has been the case, to support this scenario as plausible.

Scenario 2 - Russian Law Enforcement (LE) operation

AdvIntel assesses with a moderate level of confidence that this is a possible scenario behind REvil's disappearance. DarkWeb chatter conducted by Russian-speaking cybercriminals since June 2021, has been explicitly centered around fears of such an operation. According to elite underground members, fears of an action by the Russian law enforcement have been the main reason for Avaddon ransomware withdrawal and may refer to other groups as well.



Elite threat actor starting a forum thread which will become very popular - the thread was devoted to fears of US-Russia cooperation against ransomware and cybercrime leading to Russian law enforcement operations against hackers

Thread Translation

In light of recent events (pipeline ransomware attack): rapprochement between the USA and the Russian Federation, extradition of hackers from the Russian Federation to the USA in a special order, an agreement on consultations in the field of cybersecurity - what do you think about these developments?

Russia is no longer safe haven (for hackers)? and if in our country extradition is supposedly prohibited under the Constitution, why is such an option is discussed? Maybe you have some insider information (from the government) or ideas about how it will actually work.

The speed with which they (FBI) managed to return the main payment (for Colonial Pipeline ransom) also raises questions. What if the affiliate (responsible for ransom payment) was arrested here in Russia (and returned the payment). They (DarkSide) were unlikely to be so

stupid as to simply upload money onto the crypto exchange.

Other top-tier forum members joined the thread discussion and agreed that ongoing tight cooperation happens between the US and Russia leading to arrests and operations against Russian-based ransomware affiliates.

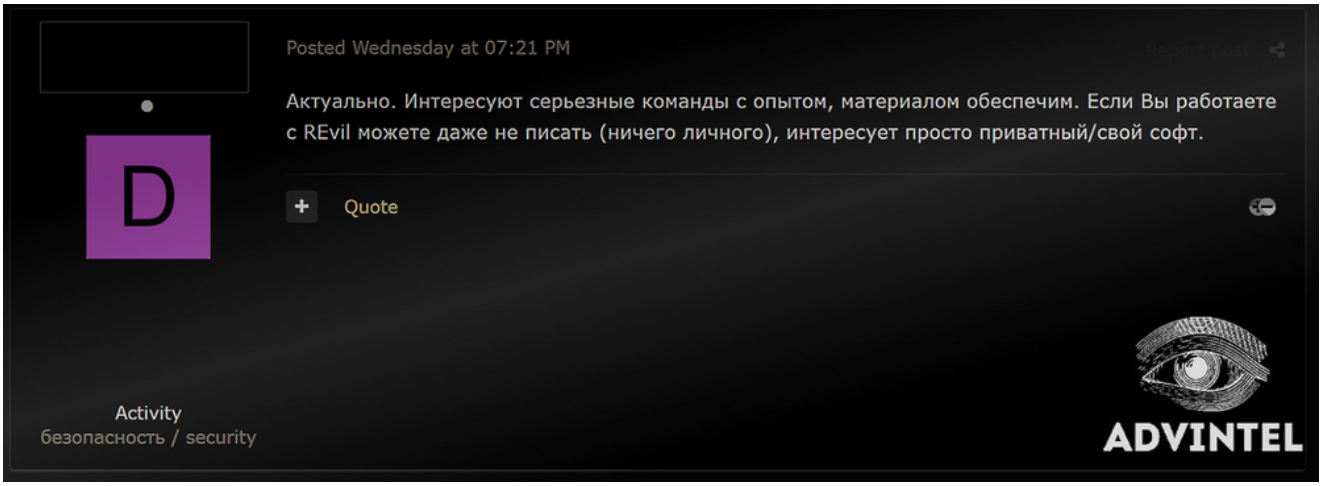
The main interpretation offered by the actors is that Russia is trying to mitigate the consequences of 2016-2020 cyberattacks against the US in order to achieve a more stable relationship with Biden.

> ***Russia is no longer safe haven (for hackers)?***

Scenario 3 - Outage is planned by REvil

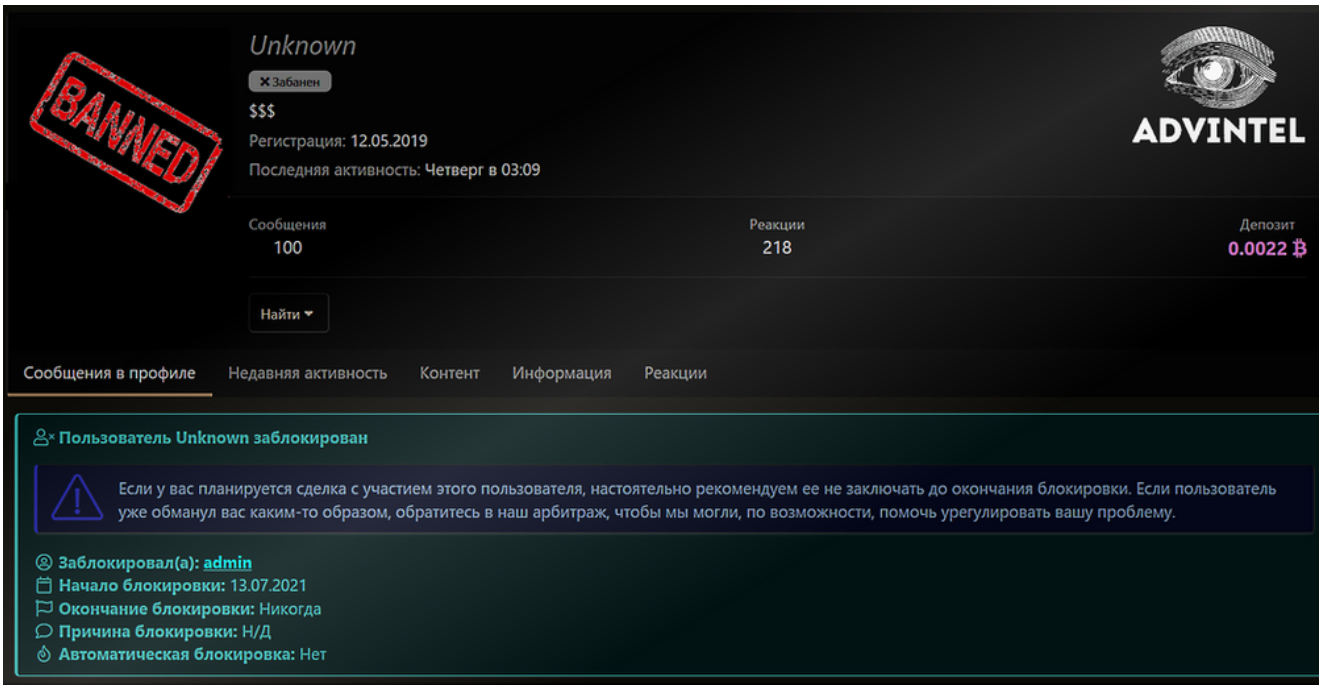
The behavior patterns and coordination of REvil suggest a planned outage and revaluation for future attacks. For example, Babuk ransomware shut down after the Washington Metro Police hack then returned as a new entity. DarkSide attempted the same operation after the Colonial Pipeline. REvil's patterns suggest the same line of action.

Most likely the group was forced to take such actions as the cybercrime community became openly rejecting REvil and seeing it as a potential trigger for a complex retaliatory operation by the US government.

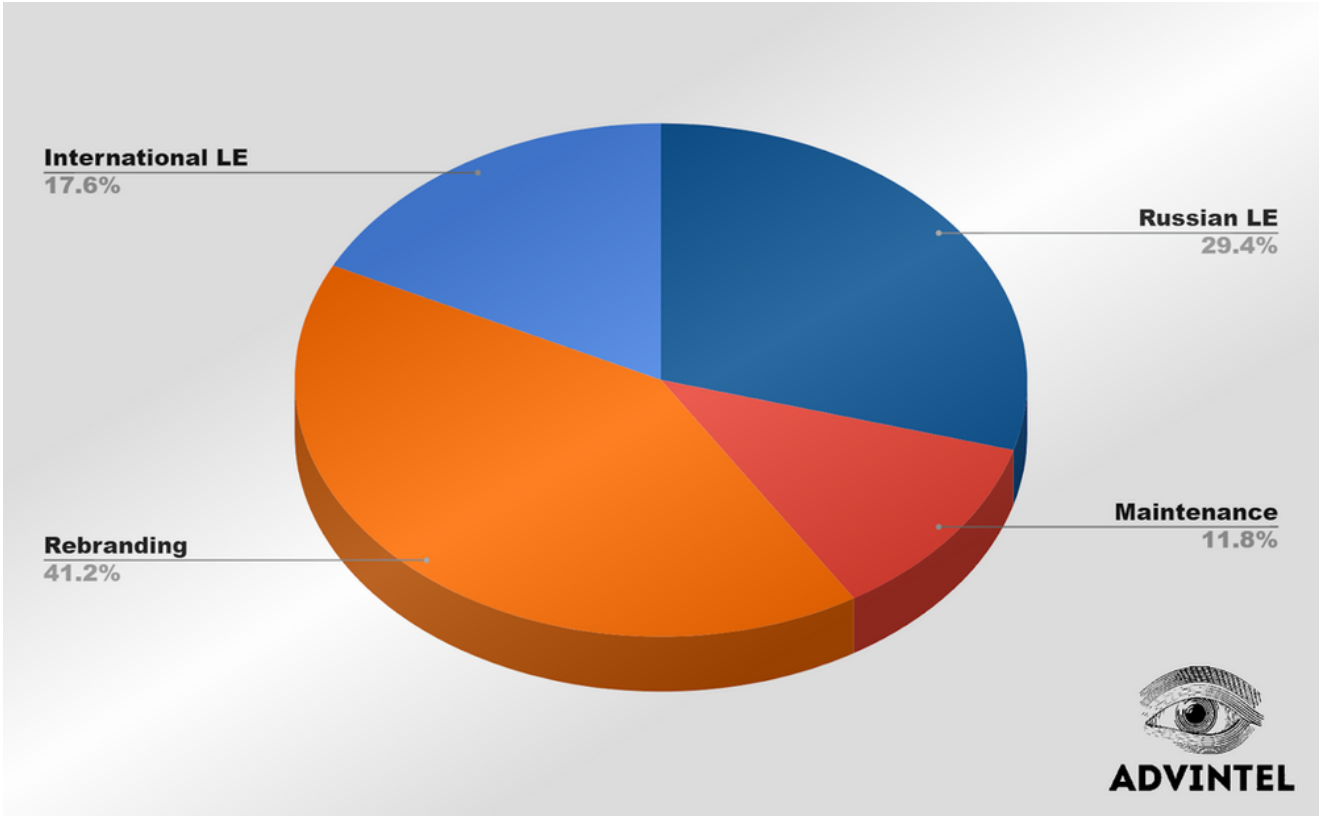


Threat actor offering a pentest job position for their ransomware group openly asking former REvil adverts to not contact them.

The bad reputation associated with REvil may have led to the creation of a critical mass of rejection after the MSPs attack. This may have lead to REvil being forced to rebrand. On June 24, 2021, threat actors started to report on stolen REvil source code which was likely leaked as an attempt of the syndicate to rebrand and reemerge under a new name.



"Unknown" - the alleged leader of REvil has been banned from major community forums on July 13, 2021



The four most popular opinions (by percent of actors sharing the opinion) discussed by top-tier/elite members of the cybercrime community, regarding the REvil disappearance. The most popular version (41,2%) is that REvil decided to shut down their systems to rebrand. Law enforcement actions are the second most popular version,

Conclusion

Communication between threat actors on underground forums suggests that the disappearance of REvil prompts a greater resurfacing of the ransomware group. Yet no evidence to suggest an outage caused by law enforcement. Threat actors on forums call to mind a common rebranding strategy used by ransomware syndicates. Often, after large-scale attacks, groups will go dark and rebuild infrastructure. AdvIntel analysts point out that REvil could be anticipating government actions. Underground actors anticipate a “sequel coming soon” for REvil entitled, “GranCrab-REvil.”