Storm in "Safe Haven": Takeaways from Russian Authorities Takedown of REvil

advintel.io/post/storm-in-safe-haven-takeaways-from-russian-authorities-takedown-of-revil

AdvIntel January 14, 2022

- Jan 14
-
- 6 min read

By Yelisey Boguslavskiy

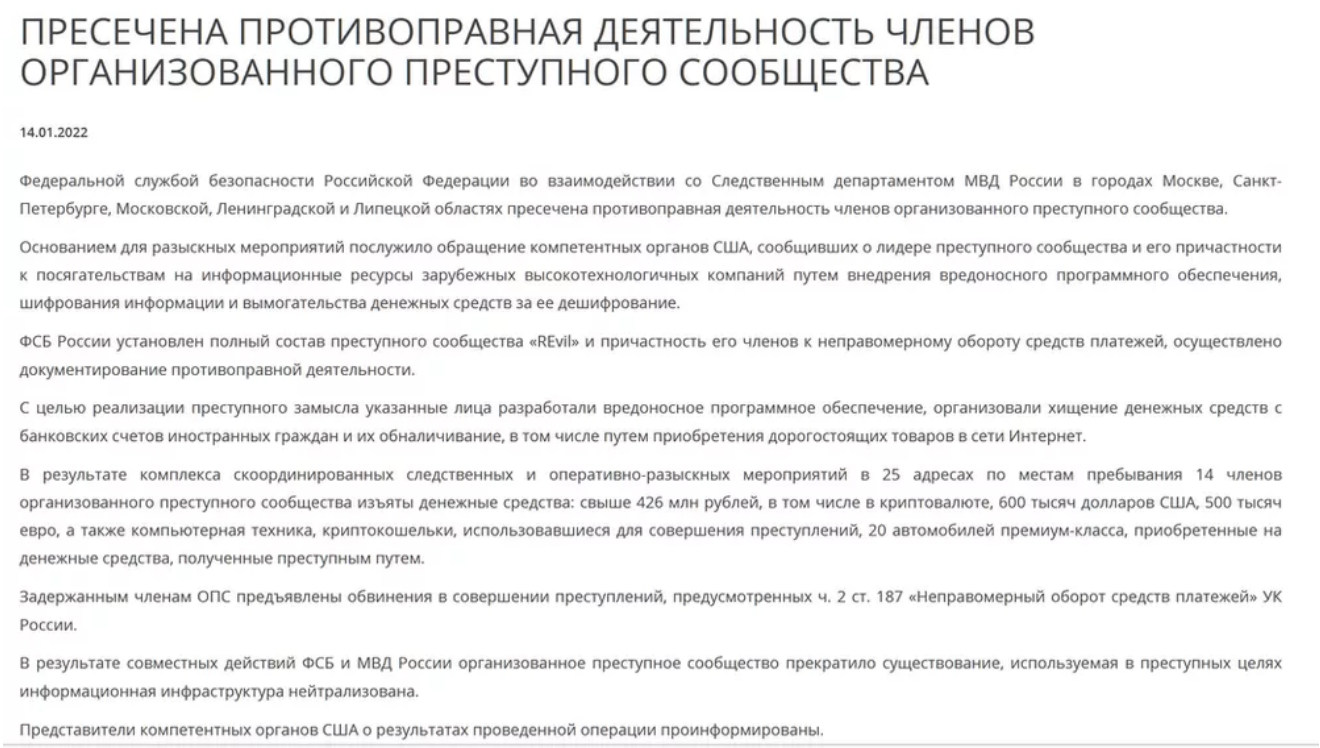
On January 14, 2022, the Russian Federal Security Service (FSB) claimed that they had arrested and shut down the REvil ransomware gang in Moscow and St. Petersburg cities and districts in response to the U.S. authorities' request.

This became one of the first and largest Russian-lead operations on arresting cybercrime group members active against Western countries per U.S. government request.

"[+] Whats Happen [+]"

AdvIntel has extensively tracked any underground chatter and most importantly, the reaction of other ransomware groups in order to identify if this arrest can significantly shift the ransomware ecosystem. The ransomware gang members do not believe that the arrest may lead to any significant changes

- Overall, criminals conclude that this arrest was a publicity operation aimed at a formal public demonstration of Russia's political intent to cooperate with the West on combating ransomware, by targeting low-tier members of an already defunct group. As such, this is a single operation and not a defined policy that can affect the cybercrime domain.
- The timing of this arrest is coincidental with the recent U.S.-Russia security talks and can be directly related to the political discussions within the geopolitical relationships between the countries.
- The arrests are related to the hacking group charged only so far for the "illicit money control/laundering" and not hacking. This may be defined by the domestic policies which Russian applies to de-criminalize hacking and criminalize cryptocurrency anonymity. Such policies aim at bringing a stronger state control over the ransomware market.



ПРЕСЕЧЕНА ПРОТИВОПРАВНАЯ ДЕЯТЕЛЬНОСТЬ ЧЛЕНОВ ОРГАНИЗОВАННОГО ПРЕСТУПНОГО СООБЩЕСТВА

14.01.2022

Федеральной службой безопасности Российской Федерации во взаимодействии со Следственным департаментом МВД России в городах Москве, Санкт-Петербурге, Московской, Ленинградской и Липецкой областях пресечена противоправная деятельность членов организованного преступного сообщества.

Основанием для разыскных мероприятий послужило обращение компетентных органов США, сообщивших о лидере преступного сообщества и его причастности к посягательствам на информационные ресурсы зарубежных высокотехнологичных компаний путем внедрения вредоносного программного обеспечения, шифрования информации и вымогательства денежных средств за ее дешифрование.

ФСБ России установлен полный состав преступного сообщества «REvil» и причастность его членов к неправомерному обороту средств платежей, осуществлено документирование противоправной деятельности.

С целью реализации преступного замысла указанные лица разработали вредоносное программное обеспечение, организовали хищение денежных средств с банковских счетов иностранных граждан и их обналичивание, в том числе путем приобретения дорогостоящих товаров в сети Интернет.

В результате комплекса скоординированных следственных и оперативно-разыскных мероприятий в 25 адресах по местам пребывания 14 членов организованного преступного сообщества изъяты денежные средства: свыше 426 млн рублей, в том числе в криптовалюте, 600 тысяч долларов США, 500 тысяч евро, а также компьютерная техника, криптокошельки, использовавшиеся для совершения преступлений, 20 автомобилей премиум-класса, приобретенные на денежные средства, полученные преступным путем.

Задержанным членам ОПС предъявлены обвинения в совершении преступлений, предусмотренных ч. 2 ст. 187 «Неправомерный оборот средств платежей» УК России.

В результате совместных действий ФСБ и МВД России организованное преступное сообщество прекратило существование, используемая в преступных целях информационная инфраструктура нейтрализована.

Представители компетентных органов США о результатах проведенной операции проинформированы.

(The official announcement by the FSB clearly state that the arrest has been conducted on the grounds of the request from the U.S. security officials)

Video of the purported arrest:

https://www.youtube.com/watch?time_continue=1&v=P_0j2k9aqDo&feature=emb_logo

Adversarial Perspective: Underground Insights

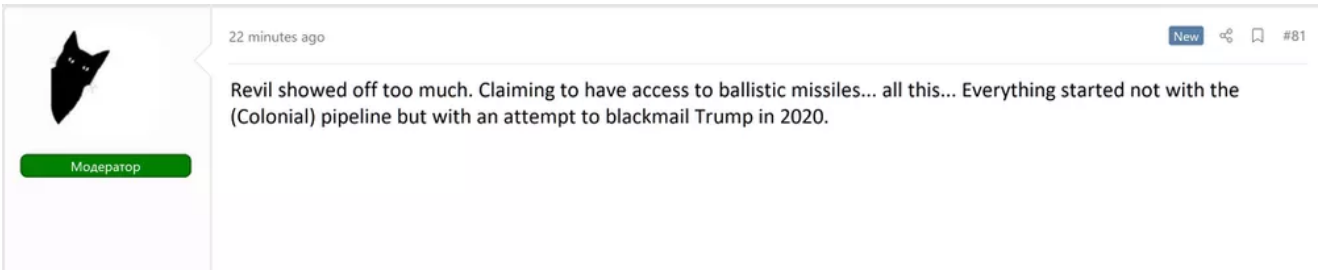
Today AdvIntel has extensively tracked any underground chatter and most importantly, the reaction of other ransomware groups in order to identify if this arrest can significantly shift the ransomware ecosystem. Our preliminary findings identify a clear consensus within the ransomware community that the arrest itself is not yet significant since it is a part of a long-term process initiated by Russian law enforcement since Spring 2021. A process associated with high-profile ransomware attacks against the U.S. critical infrastructure and inherently related to the broader geopolitical context of US-Russia relationships.

Indeed, previously AdvIntel has identified private statements by ransomware top-affiliates and leaders in the groups including **Avaddon**, **Darkside**, **HIVE**, and **BlackMatter**, who claimed that since Spring 2021, the Russian security apparatus has been applying gradual pressure on ransomware. For instance, high-profile actors directly affiliated with the **Avaddon** gang claimed that it was a direct pressure by the FSB that forced the group to release security keys. Similar statements were made on underground forums regarding **Darkside** and **REvil** when the groups released attack-related information. Even Conti ransomware, which is known for its resilience, has expressed concerns over potential pressure from Russian law enforcement.

As such, the ransomware community remains skeptical of the arrest. AdvIntel's sensitive source intelligence confirmed that Russian-speaking criminal actors agree that the individuals who were arrested today are most likely low-tier affiliates who have directly linked to the REvil auxiliary operations such as money transfers, money laundering, and other support activities that follow ransomware attacks. In other words, threat actors are confident that neither developers nor skillful pentesters of REvil have been arrested based on the AdvIntel insights into the actual affiliate ecosystem.

The broader non-ransomware underground chatter is characterized by generic comments and moderate support of REvil's arrest. This support is due to the group's poor reputation across the Russian-speaking cybercrime. Some cheer since Revil was known across the underground as a group scamming their affiliates, in this sense, the forum actors believe that the arrest indeed serves some sort of justice.

The underground community agrees that REvil has been continuously making strategic mistakes by focusing on political publicity, committing political attacks, and attracting media and public attention. Actors conclude that if a certain group remains within a traditional cybercrime pass, i.e. being strictly non-public and for-profit, such a group can sustain peacefully and continue to operate.



(The moderator of the XSS and Exploit forums who is responsible for audit and review of all ransomware and malware partnerships on these two major forums has been one of the most consistent critics of REvil)

Actors from the older generation of cybercrime recall their traditional comment that ransomware is a form of intellectual primitivism, as it does not require sophistication. (read more in AdvIntel's research: [DarkWeb Insights] The Digital "Thief War": How COVID-19 Pandemic Triggered a Generational Conflict). They add that due to this primitivism it was not surprising that ransomware operators were caught so easily.

Overall, criminals conclude that this arrest was a publicity operation aimed at a formal public demonstration of Russia's political intent to cooperate with the West on combating ransomware, by targeting low-tier members of an already defunct group. As such, this is a single operation and not a defined policy that can affect the cybercrime domain.

AdvIntel's analysis: Geopolitics and cryptocurrencies; is Russia a "Safe Haven" for hackers?

De-Escalation Rollercoaster

The timing of this arrest is coincidental with the recent US-Russia security talks and can be directly related to the political discussions within the geopolitical relationships between the countries.

(The United States and Russia meet for highest level security talks on January 10, 2022, in Geneva; image source: Associated Press)

AdvIntel previously noted on this connection between geopolitics and cybercrime in the context of the Avaddon group security key release. Since May 2021, we observe a clear intervention of politics into the cybercrime domain, including multiple statements made by the Russian government, the Russian Ministry of Foreign Affairs, and by President Putin personally about establishing an international Russian-American initiative to establish a joint cybersecurity landscape. The Russian officials likely see this as a tool of de-escalating the US-Russian relationships.

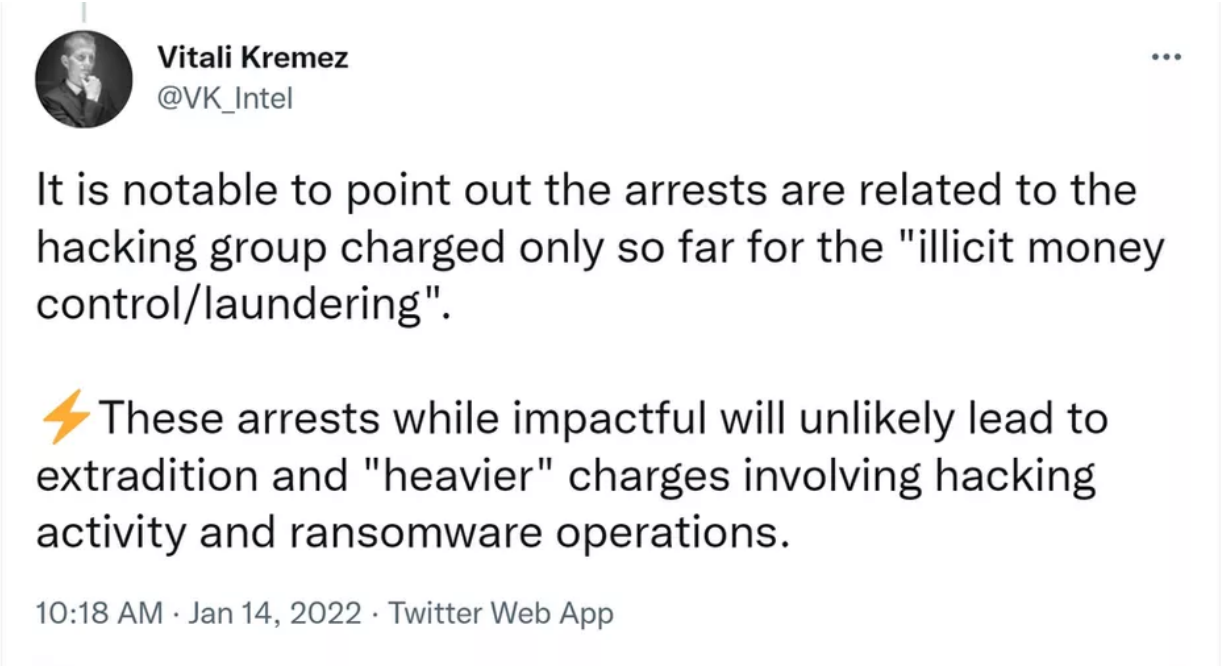
Today's situation mimics the May 2021 case, when troops were also concentrated on the Ukrainian border (cyberattacks against Ukrainian government entities occurred on the day of REvil arrest), and Russia was facing threats of domestic turbulence. Indeed, the Russian

government traditionally goes through rounds of escalation and de-escalation with the West. Just like in Spring 2021, the Kremlin may now be aiming to create a framework of stability in the international arena and cybersecurity - a controversial space or the Russia-U.S. relationship is once again on the frontlines of this de-escalation agenda.

(The REvil arrest happened on the same day as a massive attack on Ukrainian the websites of the Ministry of Foreign Affairs and a number of other government agencies that are temporarily down. The attack happened during another round of escalation of tensions on Ukraine-Russia border)

REvil & the War on Crypto

What is even more interesting is the domestic context. AdvIntel's CEO Vitali Kremez noted that the arrests are related to the hacking group charged only so far for the "illicit money control/laundering" and not hacking.



(https://twitter.com/VK_Intel/status/1482008331136942081)

This may be a consequence of deliberate legal modeling which Russia has been using since the 2000th.

Indeed, the Russian Criminal Code's Articles 272, 273, and further, which define punishment for hacking only presume minimum sentences of 1 year for "Illegal access to computer information protected by law, if this act has caused the destruction, blocking, modification or copying of computer information". The sentence can reach 2-3 years if the crime was committed by a group of people and for-profit and 4 years if the accused has performed insider crime by using their position in an entity.

This way, the specific development of the Russian criminal code in regards to hacking, makes long-term sentences of hackers unlikely. (Note: the Russian criminal code also limits the accumulation of sentence years based on different charges, in other words, the lengths of the sentence is defined by the strongest charge and not by the combination of different charges which do not sum up)

This can explain why REvil members were charged with the illicit funds' charge that has a maximum sentence of seven years, and this may not be a simple judicial compilation but a consequence of Russian domestic policies.

Previously, AdvIntel has investigated a major change in Russian legislation regarding cryptocurrencies: New Russian Crypto Law - A Government Tool to Take Control Over the DarkWeb Market? We predicted that by introducing the January 1, 2021, law regulating cryptocurrencies, the Russian government aims to seek control over the ransomware sector of the illicit economy that became extremely prolific over the past two years. We assessed that by establishing this crypto law, the Russian government built a legal foundation to take over ransomware “businesses”. Tightened on cryptocurrency flows and obligated to report their balances, hackers will no longer be able to “legally” stay in the shade. The criminal enterprise might be easily taken down completely or more likely to be obligated to cooperate with the government for its financial and national good.

Interestingly enough, on January 13, 2022, the day before the REvil arrest, Alexander Bastrykin, the Chairman of the Russian Investigative Committee and one of the top government officials demanded mandatory deanonymization of all cryptocurrency holders in Russia. He specifically stated that the anonymity associated with cryptocurrency manifests in major risks for public safety.

All these are signs that domestically Russia is aiming to keep its hacking-related legislation mild and ambiguously defined, while significantly cracking down on cryptocurrencies. This way, loyal hackers can still operate freely, while those who are chosen as a target of the state can be charged with illicit funds law within the broader context of criminalization of cryptocurrency use. REvil’s arrest may be defined by these dynamics.

Disrupt ransomware attacks & prevent data stealing with AdvIntel’s threat disruption solutions. Sign up for AdvIntel services and get the most actionable intel on impending ransomware attacks, adversarial preparations for data stealing, and

ongoing network investigation operations by the most elite cybercrime collectives.