The moral underground? Ransomware operators retreat after Colonial Pipeline hack

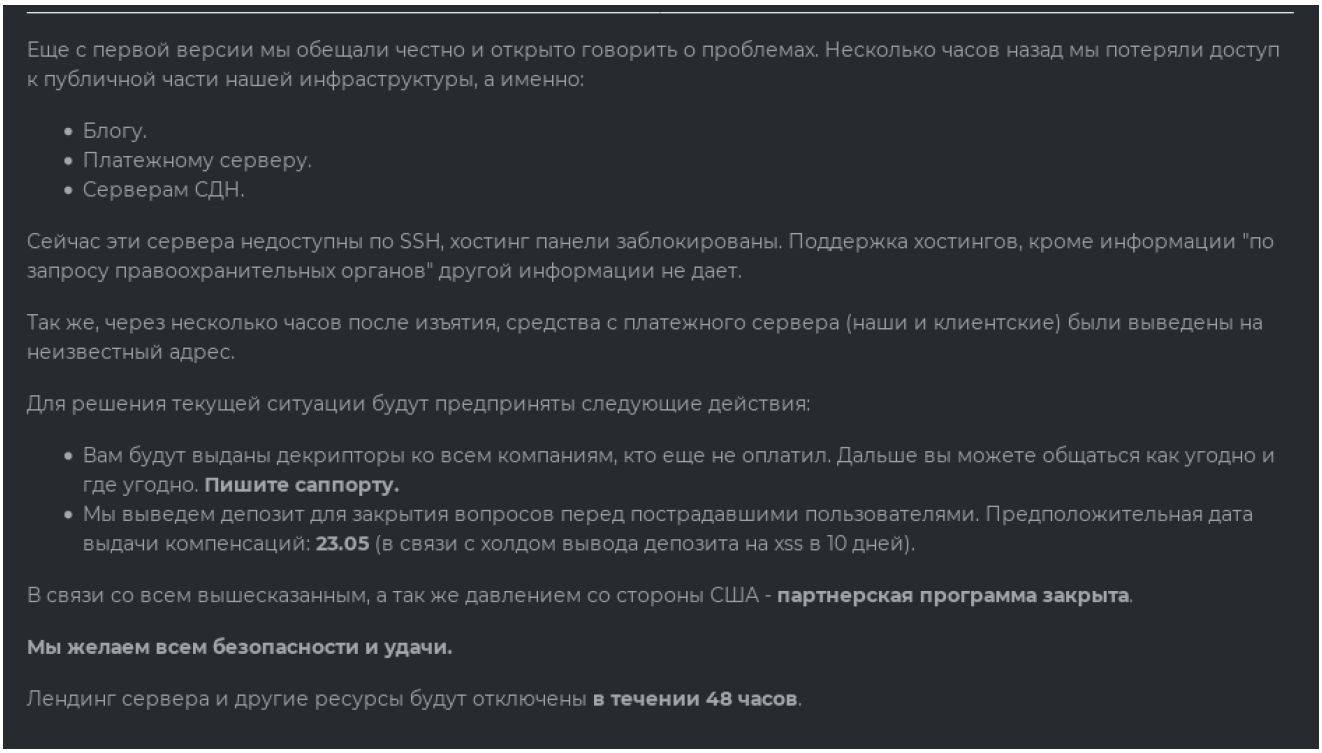
intel471.com/blog/darkside-ransomware-shut-down-revil-avaddon-cybercrime

The ransomware attack on Colonial Pipeline has caused a large amount of trouble in the United States. It looks as if that trouble has made its way back to the cybercrime underground.

Intel 471 has observed numerous ransomware operators and cybercrime forums either claim their infrastructure has been taken offline, amending their rules, or they are abandoning ransomware altogether due to the large amount of negative attention directed their way over the past week.

On May 13, 2021, the operators of the DarkSide Ransomware-as-a-Service (RaaS) announced they would immediately cease operations of the DarkSide RaaS program. Operators said they would issue decryptors to all their affiliates for the targets they attacked, and promised to compensate all outstanding financial obligations by May 23, 2021. The group, which has been named as the one responsible for the Colonial Pipeline incident, also passed an announcement to its affiliates claiming a public portion of the group's infrastructure was disrupted by an unspecified law enforcement agency. The group’s name-and-shame blog, ransom collection website, and breach data content delivery network (CDN) were all allegedly seized, while funds from their cryptocurrency wallets allegedly were exfiltrated.

Intel 471 obtained the announcement, which is available below.



The note DarkSide passed to affiliates.

Translated in English, the note reads:

Starting from version one, we promised to speak about problems honestly and openly. A couple of hours ago, we lost access to the public part of our infrastructure, in particular to the

blog

payment server

CDN servers

At the moment, these servers cannot be accessed via SSH, and the hosting panels have been blocked.

The hosting support service doesn't provide any information except "at the request of law enforcement authorities." In addition, a couple of hours after the seizure, funds from the payment server (belonging to us and our clients) were withdrawn to an unknown account.

The following actions will be taken to solve the current issue: You will be given decryption tools for all the companies that haven't paid yet.

After that, you will be free to communicate with them wherever you want in any way you want. Contact the support service. We will withdraw the deposit to resolve the issues with all the affected users.

The approximate date of compensation is May 23 (due to the fact that the deposit is to be put on hold for 10 days on XSS).

In view of the above and due to the pressure from the US, the affiliate program is closed. Stay safe and good luck.

The landing page, servers, and other resources will be taken down within 48 hours.

DarkSide was not the only group to make this type of announcement on May 13. Another RaaS group, Babuk, claimed it handed over the ransomware's source code to "another team," which would continue to develop it under a new brand. The group pledged to stay in business, continuing to run a victim name-and-shame blog, while also encouraging other ransomware gangs to switch to a private mode of operation. This announcement came after the group released the remaining portions of the data stolen from the District of Columbia's Metropolitan Police Department. That archive, which contained 250 GB worth of data, allegedly included officers' and auxiliary personnel personal data, a database filled with information on criminals, as well as information on police informants.

While Babuk pledged to keep its operations running, it may find it difficult to find affiliates. Shortly after the above announcements, the administrator for one of the most popular Russian-language cybercrime forums announced an immediate ban of all ransomware-related activity on their forum. The forum now prohibits ransomware advertising, sales, ransom negotiation services and similar offers. Any listings that are currently on the forums will be deleted. The administrator explained the move by saying ransomware operations are becoming "more and more toxic" and dangerous for the underground community.

That announcement caused a ripple effect on the forum, causing other well-known RaaS affiliates to make their own announcements regarding the status of their operations. One operator known to be behind the REvil ransomware program announced they would stop promoting their malware on the forum, deleting the forum thread where the service was advertised. The operator said REvil would continue operating on another well-known Russian-language cybercrime forum, but expected that forum would soon also ban all ransomware-related activity. If that is to occur, the operator said REvil would likely go fully private.

Shortly thereafter, REvil's operator released coordinated statements with an operator behind the Avaddon RaaS program, announcing an amendment to the "rules" of their organizations. The updates barred affiliates from targeting government, healthcare, educational and charity organizations regardless of their country of operation. Additionally, all other targets need to be pre-approved by the ransomware's operators prior to actual deployment.

Intel 471 believes that all of these actions can be tied directly to the reaction related to the high-profile ransomware attacks covered by the media this week. However, a strong caveat should be applied to these developments: it's likely that these ransomware operators are

trying to retreat from the spotlight more than suddenly discovering the error of their ways. A number of the operators will most likely operate in their own closed-knit groups, resurfacing under new names and updated ransomware variants. Additionally, the operators will have to find a new way to “wash” the cryptocurrency they earn from ransoms. Intel 471 has observed that BitMix, a popular cryptocurrency mixing service used by Avaddon, DarkSide and REvil has allegedly ceased operations. Several apparent customers of the service reported they were unable to access BitMix in the last week.

Furthermore, there will be ransomware operators that continue with their own operations despite all of this week’s attention. On the same day as the coordinated announcements from REvil and Avaddon: Ireland's health service operator had to shut down all of its IT systems due to a "significant" ransomware attack.

Intel 471 will continue to watch and report on further developments as ransomware operators adjust their enterprises.