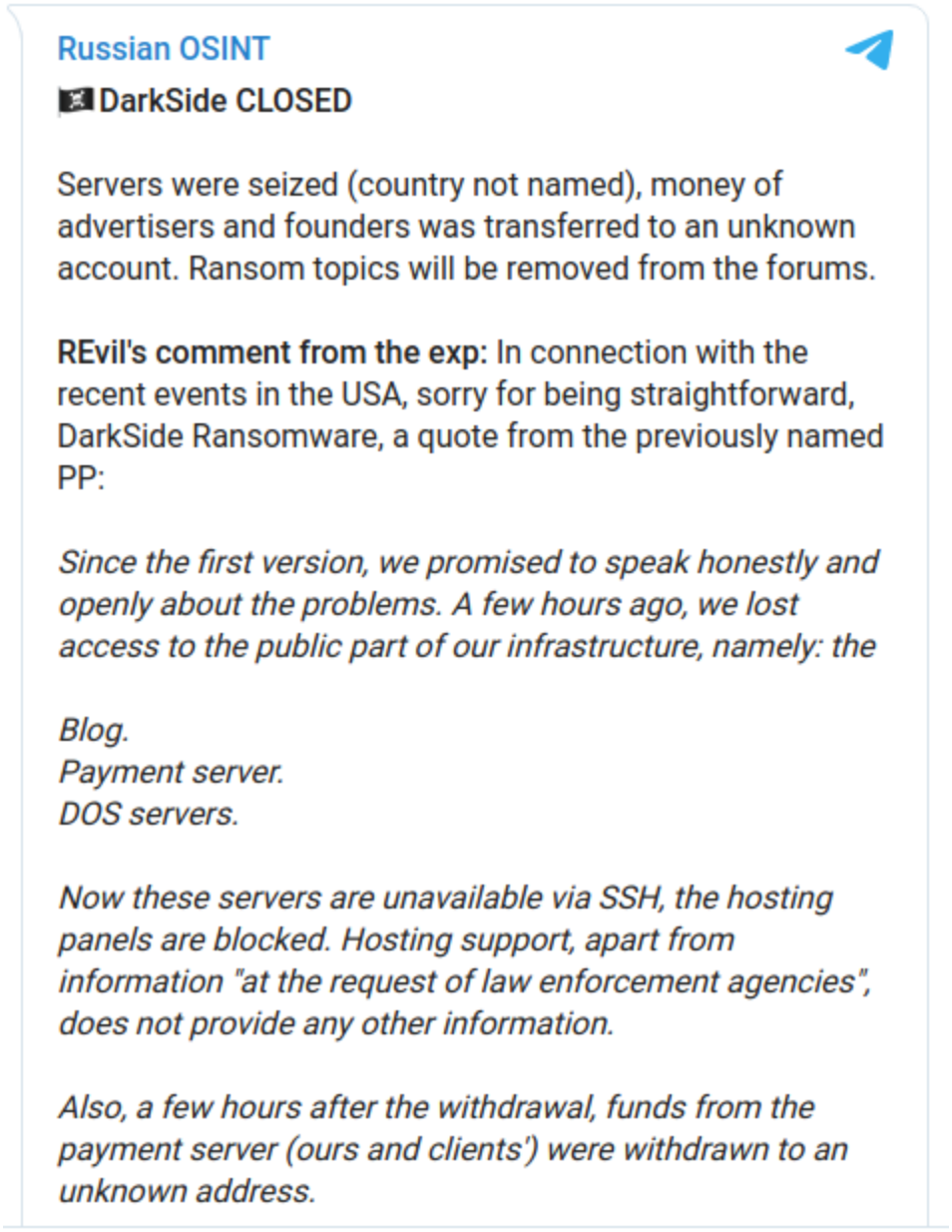
DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized

krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/

The **DarkSide** ransomware affiliate program responsible for the six-day outage at **Colonial Pipeline** this week that led to fuel shortages and price spikes across the country is running for the hills. The crime gang announced it was closing up shop after its servers were seized and someone drained the cryptocurrency from an account the group uses to pay affiliates.

“Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account,” reads a message from a cybercrime forum reposted to the Russian OSINT Telegram channel.



“A few hours ago, we lost access to the public part of our infrastructure,” the message continues, explaining the outage affected its victim shaming blog where stolen data is published from victims who refuse to pay a ransom.

“Hosting support, apart from information ‘at the request of law enforcement agencies,’ does not provide any other information,” the DarkSide admin says. “Also, a few hours after the withdrawal, funds from the payment server (ours and clients’) were withdrawn to an unknown address.”

DarkSide organizers also said they were releasing decryption tools for all of the companies that have been ransomed but which haven’t yet paid.

“After that, you will be free to communicate with them wherever you want in any way you want,” the instructions read.

The DarkSide message includes passages apparently penned by a leader of the REvil ransomware-as-a-service platform. This is interesting because security experts have posited that many of DarkSide's core members are closely tied to the REvil gang.

The REvil representative said its program was introducing new restrictions on the kinds of organizations that affiliates could hold for ransom, and that henceforth it would be forbidden to attack those in the "social sector" (defined as healthcare and educational institutions) and organizations in the "gov-sector" (state) of any country. Affiliates also will be required to get approval before infecting victims.

The new restrictions came as some Russian cybercrime forums began distancing themselves from ransomware operations altogether. On Thursday, the administrator of the popular Russian forum **XSS** announced the community would no longer allow discussion threads about ransomware moneymaking programs.

"There's too much publicity," the XSS administrator explained. "Ransomware has gathered a critical mass of nonsense, bullshit, hype, and fuss around it. The word 'ransomware' has been put on a par with a number of unpleasant phenomena, such as geopolitical tensions, extortion, and government-backed hacks. This word has become dangerous and toxic."

In a blog post on the DarkSide closure, cyber intelligence firm **Intel 471** said it believes 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," Intel 471 wrote. "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."