How Ransomware Adversaries Reacted to the DarkSide Attack

crowdstrike.com/blog/how-ransomware-adversaries-reacted-to-the-darkside-pipeline-attack/

CrowdStrike Threat Intel Team

May 28, 2021

The repercussions from the Colonial Pipeline DarkSide ransomware incident have garnered global attention and caused major shifts in the ransomware ecosystem. Many criminal forums have now banned ransomware, and as a result, many ransomware-as-a-service (RaaS) operators have already ended their public communications regarding affiliate and partner recruitment. While this incident will have a significant short- to medium-term impact on the public-facing operations of RaaS provisions,the RaaS operation model will unlikely be abandoned and will likely continue in more private and secure communication channels.

Ransomware Infection at Pipeline Company

On May 7, 2021, Colonial Pipeline — operator of 5,500 miles of pipeline from the Gulf Coast to the U.S. East Coast providing 45% of the gasoline to this region — was the victim of a ransomware infection. Initial details surrounding the incident were very tightly controlled, and information filtered out slowly, likely due to the engagement of U.S. government and law enforcement agencies. On May 9, 2021, the FBI released a public statement expressing they were “working closely with the company and our government partners.” The FBI’s follow-up statement on May 10 publicly indicated the incident involved the *DarkSide* ransomware. It was later reported Colonial Pipeline had approximately 100GB of data stolen from their network, and the organization allegedly paid almost $5 million USD to a *DarkSide* affiliate.

Government Statements Regarding Attribution

On May 10, President Biden stated the U.S. intelligence community had no evidence at the time that the Russian government was involved in this incident — but evidence did exist that the actors responsible were located in Russia. In response to a question about possible state ties of the *DarkSide* operators, the United States National Security Council's most senior cybersecurity official publicly described them as "a criminal actor." On May 11, 2021, the Russian Embassy in the U.S. released a statement that they "took note of the attempts of some media to accuse Russia of a cyberattack on Colonial Pipeline" and distanced themselves from the ransomware incident, stating they "categorically reject the baseless fabrications of individual journalists and reiterate that Russia does not conduct 'malicious' activity in the virtual space."

CARBON SPIDER

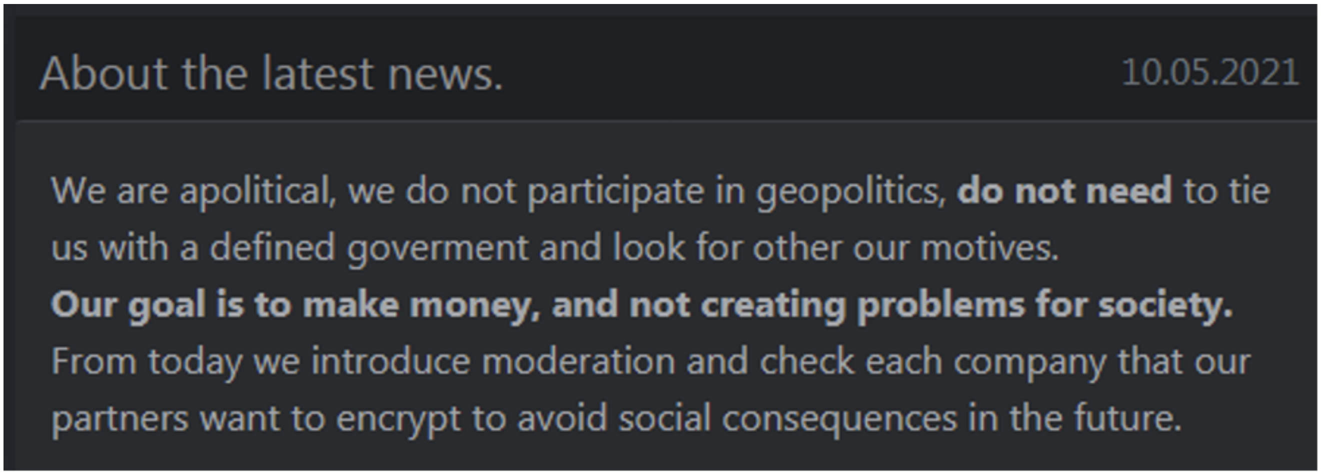
CrowdStrike Intelligence attributes the operation of the *DarkSide* RaaS to CARBON SPIDER, and is a skilled eCrime (ECX) group, highly likely Eastern Europe- or Russia-based.

CARBON SPIDER has been active since at least 2013 and previously targeted the hospitality and retail sectors in pursuit of payment card data. In April 2020, CARBON SPIDER began conducting big game hunting (BGH) operations. The evolution from targeted eCrime to BGH is reminiscent of how other adversaries (such as INDRIK SPIDER and WIZARD SPIDER) have shifted their operations to focus primarily or exclusively on BGH.

CARBON SPIDER's BGH campaigns were likely motivated by the COVID-19 pandemic and the reduction in point-of-sale (POS) transactions. The adversary used PINCHY SPIDER's *REvil* RaaS prior to introducing their own ransomware, *DarkSide,* in August 2020, and were among the first ransomware operators to target VMWare ESXi systems. In November 2020, CARBON SPIDER made the business decision to advertise their *DarkSide* ransomware to affiliates via a RaaS model and have been successfully growing their operations since.

CARBON SPIDER's Reaction

On May 10, 2021, CARBON SPIDER posted a press release to the *DarkSide* dedicated leak site (DLS) stating they are "apolitical," do not participate in "geopolitics," and their "goal is to make money, and not creating problems for society" (Figure 1).



About the latest news. 10.05.2021

We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined goverment and look for other our motives.
Our goal is to make money, and not creating problems for society.
From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

Figure 1. CARBON SPIDER’s press release on their DLS

CARBON SPIDER further stated there is “no need” to associate the group with a “defined government,” and that they are introducing a system to check potential affiliate victims of the RaaS before encryption to prevent “social consequences.” CrowdStrike Intelligence assesses that CARBON SPIDER is highly likely located in Russia or neighboring countries, and there is currently no indication the group or any *Darkside* RaaS affiliates are associated with any state-operated or politically motivated threat actors.

The rapid response and introduction of a vetting process for affiliate victims suggests CARBON SPIDER is aware the Colonial Pipeline incident was conducted by an affiliate of the *DarkSide* RaaS as opposed to CARBON SPIDER themselves. This is based on the imposition of moderation and checking of potential partner victims prior to infection with *DarkSide*.

A statement on May 13, 2021 — purportedly from CARBON SPIDER — claimed the adversary group lost access to the *DarkSide* DLS, payment servers and content delivery network (CDN) servers. The statement also claimed CARBON SPIDER servers had been blocked “at the request of law enforcement agencies.” Furthermore, cryptocurrency allegedly belonging to CARBON SPIDER and their clients had been transferred to an unknown address. A revision to the statement (subsequently made by the “Russian OSINT” Telegram channel) claimed that “no arrests were made” and “DarkSide has simply shut down.” Whether the *DarkSide* RaaS will remain closed permanently is currently unclear; however, new infrastructure for other CARBON SPIDER tools has been identified since the alleged *DarkSide* shutdown, indicating CARBON SPIDER will highly likely remain a sophisticated and active threat actor.

Forum Reactions

On May 13, 2021, XSS forum administrators made an extensive post detailing their prohibition of ransomware-related posts and ban on threads associated with ransomware affiliate programs, rental and sale. All future topics meeting any of the criteria will reportedly be removed — threads related to *Avaddon*, *DarkSide*, *LockBit*, *REvil* and *Trinage* ransomware were all removed from the forum. The following reasons were provided for the change in policy:

- The main purpose of the forum is “technical education” and research, and these goals do not align with the purely financial motivations of ransomware operators.
- “Newbies” attract media attention under the pretense of making large sums of money without learning, coding, or thinking, and with minimal effort and restraint.
- Ransomware has become a hugely covered topic in the media and attracts negative attention through “hype,” “noise,” and “nonsense.”
- Ransomware has become associated with a “number of unpleasant phenomenon,” including geopolitics, extortion and government hacking.

The following day, similar posts appeared on Exploit and RaidForums stating that due to the mass-media attention, it was no longer feasible to entertain posts relating to ransomware. The statement on Exploit suggested that this restriction only applied to ransomware specifically, allowing other content — criminal or otherwise — to continue without restriction.

Ransomware Operators’ Reactions

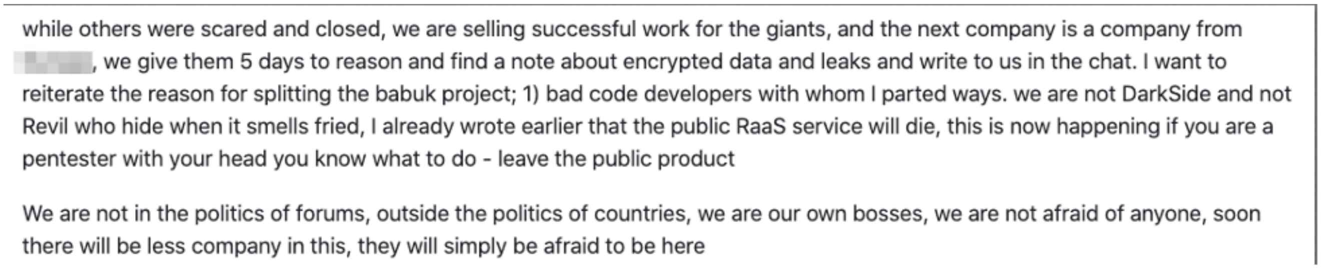
PINCHY SPIDER, developers and operators of the popular *REvil* RaaS, announced intentions to move away from the forums to private communications, and additionally detailed “significant restrictions” on future *REvil* operations:

- Social-sector victims (such as academic and healthcare organizations) are not to be infected.
- Infections against government-sector entities in any country are strictly prohibited.
- Affiliates must provide the owners of the RaaS with detailed information regarding any potential target and obtain permission prior to initiating ransomware operations.

RIDDLE SPIDER, operators of the *Avaddon* RaaS, posted a similar announcement “due to the current situation” in the U.S., listing the following restrictions on future *Avaddon* operations:

- Entities in the Commonwealth of Independent States (CIS) are not to be infected.
- Work against public-sector victims (such as academic and healthcare organizations) is prohibited.
- Permission of the “administration” must be sought prior to infection.

In contrast, the operators of *Babuk Locker* ransomware criticized the reactions within the eCrime community, predicted RaaS “will die,” encouraged “pentesters” (likely a reference to eCrime actors specializing in compromising networks) to abandon public RaaS programs, and announced intentions to launch a “huge platform for independent leaks” — supposedly for use by “successful no-name teams” who do not run from the “ship like rats and change the policy” of their operations (Figure 2).



while others were scared and closed, we are selling successful work for the giants, and the next company is a company from [redacted], we give them 5 days to reason and find a note about encrypted data and leaks and write to us in the chat. I want to reiterate the reason for splitting the babuk project; 1) bad code developers with whom I parted ways. we are not DarkSide and not Revil who hide when it smells fried, I already wrote earlier that the public RaaS service will die, this is now happening if you are a pentester with your head you know what to do - leave the public product

We are not in the politics of forums, outside the politics of countries, we are our own bosses, we are not afraid of anyone, soon there will be less company in this, they will simply be afraid to be here

Figure 2. Extract of an announcement by *Babuk Locker* operators on their DLS

Access Brokers

The changes on the criminal underground forums have also impacted other eCrime actors, including access brokers. Access brokers are threat actors that gain backend access to various organizations and advertise this access to other eCrime actors via criminal underground forums or private communication channels. Access broker offerings are heavily tailored toward BGH operators and their affiliates, often including the annual revenue of the victim — acquired from public sources — as this can be used to calculate the potential ransom demand.

Since the beginning of 2021, CrowdStrike Intelligence has observed access brokers advertise initial access to entities in the energy sector, including oil and gas companies. Entities in these sectors can be lucrative victims since they often possess relatively large annual revenues that are of interest to ransomware operators and affiliates. On Jan. 2, 2021, a Ukraine-based access broker stated in a dual English- and Russian-language forum that they were planning to deploy an unspecified ransomware variant against an oil and gas entity. A portion of funds received from this operation was later transferred to an associated group of Bitcoin (BTC) wallets that also received the ransom from the Colonial Pipeline incident. On Feb. 13 and March 7, 2021, the access broker *barf* advertised administrator and user access to two different entities in the energy and the oil and gas sectors on a dual English- and Russian-language forum.

Since the Colonial Pipeline incident and the changes introduced by the forum administrators, there has been a general decline in the number of access broker advertisements on the forums — aside from one Brazil-based access broker targeting a Europe-based oil and gas company who is seemingly intent on selling their access despite the ban on ransomware-related offerings. Similar to the reaction by RaaS operators, access broker activity is unlikely to cease, but brokers will likely increasingly adopt the use of private communications for advertising and selling access in the near term. Access brokers will almost certainly continue to target entities within the energy sector as the vertical remains a lucrative target for ransomware operations, and access brokers profit from providing initial access opportunities.

Looking Forward

The intense attention surrounding the Colonial Pipeline incident has had a significant impact on the criminal marketplace and the political landscape. Scrutiny of this event will almost certainly alter how ransomware operators conduct their activity and how government and law enforcement agencies respond to the ransomware threat.

RaaS operators, such as CARBON SPIDER (*DarkSide*), PINCHY SPIDER (*REvil*), and RIDDLE SPIDER (*Avaddon*), have apparently accepted blanket forum bans on the discussion and marketing of ransomware services. These bans likely spell the end for most public communications regarding affiliate and partner recruitment. The aforementioned groups have also issued warnings to their affiliates that they must request approval prior to deploying ransomware across a victim environment. These new guidelines are a response to fallout from the Colonial Pipeline incident — likely caused by an unseasoned *DarkSide* RaaS affiliate — who likely failed to conduct proper due diligence on Colonial Pipeline before infecting them. While the attack was certainly deliberate, the significant social and economic consequences were either unconsidered or underestimated. This attack was likely not meant to intentionally disrupt gasoline supply to a wide swath of the U.S. East Coast: Colonial Pipeline stated that it "proactively took certain systems offline to contain the threat, which temporarily halted all pipeline operations."

While the operators of *Babuk Locker* have been defiant in the wake of the Colonial Pipeline ransomware incident, other actors (such as WIZARD SPIDER) have not publicly responded to the attention on the ransomware marketplace. These adversaries already operate a private operation with only trusted partners and affiliates, and it is unlikely such groups will publicly respond at all. Most public RaaS vendors will likely retreat for a short- to medium-timeframe and will continue to operate in a more closed and private fashion — a choice already demonstrated by PINCHY SPIDER. While CARBON SPIDER allegedly closed their *DarkSide* RaaS, the adversary is successful, sophisticated, and resourceful, and has not ceased all activity. CARBON SPIDER, and possibly other RaaS vendors, will likely take time to reevaluate their operations and return to eCrime activity — albeit not necessarily involving ransomware — under a new name or brand.

The recent developments surrounding the Colonial Pipeline incident and subsequent reactions from ransomware operators showcase the importance of maintaining situational awareness of quickly evolving threats. This is facilitated by monitoring the shifting dynamics in underground criminal communities but also by understanding the context and impact these activities have on the overall ecosystem. Proactive measures (such as active monitoring) are critical to staying ahead of the adversary to protect your organization.

Additional Resources

- *Read more about CARBON SPIDER’s tactics and DarkSide ransomware in this blog: Hypervisor Jackpotting: CARBON SPIDER and SPRITE SPIDER Target ESXi Servers With Ransomware to Maximize Impact.*
- *Download the CrowdStrike 2021 Global Threat Report for more information about big game hunting adversaries tracked by CrowdStrike Intelligence in 2020.*
- *To learn more about how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Premium Threat Intelligence page.*
- *See how the powerful, cloud-native CrowdStrike Falcon® platform protects customers from DarkSide ransomware in this blog: DarkSide Goes Dark: How CrowdStrike Falcon Customers Were Protected.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today’s most sophisticated threats.*