

A Closer Look at the DarkSide Ransomware Gang

krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/

The **FBI confirmed** this week that a relatively new ransomware group known as **DarkSide** is responsible for an attack that caused **Colonial Pipeline to shut down 5,550 miles of pipe**, stranding countless barrels of gasoline, diesel and jet fuel on the Gulf Coast. Here's a closer look at the DarkSide cybercrime gang, as seen through their negotiations with a recent U.S. victim that earns \$15 billion in annual revenue.



Colonial Pipeline has shut down 5,500 miles of fuel pipe in response to a ransomware incident.

Image: colpipe.com

New York City-based cyber intelligence firm Flashpoint said its analysts assess with a moderate-strong degree of confidence that the attack was not intended to damage national infrastructure and was simply associated with a target which had the finances to support a large payment.

“This would be consistent with DarkSide’s earlier activities, which included several ‘big game hunting’ attacks, whereby attackers target an organization that likely possesses the financial means to pay the ransom demanded by the attackers,” Flashpoint observed.

In response to public attention to the Colonial Pipeline attack, the DarkSide group sought to play down fears about widespread infrastructure attacks going forward.

“We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other our motives [sic],” reads an update to the DarkSide Leaks blog. “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.”

First surfacing on Russian language hacking forums in August 2020, DarkSide is a ransomware-as-a-service platform that vetted cybercriminals can use to infect companies with ransomware and carry out negotiations and payments with victims. DarkSide says it targets only big companies, and forbids affiliates from dropping ransomware on organizations in several industries, including healthcare, funeral services, education, public sector and non-profits.

Like other ransomware platforms, DarkSide adheres to the current badguy best practice of double extortion, which involves demanding separate sums for both a digital key needed to unlock any files and servers, and a separate ransom in exchange for a promise to destroy any data stolen from the victim.

At its launch, DarkSide sought to woo affiliates from competing ransomware programs by advertising a victim data leak site that gets “stable visits and media coverage,” as well as the ability to publish victim data by stages. Under the “Why choose us?” heading of the ransomware program thread, the admin answers:

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled.**
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

An advertisement for the DarkSide ransomware group.

“High trust level of our targets. They pay us and know that they’re going to receive decryption tools. They also know that we download data. A lot of data. That’s why the percent of our victims who pay the ransom is so high and it takes so little time to negotiate.”

In late March, DarkSide introduced a “call service” innovation that was integrated into the affiliate’s management panel, which enabled the affiliates to arrange calls pressuring victims into paying ransoms directly from the management panel.

In mid-April the ransomware program announced new capability for affiliates to launch distributed denial-of-service (DDoS) attacks against targets whenever added pressure is needed during ransom negotiations.

DarkSide also has advertised a willingness to sell information about upcoming victims before their stolen information is published on the DarkSide victim shaming blog, so that enterprising investment scammers can short the company’s stock in advance of the news.

“Now our team and partners encrypt many companies that are trading on NASDAQ and other stock exchanges,” DarkSide explains. “If the company refuses to pay, we are ready to provide information before the publication, so that it would be possible to earn in the reduction price of shares. Write to us in ‘Contact Us’ and we will provide you with detailed information.”

DarkSide also started recruiting new affiliates again last month — mainly seeking network penetration testers who can help turn a single compromised computer into a full-on data breach and ransomware incident.

Now, let's talk about important stuff. We have grown significantly in terms of the client base and in comparison to other projects (judging by the analysis of publicly available information), so we are ready to grow our team and a number of our affiliates in two fields:

Network penetration testing.

We're looking for one person or a team. We'll adapt you to the work environment and provide work. High profit cuts, ability to target networks that you can't handle on your own. New experience and stable income.

Providing networks.

You'll work with us and with our affiliates. Before providing networks, we'll give you the affiliate payout statistics (upon agreement). When you use our product and the ransom is paid, we guarantee fair distribution of the funds. A panel for monitoring results for your target. We only accept networks where you intend to run our payload.

Regarding these two aforementioned fields, you'll need to PM us with the message title "Pentesting" or "Networks" and go through an interview.

Portions of a DarkSide recruitment message, translated from Russian. Image: Intel 471.

“We have grown significantly in terms of the client base and in comparison to other projects (judging by the analysis of publicly available information), so we are ready to grow our team and a number of our affiliates in two fields,” DarkSide explained. The advertisement continued:

“Network penetration testing. We're looking for one person or a team. We'll adapt you to the work environment and provide work. High profit cuts, ability to target networks that you can't handle on your own. New experience and stable income. When you use our product and the ransom is paid, we guarantee fair distribution of the funds. A panel for monitoring results for your target. We only accept networks where you intend to run our payload.”

DarkSide has shown itself to be fairly ruthless with victim companies that have deep pockets, but they can be reasoned with. Cybersecurity intelligence firm Intel 471 observed a negotiation between the DarkSide crew and a \$15 billion U.S. victim company that was hit with a \$30 million ransom demand in January 2021, and in this incident the victim's efforts at negotiating a lower payment ultimately reduce the ransom demand by almost two-thirds.

Your network has been locked!

You need pay **\$ 30,000,000** now, or **\$ 60,000,000**
after doubled.
1208.13 BTC (+20%) or 233863.42 XMR 2416.26 BTC (+20%) or 467726.85 XMR

After payment we will provide you universal decryptor for all network.

Don't worry, we are good decryption specialists.

Time left

04:44:54

Time ends on 27 Jan 2021, 23:06

* The price will be doubled if you do not pay.

The DarkSide ransomware note.

The first exchange between DarkSide and the victim involved the usual back-and-forth establishing of trust, wherein the victim asks for assurances that stolen data will be deleted after payment.

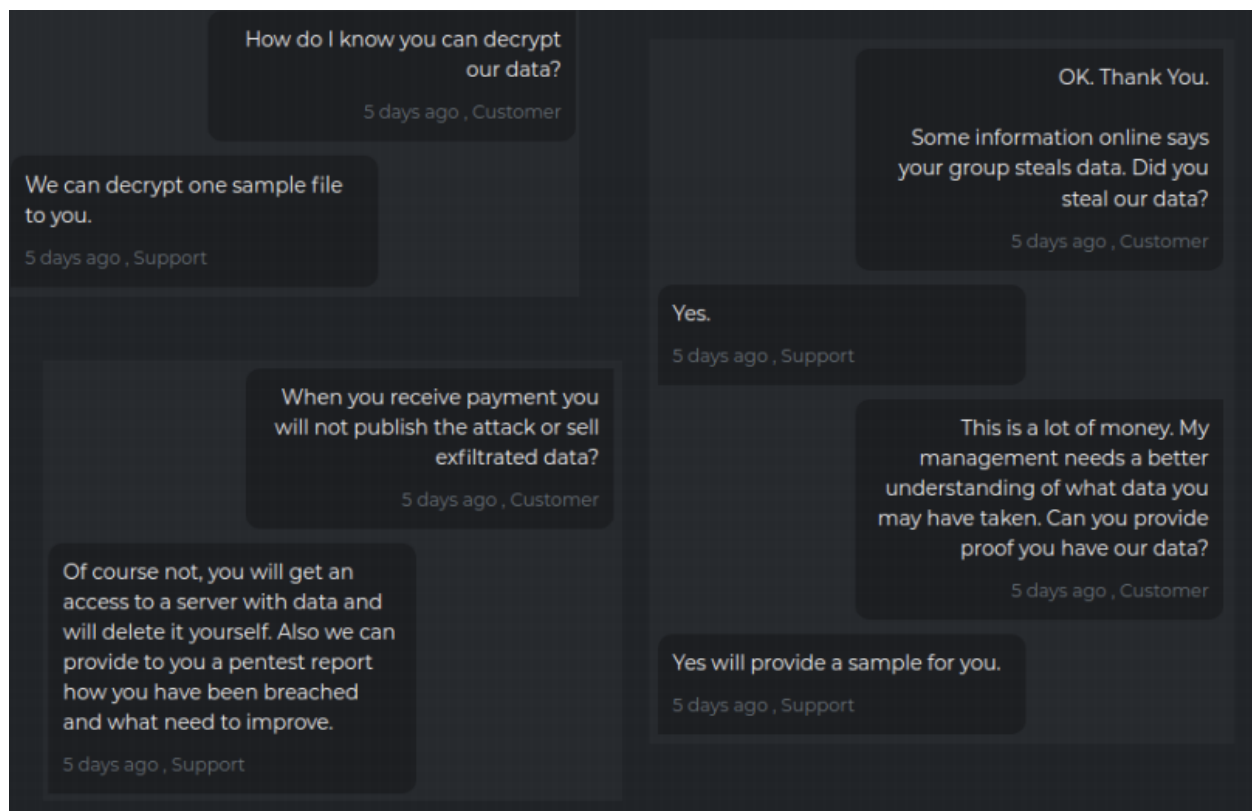
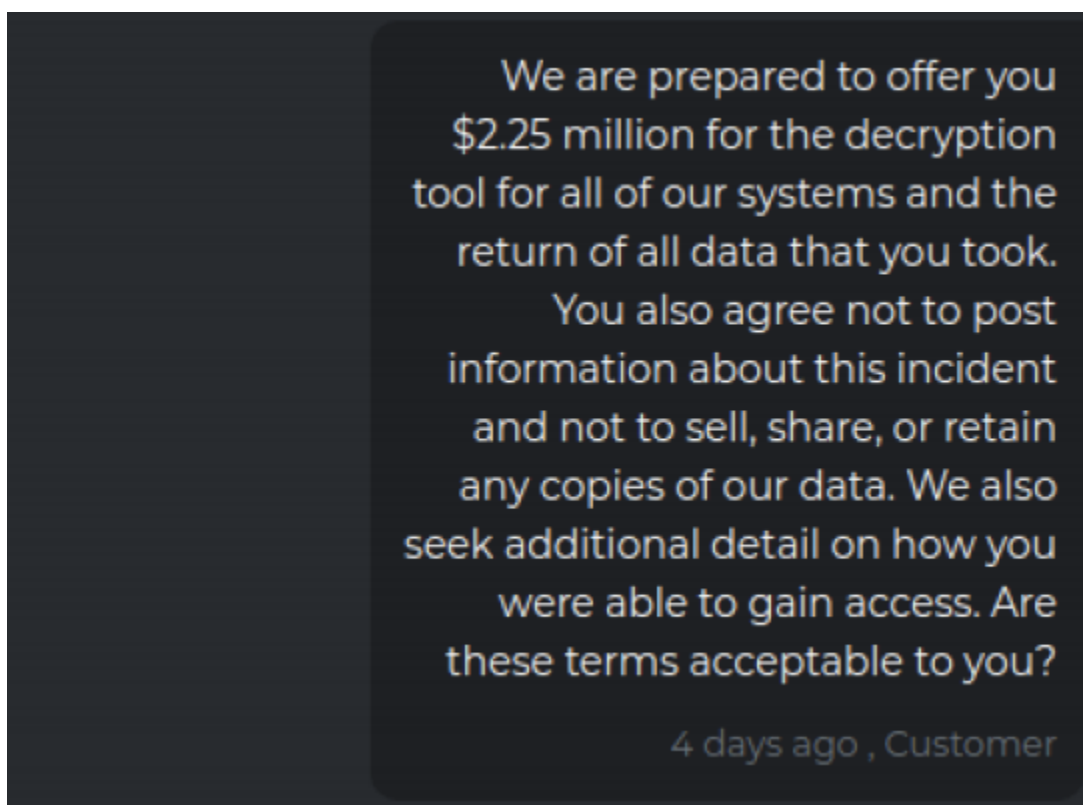
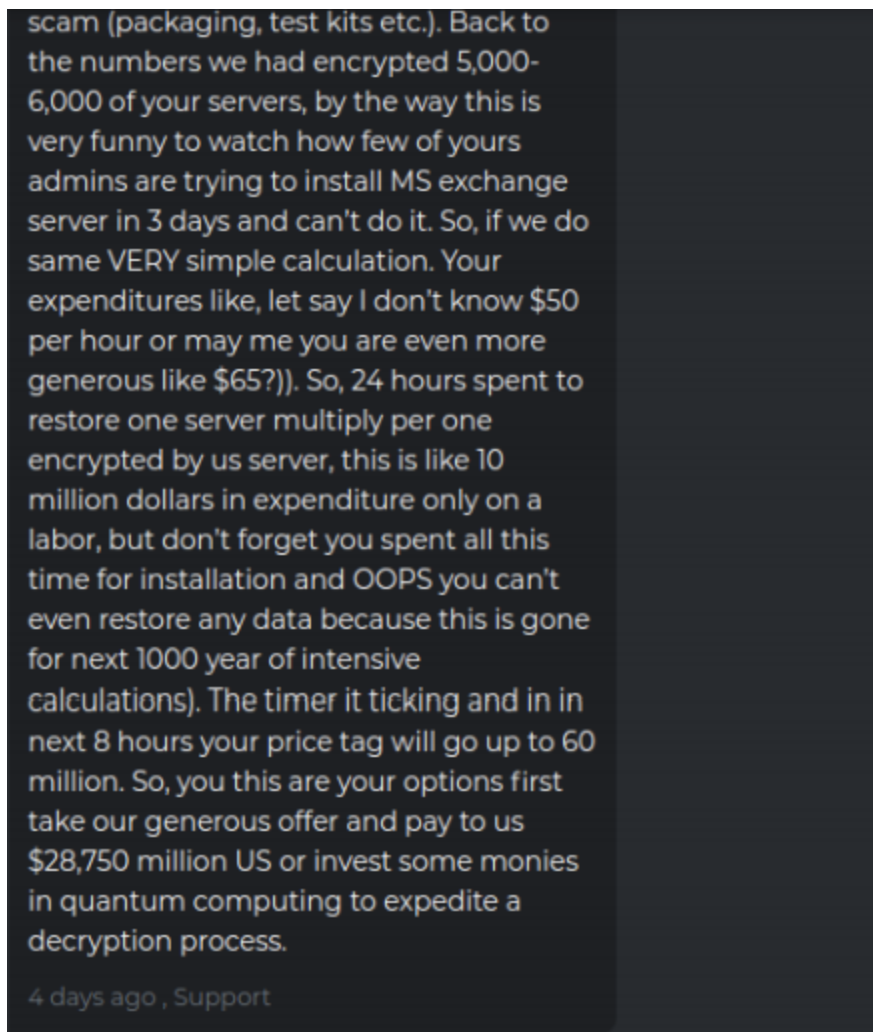


Image: Intel 471.

When the victim counter-offered to pay just \$2.25 million, DarkSide responded with a lengthy, derisive reply, ultimately agreeing to lower the ransom demand to \$28.7 million.



“The timer it [sic] ticking and in in next 8 hours your price tag will go up to \$60 million,” the crooks replied. “So, you this are your options first take our generous offer and pay to us \$28,750 million US or invest some monies in quantum computing to expedite a decryption process.”



scam (packaging, test kits etc.). Back to the numbers we had encrypted 5,000-6,000 of your servers, by the way this is very funny to watch how few of yours admins are trying to install MS exchange server in 3 days and can't do it. So, if we do same VERY simple calculation. Your expenditures like, let say I don't know \$50 per hour or may me you are even more generous like \$65?)). So, 24 hours spent to restore one server multiply per one encrypted by us server, this is like 10 million dollars in expenditure only on a labor, but don't forget you spent all this time for installation and OOPS you can't even restore any data because this is gone for next 1000 year of intensive calculations). The timer it ticking and in in next 8 hours your price tag will go up to 60 million. So, you this are your options first take our generous offer and pay to us \$28,750 million US or invest some monies in quantum computing to expedite a decryption process.

4 days ago , Support

Image: Intel 471.

The victim complains that negotiations haven't moved the price much, but DarkSide countered that the company can easily afford the payout. "I don't think so," they wrote. "You aren't poor and aren't children if you f*cked up you have to meet the consequences."

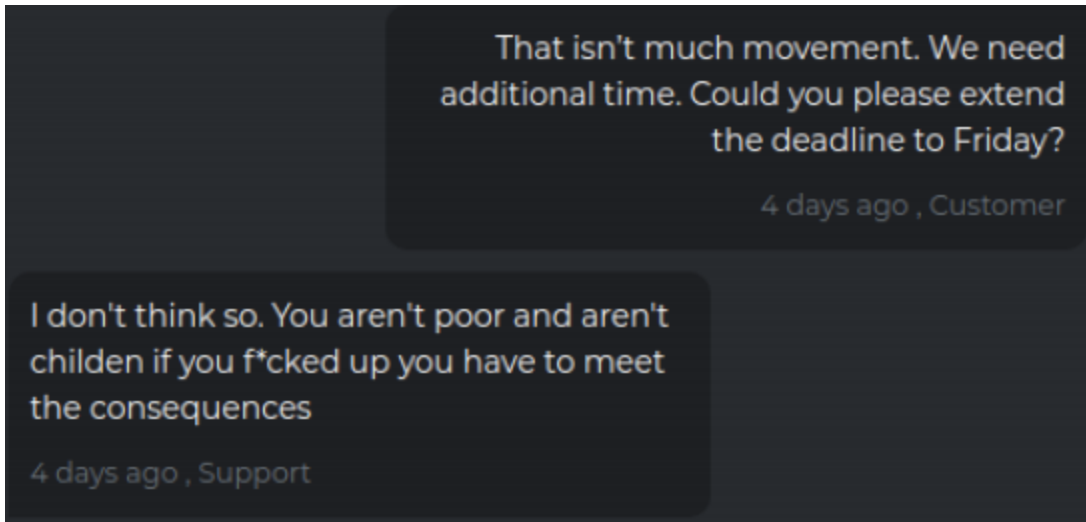


Image: Intel 471.

The victim firm replies a day later saying they've gotten authority to pay \$4.75 million, and their tormentors agree to lower the demand significantly to \$12 million.

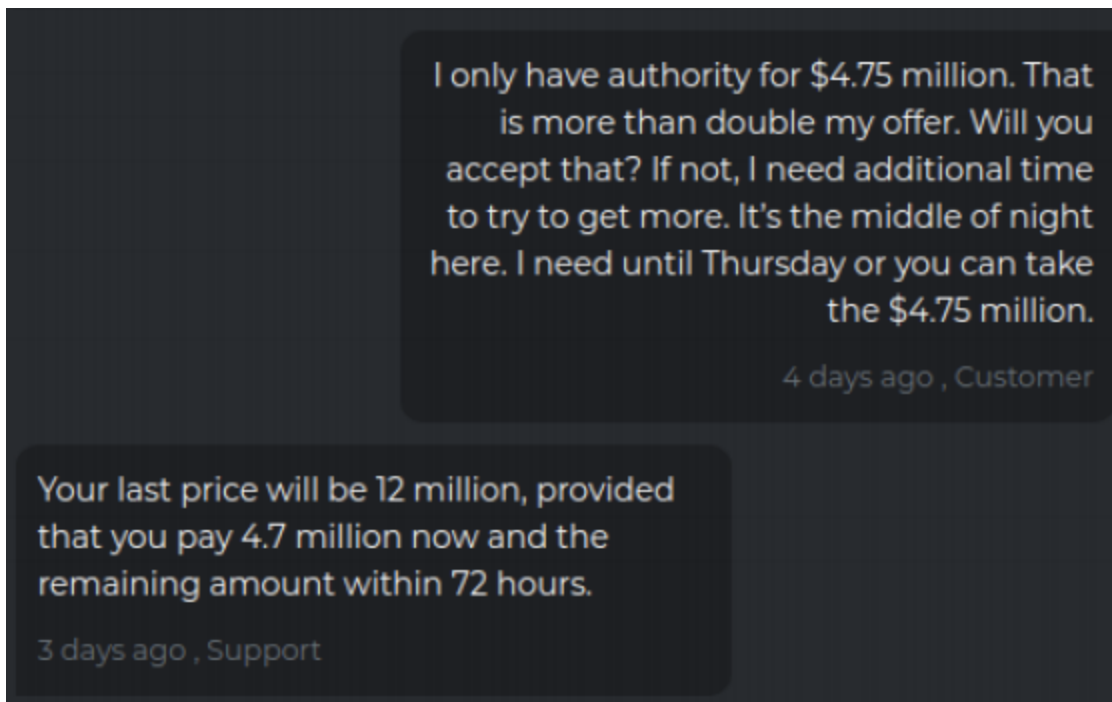


Image: Intel 471.

The victim replies that this is still a huge amount, and it tries to secure additional assurances from the ransomware group if it agrees to pay the \$12 million, such as an agreement not to target the company ever again, or give anyone access to its stolen data. The victim also tried to get the attackers to hand over a decryption key before paying the full ransom demand.

That is still a lot of money. To resolve this quickly, we will agree to pay on your terms, as long as you turn over the decryption tools with our initial payment of \$4.7 million and agree to immediately disconnect from our systems. Upon payment of the remaining \$7.3 million within 72 hours, you will –

1. provide us access to all of the data you took.
2. agree not to post information about this incident.
3. agree not to sell, share, or retain any copies of our data.
4. provide detail on how you were able to gain access.
5. agree to never target our company again.
6. not give access to or assist anyone else in gaining access.

Are these terms acceptable to you?

3 days ago , Customer

Image: Intel 471.

The crime gang responded that its own rules prohibit it from giving away a decryption key before full payment is made, but they agree to the rest of the terms.

We cannot agree to comply with ALL your terms because issuing a decryption tool before full payment violates the Darkside rules, and we cannot change these rules. Darkside values its reputation and you can easily find information that all the conditions have always been met. At this point, we can only promise that we will not launch any new attacks. After full payment, we guarantee: 1. You will get the tool and be able to fully decrypt the encrypted data. 2. We will completely leave your network and it will never be our target again. 3. You will get access to the data, delete it yourself. They will never be published or resold, as it doesn't make sense given the amount of the buyout. 4. You will receive a full report on our actions, how we got into the network and how the attack was carried out. And the report will also contain tips for improving security, and protecting against the penetration of other hackers.

3 days ago , Support

Image: Intel 471.

The victim firm agrees to pay an \$11 million ransom, and their extortionists concur and promise not to attack or help anyone else attack the company's network going forward.

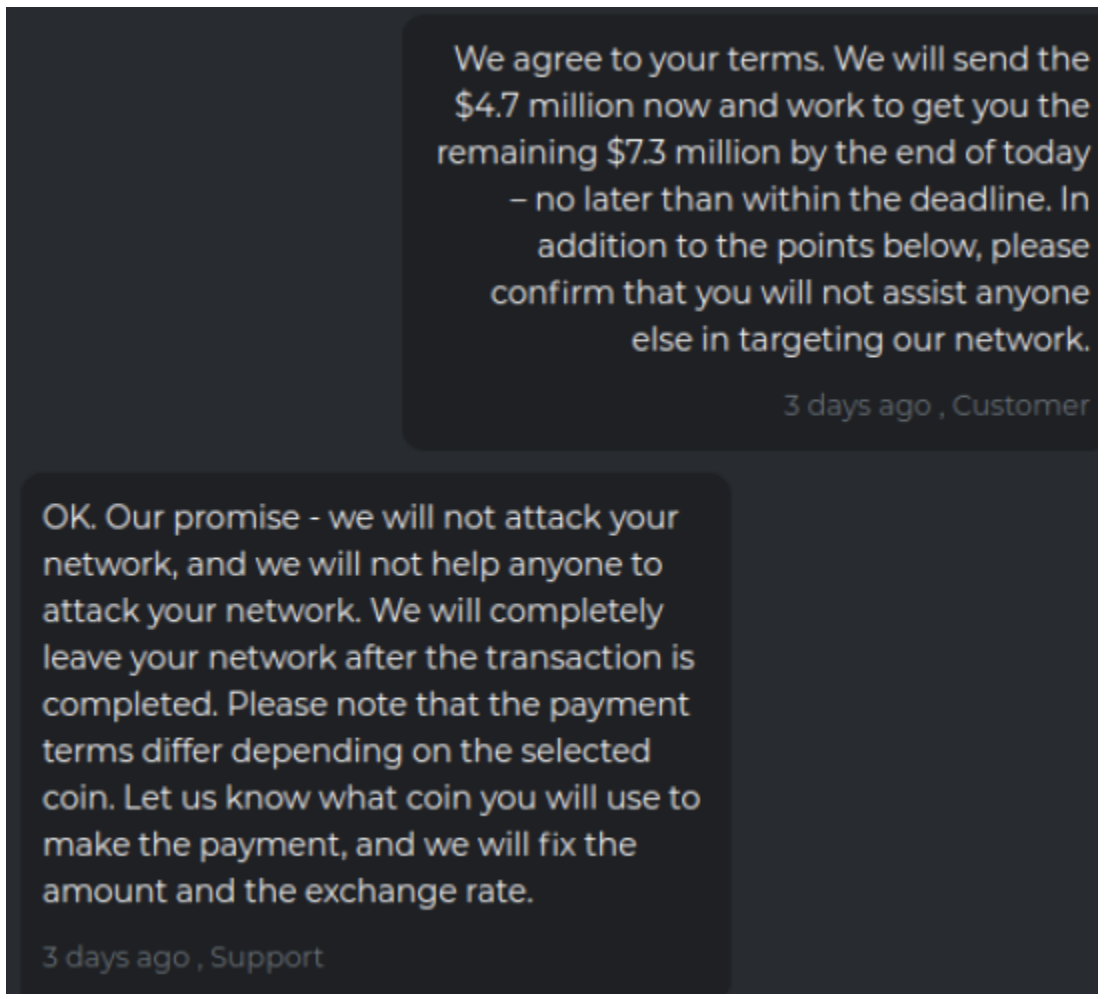


Image: Intel 471

Flashpoint assesses that at least some of the criminals behind DarkSide hail from another ransomware outfit called “REvil,” a.k.a. “Sodinokibi” (although Flashpoint rates this finding at only “moderate” confidence). REvil is widely considered to be the newer name for GandCrab, a ransomware-as-a-service offering that closed up shop in 2019 after bragging that it had extorted more than \$2 billion.

Experts say ransomware attacks will continue to grow in sophistication, frequency and cost unless something is done to disrupt the ability of crooks to get paid for such crimes. According to a report late last year from **Coveware**, the average ransomware payment in the third quarter of 2020 was \$233,817, up 31 percent from the second quarter of last year. Security firm Emsisoft found that almost 2,400 U.S.-based governments, healthcare facilities and schools were victims of ransomware in 2020.

Last month, a group of tech industry heavyweights lent their imprimatur to a task force that delivered an 81-page report to the Biden administration on ways to stymie the ransomware industry. Among many other recommendations, the report urged the White House to make finding, frustrating and apprehending ransomware crooks a priority within the U.S. intelligence community, and to designate the current scourge of digital extortion as a national security threat.

Further reading: [Intel 471's take on the Colonial Pipeline attack.](#)