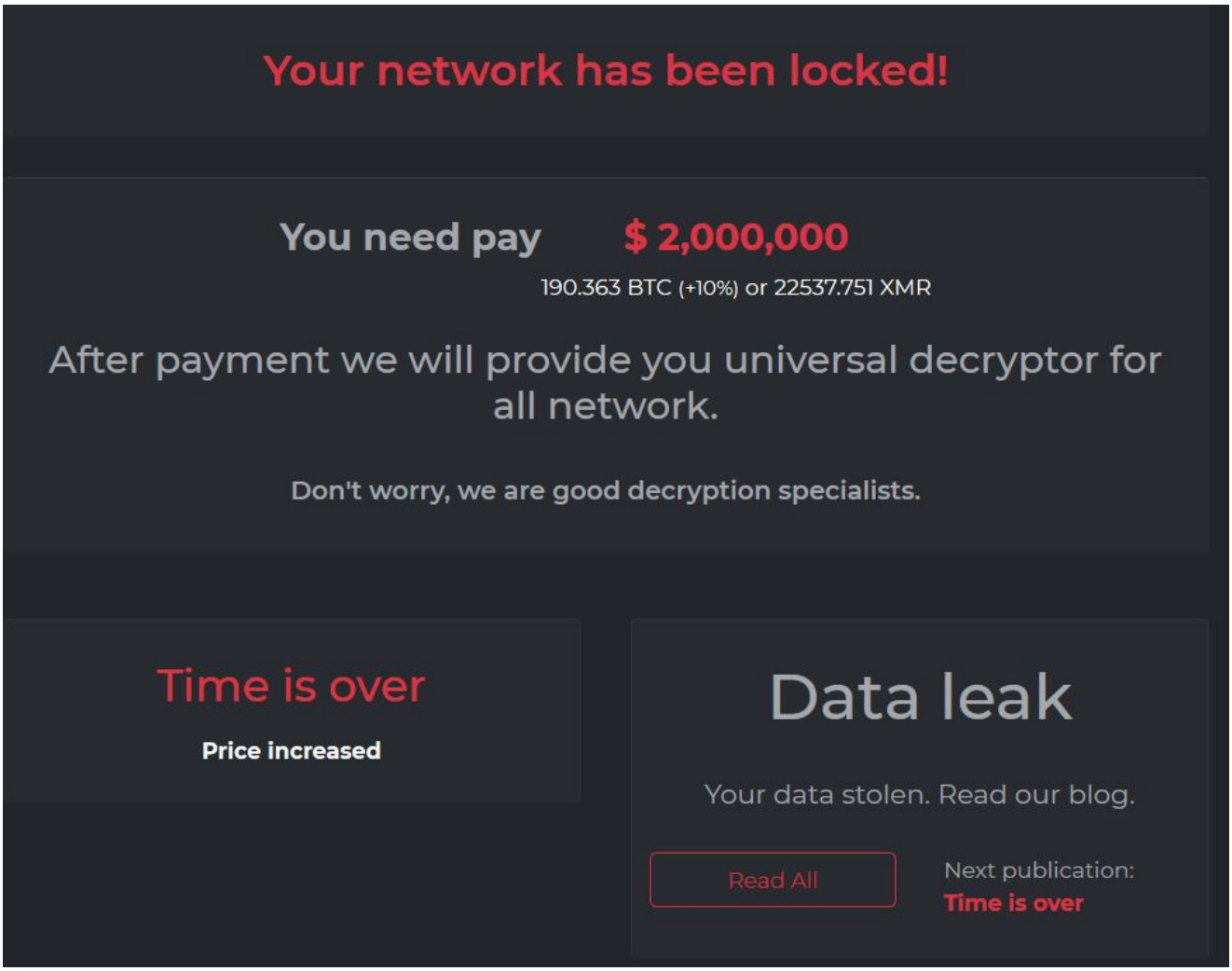
A chat with DarkSide

databreaches.net/a-chat-with-darkside/

> *If you would meet us on the street – you would never realize that we are cyberpests, because we are the same normal people like everyone else. Many have families and children, the only thing that these circumstances in which we found themselves in our country are. We have no hatred and desire to cause damage, we perceive our business as any other, the ultimate goal of which is profit.*
>
> *— DarkSide*



One of Darkside's earlier notices.

In a recent article on BankInfoSecurity, Mathew J. Schwartz reports that ransomware threat actors have been on somewhat of a "charm offensive" since last year, giving interviews to media. Because this blogger has absolutely no hacking knowledge or skills, I would never try to do an actual technical interview with any threat actor. In fact, given my professional background, I have always been more interested in why and how threat actors make the decisions they make — and how some seem to have absolutely no scruples or ethics about

attacking some victims while others appear to develop some sort of ethics code. With those interests in mind, DataBreaches.net recently interviewed DarkSide operators about their approach to their ransomware operations and changes since they first emerged as DarkSide.

In August, 2020, when the ransomware group known as DarkSide introduced themselves via a press release on their web site, they made a point of immediately claiming that although their product might be new, they were not new kids on the block:

> 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.

Their announcement also stated what kinds of entities they did not attack, and that they only attacked companies that could pay the demanded amount — an amount they claim they determine by researching the companies they attack.

Their launch announcement was met with skepticism by some and outright scorn or ridicule by others, and Brian Barrett's description of DarkSide as having a "veneer of professionalism" was somewhat understandable. But in some respects, DarkSide has proved Barrett wrong. They actually are more professional in their conduct than some other ransomware groups, even though their conduct is certainly illegal and cruel to victims. And they have not only kept their word about who they will not attack, but they actually expanded the exclusions.

So seven months after they announced their launch and then put their heads down and got to work, what, if anything, has changed for them?

"Big-Game Hunters"

Like other groups such as REvil, Ryuk, and DoppelPaymer, DarkSide is considered a "big-game hunter," targeting larger corporations that can afford to pay higher ransoms. DarkSide's dedicated leak site currently lists **Guess,** the well-known American clothing and fashion accessories retailer. Guess's revenue last year was estimated at $2.68 billion. DarkSide claims to have exfiltrated more than 200 GB of data, and posted a number of samples as proof. DataBreaches.net does not know how much ransom DarkSide has demanded for the decryption key, but they publicly advise Guess:

> We recommend using your insurance, which just covers this case. It will bring you four times more than you spend on acquiring such a valuable experience.

That statement is consistent with DarkSide's first press release in which they stated that they were not out to kill companies. It is also consistent with DarkSide's explanation to DataBreaches.net in the interview recently conducted by email. [Because of language

issues, DarkSide would translate my e-mailed questions into Russian, answer me in Russian, and then translate the answers back into English. With only one exception, that seemed to work fairly decently]. One of the exchanges was:

DataBreaches.net (DBN): Do you ever demand more than what their cyberinsurance policy might cover?

DarkSupp: Always before putting the amount of ransom, we study the internal reporting of the company and definitely understand how much they can really pay, all our partners work in the same way and we always remind about it. Basically, we do not require more than the amount of cyber insurance, but we can not always check the actions of our partners.

DBN: Someone suggested that if companies didn't have cyberinsurance, ransomware threat actors would lose interest and just go away. Do you think that's true?

DarkSupp: (no response or comment)

From the files on their site, it would appear that Guess was attacked in February. Unlike some groups that reach out to media quickly to get coverage, DarkSide had not reached out about Guess or other victims. When asked about how long they wait and what steps they take, they answered:

> **DarkSupp: We act in stages and notify the press usually already when exactly sure that the company will not pay. As for [Guess and another company DBN had named] – I think the press will see them.**
>
> *DBN: Do you notify the press to punish the companies for not paying or to try to pressure them more — or for both reasons?*
>
> **DarkSupp: For both reasons.**
>
> *DBN: Do you actually call targets on the phone like some others do? Do you ever contact targets' customers directly like CLOP seems to be doing about the Accellion breach?*
>
> **DarkSupp: Yes, a few weeks ago, we launched a balanced service of the calls to our victims, while we call only our customers, but soon we also want to put pressure on their partners. A few days ago, we launched DDOS of our targets (Layer 5 Layer 7), which significantly increased pressure and has already brought the first results.**

Exclusions

Like some other RaaS groups, DarkSide uses a popular Russian-language forum to advertise or recruit partners and to promote its service and updates to its product. A recent announcement in early March described a number of updates to the features and rates for partners, as well as seeking affiliates. The announcement also repeated the rules about what was not permissible to attack:

> 1. The following areas are prohibited:
> – Medicine (only: hospitals, hospitals, any palliative care organization, nursing homes, companies that develop and participate (largely at the supply chain level) in the distribution of the COVID-19 vaccine).
> – Funeral services (Morgues, crematoria, funeral homes).
> – Education (Universities, schools).
> – Public sector (municipalities, any government bodies).
> – Non-profit organizations (charities, associations).
> 2. Any actions that damage the reputation of the product are prohibited.
> 3. Any work in the CIS (including Georgia, Ukraine) is prohibited.
> 4. It is forbidden to transfer the account to third parties.
> 5. It is forbidden to use other lockers in one project.

The list of excluded entities is what they had established in August, with one difference: funeral services (morgues, crematoria, and funeral homes) were added to the list. When DataBreaches.net asked DarkSupp if they had ever regretted attacking a target, they had replied:

DarkSupp: Yes, for the actions of our partners. After that, a ban on blocking of morgues and crematoriums appeared.

So unlike what we saw with some entities refusing to commit to leaving medical entities alone or reneging on pledges, DarkSide has consistently prohibited attacks on medical entities as defined in their rules. They also have a more extensive exclusion list than any other group. [There will be some who argue, “So what? They are still criminals.” Yes, they are, but DataBreaches.net believes in giving credit where it’s due, and if they stick to leaving medical alone, I give them credit for that.]

That said, and while their intentions may sound noble in excluding medical, DataBreaches.net was surprised to learn that DarkSide doesn’t consider medical targets likely to pay, as indicated in this exchange in the interview:

DBN: You seem to have kept your word about leaving medical entities alone. Will you always leave medical, schools, and non-profits alone, or will that change when the pandemic ends?

DarkSupp: There are several reasons why we do not attack medical institutions: 1. This may lead to aggravation of health problems and the death of people, which is unacceptable for us. In the encryption of medical institutions, they lose the history of

patient diseases, a schedule of operations (including due to the loss of test results, which is now digitized) 2. Such companies on reviews of our colleagues usually do not pay a ransom.

DBN: Are you saying that hospitals usually do NOT pay ransom when they are attacked or are you saying something else?

DarkSupp: Yes, we mean that in addition to negative moral consequences, hospitals also pay money less often than companies.

That statement seems to directly contradict what was reported at the same time last year when we were told that "Hospitals pay 80% to 90% of the time because they simply have no choice." Have they stopped paying as often? Hospitals in Germany, Belgium, and France have been in the news in recent months as victims of ransomware attacks — in at least some cases by DoppelPaymer. But are any paying? And are those who are attacking them making demands that far exceed cyberinsurance? Have the criminals gotten so greedy that more victims are now refusing to pay?

DarkSide did acknowledge that some things may change after the pandemic, but not everything:

DarkSupp: If we talk about medical companies: the ban on their encryption will always be, other spheres may be permissible but with a preliminary change of rules.

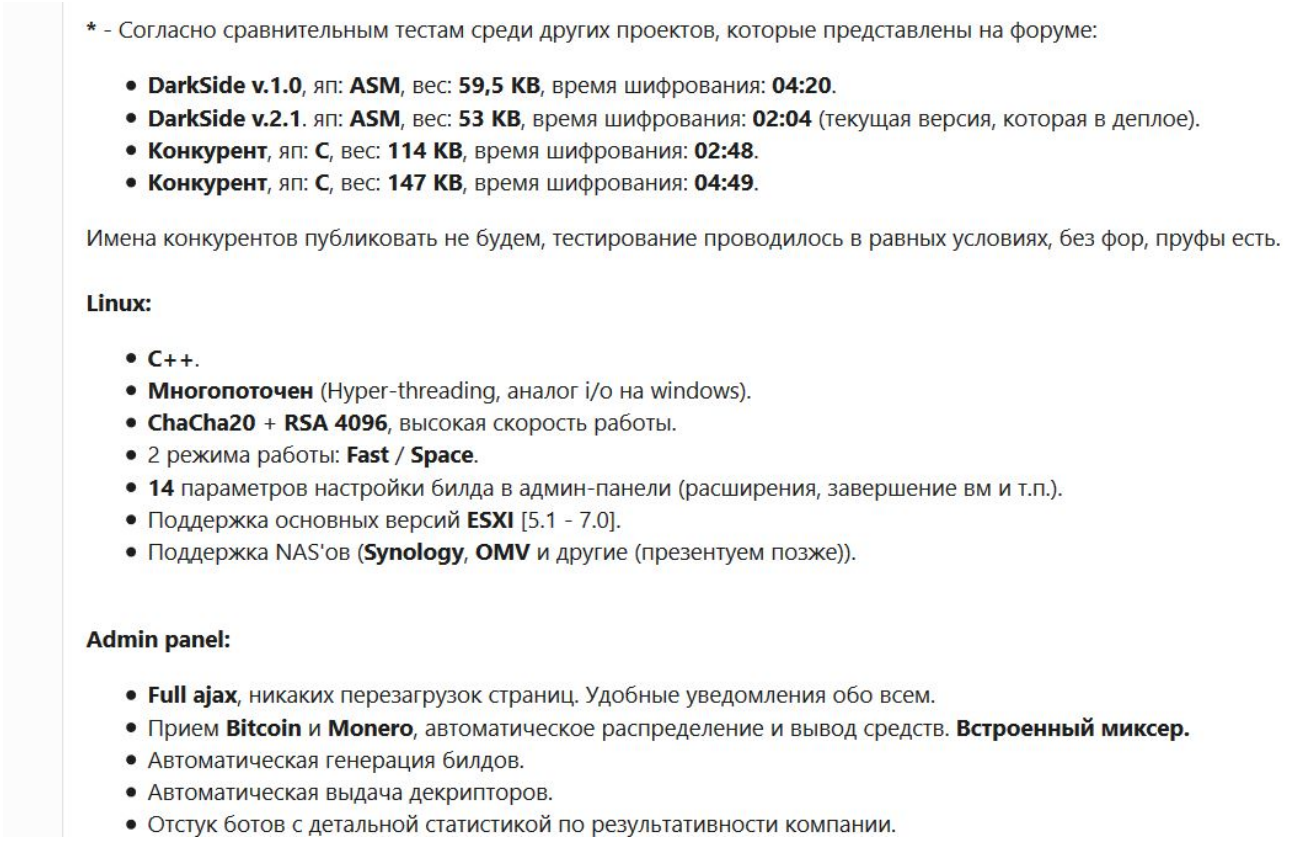
Charitable Donations

In an October press release, DarkSide revealed that they had made donations to some charities. It did not get a positive response from the security community, members of the forum where it was discussed, or the general public. Concerned that entities might reject their donations if they knew the source, DarkSide announced that in the future, they would make their donations anonymously. DataBreaches.net followed up on that by asking them whether they had been making any donations (DBN did not ask them to name any organizations specifically).

> **DarkSupp: At that time, we did not consider it as an advertising move, donations were really shipped to help people. We do not know about the unpleasant consequences that in the end happened with money, but no one returned to us, as the money was sent through a mixer.**
>
> **DarkSupp: Yes, sometimes we sacrifice money for enlightenment with various charitable funds (not everyone who we wanted to give money to accept Bitcoin), but mostly we are anonymously supporting several open-source projects on anonymity on the Internet.**

Unurprisingly, perhaps, Unknown of REvil also specifically mentioned supporting anonymity projects when interviewed by Dmitry Smilyanets of Recorded Future last month.

Indeed, there were many respects in which the two groups seemed comparable in their statements about their operations and approach to ransomware-as-a-service. They both recognize that ransomware groups are in competition to give affiliates what they want and that affiliates may jump ship to get better features or percentages of take. At the beginning of March, DarkSide published a detailed update and solicitation for partners. In it, they promote themselves as serious competitors whose features are better than what others have to offer potential affiliates.



* - Согласно сравнительным тестам среди других проектов, которые представлены на форуме:

- **DarkSide v.1.0**, яп: **ASM**, вес: **59,5 KB**, время шифрования: **04:20**.
- **DarkSide v.2.1**. яп: **ASM**, вес: **53 KB**, время шифрования: **02:04** (текущая версия, которая в деплое).
- **Конкурент**, яп: **C**, вес: **114 KB**, время шифрования: **02:48**.
- **Конкурент**, яп: **C**, вес: **147 KB**, время шифрования: **04:49**.

Имена конкурентов публиковать не будем, тестирование проводилось в равных условиях, без фор, пруфы есть.

Linux:

- **C++**.
- **Многопоточен** (Hyper-threading, аналог i/o на windows).
- **ChaCha20** + **RSA 4096**, высокая скорость работы.
- 2 режима работы: **Fast** / **Space**.
- **14** параметров настройки билда в админ-панели (расширения, завершение вм и т.п.).
- Поддержка основных версий **ESXI** [5.1 - 7.0].
- Поддержка NAS'ов (**Synology**, **OMV** и другие (презентуем позже)).

Admin panel:

- **Full ajax**, никаких перезагрузок страниц. Удобные уведомления обо всем.
- Прием **Bitcoin** и **Monero**, автоматическое распределение и вывод средств. **Встроенный миксер.**
- Автоматическая генерация билдов.
- Автоматическая выдача декрипторов.
- Отстук ботов с детальной статистикой по результативности компании.

In an announcement on a Russian-language forum, DarkSide advertises the competitive features of DarkSide v. 2.1.

In our interview, they elaborated on how they see their position in the community:

> **DarkSupp: Objectively speaking, we have only a few competitors, the rest of the partnership programs at least do not provide the level of service that we have. After we started to develop and take the audience from them – they began to more actively develop their projects and create new services (it can easily notice the nomination of Russian hacker forums). So it can be said that our project globally affected the market for the development of cryptolocrineers.**

REvil would probably make the same claim. And both groups have put up money on the forum to cover any incidents or problems that might develop (DarkSide put up 23 btc in November for such contingencies, while REvil recently explained that they removed their

deposit because of the exchange rate).

Their commitment became important after BitDefender released a free decryptor for victims of DarkSide ransomware. DarkSide's response was immediate and public: they acknowledged what had happened and how (as translated below):

> Bitdefender has released a utility that can decrypt some of our Windows lockers. Linux is not decrypted. This is not connected with breaking our encryption or another bug in the locker (RSA + Salsa20), but with the generation of keys. Due to the way the generator works under Linux, some private keys of the targets could be generated the same, so BitDefender created its own decryptor based on one public key (previously purchased). We estimate that up to 40% of private keys are affected.
>
> At the moment, this problem has been resolved, no new targets will be decrypted, there have been no bugs in the locker itself, and there never will be.

DarkSide offered monetary compensation to any affiliates who had lost money because of the error, and then offered new affiliates a better deal for the next 30 days with higher shares. They also thanked BitDefender publicly for helping them improve their product.

Because the decryptor was released right before the holidays, fewer than 5 victims were reportedly able to benefit from it, and DarkSide claimed that not only had the incident not cost them any affiliates, but it had actually helped them attract even more affiliates within 48 hours because they offered a better deal to new affiliates while compensating any existing ones who had suffered any losses. But they also told DBN:

> **If we talk about Bitdefender, we can say that they have made a big mistake by publishing the decryption key in public. In their place, we would distribute it among the recovery companies, and that would have caused more damage later for us.**

At the present time, DarkSide claims to work with more than 20 affiliates or partners. That is significantly less than what Unkn of REvil claimed Sodinokibi had as a maximum number of affiliates at any one time, and DarkSide is generally not listed among the currently most profitable ransomware groups that seem to include Ryuk, REvil, and DoppelPaymer. But the competition is certainly evident as we have seen groups come and go in the past seven months and some grouping into what has been labeled by others as a cartel. DarkSide has not expressed any public interest in joining any cartel, and made no mention of anything like that in our interview.

But will DarkSide ever make enough money to quit? I put the question to them.

DBN: Unknown from REvil had said he can never have too much money because he grew up poor. How about you? Do you have some monetary goal in mind, and if you reach it, you will retire, or will you just keep going to make even more money?

DarkSupp: We have a definite goal after which we will retire.

It seems that they haven’t reached it yet.

Related Posts:

- Secrets and Lies: The Games Ransomware Attackers Play
- Fake DarkSide gang targets energy, food industry in…
- "We are apolitical" -- DarkSide threat actors
- DarkSide ransomware decryptor recovers victims' files for…
- DarkSide ransomware is creating a secure data leak service…