BlackBasta Leaks: Lessons from the Ascension Health attack

blog.bushidotoken.net/2025/02/blackbasta-leaks-lessons-from-ascension.html

The BlackBasta ransomware group's leaked chat logs have proven to already be another unique and fascinating opportunity for researchers to better understand the internal operations of a Russia-based organised cybercrime enterprise. These leaks followed a major leak of Conti chat logs in 2022, which also proved to be a treasure trove of intelligence on the cybercrime enterprise. The BlackBasta gang consists of former Conti ransomware members and it should come as no surprise that their operations are similar in nature and structure.

Ransomware researchers have several valuable resources to conduct investigations with nowadays. This includes ransomware.live, which contains several resources including ransomch.at, a collection of negotiation chats between ransomware gangs and their victims, as well as the ransomware tool matrix and ransomware vulnerability matrix. These resources allow to deeply understand the capabilities and motivations of these ransomware gangs. However, leaked chat logs are the final missing piece of the puzzle and offer a deeper understanding from the cybercriminal's very own perspective and organisational structure.

Active since April 2022, BlackBasta is one of the top-tier ransomware gangs and one of the largest cybercrime enterprises in the world. According to the US Cybersecurity Infrastructure and Security Agency (CISA), BlackBasta impacted up to 500 different businesses and critical infrastructure in North America, Europe, and Australia as of May 2024.

The importance of the Ascension Health incident

This blog shall dive deep into the Ascension Health attack by BlackBasta. It is a step-by-step extraction of the conversation between the BlackBasta members while they decide how to handle the attack.

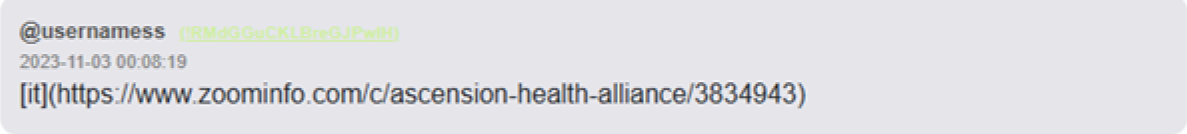
The new insights around how BlackBasta and other ransomware gangs perceive being involved with incidents at healthcare sector victim should prove useful for incident responders, law enforcement, and governments that have to resolve these types of attacks on the healthcare sector on an alarmingly regularly basis.

Background

On 9 May 2024, mainstream news organisations in the US reported about a cyberattack and significant disruption of services of Ascension Health, one of the largest healthcare providers in the country. On 11 May 2024, BleepingComputer reported that BlackBasta was to blame for the attack on Ascension Health and that ambulances had been disrupted and patients were being redirected to other hospitals.

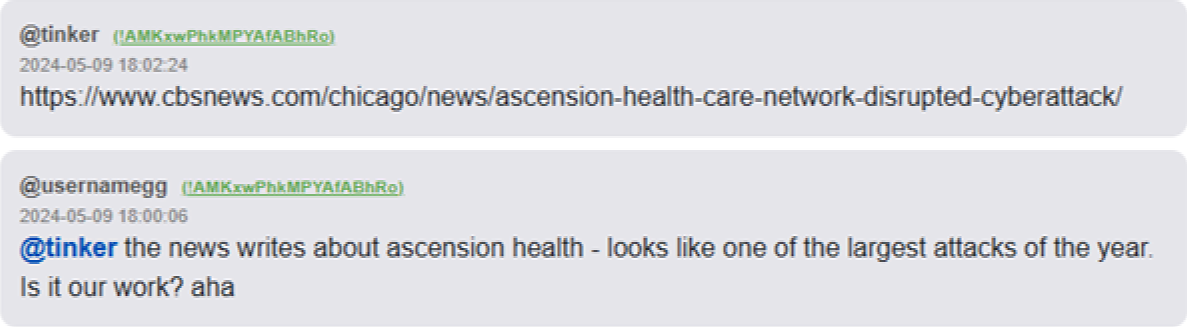
How the Incident Began

The BlackBasta attack on Ascension Health began many months before the ransomware was deployed on their network. Reconnaissance of Ascension Health by members of BlackBasta began around 3 November 2023. They shared 14 email addresses of Ascension Health employees, which we can only assume were used for phishing or password guessing. Ransomware gangs often used Zoominfo to profile their targets to determine whether it is worth it for them to attack and get a ransom from them.



@usernamess (!RMdGGuCKLBreGJPwlH)
2023-11-03 00:08:19
[it](https://www.zoominfo.com/c/ascension-health-alliance/3834943)

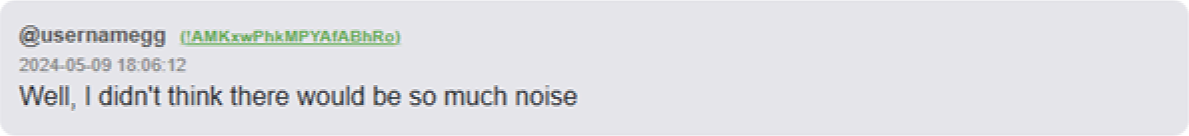
The ransomware gang themselves wrote in their Matrix chat that CBS News had written about a cyberattack on Ascension Health on 9 May 2024 and exclaimed that “it looks like one of the largest attacks of the year.”



@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:02:24
https://www.cbsnews.com/chicago/news/ascension-health-care-network-disrupted-cyberattack/

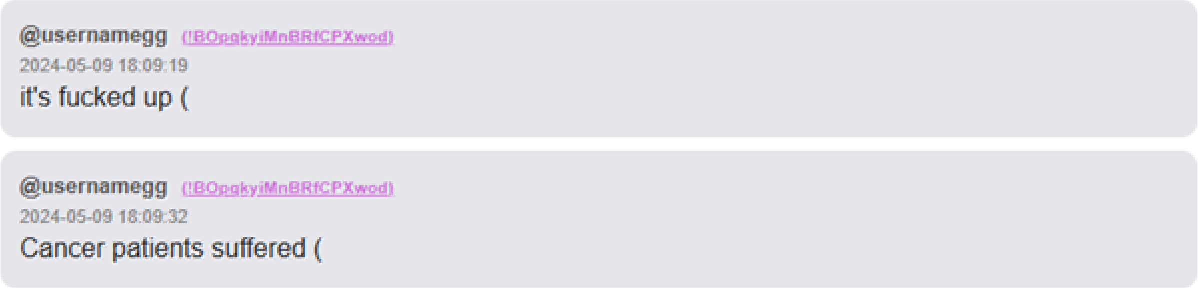
@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:00:06
@tinker the news writes about ascension health - looks like one of the largest attacks of the year.
Is it our work? aha

Another BlackBasta member “gg” confirmed in the chat that it was them and appeared to be surprised that the news was writing about it.



@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:06:12
Well, I didn't think there would be so much noise

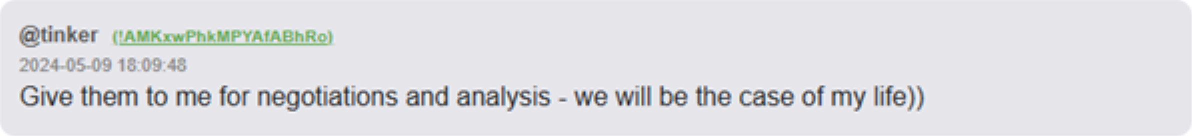
Later, “gg” appeared to feel bad about the attack and concerned that cancer patients were suffering. However, at this stage it is hard to tell if they are serious or being sarcastic.



@usernamegg (!BOpgkyiMnBRfCPXwod)
2024-05-09 18:09:19
it's fucked up (

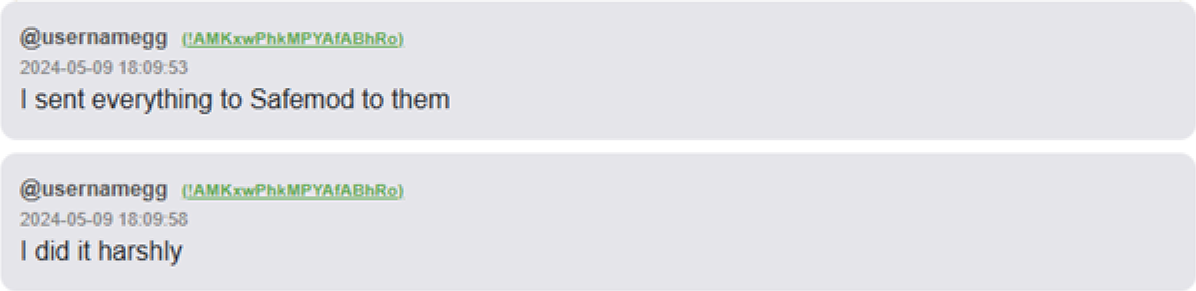
@usernamegg (!BOpgkyiMnBRfCPXwod)
2024-05-09 18:09:32
Cancer patients suffered (

One member of BlackBasta who used the moniker “tinker” then stated that he wanted to be the negotiator for the BlackBasta team and began to strategize how to extract a ransom payment.



@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:09:48
Give them to me for negotiations and analysis - we will be the case of my life))

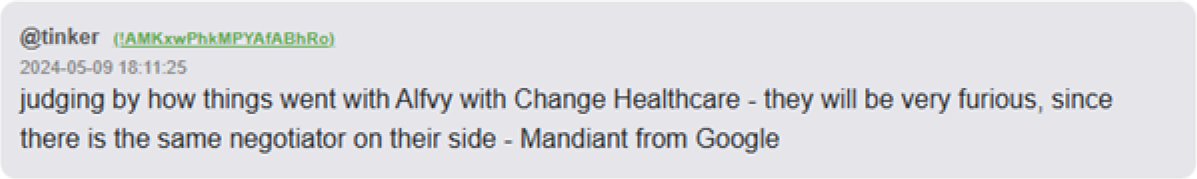
“gg” says they encrypted Ascension Health’s network using the Windows Safe Mode Boot technique, which is a function that BlackBasta is well-known to do.



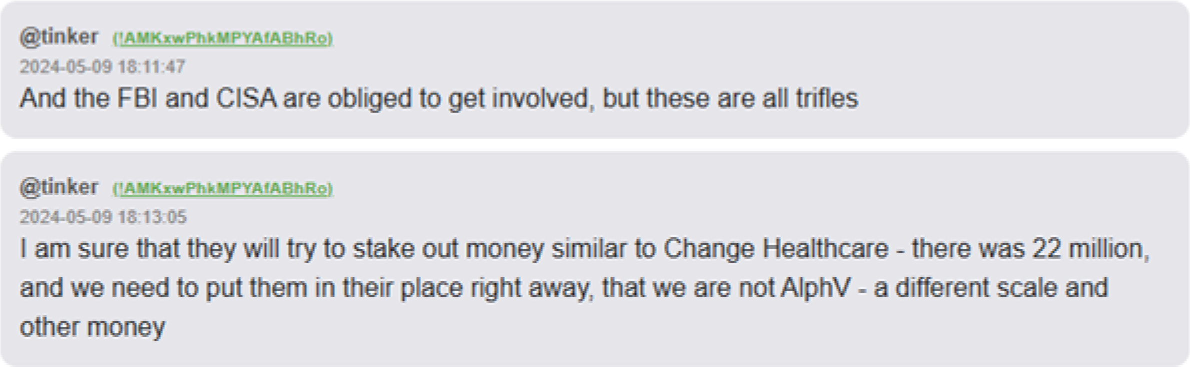
@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:09:53
I sent everything to Safemod to them

@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:09:58
I did it harshly

The negotiator, “tinker” begins to weigh up their options. He states he believes the FBI and CISA will be involved, as well as Mandiant and begins to compare the incident to the Change Healthcare attack by ALPHV/BlackCat (and later RansomHub) who received a 22 million USD ransom payment.



@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:11:25
judging by how things went with Alfvy with Change Healthcare - they will be very furious, since there is the same negotiator on their side - Mandiant from Google

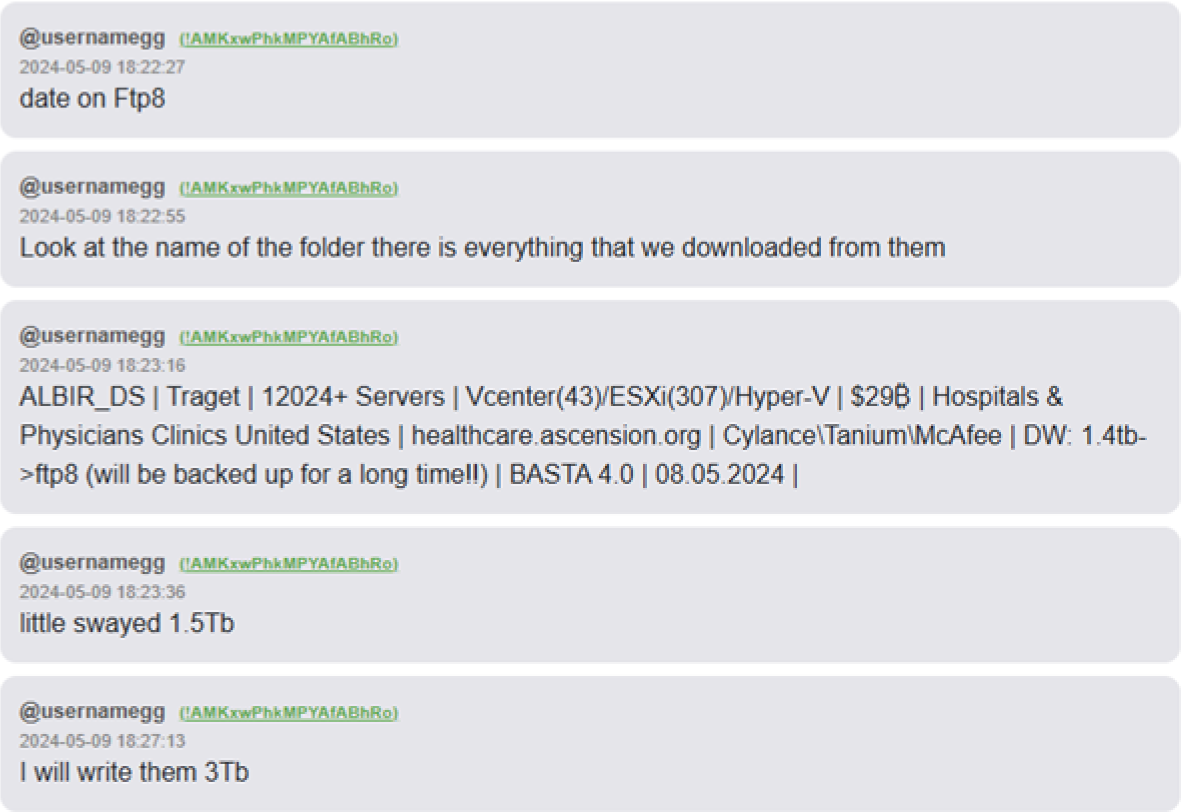


@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:11:47
And the FBI and CISA are obliged to get involved, but these are all trifles

@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:13:05
I am sure that they will try to stake out money similar to Change Healthcare - there was 22 million, and we need to put them in their place right away, that we are not AlphV - a different scale and other money

“gg” shares that all the stolen data was put on a server named “ftp8” and tagged as “ALBIR_DS” and says to “tinker” that he should “look at the folder name, everything we downloaded from them is there."

The operator, “gg” also shared a summary of the target environment of Ascension Health. This includes number of servers being over 12,000, what security tools they use such as Cylance, Tanium, and McAfee. Plus, “gg” said they downloaded over 1.4TB of data to "ftp8" and used BlackBasta ransomware version 4.0 and attacked them on 8 May 2024.



@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:22:27
date on Ftp8

@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:22:55
Look at the name of the folder there is everything that we downloaded from them

@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:23:16
ALBIR_DS | Traget | 12024+ Servers | Vcenter(43)/ESXi(307)/Hyper-V | $29฿ | Hospitals & Physicians Clinics United States | healthcare.ascension.org | Cylance\Tanium\McAfee | DW: 1.4tb->ftp8 (will be backed up for a long time!!) | BASTA 4.0 | 08.05.2024 |

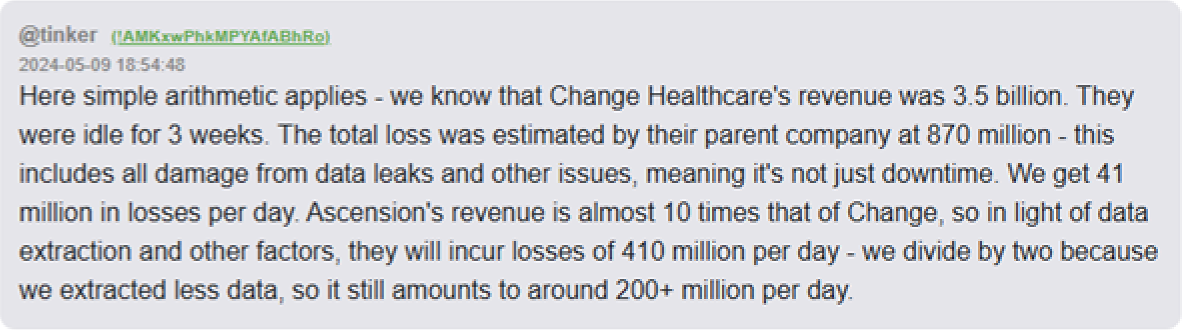
@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:23:36
little swayed 1.5Tb

@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:27:13
I will write them 3Tb

Interestingly, “gg” appears to have also recommended to bluff to the victim that they stole more than 1.5TB and say to the victim that they stole 3TB instead.

Negotiation Strategizing

After having established the details of the incident, Tinker (the negotiator) began to wonder about the likelihood of getting a ransom payment as well as estimate how much Ascension Health is likely losing per day.

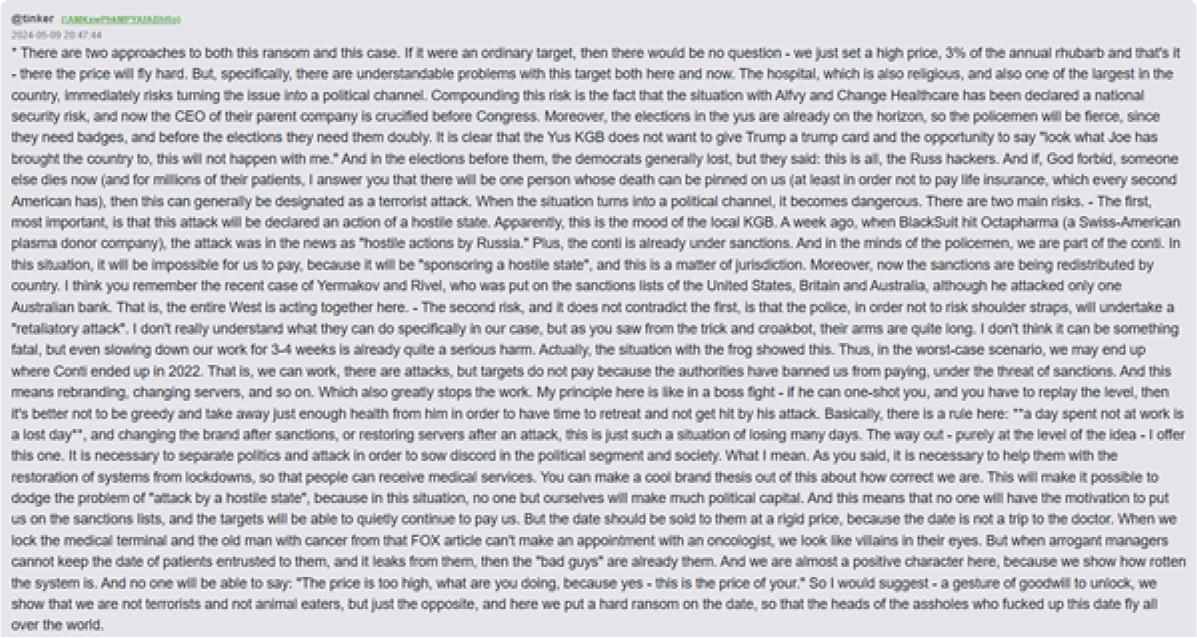


@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-09 18:54:48
Here simple arithmetic applies - we know that Change Healthcare's revenue was 3.5 billion. They were idle for 3 weeks. The total loss was estimated by their parent company at 870 million - this includes all damage from data leaks and other issues, meaning it's not just downtime. We get 41 million in losses per day. Ascension's revenue is almost 10 times that of Change, so in light of data extraction and other factors, they will incur losses of 410 million per day - we divide by two because we extracted less data, so it still amounts to around 200+ million per day.

Tinker (negotiator) then explains to the rest of the BlackBasta members involved in the attack what course of action they should take to get the ransom from Ascension Health. Tinker says they would normally set a 3% of the annual revenue and negotiate from there. They note that there are clear problems with the victim being a hospital and that this attack followed the Change Health attack by ALPHV/BlackCat. They also noted that they are worried as they believe the US National Security Agency (NSA) attacked TrickBot's servers four years ago and that the FBI took down Qakbot more recently. Tinker is also worried that one of Ascension Health’s patients will die and they will be blamed and labelled as a terrorist attack.

Tinker also noted that when BlackSuit attacked Octapharma that it was labelled by the news as "hostile actions by Russia" and they warned that Conti was already under sanctions and that because they are tied to Conti they may not get paid.

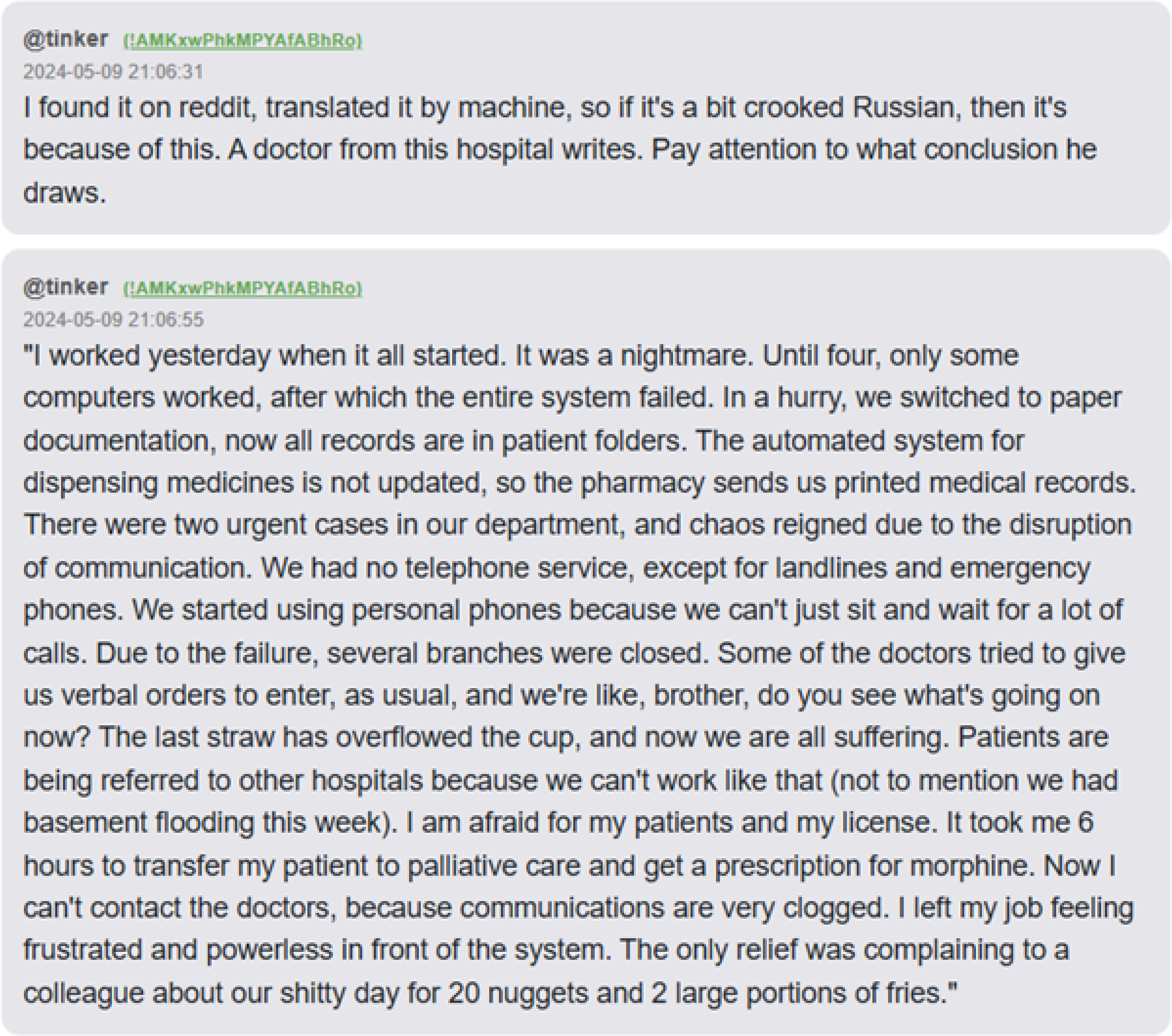
Tinker, ransomware negotiator for BlackBasta, ultimately recommended giving the decryptor for free to Ascension Health and resorting to data theft extortion. This is notable, as it is a similar situation to the Irish HSE ransomware attack by Conti, who also provided the decryptor for free.



@tinker [illegible]
2024-05-09 20:47:44
* There are two approaches to both this ransom and this case. If it were an ordinary target, then there would be no question - we just set a high price, 3% of the annual rhubarb and that's it - there the price will fly hard. But, specifically, there are understandable problems with this target both here and now. The hospital, which is also religious, and also one of the largest in the country, immediately risks turning the issue into a political channel. Compounding this risk is the fact that the situation with Alfvy and Change Healthcare has been declared a national security risk, and now the CEO of their parent company is crucified before Congress. Moreover, the elections in the yus are already on the horizon, so the policemen will be fierce, since they need badges, and before the elections they need them doubly. It is clear that the Yus KGB does not want to give Trump a trump card and the opportunity to say "look what Joe has brought the country to, this will not happen with me." And in the elections before them, the democrats generally lost, but they said: this is all, the Russ hackers. And if, God forbid, someone else dies now (and for millions of their patients, I answer you that there will be one person whose death can be pinned on us (at least in order not to pay life insurance, which every second American has), then this can generally be designated as a terrorist attack. When the situation turns into a political channel, it becomes dangerous. There are two main risks. - The first, most important, is that this attack will be declared an action of a hostile state. Apparently, this is the mood of the local KGB. A week ago, when BlackSuit hit Octapharma (a Swiss-American plasma donor company), the attack was in the news as "hostile actions by Russia." Plus, the conti is already under sanctions. And in the minds of the policemen, we are part of the conti. In this situation, it will be impossible for us to pay, because it will be "sponsoring a hostile state", and this is a matter of jurisdiction. Moreover, now the sanctions are being redistributed by country. I think you remember the recent case of Yermakov and Rivel, who was put on the sanctions lists of the United States, Britain and Australia, although he attacked only one Australian bank. That is, the entire West is acting together here. - The second risk, and it does not contradict the first, is that the police, in order not to risk shoulder straps, will undertake a "retaliatory attack". I don't really understand what they can do specifically in our case, but as you saw from the trick and croakbot, their arms are quite long. I don't think it can be something fatal, but even slowing down our work for 3-4 weeks is already quite a serious harm. Actually, the situation with the frog showed this. Thus, in the worst-case scenario, we may end up where Conti ended up in 2022. That is, we can work, there are attacks, but targets do not pay because the authorities have banned us from paying, under the threat of sanctions. And this means rebranding, changing servers, and so on. Which also greatly stops the work. My principle here is like in a boss fight - if he can one-shot you, and you have to replay the level, then it's better not to be greedy and take away just enough health from him in order to have time to retreat and not get hit by his attack. Basically, there is a rule here: "*a day spent not at work is a lost day*", and changing the brand after sanctions, or restoring servers after an attack, this is just such a situation of losing many days. The way out - purely at the level of the idea - I offer this one. It is necessary to separate politics and attack in order to sow discord in the political segment and society. What I mean. As you said, it is necessary to help them with the restoration of systems from lockdowns, so that people can receive medical services. You can make a cool brand thesis out of this about how correct we are. This will make it possible to dodge the problem of "attack by a hostile state", because in this situation, no one but ourselves will make much political capital. And this means that no one will have the motivation to put us on the sanctions lists, and the targets will be able to quietly continue to pay us. But the date should be sold to them at a rigid price, because the date is not a trip to the doctor. When we lock the medical terminal and the old man with cancer from that FOX article can't make an appointment with an oncologist, we look like villains in their eyes. But when arrogant managers cannot keep the date of patients entrusted to them, and it leaks from them, then the "bad guys" are already them. And we are almost a positive character here, because we show how rotten the system is. And no one will be able to say: "The price is too high, what are you doing, because yes - this is the price of your." So I would suggest - a gesture of goodwill to unlock, we show that we are not terrorists and not animal eaters, but just the opposite, and here we put a hard ransom on the date, so that the heads of the assholes who fucked up this date fly all over the world.

Healthcare Impact

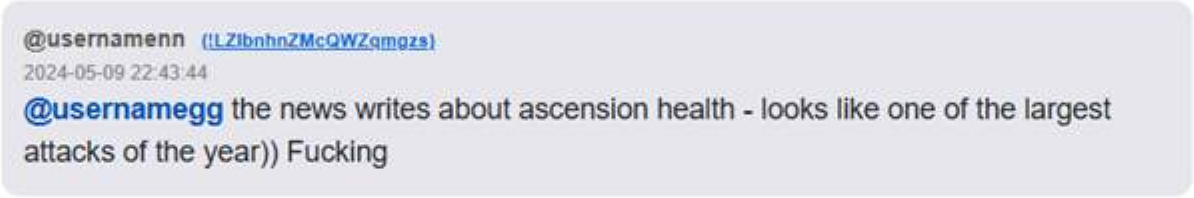
The fact Ascension Health is a major medical organisation with many patients appeared to take its toll on the BlackBasta members. Tinker wrote in the BlackBasta chat they he found a post on Reddit by a doctor that works for Ascension Health who described the damage of the attack.



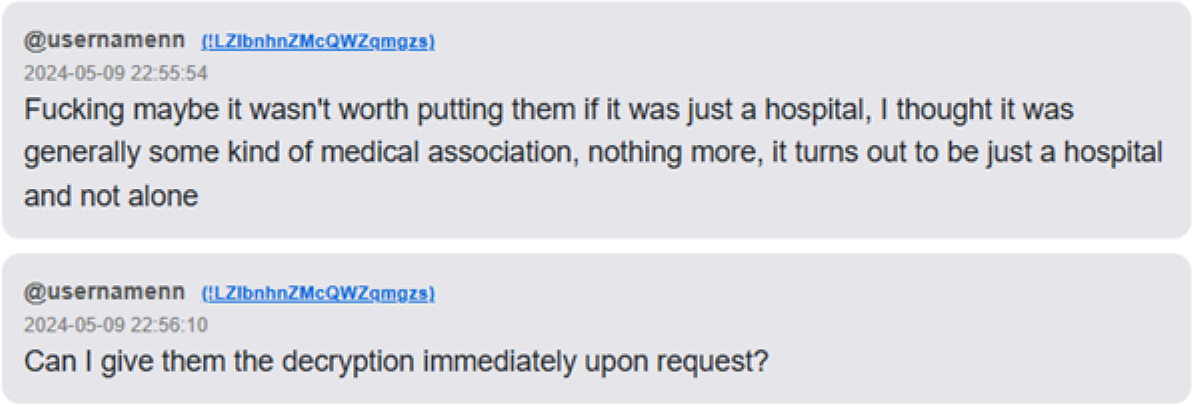
@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-09 21:06:31
I found it on reddit, translated it by machine, so if it's a bit crooked Russian, then it's because of this. A doctor from this hospital writes. Pay attention to what conclusion he draws.

@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-09 21:06:55
"I worked yesterday when it all started. It was a nightmare. Until four, only some computers worked, after which the entire system failed. In a hurry, we switched to paper documentation, now all records are in patient folders. The automated system for dispensing medicines is not updated, so the pharmacy sends us printed medical records. There were two urgent cases in our department, and chaos reigned due to the disruption of communication. We had no telephone service, except for landlines and emergency phones. We started using personal phones because we can't just sit and wait for a lot of calls. Due to the failure, several branches were closed. Some of the doctors tried to give us verbal orders to enter, as usual, and we're like, brother, do you see what's going on now? The last straw has overflowed the cup, and now we are all suffering. Patients are being referred to other hospitals because we can't work like that (not to mention we had basement flooding this week). I am afraid for my patients and my license. It took me 6 hours to transfer my patient to palliative care and get a prescription for morphine. Now I can't contact the doctors, because communications are very clogged. I left my job feeling frustrated and powerless in front of the system. The only relief was complaining to a colleague about our shitty day for 20 nuggets and 2 large portions of fries."

Another member of BlackBasta, “nn” also found out that Ascension Health is a group of hospitals. He immediately recommends giving them a decryptor for free.



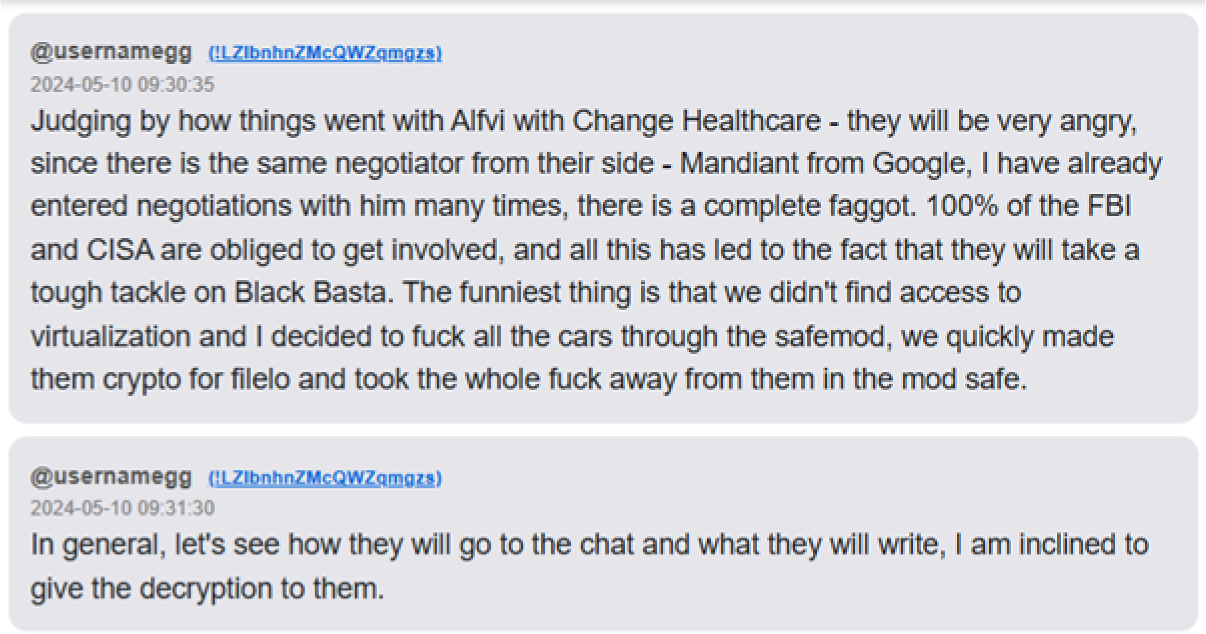
@usernamenn (!LZIbnhnZMcQWZqmgzs)
2024-05-09 22:43:44
@usernamegg the news writes about ascension health - looks like one of the largest attacks of the year)) Fucking



@usernamenn (!LZIbnhnZMcQWZqmgzs)
2024-05-09 22:55:54
Fucking maybe it wasn't worth putting them if it was just a hospital, I thought it was generally some kind of medical association, nothing more, it turns out to be just a hospital and not alone

@usernamenn (!LZIbnhnZMcQWZqmgzs)
2024-05-09 22:56:10
Can I give them the decryption immediately upon request?

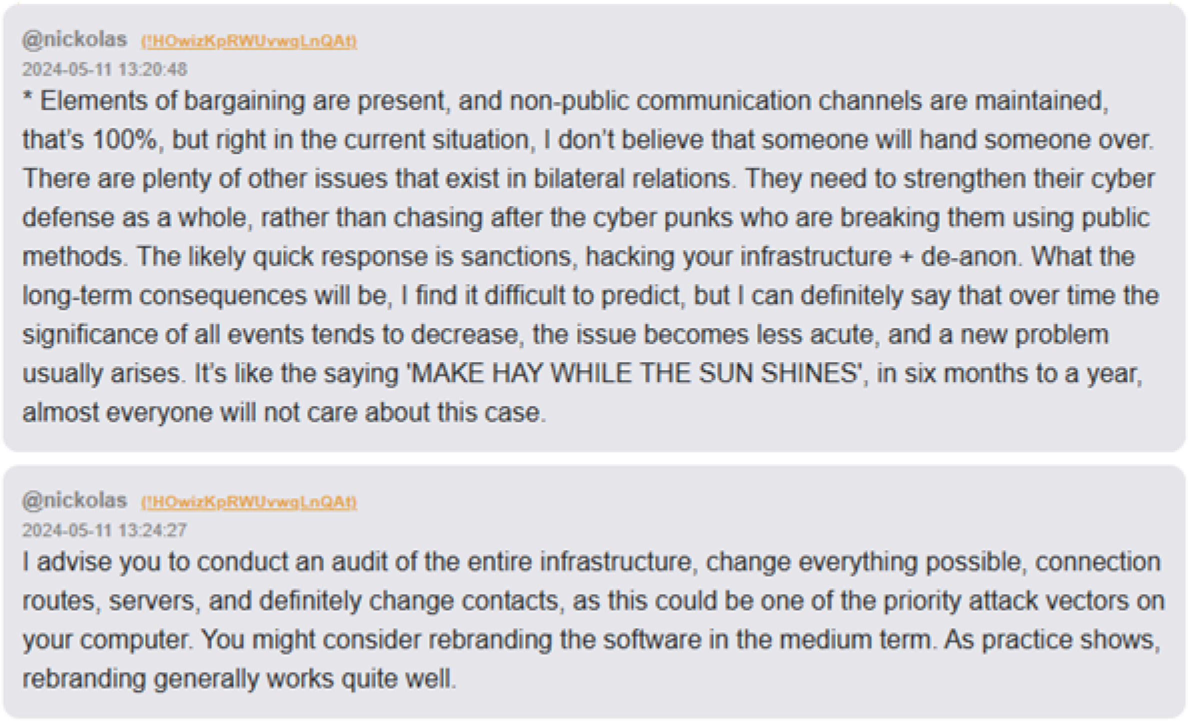
Interestingly, “gg” compares the attack on Change Health and also recognises Mandiant and warns that the FBI and CISA will be involved. Plus, “gg” noted that they did not encrypt via virtualization (such as vCenter, ESXi or Hyper-V) and reconfirmed they used Safe Mode Boot. Further, “gg” was also inclined to give Ascension the decryptor for free too.



@usernamegg (!LZIbnhnZMcQWZqmgzs)
2024-05-10 09:30:35
Judging by how things went with Alfvi with Change Healthcare - they will be very angry, since there is the same negotiator from their side - Mandiant from Google, I have already entered negotiations with him many times, there is a complete faggot. 100% of the FBI and CISA are obliged to get involved, and all this has led to the fact that they will take a tough tackle on Black Basta. The funniest thing is that we didn't find access to virtualization and I decided to fuck all the cars through the safemod, we quickly made them crypto for filelo and took the whole fuck away from them in the mod safe.

@usernamegg (!LZIbnhnZMcQWZqmgzs)
2024-05-10 09:31:30
In general, let's see how they will go to the chat and what they will write, I am inclined to give the decryption to them.

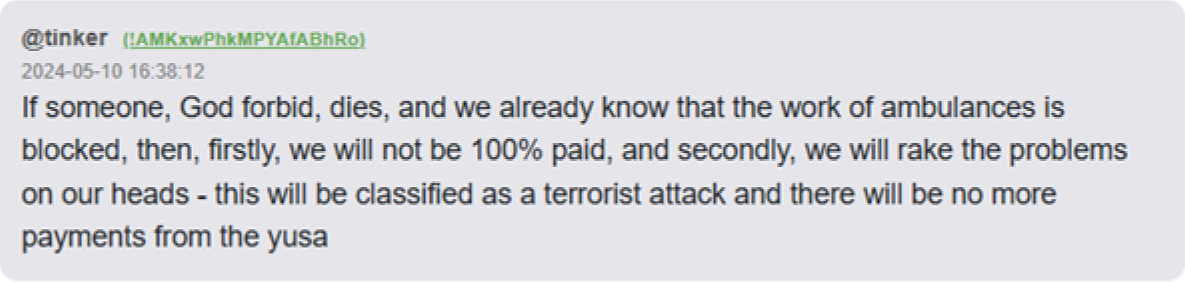
Another BlackBasta member, “nickolas” comments about the situation. He warned and was particularly concerned about law enforcement retaliation, such as hacking back, sanctions, indictments. He recommended auditing the entire infrastructure and having a rebrand of the BlackBasta name, which means changing the ransomware, leak site, and other personas.



@nickolas (!HOwizKpRWUvwgLnQAt)
2024-05-11 13:20:48
* Elements of bargaining are present, and non-public communication channels are maintained, that's 100%, but right in the current situation, I don't believe that someone will hand someone over. There are plenty of other issues that exist in bilateral relations. They need to strengthen their cyber defense as a whole, rather than chasing after the cyber punks who are breaking them using public methods. The likely quick response is sanctions, hacking your infrastructure + de-anon. What the long-term consequences will be, I find it difficult to predict, but I can definitely say that over time the significance of all events tends to decrease, the issue becomes less acute, and a new problem usually arises. It's like the saying 'MAKE HAY WHILE THE SUN SHINES', in six months to a year, almost everyone will not care about this case.

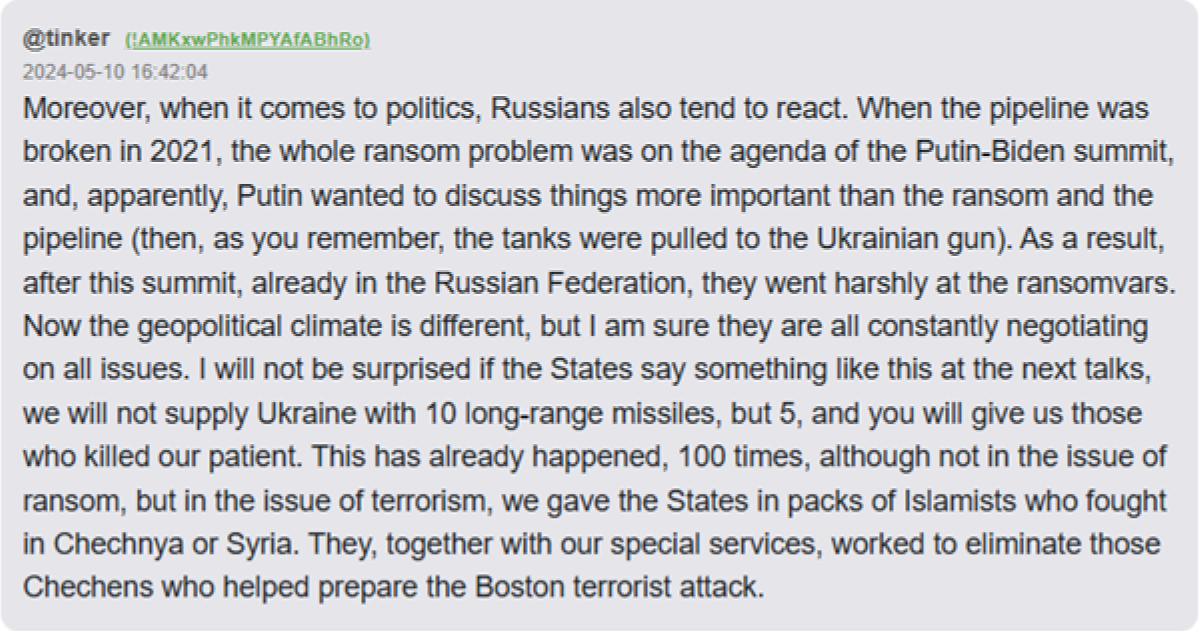
@nickolas (!HOwizKpRWUvwgLnQAt)
2024-05-11 13:24:27
I advise you to conduct an audit of the entire infrastructure, change everything possible, connection routes, servers, and definitely change contacts, as this could be one of the priority attack vectors on your computer. You might consider rebranding the software in the medium term. As practice shows, rebranding generally works quite well.

Tinker (negotiator) is aware however of the risk of someone dying and how it will impact their chances of getting the ransom.

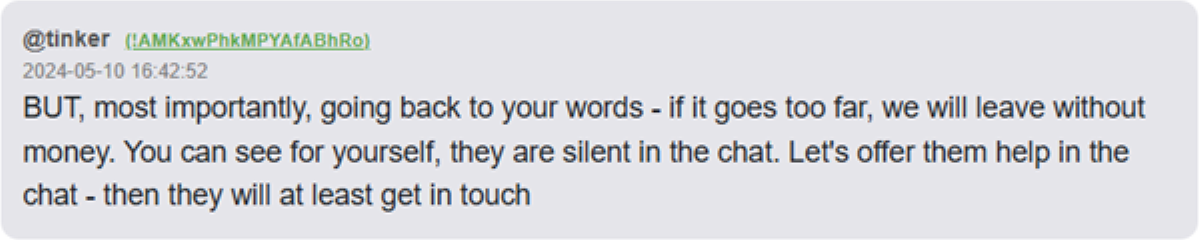


@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-10 16:38:12
If someone, God forbid, dies, and we already know that the work of ambulances is blocked, then, firstly, we will not be 100% paid, and secondly, we will rake the problems on our heads - this will be classified as a terrorist attack and there will be no more payments from the yusa

Tinker also discussed the politics of the scenario. He compared the situation to the colonial pipeline incident of 2021. He mentioned how Russia reacted and arrested ransomware operators. He also brought up the war in Ukraine and how ransomware attacks on the US impact the politics with Russia.

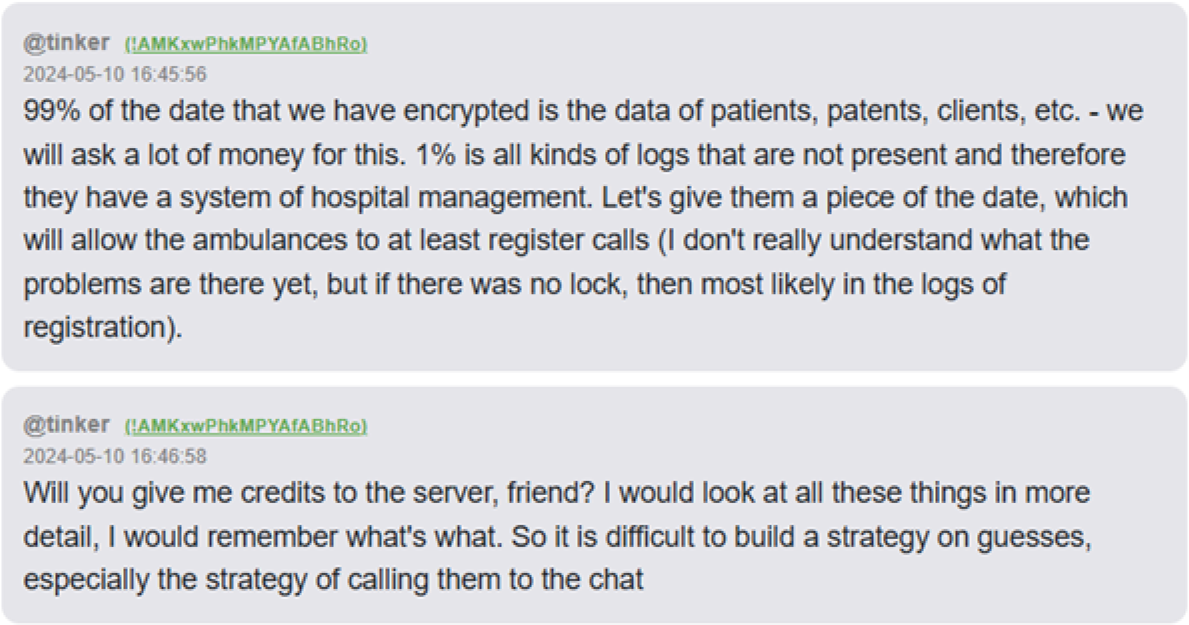


@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-10 16:42:04
Moreover, when it comes to politics, Russians also tend to react. When the pipeline was broken in 2021, the whole ransom problem was on the agenda of the Putin-Biden summit, and, apparently, Putin wanted to discuss things more important than the ransom and the pipeline (then, as you remember, the tanks were pulled to the Ukrainian gun). As a result, after this summit, already in the Russian Federation, they went harshly at the ransomvars. Now the geopolitical climate is different, but I am sure they are all constantly negotiating on all issues. I will not be surprised if the States say something like this at the next talks, we will not supply Ukraine with 10 long-range missiles, but 5, and you will give us those who killed our patient. This has already happened, 100 times, although not in the issue of ransom, but in the issue of terrorism, we gave the States in packs of Islamists who fought in Chechnya or Syria. They, together with our special services, worked to eliminate those Chechens who helped prepare the Boston terrorist attack.



@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-10 16:42:52
BUT, most importantly, going back to your words - if it goes too far, we will leave without money. You can see for yourself, they are silent in the chat. Let's offer them help in the chat - then they will at least get in touch

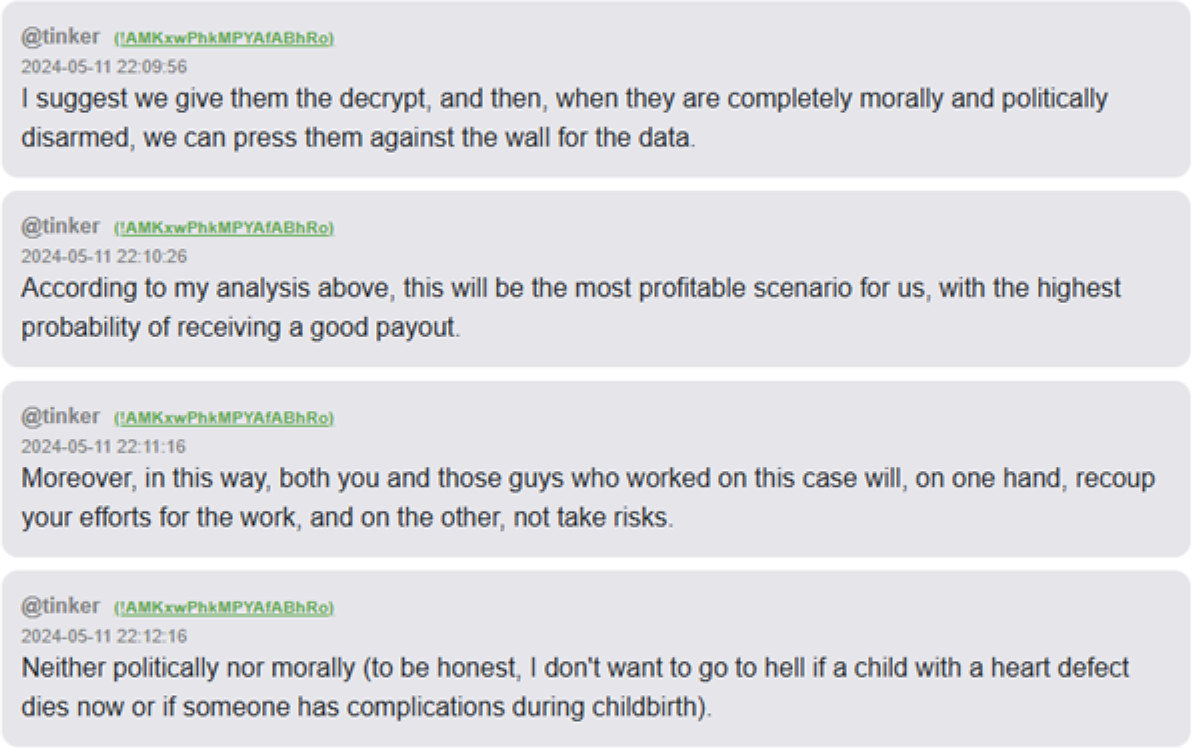
Tinker highlighted that the ransomware was used to encrypt patient data and how it caused the hospital management system to crash. He was particularly concerned about the ambulances being unable to operate but also tries to minimize the severity of the incident. Nevertheless, he asked to see the stolen data himself to get a better understanding of what data BlackBasta operators have that they can leverage against Ascension Health.



@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-10 16:45:56
99% of the date that we have encrypted is the data of patients, patents, clients, etc. - we will ask a lot of money for this. 1% is all kinds of logs that are not present and therefore they have a system of hospital management. Let's give them a piece of the date, which will allow the ambulances to at least register calls (I don't really understand what the problems are there yet, but if there was no lock, then most likely in the logs of registration).

@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-10 16:46:58
Will you give me credits to the server, friend? I would look at all these things in more detail, I would remember what's what. So it is difficult to build a strategy on guesses, especially the strategy of calling them to the chat

By the end of deliberations, Tinker recommends giving a free decryptor and then demand a ransom for the stolen data.



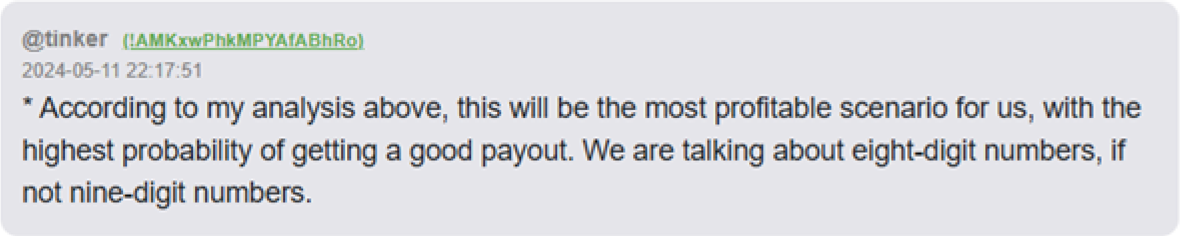
@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-11 22:09:56
I suggest we give them the decrypt, and then, when they are completely morally and politically disarmed, we can press them against the wall for the data.

@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-11 22:10:26
According to my analysis above, this will be the most profitable scenario for us, with the highest probability of receiving a good payout.

@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-11 22:11:16
Moreover, in this way, both you and those guys who worked on this case will, on one hand, recoup your efforts for the work, and on the other, not take risks.

@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-11 22:12:16
Neither politically nor morally (to be honest, I don't want to go to hell if a child with a heart defect dies now or if someone has complications during childbirth).

tinker edited his message to then clarify that he reckons they should demand a ransom in the 10s of millions USD or over 100 million USD.

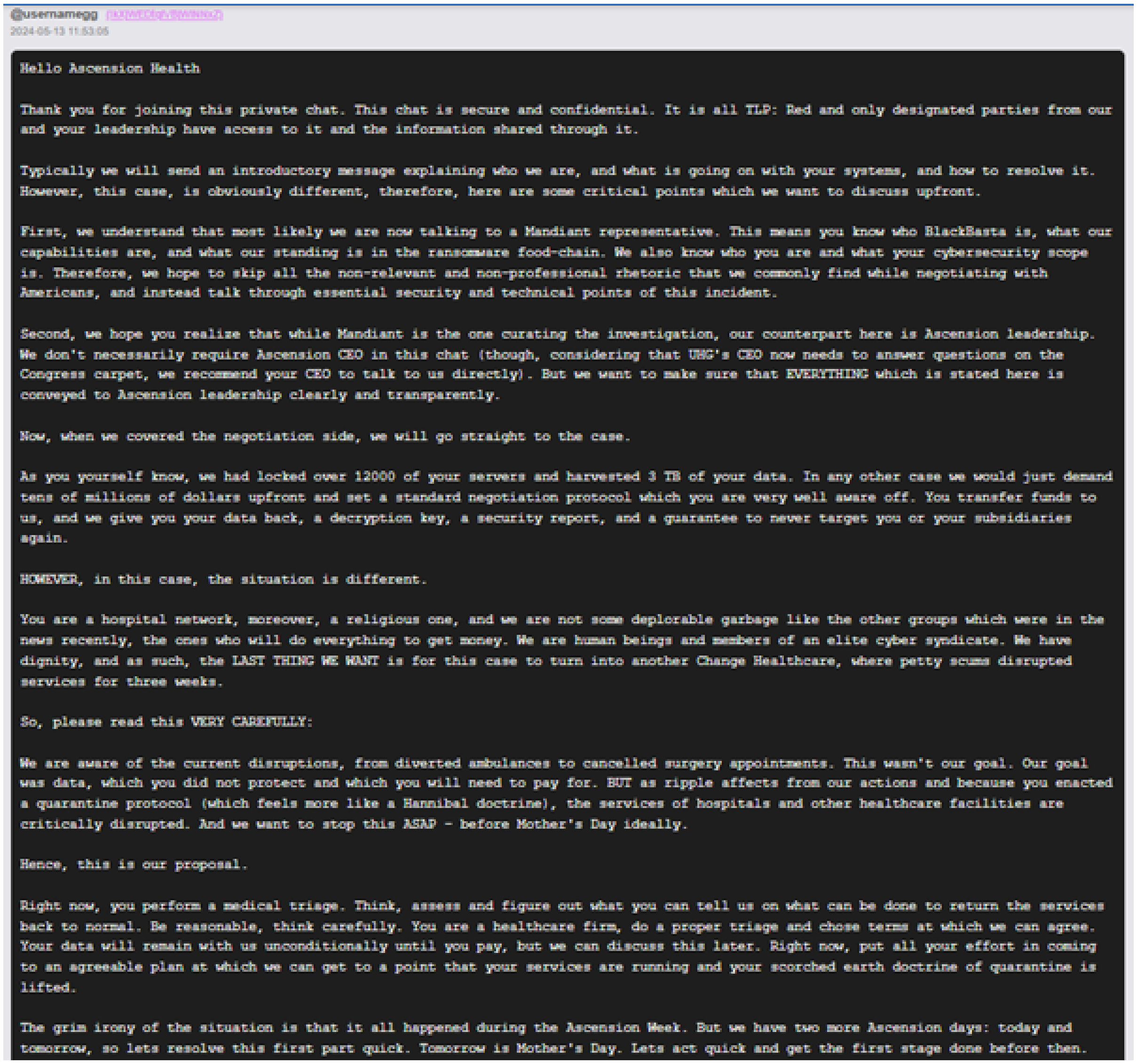


@tinker (!AMKxwPhkMPYAfABhRo)
2024-05-11 22:17:51

* According to my analysis above, this will be the most profitable scenario for us, with the highest probability of getting a good payout. We are talking about eight-digit numbers, if not nine-digit numbers.

Ransomware Negotiations

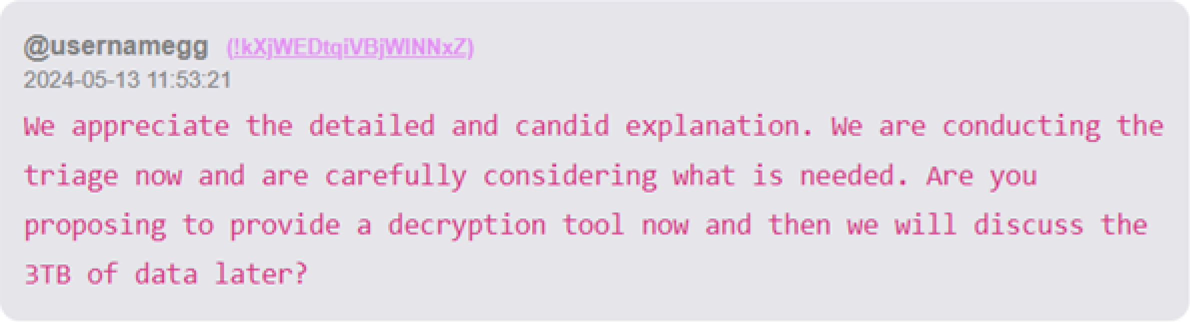
The operator “gg” then shared the opening message to Ascension Health shared via the Black Basta negotiation portal:



@usernamegg ([illegible])
2024-05-13 11:53:05

```
Hello Ascension Health

Thank you for joining this private chat. This chat is secure and confidential. It is all TLP: Red and only designated parties from our
and your leadership have access to it and the information shared through it.

Typically we will send an introductory message explaining who we are, and what is going on with your systems, and how to resolve it.
However, this case, is obviously different, therefore, here are some critical points which we want to discuss upfront.

First, we understand that most likely we are now talking to a Mandiant representative. This means you know who BlackBasta is, what our
capabilities are, and what our standing is in the ransomware food-chain. We also know who you are and what your cybersecurity scope
is. Therefore, we hope to skip all the non-relevant and non-professional rhetoric that we commonly find while negotiating with
Americans, and instead talk through essential security and technical points of this incident.

Second, we hope you realize that while Mandiant is the one curating the investigation, our counterpart here is Ascension leadership.
We don't necessarily require Ascension CEO in this chat (though, considering that UHG's CEO now needs to answer questions on the
Congress carpet, we recommend your CEO to talk to us directly). But we want to make sure that EVERYTHING which is stated here is
conveyed to Ascension leadership clearly and transparently.

Now, when we covered the negotiation side, we will go straight to the case.

As you yourself know, we had locked over 12000 of your servers and harvested 3 TB of your data. In any other case we would just demand
tens of millions of dollars upfront and set a standard negotiation protocol which you are very well aware off. You transfer funds to
us, and we give you your data back, a decryption key, a security report, and a guarantee to never target you or your subsidiaries
again.

HOWEVER, in this case, the situation is different.

You are a hospital network, moreover, a religious one, and we are not some deplorable garbage like the other groups which were in the
news recently, the ones who will do everything to get money. We are human beings and members of an elite cyber syndicate. We have
dignity, and as such, the LAST THING WE WANT is for this case to turn into another Change Healthcare, where petty scums disrupted
services for three weeks.

So, please read this VERY CAREFULLY:

We are aware of the current disruptions, from diverted ambulances to cancelled surgery appointments. This wasn't our goal. Our goal
was data, which you did not protect and which you will need to pay for. BUT as ripple affects from our actions and because you enacted
a quarantine protocol (which feels more like a Hannibal doctrine), the services of hospitals and other healthcare facilities are
critically disrupted. And we want to stop this ASAP - before Mother's Day ideally.

Hence, this is our proposal.

Right now, you perform a medical triage. Think, assess and figure out what you can tell us on what can be done to return the services
back to normal. Be reasonable, think carefully. You are a healthcare firm, do a proper triage and chose terms at which we can agree.
Your data will remain with us unconditionally until you pay, but we can discuss this later. Right now, put all your effort in coming
to an agreeable plan at which we can get to a point that your services are running and your scorched earth doctrine of quarantine is
lifted.

The grim irony of the situation is that it all happened during the Ascension Week. But we have two more Ascension days: today and
tomorrow, so lets resolve this first part quick. Tomorrow is Mother's Day. Lets act quick and get the first stage done before then.
```

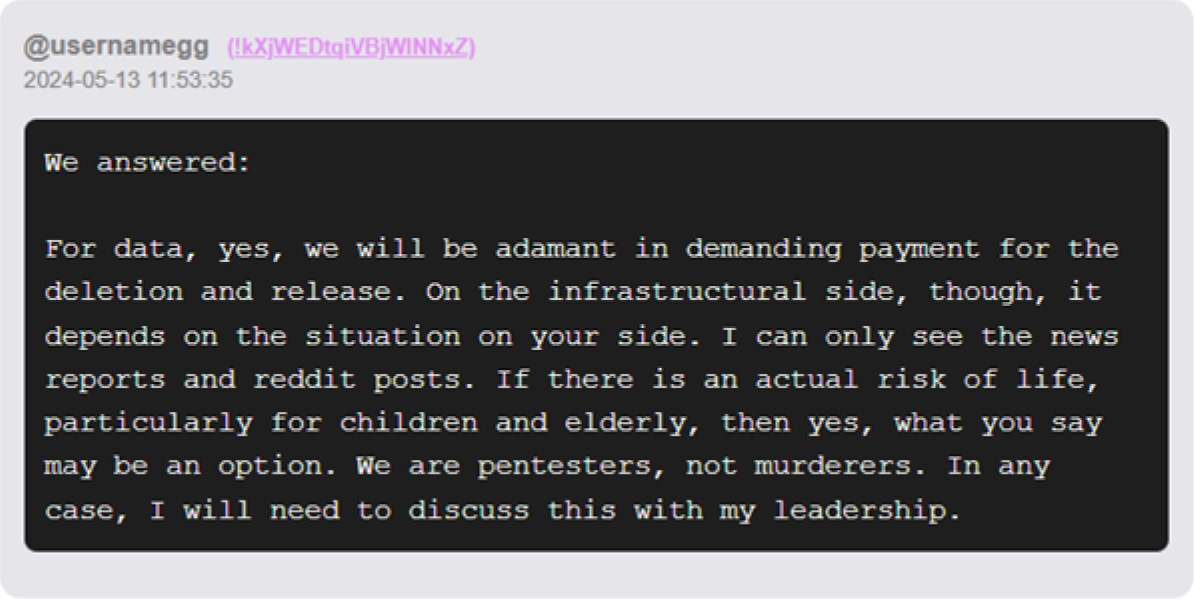
The negotiator for Ascension Health (who BlackBasta believes is Mandiant) replied to the negotiation chat portal:



@usernamegg (!kXjWEDtqiVBjWINNxZ)
2024-05-13 11:53:21

We appreciate the detailed and candid explanation. We are conducting the triage now and are carefully considering what is needed. Are you proposing to provide a decryption tool now and then we will discuss the 3TB of data later?

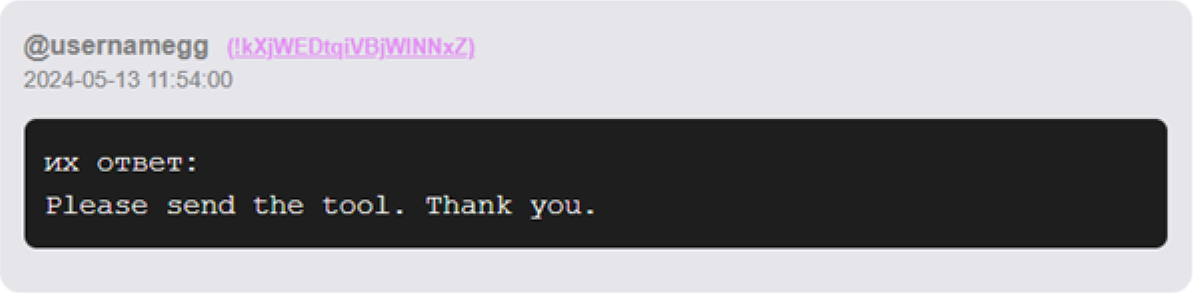
“gg” then clarified the terms of the ransom demand. A payment will be needed to delete and share the stolen data He maintains the offer to provide a free decryptor:



@usernamegg (!kXjWEDtqiVBjWINNxZ)
2024-05-13 11:53:35

```
We answered:

For data, yes, we will be adamant in demanding payment for the
deletion and release. On the infrastructural side, though, it
depends on the situation on your side. I can only see the news
reports and reddit posts. If there is an actual risk of life,
particularly for children and elderly, then yes, what you say
may be an option. We are pentesters, not murderers. In any
case, I will need to discuss this with my leadership.
```

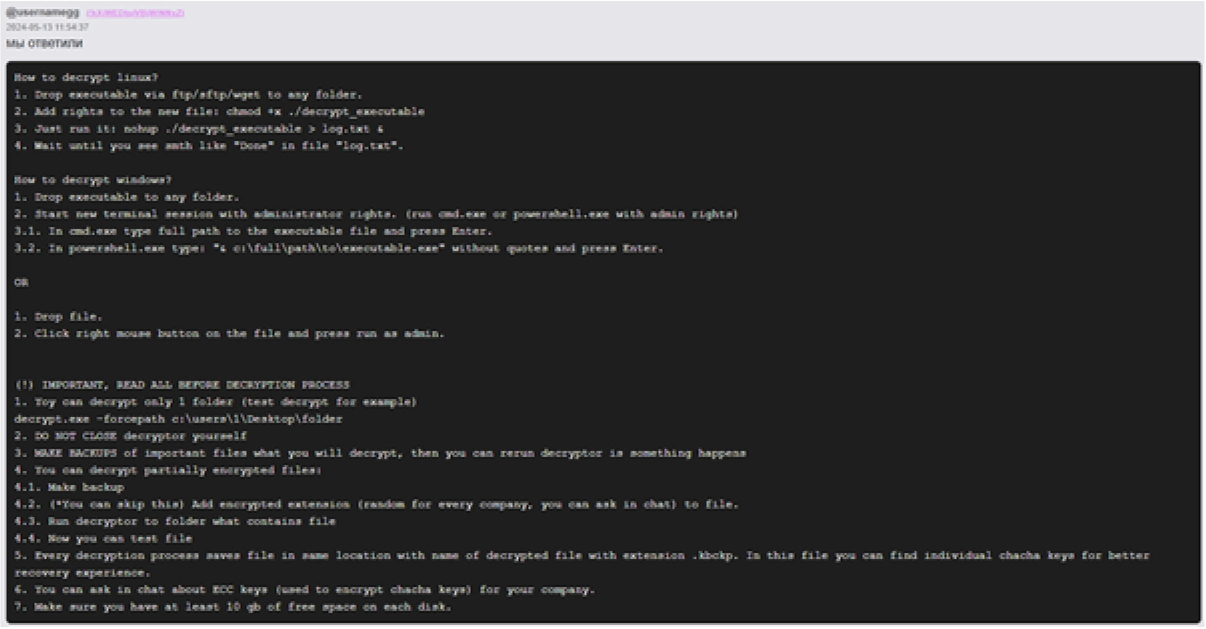
The negotiator for Ascension Health asked for the decryption tool:



@usernamegg (!kXjWEDtqiVBjWINNxZ)
2024-05-13 11:54:00

```
их ответ:
Please send the tool. Thank you.
```

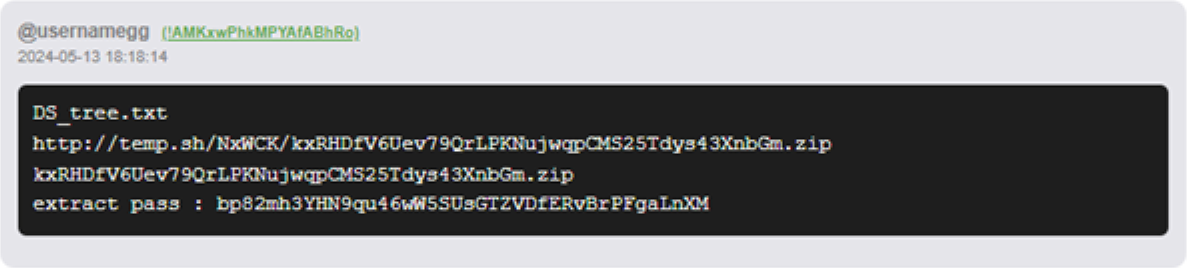
The decryptor was then provided to Ascension Health:



@usernamegg [illegible]
2024-05-13 11:54:37
мы ответили

```
How to decrypt linux?
1. Drop executable via ftp/sftp/wget to any folder.
2. Add rights to the new file: chmod +x ./decrypt_executable
3. Just run it: nohup ./decrypt_executable > log.txt &
4. Wait until you see smth like "Done" in file "log.txt".

How to decrypt windows?
1. Drop executable to any folder.
2. Start new terminal session with administrator rights. (run cmd.exe or powershell.exe with admin rights)
3.1. In cmd.exe type full path to the executable file and press Enter.
3.2. In powershell.exe type: "& c:\full\path\to\executable.exe" without quotes and press Enter.

OR

1. Drop file.
2. Click right mouse button on the file and press run as admin.


(!) IMPORTANT, READ ALL BEFORE DECRYPTION PROCESS
1. Toy can decrypt only 1 folder (test decrypt for example)
decrypt.exe -forcepath c:\users\1\Desktop\folder
2. DO NOT CLOSE decryptor yourself
3. MAKE BACKUPS of important files what you will decrypt, then you can rerun decryptor is something happens
4. You can decrypt partially encrypted files:
4.1. Make backup
4.2. (*You can skip this) Add encrypted extension (random for every company, you can ask in chat) to file.
4.3. Run decryptor to folder what contains file
4.4. Now you can test file
5. Every decryption process saves file in same location with name of decrypted file with extension .kbckp. In this file you can find individual chacha keys for better
recovery experience.
6. You can ask in chat about ECC keys (used to encrypt chacha keys) for your company.
7. Make sure you have at least 10 gb of free space on each disk.
```

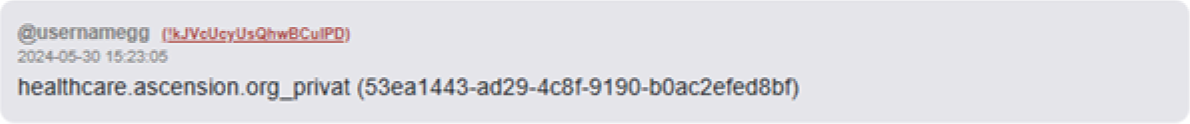
Later, “gg” then shares a file tree for ""DS"" (which is equal to Ascension Health). The file is added to a ZIP and shared via a temp[.]sh link and is password protected:



@usernamegg (!AMKxwPhkMPYAfABhRo)
2024-05-13 18:18:14

```
DS_tree.txt
http://temp.sh/NxWCK/kxRHDfV6Uev79QrLPKNujwqpCMS25Tdys43XnbGm.zip
kxRHDfV6Uev79QrLPKNujwqpCMS25Tdys43XnbGm.zip
extract pass : bp82mh3YHN9qu46wW5SUsGTZVDfERvBrPFgaLnXM
```

The operator “gg” then uses Privat (a screenshot sharing site) to show the proof that they have deleted the data of Ascension Health:



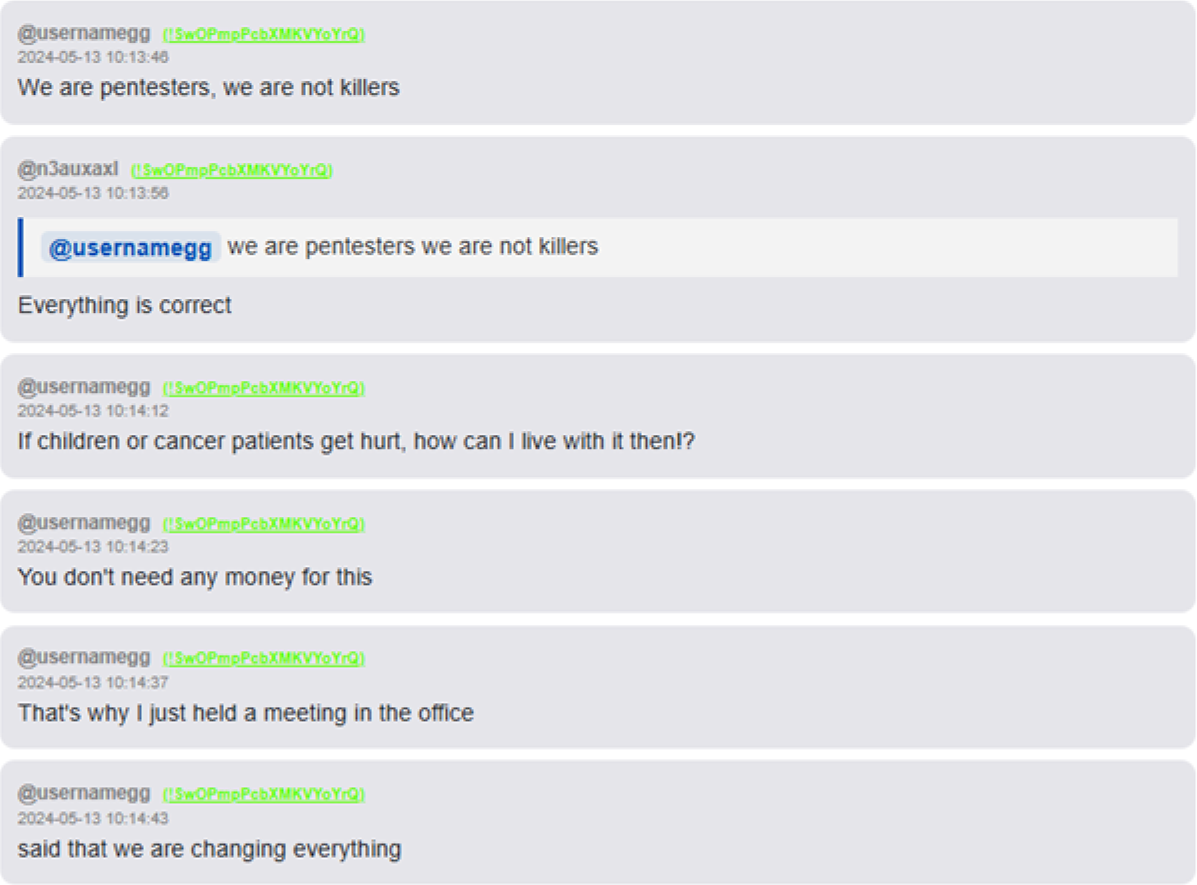
@usernamegg (!kJVcUcyUsQhwBCuIPD)
2024-05-30 15:23:05
healthcare.ascension.org_privat (53ea1443-ad29-4c8f-9190-b0ac2efed8bf)

From these messages, it appears no ransom was paid and BlackBasta returned the data and deleted it.

Change of Heart

The most interesting part of this engagement with Ascension Health by BlackBasta was that the members deliberated back and forth about whether to provide a free decryption tool but all appeared to be fine with demanding a ransom for the victim data.

The operator “gg” appears to have a change of heart. He exclaims that they (the members of the BlackBasta ransomware gang) are "pentesters" and not "killers" and claims he “held a meeting in the office” which is interesting as it further proves they are a cybercrime enterprise, potentially with full-time employees.



@usernamegg (!$wOPmpPcbXMKVYoYrQ)
2024-05-13 10:13:46
We are pentesters, we are not killers

@n3auxaxl (!$wOPmpPcbXMKVYoYrQ)
2024-05-13 10:13:56

> @usernamegg we are pentesters we are not killers

Everything is correct

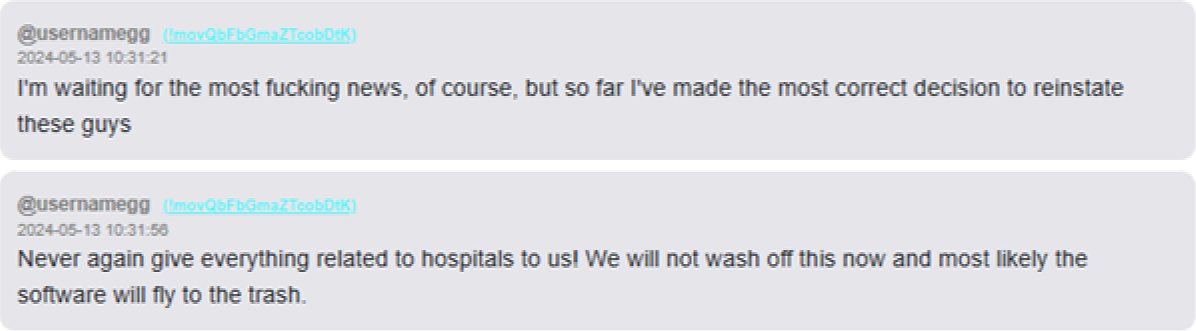
@usernamegg (!$wOPmpPcbXMKVYoYrQ)
2024-05-13 10:14:12
If children or cancer patients get hurt, how can I live with it then!?

@usernamegg (!$wOPmpPcbXMKVYoYrQ)
2024-05-13 10:14:23
You don't need any money for this

@usernamegg (!$wOPmpPcbXMKVYoYrQ)
2024-05-13 10:14:37
That's why I just held a meeting in the office

@usernamegg (!$wOPmpPcbXMKVYoYrQ)
2024-05-13 10:14:43
said that we are changing everything

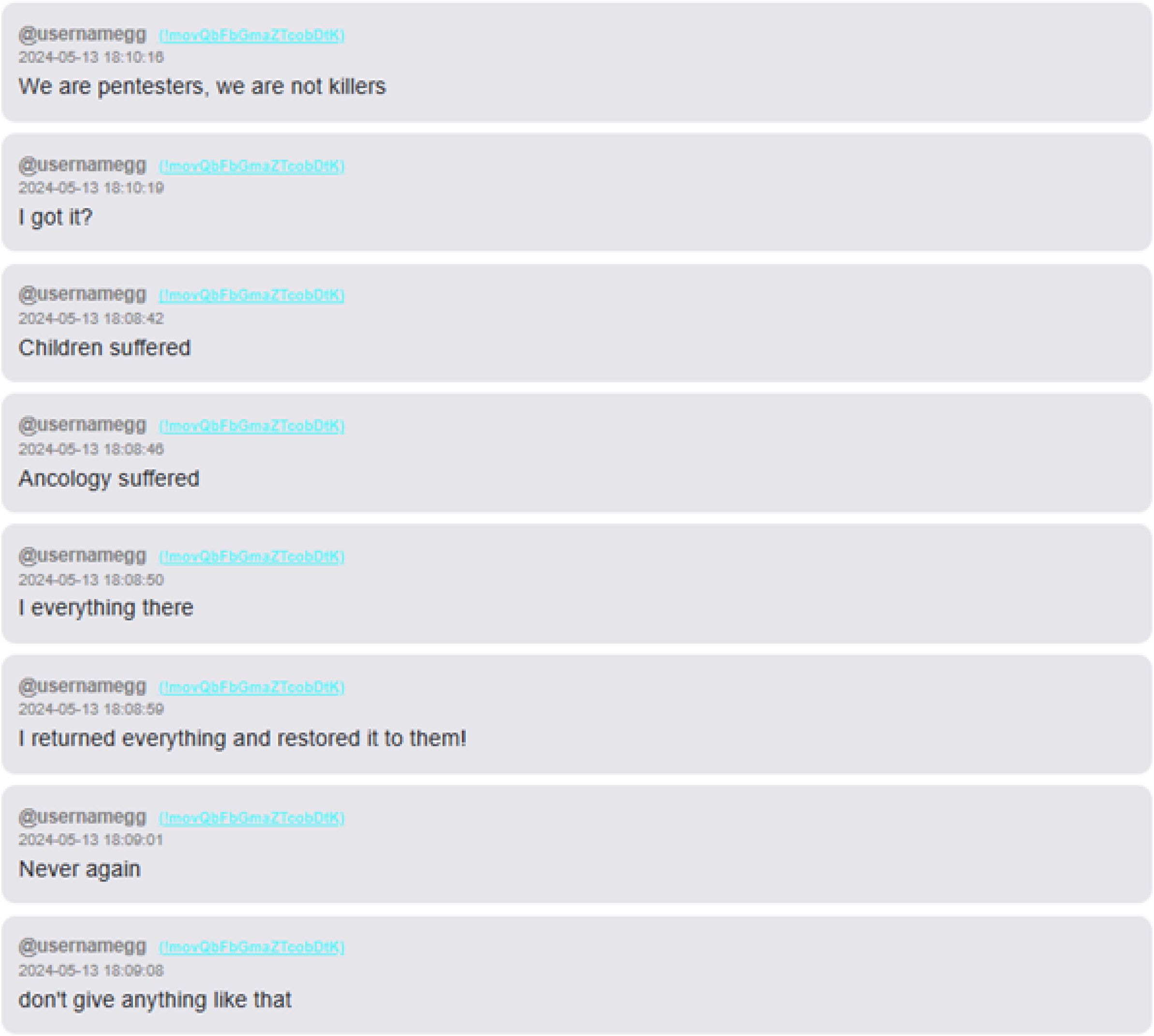
The operator “gg” decided to help Ascension Health and requests not to work on hospitals anymore.



@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 10:31:21
I'm waiting for the most fucking news, of course, but so far I've made the most correct decision to reinstate these guys

@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 10:31:56
Never again give everything related to hospitals to us! We will not wash off this now and most likely the software will fly to the trash.

He also said “the software will fly to the trash” which likely means the group was thinking of ditching the brand of BlackBasta and rebrand to another name. Finally, “gg” warns other BlackBasta members not to target hospitals any more:



@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 18:10:16
We are pentesters, we are not killers

@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 18:10:19
I got it?

@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 18:08:42
Children suffered

@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 18:08:46
Ancology suffered

@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 18:08:50
I everything there

@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 18:08:59
I returned everything and restored it to them!

@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 18:09:01
Never again

@usernamegg (!movQbFbGmaZTcobDtK)
2024-05-13 18:09:08
don't give anything like that

The Impact of the BlackBasta Attack on Ascension Health

According to the HIPAA Journal, the personal data of up to 5.6 million patients was exposed and Ascension confirmed that some patient data was stolen during the attack. Ascension said that it found no evidence that the ransomware group gained access to electronic health records or other clinical systems, so full medical histories have not been stolen. During the attack, however, Ascension was forced to divert ambulances, close pharmacies, take critical IT systems offline and resort to pen and paper to record patient information. The attack affected a large percentage of its 136 hospitals across the US and took Ascension around 6 weeks to restore access to its electronic medical record system and resume normal operations. The ransomware attack reportedly caused delays in revenue cycle processes, claims submission, and payment processing, in addition to significant remediation costs.

Lessons Learned

This chat log confirms that BlackBasta attacked Ascension Health using version 4.0 of their ransomware and used the Safe Mode Boot technique on 12,000 endpoints of the healthcare system.

If reconnaissance began on 3 November 2023 and the attack happened on the 8 May 2024, that would make the amount of time they took to gain access and deploy the ransomware was up to 187 days long or around six months. Due to this, cybercriminal campaign appears to be comparable to a more focused state-sponsored level intrusion where months of planning and numerous attempts are made to infiltrate a target.

The BlackBasta negotiator, Tinker, believed that they were going to get a very high ransom payment in the 10s of millions or up to 100 million USD and compared the attack to the Change Health incident by ALPHV/BlackCat who got 22 million USD.

The high ransom payment by Change Health has appeared to be like a dinner bell for ransomware gangs to go after other healthcare sector victims. Paying the ransom as a healthcare organisation clearly has significant downstream impact on the rest of the industry and it should be an absolute last resort and default to be to never pay the ransom.

There was an interesting change of heart and moment where the operator “gg” decided to give up on the Ascension Health attack, provide them a decryptor, provide the data back to them, and share proof that they deleted it. The members of BlackBasta were clearly concerned about hack-backs from law enforcement or intelligence services, as well as sanctions and deanonymization. The BlackBasta team also mentioned several times during this incident that they were going to have to rebrand because of the attack.

Overall, this incident goes to show that even Russia-based cybercrime enterprises with dozens of members remain paranoid about being attack by law enforcement and intelligence services. It is really interesting that they themselves admit that their actions warrant such a response.

One of the key lessons to learn from this engagement is that if a healthcare organisation is attacked by a ransomware gang, then it would be a valid strategy to tell the news about the incident. News about patients lives being at risk and dying will get the attention of these ruthless cybercriminals who will realise the mistakes they made and are potentially likely to at least provide a free decryptor and may give up entirely on their ransom payment pursuit and move on to the next target.

Lastly, these chat logs appear to prove that the West’s policies aimed at increasing pressure on Russia-based ransomware gangs is evidently working. These organised cybercrime enterprises are beginning to alter their targeting behaviour as a result to avoid the wrath of law enforcement retaliation.

Raspberry Robin: A global USB malware campaign providing access to ransomware operators

The Ransomware Tool Matrix

The Russian APT Tool Matrix