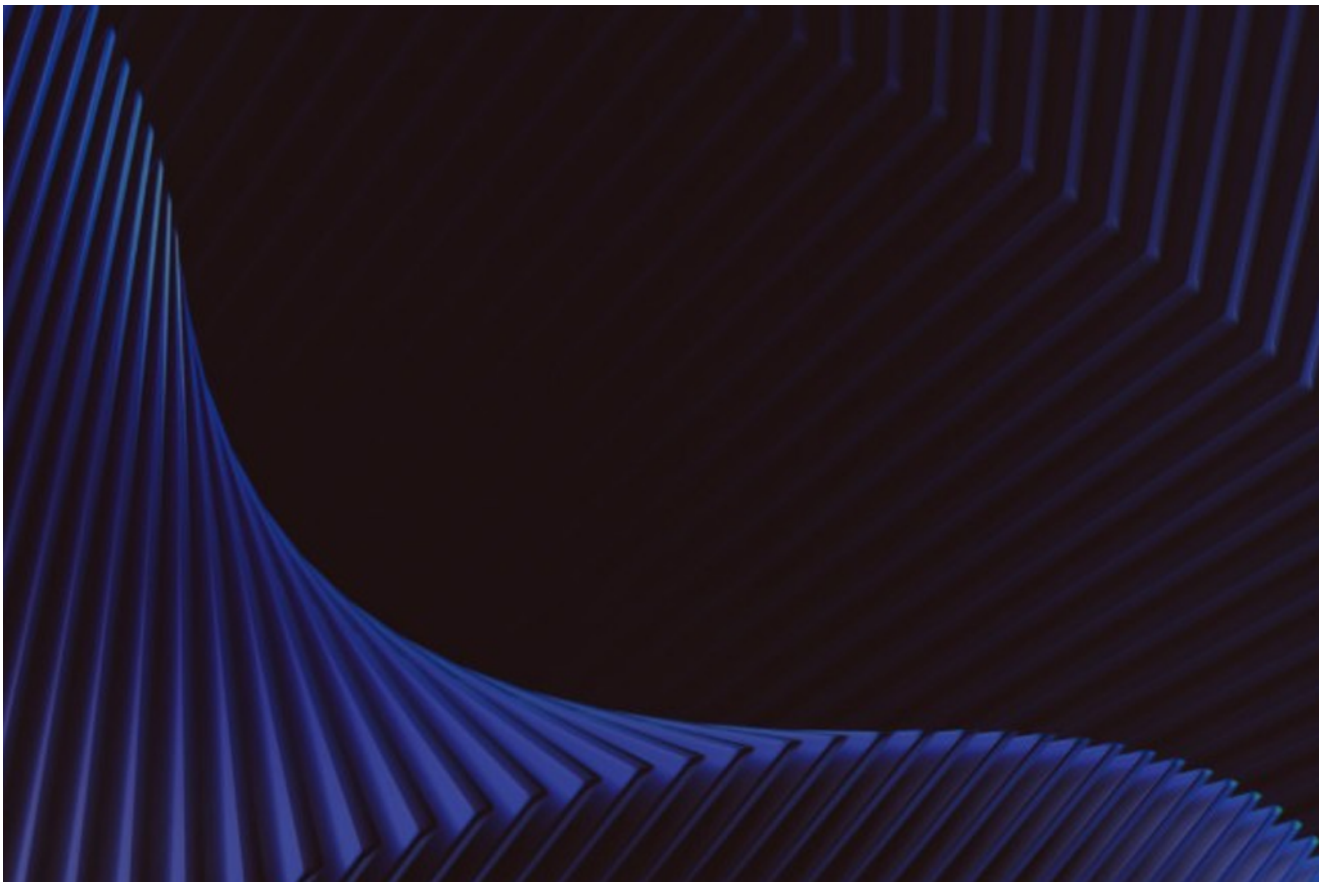
Conti Leaks: Examining the Panama Papers of Ransomware



By John Fokker, Jambul Tologonov · March 31, 2022

Introduction

It isn't often the whole world gets an inside look of the business operations of a top tier cybercriminal group. Very early on in the Russian-Ukrainian Crisis the predominantly Russian based ransomware group Conti made a public statement where they expressed their loyalty to the Russian Administration.

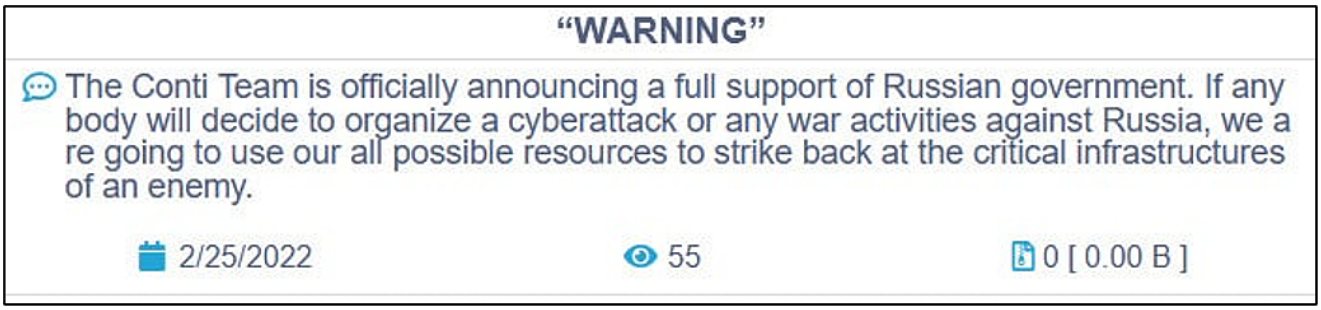


Figure 1. Conti expressing their support to the Russian Administration. Source: BleepingComputer

As a reaction to this statement and the current conflict, a Ukrainian security researcher, operating by the twitter handle @contileaks decided to publish years of Conti's internal Jabber conversations online. The chats that were dumped span across several years consisted of thousands of messages making this the "**Panama Papers of Ransomware**".

This wasn't the first time the Conti gang got hit, last summer a disgruntled affiliate posted their attack playbook online, which was full of very useful intelligence for our customers.

Since it was public, the whole security community jumped to review the chats and within hours the first findings appeared on Twitter. Trellix was also quick to obtain the dataset and realized that this might be one of the largest "crowd-sourced cyber investigations" ever seen. What this means is that as a research team you must devise a flexible dissemination strategy because findings by the crowd will appear online. So, it is constant balance between verification of the published findings by others, investing in your own research goals and adjusting some of these goals based on new information.

Even though it was very tempting to dive down the rabbit hole immediately we did make sure we attacked the dataset with a certain plan.

Dissemination strategy; How to avoid the rabbit hole

Attack infrastructure

The first batch of leaked chats were only a couple of days old and ranging back quite some time. From the start we realized that the criminals might have left valuable data on their attack infrastructure in the chats. We wrote a quick extraction script and compared the mentioned network artifacts to our current dataset and saw a lot of overlap. Not only did we see overlap with infrastructure we attributed to TrickBot and Cobalt Strike in the past, but a good portion of the systems we filtered out were still alive and kicking. To prevent any retaliation by the Conti group directed at our customers, blocking this infrastructure was top priority.

Some of these live systems were actually located in the countries where we have a good relationship with Law Enforcement, so naturally we reached out and made sure they got a heads-up to take appropriate measures quickly.

The intelligence gathered from this was very actionable, but with a short shelf life, the next stop for us was tradecraft.

TTPs and tradecraft

Due to the severity of the leaks, there was a good chance that the Conti gang would rebrand or disperse it members across other ransomware families. In the prior leak where Conti's playbook got dumped online there were excellent descriptions of the different tools and scripts they would use to attack their victims. So, looking at around 200 thousand leaked messages (Conti & TrickBot leaks combined) span over the period 2020-2022, it was likely members would share custom TTP's or tradecraft amongst each other.

By filtering tool names and command line structures we found several examples where members discussed tool usage. Given the crowd sourced nature of this dump we would also like to thank The DFIR Report for their excellent findings which they published via their Twitter account.

Affiliates might leave Conti and their network, but wherever they go they will take along their tradecraft. Without an external intervention, like an arrest, we should anticipate that cybercriminals won't stop their line of business, and thus we can expect to see their TTPs pop up in the future. However, through proper dissemination of the data we were able to empower many of our XDR product teams to improve the product efficacy against this tradecraft and incorporate our findings in MVISION Insights for customer visibility.

Did we ignore the juicy conversations completely? Not at all, fortunately we have a native Russian speaking research capability that made a huge difference while going down the rabbit hole. In the following section we will highlight some of the findings we found interesting to share.

Interesting chats

For transparency purposes we have included both the original Cyrillic and our human translated text to allow readers to delve into the intricacies of some of the Conti's discussions. For readability purposes we have put the original leaked messages into 1-2-1 conversations to make it easier to understand/follow the context.

Conti as an *enterprise*

It is fascinating how much Conti resembles an ordinary firm with an office building, HR and other departments (testers, reversers, OSINT, coders, training team, etc.) with their regular salaries on the 15th and 30th of each month. Working hours are 10.00-18.00 Moscow time, five days a week. **Stern** is the boss who oversees everything and has 100 people on the payroll. "*The weekend are the weekends. And nobody cancelled the vacations and sick days. All the other holidays - with the management's agreement*" says **Salmon** (recruiter) to new hire-coder **Core**. According to **Bentley** (manager), he worked there for a year, but the

company has existed for more than 10 years. Below are excerpts from various chats which provide a good glimpse into Conti's organization and the presence of a physical office(s) in Russia:

```
2020-09-11T02:32:55.040081  target  "сейчас 8 трудятся это кем проф и думс довольны, остальных убрали
по итогу 50 - 3 офиса в ожидании профа и набору
новый набор под конец месяца, проф просил немного сбавить обороты
фот в неделю составляет 140 000 руб грязными без учета офиса, уборок, администрирования"
2020-09-11T02:32:55.041906  target  "+ начальные расходы это аренда, депозит, техника, хоз расходы мелкие- камеры чашки чайники, без мебели,
+ ежедневные расходы это обеды по 1500-1700 на всех в офис"
2020-09-11T02:32:55.043542  target  + субподрядчики кто помогает прфоу в лабе, кобе, еще что то настраивать
```

```
2020-09-11T02:32:55.040081  target  "at the moment there are 8 people who work and prof and dums are happy about, the rest are removed
in total 50 - 3 offices are awaiting prof and recruitment
new recruitment towards the end of the month, prof asked to slow down a bit
expenses a month are 140 000 rubbles dirty money without office costs, cleaning, administration"
2020-09-11T02:32:55.041906  target  "+ initial expenses which are rent, deposit, equipment, small household expenses- cameras, cups kettles, without furniture,
+ daily expenses which is lunch of 1500-1700 for the entire office"
2020-09-11T02:32:55.043542  target  + subcontractors who help prof in lab, cob, and set up something else
```

Figure 2. Target's messages to Stern about office expenses

```
2020-09-28T00:21:13.572941  troy    ponyal po dnu budu v ofice
2020-09-28T00:22:23.679788  troy    odnogo rabotnika vignal nahuy
2020-09-28T00:22:30.526240  troy    disciplinu rozlagal
2020-09-28T00:22:38.956771  target  так по факту
2020-09-28T00:22:40.899449  troy    kak ne priydu postoyanno spit
```

```
2020-09-28T00:21:13.572941  troy    got it will be in the office during the day
2020-09-28T00:22:23.679788  troy    I fucking fired one of the workers
2020-09-28T00:22:30.526240  troy    was corrupting the discipline
2020-09-28T00:22:38.956771  target  just as a fact
2020-09-28T00:22:40.899449  troy    every time I arrive he is sleeping
```

```
2021-07-16T10:28:56.793831  mango   "ЗП банде сюда bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df

сумма общая 85к
_____
99947 основная команда 62 человека, зп у меня получают 54
33847  - команда реверса, 23 человека
8500  - новая команда кодеров, 6 человек, пока только 4 зп получают
12500 реверсы, 6 человек
10000 ОСИНТ отдел 4 человека
3000 на расходы (серваки\прокладки\тестовые задания для новых людей)

164.8к всего в месяц"
```

```
2021-07-16T10:28:56.793831  mango   "salaries for the band here bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df

total 85k
_____
99947 main team 62 people, 54 of them get salaries from me
33847  - reversing team, 23 people
8500  - new team of coders, 6 people, at the moment only 4 receive salaries
12500 reversers, 6 people
10000 OSINT department 4 people
3000 on expenses (servers\layers\testing assignments for new people)

164.8к in total a month"
```

Figure 3. Mango to Stern about teams' monthly salary

```
2021-07-27T13:43:25.007728  mango   "Значитс так. Добавь:
revers@ - оператор хакеров, нормальный чел, он даст кобу, будет держать связь от нас, даст доступ в чат как пойдут движения
hors@ - вторая команда хакеров, хорс тоже ровный тип, если вдруг там какие то пробелмы у первых с пейлоадом - можно к вторым, они все знакомы, ниче страшного нет,я стараюсь всех нагружать равномерно.
bentley@ - собирает крипты на трик, лоадер, на кобы, повершеллы и прочее, если срочно что то надо можно сказать что от меня и он все сделает.
buza@ тимлид кодеров, если надо какие то доработки\консультации можно к нему. Он же начальник разведки OSINT у нас, можно через него запросить пробив какой то инфы по каким то компаниям.
По все, если надо будет дам еще хакеров или каких то других людй в помощь"
```

```
2021-07-27T13:43:25.007728  mango   "So here it is. To add:
revers@ - hackers' operator, good fellow, he will give cob, will keep a connection from our end, will give an access to the chat when things start moving
hors@ - 2nd team of hackers, hors is also a good guy, in case there are problems with the payloads from the first group - the second one can also be approached, they all know each other, there is nothing to worry there, I try to load everyone evenly.
bentley@ - gather crypts for trick, loader, cob's, PowerShell, etc, if there is anything urgent, you can say it is from me and he will do everything needed.
buza@ teamlead of coders, if you need any development/consultation you can approach him. He is also the head of OSINT and you can request intel from him about certain companies.
That is it, if you need I will give you more hackers or some other people to help"
```

Figure 4. Mango to Qwerty about team composition

It is particularly interesting that in the Conti-TrickBot enterprise they are very careful about malware code overlapping. They have external experts who scrutinize developed illegal software code and ensure the code fingerprints are unique to each team of coders. Avoiding overlap seems to be important to segregate activities of different sub-teams and make it difficult for security researchers to piece various Russian speaking threat actors' campaigns together.

```
[30.11.21 13:46:27] salmon:     Насчет политики компании по интеллектуальной собственности.
[30.11.21 13:46:45] salmon:     Все принадлежит компании, как сам код, который разрабатывается, проекты и т.д., любая информация.
В том числе результаты программ (криптеры, что-то обфусцированное и т.д.).
Нигде нельзя ни публиковать ни распространять, ни как-либо иначе использовать наработки в своих интересах.
Это связано еще с совпадением отпечатков внутри исходного кода, внутри результатов.
Некоторые эксперты со стороны оценивают по отпечаткам принадлежность софта разным командам. Чтобы небыло лишних пересечений.
```

```
[30.11.21 13:46:27] salmon:     Regarding the company's policy on intellectual property.
[30.11.21 13:46:45] salmon:     Everything is owned by the company, the code itself which is being developed, projects and etc., any information.
Including the results of the programs (cryptors, obfuscators, etc.). It is forbidden to publish, distribute or use elsewhere anything developed, created here.
This is also related to overlap of fingerprints of the code and the results.
Some experts from outside evaluate the fingerprints to determine to which team the soft belongs to. So that there are no unnecessary overlaps.
```

Figure 5. Salmon to Core about company's policy on intellectual property

Possible government connections

According to **Angelo** (tester/coder), **Stern** is closely affiliated with FSB or other structures and works for 'Pu'. If **Stern** was not as almighty as God, they all would have ended up as REvil:

```
[17.09.21 09:41:40] hammer:     стерн в часах
[17.09.21 09:41:49] hammer:     долгих
[17.09.21 09:43:09] angelo:     может С на приёме у министров
[17.09.21 09:43:42] hammer:     а может он сам министр
[17.09.21 09:44:39] hammer:     клиенты не бухтят?
[17.09.21 10:01:53] angelo:     моё личное мнение, он приближенный к ФСБ или другим страуктурам
[17.09.21 10:01:59] angelo:     но не сам
```

```
[17.09.21 09:41:40] hammer:     stern in hours
[17.09.21 09:41:49] hammer:     long ones
[17.09.21 09:43:09] angelo:     may be S at the ministers' reception
[17.09.21 09:43:42] hammer:     or may be he is himself a minister
[17.09.21 09:44:39] hammer:     anything from the clients?
[17.09.21 10:01:53] angelo:     my personal opinion is that he is close to FSB or other structures
[17.09.21 10:01:59] angelo:     but not himself
```

Figure 6. Angelo saying to Hammer that Stern is close to FSB

```
[02.02.22 20:05:57] elroy:      Приветствую
[02.02.22 20:06:02] elroy:      Повтори пожалуйста
[02.02.22 20:06:13] angelo:     да блин, вы со своимм Приветствую меня пугаете уже
[02.02.22 20:06:15] angelo:     слишком большие мы, и распиздяйства много (( плохо всё это пахнет
[02.02.22 20:06:27] angelo:     переживаю я
[02.02.22 20:06:32] elroy:      ))
[02.02.22 20:06:40] elroy:      Да, пахнет плохо
[02.02.22 20:07:09] angelo:     я думал С всемогущь как господь БОг
[02.02.22 20:07:21] elroy:      Мне сегодня пришлось административной работой заниматься, у меня в настройке маршрутизатор..
[02.02.22 20:07:41] elroy:      Будь он не всемогущь, мы пошли бы вслед за Ревилами
[02.02.22 20:08:03] elroy:      Там же написано, в статье, единственная в россии крупная компания
[02.02.22 20:08:22] angelo:     да я уже понял что С на службе у Пу
[02.02.22 20:08:30] angelo:     понимаю всё очень масштабно
[02.02.22 20:08:38] angelo:     что заказы мы делаем и кто порой наши клиенты
```

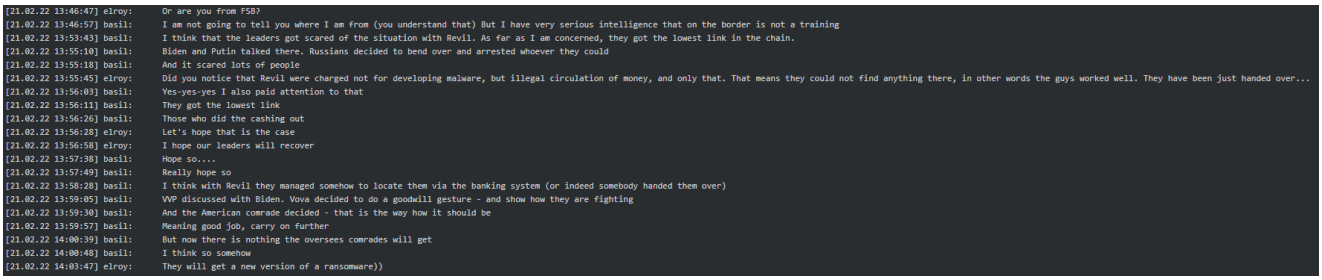
```
[02.02.22 20:05:57] elroy:      Good day!
[02.02.22 20:06:02] elroy:      Can you repeat please
[02.02.22 20:06:13] angelo:     you guys with your Good day already scaring me
[02.02.22 20:06:15] angelo:     we are too big and there is a lot of fuck ups (( all smell bad
[02.02.22 20:06:27] angelo:     I am worried
[02.02.22 20:06:32] elroy:      ))
[02.02.22 20:06:40] elroy:      Yes, smells bad indeed
[02.02.22 20:07:09] angelo:     I thought S is almighty as God
[02.02.22 20:07:21] elroy:      I had to do today administrative work, my router is in Settings...
[02.02.22 20:07:41] elroy:      If he was not almighty, we all would have ended up as Revil
[02.02.22 20:08:03] elroy:      It is written there in the article, the only big organisation in Russia
[02.02.22 20:08:22] angelo:     yes, I already figured that S is in service of Pu
[02.02.22 20:08:30] angelo:     I understand that everything is on a large scale ))
[02.02.22 20:08:38] angelo:     what orders we do and who sometimes our clients are
```

Figure 7. Elroy and Angelo discussing how almighty their boss Stern is

The Conti leadership was concerned over the situation surrounding the REvil ransomware group. However, Conti believed Russian authorities arrested only the lowest ranked members of REvil who were involved in the cash out.

It is worth mentioning that **Basil** (tester/coder) was asked if he is from FSB, he subsequently replied he had serious intelligence related to Ukrainian border activity. This statement was made seven days prior to Russia's incursion into Ukraine:

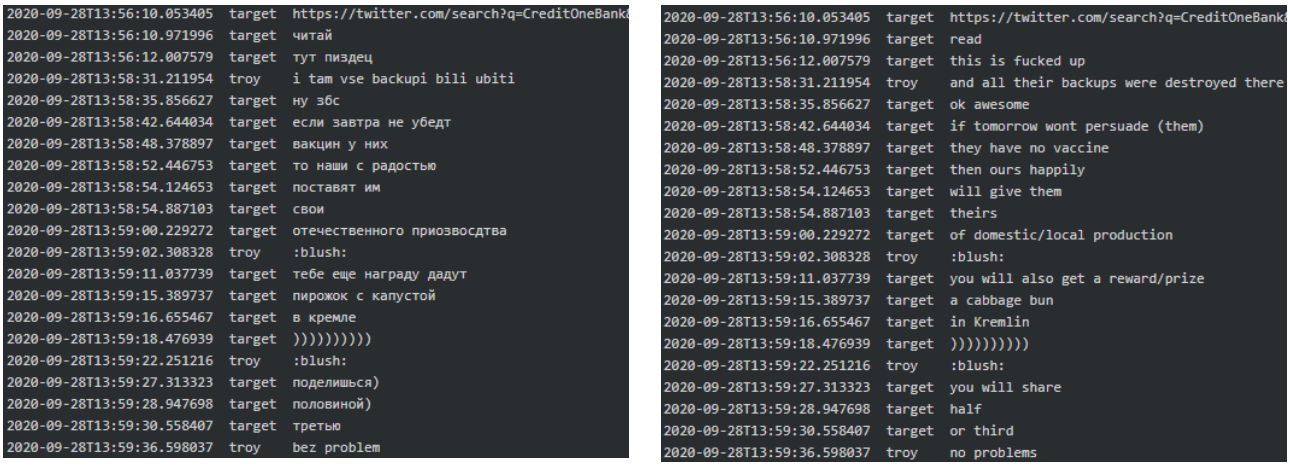
```
[21.02.22 13:46:47] elroy:      Или из фсб?
[21.02.22 13:46:57] basil:      Не буду говорить откуда (сам понимаешь) Но у меня очень серьезные сведения что на границе не учения
[21.02.22 13:53:43] basil:      Я думаю чт руководителей ситуация с равилами напугала. А по мне так низшее звено взяли.
[21.02.22 13:55:10] basil:      Байден Путин там поговорили. Россияне решили прогнуться взяли кого могли
[21.02.22 13:55:18] basil:      И это многих напугало
[21.02.22 13:55:45] elroy:      Обрати внимание, тчо Ревилам предъявили не разработку вредоносных программ, а незаконны оборот средств, и только. А значит у них ничего не нашли, т.е. ребята хорошо работали. Их просто сдали...
[21.02.22 13:56:03] basil:      Да-да-да я тоже обратил на это внимание
[21.02.22 13:56:11] basil:      Низшее звено взяли
[21.02.22 13:56:26] basil:      Тех кто обнал делал
[21.02.22 13:56:28] elroy:      Будем надеяться что так
[21.02.22 13:56:58] elroy:      Надеюсь у нас руководство очухается
[21.02.22 13:57:38] basil:      Надеюсь....
[21.02.22 13:57:49] basil:      Дейсвительно надеюсь
[21.02.22 13:58:28] basil:      Я думаю что с ревилами там как то через банковскую систему на них вышли (ну или кто-то сдал)
[21.02.22 13:59:05] basil:      ВВП с Байденом переговорил. Вова решил сделать жест доброй воли - и показать как они борются
[21.02.22 13:59:30] basil:      А Амерский товарищь решил - что так и должно быть
[21.02.22 13:59:57] basil:      т.е. "молодцы" продолжайте дальше
[21.02.22 14:00:39] basil:      Ну а теперь ничего этим товарищам из-за океана не отвалится
[21.02.22 14:00:48] basil:      Мне почему то так кажется
[21.02.22 14:03:47] elroy:      Отвалится им новая версия шифровальщика))
```



```
[21.02.22 13:46:47] elroy:    Or are you from FSB?
[21.02.22 13:46:57] basil:    I am not going to tell you where I am from (you understand that) But I have very serious intelligence that on the border is not a training
[21.02.22 13:53:43] basil:    I think that the leaders got scared of the situation with Revil. As far as I am concerned, they got the lowest link in the chain.
[21.02.22 13:55:10] basil:    Biden and Putin talked there. Russians decided to bend over and arrested whoever they could
[21.02.22 13:55:18] basil:    And it scared lots of people
[21.02.22 13:55:45] elroy:    Did you notice that Revil were charged not for developing malware, but illegal circulation of money, and only that. That means they could not find anything there, in other words the guys worked well. They have been just handed over...
[21.02.22 13:56:03] basil:    Yes-yes-yes I also paid attention to that
[21.02.22 13:56:11] basil:    They got the lowest link
[21.02.22 13:56:26] basil:    Those who did the cashing out
[21.02.22 13:56:28] elroy:    Let's hope that is the case
[21.02.22 13:56:58] elroy:    I hope our leaders will recover
[21.02.22 13:57:38] basil:    Hope so....
[21.02.22 13:57:49] basil:    Really hope so
[21.02.22 13:58:28] basil:    I think with Revil they managed somehow to locate them via the banking system (or indeed somebody handed them over)
[21.02.22 13:59:05] basil:    VVP discussed with Biden. Vova decided to do a goodwill gesture - and show how they are fighting
[21.02.22 13:59:30] basil:    And the American comrade decided - that is the way how it should be
[21.02.22 13:59:57] basil:    Meaning good job, carry on further
[21.02.22 14:00:39] basil:    But now there is nothing the oversees comrades will get
[21.02.22 14:00:48] basil:    I think so somehow
[21.02.22 14:03:47] elroy:    They will get a new version of a ransomware))
```

Figure 8. Basil and Elroy on REvil arrest

In another conversation involving **Target** (manager) he stated if they indeed encrypted Credit One Bank **Troy** (tester/crypter) would get a reward in the Kremlin:



```
2020-09-28T13:56:10.053405  target  https://twitter.com/search?q=CreditOneBank&
2020-09-28T13:56:10.971996  target  читай
2020-09-28T13:56:12.007579  target  тут пиздец
2020-09-28T13:58:31.211954  troy    i tam vse backupi bili ubiti
2020-09-28T13:58:35.856627  target  ну збс
2020-09-28T13:58:42.644034  target  если завтра не убедт
2020-09-28T13:58:48.378897  target  вакцин у них
2020-09-28T13:58:52.446753  target  то наши с радостью
2020-09-28T13:58:54.124653  target  поставят им
2020-09-28T13:58:54.887103  target  свои
2020-09-28T13:59:00.229272  target  отечественного приозводтва
2020-09-28T13:59:02.308328  troy    :blush:
2020-09-28T13:59:11.037739  target  тебе еще награду дадут
2020-09-28T13:59:15.389737  target  пирожок с капустой
2020-09-28T13:59:16.655467  target  в кремле
2020-09-28T13:59:18.476939  target  ))))))))))
2020-09-28T13:59:22.251216  troy    :blush:
2020-09-28T13:59:27.313323  target  поделишься)
2020-09-28T13:59:28.947698  target  половиной)
2020-09-28T13:59:30.558407  target  третью
2020-09-28T13:59:36.598037  troy    bez problem
```

```
2020-09-28T13:56:10.053405  target  https://twitter.com/search?q=CreditOneBank&
2020-09-28T13:56:10.971996  target  read
2020-09-28T13:56:12.007579  target  this is fucked up
2020-09-28T13:58:31.211954  troy    and all their backups were destroyed there
2020-09-28T13:58:35.856627  target  ok awesome
2020-09-28T13:58:42.644034  target  if tomorrow wont persuade (them)
2020-09-28T13:58:48.378897  target  they have no vaccine
2020-09-28T13:58:52.446753  target  then ours happily
2020-09-28T13:58:54.124653  target  will give them
2020-09-28T13:58:54.887103  target  theirs
2020-09-28T13:59:00.229272  target  of domestic/local production
2020-09-28T13:59:02.308328  troy    :blush:
2020-09-28T13:59:11.037739  target  you will also get a reward/prize
2020-09-28T13:59:15.389737  target  a cabbage bun
2020-09-28T13:59:16.655467  target  in Kremlin
2020-09-28T13:59:18.476939  target  ))))))))))
2020-09-28T13:59:22.251216  troy    :blush:
2020-09-28T13:59:27.313323  target  you will share
2020-09-28T13:59:28.947698  target  half
2020-09-28T13:59:30.558407  target  or third
2020-09-28T13:59:36.598037  troy    no problems
```

Figure 9. Target to Troy saying he gets a reward in the Kremlin

Occasionally Conti seems to be asked to do so-called ‘pioneering’ (volunteering) work on a special request from one of two ‘offices’. As Soviet Pioneers (aka scouts) they do their fair share of work similarly to what Cozy Bear does:

```
2020-07-20T17:02:13.288029  professor   че нам надо от академи?
2020-07-20T17:02:25.472364  professor   это контора просила какая-то из двух известных?
2020-07-20T17:02:26.978371  stern   отписал там реверсу
2020-07-20T17:02:28.775027  stern   да
2020-07-20T17:02:33.493244  professor   он поднял там
2020-07-20T17:02:33.892018  professor   что искать надо?
2020-07-20T17:02:35.227086  stern   переписка
2020-07-20T17:02:39.491168  professor   платить будут? или в пионеров играем?
2020-07-20T17:02:40.613491  stern   контракты
2020-07-20T17:02:42.493082  professor   =)
2020-07-20T17:02:43.571499  stern   бухгалтерия
2020-07-20T17:02:55.596933  stern   да пофиг на деньги
2020-07-20T17:02:59.668147  stern   поиграем )
2020-07-20T17:03:03.193255  professor   да ноу проб
2020-07-20T17:03:08.928615  professor   галстук красный одену значит
2020-07-20T17:03:13.363079  stern   :)
2020-07-20T17:03:18.067217  professor   задача то несложная при наличии прав
2020-07-20T17:03:27.699292  stern   таргет там собрался отдельный офис делать у себя
2020-07-20T17:03:29.380011  stern   под гос темы
2020-07-20T17:03:31.107425  stern   ем понравилась
2020-07-20T17:03:48.261911  professor   это эксклюзивно передать надо будет? или можно предложить тем кто заплатит в госах?
2020-07-20T17:04:09.948620  professor   у меня есть кое кто по внешке кто платит помимо того что пеонерить просят)))
2020-07-20T17:04:19.099657  stern   эксклюзивно желательно для начала
2020-07-20T17:04:27.917007  stern   попробовать
2020-07-20T17:04:47.624958  professor   окей, договор
2020-07-20T17:04:50.495262  stern   а те сколко платят?
2020-07-20T17:04:52.118220  stern   тебе платили?
2020-07-20T17:04:56.378572  professor   да)
2020-07-20T17:05:03.617473  professor   ну зависит от того насколько им будет интересно
2020-07-20T17:05:09.845052  stern   тогда можно у них целей 10 взят
2020-07-20T17:05:11.999936  stern   или 5
2020-07-20T17:05:14.892028  stern   точечно
2020-07-20T17:05:16.002384  stern   для таргета
2020-07-20T17:05:16.857506  stern   как раз
2020-07-20T17:05:18.545998  stern   ему интересно
2020-07-20T17:05:22.319487  professor   "не много, но типа ""все свои"""
2020-07-20T17:05:30.441540  professor   по ковиду они хотят щас очень
2020-07-20T17:05:37.757289  professor   кози медведи вон уже работают по списку
```

```
2020-07-20T17:02:13.288029  professor   what do we need from academi?
2020-07-20T17:02:25.472364  professor   is it an office request, from one of the two?
2020-07-20T17:02:26.978371  stern   replied to revers
2020-07-20T17:02:28.775027  stern   yes
2020-07-20T17:02:33.493244  professor   he brought it up
2020-07-20T17:02:33.892018  professor   what are we looking?
2020-07-20T17:02:35.227086  stern   chat
2020-07-20T17:02:39.491168  professor   are they paying or are we playing pioneers?
2020-07-20T17:02:40.613491  stern   contracts
2020-07-20T17:02:42.493082  professor   =)
2020-07-20T17:02:43.571499  stern   accounting
2020-07-20T17:02:55.596933  stern   yes fuck the money
2020-07-20T17:02:59.668147  stern   we will play )
2020-07-20T17:03:03.193255  professor   yes no probs
2020-07-20T17:03:08.928615  professor   will wear a red tie then
2020-07-20T17:03:13.363079  stern   :)
2020-07-20T17:03:18.067217  professor   the task is not that difficult if you have the rights
2020-07-20T17:03:27.699292  stern   target there has decided to build a new office at his
2020-07-20T17:03:29.380011  stern   for gov themes/topics
2020-07-20T17:03:31.107425  stern   he liked it
2020-07-20T17:03:48.261911  professor   do we need to relay it exclusively? or this can be offered to those who pay in gov?
2020-07-20T17:04:09.948620  professor   I have somebody externally who pays next to the pioneering we have been asked )))
2020-07-20T17:04:19.099657  stern   preferably exclusively at the beginning
2020-07-20T17:04:27.917007  stern   we should try to
2020-07-20T17:04:47.624958  professor   ok agreed
2020-07-20T17:04:50.495262  stern   and how much others pay?
2020-07-20T17:04:52.118220  stern   did you get paid?
2020-07-20T17:04:56.378572  professor   yes)
2020-07-20T17:05:03.617473  professor   depends on how interested they are
2020-07-20T17:05:09.845052  stern   then we can take from them 10 targets
2020-07-20T17:05:11.999936  stern   or 5
2020-07-20T17:05:14.892028  stern   appointed/specific
2020-07-20T17:05:16.002384  stern   for Target
2020-07-20T17:05:16.857506  stern   since
2020-07-20T17:05:18.545998  stern   he is interested
2020-07-20T17:05:22.319487  professor   "not much/many, but sort of ""we all know each other"""
2020-07-20T17:05:30.441540  professor   they want around covid now a lot
2020-07-20T17:05:37.757289  professor   Cozy Bears already started down the list there
```

Figure 10. Stern and Professor discussing what they need from Academi hack

It is probable that one of the two offices is a so-called ‘Bolshoy Dom’ (Big House), an office building located at 4 Liteyny Avenue which serves as the headquarters of Saint Peterburg’s local branch of FSB:

```
2020-09-28T17:42:49.518165  target  "Литейный пер. 4 - ответственный
ребята спрашивают на сколько задерживаемся, заказывать еду или нет, омар молчит"
2020-09-28T17:43:48.445641  professor   сейчас узнаю что он там пропустить мог, я такого вопроса в конфе не видел
2020-09-28T17:47:32.283551  professor   ты стерна на видел сегодня? не в курсе будет он/нет? там на мыло ответили а потом мыло абузнулось
```

```
2020-09-28T17:42:49.518165  target  "Liteyny av. 4  is in charge
the guys are asking how late we are going to be, should they order food or not, omar is not responding"
2020-09-28T17:43:48.445641  professor   will now check what he might have missed there, I did not see such a question in the conference
2020-09-28T17:47:32.283551  professor   did you see stern today? any clue whether he will be (in the office) or not? there is an email reply but the email got abused
```

Figure 11. Target to Professor mentioning FSB’s HQ address

In line with geo-political interests of Russia, Conti seems to have a ‘stop’ on China and get terrified every time they see a Russian company or ‘OOO’ abbreviation (equivalent of ‘LLC’ in CIS countries) in the list of their victims:

```
2020-09-22T19:40:24.169665  troy    RU ru.zohocorpin.com
2020-09-22T19:40:36.680502  troy    etu ne stavim
2020-09-22T19:40:40.888162  troy    udalyau
2020-09-22T19:41:53.452053  target  вот мудаки какието
2020-09-22T19:41:55.108291  target  на аусорсе
2020-09-22T19:42:07.792856  target  это зохосрм
2020-09-22T19:42:09.630565  target  пидары
2020-09-22T19:42:14.064561  target  из ру что ли какой то аутсорсер
2020-09-22T19:42:14.775342  target  мудак
2020-09-22T19:42:17.895671  target  сука
2020-09-22T19:42:24.483896  troy    pizdi dat za takoe
2020-09-22T19:42:24.592551  target  это ебануто огромная кормопрация
2020-09-22T19:42:31.803072  troy    a esli bi ya ne usledil
2020-09-22T19:42:35.091559  troy    to ebanuli bi
2020-09-22T19:42:37.159864  target  сука и надо же было чтобы этот был урод из просторов ру
2020-09-22T19:42:44.534086  target  да молодец
2020-09-22T19:42:48.278498  target  слушай ну кто знал
2020-09-22T19:42:51.807320  target  что там будет домен у них
2020-09-22T19:42:56.922116  target  из ру части в сетке
```

```
2020-09-22T19:40:24.169665  troy    RU ru.zohocorpin.com
2020-09-22T19:40:36.680502  troy    not this one
2020-09-22T19:40:40.888162  troy    removing it
2020-09-22T19:41:53.452053  target  such assholes/idiots
2020-09-22T19:41:55.108291  target  on outsource
2020-09-22T19:42:07.792856  target  this is zohoCRM
2020-09-22T19:42:09.630565  target  faggots
2020-09-22T19:42:14.064561  target  is it an outsourcer from RU
2020-09-22T19:42:14.775342  target  asshole
2020-09-22T19:42:17.895671  target  bitch
2020-09-22T19:42:24.483896  troy    they should be beaten up for such a thing
2020-09-22T19:42:24.592551  target  that is a fucking enormous corporation
2020-09-22T19:42:31.803072  troy    what if I did not notice that?
2020-09-22T19:42:35.091559  troy    then would have been fucked
2020-09-22T19:42:37.159864  target  bitch and what a chance this freak is from RU internet space
2020-09-22T19:42:44.534086  target  yeah good job!
2020-09-22T19:42:48.278498  target  listen, who would have known
2020-09-22T19:42:51.807320  target  that they would have their domain there
2020-09-22T19:42:56.922116  target  from RU part in the network
```

Figure 12. Target and Troy discovered a RU entity in their list of potential victims

```
2020-10-08T02:49:59.520966  target  "я когда увидел что в отчете там ООО какая то
у меня сердце остановилось
слава богу какой то приколист у вас ЛЛС перевел как ООО"
2020-10-08T02:53:14.963541  target  "[05:49:53] <troy> chinu ne gruzi
[05:49:58] <troy> mi ee ne stavim
что еще за сеткие"
2020-10-08T02:53:21.132783  target  конкретно о чем речь
2020-10-08T02:53:42.404395  troy    tam chisto kitay
2020-10-08T02:53:46.438901  troy    setki 3 est
2020-10-08T02:54:01.631849  target  так крупные
2020-10-08T02:54:02.414644  target  вроде
2020-10-08T02:54:04.087883  target  по 4.5 ярда
2020-10-08T02:54:04.917692  target  нет?
2020-10-08T02:54:20.639868  target  если на память
2020-10-08T02:54:31.063120  troy    da
2020-10-08T02:54:49.959573  target  стрип
2020-10-08T02:54:51.097368  target  да
2020-10-08T02:55:04.458470  target  так
2020-10-08T02:55:13.897722  target  у нас стоп на Китай?
2020-10-08T02:55:19.300923  troy    da
2020-10-08T02:56:28.762197  target  +
2020-10-08T02:56:41.504264  target  Китай +
```

```
2020-10-08T02:49:59.520966  target  "when I saw an OOO in the report
my heart stop beating
Thanks god some pranker of yours translated LLC as OOO"
2020-10-08T02:53:14.963541  target  "[05:49:53] <troy> don't load China
[05:49:58] <troy> we don't put her
what sort of networks are they"
2020-10-08T02:53:21.132783  target  what are you talking about
2020-10-08T02:53:42.404395  troy    there is purely China
2020-10-08T02:53:46.438901  troy    3 networks
2020-10-08T02:54:01.631849  target  big ones
2020-10-08T02:54:02.414644  target  I think
2020-10-08T02:54:04.087883  target  around 4.5 bln
2020-10-08T02:54:04.917692  target  no?
2020-10-08T02:54:20.639868  target  from top of my head
2020-10-08T02:54:31.063120  troy    yes
2020-10-08T02:54:49.959573  target  ctrip(corp)
2020-10-08T02:54:51.097368  target  yes
2020-10-08T02:55:04.458470  target  ok
2020-10-08T02:55:13.897722  target  do we have a stop on China?
2020-10-08T02:55:19.300923  troy    yes
2020-10-08T02:56:28.762197  target  +
2020-10-08T02:56:41.504264  target  China +
```

Figure 13. Troy confirms to Target they have a stop on China

All these messages corraborate the fact that Conti-TrickBot enterprise has a close relationship with Russian government and/or act in its interests.

Collaboration with other Malware families

Conti-Ryuk

Collaboration with Ryuk seemed to have started around August 2020 when **Stern** said, "*Ryuk is going start as of Monday.*" **Target** seemed to responsible for updating **Stern** on how the Conti-Ryuk collaboration was going and if Ryuk team is able to work together and smoothly with his team:

```
2020-08-27T15:19:36.631199  target  "по поводу рюка - на след неделе начнем и за 1-2 недели сработаются мои люди из офиса с его людьми по схеме:
чтобы делали объекты > сразу люди рюка их в рабоут брали из бк > что не так пошло или коба не погурзилась: они сразу решили ну или еще точки вход заразить какие то
начнем постепенно в таком режиме и к концу месяца с рюком устранимся от этих процессов: пусть сами мои и его взаимодействуют напрямую"
2020-08-27T15:19:36.633166  target  ну и потестируем разные сетки с ним в обороте, поймем что конкретно ему доставать лучше и из какого сектра
2020-08-27T15:19:36.636252  target  "вообщем след неделя
- рюк и наши начнут учиться взаимодействоать между собой: потихоньку начнем по немногу
- профу на его онлайн хакеров чтобы начать зарабатывать + обкатал для офис схему работы
- электрон то что просил попутно
с 10 по 20 чисел сентября
- рюк уже начнем увеличивать
- проф онлайн команде и немного офису уже делать
с 20 по 30 сентября
- рюк люди и мои старшие менеджеры сами уже взаимодействуют
- потихоньку начнем загружать офис работой  с профом"
2020-08-27T15:19:36.638663  target  "в октябре если все пойдет как планирует проф
- грузим рюку
- грузим нашим хакерам (офис)
```

```
2020-08-27T15:19:36.631199  target  "As for Ryuk - as of next week we will kick off and for 1-2 weeks my people from the office will work together with his people according to the following scheme:
in order to do the objects > immediately Ryuk's people take them from the BC (backdoor controller) to work on > if something went wrong or coba has not loaded: they immediately decide if they infect some points of access
we will start gradually in this regime and towards the end of the month Ryuk and I will remove ourselves: let my and his people to interact directly with each other"
2020-08-27T15:19:36.633166  target  and will test different networks with him in the turn, will understand in concrete terms what is easy for him to reach and from what sector
2020-08-27T15:19:36.636252  target  "to sum up the next week
- Ryuk and our people will learn how to interact with each other: will start slowly and little by little
- will give to prof for his online hackers so that they start earning + rolled out the work scheme for the office
- electron what he asked along the way
from 10 to 20 September
- will be increasing Ryuk
- will give to prof's online team and less to do for the office
from 20 to 30 September
- Ryuk's people and my senior managers are interacting on their own
- slowly will start loading the office with prof's work"
2020-08-27T15:19:36.638663  target  "in October if everything works out as per prof's plan
- will load Ryuk
- will load our hackers (office)
```

Figure 14. Conti-Ryuk initial plans on collaboration

As per the chat between **Stern**, **Target** and **Troy**, it is evident that from September 2020 to October 2020 Conti-Ryuk successfully executed attacks on Sopra Steria, Steelcase, Merieux NutriSciences and Northern Trust and received 1.5 million (currency is unknown) in ransom payments:

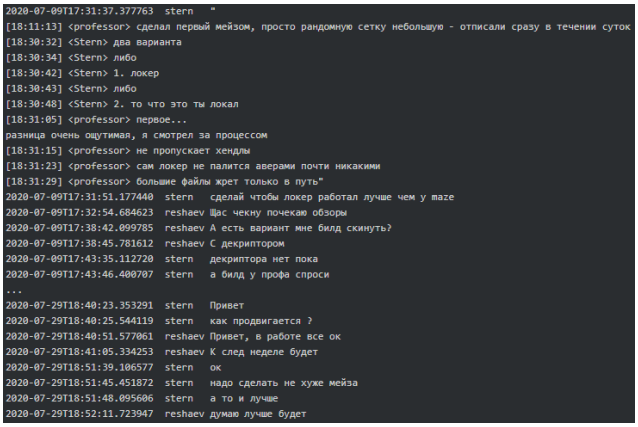
```
2020-10-23T12:37:29.772988  target  трой еще локнул 2 очень крупных конторы
2020-10-23T12:37:29.773806  target  от 1 млд
2020-10-23T12:37:29.774196  target  и 3 млрд
2020-10-23T12:37:29.811402  target  проф сказал выплатили нам 1.5 мл
2020-10-23T12:37:29.815636  target  " fx1-16 | usa | server:  1200/1200 |computer: 3000/1000+ |
memory: 380+tb | revenue: 3bill | Employees: 12000 | Website: https://www.steelcase.com/"
2020-10-23T12:37:29.816853  target  раз
2020-10-23T12:37:29.818943  target  два
2020-10-23T12:37:29.817273  target  "fx3-16 | IP: 192.168.54.6 | USA, IT, ESP | server:  702/866 |
computer: 1000+/2300 | memory: 243TB revenue: 1B | Employees: 7,000 | site: www.merieuxnutrisciences.com"
2020-10-23T12:37:29.820244  target  "FX1-10 | usaserver:5000/3000+ | comps 50000/1000+ | revenue: 9 bill
employees:50000 | website:    www.soprasteria.com | www.soprabanking.com"
2020-10-23T12:37:29.820632  target  три
2020-10-23T12:37:29.821616  target  "fx2-12 | IP: 10.1.10.250 | USA | server:  5/5 | computer: 9/9
memory: 1 TB | revenue: 6b | Employees: 19,800 Website: www.northerntrust.com"
2020-10-23T12:37:29.822791  target  ччетыре
```

```
2020-10-23T12:37:29.772988  target  troy also locked 2 very big firms
2020-10-23T12:37:29.773806  target  from 1 bln
2020-10-23T12:37:29.774196  target  and 3 bln
2020-10-23T12:37:29.811402  target  prof said they paid us 1.5 mln
2020-10-23T12:37:29.815636  target  " fx1-16 | usa | server:  1200/1200 |computer: 3000/1000+ |
memory: 380+tb | revenue: 3bill | Employees: 12000 | Website: https://www.steelcase.com/"
2020-10-23T12:37:29.816853  target  one
2020-10-23T12:37:29.818943  target  two
2020-10-23T12:37:29.817273  target  "fx3-16 | IP: 192.168.54.6 | USA, IT, ESP | server:  702/866 |
computer: 1000+/2300 | memory: 243TB revenue: 1B | Employees: 7,000 | site: www.merieuxnutrisciences.com"
2020-10-23T12:37:29.820244  target  "FX1-10 | usaserver:5000/3000+ | comps 50000/1000+ | revenue: 9 bill
employees:50000 | website:    www.soprasteria.com | www.soprabanking.com"
2020-10-23T12:37:29.820632  target  three
2020-10-23T12:37:29.821616  target  "fx2-12 | IP: 10.1.10.250 | USA | server:  5/5 | computer: 9/9
memory: 1 TB | revenue: 6b | Employees: 19,800 Website: www.northerntrust.com"
2020-10-23T12:37:29.822791  target  four
```

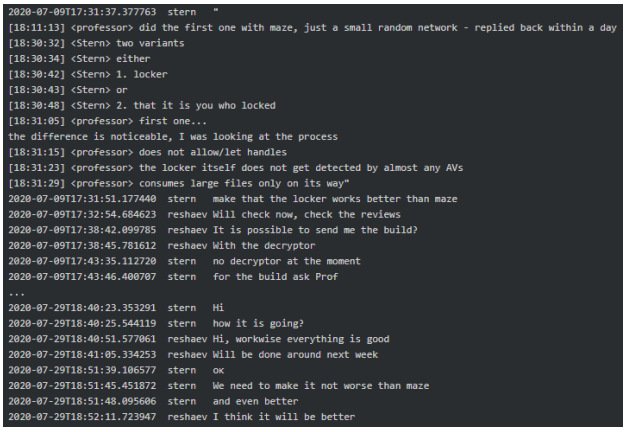
Figure 15. Potential victims of Conti-Ryuk collaboration

Conti-Maze

The first mention of Conti-Maze potential connection dates back July 2020, when **Kevin** (coder/crypter) says to **Stern** "*Prof took a different locker as far as I understood. Appears to be Maze. Said he has rolled it at night*". Then **Kevin** suggests to **Prof** (team lead/manager) that Conti-Maze negotiation should be handled by **Stern** himself as he is more experienced. He then says Maze will take 25-30%. It seems that **Prof** contacted developers of Maze and managed to get the ransomware build which was later given to Conti reversers to figure out how it works and build a locker "*not worse than Maze, and even better*":



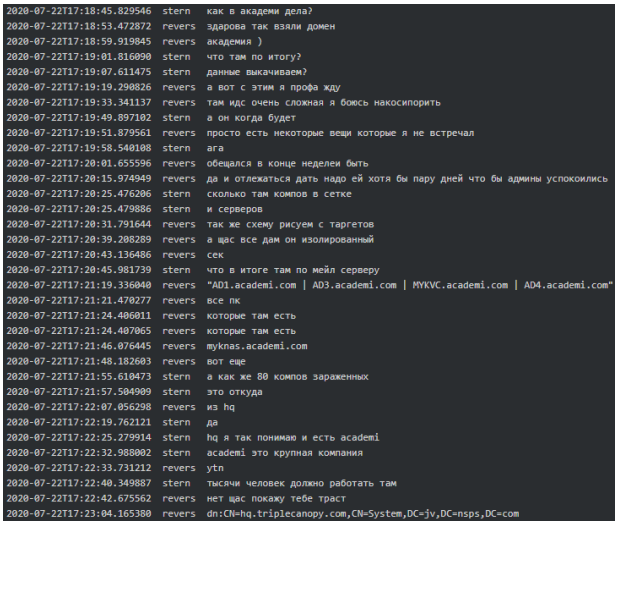
```
2020-07-09T17:31:37.377763  stern   "
[18:11:13] <professor> сделал первый мейзом, просто рандомную сетку небольшую - отписали сразу в течении суток
[18:30:32] <Stern> два варианта
[18:30:34] <Stern> либо
[18:30:42] <Stern> 1. локер
[18:30:43] <Stern> либо
[18:30:48] <Stern> 2. то что это ты локал
[18:31:05] <professor> первое...
разница очень ощутимая, я смотрел за процессом
[18:31:15] <professor> не пропускает хендлы
[18:31:23] <professor> сам локер не палится аверами почти никакими
[18:31:29] <professor> больше файлы жрет только в путь"
2020-07-09T17:31:51.177440  stern   сделай чтобы локер работал лучше чем у maze
2020-07-09T17:32:54.684623  reshaev Щас чекну почекаю обзоры
2020-07-09T17:38:42.099785  reshaev А есть вариант мне билд скинуть?
2020-07-09T17:38:45.781612  reshaev С декриптором
2020-07-09T17:43:35.112720  stern   декриптора нет пока
2020-07-09T17:43:46.400707  stern   а билд у профа спроси
...
2020-07-29T18:40:23.353291  stern   Привет
2020-07-29T18:40:25.544119  stern   как продвигается ?
2020-07-29T18:40:51.577061  reshaev Привет, в работе все ок
2020-07-29T18:41:05.334253  reshaev К след неделе будет
2020-07-29T18:51:39.106577  stern   ок
2020-07-29T18:51:45.451872  stern   надо сделать не хуже мейза
2020-07-29T18:51:48.095606  stern   а то и лучше
2020-07-29T18:52:11.723947  reshaev думаю лучше будет
```



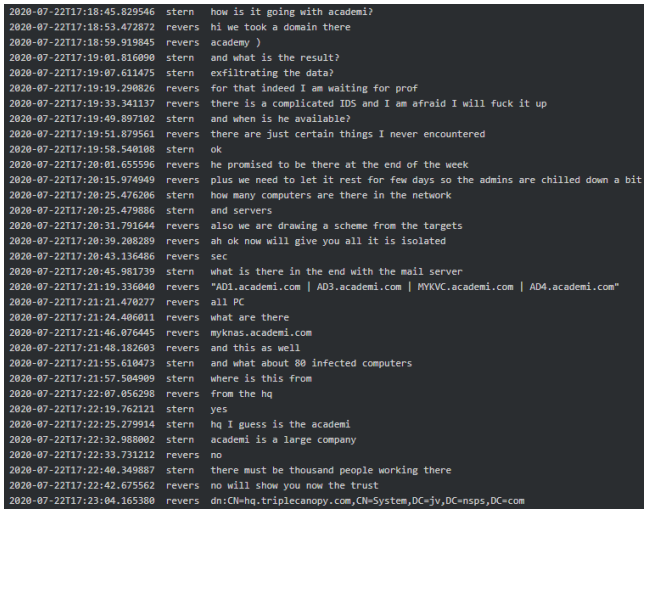
```
2020-07-09T17:31:37.377763  stern   "
[18:11:13] <professor> did the first one with maze, just a small random network - replied back within a day
[18:30:32] <Stern> two variants
[18:30:34] <Stern> either
[18:30:42] <Stern> 1. locker
[18:30:43] <Stern> or
[18:30:48] <Stern> 2. that it is you who locked
[18:31:05] <professor> first one...
the difference is noticeable, I was looking at the process
[18:31:15] <professor> does not allow/let handles
[18:31:23] <professor> the locker itself does not get detected by almost any AVs
[18:31:29] <professor> consumes large files only on its way"
2020-07-09T17:31:51.177440  stern   make that the locker works better than maze
2020-07-09T17:32:54.684623  reshaev Will check now, check the reviews
2020-07-09T17:38:42.099785  reshaev It is possible to send me the build?
2020-07-09T17:38:45.781612  reshaev With the decryptor
2020-07-09T17:43:35.112720  stern   no decryptor at the moment
2020-07-09T17:43:46.400707  stern   for the build ask Prof
...
2020-07-29T18:40:23.353291  stern   Hi
2020-07-29T18:40:25.544119  stern   how it is going?
2020-07-29T18:40:51.577061  reshaev Hi, workwise everything is good
2020-07-29T18:41:05.334253  reshaev Will be done around next week
2020-07-29T18:51:39.106577  stern   ok
2020-07-29T18:51:45.451872  stern   We need to make it not worse than maze
2020-07-29T18:51:48.095606  stern   and even better
2020-07-29T18:52:11.723947  reshaev I think it will be better
```

Figure 16. Reshaev to Stern advising a new Maze-based locker will be better than Maze

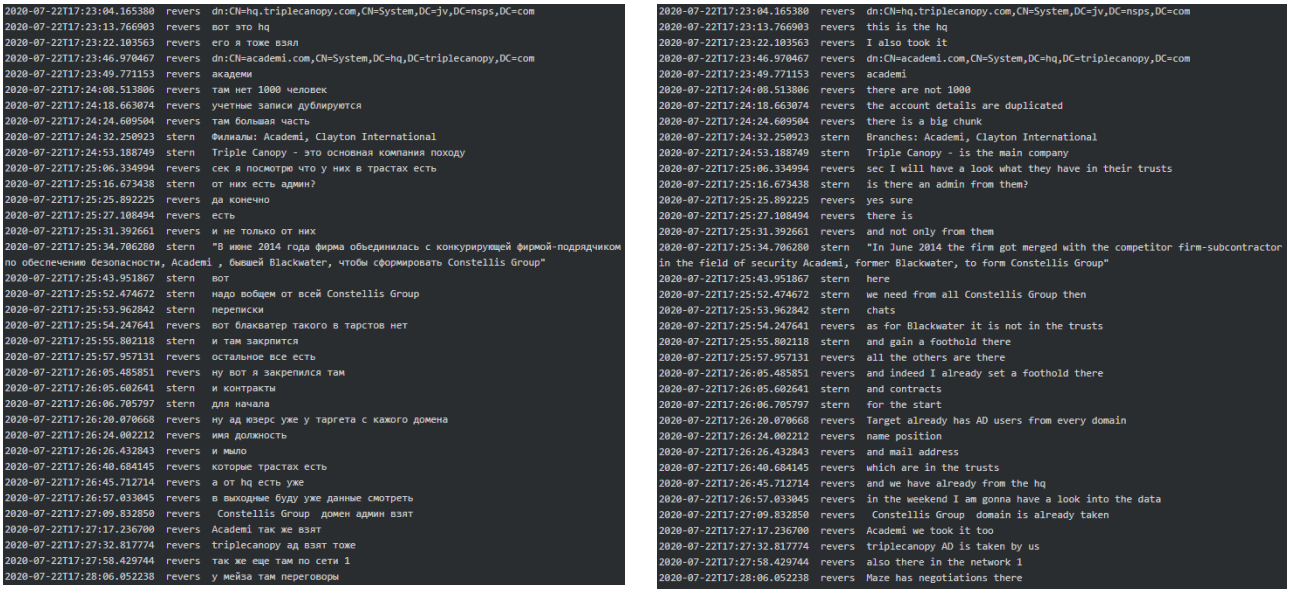
When it comes to Conti-Maze victims, it seems that both were involved in hacking Academi (former Blackwater), a U.S. private military company who provides services to CIA. "*We [expletive] Academi for almost a year*" says **Target** to **Dandis** (tester). Academi and the affiliated Triple Canopy, Olive Group Capital Ltd, Strategic Social LLC and Constellis Group were all infected/hacked around mid-July 2020 and Maze had negotiations in one of the victim's networks. **Stern** informed his subordinates that they are primarily looking for chats, contracts, PII, emails and accounting and that the request seems to be originating from one of the two 'offices' (see above, the chat where they mentioned Cozy Bear). **Target** reports to **Stern** they infected 30+ military companies along with some agencies, one of which is The US Environmental Protection Agency:



```
2020-07-22T17:18:45.829546  stern   как в академи дела?
2020-07-22T17:18:53.472872  revers  здарова так взяли домен
2020-07-22T17:18:59.919845  revers  академия )
2020-07-22T17:19:01.816090  stern   что там по итогу?
2020-07-22T17:19:07.611475  stern   данные выкачиваем?
2020-07-22T17:19:19.290826  revers  а вот с этим я профа жду
2020-07-22T17:19:33.341137  revers  там идс очень сложная я боюсь накосипорить
2020-07-22T17:19:49.897102  stern   а он когда будет
2020-07-22T17:19:51.879561  revers  просто есть некоторые вещи которые я не встречал
2020-07-22T17:19:58.540108  stern   ага
2020-07-22T17:20:01.655596  revers  обещался в конце неделеи быть
2020-07-22T17:20:15.974949  revers  да и отлежаться дать надо ей хотя бы пару дней что бы админы успокоились
2020-07-22T17:20:25.476206  stern   сколько там компов в сетке
2020-07-22T17:20:25.479886  stern   и серверов
2020-07-22T17:20:31.791644  revers  так же схему рисуем с таргетов
2020-07-22T17:20:39.208289  revers  а щас все дам он изолированный
2020-07-22T17:20:43.136486  revers  сек
2020-07-22T17:20:45.981739  stern   что в итоге там по мейл серверу
2020-07-22T17:21:19.336040  revers  "AD1.academi.com | AD3.academi.com | MYKVC.academi.com | AD4.academi.com"
2020-07-22T17:21:21.470277  revers  все пк
2020-07-22T17:21:24.406011  revers  которые там есть
2020-07-22T17:21:24.407065  revers  которые там есть
2020-07-22T17:21:46.076445  revers  myknas.academi.com
2020-07-22T17:21:48.182603  revers  вот еще
2020-07-22T17:21:55.610473  stern   а как же 80 компов зараженных
2020-07-22T17:21:57.504909  stern   это откуда
2020-07-22T17:22:07.056298  revers  из hq
2020-07-22T17:22:19.762121  stern   да
2020-07-22T17:22:25.279914  stern   hq я так понимаю и есть academi
2020-07-22T17:22:32.988002  stern   academi это крупная компания
2020-07-22T17:22:33.731212  revers  ytn
2020-07-22T17:22:40.349887  stern   тысячи человек должно работать там
2020-07-22T17:22:42.675562  revers  нет щас покажу тебе траст
2020-07-22T17:23:04.165380  revers  dn:CN=hq.triplecanopy.com,CN=System,DC=jv,DC=nsps,DC=com
```



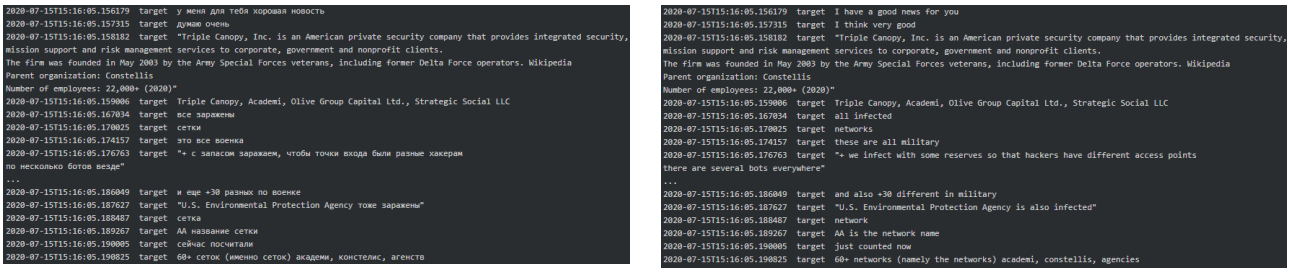
```
2020-07-22T17:18:45.829546  stern   how is it going with academi?
2020-07-22T17:18:53.472872  revers  hi we took a domain there
2020-07-22T17:18:59.919845  revers  academy )
2020-07-22T17:19:01.816090  stern   and what is the result?
2020-07-22T17:19:07.611475  stern   exfiltrating the data?
2020-07-22T17:19:19.290826  revers  for that indeed I am waiting for prof
2020-07-22T17:19:33.341137  revers  there is a complicated IDS and I am afraid I will fuck it up
2020-07-22T17:19:49.897102  stern   and when is he available?
2020-07-22T17:19:51.879561  revers  there are just certain things I never encountered
2020-07-22T17:19:58.540108  stern   ok
2020-07-22T17:20:01.655596  revers  he promised to be there at the end of the week
2020-07-22T17:20:15.974949  revers  plus we need to let it rest for few days so the admins are chilled down a bit
2020-07-22T17:20:25.476206  stern   how many computers are there in the network
2020-07-22T17:20:25.479886  stern   and servers
2020-07-22T17:20:31.791644  revers  also we are drawing a scheme from the targets
2020-07-22T17:20:39.208289  revers  ah ok now will give you all it is isolated
2020-07-22T17:20:43.136486  revers  sec
2020-07-22T17:20:45.981739  stern   what is there in the end with the mail server
2020-07-22T17:21:19.336040  revers  "AD1.academi.com | AD3.academi.com | MYKVC.academi.com | AD4.academi.com"
2020-07-22T17:21:21.470277  revers  all PC
2020-07-22T17:21:24.406011  revers  what are there
2020-07-22T17:21:46.076445  revers  myknas.academi.com
2020-07-22T17:21:48.182603  revers  and this as well
2020-07-22T17:21:55.610473  stern   and what about 80 infected computers
2020-07-22T17:21:57.504909  stern   where is this from
2020-07-22T17:22:07.056298  revers  from the hq
2020-07-22T17:22:19.762121  stern   yes
2020-07-22T17:22:25.279914  stern   hq I guess is the academi
2020-07-22T17:22:32.988002  stern   academi is a large company
2020-07-22T17:22:33.731212  revers  no
2020-07-22T17:22:40.349887  stern   there must be thousand people working there
2020-07-22T17:22:42.675562  revers  no will show you now the trust
2020-07-22T17:23:04.165380  revers  dn:CN=hq.triplecanopy.com,CN=System,DC=jv,DC=nsps,DC=com
```



```
2020-07-22T17:23:04.165380  revers  dn:CN=hq.triplecanopy.com,CN=System,DC=jv,DC=nsps,DC=com
2020-07-22T17:23:13.766903  revers  вот это hq
2020-07-22T17:23:22.103563  revers  его я тоже взял
2020-07-22T17:23:46.970467  revers  dn:CN=academi.com,CN=System,DC=hq,DC=triplecanopy,DC=com
2020-07-22T17:23:49.771153  revers  академи
2020-07-22T17:24:08.513806  revers  там нет 1000 человек
2020-07-22T17:24:18.663074  revers  учетные записи дублируются
2020-07-22T17:24:24.609504  revers  там большая часть
2020-07-22T17:24:32.250923  stern   Филиалы: Academi, Clayton International
2020-07-22T17:24:53.188749  stern   Triple Canopy - это основная компания походу
2020-07-22T17:25:06.334994  revers  сек я посмотрю что у них в трастах есть
2020-07-22T17:25:16.673438  stern   от них есть админ?
2020-07-22T17:25:25.892225  revers  да конечно
2020-07-22T17:25:27.108494  revers  есть
2020-07-22T17:25:31.392661  revers  и не только от них
2020-07-22T17:25:34.706280  stern   "В июне 2014 года фирма объединилась с конкурирующей фирмой-подрядчиком
по обеспечению безопасности, Academi , бывшей Blackwater, чтобы сформировать Constellis Group"
2020-07-22T17:25:43.951867  stern   вот
2020-07-22T17:25:52.474672  stern   надо вобщем от всей Constellis Group
2020-07-22T17:25:53.962842  stern   переписки
2020-07-22T17:25:54.247641  revers  вот блакватер такого в тарстов нет
2020-07-22T17:25:55.802118  stern   и там закрпится
2020-07-22T17:25:57.957131  revers  остальное все есть
2020-07-22T17:26:05.485851  revers  ну вот я закрепился там
2020-07-22T17:26:05.602641  stern   и контракты
2020-07-22T17:26:06.705797  stern   для начала
2020-07-22T17:26:20.070668  revers  ну ад юзерс уже у таргета с кажого домена
2020-07-22T17:26:24.002212  revers  имя должность
2020-07-22T17:26:26.432843  revers  и мыло
2020-07-22T17:26:40.684145  revers  которые трастах есть
2020-07-22T17:26:45.712714  revers  а от hq есть уже
2020-07-22T17:26:57.033045  revers  в выходные буду уже данные смотреть
2020-07-22T17:27:09.832850  revers   Constellis Group  домен админ взят
2020-07-22T17:27:17.236700  revers  Academi так же взят
2020-07-22T17:27:32.817774  revers  triplecanopy ад взят тоже
2020-07-22T17:27:58.429744  revers  так же еще там по сети 1
2020-07-22T17:28:06.052238  revers  у мейза там переговоры
```

```
2020-07-22T17:23:04.165380  revers  dn:CN=hq.triplecanopy.com,CN=System,DC=jv,DC=nsps,DC=com
2020-07-22T17:23:13.766903  revers  this is the hq
2020-07-22T17:23:22.103563  revers  I also took it
2020-07-22T17:23:46.970467  revers  dn:CN=academi.com,CN=System,DC=hq,DC=triplecanopy,DC=com
2020-07-22T17:23:49.771153  revers  academi
2020-07-22T17:24:08.513806  revers  there are not 1000
2020-07-22T17:24:18.663074  revers  the account details are duplicated
2020-07-22T17:24:24.609504  revers  there is a big chunk
2020-07-22T17:24:32.250923  stern   Branches: Academi, Clayton International
2020-07-22T17:24:53.188749  stern   Triple Canopy - is the main company
2020-07-22T17:25:06.334994  revers  sec I will have a look what they have in their trusts
2020-07-22T17:25:16.673438  stern   is there an admin from them?
2020-07-22T17:25:25.892225  revers  yes sure
2020-07-22T17:25:27.108494  revers  there is
2020-07-22T17:25:31.392661  revers  and not only from them
2020-07-22T17:25:34.706280  stern   "In June 2014 the firm got merged with the competitor firm-subcontractor
in the field of security Academi, former Blackwater, to form Constellis Group"
2020-07-22T17:25:43.951867  stern   here
2020-07-22T17:25:52.474672  stern   we need from all Constellis Group then
2020-07-22T17:25:53.962842  stern   chats
2020-07-22T17:25:54.247641  revers  as for Blackwater it is not in the trusts
2020-07-22T17:25:55.802118  stern   and gain a foothold there
2020-07-22T17:25:57.957131  revers  all the others are there
2020-07-22T17:26:05.485851  revers  and indeed I already set a foothold there
2020-07-22T17:26:05.602641  stern   and contracts
2020-07-22T17:26:06.705797  stern   for the start
2020-07-22T17:26:20.070668  revers  Target already has AD users from every domain
2020-07-22T17:26:24.002212  revers  name position
2020-07-22T17:26:26.432843  revers  and mail address
2020-07-22T17:26:40.684145  revers  which are in the trusts
2020-07-22T17:26:45.712714  revers  and we have already from the hq
2020-07-22T17:26:57.033045  revers  in the weekend I am gonna have a look into the data
2020-07-22T17:27:09.832850  revers   Constellis Group  domain is already taken
2020-07-22T17:27:17.236700  revers  Academi we took it too
2020-07-22T17:27:32.817774  revers  triplecanopy AD is taken by us
2020-07-22T17:27:58.429744  revers  also there in the network 1
2020-07-22T17:28:06.052238  revers  Maze has negotiations there
```

Figure 17. Stern and Revers's discussion around Academi hack



```
2020-07-15T15:16:05.156179  target  у меня для тебя хорошая новость
2020-07-15T15:16:05.157315  target  думаю очень
2020-07-15T15:16:05.158182  target  "Triple Canopy, Inc. is an American private security company that provides integrated security,
mission support and risk management services to corporate, government and nonprofit clients.
The firm was founded in May 2003 by the Army Special Forces veterans, including former Delta Force operators. Wikipedia
Parent organization: Constellis
Number of employees: 22,000+ (2020)"
2020-07-15T15:16:05.159006  target  Triple Canopy, Academi, Olive Group Capital Ltd., Strategic Social LLC
2020-07-15T15:16:05.167034  target  все заражены
2020-07-15T15:16:05.170025  target  сетки
2020-07-15T15:16:05.174157  target  это все военка
2020-07-15T15:16:05.176763  target  "+ с запасом заражаем, чтобы точки входа были разные хакерам
по несколько ботов везде"
...
2020-07-15T15:16:05.186049  target  и еще +30 разных по военке
2020-07-15T15:16:05.187627  target  "U.S. Environmental Protection Agency тоже заражены"
2020-07-15T15:16:05.188487  target  сетка
2020-07-15T15:16:05.189267  target  АА название сетки
2020-07-15T15:16:05.190005  target  сейчас посчитали
2020-07-15T15:16:05.190825  target  60+ сеток (именно сеток) академи, констелис, агенств
```

```
2020-07-15T15:16:05.156179  target  I have a good news for you
2020-07-15T15:16:05.157315  target  I think very good
2020-07-15T15:16:05.158182  target  "Triple Canopy, Inc. is an American private security company that provides integrated security,
mission support and risk management services to corporate, government and nonprofit clients.
The firm was founded in May 2003 by the Army Special Forces veterans, including former Delta Force operators. Wikipedia
Parent organization: Constellis
Number of employees: 22,000+ (2020)"
2020-07-15T15:16:05.159006  target  Triple Canopy, Academi, Olive Group Capital Ltd., Strategic Social LLC
2020-07-15T15:16:05.167034  target  all infected
2020-07-15T15:16:05.170025  target  networks
2020-07-15T15:16:05.174157  target  these are all military
2020-07-15T15:16:05.176763  target  "+ we infect with some reserves so that hackers have different access points
there are several bots everywhere"
...
2020-07-15T15:16:05.186049  target  and also +30 different in military
2020-07-15T15:16:05.187627  target  "U.S. Environmental Protection Agency is also infected"
2020-07-15T15:16:05.188487  target  network
2020-07-15T15:16:05.189267  target  AA is the network name
2020-07-15T15:16:05.190005  target  just counted now
2020-07-15T15:16:05.190825  target  60+ networks (namely the networks) academi, constellis, agencies
```

Figure 18. Target to Stern about 30+ military companies they infected

Conti-Netwalker

Mid-April 2021 **Stern** asked **Bentley** and **Professor** to add Netwalker's jabber account to their contact list. In mid-2020, Trellix wrote an in-depth blog on Netwalker explaining not only their malware but how we uncovered a large portion of their funds. In January 2021, Law Enforcement managed to takedown the Netwalker's dark web site and arrested an affiliate based in Canada. After these interventions, it got really quiet arround Netwalker. Given the appearance date of the Netwalker moniker within the Conti jabber server, it is possible that Netwalker affiliates found a new home within the Conti group.

According to **Stern**, **Netwalker** will use the TrickBot botnet to distribute their malware. **Bentley** was in charge of onboarding **Netwalker** to their admin panel, VNC, etc. and providing them with tested LNK/XLS files with payload to use in their campaigns. It looks like there was friction in the beginning of the collaboration and **Netwalker** did not get the promised bonus from **Stern**, and **Stern** did not like that **Netwalker** was passing the Citrix'es given to him to other parties:

```
2021-04-30T13:52:52.243054  netwalker   Arma 300k poprosil
2021-04-30T13:52:52.259520  netwalker   Ty eshe govoril nam bonus sdelaesh posle loka pervogo! O4en' v nem nujdaemysa bratishka.
2021-04-30T14:17:25.655589  netwalker   Videl 4o pisal ?
2021-04-30T15:23:32.929502  netwalker   Eshe raz priv bratish ty videl 4to pisal ?
2021-04-30T15:37:36.586261  stern   чел дал цитриксы, хорс скинул тебе, а ты другому челу который их дал в итоге) круговорот такой )
2021-04-30T15:44:47.243076  netwalker   Какой ? Щас узнаю кто по лбу получит. Ну да все ведь друг друга знают.
2021-04-30T15:45:26.281785  netwalker   Ты чекал мой спам потихоньку грузит.
2021-04-30T15:45:48.189872  stern   посмотрю сегодня
2021-04-30T17:03:11.985721  netwalker   Разобрались. Извенились все друг перед другом .
Моя вина, все хочу тебе результата больше показать т.к. без таргов сидим.
И пока все заняты разбором и выгрузкой ,попросили чела всего лишь прочекать, а он оказывается их и дал.
Смешно. Но суть никто никого обманывать не хотел это факт.  Не повториться такого никогда.
Больше чем рук целей не возьму. Выше головы прыгать не буду.
```

```
2021-04-30T13:52:52.243054  netwalker   Arma asked 300k
2021-04-30T13:52:52.259520  netwalker   You said that you will give us some bonus after the first lock! We really need it bro.
2021-04-30T14:17:25.655589  netwalker   Did you see what I wrote ?
2021-04-30T15:23:32.929502  netwalker   Again hi bro did you see what I wrote here ?
2021-04-30T15:37:36.586261  stern   a guy gave some citrix'es, hors passed them to you, and you gave it to another person from whom they actually originated from) a kind of a circle )
2021-04-30T15:44:47.243076  netwalker   What ? I will find out who gets a slap on the forehead. Although everyone anyway knows each other.
2021-04-30T15:45:26.281785  netwalker   Did you check, my spam is slowly loading.
2021-04-30T15:45:48.189872  stern   will have a look today
2021-04-30T17:03:11.985721  netwalker   We figured things out. Apologized to each other .
My bad, all I want is to show you more results cause we are sitting here without any targets.
And while everyone is busy with loading/analysing and exfiltrating, we asked the guy just to check, and he apparently passed it further.
Funny. But the truth is nobody wanted to fool anyone that is the fact.  It is not going to happen again ever.
I am not going to take more targets than the hands I have. I am not gonna jump over the head.
```

Figure 19. Initial friction between Netwalker and Stern

Later in May 2021 **Netwalker** provided **Stern** the details of their two potential victims, Blackbaud, Inc. and Ellsworth Adhesives, and asked him to pay to his team as they worked hard:

```
2021-05-21T19:40:48.232042  netwalker   "173.167.160.17 DEV1 (\\PGMDC) blackbaud.com blackbaud.com 900кк хорсику отдал в разбор
у меня все 196.155.13.118 ellsworth.com 700к заняты.
Не забудь плиз спамилке закинуть. Он так порадовал."
2021-05-21T19:53:39.872258  netwalker   Братишка прием.
2021-05-21T20:18:48.329290  netwalker   "[21:44:35] <netwalker> )> 16evvEiZ6HKkV9WAbysJfJG1Qa7DzJGUFp koshelek.
Очень прошу не забудь челику закинуть мотивацию он на славу постарался. и нужно дать ему стимула.  А то мы ему да же базу не всю оплатили бро."
2021-05-21T20:34:08.012841  stern   скинул 16тц
```

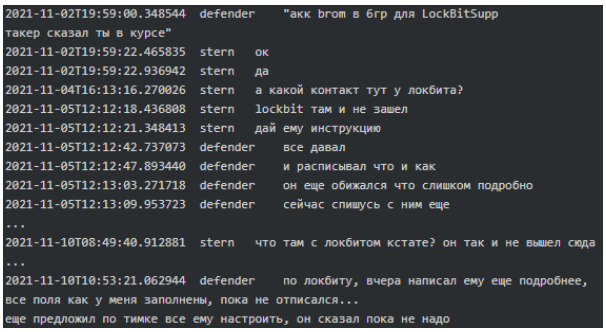
```
2021-05-21T19:40:48.232042  netwalker   "173.167.160.17 DEV1 (\\PGMDC) blackbaud.com blackbaud.com 900кк gave it to hors for further work
I have all 196.155.13.118 ellsworth.com 700k busy with.
Dont forget please to pay to spamilka. He was so joyful."
2021-05-21T19:53:39.872258  netwalker    Bro ping.
2021-05-21T20:18:48.329290  netwalker   "[21:44:35] <netwalker> )> 16evvEiZ6HKkV9WAbysJfJG1Qa7DzJGUFp wallet.
Please dont forget to send the motivation to the guy, he did his best. and we need to give him some incentive. We did not even pay him the whole base bro."
2021-05-21T20:34:08.012841  stern   sent 1BTC
```

Figure 20. Potential Conti-Netwalker victims

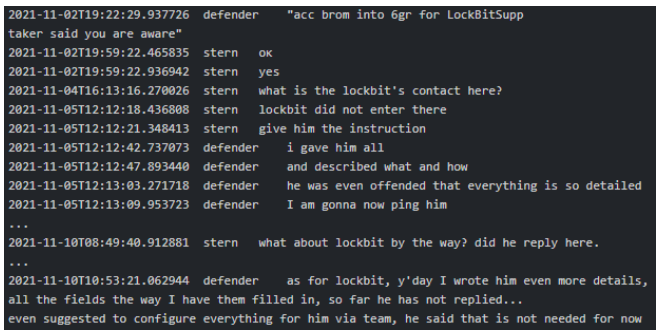
Blackbaud, Inc. disclosed that they indeed paid ransom to the perpetrators but never mentioned who they actually were nor the amount of ransom they paid.

Conti-Lockbit

There is a hint of Conti-TrickBot potentially collaborating with LockBit group. At the beginning of November 2021, **Defender** (manager) said to **Stern** that the account **Brom** was (re)created in Group 6 for LockbitSupp (an alias strongly associated with LockBit ransomware group):



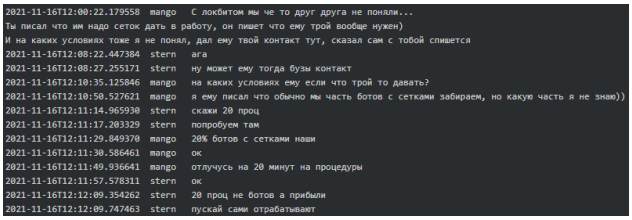
```
2021-11-02T19:59:00.348544  defender    "акк brom в 6гр для LockBitSupp
такер сказал ты в курсе"
2021-11-02T19:59:22.465835  stern   ок
2021-11-02T19:59:22.936942  stern   да
2021-11-04T16:13:16.270026  stern   а какой контакт тут у локбита?
2021-11-05T12:12:18.436808  stern   lockbit там и не зашел
2021-11-05T12:12:21.348413  stern   дай ему инструкцию
2021-11-05T12:12:42.737073  defender    все давал
2021-11-05T12:12:47.893440  defender    и расписывал что и как
2021-11-05T12:13:03.271718  defender    он еще обижался что слишком подробно
2021-11-05T12:13:09.953723  defender    сейчас спишусь с ним еще
...
2021-11-10T08:49:40.912881  stern   что там с локбитом кстате? он так и не вышел сюда
...
2021-11-10T10:53:21.062944  defender    по локбиту, вчера написал ему еще подробнее,
все поля как у меня заполнены, пока не отписался...
еще предложил по тимке все ему настроить, он сказал пока не надо
```



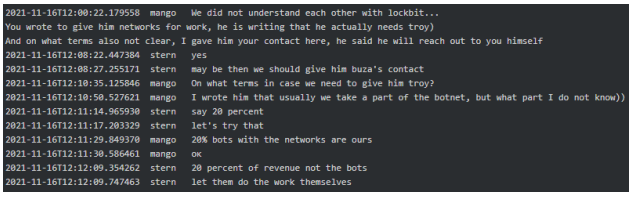
```
2021-11-02T19:22:29.937726  defender    "acc brom into 6gr for LockBitSupp
taker said you are aware"
2021-11-02T19:59:22.465835  stern   ok
2021-11-02T19:59:22.936942  stern   yes
2021-11-04T16:13:16.270026  stern   what is the lockbit's contact here?
2021-11-05T12:12:18.436808  stern   lockbit did not enter there
2021-11-05T12:12:21.348413  stern   give him the instruction
2021-11-05T12:12:42.737073  defender    i gave him all
2021-11-05T12:12:47.893440  defender    and described what and how
2021-11-05T12:13:03.271718  defender    he was even offended that everything is so detailed
2021-11-05T12:13:09.953723  defender    I am gonna now ping him
...
2021-11-10T08:49:40.912881  stern   what about lockbit by the way? did he reply here.
...
2021-11-10T10:53:21.062944  defender    as for lockbit, y'day I wrote him even more details,
all the fields the way I have them filled in, so far he has not replied...
even suggested to configure everything for him via team, he said that is not needed for now
```

Figure 21. Defender advising to Stern he added LockBitSupp to their Jabber

Two weeks after, **Mango** (team lead/manager) told **Stern** that there was misunderstanding with LockBit and asked him about the percentage of networks and revenue they will take from LockBit in case of successful collaboration:



```
2021-11-16T12:00:22.179558  mango   С локбитом мы че то друг друга не поняли...
Ты писал что им надо сеток дать в работу, он пишет что ему трой вообще нужен)
И на каких условиях тоже я не понял, дал ему твой контакт тут, сказал сам с тобой спишется
2021-11-16T12:08:22.447384  stern   ага
2021-11-16T12:08:27.255171  stern   ну может ему тогда бузы контакт
2021-11-16T12:10:35.125846  mango   на каких условиях ему если что трой то давать?
2021-11-16T12:10:50.527621  mango   я ему писал что обычно мы часть ботов с сетками забираем, но какую часть я не знаю))
2021-11-16T12:11:14.965930  stern   скажи 20 проц
2021-11-16T12:11:17.203329  stern   попробуем там
2021-11-16T12:11:29.849370  mango   20% ботов с сетками наши
2021-11-16T12:11:30.586461  mango   ок
2021-11-16T12:11:49.936641  mango   отлучусь на 20 минут на процедуры
2021-11-16T12:11:57.578311  stern   ок
2021-11-16T12:12:09.354262  stern   20 проц не ботов а прибыли
2021-11-16T12:12:09.747463  stern   пускай сами отрабатывают
```

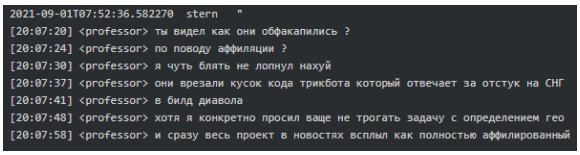


```
2021-11-16T12:00:22.179558  mango   We did not understand each other with lockbit...
You wrote to give him networks for work, he is writing that he actually needs troy)
And on what terms also not clear, I gave him your contact here, he said he will reach out to you himself
2021-11-16T12:08:22.447384  stern   yes
2021-11-16T12:08:27.255171  stern   may be then we should give him buza's contact
2021-11-16T12:10:35.125846  mango   On what terms in case we need to give him troy?
2021-11-16T12:10:50.527621  mango   I wrote him that usually we take a part of the botnet, but what part I do not know))
2021-11-16T12:11:14.965930  stern   say 20 percent
2021-11-16T12:11:17.203329  stern   let's try that
2021-11-16T12:11:29.849370  mango   20% bots with the networks are ours
2021-11-16T12:11:30.586461  mango   ok
2021-11-16T12:12:09.354262  stern   20 percent of revenue not the bots
2021-11-16T12:12:09.747463  stern   let them do the work themselves
```

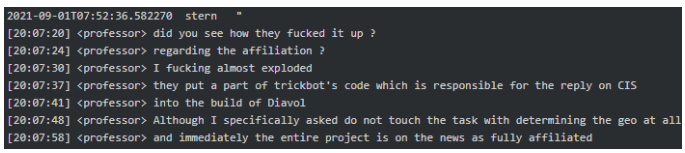
Figure 22. Stern to Mango on percentage of revenue they take from Conti-LockBit collaboration

TrickBot, Buer, Amadey and IcedID

On June 26, 2020, **Taker** (tester) who just began the conversation with **Stern** asked questions around what TrickBot was and how it got started. "*It started as a banking bot, gathering logs, logins, and passwords. It was a financial matter*" replied **Stern**. Later in October 2020, **Target** said to **Troy**, "*They managed to connect Cobalt, Bazar and TrickBot together. They figured that TrickBot is us.*" On the August 19, 2021, **Professor** got furious when somebody mistakenly included the TrickBot module designed to not infect CIS countries into Diavol ransomware (aka Conti) build, which allowed security researchers to attribute TrickBot and Conti teams to the same threat actor:



```
2021-09-01T07:52:36.582270  stern   "
[20:07:20] <professor> ты видел как они обфакапились ?
[20:07:24] <professor> по поводу аффиляции ?
[20:07:30] <professor> я чуть блять не лопнул нахуй
[20:07:37] <professor> они врезали кусок кода трикбота который отвечает за отстук на СНГ
[20:07:41] <professor> в билд диавола
[20:07:48] <professor> хотя я конкретно просил ваще не трогать задачу с определением гео
[20:07:58] <professor> и сразу весь проект в новостях всплыл как полностью аффилированный
```



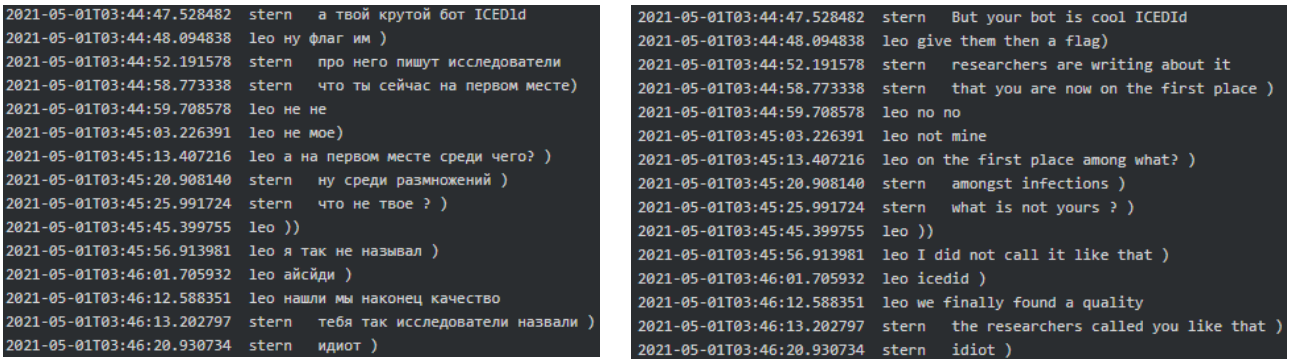
```
2021-09-01T07:52:36.582270  stern   "
[20:07:20] <professor> did you see how they fucked it up ?
[20:07:24] <professor> regarding the affiliation ?
[20:07:30] <professor> I fucking almost exploded
[20:07:37] <professor> they put a part of trickbot's code which is responsible for the reply on CIS
[20:07:41] <professor> into the build of Diavol
[20:07:48] <professor> Although I specifically asked do not touch the task with determining the geo at all
[20:07:58] <professor> and immediately the entire project is on the news as fully affiliated
```

Figure 23. Professor advising Stern TrickBot module was added into Conti ransomware build

Amadey and Buer were also mentioned multiple time in Conti chats as alternative loaders. In June 2020, **Price** (coder) said to **Target**, "*Hof referred me to a hacker forum, I got access to it (for money) and copied Buer's entire ins and outs from there.*" As for Amadey loader, it

looks that Conti team bought it and every time Amadey required a ‘re-crypt’ they would pay for that.

Furthermore, **Leo** (coder) from Conti gang appears to be the creator of IcedID loader which in May 2021 was ‘on the first place among infections’:



```
2021-05-01T03:44:47.528482  stern   а твой крутой бот ICEDId
2021-05-01T03:44:48.094838  leo ну флаг им )
2021-05-01T03:44:52.191578  stern   про него пишут исследователи
2021-05-01T03:44:58.773338  stern   что ты сейчас на первом месте)
2021-05-01T03:44:59.708578  leo не не
2021-05-01T03:45:03.226391  leo не мое)
2021-05-01T03:45:13.407216  leo а на первом месте среди чего? )
2021-05-01T03:45:20.908140  stern   ну среди размножений )
2021-05-01T03:45:25.991724  stern   что не твое ? )
2021-05-01T03:45:45.399755  leo ))
2021-05-01T03:45:56.913981  leo я так не называл )
2021-05-01T03:46:01.705932  leo айсйди )
2021-05-01T03:46:12.588351  leo нашли мы наконец качество
2021-05-01T03:46:13.202797  stern   тебя так исследователи назвали )
2021-05-01T03:46:20.930734  stern   идиот )
```

```
2021-05-01T03:44:47.528482  stern   But your bot is cool ICEDId
2021-05-01T03:44:48.094838  leo give them then a flag)
2021-05-01T03:44:52.191578  stern   researchers are writing about it
2021-05-01T03:44:58.773338  stern   that you are now on the first place )
2021-05-01T03:44:59.708578  leo no no
2021-05-01T03:45:03.226391  leo not mine
2021-05-01T03:45:13.407216  leo on the first place among what? )
2021-05-01T03:45:20.908140  stern   amongst infections )
2021-05-01T03:45:25.991724  stern   what is not yours ? )
2021-05-01T03:45:45.399755  leo ))
2021-05-01T03:45:56.913981  leo I did not call it like that )
2021-05-01T03:46:01.705932  leo icedid )
2021-05-01T03:46:12.588351  leo we finally found a quality
2021-05-01T03:46:13.202797  stern   the researchers called you like that )
2021-05-01T03:46:20.930734  stern   idiot )
```

Figure 24. Leo is the creator of IcedID malware

Conti’s victims: NGO, Medical institutions among others

We went through the Conti leaked messages and compiled a list of their potential victims which mainly includes EU and U.S. entities across various sectors. Most of the 103 potential victims we have identified were located via a Zoominfo URL Conti used to check a company’s size and revenue to determine a ransom amount to ask. “*Found a way of buying a Zoominfo account, 2 managers for Buza, for his pricing research, the price is 2k*” advised **Mango** to **Stern**. Later **Stern** said to **Mavelek** (coder/tester), “*@ali has a script to check domains on Zoominfo to get data on number of employees and the revenue of the company.*”

Between 2020-2022 Conti and its affiliates targeted and potentially attacked twelve healthcare organizations (clinics, hospitals, care houses including UHS, Prodemica, Geo Group), five educational institutions (schools, colleges, universities, etc.), a charitable organization, a governmental agency, and numerous companies in financial, retail, business services, manufacturing, and other industries:

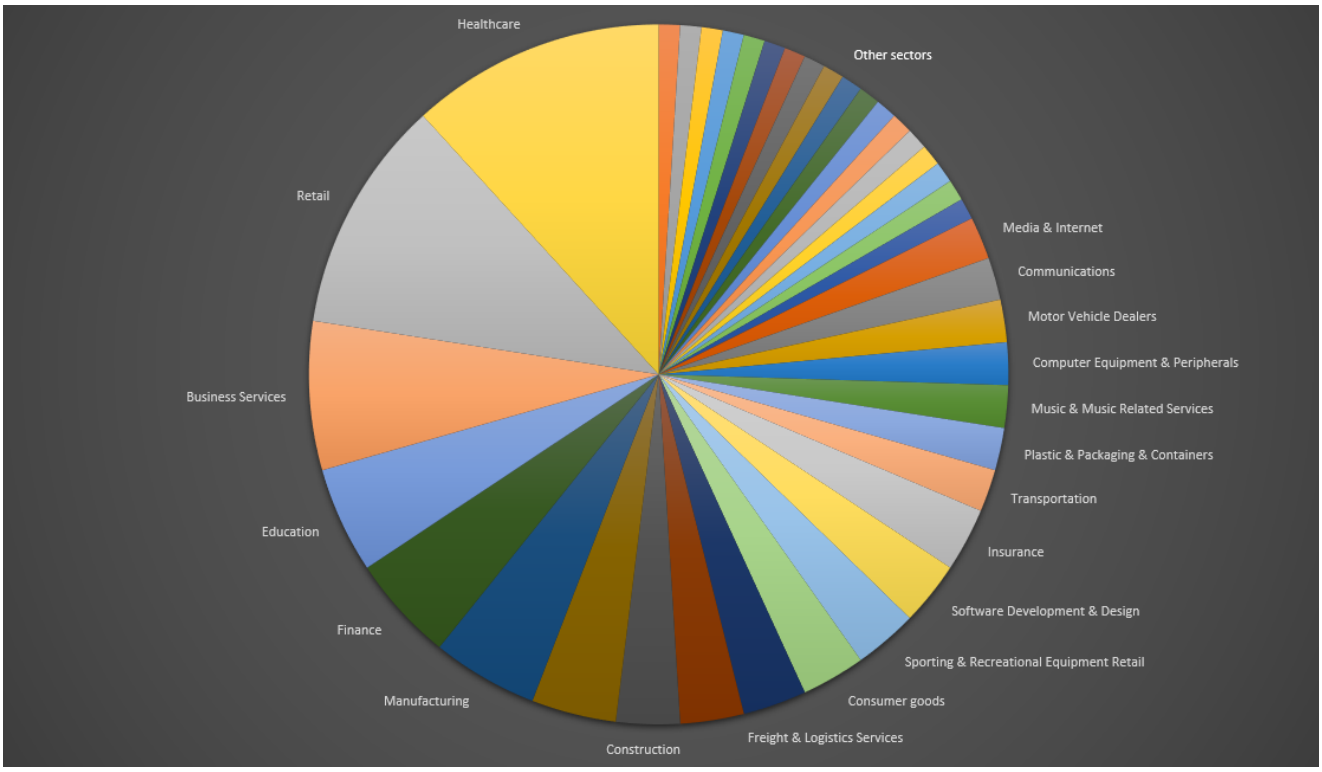
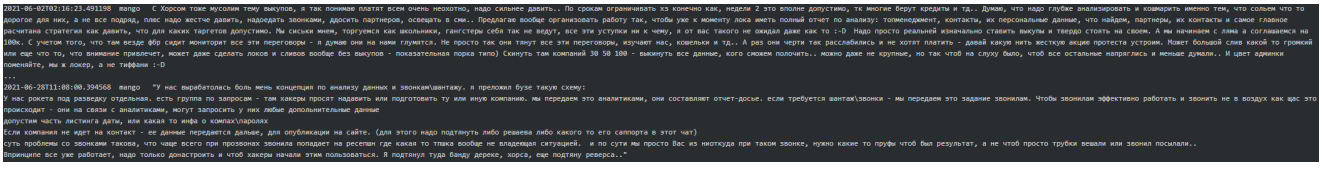


Figure 25. The chart gives an overview of the Conti's potential victims by sector
Call center services

Among other departments, Conti has a team of callers. A caller is required to have a good knowledge of spoken English (level B2-C1) and between age 18 and 25. They are recruited by Conti's HR team to work remotely for 'an online store' abroad. The callers earn $450-500 a month (salary increases by $100 - $200 - $300, depending on the success of the call-centre), working hours are 18:00-2:00 Moscow time (correspond to usual working hours in Western hemisphere), and they receive paid holidays but get no official contract as per the Labour Code.

Below are **Mango**'s messages to **Stern** where he suggests some improvements around blackmailing/call-center and explains a concept which is 'more or less' working for them:



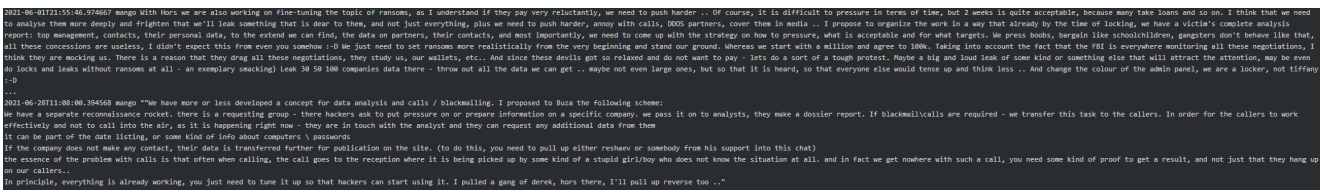


Figure 26. Mango's vision on how their call center should operate

Here is a call sample from Conti's caller to one of their victims, curtesy of Northwave Security:

Conti call sample.mp3

Your browser does not support the `audio` element.

Cybercriminal entrepreneurship (crypto and Forum)

By end of May 2021 **Stern** instructed **Mango** to get in touch with the administrators of exploit forums to see if they were willing to sell to Conti. "*Also get a list of forums which can be considered for sale. XSS - find out a list of active users, per day, week, month. The same for Antichat and WWH,*" continued **Stern**. Later **Mango** replied that WWH had laughed out loud at their offer and that hxxp://korovka32xc3t5cg[.]onion and hxxp://crdclub4wraumez4[.]onion were available for sale. However, he advised those forums are rubbish, a hotbed of grifters, and instead of trying to buy a forum they should create one on their own. The following is **Mango**'s suggestion to which he got a 'go-ahead' from **Stern**:

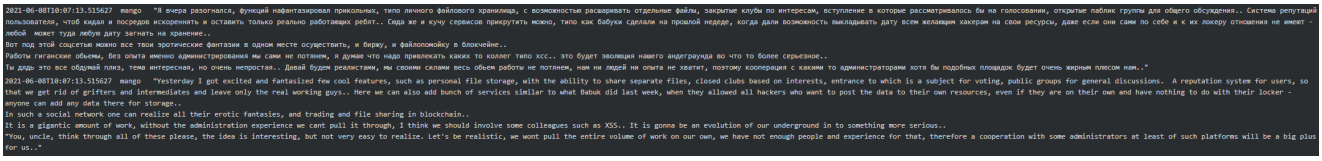


Figure 27. Mango to Stern on their new hacker forum and it's functionalities

In July 2021, **Mango** sent two design suggestions for the social network (aka forum) to **Stern** – one in dark-green and another in dark-blue color schemes. **Stern** approved the dark-green variant for the forum and suggested it was ready to make it available with a minimum functionality:

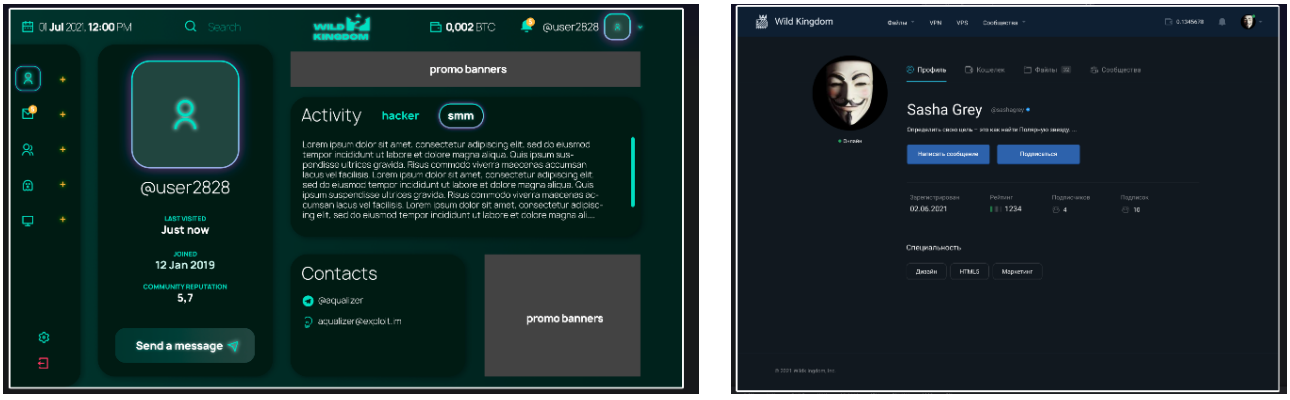
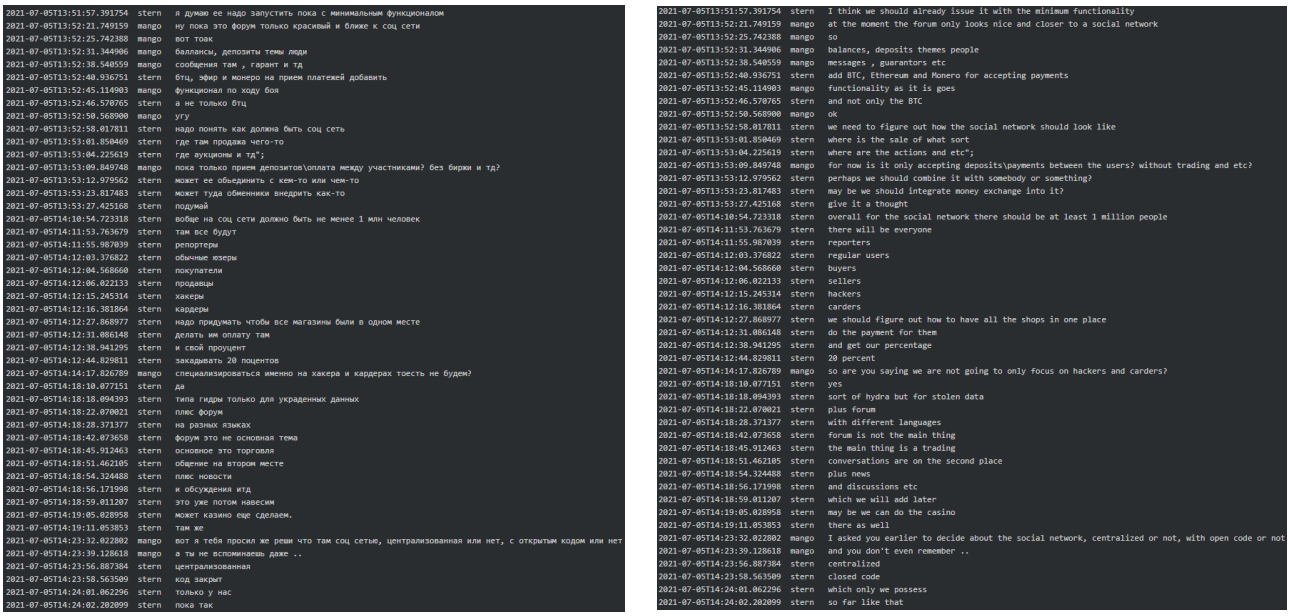


Figure 28. Two design suggestions for the hacker forum

Below are the conversation extracts between **Stern** and **Mango**, full of entrepreneurial spirit, where they brainstorm what functionalities the forum should have and what might potentially work for it and what might not:



2021-07-05T13:51:57.391754 stern я думаю ее надо запустить пока с минимальным функционалом
2021-07-05T13:52:21.749159 mango ну пока это форум только красивый и ближе к соц сети
2021-07-05T13:52:25.742388 mango вот тоак
2021-07-05T13:52:31.344906 mango балланс, депозиты темы люди
2021-07-05T13:52:38.540559 mango сообщения там , гарант и тд
2021-07-05T13:52:40.936751 stern бтц, эфир и монеро на прием платежей добавить
2021-07-05T13:52:45.114903 mango функционал по ходу боя
2021-07-05T13:52:46.570765 stern а не только бтц
2021-07-05T13:52:50.568900 mango угу
2021-07-05T13:52:58.017811 stern надо понять как должна быть соц сеть
2021-07-05T13:53:01.850469 stern где там продажа чего-то
2021-07-05T13:53:04.225619 stern где аукционы и тд";
2021-07-05T13:53:09.849748 mango пока только прием депозитов\оплата между участниками? без биржи и тд?
2021-07-05T13:53:12.979562 stern может ее объединить с кем-то или чем-то
2021-07-05T13:53:23.817483 stern может туда обменники внедрить как-то
2021-07-05T13:53:27.425168 stern подумай
2021-07-05T14:10:54.723318 stern вобще на соц сети должно быть не менее 1 млн человек
2021-07-05T14:11:53.763679 stern там все будут
2021-07-05T14:11:55.987039 stern репортеры
2021-07-05T14:12:03.376822 stern обычные юзеры
2021-07-05T14:12:04.568660 stern покупатели
2021-07-05T14:12:06.022133 stern продавцы
2021-07-05T14:12:15.245314 stern хакеры
2021-07-05T14:12:16.381864 stern кардеры
2021-07-05T14:12:27.868977 stern надо придумать чтобы все магазины были в одном месте
2021-07-05T14:12:31.086148 stern делать им оплату там
2021-07-05T14:12:38.941295 stern и свой проуцент
2021-07-05T14:12:44.829811 stern закадывать 20 поцентов
2021-07-05T14:14:17.826789 mango специализироваться именно на хакера и кардерах тоесть не будем?
2021-07-05T14:18:10.077151 stern да
2021-07-05T14:18:18.094393 stern типа гидры только для украденных данных
2021-07-05T14:18:22.070021 stern плюс форум
2021-07-05T14:18:28.371377 stern на разных языках
2021-07-05T14:18:42.073658 stern форум это не основная тема
2021-07-05T14:18:45.912463 stern основное это торговля
2021-07-05T14:18:51.462105 stern общение на втором месте
2021-07-05T14:18:54.324488 stern плюс новости
2021-07-05T14:18:56.171998 stern и обсуждения итд
2021-07-05T14:18:59.011207 stern это уже потом навесим
2021-07-05T14:19:05.028958 stern может казино еще сделаем.
2021-07-05T14:19:11.053853 stern там же
2021-07-05T14:23:32.022802 mango вот я тебя просил же реши что там соц сетью, централизованная или нет, с открытым кодом или нет
2021-07-05T14:23:39.128618 mango а ты не вспоминаешь даже ..
2021-07-05T14:23:56.887384 stern централизованная
2021-07-05T14:23:58.563509 stern код закрыт
2021-07-05T14:24:01.062296 stern только у нас
2021-07-05T14:24:02.202099 stern пока так

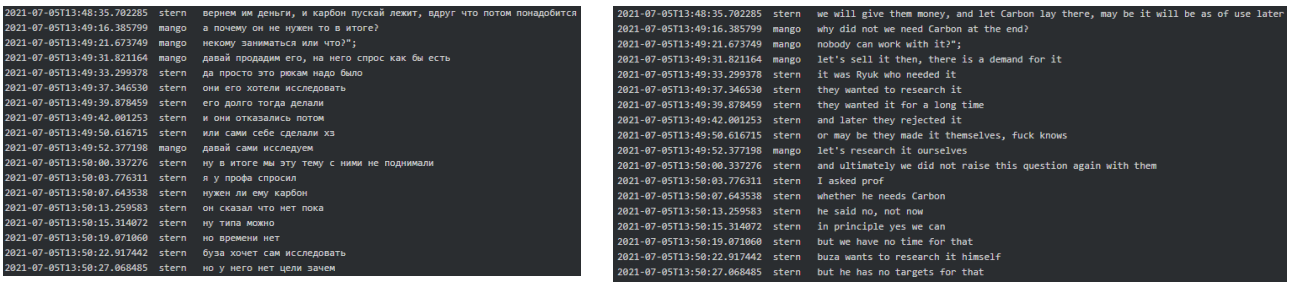
2021-07-05T13:51:57.391754 stern I think we should already issue it with the minimum functionality
2021-07-05T13:52:21.749159 mango at the moment the forum only looks nice and closer to a social network
2021-07-05T13:52:25.742388 mango so
2021-07-05T13:52:31.344906 mango balances, deposits themes people
2021-07-05T13:52:38.540559 mango messages , guarantors etc
2021-07-05T13:52:40.936751 stern add BTC, Ethereum and Monero for accepting payments
2021-07-05T13:52:45.114903 mango functionality as it is goes
2021-07-05T13:52:46.570765 stern and not only the BTC
2021-07-05T13:52:50.568900 mango ok
2021-07-05T13:52:58.017811 stern we need to figure out how the social network should look like
2021-07-05T13:53:01.850469 stern where is the sale of what sort
2021-07-05T13:53:04.225619 stern where are the actions and etc";
2021-07-05T13:53:09.849748 mango for now is it only accepting deposits\payments between the users? without trading and etc?
2021-07-05T13:53:12.979562 stern perhaps we should combine it with somebody or something?
2021-07-05T13:53:23.817483 stern may be we should integrate money exchange into it?
2021-07-05T13:53:27.425168 stern give it a thought
2021-07-05T14:10:54.723318 stern overall for the social network there should be at least 1 million people
2021-07-05T14:11:53.763679 stern there will be everyone
2021-07-05T14:11:55.987039 stern reporters
2021-07-05T14:12:03.376822 stern regular users
2021-07-05T14:12:04.568660 stern buyers
2021-07-05T14:12:06.022133 stern sellers
2021-07-05T14:12:15.245314 stern hackers
2021-07-05T14:12:16.381864 stern carders
2021-07-05T14:12:27.868977 stern we should figure out how to have all the shops in one place
2021-07-05T14:12:31.086148 stern do the payment for them
2021-07-05T14:12:38.941295 stern and get our percentage
2021-07-05T14:12:44.829811 stern 20 percent
2021-07-05T14:14:17.826789 mango so are you saying we are not going to only focus on hackers and carders?
2021-07-05T14:18:10.077151 stern yes
2021-07-05T14:18:18.094393 stern sort of hydra but for stolen data
2021-07-05T14:18:22.070021 stern plus forum
2021-07-05T14:18:28.371377 stern with different languages
2021-07-05T14:18:42.073658 stern forum is not the main thing
2021-07-05T14:18:45.912463 stern the main thing is a trading
2021-07-05T14:18:51.462105 stern conversations are on the second place
2021-07-05T14:18:54.324488 stern plus news
2021-07-05T14:18:56.171998 stern and discussions etc
2021-07-05T14:18:59.011207 stern which we will add later
2021-07-05T14:19:05.028958 stern may be we can do the casino
2021-07-05T14:19:11.053853 stern there as well
2021-07-05T14:23:32.022802 mango I asked you earlier to decide about the social network, centralized or not, with open code or not
2021-07-05T14:23:39.128618 mango and you don't even remember ..
2021-07-05T14:23:56.887384 stern centralized
2021-07-05T14:23:58.563509 stern closed code
2021-07-05T14:24:01.062296 stern which only we possess
2021-07-05T14:24:02.202099 stern so far like that

Figure 29. Mango and Stern discussing their new hacker forum

Later **Mango** suggested a potential domain for the forum and a logo for it: "*matryoshka[.]space (already with the domain:)) and as a logo matryoshka but angry, in our color scheme, dark-green, and may be draw a laptop next to it. In principle matches the theme. We are one big system amongst the multiple other sub-systems in one place. And it is clear that it is a Russian theme. It is going to be cool, and easy to remember, I think it will resonate with everyone*".

Purchase of Carbon Black and SonicWall

In March 2021 **Stern** said to **Defender** that he needs Carbon Black AV. In April 2021 **Mango** asked **Professor** if 60k (currency is unknown) is a lot for Carbon, 30k for the firm who buys and 30k for the Carbon itself for 250 PCs. A week later it seems that **Mango** managed to purchase Carbon Black via a firm in France for 14.8k euros (plus 20% for BTC conversion and 30k for the firm as promised). However, **Stern** did not take Carbon Black AV and in July 2021 **Mango** asked him why they aren't doing anything with Carbon Black to which **Stern** replied that originally Ryuk needed it and now for some reason they no longer do:

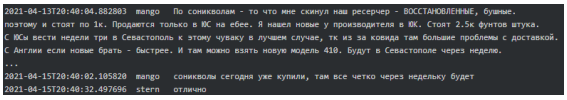


2021-07-05T13:48:35.702285 stern вернем им деньги, и карбон пускай лежит, вдруг что потом понадобится
2021-07-05T13:49:16.385799 mango а почему он не нужен то в итоге?
2021-07-05T13:49:21.673749 mango некому заниматься или что?";
2021-07-05T13:49:31.821164 mango давай продадим его, на него спрос как бы есть
2021-07-05T13:49:33.299378 stern да просто это рукам надо было
2021-07-05T13:49:37.346530 stern они его хотели исследовать
2021-07-05T13:49:39.878459 stern его долго тогда делали
2021-07-05T13:49:42.001253 stern и они отказались потом
2021-07-05T13:49:50.616715 stern или сами себе сделали хз
2021-07-05T13:49:52.377198 mango давай сами исследуем
2021-07-05T13:50:00.337276 stern ну в итоге мы эту тему с ними не поднимали
2021-07-05T13:50:03.776311 stern я у профа спросил
2021-07-05T13:50:07.643538 stern нужен ли ему карбон
2021-07-05T13:50:13.259583 stern он сказал что нет пока
2021-07-05T13:50:15.314072 stern ну типа можно
2021-07-05T13:50:19.071060 stern но времени нет
2021-07-05T13:50:22.917442 stern буза хочет сам исследовать
2021-07-05T13:50:27.068485 stern но у него нет цели зачем

2021-07-05T13:48:35.702285 stern we will give them money, and let Carbon lay there, may be it will be as of use later
2021-07-05T13:49:16.385799 mango why did not we need Carbon at the end?
2021-07-05T13:49:21.673749 mango nobody can work with it?";
2021-07-05T13:49:31.821164 mango let's sell it then, there is a demand for it
2021-07-05T13:49:33.299378 stern it was Ryuk who needed it
2021-07-05T13:49:37.346530 stern they wanted to research it
2021-07-05T13:49:39.878459 stern they wanted it for a long time
2021-07-05T13:49:42.001253 stern and later they rejected it
2021-07-05T13:49:50.616715 stern or may be they made it themselves, fuck knows
2021-07-05T13:49:52.377198 mango let's research it ourselves
2021-07-05T13:50:00.337276 stern and ultimately we did not raise this question again with them
2021-07-05T13:50:03.776311 stern I asked prof
2021-07-05T13:50:07.643538 stern whether he needs Carbon
2021-07-05T13:50:13.259583 stern he said no, not now
2021-07-05T13:50:15.314072 stern in principle yes we can
2021-07-05T13:50:19.071060 stern but we have no time for that
2021-07-05T13:50:22.917442 stern buza wants to research it himself
2021-07-05T13:50:27.068485 stern but he has no targets for that

Figure 30. Stern advising to Mango Carbon Black AV was bought for Ryuk team

In February 2021 **Stern** said to **Swift** (tester/coder) that he also needs SonicWall solution. He broadcast to all the contacts in Jabber “Who can figure out the vulnerability in SonicWall and make a working scanner for it?” to which **Ghost** (tester/coder) replied “*This one, CVE-2020-5135: Critical SonicWall VPN Portal Stack-based Buffer Overflow Vulnerability, right?*”. The CVE-2020-5135 is a CVSSv3 9.4/10 critical vulnerability which was fixed around November 2020 and according to SonicWall PSIRT there was no exploitation observed in the wild. Mid-April 2021 **Mango** advised **Stern** there are several ways to buy SonicWall (even a new model SMA 410) and later that they manage to buy new as well as refurbished ones:



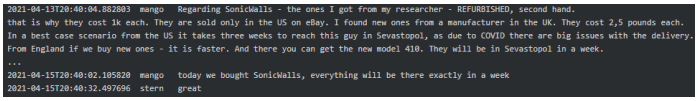


Figure 31. Mango to Stern on the purchase of SonicWall

There is not much further information regarding SonicWall, except that in June 2021 **Subzero** (tester/coder) advised to **Stern** that he “*figured out the SonicWall*”.

Conclusion

Financially motivated cyber criminals have a history of collaboration across borders and often stay away from politics. However, the current Russia-Ukraine conflict isn’t one to ignore, not even for cybercriminals, as they are forced to choose sides.

The ContiLeaks and TrickBotLeaks were a direct result of this conflict. The leaks are of an unprecedented level and show the world how a government backed, multimillion-dollar ransomware gang operates. In some fashion it was almost like a normal business; wages needed to be paid, software licenses obtained, customer service initiated, and strategic alliances had to be formed. However, make no mistake, this business is dealing in top level cybercrime, with a strategic alliance to an intelligence apparatus responsible for several nation-state attacks.

In our line of work, we are often aware of technical innerworkings, partnerships between malware families and suspected nation state relationships but reading the internal conversations and having our suspicions confirmed was very insightful.