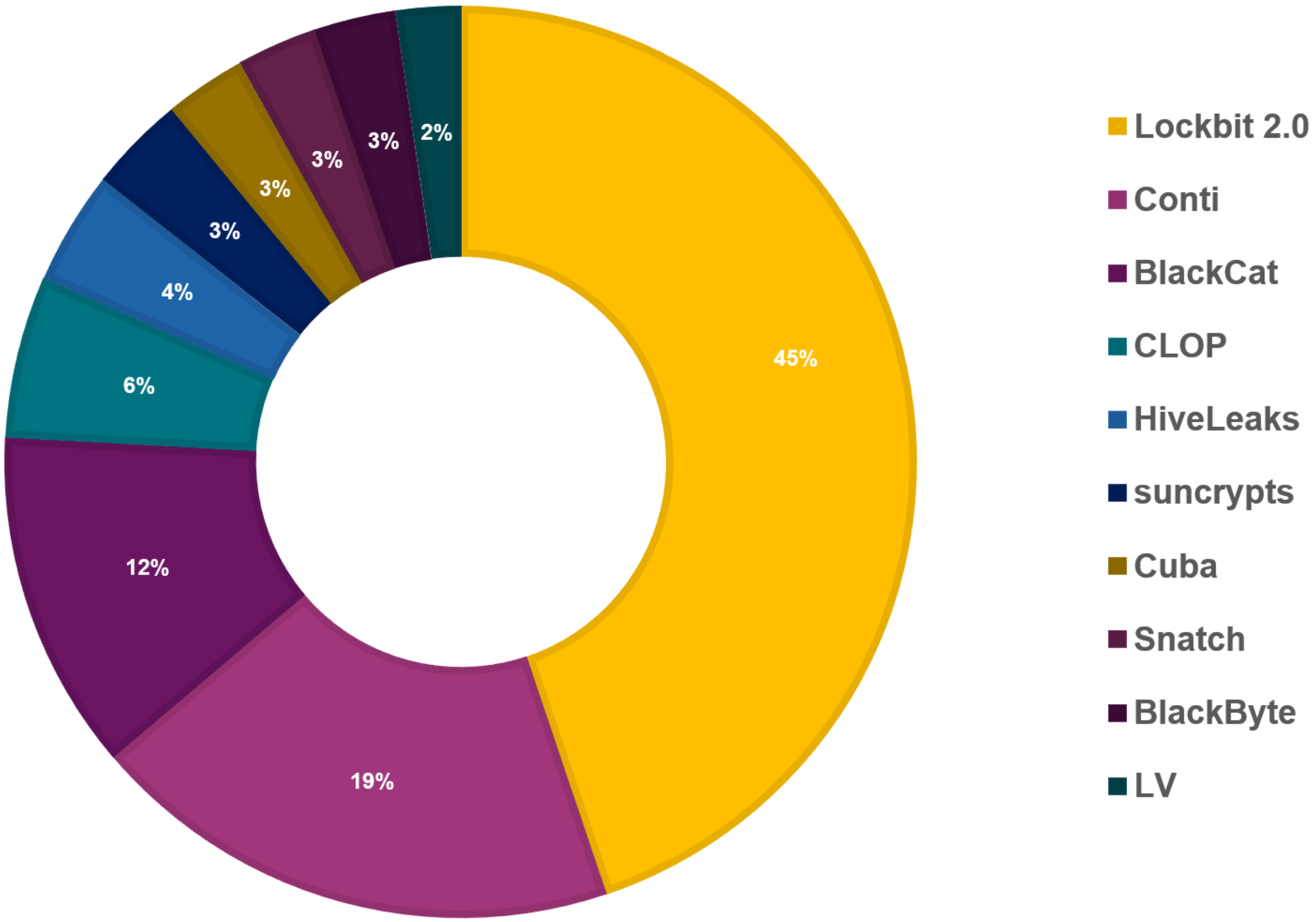
Monthly Threat Pulse February 2022

We are continuing to track ransomware groups operating the hack and leak double extortion tactic, this is achieved by actively monitoring the leak sites used by each ransomware group and scraping victim details as they are released.

By recording this data and classifying the victims by sector, we are able to derive additional insights such as, which sectors are being targeted this last month, and how do these insights compare to previous months?

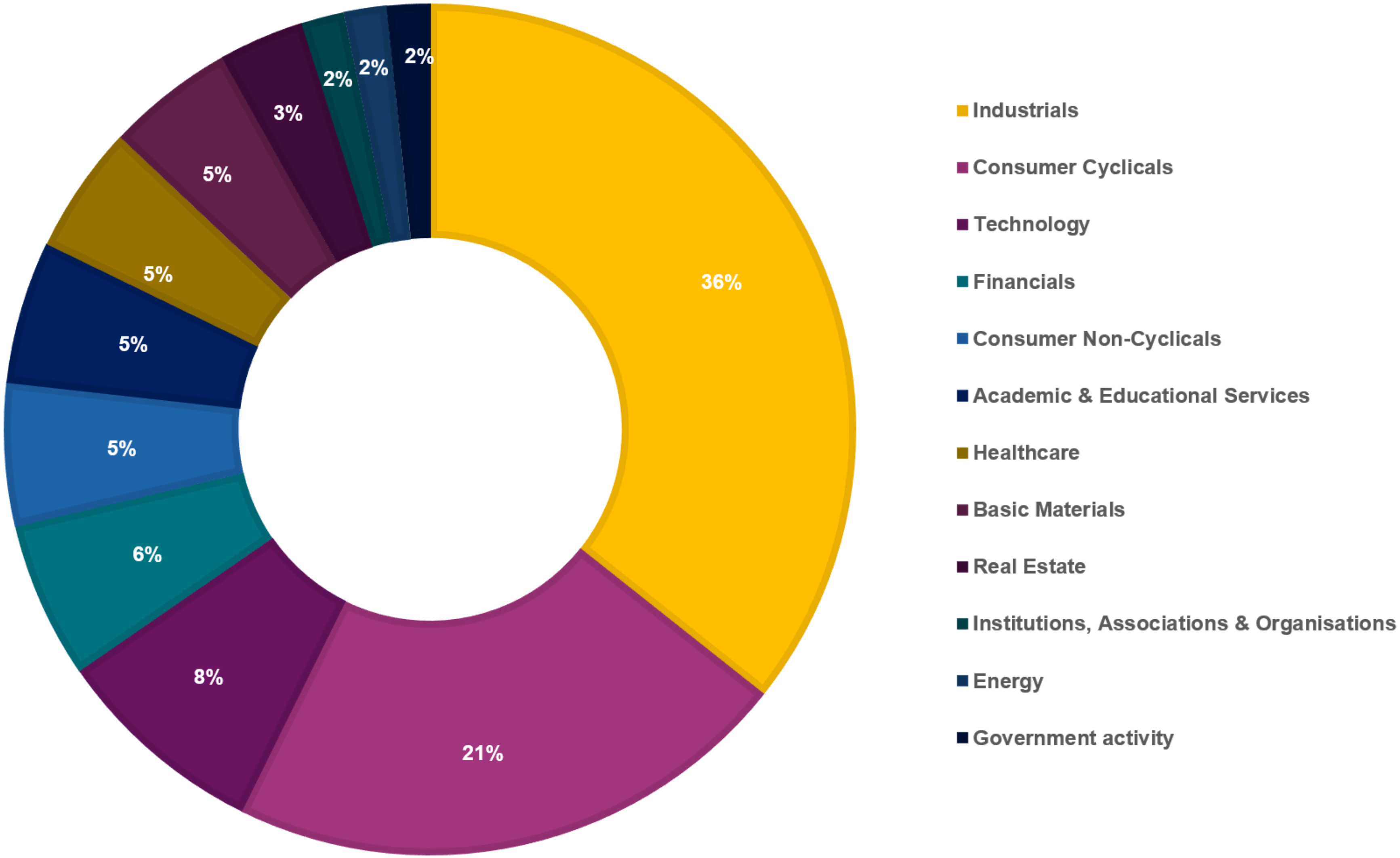
Key data

Percentage of Victims by Group in February



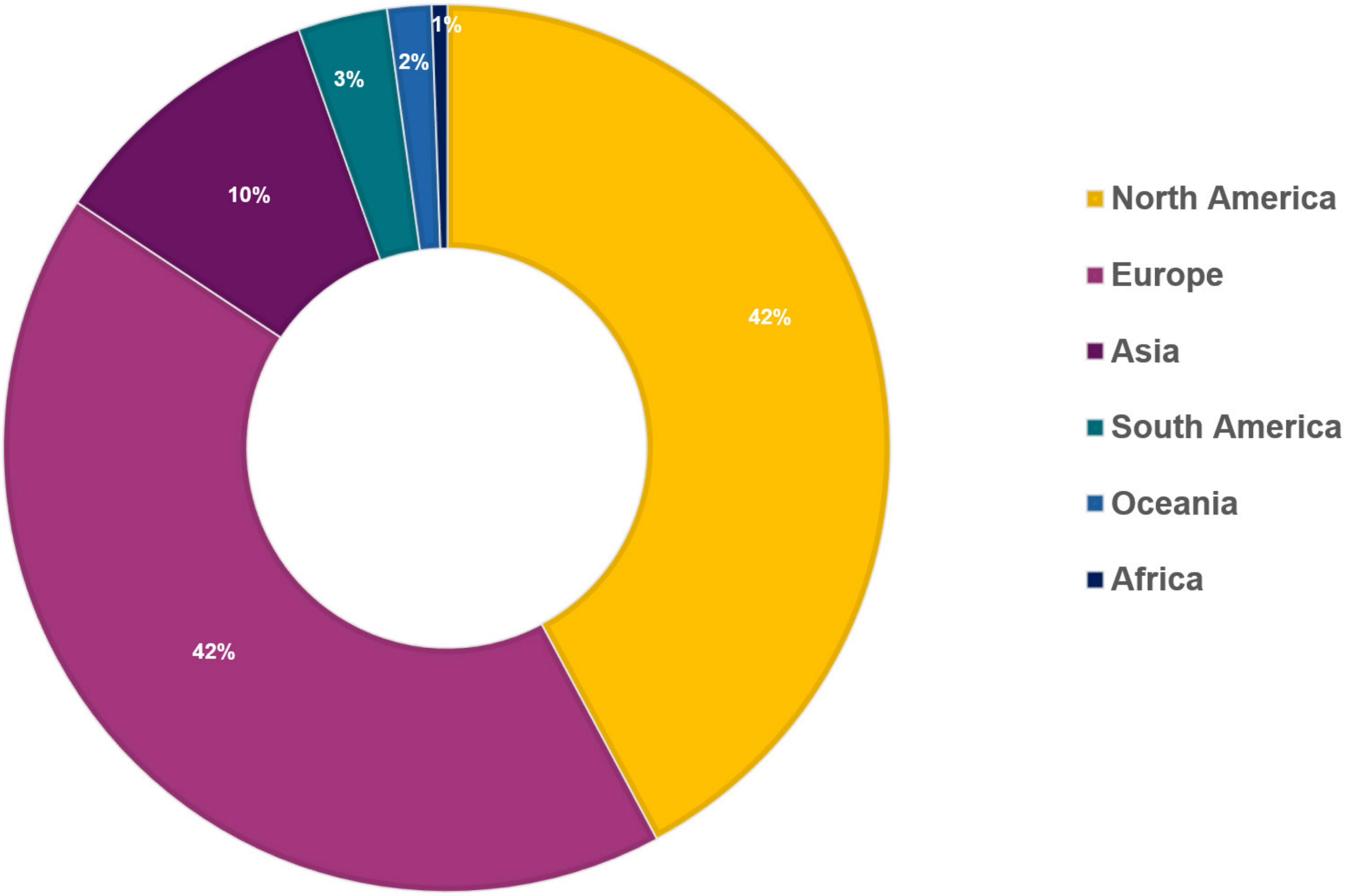
Key data

No. of Victims by Sector in February 2022



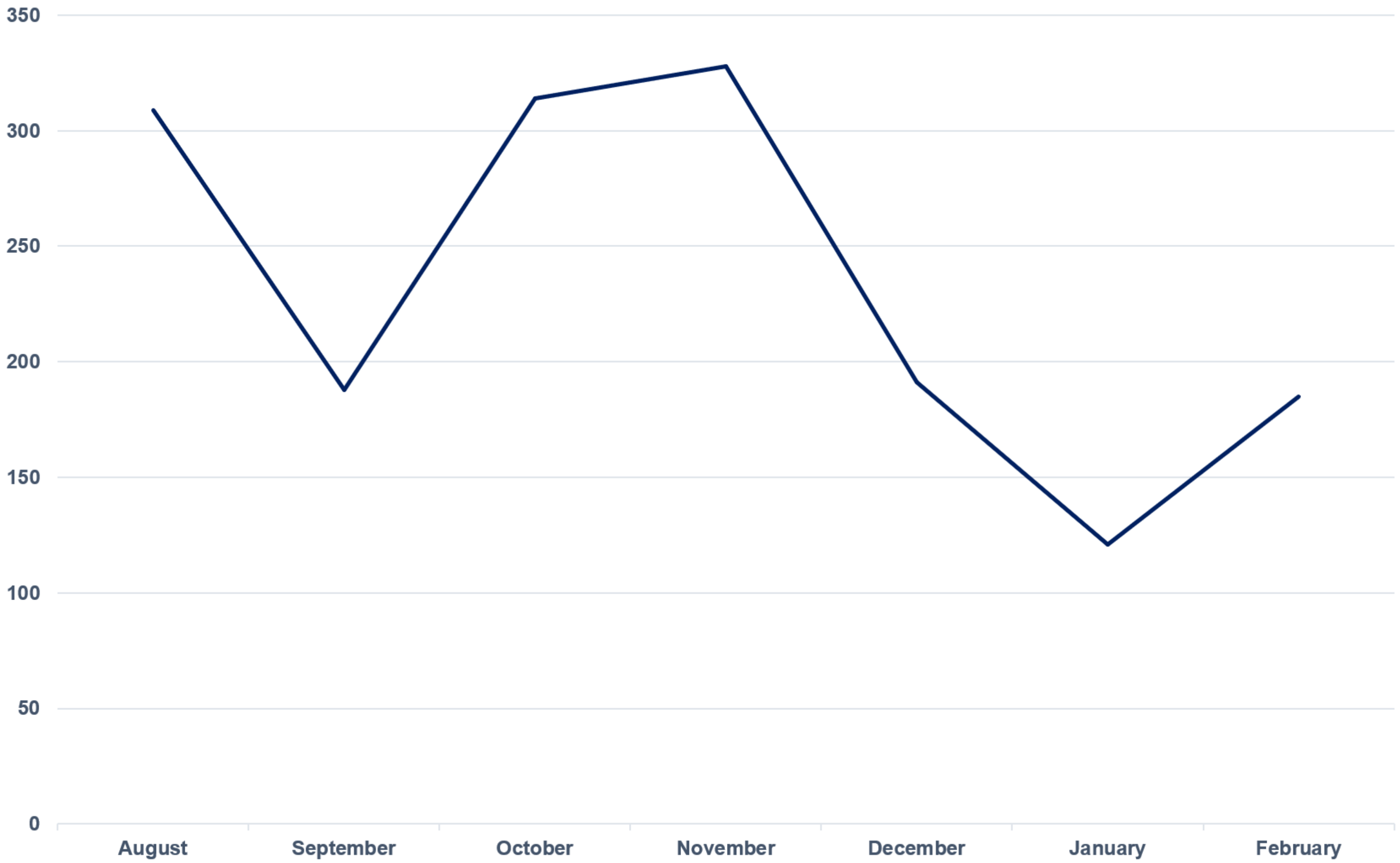
Key data

Percentage of victims per region in February



Key data

Number of cases per month



Analyst comments

This month we observed a 52.89% increase in ransomware attacks compared to January, with the number of incidents rising from 121 in January, to 185 this February.

This increase may represent a marked exit from the seasonal reduction in ransomware behaviour we observed across December and January.

In addition, this pattern is mirrored by our 2021 findings, where a 55.1% increase was observed between January 2021 (127 incidents) and February 2021 (197 incidents).

As such, we may begin to observe ransomware campaigns increase as the year unfolds and threat actors get back to 'work'.

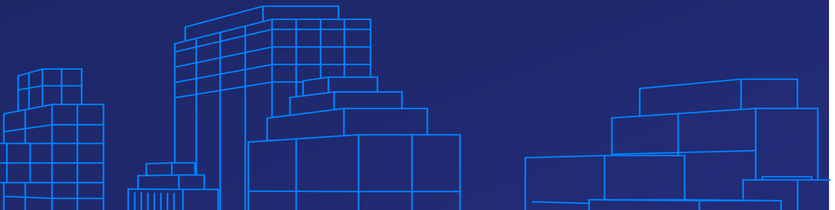
Threat actors

Though there was a significant increase in total cases from January to February, the top players remained consistent (Lockbit 2.0 with 42.2% of all attacks, and Conti with 17.8%).

The third largest contributor in February however was BlackCat, as opposed to Snatch in January.

In February, BlackCat accounted for 11.4% of all attacks as opposed to the negligible 5% that they exhibited in January, showing a steady increase in their activity.

In fact, BlackCat were well publicised in February, being attributed to high-profile attacks such as the two German oil companies that had data stolen on the 1st, and the Swissport ransomware attack on the 4th.



With their heightened frequency in our data as well as their recent infamy, NCC Group expect this trend to steadily persist and propose that BlackCat will remain within the top 3 aggressors in March. As such, we will continue to closely monitor their activity.

Lockbit 2.0's most targeted sector remains to be Industrials, accounting for a sizeable 30.77% of their total attacks in February.

Interestingly, this February sees their specific industry targeting within industrials displaying an indiscriminate approach for the most part, except for one industry that remains high on their list of priorities: Professional & Commercial Services, accounting for 37.5% of them.

In the last threat pulse, we described how this industry presents itself as a profoundly attractive target to extortive ransomware groups, which can provide some insight into why Lockbit 2.0 have continued to concentrate their resources on this industry.

Conti appears to be mirroring this same behaviour in February, with their most targeted sector equally being Industrials (48.4%).

Their specific targeting of industries within these sectors, however, is also largely indiscriminate, implying that they are not currently focusing on specific organisations but are selecting victims within these sectors opportunistically.

Therefore, any organisation (especially those residing within either the Industrials or Consumer Cyclicals sectors) should secure their systems with the assumption that Conti have them within their sights.

Last month we mentioned that although Conti had exhibited a 65.6% decrease in victims from December to January, they should not be considered as less of a threat, and we predicted that this number would rise once again in the coming months.

In February, our suspicions were proven to be correct with a mammoth 200% increase in their victims from January – February (from 11 to 33).

As we move out of the lull of the 1st quarter and into the 2nd, we may begin to witness what could be the baseline for ransomware activity that we can expect to see this year from all ransomware groups, if the pattern we witnessed in 2021 repeats itself.

Sectors

Overall, our analysis of this month's ransomware victims revealed similar findings to those observed in January.

Once again, the Industrial (35.68%) and Consumer Cyclicals (21.62%) sectors placed first and second as the most targeted sectors. Interestingly, both had suffered the greatest increase in number of attacks and thus were responsible for the overall growth we observed this month. Specifically, Industrials spiked from 30 to 66 incidents, revealing a 106% percentage increase, whilst consumer cyclicals rose from 27 to 40, a 48.15% percentage increase.

By consequence, their leading positions continue to reflect our wider observations from the last 7 months, supporting the trend in which they continue to be perceived as highly attractive targets.

In third place was the Technology sector (8.11%) which has moved up in the ranks from fifth place (6.03%) in January.

The growth in the number of targeted incidents is however not unusual as, prior to January, the sector had placed within the top three most victimised throughout the last 5 months of 2021.

This is not to say that ransomware campaigns targeting the Technology sector are not a cause for concern, but that these findings were not unexpected.

If anything, they stress the importance for continued hardened security measures within the sector itself and demonstrate that a decline in incidents in any sector, for even a short period of time (January), cannot justify any respite.

While our analysis reveals a rather persistent pattern, certainly with regards the prominence of the Industrial and Consumer Cyclicals sectors, it is will be critical to monitor and observe any changes over the upcoming months.

As the West delivers its plethora of economic sanctions targeting Russia for its ongoing invasion of the Ukraine, it will be interesting to observe if, in the context of Russian retaliation, there are any modifications to the sectors targeted, e.g. geared more towards the financials.

Regions

This month, the highest number of ransomware incidents were identified in North America (42.16%) and Europe (42.16%), followed by Asia (10.27%), South America (3.24%), Oceania (1.62%) and Africa (0.54%).

Last month, we identified the rather unusual finding that North America and Europe had suffered a roughly equal number of attacks, with 53 and 51 incidents respectively. This proved abnormal as up until then, North America had adopted a clear leading position. Hence, we questioned whether this closing of the gap was a by-product of the overall decrease in attacks in January, or something more.

This month, we observed an equal number of ransomware incidents recorded in Europe and North America (in our database) since pre-2021. The data suggests that both continents suffered 78 incidents respectively, together accounting for 84.32% of total incidents.

This is a possible turning-point, one that may be the result of the current political crisis and heightened threat towards the EU. As such, NCC Group will continue to closely monitor if this pattern persists, and what this means for the wider European threat landscape.

A closer analysis of the countries revealed the UK to be most victimised (26.92%), followed by Germany (14.10%), with France and Italy in joint third (10.26% respectively). Unsurprisingly, the most targeted sector in Europe was the Industrials with 29 incidents, 37.18%. Again, this was succeeded by Consumer Cyclicals with 22 incidents, 28.21%.

These were noticeably far removed from all other sectors, as the others concerned 6 incidents or less, again reinforcing the notion that both the Industrials and Consumer Cyclicals sectors remain highly attractive targets.

With respect to North America, Industrials took an undisputed lead accounting for 29 incidents (37.18%), with all other sectors accounting for under 10 incidents. Unlike the EU, consumer cyclicals was much less prominent (11.54%). The US remains the top target accounting for 93.59% of incidents in North America, whilst Canada contributed 5.3% and Cost Rica 1.28%.

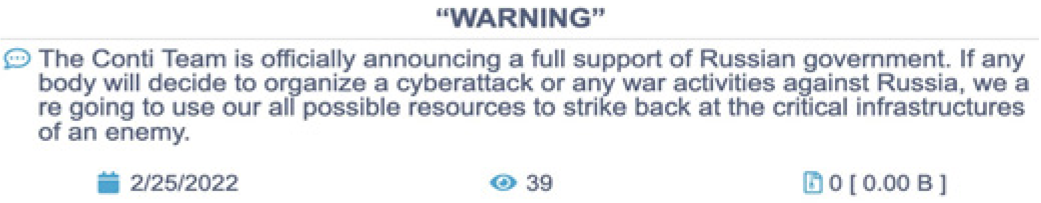
In sum, the change in direction with regards what appears to be a growth in targeting of EU organisations, raises questions as to whether this reflects a shift in threat actor targeting that may reshape the threat landscape. As such, we will continue to monitor the data and its evolution to assist us with better advising and supporting prevention measures according to regional needs.

Threat Actor Spotlight: Conti Group Leaks... again

Summary

There has been significant activity across the security community this week in relation to Conti Group, the ransomware gang also known as Wizard Spider, TheTrick or TrickBot.

On 25th February, the group posted a 'Warning' message on its public facing blog site, officially announcing its full support of the Russian government. It is clear that this declaration was hastily made in light of the crisis in Ukraine and without considering both the heightened interest from the wider security community, and the allegiance of some of its own employees.

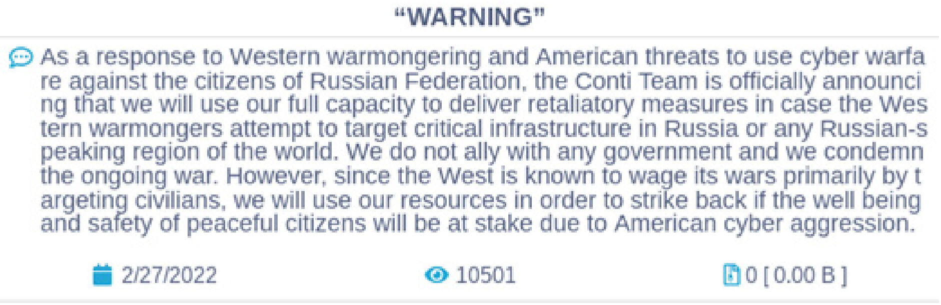


"WARNING"

The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022 39 0 [0.00 B]

Within a short time after, the group amended this declaration to state that they are not allied with a government, or support the current war situation. Conversely, however, the group has stated that they will retaliate against any targeting of Russian critical infrastructure in the face of a war generated by the West.



"WARNING"

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

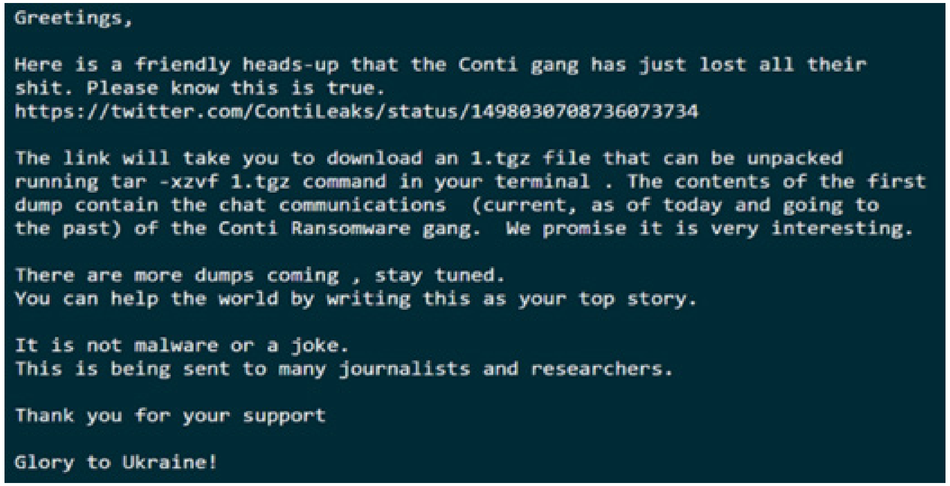
2/27/2022 10501 0 [0.00 B]

This intention, and confirmed support, suggests that the leaders of the group are either sympathetic to the Russian government, or have their hands tied. The latter, of course, would certainly align with Conti's previous backtracking following the Graff jewellers hack and leak episode, whereby the group apologised for leaking the information of individuals with close ties to the Russian government.

In response to this latest incident, it would seem that an anonymous member of the group has spoken out, by releasing a significant amount of internal communications, screenshots, and tactics used by the gang.

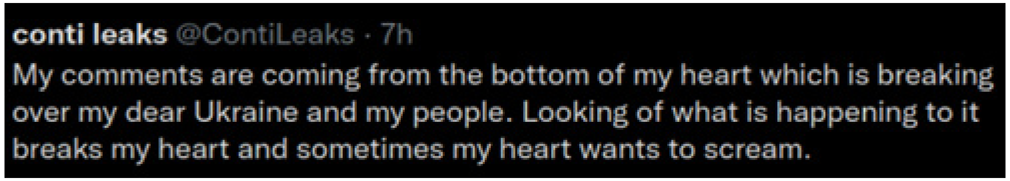
This is not the first time that Conti has suffered internal issues. In June 2021 a 55-year-old Latvian national called Alla Wiite was arrested and charged by the US government for her role in Conti Group, targeting organisations worldwide and stealing information . Another event during August 2021 saw a disgruntled member leak internal training manuals and IP addresses of the infrastructure utilised by the gang. It is believed this was in response to the employee not receiving a sufficient salary for their efforts.

With regards to the recent Conti leak, it is understood that a number of security vendors, journalists and researchers received the tip-off directly with the following message.



```
Greetings,

Here is a friendly heads-up that the Conti gang has just lost all their
shit. Please know this is true.
https://twitter.com/ContiLeaks/status/1498030708736073734

The link will take you to download an 1.tgz file that can be unpacked
running tar -xzvf 1.tgz command in your terminal . The contents of the first
dump contain the chat communications  (current, as of today and going to
the past) of the Conti Ransomware gang.  We promise it is very interesting.

There are more dumps coming , stay tuned.
You can help the world by writing this as your top story.

It is not malware or a joke.
This is being sent to many journalists and researchers.

Thank you for your support

Glory to Ukraine!
```

Although the identity of the recent internal leak remains unknown, we can deduce that they are likely to be a Ukrainian national, based on comments within the Twitter leak page.



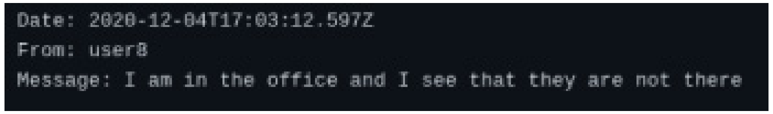
conti leaks @ContiLeaks · 7h
My comments are coming from the bottom of my heart which is breaking over my dear Ukraine and my people. Looking of what is happening to it breaks my heart and sometimes my heart wants to scream.

While NCC Group analysts and members of the wider security community race to analyse the data, looking for hostnames, IP addresses, tools, bitcoin addresses and so forth, we will review some translated snippets to understand how the organisation operates and the politics that take place within the group.

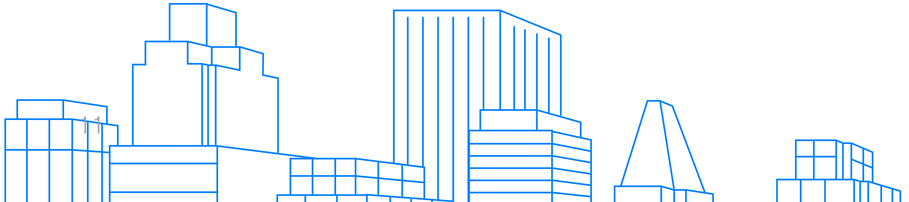
The leaked communication logs are dated from early 2020 until the February 2022. As has long been known, the group make reference to the use of free and commercial tooling to conduct their operations, such as Cobalt Strike, hydra and MSFVenom.

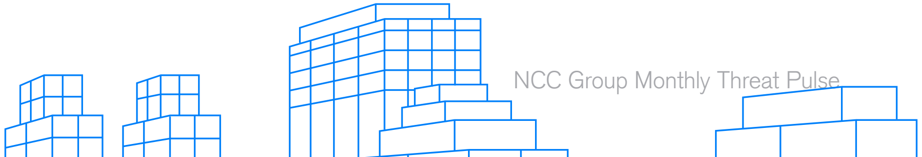
They are frequently seen to guide new joiners by referring them to online training videos and popular blog posts by security researchers.

Comments within the chat logs indicate that the team have managed an office location from at least 2020.



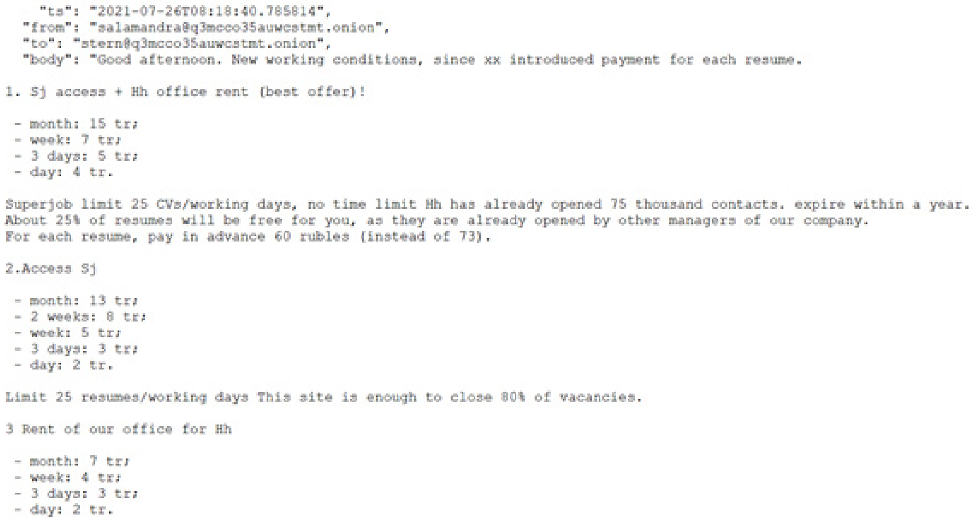
```
Date: 2020-12-04T17:03:12.597Z
From: user8
Message: I am in the office and I see that they are not there
```





Threat Actor Spotlight: Conti Group Leaks… again

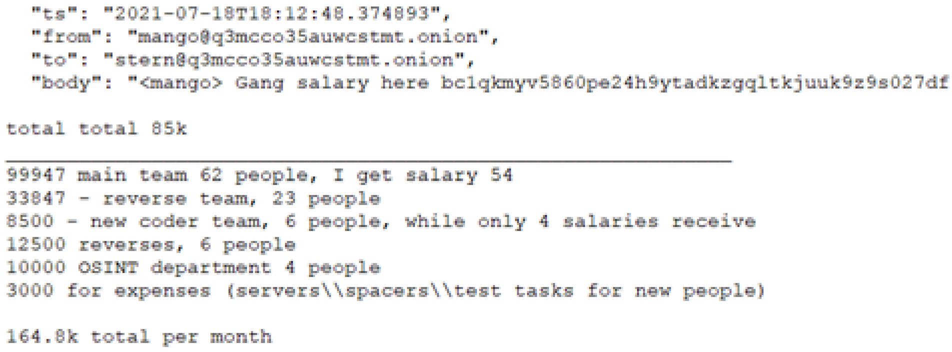
Followed up with a comment in July 2021, it appears that the group may have enquired about alternative office space to house employees.



```
   "ts": "2021-07-26T08:18:40.785814",
  "from": "salamandra@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "Good afternoon. New working conditions, since xx introduced payment for each resume.

1. Sj access + Hh office rent (best offer)!

 - month: 15 tr;
 - week: 7 tr;
 - 3 days: 5 tr;
 - day: 4 tr.

Superjob limit 25 CVs/working days, no time limit Hh has already opened 75 thousand contacts. expire within a year.
About 25% of resumes will be free for you, as they are already opened by other managers of our company.
For each resume, pay in advance 60 rubles (instead of 73).

2.Access Sj

 - month: 13 tr;
 - 2 weeks: 8 tr;
 - week: 5 tr;
 - 3 days: 3 tr;
 - day: 2 tr.

Limit 25 resumes/working days This site is enough to close 80% of vacancies.

3 Rent of our office for Hh

 - month: 7 tr;
 - week: 4 tr;
 - 3 days: 3 tr;
 - day: 2 tr.
```

Internal politics

Additional communications during this time indicated that there were at least 62 members within the group, made up of coders, reverse engineers, and OSINT researchers. The following translated snippet also gives an indication around the salaries each member receives.

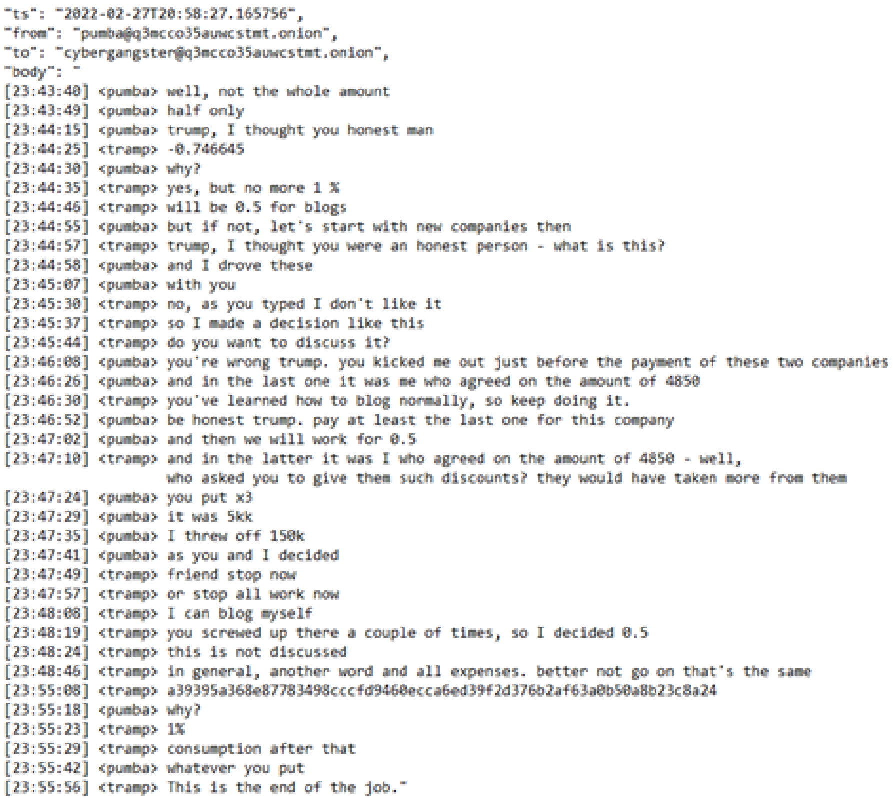


```
  "ts": "2021-07-18T18:12:48.374893",
  "from": "mango@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "<mango> Gang salary here bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df

total total 85k

______________________________________________________
99947 main team 62 people, I get salary 54
33847 - reverse team, 23 people
8500 - new coder team, 6 people, while only 4 salaries receive
12500 reverses, 6 people
10000 OSINT department 4 people
3000 for expenses (servers\\spacers\\test tasks for new people)

164.8k total per month
```

The currency referred to here is not known, although if USD are used as a point of reference, the salaries for each employee is not significant given that some members have mentioned working 12hr days.

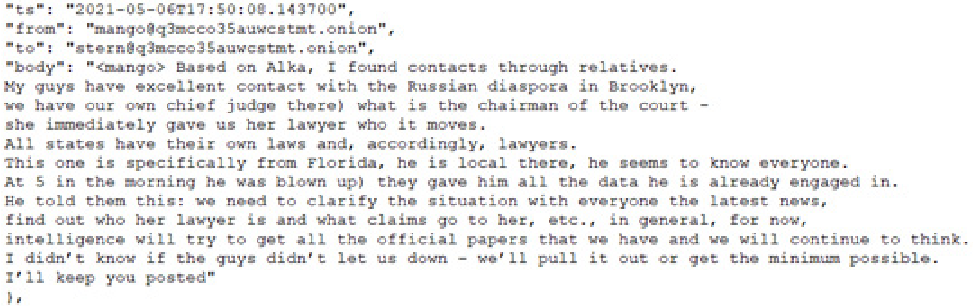
The working schedule of the group is often references, but the specifics currently remain unknown.

As already highlighted, historic leaks from within the group were thought to be due to salary issues. The following excerpt between members Pumba and Tramp within the last few days indicate that this remains to be an area of concern.



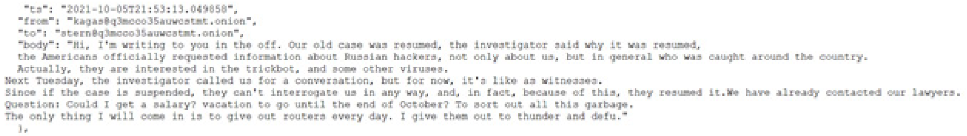
```
"ts": "2022-02-27T20:58:27.165756",
"from": "pumba@q3mcco35auwcstmt.onion",
"to": "cybergangster@q3mcco35auwcstmt.onion",
"body": "
[23:43:40] <pumba> well, not the whole amount
[23:43:49] <pumba> half only
[23:44:15] <pumba> trump, I thought you honest man
[23:44:25] <tramp> -0.746645
[23:44:30] <pumba> why?
[23:44:35] <tramp> yes, but no more 1 %
[23:44:46] <tramp> will be 0.5 for blogs
[23:44:55] <pumba> but if not, let's start with new companies then
[23:44:57] <tramp> trump, I thought you were an honest person - what is this?
[23:44:58] <pumba> and I drove these
[23:45:07] <pumba> with you
[23:45:30] <tramp> no, as you typed I don't like it
[23:45:37] <tramp> so I made a decision like this
[23:45:44] <tramp> do you want to discuss it?
[23:46:08] <pumba> you're wrong trump. you kicked me out just before the payment of these two companies
[23:46:26] <pumba> and in the last one it was me who agreed on the amount of 4850
[23:46:30] <tramp> you've learned how to blog normally, so keep doing it.
[23:46:52] <pumba> be honest trump. pay at least the last one for this company
[23:47:02] <pumba> and then we will work for 0.5
[23:47:10] <tramp> and in the latter it was I who agreed on the amount of 4850 - well,
                  who asked you to give them such discounts? they would have taken more from them
[23:47:24] <pumba> you put x3
[23:47:29] <pumba> it was 5kk
[23:47:35] <pumba> I threw off 150k
[23:47:41] <pumba> as you and I decided
[23:47:49] <tramp> friend stop now
[23:47:57] <tramp> or stop all work now
[23:48:08] <tramp> I can blog myself
[23:48:19] <tramp> you screwed up there a couple of times, so I decided 0.5
[23:48:24] <tramp> this is not discussed
[23:48:46] <tramp> in general, another word and all expenses. better not go on that's the same
[23:55:08] <tramp> a39395a368e87783498cccfd9460ecca6ed39f2d376b2af63a0b50a8b23c8a24
[23:55:18] <pumba> why?
[23:55:23] <tramp> 1%
[23:55:29] <tramp> consumption after that
[23:55:42] <pumba> whatever you put
[23:55:56] <tramp> This is the end of the job."
```

Back in May of 2021, members Mango and Stern were discussing contacting a judge and lawyer within the Russian Diaspora in Brooklyn, and refer to 'her' lawyer. In this instance, 'her' is thought to relate to Alla Witte, the Latvian national arrested by US authorities.



```
"ts": "2021-05-06T17:50:08.143700",
"from": "mango@q3mcco35auwcstmt.onion",
"to": "stern@q3mcco35auwcstmt.onion",
"body": "<mango> Based on Alka, I found contacts through relatives.
My guys have excellent contact with the Russian diaspora in Brooklyn,
we have our own chief judge there) what is the chairman of the court -
she immediately gave us her lawyer who it moves.
All states have their own laws and, accordingly, lawyers.
This one is specifically from Florida, he is local there, he seems to know everyone.
At 5 in the morning he was blown up) they gave him all the data he is already engaged in.
He told them this: we need to clarify the situation with everyone the latest news,
find out who her lawyer is and what claims go to her, etc., in general, for now,
intelligence will try to get all the official papers that we have and we will continue to think.
I didn't know if the guys didn't let us down - we'll pull it out or get the minimum possible.
I'll keep you posted"
},
```

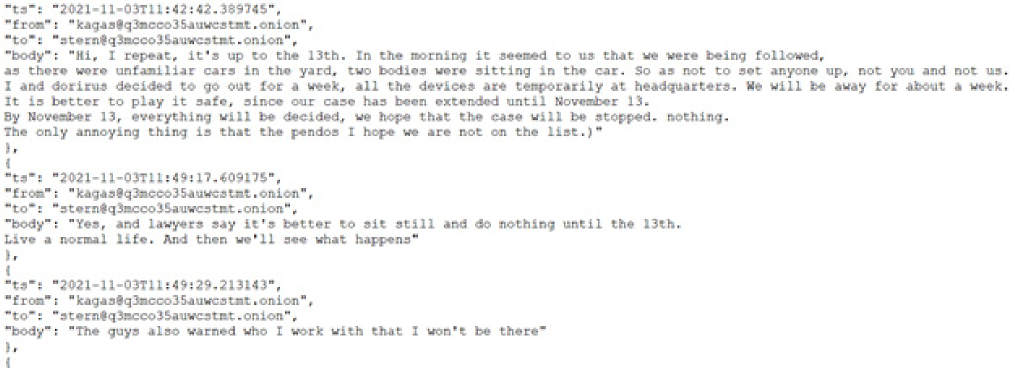
This legal issues do not not appear to escape the group, and by October of 2021 we can see that members continue liaison with an investigator.



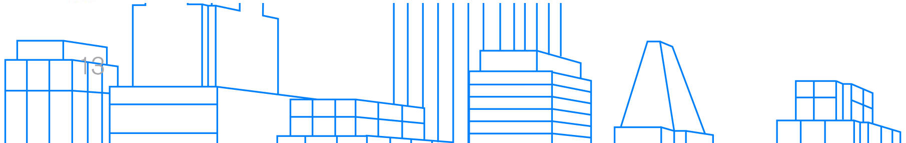
```
 "ts": "2021-10-05T21:53:13.049858",
"from": "kagas@q3mcco35auwcstmt.onion",
"to": "stern@q3mcco35auwcstmt.onion",
"body": "Hi, I'm writing to you in the off. Our old case was resumed, the investigator said why it was resumed,
the Americans officially requested information about Russian hackers, not only about us, but in general who was caught around the country.
Actually, they are interested in the trickbot, and some other viruses.
Next Tuesday, the investigator called us for a conversation, but for now, it's like as witnesses.
Since if the case is suspended, they can't interrogate us in any way, and, in fact, because of this, they resumed it.We have already contacted our lawyers.
Question: Could I get a salary? vacation to go until the end of October? To sort out all this garbage.
The only thing I will come in is to give out routers every day. I give them out to thunder and defu."
 },
```

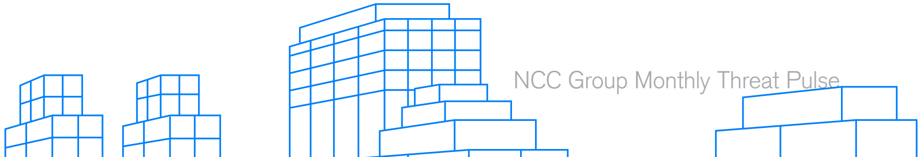
Subsequent communications in early November regarding their legal case suggest that members of the group were concerned for their security having noted unfamiliar cars within the yard.

Again, we can see that a single office acts as their primary base of operations. 'Pendos' is believed to be a slang term used for Westerners.



```
"ts": "2021-11-03T11:42:42.389745",
"from": "kagas@q3mcco35auwcstmt.onion",
"to": "stern@q3mcco35auwcstmt.onion",
"body": "Hi, I repeat, it's up to the 13th. In the morning it seemed to us that we were being followed,
as there were unfamiliar cars in the yard, two bodies were sitting in the car. So as not to set anyone up, not you and not us.
I and dorirus decided to go out for a week, all the devices are temporarily at headquarters. We will be away for about a week.
It is better to play it safe, since our case has been extended until November 13.
By November 13, everything will be decided, we hope that the case will be stopped. nothing.
The only annoying thing is that the pendos I hope we are not on the list.)"
},
{
"ts": "2021-11-03T11:49:17.609175",
"from": "kagas@q3mcco35auwcstmt.onion",
"to": "stern@q3mcco35auwcstmt.onion",
"body": "Yes, and lawyers say it's better to sit still and do nothing until the 13th.
Live a normal life. And then we'll see what happens"
},
{
"ts": "2021-11-03T11:49:29.213143",
"from": "kagas@q3mcco35auwcstmt.onion",
"to": "stern@q3mcco35auwcstmt.onion",
"body": "The guys also warned who I work with that I won't be there"
},
{
```

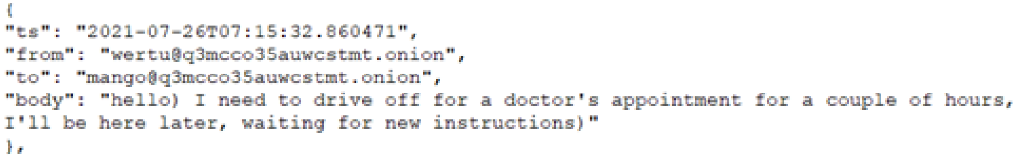




Threat Actor Spotlight: Conti Group Leaks... again

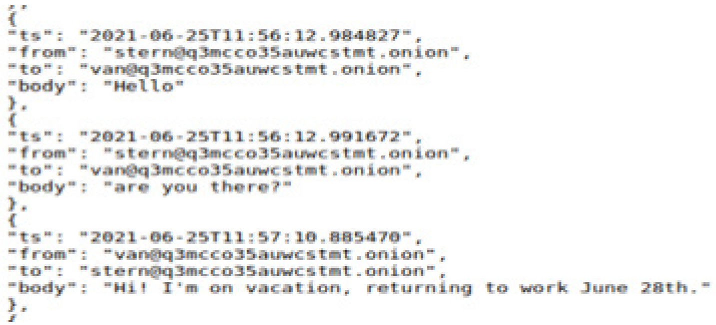
Vacations

It appears that vacations and flexible working are just as important to the group as any legitimate company. One member mentions to their team leader Mango, that they will be attending a doctor's appointment during the working day, however, they will resume work upon their return.

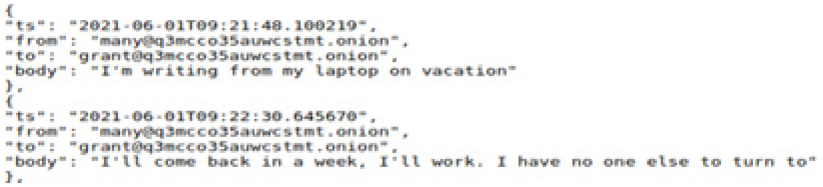


```
{
"ts": "2021-07-26T07:15:32.860471",
"from": "wertu@q3mcco35auwcstmt.onion",
"to": "mango@q3mcco35auwcstmt.onion",
"body": "hello) I need to drive off for a doctor's appointment for a couple of hours,
I'll be here later, waiting for new instructions)"
},
```

From the two following snippets we can deduce that members of the group also have access to communications remotely, even when on vacation. Extended breaks away from work are frequently seen by members of the group throughout the summer months.



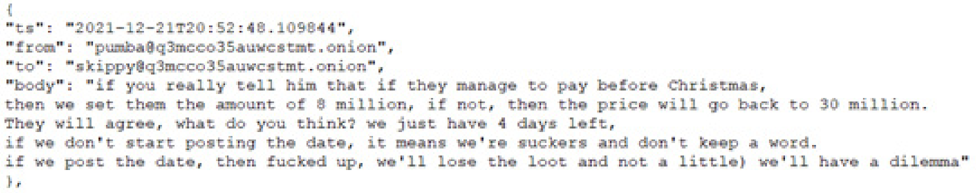
```
,,
{
"ts": "2021-06-25T11:56:12.984827",
"from": "stern@q3mcco35auwcstmt.onion",
"to": "van@q3mcco35auwcstmt.onion",
"body": "Hello"
},
{
"ts": "2021-06-25T11:56:12.991672",
"from": "stern@q3mcco35auwcstmt.onion",
"to": "van@q3mcco35auwcstmt.onion",
"body": "are you there?"
},
{
"ts": "2021-06-25T11:57:10.885470",
"from": "van@q3mcco35auwcstmt.onion",
"to": "stern@q3mcco35auwcstmt.onion",
"body": "Hi! I'm on vacation, returning to work June 28th."
},
,
```



```
{
"ts": "2021-06-01T09:21:48.100219",
"from": "many@q3mcco35auwcstmt.onion",
"to": "grant@q3mcco35auwcstmt.onion",
"body": "I'm writing from my laptop on vacation"
},
{
"ts": "2021-06-01T09:22:30.645670",
"from": "many@q3mcco35auwcstmt.onion",
"to": "grant@q3mcco35auwcstmt.onion",
"body": "I'll come back in a week, I'll work. I have no one else to turn to"
},
```

However, as with many organisations the need to close a deal before Christmas and New Year creates additional pressure for the team.

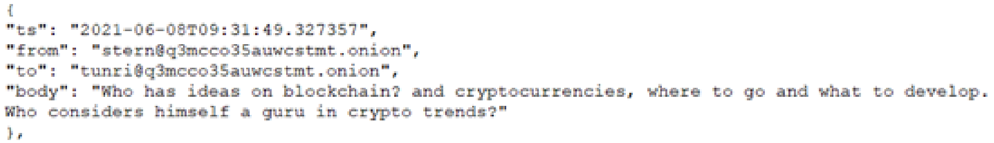
Here we can see members Pumba and Skippy discussing a negotiation with a ransom discount before Christmas.



```
{
"ts": "2021-12-21T20:52:48.109844",
"from": "pumba@q3mcco35auwcstmt.onion",
"to": "skippy@q3mcco35auwcstmt.onion",
"body": "if you really tell him that if they manage to pay before Christmas,
then we set them the amount of 8 million, if not, then the price will go back to 30 million.
They will agree, what do you think? we just have 4 days left,
if we don't start posting the date, it means we're suckers and don't keep a word.
if we post the date, then fucked up, we'll lose the loot and not a little) we'll have a dilemma"
},
```

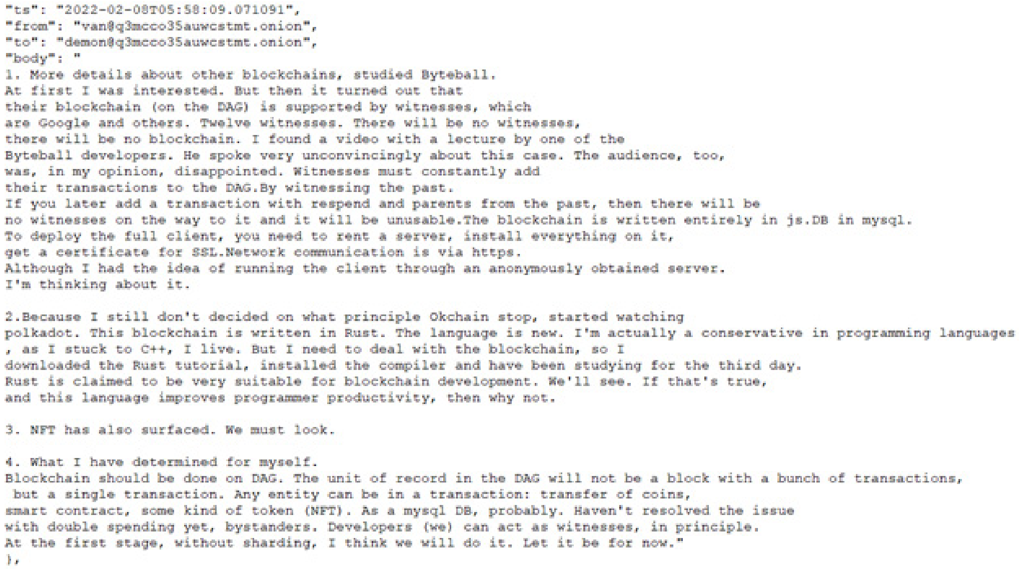
The future of Conti

Like many organisation’s within the tech space, the gang have been looking into additional areas with which they can develop. This extract from June 2021 shows a desire to develop capabilities in blockchain technology.



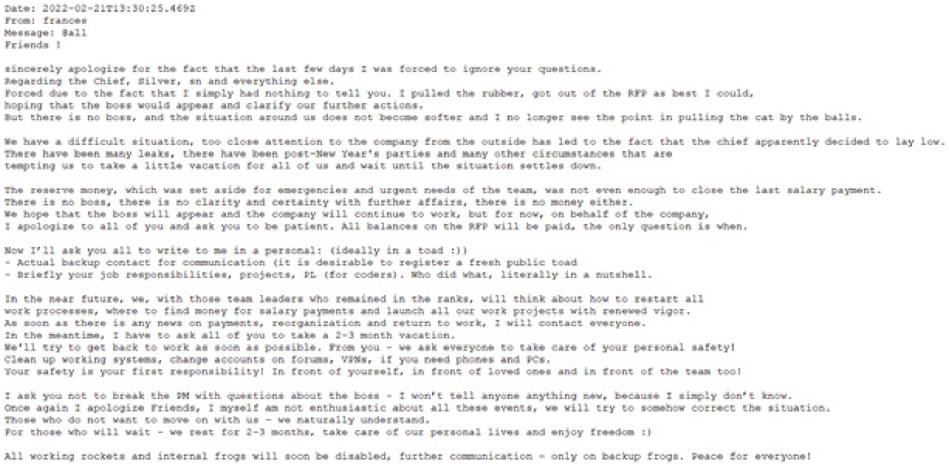
```
{
"ts": "2021-06-08T09:31:49.327357",
"from": "stern@q3mcco35auwcstmt.onion",
"to": "tunri@q3mcco35auwcstmt.onion",
"body": "Who has ideas on blockchain? and cryptocurrencies, where to go and what to develop.
Who considers himself a guru in crypto trends?"
},
```

By early February 2022, the desire to develop their capabilities has not waivered. Additional technologies such as the Rust language and NFT’s have also piqued one members interest.



```
"ts": "2022-02-08T05:58:09.071091",
"from": "van@q3mcco35auwcstmt.onion",
"to": "demon@q3mcco35auwcstmt.onion",
"body": "
1. More details about other blockchains, studied Byteball.
At first I was interested. But then it turned out that
their blockchain (on the DAG) is supported by witnesses, which
are Google and others. Twelve witnesses. There will be no witnesses,
there will be no blockchain. I found a video with a lecture by one of the
Byteball developers. He spoke very unconvincingly about this case. The audience, too,
was, in my opinion, disappointed. Witnesses must constantly add
their transactions to the DAG.By witnessing the past.
If you later add a transaction with respend and parents from the past, then there will be
no witnesses on the way to it and it will be unusable.The blockchain is written entirely in js.DB in mysql.
To deploy the full client, you need to rent a server, install everything on it,
get a certificate for SSL.Network communication is via https.
Although I had the idea of running the client through an anonymously obtained server.
I'm thinking about it.

2.Because I still don't decided on what principle Okchain stop, started watching
polkadot. This blockchain is written in Rust. The language is new. I'm actually a conservative in programming languages
, as I stuck to C++, I live. But I need to deal with the blockchain, so I
downloaded the Rust tutorial, installed the compiler and have been studying for the third day.
Rust is claimed to be very suitable for blockchain development. We'll see. If that's true,
and this language improves programmer productivity, then why not.

3. NFT has also surfaced. We must look.

4. What I have determined for myself.
Blockchain should be done on DAG. The unit of record in the DAG will not be a block with a bunch of transactions,
 but a single transaction. Any entity can be in a transaction: transfer of coins,
smart contract, some kind of token (NFT). As a mysql DB, probably. Haven't resolved the issue
with double spending yet, bystanders. Developers (we) can act as witnesses, in principle.
At the first stage, without sharding, I think we will do it. Let it be for now."
},
```

However, a message dated 21st February by one member to the wider group on Rocket Chat indicated that there continues to be problems internally. Senior members have been missing and deemed to be laying low, while other members are advised to rest for several months. Although the group have amassed significant sums from their ransomware victims, this member insists that there isn’t enough money to pay the salaries for all staff.



```
Date: 2022-02-21T13:30:25.469Z
From: frances
Message: @all
Friends !

sincerely apologize for the fact that the last few days I was forced to ignore your questions.
Regarding the Chief, Silver, sn and everything else.
Forced due to the fact that I simply had nothing to tell you. I pulled the rubber, got out of the RFP as best I could,
hoping that the boss would appear and clarify our further actions.
But there is no boss, and the situation around us does not become softer and I no longer see the point in pulling the cat by the balls.

We have a difficult situation, too close attention to the company from the outside has led to the fact that the chief apparently decided to lay low.
There have been many leaks, there have been post-New Year's parties and many other circumstances that are
tempting us to take a little vacation for all of us and wait until the situation settles down.

The reserve money, which was set aside for emergencies and urgent needs of the team, was not even enough to close the last salary payment.
There is no boss, there is no clarity and certainty with further affairs, there is no money either.
We hope that the boss will appear and the company will continue to work, but for now, on behalf of the company,
I apologize to all of you and ask you to be patient. All balances on the RFP will be paid, the only question is when.

Now I’ll ask you all to write to me in a personal: (ideally in a toad :))
- Actual backup contact for communication (it is desirable to register a fresh public toad
- Briefly your job responsibilities, projects, PL (for coders). Who did what, literally in a nutshell.

In the near future, we, with those team leaders who remained in the ranks, will think about how to restart all
work processes, where to find money for salary payments and launch all our work projects with renewed vigor.
As soon as there is any news on payments, reorganization and return to work, I will contact everyone.
In the meantime, I have to ask all of you to take a 2-3 month vacation.
We'll try to get back to work as soon as possible. From you - we ask everyone to take care of your personal safety!
Clean up working systems, change accounts on forums, VPNs, if you need phones and PCs.
Your safety is your first responsibility! In front of yourself, in front of loved ones and in front of the team too!

I ask you not to break the PM with questions about the boss - I won’t tell anyone anything new, because I simply don’t know.
Once again I apologize Friends, I myself am not enthusiastic about all these events, we will try to somehow correct the situation.
Those who do not want to move on with us - we naturally understand.
For those who will wait - we rest for 2-3 months, take care of our personal lives and enjoy freedom :)

All working rockets and internal frogs will soon be disabled, further communication - only on backup frogs. Peace for everyone!
```

Conti Group are certainly going through a turbulent phase after significant successes. Regardless, they are a large entity and continue to target organisations from around the world.

Since the gangs warning message on 25th February, and at the time of writing, they have declared 30 new ransomware victims, indicating that operations continue in the face of disruption.

About the NCC Group Monthly Threat Pulse

NCC Group's Strategic Threat Intelligence Practice has been working tirelessly to develop various software solutions for a broader, more insightful look at current threat landscapes and the way they impact businesses around the world.

Our technical team has developed a web scraper, which we use to gather data on ransomware data leaks on the dark web in real time to give us regular insights into who are the most recent ransomware victims.

By recording this data and classifying the victims by sector, we are able to derive additional insights highlighting the sectors that have been targeted, and how current ransomware threats compare to previous months.

nccgroup