Introduction to Digital Forensics Assignment 3

Emma van den Broek | s2804859
Aukje Hekstra | s2294184
Rik Helder | s2864010
Inèz Hemme | s2429837
Ewoud Janus | s2395762
Koen Wilms | s1818872

University of Twente
Introduction to Digital Forensics for Cybercrime

Motivation and Goals

The Conti ransomware variant transnational organised crime group is a notorious cybercriminal group from Eastern Europe with ties to the Russian government, whose activity has first been observed in or around June 2020. Conti operates with the use of a Ransomware-as-a-Service (RaaS) model, meaning that Conti would employ affiliates and train them in Conti's ransomware deployment and management. Then, Conti takes a 30% cut of the profits themselves (Fier, 2021).

RaaS especially can have a large impact on society, because it lowers the bar for entry into cybercrime. Using the services of a business that uses a RaaS model, an actor with limited technical skills can carry out cyber attacks.

Ransomware attacks can have a big negative impact on their victims, like financial losses, loss of files and data and being unable to work due to a shutdown of critical business systems. Victims can be multimillion dollar companies or just individual persons. Ransomware attacks have changed a lot in the last decade. In 2013 a spray-and-pray type of attack was more popular, which is an opportunistic type of ransomware attack which is monetised by extorting the need to access data of individual devices. This is not a targeted attack, but operates by a high-volume of tries in the hope that some people fall victim. The high-volume, opportunistic approach is less popular these days, since cybercriminals have moved to lower-volume, targeted ransomware attacks. Conti also has a lower-volume, targeted attack type of approach.

Conti additionally uses double extortion techniques. Not only do they encrypt the victim's files, they also steal and threaten to publish the victim's data if the ransom is not paid. Conti has been one of the most successful ransomware groups ever recorded. The FBI estimates that as of February 2022, over 1,000 victims of Conti have been reported with victim payouts exceeding 150 million USD (*Conti Ransomware*, 2022). Notable attack vectors of Conti include Trickbot and Cobalt Strike. Trickbot and Cobalt Strike are used during spear phishing campaigns to deliver Conti ransomware.

On the 25th of February 2022, Conti officially announced their full support of the Russian Government, shortly after Russia invaded Ukraine. Three days later, on the 28th of February, leaks of Conti's internal messages started, posted on the Twitter account "ContiLeaks" by an Ukranian employee who took issue with Conti's support of Russia (Pitrelli, 2022). These leaked chats revealed a lot about the inner workings of Conti and were a starting point for a lot of investigations. It was determined that Conti has a clear management, has finance and human resource functions, along with a hierarchy that is typically found in classic organisations, with team leaders that report to upper management. Additionally, in Conti, performance reviews are held and there are training opportunities. Conti even has an employee of the month.

The Department of State of the USA is currently offering a reward of up to 10 million USD for information that leads to the identification and/or location of any key leaders of the Conti group (Price, 2022). They are additionally offering a reward of up to 5 million USD for information that leads to the arrest and/or conviction of any individual in any country who plans to or attempts to use Conti's services to hold a ransomware attack.

Conti especially is a notorious group, considering their size and the number of and size of their attacks. Conti has cost more than $150 million in ransomware fees and has attacked more than a thousand businesses. Taking action against Conti to ensure that attacks are less effective and that there are less - or ideally, no more - victims is important. Learning more about how Conti works can also help in the investigation of other major ransomware groups. In order to be able to take action against this group, it can be an important step to first make an analysis of the group. This will be done in this report using the leaked data of the Jabber chat from 2021 to 2022.

Method and Results

The data that was provided are time-stamped messages that were translated to english. The data should be analysed on 16 different aspects. In order to figure out all of the answers to these questions, some python scripts were written to find the data in a timely and orderly manner. These scripts can be found on the github page (*Github*, 2023). The scripts were written using Python in Jupyter Notebook. Some answers were found by searching through the raw data using different search tools, one of these tools is the “Find” tool accessible in Google Chrome.

1. How many records are in the data?

There are a total of 60772 records in the data. This is simple to find out because the entries are indexed and thus the last index is 60772.

2. Time-span of the collected records?

The time-span over which the records were collected is from the 29th of January in 2021 to March 2nd of 2022. This means that these messages were collected over a period of a little more than two years. This was found by finding the earliest and latest timestamps in the ‘ts’ columns see the Github repository (Github, 2023).

3. What is the average of messages per person?

The average per person is 221.8 messages. That is an quite impressive amount to have on average. But with the amount of days that the data was collected, it comes to around 0,6 messages per day per person. $221.8/397 \approx 0.558$

4. Who are the top players?

The top players that have sent the most messages are in the table below with how many they have sent. Defender@q3mcco35auwcstmt.onion has sent a total of 8246 messages.

1.	defender@q3mcco35auwcstmt.onion	8246
2.	stern@q3mcco35auwcstmt.onion	4323
3.	driver@q3mcco35auwcstmt.onion	3968
4.	bio@q3mcco35auwcstmt.onion	3196
5.	mango@q3mcco35auwcstmt.onion	3194
6.	ttrr@conference.q3mcco35auwcstmt.onion	3122
7.	veron@q3mcco35auwcstmt.onion	2955
8.	hof@q3mcco35auwcstmt.onion	2389
9.	bentley@q3mcco35auwcstmt.onion	1810
10.	bloodrush@q3mcco35auwcstmt.onion	1798

5. What roles are players responsible for?

There are many roles that are regularly mentioned in the messages. The puzzle is to find the role that is tasked to one person. As is mentioned in the blog of northwave cybersecurity on ‘when the hackers get hacked - part 2 (Northwave Cybersecurity, n.d.)’, the roles of the group can be found out. We have first analysed the common roles. These are ‘administrator’, ‘target', 'decryptor', 'encryptor', 'coder', 'maintainer', 'manager', 'recruiter', 'accountant', 'tester' and 'exfiltrator'. Any message in which one of these roles is mentioned, is put into a file. That way, it is simple to look into the messages that provide information on the roles.

For example, entry 21370 is the 16th message of our batch that contains the word manager. This is send from mango@q3mcco35auwcstmt.onion and it says: “Ops, by the way, I&#39;m support C, manager for general issues of the team \ trick \ locker, now I&#39;m looking for access to work for the gang, well, in general, there is no C on the farm yet”. We can conclude from this that mango is some sort of general manager. In the recording period, he has sent 3194 messages and is number 5 of the top players.

Some of the other roles are harder to define as they are not signed by their title. The blog (Northwave Cybersecurity, n.d.) mentions some of these roles. Most of them are defined by the messages that they got from other people or the type of assignments that they provided.

6. How many accounts @gmail.com are there? What are they for?

There are a number of different Gmail accounts mentioned in the messages. No messages are sent to or from a gmail mail address, but in total 7 different messages are mentioned in the text itself. These are:

1. nacho.travesib@gmail.com
2. basils1991@gmail.com
3. xvioletta2013@gmail.com
4. tdemeza@gmail.com
5. itserviceemilabkarov@gmail.com
6. nikola131189@gmail.com
7. loguntsov@gmail.com

Some of the gmail addresses are recovery addresses or possibly log in credentials. For example entry 23311 says: “*olaf@scholja.de:Jenny+1992 nacho.travesib@gmail.com: 01031988Almu https://www.crunchbase.com/*”. Crunchbase is an organisation for a professional business platform. This might be log in credentials to be able to get access to their computers and to be able to put ransomware on it.

7. Give example(s) of IP addresses in the data? And say what are they for.

All IP addresses that are mentioned in the recording are processed by the github code (*Github*, 2023). Some of these are: IP Address: 5.139.220.204, IP Address: 185.64.104.5 and IP Address: 172.83.155.195. These IP addresses might be possible victims.

8. Give example(s) of URLs in the data? And say what they are for.

There are many URLs that were mentioned in the recording. They are counted per website roots and the 10 most mentioned are in the table below.

1. privnote.com, Count: 425
2. qaz.im, Count: 370
3. privatlab.com, Count: 195
4. sendspace.com, Count: 45
5. 1ty.me, Count: 41
6. file.io, Count: 32
7. prnt.sc, Count: 29
8. continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion, Count: 28
9. dropfiles.me, Count: 25
10. zoominfo.com, Count: 23

The most common website is privnote, which is a website that lets people create and send encrypted messages. The messages self-destruct after being read. Most of these websites are ways of anonymously sharing information, files, or messages with others. This is one of the other possibilities to communicate with each other.

9. Give example(s) of bitcoin wallets. Try to identify the owner of the wallet.

We have identified a lot of bitcoin wallets. Here are just three of them displayed. The first two wallets are from mango and the third is one from tramp. The transaction amounts are massive. In the code on github (*Github*, 2023), all the mentions of bitcoin wallets can be found.

- Wallet: bc1qnf6drcfl786d70wlhfytyr5xg3qqgknlsh8dc3
  Owner:mango@q3mcco35auwcstmt.onion
  Transaction amount: 1.03945389 BTC $35,311.26

- Wallet: bc1qptn5qsllcxmrndmwucelazjt0z68zkrgrlumy0
  Owner: mango@q3mcco35auwcstmt.onion
  Transaction amount:1.81029779 BTC $61,589.63

- Wallet: 1LYiEgq9k3xSAddbqMZcsVTayJVoKbTFub
  Owner: tramp@q3mcco35auwcstmt.onion
  Transaction amount: $1,150,000

10. Give 3 example(s) of interesting conversations.

There are many interesting conversations going on. Sometimes they spread over multiple messages between two persons. Others are interesting by themselves. Here we discuss three of such conversations.

First of all, entry 30219, as some other entries, give personal information about people. This particular message is in a conversation about recruiting people. It gives names, contact information, phone numbers and the years of experience they have.

- Entry 7371
- Entry 3399: This message contains a link to the DNB (De Nederlandse Bank) with the registry of many companies. This may have been a conversation about what companies to target.

11. Give 3 examples of complaining

Here are three messages included that complain. These are based on words such as ‘dissatisfied’, ‘terrible’ and ‘unacceptable’. See the python code to get the whole list of specification words. From the results, three messages were put here.

“*Regarding the whole story with the repository, here is my position. 1. For my part, I do not agree with the idea that I should be in touch 24 hours, I sold 8 hours of my time, and sometimes I stay late at work at will, but this is my free will, if I don’t want to, I won’t. I agree with you that I need to adjust my time, I&#39;m doing this, I&#39;ll try to solve it and be in touch during working hours, I generally have difficulty sleeping. It&#39;s not your problem, but I think it&#39;s good for you to know.*”

“*and why the heck did you sew on 31.14....? I didn’t ask for this from the list GENERAL_3 FAIL = 13 OF 30 instead of 13 you gave 6 fuck you touched other servers MODULES_2 FAIL = 21 OF 29 everything was normal now almost everything is not liquid what the fuck I ask you to flash routers once a month, what is it hard to do it??? what is the problem? I said 15 for each server, now it turns out to be complete garbage, come out urgently and fix it! otherwise we’ll say goodbye to me I don’t need such work --- 103.101.104.229:449 --- 103.102.73.165:449 --- 103.124.145.98:449 you flashed these in the wrong place, fucked up, everything went wrong in the wrong place, how can you screw up in three pines got lost I won’t even check further, take that original list that you gave me, change everything as it was, replace the fallen ones, and do everything urgently*”

“stern tells me where the results are and what can I do if they don’t want to work for 150k [01:21:56]<buza> so it&#39;s not me who raises [01:22:03]<buza> sn stern and raises [01:22:08]<buza> so tell him [01:22:33]<buza> my position is this: we are ready to raise the salary to what the candidate wants, if he can CONvincingly prove that he is worth the money [01:22:39]<salamandra> I write to him about the salary, he will get it. and now I put the question point-blank where are the results, otherwise I’ll fire you [01:22:58]<buza> let him not fire [01:23:07]<salamandra> pissing) [01:23:21]<buza> well, quote me to him, and give him statistics on how many resumes you had and how many of them were rejected because of salary [01:23:53]<buza> the problem is that I have no idea how he can convincingly prove his worth [01:24:20]<buza> if you do something difficult, he will solve it for a long time

[01:24:28]<buza> and some will refuse altogether [01:24:39]<buza> so he must show some of his past merits [01:24:43]<buza> like, I found such and such a CVE [01:25:23]<buza> in general, these are the problems of the candidate - I think that if a person wants 5-7k, and he REALLY deserves them, then he has baggage behind him that he can show"

12. How much they earn?

In the python code, messages that mention 'salary' are filtered.

"Hello, can you send a salary to this address 1KfDPgc6CiWb6Fnin1bLWi2moX1ViXANxW?" This bitcoin wallet had a transaction of $5774.08 USD.

"Hello. will you send a salary for 15QULY9y2HJj1i85LiJGMYWChhAqnGkCSx ?" This bitcoin wallet had a transaction of $3638.99 USD.

"bc1qc2gtz9eadvr9mf2xcptyatajakx93schz35aq7 3.5k was not enough for all the salary" This bitcoin wallet had a transaction of $2336.87 USD.

This means that employees from the company received earnings ranging from $2,336.87 to $5,774.08.

Amount from thousands or millions come across in the messages. Here are some examples of some of those messages:

"Yes, we gave you the not even standard discount, but probably in vain, because youâ€™re starting to repeat the old song again. you will see all the documents after we will publish it, if we do not achieve the result. Our price $5,500,000. You must explain this to the company. Now it's your problem."

"$3,700,000 is final for you! but may be not final for the the company. Now we are taking with director....waiting."

"and we charged them 25 million"

14. Language distribution

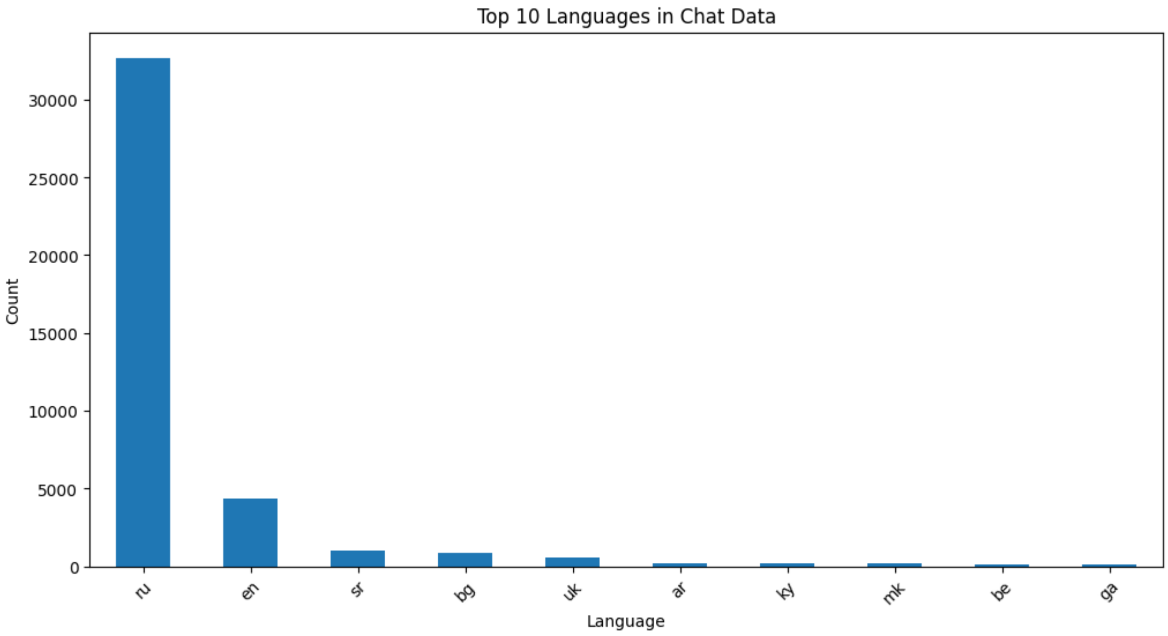

Figure X. Top 10 Languages in the data from the chat

In figure X. The most spoken languages from the chat can be seen. Russian is by far the most spoken language in the chats.

15. Percentage of unreadable messages

In the records a lot of entries have the text: “[Error: The message is encrypted and cannot be decrypted.]”, which could mean that these messages are more important and for that reason have to be encrypted even in the Jabber chat. When searching through all the records 14374 instances of these encrypted messages can be found. Comparing this to the total number of messages, the ratio 14374/60772 is found. Transforming this ratio in a percentage it is found that 23.7% of the messages are encrypted and can for this reason not be investigated. This is quite a large amount of data that can not be taken into account while possibly being very important due to the encrypted nature of the messages.

16. User activity

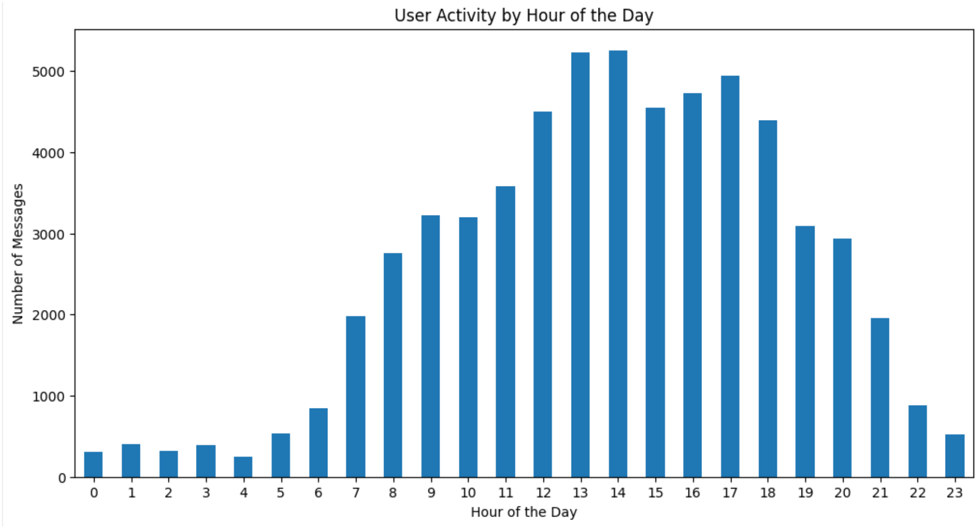

Figure X. User activity by hour

The peak activity during the day is between 13:00 and 14:00, see Figure X. This is from all dates represented in the ‘ts’ column. From this it can be seen that most of the activity happens during “normal” business hours.

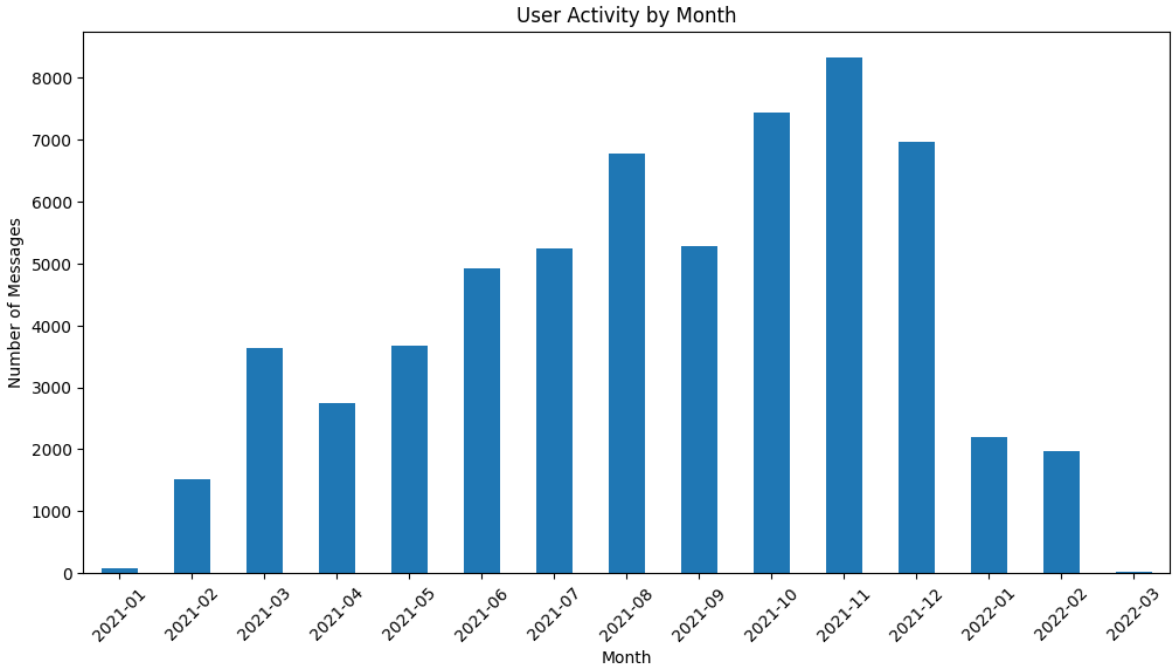

Figure X. User activity by Month

As can be seen in figure X, the most active months were October and November of 2021.

Conclusion and Reflection

In conclusion, this assignment explored the Conti ransomware group. The ransomware group was linked to the Russian government. The group operated with the use of a Ransomware-as-a-Service (RaaS) model. Double extortion techniques were used, to encrypt files and threaten the victim if the ransom isn't paid. With over 1.000 reported victims and over $150 million in payouts, it is the most successful known ransomware group. This enormous success makes this group a prime target to investigate and attempt to take down for government agencies such as the FBI. It also gives a lot of insight into the inner workings of this kind of ransomware groups, how they find their customers and how they move the money around. However this might prove to be difficult since by far the main language spoken is Russian, suggesting that the group is likely based in Russia and Russia is not known for aiding in the investigations into its cyber groups.

In the analysis, the activities of the Conti ransomware group were examined. For the analysis, multiple aspects were looked at. For some aspects, use of python was made to make sense of the data. The data was a large dataset of the leaked Jabber chat, consisting of 60772 records. The investigation involved multiple aspects, such as number of records, time span, top players, roles, mail accounts, IP addresses, URLs, bitcoin wallets, and more. This gave insight into the activities of the Conti group, but also the huge amounts of money transactions that were made, the financial impact it had, and the inner workings of the group.

A deeper analysis like this can be used by law enforcement agencies to get an overview of how such an organisation works.The information uncovered during this analysis could be used by law enforcement to more easily track down the individual criminals and have them face justice.

There are, however, some implications regarding the use of this analysis should be mentioned. The organisation Conti is an international organisation, which means that when law enforcement comes into play, they do not always have the means or authority to stop such an organisation. Conti had a number of active employees which were from a number of different countries. When they, for example, use their ransomware against a US company, the incident becomes of international nature. As the rules, regulations, and punishments vary from country to country, it is not as straightforward as to how the hackers should be prosecuted.

Another point which should be mentioned, is that not all aspects discussed give the full picture of the organisation Conti. For some, as mentioned in their titles, the analysis only covers the top results. For others, the analysis only covers the most interesting, according to the researchers. As the entire dataset consists of over 60.000 records, it was not possible to analyse all of them. Though this does not mean that the analysis is incomplete or worthless, the top results for most aspects are the most important for authorities to be aware of. Not every single individual who has sent a message to or from the Conti group needs to be paid as much attention as some of the top parties.

References

Conti Ransomware. (2022, March 9). CISA. Retrieved October 25, 2023, from https://www.cisa.gov/news-events/alerts/2021/09/22/conti-ransomware

Fier, J. (2021, December 7). *The double extortion business: Conti Ransomware Gang finds new avenues of negotiation*. Dartkrace. https://darktrace.com/blog/the-double-extortion-business-conti-ransomware-gang-finds-new-avenues-of-negotiation

Github: Digital Forensics Assignment 3. (2023, october 25). Github. Retrieved October 25, 2023, from https://github.com/Emma2002/DigitalForensics_Assignment3

Northwave Cybersecurity. (n.d.). *When the hackers get hacked pt 2*. Threat intel research. Retrieved October 25, 2023, from https://northwave-cybersecurity.com/threat-intel-research/when-the-hackers-get-hacked-pt2#NR1

Pitrelli, M. (2022, April 13). Leaked documents show notorious ransomware group has an HR department, performance reviews and an 'employee of the month'. *CNBC*. https://www.cnbc.com/2022/04/14/conti-ransomware-leak-shows-group-operates-like-normal-tech-company.html

Price, N. (2022, May 6). *Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice - United States Department of State*. State Department. Retrieved October 25, 2023, from https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/