CONFIDENTIAL

KELA
Intelligence Report

KELA
TARGETED CYBER INTELLIGENCE

Analysis of leaked Conti's internal data

March 15, 2022

Executive summary

On February 27, 2022, as a response to the Conti ransomware gang's support of the Russian invasion of Ukraine, a suspected Ukrainian researcher leaked internal conversations of its members. KELA analyzed the leaks to understand the group's evolution and TTPs, as well as organizational structure.

Main findings:

- Internal conversations show **an evolution of a gang of ransomware attackers who at first were not a part of a specific ransomware group.** They discussed Ryuk, Conti, and Maze as separate projects. Their activity eventually led to the formation of the modern Conti operation.
- The group used various malware and tools. KELA found **proof of Conti's strong connection to Trickbot and Emotet, as well as BazarBackdoor**, used for gaining initial access. The **Diavol ransomware appears to be Conti's side project**. As for legitimate tools, Conti attempted to **test products of VMware CarbonBlack and Sophos**.
- Conti used **services of Initial Access Brokers** to gain initial access.
- Conversations regarding **almost 100 victims - about a half of which were not publicly disclosed on Conti's blog - shed light on the attacks' process**, including multiple steps before and after the ransomware deployment.
- The gang's members **expressed interest in attacking the US public sector.**
- Conti's team is highly organized and includes **the following teams: hackers, coders, testers, reverse specialists, crypters, OSINT specialists, negotiators, IT support, HR**.
- KELA prepared **descriptions of the top-15 actors** based on the amount of their messages, as well as **their connection maps**.

Background

On February 25, 2022, the Conti ransomware gang pledged support in the Russian invasion of Ukraine. As a response, on February 27, 2022, a person who is suspected to be a Ukrainian researcher,[1] leaked internal conversations of Conti's members via a Twitter account called ContiLeaks. The conversations included:

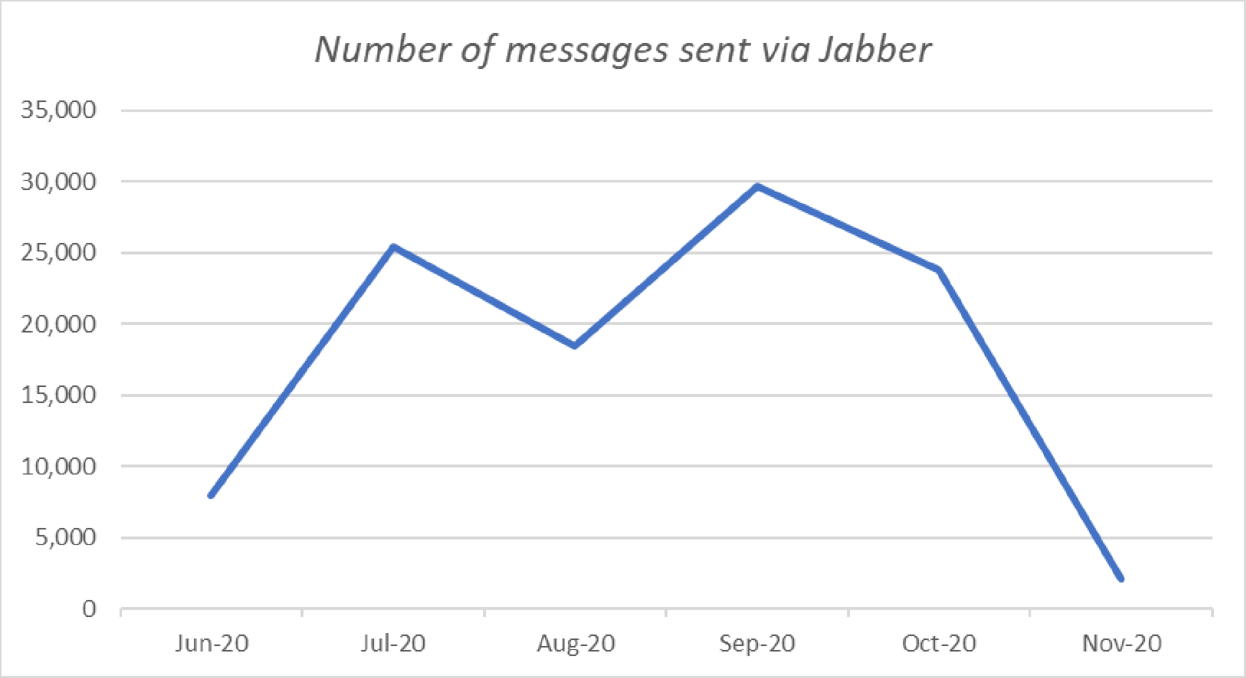
- Jabber logs posted in several parts by the original ContiLeaks profile on Twitter. Those appear to originate from the Conti Jabber server hosted at q3mcco35auwcstmt[.]onion. Most of the Jabber chats seem to be individual chats between each two members. The first part contains messages from June 21, 2020 to November 16, 2020, while the second part contains archives from January 29, 2021 to February 27, 2022, with some gaps.
- Rocket.Chat logs, also leaked by the original ContiLeaks profile. The leak included information from 6 different Rocket.Chat servers from August 31, 2020 to February 26, 2022. [2]

For this report, KELA analyzed conversations of actors extracted from Jabber logs, and partially used contents of Rocket.Chat logs to corroborate findings. It seems that at first Jabber was used for all kinds of conversations, including ongoing attacks. Towards 2021, most of the "technical conversations" (including hacking specific companies, coding assignments, etc.) were moved to Rocket.Chat. KELA is continuing to analyze the leaks to gain more insights.

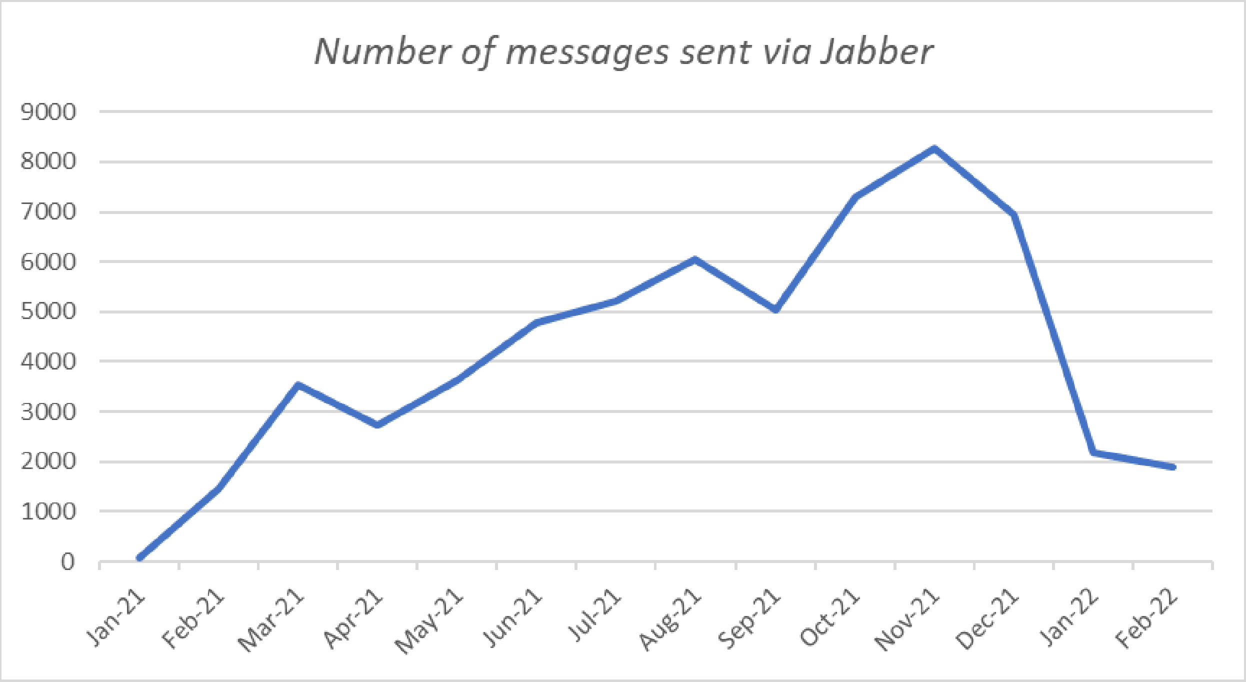
In addition, two Twitter accounts called Trickbotleaks and trickleaks (the second one emerged after the first one was banned) leaked Jabber logs alleged to originate in Trickbot operators' correspondence, as well as files that include information about 21 alleged Trickbot members. According to KELA's analysis, the chat data partially overlaps with information published by ContiLeaks, therefore, it was also used to supplement this report.

[1] https://www.databreachtoday.com/ukrainian-researcher-leaks-conti-ransomware-gang-data-a-18620

[2] Available in DARKBEAST by crawler:ContiJabberLeaks and crawler:ContiRocketChat*



Based on data from June 21, 2020 to November 16, 2020

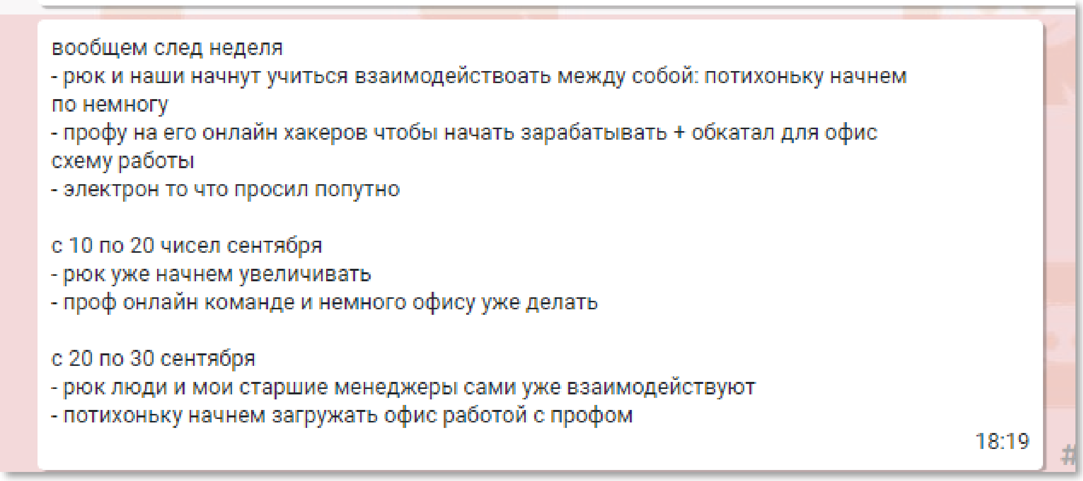


Based on data from January 29, 2021 to February 27, 2022

Conti's evolution

Conti was long ago suspected to be a successor of the Ryuk ransomware gang based on code similarities and the same template used in ransom notes.[3] Chainalysis, a blockchain investigation firm, claimed that the newly found "blockchain transactions confirm the substantial financial and operational overlap". For example, one of the high-ranking members of Conti - stern - was receiving commissions from both Conti and Ryuk.[4]

However, as observed by KELA, at least in some conversations Ryuk is described as a separate project. For example, when the group's ransomware was under development, the actor **stern** offered to **buza** to use Ryuk's samples found online. Another confusion is a cybercriminal referred to as **рюк** (ryuk) who is discussed as a person having his team of attackers. Conti's members are sharing conversations with him but the leak does not contain his messages; probably, they communicate on another platform. If he is connected to the Ryuk ransomware, then these teams indeed collaborated and possibly eventually united; it is also possible that this individual just uses the same name.



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

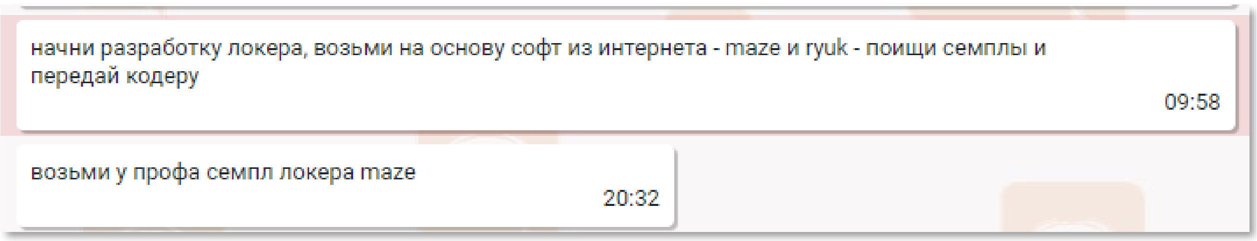
18:19

*August 27, 2020: **target** says to **stern** that their and **ryuk**'s employees will start to work together in September*

[3] https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/

[4] https://twitter.com/JBurnsKoven/status/1498679108812877824

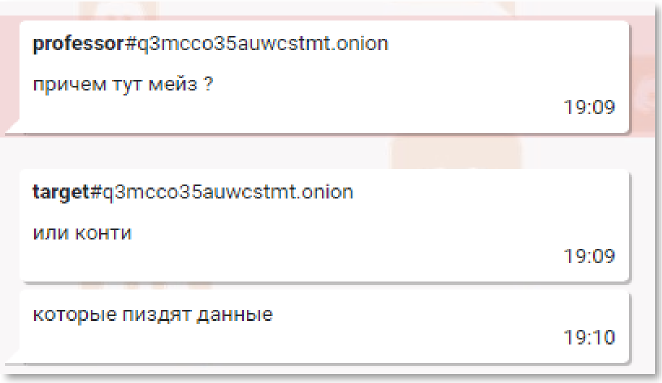
Early conversations of actors reveal that the group's members were using other ransomware strains, namely Maze — both for developing their own ransomware and both for attacking companies. The actors described even Conti as a separate project and mentioned that they were using their "own lockers" (locker is a slangy word for ransomware) in 2020 and early 2021.



начни разработку локера, возьми на основу софт из интернета - maze и ryuk - поищи семплы и передай кодеру
09:58

возьми у профа семпл локера maze
20:32

*July 9, 2020: **stern** asks **buza** to look for samples of "the software from the Internet - maze and ryuk" and ask a coder to develop a locker based on the samples*



professor#q3mcco35auwcstmt.onion
причем тут мейз ?
19:09

target#q3mcco35auwcstmt.onion
или конти
19:09

которые пиздят данные
19:10

*October 9, 2020: **professor** and **target** discuss Maze and Conti as separate operations*

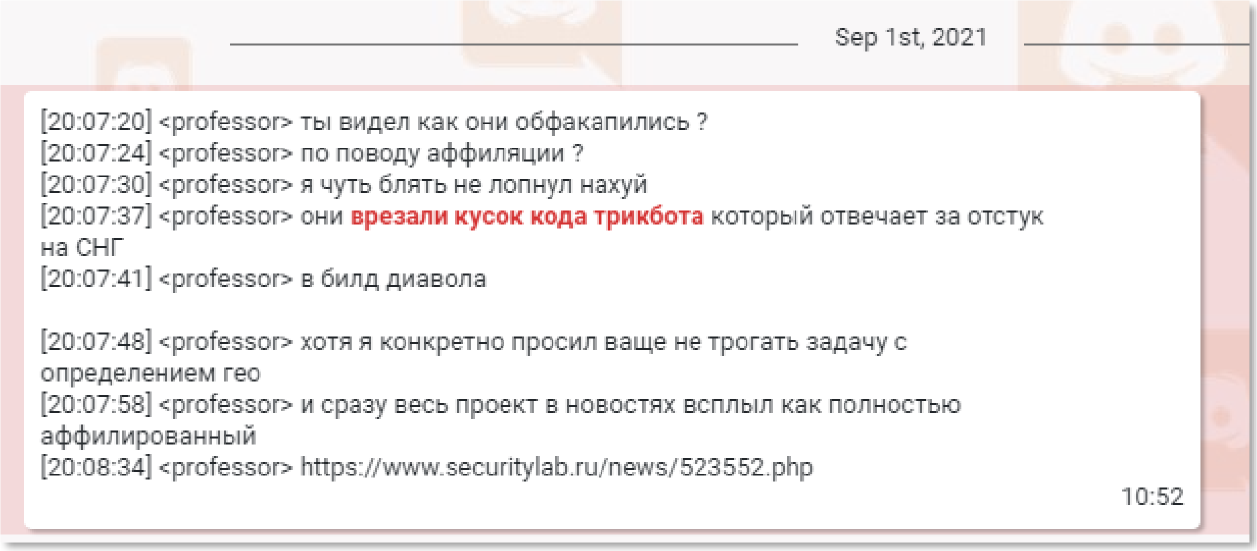
Therefore, KELA suggests that the Jabber server originally belonged to a gang of cybercriminals who were not a part of a specific ransomware group. Members of this group seem to have used different ransomware strains and collaborated with other cybercriminals, which eventually led to a formation of the Conti operation as it became known in the recent year. Some actors active in the early days seem to have become high-ranking managers of Conti. KELA has also seen indications that even in 2021-2022 some actors are running parallel operations and referring to Conti in the third person.

TTPs

Malware and tools

KELA found proof of Conti's strong connection to Trickbot and Emotet; both are infamous malware used by cybercriminals to initially install their ransomware. BazarBackdoor is also mentioned in conversations as another source of remote access to corporate networks.

As a side project, Conti appears to have the Diavol ransomware developed by a user called baget.



```
[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
[20:08:34] <professor> https://www.securitylab.ru/news/523552.php
10:52
```

*September 1, 2021: **professor** complains that Diavol's developers used part of the TrickBot code in the ransomware build, therefore Diavol was publicly affiliated with TrickBot*

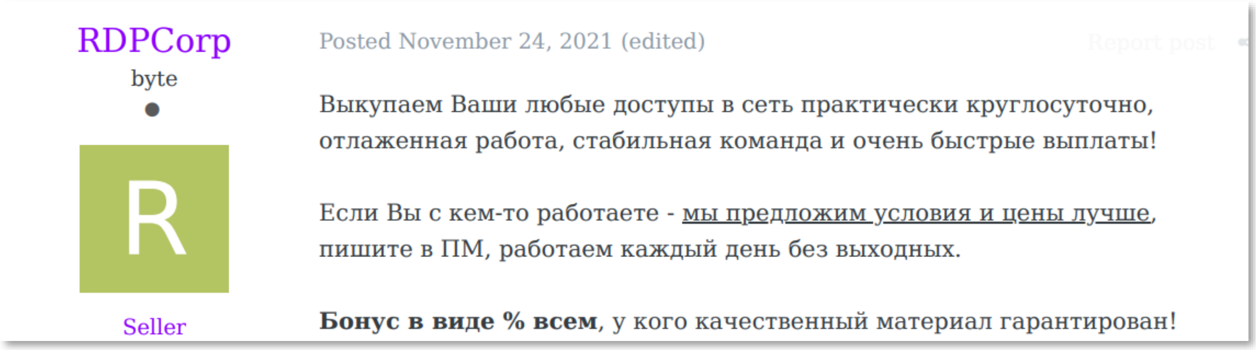
The group also widely abused legitimate tools, for example, tried to set up demos with security firms VMware CarbonBlack and Sophos attempting to test their products. At least with CarbonBlack, the actors succeeded in buying the products. Such tactics enable cybercriminals to practice their malware and methods against existing security solutions and learn how to bypass them.

Some tools popular among ransomware attackers were again confirmed to be in the group's arsenal: the post-exploitation tool CobaltStrike, the open-source application for collecting credentials Mimikatz, the Metasploit and Poverview frameworks, Cookie GRaber (originally

TrickBot's module) and more. The group was also seen discussing how to buy and/or develop exploits and scanning tools for specific vulnerabilities, such as CVE-2020-5135, a critical SonicWall VPN stack-based buffer overflow, and zero-day flaws.

Collaborations with IABs

Initial Access Brokers (IABs)[5] serve as another source of initial access for Conti's operators. Most of them appear to work with Conti for a share of ransom. One of the conversations, for example, reveals a negotiation between Conti and an actor active on the Russian-speaking cybercrime forums XSS, Exploit and RAMP. The actor used the Jabber account rdpcorp_@thesecure[.]biz, and was linked by KELA to a user called **RDPCorp** on these forums. There**,** actors behind RDPCorp buy "any network accesses" for a fixed price and then resell to Conti for a share of ransom. Discussing the working conditions with Conti, RDPCorp said they asked 35% of ransom for domain admin access and 15% for user-privileged access. Conti agreed to take only unprivileged access.



RDPCorp
byte
●
R
Seller

Posted November 24, 2021 (edited)

Report post

Выкупаем Ваши любые доступы в сеть практически круглосуточно, отлаженная работа, стабильная команда и очень быстрые выплаты!

Если Вы с кем-то работаете - мы предложим условия и цены лучше, пишите в ПМ, работаем каждый день без выходных.

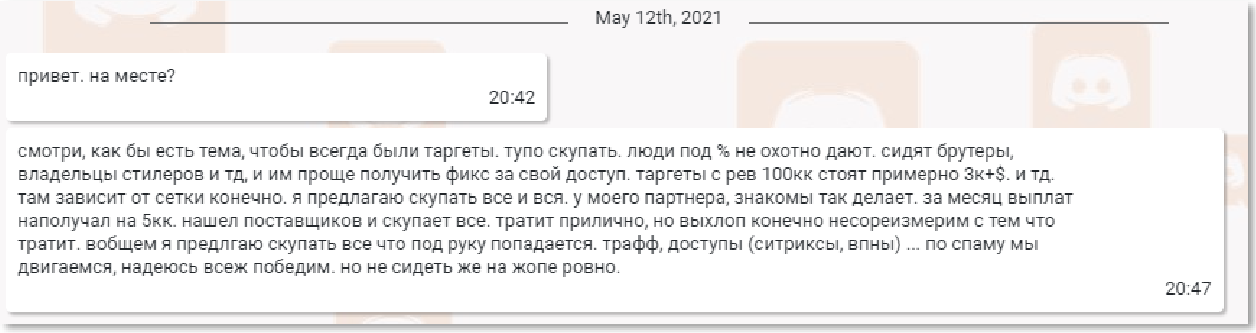
Бонус в виде % всем, у кого качественный материал гарантирован!

RDPCorp's announcement on Exploit: "We will buy any network access almost 24/7, we have an established process, stable team and really fast payment!"

On May 12, 2021, the actor **kevin** offered to **stern** to use a different strategy and just to buy all available network access for a fixed price: "My partner has a guy who does it. During one month, he received [ransom - KELA] payments of USD 5 million. He has found suppliers and

[5] These actors significantly facilitate network intrusions by selling remote access to a computer in a compromised organization (Initial Network Access) and linking opportunistic campaigns with targeted attackers. Read 5 real cases showing the path from start to end: https://ke-la.com/from-initial-access-to-ransomware-attack-5-real-cases-showing-the-path-from-start-to-end/

buys it all. He spends a lot, but his profits are incomparable to what he spends." Before and after this offer, **kevin** was seen "preparing targets" for Conti's hacking teams, meaning providing them with initial access to potential victims.



May 12th, 2021

привет. на месте?
20:42

смотри, как бы есть тема, чтобы всегда были таргеты. тупо скупать. люди под % не охотно дают. сидят брутеры, владельцы стилеров и тд, и им проще получить фикс за свой доступ. таргеты с рев 100кк стоят примерно 3к+$. и тд. там зависит от сетки конечно. я предлагаю скупать все и вся. у моего партнера, знакомы так делает. за месяц выплат наполучал на 5кк. нашел поставщиков и скупает все. тратит прилично, но выхлоп конечно несореизмерим с тем что тратит. вобщем я предлгаю скупать все что под руку попадается. трафф, доступы (ситриксы, впны) ... по спаму мы двигаемся, надеюсь всеж победим. но не сидеть же на жопе ровно.
20:47

May 12, 2021: kevin offers to buy all available network access: "People don't like to sell for %. There are brutes, owners of stealers, it is easier for them to receive a fix payment for their access."

Dissecting a Conti attack

When researching Conti's leaks, KELA found more than 50 victims that were attacked by Conti but that never publicly appeared on the blog, most likely meaning that these companies paid the ransom.[6] More than 40 victims found in conversations already appeared on the blog; some entries were later deleted due to the companies paying the ransom. The victims found and analyzed so far appear to be just the tip of the iceberg - KELA is continuing to analyze the leaks and expects to find more of those.

Conti members' conversations about the victims shed light on the attacks' process:

1. Hacking teams compromise a company's network, deploy ransomware and steal data. In the Rocket.Chat logs, a channel called "manuals_team_c" reveals 16 procedures used

[6] Available in Darkbeast by tag:"Conti leak" and category:"Ransom Event"

by Conti — from reconnaissance to exfiltration.[7] At least some of the manuals overlap with previously leaked manuals of the gang.[8]

2. An OSINT team collects information about the victim that can be used for further threats (contacts, top managers, etc.).
3. The OSINT team and other members analyze stolen data, try to brute-force password-protected folders and files and prepare a hidden post for Conti's "name and shame" blog based on the data. They also prepare reports that can be used for calling a company's employees/managers and blackmailing them.
4. OSINT teams and negotiators set ransom depending on the company's revenue gathered via business database services such as Zoominfo or DNB.
5. Negotiations take place. The person responsible for preparing the blog post negotiates with victims.
6. If the company agrees to pay ransom, it receives a decryptor and, in some cases, a report about methods used to compromise its network. If the company agrees to pay ransom after the blog post was published, the post is deleted.

For example, SVL, a provider of heating, ventilation, and air conditioning equipment (svl.com), was mentioned as one of the victims on December 12, 2021. The actors **bio** and **tramp** agreed to set a ransom amount of USD 800,000, based on the company's revenue of around USD 19 million as stated on ZoomInfo.

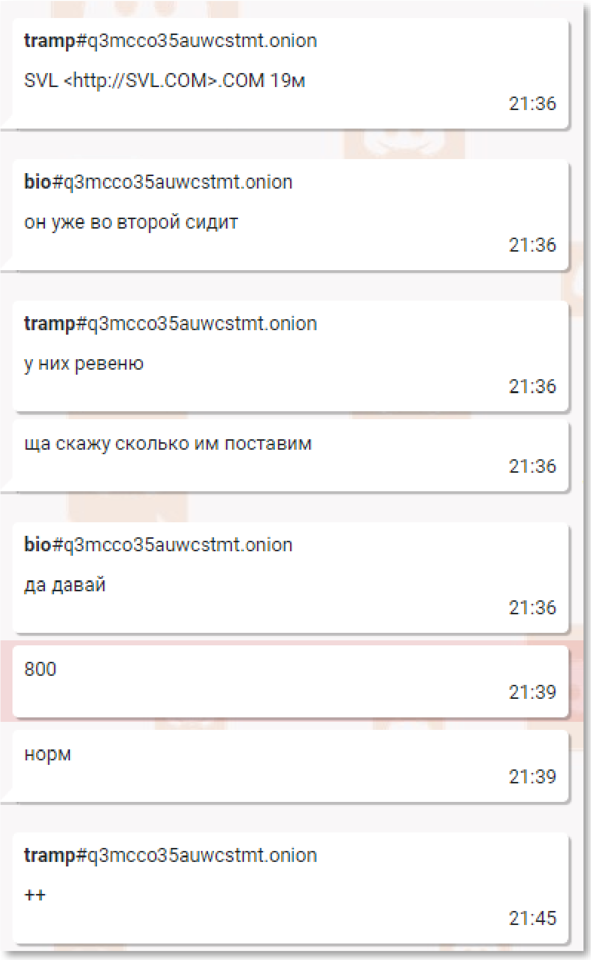
Then, they discussed negotiations and were going to threaten to call the company's managers to pressure them. **tramp** asked **bio**: "Write to him [a company's negotiator - KELA] that every day we will be calling to the management of the company and say that you are a person who

[7] https://github.com/Res260/conti_202202_leak_procedures

[8] On August 5, 2021, KELA observed the threat actor m1Geelka publishing what is claimed to be Conti ransomware gang's manuals on the XSS forum. The actor was apparently disappointed by the fact that the Conti operators promise to pay to affiliates a monthly fee of USD 1500 but do not rush to pay.

is not competent enough to negotiate with us. If they do not want problems and lawsuits from their own employees, they will just pay".

On December 20, 2021, bio said the company agreed to pay USD 500,000. The company apparently paid the ransom. In January 2022, according to the correspondence of the actors, SVL had issues with decrypting files; the actor **cybergangster** was taking care of the issues.



tramp#q3mcco35auwcstmt.onion
SVL <http://SVL.COM>.COM 19м
21:36

bio#q3mcco35auwcstmt.onion
он уже во второй сидит
21:36

tramp#q3mcco35auwcstmt.onion
у них ревеню
21:36

ща скажу сколько им поставим
21:36

bio#q3mcco35auwcstmt.onion
да давай
21:36

800
21:39

норм
21:39

tramp#q3mcco35auwcstmt.onion
++
21:45

December 12, 2021: ***bio*** *and* ***tramp*** *discuss what ransom amount to demand from SVL*

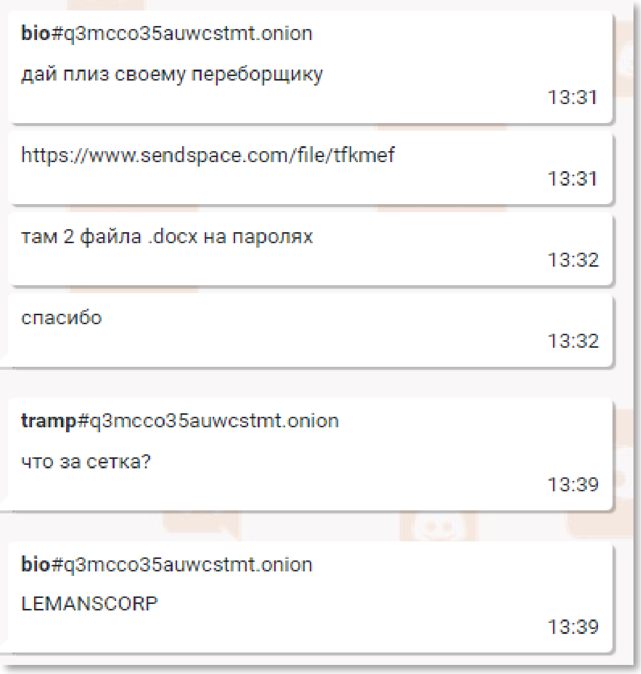
In conversations KELA reviewed, most of the ransoms demanded ranged between USD 800,000 and 8.3 million, usually equal to 1-3% of a company's revenue. During negotiations, a ransom could be lowered. For example, BSCR, a law firm (bscr-law.com), was asked for USD 1 million as a ransom. During negotiations, bio complained to tramp that no valuable data was stolen: most of the files were from 2016-2018, and the amount of data stolen was small. Conti and

BSCR agreed for a final payment of USD 300,000-400,000 (the final size of the ransom was not clear).

Conti was not always ready however to accept smaller ransom. Spencer Gifts, a mall retailer in the US and Canada (spencersonline.com), was attacked in November 2021. On December 2, 2021, bio and skippy discussed that a ransom amount that the victim agreed to pay - USD 450,000 - is too small. Following the discussion, the actors proceeded with publicly disclosing the victim.

Working with stolen data

Conti's methods of working with stolen data are interesting enough to discuss them separately. For example, they try to hack into password-protected files to gain more sensitive information that can be used to persuade a victim to pay ransom. For example, when discussing LeMans Corporation, a distributor in the powersports industry (lemanscorporation.com), **bio** asked if **tramp** can assign another member to brute force password-protected files stolen from the network.



bio#q3mcco35auwcstmt.onion

дай плиз своему переборщику 13:31

https://www.sendspace.com/file/tfkmef 13:31

там 2 файла .docx на паролях 13:32

спасибо 13:32

tramp#q3mcco35auwcstmt.onion

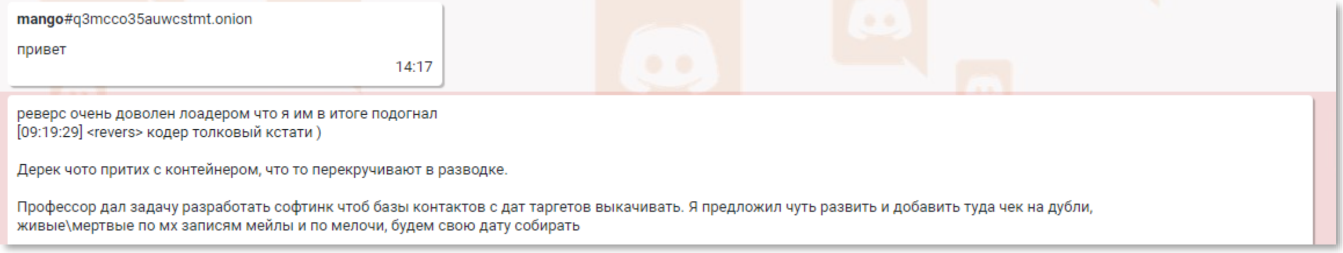
что за сетка? 13:39

bio#q3mcco35auwcstmt.onion

LEMANSCORP 13:39

*December 10, 2021: **bio** asks **tramp** to assist with hacking passwords for two password-protected files*

Also, the actors may use specific tools to extract email and other contacts of a victim company's employees, partners, and other third parties from the stolen data — it was a task discussed by actors in March 2021. The tool was supposed to remove duplicates and check if emails are active.



mango#q3mcco35auwcstmt.onion

привет

14:17

реверс очень доволен лоадером что я им в итоге подогнал
[09:19:29] <revers> кодер толковый кстати)

Дерек чото притих с контейнером, что то перекручивают в разводке.

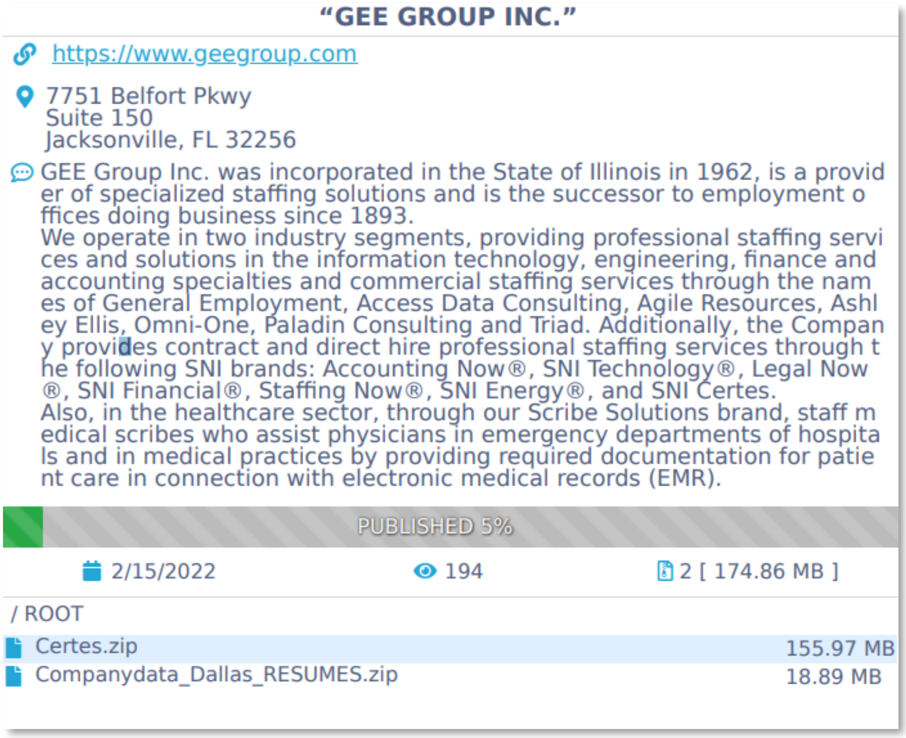
Профессор дал задачу разработать софтинк чтоб базы контактов с дат таргетов выкачивать. Я предложил чуть развить и добавить туда чек на дубли,
живые\мертвые по мх записям мейлы и по мелочи, будем свою дату собирать

*March 16, 2021: **mango** describes that **professor** has a task to develop software "to extract databases containing contacts from our targets' data." He offers to add several features, such as checking for duplicates and emails' validity*

Hidden blogs and negotiations

The Conti actors prepare hidden blog posts about victims meaning the posts can be accessed only via a specific URL. They share this hidden blog post with a victim to intimidate them by how easy the victim's data can be accessed. If a victim agrees to pay, the post is never released; if a negotiation fails, the blog becomes publicly accessible, and the victim's name is disclosed. On November 10, 2021, **bio** described it as a significant leverage: "Say what you like, but a hidden blog is really a cool thing, it is working on them."

Some victims were not persuaded by hidden blogs but agreed to pay when the blog was published for everyone. Gee Group, a provider of staffing solutions in the US (geegroup.com), was published as a victim on Conti's blog on February 15, 2022. Two days later, **pumba (bio)** asked **tramp** to provide him with a bitcoin wallet for "geegroup" and to send them "deletion logs". KELA reviewed Conti's website and found that the entry for Gee Group is not available on the website anymore. This would mean that the bitcoin wallet was requested for payment from Gee Group, and that the company indeed paid.



“GEE GROUP INC.”

https://www.geegroup.com

7751 Belfort Pkwy
Suite 150
Jacksonville, FL 32256

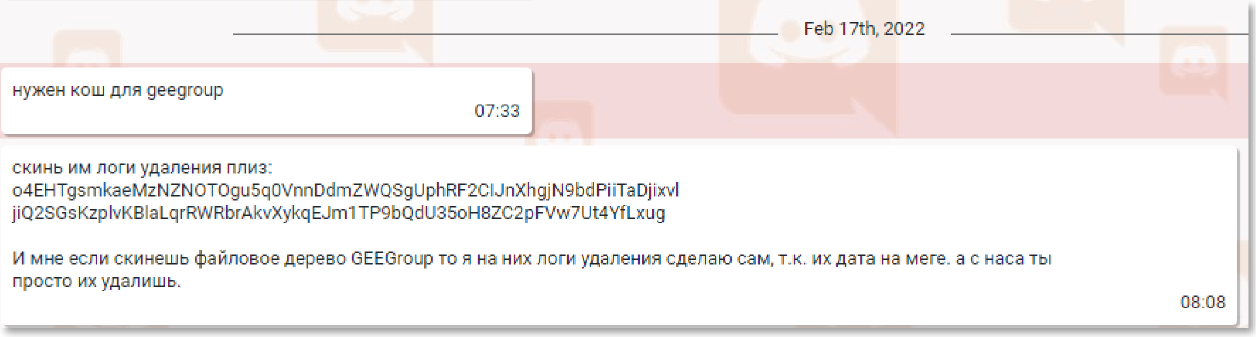
GEE Group Inc. was incorporated in the State of Illinois in 1962, is a provider of specialized staffing solutions and is the successor to employment offices doing business since 1893.
We operate in two industry segments, providing professional staffing services and solutions in the information technology, engineering, finance and accounting specialties and commercial staffing services through the names of General Employment, Access Data Consulting, Agile Resources, Ashley Ellis, Omni-One, Paladin Consulting and Triad. Additionally, the Company provides contract and direct hire professional staffing services through the following SNI brands: Accounting Now®, SNI Technology®, Legal Now®, SNI Financial®, Staffing Now®, SNI Energy®, and SNI Certes.
Also, in the healthcare sector, through our Scribe Solutions brand, staff medical scribes who assist physicians in emergency departments of hospitals and in medical practices by providing required documentation for patient care in connection with electronic medical records (EMR).

2/15/2022 | 194 | 2 [174.86 MB]

/ ROOT

Certes.zip	155.97 MB
Companydata_Dallas_RESUMES.zip	18.89 MB

Conti’s post about Gee Group (now deleted)



Feb 17th, 2022

нужен кош для geegroup
07:33

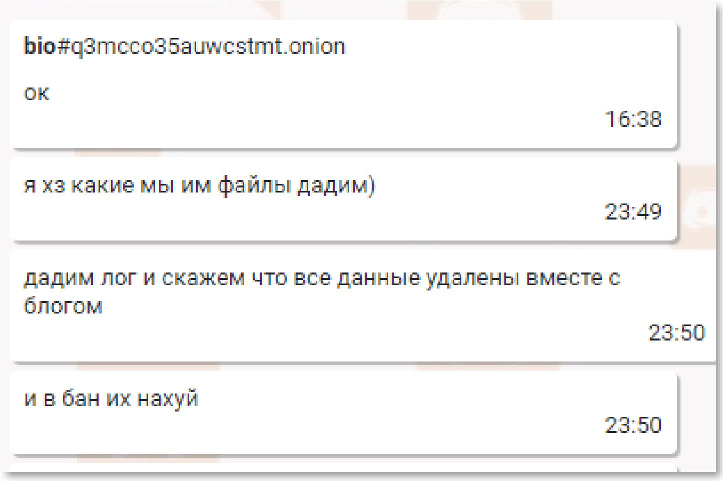
скинь им логи удаления плиз:
o4EHTgsmkaeMzNZNOTOgu5q0VnnDdmZWQSgUphRF2ClJnXhgjN9bdPiiTaDjixvl
jiQ2SGsKzplvKBlaLqrRWRbrAkvXykqEJm1TP9bQdU35oH8ZC2pFVw7Ut4YfLxug

И мне если скинешь файловое дерево GEEGroup то я на них логи удаления сделаю сам, т.к. их дата на меге. а с наса ты просто их удалишь.
08:08

*February 17, 2022: **bio** asks **tramp** to provide deletion logs for Gee Group*

Interestingly, Conti frequently lies to victims about the stolen data insisting that they have more than what was actually stolen. For example, when discussing Houle, an electrical contractor in Canada (houle.ca), **bio** complained to **skippy** that he could not find files requested by the victim. **bio** claimed the team that was attacking the network did not download all the files from the file tree that was later demonstrated to the victim. Another example is HKI (Helen Keller International), a global health organization (hki.org): **bio** said to

skippy that only 8 GB of data were stolen from their network, though a larger amount was claimed in discussions with the victim. HKI agreed to pay USD 1,150,000.



bio#q3mcco35auwcstmt.onion

ок

16:38

я хз какие мы им файлы дадим)

23:49

дадим лог и скажем что все данные удалены вместе с блогом

23:50

и в бан их нахуй

23:50

*November 30, 2021: **bio** doubts how to provide stolen files to HKI; he decides to give them "logs" (most likely deletion logs) and say that all the data is deleted together with the blog post*

Government-related attacks and issues

Conti's leaks reveal numerous conversations about US and Russian authorities. Especially interesting is the group's planned focus on the US public sector. In July 2020, **target** suggested creating a team responsible for attacks on this sector. The group was supposed to research documents stolen from already compromised victims to define possible interesting government targets. He offered identifying all counterparties by their payments and correspondence and dividing them by priority. The main department will be preparing the attacks and compromising networks.

target stated that the current work-scheme does not have consistency and control over the US public sector, and if this mission is important, they ought to build a specific system. Since the conversation took place in 2020, when Conti was not a well-established operation, it is not clear if the plan was performed.

A month after the US public sector conversation, **stern** and **electronic** suspected the US authorities were hitting them back. On August 21, 2020, **stern** said that an individual had hacked his server and left their Jabber in a note. When connected, the individual asked several questions about whether Conti accepted requests to compromise specific networks and how Conti is connected to “US hacks”. **stern** speculated that the person might be a researcher or a government-related hacker. **electronic** shared he was also approached with questions concerning the elections (likely the US elections) previously.

Organization

Structure

The current Conti team is highly organized and divided into different teams:

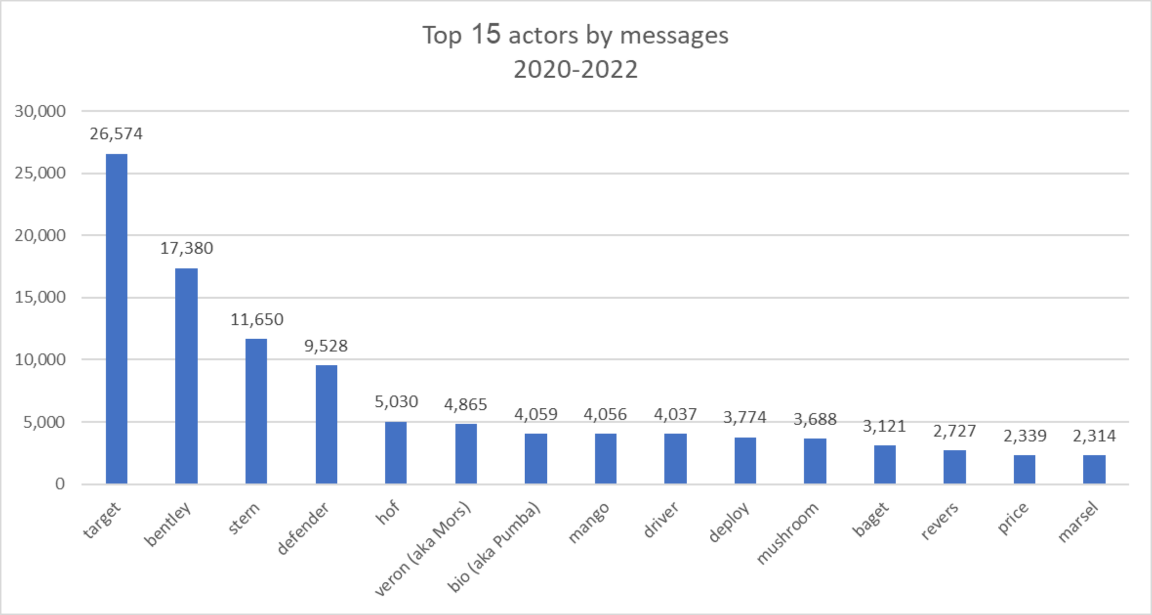
- Hackers - members directly compromising the network. They escalate privileges, move laterally, download data, and deploy ransomware. There are several teams of hackers, **revers** and **hors** are among the team leaders.
- Coders - members responsible for developing malware. Some of them are not familiar with the product they are writing the code for and were found through legitimate job searching sites. **Buza** is their team leader.
- Reverse engineering specialists - members capable of reverse engineering to contribute to the malware developers.
- Crypters - members engaging with obfuscating the malware builds in order to avoid detection by security solutions. **Bentley** is one such actor.
- Testers - members testing malware for detection by security solutions.
- OSINT specialists - members working with stolen data and finding more information about the company and preparing blog posts about victims. **Bio/pumba** and **buza** are such actors.
- Negotiators - members handling negotiations with victims, discussing ransom amounts and assisting with their requests to other team members (test decrypting, getting deletions logs, etc.).
- Callers – members who call a company’s employees/managers and blackmail them using data from the OSINT team.

- IT support - members supporting the operation's infrastructure and serving as system administrators.
- HR - a department hiring members through various sources. Aside from cybercrime forums, Conti uses various legitimate job searching sites, mostly Russia-focused, such as HH.ru and SuperJob.ru. **Salamandra** is one such actor.

In July 2021, Conti employed more than 100 people. Salary budget in this month was USD 164,800 as claimed by mango, who was distributing salaries between members of the team. Average salary for a member in July 2021 was around USD 1800. At least some members of the group were sitting in one office in Russia, based on their conversations related to ordering food and meeting in a real-life setting.

Top actors

KELA analyzed Conti's leaks and identified the top 15 actors who are highly involved in the conversations. For each actor, KELA prepared a description of their activity.



Source: Jabber Logs

#1 - target

# of messages	26,574
Period of activity	June 22, 2020 - October 2021
Role	Manager
Top connected actors	bentley, stern, troy

Target is a manager, responsible for the daily workload and intercommunication between different teams. On October 9, 2020, target discussed with **stern** the percentage of ransom payment they are going to receive after a successful operation. Moreover, they discussed changes in the hacking team and their intention to expand the recruiting process.

#2 - bentley

# of messages	17,380
Period of activity	Since June 22, 2020
Role	Technical lead
Top connected actors	deploy, target, marsel

bentley is a technical lead, a crypter whose role is to encrypt, obfuscate and manipulate the group’s malware in order to make it difficult to detect by security software. A chat from July 27, 2021 reveals that bentley is in charge for crypting different types of malware such as Trickbot, various malware loaders, Cobalt Strike and PowerShell-based malware.

bentley is also mentioned within the TrickBot doxxing leak. Pivoting on his Jabber account from the dox, KELA managed to identify his threads on the Exploit forum, under the moniker volhvb. It seems that the actor is responsible also for buying code signing certificates.

#3 - stern

# of messages	11,650
Period of activity	June 22, 2020 - December 2021
Role	High-ranking manager
Top connected actors	target, bentley, mango

stern is an important leader, managing the group's operation and considered the "big boss". As such, he frequently asked various departments for updates on their daily assignments. Moreover, it seems that the actor was directly involved in the recruitment and onboarding process and also responsible for paying salaries to different members.

On July 17, 2020, stern was mentioned as the "boss" responsible for the salary. Furthermore, on September 15, 2020, stern asked **mango** to recruit 3-4 "testers" and stated the salary - USD1200. It seems that stern is actively involved in the projects, checking on the members and their tasks' progress. For example, In March 2021, stern asked **hof** to fix the problems with TrickBot, saying that bots are not loaded properly.

#4 - defender

# of messages	9528
Period of activity	Since June 22, 2020
Role	Coders' lead
Top connected actors	driver, veron (aka mors) and hof

defender is most likely a technical lead of some of the coders including **zulas, ttrr, flip, driver** and **steller**. For those purposes, he was also seen seeking out tools for his work. On September

24, 2020, defender asked **ganesh** to buy accesses from Exploit forum and also asked to search for a person who brute forces and sells compromised routers. defender was the most dominant actor in 2021 with the highest number of messages.

#5 - hof

# of messages	5030
Period of activity	June 22, 2020 - December 2021
Role	Head of the hacking team
Top connected actors	Defender, bentley, driver

hof is considered as the head of the team of the malware' coders. On August 24, 2020, **stern** told **dark**, a new programmer, to reach out to hof for his first assignment. Also, on September 4, 2020, **stern** asked **viper** to assist hof with recruitment of coders with special languages' knowledge.

#6 - veron (mors)

# of messages	4865
Period of activity	Since June 26, 2020
Role	A coder
Top connected actors	defender, deploy, marsel

veron (aka mors) was discussed in the context of providing traffic from spam, and in one of the chats, he specifically introduced himself as someone who was "loading from Emotet." On September 21, 2020, **stern** told **mango** that "mors is our most important person", to which mango answered - "the most important coder or generally speaking?"

#7 - bio

# of messages	4059
Period of activity	Since November 2, 2021
Role	OSINT specialist and negotiator
Other aliases	Pumba
Top connected actors	tramp, skippy, cybergangster

bio (aka pumba) joined the team in November 2021. It appears that bio is responsible for reviewing documents for blog posts, preparing and publishing blogs and in some cases even setting ransom payments. He messaged the most with the actor **tramp**, usually consulting with him about the victims and the timeframe of publishing blogs.

#8 - mango

# of messages	4056
Period of activity	Since June 21, 2020
Role	General manager
Other aliases	khano
Top connected actors	stern, bentley, dollar

mango is a general manager providing support to **stern**, and assistance to the teams. As part of his activities, he was also looking for compromised network accesses for deploying ransomware. mango claimed to also solve problems between the “traffers” (people who supply traffic for infections) and the coders. On August 3, 2021, mango asked **elvira** to write a report indicating the new people that joined the teams including their nicknames, starting date of employment, their team leaders, a backup of jabber communication and the salary they agreed on. On December 3, 2021, mango said to one of the new employees: "I'm like a local sheriff here:)"

Based on the conversations' analysis, the majority of the conversations (69%) occurred in 2021. 45% of mango's conversations in 2021 were addressed to **stern**. On February 1, 2021, in a conversation between them, mango reported that he "published on all forums that I'll take different accesses for percentage: bots, rdp, vpn". KELA looked for similar posts in the cybercrime forums monitored, and was able to track two publications on the XSS and Exploit forums that were phrased in this manner by an actor named khano on the same day. Based on other posts by khano, where an affiliation with "one of the best solutions on the market" is mentioned, KELA concludes with high confidence that this is at least one of the aliases used by mango in those sources.

#9 - driver

# of messages	4037
Period of activity	Since October 28, 2020
Role	coder
Top connected actors	defender, specter, hof

driver is a backend php coder, most likely part of the coders' team directed by **defender**. The actor was recruited in October 2020 and expressed his willingness to take part in high load projects. In July 2021, driver was already experienced in the daily work, assisting other new coders.

#10 - deploy

# of messages	3774
Period of activity	June 22, 2020 - November 2020
Role	Crypter
Top connected actors	bentley, veron (mors), hof

deploy is one of the crypters described by **stern** as “the chief among the crypters”. Logically, the majority of his messages (58%) were submitted to **bentley**, who is a technical manager, involved in obfuscating Conti’s malware.

#11 - mushroom

# of messages	3688
Period of activity	June 22, 2020 - September 2021
Role	Loader builder
Top connected actors	bentley, price, frog

Among other things, mushroom appears to be responsible for building and developing the malware loader, improving its runtime. On September 16, 2020, he claimed that **stern** asked him to make the runtime shorter due to several detections, complaining about the difficult task. Almost a third of his messages were addressed to **price**, for example in one of the chats they discussed testing the “bot loader.” Mushroom was mentioned in TrickBot doxxing, including his contact details and social media accounts.

#12 - baget

# of messages	3121
Period of activity	Since June 22, 2020
Role	Coder
Top connected actors	braun, hof, stern

baget is one of the coders. On September 8, 2020, **buza** claimed that baget finished writing the backdoor, a type of malware. Baget was also mentioned within TrickBot doxxing leak as a coder, proficient in C/C++ programming languages and the developer of Diavol ransomware.

#13 - revers

# of messages	2727
Period of activity	June 22, 2020 - January 2022
Role	Hacking team lead
Top connected actors	Target, stern, taker

reverse is a hacking team lead. On May 11, 2021, **viper**, an actor seen to be active in the recruitment process, told **cheesecake**, a new coder, to contact revers, who is a team leader and will serve as his supervisor.

#14 - price

# of messages	2339
Period of activity	June 21, 2020 - October 2021
Role	Coder
Top connected actors	mushroom, target, hof

price is a coder developing, among other projects, backdoors and loaders The actor was active mainly in 2020, while in 2021 he was involved only in 3 conversations.

#15 - marsel

# of messages	2314
Period of activity	June 22, 2020 - October 2021
Role	Crypter
Top connected actors	bentley, veron (mors), green

marsel was seen chatting mainly in 2020 and appears to be a crypter.

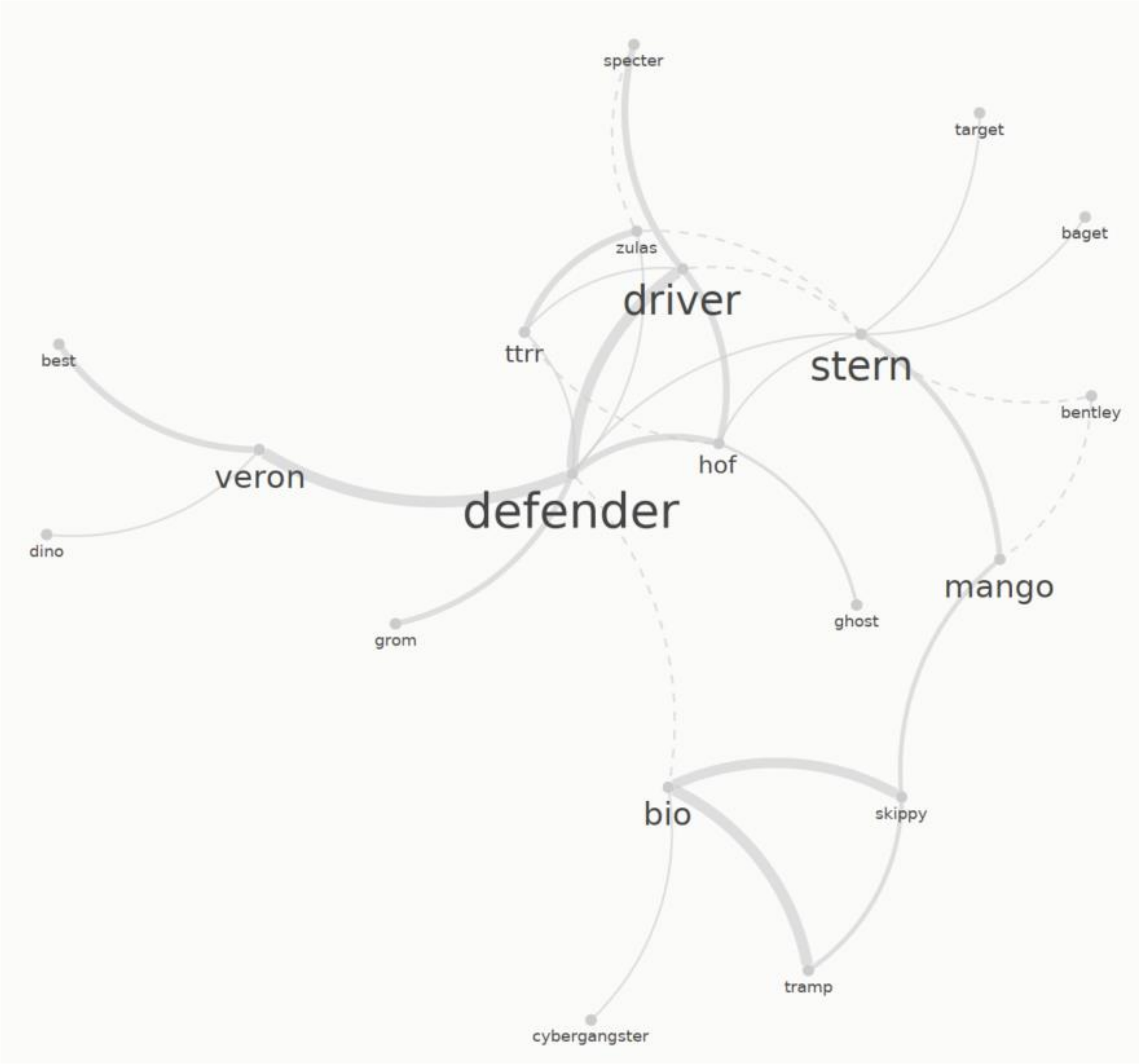
KELA identified other important actors that were mentioned in Conti's leaks but were not in the top. For example, **buza,** who served as head of OSINT intelligence and team leader of coders. He was active from June 2020 to January 2022.

professor seems to be a high-ranking manager, who was responsible for managing Conti's tools. The actor was active from June 2020 to December 2021. On July 9, 2020, he stated to stern that he is in contact with Maze developers.

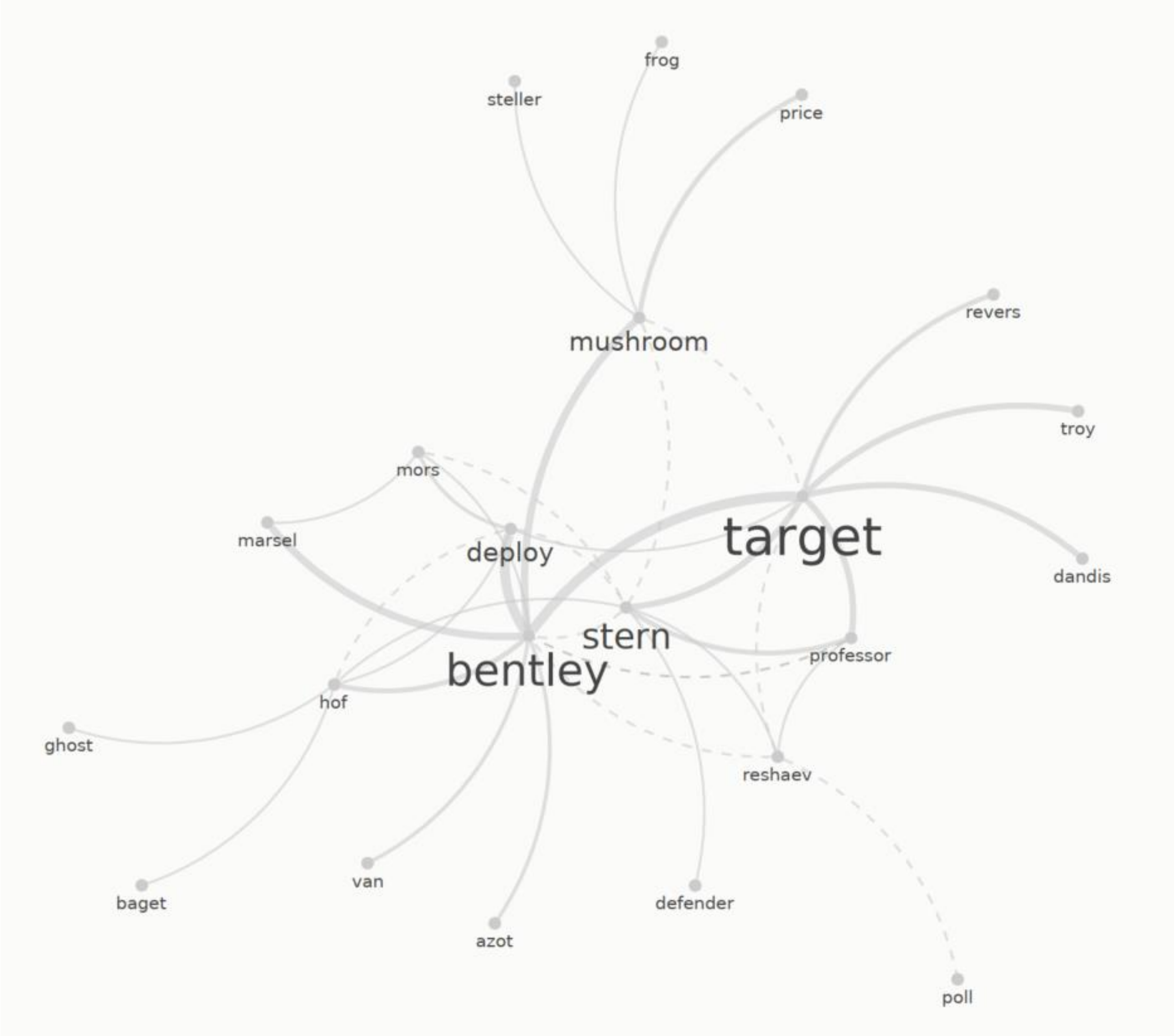
tramp is another high-ranking manager who is active under this handle from November 2021. However, the actor seems to play too important role to join so recently; it is possible he was active under another handle. This is strengthened by a correspondence between tramp and bio whereby tramp stated that he also operates "a second panel and a second team." Another important actor is **reshaev** who is a senior manager helping to coordinate other development tasks. The actor was active from June 2020 to November 2021.

Top actors' interaction

When exploring the actors' interaction, KELA found that the most active actors and the most popular chats are drastically different in 2020 and 2021-2022. KELA suggests it can be caused both by changes in Conti's team and the increased usage of Rocket.Chat after 2020. The following maps present the top actors' interactions for both periods, with the bold lines being the strongest connections and dashed lines being the weakest connections. Size of the actor's name depends on the amount of messages sent.



Actors' interactions in 2021-2022



Actors' interactions in 2020

Conclusion

The leak of Conti's internal information contains a massive amount of data; they were already compared to Panama Papers[9] and various new IOCs were found.[10] Further analysis of the leak will provide more insights on Conti's TTPs and methods of work, though it is already clear that the group operates like a highly organized legitimate business. It is possible that more information about other cybercriminals will be leaked following this incident. For example, a Twitter account f_0_r_e_v_e_r_ hinted that a leak of TOX messages of LockBit could be on the way.[11] In the era of increased competition between ransomware gangs and during a tense political situation, enterprise defenders should closely monitor cybercrime sources to timely detect such leaks and use them for protection.

[9] A leak of more than 11.5 million financial and legal records that took place in April 2016 and exposes a system that enables crime and corruption.
[10] Shared by KELA in an Excel spreadsheet along with this report. Sources:
https://www.cisa.gov/uscert/ncas/alerts/aa21-265a
https://www.forescout.com/resources/analysis-of-conti-leaks/
https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/
[11] https://twitter.com/f_0_r_e_v_e_r_?t=ssOLFBJ88U-ZyrGjiO75MA&s=09

KELA

TARGETED CYBER INTELLIGENCE