CYJAX

Threat Intelligence
Securing The Future

Who is Trickbot?

Analysis of the Trickbot Leaks

CYJAX

Contents

Introduction 3
Overview 3
Methodologies of Investigation 4
Key Findings 4
The Members Uncovered 4
The “Doxing PDFs” 5
The Member List 6
Operational Infrastructure 8
“Bots and Loaders” 8
Operational Servers 9
Example usage of infrastructure 10
Botleggers Club 11
Development Teams 12
Crypter group 12
Loader groups 13
Tox group 14
Locker group 15
Fire_Team group 15
Observations 17
Trickbot is a business 17
Trickbot are collaborating 20
Trickbot are changing 23
Conclusion 24
Appendices 25
Appendix 1: The Cryptolocker Terms of Reference 25

Introduction

CYJAX limited is a cyber threat intelligence company based in London, United Kingdom. The work we do helps organisations globally to protect their critical business assets from cyber-attacks. The selected research reports we make publicly available are for informational purposes only and are based on evidence that was available at the time of writing. We encourage you to share with the opensource community any new insights that this research leads to.

Overview

Since the start of the Russia-Ukraine conflict, Russian based cybercrime groups have been placed into a difficult position. With many groups being comprised of a variety of different nationalities, the various members need to make decisions on allegiance. Leading the charge was the Conti ransomware group who decided on 25 February 2022 to make a post detailing their full support for the Russian government, shown in ***Figure 1***, communicating their willingness to fight against those who oppose them. This post came only one day after the invasion of Ukraine on 24 February 2022. It is possible that Conti were required to post this, resulting in the fast reaction time to the invasion, due to the Russian governmental ties the group holds.

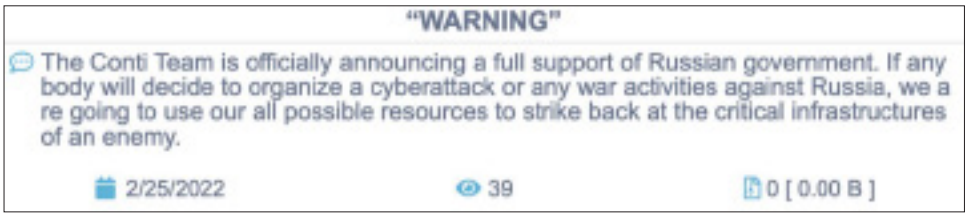


Figure 1

This post caused shockwaves in both the intelligence community and within Conti itself. Many members of the group were unhappy with this decision, either not wishing to be seen supporting the Russian government or being from the victim country Ukraine. This inevitably led to Conti retracting their statement only two days later, now saying they only wish to target the "Western warmongers" and "[do] not ally with any governments and [...] condemn the ongoing war".

Figure 2

However, this reversal was not enough for most members, resulting in them becoming one of the most targeted ransomware groups by Ukrainian supporting organisations and other threat actors. It did not take long for this unrest to lead to action when on 27 February 2022, a Twitter account @ContiLeaks began posting links to the logs of internal communications by the group. Within hours threat intelligence researchers around the world were beginning to conduct analysis into the dump, containing over 60,000 messages. This leak caused significant unrest within the group, with the @ContiLeaks account itself tweeting: "We know everything about you Conti, go to panic, you can['t] even trust your gf, we against you!".

On 4 March 2022, whilst mass attention was focused on @ContiLeaks, another account @trickleaks was created, posting the tweet: "We have evidence of the FSB's cooperation with members of the Trickbot criminal group (Wizard Spider, Maze, Conti, Diavol, Ruyk)". After this damning message, tweets began to appear containing links to internal communications from members of the Trickbot group. At time of writing, the @trickleaks account has approximately 1,700 followers. This is about five times less followers than the @ContiLeaks account. These leaks, which I will refer to as the Trickbot Leaks, were posted increasingly

quickly as 35 believed member's messages were uploaded over a two-month period. This led to a total of over 1000 communication extracts.

Each file consists of a direct communication or a group chat involving the user, which range in size. Some files contain nearly 10,000 messages. In total, there are approximately 250,000 messages which contain over 2,500 IP addresses, around 500 potential crypto wallet addresses, and thousands of domains and email addresses.

This leak was like nothing seen before and gave cyber threat intelligence researchers unprecedented access to the Trickbot organisation. To put this leak into perspective, it was over four times the size of the Conti leaks which was seen by some researchers as one of the most useful information dumps of the past few years. Alongside these messages, PDF files were leaked which contained large amounts of information reportedly about individual members. This included full names, addresses and identification numbers. These "Doxing PDF" files have given us the ability to analyse the people behind the usernames, examining how and why they are working for the criminal organisation.

Within this report we will analyse and discuss the full extent of the content of these leaks, from the infrastructure and tooling the criminal organisation uses to the inner workings of how the group operates.

Methodologies of Investigation

Researching these leaks was a task which required development of a series of bespoke tools and processes to accurately analyse the data. Not only was the information in large quantities, but almost all of it was of Russian origin and composed in the Russian language. As a UK-based cyber security researcher, I am not fluent in Russian nor the slang that is commonly used throughout the messages which can be a language of itself. For example, words such as "Жаба" refer to the messaging service "Jabber", whilst directly translating to the word "Toad". This means that standard translation tools can encounter issues with these messages and some nuance could be missed, as well as specific cybercriminal group "code" or "hacker speak" words.

It is also apparent that some context may be missing from certain conversations, as I cannot be certain that I have all the messages from all communication platforms. Despite this being a large leak with thousands of messages, there is potentially other platforms, channels, or conversations that exist which I do not have access to. This may lead to exchanges where I am missing certain context or background information.

Despite these challenges, this paper contains key findings which break open and reveal some of the fundamental processes behind the Trickbot organisation. This analysis includes a breakdown of the attack infrastructure used by the organisation, enabling researchers to analyse and develop heuristic defence approaches. It also creates an understanding of how the group operates, identifying their "business-like" nature and efficient teamwork.

Key Findings

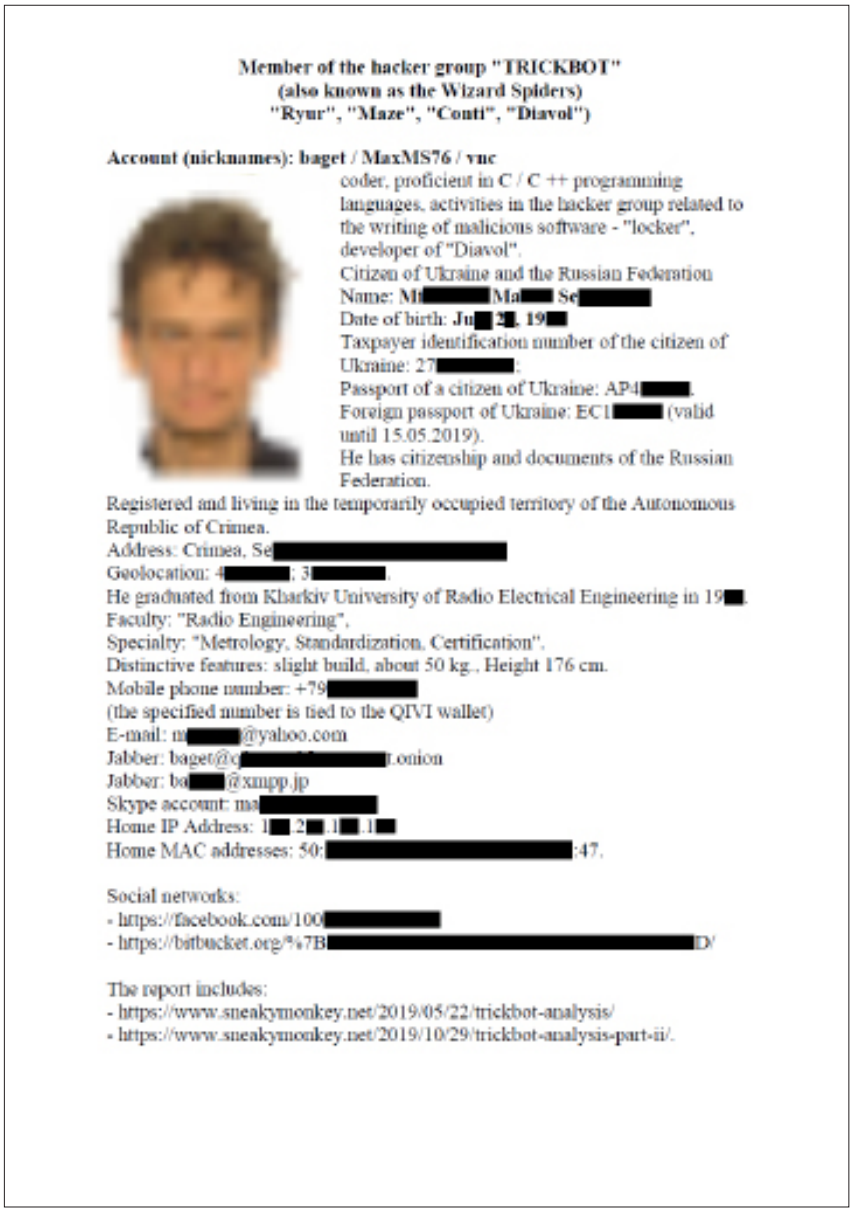
The Members Uncovered

What immediately stood out about this leak was the sheer amount of personal information and organisational elements provided on members of the Trickbot organisation. This information gave a strong insight into not only the scope of the organisation, showing total member counts, but also gave us a view into personal member situations. Specifically, it revealed where they are based, what real jobs they have held in the criminal organisation and commercial world as well as in some cases, why the member joined the group.

One key point to make is with the level of information leaked, it is clear whoever is behind this leak was either very close to the group itself or had broad access to group records. It is difficult to verify the information contained within the PDFs as some group members have been displaced by the conflict between Ukraine and Russia. However, given the amount of information, it can be assumed that most of the "doxed" details were accurate at some point or remain so.

The “Doxing PDFs”

The “Doxing PDFs” are a series of PDF documents which were included alongside the leaks of the messages. Each tweet contained a link to a zip of the communication files, but also the option to download a PDF which includes a variety of personal information. This information was highly detailed, with each PDF housing enough information to identify each individual member with intelligence that could be easily corroborated. For reasons unknown, these PDFs stopped being posted alongside the tweets. Eventually the PDFs were deleted from the hosting site for violating the terms of service, but our team was able to recover 27 of them before the removal. A PDF shown in ***Figure 3***, which has been redacted for privacy, gives an example of the level of information leaked.



Member of the hacker group "TRICKBOT"
(also known as the Wizard Spiders)
"Ryuk", "Maze", "Conti", "Diavol")

Account (nicknames): baget / MaxMS76 / vuc

coder, proficient in C / C ++ programming languages, activities in the hacker group related to the writing of malicious software - "locker", developer of "Diavol".
Citizen of Ukraine and the Russian Federation
Name: M[redacted] Ma[redacted] Se[redacted]
Date of birth: Ju[redacted] 2[redacted], 19[redacted]
Taxpayer identification number of the citizen of Ukraine: 27[redacted].
Passport of a citizen of Ukraine: AP4[redacted].
Foreign passport of Ukraine: EC1[redacted] (valid until 15.05.2019).
He has citizenship and documents of the Russian Federation.
Registered and living in the temporarily occupied territory of the Autonomous Republic of Crimea.
Address: Crimea, Se[redacted]
Geolocation: 4[redacted], 3[redacted].
He graduated from Kharkiv University of Radio Electrical Engineering in 19[redacted].
Faculty: "Radio Engineering",
Specialty: "Metrology, Standardization, Certification".
Distinctive features: slight build, about 50 kg., Height 176 cm.
Mobile phone number: +79[redacted]
(the specified number is tied to the QIVI wallet)
E-mail: m[redacted]@yahoo.com
Jabber: baget@q[redacted].onion
Jabber: ba[redacted]@xmpp.jp
Skype account: ma[redacted]
Home IP Address: 1[redacted].2[redacted].1[redacted].1[redacted]
Home MAC addresses: 50:[redacted]:47.

Social networks:
- https://facebook.com/100[redacted]
- https://bitbucket.org/%7B[redacted]D/

The report includes:
- https://www.sneakymonkey.net/2019/05/22/trickbot-analysis/
- https://www.sneakymonkey.net/2019/10/29/trickbot-analysis-part-ii/.

Figure 3

This information includes the full name, date of birth, tax identification number, passport number, addresses and a multitude of accounts and email addresses of the person. The amount of information that is included within the PDFs varies. Some individuals only have basic information whilst others, such as the one above, feature a wide range.

The information source and details of these PDFs is unknown, with the leaker not revealing their origin. We believe these PDFs have been created using a mixture of open-source intelligence research and information which was held privately by Trickbot. It would of course be standard information for a human resources department to hold. However, within Trickbot this collection effort remains elusive, namely

why was so much detailed information was being collected? This gives rise to speculation that perhaps these cybercriminals are aligned, affiliated, or controlled by a nation state protagonist which required this information. IBM X-Force's analysis potentially indicates this due to a series of attacks confined to Ukraine.[1]

It seems some information may have been obtained from the Trickbot "employees" themselves, such as names, dates of birth and potentially even passport numbers to show citizenship. Information such as phone numbers, email addresses, and accounts may have come from similar backend sources; however, information such as social media accounts could potentially come from public research. One anomaly is multiple PDFs contain bank card information. This information would not be surprising for a standard employer, but we know from messages such as ***Figure 4*** that members are paid in bitcoin ("btu" being a translation of "бтц" which is a Russian acronym for BTC). As such, bitcoin wallet addresses would be required for transactions between members to distribute the proceeds of crime.

```
[01.07.21 16:42:17] frances: man. we got 200 people here and more.
[01.07.21 16:42:22] frances: all get paid in btu
[01.07.21 16:42:28] frances: I won't make exceptions for one person
[01.07.21 16:42:38] frances: I have a boss' order to pay in bitcoins
[01.07.21 16:42:48] frances: I'm powerless here
```

Figure 4

The Member List

On the 13 March 2022, the @trickleaks account posted a tweet which is detailed in ***Figure 5***. This Tweet contained only the word "LIST" and had a single link to a file hosted on mega[.]nz. The file allegedly contained a list of usernames and emails reportedly for members of the Trickbot organisation.

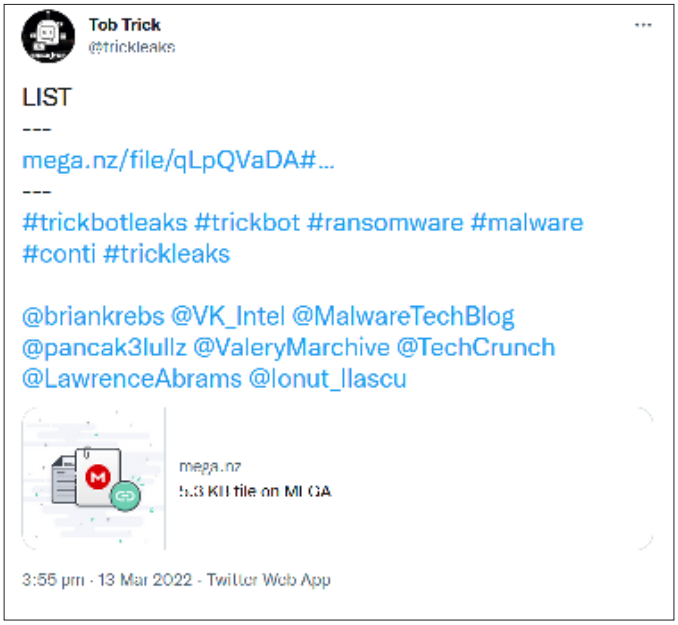


Figure 5

1 https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine/

The list featured 133 individuals, containing their usernames and other information. This data helped identify the different usernames used across different platforms, which appear to be the same threat actor within the group. ***Figure 6*** provides an example of the details leaked.

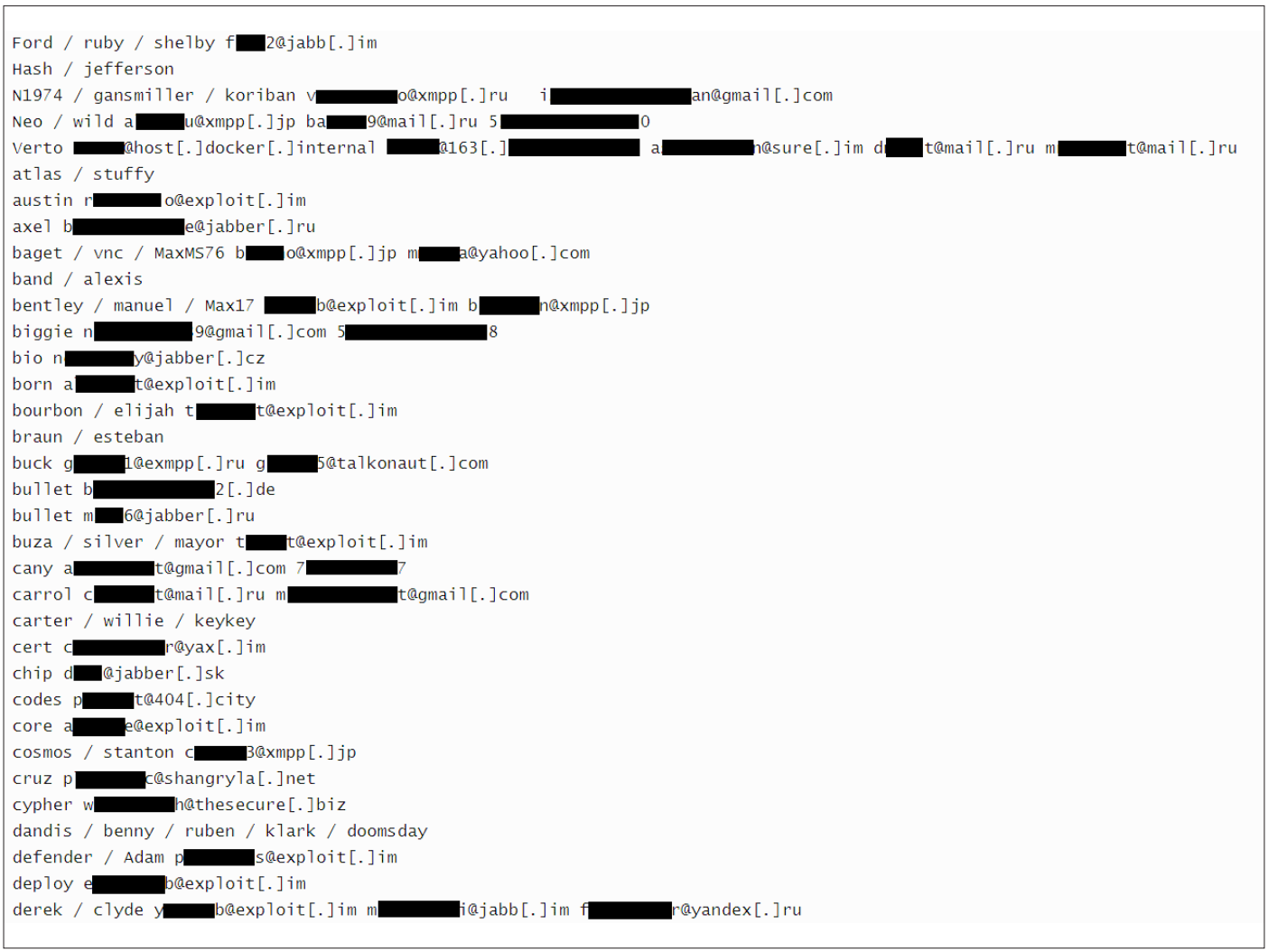


Figure 6

Individuals with multiple usernames have been collated together, alongside email addresses. In some occurrences, as shown below in ***Figure 7***, full names and what appears to be bank card, phone and ID numbers were also included.

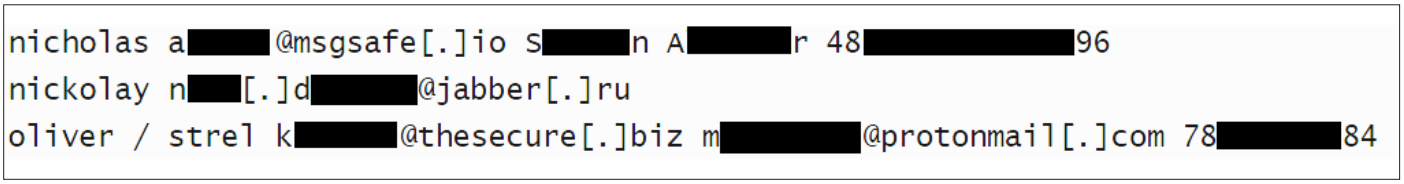


Figure 7

Operational Infrastructure

“Bots and Loaders”

Within Trickbot’s operational infrastructure, a prominent feature is what they refer to as their “Bots and Loaders”. These hosts appear to be the main infrastructure supporting the management and distribution of malware.

An example of this can be seen in ***Figure 8***, where the user green is listing to the user bentley the IP addresses of the “Bots and Loaders”. This kind of message happens on a regular occurrence, being sent once or twice a week, to detail the current operational infrastructure.

```
2020-07-09T05:27:08 green -> bentley
hi

LOADERS
51.77.112.254
86.104.194.108
217.12.209.44
185.99.2.191
66.70.218.37
134.119.191.22


bot
85.204.116.188
86.104.194.109
194.87.145.86
185.99.2.221
5.1.81.68
185.164.32.148
```

```
2020-07-21T05:49:02 green -> bentley
Hi

LOADERS
31.214.240.203
78.108.216.13
217.12.209.44
194.5.249.163
80.82.68.132
62.108.35.215


bot
85.204.116.188
80.82.68.32
194.5.249.164
185.14.31.135
45.148.120.142
62.109.13.184
```

Figure 8

As an example, to show the connectivity, using VT Graph reveals the link between an IP address listed as a “Bot” to another listed as a “Loader”. The graph shown in ***Figure 9*** identifies the connected nature of the infrastructure. It appears that “Bots” are used to distribute malware, hosting the initial malicious file for download either as part of a phishing campaign or a different attack vector.

The “Loader” IP addresses are used for Command and Control (C2) communication and delivery of secondary payloads. As we can see in ***Figure 9***, the malicious file is downloaded from a URI on the “Bot” IP address which makes connections to the “Loader”. This is a standard attack setup, with the malware potentially using this C2 communication to deliver further payloads. Additionally, it could also be used to add the infected machine into the bot herding infrastructure. Further analysis shows several other files communicated with this “Loader” IP address, further emphasising that this C2 could be transmitting to hundreds of compromised hosts at one time.

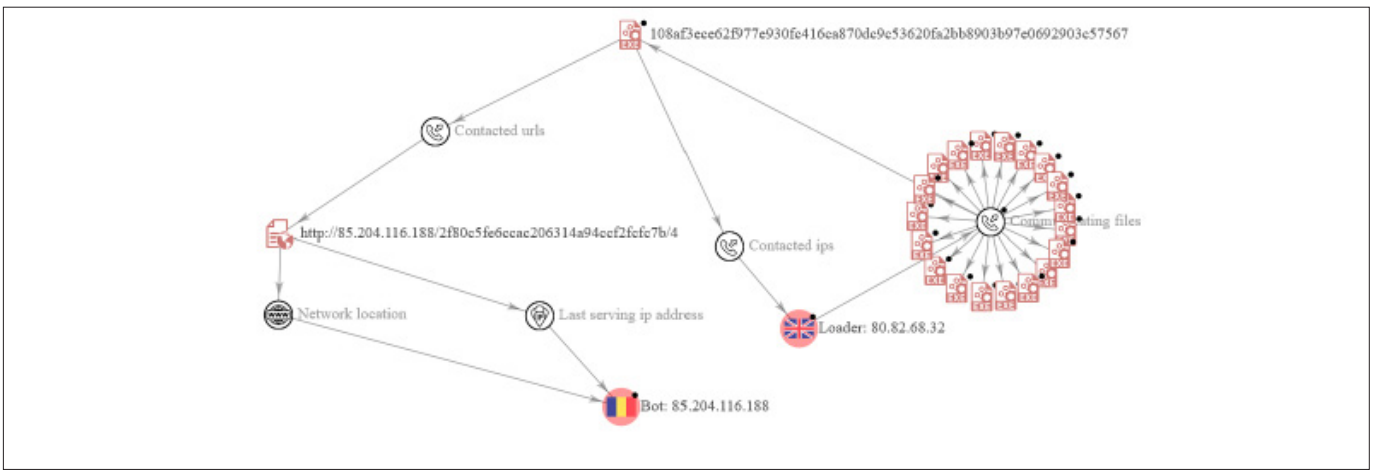


Figure 9

Operational Servers

Alongside these “Bots and Loaders”, another set of hosts were identified alongside credentials posted in chats.

These hosts are being used for a variety of different activities and tasks. In total, over 1,000 username and password combinations with their corresponding IP addresses were discovered. The predominant user was found to be root. The passwords associated with these accounts also have no standardisation, with some having many characters and others with very few. An example of this is shown in ***Figure 10***, where the user ruben is messaging the user adam a list of servers, which happens on a regular basis, and includes a set of credentials. Once again, this is along with the username, IP address, password, and the country the server resides in.

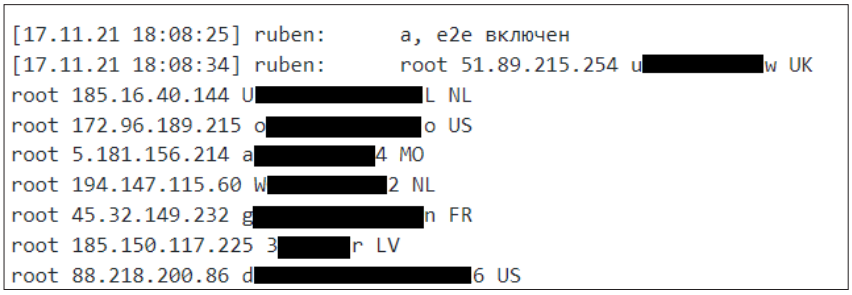


Figure 10

Given the nature of the group, it could be assumed that some of these servers may have been gained through exploitation of vulnerable services. However, it is apparent that Trickbot pay for some of their server infrastructure. This can be seen in messages such as the one in ***Figure 11***, in which the user strix is reminding the user carter that a set of their server infrastructure needs renewing and paying for.

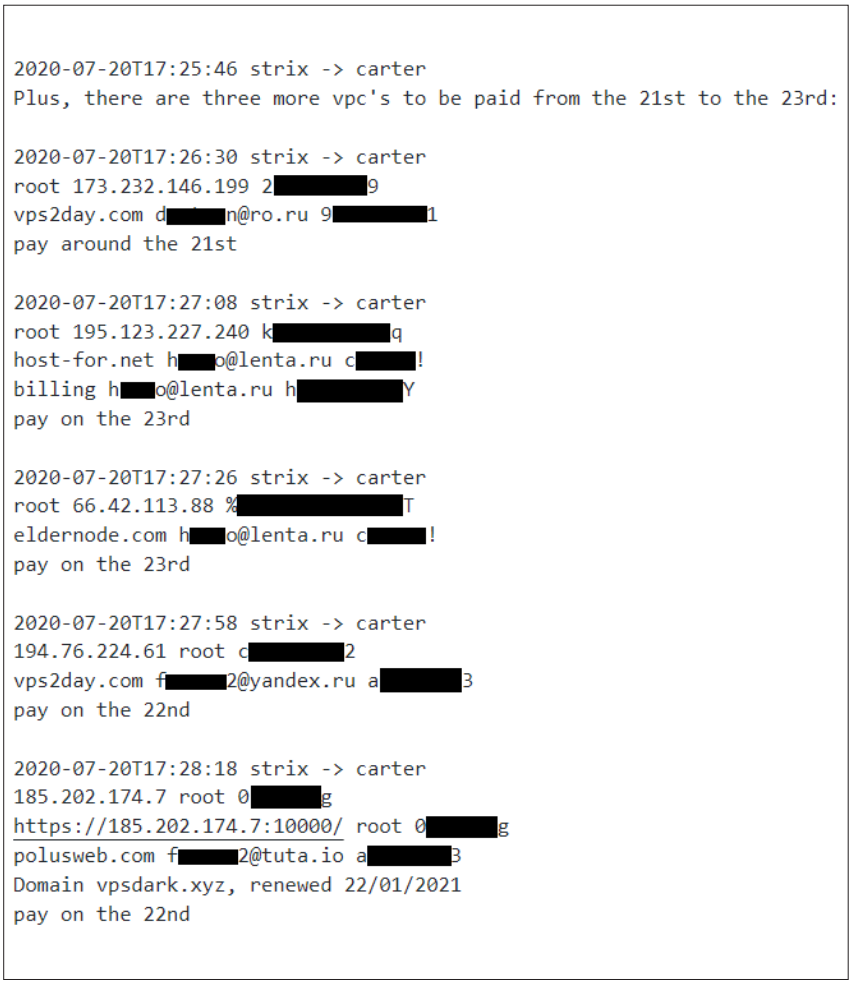


Figure 11

Example usage of infrastructure

Trickbot's server usages vary greatly with some specific examples being mentioned within the leaks. One such use of this server infrastructure is for antivirus detection testing. Whilst developing malware and testing crypters, the teams often use a series of servers with different operating system specifications and antivirus configurations. This is used in conjunction with a variety of other tools, such as dyncheck and avcheck.net. These are like VirusTotal as these tools do not require the samples to be published publicly. This enables the threat actors to discover which antivirus products are detecting Trickbot's family of malware, but also to test the effectiveness of different crypters and their configurations. This infrastructure is shown in a series of messages, ***Figure 12***, between the user stern and the user bentley, two senior members within Trickbot. The messages discuss the licences which need to be purchased for each antivirus product.

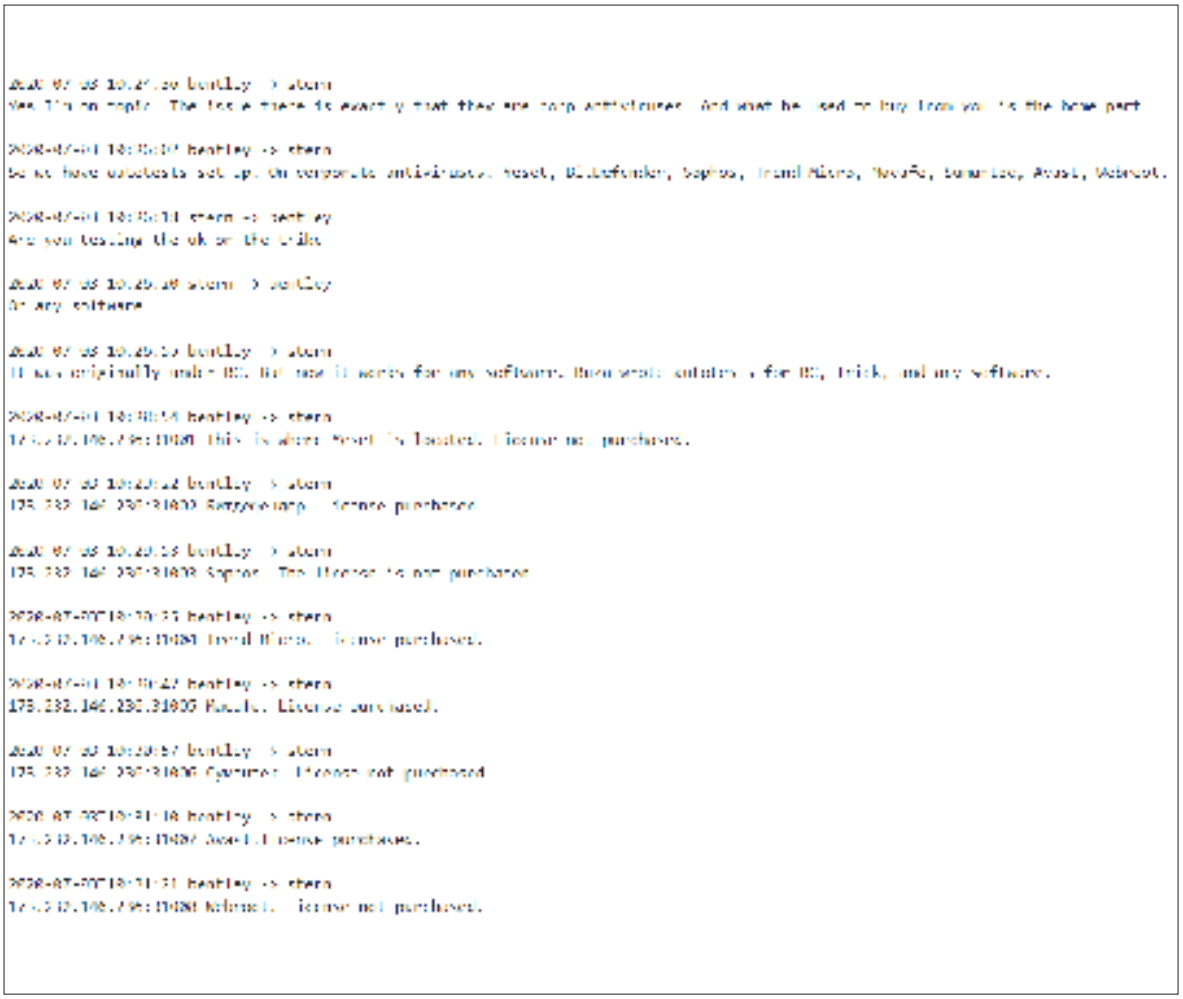


Figure 12

Another known use of this SSH host infrastructure is for the creation and operation of proxy servers. This can be for both HTTP/SOCKS and Tor, enabling the threat actors to add another layer of protection to their operations by hiding behind multiple proxies. The threat actors also make good use of the tool torify, which is an application to help tools make use of the Tor network which do not feature supports by default. In ***Figure 13*** we can see the user fuzz discussing a new tool being developed by the user lucas which must be executed through a SOCKS5 proxy or anonymiser.

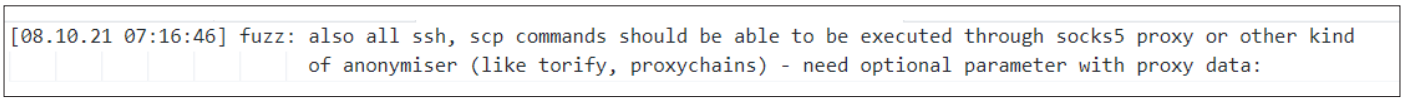


Figure 13

Botleggers Club

As discussed previously, the group manages a significant number of bots inside of their infrastructure. Until this point, it was unclear how the group centrally managed this infrastructure; however, there is evidence to suggest that they were using a service known as the “Botleggers Club”.

In ***Figure 14***, you can see the user rudolf discussing the “Botleggers Club” admin panel, describing it as an administration interface to interact with clients (the bots).

```
[22.10.21 15:15:35] rudolf: API Botleggers admins with plugins

General:
The Botleggers admins are designed to manage any clients through user interfaces.
User interfaces are php scripts written in php 7 vanila and designed to convert the admin commands protocol to client protocol and return the results to the admin.
```

Figure 14

Throughout the leak we can see multiple references to the “Botleggers Club”, often just referred to as “Botleggers”, in multiple contexts. In ***Figure 15***, we can see that scripts are being uploaded to “Botleggers” which leads to the belief that that it not only manages the bot infrastructure itself, but also the malware being delivered by these hosts. This is further reinforced in ***Figure 16***, where we see the user steller telling the user mushroom to try selecting the file test.dll in “Botleggers”. This customisation may allow the threat actors to avoid detection further, dynamically changing their payload delivery to use different crypted versions on a regular basis.

```
2020-09-07T06:50:45 steller -> mushroom
Hi.
Tested the script on the updated 10. It works.
Uploaded it to botleggers
```

Figure 15

```
2020-08-03T15:18:12 steller -> mushroom
Maybe the bot is falling off.
Try displaying the message again instead of the bot.
Select test.dll in botlegger
```

Figure 16

Further analysis into this platform led to an IP address for the “Botleggers Club”. The IP 217[.]12[.]204[.]65, is referenced in the message shown in ***Figure 17*** discussing “Loader & Bot Equipment”. This IP address is also mentioned multiple other times with similar looking directories.

```
[11/23/11/21 11:06:35] elliott: I don't think the rest has changed.
[23.11.21 12:11:56] alphonse: https://217.12.204.65/sOIDFhsAIUfhu42332uygt27634ft7yuaFGyaugkJFsayjegf--_-GBASfdvt23fv/index.php?r=groups%2Floadertool&id=27
                              what do you see here?
[23.11.21 12:13:25] elliott: Loader & Bot equipment
```

Figure 17

The IP address is hosted within Ukraine and appears to no longer be hosting the “Botleggers Club” on it. However, in October 2021 scans were conducted on the service URLScan.io. Through this we were able to gain some screenshots of the interface. This has changed over time, but a consistent theme can be seen in ***Figure 18***.

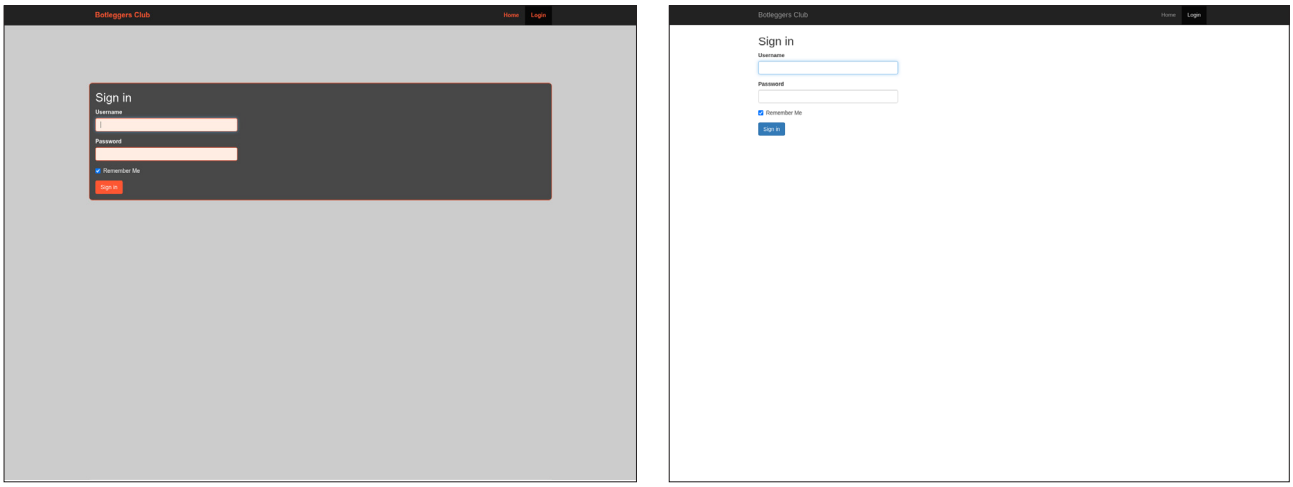


Figure 18

Despite the “Botleggers Club” portal no-longer being live to our knowledge, it gives us valuable insight into the custom tools used by the threat actors, to manage, operate, and deploy their malware. It also gives an insight into the supporting infrastructure required for ransomware operations.

Development Teams

Despite what most researchers believe about threat actors such as Trickbot, the leaks have shown us how conventional, structured, and business-like the operation of this group is. One key point of interest is the clearly defined teams which each individual works within, each with specific and parameterised objectives.

Some teams are obvious within the leaks, having group chats to discuss work and developmental tasks. Others are less so, such as smaller projects in which two or three people coordinate through personal messages.

In leaked communications from certain members are filenames beginning with the word “GROUP_”. These are groups chats which contain multiple members, as opposed to standard two-way communications. Among these groups are: crypters, find_grep, adam_and_garsons, general, loader, loader2, locker, testforme, Fire_Team and tox. Some groups contain large amounts of information which will be explored in depth in this paper, whilst others will be given brief descriptions due to a lack of information.

One such group is testforme, which contains just one individual pasting a Python script which finds all Symantec logs from today’s date and returns them. The adam_and_garsons group follows a similar pattern and contains users’ silver, rocco, and adam, who discuss issues with a backdoor malware’s efficiency. The find_grep group, is again a small set of members who discuss an issue with a tool which finds all files on a system. They eventually arrive at the solution of a missing backslash in the code. Finally, the general group contains chatter, as the name suggests. The user frances regularly informs members to send wallet addresses in private messages for payment.

Crypter group

The crypters group contains users’ silver, fish, dash, stout, brick, pyro, gibby, rags, austin, zanzi, mark, lucas, bullet, fuzz, orin, gary, oliver, thomas, ernest, core, buck, and a user named admin who appears to administrate the group chat. Within this group the most active users are stout and silver with over 150 messages each. Some users such as ernest and core were added later and only have one or two messages. In ***Figure 19*** we can also see it is declared that fuzz is the team leader of the group, despite not being the most active.

```
[12.07.21 09:46:12] fuzz: hi!
[12.07.21 09:48:51] stout: Hi, everybody. Guys, fuzz is our teamleader, we deal with crypto topic together.
                           If anything, you can go to him when you can't contact me, or he may demand something from you)
```

Figure 19

The main topic of conversation within this group is the development of crypters, a tool used to obfuscate

malware. Each developer within the group is developing their own crypter, but uses this chat to share ideas and development tips. Within this chat are discussions around how Trickbot develops the crypters. An example of this can be seen in ***Figure 20***, where the user silver is giving advice to the group about different techniques when building crypters. This includes reminding them to use standardised elements to make it less noticeable.

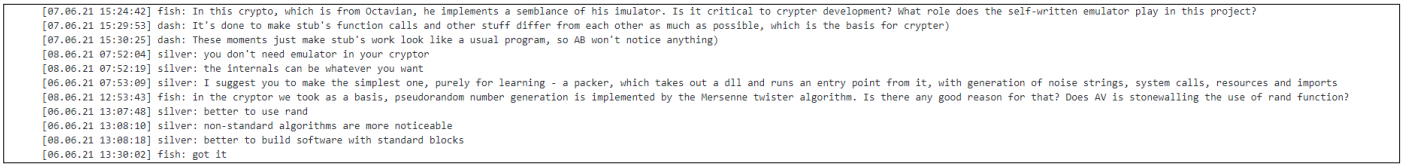

[07.06.21 15:24:42] fish: In this crypto, which is from Octavian, he implements a semblance of his imulator. Is it critical to crypter development? What role does the self-written emulator play in this project?
[07.06.21 15:29:53] dash: It's done to make stub's function calls and other stuff differ from each other as much as possible, which is the basis for crypter)
[07.06.21 15:30:25] dash: These moments just make stub's work look like a usual program, so AB won't notice anything)
[08.06.21 07:52:04] silver: you don't need emulator in your cryptor
[08.06.21 07:52:19] silver: the internals can be whatever you want
[06.06.21 07:53:09] silver: I suggest you to make the simplest one, purely for learning - a packer, which takes out a dll and runs an entry point from it, with generation of noise strings, system calls, resources and imports
[08.06.21 12:53:43] fish: in the cryptor we took as a basis, pseudorandom number generation is implemented by the Mersenne twister algorithm. Is there any good reason for that? Does AV is stonewalling the use of rand function?
[06.06.21 13:07:48] silver: better to use rand
[06.06.21 13:08:10] silver: non-standard algorithms are more noticeable
[08.06.21 13:08:18] silver: better to build software with standard blocks
[06.06.21 13:30:02] fish: got it

Figure 20

Loader groups

Within the leaks are two loader groups, loader and loader2. The first group contains silver, fuzz, stout, henry, rudolph, and lucas whilst the second group has just silver, mark, joe, and fuzz. The first group are tasked with developing a loader, with the specifications shown in ***Figure 21***. These appear to detail a highly advanced loader. The specification requires the tool to deploy additional malware payloads using a variety of different methods, whilst also uniquely identifying each target with basic system information and logging that to a main server. This server would likely have been the “Botleggers Club” mentioned previously, due to the detailed descriptions of the platform being shared within the chat.

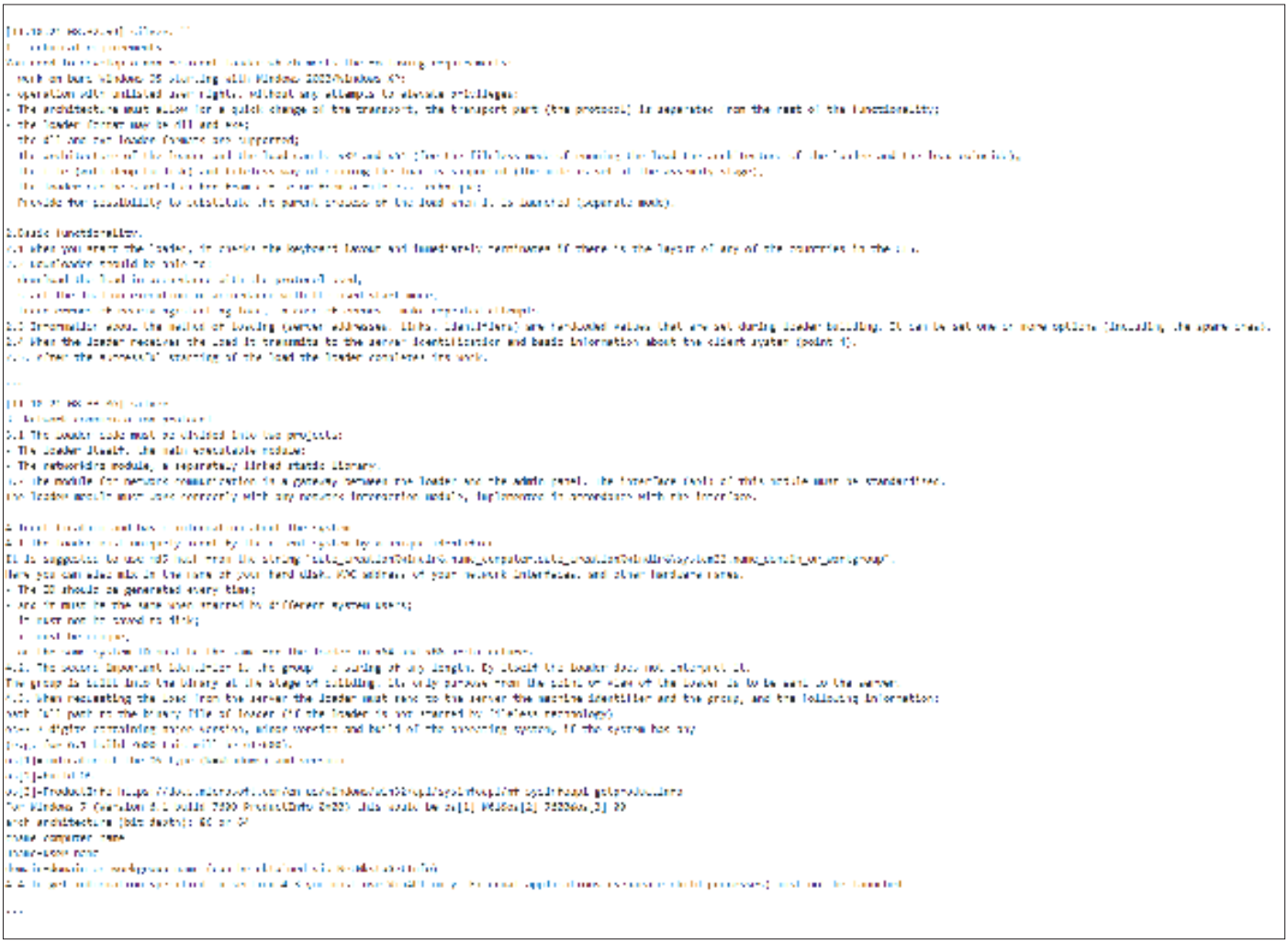


Figure 21

Tox group

The tox group is a team solely dedicated to attempting to move communications to the messaging service Tox. The team consists of silver, kitten, and fuzz; however, almost all conversation is between silver and kitten with the latter user as the lead on this project. Tox is a peer-to-peer messaging and video calling protocol which aims to provide secure communication between two parties. Moreover, it can also be tunnelled through Tor. Despite this, it appears that standard Tox does not support group chats, so the team wishes to use a forked version of the repo known as the NGC (New Group Chats) version which is developed by GitHub user JFreegman. The most interesting part within this group chat, shown in ***Figure 22***, is the discussion of communicating with the developer to speed up the process of adding the new NGC feature.

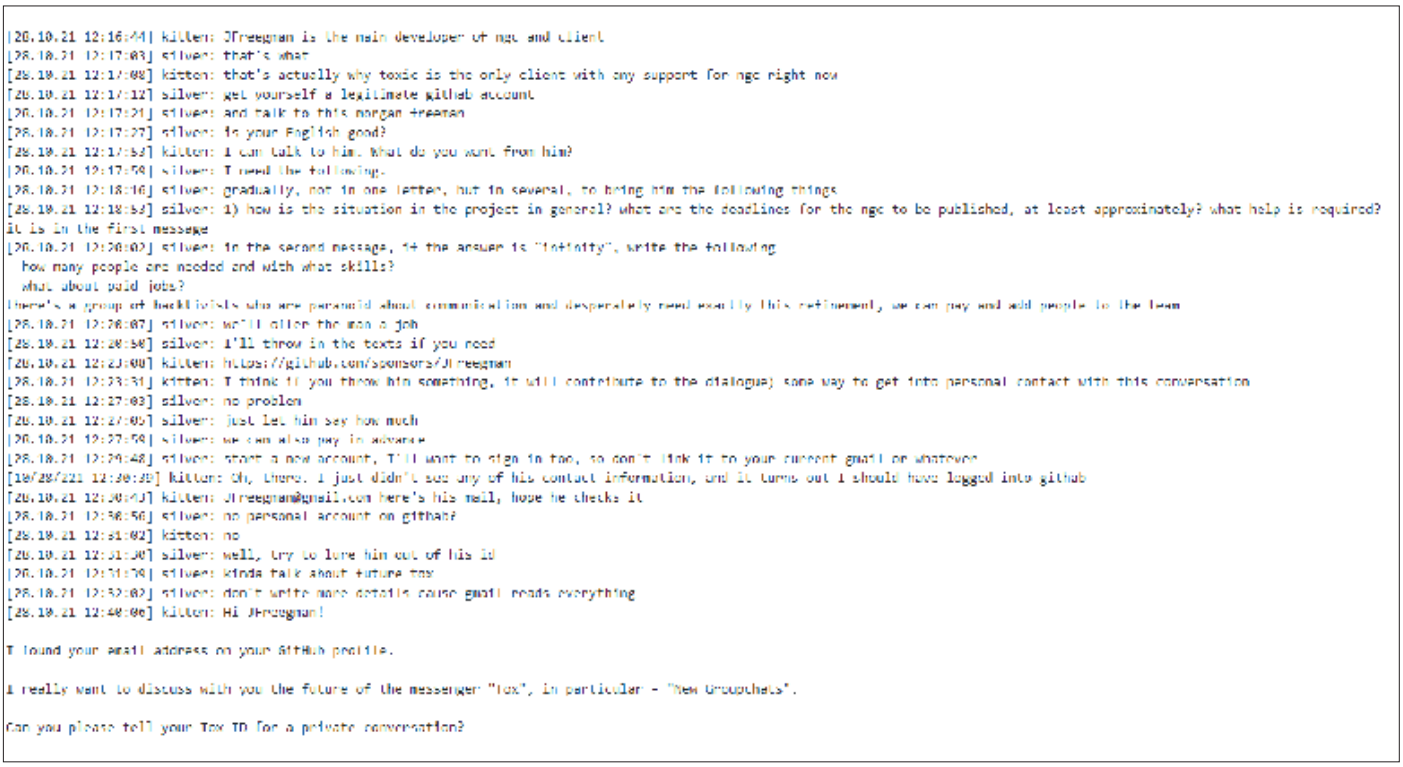


Figure 22

Within this conversation the user silver, one of the senior members of Trickbot, asks three important questions: “how is the situation in the project?”; “what are the deadlines?”; and “what help is required?”. The team states that if the project is going to take forever, user silver will offer people to help work on the project from the Trickbot organisation as they “desperately need this refinement”. Finally, silver may even offer the developer of NGC money or a job within the Trickbot organisation.

The members continue discussing this situation and the best ways of contacting JFreegman. The final messages from the user silver looks like it is from a series of private messages between themselves and JFreegman who is potentially going by epitaph, as shown in ***Figure 23***.

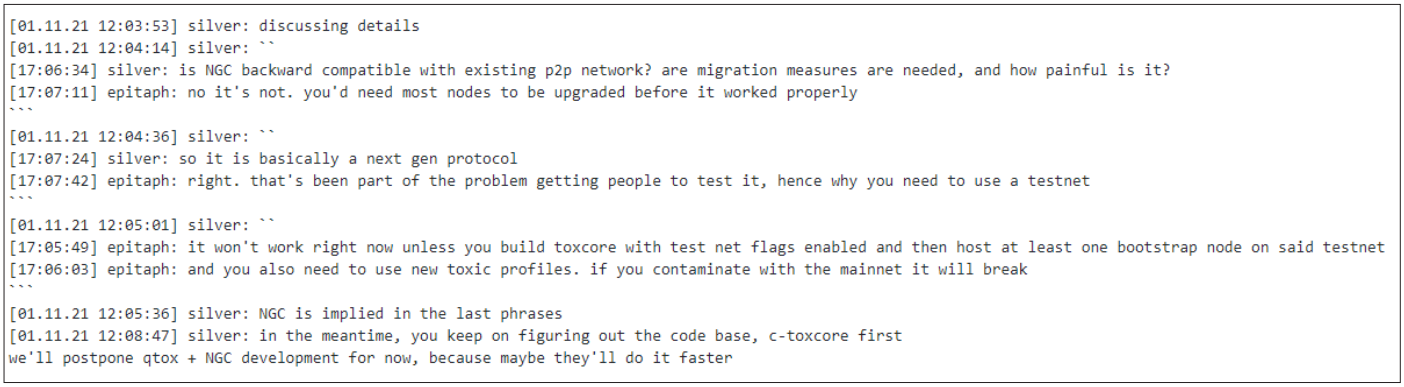


Figure 23

Locker group

The locker group is composed of the users' silver, dash, stout, fish, and lucas. Silver, dash, and stout appear to take the lead on most conversations. This team is dedicated to the development of fast and efficient encryption systems which can be built into ransomware or wiper malware payloads. To explain the process to others, the user silver gives a breakdown of what they need to focus on when developing their lockers, this is shown in ***Figure 24***.

```
[02.09.21 12:24:07] stout: I propose to make a development process like this: discuss which modules can be divided into the project, take a template,
                           make a skeleton by the discussed modules, make stouts and start building up
[02.09.21 12:25:05] silver: actually the most serious part isn't the cryptography
[02.09.21 12:25:12] silver: cryptography is a couple of functions
[02.09.21 12:25:44] silver: there's going to be a lot of hassle with
- searching and processing network balloons
- organizing multi-threaded model for maximum speed
```

Figure 24

Within this group chat in November 2021, a project known as "Cryptolocker" is mentioned and is referred to as being "quite complicated software". This project is being worked on initially by the user dash. However, it appears that the user lucas is brought in to provide oversight and help with completion. We can see that the beta version of this software is estimated to be released around the second week of December 2021, thanks to messages shown in ***Figure 25***.

```
[01.12.21 10:14:00] dash: Hi, everything is going good, next week probably will be already beta)
[01 12/221 10:21:10] lucas: Ok. Looking forward to it.
```

Figure 25

Interestingly, when comparing to the previous Conti leaks, a file called "Cryptolocker Terms of Reference" was leaked as part of their internal documentation. This document details the requirements, specification, process, information sources, and a testing plan for the software. The full document can be read in translated form in **Appendix 1**.

From cross-referencing this document with the messages, we can predict some features of the locker. For example, it is probably using a ChaCha20 encryption system for efficiency and RSA-4096 keys to encrypt the data. The locker also potentially has two modes of encryption called "fast and full". The first encrypts just the first megabyte of the file to cause corruption, whereas the latter encrypts the entire file. Once the locker has run, it states in the brief that "it destroys itself" so no samples can be found.

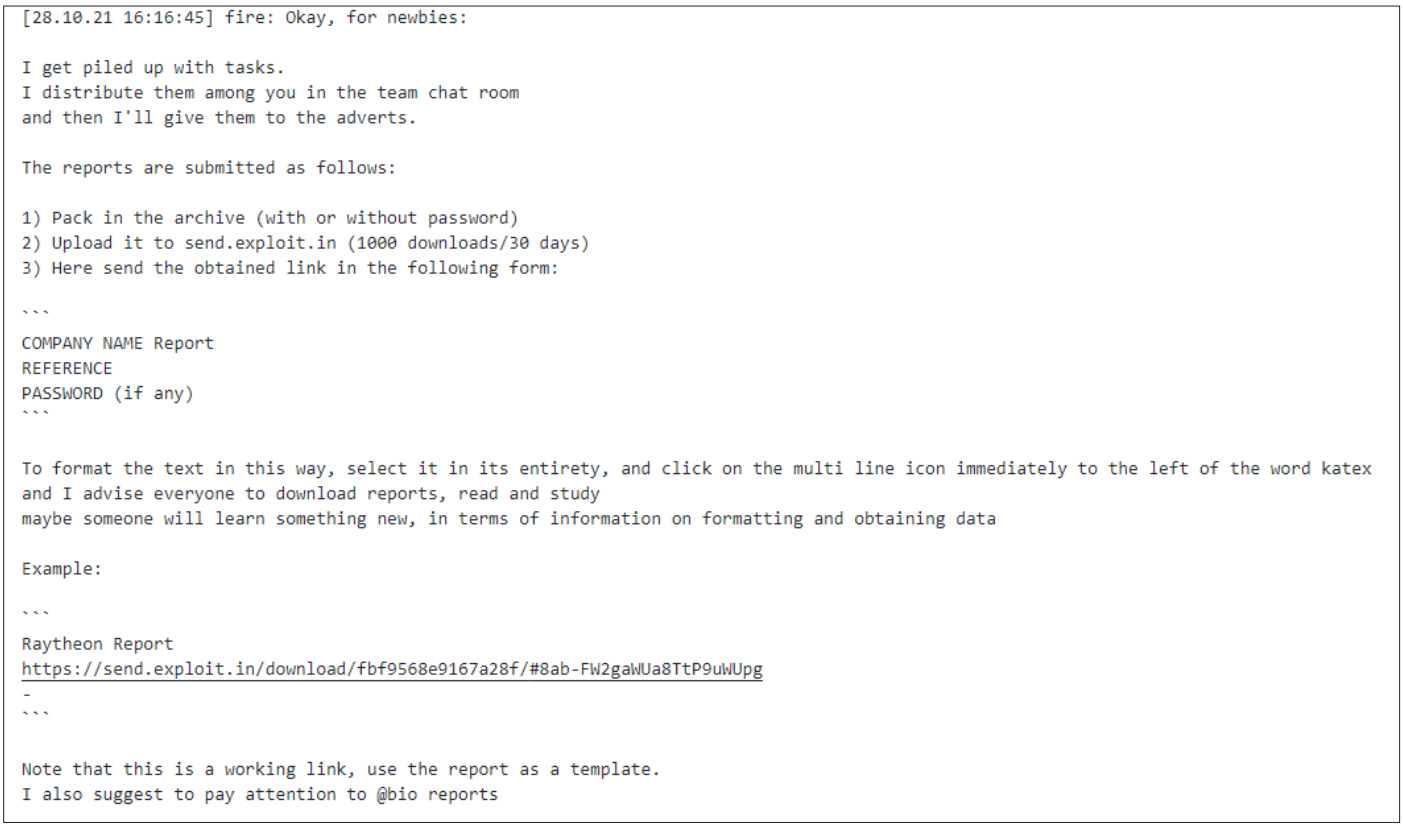
One point of interest is the combination of the ChaCha20 encryption algorithm and the use of an RSA-4096 key is the setup currently used by the BlackBasta ransomware[2]. This ransomware has previously been linked with Conti and Trickbot due to having similar forums and payment pages. This link also potentially fits the time scale, with the first recorded occurrence of BlackBasta being in the second week of April. This would be five months after the "Cryptolocker" project was released into beta. While not definitive, this link is appropriate to mention given the already existing ties between the two groups[3].

Fire_Team group

The Fire_Team is the largest group chat contained within the leaks with the highest total messages. The group is comprised of users' fire, venom, cypher, sin, bio, mayor, loki, liam, heretic, snow, frances, and jeronimo and contains over 1,000 messages. The aim of the group appears to be the collection of information on different companies and individuals. It is currently unclear as to what information is being collected and what it is used for. However, initial analysis concludes this appears to be for target identification, to uncover potential avenues for exploitation, and/or to conduct blackmail.

A message from the user fire, the leader of the group, shown in ***Figure 26*** explains the process that the team operates under.

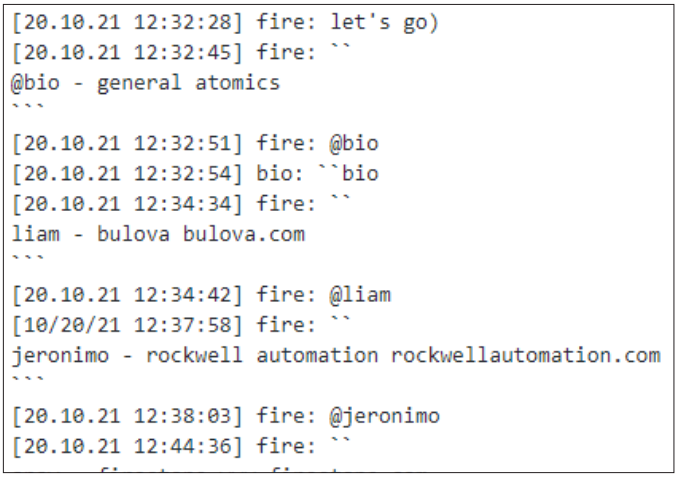
2 https://www.packetlabs.net/posts/black-basta/
3 https://blogs.blackberry.com/en/2022/05/black-basta-rebrand-of-conti-or-something-new

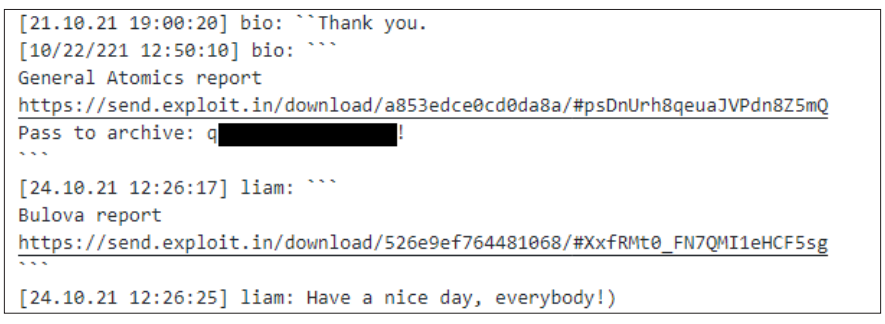


```
[28.10.21 16:16:45] fire: Okay, for newbies:

I get piled up with tasks.
I distribute them among you in the team chat room
and then I'll give them to the adverts.

The reports are submitted as follows:

1) Pack in the archive (with or without password)
2) Upload it to send.exploit.in (1000 downloads/30 days)
3) Here send the obtained link in the following form:

```
COMPANY NAME Report
REFERENCE
PASSWORD (if any)
```

To format the text in this way, select it in its entirety, and click on the multi line icon immediately to the left of the word katex
and I advise everyone to download reports, read and study
maybe someone will learn something new, in terms of information on formatting and obtaining data

Example:

```
Raytheon Report
https://send.exploit.in/download/fbf9568e9167a28f/#8ab-FW2gaWUa8TtP9uWUpg
-
```

Note that this is a working link, use the report as a template.
I also suggest to pay attention to @bio reports
```

Figure 26

This process can be seen in more detail in ***Figure 27*** and ***Figure 28***, where simple company names and domains are posted with a specific user assigned to conduct research. Often one or two days later an exploit[.]in link is posted into the chat by the researcher, containing the finished intelligence report on the company.



```
[20.10.21 12:32:28] fire: let's go)
[20.10.21 12:32:45] fire: ``
@bio - general atomics
```
[20.10.21 12:32:51] fire: @bio
[20.10.21 12:32:54] bio: ``bio
[20.10.21 12:34:34] fire: ``
liam - bulova bulova.com
```
[20.10.21 12:34:42] fire: @liam
[10/20/21 12:37:58] fire: ``
jeronimo - rockwell automation rockwellautomation.com
```
[20.10.21 12:38:03] fire: @jeronimo
[20.10.21 12:44:36] fire: ``
```

***Figure 27***



```
[21.10.21 19:00:20] bio: ``Thank you.
[10/22/221 12:50:10] bio: ```
General Atomics report
https://send.exploit.in/download/a853edce0cd0da8a/#psDnUrh8qeuaJVPdn8Z5mQ
Pass to archive: q[redacted]!
```
[24.10.21 12:26:17] liam: ```
Bulova report
https://send.exploit.in/download/526e9ef764481068/#XxfRMt0_FN7QMI1eHCF5sg
```
[24.10.21 12:26:25] liam: Have a nice day, everybody!)
```

***Figure 28***
```

Throughout the latter half of 2021, the team's capability grows as they generate a much larger list of targets which are sent to other members on a regular basis. These lists contain more information and details to help the Fire_Team's investigations. An example of this new kind of message can be seen in ***Figure 29***, with a message from December 2021.

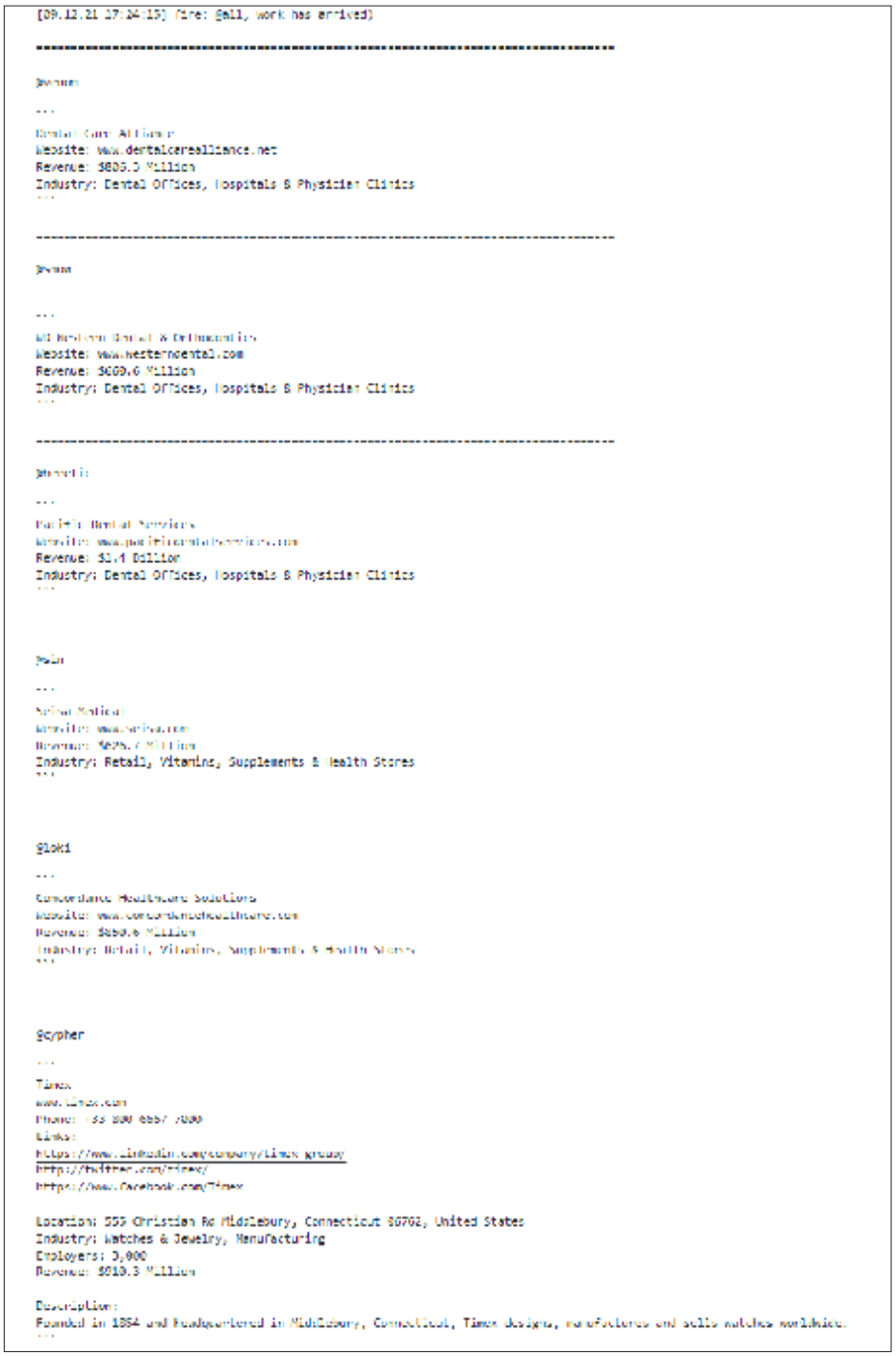


Figure 29

These messages are sent on a semi-regular basis, every week or so, with each one containing a company that fits a specific industry vertical. This one has targets for the Dental / Medical vertical, with others targeting Gaming / Entertainment and Transportation / Logistics verticals.

Observations

Trickbot is a business

Throughout the leak, it becomes obvious that groups like Trickbot are not simple organisations constructed by a few malicious programmers. In fact, this is a large business which operates at a commercial level. With a full management structure; a HR system with salaries and bonuses; and even mentions of lawyers, the Trickbot threat actors are very much a criminal advanced persistent threat. This is supported by their advanced tactical capabilities in malware development and exploitation. Combined with their persistence in attacking different verticals through investigation conducted in the Fire_Team, they have the ability to mutate and avoid detection by developing new tactics.

When it comes to Trickbot, the management structure is not wholly clear, but some important observations can be made. The user known as silver / buza / mayor seems to be prominent within the organisation. Not just due to having the largest leak of all, with 324 communication files, but also due to some of the high-level conversations in which they are involved. One such example is that they are the creator of most of the development group chats mentioned above, leading one to believe they oversee the coordination of the development teams within Trickbot. It is also important to note that within their leaked communication files there is a folder known as the “silver_room”. This makes silver the only user to have a folder named as such which contains messages from a user named admin, alongside conversations around salaries and hiring. This combined with the message in ***Figure 30*** all goes to paint the user silver as a one of the most important individuals within Trickbot.

```
[16.07.21 12:14:34] fire: Payday, right?
[16.07.21 12:15:50] mayor: was supposed to be yesterday, waiting for boss with a bag of dough
[16.07.21 12:15:54] mayor: no one's been paid yet.
[16.07.21 12:16:11] fire: Ah, got it.
[16.07.21 12:16:19] fire: Thought you were the boss.)
[16.07.21 12:17:22] mayor: I'm the technical boss.
[16.07.21 12:17:41] mayor: and the big boss shows up seldom, pours his dough and leaves again)
[16.07.21 12:17:58] mayor: pistols everybody in the process)
```

Figure 30

Another prominent figure is the user frances, who appears to manage general queries and HR. Tasks such as paying salaries; conducting pay rises and overseeing hiring and firing places the user in an important operational position. Conversations, such as the one shown in ***Figure 31***, show the employment process a potential candidate may go through. In this conversation, we see the user frances explain how they found the user fire on a forum and got in contact with them to offer them a position. It is important to note that the potential candidate has no knowledge of Trickbot upon initial communication, being told “Google it, you’ll understand it”.

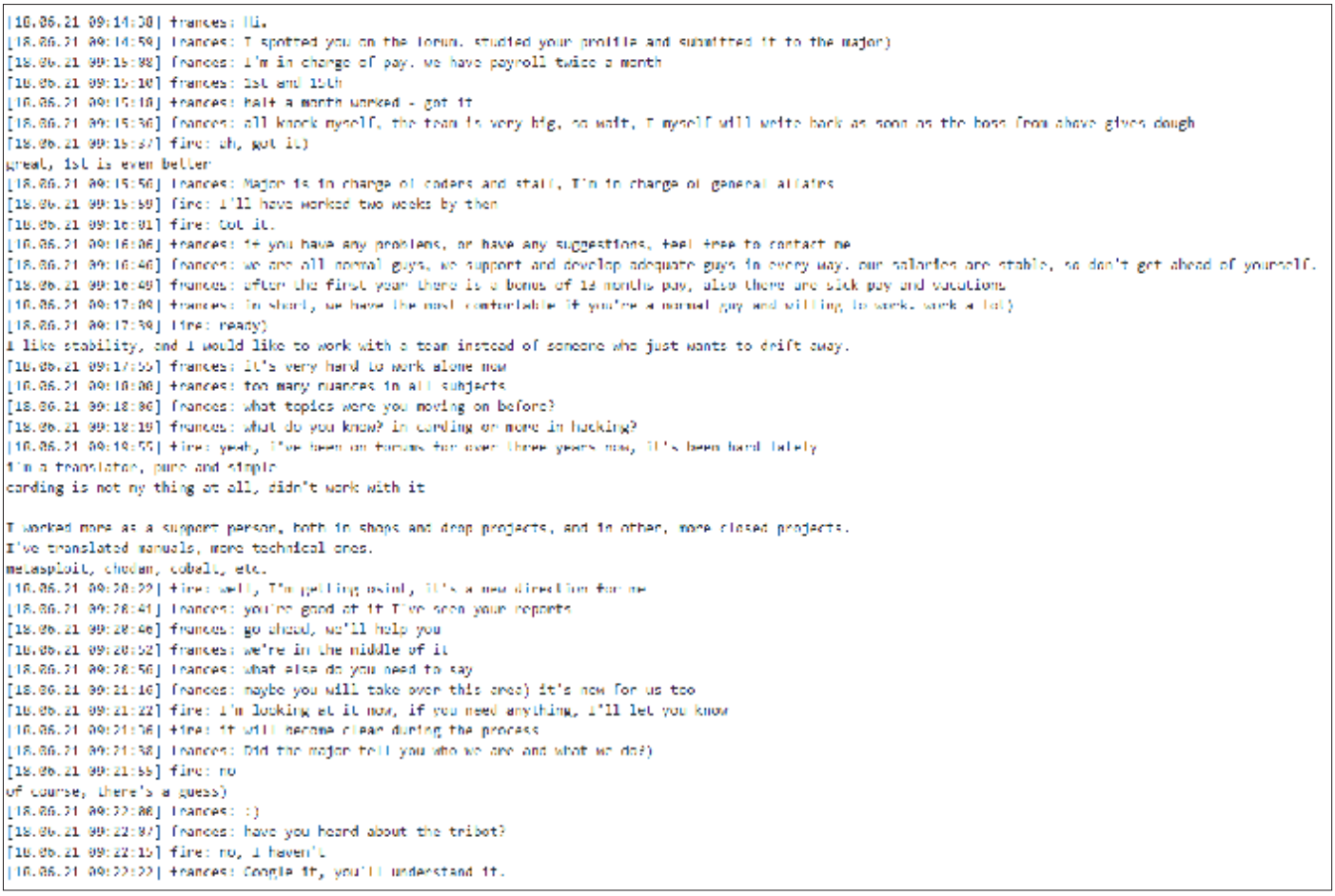


Figure 31

Each member within the organisation has an agreed salary, with most developers starting on around $2,000 per month. This is paid on the 1st and the 15th of the month. All salaries are paid in cryptocurrency, with the most common one being Bitcoin. Staff are instructed to inform their manager of their current wallet address, which is often a task carried out by the previously mentioned the user frances. Below in ***Figure 32***, the user fire can be seen sending their wallet address for payment. However, there is a delay due to the wallet being “hot” and so, the payment is made on the 19th of July.

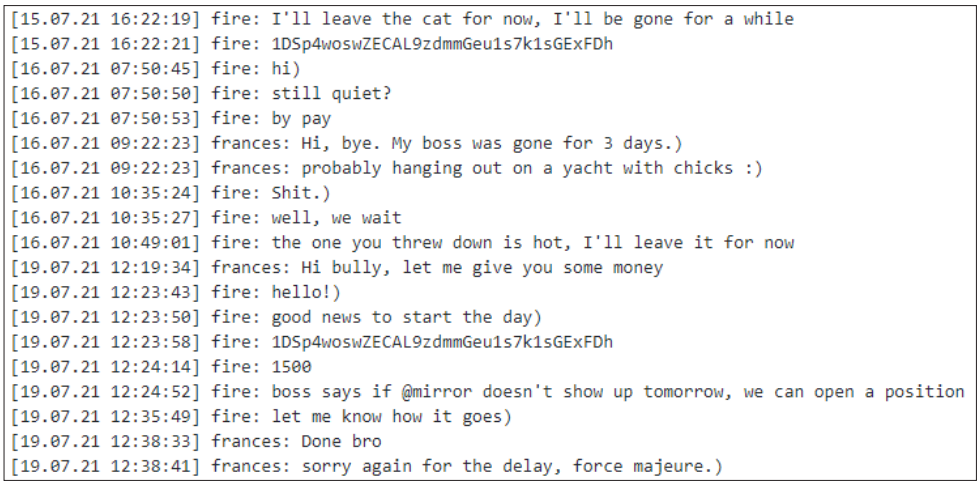


Figure 32

The user fire provided their wallet address 1DSp4woswZECAL9zdmmGeu1s7k1sGExFDh and this transaction can be tracked. To visualise this, a graph was made in Crystal Explorer which is shown in ***Figure 33***. In this we can see that 0.04868817 BTC is transferred into the user fire’s wallet at 12:52 on 19 July 2021. According to blockchain.com at 13:00 on July 19, 2021, the price of one BTC was $30,731.73. This means that the transactional value at the time is $1,496.27, almost exactly the $1,500 asked for. This

leads one to estimate with a strong level of confidence that the salary payment shown below is one of the many made by the organisation.

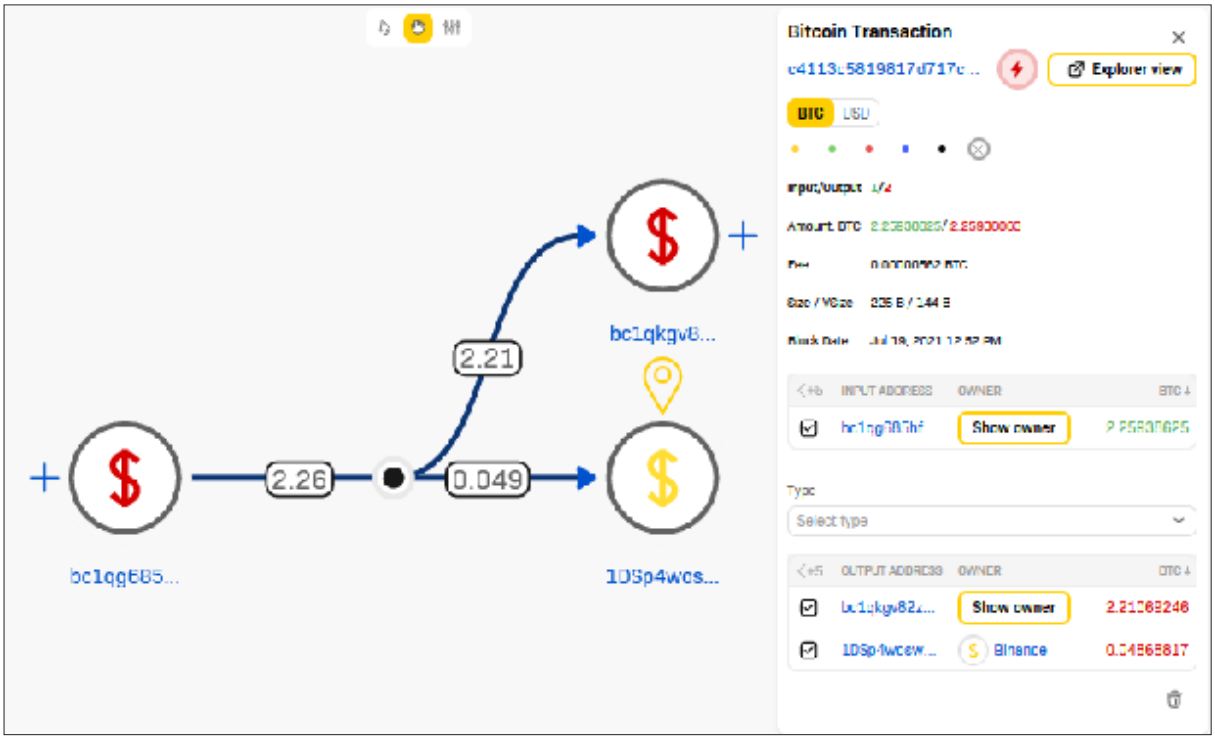


Figure 33

All the analysis identifies a highly sophisticated organisation, with strong management structure but also an efficient system of payment to encourage high quality work. It also identifies the need to consider all development work, as operational security measures require a full team working against deadlines. What used to be described by some as a “loose affiliation of malicious criminal actors” is now a cybercrime business in competition with others.

While IOCs and code samples play a key part in the battle against these organisations, it may be a lost cause. The analysis of the resources and coordination within the teams allows for a level of development capability, mutating fast enough to negate most standard commercial cyber security precautions.

It is critical to deconstruct these organisations and make use of the tactics, techniques and procedures (TTP) used by them to augment traditional security controls and frameworks. Threat hunting, machine learning, security visibility, orchestration and automation all need to be tuned to activity that matches MITRE ATT&CK® to “outpace” enterprise level operators, such as Trickbot.

Trickbot are collaborating

Another important takeaway from analysing this data is identifying the interconnected nature of cybercriminal groups. It appears that Trickbot encompass or is part of many groups. In the title of the PDFs alongside the messages, shown in ***Figure 34***, the leaker alleges that the Trickbot organisation is encompassed within the Wizard Spider organisation alongside Conti, Maze, Ryuk and Diavol.

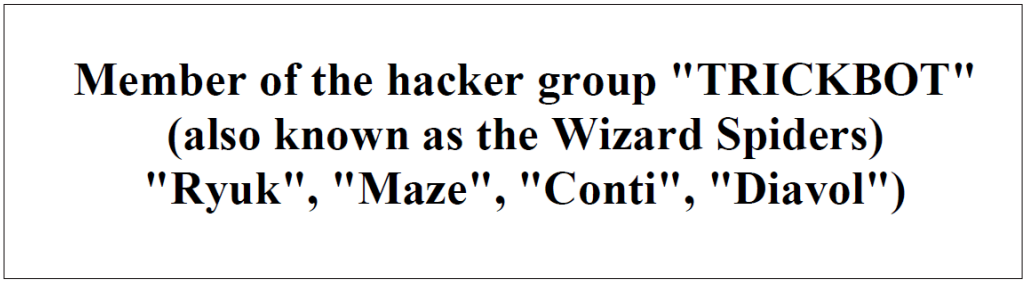


Figure 34

Our analysis of the leaked data supports this hypothesis. It seems the Wizard Spider group may be the main organisation, where each separate group is a different branch beneath it. Each branch, however, is not exclusive and it seems individuals who work with for Conti may also work with Trickbot and vice versa. An example of this within Trickbot's leak is the user esteban, who appears to be the manager of the Diavol malware. This conclusion comes from not only being one of the only people to mention the malware by name, but in a message from the user silver in which he directly references the user esteban as the manager of the Diavol project, shown in ***Figure 35***.

```
[10.11.21 14:11:23] silver: esteban is sick
[10.11.21 14:11:36] silver: take away his access to both the git and the admin
[10.11.21 14:11:41] silver: he needs to be replaced by someone else for now
[10.11.21 14:12:01] martin: What's his project?
[10.11.21 14:12:07] silver: admin locker
[10.11.21 14:12:40] silver: diavol is called
[10.11.21 14:14:35] martin: Copy that, I'll text him now.
```

Figure 35

However, not all groups seem to fall under the Wizard Spider banner, with some associates appearing to be what the group refer to as "clients". One such client is "Zeus", who is referenced multiple times throughout the leak. We know from messages shown in ***Figure 36*** that there is a user named zeus, who also goes by the pseudonym robin.

```
[03.08.21 07:35:26] silver: hi
[03.08.21 07:35:37] silver: adam yes, robin don't know
[03.08.21 07:35:40] silver: that's our inside kitchen.
[03.08.21 07:35:43] rocco: robin is zeus
[03.08.21 07:35:48] silver: I know
```

Figure 36

However, it is possible that "Zeus" also refers to the Zeus family of banking malware, also known as Zbot. This is a Trojan used to steal banking information and conduct other kinds of generic info-stealing. This conclusion is drawn from the way that members talk about "Zeus", both as an individual and as a group, as well as occasionally referring to it as software. An example of this is when the user angelo and the user hugo are discussing how the user angelo, who appears to do a significant amount of work for "Zeus", has a new task. This conversation can be seen in ***Figure 37***, and in it we find some important revelations.

```
[06.12.21 17:52:34] angelo: I have a new task
[06.12.21 17:52:43] hugo: What?
[06.12.21 17:53:06] angelo: with zeus.
[06.12.21 17:53:07] hugo: To get fucked up?)
[06.12.21 17:53:11] angelo: which one is not important
[06.12.21 17:53:20] angelo: i got a fuckload of stuff everywhere
[06.12.21 17:53:21] hugo: You're admin?
[06.12.21 17:53:26] angelo: and admin
[06.12.21 17:53:32] angelo: and what not
[06.12.21 17:53:55] hugo: Nice panel?
[06.12.21 17:54:33] hugo: I thought zeus died a long time ago
[06.12.21 17:54:43] hugo: Or obsolete.
[06.12.21 17:54:53] hugo: It's a banking trojan
[06.12.21 17:58:13] angelo: Zeus is human.
[06.12.21 17:58:32] hugo: ?
[06.12.21 17:58:34] angelo: important client
[06.12.21 17:58:41] hugo: hmm.
[06.12.21 17:58:54] hugo: There's also a banking trojan
[06.12.21 18:00:14] angelo: heard that.
[06.12.21 18:00:26] angelo: we have all kinds of clients/cooperation
```

Figure 37

Here the user angelo not only confirms the initial suspicions and shows that “Zeus” is both a person and a banking trojan, but also, they appear to be an important client of Trickbot. While the context of being a client is not clear, one can assume smaller groups or individuals can pay or offer services to gain knowledge or work from the Trickbot organisation. The process potentially follows cyber criminals being for hire by other cyber criminals. This activity seems to develop a beneficial relationship between threats actors, enabling newer actors to gain from the experience of the larger group. In addition, the larger groups can gain insight or potential recruitment pipelines for their organisation. One more important thing to note is that the user angelo also says “we have all kinds of clients/cooperation”. This clearly states Trickbot is not working alone but instead is working alongside, and for, a wide variety of other threat groups.

An example of the work being done for “Zeus” by Trickbot is known internally as “Project Anubis”. This appears to a loader malware with potential VNC modules used for exploitation and remote access. Through research it appears that the project, whilst initially developed for “Zeus”, is now part of Trickbot’s modules known as anubisDll[4] . From messages between the user angelo and the user manuel, shown in ***Figure 38***, it appears the relationship with “Zeus” developed to the point where the groups partnered together. This allowed Trickbot to not only make use of the Anubis loader they developed, but also incorporate the Zeus banking trojan payload which was suspected to be implemented into Trickbot as early as July 2021[5].

```
|07.12.21 15:28:49| angelo: Anubis is ours now
[07.12.21 15:29:21] manuel: Who's anubis?
[07.12.21 15:29:23] manuel: )
[07.12.21 15:29:46] angelo: if we're not talking about deities
|07.12.21 15:29:51| angelo: the Zeus botnet)
[07.12.21 15:31:08] manuel: Which one is working now? The new one, right?
[07.12.21 15:31:18] angelo: Yeah.
|07.12.21 15:31:29| angelo: I still don't understand they're us now
[07.12.21 15:34:52] manuel: What do you mean us? )
[07.12.21 15:35:06] angelo: You mean their bot
[07.12.21 15:35:10] angelo: It's our bot too
|07.12.21 15:35:15| angelo: or all separately ?!
[07.12.21 15:35:22] angelo: just wondering what is the relationship
[07.12.21 15:35:25] angelo: you never know
|07.12.21 15:36:29| manuel: I understood that they bought it all together with the coder from someone of our client
[07.12.21 15:37:08] angelo: did they buy it?)
[07.12.21 15:37:48] angelo: I think i  different
[07.12.21 15:38:45] manuel: that's what zeus told me
|07.12.21 15:38:59| angelo: Hmm.
[07.12.21 15:39:07] angelo: but zeus is our client ?
[07.12.21 15:39:12] angelo: no more
|07.12.21 15:39:14| manuel: Yeah.)
[07.12.21 15:39:28] manuel: Partner, let's say.)
[07.12.21 15:40:02] angelo: got it
[07.12.21 15:40:09] angelo: I thought we kind of teamed up
|07.12.21 15:40:13| angelo: with them
[07.12.21 15:40:47] manuel: That's right.
[07.12.21 15:42:29] angelo: that's it, we're friends
```

Figure 38

This level of collaboration between cybercriminal groups is significant. Groups such as Trickbot are not working alone and instead appear to be working within larger organisations, such as Wizard Spider. This seems to not only greatly improve their technical capabilities, but their gravitas and reputation within the community. This enables cybercriminal groups to develop professional relationships with one another, improving all aspects of the community.

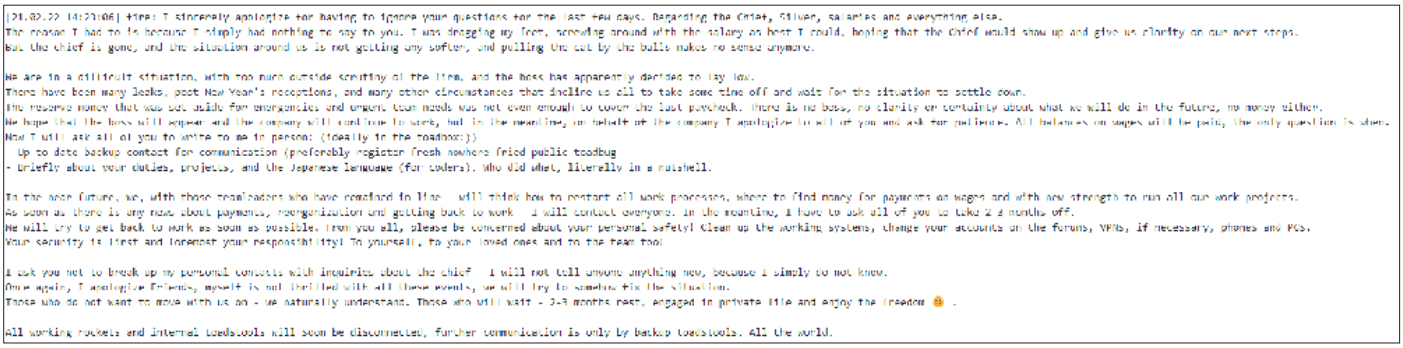
Defending against of the agility and diversity of cybercriminal groups working in collaboration is daunting. Knowing this is the current situation reinforces the need for good security information sharing within the security community. By building large knowledge bases of TTPs, IOCs and MITRE ATT&CK® profiles we can strengthen cyber defences, build better intelligence lead organisation architectures and deploy security products and services which are matched against cybercriminal innovations.

4 https://securelist.com/trickbot-module-descriptions/104603/
5 https://www.kryptoslogic.com/blog/2021/07/trickbot-and-zeus/

Trickbot are changing

A final observation is that the state of Trickbot is changing dramatically. Conversations found within this leak paint a dire picture for the future of Trickbot. Despite their success over the past few years, messages seem to imply towards the end of February 2022 that the situation in the company was not ideal.

A message sent by user fire into the previously mentioned Fire_Team chat on the 21 February 2022, pictured in ***Figure 39***, explains the situation the group is currently facing.


[21.02.22 14:21:06] fire: I sincerely apologize for having to ignore your questions for the last few days. Regarding the Chief, Silver, salaries and everything else.
The reason I had to is because I simply had nothing to say to you. I was dragging my feet, scrolling around with the salary as best I could, hoping that the Chief would show up and give us clarity on our next steps.
But the Chief is gone, and the situation around us is not getting any softer, and pulling the cat by the bulls makes no sense anymore.

We are in a difficult situation, with too much outside scrutiny at the time, and the boss has apparently decided to lay low.
There have been many leaks, post New Year's receptions, and many other circumstances that incline us all to take some time off and wait for the situation to settle down.
The reserve money that was set aside for emergencies and urgent team needs was not even enough to cover the last paycheck. There is no boss, no clarity or certainty about what we will do in the future, no money either.
We hope that the boss will appear and the company will continue to work, but in the meantime, on behalf of the company I apologize to all of you and ask for patience. All balances on wages will be paid, the only question is when.
Now I will ask all of you to write to me in person: (ideally in the roadmax:))
  Up to date backup contact for communication (preferably register fresh nowhere fried public toodbug
- briefly about your duties, projects, and the Japanese language (for coders). Who did what, literally in a nutshell.

In the near future, we, with those roadleaders who have remained in line - will think how to restart all work processes, where to find money for payments on wages and with new strength to run all our work projects.
As soon as there is any news about payments, reorganization and getting back to work - I will contact everyone. In the meantime, I have to ask all of you to take 2-3 months off.
We will try to get back to work as soon as possible. From you all, please be concerned about your personal safety! Clean up the working systems, change your accounts on the forums, VPNs, if necessary, phones and PCs.
Your security is first and foremost your responsibility! To yourself, to your loved ones and to the team too!

I ask you not to break up my personal contacts with inquiries about the chief - I will not tell anyone anything new, because I simply do not know.
Once again, I apologize friends, myself is not thrilled with all these events, we will try to somehow fix the situation.
Those who do not want to move with us on - we naturally understand. Those who will wait - 2-3 months rest, engaged in private life and enjoy the freedom 😊 .

All working rockets and internal toodstools will soon be disconnected, further communication is only by backup toodstools. All the world.

Figure 39

The message details that the organisation has had trouble paying employee salaries and difficulty communicating with some of the more prominent members, such as user silver and “the Chief”. While it is not clear who “the Chief” is, it is likely the user stern, who prominently features in both the Trickbot and Conti leaks. This user is potentially the CEO of the organisation. This is due to the user stern featuring prominently in the management conversations in both Conti and Trickbot, placing them as the leader of the whole organisation with control over funds and assets.

It is important to note this message was sent on the 21 February 2022, which was before the Conti and Trickbot leaks were released. Inside this message the user fire says “many leaks, post-New Year’s receptions, and many other circumstances” are responsible for the current cashflow situation. While we can try to speculate on the reasons for this situation, it is not clear what is meant by “other circumstances”. However, the context of this message coming only three days before Russia’s declaration of war on Ukraine may not be entirely a coincidence. From what we have seen within the leaked PDFs, multiple members of Trickbot hold Ukrainian passports and potentially have or still do live in the country. This could have led to difficult internal situations for Trickbot and strained potential ties or alignment with the FSB and Russian government. It is unclear how involved this conflict was with the group and how the management felt about that.

Further in the message, the user fire also states that they hope the boss reappears and the company will begin to operate again. This reaffirms how reliant the organisation is on its “management team”. Despite the large teams, communication with other groups, and large pools of money, it appears as if a few of the key management members are removed. The group, therefore, may be highly vulnerable to fragmentation. The managers are likely to control access to Trickbot’s assets and provide clarity as to their aims. It seems the managers within the criminal organisation are the weakest point of the group, with minimal thought given to succession planning.

Adversity often breeds innovation, and it appears Trickbot is preparing to start again. They are looking at potential ways they can restart the processes within the company, collecting the details of current members and informing them that when there is work again, they will be contacted. The time scale they give is around 2-3 months from the message, which coincides with the end of May / start of June 2022.

Trickbot directed all members to change all forum accounts, VPNs, phones, and even PCs if necessary; stating that “security is first and foremost your responsibility” and finally all Rocket Chats and Jabbers will be taken offline. By making the responsibility of security on the members themselves, this severely weakens the operational security of the group. This is because the removal of centralised control requires the trust of members to carry out operations securely. Moreover, this also potentially coincides with what we have seen happen to other groups under the Wizard Spider banner, with reports of the Conti organisation

disbanding. These rumours appeared after large sections of the Conti's backend infrastructure was taken offline. While this message does not confirm the suspicion the activity was leak related, it seems to provide a plausible explanation for reasons why members of the Trickbot and Conti organisations may have moved elsewhere to work for groups such as HelloKitty and AvosLocker.

While it is difficult to say what the state of Trickbot, Conti and the whole organisation is currently, it is clear that they have undergone some impactful changes. This has led to Trickbot starting to collapse before the leaks even surfaced. Now that samples of their malware, personal information, and nearly all the tactics, techniques and procedures used by the group have been leaked, we can confidently say that Trickbot's operations and organisation has substantially degraded. It is important to realise cybercriminals can and will improvise, adapt, and re-organize quickly and join other organisations. Those with "managerial" talent will start assembling a new organisation. Just like the malware itself, cybercriminals are also innovating at a rapid pace to survive in this changing landscape.

Conclusion

Through the research into the Trickbot leaks, we now have a better understanding of not only the organisation, but of the wider cybercriminal threat landscape. These leaks have provided greater insight into the infrastructure used in an operation of this size, including the creation of bespoke management consoles like Botleggers Club and the thousands of bots and servers used for distribution and operation.

The most valuable insight has been through Trickbot's management teams and the ability to focus on the members themselves, giving us a different perspective into what comprises a cybercriminal group. This enables one to view Trickbot as the business it is, as opposed to some incomprehensible entity which causes harm. Whilst simple, this business model enables researchers, and perhaps law enforcement, to identify real-world weaknesses more accurately within the organisation. Identification of Trickbot's operational security, tactics and structure may be identified and exploited by those wishing to disrupt their operations. As we have seen, multi-million-dollar crime operations, with potential governmental ties, can be halted by the loss key members. This is best demonstrated by the departure of users' stern and silver.

The threat we face today is often depicted as hundreds of individual groups, each with different tactics, techniques, and procedures vying for money and notoriety. From what we have seen, it appears this claim is highly exaggerated. Evidence, such as the overlap in members from the Conti leaks, and the conversation around clients suggests the cybercriminal community is more closely connected than reported. Cybercriminal groups are working together, helping each other, and most of all collaborating on developing the capabilities to cause maximum harm, or in cybercriminal dialect "make the most money possible".

Through this set of over two years' worth of messages, we have been given unprecedented insight into not only how Trickbot operates, but also how the industry leaders and managers in organised cybercrime are operating. Through the analysis of the leaks, we gained an exposed look at Trickbot, revealing not only their TTPs, but the malware and C2 developmental process. It also revealed the recruitment process and a managerial structure which underpins the way this and perhaps other criminal organisations work.

Joe Wrieden
Intelligence Analyst

sales@CYJAX.com

Appendices

Appendix 1: The Cryptolocker Terms of Reference

CRYPTOLOCKER
TERMS OF REFERENCE

OBJECTIVE

To develop a simple and effective minimalistic cryptolocker.

REQUIREMENTS

- Minimal binary size
- Conformance to requirements in “code and assembly design”.
This includes treating the program as a dll and having an entry point for Cobalt Strike
- Availability of a builder (configurator) that flashes the settings and creates a locker-anlocker pair
- Use of fast streaming cipher (ChaCha20 or similar), to achieve maximum speed and speed of covering the
system.
The key management scheme can replicate the REvil/Sodinokibi https://blog.amossys.fr/sodinokibi-malware-analysis.html
(A symmetric key to cover the Chacha20 files is generated at the start of the locker;
it is encrypted with RSA4096 public key embedded in the locker and saved on the disk of the covered machine;
the RSA4096 private key is flashed into the locker, allows reading and decrypting the ChaCha20 symmetric key used for the locker)
- The program should cover all available network shares.
- the streaming model of the program should maximize disk and network balls processing
- the key quality of the program’s performance is its speed of disk processing.

PROTECTIVE MEASURES

- Obfuscation of strings and system calls
- Remove AB hooks at startup
- Mitigation for protection against injection
- Injection protection with BaseThreadInitThunk hook
- process halt protection (check under WOW64!)
- Protection against computer restart while running (check under WOW64!)
- remove shadow copies at startup (check with WOW64!)
- Disable Windows recovery mode

IDENTIFICATION

The bot is identified by a pair of
1. dev-id, which is calculated as a hash function of the system’s unique hardware and OS characteristics.
Purpose: to identify the computer.
2. encryption key, which is stitched at the build stage.
Purpose: to identify the target being attacked, find an unlocker for a specific target based on this fingerprint.

Details:
1. It is suggested to use md5/sha-hash from the string “creation_date%windir%.computer_name.
creation_date%windir\system32%.domain_name_or_workgroup”.
This can also include the name of the hard disk, MAC address of the network interfaces, and other

hardware names.
The key properties of dev-id are
- dev-id must be generated every time
- it must be the same every time it is run from different users on the system
- it must not be saved to disk
- it must be unique
- it must always be generated identically on the same computer.
2. the Bilder creates a pair of executable files “locker-anlocker”, generating for them a pair of crypto-keys and flashing them into the files.
Wherever a key is used for identification purposes (rather than disk encryption), a short key fingerprint must be used.

BILDER

A builder is a console program that
- takes two files as input - a locker and an unlocker
- generates a pair of crypto-keys, exports them to files
- flashing these keys into the locker and the locker.
- you must have possibility to generate key pairs and use previously generated key pairs (from files).
- flash other settings, given from the command line (see #9 of the ALGORITHM section).
- Outputs the flashing of the locker and the locker with the changed names.
The name of the locker and the anchor must have a key fingerprint and creation date mixed in, e.g: locker_aabbccddeeff_01012020.ex_
- the output file extension should be .ex_ to prevent accidental startup!!!

ALGORITHM

1. Check keyboard layout, and if it matches any country from CIS + Ukraine area, terminate immediately. This feature should be disabled via conditional compilation.
2. Generate your dev-id
3. Generate key fingerprint
4. Generate text for the in-memory lending file, substituting your identifiers in it.
(left blank here on purpose).
8.3 The program works in one of two modes: fast or full.
In fast mode, only the first megabyte of the file is encrypted. This is needed to get a quick lock on the system.
Full mode encrypts the entire file.
Settings are provided for the fast mode:
- file coverage percentage
- Maximum file size for full cover (after this size the file will be partially covered)
These settings are best configured on the command line.
If you want to cover part of the file, do it either in staggered order (first 1M covered, next 1M skipped, next 1M covered, etc.),
or according to some predictable formula (golden section progression to avoid concentrating the maximum area to be covered
in only one area of the file).
8.3.1 After the directory is processed, a lending file with redemption text is created in it.
8.4 If a Share violation occurs (file is occupied by another process),
the program finds the blocking process and kills it, or stops the corresponding service.
When an error occurs the program tries to repeat the action three times with an interval of 2 minutes and then skips the file.

Further operation does not depend on the result of this step.
8.5 The program first processes the directories from a special “fast” list, the list of directories
The program first processes the directories in a special “fast list” - a list of directories to be skipped.
8.6 The program DOES NOT TAKE files or directories from the special stop list - the list of files which must not be touched.

Combinations of fast and stop lists are handled as follows: (*)
8.6.1 We cover all paths in the fast list that are not in the stop list
8.6.2 If the stop-list contains the whole disk, on that disk, we cover only the paths in the fast list, without affecting the rest of the disk
8.6.3 If the stop-list is empty, cover the folders from the fast list first; the rest of the files afterwards.
* See also item 12 about network modes.

8.7. The program encrypts only files with extensions from the list of working extensions; all other files are ignored.
8.8. The program deletes files from the special list, overwriting their contents three times
- first time with constant 0
- second time with constant FF
- for the third time with random rubbish
- on the fourth time, the file is deleted.
8.9. The program handles all drives in this way.
All operational errors are ignored.
8.9.1 All disks also include all available network shares as well as network drives.

9. List of settings which can be changed in the programme:
9.1. operating mode (fast/full)
9.2 encryption key
9.4. fast list
9.5. stop list
9.6. list of working extensions
9.7. delete list
9.8. lending file text
All lists can be directory paths or individual files.
All file related settings should support:
- wildcards (* character)
- Environment variables.
There should be provision for handling files without an extension (by default they should be handled).
All lists must be validated for correctness (known incorrect paths must be ignored).

10. The program will self-destruct after completion.

11. There should be two counters in the test build:
11.1. how much data is encrypted, in bytes
11.2. the size of the processed files, including partially encrypted, skipped, deleted, etc. - this is an indication of the overall processing speed.
These counters should be periodically logged along with current timestamp.
This is needed to measure the speed.

12. In addition you need to provide the following modes of scanning network resources/fileballs
12.1. local - encrypts local files only + priority list
12.2. net - encrypts only network resources + priority list.
List of network resources is specified in file, in ip\host address format, one line per host.
12.3. all - Encrypts as net + local (set by default)
12.4. scan - Encrypts as net + auto-scan by subnet mask
12.5. scanext - Host list is specified in file + as scan

Parameter can only be specified with -m net or without -m parameter.
Hosts file must contain ip\host address one line per host.

Network scanning and balloon processing takes a long time, so local file processing
in network modes must be started immediately.
Note that the same network disks may be mounted as local disks and be detected as a separate network balloon.
In such a case, re-encryption of the disk should be prevented.
In general great care must be taken to detect re-encryption of an already covered directory/resource,
as encryption can and will be run in parallel from multiple computers.

LANDING FILE

This is a text file with text about the ransomware.
The name is readme.<6 random letters and numbers>.txt.

Macros used in the file are:
%devid% - dev-id of computer
%fingerprint% - key fingerprint

The values created in steps 2 and 3 are used instead.

File text is set from the Bilder.

KNOWN BUGS AND LIMITATIONS OF WINDOWS

- when trying to open a file with WOW64-process on 64-bit Windows 7/8/2009,
the CreateFile/OpenFile functions always return TRUE status and no error code is returned.
at the same time a crash is possible while trying to read/write.
As a solution, the number of open process handles before and after attempting to open a file is checked.
- WOW64 process can't get a valid list of all descriptors in the system on 64bit Windows XP/2003
- When a file is opened by WOW64 process with FILE_FLAG_OVERLAPPED flag,
the file can be opened almost simultaneously by multiple read/write processes.
The file can be consecutively overwritten by all these processes.
Be careful when running multiple locks at the same time!
A named mutex will only help with local drives!
- Large buffer access delays when using virtual memory, especially noticeable on Windows 10.
Better to allocate memory from heap.
- File system/file corruption can lead to freezes when processing such files
- some encryption algorithms are slow on files with high entropy (media - .mp3, .mp4, .avi, archives, etc)

RESOURCES

https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
https://habr.com/ru/company/acronis/blog/522022/
https://www.carbonblack.com/blog/tau-threat-discovery-conti-ransomware/
https://www.carbonblack.com/blog/tau-threat-analysis-medusa-locker-ransomware/
https://blog.amossys.fr/sodinokibi-malware-analysis.html
More alive than ever: analysing the first sample of the new BlackMatter cipher
https://habr.com/ru/company/group-ib/blog/571940/

TEST PLAN

1. Functionality
Testing is performed with AV disabled.
All encryption modes and setting variations are tried.
Confirmed:
1.1. response of software to settings
1.2. compliance with specified encryption mode
1.3. correct handling of network drives and balloons
1.4. operation with several concurrently running instances of software on one computer
1.5. Same as 1.4, but same network ball is processed from different computers
1.6. Removing shadow copies of operating system volumes
1.7. maintaining operating system operability after work ends
1.8. stopping the locker from a normal user
1.9. stopping the locker from an administrator
1.10. preventing rebooting/stopping the machine

2. Compatibility
The test is done on the following versions of Windows:
2.1. Windows 10
2.2. Windows Server 2012-2018
2.3. Windows 8.1
2.4. Windows 7
2.5. Windows Server 2008 R2
2.6. Windows Server 2008 (no R2)
2.7. Windows XP
2.8. Windows Server 2003

3. speed.
The speed of operation is measured.
To do this, the software has to have built-in statistics metrics - you need a way to know the speed
3.1. in megabytes per second
3.2. file descriptors per second (as files might be small).
Of course, a correction is made for the fact that the test is carried out on virtual machines, however, it is possible to compare the figures with the competitors' software on the same VM.

4. antiviruses
4.1 Windows Defender
4.2. ESET.
4.3. Sophos.
4.4. Avast
4.5. BitDefender
4.6. Norton
4.7. Kaspersky
No detects 4.1-4.3 are required.
It is acceptable for an AV to make a behavioral detection, but not to take down the process before it has finished working.

About CYJAX

CYJAX is an award-winning technology company and provider of digital Threat Intelligence services to international corporations, law enforcement agencies and the public sector.

Using our state of the art technology and our world-class team of analysts, CYJAX monitors the Internet to identify the digital risks to your organisation from cyber threats, reputational risk, and the Darknet.

CYJAX provides an Incident Response and Investigation service that provides a calming and structured approach in helping organisations when a breach does occur.

Our proactive methodologies make sense of the noise and help make intelligence decisions, securing the future for our customers.

Trusted by enterprises like ***AstraZeneca, Disney, UK Power Networks, Viatris, HM Revenue & Customs,*** and more...