WAVESTONE

Summary of the study

THE CYBERCRIME ECONOMY:
AN OVERVIEW OF RANSOMWARE PLATFORMS

Laurenne-Sya LUCE

06/05/22 | Laurenne-Sya LUCE

The Positive Way

WAVESTONE

EXECUTIVE SUMMARY

The current invasion of Russia in Ukraine and the resulting tensions have led to the exposure of several Russian hacking groups.

Based on this new information, we were able to **characterize the organization** and **business model** of these groups more accurately .

Operating as genuine businesses, ransomware platforms are directly or indirectly responsible for **thousands of attacks** per year.

The profits generated by the ransom payments associated with these attacks enable these groups to **structure themselves as real businesses** with **salary systems** and a yearly profit of **tens of thousands of dollars**.

Introduction to the ransomware platforms ecosystem

Focus on CONTI

Introduction to the ransomware platforms ecosystem

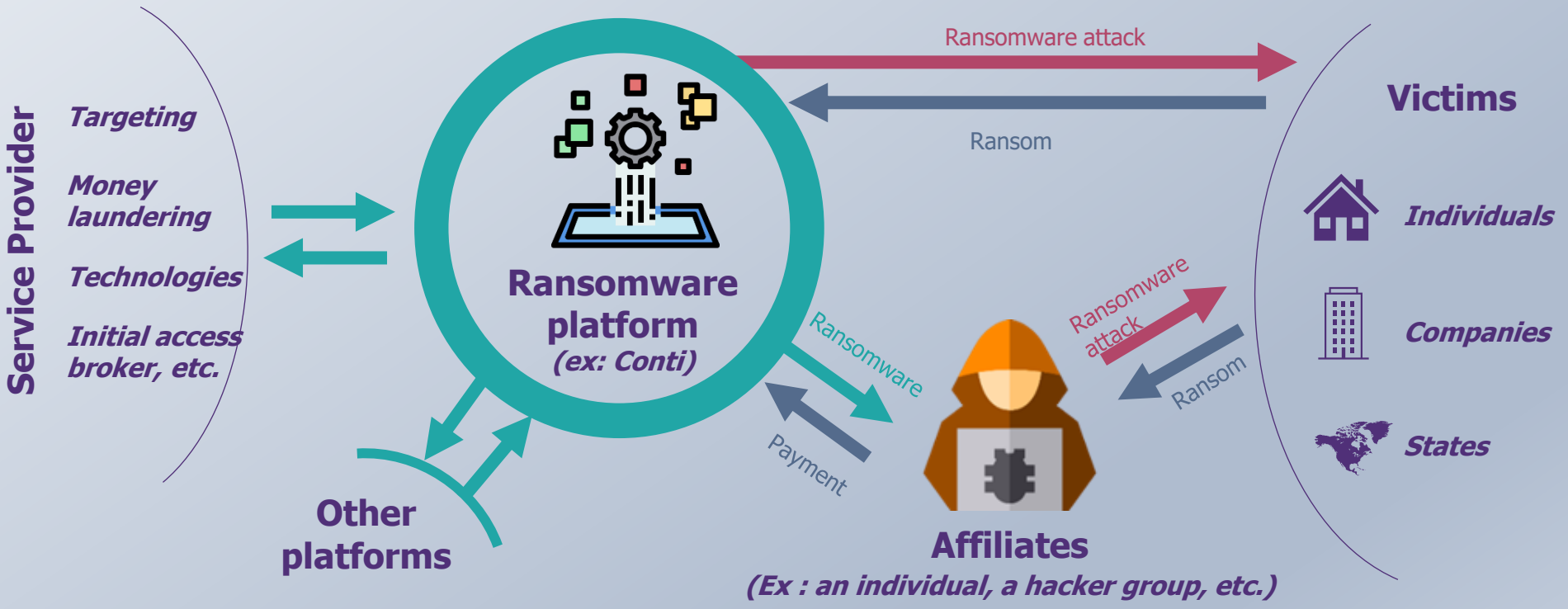
OVERVIEW OF THE RANSOMWARE PLATFORM ECOSYSTEM

Glossary

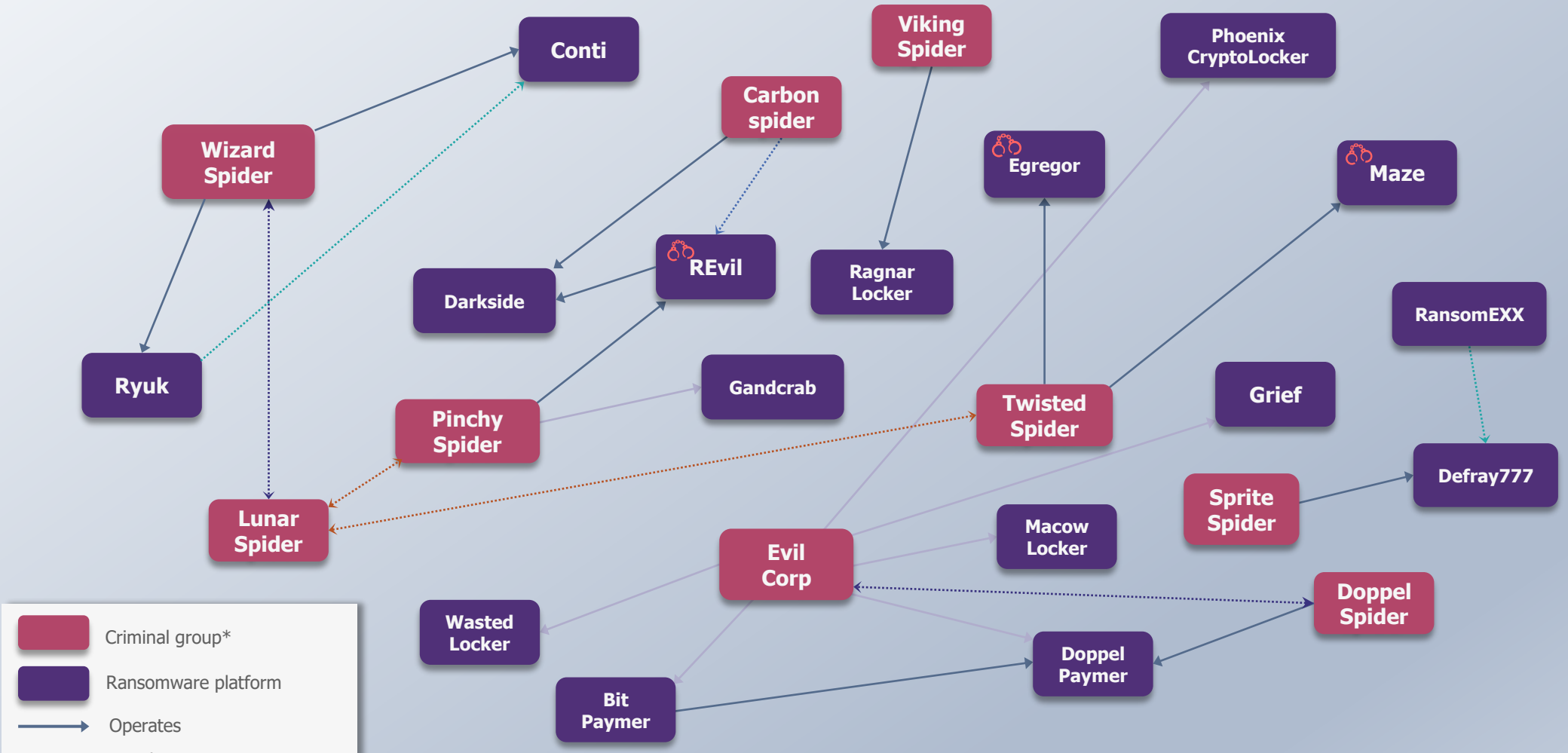
Ransomware platform: In charge of **developing and maintaining the malware infrastructure** and its **encryption**. The operator collects a certain percentage as a commission in exchange for access to the platform.

Affiliates: A person or a group, who rents access to a RaaS platforms**,** in charge of **spreading the ransomware strain**. The assembly line of ransom payouts are split between the developer and themselves.

An overview of the links between affiliates and ransomware platforms



THE RELATIONSHIPS BETWEEN THE VARIOUS CYBERCRIME PLAYERS



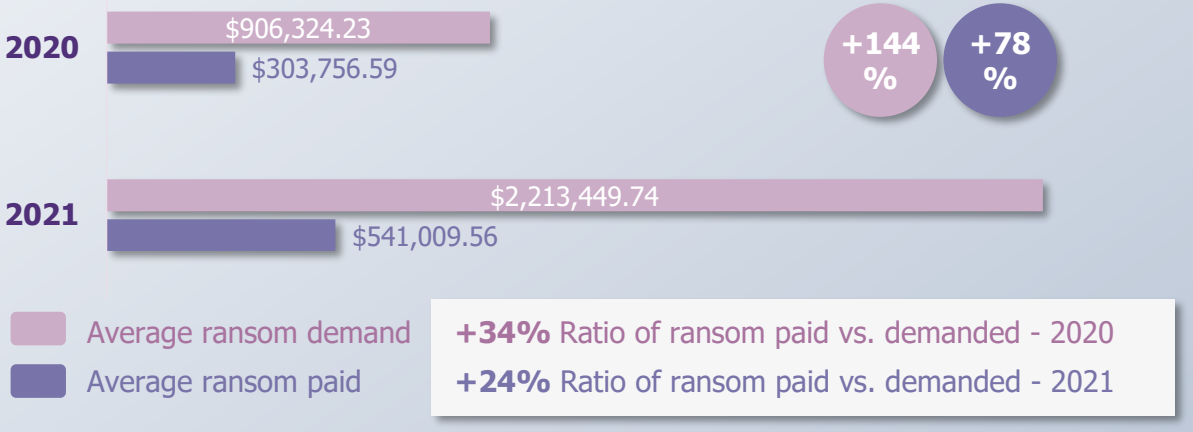
Threat actors often **rely on various ransomware platforms**. There are historical reasons for this, with hackers often having worked for both the ransomware platform and the attackers.

* Criminal groups with diverse activities (ransomware, malware, etc.) | sources available in appendix

"RANSOMWARE AS A SERVICE" AS A BUSINESS MODEL – WHICH RANSOMS FOR THE HACKERS...?

Average ransom demands vs. average ransom payment in 2021 and 2020*

according to Unit42 incident response data



The **aggressive tactics** of attacker groups, as well as the **criticality of the targeted data**, force victims to **pay increasingly high ransoms**: The average ransom paid from 2021 cases climbed to $541,010, which was **78% higher** than the previous year.

However, the **ratio of amounts paid to amounts demanded is decreasing** in 2021.

....WHAT ARE THE BENEFITS FOR RAAS OPERATORS?

Darkside's model

25% for ransoms less than $500,000
10% for ransoms greater than $5 million

Lockbit's model

20-30% of the ransom amount received from affiliates

Affiliates usually pay a **percentage** of their ransomware earnings back to the platforms they used.
These percentages **can vary**, for example, depending on the amount of ransom payments collected.

*Source : Unit 42 - Palo Alto Networks

Focus on CONTI

BREAKING NEWS : CONTI LEAKS?

ContiLeaks: Ransomware Gang Suffers Data Breach

Ukrainian Security Researcher Leaks Newer Conti Ransomware Source Code

By Eduard Kovacs on March 21, 2022

Greeting

Here is
shit. Pl
https://

The link will take you to download an 1.tgz file that can be unpacked
running tar -xzvf 1.t
dump contain the chat
the past) of the Cont

There are more dumps
You can help the worl

It is not malware or
This is being sent to

Thank you for your support

Glory to

"WARNING"

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

2/27/2022 3723 0 [0.00 B]

"WARNING"

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

2/25/2022 39 0 [0.00 B]

February 27, 2022

A Ukrainian Security Researcher, displeased with this position, **discloses 13 months of exchanges** and **sensitive data** on the operations of the gang

February 27, 2022

…before withdrawing and toning down their words a few days later

February 25, 2022

Pro-Russian members of the Conti group **publicly announce their support for the Russian authorities** in the ongoing conflict..

February 24, 2022

Beginning of the Russian military invasion in Ukraine

2022

FOCUS ON CONTI

WHO IS CONTI?

The **Conti** cybercrime group counts **more than 1,000 victims** to its name.
It is particularly highlighted following **data leaks revealing important information about the group's operations**.

Members
between **80** and **100**

RaaS operator

Discovery date| 2020

Associates/Alias
Wizard Spider, Ryuk, etc.

Revenues
Approximately $180 million earned in 2021

Number of attack
494 (2021)

Attack mode
Ransomware

Victims: ExaGrid, Irish Health Service Ex, etc.

Conti has been responsible for major attacks that have **destabilized** countries or **major organizations** over the past two years: **Assu2000, Inserm Transfert, ExaGrid, Solware, Irish Health Service Executive**, etc.

ESTIMATED CASH FLOW STATEMENT OF CONTI

Recent disclosures about the Conti Group have provided **insight into its organization**.

To understand the business model of ransomware platforms, the following is aimed at establishing an estimate of revenues, various cost items as well as the **net profits earned by Conti** in 2021.

NOW LET'S BUILD CONTI'S CASH FLOW STATEMENT

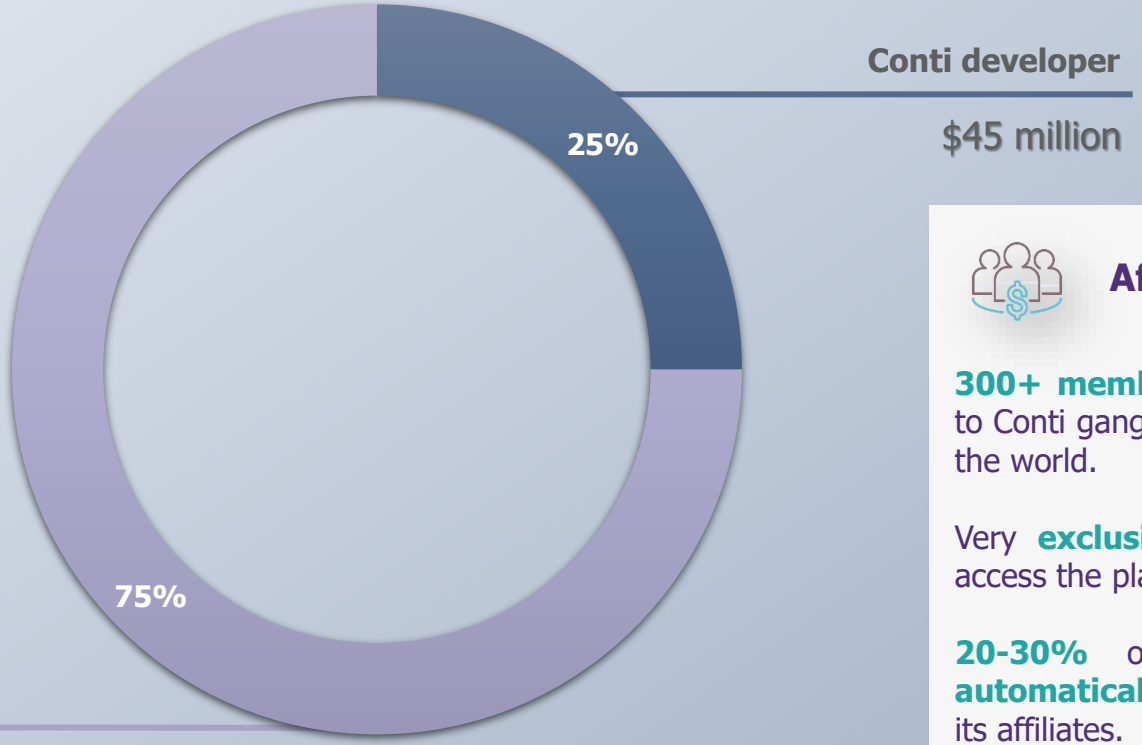
OVERDRAFT FACILITIES	M$ IN 2021	HYPOTHESIS
Affiliate ransom		
Income allocated to affiliates		
Turnover		
Offices		
Capital assets		
…		
…		
..		
Net cash from operations in 2021		

CONTI : THE MOST LUCRATIVE RANSOMWARE PLATFORM IN 2021

Turnover

With more than **494 attacks**, the Conti group raked in more than **$180 million**, topping the list of most lucrative ransomware platforms in 2021.

Share of ransom payments received by the Conti developer and affiliate
in 2021



Affiliation program

300+ members and affiliates belonging to Conti gang are conducting attacks around the world.

Very **exclusive** about who is allowed to access the platform.

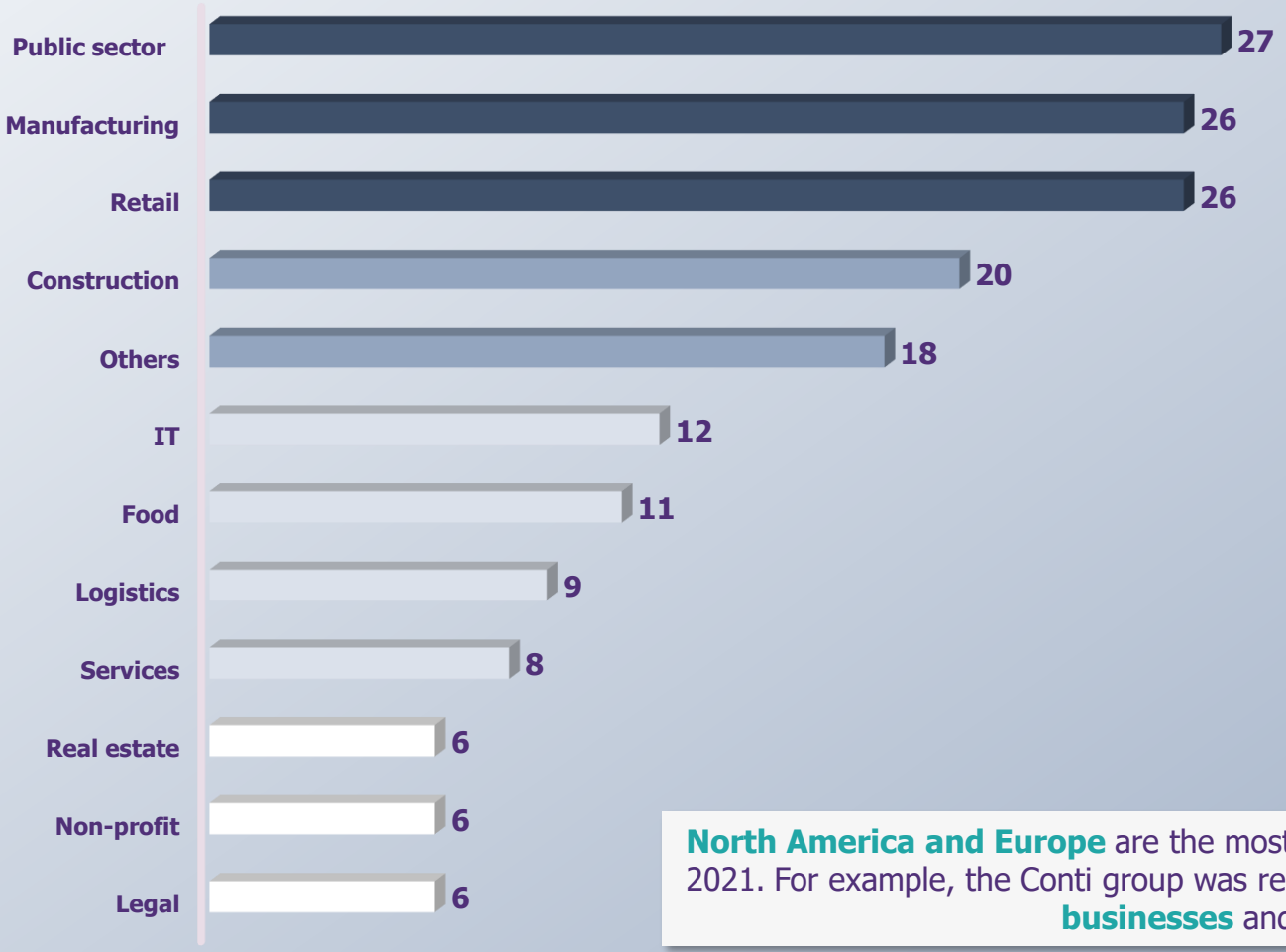
20-30% of the ransom amount is **automatically paid to the platform** by its affiliates.

1.Source : Varonis 2. Sources : Secure works, ZdNet 3. Source : l'Usine Digitale 4. Source : Breachquest

FOCUS ON CONTI'S TARGET

Targeted sectors/industries by Conti

According to data published in "Conti News" site (February 2021)



Although no single sector has been spared by the gang, Conti has primarily targeted the **retail**, **Manufacturing**, and **public sectors**. These targeted attacks can be explained by the **higher vulnerability** of these industries to such attacks, and/or by **their high visibility** to the public.

North America and Europe are the most targeted regions for ransomware attacks in 2021. For example, the Conti group was responsible for at least **400 attacks**[2] **on U.S. businesses** and **organizations**.

1. Source : Sophos 2. Source : CSA

ESTIMATED CASH FLOW STATEMENT OF CONTI*

OVERDRAFT FACILITIES	M$ IN 2021	HYPOTHESIS
Affiliate ransom	180	*See attached sources*
Income allocated to affiliates	135	75%, *See attached sources*
Turnover	**45**	

We **hypothesized** that Conti may be receiving **subsidies** of various kinds from the **Russian government**.

However, it is **not confirmed** by any sources for the moment.

Over 200 Bitcoin addresses have been identified pointing to Conti since the beginning of the war, with a value of approximately $180 million in 2021.

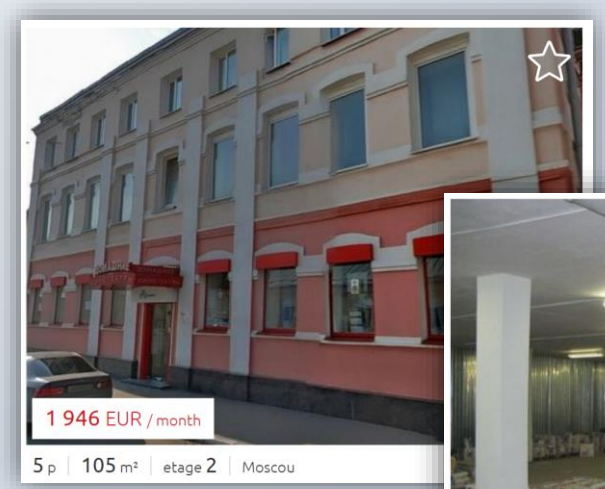
The **20 to 30% of the earnings returned by affiliates** enable the platform to generate a turnover of about **$45 million**.

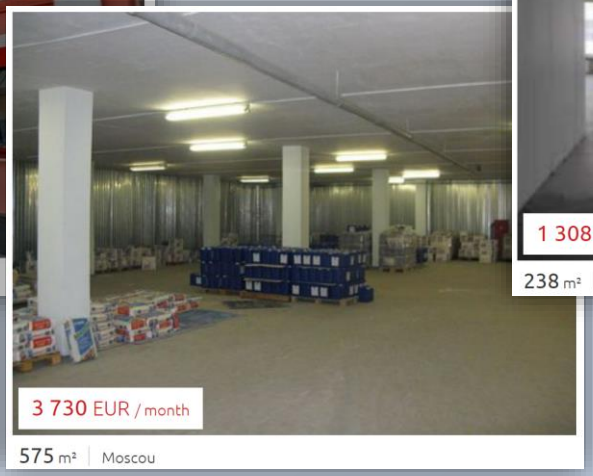
*All the sources to build this table are listed in this excel.

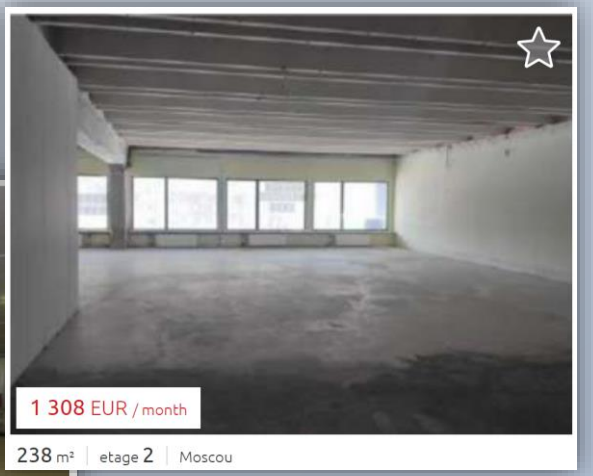
CONTI'S EXPENDITURE ITEMS

Capital assets

The group rents between **3 to 4 physical offices** in Russia. These offices are fully equipped and are **available for use** by the various teams.







target
now money is flowing in three directions

1) these are operators current expenses + expansion = total 2 offices with large teams - one main and one new on training
2) hacker offices (3 pcs) - interviews, equipment, rent, interviews, deposits, inside servers, equipment, hiring and hiring assistance and a whole lot more, and in a week another salary will be added for those who will work there (20+ hackers)
3) an office with programmers and equipment for everything + a good team leader has already been hired and he will collect the team for the pro, this is an important devops for the pro, the pro is happy with everything and he really needs it

+ we hire third-party specialists with a professional to speed up various processes

I'm sure everything will pay off, so I'm not nervous

Sources : Arkadia, Check Point Reaserch

ESTIMATED CASH FLOW STATEMENT OF CONTI*

OVERDRAFT FACILITIES	M$ IN 2021	HYPOTHESIS
Affiliate ransom	180	*See attached sources*
Income allocated to affiliates	135	75%, *See attached sources*
Turnover	**45**	
Offices	0.14	*See attached sources*
Capital assets	**0.14**	

Unlike a traditional company**, capital costs weigh very little** on the group.

*All the sources to build this table are listed in this excel.

CONTI'S EXPENDITURE ITEMS

Expenditures

6M$

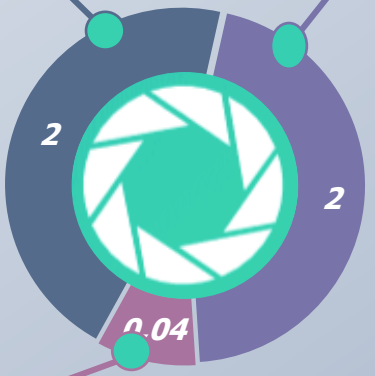
estimated expenses on professional services, tooling and employee salary*

(*excluding commissions and bonuses*)

Tooling & SaaS subscription ~$2M

/ These expenses mainly includes the purchase of **antivirus tools**, **VPN service,** test software (such as **Cobalt Strike**) and so on.

/ Conti invested **$60,000** in acquiring a valid license to **Cobalt Strike**. Half of the investment was paid to a legitimate company that secretly purchased the license on Conti's behalf.



Infrastructure ~$0,04M

/ **$3-4k** per month is spent on **server** and **router maintenance**

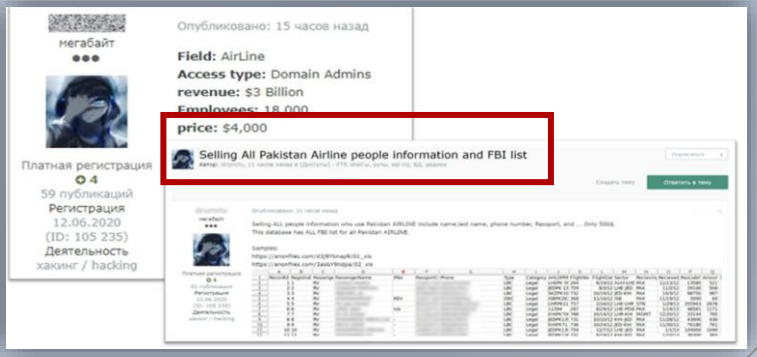
total 146 294 \ 2 = 73 147 for salary + 700 bucks will go to commissions for transfers from wallets / withdrawals from exchanges and 3-4k are needed for expenses on routers / servers / gaskets

Excerpt from a conversation

Professional services ~$2M

/ The group would use **initial access brokers** such as EXOTIC LILY.

/ The **average selling price** of a victim's network access is approximately **$4600** in 2021. These **prices can fluctuate** depending on several parameters such as the visibility of the targeted company.



An actor sells access to Pakistan Airlines and an FBI list

Sources : Breachquest, KrebsOnSecurity, Check Point Reaserch, ZdNet, Kela

ESTIMATED CASH FLOW STATEMENT OF CONTI*

OVERDRAFT FACILITIES	M$ IN 2021	HYPOTHESIS
Affiliate ransom	180	*See attached sources*
Income allocated to affiliates	135	75%, *See attached sources*
Turnover	**45**	
Offices	0.14	*See attached sources*
Capital assets	**0.14**	
Infrastructure (servers, routers, EDR, etc.)	0.04	Between $3-4k, *See attached sources*
Tooling & SaaS subscriptions (software, etc.)	2	Approximately $2M would be spent out of the $6M expenses, *See attached sources*
Professional services (Initial access broker (IAB), etc.)	2	$4600 average network access price, *See attached sources*
Money laundering	**23**	50%, *See attached sources*
Expenditures	**27**	

Our sources do not specify the amounts allocated by Conti to **laundering ransom money**.

In other crime fields, these amounts are generally estimated at **50% of the profits made**.

The **main cost components** for the group are related to **money laundering** and **third-party services**.

*All the sources to build this table are listed in this excel.

CONTI'S EXPENDITURE ITEMS

Personnel expenses


```
{ "from": "mango@q3mcco35auwcstmt.onion",
{ "to": "stern@q3mcco35auwcstmt.onion",
{ "body": "<mango> Pay the gang here bc1qkmyv5860pe24h9ytadkzgqltkjuuk9z9s027df
                \nsum total 85k
                \n99947 core team 62 people, I get 54 paychecks\n3847 - reverse team, 23 people
                \n8500 - new team of coders, 6 people, only 4 are getting salaries so far
                \n12500 Reverses, 6 people \n10000 OSINT department 4 people
                \n3000 for expenses (servers/protections/ test tasks for new people)
                \n164.8k total per month."
```


Tomorrow is the salary day:

main team - 97 447; 52 people

new team - 4000; 3 people, one has not yet started

reverse team - 23,347; 16 people

research team - 12,500; 6 people

team OSINT intelligence - 9,000; 4 people

total 146 294 \ 2 = 73 147 for salary + 700 bucks will go to commissions for transfers from wallets / withdrawals from exchanges and 3-4k are needed for expenses on routers / servers / gaskets

bc1q5aqs5hrlt3wj5xrnj0craykgsq6h8mse3cftf8

Throughout these conversations, we can see that its organization is that of a **structured company** with a real HR organization.

Today, there are **more than 80 people operating** 5 days a week in teams to deploy and maintain this platform.

1.Source : Breachquest 2. Source : ZdNet

CONTI MAIN TEAMS

CODERS

In charge of **writing malicious code** by integrating various new technologies.

CRYPTERS

In charge of **making syntactic changes** to payloads, binaries and scripts to **make them more difficult to detect**.

OFFENSIVE TEAM

In charge of obtaining **initial access** to the victims' network, battling against corporate security teams to **steal data**, and **plant ransomware**.

OSINT

In charge of **conducting research** on the **targeted company**.

REVERSE ENGINEERS

In charge of **disassembling** the victims' computer code to study it and **identify vulnerabilities**.

HUMAN RESSOURCES (HR)

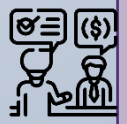
In charge of **recruitment** (online interview, profile search, etc.)

SYSADMINS

Responsible **for setting up the attack infrastructure** and provide assistance if needed.

TESTERS

Check various malware against known security solutions to **make sure that they avoid detection**

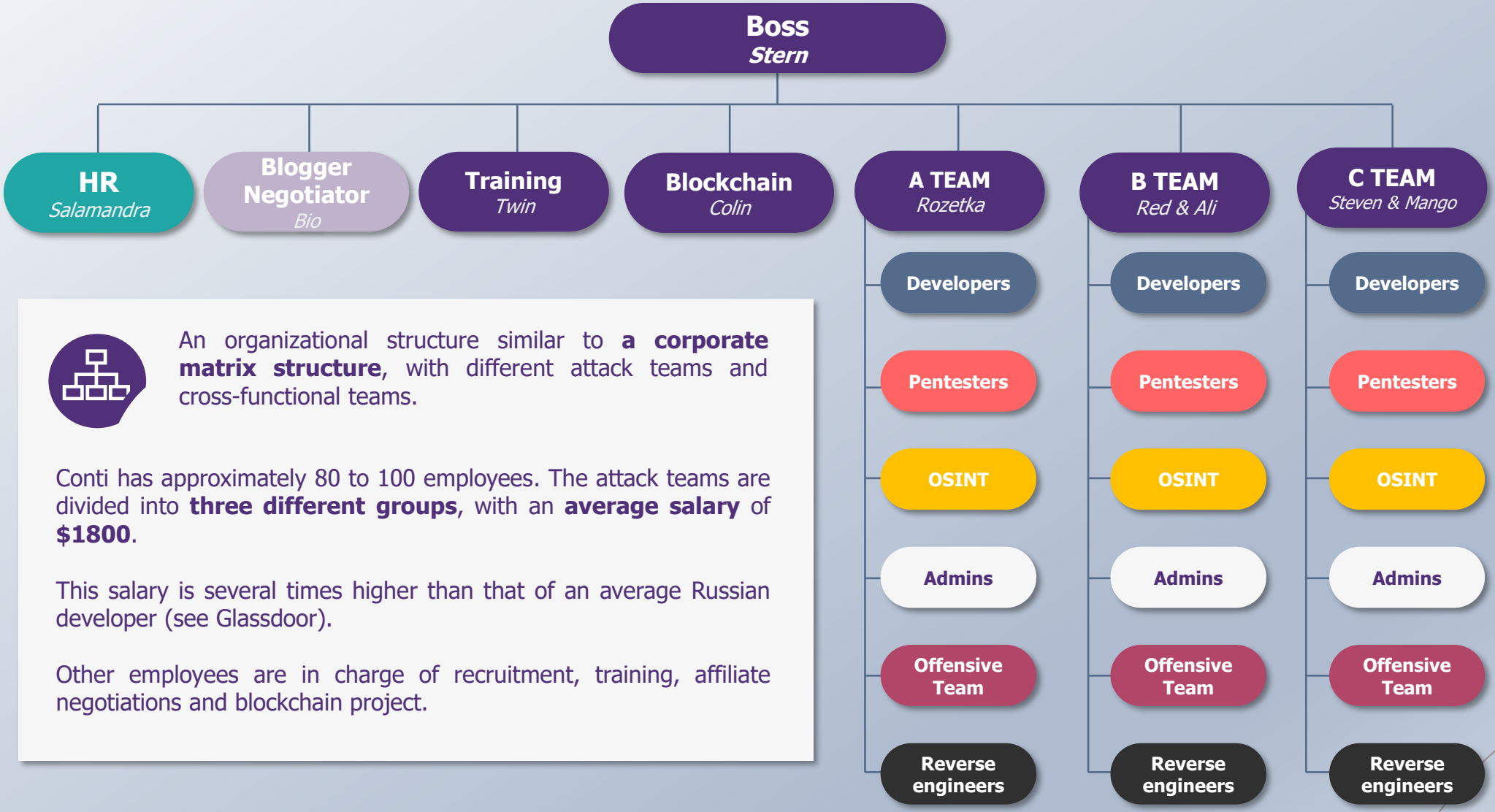


NEGOTIATION STAFF

In charge of **negotiating ransom** payments and securing a deal with victims.

Sources : Check Point Reaserch, Breachquest, KrebsOnSecurity

ORGANIZATIONAL STRUCTURE OF CONTI



An organizational structure similar to **a corporate matrix structure**, with different attack teams and cross-functional teams.

Conti has approximately 80 to 100 employees. The attack teams are divided into **three different groups**, with an **average salary** of **$1800**.

This salary is several times higher than that of an average Russian developer (see Glassdoor).

Other employees are in charge of recruitment, training, affiliate negotiations and blockchain project.

Sources : Check Point Research, Breachquest

FOCUS ON CONTI

HIRING PROCESS

Recruitment Sites

- **Recruitment sites**: Headhunter.ru, Superjobs.ru, etc.
- **Bypass the system** of these sites in order **to access the CV** and contact potential recruits directly **without leaving any trace**

salamandra

Innovative firm "Sniip-Atom" 2006 – 2008
NRC "Kurchatov Institute" 2008 – 2015
NRC "Kurchatov Institute" 2015 - to this day
[redacted]
work experience
Software Engineer
Embedded software development in C language
Development of embedded software for information processing modules for the in-reactor control system
VVER-440 reactors
First category programmer
Embedded software development in C language
Development of measuring channels and embedded software for the in-reactor control system of reactors
VVER-1000
Development of the measuring channel and software for the neutron flux control system
Development of embedded software for fuel refueling control system

Darknet forums

4. Contacted Hors about admins - he clarified the task, He says we need pentesters rather than admins. And at 6 in the morning, a great idea came to my beautiful and drunk head where to get them :) Do you remember the Revil were promoting on damage - they deposited a million dollars in bitcoins on a deposit and then the topic began to burst - they wrote there that they were inviting teams of hackers / pentesters to work with them . They wrote 5 pages of the topic with suggestions! They write something like that. "Team 3 people experience, etc" and there are a lot of them, 5 or more even pages! That's where we'll take them! I will spam PMs with a job offer for them all + many left contacts there themselves (although everyone has tox). By the 10th it will be done. The only question is how to pay them. How much do we pay? 2k - like to everyone?

Word of mouth

- **« Refer-a-friend bonuses”** allowing to receive bonuses in compensation for bringing in highly skilled profiles

stern

programmers bring each other, who starts looking for a job, I pay them bonuses if they bring another

stern

well, like 2 salaries, if the second proger works for more than a month. Therefore, they bring them themselves, no idea where they find)

Source : Check Point Reaserch

ESTIMATED CASH FLOW STATEMENT OF CONTI*

OVERDRAFT FACILITIES	M$ IN 2021	HYPOTHESIS
Affiliate ransom	180	*See attached sources*
Income allocated to affiliates	135	75%, *See attached sources*
Turnover	**45**	
Offices	0.14	*See attached sources*
Capital assets	**0.14**	
Infrastructure (servers, routers, EDR, etc.)	0.04	Between $3-4k, *See attached sources*
Tooling & SaaS subscriptions (software, etc.)	2	Approximately $2M would be spent out of the $6M expenses, *See attached sources*
Professional services (Initial access broker (IAB), etc.)	2	$4600 average network access price, *See attached sources*
Money laundering	23	50%, *See attached sources*
Expenditures	**27**	
Salaries	2	Average salary : $1.8k, *See attached sources*
Commissions	Variable amount	from 0.5% to 1% commission paid to negotiation and OSINT team, *See attached sources*
Personnel expenses	**2**	

Salaries ~$2M

(of the estimated $6M invested in expenses excluding commissions and bonuses)

- Between **80 to 100 "employees"** operate on behalf of the platform internally
- The **average salary** is estimated at **$1800**
- **Commissions or bonuses** calculated as a percentage of the paid ransom an also be granted to the members of the different teams. Between **0.5 to 1%** for the negotiation staff

*All the sources to build this table are listed in this excel.

ESTIMATED CASH FLOW STATEMENT OF CONTI*

OVERDRAFT FACILITIES	M$ IN 2021	HYPOTHESIS
Affiliate ransom	**180**	*See attached sources*
Subsidies	-	No information
Income allocated to affiliates	135	75%, *See attached sources*
Turnover	**45**	
Offices	0.14	*See attached sources*
Capital assets	**0.14**	
Infrastructure (servers, routers, EDR, etc.)	0.04	Between $3-4k, *See attached sources*
Tooling & SaaS subscriptions (software, etc.)	2	Approximately $2M would be spent out of the $6M expenses, *See attached sources*
Professional services (Initial access broker (IAB), etc.)	2	$4600 average network access price, *See attached sources*
Money laundering	**23**	50%, *See attached sources*
Expenditures	**27**	
Corporate tax	-	No information
Salaries	2	Average salary : $1.8k, *See attached sources*
Commissions	Variable amount	from 0.5% to 1% commission paid to negotiation and OSINT team, *See attached sources*
Payroll social charges	-	No information
Personnel expenses	**2**	
Total cash spent	**29**	
Net cash from operations in 2021	**16**	

*All the sources to build this table are listed in this excel.

The overall research on Conti's costs and expenses reveals that, out of a turnover of $45M, Conti generated a **net profit of approximately $16M**, becoming by far the most profitable group.

However, **70 to 80% of the ransom revenue** is still transferred to affiliates.

The **main cost items** are related to **money laundering** and **third-party services**.

Finally, the usual high cost items **(office space, salaries)** are **not very costly** compared to the benefits obtained.

ESTIMATED CASH FLOW STATEMENT OF CONTI*

OVERDRAFT FACILITIES	M$ IN 2021	HYPOTHESIS
Affiliate ransom	**180**	*See attached sources*
Subsidies	-	No information
Income allocated to affiliates	135	75%, *See attached sources*
Turnover	**45**	
Offices	0.14	*See attached sources*
Capital assets	**0.14**	
Infrastructure (servers, routers, EDR, etc.)	0.04	Between $3-4k, *See attached sources*
Tooling & SaaS subscriptions (software, etc.)	2	Approximately $2M would be spent out of the $6M expenses, *See attached sources*
Professional services (Initial access broker (IAB), etc.)	2	$4600 average network access price, *See attached sources*
Money laundering	**23**	50%, *See attached sources*
Expenditures	**27**	
Corporate tax	-	No information
Salaries	2	Average salary : $1.8k, *See attached sources*
Commissions	Variable amount	from 0.5% to 1% commission paid to negotiation and OSINT team, *See attached sources*
Payroll social charges	-	No information
Personnel expenses	**2**	
Total cash spent	**29**	
Net cash from operations in 2021	**16**	

*All the sources to build this table are listed in this excel.

CONCLUSION

TODAY OUR CLIENTS ARE BEING CHALLENGED BY CYBERCRIMINAL GROUPS :

More Structured

These ransomware groups are structured as companies. They are setting up recruitment strategies, optimizing their costs, their benefits and their ability to identify vulnerabilities more efficiently.

Increasingly active

Numerous strains of ransomware are developed each year by ransomware platforms, providing hackers an increasingly diverse malware offering.

More profitable

The amounts paid by the victims continue to rise, as well as the number of attacks carried out.

More disruptive

Over the last few years, cybercrime actors have been targeting critical sectors that are capable of paralyzing all or part of an organization or a state: Health care sector, construction, retail, etc.

The Positive Way

WAVESTONE

Laurenne-Sya LUCE
Analyst

M +33 (0)6 52 90 50 49
Laurennesya.Luce@wavestone.com

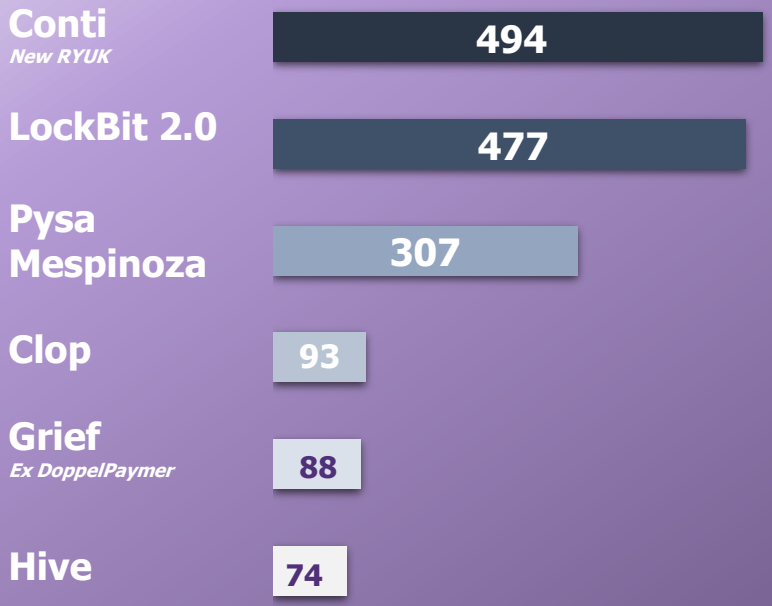
Tristan PUECH
Senior Consultant

M +33 (0)7 63 99 16 80
Tristan.Puech@wavestone.com

wavestone.com
@wavestone_

ESTIMATED NUMBER OF ATTACKS RELYING ON RANSOMWARE PLATFORMS IN 2020 AND 2021

Ransomware attack statistics 2021[1]



Ransomware attack statistics 2020[2]

The collected data from Varonis and Cyberdays 2021 sources highlights that ransomware platforms were used in **hundreds of attacks per year**. As a result, in 2020, Ryuk was responsible for **over 600 attacks**.

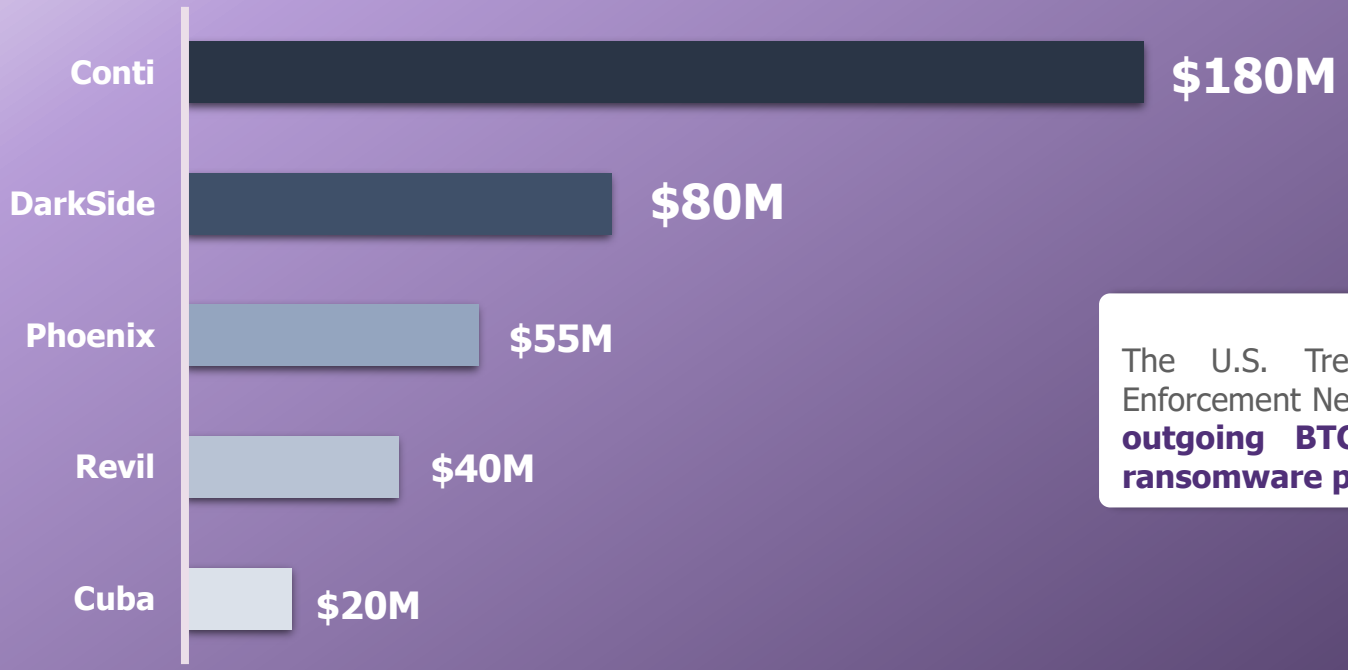
However, the use of disparate sources and the difficulty to collect reliable data make it impossible to estimate the direct evolution of the same ransomware groups year after year.

1. Source : Varonis 2. Source : Cyberdays 2021

TOP 5 MOST PROFITABLE RANSOMWARE OPERATORS IN 2021

Top 5 ransomware operators by revenue*

Million dollar, 2021



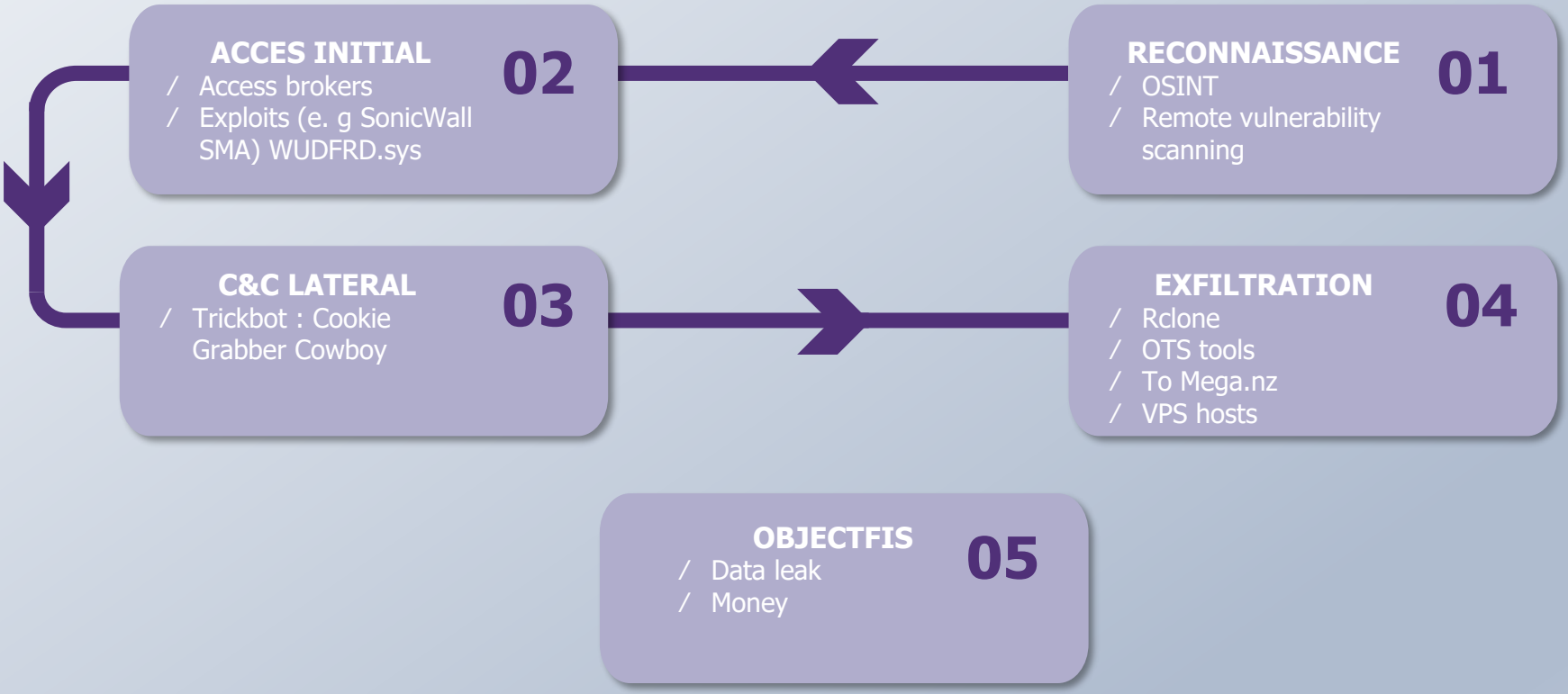
The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) identified **$5.2 billion in outgoing BTC transactions potentially tied to ransomware payments.**

Les groupes de ransomware dégagent leurs principaux **revenus de rançons payées en Bitcoins**. Ces revenus sont donc estimés grâce aux adresses bitcoin (publiques) pointant vers les comptes des différents groupes.

1.Source : Chainalysis 2. source : Financial Crime Enforcement Network 3.Source : Bleeping Computer

FOCUS ON CONTI

TECHNIQUES USED*



Source : Varonis

REFERENCES

Article	Source
[1]	Flashpoint Team., (2021). *DarkSide Ransomware Links to REvil Group Difficult to Dismiss.* Flashpoint blog DarkSide Ransomware Links to REvil Group Difficult to Dismiss
[2]	Dalman-Heather Smith, J., (2021) *Ransomware Actors Evolved Their Operations in 2020*. Crowdstrike blog Ransomware Actors Evolved Their Operations in 2020 | crowdstrike.com
[3]	Cimpanu, C., (2021). *Ce graphique montre les liens entre les groupes de cybercriminalité*, ZDNET Ce graphique montre les liens entre les groupes de cybercriminalité - ZDNet
[4]	*Cyber-Weather, Monthly news roundup*. (2021) Cyber Threat Intelligence Insight. Sogeti Présentation PowerPoint (sogeti.com)
[5]	Olson, R., (2022). *2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner*. Palo Alto Networks, p.20 2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner (paloaltonetworks.com) 2022-unit42-ransomware-threat-report-final.pdf (paloaltonetworks.com)
[6]	Pagani, P., (2021). *Conti ransomware affiliate leaked gang's training material and tools.* Cyber Defense Magazine Conti ransomware affiliate leaked gang's training material and tools - Cyber Defense Magazine
[7]	Dr. Robinson, T., (2021). *DarkSide Ransomware has Netted Over $90 million in Bitcoin*. Elliptic DarkSide Ransomware has Netted Over $90 million in Bitcoin (elliptic.co)
[8]	Security Advisories., (2022). *Conti Ransomware Gang Claims 50+ New Victims including Oil Terminal Operator Sea-Invest Disrupting Operations at 24 Seaports Across Europe and Africa*. Esentire Conti Ransomware Gang Claims 50+ New Victims including Oil Terminal Operator Sea-Invest Disrupting Operations at 24 Seaports Across Europe and Africa
[9]	Grauer, K. Kueshner, W., Updegrave, H., (2022). The 2022 Crypto Crime Report. Chain Analysis, p. 39 Crypto-Crime-Report-2022.pdf (chainalysis.com)
[10]	Akamo, A., (2022). *Crypto ransomware payments hit at least $602 million in 2021* – Chainalysis. Nairametrics Crypto ransomware payments hit at least $602 million in 2021 – Chainalysis - Nairametrics
[11]	*Wizard Spider*. Crowdstrike Adversary: Wizard Spider - Threat Actor | Crowdstrike Adversary Universe

REFERENCES

Article	Source
[12]	Beky, A., (2022). *Ransomwares : les 3 secteurs les plus ciblés*. Silicon Ransomwares : les 3 secteurs les plus ciblés
[13]	Osborne, C., (2022). *This is how much the average Conti hacking group member earns a month*. ZDNet This is how much the average Conti hacking group member earns a month
[14]	Waterman, S., (2022). *Inside the Conti leaks rattling the cybercrime underground*. Medium Inside the Conti leaks rattling the cybercrime underground
[15]	Miget, V., (2022). *Conti : Le groupe de rançongiciels a payé cher son soutien à Vladimir Poutine*. Linformaticien Conti : Le groupe de rançongiciels a payé cher son soutien à Vladimir Poutine
[16]	Krebs, B., (2022). *Conti Ransomware Group Diaries, Part III: Weaponry*. KrebsOnSecurity Conti Ransomware Group Diaries, Part III: Weaponry
[17]	Counter threat unit research team, (2022). *GOLD ULRICK Continues Conti Operations Despite Public Disclosures*. Secureworks GOLD ULRICK Continues Conti Operations Despite Public Disclosures
[18]	Thierry, G., (2022). *Après s'être positionné en soutien de la Russie, le gang de rançongiciel Conti victime d'une sévère fuite*. L'Usine Digitale Après s'être positionné en soutien de la Russie, le gang de rançongiciel Conti victime d'une sévère fuite (usine-digitale.fr)
[19]	Figueroa, M., Bing, N., Silvestrini, B., (2022). *The Conti Leaks | Insight into a Ransomware Unicorn*. BreachQuest The Conti Leaks - Insight into a Ransomware Unicorn | BreachQuest
[20]	CISA, FBI, NSA, (2022). *Conti Ransomware*. Joint Cybersecurity Advisory CSA_CONTI_RANSOMWARE_20210922.PDF (defense.gov)
[21]	Heller, M., (2021). *A Conti ransomware attack day-by-day*. Sophos A Conti ransomware attack day-by-day – Sophos News Ransomware Conti : une attaque détaillée jour après jour – Sophos News
[22]	CPR Team., (2022). *Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up… Sort Of*. Check Point Research Leaks of Conti Ransomware Group Paint Picture of a Surprisingly Normal Tech Start-Up... Sort Of - Check Point Research

REFERENCES

Article	Source
[23]	Krebs, B., (2022). *Conti Ransomware Group Diaries, Part II: The Office*. KrebsOnSecurity Conti Ransomware Group Diaries, Part II: The Office – Krebs on Security
[24]	The Parmak., (2022). *Translated conversations of Conti*. Github GitHub - TheParmak/conti-leaks-englished: Google and deepl translated conti leaks, which is shared by a member of the conti ransomware group.
[25]	(2022). *Analysis of leaked Conti's internal data*. KELA KELA-Intelligence-Report-ContiLeaks-1.pdf (ke-la.com)
[26]	(2022). *From Initial Access to Ransomware Attack – 5 Real Cases Showing the Path from Start to End.* KELA From Initial Access to Ransomware Attack - 5 Real Cases Showing the Path from Start to End - Kela (ke-la.com)
[27]	Fourdriinier, R., Vinckenbosch, T., Rahmati-Georges, T., (2022). *Situation actuelle en matière de cybercriminalité.* Webinaire VARONIS Varonis Engagement de Adrien Rahmati-Georges (highspot.com)
[28]	Chabre, F., (2021). *Cyberdays 2021 CACF-CALF : Ransomware : meilleure arme du cybercrime ?* Cyberdays 2021
[29]	*Ransomware trends in bank secrecy act data between January 2021 and June 2021*. Financial Crimes Enforcement Network (FinCEN) Financial Trend Analysis (fincen.gov)
[30]	Gatlan, B., (2021). *US links $5.2 billion worth of Bitcoin transactions to ransomware*. Bleeping Computer US links $5.2 billion worth of Bitcoin transactions to ransomware (bleepingcomputer.com)