WAVESTONE

Fiche de synthèse

L'économie de la cybercriminalité :
Synthèse des plateformes de ransomware

Laurenne-Sya LUCE

06/05/22 | Laurenne-Sya LUCE

The Positive Way

WAVESTONE

EXECUTIVE SUMMARY

La récente attaque de l'Ukraine par la Russie et les tensions qui en découlent ont favorisé les révélations sur plusieurs groupes d'attaquants Russes.

À la lumière de ces nouvelles informations, il nous a été possible de mieux **caractériser l'organisation** et **le modèle économique** de ces groupes.

Fonctionnant comme de véritables entreprises, les plateformes de ransomware sont directement ou indirectement responsables de **milliers d'attaques** par an.

Les bénéfices liés aux rançons de ces attaques permettent notamment à ces groupes de s'organiser en véritables **entreprises** engagées dans des **logiques salariales** et dégageant des profits ce chiffrant en **dizaines de milliers de dollars** par an.

Les plateformes ransomware

Focus sur le groupe CONTI

Les plateformes ransomware

Introduction à l'écosystème des plateformes de ransomware
Page 5

Relations entre les différents acteurs du cybercrime
Page 6

Le modèle économique des groupes de RaaS
Page 7

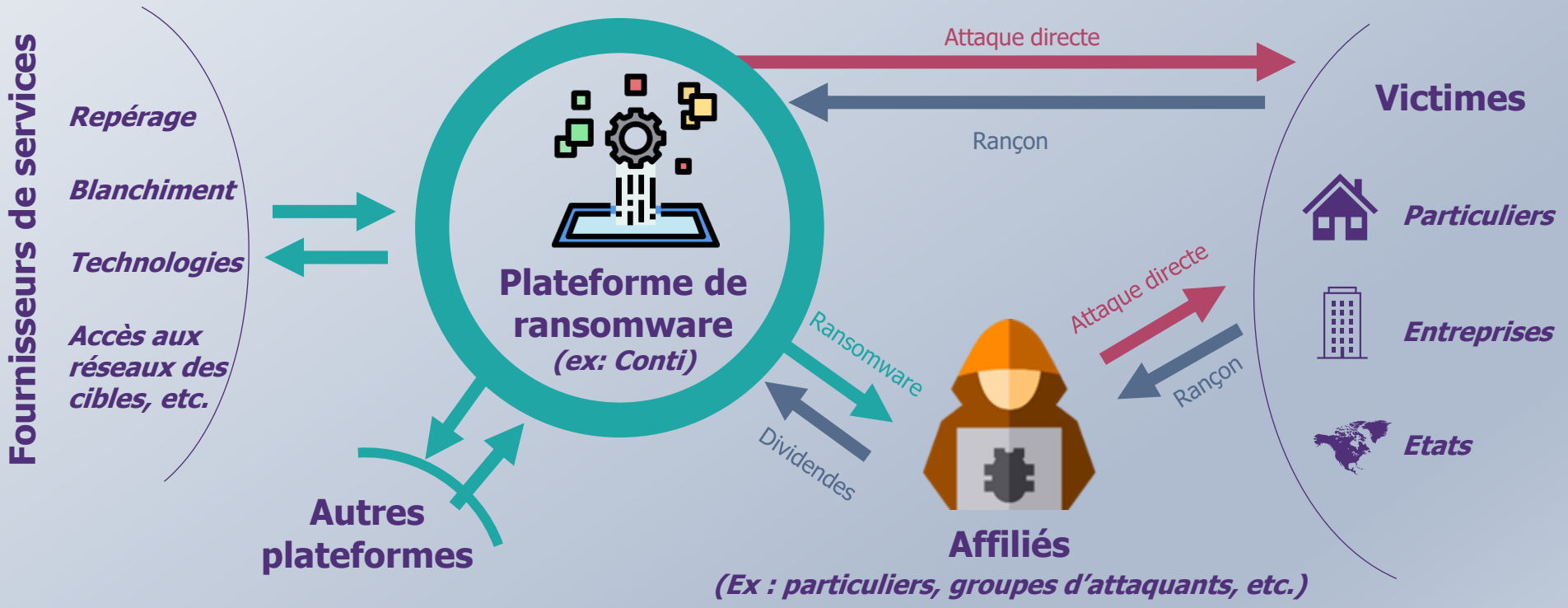
INTRODUCTION À L'ECOSYSTEME DES PLATEFORMES DE RANSOMWARE

Glossaire

Plateforme de ransomware : Chargée du **développement et de la maintenance de l'infrastructure du logiciel malveillant et de son chiffrement.** L'opérateur prélève un certain pourcentage à titre de commission en échange de l'accès à ce dernier

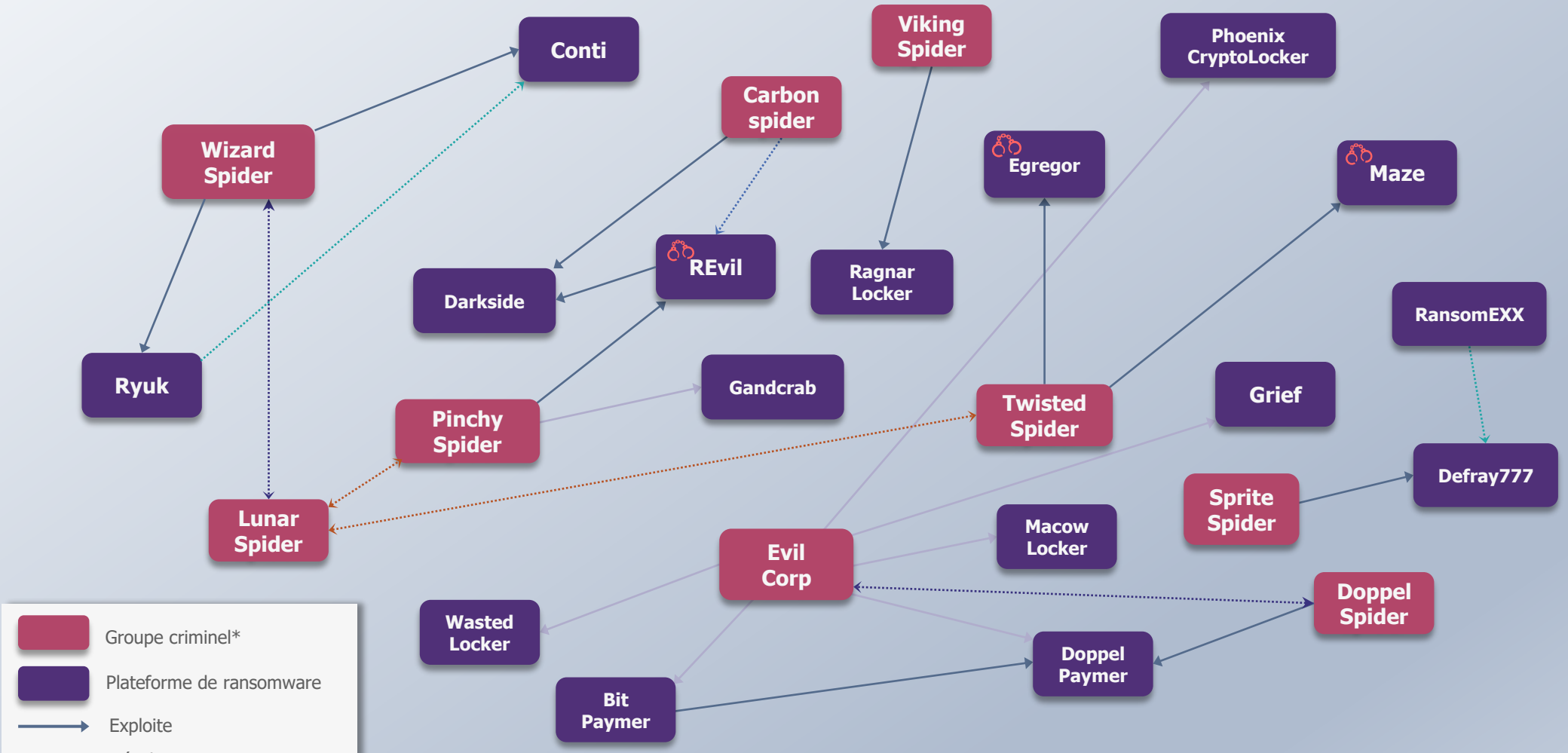
Affilié : Chargé de la **diffusion du ransomware** afin de **créer une chaîne de paiement de rançon** qui sera partagée entre le développeur et eux-mêmes

Aperçu des liens entres affiliés et plateformes de ransomware



Attaque
Paiements
Transferts technologiques / Autres

RELATIONS ENTRE LES DIFFERENTS ACTEURS DU CYBERCRIME



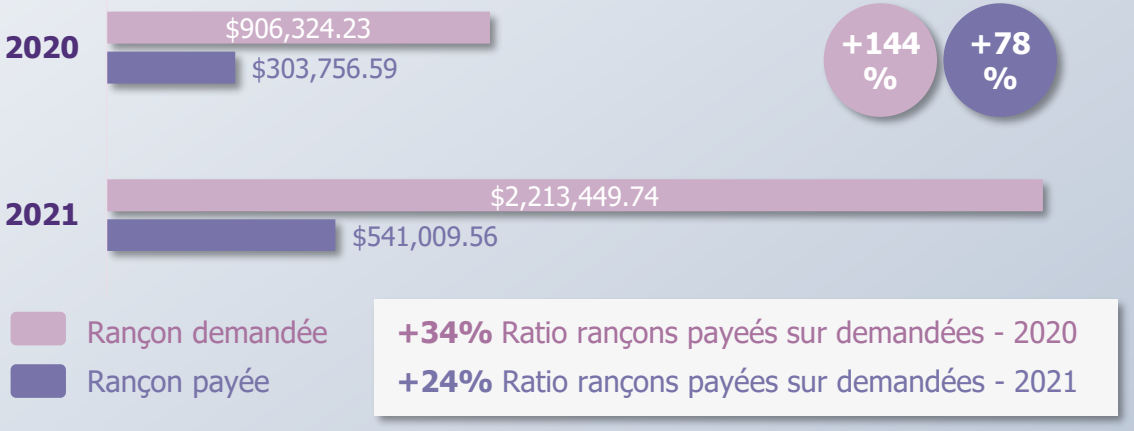
Les groupes d'attaquants s'appuient bien souvent sur **diverses plateformes** de ransomware. Ces liens s'expliquent notamment pour des raisons historiques, avec des hackeurs ayant bien souvent travaillé pour la plateforme de ransomware et pour les attaquants.

*Groupes d'attaquants ayant des activités diverses (ransomware, malware, etc.) | sources disponibles en annexe

LE MODÈLE ÉCONOMIQUE DES GROUPES DE RAAS – QUELLES RANÇONS POUR LES ATTAQUANTS…?

Montants moyens des demandes de rançons comparés à leur paiement effectif*

En dollars, sur les années 2020/2021, selon les données de Unit42



Les **tactiques agressives** des groupes d'attaquants, ainsi que la **criticité des données ciblées,** contraignent les victimes à **payer des rançons toujours plus importantes : +78%** d'augmentation du montant moyen d'une rançon en un an.

Toutefois, le **ratio des montants payés par rapports à ceux demandés est en diminution** sur l'année 2021.

….ET QUELS GAINS POUR LES PLATEFORMES?

Modèle Darkside

25% pour les rançons inférieures à 500k
10% pour les rançons supérieures à 5 millions de dollars.

Modèle Lockbit

20-30% du montant de la rançon versé par les affiliés

Les affiliés reversent généralement **un pourcentage des gains** de leur rançons aux plateformes qu'ils ont utilisés.
Ces **pourcentages peuvent varier**, par exemple selon les montants de rançons perçus.

*Source : Unit 42 - Palo Alto Networks

Focus sur le groupe CONTI

Conti Leaks - *Page 9*

Fiche identité du groupe Conti - *Page 10*

Conti : plateforme de ransomware la plus rentable en 2021- *Page 12*

Les différents postes de dépenses du groupe Conti - *Page 15*

Tableau de trésorerie estimé - *Page 24*

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

Greetings,

their

running tar -xzvf 1.tgz command in your terminal . The contents of the first
dump contain the
the past) of the

There are more du
You can help the

It is not malware
This is being sen

Thank you for your support

Glory

"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]

27 février 2022

Un chercheur ukrainien, mécontent de cette prise de position, **divulgue 13 mois** d'échanges et de **données sensibles** sur le fonctionnement du gang

27 février 2022

… avant de se rétracter et nuancer leur propos à quelques jours plus tard

25 février 2022

Des **membres pro-russe** du groupe Conti **annoncent publiquement leur soutien** aux autorités russes dans le conflit en Ukraine…

24 février 2022

Lancement de l'invasion militaire russe en Ukraine

2022

FOCUS SUR LE GROUPE CONTI

FICHE IDENTITÉ DU GROUPE CONTI

Le groupe cybercriminel **Conti** compte à son actif **plus de 1000 victimes**.
Il est particulièrement mis en lumière suite aux **fuites de données révélant d'importantes informations sur le fonctionnement du groupe**.

Nombre d'employés
Entre **80** et **100**

Plateforme de RaaS

Début d'activité | 2020

Associés aux groupes d'attaquants
Wizard Spider, Ryuk, etc.

Bénéfices
Environ **180M$** perçus en 2021

Nombre d'attaques
494 (2021)

Mode d'attaque favorite
Ransomware

Responsable de : Attaque d'ExaGrid, Irish Health Service Ex, etc.

Le groupe Conti est responsable d'attaques importantes, ayant déstabilisé **des pays ou des groupes d'envergures nationales** au cours des deux dernières années : **Assu2000, Inserm Transfert, ExaGrid, Solware, Irish Health Service Executive, etc.**

TABLEAU DE TRÉSORERIE ESTIMÉ DU GROUPE CONTI

Les récentes informations qui ont été divulguées sur le groupe Conti ont permis de mieux **comprendre son organisation**.

Dans une démarche de compréhension du modèle économique des plateformes de ransomware, l'**objectif** suivant va être d'établir une **estimation** : des gains, différents postes de coûts ainsi que les **bénéfices net perçus par Conti** en 2021.

CONSTRUISONS ENSEMBLE LE TABLE DE TRESORERIE DU GROUPE CONTI

LIGNES DE TRÉSORERIE	M$ EN 2021	HYPOTHÈSES
Rançons des affiliés		
Revenu alloués aux affiliés		
Chiffre d'affaires		
Locaux		
Immobilisations		
...		
...		
Gain totaux pour l'exercice 2021		

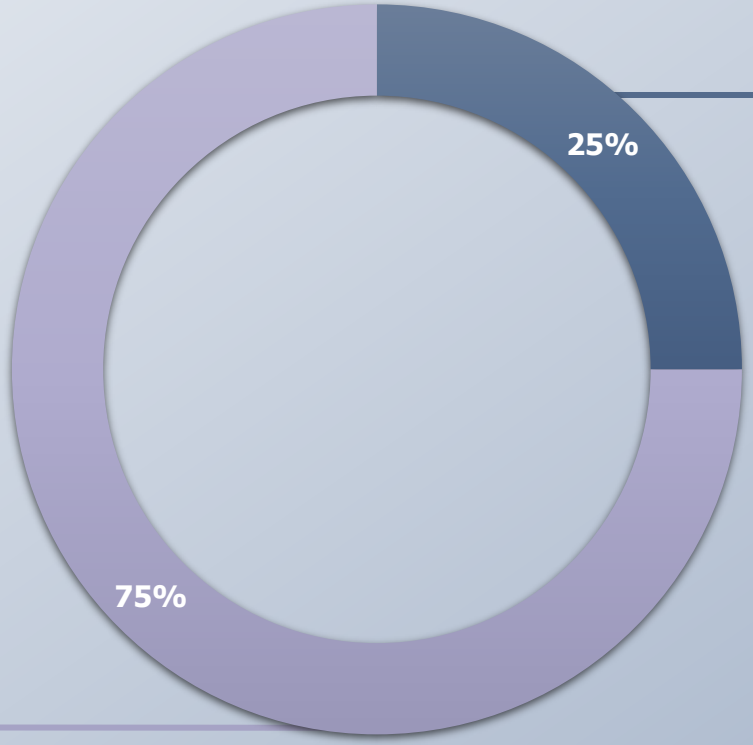
CONTI : PLATEFORME DE RANSOMWARE LA PLUS RENTABLE EN 2021

Chiffre d'affaires du groupe Conti

Avec plus de **494 attaques**, le groupe Conti a engrangé plus de **180 millions de dollars**, se plaçant en tête des groupes de ransomware les plus prolifiques en 2021.

Estimation de la part des revenus distribués entre les développeurs de la plateforme Conti et ses affiliés

en 2021



Développeurs Conti

$45 millions

Affiliés Conti

$135 millions

Programme d'affiliation

+300 membres et affiliés appartenant au groupe Conti mènent des attaques partout dans le monde.

Très **sélectif** quant aux personnes habilitées à distribuer le ransomware

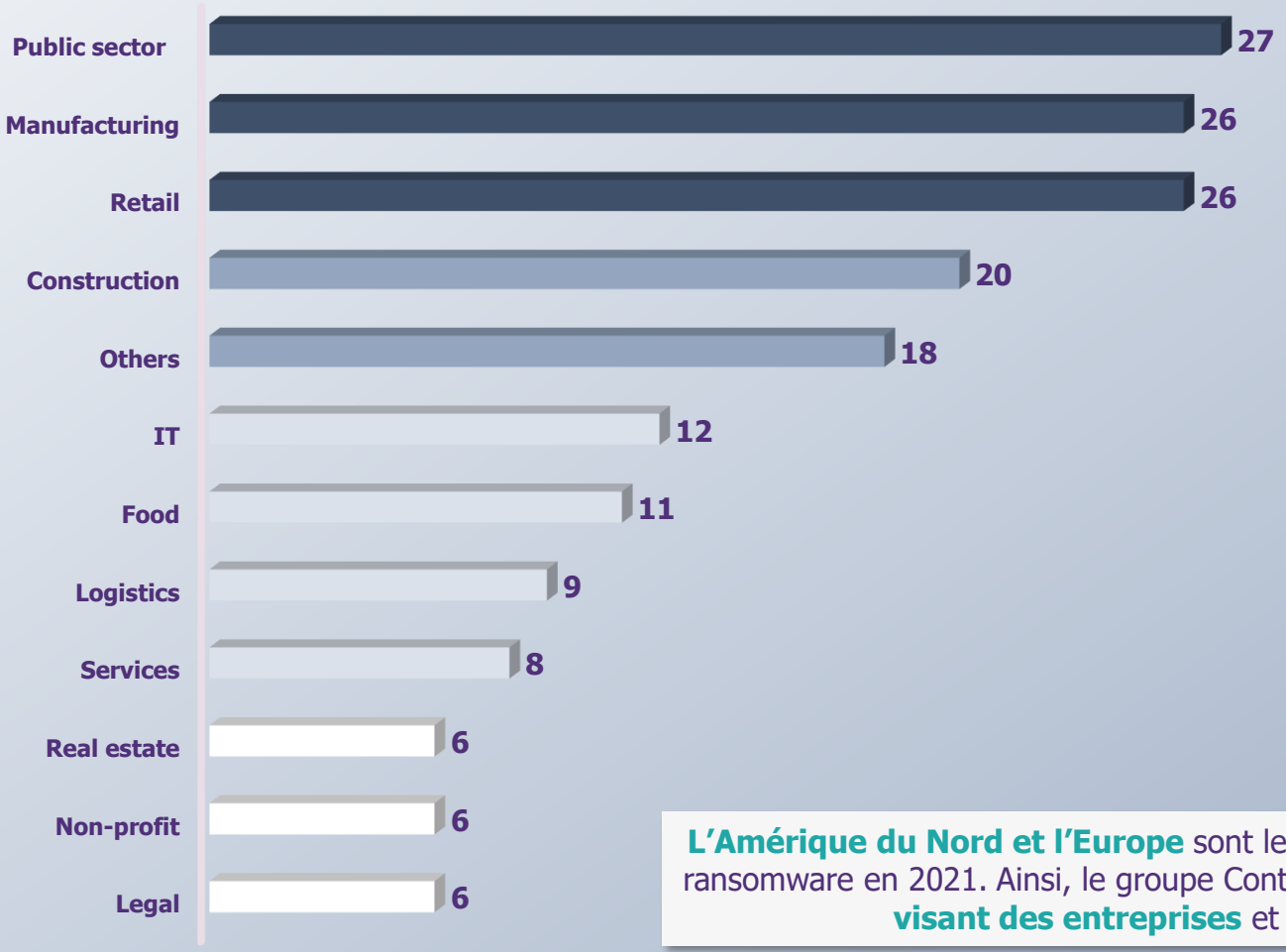
20-30% du montant des rançons est automatiquement **versé à la plateforme** par ses affiliés.

Sources : Varonis, Secure works, ZdNet, l'Usine Digitale, Breachquest

FOCUS SUR LES CIBLES DU GROUPE CONTI

Les secteurs cibles du groupe Conti[1]

En nombre d'attaques sur 2021 dans le monde (sur les victimes identifiées)



Bien qu'aucun secteur ne soit épargné par le groupe, Conti a principalement visé les entreprises du secteur de la **vente**, de la **production**, de la **construction** et du **secteur public.**
Ces attaques ciblées peuvent s'expliquer par la plus grande **vulnérabilité** de ces secteurs aux attaques, et/ou par la **forte visibilité** de ces attaques auprès du public.

L'Amérique du Nord et l'Europe sont les régions les plus ciblées par les attaques de ransomware en 2021. Ainsi, le groupe Conti a été à l'origine d'au moins **400 attaques**[2] **visant des entreprises** et **organisations américaines**

1. Source : CSA 2. Source : Sophos

TABLEAU DE TRÉSORERIE ESTIMÉ DU GROUPE CONTI*

LIGNES DE TRÉSORERIE	M$ EN 2021	HYPOTHÈSES
Rançons des affiliés	**180**	*Cf.* sources annexes
Revenu alloués aux affiliés	135	75%, *Cf.* sources annexes
Chiffre d'affaires	**45**	

Nous avons émis l'**hypothèse** selon laquelle le groupe Conti percevrait des **subventions** de diverses natures de la part du **gouvernement Russe**.

Toutefois, elle n'est **pour le moment pas avérée** par des sources qui le confirme.

Depuis le début de la guerre, plus de **200 adresses Bitcoins ont été identifiées pointant vers Conti**, pour une valeur d'environ 180M$ en 2021.

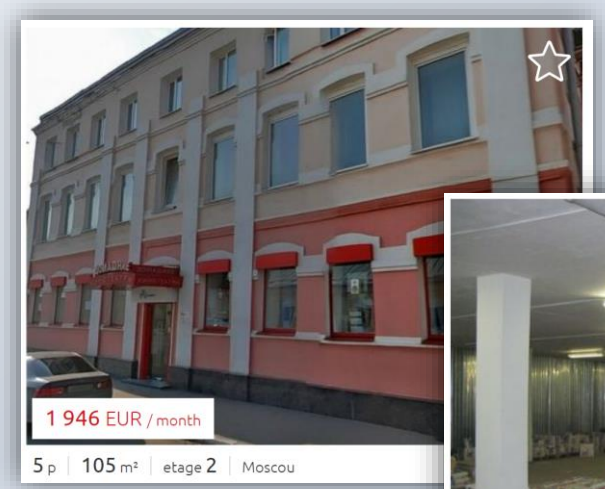
Les **20 à 30% des gains reversés par les affiliés** permettent à la plateforme de dégager un chiffre d'affaires d'environ **45 millions de dollars**.

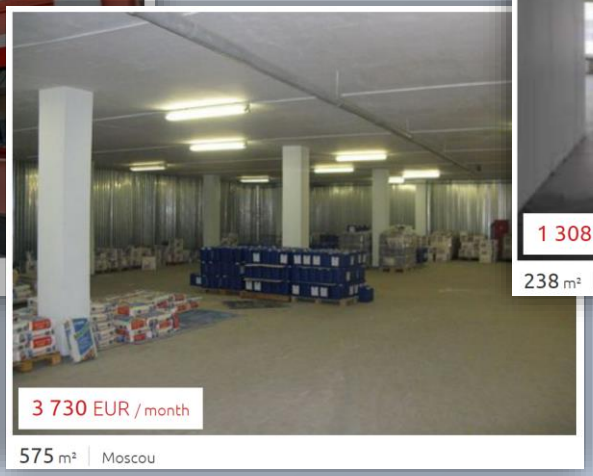
*L'ensemble des sources pour réaliser ce tableau sont listées dans cet excel.

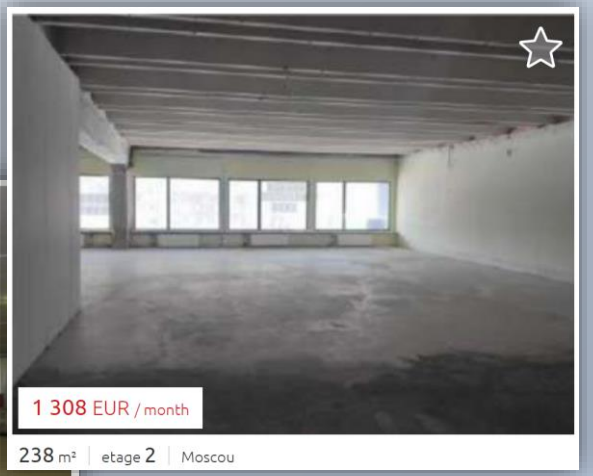
LES POSTES DE DÉPENSES DU GROUPE CONTI

Immobilisations

Le groupe loue entre **3 et 4 bureaux physiques** en Russie. Ces locaux entièrement **équipés**, sont mis à disposition des différentes équipes.







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

TABLEAU DE TRÉSORERIE ESTIMÉ DU GROUPE CONTI*

LIGNES DE TRÉSORERIE	M$ EN 2021	HYPOTHÈSES
Rançons des affiliés	180	*Cf.* sources annexes
Revenu alloués aux affiliés	135	75%, *Cf.* sources annexes
Chiffre d'affaires	**45**	
Locaux	0.14	*Cf.* sources annexes
Immobilisations	**0.14**	

Contrairement à une entreprise classique, les **coûts d'immobilisations pèsent** finalement **très peu** sur le groupe.

*L'ensemble des sources pour réaliser ce tableau sont listées dans cet excel.

LES DIFFERENTS POSTES DE DÉPENSES DU GROUPE CONTI

Achats BAU

6M$

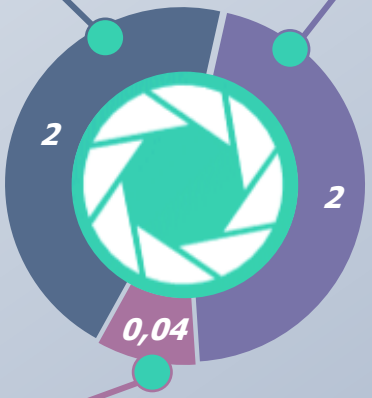
de dépenses en services externes, outils, salaires et primes mensuelles, en 2021*

(hors commissions et bonus)

Outils et Abonnement SaaS ~$2M

/ Ces dépenses comprennent principalement l'achat **d'antivirus, de VPN** ou encore de **logiciels de simulation.**

/ Conti a investi **$60 000** dans l'acquisition d'une licence valide de **Cobalt Strike**. La moitié de cet investissement a été versée à une société légale qui a secrètement acheté la licence au nom de Conti.



Infrastructure ~$0,04M

/ **$3-4k** par mois sont dépensés par le groupe dans le maintien des **serveurs et routeurs**

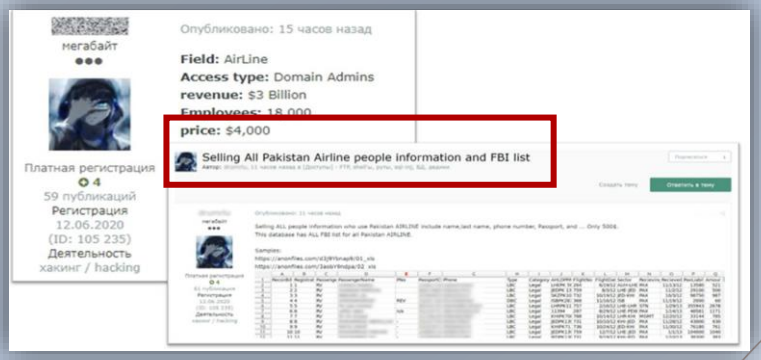
total 146 294 \ 2 = 73 147 for salary + 700 bucks will go to commissions for transfers from wallets / withdrawals from exchanges and 3-4k are needed for expenses on routers / servers / gaskets

Extrait d'une conversation

Services tiers ~$2M

/ Le groupe ferait appel à des **courtiers en accès initial aux réseaux** comme le fournisseur EXOTIC LILY.

/ Le **prix de vente moyen d'accès** au réseau d'une victime s'élève à environ **$4600** en 2021. Ces **prix peuvent varier** en fonction de nombreux paramètres comme la notoriété de l'entreprise ciblée.



Exemple de proposition de vente d'accès

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

TABLEAU DE TRÉSORERIE ESTIMÉ DU GROUPE CONTI*

LIGNES DE TRÉSORERIE	M$ EN 2021	HYPOTHÈSES
Rançons des affiliés	180	*Cf.* sources annexes
Subventions Etat	-	Pas d'information
Revenu alloués aux affiliés	135	75%, *Cf.* sources annexes
Chiffre d'affaires	**45**	
Locaux	0.14	*Cf.* sources annexes
Immobilisations	**0.14**	
Infrastructures (serveurs / meubles / BAU…)	0.04	Entre $3-4k, *cf.* sources annexes
Outils & abonnements SaaS (logiciels de tests, etc.)	2	Environ $2M serait dépensé en abonnements SaaS sur les $6M de frais, *cf.* sources annexes
Achats services tiers (services tiers de repérage des cibles, etc.)	2	$4600 en moyenne pour accéder au reseau d'une victime, *cf.* sources annexes
Coûts liés blanchiment	**23**	50%, *Cf.* sources annexes
Achats BAU	**27**	

Nos sources ne précisent pas les montants alloués par Conti au **blanchiment de l'argent** des rançons.

Ces montants sont généralement estimés à **50% des gains effectués** dans d'autres secteurs criminels.

Les **principaux postes de coûts** pesant sur le groupe sont liés au **blanchiment d'argent** et aux **services tiers** associés.

*L'ensemble des sources pour réaliser ce tableau sont listées dans cet excel.

LES POSTES DE DÉPENSES DU GROUPE CONTI

Charges de Personnel


```
{ "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

Au travers de ces échanges, nous pouvons voir que son organisation est celle d'une **entreprise structurée** avec une véritable organisation RH.

Aujourd'hui ce sont **plus de 80 personnes déployées en continue sous forme d'équipes,** qui œuvrent dans le déploiement et la maintenance de cette plateforme.

Sources : Breachquest, ZdNet

FOCUS SUR LES DIFFERENTS POSTES AU SEIN DE L'ORGANISATION CONTI

CODEURS

Equipe chargée d'**écrire les codes malveillants** en intégrant diverses nouvelles technologies.

CRYPTEURS

Equipe chargée de rendre les charges utiles, fichiers binaires et scripts plus **difficiles à détecter**.

EQUIPE D'INTRUSION

Equipe chargée d'obtenir **l'accès initial au réseau des victimes.**

OSINT

Equipe chargée de **collecter des informations en sources ouvertes** sur leurs cibles.

REVERSE ENGINEERS

Equipe chargée du **désassemblage du code** informatique des victimes pour **identifier les vulnérabilités**.

RESSOURCES HUMAINES

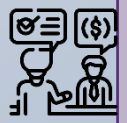
Equipe chargée du **recrutement** (entretien en ligne, recherche de profil, etc..) au sein de Conti.

SYSADMINS

Equipe chargée de **mettre en place l'infrastructure d'attaque** et fournir assistance si besoin.

TESTEURS

Equipe chargée de **tester le malware de Conti** contre les outils de sécurité.

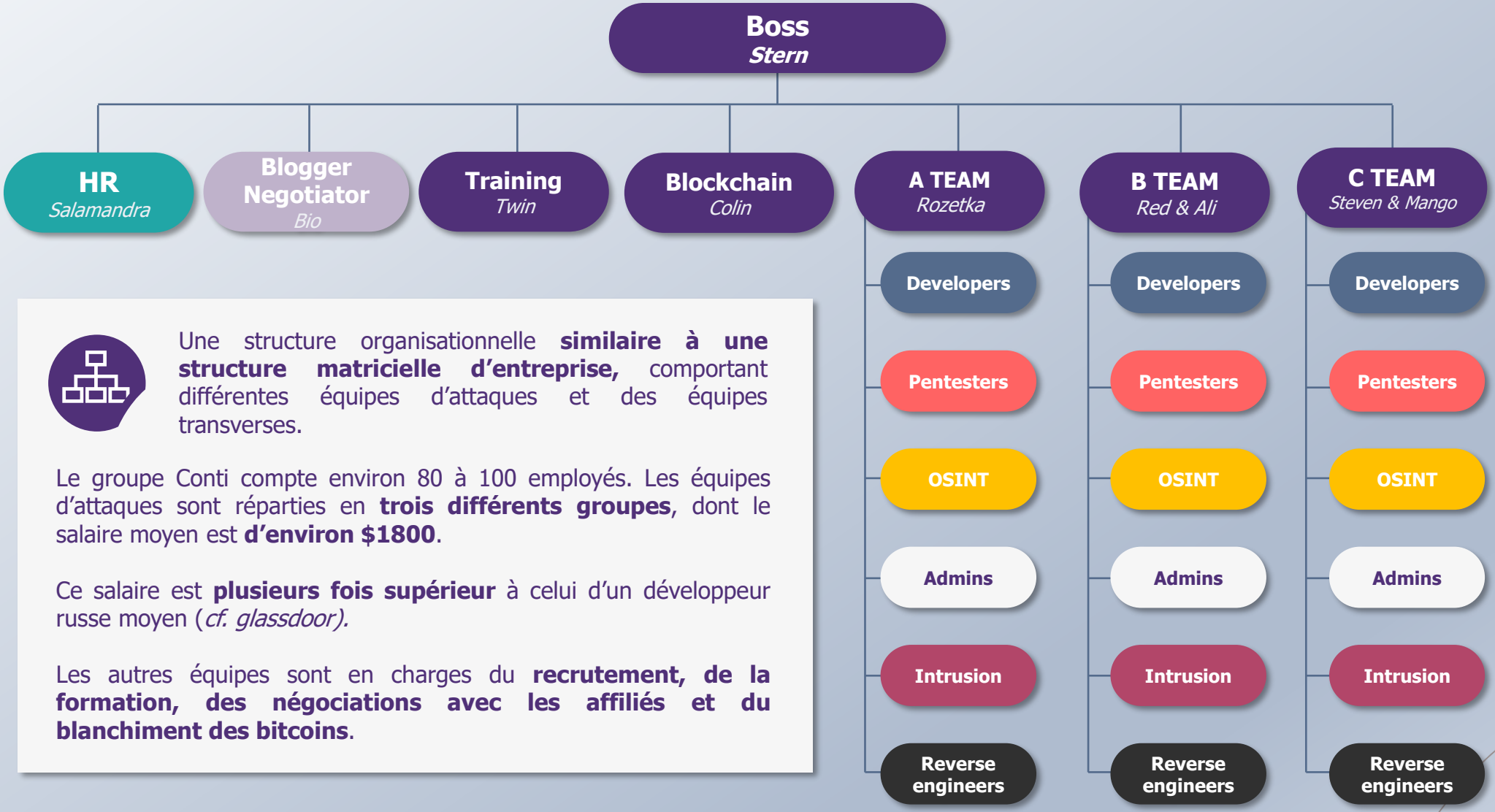


EQUIPE DE NEGOCIATION

Equipe chargée de **négocier** les montants des **rançons avec les victime**s.

Sources : Check Point Reaserch, Breachquest, KrebsOnSecurity

STRUCTURE HIERARCHIQUE DU GROUPE CONTI



Une structure organisationnelle **similaire à une structure matricielle d'entreprise,** comportant différentes équipes d'attaques et des équipes transverses.

Le groupe Conti compte environ 80 à 100 employés. Les équipes d'attaques sont réparties en **trois différents groupes**, dont le salaire moyen est **d'environ $1800**.

Ce salaire est **plusieurs fois supérieur** à celui d'un développeur russe moyen (*cf. glassdoor).*

Les autres équipes sont en charges du **recrutement, de la formation, des négociations avec les affiliés et du blanchiment des bitcoins**.

Sources : Check Point Research, Breachquest

CANAUX DE RECRUTEMENT

Site de recrutement

/ **Sites de recrutement** :
Headhunter.ru, Superjobs.ru, etc.

/ **Contournement du système** de ces sites afin **d'accéder au CV** et contacter les recrues potentielles directement **sans laisser de traces**

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

Forums clandestins du Dark web

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?

Bouche à oreille

/ **Système de "cooptation"** permettant d'obtenir des bonus en échange d'apport de profil hautement qualifiés

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

TABLEAU DE TRÉSORERIE ESTIMÉ DU GROUPE CONTI*

LIGNES DE TRÉSORERIE	M$ EN 2021	HYPOTHÈSES
Rançons des affiliés	180	*Cf.* sources annexes
Revenu alloués aux affiliés	135	75%, *Cf.* sources annexes
Chiffre d'affaires	**45**	
Locaux	0.14	*Cf.* sources annexes
Immobilisations	**0.14**	
Infrastructures (serveurs / meubles / BAU…)	0.04	Entre $3-4k, *cf.* sources annexes
Outils & abonnements SaaS (logiciels de tests, etc.)	2	Environ $2M serait dépensé en abonnements SaaS sur les $6M de frais, *cf.* sources annexes
Achats services tiers (services tiers de repérage des cibles, etc.)	2	$4600 en moyenne pour accéder au réseau d'une victime, *cf.* sources annexes
Coûts liés blanchiment	23	50%, *Cf.* sources annexes
Achats BAU	**27**	
Salaires	2	Salaire moyen : $1,8k, *cf.* sources annexes
Commissions	Montant varible	0,5 à 1% des rançons aux négociateurs
Charges de personnel	**2**	

Salaires ~$2M

(sur les $6M estimés investis en dépenses internes hors commissions et bonus)

/ Entre **80 et 100 "employés"** travaillent en interne pour le compte du groupe

/ Le **salaire moyen** des "employés" du groupe est estimé à **$1800**

/ Entre **0,5 à 1%** du montant de la rançon perçu est versée aux membres des **équipes de négociation**

*L'ensemble des sources pour réaliser ce tableau sont listées dans cet excel.

TABLEAU DE TRÉSORERIE ESTIMÉ DU GROUPE CONTI*

LIGNES DE TRÉSORERIE	M$ EN 2021	HYPOTHÈSES
Rançons des affiliés	**180**	*Cf.* sources annexes
Subventions Etat	-	Pas d'information
Revenu alloués aux affiliés	135	75%, *Cf.* sources annexes
Chiffre d'affaires	**45**	
Locaux	0.14	*Cf.* sources annexes
Immobilisations	**0.14**	
Infrastructures (serveurs / meubles / BAU…)	0.04	Entre $3-4k, *cf.* sources annexes
Outils & abonnements SaaS (logiciels de tests, etc.)	2	Environ $2M serait dépensé en abonnements SaaS sur les $6M de frais, *cf.* sources annexes
Achats services tiers (services tiers de repérage des cibles, etc.)	2	$4600 en moyenne pour accéder au réseau d'une victime, *cf.* sources annexes
Coûts liés blanchiment	**23**	50%, *Cf.* sources annexes
Achats BAU	**27**	
Impôts sur société	-	Pas d'information
Salaires	2	Salaire moyen : $1,8k, *cf.* sources annexes
Commissions	Montant variable	0,5 à 1% des rançons aux négociateurs
Charges sociales & salariales	-	Pas d'information
Charges de personnel	**2**	
Total des coûts	**29**	
Gain totaux pour l'exercice 2021	**16**	

*L'ensemble des sources pour réaliser ce tableau sont listées dans cet Excel.

L'ensemble des recherches sur les coûts et dépenses de Conti montrent que, sur un CA de 45M de $, Conti dégage un **bénéfice net** d'environ **16 millions de dollars**, faisant un groupe extrêmement rentable.

Cependant, **70 à 80% des revenus des rançons** sont tout de même reversés aux affiliés.

Les **principaux postes de coûts** sont liés au **blanchiment d'argent** et aux **services tiers** associés.

Enfin, les postes de coûts traditionnellement élevés **(locaux, salaires) sont ici peu dépensiers** au regard des gains engrangés.

CONCLUSION

AUJOURD'HUI NOS CLIENTS FONT FACE À DES GROUPES DE CYBERATTAQUANTS :

De plus en plus organisés

Les groupes se structurent sous la forme d'entreprises. Ils mettent en place des logiques de recrutement, d'optimisation de leurs coûts, de leurs bénéficies et de leur capacité à identifier les failles toujours plus efficaces.

De plus en plus actifs

De nombreuses souches de ransomware sont développées chaque année par les plateformes de ransomware, offrant aux groupes d'attaquants une offre de malware toujours plus variée.

De plus en plus rentables

Les montants payés par les victimes ne cessent d'augmenter, tout comme le nombre d'attaques perpétrées.

De plus en plus déstabilisants

Les attaques de ces dernières années visent des secteurs critiques et sont à même de paralyser tout ou une partie d'une organisation ou d'un Etat : secteur hospitalier, construction, retail, etc.

The Positive Way

WAVESTONE

Laurenne-Sya LUCE
Analyste

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

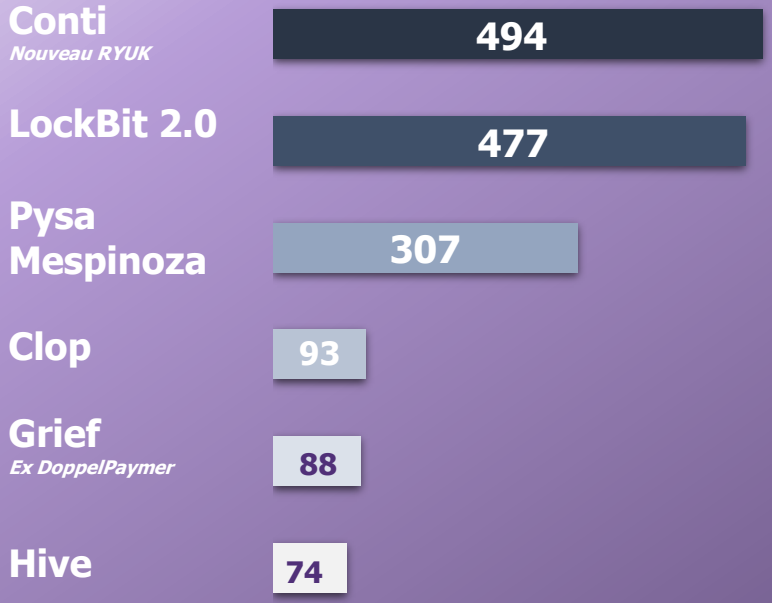
Tristan PUECH
Senior Consultant

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

wavestone.com
@wavestone_

ESTIMATION DU NOMBRE D'ATTAQUES S'APPUYANT SUR DES PLATEFORMES RANSOMWARE EN 2020 ET 2021

Nombre d'attaques en 2021[1]



Nombre d'attaques en 2020[2]

Les données collectées selon les sources Varonis et Cyberdays 2021 mettent en évidence que les plateformes de ransomware ont été utilisées dans le cadre de **plusieurs centaines d'attaques par année**. Ainsi en 2020, le groupe Ryuk était responsable **de plus de 600 attaques**.

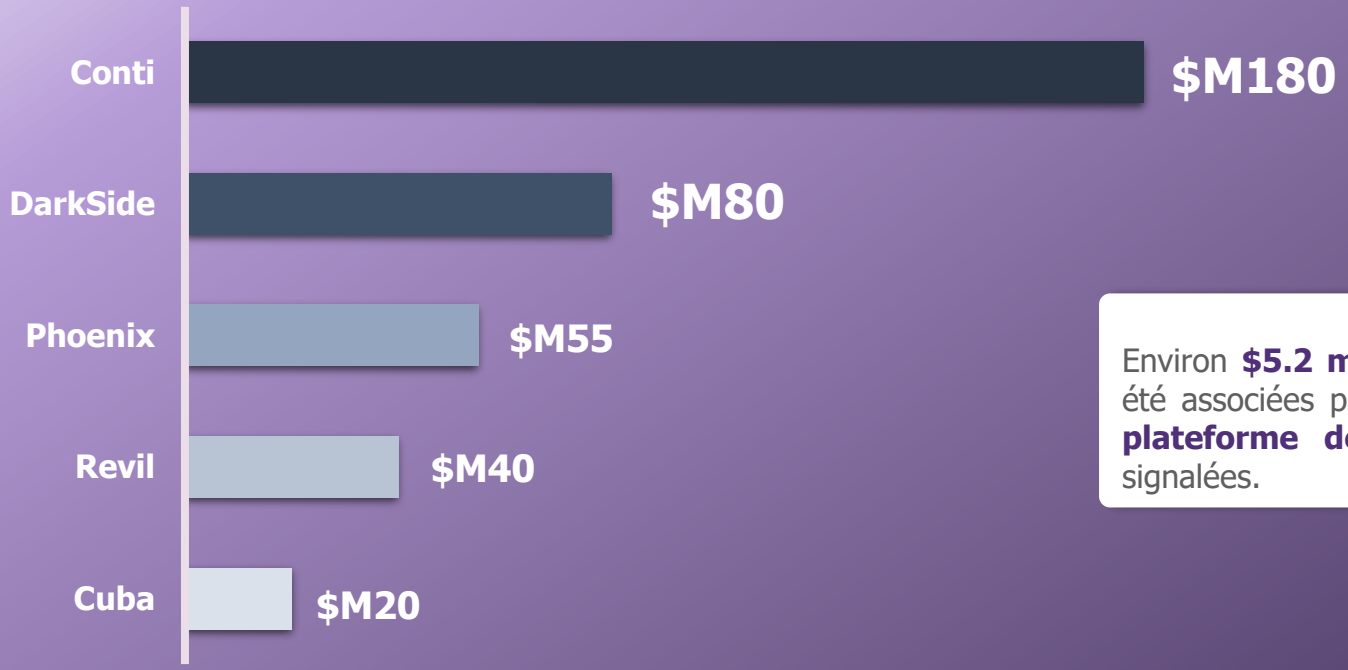
Néanmoins, l'utilisation de sources différentes et la difficulté à collecter des données fiables ne permettent pas d'estimer l'évolution directe des mêmes groupes de ransomware d'une année sur l'autre.

1. Source : Varonis 2. Source : Cyberdays 2021

APERÇU DU TOP 5 DES GROUPES DE RANSOMWARE LES PLUS RENTABLES EN 2021

Montant des revenus des groupes de ransomware*

En million de dollars, sur l'année 2021

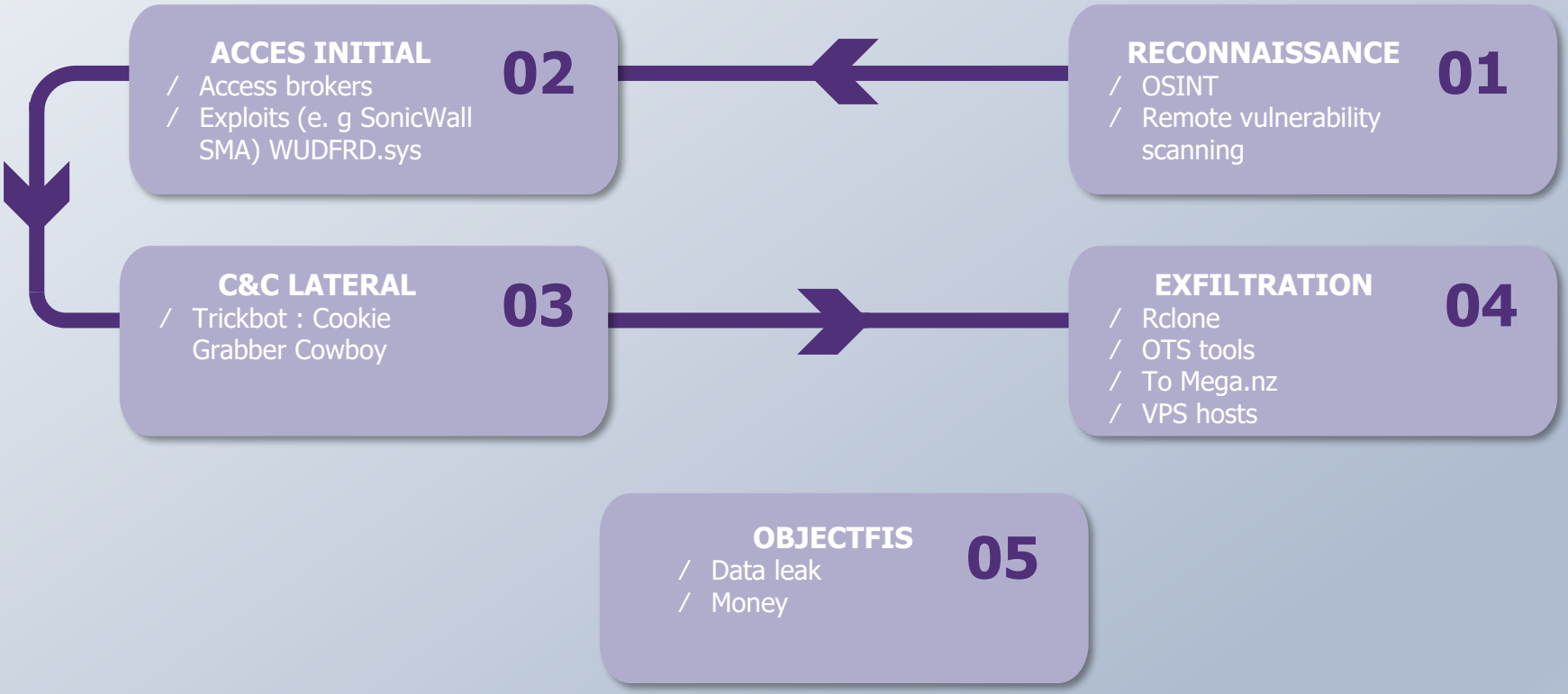


Environ **$5.2 milliards* de transactions en BTC** ont été associées par le Trésor Américain au **paiement de plateforme de ransomware** les plus couramment signalées.

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

SCHÉMA D'ATTAQUE DE CONTI*



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)