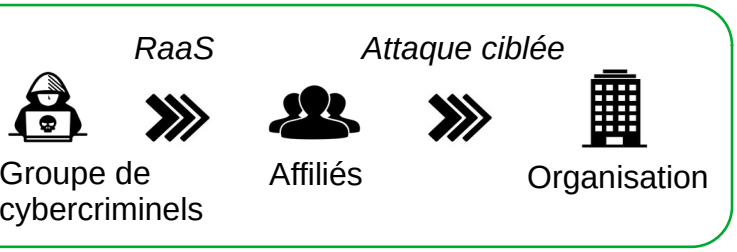
TLP:AMBER+STRICT

Strat CECYBER

STR-2023-02-22

Les rançongiciels *(ransomwares)*

Confiance : **FORTE**
Statut : **EN COURS**
Secteurs affectés : **TOUS**
Zones géographiques touchées : **MONDE**
Objectif : **LUCRATIF**



SYNTHÈSE

Les attaques par rançongiciel représentent un phénomène cyber en pleine expansion - ces dernières années - qui impacte tous les secteurs et tous types de victimes. Ce type d'attaque est le fait d'une criminalité organisée, compte tenu des moyens humains et techniques déployés. Pour autant, un arsenal juridique existe, et la collaboration des services d'enquête mène à des arrestations de cybermalfaiteurs.

I. Le phénomène criminel

Dans le monde en 2022, une attaque par rançongiciel serait revendiquée toutes les **3 heures** en moyenne[1]. Depuis 2022, chaque attaque aurait engendré en moyenne la violation des données de plus de **3 300 personnes**[2].

Le rançongiciel peut être défini comme un *« logiciel malveillant ou un virus qui bloque l'accès à l'ordinateur ou à ses fichiers et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès »*[3]. Le phénomène impacte tous types de victimes : particuliers, professionnels (grandes sociétés, PME, TPE), collectivités territoriales et administrations ou encore associations.

Si tout le tissu économique est impacté, certains secteurs sont plus souvent la cible des cyberattaquants, notamment l'industrie, les technologies de l'information, la finance ou encore le bâtiment[4]. Il s'agit d'une délinquance qui ne se cache pas et profite de la médiatisation de ses attaques.

Le rançongiciel constitue une menace sous-évaluée par les professionnels. En Europe, près d'une attaque sur deux concerne une TPE-PME[5].

Ce phénomène cyber a pu se développer grâce à de nombreuses vulnérabilités, exacerbées par :

- L'essor du télétravail
- Le peu de risques pour les attaquants
- Le faible niveau de protection
  Le faible acculturation à la cybersécurité
- La rentabilité d'une attaque au regard des coûts d'achat ou de location du logiciel malveillant

Outre le risque ultime de mise en péril de l'entité ciblée, les impacts d'un rançongiciel peuvent être de plusieurs ordres : perte d'informations, paralysie temporaire ou définitive de l'activité, impact sur la réputation, perte de confiance des collaborateurs, sans compter le vol et parfois la diffusion de données personnelles.

Le plus souvent, le temps de la restauration des systèmes et de la remise en état du service représente un coût supplémentaire considérable. En 2022, les pertes de chiffre d'affaires consécutives à ce type d'attaque s'élèveraient à **2,8 milliards d'euros** pour les sociétés françaises[6]. Dans le monde en 2022, **62 % des entreprises victimes d'une attaque de rançongiciel auraient payé une rançon**[7].

SOURCES

[1][6] « Baromètre Anozr Way du ransomware - 5e édition bilan annuel 2022 », Anozr Way, publié en janvier 2023.
[2][5] « Baromètre Anozr Way du ransomware - 4e édition Évolution de la menace mai à août 2022 », Anozr Way, publié en septembre 2022.
[3] « Rançongiciel ou ransomware, que faire ? », cybermalveillance.gouv.fr.
[4] « Le paysage des menaces ransomware observé par Sekoïa », Sekoïa, publié le 28 juillet 2022.
[7] « Rapport Hiscox sur la gestion des cyber-risques », Hiscox, publié en novembre 2022.

II. Cyberdélinquance

Les attaques par rançongiciels sont le fait d'une **cybercriminalité organisée**, aux structures protéiformes et évolutives. L'un des modèles économiques développés est celui du ***Ransomware-as-a-Service*** (RaaS) qui :

- met à disposition un logiciel malveillant, des outils et des compétences humaines, auprès d'affiliés, en contrepartie du reversement d'un pourcentage de la rançon ;
- permet de mener des cyberattaques complexes, même pour des individus d'un niveau technique modéré.

Les cybermalfaiteurs se répartissent entre groupes spécialisés en rançongiciel, indépendants et affiliés :

- opérateurs de rançongiciel : développent un modèle RaaS et éditent les logiciels malveillants ;
- initial access brokers : spécialistes dans l'identification des vulnérabilités permettant d'avoir un accès sur le SI de la victime, qui revendent ces accès à d'autres acteurs malveillants ;
- affiliés : cybercriminels déployant le rançongiciel sur le SI de la victime. Ils passent par un processus de candidature et négocient la part de la rançon leur revenant, qui pourrait atteindre 80 %[8].

Chaque groupe ou affilié est libre d'agir au moyen de méthodes sophistiquées et uniques. Les techniques d'attaque utilisées sont pensées pour exercer une pression psychologique auprès des victimes, en les plaçant dans un état de sidération et de résignation afin qu'ils acceptent de payer la rançon.

L'écosystème des cybermalfaiteurs est alimenté à la fois par :

- les rançons, avec un montant moyen demandé en 2021 qui aurait atteint 2,2 millions de dollars[9] ;
- la revente des données personnelles exfiltrées lors des attaques.

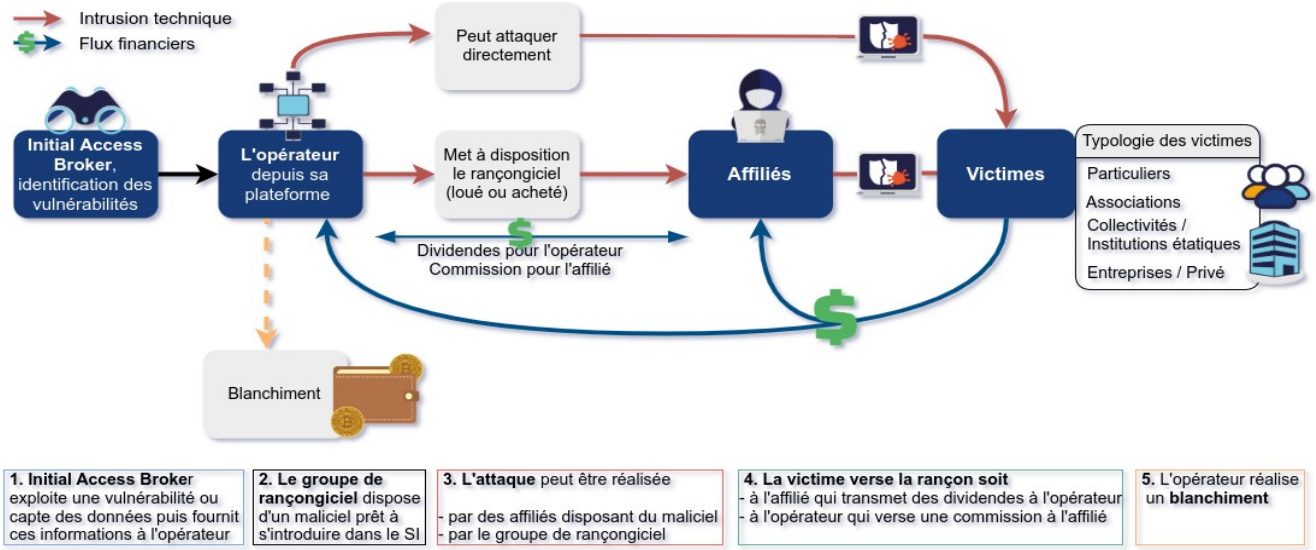
Lorsqu'il s'agit de cibler les victimes, deux méthodes coexistent :

- la chasse au gros gibier *(Big game hunting)* : actions ciblées de haute technicité sur des organisations importantes disposant de moyens élevés.
- les attaques de masse : actions opportunistes sur des cibles vulnérables.

Exemples de modes opératoires employés pour infiltrer les systèmes d'information d'une victime :

- *insiders* : (anciens) employés agissant par opportunisme financier ou par vengeance ;
- ingénierie sociale : invite la victime à fournir ses données personnelles par manipulation ou par ruse ;
- attaques par *supply chain* : sous-traitants d'une société ciblée à l'origine, supposés moins protégés.

RaaS - Modélisation d'une attaque par rançongiciel



SOURCES

[8] Page TOR de Lockbit
[9] « 2022 Unit 42 Ransomware Threat Report Highlights: Ransomware Remains a Headliner », Unit42, publié le 24 mars 2022.

III. Prise en compte et traitement de la menace

Une attaque par rançongiciel se rapporte à plusieurs infractions :

- l'extorsion de fonds (Code Pénal, article 312-1) ;
- l'introduction frauduleuse de données dans un système de traitement automatisé -STAD (C.P, article 323-3) ;
- l'entrave ou l'altération du fonctionnement du STAD (C.P, article 323-1) ;
- l'extorsion en bande organisée est une circonstance aggravante (C.P, article 312-6). La conception et l'utilisation de ces logiciels malveillants supposent en effet des acteurs et des compétences particulières.

La législation relative aux STAD tend également à s'enrichir afin de s'adapter à la menace. La loi du 24 juillet 2015 a doublé le montant de l'amende des articles 323-1 et suivants du Code Pénal, atteignant 150 000 euros. Par ailleurs, la loi d'orientation et de programmation du ministère de l'intérieur (LOPMI) promulguée en janvier 2023, encadre le remboursement par les assurances du paiement de la rançon en cas de cyberattaque. Le remboursement est conditionné au dépôt de plainte dans les 72h après connaissance de l'infraction.

Depuis 2019, la section J3 de la JIRS-JUNALCO du parquet de Paris dispose d'une compétence nationale concernant tous les faits de rançongiciel et centralise ces enquêtes. Au cours de l'année 2022, sur les 600 enquêtes cybercriminelles ouvertes par la section J3, 397 enquêtes avaient un rapport avec les rançongiciels[10].

Attaques visant les collectivités territoriales	Attaques visant les établissements de santé
09/22 : Mairie Maison-Alfort (94) ; 10/22 : Conseil départemental Seine-Maritime (76) ; 11/22 : Conseil départemental Seine-et-Marne (77) ; 11/22 : Conseil régional Guadeloupe.	08/22 : Hôpital de Corbeil-Essonnes (91) ; 11/22 : Centre d'oncologie et de radiothérapie Saint-Jean à Saint-Doulchard (18) ; 12/22 : Centre hospitalier de Versailles (78).
Éléments saillants : - Ce phénomène qui impacte les collectivités peut également être mis en perspective au regard du pré-diagnostic Di@GoNal[11]. Sur 764 collectivités qui ont pris part à ce dernier, 1 sur 10 a été victime d'un rançongiciel. La plus petite collectivité touchée compte 200 habitants. - Les attaques sont lancées principalement en fin de semaine. Le centre hospitalier de Versailles avait ainsi été ciblé dans la nuit du samedi au dimanche.	

Attaques récentes sur le territoire français

A titre d'exemple, les investigations menées par les services de police judiciaire ont abouti aux opérations suivantes :

- Janvier 2022 : arrestation par la police ukrainienne de 5 membres affiliés d'un groupe de rançongiciel ;
- Mars 2022 : un ancien employé du gouvernement canadien est interpellé par la Gendarmerie royale du Canada. Il figure parmi les membres les plus prolifiques du groupe Netwalker ;
- Novembre 2022 : arrestation d'un membre du groupe de rançongiciel Lockbit au Canada résultant d'une opération coordonnée entre le C3N, le FBI, Europol et la Gendarmerie royale canadienne.

Préconisations

Avant une attaque

- Acquérir une assurance cyber et des solutions techniques ;
- Procéder à des tests d'intrusion ;
- Mettre en place des outils de surveillance et de réaction sur les postes de travail et les serveurs;
- Surveiller les activités suspectes liées à l'Active-Directory ;
- Promouvoir la prévention et la sensibilisation.

Après une attaque

- Éviter de payer la rançon : 80 % des payeurs seraient victimes d'une nouvelle attaque [12] ;
- Systématiser le dépôt de plainte sans délai pour initier les investigations et accéder aux remboursements ;
- Conserver la preuve numérique (effectuer un gel des lieux numériques).

SOURCES

[10] « Cyberattaques : 600 enquêtes ouvertes par le parquet de Paris depuis janvier 2022 », FranceInfo, publié le 13 décembre 2022.
[11] Di@GoNal est un outil de pré-diagnostic élémentaire à destination des collectivités, entreprises et établissements de santé proposé par le ComCyberGend.
[12] « Situation actuelle en matière de cybercriminalité », Varonis, publié en mars 2022.