RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inter//stats
Analyser pour agir
SERVICE STATISTIQUE MINISTÉRIEL DE LA SÉCURITÉ INTÉRIEURE

N° 37
Novembre 2021

Analyse

Attaques par rançongiciel envers les entreprises et les institutions

Entre 2016 et 2020, on estime que les services de police et de gendarmerie nationales ont enregistré entre 1 580 et 1 870 procédures en lien avec des attaques par rançongiciel (logiciels malveillants de demande de rançon par blocage de l'accès aux données) visant des entreprises et des institutions. Quelle que soit l'estimation retenue, les tendances sont les mêmes. En particulier, selon l'estimation haute, le nombre de procédures ouvertes en lien avec des attaques par rançongiciel a augmenté en moyenne de 3 % chaque année jusqu'en 2019, avec une accélération entre 2019 et 2020 (+32 %). Bien que ce phénomène soit en hausse, les procédures en lien avec des attaques par rançongiciel envers les entreprises et les institutions ne représentent cependant que 15 % des atteintes aux systèmes de traitement automatisé de données enregistrées entre 2016 et 2020.

Certains secteurs d'activité sont plus visés que d'autres. Le secteur industriel est particulièrement touché : il représente 15 % des victimes enregistrées contre 7 % du tissu économique en France. De même, le secteur des administrations publiques, de l'enseignement, de la santé humaine et de l'action sociale est surreprésenté : 20 % des victimes pour 13 % des établissements en France.

Sur la période 2016-2020, les enregistrements issus des logiciels de rédaction des procédures ne permettent pas d'approcher de manière exhaustive le nombre de cyberattaquants identifiés par les services. Sur l'ensemble des procédures en lien avec des rançongiciels, seules 0,3 % ont au moins un mis en cause enregistré.

Enfin, en lien avec des attaques de plus en plus ciblées, les entreprises et les institutions se voient réclamer des rançons de plus en plus importantes, le plus souvent en cryptomonnaie. Ainsi, selon les données enregistrées par la police et la gendarmerie, lorsque les montants sont renseignés (dans 16 % des procédures seulement), la valeur médiane a progressé d'environ 50 % par an entre 2016 et 2020, s'élevant à 6 375 euros pour cette dernière année.

La cyberdélinquance recouvre l'ensemble des infractions pénales commises essentiellement ou exclusivement à l'aide des technologies numériques. Deux grandes catégories d'infractions relèvent de la cybercriminalité : lorsque le cyberespace est utilisé comme moyen de commission d'une infraction (comme les escroqueries en ligne) ou lorsqu'en plus d'en être le moyen, les technologies numériques en sont aussi la cible. Ces dernières infractions sont communément appelées les atteintes aux systèmes de traitement automatisé de données (STAD) et comprennent notamment les rançongiciels.

Les rançongiciels, également appelés *ransomwares*, font partie de la famille des logiciels malveillants ou *malwares* (Bourrier & Nova, 2019), qui se définissent comme des logiciels conçus pour infecter et endommager le système hôte d'un utilisateur. Plus précisément, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) définit le rançongiciel de la manière suivante : « technique d'attaque courante de la cybercriminalité, le rançongiciel ou *ransomware* consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement ». La motivation principale derrière une attaque par rançongiciel est donc la recherche de profit, soit directement par l'obtention de la rançon, soit indirectement par la revente des données dérobées. Ce type d'attaque peut se propager aux ordinateurs par le biais de pièces jointes ou de liens contenus dans des emails de *phishing*[1], via des sites Web ou des clés USB infectés. Les deux rançongiciels les plus utilisés sont les *crypto-ransomwares* qui chiffrent les données d'un ordinateur, et les *ransomwares* « *locker* » qui ne chiffrent pas les données, mais empêchent la victime d'accéder à son appareil.

1. Selon le GIP ACYMA, le phishing correspond à un « vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge ».

Encadré 1 - Identifier les attaques par rançongiciel dans les procédures

Les résultats présentés dans cette étude sont issus de premiers travaux exploratoires. La cyberdélinquance ne s'appréhendant pas par nature d'infraction ni par un des index de l'État 4001 (séries historiques suivies par le ministère de l'Intérieur), la mesure du phénomène est en cours d'élaboration.

Dans le cadre de leur activité judiciaire, les services de police et les unités de gendarmerie rédigent des procédures relatives à des infractions, avant de les transmettre à l'autorité judiciaire qui est susceptible de les requalifier par la suite. Ces infractions ont pu être constatées suite à une plainte, à un signalement, à un témoignage, à un délit flagrant, à une dénonciation, ou encore sur l'initiative des forces de sécurité. La base de données des crimes et délits, portant sur les infractions enregistrées, a été extraite en février 2021 et porte sur toute la période 2016-2020, entraînant ainsi des requalifications différenciées dans le temps (les procédures ouvertes en 2016 ont pu être modifiées pendant quatre ans quand les procédures de 2020 apparaissent dans leur forme quasi-initiale d'enregistrement). Pour cette étude, seules les procédures avec au moins une victime personne morale ont été retenues. Leur secteur d'activité est classé selon la nomenclature d'activités française en 10 postes. La répartition en taille d'unité urbaine est faite selon le lieu de commission de l'infraction et le champ géographique couvert ici est celui de la France (métropole et DROM). Enfin, l'analyse étant menée au niveau des procédures, c'est la date d'ouverture de procédure qui est retenue pour mener les exploitations temporelles.

L'identification des procédures en lien avec des attaques par rançongiciel se fait grâce à l'analyse textuelle du descriptif de l'affaire et à l'utilisation de variables caractérisant l'infraction ou la procédure. Les traitements effectués pour identifier les rançongiciels sont en partie différents pour la police et pour la gendarmerie. Dans les bases de données de la police, il existe une variable permettant d'identifier le mode opératoire « rançongiciel » au niveau des infractions. Cette variable est donc directement exploitée pour repérer les procédures en lien avec des attaques par rançongiciel. Cette dernière n'a pas son équivalent dans les bases de la gendarmerie d'où la nécessité d'exploiter en complément le champ textuel des manières d'opérer.

L'analyse de ce champ utilisant les techniques classiques du Natural Language Processing (NLP) appliquées aux manières d'opérer décrivant l'affaire permet d'identifier par un autre biais les attaques par rançongiciel. La recherche textuelle prend en compte la possibilité de fautes d'orthographe ou de frappe. Les mots recherchés peuvent être des mots uniques comme le terme « rançongiciel », le nom d'un rançongiciel comme « *ryuk* », ou des recherches combinées associant plusieurs termes comme « cryptage » et « versement ». Les manières d'opérer concernant les procédures comprenant des victimes personnes morales de crimes et délits sont manquantes pour 83 % des procédures de la police nationale et pour 2 % des procédures de la gendarmerie. Ceci s'explique par le fait qu'en police nationale la saisie du champ textuel de la manière d'opérer n'est pas obligatoire dans le logiciel de rédaction des procédures. Ceci pourrait donc conduire à une sous-estimation du phénomène.

Une difficulté supplémentaire dans la détection des rançongiciels tient à la centralisation systématique des enquêtes : en effet l'organisation de l'investigation est répartie par familles de rançongiciel entre les différents services à compétence nationale qui concentrent donc toutes les affaires liées à leur champ de compétence. Ces procédures transférées à partir des plaintes initiales sont hors du champ de l'étude mais leur détection peut être partielle si les numéros de procédure précédents sont absents et si des faits constatés sont enregistrés dans la procédure transférée.

Par ailleurs, certaines procédures semblent bien correspondre à des rançongiciels suite au cryptage des ordinateurs ou serveurs des entreprises et institutions, mais la demande du versement d'une rançon n'est pas toujours précisée dans la manière d'opérer, ce qui conduit à les identifier ou non comme attaque par rançongiciel selon l'hypothèse retenue. Ces différentes incertitudes nous conduisent à produire une **première estimation** plutôt qu'un nombre exact de procédures de rançongiciel enregistrées par an.

Les données décrivent uniquement ce qui est connu des services de police et de gendarmerie. Les victimes ne déposant pas plainte auprès des forces de sécurité à la suite d'une attaque par rançongiciel ne sont donc pas comptabilisées.

Les attaques par rancongiciel présentées dans cette étude sont celles ayant été identifiées par les services de police et de gendarmerie en tant que telles. Dès lors, il est possible que certains faits ne correspondent pas à la définition stricte d'un rançongiciel, la saisie s'effectuant selon l'appréciation de l'atteinte par les forces de sécurité.

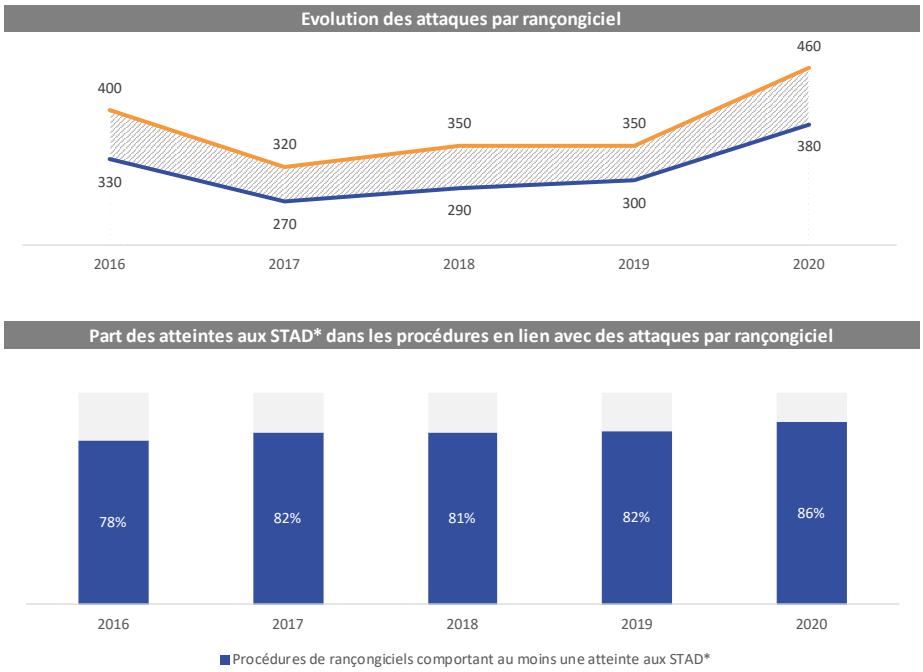
Cette étude se restreint aux attaques par rançongiciel visant les personnes morales[2]. Les entreprises et les institutions, plus que les particuliers, sont actuellement les cibles privilégiées des cyberattaquants. En effet, elles ont des capacités financières plus importantes et peuvent être plus enclines à payer rapidement la rançon afin de pouvoir accéder à leurs données et limiter ainsi l'impact sur leurs activités (ANSSI, 2020b). En outre, dans les plaintes déposées par les particuliers, les arnaques au faux support technique[3] sont parfois assimilées à des rançongiciels dans les données enregistrées par les forces de sécurité car un non-professionnel est plus souvent susceptible de ne pas identifier si les données du système d'information ont été réellement cryptées.

Les plaintes pour rançongiciel en augmentation de 32 % entre 2019 et 2020

Entre 2016 et 2020, on estime entre 1 580 et 1 870 le nombre de procédures en lien avec des attaques par rançongiciel envers les entreprises et les institutions qui ont été enregistrées par les forces de sécurité (*encadré 1*). L'identification stricte et unique des attaques par rançongiciel est rendue difficile par un certain nombre de facteurs liés à l'enregistrement des procédures (description approximative de l'attaque, présence de doublon), c'est pourquoi le nombre de procédures par an est estimé à l'aide d'une hypothèse basse et haute (voir *encadré 1*). Ainsi, en 2020, on estime le nombre de procédures entre 380 et 460. Les tendances pour des hypothèses basse et haute sont les mêmes. Ainsi, la suite de l'analyse se base uniquement sur l'hypothèse haute. Ces procédures ont ainsi connu un taux de croissance annuel moyen de 3 % entre 2016 et 2019

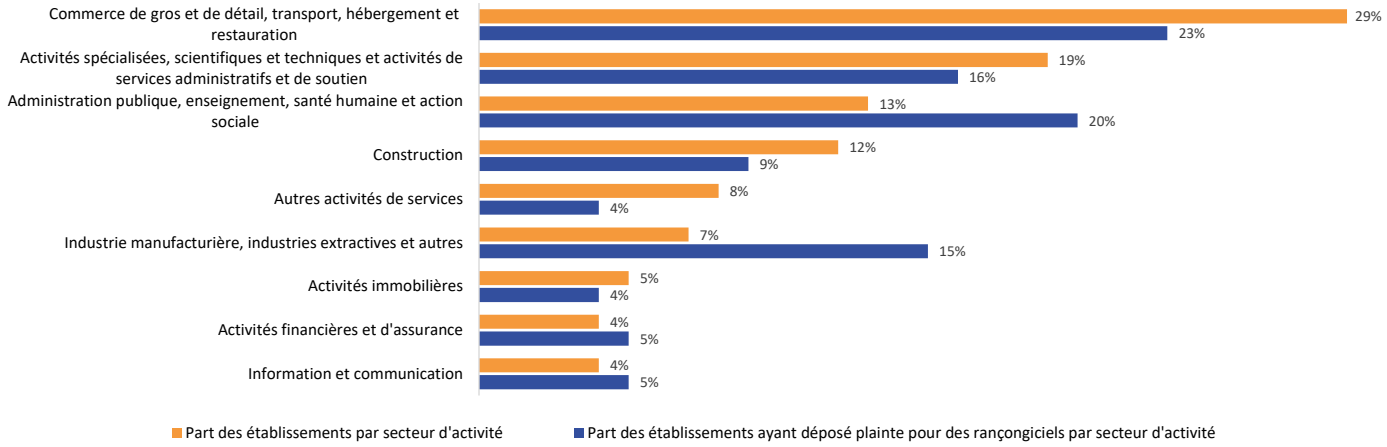
2. Les personnes morales sont désignées ci-après comme entreprises et institutions pour simplifier la lecture.
3. Les arnaques au faux support technique se caractérisent par l'apparition d'une page bloquant l'ordinateur de la victime et demandant d'appeler un support technique pour le déblocage de l'ordinateur.

1 Procédures en lien avec les attaques par rançongiciel



*STAD : Système de traitement automatisé de données.
Note : L'identification stricte et unique des attaques par rançongiciel est rendue difficile par un certain nombre de facteurs liés à l'enregistrement des procédures (description approximative de l'attaque, présence de doublon), c'est pourquoi le nombre de procédures par an est estimé à l'aide d'une hypothèse basse et haute.
Lecture : En 2020, entre 380 et 460 procédures en lien avec des attaques par rançongiciel envers les entreprises et les institutions ont été enregistrées par la police ou la gendarmerie. Parmi ces dernières, 86 % comprennent au moins une infraction relative à des atteintes aux STAD.
Champ : France, procédures ouvertes sur la période 2016-2020.
Source *: SSMSI, base des crimes et délits enregistrés par la police et la gendarmerie entre 2016 et 2020.*

2 Part des secteurs d'activité visés par des attaques de rançongiciel

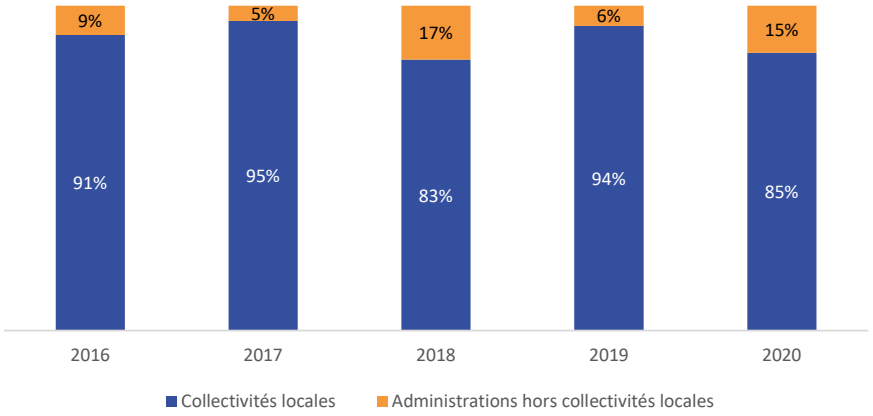


Note : Les secteurs d'activité n'ont pas pu être identifiés pour 21 % des personnes morales victimes, les non-réponses sont exclues du graphique. Le secteur agricole n'est pas représenté sur cette figure.
Lecture : Entre 2016 et 2020, 20 % des personnes morales victimes d'attaques par rançongiciel font partie du secteur des administrations publiques, de l'enseignement, de la santé humaine et de l'action sociale selon les données enregistrées par la police et la gendarmerie. La part de ce secteur d'activité est de 13 % en France.
Champ : France, procédures ouvertes sur la période 2016-2020.
Sources *: SSMSI, base des crimes et délits enregistrés par la police et la gendarmerie entre 2016 et 2020 ; Insee, Répertoire des entreprises et des établissements (Sirene) en géographie au 01/01/2021.*

malgré une importante baisse entre 2016 et 2017 (-20 %). Entre 2019 et 2020, ces attaques ont fortement augmenté : +32 % (*figure 1*). Les attaques par rançongiciel n'ayant pas de qualification juridique propre, différentes infractions peuvent être retenues (*encadré 2*). Une infraction d'atteinte aux STAD est enregistrée dans 82 % des procédures de rançongiciel. Des infractions liées à des menaces ou chantages pour extorsion de fonds, et à des escroqueries et abus de confiance peuvent également être enregistrées. Une même procédure peut être liée à la fois à des atteintes aux STAD, à des menaces ou chantages et à des escroqueries.

Les rançongiciels enregistrés par les forces de sécurité ne représentent qu'une faible part des atteintes aux STAD envers les personnes morales (15 % entre 2016 et 2020). Ils se retrouvent principalement dans les atteintes aux STAD concernant les interférences illégales avec un système informatique (50 %) ainsi que celles concernant les interférences illégales avec des données informatiques (39 %). Les atteintes aux STAD dans leur ensemble ont progressé plus vite que le nombre de procédures pour rançongiciels identifiées comme atteintes aux STAD entre 2018 et 2019 (+7 % contre 1 % pour les rançongiciels) mais moins fortement en 2020 (+10 % contre +38 % pour les rançongiciels). Pour l'ensemble des procédures concernant les rançongiciels, cette augmentation est de 32 % entre 2019 et 2020.

3 Part des collectivités locales dans les administrations publiques touchées par un rançongiciel



Lecture : En 2020, 85 % des administrations publiques victimes d'un rançongiciel sont des collectivités locales selon les données enregistrées par la police ou la gendarmerie.
Champ : France, procédures ouvertes sur la période 2016-2020.
Source *: SSMSI, base des crimes et délits enregistrés par la police et la gendarmerie entre 2016 et 2020.*

4 Répartition des personnes morales victimes d'attaques par rançongiciel selon l'unité urbaine du lieu de commission *(en %)*

Tranche unité urbaine	Commune hors unité urbaine (zone rurale)	Commune appartenant à une unité urbaine de : 2 000 à 9 999 habitants	10 000 à 49 999 habitants	50 000 à 199 999 habitants	200 000 à 1 999 999 habitants	Unité urbaine de Paris
Agriculture	34	19	19	9	19	0
Industrie manufacturière, industries extractives et autres	25	17	18	13	22	6
Construction	26	17	15	13	20	9
Commerce de gros et de détail, transports, hébergement et restauration	15	16	17	12	26	14
Information et communication	2	10	7	8	27	46
Activités financières et d'assurance	10	8	11	15	34	21
Activités immobilières	7	5	19	21	33	14
Activités spécialisées, scientifiques et techniques et activités de services administratifs et de soutien	8	11	10	9	35	27
Administration publique, enseignement, santé humaine et action sociale	19	28	16	11	19	7
Autres activités de services	11	9	8	12	40	20
Ensemble des victimes	**17**	**17**	**14**	**11**	**26**	**15**

Note : Les lieux de commission n'ont pas pu être identifiés pour 2 % des victimes personnes morales et les secteurs d'activités pour 21 % de ces dernières.
Lecture : Entre 2016 et 2020, selon les données enregistrées par la police ou la gendarmerie, 17 % des victimes de rançongiciel se trouvent dans des zones rurales.
Champ : France, procédures ouvertes sur la période 2016-2020.
Source *: SSMSI, base des crimes et délits enregistrés par la police et la gendarmerie entre 2016 et 2020.*

Le secteur industriel et celui des administrations publiques, de l'enseignement, de la santé humaine et de l'action sociale surreprésentés parmi les victimes de rançongiciel

Les attaques par rançongiciel peuvent toucher l'ensemble des entreprises et des institutions, allant du secteur agricole à celui de l'industrie. Cependant, tous les secteurs ne sont pas visés dans les mêmes proportions. Les entreprises du secteur commercial, transport, hébergement et restauration sont les plus nombreuses parmi les personnes morales déposant plainte à la police ou à la gendarmerie pour des attaques par rançongiciel (23 %), mais cette proportion est inférieure à leur poids dans le tissu économique (29 % des établissements, *figure 2*). En revanche, le secteur industriel est plus particulièrement touché, représentant 15 % des victimes enregistrées contre 7 % du tissu économique national. Le secteur des administrations publiques, de l'enseignement, de la santé humaine et de l'action sociale est également surreprésenté : 20 % des victimes enregistrées pour 13 % des établissements en France.

Parmi les administrations publiques ayant déposé plainte suite à une attaque par rançongiciel, 89 % sont des collectivités locales, soit 9 % de l'ensemble des victimes (*figure 3*). Elles ont d'ailleurs été particulièrement touchées en 2020 avec 2,7 fois plus de procédures enregistrées qu'en 2019. Dans l'ensemble, le nombre de procédures enregistrées, liées aux rançongiciels visant des administrations publiques, a triplé entre 2019 et 2020. Selon l'ANSSI (2021), le secteur administratif, notamment les collectivités locales, est en effet particulièrement ciblé. Ces dernières ont souvent un faible niveau de protection informatique, alors qu'il est important que leur activité ne soit pas suspendue. Les cyberattaquants peuvent également utiliser les données sensibles présentes dans leurs systèmes d'information pour exercer un chantage puisque la publication de telles données porterait atteinte aux administrés.

Encadré 2 - Cadre juridique du rançongiciel

Le rançongiciel n'a pas de qualification juridique propre (Martinon, 2019). En effet, il n'existe pas d'article de loi traitant spécifiquement de cette cyberattaque. Cependant, plusieurs articles du Code pénal peuvent s'appliquer.

Les articles se rapprochant le plus de la définition du rançongiciel sont les articles relatifs aux atteintes aux STAD (art. 323-1 à 8 du Code pénal). Les peines correspondantes peuvent aller jusqu'à dix ans de prison et 300 000 € d'amende. Par ailleurs, le cyberdélinquant pourra être puni des mêmes peines simplement pour la possession d'un rançongiciel (ou de tout autre instrument, équipement ou programme informatique permettant la réalisation des infractions d'atteintes aux STAD) comme le dispose l'article 323-3-1 du Code pénal.

Le rançongiciel correspond aussi à la définition de délits plus classiques comme l'extorsion puisqu'il s'agit d'exiger la remise de fonds sous la contrainte. L'extorsion est passible de sept ans d'emprisonnement et de 100 000 € d'amende (art. 312-1 du Code pénal).

En outre, depuis 2016 et la mise en place du règlement général sur la protection des données, lorsque des données personnelles sont perdues, l'entreprise ou l'institution attaquée doit le notifier à la CNIL dans les 72 heures (Martinon, 2019).

D'autres types d'infractions sont constatées par les forces de sécurité dans les procédures en lien avec des attaques par rançongiciel comme le chantage (art.312-10 du Code pénal) ou encore l'escroquerie (art. 313-1 du Code pénal). Concernant le chantage, le cyberdélinquant peut en effet menacer de rendre publique certaines données personnelles si la rançon n'était pas payée (ANSSI, 2020a).

Le secteur de la santé est également une cible privilégiée, particulièrement depuis la pandémie de Covid-19. Les atteintes dans le secteur de la santé humaine et de l'action sociale représentent 7 % des attaques. Leur nombre a été multiplié par 1,6 entre 2019 et 2020.

41 % des victimes sont situées dans des unités urbaines de plus de 200 000 habitants

Selon les données de la police et de la gendarmerie, les attaques par rançongiciel visent des entreprises et des institutions sur tout le territoire (*figure 4*), mais plus particulièrement celles situées dans les plus grandes unités urbaines. En effet, 41 % de ces attaques par rançongiciel ont eu lieu dans une commune appartenant à une unité urbaine de plus de 200 000 habitants. Cependant, les entreprises et les institutions des zones rurales ne sont pas épargnées : une entreprise ou institution sur six qui a subi une attaque par rançongiciel est située dans une commune hors unité urbaine. Ces attaques en zone rurale ou dans des petites communes concernent particulièrement le secteur de l'agriculture, de l'industrie et de la construction, ainsi que le secteur des administrations publiques, enseignement, santé humaine et action sociale. Les entreprises des secteurs de l'information et de la communication, des activités financières et des assurances ainsi que des activités spécialisées scientifiques et techniques sont plus souvent touchées dans les grandes unités urbaines, notamment celle de Paris pour respectivement 46, 21 et 27 %, en cohérence avec les implantations effectives de ces secteurs sur le territoire français.

Très peu de mis en cause enregistrés sur la période 2016-2020

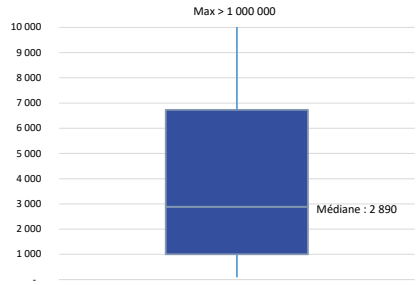
Les mis en cause pour attaques par rançongiciel figurent rarement dans les enregistrements de la police et la gendarmerie sur la période 2016-2020. Sur les 1 870 procédures (hypothèse haute) enregistrées entre 2016 et 2020 en lien avec des rançongiciels visant des entreprises ou des institutions, seules six procédures ont au moins un mis en cause enregistré, soit 0,3 % de ces procédures. L'identification des mis en cause à la suite d'attaques par rançongiciel est complexe, et leur recherche se fait au sein d'enquêtes centralisées par famille de rançongiciel. De plus, en gendarmerie, dès lors que la procédure n'est pas clôturée, les mis en cause ne sont pas enregistrés. Les procédures de rançongiciel pouvant être particulièrement longues, il est possible que le nombre de mis en cause soit sous-estimé.

Étant donné le faible nombre de mis en cause, il n'est pas possible de déterminer un profil à partir des données de police ou de gendarmerie. Au niveau international, l'ONUDC estime que 80 % des cyberdélinquants agissent au sein de groupes criminels, il s'agirait principalement d'hommes (entre 81 % et 94 % selon les études), jeunes (la plupart des études suggèrent que les auteurs de cyberdélits sont généralement âgés de 18 à 30 ans), n'ayant pas nécessairement suivi d'études supérieures notamment en informatique (UNODC, 2013).

La difficulté d'identification des mis en cause résulte de différents facteurs. Le développement récent de tout un écosystème cybercriminel professionnalisé, comparable à celui du système économique légal rend la recherche des auteurs particulièrement ardue. Les cybercriminels peuvent ainsi acheter des données personnelles volées, des logiciels malveillants, ou encore louer des *botnets* sur le *darkweb*. Cet écosystème, également appelé *cybercrime as a service*, permet d'accéder à différentes ressources spécialisées nécessaires à la commission d'un acte cybercriminel, multipliant les acteurs impliqués dans les attaques (Meurant & Cardon, 2021).

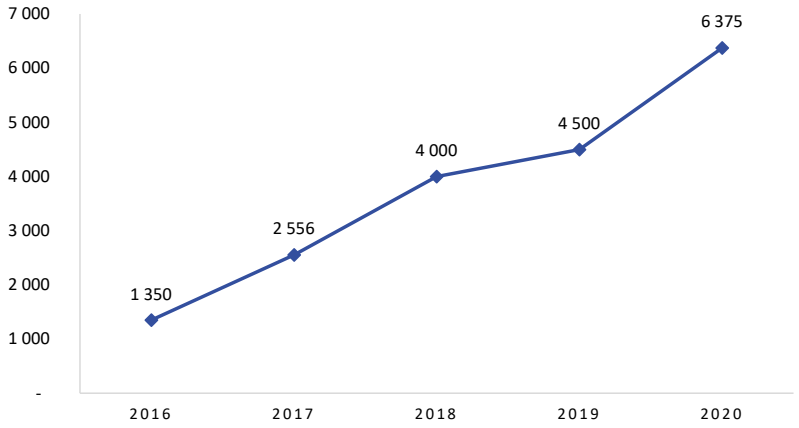
La première étape pour les cybercriminels est l'infiltration dans le système de la cible afin de chiffrer ses données. Pour cela, ils peuvent faire appel à des

5 Distribution du montant des rançons sur la période 2016 - 2020 *(en euro)*



Note : Les montants des rançons ne sont connus que dans 16 % des procédures ayant été identifiées comme des attaques par rançongiciel (hypothèse haute).
Lecture : Entre 2016 et 2020, la moitié des personnes morales se sont vu demander une rançon inférieure à 2 890 euros selon les enregistrements de la police et de la gendarmerie.
Champ : France, procédures ouvertes sur la période 2016-2020.
Source *: SSMSI, base des crimes et délits enregistrés par la police et la gendarmerie entre 2016 et 2020.*

6 Évolution de la valeur médiane du montant des rançons de 2016 à 2020 *(en euro)*



Note : Les montants des rançons ne sont connus que dans 16 % des procédures ayant été identifiées comme des attaques par rançongiciel (hypothèse haute).
Lecture : En 2019, la moitié des personnes morales se sont vu demander une rançon inférieure à 4 500 euros selon les enregistrements de la police et de la gendarmerie. Ce montant s'élève à 6 375 en 2020.
Champ : France, procédures ouvertes sur la période 2016-2020.
Source *: SSMSI, base des victimes de crimes et délits enregistrés par la police et la gendarmerie entre 2016 et 2020.*

groupes qui trouvent des failles dans les réseaux d'organisations publiques ou privées afin d'y installer un accès à distance, c'est-à-dire un logiciel permettant d'accéder au réseau piraté et d'en prendre le contrôle à distance. Ces groupes vendent ces accès : ils n'attaquent donc pas directement l'entité visée, mais donnent aux attaquants les moyens de réaliser leur attaque en échange d'une rémunération.

Concernant le choix du type d'attaque, les attaquants peuvent également avoir recours à des plateformes de « *Ransomware-as-a-Service* », qui fournissent directement des rançongiciels. En guise de rémunération, une partie de la somme rançonnée est versée à la plateforme.

La rançon est ensuite réclamée à la victime le plus souvent en cryptomonnaie, et majoritairement en bitcoin, afin de conserver l'anonymat des attaquants. Chaque bitcoin possède un numéro de série unique, qui permet de l'identifier et facilite son traçage. Cependant, il existe des services de « mixage » de cryptomonnaies : le cybercriminel envoie à une plateforme un certain montant en bitcoin. Ces pièces vont être conservées par cette plateforme, qui va lui renvoyer la même somme, mais constituée d'autres pièces qui appartiennent à d'autres usagers réalisant la même opération afin de garder leur anonymat lors de leurs transactions. Par conséquent, l'efficacité de la plateforme dépend de son nombre d'utilisateurs (Charpiat, 2014).

Enfin, les attaquants souhaiteront blanchir leurs gains et pouvoir les retirer. Là encore, ils peuvent faire appel à des groupes spécialisés, qui procèdent via des passeurs d'argent, également appelés « money-mules ». Ces money-mules sont des personnes pouvant être complices ou avoir été manipulées (via de fausses offres d'emplois ou du chantage par exemple) afin d'autoriser l'utilisation de leurs comptes à des fins criminelles[4].

Ainsi, la professionnalisation et la multiplication des acteurs rendent le travail d'investigation particulièrement ardu. En outre, le cyberespace permet à ces différents acteurs d'agir depuis des pays différents (Europol, 2021), dont certains avec lesquels la coopération judiciaire est limitée voire inexistante.

Des montants de rançons rarement renseignés

Les descriptifs des affaires enregistrées par la police et la gendarmerie indiquent les méthodes utilisées par les cyberattaquants (*encadré 2*). Sur les 1 870 procédures de l'hypothèse haute en lien avec les rançongiciels, seules 304 ont un montant de rançon renseigné, soit 16 % des procédures ayant été identifiées comme des attaques par rançongiciel. Il s'agit donc d'une sous-population des procédures en lien avec des rançongiciels : ce groupe ne présente pas de biais significatif quant à la répartition par secteur d'activité, en revanche les victimes sont plus souvent situées dans les petites communes (moins de 10 000 habitants) et très peu présentes dans l'unité urbaine de Paris par rapport à l'ensemble.

Dans la plupart des cas, selon les descriptifs des affaires, un message s'affiche indiquant le montant de la rançon à verser avec la méthode permettant d'effectuer le paiement. Il s'agit souvent de paiement en bitcoin. Il n'est pas rare que la rançon demandée augmente si le versement n'est pas réalisé dans un temps imparti. Dans d'autres cas, un message s'affiche, demandant de prendre contact avec les cybercriminels afin de définir le montant et les modalités de paiement de la rançon. Les statistiques présentées ci-dessous n'exploitent que les rançons réclamées au moment de l'attaque et non celles qui ont pu être réclamées lors de la négociation lorsque celle-ci a lieu. La conversion en euros est faite à partir d'un taux de change pris à la date de début de fait.

Ainsi, entre 2016 et 2020, selon les données de la police et de la gendarmerie, le montant des rançons demandées

4. Pour plus d'information, consulter : https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/money-muling

Encadré 3 - 12 % des sociétés de 10 personnes ou plus du secteur privé déclarent avoir subi en 2018 une indisponibilité des services informatiques

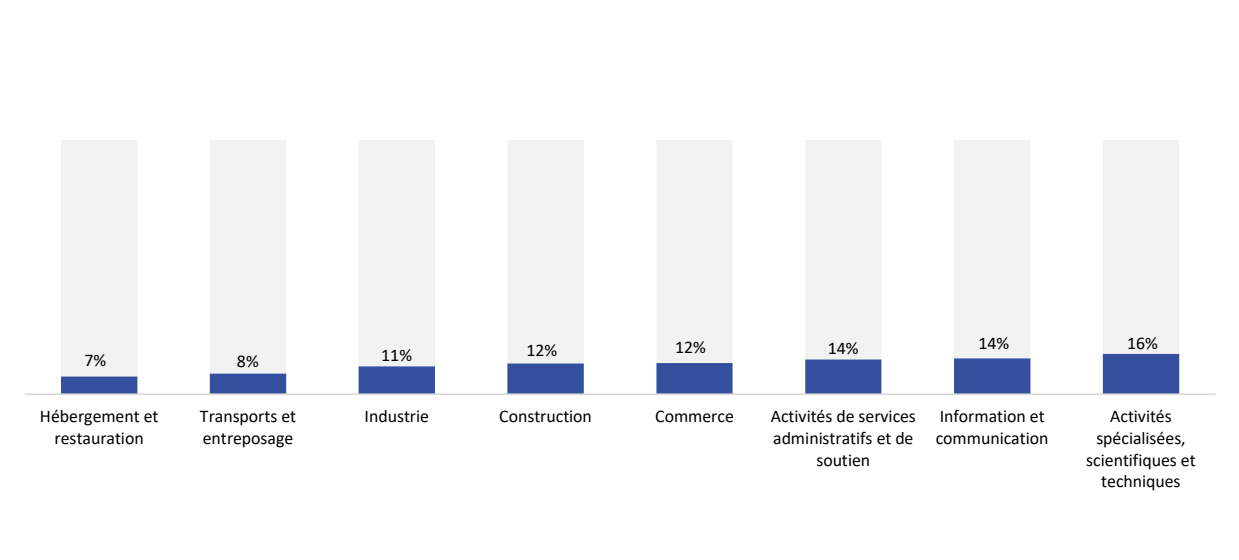
L'enquête Technologies de l'Information et de la Communication (TIC) de l'Insee interroge tous les 5 ans les entreprises de plus de 10 salariés (hors secteurs d'activités liés à la santé et aux administrations publiques) sur le développement et l'utilisation des nouvelles technologies dont une partie est consacrée aux problèmes liés à la sécurité informatique.

Sans que l'information soit spécifique aux rançongiciels, l'enquête TIC Entreprises interroge les entreprises sur les indisponibilités des services informatiques (incluant les attaques extérieures par déni de service[1] ou rançongiciel, les pannes de logiciel ou de matériel informatique - à l'exclusion des pannes mécaniques et des vols) subies l'année précédant l'enquête. Selon la dernière enquête, 12 % des sociétés de 10 personnes ou plus du secteur privé déclarent avoir subi en France, en 2018, une indisponibilité des services informatiques. L'échantillon étant représentatif d'un peu plus de 180 000 sociétés, cela correspondrait à environ 21 000 sociétés victimes en une année. Ce chiffre démontre l'importance des attaques informatiques que peuvent subir les entreprises. En outre, cette part était en augmentation entre 2015 et 2018 (+4 points).

C'est le secteur des activités spécialisées, scientifiques et techniques qui est le plus touché avec 16 % des entreprises ayant été victimes d'indisponibilité des services informatiques, ainsi que le secteur de l'information et de la communication (14 %, *figure E1*).

Ces secteurs sont les plus touchés mais ils comprennent un nombre d'entreprises plus faible que celui du commerce ou de l'industrie, ils représentent donc une part plus faible des entreprises touchées par ces indisponibilités de services informatiques. Au cours de l'année 2018, 24 % des entreprises ayant subi une indisponibilité des services informatiques appartiennent au secteur du commerce, 18 % de celui de l'industrie et 16 % de la construction (*figure E2*). Selon les données de cette enquête, les entreprises les plus grandes sont également les plus concernées (23 % de celles ayant de plus de 250 salariés et 10 % de celles de 10 à 20 salariés).

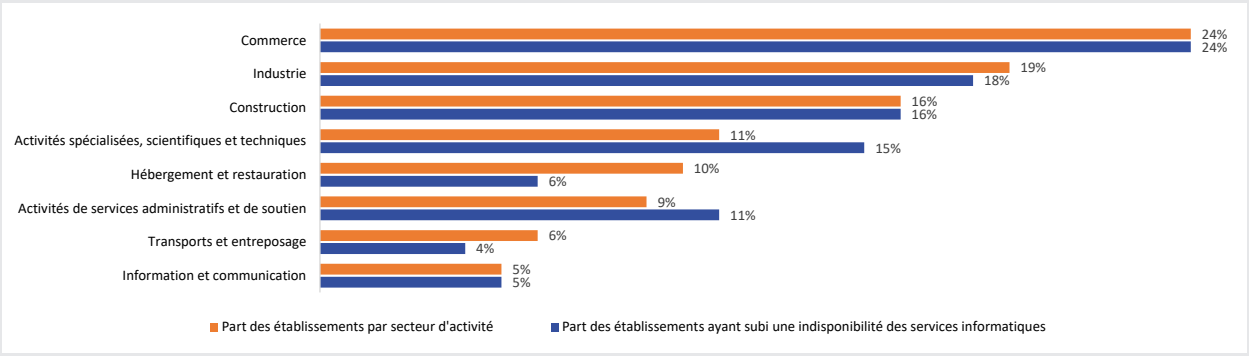
E1 Part des entreprises du secteur privé victimes d'indisponibilité de données dans chaque secteur



Lecture : En 2018, 16 % des entreprises du secteur des activités spécialisées, scientifiques et techniques déclarent avoir subi une indisponibilité des services informatiques.
Champ : Sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricoles, financiers et d'assurance.
Source *: Insee, enquête TIC entreprises 2019.*

1. Une attaque en déni de service « vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé » (GIP ACYMA, 2019).

E2 Répartition des secteurs d'activité des entreprises ayant subi une indisponibilité des services informatiques en 2018



Lecture : En 2018, 18 % des entreprises ayant déclaré avoir subi une indisponibilité des services informatiques appartiennent au secteur de l'industrie. La part de ce secteur d'activité représente 19% des établissements dans l'enquête TIC Entreprises.
Champ : Sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricoles, financiers et d'assurance.
Source *: Insee, enquête TIC entreprises 2019.*

est compris entre quelques dizaines d'euros et plus d'un million d'euros (*figure 5*). Pour un quart des personnes morales, la rançon s'élève à un montant supérieur à 6 730 euros, la moyenne s'établissant à 23 710 euros. Sur la même période, seules sept entreprises ou institutions ont déclaré des rançons supérieures ou égales à 250 000 euros. Si en 2016, pour la moitié des victimes, la rançon était inférieure à 1 350 euros, en 2020 cette valeur médiane est passée à 6 375 euros (*figure 6*), augmentant en moyenne de 50 % par an entre 2016 et 2020.

Cette augmentation s'explique par l'évolution du mode opératoire des cyberattaquants durant les dernières années vers les attaques dites ciblées. La littérature et les sites spécialisés distinguent en effet trois types d'attaques par rançongiciel : les campagnes d'attaques non ciblées, les campagnes d'attaques massives automatiques, et les attaques ciblées (ANSSI, 2020a).

Les campagnes d'attaques non ciblées sont majoritaires. Elles ont le plus souvent pour origine une pièce jointe contenant le logiciel ou une page web malveillante (ANSSI, 2020b). Les principaux vecteurs de propagation sont donc l'email, le *drive-by-download* (téléchargement se lançant automatiquement), les logiciels gratuits, et les publicités malveillantes aussi appelées *malvertising*. Les moyens financiers des victimes étant souvent limités et l'enjeu de la perte des données parfois faible, peu payent la rançon (ANSSI, 2020b). Les délinquants cherchent donc à rediriger leurs attaques en achetant, par exemple, des listes d'adresses de messagerie professionnelle sur les marchés noirs : les employés ayant plus de chance d'avoir des données importantes sur leurs propres machines.

Ces attaques ciblées dites *Big Game Hunting* sont en très forte hausse depuis 2018 selon l'ANSSI. Ce sont des attaques qui touchent des entreprises ou des institutions en capacité de payer une rançon importante. Ces attaques nécessitent de meilleures compétences techniques ainsi que des ressources financières plus importantes et sont réalisées par des groupes cybercriminels. Il existe une troisième catégorie d'attaques dites campagnes d'attaques massives automatiques qui ont pour particularité de se propager automatiquement d'un réseau à un autre et d'un ordinateur à un autre, sans interaction humaine. Le seul cas connu est le rançongiciel *Wannacry* qui en mai 2017, a infecté en une journée au moins 200 000 machines dans plus de 150 pays (en exploitant une faille de sécurité dans le système Windows, se diffusant automatiquement et très rapidement (Aminot, 2020)).

Les entreprises et les institutions, comme les particuliers, ne déposent pas systématiquement plainte, notamment à la suite d'une attaque dite cyber. Les données enregistrées par la police et la gendarmerie ne permettent donc pas d'estimer la cybervictimation dans sa globalité, elles reflètent uniquement ce qui est porté à la connaissance des services. C'est pourquoi des enquêtes auprès d'échantillons représentatifs seraient nécessaires pour approcher la proportion de victimes de ce type de phénomènes délinquants. Aujourd'hui, aucune enquête ne permet de mesurer le taux de dépôt de plainte à la suite d'une attaque par rançongiciel, ni pour les entreprises ou les institutions, ni pour les particuliers. Cela conduit à interpréter les résultats de cette étude avec précaution.

Néanmoins, une enquête représentative des sociétés de 10 personnes ou plus (représentant un sous-champ des personnes morales du secteur privé, hors administration et santé), s'intéressant notamment aux incidents de sécurité informatique, est menée régulièrement par l'Insee et donne certaines indications concernant les indisponibilités de services informatiques (*encadré 3*). Dans la prochaine édition de cette enquête (en 2022), toutes les entreprises victimes d'une indisponibilité de services informatiques seront interrogées sur les suites qu'elles ont données à l'attaque (dépôt de plainte, signalement ou encore déclaration de pertes de données à la CNIL).

Pour en savoir plus

- ANSSI. (2021). Etat de la menace rançongiciel à l'encontre des entreprises et des institutions. Paris: SGDSN.
- CNIL. (2021). Rapport d'activité 2020. Paris: CNIL.
- Europol. (2021). Internet Organised Crime Threat Assessment 2021. Luxembourg: Publications Office of the European Union.
- Meurant, S., & Cardon, R. (2021). Rapport d'information n°678 : La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ? Paris: Rapport du Sénat.
- Sondage OpinionWay pour le CESIN. (2021). Baromètre de la cyber-sécurité des entreprises. Vague 6 - Janvier 2021. Paris: OpinionWay.
- Aminot, J.-L. (2020). WannaCry, une frayeur à l'échelle planétaire. Annales des Mines - Responsabilité et environnement, 98, 53-56.
- ANSSI. (2020a). État de la menace rançongiciel à l'encontre des entreprises et institutions. Paris: SGDSN.
- ANSSI. (2020b). Attaques par rançongiciels, tous concernés. Comment les anticiper et réagir en cas d'incident? Paris: SGDSN.
- Joissains, S., & Bigot, J. (2020). Rapport d'information n°613 : Cybercriminalité un défi à relever aux niveaux national et européen. Paris: Rapport du Sénat.
- Bourrier, M., & Nova, N. (2019). (En)quêtes de pannes. Intraduction. Techniques & Culture, 72, 12-29.
- Martinon, J. (2019). Les défis du traitement judiciaire de la cybercriminalité. LIREC, 59, 14-16.
- Nocetti, J. (2018). La menace dans le champ cyber : une menace multiforme et diffuse. Dans Thierry de Montbrial éd., Les chocs du futurs : Ramses 2019 (pp. 296-299). Paris: Institut français des relations internationales.
- Pinte, J.-P. (2018, 12 31). Les jeunes et le Dark Web. Consulté le 10 15, 2021, sur Terminal: https://journals.openedition.org/terminal/3278
- Charpiat, V. (2014). Le Bitcoin devient monnaie courante : les monnaies digitales entre transparence, régulation et innovation. La Revue des Juristes de Sciences Po, 9, 41-62.
- UNODC. (2013). Étude détaillée sur la cybercriminalité. Vienne: United Nations Publication.
- Site de l'ANSSI : www.ssi.gouv.fr
- Site du GIP Acyma : www.cybermalveillance.gouv.fr

Les données des tableaux, cartes et graphiques associés à cette étude sont disponibles sur le site internet du SSMSI

SSMSI
Service statistique ministériel de la sécurité intérieure

STATISTIQUE PUBLIQUE

SSMSI : place Beauvau 75008 Paris

Directrice de la publication : Christine Gonzalez-Demichel
Rédactrice en chef : Mathilde Poulhes
Auteurs : Sylvie Plantevignes et Benoit Cotreuil
Conception graphique : François Tugores

ISSN 2495-5078

Visitez notre site internet
www.interieur.gouv.fr/Interstats

Suivez-nous sur Twitter **@Interieur_stats**

Contact presse
ssmsi-communication@interieur.gouv.fr