Le décryptage

CYBERATTAQUE : LA MENACE PLANE

Les cyberattaques et les crises qu'elles impliquent sont de plus en plus courantes pour les entités publiques comme privées. Pour monter en capacité face à ces menaces, les organisations doivent s'organiser, maîtriser leur système d'information, mais aussi se préparer à une éventuelle crise à venir...

Rédaction **Jérémy Paradis**

Marseille, Angers, La Rochelle, l'hôpital de Villefranche-sur-Saône... Les cyberattaques ne cessent de se multiplier en France plongeant des collectivités et des institutions dans une situation de crise brutale pendant des semaines, voire des mois. En décembre dernier, ce sont les mairies de plusieurs villes de Seine-Saint-Denis qui ont été victimes d'une paralysie par rançon logiciel. Cette attaque, qui chiffre des données et réclame le paiement d'une importante rançon pour rétablir l'accès, a frappé les serveurs du Syndicat intercommunal d'informatique (SII) de Bobigny, dont dépendent plusieurs municipalités et organismes publics du département. Administration la plus exposée aux infrastructures contaminées, la mairie de Bobigny a dû débrancher son accès à internet pour tenter de limiter la propagation. À La Courneuve, ville moins impactée par l'attaque, « *nous n'avions plus aucun mail* », raconte Anthony Giunta, directeur général des services. Avant de pouvoir rallumer entièrement les serveurs, les autorités ont dû s'assurer que la menace avait été circonscrite et que les systèmes ne risquaient pas une nouvelle attaque aussitôt après.

Rien qu'en l'espace d'une année, pour la seule Seine-Saint-Denis, les villes de Bondy, Pantin et Villepinte ont précédemment fait état d'agressions informatiques d'ampleur affectant leur fonctionnement. « *Les collectivités territoriales ont des enjeux qui sont de plus en plus importants, nous gérons de grandes quantités de données, tant sur les salariés de la ville que sur nos habitants,* analyse Rached Zehou, conseiller municipal délégué à Bobigny, président du SII et par ailleurs ingénieur informatique spécialisé dans le déploiement d'infrastructures. L'État nous transfère de plus en plus de compétences, dit-il, ce qui demande plus de numérisation, sans que de l'autre côté les moyens pour se protéger suivent. »

255% D'ATTAQUES EN PLUS ENTRE 2019 ET 2020

Dans un récent rapport, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) notait une accélération des attaques au rançongiciel contre les collectivités locales. Entre 2019 et 2020, en France, leur nombre a augmenté de 255%. « *Ces attaques dites « Big Game Hunting »* visent des organisations aux activités critiques, note l'ANSSI. *Elles affectent leurs réseaux pour générer une interruption de leur activité avec des conséquences économiques, industrielles et sociales importantes : perte d'exploitation, exfiltration de données confidentielles pouvant affecter leur réputation ou des opérations de fusion et d'acquisition, etc.* »

Le ciblage des cybercriminels se caractérise par une préparation des opérations d'extorsion en amont, parfois plusieurs mois à l'avance et, de plus en plus fréquemment, par un chantage à la divulgation de données sensibles exfiltrées lors de la cyberattaque. Cette méthode qui consiste à annoncer publiquement l'attaque permet d'exercer une pression supplémentaire sur les victimes. En cas de refus d'obtempérer, les cybercriminels publient alors les informations sensibles volées. Dans d'autres cas, ils tentent de les vendre, parfois en les mettant aux enchères.

« *Certaines attaques par rançongiciel ne peuvent plus être reléguées au rang de simples attaques à but lucratif. En effet, leur sophistication, leur impact sur les données sensibles de la victime et la perte de continuité des activités les élèvent au niveau des attaques traditionnellement associées à des groupes d'attaquants*

1 MILLIARD

Soit la somme mobilisée par le gouvernement pour la Stratégie nationale pour la cybersécurité. Parmi les objectifs clés fixés à l'horizon 2025 :

Multiplier par trois le chiffre d'affaires de la filière (passant de 7,3 milliards à 25 milliards d'euros)

Positionner la France par rapport à la concurrence internationale en doublant notamment les emplois de la filière (passant de 37 000 à 75 000)

Structurer la filière et repositionner la France par rapport à la concurrence internationale en nombre d'entreprises

Faire émerger trois licornes françaises en cybersécurité en s'appuyant sur les grandes start-up du secteur, et notamment celles membres du French Tech 120

Diffuser une véritable culture de la cybersécurité dans les entreprises

Stimuler la recherche française en cyber et l'innovation industrielle (hausse de 20% des brevets)

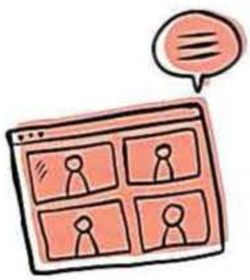
étatiques. Les rançongiciels peuvent en outre être utilisés pour d'autres motivations que l'extorsion financière, notamment à des fins de protestation, de déstabilisation, de sabotage ou d'espionnage informatique. »

3 JOURS, 3 SEMAINES, 3 MOIS FACE À LA CRISE

Face à une cyberattaque, que faire ? Premier réflexe, les spécialistes conseillent d'arrêter les machines ou de les couper du réseau pour tenter de freiner la propagation du virus de proche en proche. « *Au moment où l'on constate les premiers dégâts (...), on ne sait pas si le virus est encore en train de se propager dans le réseau ou bien si c'est déjà fini* », explique Robinson Delaugerre, cyberpompier d'Orange Cyberdéfense. Cette filiale de l'opérateur télécom intervient en urgence pour venir en aide aux institutions et aux entreprises touchées par une cyberattaque.
Après l'arrêt d'urgence, il faut ensuite rechercher les causes de l'infection, tout en montant une cellule de crise et en organisant la continuité de l'activité, parfois sans ordinateurs, sans courriels, sans téléphone... « *Nous parlons de la règle des 3X3*, explique Gérôme Billois, associé chez Wavestone, un cabinet de conseil qui dispose lui aussi d'équipes de cyberpompiers mobilisables à la demande. *Il y a trois jours de sidération, où tout le monde court partout, consomme une énergie folle... Puis trois semaines de gestion de crise* », ou les administrations fonctionnent avec « *du papier et des crayons* » et « *10, 15, 20%* » de leur activité informatique, remises en route après avoir nettoyé le réseau du virus.
Il faut souvent 3 mois pour arriver à retrouver une organisation adéquate, en remettant progressivement en route, par ordre de priorité, toutes les machines et applications, nettoyées des éléments d'infection. « *Nous avons dû formater 1 500 ordinateurs et réinitialiser 250 serveurs* », explique Arnaud Mabire, vice-président de la Communauté d'agglomération Évreux Portes de Normandie, frappée par un rançongiciel en décembre 2020. Selon lui, il a fallu « *un mois et demi* » pour retrouver un fonctionnement à peu près normal.
Quant au paiement de la rançon demandée par les pirates informatiques, l'ANSSI demande aux victimes de ne pas la payer, pour tenter de casser la rentabilité des attaques pour les pirates. « *L'ANSSI et l'écosystème français sont entièrement mobilisés* », assure Guillaume Poupard, Directeur général de l'ANSSI.

DES RÈGLES POUR MAXIMISER SA SÉCURITÉ

Pour lutter contre les cyberattaques, l'agence nationale de la sécurité des systèmes d'information livre dans son "Guide d'hygiène informatique" 42 règles permettant de maximiser la sécurité du système d'information, berceau des données de chaque entité. Véritable plan d'action, ce recueil incite les institutions publiques et privées à : sensibiliser et former leurs équipes ; connaître leur système d'information ; authentifier et contrôler les accès ; sécuriser les postes, le réseau et l'administration ; gérer le nomadisme (ordinateurs portables, tablettes) ; maintenir leur système d'information à jour. L'ANSSI incite aussi les administrations à se préparer à subir une attaque, un jour... « *On ne peut pas improviser des réponses en plein milieu d'une catastrophe !*, indique Guillaume Poupard, directeur général de l'ANSSI. *La préparation, l'outillage et l'entraînement sont indispensables pour maintenir l'activité en cas d'attaque informatique.* »



Pour aller plus loin

RETROUVEZ SUR WEKA.FR, LA WEBCONFÉRENCE « FACE AUX CYBERATTAQUES, COMMENT LES COLLECTIVITÉS TERRITORIALES ORGANISENT LA RIPOSTE ? », EN PARTENARIAT AVEC L'UGAP.

[illegible]

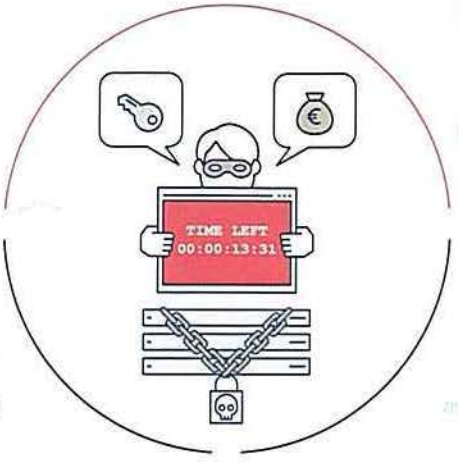
[illegible]

RANÇONGICIEL

Vos données sont prises en otage

QUE SE PASSE-T-IL ?

1. Vos données sont progressivement chiffrées, ce qui les rend inaccessibles



2. L'infection peut s'étendre à tous les appareils connectés au réseau ou aux supports USB branchés

3. On exige de vous le paiement d'une rançon pour récupérer ces données

Impact de l'attaque

Intégrité Authenticité Disponibilité

Motivations principales

Appât du gain Nuisance

COMMENT RÉAGIR ?

Vous êtes victime d'un rançongiciel – Ne payez pas !

1- Ne pas éteindre la machine concernée
La mettre en veille prolongée si possible

2- Déconnectez immédiatement les appareils du réseau

3- Ne connectez plus aucun appareil sur le réseau

4- Contactez immédiatement votre service informatique ou un expert (ou trouvez le vôtre sur cybermalveillance.gouv.fr)

5- Portez plainte auprès des services compétents

COMMENT SE PROTÉGER ?

Ne tombez pas dans le piège

Effectuez des sauvegardes régulières de vos données.

Mettez à jour régulièrement vos principaux logiciels
- Les rançongiciels utilisent les vulnérabilités des programmes pour se propager

Privilégiez un compte utilisateur pour vos usages courants

Courriers électroniques piégés
- Ne faites pas confiance à l'expéditeur de courriers électroniques dont l'origine ou la forme vous semblent douteuses
- Méfiez-vous des pièces jointes et des liens suspects

#CyberVigilant ! En savoir plus sur les attaques par rançongiciel :
https://www.cert.ssi.gouv.fr/information/CERTFR-2017-INF-001
https://www.cybermalveillance.gouv.fr/nos-articles/les-rancongiciels-ou-ransomware/

Les bonnes pratiques de l'informatique : www.ssi.gouv.fr/precautions-elementaires/
En savoir plus sur l'ANSSI : www.ssi.gouv.fr
En savoir plus sur Cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

V 4-20180119-1930