MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

Liberté
Égalité
Fraternité

Kit de sensibilisation aux risques cyber

-

Chaine vaccinale contre la COVID-19

Vous êtes victime d'une cyberattaque ?

Un point de contact unique

Le CERT-FR, centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, prendra en compte votre déclaration d'incident et sera en mesure, le cas échéant, de vous orienter directement vers les interlocuteurs adaptés à la résolution de votre incident.

Téléphone

+33 (0)1 71 75 84 68 : permanence 7j/7, 24h/24
+33 (0)1 84 82 40 70 : par télécopie

Mail : cert-fr.cossi@ssi.gouv.fr

Lien utile : https://www.cert.ssi.gouv.fr

Autres contacts utiles

1. ACSS

La cellule d'Accompagnement Cybersécurité des Structures de Santé (ACSS) peut apporter un appui aux structures de santé dans la gestion des incidents de sécurité des systèmes d'information.

En jours ouvrés de 9h à 18h

Contact : https://www.cyberveille-sante.gouv.fr/contact

2. Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est une plateforme d'assistance aux victimes de cybermalveillance, qui, à l'issue d'un parcours numérique de diagnostic de l'incident, les oriente vers des prestataires de sécurité et vers les services de polices spécialisés.

Plateforme numérique automatisée disponible 24/24, 7/7

Contact : https://www.cybermalveillance.gouv.fr

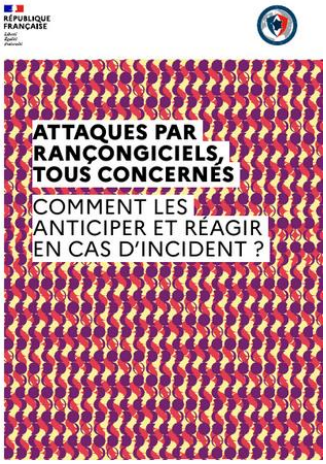
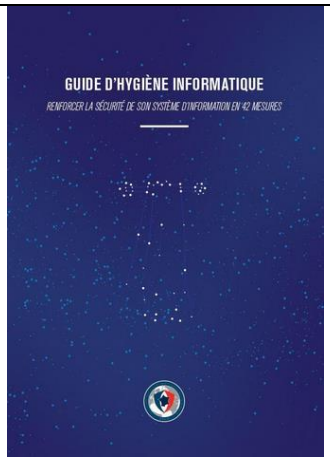
3. Prestataires qualifiés en réponse aux incidents de sécurité

Des prestataires spécialisés dans la réponse aux incidents informatiques existent et peuvent accompagner techniquement les victimes face à une cyberattaque. Certains d'entre eux se sont engagés dans une démarche de qualification par l'ANSSI, reconnaissance de leur savoir-faire en la matière.

Liste et contacts disponibles sur le site de l'ANSSI :
https://www.ssi.gouv.fr/entreprise/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris

Précautions à mettre en œuvre

1. Suivre les alertes et les bulletins du CERT-FR : **https://www.cert.ssi.gouv.fr**
2. Suivre les conseils disponibles sur le site de l'ANSSI :

Guide « rançongiciel »		Lien : https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-attaques_par_rancongiciels_tous_concernes-v1.0.pdf
Guide d'hygiène informatique		Lien : https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf
Maîtrise du risque numérique : l'atout confiance		Lien : https://www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-maitrise_risque_numerique-atout_confiance.pdf

Les bons réflexes à avoir en cas de cyberattaque

Déconnecter la machine du réseau

Déconnecter du réseau la machine compromise (ou les machines) permet de limiter la propagation de l'attaque si elle est toujours en cours. S'il était toujours connecté à la machine, l'intrus n'a plus de contrôle sur celle-ci et ne pourra donc pas surveiller ce que vous faites et/ou modifier des fichiers. En revanche, maintenez la machine sous tension et ne la redémarrez pas, car il serait alors impossible de connaître les processus qui étaient actifs au moment de l'intrusion. Vous risqueriez de provoquer une modification sur le système de fichiers et de perdre de l'information utile pour l'analyse de l'attaque.

Prévenir le responsable sécurité

Prévenez immédiatement le responsable sécurité et votre hiérarchie qu'un incident de sécurité a été détecté. Prévenez-les de préférence par téléphone ou de vive voix, car l'intrus est peut-être capable de lire les courriers électroniques échangés, depuis une autre machine du réseau.

Le responsable sécurité doit être clairement identifié par tous les administrateurs système/réseau avant que l'incident de sécurité ne soit déclaré. C'est la base de toute procédure de réaction sur incident de sécurité.

Prévenir le CERT-FR

- par courrier électronique : cert-fr.cossi@ssi.gouv.fr
- par téléphone : +33(0)1 71 75 84 68
- par fax : +33(0)1 84 82 40 70

Etat de la menace à l'encontre du secteur

1 Contexte

La distribution d'un vaccin efficace contre la Covid-19 est généralement jugée comme la solution la plus prometteuse à la pandémie. Bien que la durée de développement (de la conception à la mise sur le marché) d'un vaccin soit habituellement de l'ordre d'une dizaine d'années, les moyens exceptionnels mobilisés contre la Covid-19 devraient permettre l'arrivée d'un vaccin produit en masse en 2021. L'Union européenne abrite actuellement 27 sites de production qui fournissent 1,7 milliard de vaccins par an [1, 2]. En cas de production d'un vaccin contre la Covid-19, le nombre de doses à produire serait largement supérieur. La Commission européenne a ainsi annoncé des contrats d'achats anticipés de centaines de millions de vaccins auprès de plusieurs industriels, dont Sanofi-GSK [3].

Les candidats-vaccins actuellement en phase de tests cliniques utilisent de multiples approches thérapeutiques qui induisent des contraintes de production, de distribution et de financement distinctes ainsi qu'une variation des délais de mise en production industrielle. Certaines approches nécessitent un stockage du vaccin aux alentours de -60 °C. Il est ainsi généralement admis que plusieurs vaccins sont amenés à être produits en parallèle et que leurs administrations suivraient des procédures distinctes.

Près de 200 projets de vaccins sont actuellement en développement et certains sont portés par des structures (universités, centres de recherche...) ne disposant pas des infrastructures nécessaires à une production et une distribution à large échelle. Des entreprises de taille importantes sont également amenées à augmenter largement leurs capacités de production et de distribution : ainsi, les entreprises françaises Delpharm et Recipharm ont été sélectionnées pour des activités de conditionnement des vaccins de Pfizer/BioNTech et Moderna [4, 5]. D'autres entreprises françaises pourraient être amenées à avoir des rôles actifs dans la fourniture de vaccins sur le territoire national.

2 Principales menaces

L'importance des enjeux, notamment économiques et de souveraineté, et la concurrence entre différents acteurs pourraient augmenter le niveau des menaces pesant sur les moyens de production et de distribution en France d'un vaccin contre la Covid-19. L'industrie pharmaceutique reste également exposée aux menaces habituelles, notamment cybercriminelles.

Les entreprises du médicament font régulièrement l'objet de fusions-acquisitions. L'intégration des nouvelles structures dans le SI est complexe, régulièrement menée sans audits de sécurité et analyses des risques et les infrastructures qui en découlent présentent généralement des surfaces d'attaques importantes. La mise en place de partenariats, comme c'est le cas dans un grand nombre de projets concernant les vaccins contre la Covid-19, peut également conduire à des problématiques similaires si les infrastructures mises en place sont insuffisamment sécurisées.

2.1 Attaques par rançongiciel

Depuis 2018, l'ANSSI et ses partenaires observent une augmentation des attaques par des rançongiciels contre de grandes entreprises et institutions. Ces attaques, qui visent en particulier des organisations en raison de leur rentabilité ou de la criticité de leurs activités, sont connues en source ouverte sous le nom de « Big Game Hunting ». Elles impliquent généralement la présence d'une première charge ou des propagations manuelles et furtives des attaquants au sein des systèmes d'information (SI) afin de compromettre les ressources clés des institutions visées. Ces opérations peuvent durer moins de quelques heures [6] et se traduisent par des demandes de rançon qui peuvent se compter en dizaines de millions d'euros [7].

Pour réaliser ces compromissions, les attaquants peuvent se procurer des codes malveillants et des identifiants d'accès, parfois à hauts privilèges, sur le marché noir. Il est généralement hors de portée des opérateurs de réponse à incident de parvenir à casser les chiffrements utilisés en 2020.

Depuis 2019, l'ANSSI et ses partenaires observent une tendance nouvelle. Avant de déclencher le chiffrement, de nombreux attaquants procèdent à des exfiltrations de documents présents sur les SI de leurs victimes. Les attaquants disposent alors de moyens de pression supplémentaire sur les victimes en les menaçant de divulguer les informations extraites. L'impact de divulgations est traité plus largement en 2.3.

À l'instar d'autres secteurs d'activité, ces attaques ont affecté l'industrie pharmaceutique [8, 9, 10, 11]. Les contraintes inhérentes aux activités des entreprises pharmaceutiques peuvent en effet rendre ce type d'attaques particulièrement coûteuses. Les processus industriels de production de médicament et de vaccins peuvent être longs et ne pas supporter d'interruption. Une attaque informatique pourrait ainsi non seulement suspendre la production, mais également la compromettre.

De plus, un maintien en fonctionnement de l'appareil productif pourrait ne pas être suffisant. En effet, **une attaque informatique pourrait perturber fortement les capacités de suivi des opérations et de contrôle qualité, indispensables pour la mise sur le marché de produits pharmaceutiques**.

Certains opérateurs de rançongiciels ont annoncé en mars 2020 mettre en pause les attaques contre les entités en première ligne face à la Covid-19, comme les hôpitaux. Cependant l'industrie pharmaceutique a été explicitement exclue de ces engagements par certains des groupes [12].

En 2020, l'ANSSI a publié un état de la menace liée aux rançongiciels [13], et un guide détaillant les méthodes à adopter pour les anticiper et y réagir [14].

2.2 Attaques sur la chaîne d'approvisionnement

Comme de nombreux secteurs d'activité, la production de vaccins s'appuie sur de nombreux fournisseurs, prestataires et sous-traitants. Des attaques contre ces entités pourraient compromettre la production de vaccins. Il est également possible que des attaques ne ciblant pas spécifiquement les capacités de production vaccinales affectent des acteurs clés de la chaîne d'approvisionnement.

2.2.1 Fournisseurs de produits

La production de vaccins requiert divers composants ainsi que des consommables. Une mise en production à grande échelle d'un vaccin contre la Covid-19 en 2021 nécessitera une croissance très forte des capacités de production ce qui complique très fortement les capacités des industriels à mettre en place des stocks durables de produits. Une attaque informatique conduisant à l'interruption des livraisons depuis un fournisseur pourrait ainsi affecter rapidement toute la chaîne de production. De plus, si certains fournisseurs peuvent être substitués en cas d'attaque, ce n'est pas toujours le cas.

2.2.2 Fournisseurs de services

Les entreprises de services numériques (ESN) ont fait l'objet de multiples ciblages par des attaquants informatiques. Ces entreprises disposent en effet d'accès privilégiés auprès de leurs multiples clients. La compromission d'un ESN peut ainsi permettre à des attaquants de disposer d'accès auprès de nombreuses entités. Si les attaques à l'encontre de Cognizant et Capgemini en 2020 semblent ne pas avoir entraîné de compromissions de leurs clients, plus de 200 clients de Xefi ont été victimes d'un rançongiciel en janvier 2020 [15]. L'ANSSI a publié un rapport rapportant des attaques contre des entreprises de services en France en 2019 [16].

2.2.3 Stockage et distribution

Selon le type de vaccin mis en production, son stockage et sa distribution peuvent impliquer des contraintes logistiques importantes, notamment des chaînes de froid à des températures spécifiques. Un nombre limité de prestataires susceptible de fournir ces services et une attaque paralysant l'un d'entre eux pourrait fortement handicaper la distribution d'un vaccin. Un acteur majeur du stockage et de la distribution frigorifique aux États-Unis, Americold, a ainsi été victime d'une attaque informatique en novembre 2020 [17]. Cette attaque ne semble pas avoir causé d'interruption de la chaîne du froid, mais a contraint l'entreprise à suspendre stockage et déstockage. De plus, le 4 décembre 2020, IBM a rapporté [18] une campagne d'hameçonnage à l'encontre d'acteurs de la chaîne du froid, active depuis septembre 2020. L'absence d'intérêts économiques immédiats suggère selon IBM que cette

attaque a été mené dans un objectif de prépositionnement par un acteur étatique. Bien que l'infrastructure d'attaque utilisée soit peu discrète, aucun lien avec un groupe d'attaquants connu n'a pu être établi.

2.3 Divulgation d'informations exfiltrées

La vaccination est un sujet polémique. Certaines communautés sont ainsi farouchement opposées aux obligations vaccinales et un sondage récent indique que seuls 50 % des Français auraient l'intention de se faire vacciner contre la Covid-19 [19]. Ainsi, la divulgation de documents non publics, exfiltrés depuis un SI d'une entité impliquée dans le circuit de distribution du vaccin, pourrait être exploitée par des individus opposés à la vaccination. Même si les documents publiés ne démontrent pas de problèmes réels, un traitement partial des informations pourrait être réalisé à cette fin. La simple annonce de la compromission de l'entité pourrait suffire à étayer un discours de remise en cause de l'intégrité des éléments de suivi du vaccin.

De plus, la crédibilité et la popularité des gouvernements peuvent être fortement affectées par la perception de leurs capacités à gérer des crises. Des acteurs ayant un intérêt à déstabiliser le gouvernement actuel pourraient ainsi être tentés de mener des attaques afin de publier des informations embarrassantes concernant la gestion de la crise actuelle et en particulier concernant la gestion de la distribution d'un vaccin contre la Covid-19. La Russie a été accusée d'avoir mobilisé des unités de lutte informatique offensive (LIO) attribuées aux services de renseignement à cette fin en 2016 [20, 21].

Selon un article du journal britannique The Times [22], le GCHQ britannique aurait déployé des mesures de lutte contre la « propagande anti-vaccin par des états hostiles ».

2.4 Espionnage

Les phases préliminaires de recherche et développement des médicaments comprennent une quantité significative d'informations non publiques d'intérêt pour des adversaires. Néanmoins, les procédures d'autorisation de mise sur le marché conduisent à placer nombre de ces informations sous la protection de mécanismes de propriété intellectuelle plutôt que du secret. Cependant, les méthodes employées pour la mise en production à grande échelle peuvent, par exemple, constituer des avantages concurrentiels susceptibles d'attirer la convoitise.

En 2020, les modes opératoires des attaquants (MOA) *APT32* [23], *APT29/Wellmess* [24], *Lazarus* [25, 26] et *Ceriumv* [26] ont été associés à des attaques ayant ciblé l'industrie pharmaceutique. Selon Reuters [27], l'entreprise britannique AstraZeneca, dans les phases finales de développement de son vaccin, aurait fait l'objet d'un ciblage par un mode opératoire nord-coréen qui parait correspondre à *Lazarus*. D'autres attaques rapportées n'ont pas été attribuées à des modes opératoires spécifiques. Cependant, très peu d'informations sont disponibles concernant les données recherchées lors de ces attaques.

2.5 Sabotage

Les attaques par rançongiciel peuvent causer des pertes de données importantes et une compromission de la production. Elles se distinguent cependant des opérations de sabotage, qui visent à détruire durablement les moyens de production. Ces opérations sont rares et ont, jusqu'à présent, principalement touché le secteur de l'énergie. Les compétences requises pour mener à bien ce type d'opération semblent aujourd'hui principalement aux mains d'opérateurs disposant d'un soutien étatique. La révélation et l'attribution d'une telle activité auraient un impact fort et des répercussions à un niveau stratégique. Il semble ainsi plus probable que des pays disposant de ces moyens aient recours à des entraves réglementaires s'ils souhaitaient réellement favoriser des productions nationales. Il est cependant possible qu'une dissémination incontrôlée de codes malveillants conduise à un sabotage accidentel des moyens de production de vaccins Covid-19 en France.

3 Bibliographie

[1] VACCINES EUROPE. *The EU Vaccine Industry in Figures*. 10 fév. 2020. URL : https://www.vaccineseurope.eu/wp-content/uploads/2020/02/VE_Factsheet.pdf.

[2] LES ENTREPRISES DU MÉDICAMENT. *Où En Est l'industrie Du Vaccin ?* 24 juil. 2020. URL : https://www.leem.org/sites/default/files/questionpdf/ou-en-est-lindustrie-du-vaccin.pdf.

[3] COMMISSION EUROPÉENNE. *Le coronavirus et la stratégie de l'UE concernant les vaccins*. 24 sept. 2020. URL :https://ec.europa.eu/commission/presscorner/detail/fr/QANDA_20_1662.

[4] FRANCE BLEU. *Indre-et-Loire : le laboratoire Recipharm à Monts va produire en partie le vaccin Moderna*. 25 nov.2020. URL : https://www.francebleu.fr/infos/sante-sciences/monts-le-laboratoire-recipharmva-produire-en-partie-le-vaccin-moderna-1606312080.

[5] LE MONDE. *Dans l'Eure-et-Loir, Delpharm va mettre en flacon le vaccin Pfizer-BioNTech*. 27 nov. 2020. URL : https://www.lemonde.fr/economie/article/2020/11/27/a- saint- remy- sur- avre- delpharm-vamettre-en-flacon-le-vaccin-pfizer-biontech_6061337_3234.html.

[6] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES. *Ransomware Activity Targeting the Healthcare and Public Health Sector (Update 2)*. 16 nov. 2020. URL : https://www.aha.org/system/files/media/file/2020/11/Healthcare%20and%20Public%20Health%20Sector%20Notification.pdf.

[7] BLEEPING COMPUTER. *How Ryuk Ransomware Operators Made $34 Million from One Victim*. 7 nov. 2020. URL :https://www.bleepingcomputer.com/news/security/how- ryuk- ransomware- operators-made- 34-million-from-one-victim/.

[8] INFOSECURITY MAGAZINE. *Pharma Giant ExecuPharm Suffers Data Breach/Ransomware Combo*. 29 avr. 2020.URL : https://www.infosecurity-magazine.com:443/news/execupharm-suffers-data/.

[9] LABIOTECH.EU. *Biotech Startups Face a Growing Wave of Cyberattacks*. 21 oct. 2020. URL : https : / / www labiotech.eu/regulatory/cyberattack-biotech-startups-covid/.

[10] LEMONDEINFORMATIQUE. *NotPetya : Merck bataille avec les assureurs pour 1,3 Md $ d'indemnisation*. 10 déc.2019. URL : https : / / www . lemondeinformatique . fr / actualites / lire - notpetya - merck - bataille - avec-les-assureurs-pour-1-3-md-$-d-indemnisation-77363.html.

[11] *Dr. Reddy's Laboratories Shuts Units after Cyber Attack*. 22 oct. 2020. URL : https : / / www . thehindu . com /business/Industry/dr-reddy-laboratories-shuts-units-after-cyber-attack/article32916400.ece.

[12] BLEEPING COMPUTER. *Ransomware Gangs to Stop Attacking Health Orgs During Pandemic*. 18 mar. 2020. URL : https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-healthorgs-during-pandemic/.

[13] ANSSI/CERT-FR. *État de La Menace Rançongiciel à l'encontre Des Entreprises et Institutions*. 5 fév. 2020. URL : https://cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001/.

[14] ANSSI. *Publication : Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ?* 1er août 2020. URL : https://www.ssi.gouv.fr/guide/attaques- par- rancongiciels-tousconcernes-comment-les-anticiper-et-reagir-en-cas-dincident/.

[15] CHANNELNEWS. *Des clients de Xefi attaqués par un cryptolocker*. 19 fév. 2020. URL : https://www.channelnews.fr/des-clients-de-xefi-attaques-par-un-cryptolocker-94901.

[16] CERT-FR. *Supply Chain Attacks : Menaces Sur Les Prestataires de Service et Les Bureaux d'études*. 7 oct. 2019. URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-004/.

[17] BLEEPING COMPUTER. *Cold Storage Giant Americold Hit by Cyberattack, Services Impacted*. 16 nov. 2020. URL :https : / / www . bleepingcomputer . com / news / security / cold - storage - giant - americold - hit - by -cyberattack-services-impacted/.

[18] IBM SECURITY INTELLIGENCE. *IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain*. 3 déc. 2020. URL : https://securityintelligence.com/posts/ibm-uncovers-global-phishingcovid-19-vaccine-cold-chain/.

[19]FRANCEINFO. *Covid-19 : un Français sur deux affirme qu'il ne se fera pas vacciner, 15% des personnes interrogées refusent tout vaccin, selon notre sondage*. 12 nov. 2020. URL : https://www.francetvinfo.fr/sante/maladie/coronavirus/vaccin/covid-19-un-francais-sur-deux-affirme-qu-il-ne-se-fera-pas-vacciner-15-des-personnes-interrogees-refusent-tout-vaccin-selon-notre-sondage_4178633.html.

[20] LE MONDE. *Les preuves de l'ingérence russe dans la campagne de Macron en 2017*. 6 déc. 2019. URL : https://www.lemonde.fr/pixels/article/2019/12/06/macronleaks-des-hackeurs-d-etat-russes-ontbien-vise-la-campagne-presidentielle-de-2017_6021987_4408996.html.

[21] Robert MUELLER. *Report On the Investigation into Russian Interference in the 2016 Presidential Election*. 1er mar.2019. URL : https://www.justice.gov/storage/report.pdf.

[22] THE TIMES. *GCHQ in Cyberwar on Anti-Vaccine Propaganda*. 9 nov. 2020. URL : https://www.thetimes.co.uk/article/gchq-in-cyberwar-on-anti-vaccine-propaganda-mcjgjhmb2.

[23] FIREEYE. *Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage*. 22 avr. 2020. URL : https://projets.ops.fr/issues/1031243.

[24] NCSC-UK. *Advisory : APT29 Targets COVID-19 Vaccine Development*. 16 juil. 2020. URL : https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf.

[25] [TLP:AMBER] CISA. *North Korean Cyber Actors Targeting Vaccine and Virology Organizations*. 5 nov. 2020.

[26] MICROSOFT. *Cyberattacks Targeting Health Care Must Stop*. 13 nov. 2020. URL : https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/.

[27] REUTERS. *Exclusive : Suspected North Korean Hackers Targeted COVID Vaccine Maker AstraZeneca*. 27 nov.2020. URL : https : / / www . reuters . com / article / us - healthcare - coronavirus - astrazeneca - no -idUSKBN2871A2.