Visioconférence Organisée par

CONSEIL SUPÉRIEUR DU NOTARIAT

ASSOCIATION DU NOTARIAT FRANCOPHONE

IDEI

Dalloz IP / IT

Quelle est l'influence de la COVID-19 sur la Cybercriminalité ?

« Aspect Justice »

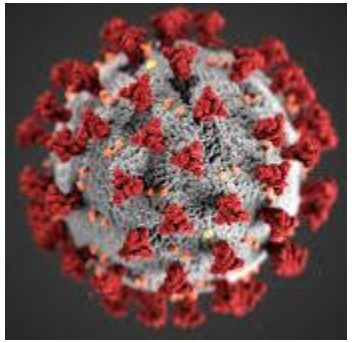
1er décembre 2020

Jacques MARTINON

Chef de la mission de lutte contre la cybercriminalité

Direction des affaires criminelles et des grâces (DACG)

Ministère de la Justice



Plan de la présentation

1. L’hameçonnage aux couleurs de la COVID 19
2. Rançongiciels & Hôpitaux : le dilemme du cybercriminel
3. Un soupçon de cyberespionnage…
4. Une pincée de cyberescroqueries (matériel contrefaits…)
5. La face cachée du télétravail, possible vecteur d’attaque

Introduction – Organisation judiciaire Cyber

- Le **parquet de Paris** contient une **section spécialisée à la lutte contre la cybercriminalité (J3)**, faisant partie de la JUNALCO (Juridiction nationale de lutte contre la criminalité organisée).
- Cette section J3 bénéficie d'une **compétence nationale concurrente en matière d'infractions STAD et de sabotage informatique** depuis 2016.
- La direction des affaires criminelles et des grâces produit régulièrement des **dépêches de politique pénale en matière de cybercriminalité**, notamment pour centraliser certains phénomènes, comme par exemple les rançongiciels (cf infra).
- De manière générale, les affaires de cybercriminalité les plus complexes ont vocation à être traitées par la section spécialisée du parquet de Paris.
- A l'échelon local, toutes les juridictions ont désigné depuis 2019 un **magistrat cyberréférent**, afin de relayer la politique pénale et assurer un dialogue de qualité avec la section J3 (et les JIRS) afin qu'elle envisage sa saisine.

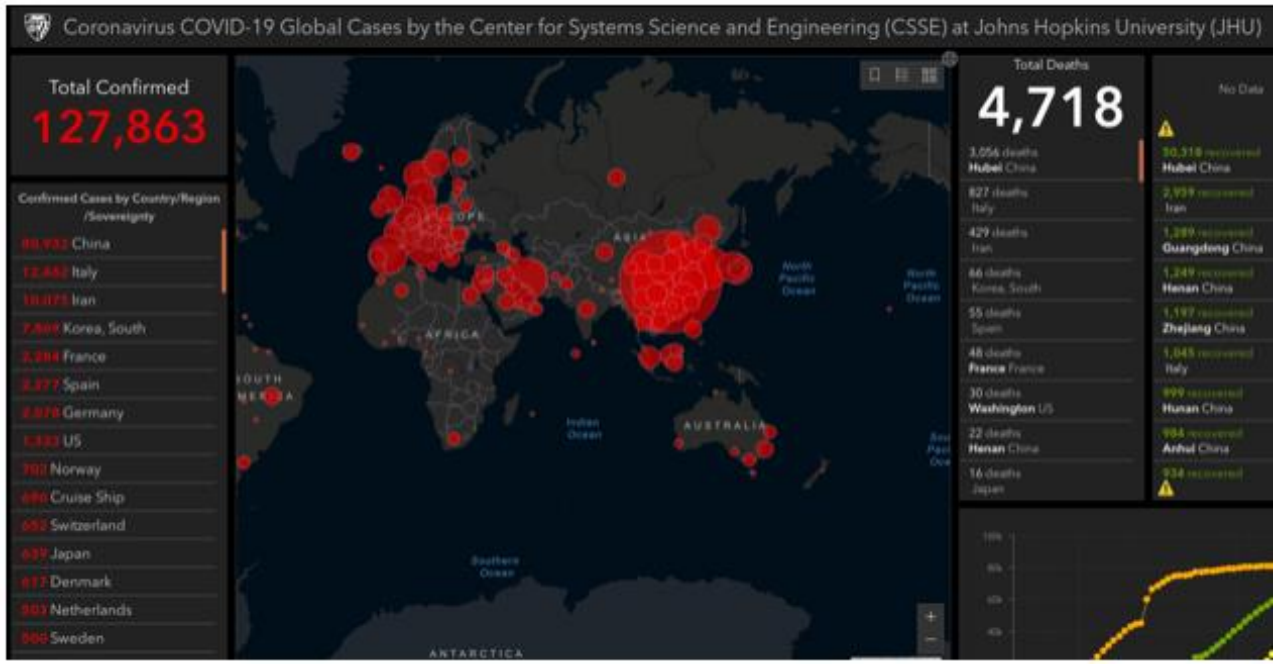
Quelques caractéristiques de l'enquête Cyber

- Le recours quasi systématique à des services d'enquête spécialisés : OCLCTIC, C3N, BEFTI, DGSI..
- La grande fréquence des demandes d'entraides pénales internationales (DEPI) pour obtenir la preuve numérique (avec des demandes de gel si Convention de Budapest applicable)
- Le recours aux perquisitions de DataCenter en France est souvent nécessaire (pour les enquêtes FR, mais aussi pour de nombreuses enquêtes internationales…).
- Le partage d'information et l'appui d'EUROPOL et d'EUROJUST sont fondamentaux.
- Les auteurs sont parfois très jeunes et primo-délinquants… Les quanta de peine devront naturellement augmenter avec les jugements futurs de cybercriminels chevronnés (message judiciaire de dissuasion). Les cybercriminels sont souvent mobiles et peuvent se faire attraper avec des mandats d'arrêt internationaux.
- Très peu d'informations judiciaires ouvertes, la plupart des procédures restent en enquêtes préliminaires à la section J3 (sauf nécessité de détention provisoire par exemple). En effet, le parquet peut obtenir du JLD la plupart des techniques spéciales d'enquête.

1. L'hameçonnage aux couleurs de la COVID 19

- **<u>Par de faux sites</u>** : début mars 2020, l'entreprise CheckPoint a établi que plus de 4 000 sites internet liés au nouveau coronavirus avaient été créés. Selon elle, 3 % d'entre eux étaient malveillants et 5 % seraient *« suspects »*, possiblement liés à des fins d'hameçonnage, dans le but d'extorquer des informations personnelles en se faisant passer pour un site légitime. Ex : faux site de l'OMS ou des sites reproduisant la carte de l'université Johns-Hopkins de Baltimore sur la propagation du coronavirus contenant un virus volant les mots de passe (kit de fabrication en vente sur un forum de cybercriminels).

Alerte cybersécurité : un faux site de l'OMS utilisé pour des opérations de phishing



Une initiative originale et internationale

- Afin de tenter de limiter les incidents cyber, l'initiative de la **Covid-19 Cyber Threat Coalition** est à relever. Animé par une communauté de volontaires, ce groupement à but non lucratif a identifié depuis sa création fin mars 2020 plus de 26 000 cybermenaces liées au coronavirus, comprenant 13 863 URL malveillantes déjà identifiées comme ayant été utilisées dans des attaques, ainsi que 12 258 domaines et noms d'hôtes frauduleux.

L’hameçonnage par courriel (non ciblé - Botnet)

- L'entreprise de cybersécurité *Bitdefender* qui protège plus de 500 millions de systèmes dans le monde, estime que **près de 40% des courriels traitant de la Covid-2019 sont frauduleux ou malveillants**..- Bitdefender

➢ Le Botnet EMOTET tente de piéger ses nouvelles victimes en les incitant à activer des macros malveillantes dans des fichiers de la suite Office, souvent Word et Excel. Placés en pièces jointes, ils prennent notamment la forme **d'alerte Covid-19**.

➢ Selon des chercheurs en sécurité de *Cisco Talos*, un accroissement des compromissions par le Botnet **Lemon Duck** a été constaté depuis la fin du mois d'août. L'infection est initiée notamment par des **courriels d'hameçonnage émis de systèmes précédemment infectés, relayant de prétendues informations sur la COVID-19 et adresse automatiquement tous les contacts du carnet d'adresses de la victime**.

L’hameçonnage ciblée (Spear Phishing) surfe sur la Covid

- Le groupe *Phosphorus,* **potentiellement iranien**, également connu sous les noms de ***APT35***, *Charming Kitten*, *Newscaster* ou *Ajax Security Team*, aurait ciblé des futurs participants à la conférence de Munich sur la sécurité et le sommet Think20 (T20) prévu en Arabie Saoudite. Les équipes de sécurité de *Microsoft* ont découvert la vaste campagne d'hameçonnage. **Les attaquants se seraient fait passer pour des organisateurs de conférences**, dans un anglais quasi parfait, en ciblant notamment une centaine d'anciens ambassadeurs, des experts politiques ou encore des universitaires. **Ils auraient ensuite exploité le prétexte de la pandémie de Covid-19 pour proposer des sessions de discussions à distance.** En conséquence ils auraient eu accès à une centaine de boites courriels, dans ce qui semble être une campagne de renseignement sur des cibles précises, afin d'exfiltrer les données de messageries ainsi que des listes de contacts - IT Security News, Security Affairs

Les smartphones ne sont pas à l'abri…

- Depuis le début de la pandémie de la COVID 19, les **campagnes d'hameçonnage par SMS seraient en forte hausse**. Les liens malveillants contenus dans ces derniers entraînent souvent l'installation d'applications malveillantes. Parmi elles, de **fausses applications de géolocalisation de personnes positives au virus de la COVID 19, téléchargées massivement entre mars et avril dernier.** Ces applications ont été utilisées pour diffuser des espiogiciels et des rançongiciels sur les machines utilisant le système d'exploitation **Android**. - Digital Shadows

2. Rançongiciels & Hôpitaux : le dilemme du cybercriminel ?

- En France, d'après la section J3 **une dizaine d'établissements de soin ont été touchés par des rançongiciels**. On se souvient de l'exemple célèbre du CHU ROUEN, antérieur à la COVID 19 en novembre 2019, frappé par le logiciel **CLOP** avec une rançon de 40 bitcoins, soit 300 000 euros. L'ANSSI évoquait le **groupe russophone TA 505**. Les soignants sont retournés pendant un temps au papier et stylo. De plus, le matériel médical est de plus en plus connecté donc aussi exposé.
- Au-delà des établissement de soin, on notera aussi que le rançongiciel ayant frappé la **mairie de Marseille** en mars 2020 (Pysa) a **bloqué pendant des semaines la remontée les chiffres de décès du Covid-19**.
- A l'étranger, selon le site des opérateurs du rançongiciel ***Mount Locker***, la société *Miltenyi Biotec* s'est fait volé 150 Go de données, en plus du chiffrement de leur infrastructure. À noter que *Miltenyi Biotec* fournit **des antigènes pour la recherche sur la COVID-19**.
- L'éditeur de logiciel spécialisé dans le secteur de la santé eResearchTechnology a également été victime d'une attaque par rançongiciel. **Cette attaque a perturbé des essais cliniques en lien avec la pandémie du Covid-19.**
- Enfin, **l'université de Californie à San Francisco a déboursé l'équivalent de 1.14 millions de dollars pour déchiffrer ses données relatives à la recherche sur le COVID-19.**

Des rançonneurs plus « éthiques » que d'autres ?

- En 2017, le ransomware Wannacry a verrouillé des milliers d'ordinateurs dans une attaque d'envergure mondiale, le dysfonctionnent du réseau du service national de santé de l'Angleterre – NHS pour National Health Service a impacté fortement ***25 à 30 entités hospitalières.***
- Pourtant **depuis 2016, la question fait débat chez les cybercriminels** (attaque d'un hôpital à Los Angeles, rançon initiale de 3,6 millions de dollars, ramené à 17 000 dollars). Code éthique ? Crainte d'une **sanction pénale bien plus lourde ? En Allemagne, une femme serait décédée** faute à une prise en charge rapide (dysfonctionnement provoqué par un rançongiciel).
- Communiqué des auteurs du ransomware Maze qui ***promet de ne pas attaquer les hôpitaux en pleine pandémie (en plus de « discounts » pour les organisations commerciales)***. **A l'inverse, le ransomware Ryuk est particulièrement actif sur les établissements de soins** (source Checkpoint). **Les tentatives de rançongiciels auraient augmenté de 50% au niveau mondial au premier semestre 2020.**

Exemple de prévention aux personnels de santé
(communiqué de l'Agence du numérique en Santé)

LE CORONAVIRUS EST UTILISÉ POUR RÉALISER DES CYBERATTAQUES

Différents messages d'information sur le Covid-19 nous ont été signalés. Il s'agit en réalité de virus informatiques. Via de faux e-mails des autorités de santé, de fausses notes internes en entreprise ou encore de fausses alertes de retard de livraison, les cybercriminels tentent dans le monde entier d'exploiter la peur liée à la pandémie pour s'infiltrer sur les réseaux informatiques des entreprises et des particuliers.

Il est à signaler que l'Organisation mondiale de la santé (OMS) est récemment sortie de son rôle pour parler de cybersécurité, en mettant en garde contre les fraudeurs qui se font passer pour elle. Elle recommande de ne pas cliquer directement sur les liens présents dans ses e-mails mais de se rendre directement sur son site web, de ne jamais transmettre un mot de passe pour avoir accès à des informations publiques et de vérifier l'adresse e-mail de l'expéditeur. Il est réaliste de penser que d'autres types d'attaques peuvent avoir lieu.

En conséquence il est demandé de surveiller de près tout élément anormal sur vos systèmes d'information et, le cas échéant de faire un signalement immédiat. Il est également demandé de vérifier le bon fonctionnement de vos sauvegardes. Enfin, sensibiliser l'ensemble des personnels. **Il convient en effet de ne pas cliquer sans vérification préalable sur les liens de messages et les pièces jointes.** Les utilisateurs ne doivent pas ouvrir de messages électroniques de provenance inconnue, d'apparence inhabituelle ou frauduleuse.

La menace incertaine des Attaques en déni de service

L'AP-HP visée par une attaque DDoS

Sécurité : *Dimanche matin, l'AP-HP a été visée par une attaque DDoS qui l'a conduit à restreindre l'accès à ses services pendant plus d'une heure. L'hôpital indique que cette attaque n'a pas perturbé son fonctionnement.*

Dimanche 22 mars 2020, une attaque par déni de service (connexion massive) a touché l'AP-HP sur deux de ses adresses internet. L'attaque qui a duré une heure a été gérée par le prestataire de l'AP-HP et n'a jamais atteint ses infrastructures ». L'AP-HP indique que le prestataire « a diminué les accès internet, ce qui a eu pour **conséquence de bloquer l'accès externe à la messagerie, à Skype ainsi que l'accès externe aux applications de l'AP-HP** ».

L'Anssi précise d'ailleurs auprès de l'AFP que « *l'incident a été géré rapidement et efficacement par les équipes de l'AP-HP, sans impact critique* ». **Une attaque DDoS comme celle ayant visé l'hôpital dimanche est d'une gravité moindre, mais les dysfonctionnements causés par ce type d'attaques peuvent venir perturber des établissements de santé déjà mis sous tension du fait de la crise sanitaire en cours.**

3. Un soupçon de cyberespionnage…

Ex : Démenti de la Russie au sujet des accusations de cyberespionnage concernant les développeurs de vaccins contre la Covid-19

Mi-novembre, *Microsoft* assurait avoir mis en lumière une **vaste campagne de cyberespionnage de groupes russes et nord-coréens à l'encontre de sociétés travaillant au développement d'un vaccin contre le virus Covid-19**. Le vice-ministre russe des Affaires Étrangères Sergei Ryabkov a démenti l'implication de Moscou dans une telle campagne. Technology Inquirer

En effet, selon *Microsoft*, les entités ciblées sont essentiellement localisées aux États-Unis, au Canada, en Inde, **en France** et en Corée du Sud et travaillent activement à développer un vaccin contre le virus Covid-19. Les équipes du géant de la technologie ont en partie détecté le groupe *APT28* (alias *Fancy Bear*, *Sednit*, *Sofacy*, *Sandworm* et *Strontium*), réputé parrainé par la Russie. Ce groupe a tenté de forcer des mots de passe et des connexions par force brute en réalisant des millions de tentatives par connexion rapide.

Deux autres groupes réputés **nord-coréens**, *Zinc* et *Cerium*, ont lancé de vaste campagnes d'hameçonnage. *Zinc* a principalement utilisé des leurres pour le vol d'authentifiants, via des courriels avec de fausses offres d'emploi. *Cerium* a quant à lui utilisé les thèmes Covid-19 aux couleurs de l'Organisation Mondiale de la Santé (OMS). La majorité de ces attaques ont été bloquées par les protections de sécurité intégrées. Microsoft

4. Une pincée de cyberescroqueries (matériel potentiellement contrefaits…)

- Selon EUROPOL, la contrefaçon de produits sanitaires et médicaux était particulièrement active pendant la première vague. On peut citer comme exemple :

➢ Un groupe Facebook pour des achats de masque ;

➢ Une personne vendant des kits de test COVID19 sur Snapchat 60€ l'unité ;

➢ 10 sites (dont 6 sur les Darknets) offrant des masques, du materiel de protection, et de la Chloroquine et autres médicaments

5. La face cachée du télétravail, possible vecteur d'attaque

- La sensibilisation des salariés et des entreprises/administrations est essentielle !
- Amélioration de la cybersécurité des outils de visio (Ex : chiffrement de bout en bout dans Zoom)
- Renvoi aux excellents conseils prodigués par le site cybermalveillance.gouv.fr : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite ;
- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

Les « gestes barrières numériques »

Méfiez-vous des messages (mail, SMS, chat…) **ou appels téléphoniques d'origine inconnue ou inattendus** :
Face à ce type de messages, ne cliquez pas sur les liens, n'ouvrez pas les pièces-jointes et en cas de doute, confirmez en contactant directement l'organisme qui prétend vous l'avoir envoyé.

Ne téléchargez vos applications que depuis les sites ou magasins officiels des éditeurs

Vérifier la fiabilité et la réputation des sites que vous visitez

Avec la crise du CORONAVIRUS – COVID19 on voit fleurir de faux sites de ventes de masque chirurgical (FFP2), de gel hydroalcoolique, de téléconsultation médiale, de médicaments miracles ou de vaccins expérimentaux qui n'existent évidemment pas et qui n'ont d'autres objectifs que de vous escroquer. Les cybercriminels pourraient même vous livrer des produits périmés ou contrefaits qui mettraient en danger votre santé ou celle de vos proches.

Conclusion

- La crise sanitaire pousse la population à accélérer son usage du numérique, que ce soit dans la vie personnelle et professionnelle. Cet usage n’est pas sans danger et les cybercriminels font feu de tout bois.
- Une société moderne résiliente doit avoir des fondamentaux de cybersécurité solides, et toute lacune sera chèrement payée.
- La justice spécialisée en cybercriminalité devrait idéalement être renforcée pour suivre cette évolution naturelle.