club
open
prospective

new normal au **next** normal

Depuis la crise sanitaire un nouveau rapport au monde émerge

Plus local, Plus numérique, Plus green

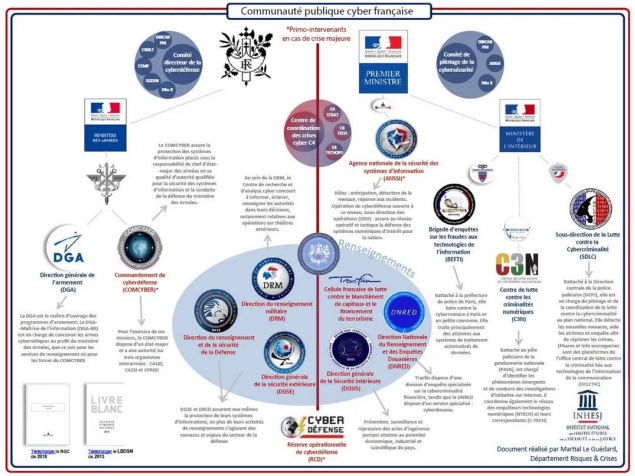
Mais moins Sécurisé Digitalement parlant

Sommaire

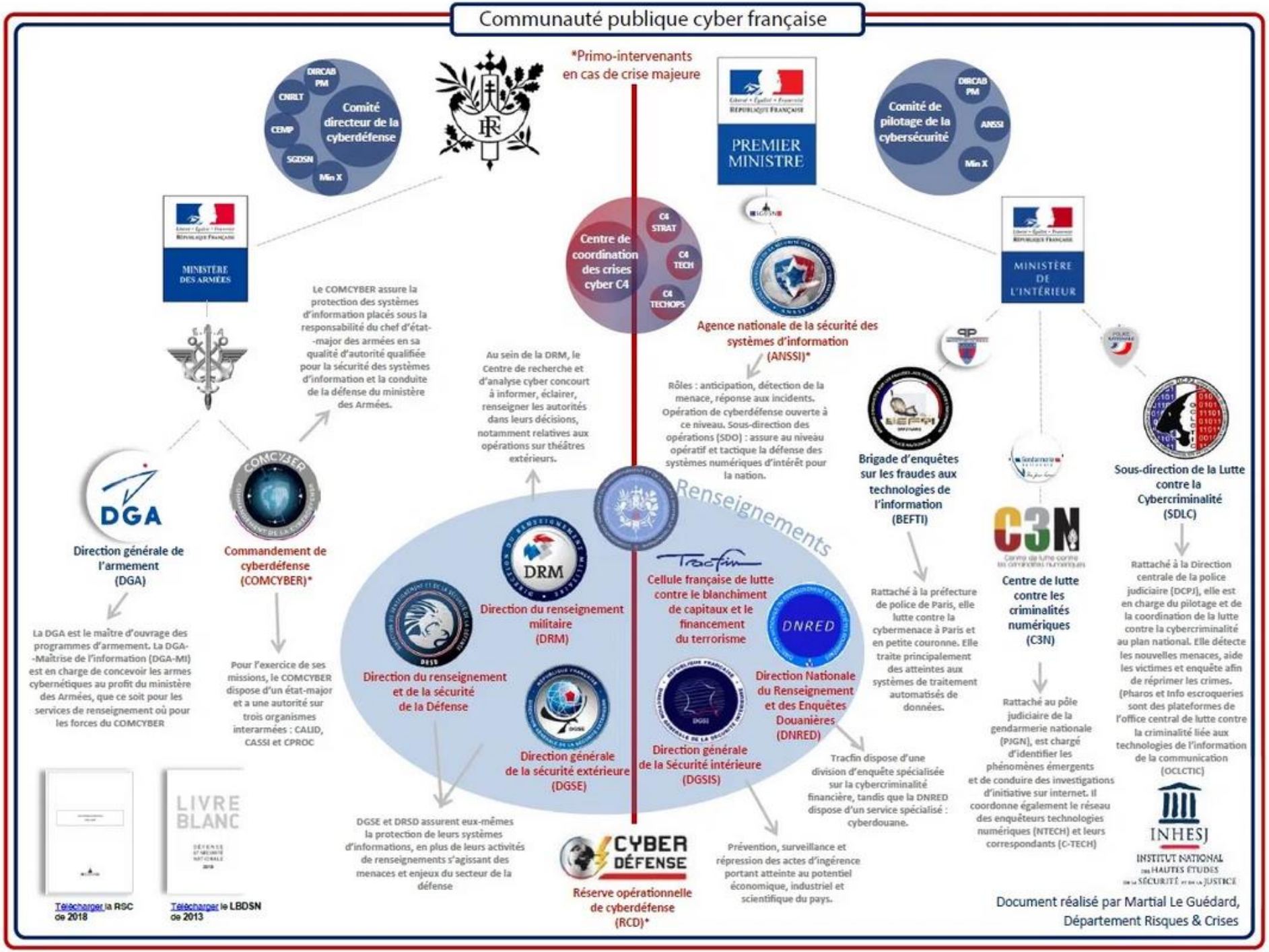
1. Cybersécurité & Cybercriminalité
2. Monde de la Cybercriminalité & des attaques
3. Effet de la Cybercriminalité & Cybersécurité face au COVID
4. Quels Scénarios et parades envisageables
5. Risques d’une Pandémie Numérique
6. Annexes

Cybersécurité & Cybercriminalité

- Cyber d'origine grec *Kubernêtikê* signifiant « gouvernail »
- Cybersécurité :
  - Ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise, de personne. C'est aussi un ensemble de lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, de gestion des risques, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger
  - La cybersécurité doit permettre de déjouer les attaques
- Cybercriminalité :
  - Toutes infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication – principalement internet
  - Ecosystème très complexe ou se retrouve de nombreux acteurs allant du Loup Solitaire à des organisations étatiques voire des groupes de terroristes

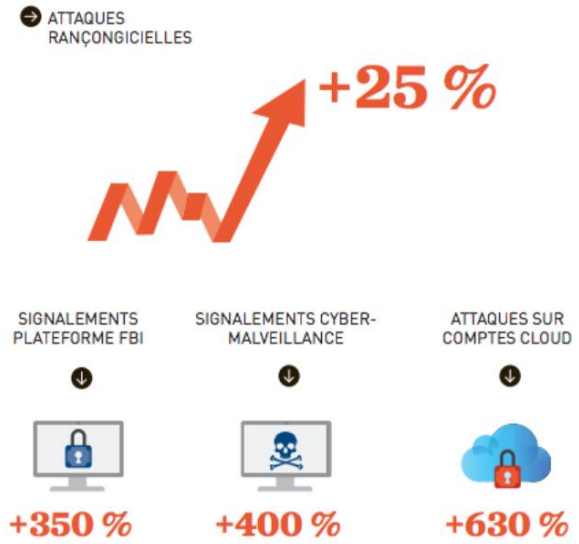


Ecosystème complexe en France pour limiter les risques et contrer les assaillants



L'état de la menace cyber en quelques chiffres

- 76 % des dirigeants d'ETI déclarent avoir subi au moins une incidence cyber en 2019
- 90 % des entreprises françaises ont été victimes de cyber-attaques en 1 an
- 12 % des entreprises ont connu des attaques par rançongiciel
- 80 % des entreprises françaises n'ont pas de plan de réponse aux incidents robustes
- 86 % des entreprises sondées n'ont toujours pas souscrit de contrat cyber-assurance
- + de 1 100 victimes d'attaques par rançongiciel en France depuis début 2020 (dont 26 % de particuliers)
- 5 200 milliards de dollars : coût de la cybercriminalité, estimé par l'ONU, pour l'économie mondiale entre 2020 et 2025
- Industries les plus attaquées en 2020 :
  - Banques : 78%
  - Santé : 73%
  - Gouvernement : 43%



Source : CESIN

Quels sont les typologies d'attaquants

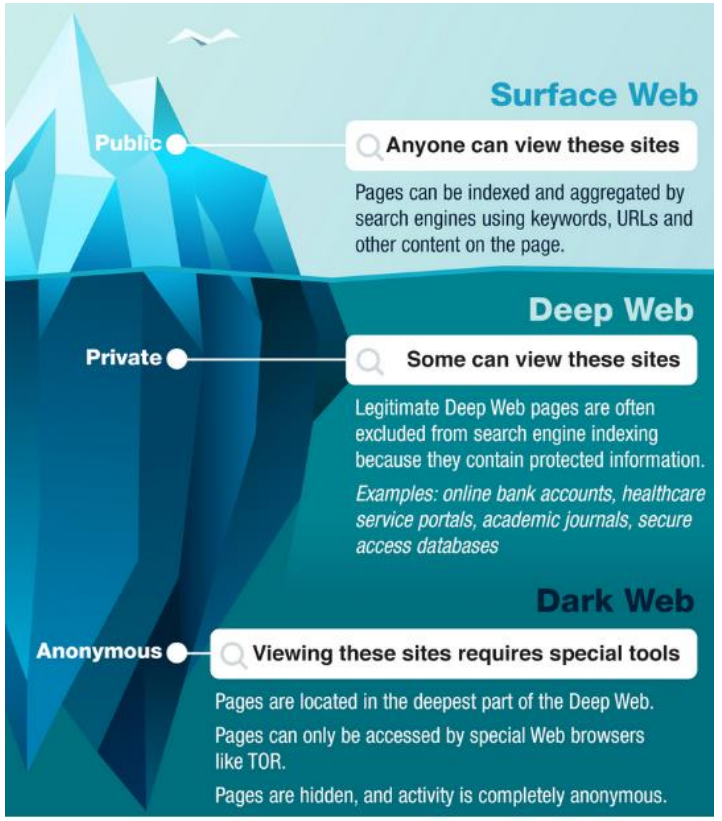
- Les Hackers (Hacktivistes)
  - Types : joueurs, Ideologues, Communauté, Lanceur d'alertes, Destructeurs d'image / Notoriété
  - Cibles : Gouvernement, Education, Médecine, Energie, Transport, Aerospatiale
- Les Cybercriminels
  - Types : Voleur (Appat du gain),
  - Cibles : Finance, Commerce, Distribution
- Les Cyberterroristes
  - Types : Prosélytisme, Terroristes, Destructeur de données
  - Cibles : Défense, Gouvernement, Médias
- Attaquants issus d'états (APT – Etats Nations)
  - Types : Cyber-espionnage, Déstabilisation politique, sabotage
  - Cibles : Défense, Gouvernement, OIV Stratégiques

Mode opératoire

1. **Pénétrer le réseau**
2. **Exécuter un code malveillant**
3. **Masquer ses positions**
4. **Accéder au bon niveau d'administration**
5. **Récupérer les identifiants et môts de passe**
6. **Rester indétectable**
7. **Comprendre l'écosystème SI**
8. **Se déplacer & analyser le SI**
9. **Collecter les informations pertinentes**
10. **Exfiltrer des données**
11. **Bloquer voire détruire des applications**

Dark web / web clandestin / web caché

- Contenu de réseaux superposés qui utilisent l'internet public, mais qui sont seulement accessibles via des logiciels, des configurations ou des protocoles spécifiques.
- Les *darknets* hébergent le *dark web* incluent des réseaux ami-à-ami de pair à pair, ainsi que de grands réseaux populaires tels que *Freenet, I2P* et *Tor*, qui sont gérés par des organisations publiques et des individus.
- Services de TOR : + 76 000 sites (fin 2020)
  - Moteur de recherche
  - Sites Commerciaux
  - Sites de communications (Mail, Réseaux, FAI, …)
  - Sites hébergeur Web
  - Sites Financiers
  - Système d'exploitation
  - Sites de Publication
  - Sites d'archivage
  - Portails
  - Medias sociaux
  - Associations
  - …



- Freedom of the Press Foundation
- La Quadrature du Net
- Telecomix

FREEDOM OF THE PRESS FOUNDATION

Rappel des types d'attaques Cyber durant les années 2010

V·T·E	Hacking in the 2010s	[hide]
← 2000s	Timeline	2020s →
Major incidents	2010	Operation Aurora · Australian cyberattacks · Operation ShadowNet · Operation Payback
	2011	DigiNotar · DNSChanger · HBGary Federal · Operation AntiSec · Operation Tunisia · PlayStation · RSA SecurID compromise
	2012	LinkedIn hack · Stratfor email leak · Operation High Roller
	2013	South Korea cyberattack · Snapchat hack · Cyberterrorism Attack of June 25 · 2013 Yahoo! data breach · Singapore cyberattacks
	2014	Anthem medical data breach · Operation Tovar · iCloud leaks of celebrity photos · 2014 JPMorgan Chase data breach · Sony Pictures hack · Russian hacker password theft · 2014 Yahoo! data breach
	2015	Office of Personnel Management data breach · Hacking Team · Ashley Madison data breach · VTech data breach · Ukrainian Power Grid Cyberattack · SWIFT banking hack
	2016	Bangladesh Bank robbery · Hollywood Presbyterian Medical Center ransomware incident · Commission on Elections data breach · Democratic National Committee cyber attacks · Vietnam Airport Hacks · DCCC cyber attacks · Indian Bank data breaches · Surkov leaks · Dyn cyberattack · Russian interference in the 2016 U.S. elections
	2017	2017 Macron e-mail leaks · WannaCry ransomware attack · Westminster cyberattack · Petya cyberattack (2017 cyberattacks on Ukraine) · Equifax data breach · Deloitte breach · Disqus breach
	2018	Trustico · Atlanta cyberattack · SingHealth data breach
	2019	Sri Lanka cyberattack · Baltimore ransomware attack · 2019 Bulgarian revenue agency hack
Groups	Hacktivism	Anonymous (associated events) · CyberBerkut · GNAA · Goatse Security · Lizard Squad · LulzRaft · LulzSec · New World Hackers · NullCrew · OurMine · PayPal 14 · RedHack · TeaMp0isoN · UGNazi
	Advanced Persistent Threat	Bureau 121 · Charming Kitten · Cozy Bear · Dark Basin · Elfin Team · Equation Group · Fancy Bear · Guccifer 2.0 · Hacking Team · Helix Kitten · Iranian Cyber Army · Lazarus Group (BlueNorOff) (AndAriel) · NSO Group · PLA Unit 61398 · PLA Unit 61486 · PLATINUM · Pranknet · Red Apollo · Rocket Kitten · Syrian Electronic Army · Tailored Access Operations · The Shadow Brokers · Yemen Cyber Army
Individuals		DkD[|| · George Hotz · Guccifer · Jeremy Hammond · Junaid Hussain · Kristoffer von Hassel · Mustafa Al-Bassam · MLT · Ryan Ackroyd · Sabu · Topiary · Track2 · The Jester · weev
Major vulnerabilities publicly disclosed		Evercookie (2010) · iSeeYou (2013) · Heartbleed (2014) · Shellshock (2014) · POODLE (2014) · Rootpipe (2014) · Row hammer (2014) · JASBUG (2015) · Stagefright (2015) · DROWN (2016) · Badlock (2016) · Dirty COW (2016) · Cloudbleed (2017) · Broadcom Wi-Fi (2017) · EternalBlue (2017) · DoublePulsar (2017) · Silent Bob is Silent (2017) · KRACK (2017) · ROCA vulnerability (2017) · BlueBorne (2017) · Meltdown (2018) · Spectre (2018) · EFAIL (2018) · Exactis (2018) · Speculative Store Bypass (2018) · Lazy FP State Restore (2018) · TLBleed (2018) · SigSpoof (2018) · Foreshadow (2018) · Microarchitectural Data Sampling (2019) · BlueKeep (2019) · Kr00k (2019)
Malware	2010	Bad Rabbit · Stuxnet · SpyEye
	2011	Kelihos · Stars · Metulji botnet · Duqu · Alureon
	2012	Mahdi · Carna · Flame · FBI · Shamoon · Red October · Dexter
	2013	DarkSeoul · CryptoLocker
	2014	Careto · DarkHotel · Duqu 2.0 · FinFisher · Brambul · Gameover ZeuS · Carbanak
	2015	Dridex · Rombertik · TeslaCrypt · Hidden Tear
	2016	Hitler · Petya (NotPetya) · KeRanger · Jigsaw · MEMZ · Pegasus · Mirai · X-Agent
	2017	LogicLocker · BrickerBot · Kirk · *Rensenware* ransomware · WannaCry · XafeCopy · Triton
	2019	Grum · Joanap · NetTraveler · NSA ANT catalog · R2D2 · Regin · Tinba · Titanium · Vault 7 · ZeroAccess botnet

Source : Wikipedia

Rappel du contexte de souveraineté

- L'affaire Snowden en 2013 a fait apparaitre une dimension d'intelligence économique insoupçonnée jusqu'alors.
- Les programmes PRISM, Xkeyscore (NSA), … remontant toutes formes d'informations à certaines institutions des US.
- La signature du Patriot Act / Freedom Act et plus récemment le Cloud Act autorise les USA a accéder sur son sol mais aussi n'importe ou aux données résidentes au sein de sociétés américaines (GAFAM et autres).
- Des initiatives comparables venant d'autres états internationaux
- Les risques de cybercriminalités étatiques n'ont cessé de croître depuis plusieurs années avec les APT (Advanced Persistent Threat) Chinoise (10-18), Russe (28-29), Corée Nord (37-38), Iranienne (33-34), …

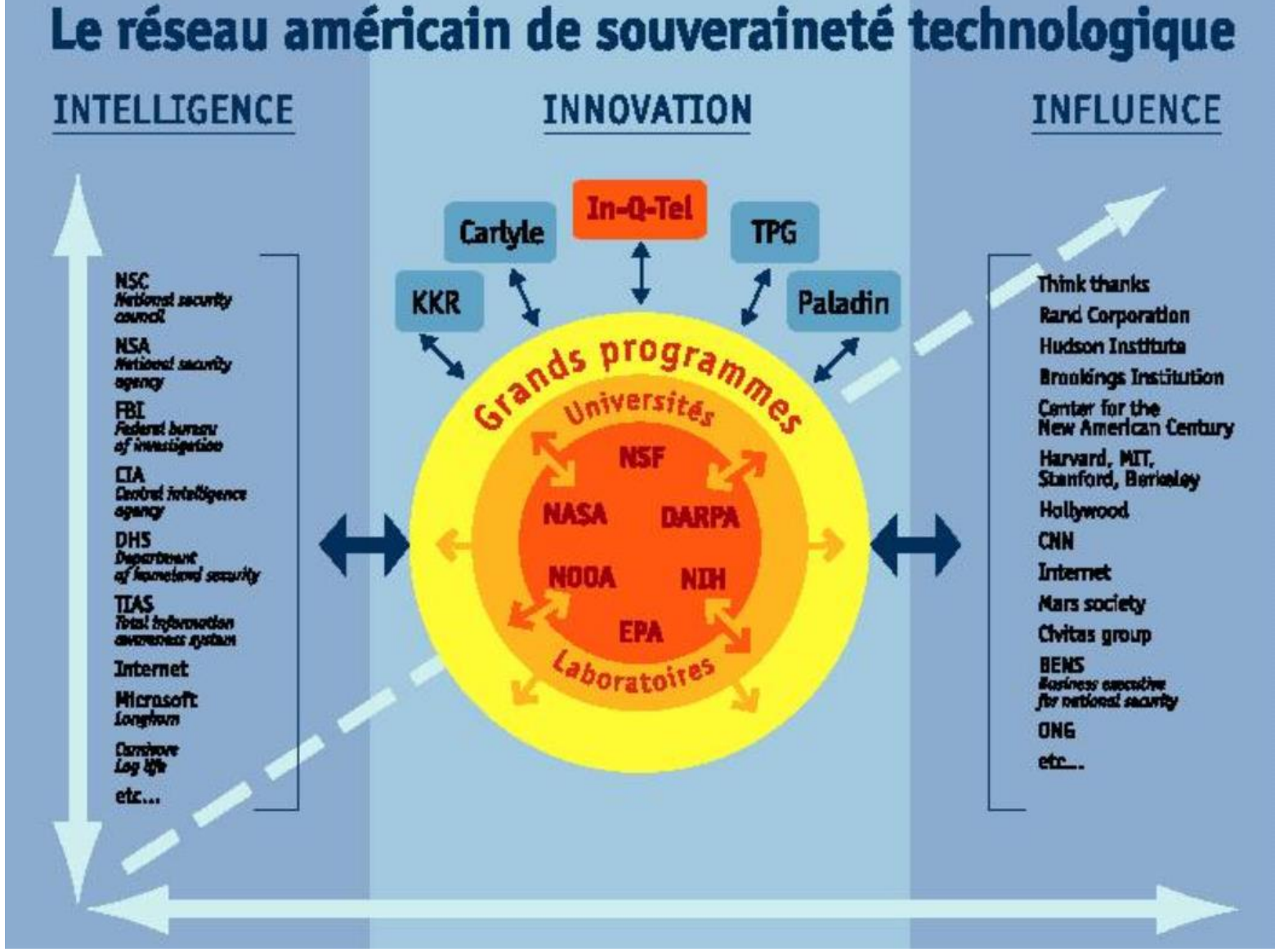
Il devient donc indispensable d'anticiper les risques pour les grandes entreprises Européennes ou innovantes afin d'éviter de perdre le contrôle

Démocratie

Les sources de la puissance américaine
par Jean-Claude Empereur
15/03/04

But : Maitiriser les chaines technologiques, maintenir une avance technologique et combler des manques si nécessaires

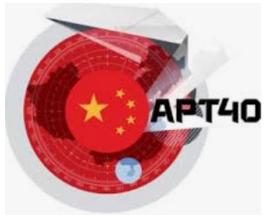
- Gemplus : Carte à puce,
- Alcatel : Telecom,
- Alsthom : Nucléaire,
- Technip : Pétrole,
- Ericsson : 5G,
- …



NSF (sciences), DARPA (défense), NASA (espace), NEOA (climat), NIH (santé), EPA (environnement)
KKR, CARLYLE, TPG, PALADIN (fonds d'investissement orientés pour une large part vers les activités sensibles), IN-Q-TEL (filiale de la CIA).
Longhorn, Carnivore, Log-Life : exemples de logiciels tournés notamment vers le traitement ou l'intégration de données sensibles. Le réseau ECHELON pourrait également figurer en bonne place dans ce tableau.

Risques Cyber venant notamment des états

- Une APT - *Advanced Persistent Threat* cible généralement une organisation pour des motifs d'affaires ou un État pour des motifs politiques.
- Une cinquantaine sont identifiées provenant d'une douzaine d'états ils peuvent regrouper plusieurs milliers d'individus (Hackers)
- Une APT exige un degré élevé de dissimulation sur une longue période de temps. Le but d'une telle attaque est de placer du code malveillant personnalisé sur un ou plusieurs ordinateurs pour effectuer des tâches spécifiques et rester inaperçu pendant la plus longue période possible.
- Le terme est aussi utilisé pour désigner un groupe, comme un gouvernement, avec à la fois la capacité et l'intention de cibler, de façon persistante et efficace, une entité spécifique.



Liste des Hackers & APT recherchés par le FBI en 2020

Chine

- PLA Unit 61398 : APT1
- PLA Unit 61486 : APT2
- Buckeye : APT3
- Red Apollo : APT10
- Codoso Team : APT19
- Wocao : APT20
- PLA Unit 78020 : APT30
- Periscope Group : APT40
- Double Dragon : APT41

Iran

- Elfin Team : APT33
- Helix Kitten : APT34
- Charming Kitten : APT35

Corée du nord

- Ricochet Chollima : APT37
- Lazarus Group : APT38

Russie

- Fancy Bear : APT28
- Cozy Bear : APT29
- Voodoo Bear
- Venomous Bear

United States

- Equation Group

Uzbekistan

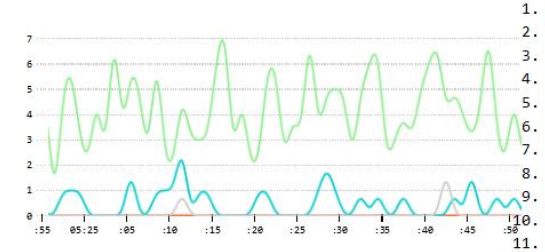
- SandCat associated with the National Security Service

Vietnam

- OceanLotus : APT32

Rapport d'analyse d'attaques le 18 Mars 2021

INFECTIONS / SECOND (5)



Start Date: 2021/3/18 9:07:42
End Date: 2021/3/18 17:25:52

LIVE ATTACKS (180095)

1.	Sality		N/A
2.	Sality	PK	Mardan
3.	Sality	EG	Cairo
4.	Sality	BR	N/A
5.	Sality	UY	N/A
6.	Sality	IN	N/A
7.	Sality	CN	Xuzhou
8.	Sality		N/A
9.	Trojan Phorpiex	GT	N/A
10.	Sality	US	San Jose
11.	Sality	RU	N/A
12.	Sality	EG	N/A
13.	Sality	IN	Bangalore

BOTNETS (7)

Total Numbers

1.	Sality	162482
2.	Mobile	17071
3.	Trojan	356
4.	Lokibot	56
5.	APT	44
6.	Conficker	43
7.	Ramdo	43

COUNTRIES (177)

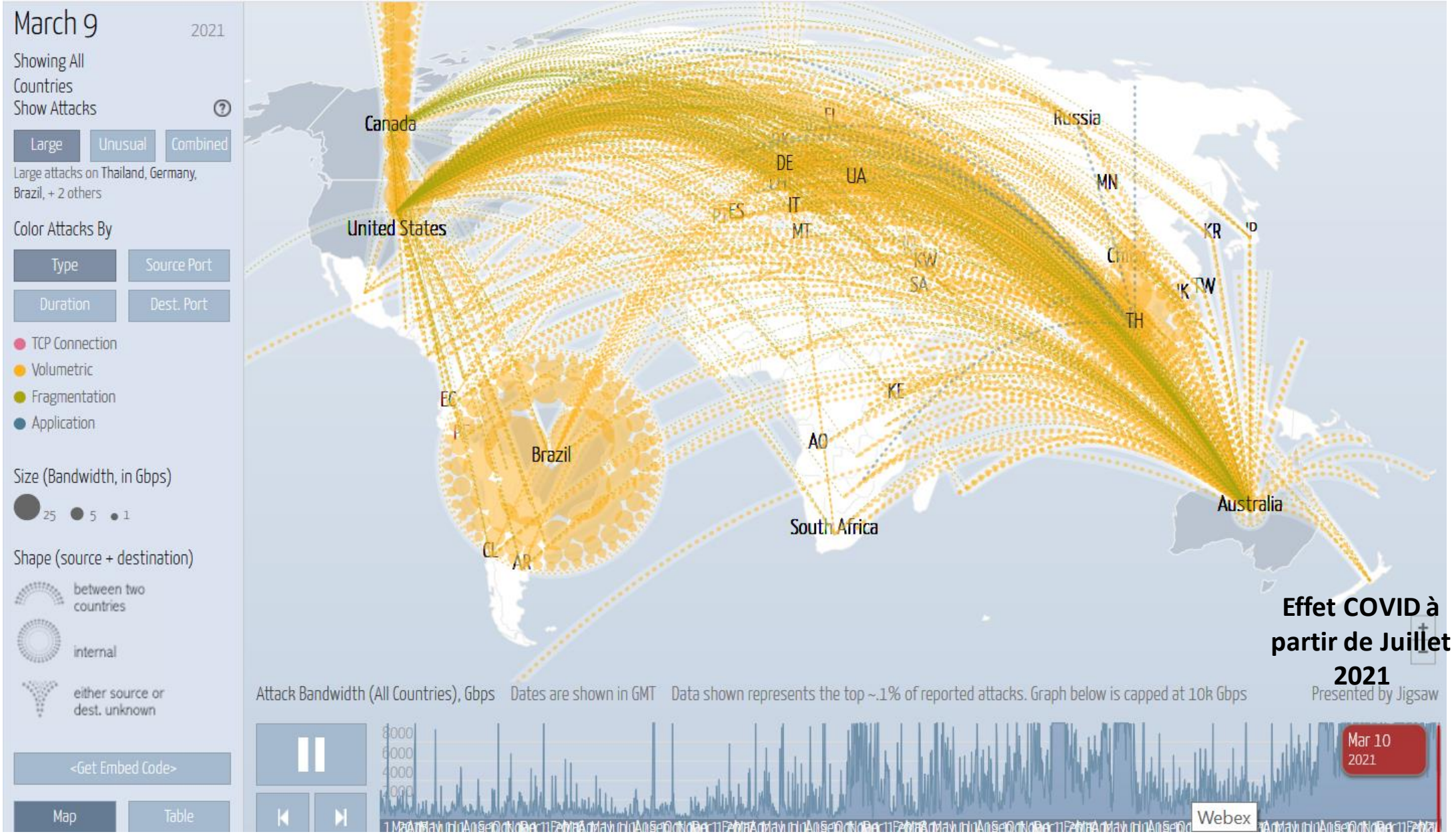
Percentage

India	21.11%
China	15.45%
Egypt	7.79%
Iran, Islamic Republic of	5.19%
South Africa	3.22%
Algeria	3.21%
Russian Federation	3.19%
Unknown	2.76%
Vietnam	2.38%
Pakistan	2.20%
Nigeria	2.13%
Indonesia	2.04%

Leaflet | Botnet data © LookingGlass | Tiles © Esri & GIS User Community

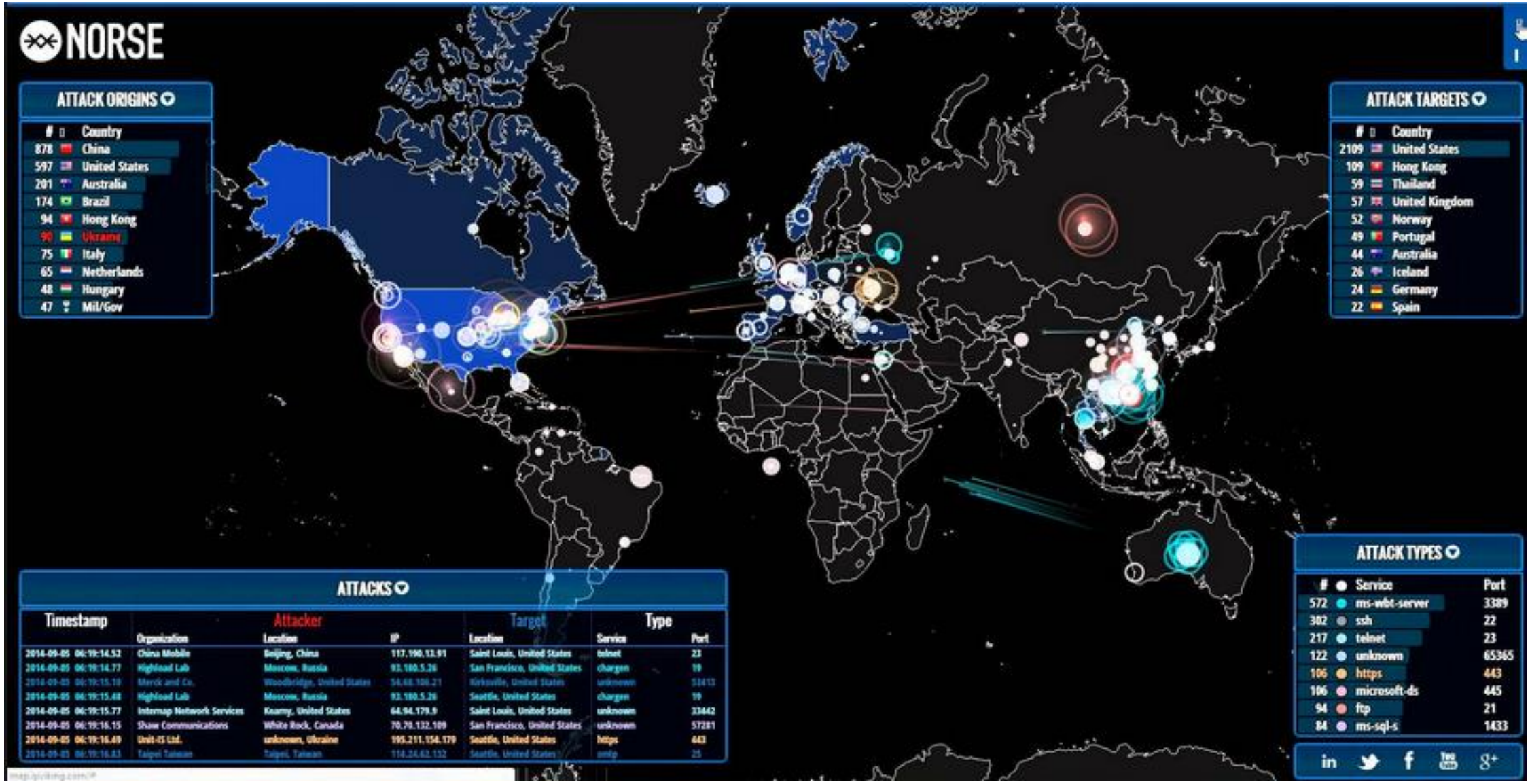
- Analyse de lookingGlass pendant 8H20 à partir de 9H07 : plus de 180 095 attaques répertoriée
- **Sur la durée on remarque que la majorité des attaques proviennent de :**
  - **Russie**
  - **Chine**
  - **USA / Canada**
  - **Iran**
  - **Corée du nord**
  - **Brésil**
  - **…**

Cartographie des attaques du 9 Mars 2021 d'Arbor Networks



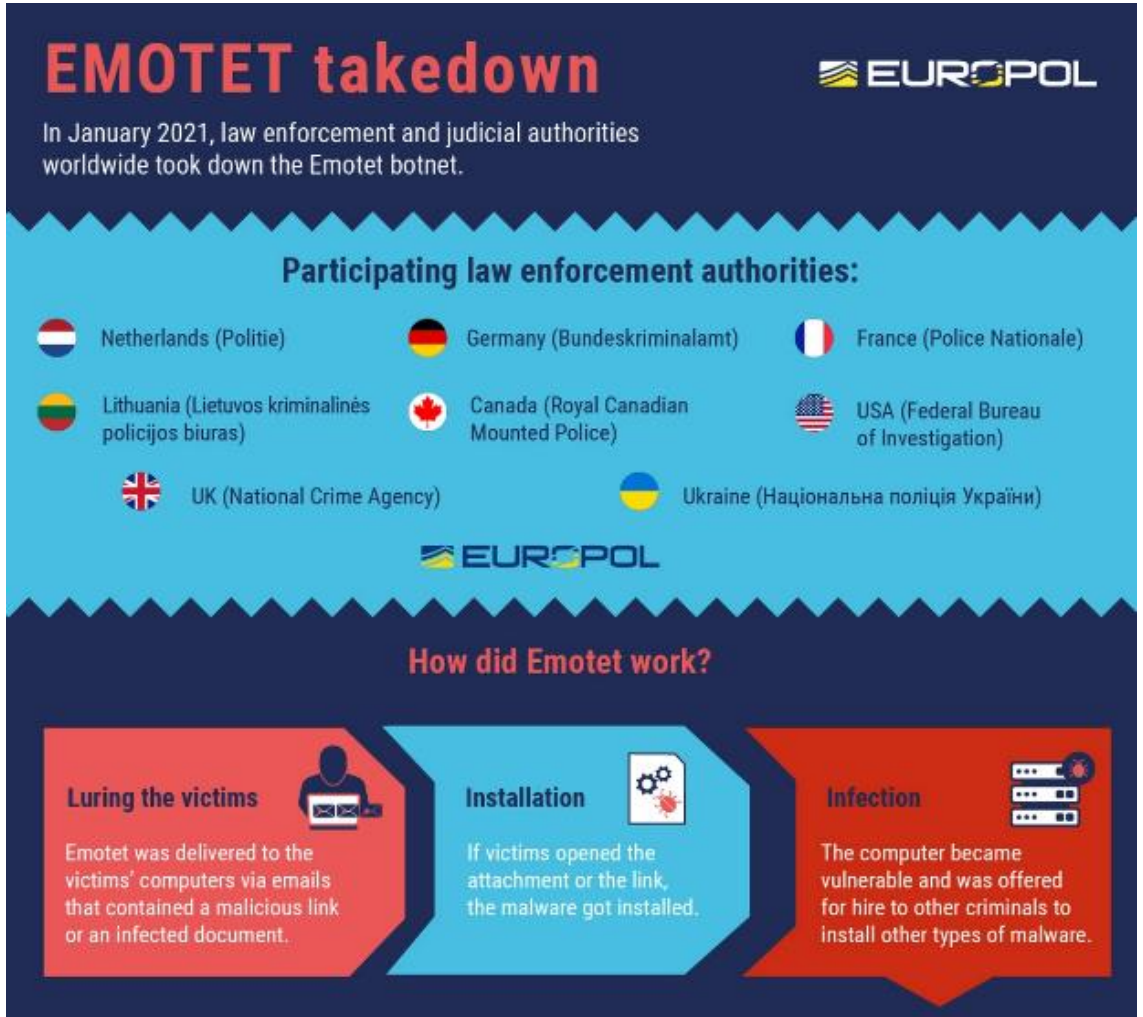
Effet COVID à partir de Juillet 2021

Autre exemple d'état des attaques selon NORSE



Exemple EMOTET

Emotet malware bancaire apparu en 2014 a évolué avec de nouveaux services de diffusion spam, de malware, chevaux de Troie.
Emotet est difficile a être détecté par les outils anti-malware il est devenu polymorphe avec le temps.
En France, réapparition en juillet 2020 avec des attaques au Tribunal de Paris, Municipalité d'Orléans, 14 académies (Tours, Nantes, Rennes, Amiens, Nancy, Strasbourg, Lyon, Grenoble, Montpellier, Toulouse, Aix-Marseille, Versailles, Paris et Créteil), Air France KLM et la SSII Humanis. Démantelement en Janvier / Février 2021 (EGREGOR en Ukraine)



BULLETIN D'ALERTE DU CERT-FR

Objet: Recrudescence d'activité Emotet en France

GESTION DU DOCUMENT

Référence	CERTFR-2020-ALE-019
Titre	Recrudescence d'activité Emotet en France
Date de la première version	07 septembre 2020
Date de la dernière version	09 février 2021
Source(s)	
Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

RISQUE(S)

[mise à jour du 22 septembre 2020]

L'ensemble des échantillons obtenus par l'ANSSI jusqu'à maintenant a permis de comparer ces derniers avec les listes de marqueurs en sources ouvertes référencés dans la section "Moyens de détection relatifs à Emotet".

La fiabilité de ces flux a été assurée et nous vous encourageons à les intégrer dans vos systèmes de détection.

Contrairement aux recommandations indiquées dans la version précédente de cette alerte, il n'est donc plus nécessaire de nous faire parvenir vos échantillons.

[version initiale]

Depuis quelques jours, l'ANSSI constate un ciblage d'entreprises et administrations françaises par le code malveillant Emotet. Il convient d'y apporter une attention particulière car Emotet est désormais utilisé pour déposer d'autres codes malveillants susceptibles d'impacter fortement l'activité des victimes.

CARACTÉRISTIQUES DU CHEVAL DE TROIE EMOTET

Observé pour la première fois mi-2014 en tant que cheval de Troie bancaire, Emotet a évolué pour devenir un cheval de Troie modulaire. Ses différents modules actuels lui permettent :

- de récupérer les mots de passe stockés sur un système ainsi que sur plusieurs navigateurs (Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera) et boîtes courriel (Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail et Gmail) ;
- de dérober la liste de contacts, le contenu et les pièces jointes attachées à des courriels ;
- de se propager au sein du réseau infecté en tirant parti de vulnérabilités SMB ainsi que des mots de passe récupérés.

Le code malveillant est distribué par le botnet éponyme (lui-même composé de trois groupements de serveurs différents Epoch 1, Epoch 2, Epoch 3, opérés par le groupe cybercriminel TA542) au travers de **campagnes massives de courriels d'hameçonnage**, souvent parmi les plus volumineuses répertoriées. Ces courriels d'hameçonnage contiennent généralement des pièces jointes Word ou PDF malveillantes, et plus rarement des URL pointant vers des sites compromis ou vers des documents Word contenant des macros.

Ces campagnes d'attaques touchent tous types de secteurs d'activités à travers le monde.

EMOTET : LOADER DE CODES MALVEILLANTS TIERS

Depuis 2017, Emotet n'est plus utilisé en tant que cheval de Troie bancaire mais distribue, fréquemment au sein des systèmes d'information qu'il infecte, des codes malveillants opérés par des groupes d'attaquants qui sont clients de TA542. Par exemple, les chevaux de Troie bancaires Qbot, Trickbot, IcedID, GootKit, BokBot, Dridex et DoppelDridex peuvent être distribués en tant que seconde charge utile, avec une prédominance en 2020 de Qbot et TrickBot.

En outre, ces derniers peuvent télécharger des rançongiciels au sein du système d'information compromis. C'est par exemple le cas de TrickBot auquel il arrive de télécharger les rançongiciels Ryuk ou Conti.

Ainsi, la détection et le traitement au plus tôt d'un évènement de sécurité lié à Emotet peut prévenir de nombreux types d'attaques, dont celles par rançongiciel avant le chiffrement.

RECRUDESCENCE DES CAMPAGNES D'ATTAQUE DURANT LE SECOND SEMESTRE 2020

Après une absence de cinq mois, Emotet a refait surface en juillet 2020. Depuis, nombre de ses campagnes d'hameçonnage exploitent une technique de détournement des fils de discussion des courriels (*email thread hijacking technique*).

Une fois la boîte courriel d'un employé de l'entité victime (ou la boîte courriel générique de l'entité elle-même) compromise, le code malveillant Emotet exfiltre le contenu de certains de ses courriels. Sur la base de ces derniers, les attaquants produisent des courriels d'hameçonnage prenant la forme d'une réponse à une chaîne de courriels échangés entre l'employé et des partenaires de l'entité pour laquelle il travaille. L'objet légitime du courriel d'hameçonnage est alors précédé d'un ou plusieurs « Re : », et le courriel lui-même contient l'historique d'une discussion, voire même des pièces jointes légitimes.

Ces courriels, d'apparence légitime, sont envoyés à des contacts de la victime, et plus particulièrement aux tierces parties de l'entité (clients et prestataires notamment) ayant participé au fil de discussion originel, afin d'accroître leur crédibilité auprès des destinataires.

Outre cette technique, TA542 construit également des courriels d'hameçonnage sur la base d'informations récupérées lors de la compromission des boîtes courriel, qu'il envoie aux listes de contact exfiltrées, ou usurpent plus simplement l'image d'entités, victimes préalables d'Emotet ou non (sociétés de transport, de télécommunication ou encore institutions financières).

Dans tous les cas, il apparaît que les boîtes courriel compromises ne sont pas utilisées pour envoyer des courriels d'hameçonnage mais que ces derniers sont envoyés depuis l'infrastructure des attaquants sur la base d'**adresses courriel expéditrices souvent typosquattées**.

La France représente une cible des campagnes récentes d'Emotet.

SOLUTION

MOYENS DE DÉTECTION RELATIFS À EMOTET

Plusieurs flux existent contenant des indicateurs de compromission actualisés relatifs à Emotet, ce code faisant l'objet de nombreuses investigations dans les secteurs public et privé. Parmi ces flux, https://paste.cryptolaemus.com/ et https://feodotracker.abuse.ch/browse/ représentent des **sources fiables qu'il est recommandé d'intégrer dans ses moyens de détection et de blocage.**

A noter aussi :

- Les chercheurs de Cryptolaemus fournissent notamment des expressions régulières permettant de détecter des liens utilisés dans les courriels malveillants. Ils sont disponibles dans les bulletins quotidiens de l'équipe de chercheurs, dans le paragraphe « Link Regex Report ».
- Des règles de détection YARA d'Emotet ont été produites par ReversingLabs : https://github.com/reversinglabs/reversinglabs-yara-rules/blob/develop/yara/trojan/Win32.Trojan.Emotet.yara.
- Emocheck, un outil créé par le CERT japonais, permet de détecter la présence du trojan Emotet sur une machine Windows. Emotet utilisant un dictionnaire prédéfini pour le nom de ses processus, ce programme vérifie si un programme en cours d'exécution correspond à ce dictionnaire précis. L'outil est disponible en source ouverte : https://github.com/JPCERTCC/EmoCheck.

RECOMMANDATIONS

Sensibiliser les utilisateurs à ne pas activer les macros dans les pièces jointes et à être particulièrement attentifs aux courriels qu'ils reçoivent et réduire l'exécution des macros.

Limiter les accès Internet pour l'ensemble des agents à une liste blanche contrôlée.

Déconnecter les machines compromises du réseau sans en supprimer les données.

De manière générale, une suppression / un nettoyage par l'antivirus n'est pas une garantie suffisante. Seule la réinstallation de la machine permet d'assurer l'effacement de l'implant.

DOCUMENTATION

Cofense – avril 2019 (https://cofense.com/emotet-gang-switches-highly-customized-templates-utilizing-stolen-email-content-victims/)

Proofpoint – mail 2019 (https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service)

Malwarebytes – 2019 (https://www.malwarebytes.com/emotet/)

JP CERT – décembre 2019 (https://www.jpcert.or.jp/english/at/2019/at190044.html)

US-CERT – janvier 2020 (https://us-cert.cisa.gov/ncas/alerts/TA18-201A)

Bleeping Computer – juillet 2020 (https://www.bleepingcomputer.com/news/security/emotet-malware-now-steals-your-email-attachments-to-attack-contacts/)

Proofpoint – août 2020 (https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-summer-2020-return)

GESTION DÉTAILLÉE DU DOCUMENT

le 07 septembre 2020
Version initiale

le 22 septembre 2020
Mise à jour

le 22 septembre 2020
retrait de la mention sur la transmission des échantillons

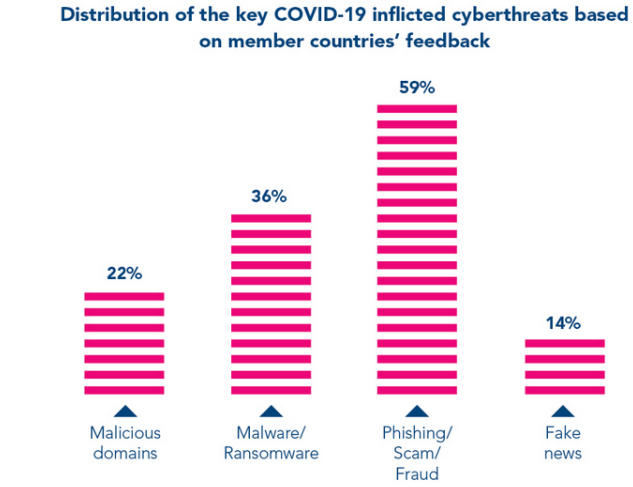
le 09 février 2021
Clôture de l'alerte.

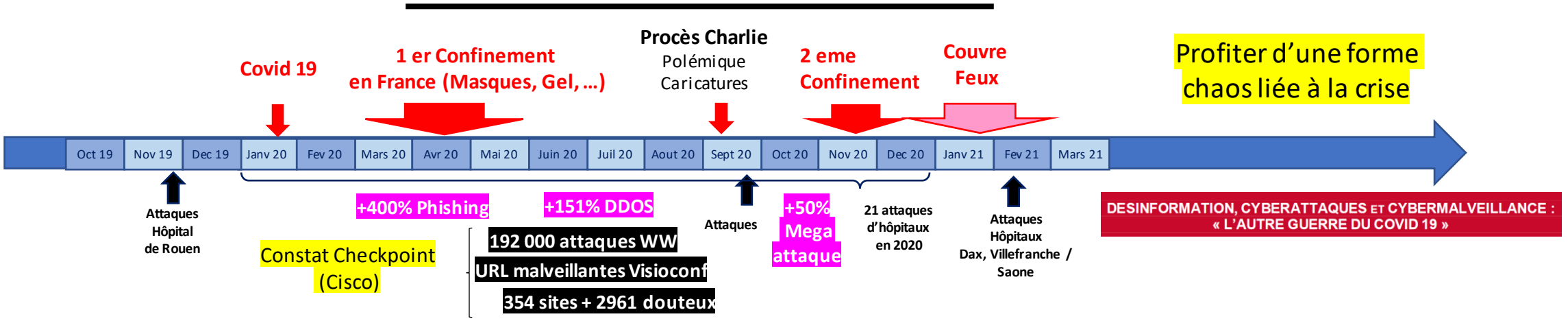
Effet COVID sur les Cyberattaques

- Conséquences du COVID-19 sur la cybercriminalité réalisée par INTERPOL
  - changement de cible, les attaques concernant plus les grandes sociétés, gouvernements et infrastructures essentielles que les particuliers et les petites entreprises.
- Télétravail :
  - Avec le déploiement rapide, par les organisations et les entreprises, de systèmes distants et de réseaux permettant le télétravail du personnel, les malfaiteurs exploitent également des vulnérabilités accrues en matière de sécurité pour dérober des données, générer des profits et provoquer des perturbations.
- Sur une période de quatre mois (de janvier à avril)
  - quelque 907 000 messages non sollicités, 737 incidents liés à des logiciels malveillants et 48 000 URL malveillantes – tous en rapport avec le COVID 19 – ont été détectés par l'un des partenaires d'INTERPOL appartenant au secteur privé.

« Les cybermalfaiteurs, qui exploitent la peur et l'incertitude liées à l'instabilité de la situation sociale et économique engendrée par le COVID-19, préparent et multiplient leurs attaques à un rythme très préoccupant »

M. Jürgen Stock, Secrétaire Général d'INTERPOL





Risques liés au télétravail

- L'effet COVID a eu un impact majeur sur :
  - Le télétravail passage de 6% à 15% voire plus actuellement
  - Les risques Cyber en augmentation de + 300%
- Avec une incidence sur les usages
  - Visioconférence : Teams, Zoom
    - Failles de sécurité, absence de chiffrement de bout en bout, visioconférences en ligne multiplateforme, mode d'installation fantôme, Ecoute clandestine, Analyse IA
    - URL malveillante impactant – Microsoft Teams, Google Meet, Zoom
  - Usage de VPN :
    - Saturation des VPN, manque de résilience des reseaux, travail hors connexion
  - Usage de l'internet personnel :
    - Ralentissement débits, usage de connexion mobile, faille sécurité
  - Usage des outils collaboratifs :
    - Moins sécurisés qu'au sein de l'entreprise, risque de phishing avec des liens malicieux
- Principaux risques
  - Phishing : Empêcher l'accès des employés aux données de l'entreprise
  - Data Breach : S'introduire sur le réseau d'entreprise pour dérober des données et exercer du chantage

Evolution des attaquants

- Commercialisation de leurs menaces
- Constitution d'Ecosystème d'attaquants
- Contextualisation des actions

➢ **Industrialisation de l'activité**

Impact Ransomware

- Impact estimé à + de 10 Md€
- + 365 % par rapport à 2019

Impact Data Breaches

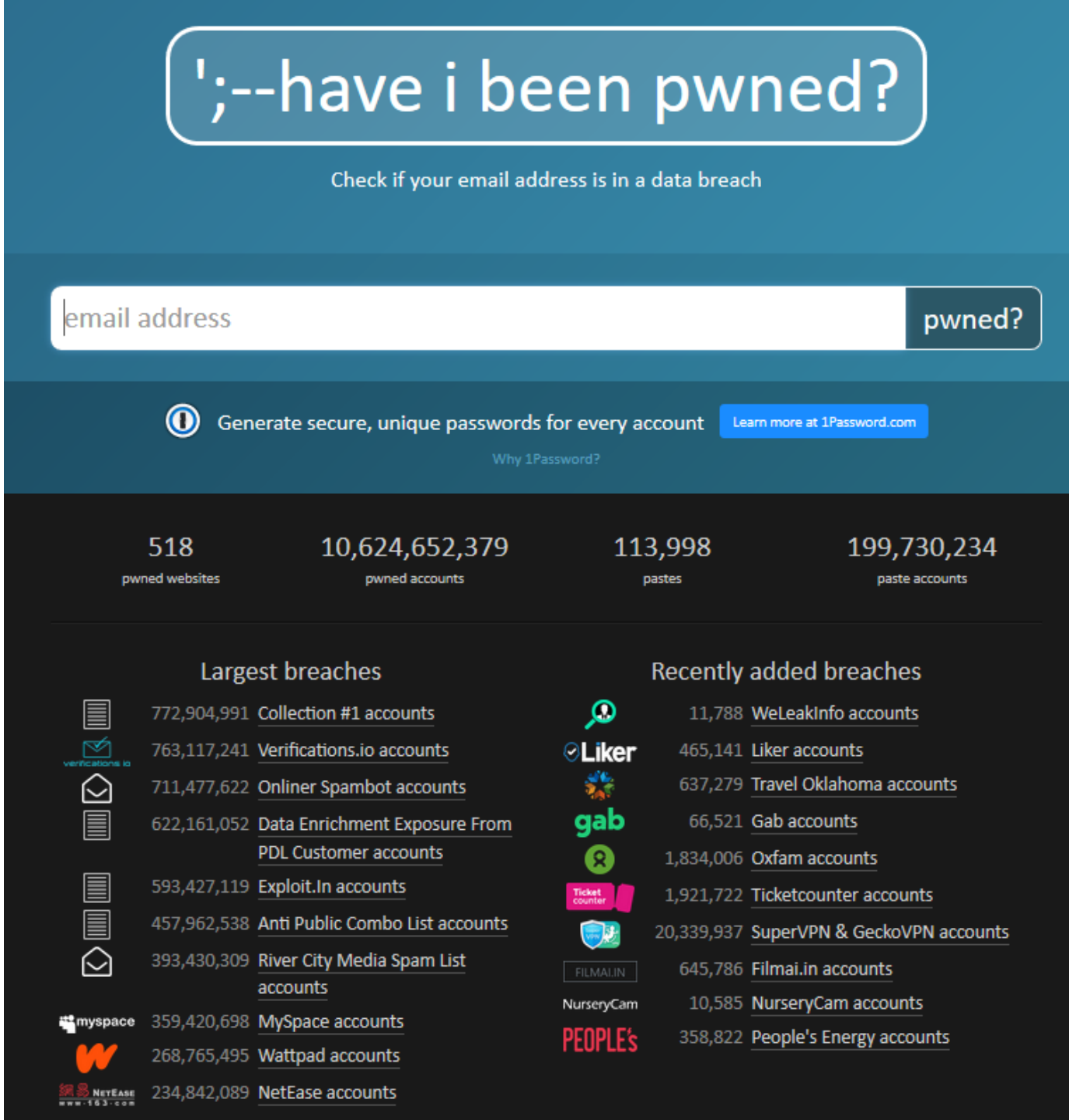
- 2953 violations de données
- 36 107 millions de données

A l'occasion de la COVID19 piratage de données personnelles notamment de santé

- Dans le domaines de la santé récemment les données se vendaient entre 50 et 300 Euros en France

Vérification du piratage de vos données personnelles

- Pour alimenter les CRM, il est quasi systématique qu'on vous demande d'ouvrir un compte client pour avoir accès aux services proposés par un site web : vente en ligne, accès à de l'information gratuite, réservation touristique…
- Ces sites sont de plus en plus piratés parmi ceux qui ont été impactés sur les 5 dernières années :
  - Yahoo (1 milliard de comptes piratés),
  - eBay (145 millions),
  - LinkedIn (117 millions),
  - Badoo (112 millions),
  - Dropbox (70 millions),
  - Marriott (52 millions)
  - Estée Lauder (440 millions), …
- Les adresses emails et mots de passe associés se vendent, s'échangent…



new normal au next normal

DOMAINES	AVANT COVID	PENDANT COVID	APRES COVID
POLITIQUE ECONOMIE FINANCE SOCIAL ECOLOGIE	• Gilet jaune, Lois, Brexit, Chine/US • Economie stable, faible croissance • Dette à gérer • Tendu conflit lois travail, … • Pollution, convent° Citoyenne	• Quoi qu'il en coute, Crise, dictature sanitaire • 3 confinements, secteurs sinistrés • Dette monumentale, épargne • Chômage partiel, total • Sensibilisation Cause du Virus	• **+ de Souveraineté** • Riche + riche, pauvre + pauvre • Disparité accrue au plan mondial • Relance, Gestion endettement ? • Dépôts de bilan ! • **Green IT, Neutralité Carbone**
SANTE	• Réduction des crédits • Limitation des lits d'hôpitaux • Marasme médical, santé + rentable • Modèle Santé repensé	• Mortalité (100 000 en france) • Crise : Masques/gel, Vaccination • Financement Labo/Startups (ARN) • **Explosion des attaques Cyber** • **Hôpitaux, Labo attaqués en France**	• Grands gagnants – ARN, innovat° • Préparation autres pandémies • Vaccination dans la durée • RETEX Médical / Expert / Crise / Rançons
TECHNOLOGIE	• Croissance significative numérique • Bascule vers le Cloud (Doctrine) • Télétravail : ~6%	• Explosion du Numérique, • Outils collaboratifs généralisés • Télétravail : ~ 18% • Vente et partage données santé	• Suprématie accrue des GAFAM, … • Perte importante de données et d'autonomie (datacrunching) • Maintien d'outils de télétravail
CYBERSECURITE	• Croissance des attaques • Attaques en majorité Hackers • Cloud Act – ingérence d'état • Attaques orchestrées, Virus polymorphes • DeepWeb & DarkWeb très présents	• **Failles de sécurité accrues** • **Explosion attaques Cyber (+300%)** • **Attaques ciblées** • **Perte de contrôle & souveraineté** • Identificat° Facilitée (confinement) • Engagement Cyber Fr (+ 1 Md)	• **Risques d'amplification Cyber** • **Automatisat° des attaques,** • **Amplificat° Amendes US** • **Attaques d'état + importantes** • Texte de loi en préparat° • Mise en place Campus Cyber

Typologies d'attaques / virus et Perspectives

Aujourd'hui

- **DDoS** : Attaque par Déni de service distribué
- **Malware** : Attaque par Logiciel malveillant
  - Ransomwares, Macro virus, virus polymorphes, Chevaux de troie, vers, Infection de fichiers / Systèmes, Bombes logiques, …
- **MitM** : Insertion dans communications entre client et serveur
- **Phishing** : Hameçonnage générique ou ciblé via Mail
- **Drive by Download** : Téléchargement furtif
- **Password :** Piratage de Mot de passe
- **Injection SQL** : infection de site Web avec Bases de données
- **Cross-site scripting (XSS)** : Corruption de navigateur cible, modification de site Web
- **Piratage réseau / Telecom** : Ecoute clandestine (Passive/Active), réseau Wifi, …
- **Cryptojacking** : attaque cryptomonnaie
- **Objets connectés** : attaques Capteurs / Actionneurs (IOT)
- **Attaques Internes** : Via Clefs USB, composants IoT connexions Wifi
- **Attaques Géopolitiques** : via groupement de pirates (APT) orchestration d'un Mix d'attaques a des fins politiques
- …

En 2030

- **Professionnalisation des activités**
- **Explosion des différentes typologies d'attaques**
- **Intelligence Artificielle au profit des Hackers**
- **Services SaaS d'attaques**
- **Dark Web +/+ puissant**
- **Attaques d'état plus imposantes et orchestrées**
- **Attaques objets connectés**
- **…**

Tendances à 10 Ans de la cybersécurité

En 2030

- Banalisation des terminaux (écran souple, pliable, virtuel, …)
- Réseaux fixe et mobile de +/+ rapides (FO, 5G/6G)
- Explosion des données & applis (modèle agile)
- Réalité augmentée
- Secrets d'entreprises, Intelligence Economique
- Informatique Quantique
- Voiture autonome
- Smart city
- + d'Intelligence Artificielle & Machine Learning
- **Normalisation & contrôle affaiblis par pression économique**
- **Puissance de calcul utilisée pour casser chiffrement, môts de passe**
- **Automatisation des Attaques (M2M)**
- **Contenu de plus en plus dans le Cloud –attaque des CSP**
- **Prolifération des Services SaaS (Cyber)**
- **Informatique industrielle - Attaques des composants industriels**

Parades & Ripostes

Mise en place de plateformes intelligentes EDR/XDR anti Attaques

Consolidation des sources et utilisations de l'IA et du ML pour une grande efficacité de parades

Formation des utilisateurs (paranoïa)

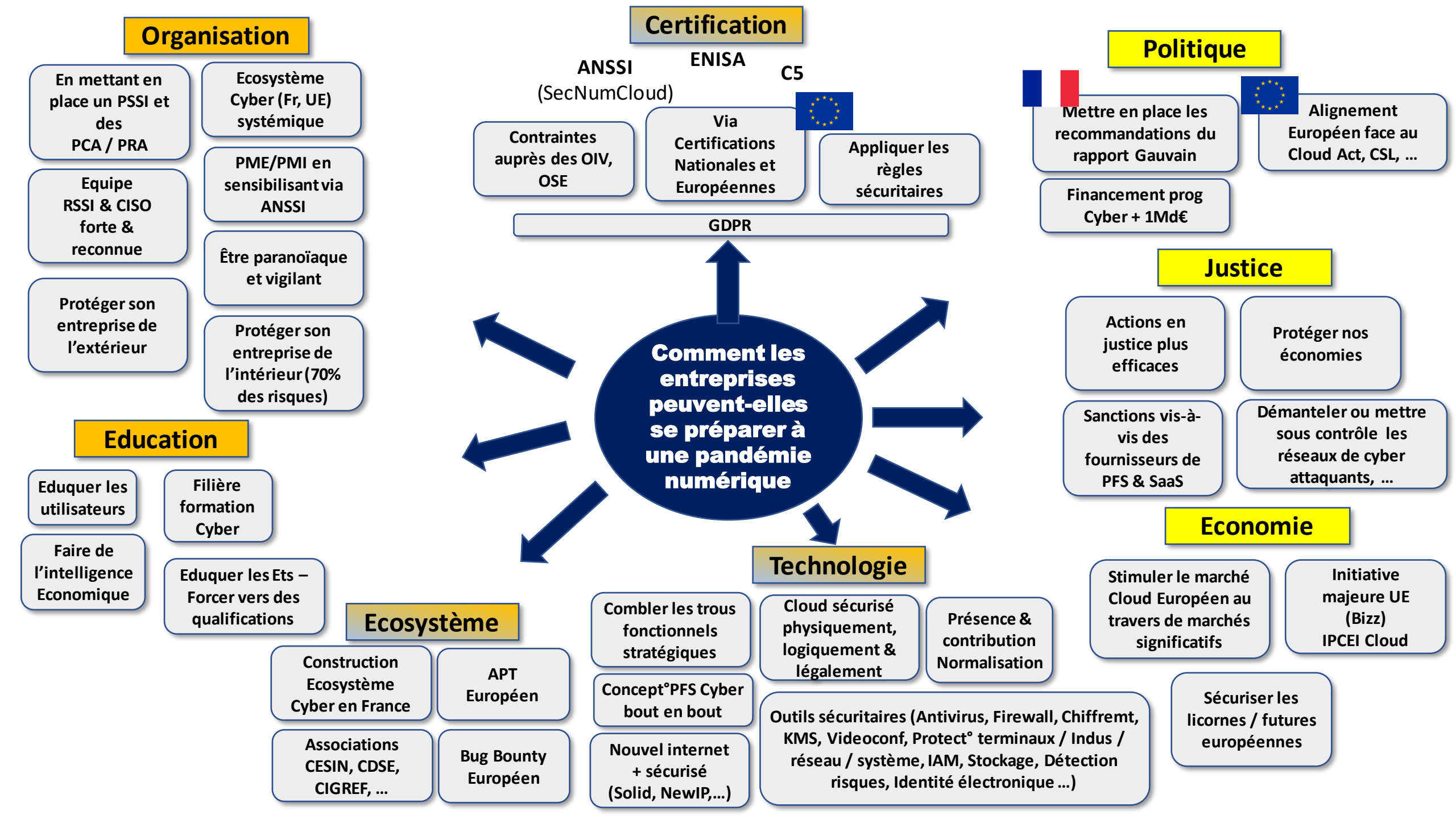
Mettre en place une gouvernance plus simple et efficace

Coordination inter – Agence pour anticiper et contrer les attaques

Emergence de protocole plus sécuritaire, repenser le WWW

Rétablir une concurrence plus forte de la part de l'Europe

Reprendre le Contrôle des normalisations (sécurité)


Organisation
En mettant en place un PSSI et des PCA / PRA
Ecosystème Cyber (Fr, UE) systémique
Equipe RSSI & CISO forte & reconnue
PME/PMI en sensibilisant via ANSSI
Être paranoïaque et vigilant
Protéger son entreprise de l'extérieur
Protéger son entreprise de l'intérieur (70% des risques)
Certification
ANSSI (SecNumCloud)
ENISA
C5
Contraintes auprès des OIV, OSE
Via Certifications Nationales et Européennes
Appliquer les règles sécuritaires
GDPR
Politique
Mettre en place les recommandations du rapport Gauvain
Alignement Européen face au Cloud Act, CSL, …
Financement prog Cyber + 1Md€
Justice
Actions en justice plus efficaces
Protéger nos économies
Sanctions vis-à-vis des fournisseurs de PFS & SaaS
Démanteler ou mettre sous contrôle les réseaux de cyber attaquants, …
Comment les entreprises peuvent-elles se préparer à une pandémie numérique
Education
Eduquer les utilisateurs
Filière formation Cyber
Faire de l'intelligence Economique
Eduquer les Ets – Forcer vers des qualifications
Technologie
Combler les trous fonctionnels stratégiques
Cloud sécurisé physiquement, logiquement & légalement
Présence & contribution Normalisation
Concept°PFS Cyber bout en bout
Outils sécuritaires (Antivirus, Firewall, Chiffremt, KMS, Videoconf, Protect° terminaux / Indus / réseau / système, IAM, Stockage, Détection risques, Identité électronique …)
Nouvel internet + sécurisé (Solid, NewIP,…)
Economie
Stimuler le marché Cloud Européen au travers de marchés significatifs
Initiative majeure UE (Bizz) IPCEI Cloud
Sécuriser les licornes / futures européennes
Ecosystème
Construction Ecosystème Cyber en France
APT Européen
Associations CESIN, CDSE, CIGREF, …
Bug Bounty Européen

Existe-t-il un risque pandémique numérique de grande ampleur ?

Le risque n'est pas totalement négligeable

CYBER

- Blocage d'état – déjà vécu avec l'interventionnisme de certains pays (Irak, Iran, Syrie, …)
- Chaine technique
  - Composants électronique – CPU, connectivités
  - Operating System
  - Accès Réseaux
  - Réseaux (Filaire, Satellitaire, Radio, …)
  - Protocoles (IPV4, IPV6, …)
  - Cœurs de réseaux
  - Système d'administration – NOC, SOC
  - Plateformes de services
  - Plateformes Applicatives
  - Applications collaboratives
  - Cloud
  - Système d'information d'exploitation
- Moyen de contrôle de supervision, Audit, certification, Réglementation
- Normalisation *-> perte de contrôle par manque de moyen*

AUTRES

- Perturbation électromagnétique
  - Eruption solaire ~ tous les 10 Ans (mars 89, 2013, …),
  - Eruption volcanique d'ampleur (Islande, Japon,…)

ANNEXES

Un plan à 1 milliard d'euros pour renforcer la cybersécurité

Publié le : 18/02/2021

Photo : ministère de l'Intérieur

Financée par France Relance et le Programme d'investissement d'avenir, la stratégie nationale pour la cybersécurité vise, entre autres, à doubler les effectifs de la filière d'ici à 2025.

La transition numérique est porteuse de progrès, mais les espaces numériques sont aussi le lieu d'actions criminelles, notamment les cyberattaques. Pour faire face à cette menace, **le Gouvernement mobilise 1 milliard d'euros, dont 720 millions de financements publics**.

Financée par France Relance et le Programme d'investissement d'avenir, la **stratégie nationale pour la cybersécurité** vise à faire émerger des champions français de la cybersécurité.

> *« À la fois essentielle à la souveraineté des États, à la pérennité du développement des entreprises et à la sécurité des citoyens, la cybersécurité est un enjeu majeur du XXIe siècle. »*
> Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance.

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 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).

Cybermalveillance, un dispositif gouvernemental d'assistance aux victimes d'actes de cybermalveillance

La campagne de l'ANSSI : "Face à la menace cyber, pas besoin de connaître quelqu'un au Bureau des légendes"

Principaux risques en France (Allianz Risk Barometer 2019)

10 PRINCIPAUX RISQUES EN FRANCE

Source: Allianz Global Corporate & Specialty.
Les chiffres représentent un pourcentage de toutes les réponses pour ce pays.
Participants: 86
Réponses: 106
Plus d'1 risque et d'1 industrie pouvaient être sélectionnés. Les chiffres ne totalisent pas 100% car 3 risques pouvaient être sélectionnés.

Classement		Pourcentage	Classement 2018	Tendance
1	**Incidents cyber (ex : cyber crimes, défaillances informatiques, violation de données...)**	**41%**	2 (46%)	▲
2	Interruptions d'activités (y compris les perturbations de la chaîne logistique)	**40%**	1 (47%)	▼
3	Incendie, explosion	**29%**	3 (21%)	=
4	Catastrophes naturelles (ex : tempête, inondation, tremblement de terre...)	**28%**	4 (21%)	=
5	Évolutions législatives et réglementaires (ex : changement de gouvernement, sanctions économiques, protectionnisme, Brexit, désintégration de la zone Euro...)	**26%**	4 (21%)	▼
6	Évolutions de marchés (ex : volatilité, concurrence accrue, nouveaux entrants, fusions/acquisitions, fluctuation de marchés)	**18%**	6 (18%)	=
6	Nouvelles technologies (ex : impact de l'inter connectivité croissante, nanotechnologie, intelligence artificielle, impression 3D, blockchain...)	**18%**	8 (14%)	▲
8	Atteinte à la réputation ou à l'image de marque	**12%**	9 (13%)	▲
8	Défaillances de qualité, défauts de série, rappel de produits	**12%**	7 (16%)	▼
10	Vol, fraude et corruption	**10%**	9 (13%)	▼

Principales lacunes rencontrées dans les entreprises

1. des systèmes et des applications, dont les sites Web, qui ne sont pas à jour de leurs correctifs de sécurité
2. une politique de gestion des mots de passe insuffisante (mots de passe par défaut ou trop simples et non renouvelés régulièrement…)
3. une absence de séparation des usages entre utilisateur et administrateur des réseaux
4. un laxisme manifeste dans la gestion des droits d'accès
5. une absence de surveillance des systèmes d'information (analyse des journaux réseaux et de sécurité)
6. un cloisonnement insuffisant des systèmes qui permet à une attaque de se propager au sein des réseaux
7. une absence de restrictions d'accès aux périphériques (supports USB…)
8. une ouverture excessive d'accès externes incontrôlés au système d'information (nomadisme, télétravail ou télé administration des systèmes)
9. une sensibilisation et une maturité insuffisantes des utilisateurs et des dirigeants face à la menace dont ils ne perçoivent pas les risques.

10 Règles de sécurité de l'ANSSI

1. Utiliser des mots de passe de qualité..
2. Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc.
3. Effectuer des sauvegardes régulières.
4. Désactiver par défaut les composants ActiveX et JavaScript.
5. Ne pas cliquer trop vite sur des liens.
6. Ne jamais utiliser un compte administrateur pour naviguer.
7. Contrôler la diffusion d'informations personnelles.
8. Ne jamais relayer des canulars. Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc.
9. Soyez prudent : l'Internet est une rue peuplée d'inconnus ! Il faut rester vigilant
10. Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants. (.pif; .com ; .bat ; .exe ; .vbs ; .lnk. …)

- **1. Protégez vos accès avec des mots de passe solides.**
  - Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaque mots de passe trop simples ou réutilisés. Au moindre doute, ou même régulièrement en prévention, changez-les. Utilisez un gestionnaire de mots de passe et activez la double authentification chaque fois que c'est possible pour renforcer votre sécurité (Voir notre fiche sur les mots de passe).
- **2. Sécurité numérique : sauvegardez vos données régulièrement**
  - En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages…). Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée (Voir notre fiche sur les sauvegardes).
- **3. Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées**
  - Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner (Voir notre fiche sur les mises à jour).
- **4. Utilisez un antivirus**
  - Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.
- **5. Téléchargez vos applications uniquement sur les sites officiels**
  - N'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater vos équipements. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streaming illégaux) qui pourraient également installer un virus sur vos matériels.
- **6. Sécurité numérique : méfiez-vous des messages inattendus**
  - En cas de réception d'un message inattendu ou alarmiste par messagerie (*email)*, SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par hameçonnage (*phishing*) visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce-jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.
- **7. Vérifiez les sites sur lesquels vous faites des achats**
  - Si le commerce en ligne facilite les achats et offre l'opportunité de faire de bonnes affaires, il existe malheureusement de nombreux sites de vente douteux, voire malveillants. Avant d'acheter sur Internet, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site officiel, la crédibilité de l'offre et consultez les avis. Sans cette vérification, vous prenez le risque de vous faire dérober votre numéro de carte bancaire et de ne jamais recevoir votre commande, voire de recevoir une contrefaçon ou un produit dangereux.
- **8. Maîtrisez vos réseaux sociaux**
  - Les réseaux sociaux sont de formidables outils de communication et d'information collaboratifs. Ils contiennent toutefois souvent de nombreuses informations personnelles qui ne doivent pas tomber dans de mauvaises mains. Sécurisez l'accès à vos réseaux sociaux avec un mot de passe solide et unique, définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire, ne relayez pas d'informations non vérifiées (*fake news*). (Voir notre fiche sur les réseaux sociaux).
- **9. Séparez vos usages personnels et professionnels**
  - Avec l'accroissement des usages numériques, la frontière entre utilisation personnelle et professionnelle est souvent ténue. Ces utilisations peuvent même parfois s'imbriquer. Matériels, messageries, « clouds »… Il est important de séparer vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise, ou inversement, que la compromission de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles. (Voir notre fiche sur les usages personnels et professionnels).
- **10. Sécurité numérique : évitez les réseaux WiFi publics ou inconnus**
  - En mobilité, privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) aux réseaux WiFi publics. Ces réseaux WiFi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire…). Si vous n'avez d'autre choix que d'utiliser un WiFi public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).
- ***Pour informer et sensibiliser les publics sur les menaces numériques, Cybermalveillance.gouv.fr met à disposition divers contenus thématiques : des supports variés pour comprendre les cybermenaces et savoir comment y réagir, ainsi que des bonnes pratiques à adopter pour assurer votre sécurité numérique.***
  > Consulter la liste de l'ensemble des ressources mises à disposition par le dispositif.

Quelques données Cyber du CESIN

- 3 minutes pour pirater un nouvel objet connecté
- 1,1 million de victimes de fraude à la carte bancaire par an
- +83 % de smartphones infectés au 2e semestre 2016
- 65 vols de données par seconde
- 41 % : le taux de succès d'un ransomware
- 201 jours pour découvrir une cyberattaque
- 1,7 milliard de publicités fraudeuses en 2016
- 140 attaques de phishing par heure
- Les particuliers deux fois plus infectés que les professionnels
- Une entreprise subit 29 cyberattaques par an

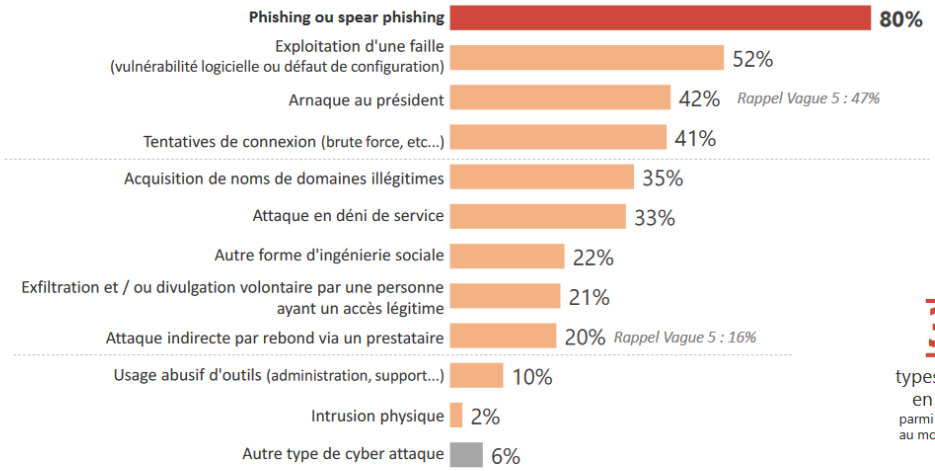
TOP 10 des attaques en France ou ayant une incidence

- Janvier 2019 : Cyberattaque d'Altran via cryptolocker paiement d'une rançon de 300 Bitcoins (1 M€) perte estimée : 20 M€
- Janvier 2019 : Attaque par hacker d'Airbus et récupération de données du personnel
- Février 2019 : Attaque de l'ICANN récupérer de données de l'annuaire d'internet
- Avril 2019 : Equateur / suppression du droit d'asile de Julian Assange nombreuses cyberattaques
- Mai 2019 : Attaque de la Ville de Baltimore neutralisation de 10 000 ordinateurs rançon de 89 000 $, perte estimée : ~ 32 M€
- Juin 2019 : Ransomware chez Eurofins leader mondial d'analyse Biologique impact de 35 % sur les résultats semestriels du groupe
- Octobre 2019 : Attaque de la ville de Cognac Rançon de 180 K€ perte de 150 K€
- Octobre 2019 : Attaque M6 par Ransomware de type TV5 monde comme en 2015 impact limité
- Novembre 2019 : Virus chez Edenred leader mondial solution de paiement dans le monde du travail
- Novembre 2019 : Attaque par rançon de l'Hôpital de Rouen (CHU) Blocage de machines et équipements électriques

Adware/Publiciel	Logiciel affichant c
Backdoor/Porte dérobée	Logiciel permettar de façon cachée.
Bot	Logiciel automatiq
Exploit	Logiciel permettar
Keylogger/Enregistreur de frappe	Logiciel permettar sur le clavier.
Ransomware/Rançongiciel	Logiciel qui cryp demande une ran
Rogue	Logiciel se faisant que le PC est gra désinfecter en éch
Rootkit	Logiciel permetta même] une infecti
Spammeur	Logiciel envoyant
Spyware/espiologiciel	Logiciel collectant
Trojan horse /Cheval de Troie	Logiciel permettar PC, il permet dérobée.
Ver/Virus réseau	Logiciel se propag

Le phishing, premier vecteur d'attaque dans les entreprises

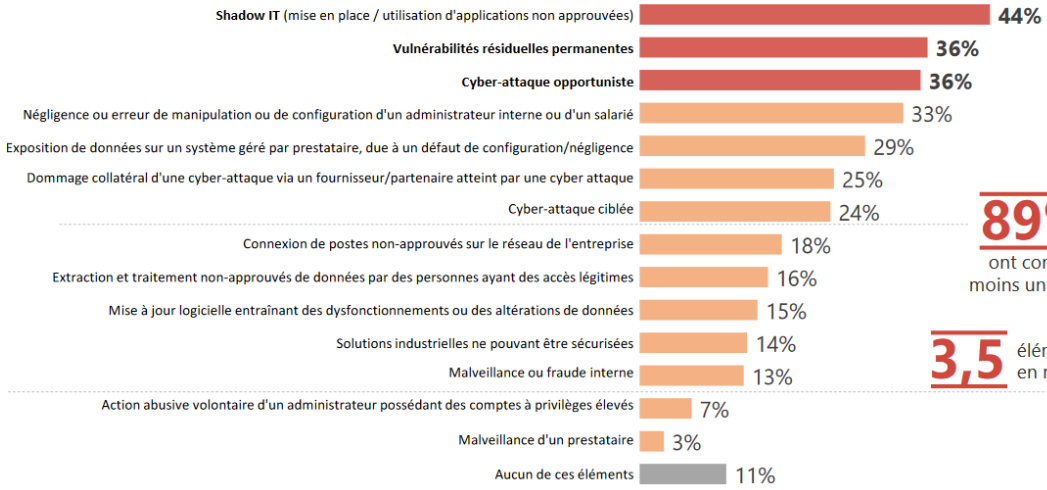
Q5A. Parmi les vecteurs d'attaques suivants, lesquels ont impacté votre entreprise au cours des 12 derniers mois ?
Base : ont constaté une attaque (129) / Plusieurs réponses possibles



3,6
types d'attaques en moyenne
parmi ceux ayant subi au moins une attaque

Le Shadow IT est la principale cause des incidents de sécurité rencontrés par les entreprises

Q6. Parmi les causes des incidents de sécurité rencontrées par l'entreprise, cyber-attaques incluses, quelles sont celles auxquelles votre entreprise a été concrètement confrontée au cours des 12 derniers mois ?
Base : ensemble (228) / Plusieurs réponses possibles

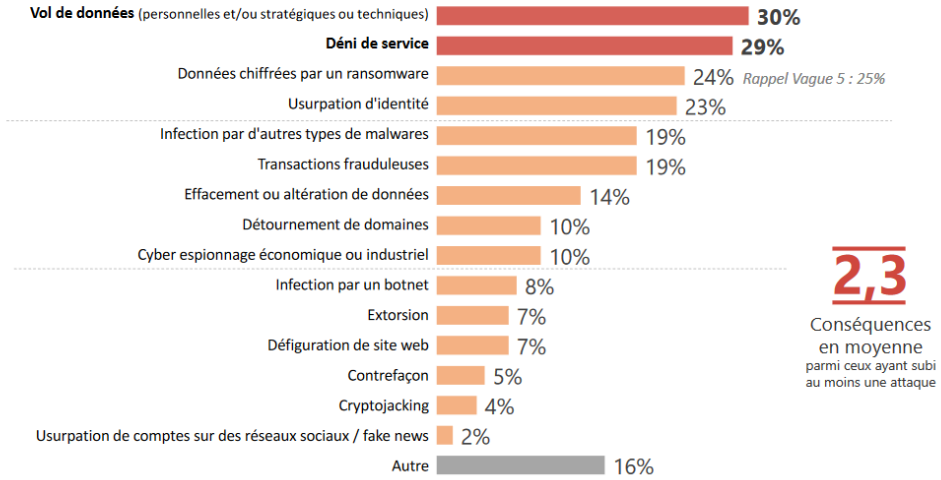


89%
ont connu au moins un élément

3,5 éléments en moyenne

Le vol de données et le déni de service sont les conséquences directes de ces attaques

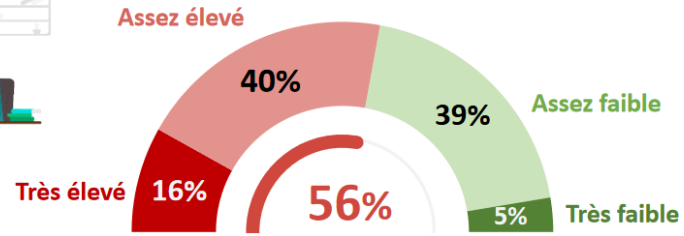
Q5B. Et quelles ont été les conséquences de cette/ces attaque(s) ?
Base : ont constaté une attaque (129) / Plusieurs réponses possibles



2,3
Conséquences en moyenne
parmi ceux ayant subi au moins une attaque

Plus de la moitié des entreprises considèrent que les menaces en lien avec le cyber-espionnage sont élevées

Q9. Aujourd'hui, comment évaluez-vous le niveau des menaces relatives au cyber-espionnage pour votre entreprise ?
Base : ensemble (228)



ESTIMENT UN NIVEAU ÉLEVÉ DES MENACES RELATIVES AU CYBER-ESPIONNAGE

Règlement Général sur la Protection des Données

Ce règlement issu de l'Union Européenne a pour but de protéger les données de toutes personnes physiques. Le texte constitué d'une centaine d'articles a été adopté et promulgué en Avril 2016, pour une entrée en vigueur le 25 Mai 2018.

Parmi les points clefs a retenir

1. *La mise en place de cadre harmonisé*
2. *L'application extra-territorial*
3. *Le consentement « explicite » et « positif » de la part des consommateurs*
4. *Le droit à l'effacement* des données
5. *Le droit à la portabilité des données personnelles*
6. *Le profilage client est soumis à contrôle voire aprobation*
7. *Les principes de « protection des données dès la conception » et de « sécurité par défaut »*
8. *Les notifications en cas de fuite de données*
9. *La possibilité de désigner un délégué à la protection des données* (*Data Protection Officer)*
10. *Les sanctions plus importantes* : le règlement donne aux régulateurs le pouvoir d'infliger des sanctions financières allant jusqu'à 4 % du chiffre d'affaires mondial annuel d'une entreprise ou 20 millions d'euros
11. *La création du Comité européen de la protection des données*
12. L'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement est encouragée (article 40 du règlement).