Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE
L'INTÉRIEUR

DELEGATION MINISTERIELLE AUX INDUSTRIES DE SECURITE ET A LA LUTTE CONTRE LES CYBERMENACES

État de la menace liée au numérique en 2017

Rapport n°1 – Janvier 2017

TABLE DES MATIÈRES

TABLE DES MATIÈRES

PREAMBULE

LE DELEGUE MINISTERIEL AUX INDUSTRIES DE SECURITE ET A LA LUTTE CONTRE LES CYBERMENACES

Le présent document est le premier rapport sur l'état de la menace, depuis qu'a été créée une délégation en charge du suivi des cybermenaces au ministère de l'Intérieur.

Dans un domaine – le cyberespace – qui se caractérise par une croissance exponentielle à un rythme jusqu'alors inconnu, décrire l'état de la menace est un exercice objectivement difficile.

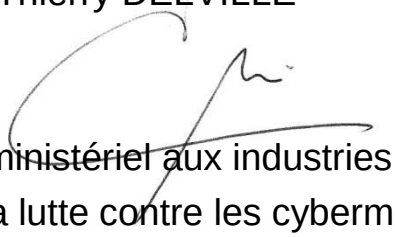
En premier lieu, car cet exercice est inédit, probablement parce que les faits de délinquance ou de criminalité apparus avec le développement de l'informatique ont pu être décrits à l'origine dans les catégories pénales existantes, sans que soit apparu le besoin de les identifier spécifiquement.

De fait, l'analyse de la cybercriminalité par les services du ministère de l'Intérieur n'est pour l'heure étayée par aucune donnée statistique globale, solide et homogène. L'objet des travaux engagés avec le service statistique ministériel de la sécurité intérieure consiste ainsi à concevoir un référentiel statistique en ce domaine, commun aux différents services du ministère. Les premiers résultats sont décrits dans la troisième partie de ce rapport au sein d'une revue plus large de l'action des services du ministère.

En second lieu, l'exercice est difficile, car la menace n'est pas un état stable, mais plutôt une succession particulièrement rapide d'états intermédiaires, si bien que pour rendre compte de la réalité de son objet, l'analyse doit être à la fois rétrospective et prospective, stratégique en somme.

Pour sa première édition, ce rapport vise donc essentiellement à fixer les principales menaces affectant les différentes cibles potentielles, sur un plan technique, et à en décrire les évolutions récentes ; il fait également un focus sur la dimension « cyber » des attentats qui ont frappé la France en 2015 et 2016.

Thierry DELVILLE



Délégué ministériel aux industries
de sécurité et à la lutte contre les cybermenaces

SYNTHESE

Partie 1 - Enjeux stratégiques

Priorités des cybercriminels

Les secteurs les plus touchés par les cybermenaces touchent à l'économie et aux flux financiers, tandis que plus généralement les données personnelles ou confidentielles sont de plus en plus souvent détournées pour être monnayées. Les secteurs de la santé et des objets connectés (ou des transports intelligents) seront particulièrement visés dans les années à venir. La protection des personnes vulnérables sur Internet (les enfants en particulier) reste une préoccupation importante.

Preuve numérique

L'accès à la preuve numérique est essentiel à l'investigation des cybermenaces, notamment pour celles qui sont réalisées intégralement sous forme numérique. Cela suppose la disponibilité de ces données, leur conservation et un régime juridique adapté permettant cet accès. L'évolution des pratiques des délinquants et les développements techniques nécessaires à la préservation de la vie privée ont entraîné un fort développement de l'usage des technologies de chiffrement et d'anonymisation. Enfin, certaines législations encadrant la conservation des données ont été remises en cause en Europe.

Partie 2 - Usages et phénomènes

Évolution des usages

Le taux de pénétration de l'Internet continue de progresser en France (84%) et dans le Monde (50%), et en particulier sur les réseaux sociaux parmi lesquels Facebook arrive en tête en France . L'évolution de l'usage des crypto-monnaies (comme Bitcoin) doit être suivie avec attention, tout comme le développement des objets communicants.

Attaques ciblées et vol de données

Les attaques ciblées concernent des secteurs de plus en plus variés : les PME comptent pour 60% des attaques recensées contre les entreprises et les secteurs clé restent ceux touchant aux gouvernements et à la défense. Le vol de données pour des motivations financières est en forte croissance, associé au développement de méthodes relevant du cyber-espionnage (intrusion au cœur des réseaux).

Diffusion de virus informatiques

Les rançongiciels et en particulier les rançongiciels chiffrants ou *cryptolockers* dominent l'actualité, mais on note aussi l'arrivée de nombreux virus ciblant les terminaux de point de vente. Les opérations de police parviennent à stopper de nombreuses activités de diffusion de virus informatiques, mais le terrain criminel est rapidement repris par des concurrents. Enfin, l'intérêt confirmé pour la diffusion de virus vers les utilisateurs de terminaux mobiles devrait logiquement appeler à la vigilance sur les véhicules connectés ou l'Internet des objets qui seront indéniablement les futures cibles de choix.

Coût de la cybercriminalité

La dimension économique de la cybercriminalité doit aussi pouvoir être mesurée par son coût - plusieurs centaines de milliards de dollars au plan mondial, souvent plusieurs millions d'euros de préjudice pour chaque entreprise victime d'un détournement de données, ou encore de quelques centaines d'euros à plusieurs dizaines de milliers d'euros pour chaque victime d'escroquerie en ligne.

Partie 3 - Action du ministère de l'Intérieur contre les cybermenaces

Le ministère de l'Intérieur s'est depuis longtemps mis en ordre de bataille pour faire face aux cybermenaces et s'adapte continûment, aujourd'hui avec la création de la délégation chargée de la lutte contre les cybermenaces (DMISC).

Partie 1 – Enjeux stratégiques liés aux cybermenaces

« La lutte contre les cybermenaces recouvre l'ensemble des actions menées en matière de lutte contre la cybercriminalité, de cyberdéfense, et de sécurité des systèmes d'information. »

1 Une nécessaire adaptation de la lutte contre les cybermenaces

À l'évolution des cybermenaces doit correspondre l'adaptation permanente des moyens de lutte contre les cybermenaces. Cette mutation passe par l'adaptation des méthodes d'investigation face à la masse de données, au développement d'équipements adaptés et de techniques spéciales d'enquête. Les procédures utilisées doivent garantir la recevabilité de la preuve numérique devant les juridictions, tout en garantissant la protection des libertés fondamentales.

Outre les enjeux techniques et procéduraux, le renforcement de la lutte contre les cybermenaces doit en effet assurer à la fois le respect des droits et des libertés et la protection de l'ordre public numérique qui incombe au ministère de l'Intérieur.

À cet égard, le ministère de l'Intérieur veille à ce que les évolutions législatives qu'il propose soient claires et précises et que les limites apportées à l'exercice des droits et libertés fondamentales soient strictement nécessaires à la défense de l'ordre et à la prévention des infractions et proportionnées à la finalité recherchée.

Ce principe de proportionnalité repose sur le point d'équilibre entre la protection des droits et libertés fondamentales, constitutionnellement et conventionnellement garantie et la nécessaire protection des citoyens, des autorités étatiques et de la nation face au développement des cybermenaces.

Les attentats terroristes des deux dernières années ont mis en exergue le recours aux technologies de l'information et de la communication dans la diffusion de propos provoquant ou faisant l'apologie du terrorisme. Par ailleurs, leur rôle indéniable dans la préparation des actes terroristes a conduit le ministère de l'Intérieur à renforcer sa stratégie de lutte contre les cybermenaces.

Cette réflexion appelle une connaissance précise de l'évolution des technologies de l'information et des communications mais également de l'impact du cadre européen et international dans lequel l'action du ministère de l'Intérieur s'inscrit.

1.1 Dimension numérique de la menace terroriste

Les organisations terroristes ont recours à Internet, notamment aux réseaux sociaux, et cet activisme, se matérialise, dans le domaine cyber[1], par un cyberdjihadisme particulièrement actif et visible. Les technologies de l'information et de la communication sont ainsi utilisées comme outil de propagande et d'influence à des fins de recrutement, d'accompagnement dans la radicalisation, de diffusion de messages hostiles et/ou d'appels à l'action terroriste, ainsi que pour la désignation de cible dans le monde physique. Ainsi, les cas d'apologie du terrorisme ont représenté, en 2015, 30 000 des 188 000 signalements et en 2016, 11 000 sur 171 000 signalements recensés par la sous-direction de la lutte contre la cybercriminalité.

Toutefois, les capacités de lutte informatique active des organisations terroristes demeurent limitées. Les attaques numériques par des personnes se revendiquant d'une telle organisation sont aujourd'hui circonscrites à des opérations de faible intensité, non coordonnées et n'affectant pas des entités ciblées. En effet, elles se caractérisent principalement par des défigurations et des attaques en déni de service. La campagne d'attaques intervenue après les attentats de janvier 2015 (non réitérée lors des attentats suivants) illustre bien l'état de la menace dans ce domaine.

Même si ces faits ne sont pas sans conséquences économiques et pourraient, pour certaines d'entre elles, s'approcher d'un acte de sabotage (en particulier les attaques en déni de service), aucune d'entre elles ne peuvent être, à ce stade, considérées comme des attaques informatiques constitutives de cyberterrorisme et attribuables à une organisation terroriste.

Dans la troisième partie de ce rapport, est présentée une description des observations et de l'action des services du ministère de l'Intérieur en réponse à cette menace terroriste qui a trouvé à s'exprimer de nombreuses fois sous forme numérique entre 2015 et 2016.

1.2 Enjeux économiques des cybermenaces

La réalité des cybermenaces motivées par l'appât du gain, le sabotage et l'espionnage pour obtenir un avantage concurrentiel pèse sur les organisations, d'un point de vue financier, notamment lorsqu'elles sont victimes d'une fraude au président ou d'un cryptovirus par exemple et réputationnel lorsqu'une défiguration d'un site par des *hacktivistes* ou son déni de service a lieu, car l'activité est entravée et le crédit de l'organisation entamé.

Les organisations doivent absolument prendre la mesure de la gravité des menaces car elles risquent d'engager leur responsabilité voire celle de leur sous-traitant (règlement européen sur les données personnelles GDPR) et de disparaître.

C'est pourquoi, la prévention se traduit aujourd'hui prioritairement par la formation ou la sensibilisation des personnels qui restent le maillon faible de la cybersécurité. Car il ne sert à rien d'ériger des cyberdéfenses en château-fort coûteuses, si d'un clic on peut abaisser le pont-levis.

[1] L'activisme qui s'illustre dans le domaine cyber est également désigné sous le terme d'hacktivisme.

Escroquerie en ligne et blanchiment

En décembre 2014, la BFMP recueillait une plainte contre un site d'achats proposant une vente privée en ligne de vêtements de marque, à des prix très attractifs relayés par des spots radiophoniques. L'enquête révélait une escroquerie en bande organisée mettant en scène un faux site Internet sur lequel les clients avaient en 20 jours pour 2 900 commandes jamais honorées, réglé 603 000€ via un compte bancaire domicilié à Paris d'où 400 000€ étaient virés vers la Chine. Le gérant de la société identifiée, prenait la fuite après avoir organisé et ventilé la collecte des fonds vers l'étranger et son exil doré. Le solde de l'e-escroquerie 200 000€ était saisi sur ce compte. 42 000 € étaient saisis à ses co-auteurs ayant créé le faux site et réalisé la campagne marketing. Ils étaient incarcérés ainsi que le gérant d'un négoce d'or et de bijoux Parisien qui participait au blanchiment de l'escroquerie, en se chargeant du recrutement des mules, des commerçants indélicats de la région parisienne collectant sur leur compte bancaire à l'étranger les fonds escroqués qu'ils lui reversaient en espèces, moyennant un pourcentage.

1.2.1 Le développement du marché de la cybersécurité

La valeur économique d'une entreprise se mesure désormais à son degré d'exposition aux cyber-risques; l'offre de cybersécurité s'est accrue sensiblement et les entreprises du secteur sont désormais en mesure de proposer des solutions adaptées à chacune.

Selon l'étude du pôle interministériel de prospective et d'anticipation des mutations économiques (PIPAME)[1] présentée à l'occasion du salon MILIPOL 2015, la cybersécurité représenterait en effet 10% du CA marchand de la filière nationale de la sécurité et 6% des emplois du secteur marchand. Le nombre d'entreprises françaises concerné serait estimé à 600 dans la filière cybersécurité.

Toujours selon cette étude, ce secteur bénéficie d'opportunités réelles de développement avec la prise de conscience des enjeux de sécurité, des réglementations nouvelles, l'émergence de thèmes nouveaux (objets connectés, villes intelligentes, automobiles connectées, transformation numérique, « privacy by design », diversification de la cybercriminalité, etc...).

Dans le même temps, le développement du marché de la cyber-assurance dédié à la couverture des risques liés à la cybercriminalité, permet aux entreprises de mieux se prémunir des coûts liés à une cyber-attaque, et de bénéficier rapidement le cas échéant, de l'assistance d'experts mobilisés et financés par l'assureur.

1.2.2 Contre-ingérence économique

Les cybermenaces reposent sur des attaques techniques et organisationnelles. Au-delà des enjeux liés à l'espionnage, au sabotage ou au terrorisme, ces cyberattaques sont aussi susceptibles d'avoir un objectif d'ingérence économique.

[1] Etude PIPAME pilotée par le Ministère de l'intérieur (DMIS), avec le concours du SGDSN, de l'ANSSI, et de la DGE en partenariat avec HexaTrust, Systematic, EDEN, pôle SCS, Cluster CNCS by Euratechnologies, la MEITO, PRISSM, couvrant une large partie du territoire national.

Elles peuvent ainsi être le moyen de capter une technologie ou un savoir-faire, d'acquérir une information stratégique, d'effectuer un chantage ou d'exiger une rançon, etc. Elles peuvent également avoir pour but de déstabiliser un acteur économique, une autorité de régulation ou encore un groupe de consommateurs pendant une période stratégique (contexte de fusion acquisition, congés, publication d'un bilan, fin d'exercice budgétaire, etc...) en altérant le fonctionnement, la productivité ou encore en neutralisant tout ou partie des capacités de la cible, pendant un temps donné.

Ces aspects, liés au maintien d'avantages concurrentiels des entreprises nationales, constituent un enjeu majeur pour les économies de marché occidentales, au sein desquelles les récentes crises ont affaibli nombre d'acteurs (baisse des commandes, besoins accrus en trésorerie, mouvements sociaux, etc...).

Les ingérences sont susceptibles d'intervenir tout au long de la vie d'un organisme, à l'occasion de la participation à un séminaire, à un salon ou à un concours, lors d'une campagne de prospection commerciale, de tentative de pénétration d'un marché étranger ou lors de la négociation d'une augmentation de capital.

Les atteintes au potentiel (scientifique, technique, économique, industriel, etc...) de la Nation résultant d'une cybermenace peuvent donc provoquer des dégâts considérables sur l'économie du pays, agir comme vecteur de déstabilisation et nuire, in fine, à la capacité de l'État à exercer sa pleine souveraineté et à agir indépendamment des interférences extérieures.

1.3 Enjeux sociétaux des cybermenaces

Les dispositifs numériques sont aujourd'hui utilisés par l'ensemble de nos institutions et de nos systèmes administratifs et industriels. Les cyberattaques, après une première phase de développement, ne constituent plus un risque conjoncturel mais sont devenues systémiques.

La réponse ministérielle doit être du même ordre et ne peut se concevoir en dehors du contexte sociétal. Elle doit appréhender en particulier l'interdépendance et la porosité entre les domaines physique et cyber (exemple : riposte militaire à une attaque cyber ou campagne d'hacktivisme consécutive à un attentat terroriste).

Il est essentiel que les capacités de défense soient supérieures aux capacités d'attaque, afin de limiter l'efficacité des cyberattaques et, in fine, de protéger les populations et les intérêts économiques et sociaux de la Nation. La pérennité des infrastructures résultera, en particulier, de :

- L'incapacité des adversaires à surprendre ;
- La capacité de l'État à disposer d'une avance technologique, organisationnelle, intellectuelle et culturelle suffisante pour rendre plus difficiles la montée en compétence des agresseurs ainsi que l'augmentation de leurs capacités d'attaque ;
- La capacité des populations à ne pas être utilisées en tant que vecteurs d'attaques ;
- La capacité de développer une culture de la résilience.

1.4 Santé publique et cybermenaces

Vecteur de commercialisation mondial, Internet fournit aux trafiquants de faux médicaments un outil idéal pour une distribution à grande échelle de leurs produits. Le trafic de faux médicaments ne cesse ainsi d'augmenter partout dans le monde. La distribution illicite de médicaments, en plein essor sur Internet, comporte des dangers sérieux pour la santé du consommateur. Le manque à gagner et la responsabilité potentielle des laboratoires pharmaceutiques impliquent la mise en œuvre de stratégies de protection à la fois pour la santé des patients et la propriété intellectuelle.

Opération PANGEA

La neuvième opération "Pangea", vaste coup de filet mondial contre le trafic de faux médicaments, a permis l'arrestation de 393 suspects et la saisie de millions de produits potentiellement dangereux d'une valeur estimée à 53 millions de dollars (46,8 millions d'euros). L'opération a rassemblé les polices de 193 pays, du 30 mai au 7 juin 2016 et a permis la saisie d'environ 12,2 millions de faux médicaments et la suspension de 4.932 sites Internet proposant ces produits délictueux. Près de 700 enquêtes ont été lancées à travers le monde.

Interpellation de revendeurs de stupéfiants sur le *darkweb*

A la suite d'une surveillance d'initiative effectuée sur un site francophone du darkweb nommé « Dream Market », les enquêteurs du C3N ont identifié des revendeurs de stupéfiants (résine, herbe, héroïne, spice). Ceux-ci diversifiaient leurs activités illicites par la vente de médicaments (Subutex, Skénan, Kétamine), de fausse monnaie et d'armes. En co-saisine avec la SR Strasbourg (67), les investigations techniques et les surveillances ont finalement permis l'interpellation de 3 individus en juin 2016. Des produits en cours d'expédition, deux pistolets d'alarme et d'auto-défense et du matériel informatique et téléphonique ont été saisis. A l'issue de leur garde-à-vue, les suspects ont été placés en détention provisoire.

1.5 L'évolution des caractéristiques des technologies de l'information et des communications

Une utilisation de plus en plus accrue des outils d'anonymisation

Depuis les révélations d'Edward Snowden en juin 2013 qui ont démontré la mise en place de programmes américains et britanniques de surveillance de masses dépassant le cadre de la lutte contre le terrorisme ou contre les risques géopolitiques, il a été constaté une utilisation exponentielle des outils d'anonymisation. Ainsi, un pic d'utilisation de Tor a été mesuré à partir du mois de septembre 2013 (voir figure 1 ci-dessus). Par ailleurs le

nombre moyen d'utilisateurs directs quotidiens de Tor en France est passé de 50.000 à près de 100.000 aujourd'hui.

Sans qu'il y ait de chiffres objectifs, les services d'enquête ont de même noté une augmentation de l'utilisation d'autres types de services d'anonymisation tels que la location de serveurs relais[1] positionnés dans différents pays, notamment européens.

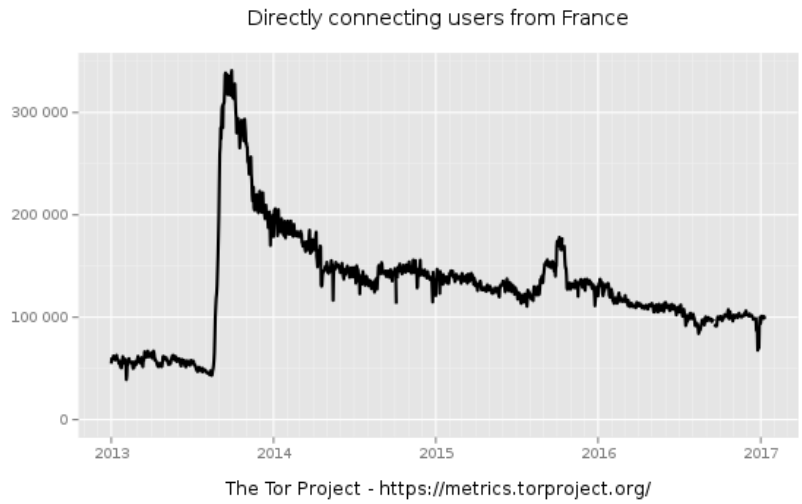


Figure 1 - Nombre d'utilisateurs directs de Tor en France

Vers une généralisation du chiffrement

Parallèlement à l'utilisation de plus en plus accrue des outils d'anonymisation, on assiste à une quasi-généralisation du chiffrement. Les récents attentats ont ainsi mis en évidence le rôle décisif des services de communication par voie électronique, et plus spécifiquement des messageries chiffrées, dans la préparation et la réalisation d'actes terroristes.

Ces outils posent des difficultés pratiques et juridiques aux enquêteurs et à l'autorité judiciaire. En effet, certaines données leur sont inaccessibles parce que stockées sur un appareil verrouillé (ordinateur, tablette, smartphone), d'autres sont accessibles mais inintelligibles parce que chiffrées.

Le **chiffrement des données stockées** sur un appareil saisi rend beaucoup plus difficile le recueil d'une éventuelle preuve exploitable de participation de l'utilisateur de l'appareil à une infraction.

Le **chiffrement des communications électroniques** rend par ailleurs inefficaces les interceptions de données échangées entre suspects sur les réseaux de télécommunications.

Dès lors, les services enquêteurs sont obligés de recourir de plus en plus souvent à des experts pour mettre au clair le contenu des communications chiffrées. Or, ces opérations d'expertise prennent du temps et se révèlent coûteuses.

[1] Egalement désignés sous la terminologie VPN pour *Virtual private network*

De plus, même si le législateur a prévu des sanctions pénales en cas de refus de communication de la convention de déchiffrement ou de refus de sa mise en œuvre alors que le chiffrement a été utilisé à des fins criminelles, de nombreux prestataires déclarent ne pas avoir la possibilité de déchiffrer les communications, régulièrement car leurs produits ont été spécifiquement développés dans un tel but.

Les ministres de l'intérieur français et allemands ont exprimé dans des courriers conjoints du 23 août et du 28 octobre 2016 leur souhait de voir le Conseil de l'Union européenne et la Commission se saisir de cette problématique afin d'élever le débat au niveau européen et de permettre que des solutions communes soient dégagées sur le sujet.

Aux problèmes techniques posés par le chiffrement en matière d'enquête, s'ajoute la complexité des réquisitions lorsque les prestataires ne sont pas établis dans l'Union européenne et qu'il est nécessaire de recourir à une demande d'entraide judiciaire. La complexité et l'efficacité des réquisitions peuvent être rendues encore plus complexes en cas de localisation des données de ce prestataire au sein de pays différents[1] notamment en matière de juridiction compétente ou d'entraide pénale. Cela peut alors susciter d'autres questions tenant à la localisation des données et à la détermination des juridictions territorialement compétentes pour y accéder.

1.6 L'évolution du cadre législatif et jurisprudentiel international et européen

Le ministère de l'Intérieur veille à l'adaptation des textes législatifs et réglementaires aux évolutions technologiques et comportementales en matière cyber, notamment en ce qu'ils permettent de poursuivre et de sanctionner les nouvelles formes de cybercriminalité.

La législation française s'adapte progressivement aux contraintes de l'enquête judiciaire ou des actions de prévention relatives aux cybermenaces.

Au plan européen et international, toutefois, certaines de ces évolutions sont loin d'être harmonisées et rencontrent des obstacles techniques, juridiques et politiques.

1.6.1 Le suivi des travaux au sein de l'assemblée générale des Nations Unies

Un projet de résolution sur le droit à la vie privée à l'ère numérique a été présenté par l'Allemagne et le Brésil à l'Assemblée générale des Nations Unies. Ce sujet a d'ores et déjà retenu l'attention des autorités françaises avec l'adoption de la loi du 30 novembre 2015[2]. L'angle choisi est celui de la responsabilité des entreprises, notamment dans la collecte et l'exploitation des données personnelles.

[1] Le 14 juillet 2016, une des Cours fédérales aux Etats Unis a ainsi considéré que les autorités de poursuite américaines étaient territorialement incompétentes pour obtenir les données électroniques stockées à l'étranger. Dans cette affaire Microsoft Corporation v. USA, débutée en 2013 dans une procédure d'infraction à la législation sur les stupéfiants, un juge de l'État de New York avait émis un mandat de perquisition à l'encontre de Microsoft, afin d'obtenir la communication des données de contenus d'un compte email stockées sur un serveur en Irlande.
[2] Loi n° 2015-1556 du 30 novembre 2015 relative aux m esures de surveillance des communications électroniques internationales.

1.6.2 Les travaux du Conseil de l'Europe en matière cybercriminalité

A ce jour, la convention du Conseil de l'Europe sur la cybercriminalité[1] signée le 23 novembre 2001 à Budapest est le seul instrument international contraignant en matière de cybercriminalité. Elle sert de lignes directrices pour tout pays élaborant une législation exhaustive dans ce domaine, mais aussi de cadre pour la coopération internationale avec les États parties. Elle comporte tout à la fois des dispositions communes en matière d'infractions pénales (atteintes aux systèmes de traitement automatisé de données, pédopornographie, propriété intellectuelle), de droit processuel et de coopération internationale.

Elle est par ailleurs complétée par le protocole relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

Parmi les 47 membres du Conseil de l'Europe, seuls deux États n'ont pas encore signé la convention : Russie et Saint-Marin, et quatre ne l'ont pas ratifiée : Grèce, Irlande, Monaco et Suède.

La convention est entrée en vigueur dans neuf États non-membres du Conseil de l'Europe : Australie, États-Unis d'Amérique, Japon, Maurice, Panama, République Dominicaine, Sri Lanka, Canada, Israël et bientôt 10 avec le Sénégal pour lequel la convention entrera en vigueur le 1er avril 2017.

Le ministère de l'Intérieur dans le cadre des réunions du Comité de la Convention sur la cybercriminalité (T-CY), a suivi avec attention le **projet de note sur l'interprétation de l'article 18 de la Convention de Budapest**, qui invite les parties à prendre les mesures nationales permettant à leurs autorités de requérir d'une part, toute personne présente sur son territoire afin de se faire communiquer des données informatiques (article 18 §1 a), et d'autre part, les fournisseurs de services (FSI) offrant des prestations sur son territoire afin de se faire communiquer les données relatives à leurs abonnés (article 18 §1 b).

Par ailleurs, il a été annoncé qu'en 2017 des négociations débuteraient pour **l'élaboration d'un protocole additionnel à la convention portant sur l'accès et l'échange de preuves numériques**. Ces négociations seront suivies par le ministère de l'Intérieur avec la plus grande attention.

1.6.3 L'impact des directives et règlements européens et de la jurisprudence de la CJUE dans la lutte contre les cybermenaces

Plusieurs textes récents ou en discussion ont ou vont avoir un impact sur les cybermenaces en Europe, en fonction de leur caractère plus ou moins contraignant, de leur champ d'application et de la rapidité de leur transposition dans les droits nationaux. A ce titre, on peut citer :

- La directive 2011/93/UE[2] du Parlement européen et du Conseil du 13 décembre 2011 relative à **la lutte contre les abus sexuels et l'exploitation sexuelle des enfants**,

[1] http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm
[2] http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32011L0093

ainsi que la pédopornographie et remplaçant la décision-cadre 2004/66/JAI du Conseil. La France a procédé à sa transposition par la loi n°2013-711 du 5 août 2013 [1]

- La directive 2013/40/UE[2] du Parlement européen et du Conseil du 12 août 2013 relative aux **attaques contre les systèmes d'information** et remplaçant la décision-cadre 2005/222/JAI du Conseil. La France est conforme à cette directive et a procédé à des compléments de transposition avec le décret n° 2015 -351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale, les arrêtés de juin et août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives à chaque secteur ou sous-secteur d'activités d'importance vitale et la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

- Le règlement 2016/679/UE[3] du 27 avril 2016 relatif à la **protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données**, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et la directive 2016/660 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, ainsi que la décision-cadre 2008/977/JAI du Conseil. Cette directive devra être transposée pour le 6 mai 2018.

- La directive 2016/1148/UE[4] du 6 juillet 2016 concernant des mesures destinées à assurer un **niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union** (directive NIS). Cette directive devra être transposée avant le 9 mai 2018. Les travaux de transposition au niveau national seront pilotés par l'ANSSI. Le résultat des travaux de transposition devraient aussi avoir des conséquences sur les relations entre acteurs de cybersécurité au niveau national.

- La révision de la directive **service de médias audiovisuels** (SMA) 2010/13/UE[5] qui vise notamment à assurer la libre prestation de ces services au sein de l'Union. Elle prévoit notamment que les services de médias audiovisuels ne peuvent contenir aucune incitation à la haine fondée sur la race, le sexe, la religion ou la nationalité. La Commission a déposé une proposition de révision de cette directive visant notamment à **inclure les services de plateforme de partage de vidéos dans le champ d'application** tout en faisant bénéficier ces opérateurs d'un régime différencié avec des obligations moindres.

- La proposition de directive du Parlement européen et du Conseil relative à la **lutte contre le terrorisme**[6] en remplacement de la décision cadre 2002/475/JAI qui définit les infractions de nature terroriste et prévoit des peines minimales correspondantes. Elle oblige les États-membres à incriminer la provocation publique à commettre une

[1] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000027805521&categorieLien=id
[2] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32013L0040
[3] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
[4] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016L1148
[5] http://eur-lex.europa.eu/search.html?qid=1484576708515&PROC_NUM=0151&DB_INTER_CODE_TYPE=OLP&type=advanced&PROC_ANN=2016&lang=fr
[6] http://www.consilium.europa.eu/fr/press/press-releases/2016/03/11-directive-on-combatting-terrorism/

infraction terroriste. Il semble désormais acquis que ce nouveau texte comprendra une obligation pour les États membres de prévoir des mesures de retrait des contenus en ligne faisant l'apologie du terrorisme s'ils sont hébergés sur leur territoire, dispositions que nous avons déjà en droit français (Article 14a). Par ailleurs, ce texte traite à l'article 21a des techniques spéciales d'enquête et indique à ce jour que les États-membres doivent prendre les mesures nécessaires afin d'assurer l'effectivité des techniques spéciales d'enquête telles que la captation de données.

- La décision-cadre 2008/913/JAI[1] relative à la **lutte contre le racisme et la xénophobie** incrimine l'incitation publique à la violence ou à la haine visant un groupe de personnes ou un membre d'un tel groupe, défini par référence à la race, la couleur, la religion, l'ascendance, l'origine nationale ou ethnique. En mai 2016, la Commission a conclu avec les principales plateformes (Facebook, Twitter, YouTube et Microsoft) un **code de conduite**[2] sur la lutte contre les discours de haine en ligne. Les opérateurs s'engagent notamment à examiner rapidement (24 heures) les demandes de retrait de contenus haineux. La mise en œuvre de ce code de conduite sera suivie par le groupe à haut niveau sur la lutte contre le racisme, la xénophobie et les autres formes d'intolérance.

- Depuis le second semestre 2015, il est discuté des difficultés liées à **l'obtention de preuves électroniques dans le cadre des procédures pénales**. Ces discussions ont abouti à l'adoption en juin 2016 de conclusions par le Conseil sur l'amélioration de la justice pénale dans le cyberespace[3]. La Commission est chargée de suivre la mise en œuvre de ces conclusions et doit produire deux rapports en décembre 2016 et juin 2017. Pour l'assister dans ces travaux, elle s'appuie sur un groupe d'experts informel comprenant des représentants des autorités des États membres et des personnes issues de la société civile. Trois axes de réflexion ont été identifiés par la Commission : favoriser la **rapidité des échanges d'informations en matière d'entraide judiciaire par la mise en place d'outils** adaptés ou leur amélioration (mesure pratique), réfléchir à de **nouveaux critères de compétence territoriale** (mesure législative), renforcer la **coopération avec les prestataires de services étrangers** (mesure pratique).

Jurisprudence

Par un arrêt du 21 décembre 2016[4], la Cour de justice de l'Union européenne vient de se prononcer dans deux affaires portant sur l'obligation générale imposée aux fournisseurs de services de communications électroniques de conserver les données relatives à ces communications en Suède et au Royaume-Uni. La CJUE a indiqué que le droit de l'Union, à savoir la directive *vie privée et communications électroniques* 2002/58/CE, lue à la lumière de la Charte des droits fondamentaux de l'Union Européenne, s'opposait à une réglementation nationale prévoyant une conservation généralisée et indifférenciée des données de trafic et supposait que l'accès aux données conservées s'effectue après un contrôle préalable par une juridiction ou une autorité administrative indépendante.

[1] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV:l33178
[2] http://europa.eu/rapid/press-release_IP-16-1937_fr.htm
[3] http://www.consilium.europa.eu/fr/press/press-releases/2016/06/09-criminal-activities-cyberspace/
[4] http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=557470

Ces arrêts font suite à l'annulation de la directive européenne n°2006/24/CE, harmonisant les obligations de conservation de ces données à l'échelle européenne, par la Cour de Justice de l'Union Européenne le 08 avril 2014, dans son l'arrêt dit Digital Rights Ireland[1].

1.7 A quels défis faut-il se préparer?

L'exercice prévisionnel des risques futurs se révèle souvent infructueux, toutefois il est important de regarder de l'avant et le parcours des nouveaux usages et des phénomènes émergents proposés dans la seconde partie de ce rapport peut aider à y répondre. Toutefois les synthèses proposées par les organisations internationales apportent des éclairages intéressants.

1.7.1 La vision européenne proposée par Europol

Europol publie chaque année au mois d'Octobre un rapport intitulé Internet Organised Crime Threat Assessment ou iOCTA[2]. Le point le plus important mis en avant dans le rapport publié en 2014 est peut-être l'avènement d'une criminalité numérique organisée reposant sur les services, avec en corollaire un renforcement du positionnement du crime organisé classique, parce qu'il peut faire appel à ces services. C'est aussi le « darknet », soit toutes les formes de communications anonymisées et surtout la mise à disposition de services et de produits criminels sur des plates-formes anonymisées qui marque l'année qui vient de se passer.

En mars 2015, Europol publiait un rapport complémentaire sur l'évolution du crime organisé[3] qui inclut de nombreuses notions liées au développement des cybermenaces dont les conclusions recoupent les précédentes.

Le rapport iOCTA 2015[4] identifie un certain nombre de points clés des évolutions les plus récentes, parmi lesquels on peut citer :

- Une posture plus agressive des délinquants, avec des modes d'action relevant de plus en plus souvent de l'extorsion: *sextorsion*, rançongiciels chiffrants, demandes de rançon à des entreprise suite au détournement de leurs données confidentielles ;
- La croissance du nombre et de l'ampleur des **détournements de données** révélés ;
- Les logiciels malveillants sont une menace croissante, avec une évolution dans le domaine des botnets bancaires avec l'irruption de Dridex ;
- La **fraude au président** (ou fraude au faux virements) ne semble plus concerner principalement la France, mais de nombreux pays occidentaux avec des formes de plus en plus sophistiquées d'accès aux informations permettant l'ingénierie sociale ;
- En matière d'atteintes aux mineurs, les craintes sont partagées du développement inquiétant des **abus sexuels filmés en direct**, en relation avec la progression de l'accès à des connexions haut débit dans les pays les plus pauvres ;

[1] http://curia.europa.eu/juris/documents.jsf?num=C-293/12
[2] https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta
[3] https://www.europol.europa.eu/sites/default/files/edi/EuropolReportDigitalToC.html
[4] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2015

- La plus grande sécurité de l'usage physique des cartes bancaires (EMV, géoblocage et dispositifs *anti-skimming*) emporte une progression relative des fraudes dites « carte non présente », par exemple suite au détournement de bases de données.

Cette vision a bien été confirmée par les faits. Du **rapport produit par Europol en 2016**[1] on peut retenir complément des constats de 2015 les tendances suivantes :

- Les **rançongiciels chiffrants** sont devenus la première menace parmi les logiciels malveillants ;
- L'intérêt de certains groupes criminels organisés pour les **technologies de paiement sans contact** (NFC) ;
- Les **attaques en déni de service** (DDoS) sont un mode opératoire en croissance, via des stressers (directement depuis des serveurs) ou grâce à des botnets ;
- Les **cryptomonnaies** et en particulier le ***bitcoin*** sont devenus le moyen transactionnel de choix pour les échanges financiers entre cybercriminels ;
- L'**utilisation des technologies de chiffrement** pour protéger les communications entre délinquants ou stocker leurs informations sont dorénavant un défi important pour les services d'enquête.

[1] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

1.7.2 Synthèse des défis à venir

De l'ensemble des constats abordés précédemment, on peut tirer une liste de défis auxquels les États et notamment la France sont confrontés et doivent se préparer :

- **L'augmentation de la surface d'attaque** est soutenue par l'arrivée permanente de nouvelles technologies et de nouveaux usages : objets connectés, nouveaux services de l'informatique en nuage, nouveaux systèmes de paiements ou encore les projets de villes intelligentes ;
- **Le débat[1] relatif au chiffrement des données demeure complexe**, entre protection des données à caractère personnel ou confidentielles et efficacité des enquêtes. Qu'il s'agisse des affaires les plus graves liées à des échanges entre terroristes présumés ou au sein des groupes criminels organisés, ou des affaires de droit commun.
- La prise de conscience de l'enjeu de la gestion de l'information est d'autant plus fort actuellement que les cas de **détournements de données** dans les réseaux des administrations et des entreprises se multiplient.
- **L'accompagnement du développement de l'offre de cybersécurité**, y compris dans sa dimension assurancielle.
- Plus généralement, l'importance de l'**échange d'information avec l'ensemble des acteurs concernés**, entreprises, associations et monde académique, détenteurs de l'information et partenaires dans le développement de solutions qui préservent la souveraineté des États.
- Outre l'émergence de **nouvelles formes de criminalité organisée**, l'importance de la **dimension sérielle** de la cybercriminalité et donc la nécessité de collecter et d'analyser une grande masse d'informations auprès des victimes et des partenaires.
- **L'ensemble des espaces cachés de l'Internet connaissent un regain d'intérêt**, pour des raisons louables de préservation de la vie privée, mais aussi pour des motifs de camouflage des activités illégales. Cette tendance complexifie le travail des services d'enquête et confirme la nécessité d'une veille technologique permanente.
- **Des nouvelles formes d'action terroriste se profilent**, grâce aux moyens financiers importants des groupes terroristes, leur capacité d'influence ou de manipulation et la disponibilité de cybercriminels offrant leurs services au plus offrant.
- La **maîtrise de la sécurisation de l'identité numérique des citoyens** dans leur relation avec l'administration ou l'entreprise, enfin, est toujours une préoccupation majeure.

[1] Dans le rapport iOCTA 2015, Europol propose une synthèse de cette problématique dans sa première annexe.

PARTIE 2 - USAGES ET PHENOMENES

Les principaux enjeux stratégiques ayant été identifiés, il convient de revenir sur le détail des **usages des citoyens et des entreprises**, ainsi que sur les **phénomènes observés**. Cette approche permet éventuellement de confirmer les enjeux identifiés ou d'envisager des enjeux émergents auxquels il faut se préparer.

T**out nouveau produit ou service numérique est une cible potentielle des cybermalveillances**. De même **toute vulnérabilité dans les systèmes et les plateformes numériques sera systématiquement exploitée**.

2 Usages

Mi 2016, le taux de pénétration de l'Internet[1] est de 50,1 % au niveau mondial, 73,9 % en Europe, 83,8 % en France. La croissance de l'Internet mobile[2] est la plus forte dans les régions en voie de développement et à la fin de l'année 2016, le taux de pénétration de ces équipements y atteint 41 %.

Les sites Internet les plus visités en France[3] sont en octobre 2016 Google, Facebook, Youtube, Microsoft, Orange, Leboncoin, Wikipédia, Amazon, puis Windows Live, Skype, Pages Jaunes et Free (Iliad).

L'usage des réseaux sociaux[4] est évidemment en hausse, avec 1,8 à 2,3 milliards d'utilisateurs au niveau mondial selon les estimations avec un nombre d'utilisateurs réguliers en septembre 2016 de 1,71 milliards pour Facebook, 1 milliard pour Whatsapp, ou encore 313 millions pour Twitter. Le classement est évidemment variable dans les différents pays, avec un taux d'usage important des réseaux sociaux chinois (comme QQ avec 899 millions d'utilisateurs dans le monde) ou russes (comme Vkontakte avec 100 millions d'utilisateurs) dans leurs pays d'origine. Le taux de pénétration des grands réseaux sociaux en France est de 50 % (nombre de comptes par rapport à la population[5]) et une durée moyenne d'utilisation quotidienne de 1,3 heures (contre 3,2 heures en Argentine par exemple). En France[6], les réseaux sociaux les plus importants sont Facebook (43 % d'utilisateurs), Google+ (11 %), Twitter (11 %), Instagram (7%), LinkedIn (6 %), Pinterest (5 %).

Les achats en ligne[7] se développent avec 77 % des habitants ayant réalisé un achat au cours de l'année 2015 au Royaume-Uni, 66 % aux USA ou encore 64 % en France. La banque en ligne quant à elle est utilisée par 23 % des français.

D'autres types d'usage sont intéressants à mesurer. Le Bitcoin, la plus célèbre des crypto-monnaies, serait ainsi acceptée[8] par plus de 100.000 commerces dans le Monde, y compris des grandes sociétés comme Microsoft, Dell ou Paypal.

[1] http://www.internetworldstats.com/
[2] http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf
[3] http://www.mediametrie.fr/internet
[4] http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
[5] We Are Social Singapour http://fr.slideshare.net/wearesocialsg/
[6] Ibid.
[7] Ibid.
[8] http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613

Le projet TOR qui autorise l'anonymisation des connexions Internet serait utilisé par un peu plus de 1,7 millions d'utilisateurs réguliers dans le Monde (dont 100.000 en France en 2016, chiffre en forte baisse par rapport à 2015)[1].

Enfin, dans les années à venir, le taux de pénétration de l'Internet des objets dans les entreprises et chez les particuliers devra être observé. Les chiffres publiés actuellement sont le plus souvent des projections et dans beaucoup de cas ne font pas toujours la distinction entre les différentes catégories d'objets connectés concernés (communication entre machines, véhicules connectés, objets portés sur les personnes, etc.).

3 Mesures de la menace cyber

La mesure de la menace cyber, lorsqu'elle est réalisée par les éditeurs de solutions de sécurité peut être discutée et parfois manquer d'activité. En effet, ils pourraient avoir tendance à souligner de façon exagérée les risques encourus par leurs parcs de clients ou de prospects. Surtout, leur mesure peut être faussée par la répartition de leur clientèle dans les différentes régions du monde.

De nombreux autres angles de mesure de la menace sont proposées dans les pages qui suivent, tant sous l'angle des évolutions techniques que de la façon dont elles sont perçues par les victimes.

3.1 Perception de la menace par les entreprises

Selon l'étude « Sécurité numérique et médias sociaux dans les entreprises en 2015 » de l'INSEE, cette année-là:

- Parmi les entreprises de 10 salariés ou plus de France métropolitaine, 7% ont subi une destruction ou altération de données due à l'attaque d'un programme malveillant ou à un accès non autorisé ;
- 3% des sociétés ont subi une indisponibilité des services TIC, destruction ou altération de données due à une attaque extérieure (déni de service par exemple) ;
- Et 2% une divulgation de données confidentielles due à une attaque par intrusion, pharming ou phishing.

Le constat du CLUSIF dans l'enquête « Menaces informatiques et pratiques de sécurité 2016 »[2] qui concerne cette fois-ci les entreprises de plus de 200 salariés et relève des taux de tentatives, réussies ou non :

- 44% ont subi une atteinte par un virus informatique ;
- 42% ont été ciblées par des tentatives de hameçonnage ;
- 26% des entreprises consultées ont été victimes de tentatives d'extorsion ou de fraude au président (faux ordres de virement).

[1] https://metrics.torproject.org
[2] https://clusif.fr/publications/menaces-informatiques-et-pratiques-de-securite-en-france-edition-2016/

3.2 *Attaques ciblées / attaques en profondeur (APT)*

Les observations des éditeurs de sécurité mettent en évidence une **progression des attaques ciblées** depuis le début des années 2010, qui dans leur forme les plus sérieuses relèvent de véritables opérations d'espionnage, mais par leur développement massif montrent clairement le développement d'une démarche criminelle de l'attaque ciblée, pour collecter des informations monnayables ensuite.

Le ***spear phishing*** est une des stratégies les plus courantes et consiste à adresser des courriers électroniques ciblant une entreprise ou un secteur économique donné avec des messages contenant des pièces jointes piégées (un document texte par exemple, qui va télécharger le virus informatique principal dans une deuxième étape). Un éditeur[1] observait une progression de 55% de ces campagnes de messages piégés entre 2014 et 2015. De plus en plus souvent ce sont des petites ou moyennes entreprises qui sont ciblées.

RAT (remote administration trojan) ou Troyen d'administration à distance

Le RAT est une forme de logiciel malveillant contenant un ensemble de modules permettant de parcourir les données sur le système de la victime ou encore d'y intercepter des frappes au clavier ou ce qui s'affiche à l'écran. C'est l'outil de prédilection des opérations d'attaque en profondeur. Ils sont aussi utilisés pour collecter les données personnelles des particuliers.

Les noms les plus courants sont: PlugX RAT, Sakula, Ghost RAT, Hikit, Snake. Ils sont le support d'évolutions techniques intéressantes pour permettre l'exfiltration des données depuis les réseaux sécurisés des entreprises par exemple via le protocole DNS de résolution des noms de domaine.

DroidJack

Le 27 octobre 2015, l'OCLCTIC interpellait 4 individus ayant acquis un logiciel permettant d'infecter les téléphones portables et les tablettes informatiques fonctionnant sous le système d'exploitation Androïd. Appelé Droïdjack, le logiciel était un RAT autorisant une prise de contrôle à distance permettant de lire le contenu du téléphone ou de la tablette, d'activer le microphone ou la caméra, d'émettre ou d'intercepter des appels, d'envoyer des SMS ou de les détourner, de localiser l'appareil infecté via le GPS intégré. L'enquête avait débuté en mai 2015, suite à des informations du BKA allemand qui avait travaillé sur des forums proposant la vente de ce logiciel. Plusieurs acheteurs étaient alors identifiés en France, aux USA, aux Pays Bas, en Belgique, au Royaume Uni et en Suisse. 20 objectifs étaient interpellés en Europe au cours de cette opération.

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

3.3 Détournement / vol de données

Les détournements de données dans les réseaux des organisations sont réalisées soit grâce aux méthodes d'attaque en profondeur que nous venons d'évoquer soit par des atteintes ciblant des vulnérabilités dans les serveurs Web ou de bases de données des victimes.

L'année 2013 avait pu être citée comme celle des records de détournement de données, avec un total de 552 millions d'enregistrements relatifs à des individus détournés[1]. Elles sont le plus souvent réalisées pour des motivations financières et ensuite d'espionnage[2]. En fait, **cette tendance se poursuit de façon inquiétante au cours des années 2015 et 2016** avec tous les mois de nouveaux records: 412 millions de comptes détournés chez Friend Finder Network (USA) en octobre 2016, ou encore les données personnelles de 49,6 millions de citoyens turcs dévoilées en avril 2016[3].

La situation en Europe et plus particulièrement en France est encore mal connue, l'obligation pour les organisations de signaler les fuites de données à caractère personnel étant encore récente.

Vol de données et extorsion d'un groupe industriel français

Le 14 avril 2016, un grand groupe industriel français déposait plainte auprès de l'OCLCTIC pour atteinte à un système de traitement automatisé de données, chantage et extorsion. un maître chanteur déclarait en effet détenir 5 tera-octets de données informatiques récupérés sur les serveurs de l'industriel français, qu'il menaçait de divulguer sur les réseaux sociaux et dans la presse s'il n'obtenait pas une compensation financière à verser en bitcoins. Après négociations, la remise de la rançon était finalement fixée devant un établissement bancaire à Genève, en Suisse. 4 individus issus de la région parisienne étaient interpellés le 20 juillet. Les perquisitions domiciliaires effectuées tant en Suisse qu'en France confortaient leur implication dans le piratage de la base de données de l'industriel français et la tentative d'extorsion. Ils faisaient tous l'objet d'un mandat d'arrêt international avant d'être extradés vers la France un mois plus tard.

3.4 Vulnérabilités

L'évolution du nombre des vulnérabilités, dans les systèmes d'exploitation ou les logiciels, est une donnée difficile à interpréter. En effet, elle révèle à la fois l'activité de ceux qui exploitent ces vulnérabilités (lorsqu'elles sont découvertes par l'action d'un groupe criminel), l'activité des chercheurs en sécurité ou encore la motivation des éditeurs (notamment lorsqu'ils mettent en place des programmes de publication des vulnérabilités qui touchent leurs produits ou de récompense pour les chercheurs qui les découvrent).

[1] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-19
[2] Data Breach Investigations Report 2014 http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf
[3] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Toutefois les vulnérabilités dites « 0-day » ou « Zero-day » découvertes au cours d'une année donnent une mesure intéressante de la menace observée. Ainsi, le nombre de vulnérabilités 0-day aurait évolué[1] entre 2013 et 2015 pour passer de 23 découvertes à 54.

Vulnérabilités « 0-day »

Une vulnérabilité 0-day est une faiblesse dans un logiciel ou un système d'exploitation pour lequel aucun correctif de sécurité n'a été développé et n'était pas connue de la communauté avant sa publication. Elles sont particulièrement précieuses pour les attaquants ou les cybercriminels puisqu'elles permettent d'atteindre à un système d'information donné à tous les coups. Certaines sont révélées avec de gros efforts de marketing (nom, logo, site Web), comme Heartbleed ou Dirty Cow, mais la plupart du temps elles restent justement confidentielles.

Elles peuvent être vendues par un chercheur en sécurité à l'entreprise qui commercialise le produit concerné (y compris via des programmes de *bug bounties*), des intermédiaires faisant parfois monter les enchères (*brokers*) ou à un développeur cybercriminel de plates-formes d'exploit (voir plus bas). Les prix varient de quelques milliers à plus d'un million d'euros.

3.5 Les logiciels malveillants

3.5.1 Les catégories de logiciels malveillants

Outre les RAT évoqués plus haut, trois catégories de logiciels malveillants (ou virus informatiques) nécessitent une attention particulière :

- Les **rançongiciels** (le virus bloque l'accès au système ou aux données et réclame le paiement d'une rançon) ;
- Les **botnets de distribution de menaces** (diffusion ou installation d'autres virus) ;
- Les **botnets ciblant les systèmes bancaires et de paiement** (ils visent l'utilisation de la banque en ligne, mais aussi les terminaux de point de vente ou encore les distributeurs de billets de banque).

Botnets

Un botnet est le système constitué par l'ensemble des machines (ordinateurs, téléphones mobiles et autres appareils) infectées par un même logiciel malveillant ou une même famille de logiciels malveillants et qui se connecte à un système de commande et de contrôle donné.

Tous les logiciels malveillants utilisent aujourd'hui cette architecture en botnet qui permet de rapatrier de l'information vers les attaquants (récupérer les données confidentielles détournées) et transmettre des ordres vers les machines infectées (exécuter une action sur la machine, télécharger une mise à jour du logiciel malveillant, etc.).

[1] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Les attaques par rançongiciels avaient progressé de 500% en 2013[1], les années suivantes ont été celles de l'explosion des **rançongiciels chiffrants**, autrement appelés ***cryptolockers***. Ils chiffrent les données personnelles des utilisateurs ou celles se trouvant sur des serveurs et affichent un message sur l'écran, soit sous forme de simple fichier texte, soit sous forme d'une boîte de dialogue. Les paiements sont souvent exigés en cryptomonnaies, notablement le *bitcoin*.

Parmi les outils de **diffusion de menaces** on peut citer ceux qui permettent des campagnes de **courriers électroniques malveillants** (comme PushDo ou Cutwail) ou ceux qui **installent de nouveaux virus** sur les machines dont elles ont d'abord le contrôle (Upatre, Andromeda ou Pony Loader[2]).

Les virus ciblant les systèmes de paiement des points de vente se sont massivement développés au cours de l'année 2014, ciblant les pays où les pistes magnétiques sont encore utilisées (notamment les États-Unis) :

- Les familles de virus de point de vente citées sont : BlackPoS, Kaptoxa (sous-composant de BlackPoS), Dexter PoS, vSkimmer, JackPoS ; ils fonctionnent en scrutant la mémoire des caisses enregistreuses à la recherche de suite de valeurs correspondant aux données d'une carte bancaire et en les vérifiant grâce à l'algorithme standard (dit algorithme de Luhn) ;

- Ces vagues d'attaques **ont amené les pays concernés (en particulier les Etats-Unis) à s'interroger sur les modalités techniques de sécurisation des paiements par carte** (carte à puce et code PIN ou systèmes de paiement sécurisés alternatifs via des plates-formes mobiles comme ApplePay)

Enfin, c'est aussi du point de vue des **technologies utilisées par les botnets** que les évolutions sont les plus notables avec l'utilisation de méthodes de **communication pair à pair entre les machines infectées et le système de commande et de contrôle**, permettant une plus grande résilience (notamment grâce à l'absence de serveur central).

Démantèlement de botnets

Plusieurs opérations ont été menées en 2014 contre des virus informatiques, pour lesquelles l'OCLCTIC a contribué au démantèlement des infrastructures des botnets :

- GameOver Zeus (juin 2014), en même temps que CryptoLocker, dans le cadre de l'opération Tovar (FBI, Europol et le UK National Crime Agency) avec l'identification de Evgeniy Mikhailovich Bogachev parmi les suspects principaux ;

- L'opération ciblant le botnet bancaire Shylock (juillet 2014), coordonnée par le UK National Crime Agency avec le soutien d'Europol et du FBI.

[1] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-19

[2] Un *loader* ou *dropper* est un virus servant à diffuser ou installer d'autres virus. Ils sont systématiquement organisés en botnet (avec un système de commande et de contrôle) et sont souvent associés à d'autres fonctions (collecte de données personnelles sur les ordinateurs victimes par exemple, en plus de la fonctionnalité d'installation de virus)

3.5.2 La diffusion des virus informatiques

Les virus se propagent traditionnellement par plusieurs modes :

- En **pièce jointe ou transfert de fichier** par courrier électronique ou sur un réseau social ;
- Par partage d'un fichier **sur un support amovible ou un partage réseau** ;
- Par **installation directe par l'utilisateur** (cas du téléchargement d'une application malveillante, installée volontairement, notamment sur les téléphones mobiles) ;
- Par **exploitation d'une vulnérabilité sur le système via une plateforme d'exploits** (ou *exploit kit*) vers lequel l'utilisateur est attiré ou redirigé dans sa navigation Internet (notamment en recevant un lien par courrier électronique ou sur un réseau social, mais aussi depuis des bannières publicitaires malveillantes ou la modification d'un site Web souvent visité – technique dite du trou d'eau).
- Enfin, de façon notable, c'est souvent un premier virus qui va être utilisé pour en installer d'autres.

L'ensemble de ces modes de diffusion doivent être pris en compte tant dans les messages de prévention, les méthodes de détection dans les réseaux des entreprises que dans les stratégies d'enquête qui vont idéalement chercher à identifier la source des attaques.

Selon les statistiques de l'institut AV-Test[1] ce sont plus de 120 millions de variantes nouvelles de logiciels malveillants qui sont détectées chaque année.

Minax Crypter

En mars 2016, l'OCLCTIC découvrait la mise en vente sur Internet d'un logiciel « Minaxcrypter » (un empaqueteur ou chiffreur) dont le but était de rendre indétectables par les anti-virus les malwares de type chevaux de Troie. Identifié grâce à un long travail d'enquête en sources ouvertes, l'auteur du programme était interpellé à Tours le 5 juillet 2016. Il reconnaissait avoir participé au développement et à la promotion de plusieurs autres *crypters* pour un gain estimé à plusieurs milliers d'euros.

3.5.3 Les plates-formes d'exploits

C'est aujourd'hui le mode de diffusion le plus couramment utilisé, plus communément appelé le *drive-by download*, littéralement le « téléchargement en chemin ». Leur présence sur les marchés cybercriminels évolue au gré de l'appréciation des délinquants eux-mêmes par rapport aux services rendus, mais aussi en fonction des opérations policières.

[1] https://www.av-test.org/en/statistics/malware/#tab-6906-1

Exploit kit

Un *exploit kit* ou *plateforme d'exploit* est un logiciel se présentant sous la forme d'un serveur Web vers lequel sont redirigés les victimes potentielles (par exemple en suivant un lien dans un courrier électronique non sollicité). Le logiciel va tester toutes les vulnérabilités du système d'exploitation, du logiciel de navigation Web et des applications additionnelles installées sur la machine de la victime potentielle. Les morceaux de code informatique qui servent à utiliser ces faiblesses sont appelées *exploits*, d'où le nom de ces plateformes.

En 2014[1], trois *exploit kits* étaient les plus couramment rencontrés : Magnitude, Angler Exploit kit, Sweet Orange. En 2016, on retrouve en tête des palmarès[2] : Neutrino, Rig et Magnitude.

En 2013, le développeur du BlackHole exploit kit avait été interpellé par la police russe et d'autres ont pu prendre sa place dans ce marché. **Pour avoir un effet à long terme sur la menace que représente les exploit kits, la coopération policière internationale devrait pouvoir frapper en même temps plusieurs familles de ces plates-formes occupant le haut du pavé.**

3.6 Actions collectives: hacktivisme et swatting

Le **cyberactivisme** est l'action militante portée sur le cyberespace. Parfois elle prend la forme d'actions illégales (détournement de sites Web, attaques en déni de service) et les revendications peuvent être liées à des activités de groupes terroristes. Par exemple en 2014, Lizard Squad est un groupe dont les actions, parfois liées à des revendications islamistes, consistent principalement en des attaques en déni de service distribué (notamment contre des sites de jeux en ligne) et des défacements. En 2015 et 2016, ce sont notamment des groupes tels que Anon Ghost ou Fallaga Team qui vont agir contre des sites Web français pour y porter des revendications en rapport avec les attentats.

D'autres formes d'actions collective se sont développées, telles le **swatting**. Il s'agit de faire intervenir des forces de police chez un particulier pris au hasard ou chez un concurrent dans un groupe de discussion ou sur une plateforme de jeux en ligne. Pour ce faire les auteurs utilisent des logiciels et plates-formes dédiés aux usurpations téléphoniques.

[1] http://blog.trendmicro.com/trendlabs-security-intelligence/whats-new-in-exploit-kits-in-2014/
[2] https://www.zscaler.com/blogs/research/top-exploit-kit-activity-roundup-summer-2016

Dossiers de « swatting»

1. De février à mai 2015, quatre mineurs agissent conjointement à l'encontre d'une famille, en usurpant numéros téléphoniques et identités des appelants. L'enquête menée par le C3N et le groupement de gendarmerie de la Sarthe révèle l'organisation, concertée par Internet, de faits sériels commis par des joueurs de jeux vidéos en ligne. Au-delà des interventions d'urgence indues de forces de sécurité, l'affaire révèle également une tentative d'extorsion, de nombreux outrages et un service de prestations payante de cyberattaques. Trois auteurs français et un résident en Belgique ont été interpellés.

2. Le préjudice du swatting est très élevé, tant pour les victimes que pour l'État c'est une menace liée à l'utilisation malveillante des technologies et d'Internet qui doit être prise en compte sérieusement comme le montre également son utilisation **dans le cas de l'Eglise Saint-Leu à Paris alors** que venait d'être assassiné le prêtre dans l'église de Saint-Etienne du Rouvray. 2 fans d'un militant sioniste ont revendiqué la fausse prise d'otage à l'église Saint-Leu en septembre 2016, affirmant être à l'origine de l'appel qui a entraîné l'opération anti-terroriste dans le quartier des Halles à Paris. Un déploiement extrêmement coûteux de moyens des forces de l'ordre, s'en était suivi et le Parquet ouvrait une enquête pour dénonciation de crime imaginaire et en 2 jours, 3 mineurs étaient interpellés, mis en examen et placés en foyer.

3.7 Les courriers électroniques non sollicités (spam)

Le spam, ou courrier électronique non sollicité, est une menace multiforme, véhiculant parfois des contenus malveillants, mais correspondant souvent à des abus commerciaux du courrier électronique ou une mauvaise perception du courrier électronique à caractère commercial.

L'association Signal Spam, au sein de laquelle le ministère est activement représenté, publie chaque trimestre un baromètre du spam, basé sur les signalements des internautes. Pour le dernier trimestre 2016[1], les observations sont les suivantes :

- La répartition entre marketing et cybercriminalité parmi les messages signalés sont de 79 % pour le marketing contre 21 % pour la cybercriminalité ;
- La provenance des messages signalés est à 51% France, 11% USA, 7% le Royaume-Uni, 3,3 % l'Allemagne.
- Les catégories de messages d'intention cybercriminelle sont rappelées dans la figure ci-après.

[1] https://www.signal-spam.fr/actualites/barom%C3%A8tre-de-la-perception-du-spam-pour-l%C3%A9t%C3%A9-2016-disponible

Figure 2 - Évolution du spam d'origine cybercriminelle (Source: Signal Spam)

D'autres formes de messages non sollicités sont particulièrement prégnants : les spams sous forme de SMS ou d'appels téléphoniques (avec ou sans message enregistré) qui ont tous pour objectif d'amener les victimes à débourser de l'argent par appel sur un numéro surtaxé ou en cliquant sur un lien. Ils sont suivis en France par la plateforme du 33700 gérée par les opérateurs concernés.

3.8 Systèmes d'information liés aux élections comme cibles

Plusieurs technologies liées aux élections ont été victimes d'attaques au cours des périodes récentes. On peut citer par exemple en 2014:

- En juin 2014, le système Popvote de vote en ligne (non officiel) utilisé par le mouvement de protestation *Umbrella revolution* à Hong Kong pour réclamer des élections locales a été victime d'une attaque massive en déni de service. Cette attaque est à rapprocher de campagnes utilisant des virus ciblant les téléphones mobiles des protestataires.

- En juillet 2014, la Tunisie a subi une attaque en déni de service contre son système d'enrôlement des électeurs.

- En octobre 2014, en Ukraine[1], le site de la Commission centrale des élections (www.cvk.gov.ua) a été victime d'une attaque en déni de service au moment de l'affichage des résultats : opération revendiquée parmi d'autres par un groupe de cyberhacktivisme appelé CyberBerkut. Dans le même temps, des écrans d'affichage géants auraient été détournés pour diffuser des images de violence. CyberBerkut est apparu en mars 2014 et a commis de nombreuses autres actions ciblant les autorités ukrainiennes ou encore l'OTAN.

[1] http://www.securityweek.com/hackers-target-ukraines-election-website

L'année 2016 fut marquée par l'actualité de la campagne électorale américaine, avec la révélation d'informations issues des systèmes d'information des partis politiques (en particulier la parti Démocrate)[1]. Le SGDSN a organisé[2] au mois d'octobre 2016 un séminaire visant à sensibiliser plus particulièrement les partis politiques français sur les risques qu'ils encourent.

Opération d'Europol contre les mûles

EMMA II, pour European Money Mule Action II, opération d'interpellations d'envergure menée sous l'égide d'Europol et coordonnée pour la France par l'OCLCTIC, a permis l'identification de plus de 500 mules en Europe, impliquées dans plus de 800 transactions frauduleuses, ciblant une centaine d'établissements bancaires et faisant 1300 victimes. Le préjudice total a été estimé à plus de 23 millions d'Euros. 178 individus étaient interpellés et les perquisitions réalisées ont permis la saisine de 410 000 Euros en liquide. Plus de 95% de transactions effectuées par l'ensemble de ces mules avaient pour origine les données massivement volées par le malware bancaire Dridex.

3.9 Le coût de la cybercriminalité

L'évaluation du coût de la cybercriminalité reste encore un exercice complexe et repose pour l'instant sur des études évaluatives ou des sondages. Très souvent, elles se basent sur l'impact économique pouvant affecter les entreprises plutôt que les particuliers. En voici quelques exemples récents :

- Selon l'étude « Menaces informatiques et pratiques de sécurité » du Clusif, l'impact financier des incidents informatiques est encore mal connu (59% ne sont pas évalués).
- Pour les entreprises[3], le coût moyen d'un détournement de données serait de l'ordre de 4 millions de dollars, avec un coût par enregistrement évalué à 158 dollars.
- L'Observatoire de la sécurité des cartes de paiement publie chaque année le volume précis des montants frauduleux, les préjudices étant portés selon les cas par les banques, les commerçants ou parfois les clients, mais étant parfois évités lorsque les transactions frauduleuses sont détectées suffisamment en amont. Dans l'illustration ci-dessous on observe que le montant global de la fraude s'élève pour la France - transactions nationales et internationales cumulées - à 522,7 M € en 2015 (dont 313 M€ réalisée sur des transactions sur Internet).

[1] http://edition.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims/
[2] http://www.lemonde.fr/pixels/article/2016/12/21/des-attaques-informatiques-a-visee-politique-envisageables-en-france_5052650_4408996.html
[3] Etude Ponemon pour IBM 2016 http://www-03.ibm.com/security/infographics/data-breach/

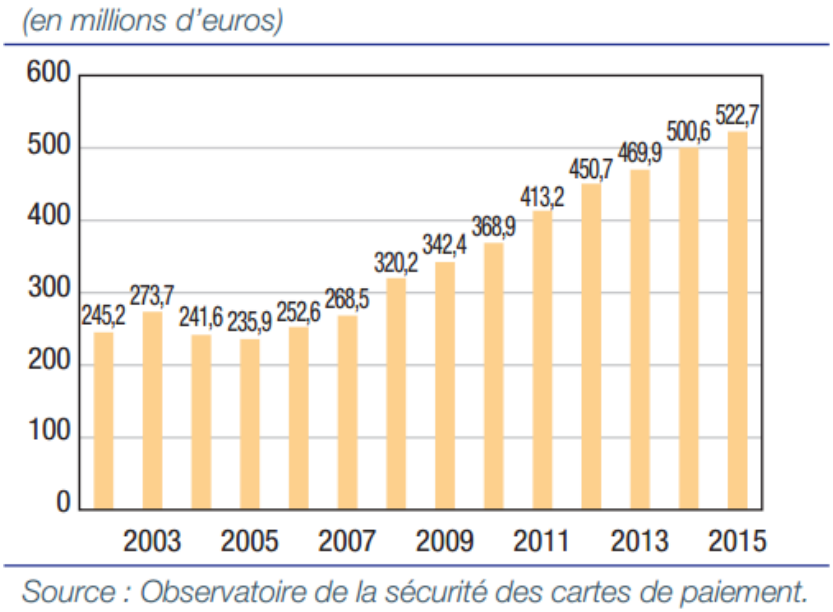


Figure 3 - Montant de la fraude sur les transactions de cartes bancaires traitées en France (source: OSCP)

- Enfin, la gendarmerie nationale réalise depuis août 2014 une étude mensuelle des dossiers se rapportant à la cybercriminalité et qui font l'objet d'une remontée de « comptes-rendus de police judiciaire ». Les préjudices relevés dans ce contexte sont de l'ordre de 4 millions d'euros chaque mois.

*

* *

Fermeture d'un site illégal de téléchargement

En juillet 2015, à l'issue d'investigations menées par un agent assermenté, la SACEM porte plainte auprès du C3N à Pontoise, contre un site de téléchargement illégal. Ce site permet à une communauté très fermée d'internautes d'échanger plus de 2 millions de titres musicaux piratés, dont une grande quantité d'albums rares. Le préjudice est évalué à plus 40 millions d'euros. L'enquête judiciaire permet d'identifier la totalité des serveurs de l'infrastructure. L'opération judiciaire menée en novembre 2016 dans les locaux d'un hébergeur a permis de débrancher et de saisir l'intégralité des serveurs du site illicite (7 serveurs, présentant un volume de plus de 10 téra-octets).

3.10 Internet des objets / objets communicants

Les objets connectés bénéficient d'un engouement médiatique important, de développements nouveaux et sont l'objet de préoccupations réelles de la communauté de la sécurité des systèmes d'information. C'est aussi un domaine qui devrait voir se développer de nouveaux champs d'exploration pour l'enquête judiciaire.

3.10.1 Description du phénomène

Il est important de se rappeler que les objets connectés, et même des objets directement connectés à Internet ne constituent pas en soi une nouveauté des dernières années, mais avant tout une tendance de fond qui est vraisemblablement en train de s'accélérer, pour des raisons technologiques (une plus grande connectivité, la miniaturisation continue de l'électronique à moindre coût) et de maturité du marché (aussi bien au niveau de la variété des produits offerts que de l'intérêt des consommateurs).

Du côté des objets dits connectés, ils sont nombreux depuis longtemps, mais essentiellement comme des extensions de dispositifs existants : oreillettes sans fil et connexion de l'autoradio au téléphone dans la voiture ; ou parce que leur connexion est nécessaire : accès à distance à des caméras ou microphones de télésurveillance, d'abord par une simple ligne téléphonique et maintenant sur Internet. On trouve ensuite les objets dont la connexion semble évidemment intéressante : les téléviseurs et lecteurs de bluray sont connectables à Internet depuis quelques années (pour mettre à jour leur microgiciel, activer des protections ou visionner des contenus distants).

Si on remonte au milieu des années 2000, le Nabaztag (un lapin en matière plastique clignotant, parlant et remuant) est un précurseur de ce qui pourrait déferler aujourd'hui sur le marché grand public. Enfin, depuis de nombreuses années, les entreprises et notamment leurs outils de production sont de plus en plus souvent connectés, ce sont les systèmes de commande industriels – ou SCADA. Les évolutions en cours pourraient être de trois ordres :

- la **connectivité d'un plus grand nombre d'objets** : par exemple, **les voitures** qui pourraient de plus en plus souvent transférer des informations vers les constructeurs, leur garagiste ou entre elles et avec les équipements routiers – tout en offrant un accès à Internet et de nouveaux services aux passagers, mais aussi l'équipement domestique (réfrigérateurs, aspirateurs, climatisation…) ; le développement des cartes bancaires et de transport sans contact est un autre exemple ;

- le **corps connecté**[1]: c'est certainement l'univers le plus important d'innovation, au travers d'objets que l'on porte sur soi, qui collectent des données à caractère personnel (position, données médicales ou sur son activité physique). Il s'agit du « Quantified Self » ; le plus souvent ces objets communiquent via un téléphone portable ;

- une **plus grande connectivité directement via Internet** : le **déploiement progressif d'IPv6**[2], un protocole Internet permettant d'attribuer littéralement à chaque objet une

[1] En mai 2014, la CNIL proposait un rapport sur le corps connecté.
http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/DEIP/CNIL_CAHIERS_IP2_WEB.pdf

[2] Une adresse IP dite v4 est composée dans sa représentation la plus courante de 4 nombres de 0 à 255, soit un nombre de combinaisons maximal de 4,3 milliards environ. Avec IP v6, l'adresse est représentée par 8 groupes de 2

adresse IP individuelle alors qu'aujourd'hui on doit le plus souvent passer par une connectivité relais (l'adresse IP de la box Internet à son domicile par exemple).

3.10.2 Incidence sur la sécurité

En matière de sécurité, les objets connectés soulèvent deux problèmes :

- l'**augmentation de la surface d'attaque** : c'est un concept important dans l'évolution de la menace en sécurité de l'information et il est particulièrement pertinent ici, puisqu'on connecte un plus grand nombre de dispositifs, contenant du reste de plus en plus de données sensibles (on pourrait passer d'un environnement avec un ordinateur par domicile et un téléphone portable par personne à près d'une dizaine d'objets communicants par personne–ordinateur, téléphone mobile, tablette, consoles de jeux mais aussi pèse-personne, dispositifs médicaux, capteurs sportifs ou d'aide au sommeil) ;
- le **manque de maturité sécuritaire de ces objets** : autant la sécurité des ordinateurs personnels est un sujet bien maîtrisé par les industriels, autant celle des téléphones mobiles est loin d'être parfaite, encore moins celles des objets communicants qui ne constituent pas encore une préoccupation réelle (sauf pour les objets qui ont des vocations sécuritaires comme les cartes de transport). Une des questions les plus importantes de la recherche scientifique dans ce domaine est le développement de protocoles de sécurité adaptés à des objets de petite taille avec une puissance de calcul plus faible.

Les risques sont bien réels : des objets aussi sensibles que les pacemakers existent en version « connectée » depuis 2009 et ils faisaient dès 2012 déjà l'objet d'expérimentations de la part de chercheurs en sécurité pour tester leurs vulnérabilités[1]. En novembre 2014, un site Web référençait des milliers de caméras de surveillance accessibles sans autre contrôle que le mot de passe par défaut mis en place par le constructeur :c'est donc aussi les utilisateurs qui sont trop peu sensibilisés au risque. A contrario, en janvier 2014, était découvert un botnet[2] composé par des réfrigérateurs infectés par un virus : il s'est ensuite avéré que leur découverte reposait uniquement sur le fait que les victimes possédaient des réfrigérateurs connectés à leur domicile, joignables via Internet et que c'étaient vraisemblablement leurs ordinateurs personnels (utilisant la même adresse IP) qui étaient connectés à ce botnet.

3.10.3 Impact sur l'enquête judiciaire

De même que le développement des téléphones mobiles et les risques associés (l'explosion du nombre de virus sur les plates-formes mobiles[3], notamment Android, mais aussi une utilisation croissante du mobile pour réaliser des transactions bancaires) entraînent une évolution progressive du nombre de cas judiciaires, la démocratisation des objets connectés aura les mêmes conséquences. Ces situations risquent d'être d'autant plus graves qu'on sera face à des usages sensibles (aide à la conduite des automobiles,

octets (un octet peut contenir une valeur de 0 à 255) soit de quoi connecter 667 millions de milliards d'appareils sur chaque millimètre carré de la surface de la Terre...

[1] Barnaby Jack présentait ses travaux sur la sécurité des pacemakers au congrès Breakpoint en octobre 2012.

[2] http://investors.proofpoint.com/releasedetail.cfm?releaseid=819799

[3] Les observations démontrent une évolution systématique des usages des délinquants vers le monde du GSM : virus rançongiciels, virus bancaires s'y sont déployés en 2013 et 2014.

dispositifs médicaux), avec des risques pour la **confidentialité des données personnelles, mais aussi pour l'intégrité physique des personnes**.

L'impact sera certainement encore plus fort du point de vue des traces exploitables dans toutes les enquêtes judiciaires. **Potentiellement, les données disponibles pour l'enquêteur et pouvant apporter un éclairage complémentaire vont ainsi se développer** : parcours et activité physique, présence d'une personne – ou en tous cas d'un objet porté – à un endroit donné ou encore duplication locale d'informations personnelles comme des détails d'agenda par exemple. L'un des exemples le plus courant est certainement la présence de données complémentaires à l'analyse des téléphones mobiles, puisque les numéros appelés ou appelant, ou encore les messages reçus ou émis pourraient être stockés dans le téléphone ou dans l'appareil porté au poignet indifféremment.

3.10.4 Botnets d'objets connectés

Mirai est un logiciel malveillant s'installant sur des serveurs tournant sous le système d'exploitation Linux. Au cours de l'année 2016 il a été utilisé (vraisemblablement commercialisé sous forme de service cybercriminel) pour réaliser des attaques à destination de plusieurs entreprises importantes telles qu'OVH (France) - le plus important hébergeur européen - et la société Dyn (USA) dont les services sont utilisés pour héberger les serveurs de résolution de noms de domaine de nombreuses entreprises.

La particularité de Mirai est d'exploiter des machines moins souvent concernées tels que des enregistreurs de vidéo surveillance domotiques ou des routeurs de réseaux locaux d'entreprises. Ce botnet s'inscrit dans la lignée des botnets de déni de service (voir l'affaire DD4BC ci-dessous).

Affaire DD4BC

Courant 2015, la SDLC et la BEFTI de la DRPJ de Paris constateient l'apparition d'une série d'attaques informatiques de type DDoS (déni de service distribué) consistant à saturer un serveur informatique de requêtes afin de la rendre indisponible. Un groupe se faisant appeler DD4BC (*DDoS for Bitcoin*) réalisait des attaques de ce type au préjudice de sociétés commerciales dont plusieurs étaient situées en France. L'attaque en DDoS durait 1 heure environ et était suivie d'une demande de rançon autour de 25 Bitcoins (environ 10.000 € à l'époque des faits). Si la somme n'était pas versée dans les 24 heures, le groupe DD4BC menaçait d'une nouvelle attaque et d'une augmentation de la rançon toutes les heures. La coopération internationale organisée à Europol permettait à la SDLC de communiquer un renseignement conduisant vers une victime ayant payé la rançon. L'analyse du paiement en Bitcoins par la société Chainalys (USA) ciblait un ressortissant bosniaque qui était interpellé au cours d'une opération conjointe lancée avec les agences allemande, autrichienne, bosniaque et britannique.

3.11 Enquête « cadre de vie et sécurité »

L'enquête « Cadre de vie et sécurité » (INSEE-ONDRP-SSMSI) est une enquête annuelle de victimation réalisée auprès de résidents de logements ordinaires, dont la collecte a commencé en 2007. Les informations recueillies dans cette enquête portent sur les deux années précédant la collecte et couvrent donc les années 2005-2006 à 2014-2015.

Méthodologie de l'enquête « Cadre de vie et sécurité »

Les informations, déclaratives, sont recueillies au cours d'un entretien en face-à-face. La personne de référence répond au questionnaire ménages. Dans les familles, il s'agit en général du père ou de la mère. Les questions sur les atteintes subies par les ménages concernent les atteintes aux biens liés aux résidences, aux véhicules ou aux escroqueries bancaires.Au sein du ménage, une personne de 14 ans ou plus est tirée au sort pour répondre au questionnaire individuel en face-à-face. Elle répond à des questions sur les atteintes personnelles telles que les vols avec ou sans violences ou menaces, les violences physiques, les menaces ou les injures (hors ménage).

Les atteintes liées au cyberespace ne font pas l'objet d'un module de l'enquête CVS même si des parties du questionnaire relatives à certaines atteintes (menaces, injures et débits frauduleux) contiennent des questions liées au domaine cyber. Ainsi, les données mises en évidence par CVS ont donc d'un côté une acception extensive - car ne distinguant pas le courrier postal du courrier électronique - et de l'autre restrictive dans la mesure où elles ne couvrent qu'une partie des cybermenaces touchant exclusivement les personnes physiques (phishing, atteintes aux STAD, infractions liées à la loi sur la liberté de la presse…) et dépend du fait que la personne interrogée ait connaissance d'une telle atteinte.

3.11.1 Les menaces et les injures

Lorsqu'une personne répondant au questionnaire a été victime de menaces ou d'injures au cours des deux années précédant l'enquête, elle est amenée à préciser le cadre dans lequel elle a subi la dernière atteinte à partir de plusieurs modalités. Une de ces modalités permet de caractériser une atteinte comme relevant du cyberespace : injures ou menaces « non verbales (par courrier postal, électronique ou sur réseaux sociaux) ».

Les données extraites de l'enquête CVS en matière de menaces ou d'injures commises par courrier électronique ou sur réseaux sociaux ne peuvent donc pas être distinguées de celles accomplies par voie postale.

Augmentation du nombre de victimes de menaces et injures par courrier postal, électronique ou sur réseaux sociaux entre 2007 et 2016

Le nombre de personnes victimes de menaces et d'injures liées au cyberespace augmente entre 2006 et 2015. En 2006, 95 000 personnes déclaraient avoir subi au moins une menace par courrier postal, électronique ou sur réseaux sociaux au cours des deux années précédentes tandis qu'elles sont 197 000 en 2015 (+ 106 %) .

Concernant les injures liées aux cybermenaces, le nombre de victimes augmente aussi, passant de 104 000 en 2007 à 160 000 en 2016 (+ 53 %).

Les atteintes liées au cyberespace représentent une part résiduelle des menaces et des injures globales (respectivement 5 % et 2 % sur l'ensemble de la période 2006-2015).

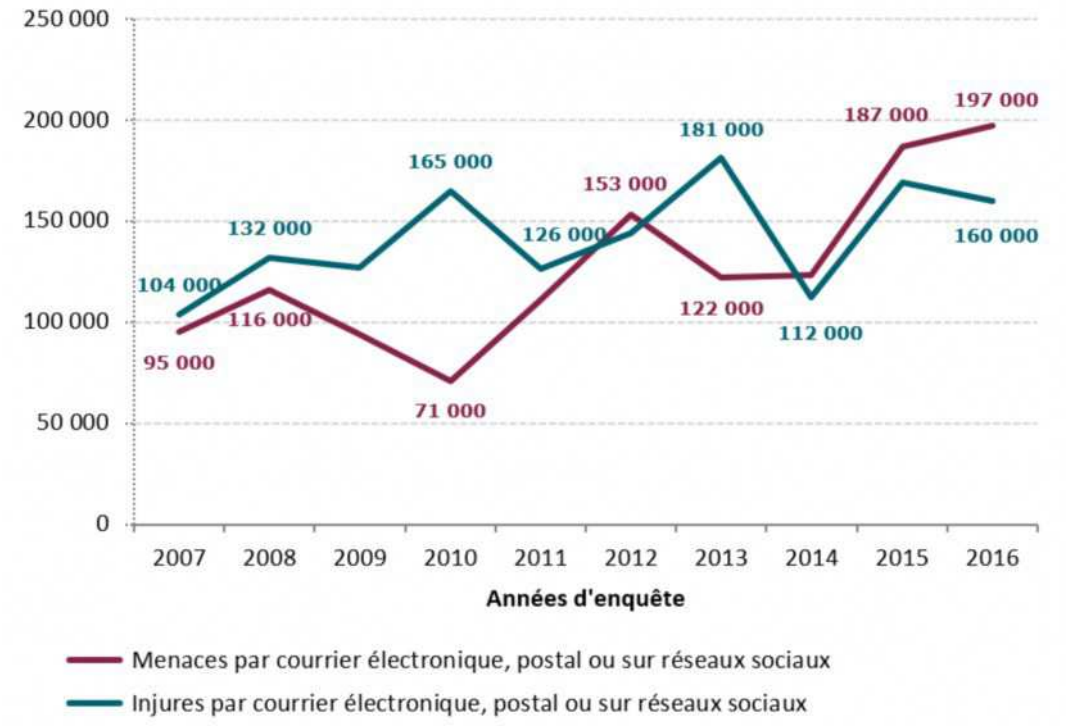


Figure 4 - Personnes déclarant avoir été victimes de menace ou injure et dont la dernière atteinte a été subie par courrier électronique, postal ou sur réseaux sociaux

Source : Enquête " Cadre de Vie et sécurité ", Insee-ONDRP-SSMsi, 2011-2016.

Le lien de l'atteinte avec le cyberespace ne permet pas de caractériser des écarts notables de comportement des victimes en termes de plainte

Les injures par courrier électronique, postal ou sur réseaux sociaux donnent légèrement moins lieu à une plainte que celles qui sont commises de visu ou par téléphone (taux de plainte de respectivement de 3 % et de 7 %).

Concernant les menaces, la tendance à porter plainte en fonction du lien de l'atteinte avec les cybermenaces est inverse puisque le taux de plainte pour celles commises par courrier électronique, postal ou sur réseaux sociaux est très légèrement plus élevé (13 %) que celui des menaces de visu ou par téléphone (10 %).

3.11.2 Les débits frauduleux

Le préjudice des débits frauduleux liés au cyberespace est moins élevé que celui des autres débits frauduleux

La moitié des ménages victimes d'un débit frauduleux lié au cyberespace ont subi un préjudice n'excédant pas 150 €. Ce préjudice s'élève à 400 € pour les autres débits

frauduleux. Le montant moyen des débits frauduleux liés aux cybermenaces s'élève à 581 euros (1 080 euros pour les débits frauduleux non liés au cyberespace).

Les taux de plainte pour les débits frauduleux liés au cyberespace diminuent entre 2011 et 2016

Les taux de plainte pour les débits frauduleux, qu'ils soient ou non liés au cybermenaces, diminuent entre 2011 et 2016. En 2016, près de 30 % des ménages victimes de débit frauduleux lié aux cybermenaces portent plainte alors qu'ils étaient près de 42 % à le faire en 2011. Sur l'ensemble de la période 2011-2016, ce taux de plainte varie en fonction du montant du préjudice : il est de 10 % quand le montant du préjudice est inférieur à 100 euros et il s'élève à 19 % quand le montant du préjudice est supérieur à 1 000 euros.

L'ONDRP mentionnait dans une précédente publication sur les débits frauduleux que cette diminution pourrait être liée au fait que la déclaration de l'incident auprès des forces de l'ordre ne soit plus exigée par les organismes bancaires pour le remboursement du préjudice.

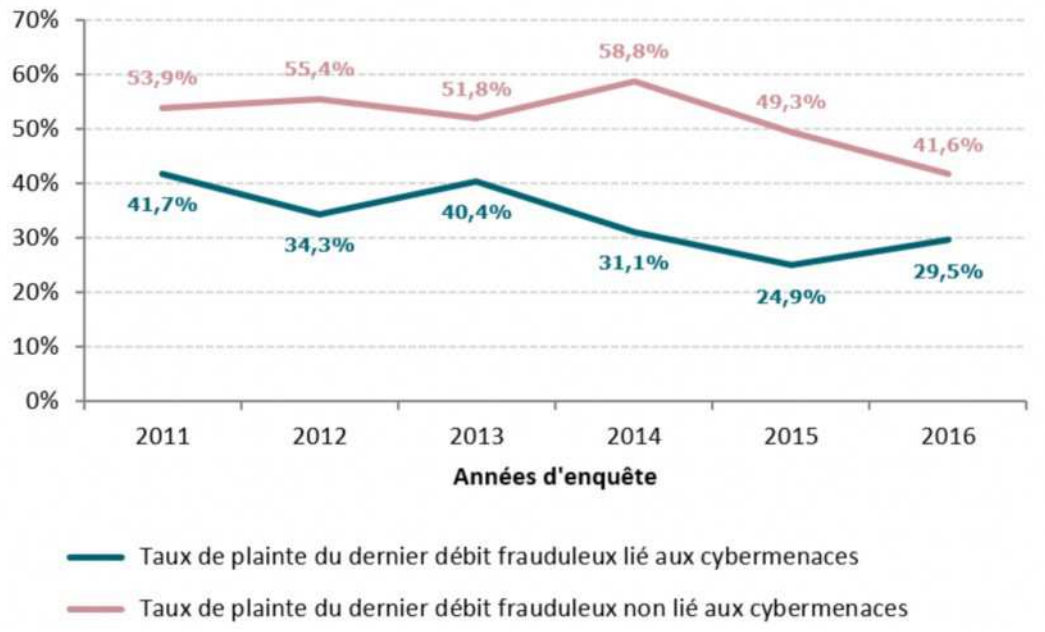


Figure 5 - Taux de plainte suite au dernier débit frauduleux selon sa nature

Source : Enquête " Cadre de Vie et sécurité ", Insee-ONDRP-SSMsi, 2011-2016.
Champ : Ménages ordinaires déclarant avoir été victimes d'un débit frauduleux dont ils connaissent le mode opératoire, France métropolitaine.

PARTIE2–USAGES ET PHÉNOMÈNES

Partie 3 - Action du ministere de l'Interieur contre les cybermenaces

4 Vision des cybermenaces par les services du ministère de l'Intérieur

4.1 Données statistiques sur les infractions constatées

Les fonctionnaires de police et les militaires de la gendarmerie nationale reçoivent les plaintes des victimes d'infractions cyber en application du code de procédure pénale. Ces plaintes font l'objet d'un enregistrement statistique qui permet de produire les statistiques de la délinquance, c'est-à-dire, sous leur forme actuelle, l'état 4001 des faits qualifiés de crimes et délits.

Cet enregistrement, traditionnellement effectué en application d'un guide de méthodologie statistique commun aux deux forces de sécurité intérieure, se modernise progressivement dans le cadre de la mise en œuvre d'un nouvel environnement informatique, notamment structuré autour de logiciels de rédaction des procédures (LRP) déployés dans la gendarmerie nationale (LRPGN) et dans la police nationale (LRPPN).

Depuis deux ans, le service statistique ministériel de la sécurité intérieure (SSMSI) a élaboré, conjointement avec les directions et leurs services spécialisés, des agrégats regroupant les catégories d'infractions liées à la cybercriminalité. Il a été choisi de distinguer les infractions ciblant les systèmes et les infractions commises via les systèmes. Ce travail permettra de fiabiliser et de stabiliser la statistique, et de s'inscrire dans le contexte de la nomenclature internationale.

Entre avril 2015 et décembre 2016, la police et la gendarmerie ont enregistré en 18 279 infractions d'atteintes aux systèmes de traitement automatisé de données (**STAD**) soit un nombre moyen mensuel de 870 infractions. Les accès frauduleux représentent la grande majorité (74,3%) des atteintes aux STAD. Viennent ensuite les altérations ou entraves au fonctionnement (13,2%) et les atteintes aux données (10,1%). La détention de moyens représente (2,4%).

Les principales Infractions d'atteintes aux STAD

Pour l'année 2016, 10 475 infractions ont été enregistrées par les services. Les atteintes aux STAD sont en très légère hausse de 0.67% par rapport à 2015. La détention de moyens d'atteinte augmente de 22.2%, l'altération ou l'entrave au fonctionnement de +1.6% et les accès frauduleux de +0.4%. Les atteintes aux données ont diminué de 4.2%.

Nombre d'infractions par catégorie d'atteinte	2015*	2016	Évolution
1 - Accès frauduleux	7740	7769	0,40%
2 - Altération ou entrave au fonctionnement	1367	1389	1,60%
3 - Atteintes aux données	1080	1036	-4,20%
4 - Détention de moyens	219	281	22,20%
Somme annuelle	10405	10475	0,67%

* :L'année 2015 est rétropolée sur la base des données de avril à décembre
Champ : France.
Source : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie.

Comparaison avec les statistiques judiciaires

A ce jour, il est encore complexe de comparer les chiffres issus du traitement des enquêtes judiciaires de ceux obtenus au niveau des condamnations. Toutefois la mise en place récente de référentiels communs et d'échanges d'informations automatisés vont permettre d'obtenir une lecture de plus en plus fine. A cela se rajoute les complexités évoquées quant à la comptabilité des infractions liées à la cybercriminalité, comme c'est le cas pour les escroqueries.

Exemple de la réponse judiciaire contre l'apologie au terrorisme

Alors que ce délit avait donné lieu à une dizaine de condamnations, jusqu'en 2015, l'actualité marquée par le terrorisme et l'état d'urgence ont eu pour conséquence une hausse significative de procédures aboutissant à des condamnations et 385 personnes ont été condamnées pour apologie du terrorisme en 2015. Il faut également noter que 95 % des mis en cause sont déférés puis condamnés des peines importantes allant jusqu'à quatre ans d'emprisonnement.

4.2 Activité de la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS)

La plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) de l'OCLCTIC exploite les signalements émis sur le site https://www.internet-signalement.gouv.fr/ par des internautes et des professionnels du numérique décrivant des comportements ou contenus de l'internet qu'ils estiment illégaux.

En 2015, PHAROS a reçu 188.055 signalements (contre 137 456 signalements en 2014). La moyenne est donc passée de 2.640 à 3.540 signalements par semaine. La majorité des signalements provient du site www.internet-signalement.gouv.fr, bien identifié comme le point d'entrée unique, tant par les particuliers que par les professionnels.

L'année 2015 a marqué une rupture avec les tendances observées entre 2009 et 2014 concernant les parts respectives des grands domaines d'infractions :

- Si les escroqueries et extorsions continuent d'augmenter (72.032 en 2014, 80.519 en 2015) leur proportion fléchit un peu : 43,6% en 2015 contre 52,4% en 2014 ;
- Le nombre d'atteintes aux mineurs (pédopornographie, prédation sexuelle, etc.) reste stable avec 16.396 signalements, mais leur proportion diminue à 8,9% ;
- Les signalements liés au terrorisme ou à son apologie ont connu une véritable explosion : 31.302 en 2015 contre 1.675 en 2014, soit +1768,7% ;

- Les signalements pour discriminations ont quasiment doublé : 26.477 en 2015, contre 13.297 en 2014.

  En valeur absolue, toutes les catégories augmentent :

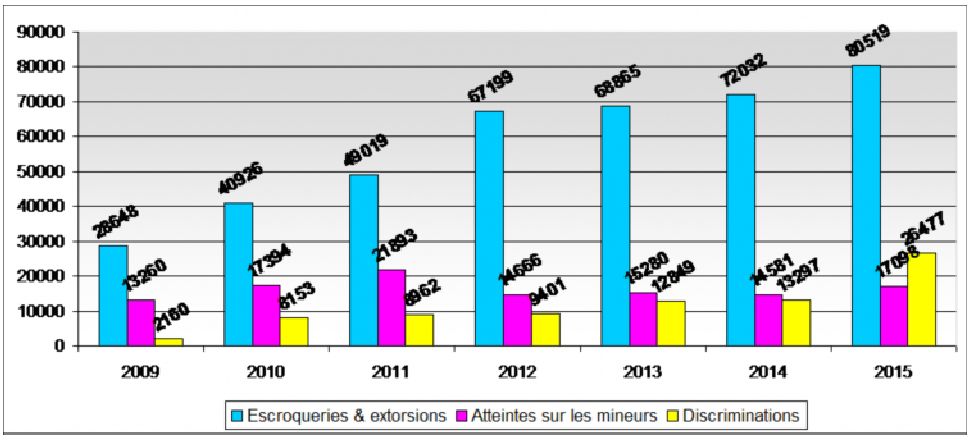


Figure 6 - Répartition des signalements par grandes catégories

Le domaine du terrorisme a connu deux pics, en janvier et novembre, moments des attentats, mais a toujours conservé un niveau soutenu, en raison notamment de l'assassinat de Saint-Quentin-Fallavier (juin) et de l'attentat du Thalys (août).

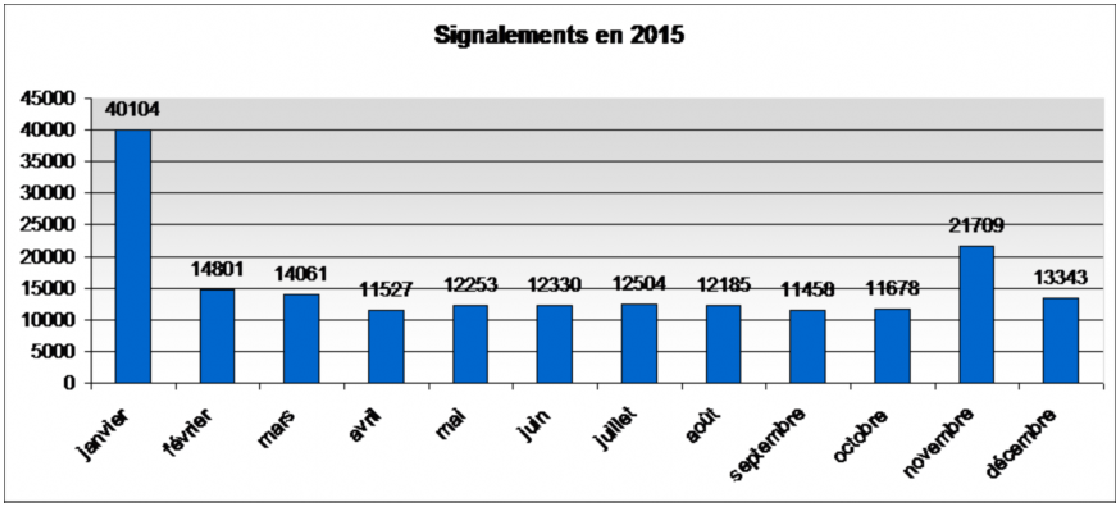


Figure 7 - Nombre de signalements mensuels

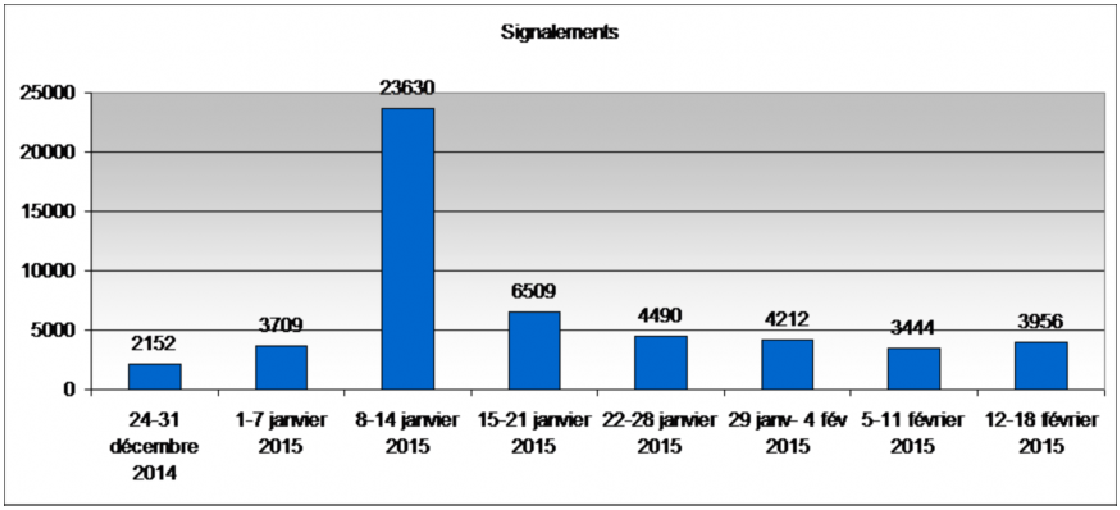


Figure 8 - Nombre de signalements hebdomadaires en janvier et février 2015

Sur la base des signalements reçus en 2015, la plateforme PHAROS a effectué :

- 26.286 transmissions, pour information ou pour action ;
- parmi lesquelles 16.848 transmissions pour action à des services d'enquête français.

Pour les besoins d'une partie de ces 16.848 transmissions, 138 enquêtes préliminaires ou de flagrance ont été ouvertes par la plateforme en 2015, afin de déterminer des critères de compétence territoriale au travers de l'identification des auteurs des faits (43,9% des procédures concernaient la pédopornographie).

En 2015, PHAROS a effectué 431 transmissions dans le domaine de la discrimination (contre 327 en 2014). Aux enquêtes judiciaires, il convient d'ajouter 1081 enquêtes pour secours à personne (741 en 2014). Il s'agit d'annonces de suicides imminents ou de massacres en milieu scolaire et de dénonciations de violences intrafamiliales ou d'abus sexuels. Malgré l'avertissement porté sur le site www.internet-signalement.gouv.fr, précisant qu'il ne faut pas signaler par ce canal les informations nécessitant une intervention urgente, la plateforme est mobilisée en moyenne trois fois par jour pour localiser des personnes à secourir et alerter les services territorialement compétents.

En **2016**, PHAROS a reçu 170 721 signalements : 49% concernaient des escroqueries, 11% des atteintes aux mineurs, 10% des discriminations et 7% des faits d'apologie et de provocation au terrorisme.

Blocage / Déréférencement

Suite à la loi du 13 novembre 2014, l'OCLCTIC a été désigné autorité administrative pour la mise en œuvre de la procédure de blocage et de déréférencement des contenus à caractère terroriste ou pédopornographique. Celle-ci se décline par étapes, le blocage des contenus n'intervenant qu'en fin de processus. L'office commence par enjoindre l'hébergeur ou l'éditeur de retirer les contenus. A défaut de retrait sous 24 heures, l'office s'adresse aux fournisseurs d'accès à internet (FAI) pour qu'ils procèdent au blocage des

sites incriminés. Lorsque les informations relatives à l'éditeur ne sont pas disponibles, l'OCLCTIC peut notifier directement les adresses aux FAI. Au final, un internaute qui tente de se connecter aux adresses bloquées est automatiquement renvoyé vers une page d'information officielle. L'OCLCTIC peut également communiquer la liste d'adresses aux éditeurs de moteurs de recherche afin qu'elles ne figurent pas parmi les résultats des requêtes des internautes (déréférencement). L'ensemble du dispositif est placé sous le contrôle de la commission nationale de l'informatique et des libertés.

Entre **mars et décembre 2015**, PHAROS effectuait 558 demandes de retrait (121 pour du contenu à caractère pédopornographique et 437 pour du contenu faisant l'apologie du terrorisme), faisait bloquer 283 adresses (240 à caractère pédopornographique et 43 faisant l'apologie du terrorisme) et déréférencer 511 adresses (323 à caractère pédopornographique et 188 faisant l'apologie du terrorisme).

L'ordre de grandeur des renvois hebdomadaires d'internautes vers la page officielle liée à la pédopornographie varie entre 20 000 et 42 000, pour un total de 2,5 millions de visites en 2016, alors que celui concernant des sites terroristes ou d'apologie du terrorisme oscille entre 200 et 800.

En **2016**, l'office a adressé aux professionnels de l'Internet 3129 demandes de retrait (2774 concernaient des faits de terrorisme et 355 des faits de pédopornographie), 834 demandes de blocage (676 concernaient des faits de pédopornographie et 158 des faites de terrorisme) et 1929 demandes de déréférencement (1158 à caractère pédopornographique et 771 faisant l'apologie du terrorisme).

Les spécificités de l'année 2015

2015 fut une année de changements majeurs pour la plateforme PHAROS, dont les effectifs ont été portés à 20 enquêteurs, policiers et gendarmes, parmi lesquels 3 enquêteurs consacrés au blocage/déréférencement. Ils sont commandés par un officier de gendarmerie et intégrés à la section de l'Internet de l'OCLCTIC qui prend également en charge la plateforme INFO ESCROQUERIES et le montage du projet de plainte en ligne pour les escroqueries du Web.

D'autre part, l'explosion du nombre de discriminations en ligne a entrainé une réponse adaptée et rapide. A l'automne 2015, une cellule spécialisée dans le droit de la presse a été installée au sein de la plateforme, justifiée par le besoin d'une expertise juridique et opérationnelle dans cette matière. Composée de quatre enquêteurs, sa mission est d'assurer le traitement des signalements dans ce domaine, le traitement judiciaire des infractions relevées et la veille et détection en amont de contenus haineux.

PHAROS est aujourd'hui une source d'information essentielle pour les services de lutte antiterroriste, notamment dans le domaine du terrorisme islamiste, certains profils détectés par les internautes sur les réseaux sociaux se révélant liés à des activistes avérés.

4.3 Les faux ordres de virement

Apparues en 2010, les escroqueries aux faux ordres de virements internationaux, après avoir connu leur apogée en 2013 et 2014, perdurent en France à un niveau élevé,

touchant en particulier les sociétés françaises et leurs filiales. En six ans, l'office central pour la répression de la grande délinquance financière (OCRGDF) a ainsi recensé plus de 2550 faits concernant 1600 sociétés victimes pour un préjudice global estimé à plus de 550 millions d'euros. Les tentatives représentent plus d'un milliard d'euros.

Aujourd'hui, l'ensemble des pays européens, ainsi que le Canada et les Etats-Unis sont concernés par le phénomène, les malfaiteurs d'origine franco-israélienne ayant formé des complices dans de nombreuses langues étrangères.

Malgré la mise en place de très nombreuses actions de prévention, les auteurs ont toujours su faire évoluer le mode opératoire initial et tirer pleinement partie de l'usage des nouvelles technologies. Cette escroquerie est fondée sur la technique de l'ingénierie sociale, visant à recueillir des informations relatives à l'organisation et au fonctionnement d'une entreprise. Elle permet aux escrocs, usurpant l'identité du dirigeant de la société, de son correspondant bancaire ou d'un de ses fournisseurs d'obtenir le versement indu de fonds.

Internet est le moyen privilégié par les malfaiteurs pour récupérer des informations sur la société visée et ses employés, via les réseaux sociaux, les sites professionnels d'information sur les entreprises Les escrocs utilisent également les messageries électroniques et les plates-formes de téléphonie dématérialisée pour asseoir leurs manœuvres frauduleuses et s'anonymiser.

Des virus informatiques sont parfois utilisés pour récupérer les données de l'entreprise. Dès 2013, des échanges avec des partenaires industriels et policiers d'autres pays attirent l'attention sur ce nouveau *modus operandi* et deux affaires judiciaires révélaient l'utilisation effective du virus BlackShades à cette fin.

Parmi les modes opératoires utilisés par les escrocs, celui consistant à informer la victime d'un changement de domiciliation bancaire est le plus utilisé et le plus difficile à détecter.

4.4 Le piratage des standards téléphoniques : prévention et répression

Dans la majorité des cas, la fraude aux auto-commutateurs téléphoniques (PABX, IPBX ou plus communément standards téléphoniques) consiste à pirater les systèmes téléphoniques afin de passer des appels gratuitement (Phreaking).

Par exemple, une commune de l'Ouest de la France a révélé en novembre 2016 qu'elle avait été victime d'une cyberattaque au printemps contre son système téléphonique. Pendant quatre jours, des cybercriminels ont eu accès à ce système et ont passé des appels internationaux à destination de l'Afrique et de l'Amérique Latine pour un montant de 80 000 euros.

Les pirates téléphoniques utilisent principalement 3 moyens :

- Le piratage du standard téléphonique en profitant d'une faille de sécurité dans le pare-feu informatique,

- Le piratage de la messagerie vocale en détournant un poste téléphonique de l'entreprise en accédant à la messagerie vocale d'un collaborateur, puis en trouvant le mot de passe de la boite vocale, et enfin en passant des appels ou en mettant en place des renvois vers des destinations internationales,
- Le piratage de l'interface d'administration en s'introduisant directement dans l'interface d'administration du compte téléphonique de l'entreprise, pour accéder aux fonctionnalités et prendre le contrôle à distance.

Les appels ainsi passés vers des numéros surtaxés peuvent rapporter des codes à jouer sur Internet qui permettent de gagner de l'argent ou des lots (jeux dits « d'instant gagnant »). Le piratage d'autocommutateurs peut aussi avoir pour objectif de passer des appels en masse vers des numéros surtaxés de sites fictifs (essentiellement basés à l'étranger) afin de créer du trafic et de se rémunérer sur des recettes publicitaires ou grâce aux reversements des opérateurs.

Les destinations des communications qui génèrent un coût macro-économique important sont très variées (tous les continents).

Fraude aux PABX un contentieux de masse

Les escroqueries aux autocommutateurs de téléphonie (PBX) facilitées par la voix sur IP (IPBX) représentent un contentieux de masse dont **le montant des préjudices a dépassé sur le ressort de la préfecture de Police les 600.000 euros en 2015 contre 300.000 euros en 2014** pour les dossiers portés à la connaissance de la BEFTI. **80 dossiers ont donné lieu à un préjudice consolidé d'un million d'euros.**

Les fraudes sont réalisées en raison d'une carence d'installation et de gestion du système d'information et non la conséquence de réelles vulnérabilités techniques du système. Les auto-commutateurs sont livrés toutes fonctionnalités ouvertes et il revient au titulaire du traitement de refermer celles considérées comme risquées notamment eu égard aux données à caractère personnel.

Il ne s'agit en général pas d'attaques cybercriminelles, mais de fraudes dont les faits sont d'abord de l'escroquerie comme infraction principale, voire de l'escroquerie en bande organisée.

Autres formes de fraude téléphonique

Le 10 mars 2015, les policiers de la sûreté départementale de la DDSP 13 et du GIR 13 ont interpellé, à Marseille et en Île-de-France, neuf individus impliqués dans une vaste escroquerie perpétrée au préjudice de milliers de particuliers. Les coordonnées bancaires de ces derniers, frauduleusement obtenues, permettaient de recharger des cartes téléphoniques pré-payées ensuite utilisées, pour appeler plusieurs dizaines de numéros surtaxés ouverts par les escrocs. Le préjudice est estimé à plus de 4 500 000 € ; le montant des avoirs criminels saisi est d'ores et déjà de 1 200 000 €.

5 La dimension cyber des attentats de 2015

A la suite des attaques terroristes ayant visé la France, le 7 janvier 2015, les cyber-djihadistes ont mené des actions contre des sites Internet français.

Ces actions ont combiné à la fois la publication de messages d'apologie du terrorisme et d'incitation à la haine raciale et à la violence véhiculés via les réseaux sociaux et les grandes plates-formes de service de l'Internet (notamment pour les vidéos) et des attaques informatiques engagées en masse contre les sites institutionnels ou de citoyens français.

Ces modes d'action ont été le prolongement des attentats terroristes parisiens déclenchant par ailleurs l'affrontement de mouvements idéologiques opposés : les groupes de hackers défendant les sites djihadistes contre les groupes de hackers Anonymous se diffusant respectivement sous les appellations #OpCharlieHebdo et #Opfrance.

Ils n'ont cependant pas été reconduits de façon notable lors des attentats ultérieurs du 13 novembre 2015 et au cours de l'année 2016.

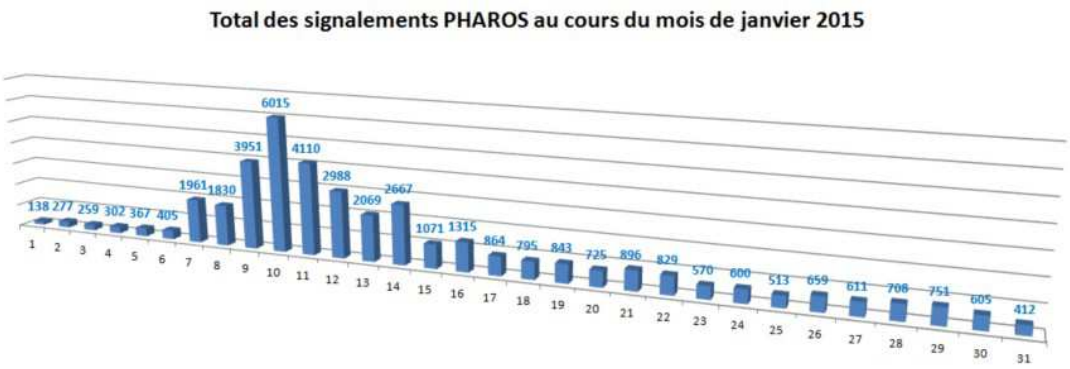
Nature des atteintes

Dans le cadre des attaques menées sous la bannière #OpFrance, il est possible d'identifier plusieurs types différents d'atteintes aux systèmes d'Information. Il s'agit de défigurations de sites Internet, de piratages avec exfiltration de données, voire d'attaques en déni de service distribué (DDoS) ou d'attaques annexes.

5.1 Activité de la plate-forme PHAROS et des services de sécurité intérieure en janvier 2015

Un volume sans précédent de signalements sur PHAROS

La plateforme PHAROS, de la sous-direction de la lutte contre la cybercriminalité a été mobilisée dés le 07 janvier 2015 en H24. Le bilan chiffré démontre une croissance inédite de la fréquentation du site Internet www.internet-signalement.gouv.fr. La volumétrie moyenne antérieure aux attentats se situait à 400 signalements par jour. Entre les 7 et 30 janvier 2015 PHAROS a reçu 37 829 signalements, toutes catégories d'infractions



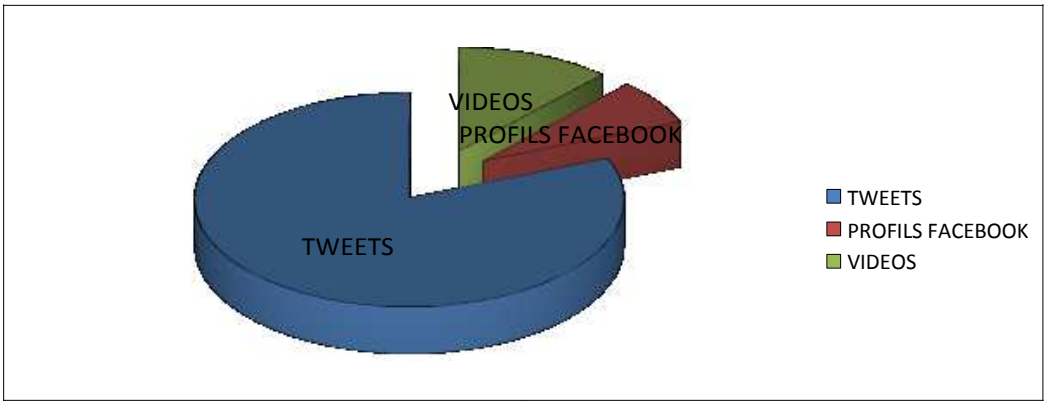
confondues. 29 000 environ étaient liés aux événements terroristes.

Apologie du terrorisme

La répartition de ces demandes se décline comme suit :

Sur la période du 07 au 21 janvier 2015, la SDLC a transmis par le canal G7/H24 20 demandes distinctes de gels de données en relation avec les événements terroristes, ciblant un total de 498 contenus (vidéos, adresses e-mail, adresses IP, comptes sur réseaux sociaux…). Ces gels de données ont été complétés par des demandes de suspension des comptes incriminés et de communication des données relatifs aux titulaires des comptes.

La répartition de ces demandes se décline comme suit :



Défigurations et piratages

Près de 1500 défigurations (défaçages) et piratages de sites Internet français ont également été recensés par la SDLC, Sur ce nombre, environ 850 provenaient de signalements reçus par la plate-forme PHAROS. Ces attaques étaient revendiquées par des équipes de hackers (Fallaga team, Arab warriors team, Anonghost, Apoca DZ).

5.2 Plusieurs dizaines de procédures judiciaires engagées par la gendarmerie nationale et son C3N

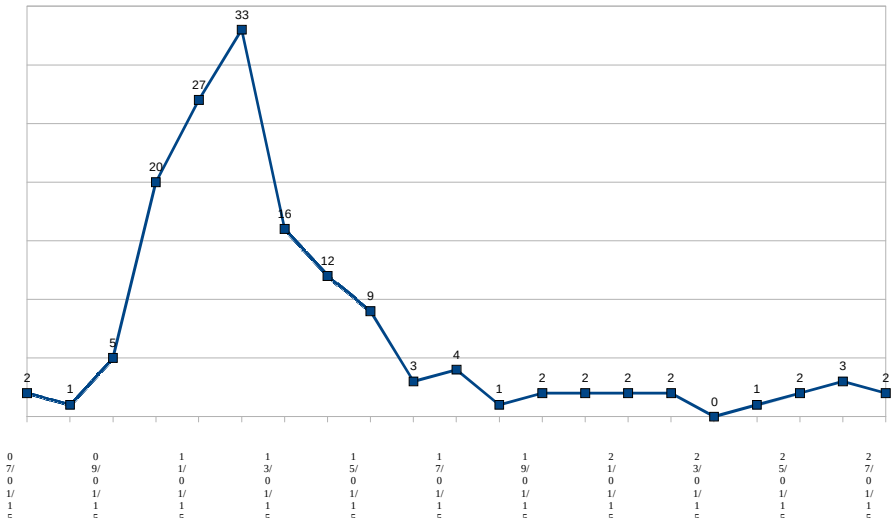
Dès le début de la crise générée par les attentats de début janvier, la gendarmerie s'est immédiatement investie dans la mission de veille, de recueil et de centralisation du renseignement, en dédiant les enquêteurs du C3N à cette tâche.

Les menaces identifiées étaient de deux ordres : attaques informatiques en direction de sites institutionnels ou privés (défaçages ou dénis de services) et faits d'apologie du terrorisme relayés sur les réseaux sociaux (Facebook ou Twitter).

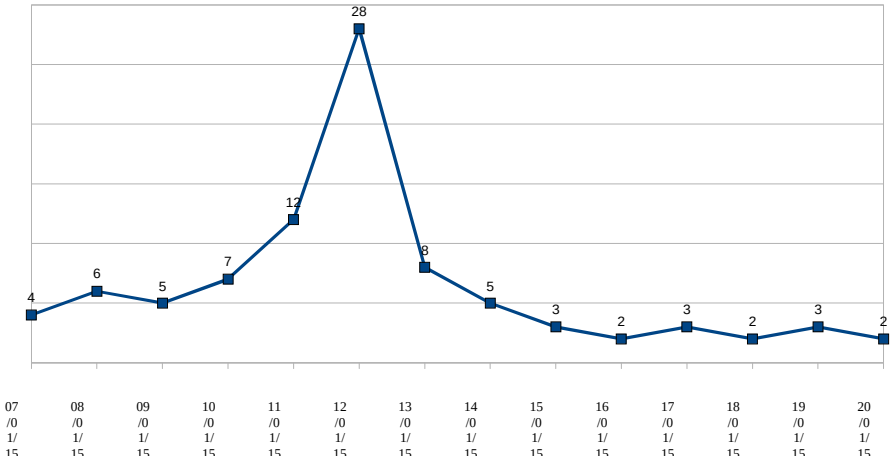
149 faits de défaçages ont été portés à la connaissance du C3N par le biais des CRPJ et 90 procédures ont été établies pour apologie du terrorisme.

Dès la survenue des attentats le 7 janvier, une surveillance de Twitter s'est mise en place au sein du C3N à l'aide d'outils logiciels spécifiques permettant de mettre en exergue des faits de soutien aux actes terroristes et constituant des infractions d'apologie du terrorisme.

Les procédures judiciaires engagées par les unités de gendarmerie pour des faits d'**apologie du terrorisme** se répartissent dans le temps selon le graphique suivant :



Les procédures judiciaires engagées par les unités de gendarmerie pour des faits de **défaçages de sites** se répartissent dans le temps selon le graphique suivant :



5.3 L'activité de la préfecture de police et de la BEFTI

Le nombre de plaintes pour défigurations ou infractions en lien avec l'entreprise terroriste recueillies et traitées par les services de l'agglomération parisienne s'établit comme suit :

- Sur les 4 parquets de l'agglomération parisienne on a pu recenser compte tenu des difficultés d'éparpillement des saisines, environ 30 à 40 affaires DRPJ liées à l'attentat et 13 dans les services locaux de Paris qui ont établi également quelques mains-

courantes : pour défigurations, dénis de service, apologies et menaces d'atteintes aux personnes sachant que plusieurs infractions sont commises dans chaque affaire et que certains signalements ont eu lieu sans plainte pour ne pas leur donner d'audience.

- Une cinquantaine de procédures ont donc été initiées, 1/4 étant traitées par le service local à Paris les autres par la BEFTI, la Brigade de Répression de la Délinquance contre la Personne (BRDP) ou les districts et Service de Police Judiciaire (DPJ) pour Paris et (SDPJ) la petite couronne. Les procédures pénales n'ont pas été nombreuses sur Paris et la petite couronne, car beaucoup d'internautes n'ont pas souhaité déposer plainte.

5.4 La France une cible mondiale

Pendant la période des attentats, la plupart des attaques cyber au niveau mondial se sont concentrées sur la France.

Le graphique ci-dessous a été réalisé à partir du nombre des défaçages et piratages de sites dans le monde, revendiqués par les équipes de hackers, soit 3717/an. Sur cette volumétrie ont été reportées les attaques revendiquées ciblant les sites nationaux, soit 1284/an.

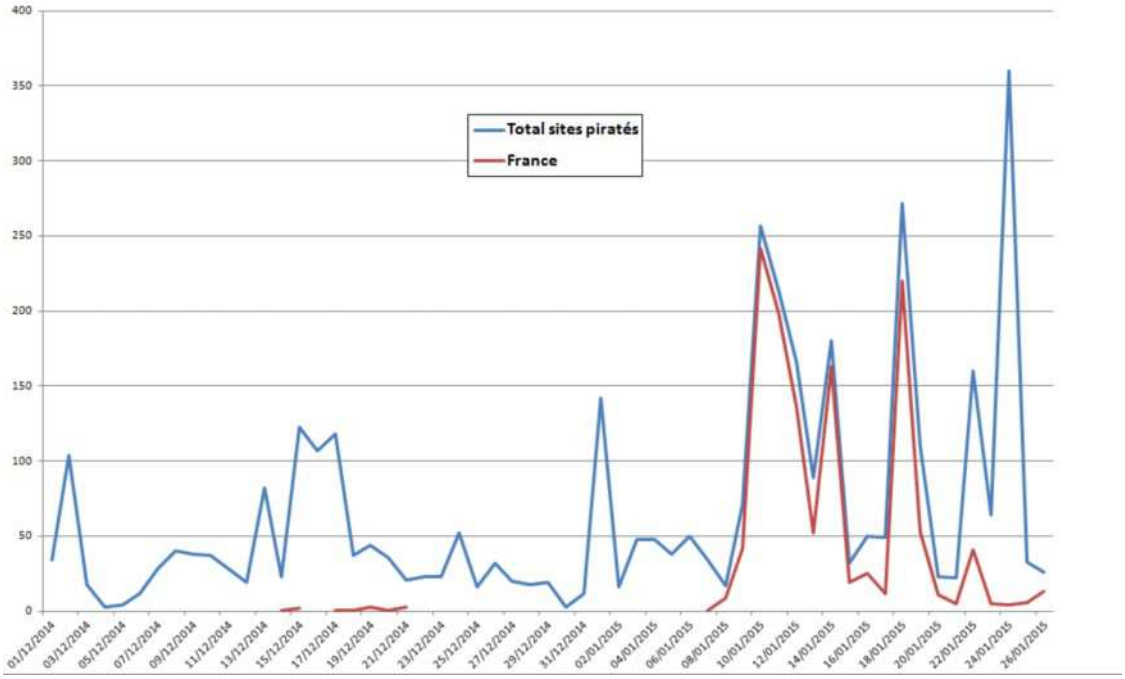


Figure 9 - Nombre de défacements revendiquéés dans le monde et en France au moment des événements du début de l'année 2015

5.5 Les mesures de traitement mis en œuvre : l'adaptation du dispositif

Au niveau de PHAROS

La plate-forme PHAROS a été transformée en cellule de crise permanente, adoptant un mode de fonctionnement 24H/24. Les effectifs de PHAROS ont été renforcés de manière significative par l'ensemble des effectifs de la SDLC et de la SDLCODF.

La priorité a été de garantir une lecture systématique en temps réel des signalements, pour discriminer ceux d'entre eux devant être dirigés en urgence vers l'UCLAT.

Une veille spécifique sur les réseaux sociaux a été mise en place, en lien constant avec le point de contact national du SCRT (service central du renseignement territorial.)

Le bureau de l'Internet de la section de l'Internet de la SDLC a mis en place un lien permanent avec les sociétés de service de l'Internet (Twitter/Facebook/ Google-Youtube/Dailymotion).

La section des relations internationales de la SDLC a tenu à jour la main courante de l'ensemble des demandes de gels de données, adressées principalement aux États-Unis.

Un travail préventif particulier a été mis en œuvre pour la détection les vidéos d'apologie du terrorisme, avec Dailymotion, Youtube (Google), Wat.tv pour TF1, à partir d'un travail d'empreinte numérique des supports vidéos.

Au total, pour l'année 2015, PHAROS recevait et traitait 31.317 signalements portant sur des faits de terrorisme. 16.429 étaient directement transmis à des services anti-terroristes. 101 faisaient l'objet d'une judiciarisation immédiate avant d'être transmis aux services territorialement compétents.

Au niveau national

La SDLC a maintenu une vigilance particulière sur l'évolution du phénomène et a mobilisé l'ensemble des correspondants des DIPJ et DRPJ afin d'organiser les prises de plaintes et de faciliter la remontée des informations de nature technique susceptibles de fournir des orientations sur les méthodes d'attaques et les pistes d'enquête à envisager. Une coordination opérationnelle avec la gendarmerie nationale a été organisée.

Une alerte au plan européen avec Europol/EC3 a été également lancée. Un travail d'exploration du darkweb est également toujours en cours.

5.6 Mesures entreprises suite aux attentats pour améliorer les capacités du ministère de l'Intérieur

Innovation

Les attentats terroristes qui ont touché la France ont obligé à revoir les outils et méthode de travail des enquêteurs spécialisés dans la lutte contre la cybercriminalité.

Ainsi, en avril 2016, s'est tenu le premier hackathon de la Gendarmerie nationale à Issy les Moulineaux. L'application Web **GendLoc**, servant à géolocaliser des personnes en montagne sans l'installation préalable d'une application sur leur smartphone, a servi de levier à idées. En effet, le projet CATEMSI développé par le STSI² permettra aux personnes détentrices d'un smartphone, coopérantes et dans la zone de couverture de leur opérateur, de transmettre automatiquement leurs coordonnées GPS ainsi que des photos permettant de décrire la situation rencontrée, sans téléchargement préalable sur un magasin d'applications.

Suite aux événements de Novembre 2015, dans le cadre de l'état d'urgence et des perquisitions administratives associées, **GendExtract** a été réalisé au sein du département informatique électronique (INL) de l'IRCGN afin de répondre aux contraintes opérationnelles auxquelles les unités territoriales étaient soumises. Il s'agissait de mettre à disposition des forces de gendarmerie un outil autonome permettant une extraction et une exploitation rapide des données contenues dans un ordinateur à analyser de type PC ou MAC, sans en modifier son contenu. GendExtract se présente sous la forme d'un système d'exploitation de type Windows et d'une suite logicielle criminalistique utilisable sans installation préalable.

Dès fin novembre 2015, GendExtract a été diffusé au sein du réseau CyberGend de la gendarmerie, puis dans les jours suivants aux services spécialisés de la police nationale et de la DGSI.

La SDLC a développé de son côté un outil gratuit et semi-automatisé, baptisé « **DARWIN »** (pour Discrimination, Analyse, Recherche, Windows). Il s'agit d'une clé USB autonome qui, connectée à un ordinateur éteint, analyse son disque dur sans l'altérer, garantissant la fiabilité de la preuve en cas de découverte d'une infraction. Elle s'adapte à tous les systèmes d'exploitation : Windows, Linux et Mac. Le projet a été mené en collaboration avec la DSCP et la DRCPN.

Dans le cadre du **PLAT** (Plan de Lutte Anti Terroriste), un budget exceptionnel a été attribué à la lutte contre la cybercriminalité en relation avec le terrorisme. Confié à la SDLC, il a permis, entre autres, la création de 14 Laboratoires d'Investigation Opérationnelle du Numérique (LION). Par exemple, au cours de l'été 2016, le LION de Marseille a été largement mis à contribution dans l'exploitation des supports numériques découverts sur la scène d'attentat du 14 juillet à Nice.

Enfin, la délégation ministérielle aux industries de sécurité se rapproche au cours de l'année 2016 de la mission de lutte contre les cybermenaces, pour créer la DMISC qui aura ainsi une vision transverse sur les questions numériques, d'innovation et de partenariats pour la sécurité.

5.7 Quelques enseignements de la crise

La dimension cyber de la menace terroriste n'a pas de frontières

Il existe une continuité des activités terroristes sur le net : elles se propagent sur un espace trans-frontières et entièrement dématérialisé.

Les réseaux sociaux amplificateurs des événements

Les réseaux sociaux sont des amplificateurs de l'apologie du terrorisme et participent via leurs usages à la consolidation du sentiment général des menaces terroristes par la population.

La problématique posée par les cyber-cafés

La problématique des cyber-cafés et autres spots Wi-Fi a ressurgi pendant les événements de janvier mettant encore une fois en évidence le non-respect de la loi par les boutiques spécialisées en accès Internet ou qui offre à titre accessoire cet accès nuisant à l'enquête en cours. Ces boutiques contrairement à leurs obligations ne conservent pas les traces de connexion et d'identification des éditeurs de contenus.

6 Les actions de prévention

La lutte contre les cybermenaces nécessite un fort investissement en matière de prévention, eu égard à la multiplicité des possibilités d'atteintes et des victimes potentielles. Il s'agit d'associer en amont l'usager à cette lutte en lui apportant les outils nécessaires pour prévenir ces risques. Les services du ministère de l'Intérieur sont pleinement impliqués dans ces efforts.

Un des axes du plan ministériel de lutte contre les cybermenaces en matière de sécurité intérieure de mai 2014 vise à améliorer le niveau de sensibilisation et de prévention contre les cybermenaces des particuliers, des acteurs économiques et des collectivités territoriales.

6.1 Grand public

La division d'anticipation et d'analyse (D2A) de la SDLC est, depuis 2 ans, membre du forum européen de prévention et sensibilisation du centre de cyber-criminalité européen (EC3) d'Europol, dans le cadre des plans d'actions contre les cyber-attaques. Rassemblant 27 états membre de l'UE, le forum est un espace de partage des approches et des idées de préventions qui se déclinent ensuite par des actions concertées et simultanées en Europe. La D2A a participé à la journée de l'internet "sécurisé" (Internet Safer Day) qui a lieu une fois par an. Il s'agit notamment de promouvoir l'événement par une action de communication utilisant le site Web de la Police Nationale. Au cours d'une autre campagne de prévention contre les malwares mobiles coordonnée par EC3, le même site Web a pu relayer des spots vidéo, documents et plaquettes de prévention via les différents sites et réseaux sociaux de la Police Nationale. La division développe actuellement un site web portant sur la cybercriminalité sur lequel figureront à l'avenir les campagnes européennes de prévention face aux attaques cyber.

Plus récemment, elle a intégré le projet **NoMoreRansom** visant à lutter contre les menaces liées aux rançongiciels. Elle relaie sur le site de la police nationale ce service européen développé en partenariat avec Microsoft, Kaspersky, Intel Security, et la police hollandaise.

En décembre 2016, l'association CECyF, dont est membre la gendarmerie nationale, a développé une version en langue française de ce site Web[1] pour rendre le contenu encore plus accessible au public de notre pays.

Protection des jeunes publics

Le Permis Internet (PI) est une action de proximité, concrète, destinée à sensibiliser les élèves de CM2 aux dangers du web et à leur donner des conseils pour utiliser Internet en toute sécurité.

Lancée le 12 décembre 2013, après une phase d'expérimentation conduite par les brigades de prévention de la délinquance juvénile (gendarmerie nationale) jusqu'en juin 2014, l'opération a été généralisée à l'ensemble des unités territoriales de cette direction.

Ce dispositif a ensuite été étendu à la police nationale et à la Préfecture de police à la rentrée scolaire de septembre 2015. Le financement des supports pédagogiques est assuré par un partenariat avec la fondation AXA Prévention.

A la fin de l'année 2016, ce sont plus de 800 000 enfants qui ont été formés.

6.2 Sensibilisation du monde économique

S'inscrivant dans le cadre du plan ministériel de mai 2014, il a été décidé de sensibiliser à la cybersécurité les réseaux des référents sûreté et des référents intelligence économique de la police et la gendarmerie nationale. Les objectifs recherchés sont de permettre au travers des contacts entrenus par ces réseaux avec notamment les PME/PMI, d'apporter une réponse adaptée au tissu économique au travers l'offre de service de la gendarmerie en matière de sécurité économique, et le cas échéant de faciliter les contacts avec le réseau des enquêteurs spécialisés de la police (ICC) et de la gendarmerie (CyberGend).

Après la session parisienne du 22 octobre 2015 et six autres en province, une dernière session de sensibilisation à la cybersécurité des référents sûreté et des référents intelligence économique s'est tenue le 30 septembre sur le site de la DGGN à Issy-les-Moulineaux.

Les référents gendarmerie peuvent également accéder à une documentation mise en place sur leur réseau social professionnel (Resogend). Par ailleurs, les nouveaux référents suivent depuis octobre 2015 un module spécifique lors de leur formation initiale.

La division d'anticipation et d'analyse de la SDLC a développé un fascicule "Réagir à une attaque informatique, 10 préconisations " qui délivre au grand public comme aux entreprises les conduites à tenir après incident, notamment en ce qui concerne

[1] https://www.nomoreransom.org/fr/index.html

l'accompagnement de la plainte et le traitement du processus judiciaire. Ce fascicule est régulièrement diffusé sur les événements du monde numérique (par exemple au FIC).

La DGSI a, quant à elle, réalisé, en 2016, un ensemble de de 1450 conférences à destination du public, essentiellement auprès d'acteurs économiques (PME, groupes industriels, décideurs institutionnels, etc.). Environ 75000 auditeurs ont ainsi été sensibilisés aux risques cyber et à leurs effets sur l'activité de leur structure d'appartenance.

6.3 Intelligence économique territoriale

6.3.1 Service central de renseignement territorial

Grâce à son maillage territorial, le service central de renseignement territorial joue un rôle essentiel de soutien et de capteur au profit des services spécialisés en charge de l'intelligence économique, dans le respect des attributions des services de l'État, de celles des ministères concernés compétents et en lien avec les préfets de région, au cœur du dispositif.

L'action du SCRT s'effectue via le pôle « Intelligence économique » (IE) de son secrétariat général, chargé de transmettre aux échelons départementaux des éléments de langage adaptés, d'animer et consolider un réseau de référents IE, d'exploiter et de valoriser les notes d'information transmises par les services territoriaux. Ces notes de valorisation sont transmises aux ministères concernés et au Service de l'information stratégique et de la sécurité économique du ministère des Finances.

Le pôle IE anime un réseau de 55 référents en intelligence économique dans les services départementaux du renseignement territorial. Cette interaction se traduit de manière optimale par des participations aux réunions des comités de pilotage organisés par les secrétariats généraux à l'administration régionale ou bien le cas échéant, par des représentations (par délégation) du chef du service central du renseignement territorial, aux groupes de travail spécialisés des services du haut fonctionnaire de défense, du secrétariat général de la défense et de la sécurité nationale et du service de l'information stratégique et de la sécurité économique (SISSE).

L'analyse économique « hors atteintes de sécurité » des entreprises, au niveau national, a représenté 3431 notes depuis la création du pôle IE en février 2014. Parmi celles-ci, le pôle « Intelligence économique » a distingué et valorisé 144 notes de fond relevant d'atteintes à la sécurité économique. La part des atteintes de cybercriminalité représente 24% de cette totalité, ce qui positionne la cybercriminalité à la 3e place des atteintes relevées juste derrière les prédations financières (25 %) et les actes de malveillances (28,5%). Les principales régions touchées par la cybercriminalité sont la Bretagne (80%), la Normandie (67%) et l'Aquitaine Limousin Poitou-Charentes (40%).

6.3.2 Gendarmerie nationale

L'organisation de la gendarmerie en la matière repose sur :

- une section intelligence économique et territoriale (SIET), à l'effectif de 2, rattachée à la SDAO, de niveau central ;
- un réseau de référents en intelligence économique (RIE) dans chaque région, chaque groupement (OAR ou cellule renseignement) et au sein de chacune des gendarmeries spécialisées.

La gendarmerie compte près de 190 référents en intelligence économique.

En 2015, 441 atteintes économiques ont été constatées en ZGN, dont 80 % concernent des entreprises de moins de 500 salariés particulièrement actives en termes d'innovations et près de 75 % sont perpétrées à partir de pays tiers (+28 % par rapport à 2013). Les risques informatiques sont les principales menaces auxquelles doivent faire face les entreprises concernées (50 % des atteintes en 2015) et il est constaté un doublement des risques financiers, qui représentent près du quart des atteintes.

Dans ce contexte, les unités de gendarmerie nationale ont effectué 6334 actions de sensibilisation d'entreprises, 682 diagnostics de vulnérabilités et rédigé 9039 fiches de renseignement traitant d'intelligence économique. Enfin, 4558 fiches «Surveillance établissement» ont été renseignées permettant d'orienter les patrouilles de surveillance générale de la gendarmerie autour de ces entreprises.

7 Coopération internationale et partenariats

Les enquêtes passent nécessairement par la coopération internationale

La collecte de la preuve numérique est très spécifique dans la mesure où les auteurs, victimes et serveurs informatiques sont situés dans différents pays. Les données techniques de connexion ou de contenus peuvent ainsi être hébergées sur des serveurs installés dans un pays donné, mais susceptibles de migrer à tout moment. L'administrateur du site quant à lui se trouvera dans un second pays, tandis que les victimes seront disséminées sur plusieurs continents. Les enquêtes ne peuvent donc aboutir sans coopération internationale, d'autant plus qu'une grande partie des infrastructures de l'Internet est basée sur le territoire américain, où sont installés tous les acteurs majeurs de l'industrie du service en ligne[1], ceux de l'industrie de l'hébergement ainsi que les organismes chargés de la gouvernance du réseau[2] et de l'attribution des noms de domaine.

7.1 Groupe de contact permanent

Sous l'impulsion du ministre de l'Interieur, Bernard Cazeneuve, dès le début de l'année 2015, un groupe de contact permanent est créé sous le pilotage de la délégation ministérielle en charge de la lutte contre les cybermenaces. L'objectif de ce groupe de travail est l'amélioration du signalement et du retrait des contenus illicites par les opérateurs (Apple, Google, Twitter, Microsoft, Facebook) et une meilleure prise en compte des

[1] Google, Facebook, Twitter, Yahoo, Microsoft, Apple
[2] ICANN, IANA

demandes adressées par les enquêteurs français pour obtenir un certain nombre de données (données de connexion ou de profil), prioritairement dans le cadre des affaires de terrorisme.

Le GCP s'est réuni en formation plénière à 6 reprises entre mai 2015 et juin 2016. Par ailleurs, la sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire a été chargée d'organiser des réunions technico-opérationnelles en bilatéral avec chacun des cinq acteurs de l'Internet, afin de traiter des difficultés propres à chacun.

Les travaux engagés ont abouti à l'élaboration de **formulaires normalisés de demandes d'information adaptés aux contraintes de chaque opérateur**. Ces standards ont été intégrés dans les logiciels de rédaction de procédure de la police et de la gendarmerie dès le 8 juin 2015.

Une **formation à destination de 200 enquêteurs** tous services confondus organisée avec les opérateurs le 20 janvier 2016, est venue compléter le dispositif en précisant les éléments pouvant faire l'objet de requêtes d'une part et les modalités pratiques des demandes, d'autre part.

Même si des difficultés résiduelles subsistent, force est de constater que les acteurs de l'Internet ont amélioré la qualité et les délais de leurs réponses depuis la mise en place du protocole de coopération. Réciproquement, les opérateurs indiquent une augmentation progressive de l'utilisation de ces standards par les enquêteurs, avec cependant des différences d'un opérateur et d'une direction à une autre. Les taux observés entre janvier et juin 2016 varient de 60% à 93,65%, puis de 70 à 92% entre septembre et décembre 2016.

Un circuit de traitement des demandes urgentes a été formalisé au sein des directions, prévoyant le recours aux guichets uniques, composés d'enquêteurs spécialisés et offrant un service d'astreinte. Ces guichets sont automatiquement destinataires de ces demandes pour information (dans le cas des urgences vitales et le terrorisme) ou pour validation (dans le cas des autres urgences).

Si l'on constate une nette amélioration des procédures, particulièrement efficaces dans les cas qui relèvent du terrorisme, le GCP explore des pistes pour améliorer encore le retour d'information vers les enquêteurs.

8 Communication de crise

La Direction générale de la sécurité civile et de la gestion des crises est chargée du pilotage d'un certain nombre de mesures facilitant la communication en cas de crise. Comme nous l'avons vu lors des événements terroristes qui ont frappé la France à partir du début de l'année 2015, les crises prennent souvent une dimension cyber et les outils numériques occupent une place croissante dans cette stratégie.

8.1 Système Alerte et d'Information des Populations (SAIP)

À la suite des attentats survenus en France en janvier et novembre 2015, la direction générale de la sécurité civile et de la gestion de crise (DGSCGC), en collaboration avec le Service d'information du gouvernement (SIG), ont travaillé au développement d'une application mobile d'alerte des populations sur smartphone : « SAIP », pour Système d'alerte et d'information des populations.

SAIP-MOBILE permet d'être alerté, via notification sur son smartphone en cas de suspicion d'attentat ou d'événement exceptionnel (accident de sécurité civile) susceptible de résulter d'un attentat.

Cette application complète le dispositif d'alerte et d'information des populations (SAIP) déjà existant (sirènes, messages radios préformatés...) et s'inscrit dans une démarche globale de sensibilisation de la population aux risques.

8.2 Médias Sociaux en Gestion d'Urgence (MSGU)

Figure 10 - Message de sensibilisation contre les rumeurs diffusé à l'occasion de l'attentat de Nice en juillet 2016

La DGSCGC utilise les médias sociaux dans le cadre de la gestion d'événements sur les trois niveaux d'engagement suivants :

- La veille : recherche d'éléments d'intérêt (dégâts, appels à l'aide...).

- La diffusion d'information qui nécessite d'impliquer la communication opérationnelle de crise à chaque étape, de la sensibilisation des publics jusqu'aux consignes de sécurité lors d'événements. Elle comprend aussi la capacité des médias sociaux à diffuser des alertes sur demande des autorités de gestion de crise.
- L'interaction avec la population implique la mise en place de liens avec les communautés d'internautes se fédérant autour de chaque crise pour soutenir les populations touchées, et également une capacité à répondre aux éventuelles sollicitations en situation d'urgence. Des initiatives peuvent alors être encouragées (ex : #PorteOuverte lors des attentats du 13 novembre).

Dans les pays francophones, c'est l'association VISOV (Volontaires Internationaux en Soutien Opérationnel Virtuel) qui accompagne le gestionnaire de crise, des conventions ayant été signées avec la DGSCGC et plusieurs EMIZ, SDIS ou préfectures. VISOV, qui compte plus de 100 bénévoles, peut réaliser un suivi des médias sociaux et fournir des informations sur la situation ou contribuer à la communication de crise via le nombre important des comptes mobilisés. L'association est mobilisée plus de 10 fois par an sur divers types d'événements depuis 2013 (attentats, catastrophes naturelles, accidents, etc.).

Glossaire

Terme/Acronyme	Définition
ANSSI	Agence nationale de la sécurité des systèmes d'information
APT	Advanced persistant threats - menaces persistantes avancées, auxquelles on pourra préférer la notion d'attaque en profondeur ou ciblée, souvent via des RAT
BEFTI	Brigade d'enquête sur les fraudes aux technologies de l'information (Préfecture de police de Paris)
C2MI	Centre de cyberdéfense du ministère de l'intérieur
C3N	Centre de lutte contre les criminalités numériques (PJGN)
CLUSIF	Club de la sécurité de l'information français
CNIL	Commission nationale informatique et libertés
Cryptlocker	Rançongiciel chiffrant: le logiciel malveillant chiffre les documents personnels de la victime et réclame le paiement d'une rançon pour obtenir la clé de déchiffrement
CyberGend	Réseau des enquêteurs spécialisés en technologies numériques (Gendarmerie)
EC3	European Cybercrime Centre (Europol)
FSSI	Fonctionnaire de sécurité des systèmes d'information
GCP	Groupe de contact permanent (Etat - prestataires de l'Internet)
ICC	Investigateurs en cybercriminalité (police)
IoT	Internet des objets - réseaux permettant de relier les objets connectés. Il s'agit parfois de connexions via Internet ou via des réseaux dédiés
NTECH	Enquêteurs en technologies numériques (gendarmerie)
OCLCTIC	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (DCPJ/SDLC)
ONDRP	Observatoire national de la délinquance et des réponses pénales
OSCP	Observatoire de la sécurité des cartes de paiement
PABX	Autocommutateur téléphonique privé
PHAROS	Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements
PJGN	Pôle judiciaire de la gendarmerie nationale
RAT	Remote administration trojan - logiciel malveillant permettant un contrôle complet de la machine infectée (ou remote administration tool lorsqu'il s'agit uniquement d'un outil d'administration)
SDLC	Sous-direction de lutte contre la cybercriminalité (DCPJ)
SISSE	Service de l'information stratégique et de la sécurité économiques
SSMSI	Service de statistique ministérielle de sécurité intérieure
STAD	Systèmes de traitement automatisé de données
T-CY	Comité chargé du suivi de la convention du Conseil de l'Europe de lutte contre la cybercriminalité (dite convention de Budapest)
Tor	The onion router - système d'anonymisation sur Internet reposant sur une succession de rebonds via des serveurs (appelés nœuds) librement accessibles, combiné à un chiffrement de la communication

DELEGATION MINISTERIELLE AUX INDUSTRIES DE SECURITE ET A LA LUTTE CONTRE LES CYBERMENACES

État de la menace liée au numérique en 2017

Équipe éditoriale

Le présent rapport a été établi grâce aux contributions de la Préfecture de police, de la Direction générale de la police nationale, de la Direction générale de la gendarmerie nationale, de la Direction générale de la sécurité intérieure, des services du Secrétariat général du ministère de l'Intérieur (SHFD/FSSI et Mission intelligence économique) et de l'Observatoire national de la délinquance et des réponses pénales.

Sa rédaction a été réalisée sous la direction de M. Thierry Delville, inspecteur général de la police nationale, Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, par le colonel Éric Freyssinet, le commissaire divisionnaire Vincent Avoine, la commissaire Adeline Champagnat, Madame Myriam Quemener, magistrate et Madame Annick Rimlinger. Les travaux préparatoires avaient été conduits sous la direction du préfet Jean-Yves Latournerie, conseiller du gouvernement en charge de la lutte contre les cybermenaces.

Pour toute question, contactez dmisc@interieur.gouv.fr

Ministère de l'Intérieur, DMISC, Place Beauvau, 75800 PARIS Cedex 08