Intervention du colonel Fabrice BOUILLIÉ
Date : 1er décembre 2020
Cadre : Visio-conférence IDEF

L'INFLUENCE DE LA CRISE COVID-19 SUR LA CYBERCRIMINALITÉ

Les événements majeurs et les mutations sociétales génèrent des opportunités pour les activités criminelles en général, et cybercriminelles en particulier. La crise COVID-19, de par son intensité et son caractère inédit a amplifié ce phénomène.

L'analyse du traitement judiciaire de la cybercriminalité permet d'observer que **les auteurs ont principalement adapté les manières d'opérer existantes**, même si **des changements conjoncturels ont créé quelques nouveaux champs d'opportunité criminelle** (fraudes aux aides d'Etat). Elle permet également de nuancer la prédiction d'une explosion de la cybercriminalité. En effet, si certains indicateurs sont en hausse, ils le sont principalement dans la continuité de leurs évolutions antérieures.

Le fonctionnement dégradé des institutions permet de révéler les vulnérabilités préexistantes parfois masquées par des indicateurs de performance liés à un fonctionnement normal. Dévoilées par le contexte, elles peuvent augmenter la surface d'exposition aux attaques, par l'adaptation des manières d'opérer aux opportunités criminelles.

PANORAMA DES INFRACTIONS CYBER

Le traitement judiciaire de la cybercriminalité en 2019-2020 fait état de 72% de faits liés à des escroqueries, et de 6% d'atteintes aux STAD. Parmi ces derniers faits, les deux catégories les plus importantes sont les connexions frauduleuses (78%) et les attaques informatiques offensives (8%)[1].
L'analyse des procédures judiciaires en 2020 met en exergue une baisse des escroqueries par rapport à l'année 2019, notamment les escroqueries hors ligne, et dans une moindre mesure les escroqueries en ligne qui n'augmentent qu'en termes de proportions.

Les effets du 1er confinement

En ce qui concerne les escroqueries, deux observations :
- Baisse des escroqueries qui nécessitent une intervention physique entraînant de facto une hausse du ratio des escroqueries réalisées par le biais d'Internet. Ainsi, durant le confinement, 8 infractions sur 10[2] étaient totalement « numériques », contre 6/10 avant cette période.
- Existence d'un report des plaintes dû aux restrictions de circulation entraînant un afflux de plaintes post-confinement.

1 Note N° 73835/00124/2020 SCRC du 1er octobre 2020 - Analyse trimestrielle comparée de la délinquance (3T) - Atteintes aux STAD

2 Note N° 73835/00078/2020 SCRC du 02 juillet 2020 - Analyse trimestrielle comparée de la délinquance (2T) - Escroqueries au préjudice des personnes physiques

En ce qui concerne les atteintes aux STAD :
- Les atteintes aux STAD ont augmenté de 12% en 2020[3] ;
- Les cyber-attaques par rançongiciels ont fortement augmenté (327 en novembre 2020 contre 249 fin 2019)[4] ;
- Les attaques ont été plus ciblées et plus sophistiquées.

Des courbes en cohérence avec les évolutions antérieures

Pour les escroqueries :
- Pas d'augmentation notable des faits enregistrés entre 2019 et 2020. L'hameçonnage (phishing) étant le principal canal de commission d'escroqueries, cette constatation est confortée par la comparaison entre le nombre de pourriels signalés (signal Spam) et le nombre d'escroqueries. Les deux courbes sont en corrélation, en dehors de la période du confinement (restrictions de circulation)[5].
- Plafond de verre induit : consommation fortement réduite, diminution mécanique des transactions et donc des transactions frauduleuses. L'augmentation de l'offre (criminelle) n'entraîne donc pas une augmentation de la consommation (des victimes) et révèle un « point de satiété » du consommateur.

Pour les atteintes aux STAD :
L'ensemble des infractions cyber augmente de 22% entre 2019 et 2018[6]. La courbe des atteintes aux STAD avait déjà fortement augmenté en 2019, l'évolution en 2020 semble donc cohérente. Depuis 2016, les attaques par rançongiciels augmentent de façon régulière. L'année 2020 est marquée par la plus forte augmentation, et marque un tournant.

L'EXPLOITATION DES OPPORTUNITÉS CRIMINELLES

Les auteurs ont exploités :
- le contexte de crise et les opportunités créées par la **dégradation du fonctionnement des services publics** ;
- les **comportements irrationnels de certains acteurs** du fait de l'urgence ou des marchés financiers,
- les **vulnérabilités structurelles existantes** mises en exergue par le contexte.

L'adaptation des manières d'opérer préexistantes

Pour les escroqueries, il s'agira principalement, d'intégration d'éléments contextuels liés à la crise dans les manières d'opérer :
- **Difficultés de livraison liées au confinement**, ou coûts supplémentaires d'acheminement ;
- Difficultés pour la victime de contacter le ou les escrocs (télétravail et problèmes de réorganisation) ;
- Usurpation de l'identité des personnes publiques étatiques exposées à la crise pour commettre des escroqueries (Ministère de la santé, sécurité sociale, DGFIP, impôts, pour obtenir des informations au prétexte fallacieux de demandes liées aux aides de l'Etat, etc.). Ces informations peuvent permettre de tromper d'autres victimes (FOVI par changement de RIB, etc).

Les « produits » faussement vendus ou produits d'investissements sont adaptés au contexte économique lié à la crise sanitaire (investissement dans des structures de recherche, masques, gel hydro-alcoolique, etc.). **Les structures logistiques criminelles et outils préexistants ont aussi**

3 cf. renvoi 1
4 Note N° 73835/00125/2020 SCRC du 1er octobre 2020 - Analyse trimestrielle comparée de la délinquance (3T) - Rançongiciels
5 Note N° 73835/00115/2020 SCRC du 29 septembre 2020 - Analyse trimestrielle comparée de la délinquance (3T) - Escroqueries au préjudice des personnes physiques
6 Rapport d'analyse sur la criminalité organisée 2020 - Gendarmerie Nationale - p.140

été adaptés en vue des nouvelles opportunités. Par exemple, l'objet social de certaines sociétés fictives est modifié pour intégrer le champ médical ou paramédical.

Les nouvelles opportunités criminelles

- Report des manières d'opérer sur des acteurs institutionnels, publics et privés :
Si les particuliers semblent avoir été moins touchés, on note une augmentation des escroqueries au FOVI visant les personnes morales[7], stimulées par la conjonction de l'urgence et de conditions dégradées d'approvisionnement concernant certains matériels (masques, gel) pour le secteur médical/paramédical et les institutions publiques.

Le contentieux des fraudes aux prestations sociales et aides de l'Etat est particulièrement révélateur de cette adaptation. Détournant les outils et structures de leur affectation initiale, les GCO ont intégré les évolutions liées à la crises (réglementaires, technologiques, évolution des besoins, etc.). Ils ont concentré leurs actions sur l'exploitation des failles structurelles révélées et amplifiées par le contexte du confinement (difficultés des contrôles liés aux demandes de chômage partiel conjuguées à l'urgence de délivrer les aides)[8] .

Le constat est analogue pour les atteintes aux STAD : les rançongiciels et l'espionnage semblent avoir particulièrement visé les hôpitaux et les laboratoires[9]. Néanmoins, ces établissements étaient déjà la cible d'attaque en 2019. Le focus médiatique peut également amplifier le sentiment d'effet « crise » sur l'évolution des attaques par rançongiciels. Il peut aussi conduire les auteurs à cibler les institutions les plus vulnérables en temps de crise, qui seront autant d'acteurs pouvant céder à la tentation du paiement de la rançon.

Il n'en demeure pas moins que d'autres structures continuent d'être la cible de ces attaques (collectivités territoriales, entreprises, etc.). Par ailleurs, les applications mobiles malveillantes se multiplient et les chevaux de Troie pour smartphone sont une menace de plus en plus prégnante[10].

ANALYSE PROSPECTIVE RELATIVE AUX OUTILS JURIDIQUES

Malgré des efforts du législateur, il demeure un décalage entre les évolutions technologiques et l'évolution du Droit positif.
Aujourd'hui, il existe un corpus juridique étendu d'incriminations pénales. Or, et à l'instar des phénomènes criminels en général, les phénomènes de cybercriminalité ne sont pas réduits aux champs des infractions pénales.
Aussi, serait-il opportun de porter la réflexion d'une mise en cohérence des outils juridiques permettant d'encadrer les nouvelles technologies et leur utilisation (réseaux-sociaux, crypto-actifs), la gestion des données et le recueil des renseignements (échanges d'informations, objets connectés) et les menaces qu'ils génèrent, à travers une approche stratégique des phénomènes cybercriminels.
A ce titre, le Renseignement criminel permet une approche originale et globale, intégrant l'identification des menaces, l'échange d'informations et de renseignements entre les administrations et avec les entreprises privées, permettant de développer des outils techniques toujours plus pertinents de lutte contre la cybercriminalité.

7 Note N° 73835 / 00067 / 2020 SCRC du 25 mai 2020 - COVID19 - Escroqueries sur internet au préjudice des professionnels
8 Note N° 73835/00064/2020 SCRC du 15 mai 2020 - COVID19 - Fraudes aux dispositifs exceptionnels / Note N° 73835/00117/2020 SCRC du 2 octobre 2020 - Escroqueries aux ordres de virement, fraude activité partielle
9 Note N° 73835/0034/2020 du 10 avril 2020 - Analyse trimestrielle comparée de la délinquance (1T) - Rançongiciels
10 Note N° 73835/00030/2020 SCRC du 10 avril 2020 - Analyse trimestrielle comparée de la délinquance (1T) - Atteintes aux STAD