Club Etat d'Alerte Cyberdéfense

❖

7 Avril 2021

Autour de ***Guy-Philippe GOLDSTEIN***

Conseiller – PWC, Expon Capital

Enseignant – Ecole de Guerre Economique

Quels seront les nouveaux types de hackers ?

Les « cyber attaques » se sont multipliées ce derniers mois en France et dans le monde. Il n'est pas exagéré de parler d'une « industrialisation » de la délinquance sur le net. Finie l'époque où le hacker en tee-shirt, bidouilleur en solitaire, utilisait des kits de piratage. Aujourd'hui, l'interdépendance des utilisateurs et des plates-formes facilite les attaques à grande échelle. La cybercriminalité se professionnalise. Les hackers sont des hommes d'affaires. Curieusement, on ne compte pas de femmes. Avec nos différents comptes Google, Facebook ou TikTok, nos adresses e-mail, nos cartes bancaires et nos comptes en ligne, nous sommes devenus des cibles pour ces cybercriminels. L'arrivée des *cryptolockers* et des *ransomwares* a enrichi les possibilités de cyber attaques.

Pour faire face à cette cybercriminalité et à ce type d'attaques par « rançongiciel », le gouvernement français a débloqué un milliard d'euros sur cinq ans pour doubler le nombre d'emplois du secteur. Est-ce à la hauteur de la menace quand on sait qu'une nouvelle pègre internationale et hautement qualifiée se met en place ?

- **A-t-on affaire à une criminalité organisée ou à des hackers solitaires ?**

Le mot hacker vient du verbe anglais ***to hack*** qui signifie bidouiller. Il désigne des personnes qui testent des systèmes pour les explorer, non pas comme des ingénieurs mais pour les attaquer. Un hacker est en général un homme très qualifié dans son domaine qui plonge dans la criminalité par appât du gain. Il peut être une « petite main » au service d'un groupe ou d'un Etat. Il a un haut niveau d'études et de faibles revenus. [1]Dans les années 90 et 2000, l'on voit apparaître des *hackers* qui travaillent en petites équipes internationales pour le bien ou pour le mal (Swordfish) et pour des groupes criminels (mafias, cartels de blanchiment d'argent).

Aujourd'hui, **l'archétype du hacker solitaire est dépassé**. Le « black hat » évolue dans un réseau qui prospère au sein d'une industrie complexe et sophistiquée.

Au même titre que l'industrie légale, la cybercriminalité fonctionne avec des entreprises fournisseurs de services spécialisés et de logiciels qui vendent leur savoir faire à des groupes pour faire un juteux *business*. Un véritable écosystème s'est mis en place avec une sociologie bien différente. On y trouve de « jeunes mercenaires » mais aussi des hommes plus âgés, souvent des pères de famille avec une façade civile légale irréprochable. Les sommes en jeu sont, il est vrai, très motivantes !

On estime que le cout de la cybercriminalité avoisine les 950 milliards de dollars, soit environ 1% du PNB de l'économie mondiale !

Des groupes comme Revid ou Carbana affichent des chiffres d'affaires de 100 millions à 1 milliard de dollars. Derrière les attaques aux rançongiciels évolue un cercle très fermé et vénal de cybercriminels qui savent monnayer leurs logiciels d'attaque. La « plateformisation » qui transforme Internet concerne aussi la cybercriminalité.

Des cyber pirates venus du froid Les éditeurs de « rancongiciels » viennent surtout des pays de l'Est et de la Russie. Ils ont bénéficié d'un haut niveau de formation en

[1] Le cinéma d'Hollywood reflète l'évolution du profil du hacker. Inspiré de Kevin Mtinick, David Lightman dans Wargames (1983) incarne le hacker solitaire qui pénètre dans les ordinateurs des systèmes de lancement de missiles nucléaires.

mathématiques et en informatique, mais de faibles revenus les ont incités à rejoindre la cybercriminalité. Entre 30 ans et 40 ans, ils mènent une « double vie » entre des activités normales et des actes criminels. Les personnages les plus emblématiques sont les deux pirates informatiques russes du groupe Evil Corp, Maxime Yakubets et Igor Turashev.

- **Un recrutement sur le *dark***

Comme dans l'Internet « légal », ce petit monde fonctionne par petites annonces et forums spécialisés (sur le *dark net* s'entend) où se font les réputations professionnelles basées sur des opérations réussies. **Le darkweb a aussi son LinkedIn**. L'on vient valoriser ses compétences, présenter son expertise, flairer les bons « tuyaux » et surtout chercher des missions. Pour bien se mesurer, les poids lourds de la profession se « hackent » l'un contre l'autre en direct, ce qui permet de voir ce qu'ils sont capables de faire.

Le marché du travail se caractérise par un important ***turnover*** à l'instar du secteur numérique légal. Fidéliser un bon hacker n'est guère aisé, cela passe par la confiance mutuelle. Evoluant dans une galaxie mondiale, les « ingenieurs hackers » courent de job en job. Dans ce systeme méritocratique, il est possible d'avoir accès à des personnes référentes qui sauront faire le « go between » avec les bons employeurs.[2]

- **Face aux menaces, des « hackers éthiques » ? Comment les attirer ?**

Le monde des hackers n'est pas seulement peuplé de *black hat*, ces cybercriminels sans foi ni loi. Les white hat, sont ces "bons" hackers qui veulent agir pour le bien des entreprises. On y trouve du reste des « repentis » passés du bon côté de la loi. Les white hat viennent en aide aux entreprises soucieuses de leur sécurité en essayant de trouver une brèche potentielle dans leur système. Pour tester les systèmes de sécurité

[2] . Ce monde est bien décrit dans l'ouvrage Industry of anonimity- Inside the Business of Cybercrime Hardcover de Jonathan Hustard (Editions Oxford).

informatique, il leur arrive souvent de se constituer en « ennemis assaillants » sous la forme d'une *red team*. Pas étonnant que les Responsables Sécurité des Systèmes Informatiques (RSSI) s'arrachent à prix d'or ces « chasseurs de primes » voués à aller chasser les chasseurs dans les réseaux. Dans cet univers du « white net » circulent des informations et des échanges de bonnes pratiques entre universitaires, groupes privés et « gentils hackers ».

Ces hackers sont d'autant plus demandés qu'ils comblent une carence : le manque de tests réalisés dans les logiciels informatiques. Rien à voir avec l'industrie pharmaceutique où les tests entrent pour près de 70% dans le cout d'un médicament avant sa mise en marché…

Que font les Etats ?

Lorsque le hacker met en balance le coût et le risque, le calcul est vite fait. La répression est rarement au rendez-vous. Aux Etats-Unis, seuls 0,3% des cyber crimes font l'objet de condamnations. De nombreux Etats ont tendance à osciller entre la répression et l'instrumentalisation de ces « nouveaux guerriers ».

Dans les régimes où les Etats se montrent plus répressifs, ils ne disposent pas d'assez de moyens pour lutter efficacement. Contre la cybercriminalité crapuleuse passe encore. Face aux actions d'espionnage pointu et d'envergure, c'est généralement insuffisant. C'est particulièrement le cas des Etats-Unis qui excellent en cyber attaque mais se révèlent plus faibles en défense. La **National Security Agency** (NSA) équivalente de notre ANSSI (l'Autorité nationale en matière de sécurité et de défense des systèmes d'information) se révèle souvent impuissante.

- **Le hacking milieu concurrentiel ?**

Le monde cybercriminel évolue selon les caractéristiques d'une économie capitaliste théorisée par Adam Smith il y a 300 ans ! Le secteur du hacking s'est structuré :

kiosques, magasins, filières de distribution, stratégies marketing, offres et mise en concurrence. Le marché de la cybercriminalité fait penser à un « gros gâteau » capable de satisfaire tous les acteurs. C'est pourquoi nous n'assistons pas à un mouvement de concentration du secteur, mais plutôt à une coopération générale. Ni apparition de gros cartels, ni de « guerres de gang » pour le contrôle de ce juteux marché. Ce que l'on constate est la sophistication, la « plateformisation » et le développement du marché avec des distributeurs de mieux en mieux structurés.

Les entreprises du *dark net* sont généralement organisées en « business unit », avec des départements définis pour chaque activité liée au crime (ciblage sur les réseaux sociaux, emails de *phishing*, centre d'appels, infographie, cellule de recrutement).
Comme dans le reste de l'économie, la course à la spécialisation est importante. De nombreuses organisations cybercriminelles ont tendance à se concentrer sur une activité pour avoir un leadership. Lorsque les prix de programmes malveillants devenus trop communs baissent sur le marché, les cybercriminels doivent se diversifier et innover. Ils cherchent à se développer comme une entreprise. Il leur faut trouver leur place sur le marché et étudier les fonctionnement des entreprises ciblées afin d'exploiter leurs faiblesses.

❖

Les organisations cybercriminelles se structurent en suivant les mêmes modèles économiques que le monde des affaires. Business comme un autre, la cybercriminalité prospère d'autant mieux et vite que les entreprises cybercriminelles ont pris plus de l'ampleur et se mondialisent plus rapidement que les entreprises « légales ». Celles-ci doivent impérativement considérer que la sécurité est uniquement un centre de coût

si elles ne veulent pas se mettre en danger face à des assaillants toujours plus innovants.

LE CEPS REMERCIE LES PARTENAIRES DU CLUB ETAT D'ALERTE CYBERDEFENSE