Avatars et renseignement humain : un complément nécessaire à l'approche technique de lutte contre les cybercriminels

Valéry-Emmanuel Gosserez

Le visage de la cybercriminalité a considérablement changé en 20 ans, la guerre en Ukraine ayant eu pour effet de rendre plus prégnantes les rivalités au sein de la communauté internationale. Les approches humaines de renseignement montrent que les acteurs de la cybercriminalité se pérennisent. Seuls les noms et les pseudonymes changent.

Dans ce contexte éminemment hostile et mouvant, le renseignement a dû s'adapter, s'adapte encore. Plusieurs succès des autorités depuis mars 2022, rendus possibles par la combinaison synchronisée de moyens techniques de compromission d'infrastructures techniques et de renseignement humain virtuel et physique, ont abouti à l'arrestation d'administrateurs de forums et de membres de groupes de *ransomware,* le montrent. On le constate par cette récente actualité, il apparaît fondamental de développer encore davantage la capacité de recherche humaine dans l'espace cyber.

Mais commençons par un peu d'histoire.

I. L'écosystème des *ransomwares*[1] : origine et évolution

Les outils d'attaques évoluent au gré des technologies, les noms des groupes au gré de leur condamnation ou de leur inscription sur des listes de sanctions internationales. Pourtant les acteurs de base de la cybercriminalité liée au *ransomware* sont les mêmes depuis des années. En leur sein, les opérateurs russes occupent une position privilégiée. Ils ont progressivement fédéré d'autres talents, changé leur *business model* et leurs techniques d'attaque, et se sont internationalisés. Ils ont entraîné dans leur sillage une multitude de petits acteurs du microcosme.

(1) Attaque informatique qui bloque l'accès à l'appareil ou aux fichiers. Les pirates exigent alors le paiement d'une rançon en échange du rétablissement de l'accès. Rangonciel est l'équivalent français de ce mot anglais. Voir https://www.cybermalveillance.gouv.fr/ (note de la rédaction).

Ces opérateurs historiques sont des femmes et des hommes apparus au moment de l'effondrement de l'empire soviétique. Les groupes constitués alors ont su exploiter une multitude de compétences à l'abandon dans le domaine de l'informatique, et pu profiter de l'absence de législation cyber en Russie à l'époque. Les premières grandes cyberattaques criminelles datent ainsi des années 1990, impliquant des acteurs tels que Vladimir Levin, le père des hackers russes.

À partir des années 2000, et avec l'arrivée de Vladimir Poutine au pouvoir, l'État russe semble avoir fait le choix de laisser prospérer cette criminalité. Les autorités russes auraient-elles vu dans la pratique des *ransomwares* l'opportunité de recueillir du renseignement à des fins politiques ou économiques, et ce à moindre coût ? Il est raisonnable de se poser la question, la masse d'informations d'au moins une partie des groupes de *ransomware* étant probablement venue enrichir les bases de données des FSB, GRU et SVR. Il reste de même curieux de constater que certains groupes de *ransomware* continuent à attaquer des systèmes d'information de municipalités en France, sachant pourtant que ces dernières n'ont ni le budget ni la capacité (morale, bientôt légale) de répondre à la demande de rançon(2).

Les groupes de *ransomware* sont ainsi devenus de nouveaux acteurs du monde de l'intelligence stratégique. Ils ont fait évoluer de manière singulière le recueil d'informations, se mettant en capacité de satisfaire aux demandes de leurs clients d'une manière comparable à celle d'une agence de renseignement.

Mais l'évolution ne s'arrête pas là, comme nous allons le voir.

Ces dernières années, le rapport de force dans le monde des chercheurs de vulnérabilités a basculé en faveur de ceux qui travaillent pour les groupes de cybercriminels.

Des groupes tels que LunarSpider et MallardSpider - développeurs respectivement des maliciels IcedID et Qakbot - mettent ainsi à disposition leur technologie à une communauté toujours plus grande, qui ne se limite plus aux seuls groupes cybercriminels russes, mais à des groupes à travers le monde en Asie, en Amérique du Sud, au Moyen-Orient et en Afrique.(3)

(2) À cet égard, il convient de rester pragmatique : des services occidentaux exploitent désormais également toutes les nouvelles sources d'informations accessibles dans les couches d'Internet, fussent-elles issues de compromissions de cibles.

(3) Source : rapport annuel des menaces - 2022 - Crowdstrike. Crowstrike est une entreprise américaine de cybersécurité fondée en 2011 et basée à Sunnyvale en Californie.

On trouve désormais dans l'écosystème des *ransomwares* des groupes tels que TA550 et FIN7 qui historiquement menaient des campagnes de phishing[4] pour récupérer des données bancaires. Ils offrent leurs services à des groupes de *ransomware* tels que Revil. Ce type de groupes que l'on qualifiera de *primo-attaquants* a vu ses rangs augmenter de manière considérable, réunissant à la fois les anciens acteurs de la cybercriminalité russe, et tous les groupes à travers le monde ayant les compétences pour compromettre une cible et maintenir les accès. Parmi ces intervenants on retrouve une large variété de profils : des experts cyber, attirés par l'appât du gain, des anciens des services et finalement toute la galaxie de personnes constituant le « bug bounty » du Darkweb.

Parallèlement, les sites d'échange ou de vente de données fuitées se sont multipliés. Alors que les sites ouverts du Darkweb tels XSS ou Exploit.in ont réduit leur activité liée aux groupes de *ransomware* par crainte d'être pris pour cible par les autorités américaines, d'autres forums à accès restreint et connus de leurs seuls membres continuent la mise en vente d'accès à des systèmes d'information compromis à des prix qui oscillent entre quelques centaines et des centaines de milliers d'euros.

S'il est vrai que les cyberattaques nécessitent des moyens de plus en plus considérables (avec notamment l'envol du prix des 0 days), la cybercriminalité demeure un secteur extrêmement lucratif : l'évolution du cours du bitcoin depuis 2019 a permis aux groupes de *ransomware* d'augmenter à proportion les moyens financiers dédiés à la création de nouveaux outils de compromission et l'acquisition d'accès compromis.

On le voit, les cybercriminels sont de plus en plus efficaces, déterminés… et riches. Pour autant, ils ne sont pas exempts de vulnérabilités dans le cyberespace.

2. L'exploitation des fuites de données sur les cybercriminels

Maîtriser son empreinte cyber laissée dans toutes les couches d'Internet est une gageure, même pour les cybercriminels et les groupes d'APT (*Advanced Persistant Threat*). La récente actualité le démontre, entre les flux de données de profils sur le Darkweb et les empreintes techniques laissées par les attaques.

(4) Type d'escroquerie sur le Web visant à l'obtention d'informations généralement bancaires sous couvert d'une société de crédit ou autre (le Canada préfère « hameçonnage »). Ainsi la fausse banque vous demande de saisir vos identifiants, sous la menace de fermer votre compte si vous ne vous exécutez pas. Le SMS sert également d'appât : nous avons tous reçu celui concernant la carte vitale à remettre à jour, ou celui du faux site ANTS (Agence nationale des titres sécurisés) pour payer une contravention0 inexistante (note de la rédaction).

La Corée du Nord, la Chine et la Russie n'ont pas échappé à la divulgation dans le Darkweb d'informations relatives à des millions de leurs ressortissants, mettant à jour les liens entre ces pays et l'activité de certains groupes cybercriminels.

> De nombreux sites, notamment chinois et russes, ont fait l'objet d'attaques laissant fuiter des millions de données sur leurs usagers (sites de jeux en ligne, réseaux sociaux, sites de vente en ligne, sites de recrutement, sites de télécommunication ou d'administration, sites adultes, sites de réservation, etc.)

La coopération entre la Corée du Nord, la Chine et la Russie s'est ainsi rendue visible par la présence de centaines de profils à consonance coréenne positionnés en Chine et en Russie utilisant les réseaux sociaux et les plateformes des pays dans lesquels ils sont positionnés.

Donghui Park, chercheur en cybersécurité d'origine sud-coréenne, situe le nombre d'agents des unités cyber-offensives nord-coréennes ainsi implantés en Chine, dans une fourchette allant de six cents à mille individus, principalement avec un statut d'étudiant.

Concernant la Russie, des cyber-combattants ont été identifiés à Vladivostok, suite notamment à l'arrestation d'un membre de l'Armée Populaire de Corée du Nord qui tentait de fuir le régime.

Ainsi, et de manière globale, les données collectées dans le Darkweb participent à l'identification de profils nord-coréens, chinois et russes à travers la planète.

Les données techniques des cyberattaques constituent une autre vulnérabilité pour les cybercriminels.

> En dehors du reverse réalisé sur les malwares employés par les groupes d'APT permettant de constater l'échange ou le partage d'outils entre eux, les données techniques relatives aux IP utilisées pour les attaques permettent de montrer la connivence (active ou passive) des États dans la conduite des opérations.
>
> Ainsi, de l'étude des attaques réalisées par les groupes d'APT nord-coréens tels que Lazarus, Kimsuky, APT 37 et 38, deux types d'adresses IP provenant d'infrastructures de *command and control* ou de diffusion des maliciels se distinguent par les adresses IP appartenant, d'une part au rang alloué à la Corée du Nord, d'autre part à celles acquises de manière démarquée dans des pays tiers.

Les adresses IP des pays tiers proviennent de fournisseurs de service d'hébergement qui peuvent potentiellement être utilisées par différents groupes d'attaquants n'ayant pas forcément de liens entre eux. Les études sur les adresses IP montrent qu'elles peuvent être utilisées à différentes époques par différents acteurs malveillants sans rapport les uns avec les autres. La surveillance de ce type d'infrastructure ne peut certes pas véritablement permettre d'évaluer

le niveau de coopération de la Russie et de la Chine avec la Corée du Nord. Pour autant les recherches sur les adresses IP des attaques liées à la Corée du Nord, au vu de la spécificité de l'Internet en Corée du Nord, fournissent des informations sur le type de structures et de personnes qui se cachent derrière les attaques. Deux types de profils se font ainsi jour : ceux pouvant d'être directement impliqués du fait de leurs origines, et ceux qui appartiennent aux sociétés soutenant les infrastructures utilisées par les Nord-Coréens pour les besoins de leurs attaques.

Sur les plages d'adresses IP en lien avec les attaques, des profils russes, chinois et nigérians ont été identifiés, illustrant également la collaboration entre ces pays. De même, des dizaines de profils chinois et russes se sont connectés sur des adresses IP nord-coréennes, montrant leur présence sur le territoire.

Ainsi les cybercriminels ont eux aussi des vulnérabilités. Ils ont même perdu quelques manches dans le duel les opposant aux autorités internationales.

3. Trois succès récents des autorités avec compromissions techniques et probablement humaines

Les affaires RaidForums et BreachForums

Le forum de pirates informatiques RaidForums, utilisé par les cybercriminels pour acheter et vendre des bases de données volées, a été officiellement fermé en avril 2022 et ses domaines ont été saisis par les autorités américaines dans le cadre d'une opération Tourniquet coordonnée par Europol et à laquelle ont participé les services de police de nombreux pays : Europol, l'Agence nationale britannique de lutte contre la criminalité (NCA), le ministère américain de la Justice, ainsi que les autorités portugaises, suédoises et roumaines.

Avant la saisie du forum, des centaines de bases de données volées contenant plus de 10 milliards d'enregistrements individuels avaient été mises en vente.

Des accusations Américaines ont également été portées contre le fondateur et administrateur en chef portugais de RaidForums, Diogo Santos Coelho, mis en cause pour avoir géré le forum, et offert aux utilisateurs un système d'adhésion payant donnant accès à des salons de discussion qui permettaient l'échange de liens, de photographies et de données liées à la cybercriminalité.

Les semaines précédant la fermeture officielle de RaidForums, les utilisateurs avaient noté de nombreux dysfonctionnements sur le site, qui laissaient supposer une potentielle compromission par les autorités. De fait, ces dernières ont vraisemblablement pu utiliser des informations essentielles recueillies sur RaidForums dans le cadre des investigations menées à l'encontre de BreachForums. Il est en tout cas permis de le penser, si l'on en juge par le fait qu'une année a suffi aux forces de l'ordre américaines pour procéder

à l'arrestation de Conor Brian Fitzpatrick administrateur de BreachForums, le 15 mars 2023.

Lors de son arrestation, ce dernier aurait avoué qu'il utilisait le pseudonyme « Pompompurin » et qu'il était propriétaire administrateur du site.

À la suite de cette arrestation, un nouvel administrateur, connu sous le nom de « Baphomet », annonçait élaborer un plan de migration vers une nouvelle infrastructure. Soupçonnant une compromission du forum après avoir remarqué une connexion postérieure à l'arrestation de Fitzpatrick, Baphomet déclara cependant : « *Les serveurs que nous utilisons ne sont jamais partagés avec qui que ce soit d'autre, il faudrait donc que quelqu'un connaisse les informations d'identification de ce serveur pour pouvoir s'y connecter. J'ai maintenant l'impression d'être placé dans une position où rien ne peut être considéré comme sûr, qu'il s'agisse de nos configurations, de notre code source ou d'informations sur nos utilisateurs, la liste est sans fin. Cela signifie que je ne peux pas confirmer que le forum est sûr, ce qui a été un objectif majeur depuis le début de cette histoire* ».

Le site BreachForums a été fermé à la suite de cette déclaration.

Les deux fermetures des sites RaidForums et BreachForums ont permis aux autorités de recueillir des informations sensibles sur l'écosystème des cybercriminels. Dans les deux cas la compromission des serveurs a été possible car elle a cumulé des approches humaines virtuelles et physiques. À ce jour, si officiellement aucun site de substitution de BreachForums n'a été dévoilé, il a été déjà constaté que les forums sont remplacés par des canaux Telegram qui servent les mêmes objectifs illicites.

Le FBI à l'offensive contre Hive

Le FBI, en collaboration avec Europol et 13 autres organismes chargés de l'application de la loi, a secrètement infiltré l'infrastructure du gang du *ransomware* Hive en juillet 2022 en ayant agrégé des approches humaines virtuelles. Après six mois de surveillance de l'activité du gang, il a réussi, en janvier 2023, à démanteler ses sites de paiement et de fuites de données. L'opération a permis d'éviter le paiement d'une rançon estimée à 130 millions de dollars, le FBI ayant pu avertir les cibles de Hive avant qu'une attaque se produise, obtenant et remettant des clés de déchiffrement que le groupe utilisait pour déverrouiller les données des organisations victimes.

Europol face aux cerveaux de DoppelPaymer

DoppelPaymer a été très actif entre 2019 et 2021, mais a changé de nom pour devenir « Grief » en juillet 2021 afin d'échapper aux sanctions internationales ressortant de ses liens avec la Russie. Il aurait ciblé plus de 600 entreprises dans le monde, en particulier dans les secteurs de la santé, des services d'urgence et de l'éducation.

Le 6 mars 2023, Europol a annoncé l'arrestation de deux « cerveaux » du groupe ainsi que la saisie de dispositifs lors de raids simultanés menés par les polices allemande et ukrainienne. Les services de Police du Danemark et des États-Unis ont participé à l'opération coordonnée par Europol. La police allemande a également émis des mandats d'arrêt à l'encontre de trois ressortissants russes vivant dans le pays.

4. La recherche humaine virtuelle ou physique : de réels succès

On le constate par cette actualité récente, le renseignement humain demeure, malgré la technicité de cette nouvelle criminalité, un des facteurs clés du succès. L'évolution de l'environnement semble au reste favorable à cette approche complémentaire à ne surtout pas négliger.

Les acteurs liés à l'écosystème des *ransomwares* (brokers de 0days, brokers d'accès compromis, sociétés de *recovery*, affiliés, etc.) constituent de notables capteurs humains permettant d'anticiper la menace des ransomwares et surtout de compléter les données statistiques le plus souvent issues de seuls relevés techniques. De plus, on aurait tort de penser l'environnement des cybercriminels comme une masse opaque et stable. Le 5 août 2022, un affilié mécontent du groupe de *ransomware* Conti, avait publié des données compromettantes pour ce groupe, montrant qu'au-delà des aspects purement techniques, ces groupes malveillants présentent des fragilités propres à toute organisation humaine.

À ce jour, des acteurs de la cyber sécurité et même des services de renseignements au niveau des États ont une connaissance assez fine des *modus operandi* des criminels et de leur biotope pour les intégrer dans leur approche. La connaissance de ces nouveaux « métiers » et des hommes qui les exercent a pu augmenter grandement la capacité d'anticipation des attaques permettant d'identifier dans tous les maillons de la chaîne des *ransomwares* celui qui est le plus faible, non pas d'un point de vue technique, mais en termes de fidélité à l'écosystème.

Par ailleurs, depuis quelque temps un rallongement de la phase d'attaque est constaté, dû à l'implication d'acteurs extérieurs aux groupes de *ransomware* (tels les affiliés primo-attaquants en charge de la compromission initiale du SI visé). Le délai entre le début de l'attaque et le chiffrement des données s'est allongé de manière significative passant de quelques jours à quelques semaines. Pire, la multiplication des cibles offertes par les primo-attaquants aux groupes de *ransomware* qui ne sont pas en mesure de tout traiter simultanément ont allongé le temps durant lequel les cybercriminels sont à l'intérieur du SI. Ce rallongement relatif de la durée de l'intrusion pourrait être exploité utilement par les possibles cibles car il augmente d'autant les chances de dépistage, d'anticipation, et de désamorçage éventuels.

En conclusion, en marge d'une approche purement technique de compromissions des serveurs des cybercriminels, il semble désormais évident que la captation de renseignements humains permet de mieux réagir. La création d'un avatar pour pénétrer une communauté et recueillir de l'information sur l'écosystème se définit comme du renseignement humain virtuel. L'efficacité de l'accès à l'information devra passer par l'accélération des opérations de recherches humaines virtuelles et techniques dont l'héritage des savoir-faire provient *in fine* du renseignement humain et non des approches purement techniques ou reposant uniquement sur l'exploitation des sources ouvertes.

Au niveau des États, avantage sera forcément donné à ceux qui auront misé sur la combinaison de cette complémentarité du renseignement, humain, physique et virtuel, et du renseignement technique.

Valéry-Emmanuel Gosserez
Président du COREXALYS