TLP:CLEAR

ÉTAT DE LA MENACE INFORMATIQUE CONTRE LES CABINETS D'AVOCATS

27 juin 2023

Sommaire

Synthèse

Les avocats et cabinets d'avocats sont régulièrement la cible d'attaques informatiques conduites par des acteurs aux origines, aux compétences et aux objectifs divers. L'exposition des cabinets d'avocats à la menace informatique s'explique notamment par leur accès à des données sensibles, mais aussi parce qu'ils traitent avec des clients que des attaquants pourraient chercher à atteindre.

L'ANSSI constate que la surface d'attaque des cabinets d'avocats ne cesse de s'étendre, notamment du fait de la numérisation croissante de la profession et des procédures judiciaires. Or, les attaques informatiques peuvent avoir de graves conséquences en matière financière, opérationnelle et réputationnelle. En dépit de ces menaces, le niveau de sécurité informatique des cabinets d'avocats français demeure hétérogène (voir Section 1).

L'objectif de ce document est de présenter les principales menaces pesant sur les systèmes d'information (SI) des cabinets d'avocats et de fournir des exemples concrets d'attaques conduites contre le secteur en France ou à l'étranger. Dans une dernière partie, l'ANSSI propose une liste de recommandations orientée sur les enjeux de confidentialité et de protection des données sensibles (voir Section 5).

L'ANSSI distingue généralement trois grands types de menace informatique : les attaques à but lucratif, l'espionnage et les opérations de déstabilisation. Aujourd'hui, les attaques à finalité lucrative représentent la principale menace observée pour les cabinets d'avocats en nombre d'attaques. Elles sont majoritairement conduites par des groupes cybercriminels cherchant à extorquer des fonds à leurs victimes ou à commettre des délits d'initié (voir Section 2).

Les cabinets d'avocats sont également des cibles de choix pour des acteurs souhaitant surveiller les activités des avocats ou de leurs clients. Si les exemples traités dans ce document confirment la persistance des attaques conduites par des acteurs présumés liés à des États, l'ANSSI note une augmentation des attaques conduites par l'intermédiaire d'entreprises privées (voir Section 3).

Enfin, plusieurs cabinets d'avocats ont déjà été victimes d'opérations de déstabilisation conduites par des groupes d'hacktivistes ou par des acteurs réputés liés à des États. Leur mode opératoire consiste à rendre publics des documents internes jugés compromettants pour décrédibiliser des cabinets d'avocats ou leurs clients, voire à saboter leurs systèmes d'information (voir Section 4).

1. Contexte

Les avocats et cabinets d'avocats sont régulièrement la cible d'attaques informatiques conduites par des acteurs aux origines et objectifs divers. Ce ciblage peut s'expliquer par trois principaux facteurs :

1. leur accès à des données sensibles concernant leurs clients et des procédures judiciaires, que des attaquants pourraient chercher à dérober ;
2. leurs échanges potentiels avec les véritables cibles des attaquants, qui pourraient compromettre un cabinet pour atteindre des personnes ou organisations jugées d'intérêt parmi leurs clients ;
3. leurs recettes financières, que des attaquants pourraient tenter d'extorquer.

Face à ces menaces, le niveau de sécurité informatique des cabinets d'avocats français demeure hétérogène. Si d'importants cabinets ont aujourd'hui mis en place une politique de sécurité des systèmes d'information (PSSI), la majorité des avocats, qui pratiquent en petite structure, ne dispose pas de responsable de la sécurité des systèmes d'information (RSSI) et ne sont pas assez sensibilisés à cette menace.

En parallèle, la surface d'attaque des cabinets d'avocats ne cesse de s'étendre, offrant un nombre toujours plus important de points d'entrée aux attaquants pour s'introduire et se maintenir sur les réseaux ciblés. Cette tendance est notamment le résultat :

- de la numérisation croissante des procédures judiciaires ;
- des interconnexions entre les réseaux des cabinets et ceux de prestataires extérieurs ;
- du manque de cloisonnement entre les équipements utilisés dans le cadre personnel et professionnel ;
- du recours croissant au télétravail ;
- de l'existence de mauvaises pratiques [1].

Il convient en outre de rappeler que la généralisation du *cloud computing* a introduit de nouvelles menaces pour les données hébergées par les cabinets d'avocats. La nature du *cloud* rend en effet complexe la localisation précise du stockage des données, dont la confidentialité peut notamment être menacée par l'extraterritorialité de certaines législations [2].

Les attaques informatiques peuvent avoir de graves conséquences sur les cabinets d'avocats en matière financière, opérationnelle et surtout réputationnelle. La fuite de données à caractère personnel peut également porter atteinte au secret professionnel et engager la responsabilité des avocats au regard de la loi Informatique et Libertés et du Règlement général sur la protection des données (RGPD) européen [1].

Ce document détaille les principales menaces pesant sur les systèmes d'information (SI) des cabinets d'avocats, en fournissant des exemples concrets d'attaques conduites contre le secteur, en France comme à l'étranger. Il consacre une section à chacun des trois grands types de menace informatique identifiés : les attaques à but lucratif, l'espionnage informatique et les opérations de déstabilisation.

Dans une dernière partie, l'ANSSI propose une liste de recommandations destinée à se prémunir contre ces menaces. Ces recommandations sont centrées sur les enjeux de confidentialité et de protection des données sensibles créées, hébergées et traitées par les cabinets d'avocats. Elles sont destinées aux directeurs des systèmes d'information (DSI) et aux RSSI, mais s'adressent aussi aux prestataires et aux décideurs des cabinets d'avocats.

1. À l'exemple de la numérisation des clés personnelles du réseau privé virtuel des avocats (RPVA), qui pourrait faciliter l'accès d'attaquants à des données sensibles.
2. Notamment le *Cloud Act* et le *Foreign Intelligence Surveillance Act* (FISA) américains.

2. Attaques à finalité lucrative

Les cabinets d'avocats représentent des cibles de choix pour les acteurs malveillants conduisant des attaques à but lucratif. Ils disposent en effet de données sensibles pouvant être revendues en ligne ou permettre, dans le cadre d'attaques par rançongiciel, d'accentuer la pression pour que la victime verse une rançon. Depuis le milieu des années 2010, certains attaquants se sont même spécialisés dans la compromission de cabinets d'avocats pour dérober des informations permettant de commettre des délits d'initié.

Les attaques à finalité lucrative, qui représentent aujourd'hui la principale menace observée pour les cabinets d'avocats en nombre d'attaques, sont majoritairement le fait d'acteurs cybercriminels. L'ANSSI note toutefois que des attaques à finalité lucrative sont également conduites contre le secteur par des groupes d'attaquants réputés liés à des États.

2.1. Spécialisation & professionnalisation des acteurs cybercriminels

2.1.1. Ciblage par rançongiciel

Depuis 2017, l'ANSSI constate une forte augmentation du nombre d'incidents impliquant l'utilisation de rançongiciels [3]. Ce mode d'action est de plus en plus associé à l'exfiltration de données que les cybercriminels menacent de rendre publiques en cas de refus de paiement de la rançon demandée. Cette technique dite de « double extorsion » permet d'accentuer la pression sur la victime pour augmenter les chances d'obtenir un paiement.

Le paiement d'une rançon n'assure cependant pas le déchiffrement des données. En 2016, un cabinet d'avocats américain a subi une attaque par rançongiciel qui a paralysé l'ensemble de ses documents de travail pendant au moins trois mois. Les outils de déchiffrement envoyés par les attaquants après le paiement de la rançon se seraient révélés inexploitables, conduisant la victime à reprendre contact avec les attaquants, qui ont alors demandé à percevoir une rançon plus importante. Le cabinet a estimé ses pertes totales à 700 000 dollars américains [2].

Les cabinets d'avocats sont également victimes d'attaques opportunistes et indirectes permises par la compromission de leurs prestataires de services numériques, attaques dites par « chaîne d'approvisionnement » (*supply chain*). À titre d'exemple, le groupe cybercriminel Everest aurait exfiltré les données et chiffré les SI d'au moins sept cabinets d'avocats français suite à la compromission de leur prestataire de services d'infogérance [3]. Les données de certains de ces cabinets ont ensuite été publiées sur le site d'Everest. Parmi les victimes figurait un cabinet spécialisé en réparation des dommages corporels ayant représenté des parties civiles aux procès de l'attentat contre Charlie Hebdo et de l'assassinat de Samuel Paty. Des éléments des dossiers d'instruction ont donc été rendus publics, dont des procès-verbaux d'auditions, des rapports d'autopsies, des comptes-rendus d'écoutes téléphoniques, la photo d'une des scènes de crime, et des données à caractère personnel relatives à des enquêteurs et des magistrats [4, 5].

Début 2022, les opérateurs du rançongiciel Lockbit 2.0 ont annoncé la publication de documents appartenant au ministère français de la Justice. Il s'agissait de documents dérobés sur les systèmes d'information d'un cabinet d'avocats français dont le SI avait été chiffré. Les données révélées par les attaquants contenaient des contrats de travail des employés du cabinet, des photos d'identité, ainsi qu'un fichier texte dans lequel étaient stockés des identifiants et mots de passe. Ces données, non chiffrées, auraient théoriquement pu permettre aux attaquants d'accéder à un compte bancaire et au réseau privé virtuel des avocats (RPVA) [6].

Commentaire : ces exemples témoignent de la fréquence et des impacts importants des attaques par rançongiciels, parfois facilitées par l'exploitation de vulnérabilités non corrigées, les interdépendances avec les réseaux de prestataires extérieurs et de mauvaises pratiques, à l'exemple du stockage de mots de passe en clair. Depuis 2017, l'ANSSI a constaté la compromission d'une douzaine de cabinets d'avocats français au moyen de rançongiciels, dont la majorité par Lockbit 2.0. Ces chiffres sont très probablement sous-évalués, puisque les cabinets d'avocats ne font pas partie des opérateurs d'importance vitale (OIV) ni des opérateurs de services essentiels (OSE).

3. Codes malveillants déployés par des acteurs cybercriminels pour chiffrer les données d'un système d'information. Les attaquants contactent ensuite les victimes pour leur demander une rançon en échange de la clé de déchiffrement.

2.1.2. Fraudes & reventes de données

Au-delà de l'utilisation de rançongiciels, les cybercriminels tentent également de monétiser la compromission de cabinets d'avocats en détournant directement leurs comptes bancaires ou en exfiltrant les données de leurs systèmes d'information afin de les exploiter ou de les revendre sur des forums spécialisés.

À titre d'exemple, le groupe cybercriminel russophone FIN7 s'est spécialisé depuis le milieu des années 2010 dans l'exfiltration de données à caractère personnel, bancaires et sensibles des réseaux de ses victimes, parmi lesquelles figurent des cabinets d'avocats. En 2021, le groupe aurait conduit une campagne d'hameçonnage [4] contre un cabinet d'avocats américain en se faisant passer pour une organisation souhaitant porter plainte contre une entreprise de vins et spiritueux [7]. Si l'objectif des attaquants n'a pas été révélé, FIN7 est connu pour revendre une partie des données dérobées sur des plateformes cybercriminelles en ligne [8].

En parallèle, certains groupes cybercriminels se sont spécialisés dans la récupération de documents commerciaux sensibles dont les informations permettre de commettre des délits d'initié. Entre 2013 et 2014, le groupe FIN4 aurait conduit des campagnes d'hameçonnage contre plus d'une centaine d'entreprises dans le but d'obtenir des informations pouvant influencer le cours de bourse d'entreprises une fois rendues publiques : fusions-acquisitions, produits en cours de développement, difficultés financières ou juridiques, etc. Si l'industrie pharmaceutique et médicale représentait plus de 60% des cibles, plusieurs cabinets d'avocats auraient été compromis [9].

En décembre 2016, le département américain de la Justice a annoncé l'arrestation à Hong Kong de trois habitants de Macao accusés d'avoir ciblé au moins sept cabinets d'avocats américains. Les attaquants auraient réussi à exfiltrer des informations sensibles des réseaux de deux cabinets engagés dans d'importantes opérations de fusion-acquisition. L'achat d'actions avant l'annonce publique de ces acquisitions, puis leur revente après officialisation, auraient permis aux attaquants de générer un profit de 4 000 000 de dollars américains [10].

Enfin, le groupe cybercriminel russophone GozNym [11] est accusé d'avoir compromis, jusqu'en 2019, plusieurs dizaines de milliers d'ordinateurs pour en exfiltrer des identifiants de comptes bancaires. Au moins deux cabinets d'avocats américains auraient été victimes du groupe [12]. Les attaquants auraient réussi, de manière opportuniste, à prendre le contrôle des comptes bancaires des cabinets, puis à effectuer des virements frauduleux de 76 000 et 41 000 dollars américains vers des comptes sous leur contrôle [13].

2.2. Émergence d'attaques opportunistes conduites par des acteurs présumés étatiques

Depuis au moins 2020, l'ANSSI constate l'émergence d'attaques par rançongiciels conduites par des groupes d'attaquants présumés liés à des gouvernements. Elles seraient notamment le fait de groupes d'attaquants ciblant des entités étrangères à des fins de déstabilisation (cf. *infra*, section 4.2, p. 10). Dans de rares cas, ces groupes auraient cherché à monétiser la compromission d'entités ne représentant pas d'intérêt particulier pour leurs objectifs, dont des cabinets d'avocats.

En septembre 2022, le département américain de la Justice a ainsi sanctionné trois membres présumés du groupe d'attaquants Nemesis Kitten [5] pour des attaques par rançongiciel contre des entités américaines, britanniques, israéliennes et iraniennes. Parmi les victimes figurait notamment le barreau d'un État américain [14]. D'après les autorités américaines, qui attribuent publiquement Nemesis Kitten au Corps des Gardiens de la Révolution iranien [15], il est probable que les opérateurs du groupe d'attaquants aient extorqué certaines de leurs victimes pour leur profit personnel.

Commentaire : en l'état, l'ANSSI considère que les attaques à finalité lucrative conduites par des acteurs présumés étatiques restent marginales. Des exemples récents démontrent toutefois que des cabinets d'avocats français pourraient être la cible d'opérations opportunistes conduites par ce type d'acteur.

4. Technique qui consiste à envoyer un courriel invitant la cible à ouvrir une pièce jointe ou à cliquer sur un lien malveillant.
5. Aussi connu sous le nom de Cobalt Mirage, UNC2448 ou DEV-0270.

3. Espionnage informatique

Les données sensibles manipulées par les cabinets d'avocats en font également des cibles de choix pour des attaquants cherchant à surveiller les activités d'avocats ou de leurs clients. Depuis au moins la fin des années 2000, des acteurs présumés étatiques ont compromis des cabinets dans le but de collecter des informations utiles à des missions d'espionnage économique ou stratégique. Ce type d'acteur s'intéresse particulièrement aux brevets, aux dossiers de fusion-acquisition, aux procédures judiciaires ou d'arbitrage, ou encore à l'application de sanctions et d'embargos internationaux.

L'ANSSI note par ailleurs une augmentation du nombre d'attaques conduites contre le secteur par des entreprises privées et des mercenaires possédant des capacités de lutte informatique offensive. Ces organisations, dotées pour certaines de compétences avancées, proposent leurs services à de nombreux États à travers le monde, mais également à des particuliers. Depuis le milieu des années 2010, dans le cadre de conflits familiaux ou commerciaux, plusieurs cabinets d'avocats ont ainsi été la cible d'attaquants recrutés par des enquêteurs privés, des entrepreneurs ou des personnalités politiques pour surveiller la partie adverse.

3.1. Persistance des attaques conduites par des acteurs présumés liés à des gouvernements

3.1.1. Espionnage économique

Depuis au moins le milieu des années 2000, des groupes d'attaquants présumés étatiques se sont spécialisés dans la compromission d'entreprises étrangères afin de collecter des informations commerciales. Leur principal objectif serait d'offrir un avantage compétitif aux entreprises de leur pays d'origine en surveillant les activités de leurs concurrents ou en dérobant de la propriété intellectuelle dans des secteurs considérés comme stratégiques.

Le groupe d'attaquants APT19[6], qui cible depuis 2013 de nombreux secteurs (énergie, santé, aérospatial, etc.), a ainsi conduit des campagnes visant spécifiquement des cabinets d'avocats. Entre 2016 et 2017, le groupe a tenté de compromettre près d'une dizaine de cabinets internationaux [16], notamment situés en Australie et aux États-Unis [17, 18, 19]. Certains messages d'hameçonnage faisaient également référence aux élections présidentielles françaises de 2017. D'après plusieurs sources publiques, les opérateurs du groupe APT19 seraient liés au gouvernement chinois [16].

D'autres groupes d'attaquants se concentrent sur le vol de technologies des clients des cabinets d'avocats. En 2017, le groupe APT10[7] aurait compromis un cabinet américain spécialisé en droit de la propriété intellectuelle[8]. Le cabinet conseillait par ailleurs des entreprises chinoises préparant leur entrée sur le marché américain. Les attaquants se seraient introduits dans les systèmes d'information en utilisant des identifiants probablement dérobés durant de précédentes attaques, puis auraient exfiltré de grandes quantités de données *via* le service de partage de fichiers Dropbox [20]. Le groupe APT10 est accusé publiquement d'opérer pour le compte du ministère chinois de la Sécurité d'État (MSE) par l'Australie, le Canada, les États-Unis, la Nouvelle-Zélande et le Royaume-Uni [21, 22, 23].

3.1.2. Espionnage stratégique

Outre l'espionnage économique, des acteurs présumés liés à des États sont accusés de conduire des attaques contre des cabinets d'avocats pour collecter des informations stratégiques sur leurs clients. De telles attaques ont notamment été observées lors de contentieux internationaux ou au cours de campagnes d'ampleur dirigées contre des secteurs sensibles de pays européens ou nord-américains.

6. Aussi connu sous le nom de C0d0s0, Codoso Team, Deep Panda ou Sunshop Group.
7. Aussi connu sous le nom de Stone Panda, Menupass Team, Potassium ou Red Apollo.
8. Les clients du cabinet étaient notamment issus du secteur de la santé, de l'électronique et de l'automobile.

En 2015, le groupe d'attaquants APT40 [9], lié en source ouverte au MSE chinois, aurait compromis plusieurs organisations impliquées dans des conflits territoriaux entre le gouvernement chinois et ses voisins en mer de Chine méridionale. Parmi les victimes figureraient le département philippin de la Justice, des membres de la Coopération économique pour l'Asie-Pacifique (APEC) et un cabinet d'avocats représentant l'une des parties devant la Cour permanente d'arbitrage (CPA) de La Haye [24]. Durant la même période, des attaquants présumés chinois auraient compromis le site de la CPA [10] pour piéger le site Web. Cette attaque dite par « point d'eau » leur permettait théoriquement de compromettre les équipements des visiteurs du site pour les surveiller [25, 26].

Ce type d'acteur mène par ailleurs des opérations d'ampleur pouvant affecter les cabinets d'avocats. En 2021, les autorités américaines et britanniques ont attribué au groupe d'attaquants APT28 [11] une vaste campagne d'attaques par force brute [12] contre des centaines d'organisations aux États-Unis et en Europe, dont des médias, des entités militaires, des entreprises du secteur de l'énergie, des *think tanks* et des cabinets d'avocats [27]. Ces attaques débutées mi-2019 auraient cherché à exfiltrer des informations stratégiques, sensibles ou personnelles du système d'information des victimes. En 2020, l'Union européenne avait attribué publiquement le groupe APT28 à une unité du renseignement militaire russe (GRU) [28].

Commentaire : ces exemples suggèrent que si la menace informatique augmente généralement lors de tensions internationales, plusieurs facteurs amplifient encore la menace d'attaques à des fins d'espionnage. Les cabinets disposant de filiales à l'étranger, traitant avec des entreprises étrangères, ou engagés dans des litiges impliquant des organisations de gouvernements conduisant des attaques informatiques sont considérées comme particulièrement exposés.

3.1.3. Ciblage par l'intermédiaire d'entreprises privées

Depuis au moins 2010, des gouvernements s'appuient par ailleurs sur des prestataires privés pour surveiller les activités de cabinets d'avocats. La sous-traitance de ces missions permet à certains États de combler leur manque de compétences en matière de lutte informatique offensive, mais aussi de rendre plus difficile l'attribution de ces attaques. Plusieurs de ces entreprises ont acquis des compétences très avancées, à l'image des vulnérabilités « zéro-clic » [13] développées par l'entreprise israélienne NSO Group [29].

L'utilisation de ces capacités pour espionner les communications d'opposants politiques, d'organisations de défense des droits de l'Homme, de journalistes et d'avocats est abondamment documentée. Des gouvernements sont ainsi soupçonnés d'avoir employé des codes malveillants développés par les entreprises israéliennes NSO Group et Candiru pour cibler des avocats sur leur propre territoire [30, 31].

De telles attaques ciblent également des avocats situés hors du pays du commanditaire. Entre 2010 et 2012, l'entreprise allemande FinFisher aurait permis au gouvernement du Bahreïn de compromettre les équipements de 77 opposants et avocats, dont certains avaient émigré aux États-Unis ou au Royaume-Uni. Les attaquants se seraient notamment servi des données exfiltrées de l'ordinateur d'un de ces avocats pour l'intimider [32]. En 2021, l'*Organized Crime and Corruption Reporting Project* a révélé qu'au moins seize avocats avaient été la cible du code malveillant Pegasus développé et vendu par NSO Group. Parmi eux figure un avocat français potentiellement ciblé par l'État marocain suite à son expulsion du pays en 2016 [33].

Depuis 2020, des organisations soupçonnées de travailler pour le gouvernement qatari ont été accusées d'avoir recruté une entreprise indienne, WhiteInt, pour conduire des attaques contre des personnalités critiquant l'organisation de la Coupe du monde de football 2022 au Qatar. L'une de leurs cibles serait un avocat américano-hongrois ayant déposé une plainte contre la famille royale du Qatar auprès du Conseil des droits de l'Homme de l'ONU. L'avocat britannique d'un homme d'affaires israélien aurait également été ciblé après la publication de rapports sur des affaires de corruption liées à la construction des stades dédiés à la Coupe du monde [34].

Commentaire : le recours croissant d'États à des entreprises privées développant des capacités de lutte informatique offensive concourt à la hausse du niveau de menace. Les révélations sur les outils de NSO Group n'ont pas infléchi

9. Aussi connu sous le nom de Leviathan, Temp.Periscope, Temp.Jumper, Gadolinium, Bronze Mohawk, Nanhaishu ou Kryptonite Panda.
10. Pour ce faire, les attaquants ont exploité une vulnérabilité Adobe Flash Player révélée seulement 72 heures auparavant (CVE-2015-5119).
11. Aussi connu sous le nom de Fancy Bear, Pawn Storm, Sofacy, Sednit ou Strontium.
12. Également appelée *bruteforce*, cette technique consiste à découvrir un identifiant et/ou un mot de passe en tentant de multiples combinaisons. Des outils et dictionnaires disponibles en source ouverte permettent d'accélérer l'attaque en automatisant les tentatives.
13. Ou « *zero-click* ». Ces vulnérabilités permettent aux attaquants de compromettre à distance un appareil sans aucune interaction de la victime, contrairement, par exemple, à l'envoi d'un courriel d'hameçonnage contenant un lien ou une pièce jointe malveillante.

cette tendance et le marché de la surveillance individuelle semble au contraire se recomposer. De nouveaux outils privés pourraient être employés à l'avenir pour cibler des avocats en France.

3.2. Un emploi croissant de capacités offensives par des acteurs privés

Ce recours à des entreprises privées ou à des mercenaires est également le fait d'acteurs privés souhaitant surveiller des avocats et/ou leurs clients, la plupart du temps lors de litiges commerciaux ou familiaux. À titre d'exemple, la Cour suprême du Royaume-Uni a conclu en octobre 2021 que Mohammed ben Rachid Al Maktoum, émir de Dubaï, vice-président, Premier ministre et ministre de la Défense des Émirats arabes unis, avait commandité la compromission des équipements de son ex-épouse, la princesse Haya bint al-Hussein ainsi que de son avocate britannique et membre de la Chambre des Lords, Fiona Shackleton, lors d'une procédure de divorce. La campagne aurait ciblé six téléphones mobiles au moyen du code malveillant Pegasus, développé par l'entreprise israélienne NSO Group [35].

En mai 2022, l'enquêteur privé israélien Aviram Azari a été arrêté aux États-Unis pour avoir commandé à une entreprise privée indienne, BellTrox , la compromission d'entités liées à des procédures judiciaires de nature commercial en cours. Ces campagnes auraient été conduites pour le compte de clients d'Aviram Azari, parmi lesquels l'oligarque russe Oleg Deripaska, impliqué dans un différend commercial en Autriche [36]. Au total, BellTrox serait responsable du ciblage de plus de 1 000 avocats issus de 108 cabinets à travers le monde entre 2013 et 2020, dont au moins un cabinet français [14]. Les documents exfiltrés par les attaquants étaient parfois publiés en ligne pour porter préjudice à la partie adverse [37].

En parallèle de ces entreprises établies, des groupes de mercenaires, communément appelés *hackers-for-hire*, commercialisent en ligne leurs compétences en lutte informatique offensive. Actif depuis au moins 2013, le groupe d'attaquants EvilNum [15] serait constitué d'opérateurs recrutés pour cibler des organisations à travers le monde. Initialement dirigé contre le secteur de la finance, le groupe a ciblé depuis 2019 des cabinets d'avocats localisés dans plus d'une dizaine de pays, dont la Suisse, le Royaume-Uni, Israël, Chypre, la Turquie, la Chine et les Émirats arabes unis [38].

D'autres mercenaires mettent directement en avant leurs services sur des plateformes en ligne. Void Balaur [16], un groupe russophone, propose ainsi de conduire différents types d'attaque (DDoS, *spam*) ou de compromettre une large gamme de messageries et de réseaux sociaux pour quelques centaines d'euros. À titre d'exemple, la compromission d'un compte de messagerie GMail était vendue environ 450 euros en mars 2021. Le groupe d'attaquants aurait ciblé des organisations localisées dans plus d'une quarantaine de pays, dont des cabinets d'avocats [39].

Commentaire : la commercialisation de services offensifs à des acteurs privés augmente significativement le niveau de menace informatique contre les avocats. Ces entreprises et mercenaires permettent en effet à un large public d'acteurs malveillants (concurrents, parties adverses ou détracteurs) d'accéder à des capacités offensives, parfois pour une somme modique. Le recours à ce type d'intermédiaire complexifie encore l'attribution, en masquant le commanditaire de l'attaque et ses objectifs.

14. D'après Reuters, BellTrox aurait ciblé plus de 80 adresses de messagerie électronique différentes appartenant au cabinet.
15. Aussi connu sous le nom de DeathStalker, Deceptikons ou TA4563.
16. Aussi connu sous le nom de Rockethack.

4. Déstabilisation

Les cabinets d'avocats ont déjà été la cible d'attaques opportunistes ou ciblées ayant eu pour conséquence de déstabiliser leurs activités ou visant directement à intimider leurs clients. Ces opérations consistent essentiellement en la divulgation d'informations exfiltrées que les attaquants jugent compromettantes pour les cabinets et/ou leurs clients ou à rendre indisponibles leur système d'information en chiffrant leurs données.

Ce type d'attaque est notamment le fait de groupes hacktivistes [17] cherchant à dénoncer les pratiques de certains cabinets ou leur soutien à des gouvernements étrangers, par exemple dans le contexte de tensions internationales. Néanmoins, des acteurs présumés étatiques emploieraient également ce mode d'action en représailles à des politiques jugées agressives ou pour décrédibiliser des dissidents réfugiés à l'étranger.

4.1. Divulgation d'information par des groupes hacktivistes

Depuis au moins le début des années 2010, plusieurs cabinets ont été la cible d'attaques informatiques, puis de la publication des données exfiltrées ou leur transmission à des médias. À titre d'exemple, des attaquants liés à la mouvance Anonymous ont compromis en 2012 le cabinet d'avocats représentant un militaire américain accusé du meurtre de civils irakiens à Haditha, en 2005. Les attaquants ont rendu publics 3 Go de documents internes du cabinet, et défiguré [18] le site de l'entreprise en publiant un manifeste critiquant le jugement rendu par la Cour martiale, considéré trop indulgent [40, 41].

Les cabinets d'avocats sont également ciblés par des attaquants les soupçonnant de malversations. Les affaires liées aux Panama Papers et aux Paradise Papers, publiées respectivement en 2016 et en 2017, ont pris potentiellement appui sur la compromission des systèmes d'information [19] d'avocats par des hacktivistes non identifiés [43, 44]. Les attaques, dirigées contre les cabinets d'avocats panaméen Mossack Fonseca et bermudien Appleby, avaient permis de dérober et d'analyser plusieurs dizaines de millions de documents détaillant leur fonctionnement, leurs pratiques et leurs clients.

Plus récemment, des cabinets d'avocats ont été ciblés pour leur proximité supposée avec le gouvernement russe. En juin 2022, le site DDoSecrets [20] a mis en ligne 1 To de données issues de la compromission d'un cabinet d'avocats moscovite par des membres de la mouvance Anonymous. L'opération s'inscrivait dans une campagne plus large (#OpRussia) de ciblage des intérêts russes par des hacktivistes pro-Ukrainiens suite à l'invasion du pays par la Russie, le 24 février 2022. Les documents fuités comprendraient des informations sensibles sur des entreprises russes, mais aussi américaines et européennes [45].

Commentaire : ces exemples démontrent que des acteurs indépendants et disposant de capacités limitées peuvent avoir un véritable impact négatif sur l'activité et la réputation des cabinets d'avocats. Si la dénonciation de malversations présumées reste la motivation principale de ce type d'attaquants, certains acteurs pourraient tenter de compromettre ou de divulguer des informations sensibles de cabinets d'avocats français de manière opportuniste, notamment en lien avec l'actualité ou des tensions internationales.

4.2. Campagnes conduites par des acteurs présumés étatiques

Depuis au moins le milieu des années 2010, des actions de déstabilisation seraient également conduites contre des cabinets d'avocats par des attaquants présumés liés à des gouvernements. Leur but est de perturber des secteurs-clés

17. Groupes plus ou moins organisés promouvant un discours politique ou idéologique au moyen d'attaques informatiques.
18. Technique consistant à modifier le contenu d'un site compromis et généralement employée pour revendiquer l'attaque.
19. Si certains commentateurs suggèrent que les fuites proviennent d'une ou plusieurs personnes qui possédaient un accès légitime à ces documents et souhaitaient porter atteinte à l'institution, des chercheurs en cybersécurité ont relevé de nombreuses vulnérabilités sur les sites et les services Internet des deux cabinets. Ces failles et/ou la compromission de leur messagerie électronique pourraient avoir permis l'intrusion initiale des attaquants sur leurs systèmes d'information [42].
20. De son nom complet, « Distributed Denial of Secrets ». Il a été fondé en 2018 et se présente comme une plateforme de « lanceurs d'alertes ».

de l'économie, ou d'atteindre la réputation de personnalités et d'opposants réfugiés dans des pays étrangers.

En juin 2017, le code malveillant NotPetya a été utilisé pour compromettre les SI de centaines d'entreprises et d'entités gouvernementales à travers le monde, dont des cabinets d'avocats. Ce faux rançongiciel, qui s'était propagé à partir d'une mise à jour vérolée du logiciel de comptabilité d'une entreprise ukrainienne [46], a notamment chiffré de manière irréversible les systèmes d'information du cabinet d'avocats britannique DLA Piper [47]. Les travaux de remédiation auraient coûté 15 000 heures de travail supplémentaires au cabinet [48]. En 2020, l'Union européenne a attribué l'attaque à une unité du renseignement militaire russe (GRU) [28] qui conduirait le groupe d'attaquants Sandworm [21].

Les tensions internationales favorisent largement ces actions opportunistes et indiscriminées contre des entités étrangères. Depuis 2020, Israël subit un nombre important d'attaques visant à chiffrer les systèmes d'informations d'entités gouvernementales et d'entreprises, puis à divulguer et/ou à saboter leurs données [49]. Cette vague d'attaques aurait notamment touché un cabinet d'avocats, dont le SI a été chiffré en novembre 2020 par le groupe d'attaquants Fox Kitten [22], puis les données rendues publiques [50, 51]. Fox Kitten est soupçonné par plusieurs éditeurs de sécurité informatique d'agir pour le compte du gouvernement iranien, et emploierait une couverture cybercriminelle [23] pour masquer à la fois ses objectifs de déstabilisation et son identité [52].

Enfin, des acteurs présumés étatiques conduisent des attaques ciblées : en septembre 2017, un acteur non identifié a divulgué sur Twitter une série de documents présentés comme exfiltrés du système d'information d'un cabinet d'avocats américain représentant Guo Wengui, un dissident chinois exilé aux États-Unis [53]. Guo Wengui et son entourage avaient déjà été la cible de plusieurs attaques informatiques [54, 55]. D'après des médias américains, ces opérations pourraient s'inscrire dans une campagne plus large d'acteurs agissant pour le compte du gouvernement chinois. Cette campagne aurait visé à la fois à décrédibiliser le critique du régime chinois et à envoyer un message d'avertissement aux membres de la diaspora chinoise [56].

Commentaire : si les cabinets d'avocats français semblent pour l'heure épargnés, ils pourraient être à l'avenir les victimes collatérales ou directes d'attaques de ce type, notamment en cas de dégradation des relations internationales ou s'ils défendent des personnalités originaires des pays employant ce mode d'action.

21. Aussi connu sous le nom d'UAC-0082, Voodoo Bear, Iridium ou FrozenBarents.
22. Aussi connu sous le nom de Pionner Kitten ou UNC757.
23. *Via* l'utilisation de rançongiciels tels que Pay2Key.

5. Recommandations

Les recommandations ci-dessous visent à répondre aux menaces présentées dans ce document, notamment autour des enjeux de confidentialité et de protection des données sensibles des cabinets d'avocats. Ces recommandations doivent être contextualisées, adaptées et priorisées en fonction de chaque cabinet d'avocats (taille de l'entité, moyens humains et financiers, sensibilité des dossiers, etc.). Elles sont destinées aux directeurs des systèmes d'information et aux RSSI, mais s'adressent aussi aux prestataires et aux décideurs des cabinets d'avocats.

5.1. Maîtrise des risques

Une étape importante est d'identifier, lors d'une première analyse, les menaces auxquelles l'entité fait face. La question de l'externalisation est un point important à traiter pour des structures dont la taille ne permet souvent pas de disposer de compétences informatiques en interne.

R1

Mener une analyse de risques intégrant l'ensemble des prestataires informatiques

Une analyse de risques doit être réalisée en prenant en compte plus particulièrement les hébergeurs, intégrateurs, mainteneurs, éditeurs de solutions, etc. Cette analyse de risques doit notamment mettre en exergue les risques numériques que ces prestataires feraient peser sur l'entité tant sur le plan technique qu'organisationnel, et les impacts sur le secret de l'instruction, le secret professionnel ou le secret des affaires. Cette réflexion doit intégrer les menaces décrites dans ce document.

Pour chaque utilisation d'un service numérique (échange de fichiers, messagerie, etc.), toujours s'interroger sur le niveau de confiance à accorder à ce service pour protéger les informations traitées au bon niveau, notamment sur l'origine du fournisseur du service, la localisation du service ou encore son niveau de protection (HTTPS, authentification, traçabilité, etc.).

R2

Faire un inventaire des données métier

Il est primordial de réaliser un inventaire des données métier : format, emplacement, sensibilité, responsabilité, besoin d'en connaître, etc.

R3

Faire régulièrement une sauvegarde hors-ligne

Il est recommandé de réaliser régulièrement (par exemple, une fois par mois) une sauvegarde hors-ligne et de stocker celle-ci dans un lieu physique sécurisé (export sur un disque externe USB et stockage dans un coffre par exemple).

R4

Prévoir à l'avance un mode d'organisation dégradé

Il est important de prévoir à l'avance un mode d'organisation dégradé dans le cas où le système d'information est indisponible à la suite d'une attaque : canal de communication de secours, récupération des données depuis la sauvegarde sur un poste de travail ou un serveur isolé, etc.

Prévoir un poste de travail de secours, ou un moyen de se doter d'un nouveau matériel, et une procédure rapide de restauration des données en cas de compromission des postes habituels.

R5

Surveiller systématiquement les interventions de vos prestataires

Il est recommandé de surveiller et de tracer systématiquement les interventions de vos prestataires sur le lieu de travail. Si l'intervention doit se faire à distance, il est important de veiller à la sécurité des accès distants (moyen de connexion et comptes utilisés) et de l'authenticité des intervenants.

Privilégier des interventions de vos prestataires informatiques sur site et en votre présence.

R6

Sensibiliser les utilisateurs sur les risques

Il est conseillé de sensibiliser les utilisateurs (avocats collaborateurs/collaboratrices, assistants/assistantes, office manager, etc.) sur les risques en lien avec la sécurité numérique : hameçonnage, clés USB malveillantes, etc.

Suivre le MOOC de l'ANSSI sur la sensibilisation à la SSI (`https://secnumacademie.gouv.fr`).

R7

Avoir un référent sécurité au sein des équipes

Il est intéressant d'avoir un référent sécurité au sein de l'entité. Il sera en charge de la sensibilisation des utilisateurs et peut éventuellement servir de point de contact en cas d'incident cyber.

Pour aller plus loin

- Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information : `https://www.ssi.gouv.fr/infogerance`
- Prestataires d'administration et de maintenance sécurisées (PAMS). Référentiel d'exigences : `https://www.ssi.gouv.fr/uploads/2022/10/anssi_pams_referentiel_v1.1_vfr.pdf`
- Maîtrise du risque numérique. L'atout confiance : `https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance`
- La méthode EBIOS Risk Manager. Le Guide : `https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide`
- Les règles d'or de la sauvegarde : `https://www.ssi.gouv.fr/les-regles-dor-de-la-sauvegarde/`

5.2. Protection du poste de travail

La protection du système d'information dans un contexte d'utilisation bureautique passe avant tout par une bonne hygiène sur les postes de travail de chaque utilisateur qui accède au système d'information du cabinet, qu'il soit avocat ou non.

L'usage de postes personnels est par définition à proscrire, tant les risques de compromission sont élevés dans ce contexte. La séparation stricte des usages professionnels et personnels est une mesure importante pour augmenter significativement le niveau de sécurité des cabinets d'avocats.

R8

Proscrire l'usage d'équipements personnels

Il est primordial de ne pas autoriser l'usage d'équipements personnels (téléphone, PC) dans un but professionnel.

R9

Imposer des comptes utilisateurs sans droits d'administrateur local sur les postes

Afin de conserver la maîtrise du niveau de sécurité des postes de travail, les utilisateurs doivent se connecter sur ceux-ci avec un compte qui ne possède aucun droit d'administrateur local.

R10

Utiliser des logiciels éprouvés et maintenus à jour

Il est recommandé d'utiliser des logiciels éprouvés, légitimes et maintenus à jour. En effet, de nombreux logiciels gratuits ou contournant les licences éditeurs sont porteurs de codes malveillants.

R11

Interdire l'installation de logiciels *via* un compte utilisateur

Les utilisateurs ne doivent pas être en mesure d'installer seuls des logiciels *via* leur compte utilisateur. Il est également possible de configurer certains outils de contrôle des logiciels autorisés (exemple : *AppLocker* sur Windows).

Sur chaque poste de travail, il faut disposer de deux comptes distincts : un compte sans privilège pour la gestion au quotidien des dossiers, un compte avec privilèges d'administrateur (auquel l'utilisateur n'a pas accès) pour l'installation/désinstallation de logiciels quand cela est nécessaire.

R12

Définir une politique de mots de passe robuste

Il est recommandé de définir une politique de mots de passe robuste pour les utilisateurs : longueur minimale, complexité, etc.

R13

Appliquer les mises à jour de sécurité rapidement

Pour maintenir un niveau de sécurité acceptable sur les postes de travail, il est important d'appliquer systématiquement les mises à jour de sécurité du système d'exploitation et des logiciels le plus rapidement possible.

Il est tout aussi important de configurer les postes de travail de manière à appliquer automatiquement et régulièrement (tous les mois) les mises à jour de sécurité du SI et des logiciels les plus courants (navigateur Internet, visionneuse PDF, application de facturation, etc.)

R14

Implémenter un logiciel EDR ou antivirus

Afin de se protéger de certains scénarios de compromission des postes de travail, il est recommandé d'utiliser un logiciel ou un service de sécurité de type antivirus ou EDR (*Endpoint Detection and Response*). La base de données de référence de ces logiciels doit être mise à jour automatiquement et quotidiennement.

R15

Limiter la connexion de clés USB à des clés dédiées à l'usage professionnel

Il est important de limiter la connexion de clés USB à des clés dédiées à l'usage professionnel, ce qui implique d'interdire la connexion de clés USB personnelles ou en provenance de l'extérieur et de privilégier les échanges *via* les messageries. Dans le cas où ce n'est pas possible, il est recommandé d'utiliser au préalable une station de décontamination USB.

R16

Configurer les fonctions de protection natives des postes reposant sur la virtualisation

Il est recommandé d'utiliser, quand elles sont disponibles, les solutions natives de virtualisation sur le poste de travail pour sécuriser les usages potentiellement dangereux comme la navigation sur Internet ou l'exécution de certains programmes (exemple : *Microsoft Defender Application Guard*, *Windows Sandbox*, etc.).

Sécuriser le poste de travail en activant un maximum de fonctions natives de protection (exemple : pare-feu local, *Secure Boot UEFI*, etc.).

Le réseau privé virtuel des avocats (RPVA) permet d'interconnecter les avocats à certaines entités juridiques étatiques. Un canal sécurisé (VPN) est implémenté au moyen d'une surcouche installée sur les navigateurs Internet, et authentifié avec un composant physique externe (*token* USB).

R17

Protéger physiquement la clé matérielle et le secret d'authentification RPVA

Il est important de protéger physiquement le matériel (*token* USB) et le secret d'authentification RPVA, de manière à ce qu'ils restent sous la maîtrise de l'utilisateur qui en est responsable, et qu'ils ne puissent pas être partagés ni utilisés par d'autres utilisateurs, même temporairement.

R18

Ne pas utiliser un mode de connexion dégradé pour l'accès au RPVA

Dans la mesure du possible, il est recommandé de ne pas utiliser de mode de connexion dégradé reposant sur une authentification potentiellement vulnérable (exemple : envoi d'un SMS sur le téléphone de l'utilisateur).

R19

Dédier un navigateur pour les accès RPVA

Il peut être opportun de dédier un logiciel navigateur sur le poste de travail pour les accès RPVA, distinct du navigateur utilisé pour accéder à Internet. Ainsi, il sera possible d'appliquer une configuration plus sécurisée et durcie (exemple : désactivation de fonctions inutiles) sur le navigateur dédié RPVA, et d'avoir une configuration un peu plus « permissive » si besoin sur le navigateur dédié à toute autre navigation sur Internet.

Pour aller plus loin

- La cybersécurité pour les TPE/PME en 13 questions : `https://www.ssi.gouv.fr/guide-tpe-pme`
- Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures : `https://www.ssi.gouv.fr/hygiene-informatique`
- Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows : `https://www.ssi.gouv.fr/windows-restrictions-logicielles`
- CNIL - Recommandation relative aux mots de passe et autres secrets partagés : `https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046437451`

5.3. Protection en confidentialité des données

Enfin, dans le contexte d'un secteur d'activité où la protection de la confidentialité des données sensibles est primordiale, les recommandations suivantes sont proposées afin de traiter ce point essentiel pour des cabinets d'avocats.

R20

Chiffrer entièrement les disques durs des postes de travail

Il est recommandé de chiffrer entièrement les disques durs des postes de travail, et de configurer un mot de passe de déchiffrement au démarrage de ces postes en activant la fonctionnalité native du système d'exploitation (exemple : *FileVault* pour MacOS, *Bitlocker* pour Windows) ou en utilisant un logiciel spécifique (exemple : *Cryhod*).

R21

Chiffrer systématiquement les données sensibles stockées

Il est recommandé de chiffrer systématiquement les données sensibles avec un logiciel maîtrisé (exemple : *Zed*, *Kleopatra PGP*, ZIP chiffré, etc.) et ce, quel que soit l'emplacement de stockage de ces données : poste de travail, serveur local, NAS, Cloud, etc.

R22

Chiffrer systématiquement les données sensibles avant de les communiquer

Il est recommandé de chiffrer systématiquement les données sensibles avant de les envoyer à un interlocuteur, quel que soit le moyen de communication (mail, solution de partage temporaire sur Internet, clé USB, etc). La communication du mot de passe de déchiffrement au destinataire doit se faire par un autre moyen que celui utilisé pour l'envoi des données.

R23

Utiliser un logiciel coffre-fort de mot de passe

Il est recommandé d'utiliser un logiciel coffre-fort de mot de passe sur les postes de travail pour gérer les secrets de chiffrement utilisés. Un mot de passe suffisamment robuste doit être exigé pour l'accès à ce coffre-fort.

R24

Diversifier les secrets de chiffrement

Il est recommandé de diversifier les secrets de chiffrement des données sensibles par client, par affaire, par service numérique utilisé ou par autre organisation segmentée des informations ayant un sens professionnel. Il est surtout important de ne pas réutiliser le même mot de passe pour plusieurs usages et, au moins, de distinguer les mots de passe à usage professionnel de tout autre usage.

R25

Ne pas utiliser votre messagerie personnelle dans un but professionnel

Il est recommandé de ne pas utiliser votre messagerie personnelle dans un but professionnel et de disposer de deux comptes de messagerie distincts pour ces deux usages.

En cas d'urgence justifiant de l'utilisation d'une messagerie personnelle, il est recommandé de chiffrer systématiquement au préalable le message et les pièces jointes.

R26

Gérer le besoin d'en connaître entre les utilisateurs

Il est important de gérer le besoin d'en connaître entre les utilisateurs, par exemple en configurant des droits d'accès stricts sur vos applications métier (répertoires d'un serveur de fichiers local, application web de partage, etc.).

R27

Journaliser tous les événements d'accès de vos utilisateurs à des données sensibles

Dans un objectif de détection des anomalies et des actions malveillantes, il est important de journaliser les événements d'accès de tous les utilisateurs à des données sensibles et au SI de manière générale.

Quand les outils le permettent, il faut activer les journaux d'activité et générer régulièrement (tous les mois par exemple) un rapport sur l'état de sécurité de chaque poste de travail et sur l'accès aux logiciels de partage collaboratif.

R28

Utiliser systématiquement un filtre de confidentialité écran

Il est recommandé d'utiliser un filtre de confidentialité écran sur les postes de travail, notamment lorsque les utilisateurs sont en situation de nomadisme.

R29

Configurer un verrouillage automatique de la session du poste

Il est recommandé de configurer par défaut un verrouillage automatique de la session du poste de travail après une courte inactivité (durée < 5 minutes).

R30

Mettre en place l'impression sécurisée

Il est recommandé de mettre en place l'impression sécurisée de vos imprimantes si celles-ci sont partagées (exemple : code PIN demandé sur l'imprimante avant impression).

Veillez à ce que les impressions papier sensibles ne soient pas accessibles ou visibles par un tiers.

Pour aller plus loin

- Recommandations pour une utilisation sécurisée de Zed ! : `https://www.ssi.gouv.fr/recos-zed`
- Authentification multifacteur et mots de passe : `https://www.ssi.gouv.fr/mots-de-passe/`

A. Bibliographie

[1] CNIL. *Guide : les avocats et la loi informatique et libertés*. 1er janvier 2011.
URL : https://www.audentia-gestion.fr/CNIL/CNIL-Guide_Avocats.pdf.

[2] ABA Journal. *Victimized by Ransomware, Law Firm Sues Insurer for $700K in Lost Billings*. 2 mai 2017.
URL : https://www.abajournal.com/news/article/victimized_by_ransomware_law_firm_sues_insurer_for_700k_in_lost_billings.

[3] LeMagIT. *Ransomware : Everest continue de menacer Xefi et ses clients*. 11 octobre 2021.
URL : https://www.lemagit.fr/actualites/252507988/Ransomware-Everest-continue-de-menacer-Xefi-et-ses-clients.

[4] France Info. *Attentat contre Charlie Hebdo : un cabinet d'avocats piraté, des éléments du dossier publiés sur Internet*. 23 novembre 2021.
URL : https://www.francetvinfo.fr/economie/medias/charlie-hebdo/info-franceinfo-attentat-contre-charlie-hebdo-un-cabinet-d-avocats-pirate-des-elements-du-dossier-publies-sur-internet_4856149.html.

[5] Radio Télévision Suisse. *Des milliers de documents des affaires Charlie Hebdo et Samuel Paty circulent sur le darknet*. 24 novembre 2021.
URL : https://www.rts.ch/info/monde/12664373-des-milliers-de-documents-des-affaires-charlie-hebdo-et-samuel-paty-circulent-sur-le-darknet.html.

[6] Numerama. *Cyberattaque contre le ministère de la Justice : la piste d'un cabinet d'avocat privilégiée*. 2 février 2022.
URL : https://www.numerama.com/cyberguerre/840213-cyberattaque-contre-le-ministere-de-la-justice-la-piste-dun-cabinet-davocat-privilegiee.html.

[7] eSentire. *Notorious Cybercrime Gang, FIN7, Lands Malware in Law Firm*. 21 juillet 2021.
URL : https://www.esentire.com/security-advisories/notorious-cybercrime-gang-fin7-lands-malware-in-law-firm-using-fake-legal-complaint-against-jack-daniels-owner-brown-forman-inc.

[8] ANSSI. *Le groupe cybercriminel FIN7*. 27 avril 2022.
URL : https://www.cert.ssi.gouv.fr/uploads/20220427_NP_TLPWHITE_ANSSI_FIN7.pdf.

[9] FireEye. *Hacking the Street ? FIN4 Likely Playing the Market*. 1er janvier 2014.
URL : https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf.

[10] US Department of Justice. *Manhattan U.S. Attorney Announces Arrest Of Macau Resident And Unsealing Of Charges Against Three Individuals For Insider Trading Based On Information Hacked From Prominent U.S. Law Firms*. 27 décembre 2016.
URL : https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-arrest-macau-resident-and-unsealing-charges-against.

[11] Europol. *GozNym Malware : Cybercriminal Network Dismantled in International Operation*. 16 mai 2019.
URL : https://www.europol.europa.eu/media-press/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation.

[12] US Department of Justice. *GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation*. 16 mai 2019.
URL : https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled.

[13] JD Supra. *GozNym Malware Attack Hits Two Law Firms for Over $117K in Losses*. 31 mai 2019.
URL : https://www.jdsupra.com/legalnews/goznym-malware-attack-hits-two-law-90639/.

[14] US Department of Justice. *Three Iranian Nationals Charged With Engaging In Computer Intrusions And Ransomware-Style Extortion Against U.S. Critical Infrastructure Providers*. 14 septembre 2022.
URL : https://www.justice.gov/usao-nj/pr/three-iranian-nationals-charged-engaging-computer-intrusions-and-ransomware-style.

[15] U.S. Department of the Treasury. *Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity*. 14 septembre 2022.
URL : https://home.treasury.gov/news/press-releases/jy0948.

[16] Mandiant. *Privileges and Credentials : Phished at the Request of Counsel*. 6 juin 2017.
URL : https://www.mandiant.com/resources/blog/phished-at-the-request-of-counsel.

[17] The New York Times. *The Chinese Hackers in the Back Office*. 11 juin 2016.
URL : https://www.nytimes.com/2016/06/12/technology/the-chinese-hackers-in-the-back-office.html.

[18] ABC News. *Chinese Hackers Targeting Australian Law Firms for Sensitive Commercial Information*. 30 novembre 2017.
URL : https://www.abc.net.au/news/2017-12-01/chinese-hackers-targeting-australian-law-firms/9213520.

[19] CyberScoop. *Roy Moore Scandal Used for Phishing Schemes Aimed at U.S. Law Firms*. 4 décembre 2017.
URL : https://cyberscoop.com/roy-moore-scandal-phishing-attacks-apt19-fireeye-harvey-weinstein/.

[20] Recorded Future. *APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign*. 30 novembre 2017.
URL : https://go.recordedfuture.com/hubfs/reports/cta-2019-0206.pdf.

[21] Australian Government Department of Foreign Affairs and Trade. *Attribution of Chinese Cyber-Enabled Commercial Intellectual Property Theft*. 21 décembre 2018.
URL : https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-chinese-cyber-enabled-commercial-intellectual-property-theft.

[22] US Department of Justice. *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*. 20 décembre 2018.
URL : https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

[23] NCSC-UK. *APT10 Continuing to Target UK Organisations*. 20 décembre 2018.
URL : https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations.

[24] F-Secure. *Nanhaishu RATing the South China Sea*. 1er juillet 2016.
URL : https://blog-assets.f-secure.com/wp-content/uploads/2019/10/15163422/NanHaiShu.pdf.

[25] Bloomberg. *China's Cyber Spies Take to High Seas as Hack Attacks Spike*. 15 octobre 2015.
URL : https://www.bloomberg.com/news/articles/2015-10-15/chinese-cyber-spies-fish-for-enemies-in-south-china-sea-dispute.

[26] Threatconnect. *China Hacks the Peace Palace : All Your EEZ's Are Belong to Us*. 20 juillet 2015.
URL : https://web.archive.org/web/20151031022526/https://threatconnect.com/china-hacks-the-peace-palace-all-your-eezs-are-belong-to-us/.

[27] NSA, NCSC-UK et FBI. *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*. 1er juillet 2021.
URL : https://media.defense.gov/2021/Jul/01/2002753896/-1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO0158036-21.PDF.

[28] Conseil de l'Union européenne. *L'UE impose les toutes premières sanctions à la suite de cyberattaques*. 30 juillet 2020.
URL : https://www.consilium.europa.eu/fr/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

[29] Citizen Lab. *FORCEDENTRY : NSO Group iMessage Zero-Click Exploit Captured in the Wild*. 13 septembre 2021.
URL : https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/.

[30] Citizen Lab. *HIDE AND SEEK : Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*. 18 septembre 2018.
URL : https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[31] The New York Times. *WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone*. 13 mai 2019.
URL : https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html.

[32] The Intercept. *Leaked Files : German Spy Company Helped Bahrain Hack Arab Spring Protesters*. 7 août 2014.
URL : https://theintercept.com/2014/08/07/leaked-files-german-spy-company-helped-bahrain-track-arab-spring-protesters/.

[33] OCCRP. *The Pegasus Project - Who's on the List - Lawyers*. 18 juillet 2021.
URL : https://cdn.occrp.org/projects/project-p/#/professions/lawyer.

[34] The Bureau of Investigative Journalism. *How Qatar Hacked the World Cup*. 5 novembre 2022.
URL : https://www.thebureauinvestigates.com/stories/2022-11-05/how-qatar-hacked-the-world-cup.

[35] CNBC. *Dubai's Sheikh Mohammed Ordered Phones of Ex-Wife and Lawyers to Be Hacked, UK Court Says*. 6 octobre 2021.
URL : https://www.cnbc.com/2021/10/06/dubais-sheikh-mohammed-ordered-phones-of-ex-wife-and-lawyers-to-be-hacked-uk-court-says.html.

[36] Reuters. *Israeli Private Detective Used Indian Hackers in Job for Russian Oligarchs, Court Filing Says*. 28 mai 2022.
URL : https://www.reuters.com/world/israeli-private-detective-used-indian-hackers-job-russian-oligarchs-court-filing-2022-05-27/.

[37] Reuters. *How Mercenary Hackers Sway Litigation Battles*. 30 juin 2022.
URL : https://www.reuters.com/investigates/special-report/usa-hackers-litigation/.

[38] Kaspersky. *Lifting the Veil on DeathStalker, a Mercenary Triumvirate*. 24 août 2020.
URL : https://securelist.com/deathstalker-mercenary-triumvirate/98177/.

[39] Trend Micro. *The Far-Reaching Attacks of the Void Balaur Cybermercenary Group*. 10 novembre 2021.
URL : https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-far-reaching-attacks-of-the-void-balaur-cybermercenary-group.

[40] The Guardian. *Anonymous Publishes Trove of Emails from Haditha Marine Law Firm*. 6 février 2012.
URL : http://www.theguardian.com/technology/2012/feb/06/anonymous-haditha-killings.

[41] Reuters. *Haditha Marine's Lawyers Call Anonymous "Cowards" after Hack*. 7 février 2012.
URL : https://www.reuters.com/article/us-marine-haditha-hackers-idUSTRE81609N20120207.

[42] Infosec Institute. *Panama Papers - How Hackers Breached the Mossack Fonseca Firm*. 20 avril 2016.
URL : https://resources.infosecinstitute.com/topic/panama-papers-how-hackers-breached-the-mossack-fonseca-firm/.

[43] France 24. *Panama Papers Law Firm : 'We Were Hacked from Abroad'*. 6 avril 2016.
URL : https://www.france24.com/en/20160406-panama-papers-mossack-fonseca-law-firm-says-hacked-abroad.

[44] ICIJ. *ICIJ Releases Paradise Papers Data From Appleby*. 17 novembre 2017.
URL : https://www.icij.org/investigations/paradise-papers/icij-releases-paradise-papers-data-appleby/.

[45] HackRead. *Anonymous Hacktivists Leak 1TB of Top Russian Law Firm Data*. 4 juin 2022.
URL : https://www.hackread.com/anonymous-hacktivists-leak-1tb-russia-law-firm-data/.

[46] ESET. *Sandworm : Une nouvelle histoire de perturbation*. 23 mars 2022.
URL : https://www.welivesecurity.com/fr/2022/03/23/sandworm-nouvelle-histoire-de-perturbation/.

[47] The Wall Street Journal. *DLA Piper CIO on 'Petya' Attack : 'The Future of the Entire Business Was At Stake'*. 18 décembre 2017.
URL : https://www.wsj.com/articles/dla-piper-cio-on-petya-attack-the-future-of-the-entire-business-was-at-stake-1513635888.

[48] Computerworld. *DLA Piper Paid 15,000 Hours of IT Overtime after NotPetya Attack*. 8 mai 2018.
URL : https://www.itnews.com.au/news/dla-piper-paid-15000-hours-of-it-overtime-after-notpetya-attack-490495.

[49] HAARETZ. *'The Iranians Are Waiting for the Israeli Response' : Who Is Behind the Latest Cyberattack on Israeli Firms ?* 19 décembre 2020.
URL : https://www.haaretz.com/israel-news/2020-12-19/ty-article/iran-israel-response-pay2key-who-behind-cyberattack-israeli-firms/0000017f-e856-df5f-a17f-fbde55db0000.

[50] CLEARSKY. *Pay2Kitten – Fox Kitten*. 17 décembre 2020.
URL : https://www.clearskysec.com/pay2kitten/.

[51] CHECKPOINT. *Pay2Key – The Plot Thickens*. 12 novembre 2020.
URL : https://research.checkpoint.com/2020/pay2key-the-plot-thickens/.

[52] SEKOIA. *Vers une nouvelle utilisation du ransomware par des acteurs étatiques ?* 2 juillet 2021.
URL : https://blog.sekoia.io/fr/vers-une-nouvelle-utilisation-du-ransomware-par-des-acteurs-etatiques/.

[53] THE WASHINGTON FREE BEACON. *FBI Eyes China in Posting Hacked Documents on Chinese Dissident*. 29 septembre 2017.
URL : https://freebeacon.com/national-security/fbi-eyes-china-posting-hacked-documents-chinese-dissident/.

[54] THE WASHINGTON FREE BEACON. *Beijing Suspected in Hacking Yacht Owned by Chinese Billionaire*. 8 septembre 2017.
URL : https://freebeacon.com/national-security/beijing-suspected-hacking-yacht-owned-chinese-billionaire/.

[55] THE WALL STREET JOURNAL. *U.S. Confronts China Over Suspected Cyberattack as Fugitive Guo Wengui Appears in Washington*. 6 octobre 2017.
URL : https://www.wsj.com/articles/chinese-governments-battle-against-fugitive-guo-wengui-spills-into-washington-1507260255.

[56] SECURITY WEEK. *Cyber Attacks Targeted Interests of Billionaire Chinese Dissident*. 9 octobre 2017.
URL : https://www.securityweek.com/cyber-attacks-targeted-interests-billionaire-chinese-dissident/.

27 juin 2023

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
cert.ssi.gouv.fr / cert-fr@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité