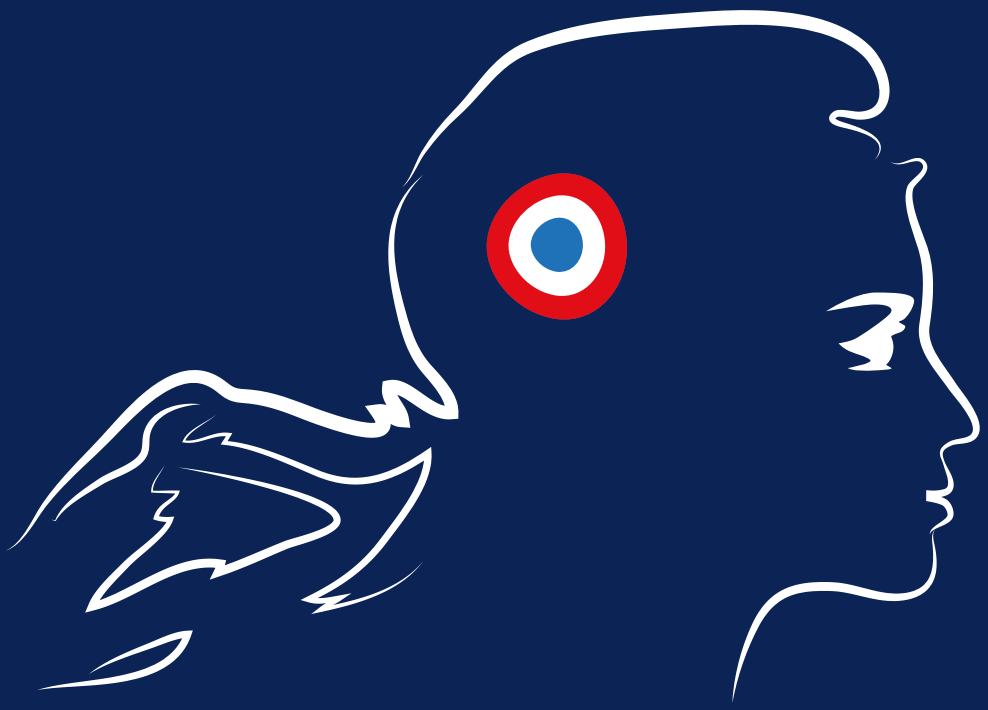


DOSSIER SPÉCIAL

Cybersécurité & Élections

PIRATER LES ÉLECTIONS : ÉTAT DES LIEUX AVANT LA PRÉSIDENTIELLE DE 2022

serenety
By xmco

Sommaire

Avant-propos.

LA NUMÉRISATION DE LA SOCIÉTÉ EST UN PHÉNOMÈNE TOTAL : VIE PRIVÉE ET SOCIALE, COMMERCE, OPÉRATIONS MILITAIRES OU CRIMINELLES, ETC. LA VIE DÉMOCRATIQUE ET LES ÉLECTIONS QUI LUI SONT PROPRES N'Y ÉCHAPPENT PAS. CET ÉTAT DE FAIT POSE LA QUESTION DE PLUS EN PLUS IMPORTANTE DE LA CYBERSÉCURITÉ DES CAMPAGNES ÉLECTORALES ET DES PROCESSUS DE VOTE.

Dans cette perspective, le CERT-XMCO propose ce dossier spécial pour passer en revue les principales menaces qui pèsent sur les prochaines échéances électorales françaises, et y associer un niveau de risque attendu.

1. S'en prendre directement aux campagnes politiques

EN AMONT DU VOTE, LES OPÉRATIONS DE DÉSTABILISATION VISENT À BOULEVERSER LE PAYSAGE INFORMATIONNEL D'UNE ÉLECTION, GÉNÉRALEMENT QUELQUES JOURS AVANT LE VOTE. CES ÉVÈNEMENTS PERMETTENT DE REBATTRE LES CARTES ET DE FAIRE ÉMERGER DES SITUATIONS NOUVELLES, DÉFAVORABLES AUX CANDIDATS VISÉS.

L'une des principales manières d'influencer le cours d'une élection revient à publier des informations compromettantes sur un candidat. dans l'espace numérique, cela revient le plus souvent à divulguer des informations secrètes ou cachées.

Les MacronLeaks, version 2022 ?

LE CAS D'ÉCOLE DE LA CAMPAGNE PRÉSIDENTIELLE D'HILLARY CLINTON EN 2016.

Comme souvent, l'un des exemples les plus emblématiques nous vient d'outre-Atlantique avec l'affaire des emails d'Hilary Clinton dans les années 2015-2016. Wikileaks a publié à plusieurs reprises des dizaines de milliers d'emails liés à Hillary Clinton. Cette affaire regroupe en réalité trois scandales distincts :

En mars 2015, le New York Times affirme qu'Hillary Clinton n'a eu aucune adresse email officielle lorsqu'elle était secrétaire d'État, entre 2009 et 2013. À la place elle avait envoyé et reçu l'intégralité de ses emails professionnels depuis un serveur privé, chez elle. Avec l'éclatement du scandale, 50 000 pages d'emails imprimés par Hillary Clinton seront épluchées par les autorités et les journalistes américains, apportant une cascade de révélations sur la gestion des affaires par Hillary Clinton.

En juillet 2016, les serveurs d'emails de la Democratic Nation Convention *(DNC)*, l'organisation en charge de la primaire et de la campagne des démocrates en vue de l'élection présidentielle, sont piratés. La publication des emails par Wikileaks révèle que les instances dirigeantes du parti démocrate ont systématiquement chercher à favoriser Hillary Clinton par rapport à Bernie Sanders, des révélations qui accentuèrent les divisions au sein du parti démocrate et poussent à la démission de la présidente de la DNC, Deborah Wasserman Schultz.

La boîte de messagerie de John Podesta, le directeur de campagne de la candidate Hillary Clinton, est piratée. L'intégralité de ses emails est transférée à Wikileaks qui les publie. Le contenu des emails apporte son lot de révélations et de contradictions flagrantes entre les propos publics de la candidate et ses échanges privés.

Si la première n'affaire n'est pas le résultat d'une cyberattaque les deux autres le sont clairement. Les organismes gouvernementaux américains ainsi que plusieurs entreprises spécialisées ont pointé du doigt la Russie, et plus spécifiquement les groupes Cozy Bear *(aka APT29)* et Fancy Bear *(aka APT28)*. Sur le cas spécifique de la DNC, les services de renseignement ont affirmé que le Republican National Committee aurait aussi été piraté, mais que ses données n'ont volontairement pas été publiées par les attaquants.

LES RÉCENTS CAS D'USAGES ALLEMANDS EN 2018 ET 2021.

Les élections allemandes auraient aussi été la cible de cyberattaques depuis plusieurs années. Par exemple, plusieurs parlementaires allemands auraient été ciblés lors des dernières élections législatives de septembre 2021. Le gouvernement allemand a accusé des organisations russes d'avoir mené ces attaques par phishing visant les parlementaires des partis majoritaires.

Toutefois, les piratages à objectifs politiques ne sont pas l'apanage de groupes malveillants liés à des États. Toujours en Allemagne, un jeune homme de 20 ans avait piraté les données[1] de presque 1000 personnalités publiques, dont de nombreux acteurs de la vie politique avec lesquels il était en opposition. Le ministre de l'Intérieur allemand avait indiqué que l'attaquant n'aurait pas été en mesure de recueillir autant de données si ses victimes avaient créé des mots de passe plus sophistiqués. Il avait ajouté « *Les mauvais mots de passe sont l'une des raisons pour lesquelles il a eu la vie si facile* », pour conclure en insistant sur le fait que les politiciens devaient accroître considérablement leur sensibilité à la cybersécurité et que de telles attaques allaient certainement devenir plus courantes. Ces propos font écho à l'affaire dite des « *MacronsLeaks* » qui a éclaté pendant la campagne présidentielle française de 2017.

LES MACRONLEAKS

En 2017, l'équipe de campagne d'Emmanuel Macron, alors candidat à la Présidence de la République a, elle aussi, été victime d'une publication massive d'emails, appelée « Macron Leaks ». En effet, le vendredi 5 mai 2017 *(soit 2 jours avant la tenue du second tour)*, un dossier de 21 075 emails[2] liés à la campagne présidentielle de l'ancien ministre de l'Économie a été massivement publié sur les réseaux sociaux. Si des investigations ultérieures ont mis en avant le fait que la campagne d'Emmanuel Macron aurait été la cible de Fancy Bear *(aka APT28)*, un groupe d'attaquants proche du pouvoir russe aussi soupçonné d'avoir piraté TV5 Monde[3] en 2015, l'ANSSI[4] n'a jamais confirmé cette hypothèse.
Le directeur de celle-ci avait même indiqué que l'attaque était si simple à mener qu'elle aurait pu être l'œuvre d'un individu isolé.

Les MacronLeaks ont eu lieu à la suite d'une simple attaque par phishing sur les membres de l'équipe de campagne d'Emmanuel Macron, dont Cédric O, le trésorier de la République en marche de l'époque. Ce dernier, devenu Secrétaire d'État au numérique en 2019 faisait partie des 5 personnes qui avaient cliqué sur la pièce-jointe malveillante ayant permis à l'attaque d'aboutir.

In total, the professional and personal email accounts of at least five of Macron's close colleagues were hacked: the Gmail accounts of Quentin Lafay (speechwriter), Anne-Christine Lang (socialist Party MP for the department of paris), Alain Tourret (Radical Party of the Left and Socialist Party MP for the department of Calvados), Pierre Person (co-founder and president of «The Young With Macron» movement), along with his Google Drive, and the en-marche.fr account of Cédric O (En Marche! treasure).[56] The stolen emails range from March 20, 2009, to April 24, 2017,[57] indicating that at least one of the successful attacks had occured that day.

Membres de la campagne d'Emmanuel Macron piratés au cours des MarconLeaks (sources : IRSEM et Atlantic Council)

Le mode opératoire de l'attaque s'est déroulé en 3 étapes principales :

1. En avril/mars 2017, plusieurs domaines[6] *(onedrive-en-marche.fr, mail-en-marche.fr, portal-office.fr, and accounts-office.fr)* sont enregistrés pour mener une campagne de phishing ciblée.

2. Envoi des emails de phishing aux membres de l'équipe de campagne, des emails assez bien faits d'après Mounir Mahjoubi[7] le responsable numérique de la campagne d'Emmanuel Macron *(à titre d'exemple, des emails ont été envoyés d'une adresse mounir.mahjobi@ au lieu de mounir.mahjoubi@)*.

3. Compromission des adresses email et premières publications sur PasteBin et 4Chan[8].

Par ailleurs, la campagne d'Emmanuel Macron aurait été visée par des tentatives de phishing à plusieurs reprises au cours des mois précédant le vote. La création des domaines ne serait donc pas forcément l'œuvre des mêmes attaquants responsables des MacronLeaks et pourrait expliquer les différentes possibilités sur l'attribution de l'attaque.

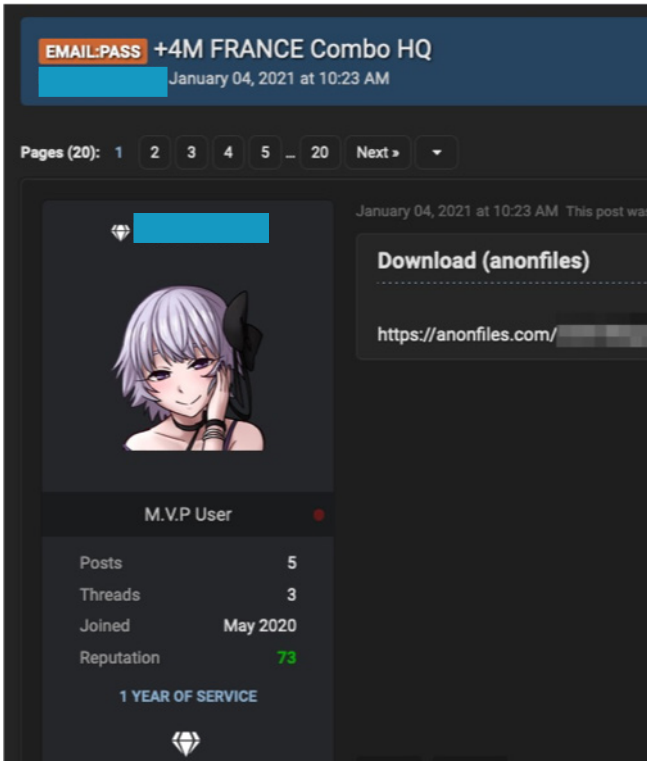
En définitive, ce piratage a pu être mené sans haut niveau de sophistication, et a donné suite à une mise à disposition soudaine de données brutes sur Internet. De ce point de vue, il s'agit plus d'une tentative de déstabilisation qu'une fuite de données sensibles, comme celles concernant Hillary Clinton un an plus tôt. Le contenu des emails étant banal et propre à toute campagne électorale, de faux documents ont été ajoutés ultérieurement aux archives par d'autres acteurs malveillants.

Si l'affaire des Macronleaks est restée dans les mémoires, elle a eu peu d'impact sur l'issue du vote, malgré la mise en scène dont elle fait l'objet de la part de groupes politiques, venant des droites américaine et française notamment, sur les réseaux sociaux.

Cependant, ses répercussions auraient pu être bien supérieures si elle avait divulgué des contenus graves et la configuration politique de l'époque n'avait pas opposé Emmanuel Macron à Marine Le Pen.

UN ÉVÈNEMENT COMPARABLE POURRAIT-IL SE REPRODUIRE EN 2022 ?

Parmi les services échangés et vendus sur les forums et marchés des cybercriminels, les emails et leurs mots de passe *(aussi appelés « COMBO »)* occupent une place de choix. Ils proviennent le plus souvent de compromissions d'entreprises par des cybercriminels[9]. Ces combos sont souvent utilisés pour mener des actions frauduleuses ou des cyberattaques.



Exemple de combo trouvé sur le Deep Web

Le phénomène est d'une telle ampleur que des dizaines de millions d'individus sont concernés. Surtout, le personnel politique ne semble pas épargné. Au travers de quelques recherches simples, sur les forums du Dark Web[10] et plus encore sur les services d'indexations de bases de données compromises comme WeLeakInfo ou Leak-Lookup *(utilisés par des journalistes et des professionnels, mais aussi par des attaquants)* il est possible d'identifier les adresses email professionnelles ou personnelles *(ainsi que leurs mots de passe associés)* de presque n'importe qui. C'est justement WeLeakInfo qui aurait été utilisé par le jeune pirate allemand pour mener son attaque contre les personnalités politiques allemandes[11].

Toutes ces informations pourraient être utilisées par des attaquants pour obtenir des accès aux boîtes email des personnes concernées. De telles actions pourraient permettre aux attaquants de voler les informations sensibles puis de les publier pour déstabiliser leurs cibles ou de menacer de les publier pour exercer un chantage dans un contexte de fortes pressions liées à la campagne présidentielle.

Par exemple, un mot de passe volé est directement exploitable par des acteurs malveillants grâce à la technique du « credential stuffing ». Cela correspond au fait d'essayer de se connecter sur le maximum de services et de plateformes grâce au mot de passe fuité, dans l'espoir que le même mot de passe soit utilisé plusieurs fois.

L'affaire Pegasus à la lumière de la présidentielle.

©Nicolas TUCAT/ AFP *©Szilard Koszticsak/EPA/MAXPPP*

Emmanuel Macron et Éric Zemmour avec leurs téléphones portables

Juillet 2021, l'affaire Pegasus prenait un tournant nouveau en France. Les médias révélaient que le logiciel espion développé et vendu par l'entreprise israélienne NSO Group avait été utilisé à des fins d'espionnage de personnalités politiques européennes, au premier rang desquelles Éric Zemmour et Emmanuel Macron *(ce dernier ayant gardé l'usage de son appareil personnel après sa prise de fonction à la présidence)*.

Pegasus est un malware qui exploite une vulnérabilité sur les systèmes d'exploitation iOS. Dès lors qu'un iPhone est infecté, les attaquants ont accès à l'intégralité du contenu de l'appareil visé : SMS, appels, répertoire, conversions d'applications chiffrées, activation du microphone, etc.

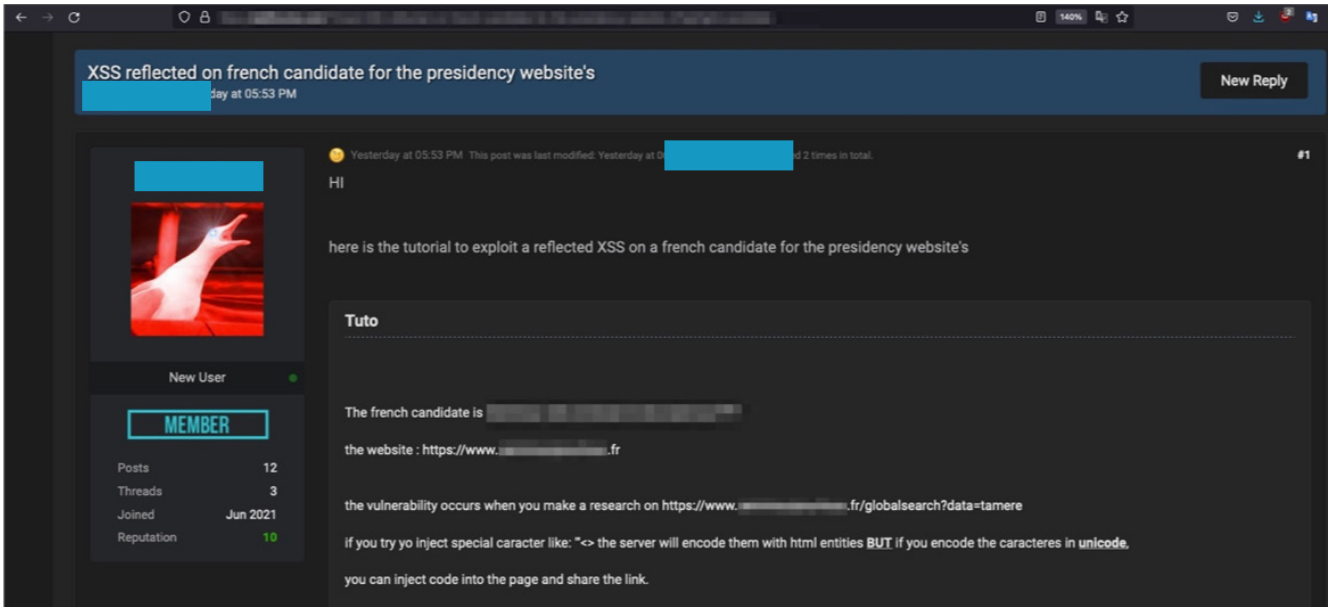
À l'aune de ces éléments, on comprend que la campagne présidentielle est en train d'avoir lieu alors même que deux des principaux prétendants ont eu leur téléphone infecté par un logiciel espion ultrasophistiqué. Les possibilités de chantage et de pression sont réelles, de même que l'éventualité de publication de données compromises seulement quelques jours avant le scrutin pour assurer la plus grande confusion possible. À cet égard, l'affaire Pegasus pourrait toujours connaître de nouveaux rebondissements dans les prochains mois.

Salir les vitrines numériques des candidats.

Les candidats misent aujourd'hui énormément sur le numérique pour faire la promotion de leurs campagnes. Leurs sites web ou leurs comptes sur les réseaux sociaux représentent des cibles de valeur pour des acteurs malveillants.

Dans les cas des comptes Twitter, il facile pour un attaquant de chercher les combos d'adresses email de responsables sur les réseaux sociaux pour accéder à leur compte Twitter ou à leurs boîtes email. Dans ce dernier cas, il est possible faire une demande de réinitialisation de mot de passe d'un compte Twitter dès lors que le compte est lié à la boîte email compromise. En procédant ainsi, l'attaquant pourrait avoir un accès au compte Twitter d'un candidat et y publier une fake news, par exemple, pour détériorer une dynamique de campagne.

Dans le cas des sites web, l'exploitation de vulnérabilités basiques peut être utilisée pour attaquer des campagnes électorales. Ainsi, on a vu fleurir sur les forums du DeepWeb, les publications d'attaquants ou d'activistes visant les infrastructures numériques de candidats à la présidentielle. C'est le cas de la publication ci-dessous, datant de décembre 2021.

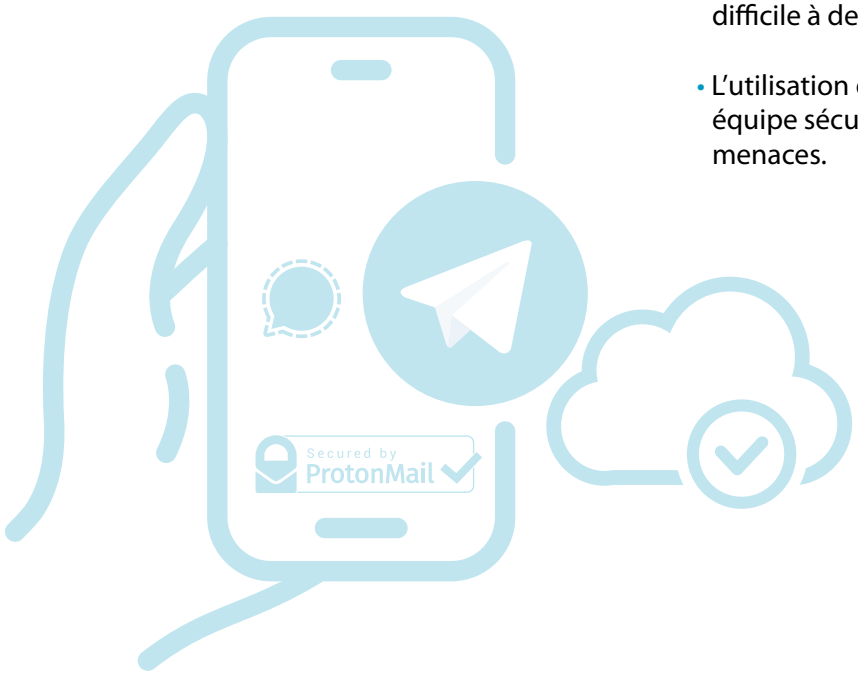


Publication d'un acteur malveillant indiquant comment mener une attaque de type Reflected XSS (ou non persistante) sur le site de campagne d'un candidat, avec la possibilité d'injecter des images par exemple.

Comment se prémunir de tels risques ?

Il semblerait que la publication des MacronLeaks en 2017 ait fait prendre conscience à une partie du monde politique de l'importance de la cybersécurité dans le cadre d'une campagne présidentielle. C'est ainsi que le magazine Marianne[12] révélait que l'équipe de campagne d'Éric Zemmour s'est organisée de manière à réduire les risques de fuite de données. En effet, celle-ci aurait adopté le système de messagerie chiffrée ProtonMail, elle indique ne pas utiliser Whatsapp, ni les SMS classiques, mais Signal et Telegram, « des applications également plébiscitées par Emmanuel Macron et ses soutiens, vaccinés depuis la mésaventure MacronLeaks », précise le journaliste.

Si ces mesures ont leur utilité, elles devraient être accompagnées d'initiatives complémentaires.



On peut notamment citer :

- L'activation généralisée de l'authentification multifacteur ;
- L'utilisation d'appareils et d'adresses email dédiés ;
- Le chiffrement systématique des fichiers sensibles *(communications internes, données financières et personnelles, axes stratégiques, etc.)* ;
- Étendre la sécurité aux adresses email personnelles ;
- L'activation de tous les paramètres de durcissement lors de l'utilisation de systèmes de partage de fichiers et cloud ;
- L'utilisation d'adresses email aux intitulés difficile à deviner pour des attaquants ;
- L'utilisation d'un service de veille et d'une équipe sécurité pour prévenir d'éventuelles menaces.

2. Les enjeux autour du vote électronique

DANS UN CONTEXTE DE CRISE DÉMOCRATIQUE, LE VOTE ÉLECTRONIQUE EST UN SUJET DE PLUS EN PLUS POPULAIRE. REGROUPANT À LA FOIS L'UTILISATION DE MACHINES DANS LES BUREAUX DE VOTE ET LE VOTE PAR INTERNET, ÉGALEMENT APPELÉ « E-VOTE », IL S'AGIT D'UNE MÉTHODE PERMETTANT À UN ÉLECTEUR, DANS LE CAS D'UN SCRUTIN EN LIGNE D'ÉVITER DE SE RENDRE PHYSIQUEMENT DANS SON BUREAU DE VOTE.

Très développé dans certains pays comme l'Estonie depuis 2005, le vote en ligne permet aux citoyens estoniens de voter à distance aux élections municipales. Ce système est promu dans de nombreux pays où le vote électronique est vu comme une solution à l'abstention.

Il faut dire que ce mode de scrutin comporte plusieurs avantages :

- Une plus grande facilité dans le comptage des voix ;
- Une traçabilité des votes ;
- Une plus grande facilité à voter pour les citoyens qui n'ont plus besoin de se rendre physiquement dans les bureaux de vote le jour J ou bien de faire une procuration de vote.

Cependant, cette pratique augmente également la surface d'exposition des systèmes d'information des infrastructures sur lesquels ils sont basés. En effet, une machine à vote demeure un ordinateur fonctionnant sur un système d'exploitation *(Windows ou Linux)* lui-même comportant des vulnérabilités exploitables pouvant potentiellement mener à une modification du contenu et donc, in fine, à modifier les votes. De même, le vote en ligne est adossé à une ou plusieurs plateformes connectées à internet et auxquelles les citoyens se connectent pour voter. Ces plateformes peuvent contenir différentes informations critiques telles que la base de données des électeurs, les informations sur le processus de vote ou les logiciels d'enregistrement et de traitement des votes. Des acteurs malveillants pourraient alors tenter de compromettre les comptes administrateurs du site afin de modifier les résultats des votes ou encore induire en erreur les électeurs en affichant de fausses informations.

Par ailleurs, la complexité des technologies employées éloigne un peu plus le citoyen lambda du processus. Contrairement au dépouillement des urnes, qui est compréhensible par tous et auquel tous les citoyens peuvent participer, le vote électronique est un outil inconnu du grand public. Cette complexité pourrait même s'avérer contreproductive en renforçant l'idée d'un scrutin truqué sur lequel aucun contrôle indépendant ne pourrait être fait.

Le sujet fait l'objet de débat depuis plusieurs années en France où deux visions s'affrontent. D'une part, ceux en faveur de son développement, comme le candidat Macron en 2017 qui disait vouloir *« généraliser le vote électronique d'ici à 2022 »*, ce qu'il concrétisa en 2017 grâce au projet de loi n° 2021-191 du 22 février 2021 sur le report des élections régionales et départementales et sur l'installation de machines à votes. D'autre part, les opposants au e-vote, également contre ce projet de loi de 2017. En cause, notamment la présence d'un amendement qui prévoyait l'instauration du vote électronique et du vote par anticipation.

Ainsi, bien que le vote électronique soit peu développé dans l'hexagone, hors cas spécifiques, il pourrait être généralisé dans un avenir proche. En effet, d'après un sondage datant de 2015 et publié par Harris Interactive, 79% des 18-25 ans déclaraient que « *s'ils pouvaient voter par internet, ils le feraient* ». Il faudrait donc dès maintenant interroger les enjeux cyber liés à ce système et ainsi intégrer le principe du « ***security by design*** ».

Le piratage des machines de vote.

UNE CERTAINE OPACITÉ DE FONCTIONNEMENT

« L'utilisation de la cryptographie »

Apparues en Angleterre au XIX^{e} siècle, les machines à vote sont aujourd'hui de deux natures : scan optique (ou **optical scan**) ou électronique à enregistrement direct ou **Direct- recording electronic** (RDE)[1].

Dans le premier cas, le choix des électeurs est matérialisé sous forme d'un code-barre ou d'un QR-code imprimé sur un papier. Pour comptabiliser le vote, il faut seulement scanner ce code. Néanmoins, cette technique peut amener de nombreuses erreurs. Dans le second cas, l'électeur a seulement besoin d'effectuer son vote sur un écran tactile. L'identité du citoyen doit coïncider avec le registre de la liste électorale et l'électeur ne peut voter qu'une seule fois. L'électeur a aussi la possibilité d'imprimer un reçu de son vote, permettant de confirmer la bonne prise en compte de son choix.

Le DRE se fonde notamment sur les quatre principes de la cryptographie pour certifier les résultats : la confidentialité et l'intégrité des données, l'authenticité et la non-répudiation.

- Le premier principe, celui de la confidentialité permet de s'assurer que la donnée soit limitée à certaines personnes. Dans le cas des élections, cela désigne l'électeur et la personne en charge du comptage des votes.
- Le second principe est celui de l'intégrité des données. Le choix du votant ne doit pas être altéré jusqu'à ce qu'il soit comptabilisé.
- Le troisième principe est l'authenticité de la donnée. Il s'agit de s'assurer que l'électeur A a bien voté pour le candidat X et l'électeur B a bien voté pour le candidat Y.
- Le dernier principe, celui de la non-répudiation, permet d'empêcher que l'électeur A ne renie son vote pour le candidat X.

Dans le cas des États-Unis, deux systèmes de RDE étaient utilisés dans 12 états en 2021[2]. Il s'agit du **Scratch & Vote protocol** et de **VoteHere**. Les deux systèmes utilisent un service similaire à celui de la **blockchain** afin de rendre traçable son vote pour un électeur.

Malgré d'importants efforts concentrés sur la transparence, ces systèmes souffrent d'un niveau de sécurité insuffisant.

DES ERREURS CONSTATÉES PAR LE PASSÉ ET DES VULNÉRABILITÉS QUI PÈSENT SUR L'AVENIR

« Exemple d'erreurs informatiques passées »

L'un des cas emblématiques liés aux machines à vote est celui des élections américaines de 2000[3]. Deux candidats sont alors au coude à coude : le démocrate Al Gore et le républicain George W. Bush, fils. C'est dans l'état de Californie qu'un bug général survient avec les machines à votes. Ce bug a un impact d'autant plus important que cet état est crucial pour départager les deux adversaires. L'impossibilité de compter les votes s'explique d'un côté par l'ancienneté des machines utilisées, certaines ayant plus de 16 ans avec des composants défectueux, et de l'autre par le manque de formation du personnel dans les bureaux de vote.

S'en est alors suivi un quasi « *désordre démocratique* » avec un recomptage fastidieux des votes à la suite duquel Georges W. Bush remporta la victoire, à une très courte majorité *(537 voix de plus)*. Ce précédent pousse les autorités américaines à faire passer la loi du **Help America Vote Act** *(ou* **HAVA***)* de 2002[4]. Cette dernière doit permettre d'aider les états à moderniser leur parc de machines à vote, devenues obsolètes. Pour cela, la loi alloue 4 milliards de dollars. Un autre volet de la loi est la création du **US Election Assistance Commission** *(***EAC***)*. Il s'agit d'une agence fédérale indépendante dont l'objectif est la création de normes pour les systèmes électoraux des municipalités et des états.

Ces erreurs informatiques minent la confiance envers un système électoral basé sur les machines à vote. Comme l'explique un spécialiste en sécurité de Cambridge Global Advisor : « ***you cannot trust a machine as white paper ballot*** »[5].

Le cas américain n'est pas le seul existant. En France, une étude a été menée entre 2007 et 2008 sur les élections présidentielles, législatives, municipales et cantonales par l'Observatoire du vote[6]. Parmi les résultats, les auteurs ont mit en lumière le fait que certains bureaux de vote, intégrant des machines à vote, avaient un écart de 29,8% entre le nombre de votes effectués et les signatures des citoyens qui se sont rendus aux bureaux de vote. À titre de comparaison, cet écart s'élevait à 5,3% pour les bureaux de vote classiques.

DES VULNÉRABILITÉS CONNUES

Au-delà des aléas techniques, de nombreuses études pointent également les vulnérabilités inhérentes au fonctionnement des machines à vote. On peut par exemple citer le cas de l'état de Géorgie[7] dont les machines **Dominion Voting System** ont été analysées par July Alex Halderman, chercheuse à l'université du Michigan. Cette dernière a démontré l'existence de vulnérabilités. Par exemple, il était possible, avec un accès physique, d'installer un malwarepermettant de changer le vote des citoyens le jour J.

Dès lors, le malware interfèrerait entre le moment où l'électeur effectue son choix sur l'écran tactile et le moment où la machine imprime le reçu, sous forme de QR-code incompréhensible pour un œil humain.

La compromission d'une seule machine à la fois rendrait un détournement des votes à grande échelle fastidieuse. Néanmoins, la démonstration illustre les dérives permises par ce genre d'appareils. À noter que ce modèle de machines était alors présent dans 12 états dont la Californie, le Michigan et le Missouri. Au vu des problèmes mentionnés ci-dessus, nous pourrions nous demander quelle est l'ampleur de la menace en France ? A priori, elle serait réduite.

UN RÔLE LIMITÉ DES MACHINES À VOTE EN FRANCE

« Quels pays en utilisent ? »

D'après le site d'information Jagranjosh[8], en 2020 il y avait 12 pays qui utiliseraient les machines à vote de façon pérenne. Parmi ces pays, 4 l'utilisaient à l'échelle nationale, il s'agit de l'Inde, du Bhoutan, du Brésil et du Venezuela. Aux échelons inférieurs, on comptait 8 pays dont : la Belgique, la France, les États-Unis, le Canada, le Mexique, le Pérou, l'Argentine et le Japon. Certaines nations ont testé le dispositif et l'ont abandonné. Parmi ces pays, on peut citer l'Australie, la Norvège, l'Allemagne ou encore le Royaume-Uni.

Il semblerait donc que ce ne soit pas le niveau de développement du pays qui détermine la position de ce dernier vis-à-vis des machines à vote. Le blocage semble résider dans le rapport à la transparence du vote. Les machines à vote ont en effet un fonctionnement difficile à comprendre pour les citoyens et ne laissent pas de « traces » sur un papier. Cela représente, aux yeux de nombreuses autorités, une menace pour la démocratie. S'appuyant sur ce constat, la Cour Suprême allemande a déclaré l'utilisation des machines à vote anticonstitutionnelle en mars 2009[9].

Vote à distance et sabotage des infrastructures.

UN CONTEXTE SANITAIRE ET DÉMOCRATIQUE/ SOCIÉTAL FAVORABLE AU E-VOTE

« Peu de français ont accès au vote en ligne »

Aujourd'hui, le code électoral stipule que les élections par internet ne concernent que les citoyens français résidant à l'étranger, et ce uniquement dans le cadre des élections législatives et consulaires[10]. Cela représente 1,4 million de citoyens soit une faible partie de la population. De plus, en 2017 le gouvernement avait décidé d'annuler le vote en ligne en raison de la menace de cyberattaques notamment russes[11].

Or, comme mentionné précédemment, les Français et notamment les jeunes générations sont favorables à une généralisation du vote en ligne.

C'est davantage du côté de la classe politique que le bât blesse. En effet, dans l'imaginaire collectif, l'élection présidentielle est un moment solennel dans la nation. L'acte de voter ne peut dès lors pas être réduit à un simple clic comme on achèterait un article en ligne. Néanmoins, l'actualité récente risque de renforcer la demande des citoyens d'une plus grande place du numérique dans le processus électoral.

« La crise du Covid-19, une aubaine ? »

À ce titre, la crise du Covid-19 et la généralisation des gestes barrières ont été d'excellents arguments en faveur du vote en ligne.

De fait, le report du second tour des élections municipales, à la suite du confinement, a créé un délai de 3 mois entre les deux tours. De nombreux observateurs ont alors dénoncé un dévoiement de la campagne avec des résultats illégitimes[12].

Si le vote avait été numérisé, on peut imaginer que de nombreux électeurs, ne souhaitant pas risquer d'être contaminés, auraient pu voter depuis chez eux. Le vote électronique pourrait donc octroyer une plus grande résilience au système électoral français.

LES PROBLÉMATIQUES ASSOCIÉES À LA CONNEXION PERMANENTE À INTERNET ET AUX VULNÉRABILITÉS EXISTANTES

« L'existence de nombreuses vulnérabilités »

Tout comme les machines à vote, les logiciels et bases de données qui sous-tendent le vote en ligne sont vulnérables. La principale différence est qu'une plateforme de e-vote est reliée 24h/24 à Internet.

Pierrick Gaudry, chercheur du CNRS, a participé en 2019 à une compétition visant à améliorer le vote en ligne russe[13]. Un organisme de surveillance des élections avait publié un faux jeu de données chiffrées contenant les votes des électeurs ainsi que la clé publique et proposait aux volontaires de tenter de déchiffrer les données. Le chercheur français a déclaré avoir réussi en 20 minutes à l'aide d'un ordinateur standard et de logiciels disponibles en **open source**.

Cet exemple, quelque peu simpliste, illustre néanmoins la facilité avec laquelle une plateforme de vote pourrait être compromise.

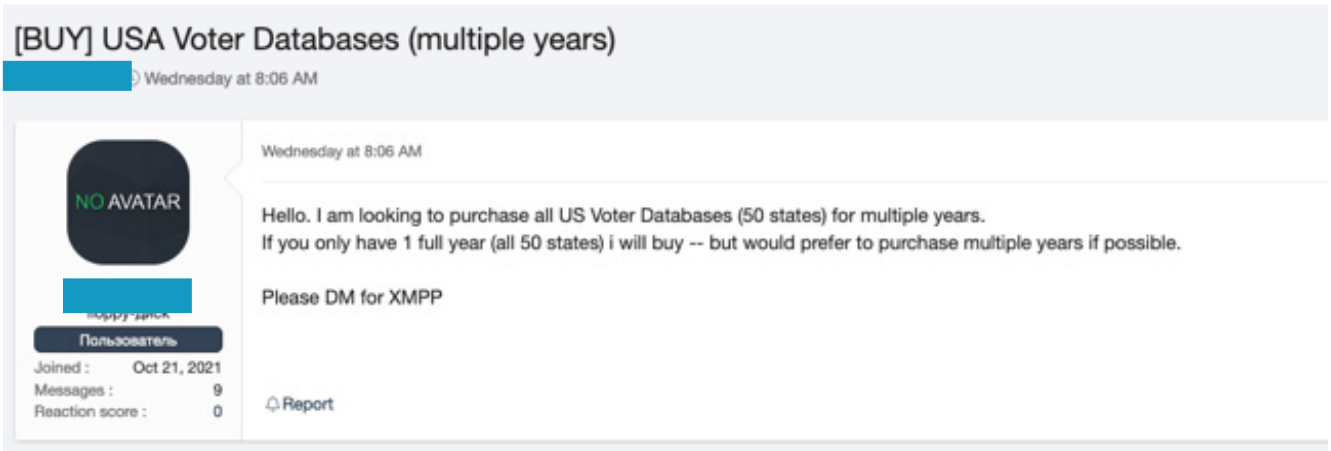
Sur le plan de la traçabilité, le vote en ligne pose également question. Le fait que les votes ne soient pas imprimés au fur et à mesure ne permet pas aux autorités de les suivre de façon optimale et ne permet pas non plus une comparaison entre les données entrantes et les résultats finaux. Tout est dématérialisé et en cas de compromission du compte administrateur de la plateforme, il est très compliqué d'effectuer des contrôles a posteriori.

« *Un intérêt croissant pour les bases de données électorales* »

Sur le plan de la traçabilité, le vote en ligne pose également question. Le fait que les votes ne soient pas imprimés au fur et à mesure ne permet pas aux autorités de les suivre de façon optimale et ne permet pas non plus une comparaison entre les données entrantes et les résultats finaux. Tout est dématérialisé et en cas de compromission du compte administrateur de la plateforme, il est très compliqué d'effectuer des contrôles a posteriori.

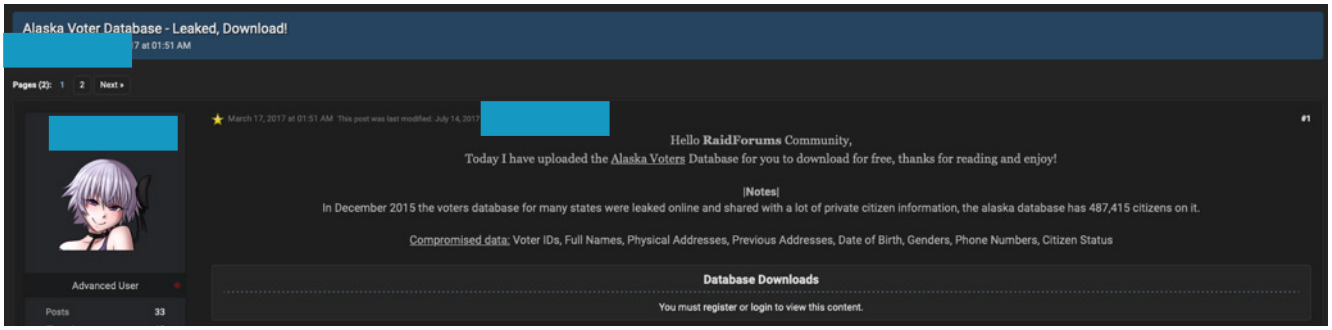
On sait que des centaines de bases de données sont régulièrement achetées et vendues sur des forums du Deep et Dark Web. Les bases de données des électeurs ne font pas exception. De fait, les cybercriminels et les organisations adossées à des États y voient des intérêts multiples dont :

- La valeur pécuniaire des données personnelles de nombreux citoyens ;
- La possibilité de faire pression sur un État en menaçant de publier les données ;
- La possibilité de mener des opérations de désinformation pour influer sur le cours d'une élection.



Aperçu d'un forum russophone dont un membre souhaite acheter des bases de données d'électeurs américains

Les adresses email des partis politiques impliqués dans une campagne électorale sont également des cibles de choix. C'est ce qu'illustrent les attaques par phishing, vraisemblablement russes, à l'encontre de membres du Parti Démocrate américain et de proches d'Hillary Clinton en 2016[14]. L'objectif était d'obtenir des informations confidentielles et de nuire à l'image de la candidate avant le jour des élections. À ce titre, on peut aussi citer le cas connu des « MacronLeaks ». Ces données, en partie obtenues via la compromission d'adresses email de collaborateurs du candidat Emmanuel Macron en 2017, avaient le même objectif.



Aperçu d'un forum anglophone dont un membre publie la liste des électeurs de l'état d'Alaska

UN NIVEAU DE RISQUE MAJEUR POUR LES ÉLECTIONS FRANÇAISES FUTURES

« Une utilisation croissante du vote en ligne pour les primaires »

Dans le cadre de la campagne présidentielle de 2022, des votes par internet ont été organisés pour les primaires écologistes en septembre 2021, pour les primaires républicaines en décembre de cette même année ainsi que pour la primaire populaire à gauche fin janvier 2022[15].

À l'exception des Républicains, les primaires étaient ouvertes à tous. Il suffisait de fournir des informations telles qu'un numéro de téléphone et de carte bancaire afin de vérifier l'identité du votant.

Les trois scrutins ont eu recours à la plateforme Neovote. Il s'agit d'une entreprise française spécialisée dans le vote en ligne et certifiée par le Conseil d'État, le Sénat, l'Assemblée nationale, le ministère de l'Intérieur et la Direction Générale de la Sécurité Intérieure *(DGSI)*.

L'entreprise a mis en place des mesures pour lutter contre la fraude massive et notamment issue de l'étranger. Par exemple, dans le cas de la primaire populaire, chaque personne souhaitant s'inscrire devait renseigner :

- Nom
- Prénom
- Adresse email
- Code postal *(optionnel)*
- Carte bleue *(seule l'empreinte est conservée par Neovote)*

Toutefois, des journalistes ont réussi à prouver l'existence de solutions de contournement à l'aide d'une carte bancaire virtuelle. On pourrait ainsi craindre que des acteurs malveillants n'interfèrent dans ces scrutins en ligne. Dès lors, le ou la vainqueur de la primaire, censé être légitime pour se présenter à l'élection présidentielle, risquerait de ne plus l'être, semant ainsi le désordre.

Il existe toutefois des solutions telles que l'utilisation d'un jeton à usage unique pour chaque électeur ou encore la division d'une clé privée entre les différents administrateurs de la plateforme.

« Un enjeu réduit dans le cadre du scrutin présidentiel mais qui pourrait le devenir à l'avenir »

Les enjeux en matière de vote en ligne sont faibles pour l'élection présidentielle de 2022. Toutefois, il ne faut pas perdre de vue que d'autres problèmes pourraient émerger dans un avenir proche.

Premier problème, dans le cas où l'ordinateur d'un citoyen aurait été compromis par un malware de type **Remote Access Trojan** (***RAT***). Un attaquant pourrait modifier le vote du citoyen, et ce sans que ce dernier s'en rende compte.

Second problème, la vérification de l'identité du votant demeure incomplète. Comme illustrées précédemment, des techniques de contournement demeurent. Le cadre juridique européen en matière de données personnelles avec le RGPD empêche les plateformes d'exiger trop d'informations pour vérifier l'identité de la personne.

Troisième problème, le cas où la personne qui vote en ligne subit une pression extérieure lors de son vote. Dans les bureaux de vote, l'isoloir est une garantie pour chaque citoyen que son scrutin est libre et secret. Il est très difficile de garantir ces deux conditions dans le cadre d'un vote par internet.

Enfin, un dernier problème serait de nature technique. Si l'on espère 48 millions de citoyens connectés sur une seule plateforme le même jour[16] une attaque par **Déni de Service Distribué** (***DDoS***) pourrait venir perturber les élections. Ainsi, il faudra que l'infrastructure qui centralise les connexions soit suffisamment stable pour permettre le bon déroulement du scrutin…

Remerciements :

Charlène GREL
Nicolas RAIGA-CLÉMENCEAU
et Paloma SIGGINI

(Sources, pages 2 à 8) **S'EN PRENDRE DIRECTEMENT AUX CAMPAGNES POLITIQUES**

(1) https://www.theguardian.com/world/2019/jan/08/germany-data-breach-man-held-in-suspected-hacking-case
(2) https://wikileaks.org/macron-emails/
(3) https://www.lemondeinformatique.fr/actualites/lire-piratage-de-tv5-monde-la-piste-russe-se-precise-61430.html
(4) https://apnews.com/article/technology-business-ap-top-news-france-hacking-b605ac78b54549d092dd9dfea32dfd9a
(5) https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf
(6) https://www.silicon.fr/en-marche-macron-cible-phishing-services-russes-172979.html#comments-172979
(7) https://www.francetvinfo.fr/politique/emmanuel-macron/video-mounirmahjoubi-patron-de-lacampagne-numerique-d-emmanuel-macron-le-macronleaks-ca-pue-la-panique_2180759.html
(8) https://cybersecurity.att.com/blogs/labs-research/macronleaks-a-timeline-of-events
(9) https://en.wikipedia.org/wiki/List_of_data_breaches
(10) https://www.theguardian.com/technology/2017/jun/23/russian-hackers-stole-passwords-of-british-mps-and-public-servants
(11) https://www.spiegel.de/netzwelt/web/passwortdatenbank-ermoeglichte-promi-hack-a-a5330335-8fd0-4d65-b358-8d88750fbd45
(12) https://www.marianne.net/politique/droite/protonmail-telegram-signal-comment-lequipe-zemmour-tire-les-lecons-des-macronleaks

(Sources, page 9 à 16) **LES ENJEUX AUTOUR DU VOTE ÉLECTRONIQUE**

(1) https://en.wikipedia.org/wiki/Voting_machine
(2)https://itif.org/files/evoting.pdf
(3)https://www.npr.org/2016/03/10/469843340/voting-machines-could-again-take-center-stage
(4)https://www.justice.gov/crt/help-america-vote-act-2002
(5)https://edition.cnn.com/videos/business/2019/08/10/voting-booth-hack-def-con-orig.cnn-business
(6)« Vote electronique - Elections présidentielles et législatives 2007 municipales et cantonales 2008 » Chantal Enguehard, Observatoire du vote, 8 juillet 2008
(7)https://www.govtech.com/security/report-hackers-can-flip-votes-in-georgias-voting-system
(8)https://www.jagranjosh.com/general-knowledge/which-countries-use-electronic-voting-machines-1548418168-1
(9)https://www.thequint.com/news/politics/reasons-for-evm-bans-aap-expose
(10) https://www.service-public.fr/particuliers/vosdroits/F16904
(11) https://www.ouest-france.fr/elections/legislatives/crainte-de-cyberattaque-pas-de-vote-electronique-pour-les-legislatives-4839515
(12) https://www.lagazettedescommunes.com/749562/municipales-2020-le-juge-de-lelection-face-au-covid-19/
(13) https://www.cnrs.fr/fr/test-du-vote-en-ligne-moscou-une-faille-de-securite-decouverte-par-un-chercheur-du-cnrs
(14) https://apnews.com/article/technology-europe-russia-hacking-only-on-ap-dea73efc01594839957c3c9a6c962b8a
(15) https://www.numerama.com/politique/829983-le-vote-en-ligne-de-la-primaire-populaire-est-il-securise.html
(16) https://www.lemonde.fr/les-decodeurs/article/2021/06/25/le-vote-electronique-remede-a-l-abstention-comprendre-le-debat-qui-agite-l-entre-deux-tours-des regionales_6085744_4355770.html

À propos de

serenety
By xmco

Créé en 2010, Serenety est un service de Cyber Threat Intelligence, développé par le CERT-XMCO et à destination des organisations publiques et privées. Son objectif est d'identifier la surface d'attaque et la surface d'exposition des organisations surveillées au travers d'un outil simple d'utilisation et ergonomique. Il se distingue de ses concurrents par la corrélation de ses résultats issus des analyses automatiques des sources ouvertes surveillées et des investigations manuelles de son équipe d'experts qualifiés. Cette surveillance permet d'identifier les menaces et d'anticiper les risques notamment liés aux fuites de données, aux systèmes exposés et vulnérables ou encore à la compromission de comptes.

xmco

Cabinet de conseil indépendant en cybersécurité, XMCO a à cœur d'accompagner ses clients, de toute taille et de tous secteurs, dans l'anticipation des vulnérabilités, la détection des failles et la réponse à incidents. XMCO est qualifié PASSI sur l'ensemble des portées, ce qui confirme le cœur de métier historique : l'audit et les tests d'intrusion.

Retrouvez-nous

Sur notre site :

www.xmco.fr

Sur les réseaux sociaux :

Envie d'échanger ?

sales@xmco.fr

01 79 35 29 30