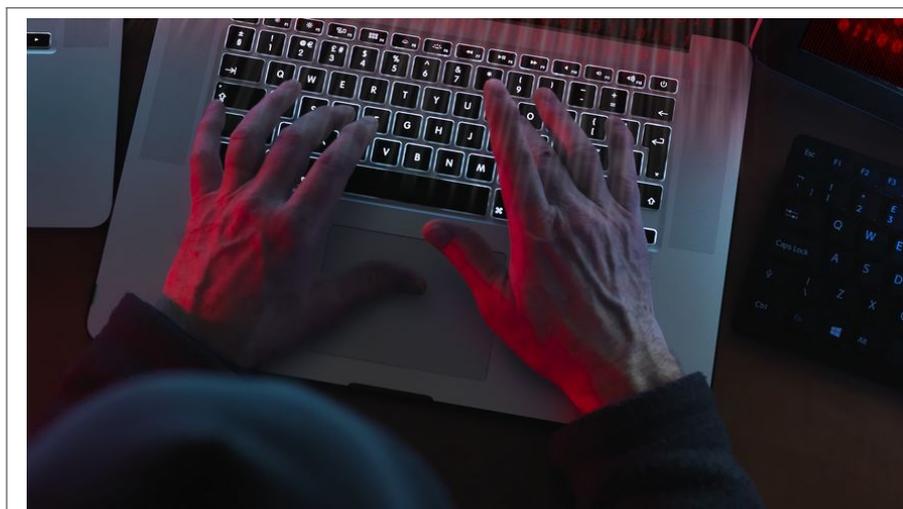


Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle



Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle

Elles ont beaucoup fait parler d'elles durant la campagne présidentielle américaine : certaines pratiques malveillantes sur Internet pourraient aussi peser sur l'élection en France. Voici en quoi elles consistent.

Interview par Marina Cabiten (France Bleu)

Des pirates informatiques qui œuvrent contre Hillary Clinton, et donc en faveur de Donald Trump, le tout commandité par le Kremlin : il ne s'agit pas d'un scénario de film mais d'une accusation très sérieuse formulée par les autorités américaines lors de la campagne présidentielle. Internet est un outil puissant pour les manipulations informatiques, à différents degrés. Et la France est, selon plusieurs acteurs de la cybercriminalité, très mal préparée à ces usages détournés. Voici comment des personnes mal intentionnées pourraient perturber la campagne.

Inonder les réseaux sociaux de faux utilisateurs : l'astroturfing

Tout un chacun peut utiliser son compte Facebook ou Twitter pour s'exprimer, et éventuellement partager ses opinions politiques. Mais cette utilisation des réseaux sociaux peut être bidonnée. Ce phénomène est appelé astroturfing, du nom d'une marque de pelouse synthétique pour les stades : Astroturf. Autrement dit, il s'agit de faire prendre aux internautes du faux gazon pour de l'herbe naturelle... Comment ? **En inondant les réseaux sociaux de faux comptes automatisés, les "bots"**, qui diffusent des messages rédigés par les initiateurs de cette technique de "marketing politique" qui ne dit pas son nom, et garantit l'anonymat.

N'importe quel internaute peut créer et animer des faux comptes. Avec un peu plus de moyens financiers, il peut payer pour qu'un réseau social comme Facebook donne plus de visibilité à une page ou à un post via un algorithme qui fera apparaître le message sur davantage de "murs" d'utilisateurs, qui n'ont rien demandé. Sur Twitter, il peut acheter des "followers" (personnes qui suivent le compte) pour donner une fausse légitimité à ses comptes artificiels. Le degré ultime est de se payer un logiciel qui fait ça tout seul, voire d'employer quelqu'un pour l'exploiter. Cela existe, au sein d'entreprises privées mais parfois aussi de partis politiques. **C'est une forme de propagande de plus en plus répandue.** Le gouvernement français a annoncé récemment son intention de surveiller les réseaux sociaux pour éventuellement repérer des "mouvements" suspects de ce type.

Quand des sites partisans se font passer pour des organes de presse : les « fake news »

L'expression "Fake news", qui se traduit littéralement par « fausses informations », est très en vogue depuis la présidentielle américaine et vient de la diffusion sur Internet de prétendus articles de presse, qui ne sont en réalité pas rédigés par des journalistes. Des articles contenant des informations non vérifiées, parfois erronées, voire carrément mensongères dans le but bien précis de manipuler l'opinion.

La mécanique est la même que pour l'astroturfing, tout faire pour que ces "fake news" soient largement vues sur Facebook et les autres réseaux sociaux ou forums. Selon les calculs du site BuzzFeed, les articles relayant de fausses informations (comme le **faux soutien du pape François à Donald Trump, ou la révélation imaginaire de ventes d'armes par Hillary Clinton à l'organisation Etat islamique**) ont suscité 8,7 millions d'interactions sur Facebook durant la campagne américaine, contre 7,3 millions pour les articles de la presse traditionnelle.

En France récemment, plusieurs médias ont fait part de leur volonté de lutter contre ce phénomène, allant même pour certains jusqu'à nouer un partenariat avec Facebook et Google. **"Le problème c'est que la rumeur court toujours beaucoup plus vite que la rectification ou la suppression du contenu"**, objecte Denis Jacopini, diplômé en cybercriminalité et sécurité de l'information, **"laissant s'installer dans l'esprit de l'électeur ces fausses affirmations."**

De vrais contenus, mais dérobés et diffusés sans autorisation : le vol de données

La menace la plus sophistiquée reste le vol d'informations numériques. C'est l'exemple des pirates informatiques (hackers) qui ont récupéré près de 20.000 courriels de responsables du parti d'Hillary Clinton. Ils sont entrés dans les serveurs du parti démocrate dès l'été 2015, accumulant ces données parfois embarrassantes sans que personne ne s'en aperçoive, pour les publier au moment opportun pour déstabiliser le camp démocrate. Une cyberattaque venue de Russie pour aider Donald Trump à gagner l'élection, affirme la CIA dans un rapport révélé par la presse américaine. **"Aucun parti politique français n'est actuellement protégé contre une telle malveillance"**, assure Denis Jacopini.

Selon le Canard Enchaîné (numéro du 8 février 2017), **les services secrets français s'inquiètent de cyberattaques russes** durant la Présidentielle, qui auraient pour but d'aider la campagne de Marine Le Pen. De son côté, le secrétaire général du mouvement « En Marche ! » Richard Ferrand a affirmé publiquement que les pirates russes visent particulièrement Emmanuel Macron et ont déjà attaqué à plusieurs reprises son site web.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Source : *Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle*