Cyberdéfense et sécurité digitale : Sommes-nous à l'abri?

Autor(en): **Snene, Mehsi**

Objekttyp: **Article**

Zeitschrift: **Bulletin / Vereinigung der Schweizerischen Hochschuldozierenden = Association Suisse des Enseignant-e-s d'Université**

Band (Jahr): **45 (2019)**

Heft 1

PDF erstellt am: **21.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-893934

Cyberdéfense et sécurité digitale: Sommes-nous à l'abri?

Mehdi Snene*

1. Introduction

L'année 2019 a débuté avec une vague de cyberattaque qui a ciblé majoritairement l'Europe et en particulier les grands groupes européens. L'avionneur Airbus s'est fait subtilisé une masse informationnelle de son personnel opérant via une porte dérobée située chez un de ses sous-traitants qui était moins sécurisé que le système d'information interne d'Airbus. L'attaque présentée comme l'œuvre du groupe APT10 appartenant «au conditionnel» à l'armée cybernétique populaire de Chine visait selon les premières conclusions de l'enquête les secrets industriels de fabrication de l'avionneur Européen. Une observation attentive des données dérobées et des moyens mis en œuvre pour orchestrer l'attaque ne semble pourtant pas étayer ces premières conclusions. Au vu de l'effort et des montants engagés pour la mise en place de l'attaque, il serait plus opportun de statuer sur l'importance des données pour la mise en place tactique d'une seconde manche d'attaque plus redoutable basée sur une approche de «social engineering». Cette approche basée sur la soustraction directe des informations en mode sociale, nécessite que se joignissent différents champs d'études allant de la sociologie, psychologie, informatique à l'électronique.

Ce modèle d'espionnage par infiltration et devenu un «modus operandi» perfectionné et répandu. Utilisé durant la première décennie par les «internet lovers», ce mode d'approche s'est professionnalisé et militarisé pour devenir l'approche de référence utilisée lors de la préparation d'attaque d'infiltration ou même de piratage directe. En reconstituant la liste du personnel, il devient plus évident de détecter les failles humaines internes à l'entreprise, déterminer les modes d'approches adéquats, et travailler la cible au corps. Pour un gouvernement, détecter ce genre de faille humaine en interne doit se faire en mode continu et surtout avant que cette cible ne soit listée par des attaquants malintentionnés. Toute la problématique de la cyberdéfense prend alors une dimension exponentielle en terme de complexité car rien ne sert de s'équiper des meilleurs dispositifs de sécurité si on finit par ouvrir la porte à notre insu aux assaillants. L'Allemagne vient d'en faire l'amer expérience avec un vol massif de données appartenant à des acteurs politiques, au gouvernement fédéral et à différents partis politiques, une attaque perpétrée par un jeune allemand de 20 ans vivant encore chez ses parents et entièrement mis en place à partir de sa chambre et non pas la Russie ou la Chine tel qu'annoncé au début.

Avec l'augmentation du nombre de dispositifs mobiles utilisés en entreprise, et avec elle la quantité de données qui transitent entre les différents points d'entrée des systèmes d'information, assurer la sécurité informatique, surtout des infrastructures critiques, se complexifie de jour en jour et requiert une constante évaluation et détection des risques. La robotisation croissante des entreprises entrainera la même problématique de sécurité qu'ont connu les entreprises avec l'adoption massive des systèmes numériques et des réseaux ouverts. Ces systèmes n'étaient presque jamais conçus en considérant l'aspect sécurité imbriquée mais étaient souvent sécurisés au fur et à mesure de la détection des failles ou après avoir subi des cyberattaques ce qui les rendaient systématiquement vulnérables face à toute nouvelle découverte de brèche. Ce retard en sécurité a entrainé un accroissement rapide des attaques et des dégâts occasionnés. La robotisation connait également un modèle de conception et de développement qui ne prend pas ou pas assez l'aspect sécurité comme élément fonctionnel essentiel pour ces plateformes robotiques. Ces dernières années, des voitures autonomes, plateformes robotisées des centrales nucléaires, drones et même des jouets robots se sont fait pirater. Tous ces objets peuvent devenir potentiellement dangereux tant au niveau confidentiel avec la divulgation de données que fonctionnel avec une utilisation non conventionnelle.

Malgré tous les efforts pour sécuriser nos infrastructures informatique et robotique, des failles persistent à tous les niveaux humains, hardwares, softwares

* Université de Genève, Battelle Bat A, Route de Drize 7, 1227 Carouge.

E-mail: *mehdi.snene@unige.ch*

Mehdi Snene, Maître d'Enseignement et de Recherche, Centre Universitaire d'Informatique de l'Université de Genève. Ancien Auditeur de sécurité Informatique dans des institutions Financières et fondateur de l'Observatoire Suisse de Cyberdéfense. Il enseigne la sécurité des Systèmes d'information et la gestion de cyber risque à l'Université de Genève. Il a dirigé plusieurs missions d'Ethical hack pour des entreprises et des organismes suisses.

et fonctionnels et ça risque d'empirer rapidement. Mais pourquoi devons-nous nous attendre à une déferlante d'attaques de plus en plus destructrices et facile à mettre en œuvre et comment construire une approche de cyberdéfense anticipative?

2. La prolifération d'infrastructures tactiques de cyberattaque

Le cours du Bitcoin s'est effondré subitement fin 2017 après avoir atteint un sommet historique avoisinant les 20000 USD. Les annonces de plusieurs groupes financiers de l'intégration de la cybermonnaie dans leurs stratégies d'investissement étaient généralement accompagnées d'une prolifération de ferme de minage de travers le monde. 70% des fermes de minage sont en Chine et la plus grande ferme est en Russie. Les coûts de minage et d'investissement initial pour la mise en place de cette infrastructure ne sont que partiellement couverts par le nombre de bitcoin généré au vu de leur prix actuel. On estime que chaque bitcoin produit et vendu à moins de 3600 USD coûte en moyenne aujourd'hui 4700 USD. Il n'est clairement pas ou peu profitable de continuer à produire mais malgré ça nombre de ces fermes continuent à se développer à travers le monde fournissant une puissance de calcul totalement mise en réseau et partagée.

Mais pourquoi parle-t-on du Bitcoin dans le contexte de cyber défense? Simplement parce que derrière les bitcoins, l'infrastructure technique qui exploite la technologie Blockchain est une infrastructure de pointe assurant une puissance de calcul basée essentiellement sur des processeurs de cartes graphiques qui rivalisent avec les plus grandes infrastructures d'hypercomputing qui existent aujourd'hui. Ces fermes de minage attisent aujourd'hui plusieurs intérêts géostratégiques et ont favorisé l'apparition d'un partenariat inédit PPP (« Private Public Partnership ») entre les détenteurs de ces fermes et les Etats qui les hébergent. En effet, ce genre d'infrastructure représente une infrastructure facilement exploitable pour mener une cyberattaque de différents types (« Distributed Deny of Service, DDoS », « Brute Force », ...). Ce genre d'attaque qui se basait jusque-là sur les réseaux dormants (machine zombie infectée par un virus ou un cheval de Troie à l'insu de son propriétaire et réquisitionnée au moment de l'attaque) possède dès lors une infrastructure largement supérieure en terme de puissance de calcul que les réseaux dormants. L'esquisse de différents scénarios d'attaque DDoS futures est facilement imaginable: une attaque de plateforme de vote électronique le jour d'une votation, l'attaque d'un système financier le jour d'une annonce majeure, d'infrastructure d'urgence (Hôpital, PC de gestion de crise...) et finalement des attaques de types commerciales (ciblant prioritairement les entreprises dont le «front end» est entièrement digitale tel que Easyjet ou les banques sur internet). Microsoft a ainsi mis en garde l'Union européenne contre une recrudescence de cyberattaques, notamment russes, après avoir détecté une série de tentatives de piratage à quelques mois des élections européennes (03-03-2019).

3. La déstabilisation informationnelle

La désinformation a récemment atteint des sommets en Inde et représente une menace pour les législatives prévues du 11 avril au 19 mai selon son gouvernement. Les principales plateformes de réseaux sociaux – Facebook, WhatsApp, Twitter, Google et Share Chat se sont engagées à ne diffuser que les publicités politiques déjà validées par la Commission électorale. Cette mesure de surveillance et d'encadrement pour la diffusion d'information vise principalement les sources classiques de diffusion (les partis politiques, les candidats aux élection) et vise à contrôler le message diffusé par voie publicitaire. La compréhension du phénomène de «fake news» et par ricochet de l'ingérence de tiers (pays étrangers, candidat adverse, lobby...) dans la perception des électeurs est totalement faussée par le gouvernement indien et nécessite une plus ample investigation. Peut-on réellement limiter la propagation des «hoax» (l'ancienne nomenclature utilisée pour désigner les «fake news» et généralement utilisée dans la terminologie de sécurité informatique). Pour mieux cerner ce phénomène il faudra examiner le cycle de vie d'un hoax en spécifiant son émetteur, le message véhiculé et le groupe de destinataire. Les émetteurs ne sont que très peu visibles généralement et se cachent derrière des médians électroniques de très grande diffusion. Ils ne sont généralement pas ou très peu affiliés aux groupes politiques ou autres même s'ils en adoptent leurs thèses. Leur stratégie est en tout point semblable à des stratégies financières de «Pump and Dump». Cette stratégie visait à propager une fausse information dans des groupes de larges audiences (ou par SPAM) annonçant des hausses spectaculaires attendues des prix de certaines actions sur les marchés financiers. Auparavant les annonceurs ont constitué un portefeuille de ces actions et au moment où les personnes touchées par le hoax commencent à affluer pour acheter les actions, le prix à la revente augmente et les annonceurs liquident leurs positions initiales. Ce schéma qui se répète aujourd'hui mais avec des fins géostratégiques, exploite en fait la même faille: la faille humaine et son raisonnement irrationnel.

Le plus dur dans cette stratégie était de déterminer le groupe réceptionnaire du message. En effet, il faut que ce groupe ait les prédispositions ethniques, re-

ligieuses, financières et sociales pour être réceptive aux messages. Les grandes plateformes de diffusion numériques se sont chargées de développé des algorithmes de profilage disponible aux grands publics qui ne demandent finalement qu'à être utilisés pour une sélection ultra ciblée. Les recommandations des vidéos sur Youtube, des amis sur Facebook ou des articles qui peuvent vous intéresser sur Google sont devenus le socle de base de toute action de cyber désinformation qui vise un ensemble d'individus reliés par un trait commun aussi infime soit-il. Pire encore, une récente étude sociologique qui s'est intéressée de près à ces algorithmes a conclu que ce système de recommandations est le premier moyen d'isolement et de confrontation cognitive. En effet à force de se voir proposer que des informations (vidéos ou articles) qui correspondent à nos centres d'intérêt, la conviction que la terre est plate, que le vaccin est à l'origine de l'autisme et autres croyances ne font que s'amplifier vu que les groupes de personnes ne se verront proposer que des informations émanant de personnes qui partagent les mêmes croyances. Dès lors la notion de désinformation s'amplifie vu qu'on prive le groupe d'individus d'accéder facilement aux informations qui infirment leurs thèses ou informations erronées de départ. Appliqué à la géopolitique, une menace de désinformation électorale est certainement à prévoir dès lors que des intérêts économiques ou stratégiques peuvent être en jeu.

4. La Cyber Défense en Suisse

La Suisse vient de se doter de sa première école de cyberdéfense intégrée au sein de l'armée. Comparé aux 140000 membres de l'APT10, un retard reste à combler rapidement afin d'assurer notre autonomie défensive en cas de guerre cybernétique. Malgré les efforts croissants de formation en sécurité informatique et cyber défense en Suisse et ailleurs dans le monde, les attaques cybernétiques risquent fort probablement de s'intensifier et de venir perturber le déroulement des cycles démocratiques ordinaires. En effet, la différence entre les politiques de cyberdéfense menées en Europe et celles menées dans des pays tel que la Russie, la Turquie ou la Chine se situe au niveau de la mission stratégique confiée à leurs cyber armées. Au lieu de se contenter de se défendre, la plupart des grandes cyber armées sont en train de mener des attaques exhaustives parfois uniquement pour tester leurs capacités offensives et qui nous rappellent fortement les manœuvres tactiques qu'opéraient les armées conventionnelles. Dans cette perspective, et avec la panoplie d'attaque qui ne cesse d'augmenter, se préparer uniquement à se défendre sans prendre en considération la mise en place d'une stratégie de cyberdéfense tournée plutôt vers l'offensive et centrée humaine, cette défense risque de devenir rapidement obsolète et inefficace en cas d'une cyberattaque d'envergure.

Une première réflexion consistante pour l'établissement d'une politique de cyberdéfense qui conservera le principe de neutralité de la Suisse, serait des réaliser des attaques auto–immune. Le principe du «stress test» appliqué à la cyberdéfense et utilisé en environnement réel comme attaque auto-immune, permettra de rapidement déceler les failles internes et y remédier. La construction d'un «stress test cybernétique» nécessitera la mise en œuvre de cellules d'action composées d'architecture d'attaque qui permettra aussi d'imaginer la typologie et la composition des attaques futures. ■