N°3 - OCTOBRE/DECEMBRE 2024

CYBER-IT

LA CYBER EST UN MARATHON PAS UN SPRINT !

BELLINGCAT

Une agence de renseignement au service du peuple

LE COIN DES PROS

Comprendre la détection des signaux faibles

ENQUÊTE

Au coeur d'une enquête pour terrorisme

DOSSIER SPECIAL

INVESTIGATIONS NUMÉRIQUES

ENTREZ DANS L'UNIVERS DES SHERLOCK DU NUMERIQUE

@arnaud_leroy

Une question ? Un besoin ?
cyberit.magazine@gmail.com

EDITORIAL

Qui n'a jamais rêvé de vivre une enquête de police comme dans les séries que nous regardons ? Qui n'a jamais été frustré de ne pas pouvoir voir l'envers du décor lors de la conclusion d'une investigation ?

Dans ce troisième numéro de Cyber-IT Mag plongez dans une enquête de plusieurs jours retraçant les périples et les doutes d'une équipe de citoyens apportant leur aide au service des plus grandes agences de renseignements du monde comme Europol ou encore le FBI.

Vous en apprendrez plus sur l'ONG Bellingcat et sur son créateur, il nous expliquera comment il a su retrouver l'identité d'un manifestant qui avait commis un acte délictuel à partir d'une photo.

Connaissez-vous le BlockInt ? Non ? Parfait, deux experts du sujet nous guideront dans les méandres de ce vaste domaine !

Egalement, une nouvelle rubrique fait son entrée dans le magazine «Le coin des pros» qui sera l'antre des sujets plus techniques et plus pointus encore. Pour sa première apparition, nous ébaucherons le thème de la détection des signaux faibles.

N'oublions pas les incontournables interviews qui seront toujours de la partie.

Bonne lecture et surtout, bienvenue dans l'univers des Sherlocks du numérique !

Arnaud Leroy

Une campagne de Sponsoring Solidaire est en cours !

Le principe ? Vous voulez votre logo dans le magazine, vous souhaitez mettre en avant un projet via une publication ? Alors faisons le ensemble ! Vous donnez à une des associations choisies par le comité éthique de Cyber-IT et le tour est joué.

Tout le monde est gagnant, une action solidaire pour aider ceux qui en ont vraiment besoin ! (Plus d'infos sur la page de Cyber-IT) ou par mail)

En partenariat avec CyberVeille

SOMMAIRE

DOSSIER SPECIAL

DOSSIER SPECIAL

Investigations numériques

Entrez dans l'univers des Sherlock du numérique

L'investigation numérique, ou cyberforensic, est devenue un pilier incontournable de la cybersécurité moderne. À l'ère où les cyberattaques se multiplient et où les données numériques sont omniprésentes, la capacité à analyser et à interpréter les preuves numériques est essentielle pour protéger les systèmes d'information et garantir la justice. Les enquêteurs numériques sont les détectives du monde virtuel, utilisant des outils sophistiqués pour traquer les cybercriminels, reconstituer les événements et préserver l'intégrité des preuves.

Dans un contexte où les menaces évoluent constamment, l'investigation numérique ne se limite pas à la simple récupération de données. Elle englobe une série de processus complexes allant de la collecte et la préservation des preuves à leur analyse minutieuse et à leur présentation devant les tribunaux. Les professionnels de ce domaine doivent non seulement maîtriser des compétences techniques avancées, mais aussi posséder une connaissance approfondie des cadres légaux et réglementaires en vigueur.

Les outils utilisés dans l'investigation numérique sont variés et spécialisés. Des logiciels comme EnCase et FTK permettent de réaliser des analyses approfondies de systèmes informatiques, tandis que des outils comme Wireshark sont essentiels pour l'analyse du trafic réseau. Ces technologies permettent de découvrir des indices cachés dans des montagnes de données, de reconstituer des communications et de suivre les traces laissées par les cybercriminels.

Cependant, l'investigation numérique présente également des défis significatifs. La quantité de données à traiter peut être immense, et les enquêteurs doivent faire preuve de discernement pour distinguer les informations pertinentes des distractions. De plus, ils doivent constamment se tenir informés des nouvelles techniques et des évolutions technologiques pour rester efficaces face à des adversaires de plus en plus sophistiqués.

En somme, l'investigation numérique est une discipline dynamique et en constante évolution, essentielle pour la protection des infrastructures numériques et la lutte contre la cybercriminalité.

L'avenir de la cybersécurité repose en grande partie sur la capacité des enquêteurs numériques à déjouer les cybermenaces et à garantir la sécurité de nos données.

L'investigation numérique ne se limite pas aux affaires de cybercriminalité. Les données numériques sont omniprésentes dans notre quotidien et peuvent servir de preuves dans diverses enquêtes judiciaires. Les enquêteurs peuvent analyser des communications téléphoniques, des échanges de messages en ligne, des activités sur les réseaux sociaux, des emails, des historiques de navigation sur Internet, ainsi que des fichiers multimédias et bureautiques. Chaque élément numérique peut fournir des indices précieux pour établir les faits et identifier les auteurs d'infractions.

Nous allons entrer dans un univers complexe mais incroyablement captivant.
Stephanie Ladel, accompagnée de son acolyte StarMD (qui souhaite garder l'anonymat) vont revenir sur une enquête dont ils ont été les principaux acteurs.

A partir de presque rien, ils nous démontrent que l'on peut arriver à de grands résultats.
Ce ne sont pas les seuls à faire un travail de fourmis à l'instar de l'ONG Bellingcat ou encore des enquêteurs de l'OFAC et de tout autre corps de métiers des forces de l'ordre comme le FBI ou encore Europol.

Bienvenue dans l'univers des Sherlock du numérique !

Zoom sur Stephanie Ladel & StarMD de OSINT-FR

Je suis à la fois investigatrice et analyste, et mon matériel de prédilection est tout ce qui traîne et qu'on peut exploiter, autrement dit toute source disponible à celui qui y prête attention et voit quoi en faire. En bref, je fais de la recherche en OSINT en général, et en G E O I N T en particulier, c'est-à-dire en OSINT appliqué au domaine géospatial. Depuis début 2023 j'ai le plaisir de participer régulièrement aux travaux de Bellingcat.
Je co-anime aussi une communauté francophone et bénévole au sein du serveur d'OSINT-FR qui oeuvre à identifier et localiser des objets présents sur des scènes pédocriminelles jusqu'alors non-géolocalisées, au profit d'Europol , du Federal Bureau of Investigation (FBI) et de la Police Fédérale Australienne.
Je viens des sciences humaines et sociales, et c'est entre autres mon intérêt pour l'analyse de problèmes et la recherche d'une aide à la décision éclairée qui m'ont amenée à développer mes compétences dans ces disciplines. D'abord autodidacte, j'ai beaucoup progressé grâce à mes pairs en lisant leurs démonstrations ou leurs analyses, en me familiarisant avec les outils qu'ils utilisent, en relevant des défis qu'on appelle dans le milieu « CTF » (capture the flag), et en participant à des formations théorico-pratiques.

J'ai des missions courtes, comme la recherche de la localisation d'un rassemblement d'un groupuscule extrémiste à une date donnée, des missions de quelques semaines, comme la collecte d'informations sur différents réseaux sociaux, sites Internet et articles de presse en lien avec un trafic d'êtres humains, et des missions longues comme la démonstration de dommages à civils en Ukraine depuis l'invasion de la Russie en 2022 pour la reconnaissance de possibles crimes de guerres en justice.
D'une journée à l'autre je navigue dans des univers très différents, dans des projets qui n'en sont pas au même stade, qui ne requièrent pas les mêmes méthodes de travail... Mais ce qui est commun est ceci : je commence toujours par faire un tour d'horizon des sources d'information que je souhaite voir quotidiennement, mes horaires de repas peuvent être décalés parce que je suis happée par une recherche ou le peaufinement d'un rapport, et je sors avec une liste de tâches aussi longue pour le lendemain.

J'aime devoir allumer mon cerveau face au risque d'écueils, j'aime chercher même longtemps, j'aime trouver évidemment, mais j'aime aussi baigner dans le rappel que la mesure et le doute peuvent s'avérer cruciaux lorsqu'il s'agit de rendre intelligible ce qu'on trouve et ne trouve pas. Le moins plaisant est sans doute le type de matériel auquel on est confronté. Beaucoup de collègues ont été affectés par les horreurs qu'ils ont dû analyser, aussi faut-il rester individuellement et collectivement vigilants sur cet aspect du métier.

Stephanie Ladel

Dans notre groupe, j'utilise le pseudonyme StarMD. Je participe aux recherches en me spécialisant dans l'analyse technique et la retouche d'images.

J'ai un parcours plutôt scientifique et artistique. J'ai fait des études en école d'art et me suis formé ensuite aux logiciels de traitement graphique pour diversifier et automatiser ma production. Je suis passionné par la création sensible comme par la technique.
J'oscille entre des projets personnels et des commandes. Je travaille pour la presse et l'édition, je les aide par exemple à préparer les fichiers numériques pour l'impression, pour qu'ils obtiennent le rendu qu'ils souhaitent.

Je n'ai pas de journée type, je suis freelance et je travaille surtout à l'envie. Je peux faire une heure de travail quotidien comme quinze. Je ne prends cependant quasiment jamais de week-ends ni de vacances.
J'ai réussi au fil des ans à acquérir une quasi totale liberté de choix. Je peux me permettre de refuser les commandes qui ne me plaisent pas et je ne fais presque que des choses dont j'ai envie, au moment où j'ai envie. En contrepartie c'est une situation financièrement précaire, et je ne connais jamais mon planning à plus de trois mois à l'avance.

L'Osint est un puits sans fond de possibilités, toutes les compétences sont nécessaires. On apprend beaucoup de choses en pratiquant, et pas seulement de la technique. C'est aussi une fenêtre sur le monde.

StarMD

Co-auteur du sujet «35 jours d'investigation pour faire parler 2500 pixels»

35 Jours d'investigation pour faire parler 2500 pixels

Depuis plusieurs années, la communauté **OSINT-FR** a constitué une plateforme de recherches répondant à l'initiative d'**Europol "Trace an Object - Stop Child Abuse"**, étendues progressivement à l'initiative de même nom de l'Australian Federal Police et à l'Endangered Children Alert Program du **FBI**.

Lorsque toutes les autres pistes ont été épuisées, des images d'objets sont révélées au public par ces autorités, chacune constituant l'ultime indice qui pourrait révéler l'emplacement d'une scène découverte dans l'ordinateur d'un pédocriminel ou sur Internet.

Chaque jour, ces OSINTeurs bénévoles se retrouvent et échangent dans une catégorie entière du serveur Discord *(https://discord.com/invite/dWY9sWFKYD)*, qui comporte un salon pour chaque objet recherché.

Et une fois par semaine, ils se réunissent dans un canal vocal et continuent de partager leurs hypothèses, leurs meilleures pistes et leurs avancées.

Cette plateforme est constituée autour de quatre co-animateurs, une ligne directrice rédigée qui explique ce que vous devez savoir avant de vous plonger avec eux, et de nombreux volontaires venant apporter leur pierre à l'édifice.

« On a cherché ensemble. On a trouvé. Tellement fière de ce qu'on produit dans une communauté variée, respectueuse et motivée ! »

Stephanie Ladel
(Investigatrice chez OSINT-FR)

STOP CHILD ABUSE
TRACE an OBJECT

25 juillet 2023

26 juillet 27 juillet 4 août 7 août 18 août 24 août 25 août 27 août 28 août 28 octobre

Nous découvrons l'image de notre nouvel objet-cible parmi la salve que comporte la dernière mise à jour du site d'Europol, sur sa page Stop Child Abuse (https://www.europol.europa.eu/stopchildabuse). À chaque occurrence, ce sont les mêmes réflexes qui s'enclenchent.

Un coup d'œil général, une prise de note personnelle des premières pistes, et nous ouvrons les investigations sur notre serveur Discord car les idées fusent déjà et il faut les organiser.

Pour des raisons de protection des victimes, Europol prend soin d'effacer sur les images tout détail qui permettrait de reconnaître un individu et fournit uniquement des images fortement tronquées. Reste donc seulement une fraction d'objet, un détail de décor, le genre d'élément qui pourrait, dans le meilleur des cas, permettre de localiser une scène et de débloquer une enquête en suspens.

"School uniform" : c'est ainsi qu'Europol le décrit, ce sera donc le nom de notre investigation parmi les autres que nous ouvrons.

Ici : des bras de chemise blanche, le haut d'une cravate bleu vif barrée de deux bandes blanches et un gilet bleu marine comportant un écusson, probable emblème d'une école d'après la description d'Europol. Cet établissement existe, quelque part dans le monde, et nous avons pour but de le trouver à partir de cette unique image. La définition de l'image comprimée est basse, à peine cinquante pixels de côté pour le logo, mais il va falloir faire avec.

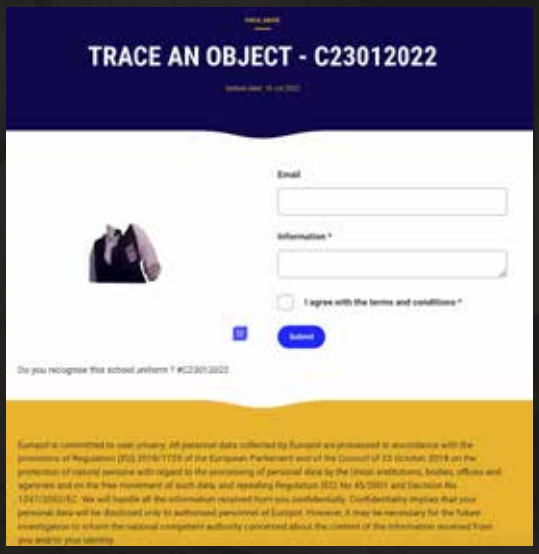


Photo de l'uniforme fourni par Europol
(https://www.europol.europa.eu/cms/sites/default/files/images/C23012022.png)

25 juillet

26 juillet 2023

27 juillet 4 août 7 août 18 août 24 août 25 août 27 août 28 août 28 octobre

Les pistes jaillissent depuis hier. L'arrivée d'une nouvelle série d'objets à identifier génère beaucoup d'activité dans notre communauté en ligne. Il nous faut au fil des jours mettre à plat nos théories, isoler les voies trompeuses, tout en nous assurant de ne pas passer à côté de notre cible. Pour le moment tout est possible, et il faut dire que dans ce genre de recherches, nous ne fermons jamais complètement les portes...

Nous commençons toujours par améliorer l'image dans la mesure du possible. Correction des couleurs, mise à l'équerre et agrandissement des zones d'intérêt ; il faut la rendre lisible sans perdre ou ajouter la moindre information. Nous exprimons aussi nos interprétations, définissons les choses que nous voyons, essayons de trouver un ou des terrains commun(s) d'interprétation.

Sur l'écusson, nous croyons d'abord voir un avion, la plume d'un stylo, puis un livre surmonté d'une torche, symbole du savoir.

Deux lettres sont également aperçues mais difficilement discernables. I K ? J K ?

Nous cherchons des significations potentielles. Le reste semble trop flou pour émettre une hypothèse solide.

Côté uniforme, la cravate nous semble vraiment signifiante. Ces deux bandes blanches sont peu communes, surtout portées très haut. Nous retrouvons rapidement des modèles similaires en Indonésie et en Inde, tant portées par des élèves qu'à plat sur des sites de fabricants ou de vendeurs.
Dans ce dernier pays, une région se nomme d'ailleurs Jammu and Kashmir. Jammu and Kashmir - J et K. Nous tenons notre première piste.

Et nous décidons de concentrer nos premières recherches sur cette zone géographique.

DOSSIER SPECIAL

25 juillet 26 juillet

27 juillet 2023

4 août 7 août 18 août 24 août 25 août 27 août 28 août 28 octobre

Les recherches autour de la région Jammu and Kashmir se poursuivent mais ne donnent pas encore de résultat convaincant. Hormis les manches longues de la chemise blanche, compatibles avec un climat montagneux, et le symbole de la flamme et du livre ouvert, rien ne rejoint vraiment nos interprétations.

Ce symbole est par ailleurs présent dans de nombreux pays, principalement en Asie et au Moyen Orient.

En parallèle, nous mettons au point des prototypes visuels que nous soumettons aux moteurs de recherche par image. C'est une technique qui complète bien la recherche textuelle, mais qui est assez chronophage.

Créer un prototype prend du temps et il en faut une version à chaque hypothèse. Avec une torche, une pointe de plume, différentes combinaisons de lettres... Nous ne sommes sûrs de rien.

Un de nos membres fait remarquer que la forme du blason ne ressemble pas à ce que nous retrouvons dans les écoles en Inde, mais malgré nos efforts pour ne rien laisser passer d'utile, le message est lu puis se perd dans le flux qui caractérise les premiers jours de l'investigation.

Etait-il trop tôt pour en juger ?

Sans le savoir, nous passons à côté d'une information précieuse.

« Voici la silhouette de l'écusson telle que nous la comprenons »

Stephanie Ladel
(Investigatrice chez OSINT-FR)

25 juillet 26 juillet 27 juillet

4 août 2023

7 août 18 août 24 août 25 août 27 août 28 août 28 octobre

Les premières pistes autour de l'Inde ne donnent toujours rien. Nous multiplions les prototypes et les recherches textuelles. Puis nous décidons d'élargir notre zone d'investigation.

La piste de l'Indonésie semblait elle aussi prometteuse mais nous manquons d'éléments tangibles pour confirmer cette intuition. Nous choisissons de balayer l'Asie dans son ensemble.

En parallèle de cet uniforme scolaire, nous cherchons à identifer une dizaine d'autres objets qui nécessitent souvent la même attention. Mais cet élargissement à l'Asie entière nous demande beaucoup d'énergie, qui ne sera pas mise dans les autres investigations.

25 juillet 26 juillet 27 juillet 4 août

7 août 2023

18 août 24 août 25 août 27 août 28 août 28 octobre

Nous trouvons des uniformes similaires dans de nombreux pays d'Asie. Mais si la coupe des vêtements correspond, le modèle précis de cravate nous échappe encore.

Hong Kong, les Philippines, la Thaïlande et Singapour sont ajoutés à notre liste de pays et territoires de prédilection. Nous ne sommes qu'un petit nombre et la quantité de zones à examiner devient difficilement tenable.

Hong Kong ?
Les Philippines ?
La Thaïlande ?
Singapour ?

25 juillet 26 juillet 27 juillet 4 août 7 août

18 août 2023

24 août 25 août 27 août 28 août 28 octobre

Zoom sur la cravate de l'uniforme fourni par Europol

Nos recherches autour de l'uniforme, de la cravate et du logo ne mènent nulle part. Nous en avons consulté des milliers, parfois au- delà de l'Asie, mais sans résultat significatif.

Plusieurs fois nous avons approfondi des pistes semblant nous rapprocher de notre uniforme-cible, mais leur étude n'a rien donné.

Nous maintenons nos efforts autour du modèle précis de cravate, cherchant les pays qui l'emploient et les fabricants. C'est pour l'heure l'élément tangible auquel nous accrochons cette investigation.

25 juillet 26 juillet 27 juillet 4 août 7 août 18 août

24 août 2023

25 août 27 août 28 août 28 octobre

Nos pistes semblent taries. Nous approchons du moment où nous pensons avoir épuisé les recherches liées à nos hypothèses.

Où mettre nos compétences et nos efforts ? Après avoir consulté des milliers de logos, uniformes, et sites d'écoles, au gré des intuitions parfois, avec méthode souvent, la plupart d'entre nous a basculé sur d'autres investigations, que nous aimerions aussi faire aboutir.

Cependant, nous restons toujours attentifs. Nous connaissons bien nos enquêtes en cours. Nous connaissons chaque détail de ces images floues et parcellaires. Et des intuitions brillantes surgissent parfois quand on s'y attend le moins.

**« Nous le savons,
il n'y a en réalité que deux
causes d'arrêt définitif d'une
investigation :
voir l'image retirée du site par
l'autorité, signifiant par là que
les recherches ne sont
plus nécessaires ou attendues,
ou bien trouver l'objet »**

25 juillet 26 juillet 27 juillet 4 août 7 août 18 août 24 août

25 août 2023

27 août 28 août 28 octobre

Devant la perte de vitesse de l'investigation, un membre du groupe décide de remettre le problème à plat.

Nous avons l'intuition collective que cet objet peut être trouvé, mais visiblement nous ne cherchons pas où il faut.

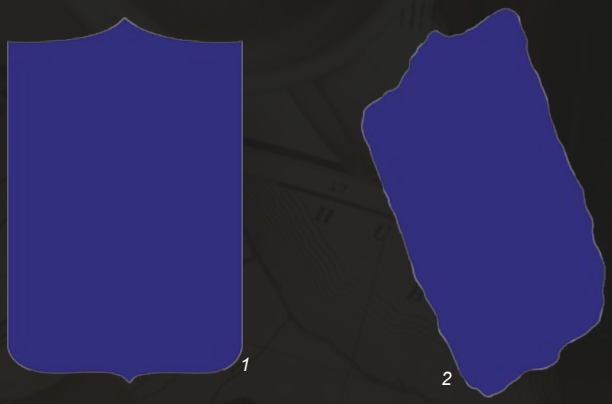
Avec toutes les informations que nous avons collectées, nous commençons à avoir une cartographie des écussons d'écoles en Asie, et un peu ailleurs dans le monde. Les formes, les couleurs, les lettres, tous ces détails sont soumis aux modes et aux coutumes locales.

Deux questions sont posées, axées sur les caractéristiques les plus spécifiques de notre objet-cible :

- La forme de l'écusson ne respecte pas les codes usuels de l'héraldique. Avons-nous jamais vu cette forme ?

- Deux lettres sont disposées de part et d'autre de cet écusson. Avons-nous jamais vu cette disposition de lettres ?

A ce stade, il nous semble possible d'affirmer que nous n'avons rencontré ces deux éléments dans aucun pays d'Asie.
Nous reprenons nos forces et relançons les recherches sur ces deux critères seuls, en nous focalisant sur le reste du monde.



1 silhouette de l'écusson telle que nous la comprenons
2 silhouette de l'écusson dans l'image de départ

25 juillet 26 juillet 27 juillet 4 août 7 août 18 août 24 août 25 août

27 août 2023

28 août 28 octobre

Nous avons prototypé l'écusson et nous nous représentons parfaitement sa silhouette. C'est donc en cherchant pays par pays, demandant aux moteurs de recherche à voir au moins une centaine d'insignes d'écoles ou d'uniformes, que nous nous faisons une idée de la possibilité d'y trouver celui qui nous intéresse.

Nous retrouvons cette forme particulière dans un pays d'Amérique du Sud, bien loin de l'Asie où nous avons effectué la majorité de nos recherches...
Puis dans ce même pays, la disposition des lettres. Une fois, puis deux, puis trois.

Finalement, nous retrouvons le fameux symbole de la torche que nous avons supposé voir au premier jour.

En une journée nous trouvons rattachés à ce pays une dizaine de logos qui collent à nos critères. Pour autant, ils ne ressemblent pas encore à notre écusson-cible, différent dans la composition et les couleurs.

C'est sans doute la raison pour laquelle ils ne sont pas remontés dans nos recherches par l'image.

A ce stade, rien n'est encore certain, mais ces retours sont très encourageants. Nous redoublons d'efforts.

Il n'est pas encore sept heures du matin quand un membre du groupe publie dans notre salon textuel une nouvelle série de logos. Il a probablement choisi de se lever plus tôt ce matin-là pour avoir le temps de faire quelques recherches avant que ses engagements le rattrape.

Il faut dire que les derniers résultats ont relancé la dynamique de cette investigation, on sent une énergie nouvelle dans le groupe qui veut croire en l'issue positive de cette recherche.
Parmi cette série se trouve un écusson peint sur la façade d'un bâtiment. Les premiers levés et disponibles se joignent au salon Discord, et cette peinture murale est vue comme approchante, mais les recherches se poursuivent sans qu'elle retienne suffisamment d'attention.

Notre écusson-cible est pourtant là, sous nos yeux, dans notre propre échange texto-visuel.

Quatre heures plus tard, les nouveaux arrivés permettent heureusement de repérer l'omission. L'image est arrivée si vite après ce dernier changement de méthodologie que nous en doutons encore. Est-ce bien le bon écusson ? Avons-nous vraiment trouvé ?

Vous devez être en train de vous dire : "Comment peut-on prétendre bien se figurer ce que l'on cherche et passer devant sans le reconnaître ?" Nous vous devons cette explication. Rapidement nous nous étions rendu compte d'une différence notoire dans ce pays entre des emblêmes présentés sur le fronton d'un établissement ou seuls (logo présenté en avatar de page Facebook par exemple), et des emblêmes portés sur les uniformes.

Leur forme différait, et leur rapport longueur-largeur également. Nous l'avions exprimé, nous tentions d'exercer nos yeux à passer de l'un à l'autre, mais nous débutions...

visuel conclusif

1 silhouette de l'écusson telle que nous la comprenons
2 silhouette de l'écusson dans l'image de départ
3 silhouette de l'écusson trouvé

Revenons à notre écusson peint sur un mur. Tout semble coïncider : formes générales, couleurs, lettres. Tout est là.
Après un peu plus d'un mois de recherches quotidiennes, nous venons d'identifier cet emblème de 50 pixels de large, pointant directement vers un collège d'une ville de 25 000 habitants, dans un pays que nous connaissons très peu.

Mais notre effort ne s'arrête pas à la trouvaille. Nous ne sommes pas dans un "Capture The Flag" ! Il nous faut maintenant vérifier et consolider nos conclusions, archiver les sources qui permettront aux enquêteurs policiers d'arriver aux mêmes constatations, et établir un rapport démonstratif pour faire en sorte que les autorités ne manquent pas d'y prêter attention.

Il s'agit d'abord d'épuiser toutes les possibilités d'erreur. Nous vérifions qu'il s'agit bien du même insigne, en observant toutes ses variantes.

L'uniforme de l'école, vite retrouvé, est lui aussi passé au crible, et comparé point par point. Types de vêtements, couleurs, tout est comparé. Nous tentons aussi de comprendre pourquoi la cravate à deux bandes n'est pas portée par tous les élèves. Nous voulons apporter le maximum d'informations utiles dans notre rapport.

Après dix heures intenses d'archivage, rédaction, multiples relectures et corrections, nous envoyons enfin le compte-rendu via le formulaire public d'Europol.

Nous sommes heureux. Rarement un objet présent sur une scène pédocriminelle, dernier indice à exploiter, amène aussi précisement à l'emplacement de la victime.

Voilà trois mois que nous avons apporté notre aide à cette investigation. Nous espérons qu'Europol a déjà pris connaissance de notre rapport, l'a vérifié, l'a confirmé, a pris contact avec les autorités locales, a permis des avancées majeures dans cette affaire...

Mais une fois n'est pas coutume, nous avons conclu notre investigation avec la connaissance de l'école fréquentée par la victime. L'un d'entre nous a donc mis en place une veille automatisée concernant cette école. Et aujourd'hui il revient dans le salon Discord avec une information qui sonne comme un coup de tonnerre.

Un article de presse locale évoque cet établissement et un adulte le fréquentant, mis en cause dans une affaire à caractère sexuel impliquant au moins une victime mineure.
Nous décidons unanimement d'envoyer une rapide notice à Europol pour l'en informer. Et maintenant vous connaissez la ritournelle... Archivage, rédaction, multiples relectures et corrections.

Nous envoyons ce court rapport le jour-même et ce sera notre dernier lien avec Europol concernant ces 2500 pixels.

bellingcat

Quelques chiffres sur bellingcat

* Eliot Higgins dirige Bellingcat
* Création de Bellingcat en 2014
* 27 personnes travaillent à temps plein et plusieurs contributeurs
* Plus de 780 000 abonnées sur X
* 74 000 sur Linkedin
* Événements et ateliers organisés afin de former des centaines de professionnels et citoyens aux méthodes de Bellingcat
* 35 prix et récompenses depuis 2015, notamment la Médaille du prix Nimègue pour la paix - Contribution à la paix et aux droits de l'homme

« Quand j'étais plus jeune j'étais d'une timidité quasi maladive, c'était à un point où je n'osais pas sortir de chez moi. J'étais un vrai Geek passionné par l'informatique et les jeux-vidéo, comme beaucoup de personnes renfermées sur elles-mêmes je passais des heures sur l'ordinateur.

Quand quelque chose me passionne je ne pense qu'à ça ! J'ai toujours été comme ça. En grandissant j'ai été attiré par ce qui était contre culture, je me suis penché sur l'impact de la politique étrangère de Etats-Unis dans le monde.

Avec le succès grandissant des réseaux sociaux en 2007 et l'arrivée des smartphones on a pu disposer de technologies qui permettent de prendre des photos et de les partager immédiatement avec le monde entier, c'était tout bonnement révolutionnaire ! »

Eliot Higgins

Propos repris du reportage
Bellingcat : les combattants de la liberté
(Avec l'autorisation de Bellingcat)

Bellingcat est un groupe international indépendant de chercheurs, d'enquêteurs et de journalistes citoyens utilisant à la fois : enquêtes 'open source' et réseaux sociaux, pour sonder une variété de sujets - trafiquants de drogue mexicains, crimes contre l'humanité, suivi de l'utilisation d'armes chimiques et conflits dans le monde entier. Avec un personnel et des contributeurs répartis dans 20 pays à travers le monde, ils travaillent dans un domaine unique dans lequel technologie de pointe, recherche médico-légale, journalisme, enquêtes, transparence et responsabilité se combinent.

Photo 1

Voici un exemple d'identification de suspect lors des manifestations d'extrême droite à Charlottesville réalisée part Eliot Higgins via Bellingcat *(propos retranscrits du reportage d'Arte s'intitulant Bellingcat : Les combattants de la liberté, avec l'accord de Bellingcat)*

« On a cette photo** (photo 1) **d'un homme en train d'en attaquer un autre, on a donc cherché à savoir qui il était. Et en étudiant des photos et des vidéos avec des suprémacistes blancs, on est tombés sur ce type** (photo 2)**, plusieurs photos montrent des similitudes, comme sa chemise par exemple.

Photo 2

On a examiné d'autres photos et tombés sur plusieurs qui semblent montrer la même personne (photo 3). Quand on compare les photos on voit que la disposition des grains de beauté sur son cou est exactement la même (photo 4).

Photo 3

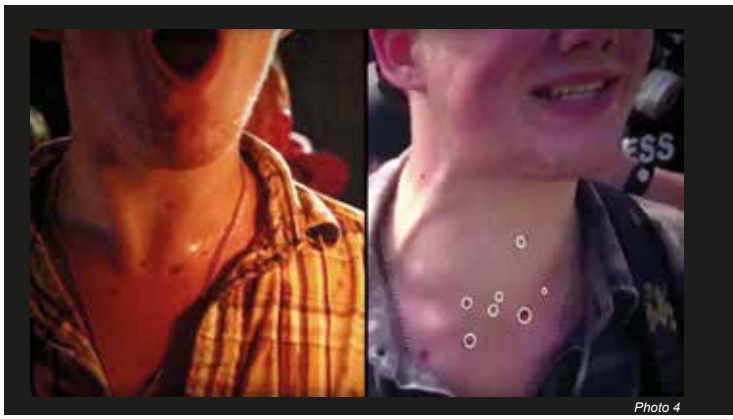


Photo 4

Ensuite, nous nous sommes intéressés aux personnes autour de lui (photo 5), certaines apparaissent et sont nommé sur un compte Twitter qui se nomme « Oui, vous êtes raciste » et qui indique leurs comptes sur les réseaux sociaux (photo 6).


Photo 5

Photo 5

On les a consultés ainsi que ceux de leurs abonnés et on est tombés sur le même gars (photo 7).

Sur sa page on trouve des photos et là encore on trouve des correspondances, on voit bien que ses grains de beauté dans le cou sont disposés de la même façon (photo 8).

C'est bien lui qui semble être en cause dans cette affaire et on essaye d'identifier les personnes derrière ce délit. Ce genre de travail intéresse de plus en plus la police.

Photo 7


Photo 8

BELLINGCAT

Le nom « Bellingcat » vient de l'idiome anglais « belling the cat », basé sur une fable dans laquelle un groupe de souris conviennent que la meilleure façon de se protéger du chat qui s'approche est de mettre une cloche sur son cou, mais échoue finalement à la tâche car aucune souris ne se porte volontaire pour la réaliser.

Connaissez-vous le BlockInt ?

BLOCKINT : Quand l'OSINT Rencontre la Blockchain

-
Jonathan Riss
Jonathan Spedale

Le BlockINT (Blockchain Intelligence) est un domaine qui combine les techniques de l'OSINT avec l'analyse des transactions et données sur les blockchains afin d'en extraire des informations précieuses.

L'Open Source Intelligence (OSINT) est une pratique qui consiste à collecter des informations à partir de sources accessibles. Dans le même temps, la blockchain est une technologie décentralisée et totalement transparente qui a révolutionné de nombreux secteurs (finance, supply chain…) en offrant un registre immuable des transactions.

La combinaison de ces deux domaines a naturellement donné naissance à un nouveau champ d'investigation : le BlockINT. Ce dernier utilise les techniques et méthodes de l'OSINT pour analyser les données disponibles sur les blockchains. Il offre ainsi de nouvelles perspectives pour la recherche, la sécurité et la conformité des transactions.

Qu'est ce que la Blockchain ?

La technologie blockchain permet de stocker des données de manière totalement décentralisée. Contrairement aux systèmes centralisés où une autorité unique contrôle les données, la blockchain fonctionne selon un modèle distribué. Cette décentralisation élimine le besoin d'intermédiaires, réduisant ainsi les coûts et augmentant la vitesse des transactions. Chacune d'entre elles sont enregistrées dans un bloc, qui est ensuite lié aux blocs précédents et ainsi de suite, formant une chaîne inaltérable.

Les différents types de blockchains

Les blockchains publiques : accessibles à tous (Bitcoin)

Les blockchains privées : réservées à des utilisateurs spécifiques (Hyperledger)

Les blockchains hybrides : qui combinent des éléments des deux précédentes

Les principales caractéristiques de la blockchain

la décentralisation : aucun acteur unique ne contrôle l'ensemble du réseau.

l'immuabilité : les données sont inviolables après leur enregistrement.

le consensus : règles sur le consentement des participants pour enregistrer les transactions.

Perspectives futures du BlockInt

Le BlockINT est un domaine en pleine expansion, avec de nombreuses évolutions technologiques à venir. Les avancées en matière d'intelligence artificielle et de machine learning promettent d'améliorer les capacités d'analyse on-chain. Ce dernier pourrait jouer un rôle crucial dans divers secteurs, comme la finance, la cybersécurité, etc... Les opportunités de carrière dans ce domaine sont en croissance, offrant des perspectives intéressantes pour les chercheurs et les professionnels de la sécurité.

Enfin, l'essor des solutions de confidentialité comme les Zero-Knowledge Proofs (ZKP) et les blockchains confidentielles (Monero et Zcash par exemple) pose de nouveaux défis pour les spécialistes du secteur.

Exemple de Blockchain

OSINT et Blockchain : Concepts et convergence

L'OSINT repose donc sur l'extraction d'informations en sources ouvertes telles que les réseaux sociaux, les forums, les bases de données publiques et toutes les autres ressources accessibles librement sur internet. Appliqué à la blockchain, il implique la collecte et l'analyse de données disponibles publiquement sur les réseaux.

Ainsi, il est possible d'avoir une vue détaillée du mouvement des fonds, des adresses de portefeuille, des relations entre différentes entités et même des messages (photo 1).

En utilisant des techniques de clustering et d'analyse spécifique, les spécialistes peuvent détecter des flux financiers inhabituels entre différentes blockchains ou identifier des adresses qui agissent comme des "mixers" pour anonymiser les transactions.

Mais cela n'est pas sans compter son lot de difficultés. La pseudonymie des adresses de portefeuille rend l'identification des utilisateurs très difficile. De plus, le volume croissant des données et la complexité de plus en plus importante des transactions nécessitent des techniques avancées ainsi que des outils puissants pour être efficacement exploités.

Photo 1

Etherscan.io

Metasleuth.io

Sentio.xyz

Techniques et outils

Le BlockINT utilise de nombreux outils et différentes techniques pour extraire des informations pertinentes. Parmi celles-ci, nous pouvons citer le "**clustering**" qui permet de regrouper les adresses appartenant à un même utilisateur afin de suivre les flux de transactions. Cela s'avère particulièrement utile lorsqu'on tente de suivre les transactions associées à des activités illicites (escroqueries, ransomwares…).

Le "**bridge tracing**" quant à lui est l'art de tracer des fonds qui transitent entre deux blockchains différentes. Le fait de transférer des actifs entre de multiples réseaux est un processus souvent utilisé pour tenter de brouiller les pistes et rendre les fonds plus difficiles à suivre. Cette technique de traçage est complexe, nécessitant une expertise en interopérabilité et une compréhension approfondie des protocoles spécifiques à chaque blockchain.

Les explorateurs de blocs tels que Etherscan.io ou btcscan.org sont des outils populaires et gratuits qui permettent l'analyse des données on-chain. Ces plateformes permettent aux utilisateurs de visualiser et d'examiner les transactions en temps réel.

D'autres plateformes comme metasleuth.io ou arkhamintelligence.com offrent la possibilité de monitorer les portefeuilles, de détecter les anomalies et de prévenir les activités suspectes.

Des solutions encore plus spécialisées, comme Phalcon ou Sentio.xyz, vont plus loin en permettant de visualiser les smart contracts, de simuler et de tester leurs différentes fonctions, offrant ainsi un niveau d'analyse encore plus granulaire.

Applications

Le BlockINT trouve des applications dans divers domaines. En matière de sécurité et de conformité, il aide les institutions financières à se conformer aux régulations **KYC** (Know Your Customer) et **AML** (Anti-Money Laundering). Il aide à surveiller les transactions suspectes, à identifier des schémas de blanchiment d'argent, et à prévenir les fraudes.

Les forces de l'ordre l'utilisent pour mener des enquêtes criminelles et financières, en traçant les transactions liées à des activités illégales. Par exemple, lors de la célèbre affaire Silk Road, les enquêteurs ont pu remonter la piste des transactions en Bitcoin pour identifier et arrêter le fondateur du site.

Dans la recherche académique, il permet d'étudier les comportements économiques et les dynamiques de marché. Les chercheurs peuvent étudier les comportements d'investissement à travers les différentes adresses de portefeuille.

Enfin, dans la supply chain, il assure la traçabilité des produits et renforce la transparence. Cela est particulièrement important pour les industries où la contrefaçon et la fraude sont des problèmes majeurs, comme dans les secteurs pharmaceutique ou alimentaire.

En suivant chaque étape du processus via la blockchain, les entreprises peuvent garantir l'authenticité et la qualité des produits qu'elles expédient.

Lumière sur les techniques d'investigations numériques

Téléphones, disques durs, GPS, cartes bancaires... Autant de dispositifs révélateurs de leurs utilisateurs. La criminalistique numérique s'est imposée comme un pilier essentiel dans les enquêtes judiciaires, requérant la mise en oeuvre d'un réseau organisé d'enquêteurs et de techniciens spécialisés, voici quelques exemples.

Ecoutes téléphoniques

IMSI-catcher (International Mobile Subscriber Identity) C'est un dispositif qui imite une tour cellulaire et force les téléphones mobiles dans une zone donnée à se connecter à lui. Une fois connecté, il peut intercepter les appels, les SMS et parfois même traquer la position d'un téléphone. Cela permet d'identifier l'appareil ou la personne utilisant le réseau.

Écoute légale Avec une autorisation judiciaire, les forces de l'ordre peuvent demander à des opérateurs téléphoniques d'intercepter des communications spécifiques. Ce processus implique la collaboration avec les fournisseurs de services pour capturer les métadonnées (heure, durée, localisation) ainsi que le contenu des communications.

Wiretapping sur les messageries instantanées Avec l'émergence des messageries chiffrées (comme WhatsApp, Signal), il est souvent nécessaire de recourir à des techniques plus complexes, comme la surveillance des communications au niveau des terminaux (piratage du téléphone pour accéder aux messages avant ou après le chiffrement).

Surveillance des réseaux

Packet Sniffing C'est une méthode d'interception de données sur un réseau en capturant et en analysant les paquets de données. Des outils comme Wireshark permettent de surveiller et d'intercepter le trafic réseau sur une certaine période, facilitant la reconstruction des communications.

Man-in-the-middle (MITM) Dans une attaque MITM, l'attaquant se place entre deux entités communicantes (exemple : un client et un serveur), souvent à leur insu, pour intercepter ou altérer les communications échangées. Cette technique permet de lire des données supposées chiffrées si le chiffrement est mal implémenté.

Intrusion dans les routeurs ou serveurs Il est également possible de prendre le contrôle d'équipements réseau, tels que des routeurs ou des serveurs DNS, pour capturer le trafic.

Analyse forensique

Capturer des images disques L'une des premières étapes consiste à cloner les disques durs, les SSD ou les mémoires des appareils suspects pour les examiner dans un environnement contrôlé. Cela permet de conserver une copie exacte (bit à bit) des données sans altérer les originaux. Outils couramment utilisés : FTK Imager, EnCase.

Analyse des systèmes de fichiers Une fois l'image capturée, l'analyse des fichiers, des métadonnées (dates de création/modification), des systèmes d'exploitation, et des logs permet de comprendre l'activité de l'utilisateur. Des logiciels comme Autopsy ou X-Ways Forensics sont utilisés.

Récupération de données effacées Dans certains cas, les données supprimées ne sont pas complètement effacées du disque. Les techniques de récupération avancée peuvent permettre de retrouver ces informations.

Analyse des artefacts de navigation En examinant les fichiers cache, l'historique et les cookies d'un navigateur, on peut retracer l'activité en ligne d'un suspect, comme ses recherches sur Internet ou les sites visités.

Analyse de la RAM (mémoire vive) La RAM contient des informations temporaires et volatiles qui peuvent être cruciales, telles que des clés de chiffrement, des fichiers en cours d'utilisation, ou des processus malveillants. L'analyse de la RAM peut être faite avec des outils comme Volatility ou Rekall.

Traçage numérique et géolocalisation

Adresses IP et traçage géographique Identifier l'adresse IP utilisée par un suspect permet de le localiser géographiquement, ou au moins de tracer son FAI (Fournisseur d'accès à Internet). À partir de là, une collaboration avec le fournisseur permet souvent d'identifier l'utilisateur derrière cette adresse (via les logs de connexion).

Suivi de la géolocalisation via GPS La géolocalisation via des services GPS intégrés dans les téléphones ou ordinateurs portables peut donner des informations précises sur les déplacements d'un suspect. De nombreux logiciels malveillants sont également conçus pour collecter et transmettre ces données à distance.

AU COEUR D'UNE ENQUÊTE POUR TERRORISME

Avec le commandant de police **Pierre Penalba**

Le commandant Pierre Penalba a été à la tête du premier groupe de lutte contre la cybercriminalité de la Police Nationale. Spécialiste du Net, il est également expert informatique et formateur auprès d'unités de police françaises et étrangères. Il nous raconte une des enquêtes sur laquelle il a pu prendre part.

AU COEUR ...

Ce récit est celui d'une enquête réelle à laquelle j'ai participé dans le domaine du terrorisme.
D'autres sont encore classées et je ne peux même pas les aborder sous forme romancée.

Pour celle-ci, moins sensible, j'ai dû changer les noms, certains éléments et quelques autres, pour des raisons de sécurité évidentes.
Aucuns détails concernant les logiciels utilisés ne peut être donné.

2022

Une note blanche vient d'être reçue par notre unité.

(Il s'agit d'une information sérieuse vérifiée par un service gouvernemental, mais dont on ne doit pas faire mention, en aucun cas, la «source» officielle n'étant pas citée ou mentionnée sur la note..)

Dans ce document, on nous informe qu'un acte terroriste est en préparation dans notre zone de juridiction.

Pas beaucoup plus d'éléments, quelques captures de conversations sur une messagerie chiffrée, un profil qui communique avec un jihadiste originaire de notre département, parti se battre en Syrie.

Je suppose que vous aimeriez savoir comment et qui a récupéré cette information...

Moi aussi…

La seule chose dont je suis sûr, à ce moment précis c'est qu'elle est valable.
Bon une messagerie chiffrée, ça veut dire aussi, pas de possibilité d'identification légale...

Puisqu'on en parle, c'est sécurisé, dans un sens oui, mais pas quand on sait où chercher...

Un élément : une identité, celle du jeune jihadiste qui avait quitté la France. Je l'appellerai Akmad.

Les échanges en français, principalement, montraient que Akmad et son contact étaient probablement proches.

Alors a commencé un travail de fourmi, en utilisant toutes les techniques d'OSINT, en tentant de reconstruire la vie et les contacts d'Akmad.

Un travail de dingue qui nous a pris des dizaines d'heures, à fouiller tous les réseaux sociaux, pro et autres, sur des années.

Vu la sensibilité du dossier on ne s'est pas limité au cyber, on s'est aussi déplacés, pour surveiller physiquement les proches, les amis, mener des enquêtes de voisinage discrètes, informateurs, etc...

Comme je l'ai dit précédemment, tout le monde fini par progresser, surtout ceux qui ont des projets d'attentats terroristes, croyez-moi.
Ils ne se connectent pas de chez eux, avec leur ordinateur ou leur téléphone, non, ils savent.

Ils utilisent des téléphones jetables, sur des wifis publics, changent régulièrement et ne font confiance à personne.
Parfois ils utilisent des clefs bootables et chiffrées pour démarrer des VM avec des VPN, bref.

Dans le cas présent on avait un avantage, non négligeable, c'était la proximité des deux jeunes, avant le départ d'Akmad.

Notre liste de suspects, s'est vite réduite à quelques noms.

Evidemment, on les a fait placer sur écoute téléphonie et data, bien sûr. Deux wifis à surveiller et trois téléphones.

On avait «obtenu» (ceux qui disent pirater... heu... ce n'est même pas v..), un ... heu ... accès dans les deux réseaux wifi ...

... DE L'ENQUÊTE

Image d'illustration

Les technologies et logiciels, nous permettaient de capter tout le trafic, mais le chiffrement posait un problème réel.
Cependant quand vous savez que quelqu'un utilise une messagerie chiffrée, il est plus simple de surveiller les flux et déterminer si quelqu'un en utilise...

Si si, on ne sait pas ce qu'il y a dedans, mais on voit passer les données chiffrées.

Les suspects avaient une activité en data intense, mais quasiment rien avec chiffrement et encore moins sur la messagerie qui nous intéressait.

Par chance, un soir, sur un des wifi sous surveillance, quelqu'un s'est connecté sur la messagerie.
On a immédiatement récupéré les «mac adresses» des matériels connectés dans la box et surprise, il s'agissait d'un téléphone inconnu!

Juste pour info, une mac adresse, c'est extrêmement utile, on peut arriver à retrouver beaucoup d'éléments liés au constructeur.

Ah oui, on avait aussi une surveillance physique qui nous a permis en croisant ces infos, d'identifier un nouveau suspect. Restait à trouver son téléphone.

J'ai utilisé les techniques liées au «roaming» et aux antennes 3G/4G du secteur, pour trouver des occurrences qui ont permis d'identifier le numéro de téléphone lié aux déplacements de notre nouveau suspect.

Ça nous a pris des heures et pas deux minutes comme dans les séries...
Un numéro jetable certes mais rien ne nous empêchait de l'écouter et de le surveiller.
On a enfin, pu mettre un nom sur le profil de l'apprenti terroriste. Samir.

Pas un ami d'enfance, mais plutôt une connaissance, qui évoluait dans un groupe, avec un prêcheur ultra radical, qui les avait formés. Ils s'étaient convertis en même temps, ce qui avait rapproché les deux, devenus «frères».

Avec sa localisation précise, une cellule spécialisée d'experts de la police a posé des «dispositifs d'écoutes» et de surveillance.

Je n'ai pas le droit de trop en dévoiler, mais en gros, on captait son trafic data en temps réel, ses conversations évidement, sans compter les surveillances physiques.
J'avais l'impression d'être derrière son épaule, en permanence.

Les conversations complètement hallucinantes entre les deux hommes, portant sur la meilleure façon de causer le plus de morts, sur les techniques pour échapper aux «kouffards».

Il a fallu documenter en détail le projet, mais là où c'était plus angoissant, c'est qu'il fallait le laisser commencer ses préparatifs d'attentat avant de l'interpeller, sinon juridiquement ça ne restait qu'un projet, du virtuel et ça n'est pas pareil que s'il y a préparation ou début d'exécution...

On voulait aussi avoir ses complices éventuels.
La préparation d'explosifs, heureusement, n'est pas simple surtout quand on veut dissimuler ça à son entourage.

Samir, disposait d'un local mais vivait encore avec sa famille, des «kouffards» pour lui...
Il a commencé à se procurer les éléments de base, tout en étant encouragé et guidé par Akmad.
Mais tout a dérapé un soir lorsque ce dernier à annoncer à Samir, qu'il allait enfin devenir un martyr !
Il venait d'apprendre que le lendemain il allait conduire une voiture piégée au milieu d'une base d'infidèles !

L'un annonce avec des cris de joie qu'il va se suicider le lendemain en tuant un maximum de gens et l'autre lui répond «T'as trop de chance !» dixit…

Samir ensuite s'est plaint de ne pas être prêt, que lui aussi, il voulait partir en martyr !
Enthousiaste, Akmad a alors expliqué à Samir, qu'il lui suffisait d'un couteau pour tuer plein d'infidèles, il avait juste à sortir et faire le plus de morts possibles !

Samir a commencé à visualiser son projet meurtrier à voix haute, expliquant qu'il allait commencer par sa famille, ces kouffards, encouragé par un Akmad quasiment hystérique qui lui certifiait qu'il s'agissait d'une façon de les sauver puisqu'il pourrait ensuite les sortir de l'enfer. (???)

Honnêtement, en assistant à une scène pareille, j'ai cru un instant que j'étais en train de faire un cauchemar.

Pas le temps de tergiverser.

Tout le monde sur le pont, pour aller interpeller Samir.
Quant à Akmad, une note blanche urgente, en retour pour informer de l'imminence de l'attaque quelque part là-bas.

Samir a été interpellé alors qu'il aiguisait soigneusement un gigantesque couteau de boucher, les éléments de fabrication de sa future bombe également. Il dort en prison pour très, très longtemps.

Akmad a disparu des réseaux et de la messagerie.

Cette enquête, une parmi tant d'autres, n'aurait pas réussi sans la technicité, l'ingéniosité et le dévouement d'hommes et de femmes qui placent tous les jours, sans compter, l'intérêt des autres avant le leur, avant leur confort, leur vie de famille. J'ai été fier de travailler avec vous. Je veux les saluer aujourd'hui. Merci pour ce que vous faites.

Interviews de ceux qui font la cyber et l'IT aujourd'hui

Nous les connaissons par leurs publications journalières mais qui sont-ils ?

Comme à son habitude Cyber-IT a rencontré divers profils qui ont répondu à nos questions.
Pour la troisième itération de la section interviews, voici une nouvelle salve de questions/réponses.
Les interviews publiées dans le magazine sont pour la majorité plus longs que ceux postés sur Linkedin (par souci de caractères maximum autorisés).

TRISTANT MANZANO
DG chez Security Data Network

Salut Tristan, comment vas-tu ? Un petit mot sur toi ?

"Hello Arnaud, bien je te remercie !

Alors, je suis Tristan Manzano, directeur général chez SECURITY DATA NETWORK et consultant en cyber sécurité"

Quel à été ton parcours ?

"J'ai commencé l'informatique a l'âge de 11ans je me suis vite rendu compte que j'étais passionnée par ce domaine, j'ai donc passé des journées entières sur l'ordinateur.

J'ai fait un bac "technicien en systèmes et réseaux" à mes 20ans puis j'ai continué avec un BTS "technicien supérieur en réseau informatique et télécommunications" puis un bac+4 en "responsable en ingénierie système et réseaux" .

Puis j'ai créé ma boîte et j'enchaîne les certifications."

Quelles sont tes missions au quotidien ?

"Mes missions sont : gestion de l'entreprise, test d'intrusion, red team, audit de sécurité, formation en école d'ingénieur."

A quoi ressemble une journée type pour toi ?

"En général je commence par de la veille technologique, lire mes mails et autres messages, après je commence ou continue mes projets. Puis en fin de journée je prépare la journée du lendemain."

Qu'est-ce que te plaît/déplaît dans ton métier ?

"L'informatique en général !

J'aime vraiment tout les domaines les systèmes ou réseaux en passant par la programmation, la sécurité informatique est vraiment la suite car cela permet de toucher à l'ensemble des domaines de l'informatique"

Un mot pour la fin ?

"Happy Hacking ! 😁"

SDN SECURITY DATA NETWORK

NATHALIE GRANIER
Chercheuse en renseignement sur les cybermenaces et les comportement humain

Bonjour Nathalie, explique nous en quelques mots qui tu es ?

🎙 "Une fille du sud-ouest, du pays de l'ovalie 😉 Epicurienne
Et accessoirement psychologue depuis quelques décennies et travaillant dans la cyber depuis 8 ans"

Quel a été ton parcours ?

🎙"J'ai exercé la fonction de psychologue dans différentes structures. Je suis psychologue, specialisée en science sociale et cognitive.

Obtenu un master2 en psychologie que j'ai complété par différentes formations spécialisées.

Également un diplôme en Ressources humaine
Et un BAC +5 en consulting

J'ai donc occupé des postes de RH, de consultante, de psy et en cyber : de delivery, de consulting , de contenu cyber, de gestion de crise et d'analyste en Threat Intelligence"

Et quelles sont tes missions ?

🎙"Je fais :
Consulting
-Apport expertise cyber
-Veille technologique et économique du marché.
-Participation salons, conférences
-Étude et analyse techniques de gestion et d'organisation de la concurrence.
-Accompagnement et conseil
-Participation à la mise en oeuvre de la solution
Je travaille en cybersécurité, en CTI ou renseignement sur la menace cyber
-Analyse des menaces qui ciblent en particulier l'environnement du client
-Collecte des données en sources ouvertes, de tierces parties et de fournisseurs d'informations d'intérêt Cyber et enrichissement avec des analyses contextuelles
-Aide aux investigations
-Participation aux réunions avec les clients en tant que référente technique
-Contribution à l'amélioration continue du service

Je suis responsable offre CTI.[Cyber Threat Intelligence]"

A quoi ressemble une journée type pour toi ?

🎙"Aucune journée ne se ressemble, et c'est très bien comme ça 😊
Il faut être prêt pour l'imprévu, le changement ce qui nécessité de l'adaptation et de la curiosité. Il n'y a pas vraiment d'horaire, la encore ça tombe bien je suis insomniaque.

Mes journées "calmes" voire mes semaines vont alterner en fonction des différentes fonctions mentionnées plus haut.
Et quand je ne fais pas tout ça , j'ai la chance de pouvoir participer à des conférences, webinar, table ronde, et écrire des articles toujours en lien avec la cyber et la psychologie"

Au final qu'es ce qui te plaît dans ton travail ?

🎙"L'imprévu, pas de routine !
L'obligation de curiosité d'apprendre en permanence.
La vie en cyber est un défi permanent et j'aime ça !
Et en plus je peux combiner ce domaine avec la psychologie. Apprendre à décoder les êtres humains derrière un écran, comprendre pourquoi on fait ça ? et en quoi un écran bouleverse les règles"

As tu un mot pour la fin ?

🎙"Si vous êtes curieux, adaptable, envie d'apprendre, de partager :
Foncez ce job est pour vous !

"Il faut être enthousiaste de son métier pour y exceller." Diderot j'ajouterai … en gardant toujours son humilité…."

DR GUILLAUME CELOSIA
RSSI industriel

Bonjour Guillaume, en deux mots qui tu es ?

"Bonjour ! Je suis Guillaume CELOSIA, RSSI Industriels (le jour) et passionné de cybersécurité (le jour et la nuit)"

Et concernant ton parcours ?

"Sur l'aspect scolaire : un parcours insalien plutôt "classique" dans un premier temps (avec une majeure en sécurité des systèmes ubiquitaires)... et puis, le drame : la passion prit le dessus ! Pour l'assouvir, une seule solution : la thèse. Une aventure que je ne peux que recommander les yeux fermés pour la myriade d'apprentissages associés.

Sur l'aspect professionnel : de la technique d'abord (pour comprendre), puis de la gouvernance ensuite (notamment pour maîtriser la technique). Quelques compétences en communication après un passage dans le conseil. On mélange le tout, et voilà !"

Quelles sont tes missions principalement ?

"Des audits, de la gouvernance, de la sensibilisation, de la formation, de l'architecture, de la veille, du pilotage de tableaux de bord sécurité, des revues fournisseurs, etc. Comme tu l'auras compris, mes missions quotidiennes sont diverses et variées... mais convergent vers un seul but : protéger mon périmètre industriel des cyber-attaquants !"

Donc à quoi ressemble une journée de travail pour toi ?

"Es-tu certain de vouloir vraiment le savoir ?! Bon, d'accord, mais tu vas être déçu : wake up - eat - calls/-mails - eat - mails/calls - eat - "sleep" - repeat !
Finalement, la vie d'un RSSI ne serait-elle pas une belle histoire culinaire ?"

Qu'est-ce que te plaît/déplaît dans ton métier ?

"Il faut l'avouer, la cybersécurité côté IT est déjà bien complexe... mais alors en environnement industriel / côté OT, je ne t'en parle pas ! C'est paradoxal, mais c'est certainement cela qui me plaît le plus.

Quant à ce qui me déplaît, sans hésiter : le AI-powered blockchain bullshit !"

Parfait, merci ! As tu un mot pour la fin ?

"On ne le répétera jamais assez : la cybersécurité est l'affaire de Tous ! Merci pour l'opportunité et la publication de cet interview !"

STEPHANE FERRER
DPO - Conformité RGPD et fondateur RGPD-SF

Salut Stéphane, heureux de te rencontrer, dit nous qui tu es ?

"Plaisir partagé Arnaud ! Je suis un affreux parano pour mes clients 😅. Mais d autres voient en moi une personne qui traduit en mots simples des notions obscures et effrayantes voire clairement ch..."

Peux-tu nous en dire plus sur le parcours qui est le tiens ?

"Mon parcours est comme pour tous : atypique. Profil scientifique (genie de l environnement) puis les hasards de la vie m ont conduits a changer de l'environnement "bio" a celui de windows.

Au final j ai trouvé le juste equilibre dans la mission du DPO : humain, it, legal, crise."

Quelles sont tes missions au quotidien ?

"J'ai plusieurs missions, mais les principales, je dirais que ce sont celles de conseils, de mise en œuvre, également de sensibilisation.

Mais la première des missions que je me fixe c'est de ne pas tomber dans la routine et heureusement aujourd'hui c'est mission accomplie"

Institution Sainte-Marie
83500 La Seyne sur mer

À quoi ressemble une journée type pour toi ?

"Etant aussi responsable informatique dans l'école ISM LES MARISTES depuis 25 ans, dès mon arrivée je suis sollicité de tous côtés par les utilisateurs, profs comme élèves.

Je les chouchoute et leur montre les risques induits dans leurs pratiques.
Je gère aussi des projets «RGPD by Design" pour la gouvernance.
De plus, je conduis également la conformité RGPD pour mes clients.

Il est rare que je m'ennuie !"

Qu'est-ce que te plaît et déplaît dans ton métier ?

"Ce qui me plaît c'est d'aider les gens en leur apportant des réponses concrètes et surtout compréhensibles !

Ce que je trouve moins plaisant ce serait d'être vu comme un empêcheur de faire ... (pour ne pas dire un emmer****). Mais ma vision des choses me pousse à croire que c'est à moi de les faire changer d'avis avec les bons arguments"

Merci à toi, as-tu un mot pour la fin ?

"Au delà de dire un mot de fin, je préfère parler de devise : le RGPD, c'est sécuriser pour protéger, non la soumission aveugle à une réglementation de plus"

VALERY RIEß-MARCHIVE
Rédacteur-en-chef, LeMagIT

Enchanté Valery, dit nous qui es-tu ?

"Je suis le rédacteur en chef du MagIT, et l'un de ses cofondateurs. Accessoirement, je suis aussi un collectionneur de cyberattaques (avec ransomware) dont je m'évertue à tenir un inventaire aussi complet que possible depuis... septembre 2020. Et cela que ce soit à partir des revendications des cybercriminels ou des faits rapportés dans la presse, dans le monde entier. Ce travail, je m'attache depuis un an à le rendre plus complet, plus précis et aussi plus transparent. Ce qui nous a permis de créer notre cyberhebdo ainsi qu'un inventaire régulièrement mis à jour sur mon répo GitHub.
Pour ce travail, je m'attache également à "redresser" la chronologie des revendications des cybercriminels afin d'éviter de laisser le champ libre à leurs efforts marketing.
Et enfin, je suis le créateur d'un recueil de négociations, nettoyées, anonynisées, et normalisées sous forme de fichier JSON, qu'il est notamment possible de consulter sur ransomch.at et ransomware.live."

Peux-tu nous expliquer ton parcours ?

" J'ai suivi une formation initiale d'informaticien, à la fac (UVSQ). J'ai connu Internet avant le Web et commencé à coder dans mon adolescence. Pendant mes études, j'ai découvert la presse informatique - comme pigiste. J'y suis donc resté. Presse Mac, presse IT pro, presse IT consumer, des livres sur les produits Apple... Et puis en 2008, LeMagIT, avec le reste un groupe de collègues et amis. C'est vers 2011 que j'ai pris le virage de la sécurité informatique, initialement en suivant l'évolution du marché et des produits. C'est en 2019 que j'ai vraiment commencé à suivre de près le paysage des menaces."

Y'a t-il des choses qui te plaisent/déplaisent dans ton métier ?

" Tout en restant dans la case journaliste, j'ai changé de métier à de nombreuses reprises. Spécialisé Mac, puis téléphonie mobile, puis IT d'entreprise, puis outsourcing en Inde, puis cyber... avec un petit orteil dans la threat intel. Cette versatilité, tout en restant globalement sur la même spécialité, c'est énorme.
Certaines pratiques de communication, notamment en temps de crise, peuvent être un peu tristes, mais j'ai pu observer une vraie progression au fil des ans. Et c'est rafraichissant."

Quelles sont tes missions quotidiennes ?

"la première de mes missions au quotidien, c'est de laisser bosser mes collègues sans leur mettre de batons dans les roues. LeMagIT est riche d'une équipe remarquablement talentueuse, professionnelle, et rigoureuse. C'est un privilège de bosser avec François, Philippe, Yann, Gaétan, Pascale ou encore notre boss, David. Et j'ajoute à cela nos pigistes, dont je pilote directement certains d'entre eux.
C'est aussi d'être là en support quand quelqu'un a besoin d'un coup de main ou d'une interface pour répondre à un attaché de presse un peu grognon.
Après, suivi de l'actualité des incidents cyber un peu partout dans le monde, afin de pouvoir alimenter le cyberhebdo. Suivi de l'actualité cyber pour trouver des idées de projets IT, de conseils, voire de tribunes - et accessoirement rédiger tout ça. Parce qu'écrire fait quand même un peu partie du job.
Dans mon cas, écrire, c'est aussi écrire du code, en Python, pour créer de nouveaux outils, de reporting notamment, pour le bulletin météoransom mensuel, mais aussi pour en faire évoluer et maintenir, à usage interne."

As-tu une journée type ?

"Ma journée type, c'est d'abord Teams pour échanger avec les collègues sur l'édition du jour. C'est aussi un lecteur de flux RSS, et la suppression d'un nombre impressionnant de messages.
A cela s'ajoutent les coup de fil plus ou moins aléatoires (et les DMs) - en plus des échanges et autres interviews programmées à l'avance, sans compter les webinaires (soit comme spectateur, soit comme intervenant).
Il y a aussi beaucoup de suivi de quelques réseaux sociaux, que ce soit pour garder un oeil sur le travail de quelques chercheurs en cybersécurité ou sur des conversations susceptibles de faire émerger de nouvelles idées de papiers ou d'angles de traitement.
Je consacre également du temps chaque jour à la pèche aux échantillons de ransomware sur les principales sandbox.
Dans tout ça, il faut encore trouver le temps d'écrire. Du coup, il n'est pas rare que ma journée ait tendance à s'étirer..."

Merci Valery, as-tu un mot pour la fin ?

"je vais me répéter, mais je pense qu'on ne commence même pas à mesurer à quelle point la menace est sérieuse et partout. Je suis convaincu que les victimes en devenir de cyberattaque, qui s'ignorent encore, sont très très nombreuses. Certaines auront peut-être la chance d'y échapper, mais pas toutes, hélas. Et, encore hélas, la grande majorité n'y est absolument pas préparée."

ETIENNE CAPGRAS
Responsable du contenu cybersécurité pour Openclassrooms

OPENCLASSROOMS

Bonjour Etienne, merci d'avoir répondu à mes questions, donc qui es tu ?

"Bonjour Arnaud, c'est un plaisir de partager avec toi.
Je suis Etienne Capgras, responsable des formations cybersécurité chez OpenClassrooms , que j'ai rejoint il y maintenant trois ans."

Tu peux m'en dire un peu plus sur ton parcours ?

"J'ai un parcours classique je dirais, diplômé de l'école d'ingénieur INSA Toulouse en 2010, j'ai fait mes premières armes chez Wavestone de 2010 à 2021. Mes premières missions ont été faites de tests d'intrusions et d'audits dans plusieurs secteurs, comme le bancaire, la santé ou les transports. J'ai ensuite accompagné plusieurs opérateurs d'importance vitale (OIV) dans leur conformité à la LPM : analyses de risques, architectures, pilotage de programmes, échanges avec l'ANSSI - Agence nationale de la sécurité des systèmes d'information …, ce qui m'a apporté une certaine expertise sur le sujet.
En parallèle, j'ai aussi eu la chance et la responsabilité d'accompagner une trentaine de consultants dans le développement de leur carrière dans la durée. Finalement, j'ai rejoint OpenClassrooms fin 2021, pour y développer le catalogue de formation en cybersécurité et en IT."

Quelles sont tes missions actuellement au sein d'Openclassrooms ?

"J'ai rejoint OpenClassrooms pour développer le catalogue de formation cyber. Concrètement, je dois faire en sorte qu'on forme aux bons métiers (ceux en tension), de la bonne manière et avec les bonnes personnes. Une autre facette de mon rôle consiste aussi à faire connaître nos formations aux employeurs et aux candidats : ça ne sert à rien de développer du contenu pertinent s'il n'est pas utilisé.
La pénurie de compétences en cybersécurité m'a profondément marquée et continue de me préoccuper : incapacité à se sécuriser autant que nécessaire, épuisement des personnes en poste, émergence d'acteurs incompétents et tout de même sollicités au vu de la demande. Il nous faut agir vite !
Donc on pourrait résumer en disant que ma mission est de rendre les carrières en cybersécurité accessibles à toutes et à tous, dans l'intérêt de tout le monde :) "

A quoi correspond une journée type dans ton travail ?

"Il n'y en a pas ! Analyse du marché pour identifier et caractériser les métiers qui sont réellement en tension, beaucoup de rencontres avec les professionnel.le.s du secteur pour capter les pratiques, les attentes et les besoins du terrain, mais aussi avec nos candidats, nos étudiants, nos partenaires comme Root-Me , CompTIA, etc. Depuis 2023, je suis également membre d'un groupe de travail européen piloté par l'ENISA sur la modélisation des compétences en cybersécurité. Et puis bien sûr, tout ce qui touche à la création ou à la mise à jour de notre contenu : cadrage d'un nouveau cours, validation de syllabus, recrutement d'expert.e.s…"

Qu'est-ce que te plaît et/ou déplaît dans ton métier ?

"Ce qui me plait le plus, je dirais que c'est l'impact que je peux avoir grâce à OpenClassrooms, quelle fierté ! D'un côté, tous nos cours sont en accès gratuit, pour une utilisation la plus massive possible. De l'autre, nos formations diplômantes visent à rendre accessibles des métiers qui ne le sont pas assez. Et le tout entouré de collègues et d'expert.e.s passionnés et passionnants ! Que demander de plus ?
Il faut en revanche apprendre à raisonner sur un temps long. Entre l'idée d'une formation et les premiers diplômés, il faut en effet compter environ deux ans, voire trois : création, mise en ligne, inscription, démarrage des premiers étudiants, progression de chacun, diplomation, et enfin, insertion dans l'emploi. Le maître-mot est la patience !"

Merci Etienne, as-tu un mot de fin ?

"On est dans une période charnière où l'écosystème cyber est conscient de la nécessité de recruter plus large et plus vite, mais n'y parvient pas suffisamment. Une bascule d'un recrutement sur diplôme vers un recrutement par les compétences s'amorce et c'est une très bonne nouvelle !

À nous de transformer l'essai !"

Nouvelle Section

LE COIN DES PROS

Détection et Interprétation des signaux faibles

ABOU JAMRA Hiba et Mathieu Pichon

Dans ce chapitre nous introduisons dans un premier temps la notion de signal faible : celle-ci n'est pas définie précisément car des auteurs, appartenant à différents champs disciplinaires, utilisent plusieurs termes pour la désigner voire même, ne la définissent pas en considérant qu'il s'agit d'une notion connue. Une autre façon de définir un signal faible est de préciser ses caractéristiques en mettant en avant des spécificités qui lui sont propres. Malgré tout, nous verrons que les différents travaux sur les signaux faibles nous ramènent à quatre caractéristiques : bien qu'étant informels, rares et difficiles à interpréter, ils sont annonciateurs d'évènement.

Signal faible : une notion multi-facettes

L'article d'Igor Ansoff « Managing Strategic Surprise by Response to Weak Signals » [8] de- meure la référence dans le domaine de la recherche sur les signaux faibles. Pour la première fois, l'idée de signal faible est identifiée dans le domaine des Sciences de Gestion. Ansoff définit les signaux faibles comme « les premiers symptômes de discontinuités stratégiques qui agissent comme une information d'alerte précoce, de faible intensité, pouvant être annoncia- trice d'une tendance ou d'un évènement important ». Cet article se focalise sur l'importance qu'il y a pour une entreprise à trouver des informations quasi imperceptibles afin d'éviter les menaces ou au contraire de favoriser les opportunités. La publication de cet article a lieu après le premier choc pétrolier de 1973 où l'instabilité politique a démontré que les plans straté- giques établis lors des trente glorieuses étaient caducs. L'entreprise ne peut plus se contenter d'extrapoler à partir des données du passé et, pour ne pas être surprise par les variations de son environnement, elle doit anticiper les évènements soudains.

La définition d'Ansoff est basée sur l'utilité d'un signal faible en l'identifiant comme un élé- ment ayant un caractère anticipatif mais cette définition n'est pas suffisamment précise, il s'agit plus d'une métaphore. Par la suite, de nombreux auteurs reprendront ce travail afin de préciser son idée.

Depuis cinquante ans, la définition d'un signal faible a évolué. Avant 1980, la notion de signal faible faisait référence à des phénomènes émergents ayant un impact dans le futur. Dans les années 1980, les définitions s'intéressent aux sources mal définies et à leurs impacts. Au cours des années 1990, de nouveaux adjectifs sont apparus pour décrire les raisons pour lesquelles ces signaux sont si difficiles à détecter : petit, dynamique, périphérique. À partir des années 2000, les définitions ont commencé à faire référence aux indicateurs d'un phénomène (comme tendance) plutôt qu'aux phénomènes eux-mêmes.

« Une perception de phénomènes stratégiques détectés dans l'environnement ou créés lors d'interprétation, éloignés du cadre de référence du récepteur »

Van Veen et Ort

La notion de signal faible s'est développée dans différents domaines, tels que le traitement du signal, la théorie de l'information, la stratégie d'entreprise, la gestion de crise et la prévention de risques industriels. En raison de cette diversité de domaines, ils font l'objet d'un champ lexical riche. Plusieurs termes sont apparus comme « pressentiment », dans le domaine de la gestion de crise nous trouvons les termes « signal d'alarme ou signal d'alerte », « signal aberrant » ou encore « anomalie » ; dans le domaine de la prévention des risques les termes « signal précoce », « alerte précoce » « signal avant-coureur » ou « signal précurseur » sont utilisés de manière interchangeable sans distinction de sens. Dans ces deux derniers domaines, les signaux faibles sont vus comme des signaux d'alerte car ils sont étudiés sous l'angle de la menace.

Un signal est qualifié de faible car il est difficile à détecter étant noyé dans une multitude de données souvent sans aucun intérêt. Paradoxalement, un tel signal est d'autant plus faible qu'il peut annoncer quelque chose de très important si les experts métier sont capables de le percevoir et de l'interpréter. Plusieurs auteurs ont mis en avant les spécificités d'un signal faible que nous pouvons résumer par les qualificatifs suivants :

fragmentaire : nous ne sommes pas face à des informations complètes sur l'évènement pouvant être anticipé, nous n'avons à notre disposition qu'un petit nombre de signaux à interpréter. À partir de leur interprétation, les experts métier devront se risquer à prendre des décisions. Dans les diverses définitions présentées dans la section précé- dente, nous trouvons aussi les adjectifs incomplet, imprécis, vague.

Signification apparente faible : il n'existe pas de lien de cause à effet, le signal faible paraît peu parlant ou ambigu, il est sans signification et demande une interprétation de la part d'experts métier.

Faible intensité : il est disséminé dans une multitude d'informations inutiles et un grand nombre de personnes passe à côté de cette information, il apparaît comme étant peu visible.

Cycle de vie d'un signal faible

Les signaux faibles étant décrits comme des indications ambigues de perturbations à venir, on considère qu'il faut franchir une série de filtres avant d'aboutir à une prise de décision.

Dès les années 1970, Ansoff suggéra que les signaux faibles devaient passer trois filtres :

Le filtre d'information ou de surveillance : correspond à la capacité du signal faible à être détecté au milieu de toutes les autres informations perçues par un acteur.

Le filtre de mentalité : renvoie à la capacité du signal à être reconnu après avoir été détecté comme une information pertinente au regard de la situation en cours. Ce filtre est expli- qué par de nombreux biais cognitifs qui font obstacle à la prise de décision. Un certain nombre de biais cognitifs, comme le biais de normalité, le biais de confirmation, le biais d'optimisme, etc. peuvent expliquer pourquoi ces informations ne sont pas retenues. Ces biais sont individuels mais d'autres facteurs organisationnels peuvent aussi expliquer pourquoi les signaux faibles sont ignorés.

Le filtre de pouvoir : renvoie à la prise de décision une fois le signal détecté et sa pertinence reconnue. Les responsables en situation d'arbitrage peuvent décider de ne pas faire de ce signal une priorité malgré le risque encouru.

Plus récemment, un quatrième filtre, celui de la transmission qui renvoie au flux d'information à l'intérieur de l'organisation et qui se situe entre le filtre de mentalité et le filtre de pouvoir a été ajouté. En effet, les personnes qui reçoivent le signal et estiment en premier de son sens et de sa pertinence ne sont généralement pas celles qui ont le pouvoir de décision.

Pour conclure sur ces différentes définitions, nous rappelons qu'Ansoff a été le premier à défi- nir les signaux faibles comme les premiers signes de changement possible mais non confirmés qui peuvent devenir plus tard des indicateurs d'opportunité ou de menace.
Cette définition générale a été reprise par les autres chercheurs où les signaux faibles sont vus en tant que matière première prédictive. Les signaux faibles sont alors définis par leurs caractéristiques : ce sont des données fragmentées, rares, à peine visibles aujourd'hui, mais qui peuvent cacher une tendance.

D'autres auteurs, comme Seidl et Rossel, proposent une approche où les signaux faibles sont considérés comme une « construction socio-cognitive de la réalité qui aide l'expert métier à forger un sens et à agir de manière significative sur la réalité ».

Nous considérons qu'un signal faible se présente comme une donnée anodine mais dont l'interprétation que les experts métier en font peut déclencher une alerte. Cette alerte indique que pourrait survenir un évènement susceptible d'avoir des conséquences en terme d'opportunité ou de menace.

Mise en situation dans un SI (Par Mathieu Pichon)

Imaginez que vous marchez en pleine nuit et qu'un h omme titube tout en effectuant des mouvements étranges. Instinctivement, vous ressentez un signal faible indiquant que cet homme est suspect, voire potentiellement dangereux.

En cybersécurité, il est souvent difficile de détecter un attaquant une fois qu'il s'est infiltré dans le système d'information (SI). La majorité de la détection des signaux faibles repose sur la capacité à repérer la moindre erreur que l'attaquant pourrait commettre une fois implanté.
La détection des signaux faibles repose avant tout sur la recherche et le développement. L'objectif est d'analyser des attaques réelles et d'observer les comportements passifs du « système » qui se déclenchent. Cela peut parfois se traduire par un simple ID d'événement ou par un nombre constant de fichiers temporaires qui apparaissent toujours de la même manière et en même quantité. Pour assurer une bonne détection des signaux faibles, la règle de détection basée sur la corrélation de ces événements ne doit pas générer plus de 10 % de faux positifs.

Pour illustrer cela, reprenons une métaphore : imaginons que je programme une IA pour qu'elle m'alerte d'un potentiel cambrioleur via la caméra de mon jardin, dès que plusieurs événements suspects y surviennent. Si ma règle de détection repose uniquement sur le fait qu'il fait nuit et que la personne est vêtue de noir, je risque de détecter un adolescent vêtu d'un sweat noir, simplement venu récupérer un ballon tombé dans mon jardin. Bien que cet adolescent n'ait initialement rien à faire là, la réponse à ce cas serait très différente de celle que j'adopterais face à un homme de 1m80 avec des intentions malveillantes.

Pour éviter les faux positifs, j'ajouterais donc des critères supplémentaires, tels que la taille de l'individu, son comportement, et ce qu'il fait dans le jardin.
Prenons maintenant un exemple concret : notre source de données initiale est le périmètre de logs où l'attaque se déroule. Imaginons un exemple de dump des credentials d'un AD. Lors de ce dump, un accès à un objet déclenche un ID d'événement. Cependant, ma règle ne peut pas se baser uniquement sur cela. Dans cet exemple, le dump est effectué sur une machine rogue en remote et non en local, donc je ne peux pas me fier aux commandes connues. Je vais réaliser un dump moi-même et analyser tous les signaux faibles du système qui se manifestent, puis vérifier si ces signaux sont récurrents à chaque dump. Je retiendrai ensuite les signaux les plus pertinents pour intégrer ma règle en pré-production.

Ce travail est long et exigeant, mais il est d'une efficacité remarquable en raison de sa pertinence, et les informations obtenues sont d'une valeur inestimable.

POUR EN SAVOIR PLUS SUR LE SUJET

Vous pouvez lire la thèse de doctorat de
ABOU JAMRA Hiba
Disponible gratuitement en ligne

Un mois pour devenir #CyberEngagé

Le mois le plus important de l'année en terme de sensibilisation est de retour !

Lancé en 2012, le Mois européen de la cybersécurité (ECSM) est une initiative de l'Agence de l'Union européenne pour la cybersécurité (ENISA). Son objectif est de sensibiliser les pays de l'UE aux menaces cybernétiques et à leur prévention.

En France, cet événement est décliné sous le nom de «Cybermoi/s» et est mené par les équipes du site de Cybermalveillance.gouv.fr.

En réponse à l'augmentation des fraudes par **ingénierie sociale**, où les cybercriminels manipulent les victimes pour obtenir de l'argent ou des informations personnelles, l'ENISA a choisi de faire de ce sujet le thème principal du Cybermoi/s 2024, en se concentrant sur l'impact de l'intelligence artificielle auprès des jeunes.

Durant tout le mois d'octobre 2024, des activités seront organisées en France et en Europe autour de la cybersécurité : événements de lancement, sessions de sensibilisation, campagnes vidéo, etc. Comme chaque année, divers acteurs publics, privés et associatifs s'uniront pour offrir un programme éducatif visant à promouvoir une culture commune de la cybersécurité en Europe.

CYBER MALVEILLANCE .GOUV.FR

Assistance et prévention en sécurité numérique

Les temps forts du CyberMoi/s

De nombreuses initiatives seront menées durant le mois d'octobre parmi lesquelles :

Coup d'envoi du Cybermoi/s le 1er octobre 2024

- Evénement de lancement à l'Assemblée nationale

- Des conférences dédiées à tous les publics
Opération cyber citoyenne #CyberEngagés : la force du collectif

- Principe : publier sur les réseaux sociaux un conseil en cybersécurité pour aider ses proches

- Action commune à partir du 1er octobre

- Ouvert à tous à titre individuel et professionnel

- Avec le hashtag commun #CyberEngagés

- Visuels à choisir sur https://cybermois.cybermalveillance.gouv.fr à partir du 1er Octobre
Agenda du Cybermoi/s (disponible en septembre)

- Regroupe les actions de sensibilisation mises en place par toutes les entités mobilisées durant le Cybermoi/s

- Vous ou votre entité organisez un événement ? Inscrivez-le dans l'agenda sur https://cybermois.cybermalveillance.gouv.fr

Exemple de sensibilisation à avoir avec ses collaborateurs

Le « Quishing » : l'hameçonnage par QR code

En 2024, l'hameçonnage demeure la principale menace pour toutes les catégories de publics. Parmi les différentes formes d'hameçonnage identifiées par l'ANSSI et le site du gouvernement Cyber Malveillance, on trouve le « quishing », une technique d'hameçonnage utilisant des codes QR.

Les QR codes, similaires aux codes-barres, sont des images codées renfermant des informations telles que des liens vers des sites ou des applications à télécharger. Leur popularité a augmenté ces dernières années grâce à leur grande praticité, permettant d'éviter la saisie manuelle de liens sur les appareils mobiles.

Le QR code : une nouvelle opportunité pour les cybercriminels ?

Comme pour toute innovation technologique, la popularisation des QR codes a rapidement capté l'attention des cybercriminels. Ces dernières années, des QR codes frauduleux ont régulièrement fait la une des actualités nationales concernant l'hameçonnage. Parmi les cas les plus fréquents, on retrouve les faux avis de contravention envoyés à domicile ou placés sur les pare-brise de voitures stationnées dans plusieurs villes de France.
Ces faux avis invitent les destinataires à scanner un QR code pour obtenir plus d'informations ou payer une amende, ce qui les redirige vers des sites malveillants.
Les victimes, en pensant régler leur contravention, fournissent en réalité des informations sensibles aux cybercriminels, telles que des données de carte bancaire ou des informations personnelles.

Un autre exemple courant est celui des faux avis de passage de La Poste déposés dans des boîtes aux lettres. Les destinataires, pensant qu'ils ont manqué une livraison importante, scannent le QR code pour reprogrammer la livraison ou récupérer leur colis.
Malheureusement, ces QR codes mènent souvent à des sites web frauduleux, habilement conçus pour dérober les informations personnelles ou financières des victimes. Cette méthode exploite la confiance des utilisateurs dans les services postaux, rendant l'attaque d'autant plus efficace.

Les cybercriminels ont également pris pour cible les parcmètres et les bornes de recharge pour véhicules électriques en collant de faux QR codes dessus. Les utilisateurs qui scannent ces codes, croyant qu'ils vont payer leur stationnement ou recharger leur véhicule, sont redirigés vers des sites malveillants. Ces sites peuvent soit tenter de voler des informations de paiement, soit installer des logiciels malveillants sur les appareils des utilisateurs. Cette forme d'attaque est particulièrement insidieuse car elle exploite des infrastructures publiques de confiance, rendant les utilisateurs moins méfiants.

En milieu professionnel, des faux QR codes de confirmation de connexion Office365 ont aussi été signalés. Ces codes, envoyés par e-mail sous prétexte de vérifications de sécurité, incitent les utilisateurs à scanner pour confirmer leur connexion, les redirigeant ensuite vers des pages de phishing où leurs identifiants sont volés. Une fois en possession de ces informations, les cybercriminels peuvent accéder aux comptes professionnels des victimes, compromettant des données sensibles de l'entreprise et facilitant d'autres attaques, comme le vol de propriété intellectuelle ou les demandes de rançon.

Ces QR codes frauduleux, connus sous le terme "quishing" en anglais, se sont multipliés de manière préoccupante. L'évolution des tactiques de quishing montre une sophistication croissante des cybercriminels qui cherchent à exploiter les habitudes numériques des utilisateurs. Les campagnes de quishing peuvent être très ciblées, visant des individus ou des entreprises spécifiques pour maximiser l'impact et les gains financiers des attaques.

Nos recommandations

Pour se protéger efficacement contre le quishing, il est crucial de suivre plusieurs conseils de cybersécurité. Tout d'abord, il est important de vérifier la source du QR code avant de le scanner ; assurez-vous qu'il provient d'une source fiable et reconnue, et soyez particulièrement vigilant face aux codes reçus par e-mail ou message texte inattendus. Utilisez des applications de scanner de QR codes réputées qui offrent des fonctionnalités de sécurité telles que l'analyse des URL pour détecter des sites suspects et la prévisualisation des liens avant d'ouvrir une page.

Avant de fournir des informations sensibles après avoir scanné un QR code, examinez attentivement l'URL pour vérifier sa légitimité, en vous assurant qu'elle commence par "https://" et en recherchant des signes de phishing tels que des fautes d'orthographe ou des domaines suspects.

En savoir plus !

Arnaud Leroy - Octobre/Décembre 2024