N°2 - JUILLET/SEPTMEBRE 2024

CYBER-IT

LA CYBER EST UN MARATHON PAS UN SPRINT !

INTERVIEWS

Découverte de nouveaux profils Cyber et IT

OSINT

Les secrets de l'utilisation des photos pour la recherche en osint

SHADOW IT

Analyse de la surface d'attaque externe d'une organisation

EUROPOL

Les dessous de l'opération "EndGame"

DOSSIER SPECIAL

JEUX OLYMPIQUES

QUELS SONT LES RISQUES MAJEURS POUR LES JEUX ?

EDITORIAL

Tout d'abord un grand merci pour vos retours et vos sollicitations vis-à-vis du premier numéro !
Vos commentaires et votre soutien m'ont poussé à me lancer dans la rédaction de ce second opus.

Ce nouveau numéro sera axé sur le plus grand événement sportif de ces prochaines années : les Jeux Olympiques de Paris 2024 !
Les enjeux liés à ce genre de rencontre mettent en lumière les défis liés au maintien de l'infrastructure informatique et de la sécurité.
Je tiens à remercier particulièrement le lieutenant-colonel Lambert pour sa participation au dossier spécial.

Également, j'ai le plaisir de vous présenter une démonstration d'une recherche en OSINT à partir d'un élément d'une photo, qui prend la forme d'un challenge.

Je reviendrai sur la mise hors d'état de nuire de plusieurs domaines et serveurs par Europol lors de l'opération EndGame, survenue lors de ces dernières semaines.

La suite des interviews des acteurs de l'IT et de la cybersécurité, qui m'ont fait l'honneur de répondre à mes questions, sera également au programme.

Je terminerai ce numéro par un petit tour de ce qu'est le Shadow IT et es risques qui en découlent.

J'espère que la lecture de ce second opus saura trouver autant d'intérêt à vos yeux que le premier et qu'il sera apprécié.

Arnaud Leroy

SOMMAIRE

4 **DOSSIER SPECIAL**
Jeux Olympiques
Risques et enjeux

14 **OSINT**
Les photos dans la recherche en sources ouvertes

20 **INTERVIEWS**
Qui sont-ils ?
La suite

26 **SHADOW IT**
Analyse de la surface d'attaque externe d'une entreprise

30 **EUROPOL**
Opération «EndGame»

Jeux Olympiques Paris 2024
Un Défi Majeur pour la Cybersécurité

Jeux et sécurité : un couple tumultueux

Les Jeux olympiques et paralympiques d'été de Paris 2024 se profilent comme l'événement le plus monumental en France depuis l'Exposition universelle de 1900.

Les chiffres sont vertigineux : un budget de 7 milliards d'euros, une audience de 4 milliards de téléspectateurs et 12 millions de spectateurs prévus. Cependant, espérons que les cyberattaques ne connaissent pas une hausse record.

Les précédents Jeux Olympiques ont montré que la menace est réelle. Lors des Jeux de Tokyo 2020, par exemple, des cyberattaques ont tenté de perturber l'événement, bien que la plupart aient été neutralisées grâce à des mesures de sécurité robustes. Paris 2024 entend tirer parti de ces expériences pour améliorer encore davantage ses défenses.

Ces Jeux peuvent-ils faire exception ?

Les systèmes d'information jouent un rôle central dans les Jeux, en assurant la transmission instantanée des résultats, la diffusion des images, et la gestion des accréditations pour les athlètes, les équipes et les officiels.
Tout cela place donc les systèmes d'information au cœur du fonctionnement des Jeux.

Les JO sont l'un des événements les plus attaqués du monde. C'est le premier cauchemar du directeur de la technologie, selon Bruno Marie-Rose le directeur de la technologie de Paris 2024.

Les Jeux Olympiques, en tant que rassemblement planétaire, sont fréquemment l'arène de jeux politiques. L'exclusion de la Russie des JO de Tokyo 2022 et les prises de position politiques de certains athlètes en sont des illustrations marquantes. Cette facette politique les expose à des menaces potentielles, aussi bien de la part d'acteurs étatiques que de cybercriminels.

Les Jeux de Paris 2024 devraient être la cible de milliards de cyberattaques, « huit à dix fois plus que les Jeux de Tokyo »

Bruno Marie-Rose
(directeur de la technologie de Paris 2024)

La France, médaille d'or de la sécurité ?

Comment contrer un ennemi invisible ? Prévention, formation, communication sont-ils suffisants pour limiter au maximum les risques lors de ces jeux ?

L'histoire des Jeux Olympiques est jalonnée d'une multitude d'incidents et d'attaques, mettant en évidence les risques inhérents à la tenue d'un événement d'une telle ampleur.

Le tragique assassinat de certains participants lors des Jeux de Munich en 1972 demeure gravé dans les mémoires, rappelant de manière poignante la vulnérabilité des Jeux face aux menaces extérieures. En outre, des cas de cyberattaques ont été signalés lors de précédentes éditions, soulignant ainsi la nécessité impérieuse de renforcer la sécurité numérique en prévision de Paris 2024.

Pour contrer ces menaces, des mesures techniques robustes s'avèrent indispensables. Il est essentiel de mettre en place des dispositifs de protection contre les attaques DDoS et les logiciels malveillants afin de garantir la disponibilité ininterrompue des réseaux. Parallèlement, il convient de ne pas sous-estimer l'importance de sensibiliser le public.

Des programmes de formation sur la sécurité numérique et physique destinés au personnel et aux athlètes revêtent une importance capitale. En outre, une communication transparente et précise avec le public est nécessaire pour anticiper les crises éventuelles et garantir la sécurité et le bien-être de l'ensemble des participants.

Le Comité d'Organisation des Jeux Olympiques se prépare à contrer les cyberattaques en s'appuyant sur les leçons des éditions précédentes. Chaque édition est unique, avec des contextes changeants, des menaces évolutives et des attaques de plus en plus nombreuses.

Pour faire face à des cyberattaques toujours plus sophistiquées et fréquentes, les autorités françaises mettent en place des mesures renforcées. L'ANSSI a conclu un accord de coopération avec le NISC (National Center of Incident Readiness and Strategy for Cybersecurity) japonais, permettant de renforcer les échanges et le partage d'expériences en matière de cybersécurité des grands événements sportifs. En parallèle, l'ANSSI intensifie ses campagnes de communication pour sensibiliser le public à l'importance de l'hygiène numérique.

La menace cyber qui plane sur les Jeux Olympiques et Paralympiques de Paris 2024, dans la continuité des éditions précédentes, est principalement liée aux perturbations étatiques. Des attaquants pourraient tenter de cibler certains systèmes pour pénétrer dans les enceintes sans autorisation, ou pour provoquer l'évacuation des spectateurs et leur rassemblement à l'extérieur des zones sécurisées, facilitant ainsi des attaques terroristes.

DOSSIER SPECIAL

Mesures concrètes et mise en oeuvre

Le Comité d'Organisation des JO 2024, conscient de la menace des cyberattaques depuis plus de trois ans avant l'événement, mise sur la collaboration internationale entre gouvernements, entreprises et organisations impliquées pour assurer la sécurité.

Pour les Jeux Olympiques de Paris 2024, plusieurs mesures de sécurité sont mises en place pour garantir la protection de l'événement contre diverses menaces, notamment les cyberattaques et les attaques physiques.

Les mesures mises en place durant ses jeux de Paris 2024 peuvent être classées en cinq points :

- **La cybersécurité**
- **Sécurité physique**
- **Sensibilisation**
- **Technologies avancées**
- **Coordination**

La Cybersécurité

Pour les Jeux Olympiques de Paris 2024, un budget substantiel de plus de 17 millions d'euros est alloué à la cybersécurité, englobant une série de mesures détaillées de prévention et de défense contre les cybermenaces.

Ce budget comprend une variété d'initiatives visant à assurer la protection maximale de l'événement. Parmi ces initiatives, des simulations grandeur nature sont réalisées pour préparer les équipes de sécurité à une diversité de scénarios d'attaque, exécutant des exercices réalistes qui simulent des cyberattaques potentielles, y compris les attaques DDoS, les intrusions réseau et les tentatives de phishing. Ces simulations visent à renforcer les capacités de réponse rapide et efficace aux incidents.

En parallèle, le développement de logiciels intègre des protocoles de sécurité extrêmement stricts. Cela inclut des audits de code rigoureux pour détecter et corriger les vulnérabilités avant le déploiement, ainsi que la mise en place d'un système de mises à jour régulières pour répondre aux nouvelles menaces. Parallèlement, l'infrastructure réseau et les serveurs sont conçus avec des niveaux élevés d'isolation et des barrières de sécurité robustes.

L'architecture réseau est segmentée pour protéger les différents niveaux du réseau, et des techniques de séparation sont employées pour assurer l'étanchéité des couches réseau et des serveurs, empêchant ainsi les intrusions et protégeant les données sensibles.

Des audits de sécurité réguliers sont menés pour identifier les vulnérabilités potentielles et appliquer les correctifs nécessaires de manière proactive. Des centres opérationnels de sécurité (SOC) sont également mis en place pour surveiller en temps réel les activités réseau, permettant une détection immédiate et une réponse rapide aux incidents de sécurité. Cette surveillance continue est cruciale pour garantir que toute anomalie soit détectée et traitée rapidement, minimisant ainsi les risques d'intrusion.

La coopération internationale est un pilier essentiel de cette stratégie de défense. Un accord de partenariat avec le National Center of Incident Readiness and Strategy for Cybersecurity (NISC) du Japon permet d'échanger des informations précieuses et des expériences en matière de cybersécurité. Ces échanges enrichissent les capacités de défense des deux nations, fournissant des aperçus sur les meilleures pratiques et les dernières innovations en matière de sécurité.

De plus, des collaborations avec d'autres agences de cybersécurité à travers le monde renforcent les défenses cybernétiques, assurant une approche coordonnée et intégrée pour contrer les menaces globales. Ces partenariats permettent de bénéficier d'une expertise diversifiée et d'une meilleure anticipation des attaques potentielles, contribuant ainsi à la sécurité globale des Jeux Olympiques de Paris 2024.

NISC
National center of Incident readiness and Strategy for Cybersecurity
内閣サイバーセキュリティセンター

La sécurité physique

Pour ces Jeux Olympiques de Paris 2024, un ensemble de mesures exhaustives de sécurité physique est mis en place pour garantir la protection de tous les participants, spectateurs et personnels. La surveillance est intensifiée grâce à l'installation de caméras de surveillance à haute résolution, stratégiquement placées dans et autour des sites des Jeux. Ces caméras permettent une observation continue et détaillée des activités, aidant à identifier rapidement tout comportement suspect ou toute menace potentielle.

En complément, des drones de sécurité sont déployés pour une surveillance aérienne, offrant une perspective globale des lieux et la capacité de détecter des incidents à une plus grande échelle et en temps réel.

Les contrôles d'accès sont renforcés de manière rigoureuse. L'utilisation de badges d'identification et de technologies biométriques, telles que la reconnaissance faciale et les empreintes digitales, assure que seules les personnes autorisées peuvent pénétrer dans les zones sensibles.
Des barrages et des points de contrôle sont établis à tous les points d'entrée stratégiques, où des vérifications d'identité minutieuses et des autorisations d'accès sont effectuées. Ces mesures visent à empêcher toute intrusion non autorisée et à garantir que l'accès aux installations soit strictement réservé aux personnes accréditées.

Le personnel de sécurité est considérablement renforcé pour l'événement. Une présence accrue de la police et des forces de sécurité assure le maintien de l'ordre public et une réponse rapide aux incidents. Ces forces sont complétées par des agents de sécurité privés, spécialement formés pour renforcer la surveillance et intervenir en cas de besoin. Ensemble, ils patrouillent les sites des Jeux, surveillent les foules, et sont prêts à réagir rapidement en cas d'urgence.

La prévention des attaques terroristes est un aspect crucial de la sécurité des Jeux Olympiques. Le plan Vigipirate, un dispositif national de vigilance et de prévention des actes terroristes, est renforcé avec des mesures spécifiques adaptées aux Jeux.

Cela inclut une augmentation des patrouilles, des contrôles plus stricts, et une vigilance accrue dans toutes les zones liées aux Jeux.
En parallèle, une collaboration étroite avec les services de renseignement est en place pour identifier et neutraliser les menaces potentielles avant qu'elles ne se concrétisent. Ce partenariat permet d'accéder à des informations de renseignement actualisées, facilitant une réponse proactive aux menaces identifiées.

Ces efforts coordonnés, incluant des technologies de pointe, une présence humaine renforcée, et des stratégies de prévention proactives, visent à créer un environnement extrêmement sécurisé pour les Jeux Olympiques de Paris 2024.

Cette approche globale garantit non seulement la sécurité physique des participants et des spectateurs, mais aussi une réponse rapide et efficace à toute éventualité, assurant ainsi la réussite et la sécurité de cet événement de grande envergure.

On s'attend à tout ! Nous voyons déjà des attaquants qui cherchent à cibler les personnes, avec des tentatives de connexion. Nous faisons attention

Bruno Marie-Rose
(directeur de la technologie de Paris 2024)

La sensibilisation

Pour les Jeux Olympiques de Paris 2024, la sensibilisation et la formation constituent des éléments fondamentaux de la stratégie de sécurité, visant à préparer de manière exhaustive tous les acteurs impliqués à faire face aux divers défis potentiels, qu'ils soient liés à la cybersécurité ou à la sécurité physique.

Les campagnes de sensibilisation sont élaborées avec soin pour atteindre un large public, englobant non seulement les spectateurs, les athlètes, et le personnel sur site, mais aussi les parties prenantes externes, tel les partenaires des Jeux. Elles fournissent des informations détaillées sur les bonnes pratiques en matière de cybersécurité, allant de l'identification des menaces potentielles à la gestion sécurisée des données personnelles et la vigilance face aux tentatives de phishing. Ces campagnes ne se limitent pas à la sphère numérique, elles abordent également les mesures de sécurité physique, telles que les procédures d'évacuation en cas d'urgence, les points de rassemblement, et les protocoles de signalement des incidents. Les formations spécifiques sont minutieusement adaptées aux besoins et aux responsabilités de chaque groupe impliqué dans l'événement. Pour le personnel et les bénévoles chargés de l'organisation et de la gestion des Jeux, ces formations comprennent une immersion approfondie dans les protocoles de sécurité, la gestion des foules, les procédures d'urgence et la coordination des interventions en cas de crise.

Des simulations pratiques sont intégrées à ces formations pour permettre aux participants de mettre en pratique leurs connaissances et leurs compétences dans des scénarios réels, renforçant ainsi leur préparation et leur réactivité en situation d'urgence.

Quant aux athlètes et aux délégations, des sessions de sensibilisation spécifiques sont organisées pour les informer des risques potentiels liés à la cybersécurité et à la sécurité physique.

Ces sessions fournissent des conseils pratiques sur la protection des informations personnelles, la sécurisation des appareils électroniques et les mesures à prendre en cas de menace ou d'incident de sécurité. Elles sensibilisent également les participants aux procédures de signalement des comportements suspects ou des activités potentiellement dangereuses, encourageant ainsi une participation active à la sécurité collective. En intégrant de manière exhaustive la sensibilisation et la formation à tous les niveaux de l'organisation des Jeux Olympiques, Paris 2024 vise à créer un environnement sécurisé et résilient pour tous les participants et les spectateurs. Ces initiatives renforcent la culture de la sécurité, promouvant une vigilance collective et une réactivité efficace face aux menaces émergentes, et contribuant ainsi au succès et à la sûreté de cet événement d'envergure internationale.

Pour compléter ces initiatives, des ressources supplémentaires sont allouées à la création de matériel pédagogique interactif, notamment des vidéos éducatives, des infographies et des guides pratiques. Ces supports permettent de rendre les informations sur la cybersécurité et la sécurité physique plus accessibles et engageantes, favorisant ainsi une meilleure compréhension et une adoption plus efficace des bonnes pratiques.

Egalement, chaque élèves de primaire s'est vu remettre une pièce commémorative de deux euros, ce qui contribue à les intéresser aux jeux de Paris.

Pièce de deux euros commémorative
(offerte aux élèves de primaire)

Technologies avancées

L'utilisation de l'intelligence artificielle permet de surveiller en permanence les réseaux pour détecter des anomalies pouvant indiquer des cyberattaques. Les systèmes d'IA sont programmés pour analyser d'énormes volumes de données en temps réel, identifiant des schémas suspects et des comportements inhabituels qui pourraient signaler une menace imminente.
Grâce à ces capacités, les équipes de sécurité peuvent réagir rapidement pour neutraliser les attaques avant qu'elles ne causent des dommages significatifs.

L'intelligence artificielle est également employée pour la gestion de la foule. Des applications d'IA analysent les flux de personnes, en utilisant des données en temps réel provenant de caméras de surveillance et de capteurs, afin de comprendre les mouvements de foule et anticiper les situations potentiellement dangereuses.

Par exemple, si un attroupement commence à se former dans une zone critique, l'IA peut alerter les responsables de la sécurité pour qu'ils prennent des mesures préventives, comme rediriger les flux de personnes ou déployer du personnel supplémentaire.
Cette technologie aide à maintenir l'ordre et à garantir la sécurité des spectateurs en évitant les surcharges et les situations de panique.

En parallèle, la technologie blockchain est mise en œuvre pour sécuriser la billetterie des Jeux Olympiques. La blockchain garantit l'authenticité des billets en rendant chaque ticket unique et infalsifiable. Chaque billet est enregistré dans un registre numérique décentralisé, ce qui empêche toute duplication ou modification non autorisée. Cette méthode innovante de gestion des billets réduit considérablement le risque de fraude et assure que les spectateurs puissent accéder aux événements en toute confiance. En outre, la transparence offerte par la blockchain permet de suivre chaque billet depuis sa création jusqu'à son utilisation, offrant une traçabilité complète et renforçant encore la sécurité.

L'implémentation de ces technologies avancées nécessite une infrastructure sophistiquée et une coordination étroite entre les différents systèmes de sécurité. Des équipes dédiées travaillent en continu pour développer, tester et améliorer ces systèmes afin de s'assurer qu'ils fonctionnent parfaitement pendant les Jeux.

Cette approche proactive et technologique de la sécurité contribue à la création d'un environnement sûr et fiable pour les Jeux Olympiques de Paris 2024, assurant la protection des données et la sécurité physique des participants et des spectateurs.

Coordination et communication

Un centre de commandement unifié sera établi pour coordonner les efforts de sécurité entre les différentes agences et services impliqués. Ce centre jouera un rôle crucial dans la gestion des opérations de sécurité, assurant une communication fluide et une réponse rapide aux incidents.

Grâce à des systèmes de communication avancés, les informations pourront être transmises en temps réel, permettant ainsi une coordination efficace et une réaction immédiate face aux éventuelles menaces. Ce dispositif centralisé est essentiel pour garantir que toutes les parties prenantes soient synchronisées et puissent agir de manière cohérente et rapide en cas d'urgence.

En parallèle, la collaboration internationale sera renforcée pour échanger des informations cruciales sur les menaces et les meilleures pratiques en matière de sécurité.

Des partenariats avec d'autres pays permettront de partager des données et des stratégies, enrichissant ainsi les capacités de défense collective. Cette coopération inclura également un support logistique et technique mutuel, où les pays s'entraideront pour renforcer leurs capacités de réponse aux incidents.

En combinant les ressources et l'expertise internationale, les organisateurs des Jeux pourront anticiper et neutraliser plus efficacement les menaces potentielles, assurant ainsi la sécurité de l'événement à une échelle globale.

Le pire serait des attaques qui provoqueraient une interruption ou une perturbation des compétitions.

Un de mes homologues en 2018 aux JO de Pyeongchang avait vu quelques systèmes s'éteindre avant la cérémonie d'ouverture. Je ne veux pas que cela arrive !

Bruno Marie-Rose
(directeur de la technologie de Paris 2024)

Plus de 10 ans de cyber-agressions visant les Jeux Olympiques

Après avoir subi 4 milliards d'attaques cyber lors des Jeux de Tokyo en 2021 et un demi-milliard à Rio en 2016, quel sera l'impact en 2024 et quelles mesures pouvons-nous prendre pour prévenir les risques ?

En 2008, durant les Jeux de Pékin, plusieurs sites trompeurs avaient été érigés pour la vente de billets falsifiés. Mais ce n'est qu'à partir de l'attaque perpétrée lors de la cérémonie d'ouverture des Jeux de Londres en 2012 que la question de la cybersécurité est devenue une préoccupation majeure pour les organisateurs.

LONDRES 2012

Les jeux de Londres représentent un tournant dans l'attention portée par les cybercriminels aux Jeux olympiques. À cette époque, dès le jour de la cérémonie d'ouverture, plus de 212 millions de cyberattaques ont été enregistrées, incluant plusieurs attaques coordonnées telles qu'une perturbation des services sur l'infrastructure électrique.

SOTCHI 2014

En 2014, lors des Jeux olympiques d'hiver à Sotchi, aucun incident notable en matière de cybersécurité n'a été rapporté. Est-ce dû à une communication étatique hermétique en Russie, au désintérêt des cybercriminels, ou à la crainte de représailles ? Cette interrogation demeure sans réponse...

RIO 2016

Durant les Jeux de Rio, les données sont alarmantes avec un total de cyberattaques atteignant un demi-milliard, soit une fréquence de 400 attaques par seconde. Des attaques DDoS d'envergure considérable et répétées ont visé les sites web des partenaires des Jeux olympiques, et cela, plusieurs mois avant le début de la cérémonie d'ouverture.

PYEONG-CHANG 2018

Pendant les jeux de 2018, le problème s'amplifie publiquement lors de la cérémonie d'ouverture des Jeux de PyeongChang. Des difficultés sont rencontrées : certains spectateurs ne peuvent pas imprimer leurs billets, des soucis de Wi-Fi sur le site, une panne d'écrans, des capteurs d'accès défaillants, et une application officielle des JO dysfonctionnelle, affectant l'accès à la billetterie, aux horaires, aux infos sur les hôtels, et aux cartes d'accès. Les conséquences sont vite ressenties.

TOKYO 2020 (2021)

Même avec les Jeux Olympiques de Tokyo 2021 se déroulant à huis clos après avoir été reportés d'un an en raison de la pandémie mondiale, l'organisation a été bombardée de 4,4 milliards de cyberattaques. La Nippon Telegraph and Telephone Corporation rapporte que ces attaques ont exploité diverses méthodes, notamment des courriels de phishing et la création de faux sites web ressemblant aux plateformes officielles des Jeux.

PEKIN 2022

En 2022, lors des Jeux d'hiver de Pékin, c'est l'application officielle de lutte contre la Covid-19, nommée My2022, qui suscite la controverse en raison des craintes de cyber-espionnage. Une analyse de rétro-ingénierie de l'application aurait révélé ultérieurement que les échanges des athlètes étaient collectés, analysés et stockés sur des serveurs chinois.

Paris, terrain propice aux attaquants ?

Les hostilités semblent déjà déclarées du côté des attaquants, en tout cas ça semble en prendre le chemin quand on voit les vols de données concernant les jeux de Paris.

Récemment, plusieurs incidents de sécurité liés aux Jeux Olympiques de Paris 2024 ont été signalés, attirant l'attention sur les vulnérabilités potentielles.

Un des incidents les plus notables concerne le vol d'un ordinateur portable et de clés USB contenant des informations sur les Jeux.
Un employé de la mairie de Paris monte à bord d'un train en direction de Creil, stationné sur le quai numéro 18 de la gare du Nord, dans le dixième arrondissement. Alors que le train subit un retard et qu'il s'apprête à changer de train, il découvre que sa sacoche a disparu.

Il précise plus tard avoir déposé cette sacoche dans le compartiment à bagages situé au-dessus de son siège. Quelques dizaines de minutes plus tard, vers 19h30, il se rend au commissariat de la gare pour signaler le vol et déposer une plainte.

Le parquet de Paris précisera plus tard que la clé USB volée ne contenait que des "notes en lien avec la circulation dans Paris lors des Jeux olympiques", et non des informations sensibles sur les dispositifs de sécurité. Il s'agissait de "banals plans de Paris".

Es-ce pour donner le change ou rassurer les futurs spéctateurs ? La question se pose d'autant que ce n'est pas le seul incident relaté dans le médias...

Deux mois après cet événement, vers 2h du matin à Sceaux (Hauts-de-Seine), le propriétaire d'un pavillon est réveillé par un bruit de fenêtre cassée... Il constate qu'il a été victime d'un cambriolage. Dans la foulée, il réalise que trois ordinateurs portables ont disparu. Surpris en plein vol, les attaquants sont parvenus à prendre la fuite avec le butin qu'ils étaient venus chercher.

Lorsque les policiers, arrivent sur place, la victime leur explique qu'elle est employée chez Thalès et que l'un des ordinateurs volés est destiné à un usage professionnel.
La victime indique que cet ordinateur contient également des "informations sensibles relatives à la surveillance territoriale et à la sécurité pour les Jeux olympiques".

Ces événements doivent-ils nous alerter ou bien ne sont-ils que de simples coïncidences ?

La sûreté, comme la sécurité de nos salariés, de nos clients, et de nos activités sont des enjeux capitaux pour le groupe et nous appliquons des procédures de sécurité très strictes, comprenant l'usage d'un système d'authentification forte ou encore de chiffrement

Réaction du groupe Thales

Rencontre avec le lieutenant-colonel Sophie LAMBERT du COMCYBER-MI

Qui de mieux placé que la responsable du département de l'anticipation et de la gestion de crise cyber du Commandement du ministère de l'intérieur dans le cyberespace pour évoquer les risques liés aux JO ?

Nous constatons une augmentation significative des activités cybercriminelles, en écho aux événements sportifs d'ampleur internationale précédents.

Sophie LAMBERT

Qui est Sophie LAMBERT ?

Je suis la lieutenant-colonel Sophie Lambert, cheffe du département de l'anticipation et de la gestion de crise au sein du commandement du ministère de l'Intérieur dans le cyberespace.

Notre rôle consiste à élaborer un état de la menace le plus exhaustif possible en matière de cyber, et ainsi adapter notre réponse opérationnelle, contrer les cybermenaces et lutter efficacement contre la cybercriminalité.

Qu'est-ce que le COMCYBER-MI ?

Le Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI) joue un rôle central dans la protection des Jeux de Paris 2024 contre les cybermenaces.

Nos missions incluent :

La surveillance continue du cyberespace pour détecter et neutraliser les menaces potentielles.

La coordination avec les partenaires nationaux et internationaux pour échanger des informations sur les cybermenaces.

La mise en place de protocoles de diffusion rapide de toute détection ou suspicion de cyberattaque afin de minimiser l'impact sur les Jeux.

La formation et la sensibilisation des acteurs impliqués aux bonnes pratiques de cybersécurité.

Notre centre d'analyse et de regroupement des cybermenaces centralise et analyse des données essentielles pour identifier les cybercriminels, analyser leurs modes opératoires, caractériser les cybermenaces et anticiper les crises. Nous produisons des alertes et des analyses spécifiques pour informer nos partenaires en cas de cyberattaques ou de nouvelles menaces émergentes.

Nous sommes positionnés au centre national de commandement stratégique (CNCS) pour les Jeux de Paris à Beauvau aux côtés de nos partenaires, dont l'ANSSI.

La cybersécurité est une responsabilité partagée. Alors que nous nous approchons des JO de Paris 2024, je tiens à souligner l'importance de la vigilance de chacun. Ensemble, nous pouvons faire face aux défis cyber, assurer la sécurité de cet événement mondial et afficher notre cyberrésilience pour décourager nos adversaires.

Je vous encourage également à ne pas laisser les cyberattaques sans réponse. Déposer plainte est une démarche essentielle pour vous protéger, protéger vos proches et contribuer à la sécurité de tous. Les menaces évoluent constamment, et il est essentiel de rester vigilant, de s'informer, de se former et de mettre en place des mesures de protection adaptées. Ne sous-estimez pas l'importance d'une véritable culture de la cybersécurité.

Quels sont les risques les plus importants ou marquants selon vous pour ces jeux ?

Cet événement mondial, qui attirera des millions de visiteurs et de spectateurs, représente non seulement un moment sportif exceptionnel, mais également une cible potentielle pour diverses menaces, particulièrement dans le domaine numérique.

Les Jeux de Paris 2024 représentent une opportunité de choix pour les cybercriminels, motivés par des raisons lucratives, de sabotage, d'hacktivisme ou encore d'espionnage. Les risques les plus importants incluent :

- Les attaques DDoS visant à perturber les services en ligne.
- Les rançongiciels, paralysant les systèmes informatiques jusqu'au paiement d'une rançon.
- Les escroqueries massives ou ciblées, exploitant la popularité de l'événement.
- Les défigurations de sites Web, souvent utilisées pour diffuser des messages de propagande.
- Les vols et diffusions massives de données sensibles, compromettant la confidentialité et l'intégrité des informations.

Les conflits internationaux et le contexte politique et social en France pourraient également intensifier les cyberattaques, visant à perturber l'événement et à véhiculer des messages de propagande. Cet événement à fort retentissement médiatique profiterait aux cybercriminels pour perturber la tenue des JO 2024, déstabiliser les intérêts français et véhiculer des messages de propagande. Les Jeux de Paris constituent également une vitrine pour recruter dans leurs rangs.

À l'approche des Jeux Olympiques et Paralympiques de 2024, nous constatons une augmentation significative des activités cybercriminelles, en écho aux précédents événements sportifs internationaux. Pour l'année 2023, 278 770 atteintes numériques ont été enregistrées par les services de police et de gendarmerie, contre 255 320 en 2022. Cela représente une augmentation de 40 % des infractions liées au cyber au cours des cinq dernières années, avec une moyenne annuelle de 8 %.

Badge d'unité COMCYBER-MI

Depuis janvier 2024, nous avons multiplié par trois nos détections d'attaques DDoS, vols de données et défigurations de sites. Certains hackers pourraient déjà être infiltrés dans des systèmes critiques, prêts à frapper au moment opportun. Entre 2022 et 2023, les cyberattaques ont augmenté de 30 % selon l'ANSSI.

Plusieurs hypothèses peuvent expliquer cette hausse : un développement des usages numériques, un accroissement de la surface d'attaque possible, mais aussi une amélioration du signalement des infractions. Toutefois, il existe encore un chiffre noir de la cybercriminalité, car seulement 0,4 % des infractions font l'objet d'un dépôt de plainte, ce qui souligne la sous-déclaration massive des attaques.

Si l'on ne s'en tient aujourd'hui qu'à l'organisation des Jeux Olympiques, celle-ci représente une cible attractive pour les cybercriminels. Il est probable que nous observions une augmentation des tentatives de cyberattaques, ciblant à la fois les infrastructures des jeux, les participants et les spectateurs.

Les attaques par rançongiciel et les vols/diffusions de données sensibles représentent nos principales préoccupations, en raison de leur potentiel de perturbation significative. Nous surveillons également les escroqueries ciblant les spectateurs, les défigurations de sites officiels et les risques liés à la supply chain. Les conséquences de ces attaques pourraient être désastreuses :

- Perturbation de la transmission des rencontres sportives.
- Suspension de l'accès du personnel habilité aux zones sécurisées.
- Perturbation des transports publics et des dispositifs de gestion des spectateurs.
- Perturbation des infrastructures des sites olympiques.
- Escroqueries en lien avec l'événement, comme le typosquatting.

Pour assurer la sécurité des Jeux, plusieurs mesures ont été mises en place.

Quelles mesures sont mises en place pour assurer ces Jeux ?

La création du CNCS dédié aux grands évènements sportifs tels que les Jeux, opérant 24/7.
L'intégration de solutions technologiques avancées pour la détection et la prévention des cyberattaques.
La réalisation de simulations et d'exercices réguliers pour tester et améliorer notre capacité de réponse.
La collaboration étroite avec les organisateurs des Jeux, les autorités publiques, les partenaires nationaux (publics, privés) et internationaux pour une approche de sécurité globale et coordonnée. Nous sommes bien conscients des risques accrus dus à la surexposition et à la surface d'attaque qu'offre les JO.

Les photos dans la recherche en source ouverte

Comment trouver des informations à partir de photos ?

L'OSINT : Qu'est-ce que c'est ?

L'OSINT (Open Source INTelligence), ou Renseignement d'Origine Source Ouverte (ROSO), consiste à collecter et analyser des données provenant de sources accessibles publiquement. Cela peut inclure des sites web, des réseaux sociaux, des registres publics, etc. L'objectif est de transformer ces données en informations utiles pour la prise de décision.

Les données en source ouverte sont accessibles au public de manière légale. Elles peuvent être gratuites ou nécessiter un achat ou une démarche officielle (comme un article de presse ou un Kbis). Il est important de savoir identifier et collecter ces données de manière légale et efficace.

Les sous-familles de l'OSINT

SOCMINT : renseignement à partir des réseaux sociaux.

IMINT : renseignement à partir d'images.

SIGINT : renseignement à partir de signaux électroniques.

HUMINT : renseignement à partir de sources humaines.

GEOINT : renseignement à partir d'imagerie géospatiale.

MASINT : renseignement à partir de mesures.

Le cycle du renseignement

Le cycle du renseignement comprend quatre phases : identification des besoins, collecte, analyse, et diffusion, avec parfois une cinquième phase de décision.

Les besoins

Il s'agit de définir les problématiques et d'identifier les informations utiles en posant des questions spécifiques pour orienter la recherche.

La collecte

Cette phase consiste à déterminer le périmètre des sources, collecter des données fiables et pertinentes, et documenter chaque pivot de recherche pour éviter les oublis.

L'analyse

Cette phase transforme les données en informations en les interprétant et les mettant en perspective, éliminant les faux positifs, et établissant des chronologies si nécessaire.

La diffusion et la décision

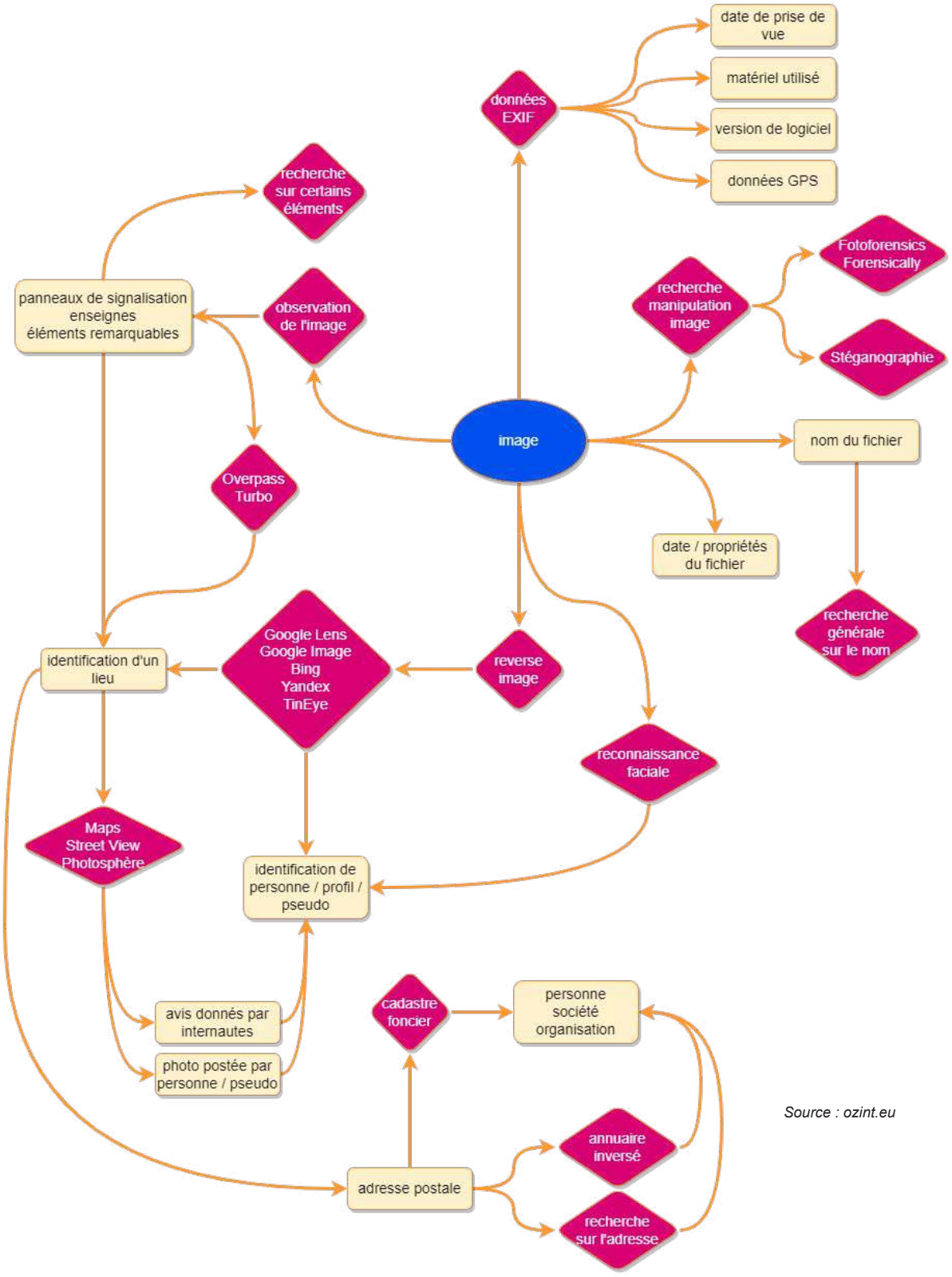
La diffusion doit être adaptée au rôle de chacun et aboutir à une prise de décision, pouvant réorienter les besoins et relancer un nouveau cycle de recherche.

Pour débuter l'analyse d'une image, il est recommandé de l'observer attentivement pour y repérer des éléments significatifs. Ceux-ci pourront ensuite être isolés pour des recherches spécifiques. L'examen des données EXIF est essentiel, tout comme l'examen des propriétés du fichier (dates de création, nom de fichier).

Ensuite, une recherche d'image inversée peut être utile, éventuellement en isolant une partie de l'image. Si un lieu est identifié, l'utilisation d'outils de visualisation cartographique, comme Google Street View et Photosphère, s'impose.
En fonction du lieu, il peut être nécessaire de rechercher à partir de l'adresse ou du cadastre.

Enfin, si l'image a été postée par un internaute, une recherche à partir de son pseudo peut fournir des informations supplémentaires.

Voici un exemple d'organigramme permettant de se faire une idée des informations que l'on peut extraire depuis une simple photo.



Source : ozint.eu

Mise en situation concrète : Des carottes, des lapins et des statues

Voici un exemple de challenge d'OSINT imaginé par Ozint.eu
(avec l'autorisation de Julien Metayer pour la diffusion)

Avec seulement l'image fournie peut-on répondre au trois questions suivantes ?

1. Combien de carottes et de lapins cette statue salue-t-elle en juin 2022 ?

Avant son entreprise actuelle, le créateur de l'oeuvre avait une autre structure commerciale aujourd'hui fermée.

2. Dans quelle ville était domiciliée cette structure ?

Dans cette ville, le monument aux morts a été créé par un sculpteur célèbre qui a proposé dans les années 30 sa vision de l'homme originel.

3. Quel est le nom du site historique situé à 18 km de cette oeuvre ?

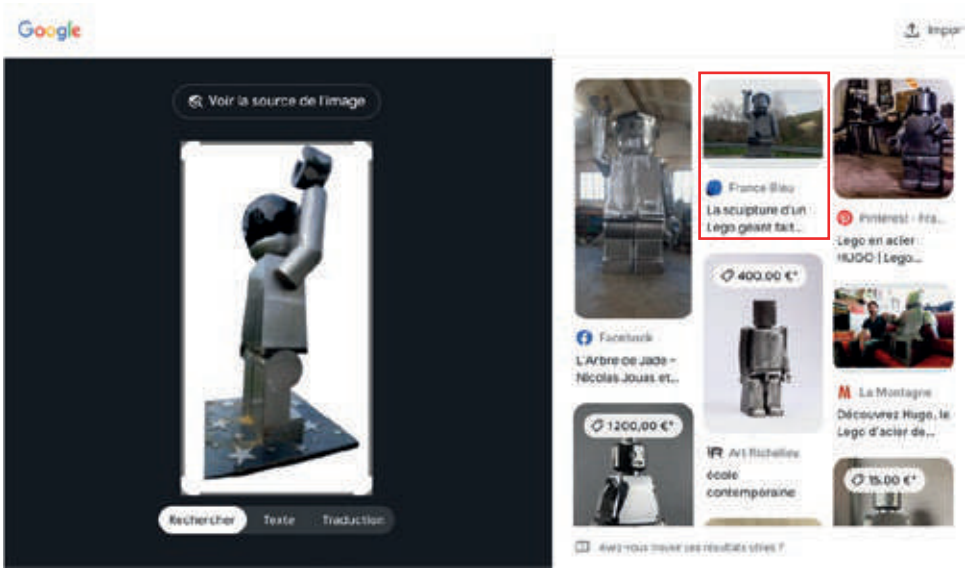


Figure 1 - Google Lens

Une recherche inversée dans Google Lens *(Figure 1)* nous permet de faire ressortir une image qui semble proche de la photo qui nous a été fournie.

Nous voyons une photo d'un article de France Bleu *(Figure 2)* qui semble parler de la statue que nous recherchons.

A la lecture de l'article nous récupérons des informations essentielles : La ville dans laquelle se trouve la statue : ***Lodève*** ainsi que le nom de l'artiste qui a réalisé celle-ci : ***Nicolas Jouas*** *(Figure 3)*

Figure 2 - Photo Article France Bleu

Les automobilistes ont eu la surprise de voir apparaître cette monumentale figurine Lego® mi-décembre à la sortie de Lodève. Avec ses **quatre mètres de haut**, et son air avenant, la sculpture fait sensation, et les curieux sont nombreux à s'arrêter pour prendre des photos.

C'est dans l'atelier Takavenir que l'artiste Nicolas Jouas et son collectif ont imaginé et créé la sculpture. **L'atelier est spécialisé dans les œuvres d'arts en métal**, et voulait fabriquer une création taille XXL. "*Techniquement c'était plus pratique de réaliser un Lego_™_, explique Nicolas, il suffisait de prendre une figurine et d'adapter ses dimensions à une œuvre de très grande taille*".

Figure 3 - Article France Bleu

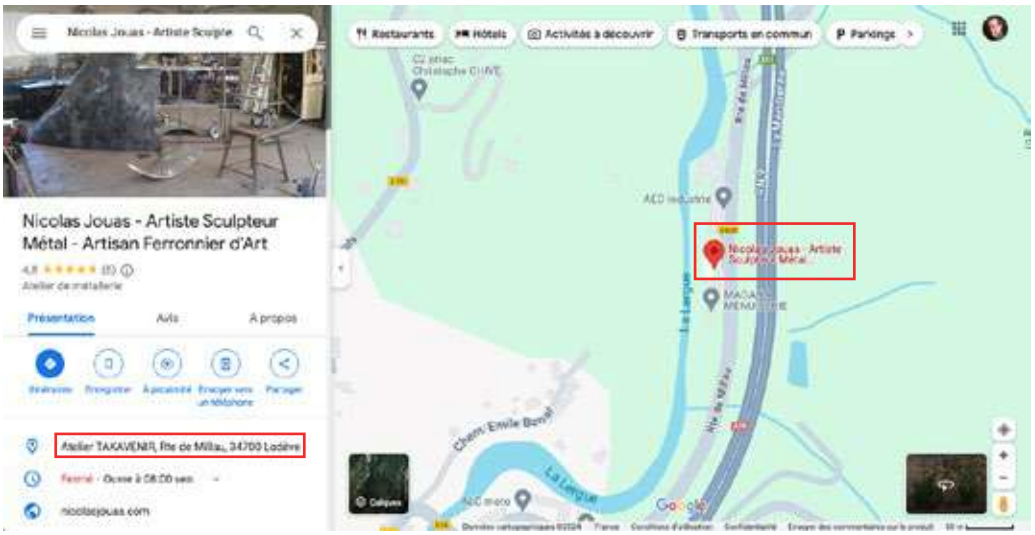


Figure 4 - Google street view

Si l'on recherche sur Google Street View le nom de l'artiste *(Figure 4)* on retrouve bien le nom de la ville de Lodève citée dans l'article précédent ainsi que la présence de son atelier.

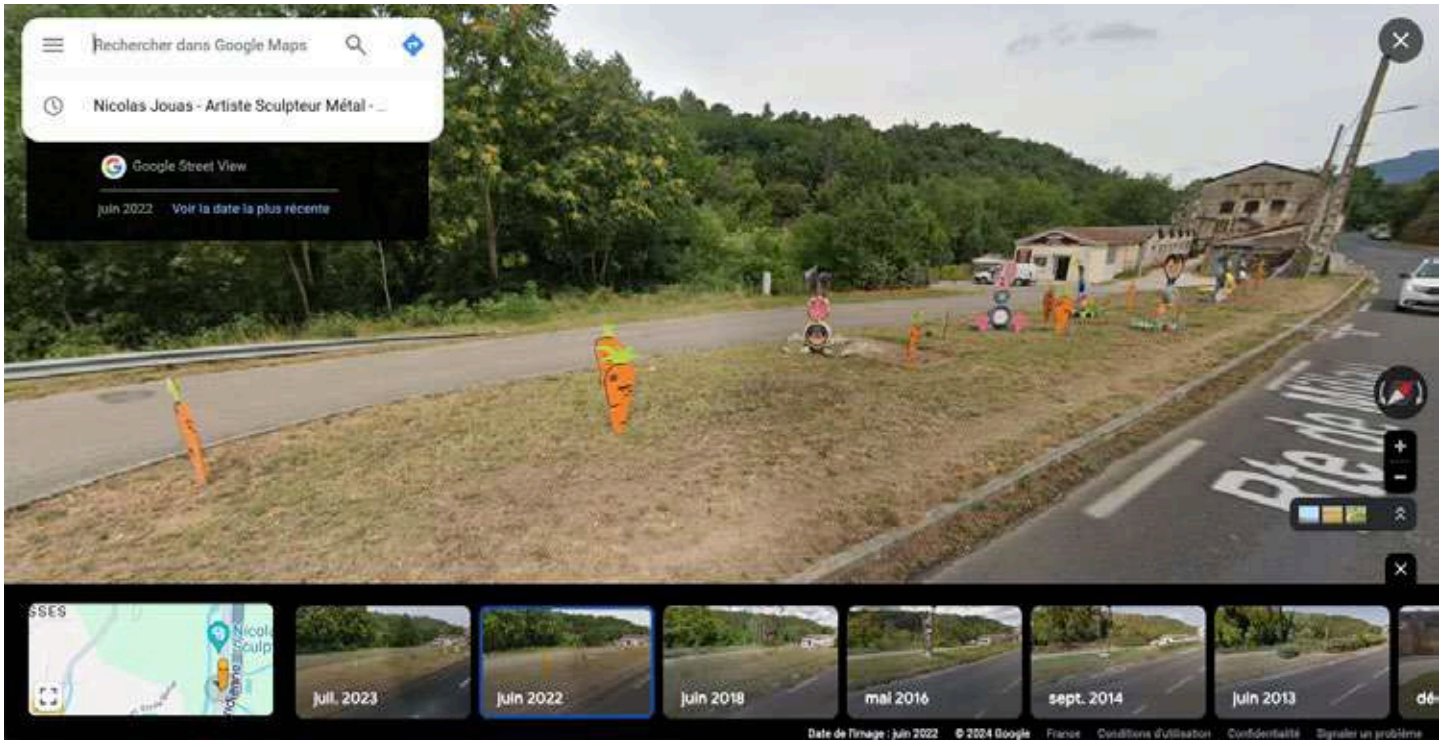
Si l'on se place en vue street nous voyons bien l'atelier mais aucune trace de la statue de Lego ...

En regardant de plus près, on peut s'apercevoir que la date de la prise de photo est Juillet 2023. On va donc changer la date de prise de vue et regarder en Juin 2022 si l'on a quelque chose qui semble être notre statue. **BINGO !**

Juillet 2023

Juin 2022

Si l'on tourne la caméra, on peut donc voir devant la statue un certain nombre de lapins et de carottes plantés dans l'herbe en face de notre statue de Lego : 9 carottes et 7 lapins au total. **La réponse à la 1ère question est donc 16 !**



On nous indique dans le résumé du challenge qu'avant d'être à la tête de l'atelier Takavenir, Nicolas Jouas etait responsable d'une autre structure qui serait fermée aujourd'hui.

Dans ce genre de cas la chose la plus évidente à faire est une recherche sur le site societe.com qui nous fourni un nombre important d'informations qui pourraient nous être utiles afin d'avancer dans notre recherche.

Pour commencer, le plus simple est de chercher le nom de l'atelier Takavenir afin d'être sur de tomber sur notre artiste et non sur un homonyme.

Le résultat obtenu est celui escompté nous retrouvons Nicolas Jouas comme le montre la capture *(Figure 5)*.

Nous pouvons donc avancer sur ce site afin de trouver de plus amples informations sur les sociétés liés à Nicolas.

Figure 5 - Societe.com Takavenir

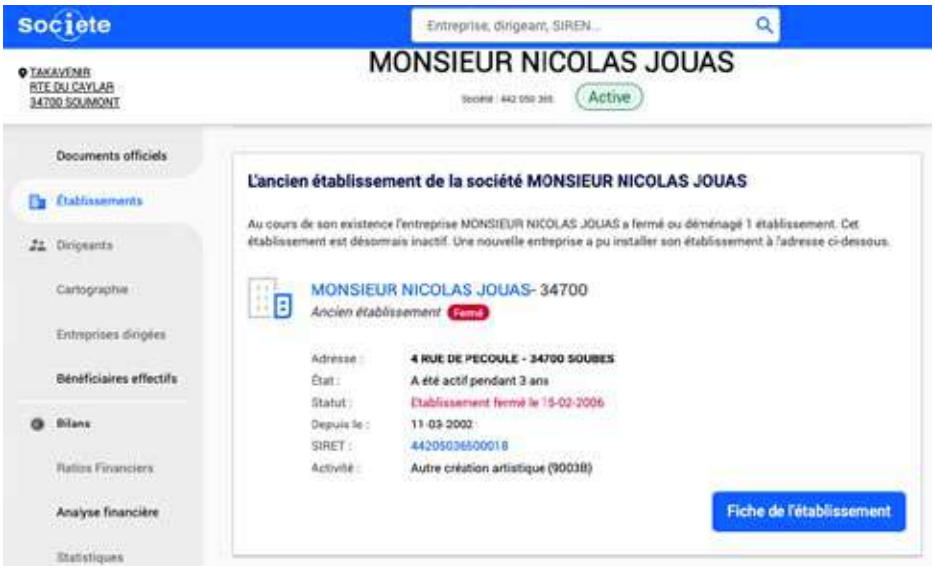


Figure 6 - Societe.com Nicolas Jouas

En cherchant un peu sur la page consacrée à l'artiste sculteur on retrouve un établissement secondaire qui serait fermé, intéressant !

Cet établissement se trouvait dans la ville de Soubes.

La réponse à la 2ème question est donc Soubes !

Dans cette ville de Soubes, le monument aux morts a été créé par un sculpteur célèbre qui a proposé dans les années 30 sa vision de l'homme originel.

Notre prochaine mission est donc de trouver dans un premier temps des info sur ce fameux monument aux morts, qui sera notre point de départ pour le troisième question de ce challenge : Quel est le nom du site historique situé à 18 km de cette oeuvre ?

Une recherche sur Google nous donne la première information crucial pour la suite : le sculteur du monument aux morts de Soubes est : Paul Dardé *(Figure 7)*.

Parmi les œuvres de Paul Dardé, on trouve celle qui nous intéresse *(Figure 8)*.

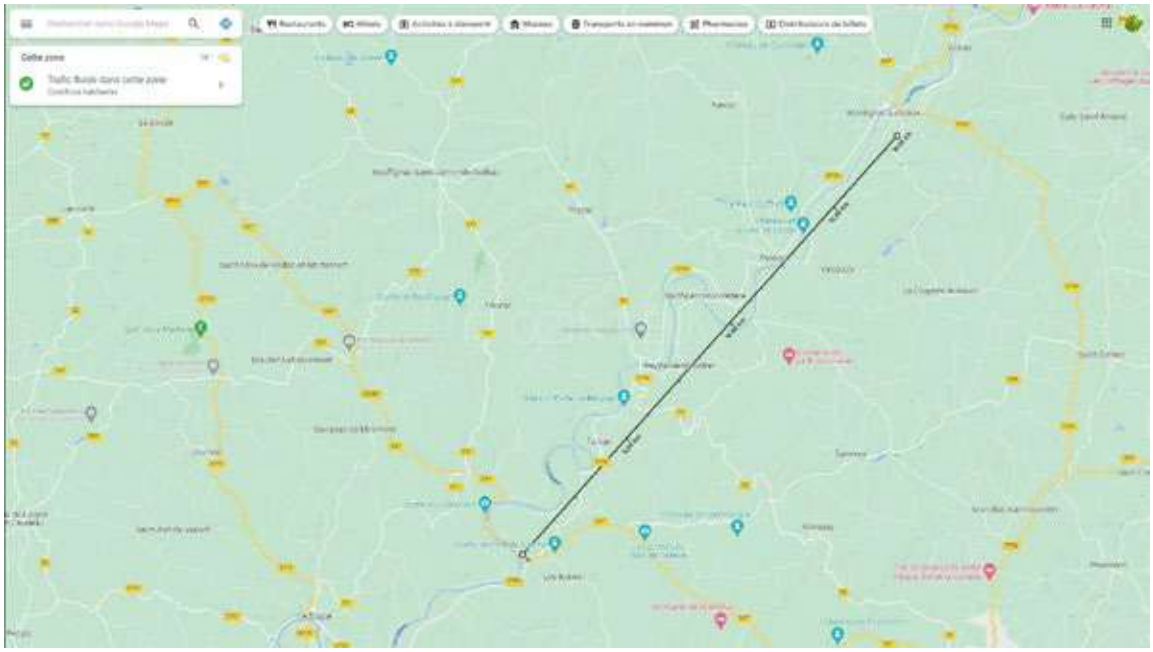
Figure 7 - Recherche Google

Autres sculptures [modifier | modifier le code]

- *L'Homme-Chèvre*, ornant anciennement le parc du Château de Vizille.
- *Stèle à la mémoire des officiers de médecine* à Béziers, Hérault.
- *Les Pleureuses*, localisation inconnue. Plateau des Glières, Haute-Savoie.
- *La Douleur*, dit aussi *Tête Aux Serpents*, *Tête de Prostituée* ou *Remords*, 1913, gypse, Paris, musée d'Orsay.
- *Laocoon*, 1919, domaine de Montplaisir, Lodève, Hérault.
- *Faune Guettant Une Nymphe*, 1924, Musée de Lodève, Hérault[11,12].
- *L'Homme Primitif*, 1931, Les Eyzies-de-Tayac-Sireuil, musée national de Préhistoire ; cette œuvre de trois mètres de haut et de cinq tonnes a été sculptée dans un seul bloc ; elle représente un homme de Néandertal et non pas un homme de Cro-Magnon, ainsi surnommé localement à cause de la proximité de l'abri de Cro-Magnon[13], distant de moins d'un kilomètre.

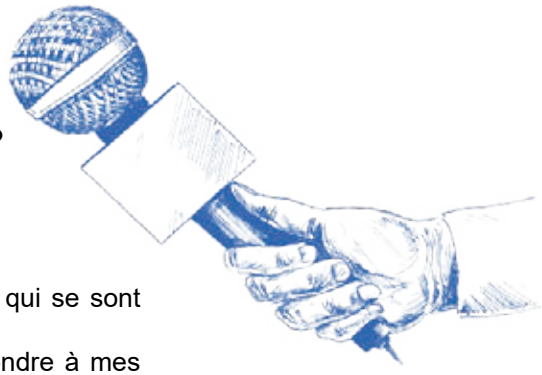
Figure 8 - L'homme primitif

En utilisant les mesures de distance Google, on peut trouver un site historique mondialement connu : la grotte de Lascaux.
La réponse à la 3ème question est donc Lascaux !



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

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



Voici la suite des interviews commencés dans le premier numéro de CYBER-IT.
J'ai de nouveau eu la chance d'échanger avec des professionnels du secteur qui se sont prêtés au jeu des questions/réponses.
Le temps est un bien précieux pour chacun et chaque moment pris pour répondre à mes questionnements est une vraie chance ! Merci à eux.
Les interviews publiées dans le magazine sont pour la majorité plus longs que ceux postés sur Linkedin (par souci de caractères maximum autorisés).

PIERRE PENALBA
Commandant de Police Honoraire

Salut Pierre, peux-tu nous expliquer selon tes mots, qui tu es ?

"Un dinosaure de la cyber parce que j'ai commencé à programmer en 1983 sur un ZX81... Mais avant tout un passionné de la technologie."

Peux-tu m'expliquer un peu ton parcours ?

"J'ai d'abord passé mon bac, puis j'ai enchaîné avec un diplôme en génie logiciel.
Puis j'ai eu plusieurs casquettes, passant d'inspecteur de police, à correspondant informatique.
Par la suite je suis devenu chef de la première unité cybercriminalité hors Paris.

J'ai également le plaisir d'être auteur d'ouvrages sur la cyber et le darknet.
Comme je n'aime pas m'ennuyer j'ai aussi le privilège d'être intervenant et formateur en cybersécurité ainsi qu'enseignant en école d'ingénieur "

Quelles sont tes missions au quotidien ?

"Actuellement je fais surtout du conseil, du pentesting et des formations. A cela s'ajoutent les periodes d'enseignement"

À quoi ressemble une journée type pour toi ?

"Je commence par checker les news, les forums du darkweb et autres sources.

Ensuite, dès que je peux, je réalise un mooc spécialisé sur la cyber, le forensic etc ...
Dans l'après-midi je réalise les missions d'analyse, d'OSINT etc ...
Fin de journée avec 2h de sport puis de bons moments en famille jusqu'à 22/23h.
Je poursuis avec quelques heures dans les méandres de la cyber.
Je ne dors que très peu comme tu peux le constater.

Il me faudrait plusieurs vies, je crois 😅"

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

"Ce que j'apprécie c'est d'apprendre, de découvrir, d'enquêter, de former et aussi enseigner.

Il y a des choses que je n'apprécie pas beaucoup, mais en particulier les gens qui pensent tous savoir, faire des factures... ah oui et aussi m'apercevoir que j'ai oublié de dormir 😆"

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

"Ne vous inquiétez pas des IA !
Ce sont des outils, l'humain peut apprendre, appréhender, et bénéficier toujours de ses capacités chaotiques et non logiques !"

KARIM LAMOURI
Co-fondateur et président de Hackers sans Frontières

Hello Karim, C'est un plaisir de partager un moment avec toi, en deux mots qui tu es ?

"Salut Arnaud, plaisir partagé, vraiment ! Je me vois comme quelqu'un de lambda, venant d'une banlieue parisienne.
Certains ont la chance de partir de 0 moi je pars de l'étage -30 environ... Je suis né d'un père militaire marocain ayant servi dans l'armée française et d'une mère que je qualifierai d'exceptionnelle ne serait-ce que par son savoir ! J'ai grandi dans une fratrie de 5 personnes, moi compris.
La cyber est un moyen de rassembler les gens, j'y suis arrivé par passion mais ce n'est qu'une facette de moi-même, ce n'est pas ce qui me définit fondamentalement.
Je me dit souvent que je souhaite vivre chaque moment comme si j'étais en phase terminal, j'essaie de vivre en croquant la vie à pleine dents ! "

Quel a été ton parcours ?

"Je vais être original et te dire que ... je suis autodidacte.
La passion, le temps que j'accorde à apprendre et à faire des rencontres, m'ont permis d'acquérir des compétences qui me permettent d'être employable et notamment lors d'incidents ou de situations compliquées"

Je suppose que tu ne peux pas en dire beaucoup mais quelles sont tes missions ?

"Effectivement, je reste le plus discret possible sur mes missions quotidiennes. Ce que je peux te dire c'est que je me force à être le plus précis et rigoureux possible dans les tâches qui me sont confiées.
Pour te donner un exemple je m'occupe de faire du conseil auprès de divers états, notamment à l'étranger.
Egalement je m'occupe de notre ONG "Hackers Without Borders" qui peut se traduire en français par "Hackers sans frontières". J'ai toujours été dans l'associatif depuis ma jeunesse.
J'aime inclure "L'autre" dans mes choix et ma vie. Une société saine se repose sur l'entraide et le savoir-vivre ensemble.
Ma passion c'est l'Humain avec un grand H c'est trop important.
Je suis également depuis peu directeur du centre de formation Effor Cyberlab à Reims/Nancy, Limoges et bientôt Paris"

Qu'est-ce qui te plaît et/ou déplaît dans la cyber ?

"J'aime tout dans la cyber mais je veux insister sur un point très important à mes yeux, en France nous avons un problème : l'entente et l'entraide !

J'entends par cela le fait que nous avons un pays de génie, avec des gens qui sont susceptibles de faire bouger les rangs, les choses, des talents formidables, mais le gros point noir c'est que nous sommes incapable de s'entendre et de fédérer !
Certes, on ne peut pas faire l'unanimité et plaire à tout le monde *(Dieu lui-même n'a pas fait l'unanimité alors comment pourrions-nous le faire nous-mêmes)*, mais le partage avec l'autre c'est ça le moteur. L'égo c'est tout simplement quelque chose d'horrible"

Merci à toi, un petit mot sur Hackers Without Borders pour la fin ?

"Avec plaisir !
HWB est une ONG qui a vu le jour en 2022 à la suite d'une discussion un soir avec Florent Curtet, suite à la cyberattaque de la Croix-Rouge en Suisse en Janvier 2022. Nous avons décidé de regrouper des spécialistes de la cybersécurité afin de monter notre association.
Avec Florent nous avons continué la réflexion en intégrant à notre projet Clément Domingo et Pierre-Marie Léoutre. Hackers Without Borders était née ! Aujourd'hui nous continuons notre cheminement et nous sommes fiers de dire que l'argent n'est pas le centre d'intérêt de l'association, d'ailleurs nous n'avons pas de compte bancaire lié à HWB.

Et pour finir, merci pour le moment passé ensemble Arnaud et au plaisir de se retrouver prochainement"

HWB

JONATHAN SPEDALE
Enquêteur et Analyste fraude

Hello Jonathan, merci d'avoir pris le temps de répondre, alors, qui tu es ?

"Hello Arnaud, je suis Spedale Jonathan, chasseur de malandrins du net !"

Et donc, quel a été ton parcours ?

"Anciennement artiste, après une blessure, je suis arrivé par hasard dans le secteur des cryptoactifs au moment où la fraude très présente devait être cachée au sous-sol, pas à la mode comme aujourd'hui. Cela m'a permis de me former de manière autodidacte premièrement puis à la détection des faux documents avec les forces de l'ordre pour ensuite m'ouvrir sur de nombreux domaines : lutte contre la fraude paiement, investissements, assurance, j'ai par la suite intégré un des milieux les plus touchés, l'e-commerce.
Passionné et curieux, j'ai évolué dans ces nombreux secteurs par envie, par soif de connaissance jusqu'à proposer aujourd'hui mes services de tests de fraude.
Ce service a fait ses preuves : comment lutter contre ce qu'on ne voit pas, ce qu'on n'explique pas, ce qu'on ne connaît pas ?"

Ok ! Tes missions au quotidien se résument à quoi exactement ?

"J'ai plusieurs types de contrats actuellement : du test de parcours, de la veille pour d'autres sociétés qui veulent savoir comment elles sont exposées aux menaces de fraudes, de la mise en place de processus ou modification de processus après une fraude détectée, la mise en place de règles de scoring avant paiement afin d'assainir les tentatives de paiement frauduleuses, c'est assez varié"

Globalement, à quoi ressemble une journée type pour toi ?

"Aucune journée ne se ressemble tout comme mes bureaux.
Sur place ou en distanciel au bon vouloir du client, j'écoute les besoins, je veille, j'informe et je conseille sur la mise en place de procédures ou d'outils pour des problématiques précises :
Constamment faire évoluer la stratégie de lutte contre la fraude et piloter des indicateurs clés pour diminuer le risque, formuler des alertes sur les nouvelles poches de fraudes détectées, contribuer à l'amélioration des outils et systèmes existants en matière de lutte contre la fraude, traiter les commandes passées en rétention, investiguer sur les suspicions de fraudes ou fraudes avérées, traiter les rapports quotidiens de données pour analyses des comportements suspicieux ou frauduleux, enregistrer et suivre les impayés, lancer et suivre les procédures de recouvrement.
Globalement, je propose des formations internes tant sur le traitement opérationnel que sur les moyens de faire des recherches et veilles"

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

"La diversité des rencontres, des sujets et surtout l'ingéniosité que je dois combattre chaque jour, un jeu d'échec imaginaire qui me donne mon adrénaline quotidienne et me laisse un sourire en coin d'amusement"

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

"Arrêtez de vous prendre au sérieux dans un secteur qui évolue chaque jour, tout le monde peut devenir hasbeen dès demain sachant que nous sommes souvent conviés après le casse, il ne sert de faire le sachant… Agissez plutôt !"

CYBER MOUSTACHE

YOHANN BAUZIL
Responsable de la sécurité

Salut Yohann, merci de passer de l'autre côté du micro pour une fois, dis nous qui es-tu ?

🎙 "J'ai 40 ans et j'habite à Toulouse.

Dans la vraie vie, je suis Directeur de la Sécurité (et DSI 😅) dans une startup NewSpace - @look up space.

Sur Linkedin, je suis un dénicheur de cyberstaaar et un combattant pour l'égalité grâce à la cyberinfluence avec robindescyberbois 🎯"

Et au niveau de ton parcours ?

🎙"Tout à fait classique :
- École d'Ingénieur en apprentissage car j'étais pas chaud pour aller travailler après mon DUT.
- 9 ans en presta dans le spatial et la Sécurité des SI.

Des planètes bien alignées 🌍, je deviens CISO d'un startup NewSpace, filiale d'Airbus, pendant 5 ans.
- Puis une erreur de parcours, et finalement, un super poste dans une super startup NewSpace 🔥🔥"

Que peux-tu dire sur tes multiples missions au quotidien ?

🎙"Étant dans une startup, on a parfois beaucoup de rôles pour une seule tête, mais c'est un super exercice de schizophrénie maîtrisée 🙃
Disons que je m'efforce de garantir toute la sécurité, du physique au numérique dans mon entreprise. Puis, j'accompagne mes utilisateurs et notre business pour trouver des solutions numériques, qui répondent à leurs besoins"

De quoi est faite une journée type pour toi ?

🎙"Les journées sont souvent longues :
- J'essaie de limiter les réunions, mais ce n'est pas rare d'en avoir 4 / jour, car énormément de sujets différents à adresser.
- Je traite tous mes mails tous les jours (tard parfois), et au pire, toutes les semaines ! Ne jamais bloquer un utilisateur ou le business, sinon ils se passeront de vous…
- J'accompagne au mieux ma super équipe (qui est bien plus productive que moi) pour apporter des améliorations et des solutions palpables tous les jours"

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

🎙"Me plaît : l'ultra-diversité de ma mission. Ces postes conceptuels n'existent qu'en startup. Aucune journée ne ressemble à la précédente !

Me déplaît : ce sont des postes où l'on réussit uniquement par un engagement démesuré, je joue au loto depuis 3 ans, il est temps de gagner 😅"

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

🎙"- « Développez votre réseau sans limite » : on devient fort grâce aux autres 💪

- « Trouvez un mentor qui vous inspire » : nos métiers sont trop compliqués, faites-vous aider 🤝

- « Travaillez votre personal branding » : aide-toi et le ciel t'aidera 👊"

Look Up SPACE

PIERRE PIVETEAU
CEO de Cyberveille

Bonjour Pierre, beaucoup te connaissent, mais dis-nous en plus sur toi !

"Et bien je suis Pierre PIVETEAU, né au siècle dernier (ah ah !) et sur différents réseaux sociaux j'interviens aussi sous le pseudonyme de Cyber Veille.
Cyber Veille est à l'origine, une petite publication interne de 4 pages, que j'écris en français d'abord et en anglais ensuite pour un état-major de l'OTAN dans lequel je travaillais. Par la suite l'idée d'exporter tout ça sur internet a fait son chemin et me voilà !
Parallèlement à cela, mon envie de ne pas rester éloigné du monde civil (en terme de cyber sécurité) m'a poussé à postuler au CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) où j'ai eu l'honneur et le privilège d'être admis en tant que membre.
J'ai aussi rejoint une association, l'OCOI (Observatoire de Cyber sécurité de l'Océan Indien) dont le but est de promouvoir la sécurité informatique et la protection des données dans la région de l'Océan Indien"

Quel est ton parcours ?

"Militaire de carrière depuis presque 35 ans maintenant, issu de l'arme des Transmissions j'ai toujours baigné dans ce monde la sécurité et de la culture du secret dès le début de ma carrière. D'ailleurs à cette époque on ne parle pas trop de SSI mais plutôt de SECOM (Sécurité des Communications). Et c'est donc tout naturellement que j'ai glissé vers la SSI dans un premier temps et puis vers la cyber sécurité avec l'arrivée de l'informatique dans les moyens de communications. Mon cursus académique a tout d'abord été militaire et au fil du temps sont venus s'ajouter de nombreux stages à l'ANSSI, Sysdream, CF2I par ex. "

Que peux-tu dire sur tes multiples missions au quotidien ?

"Je ne pense pas avoir un quotidien très différent de bon nombres de RSSI finalement. Entre les réunions avec ma hiérarchie, l'appui SSI à apporter aux chefs de projet sous forme de groupe de travail, les petits soucis à régler, inhérents à ceux d'une institution comme la mienne, et faire preuve de pédagogie et de sensibilisation au risque cyber pour les personnes avec lesquelles je suis amené à travailler. La seule différence bien sûr est une expertise sur certains sujets directement liés avec la Défense"

Peux-tu m'expliquer une journée type pour toi ?

"Je n'ai pas de journée type car mes domaines d'action sont très variés et parfois c'est l'actualité internationale qui donne le tempo !
J'ai tout de même un petit rituel si je puis dire : aussi bien dans ma peau d'OSSI que dans celui de Cyber Veille je commence tous les matins par un petit tour de presse et j'alimente ma veille.
Je mets de côté certains articles qui pourraient être intéressants pour mon travail quotidien et je trie ce qui peut alimenter ma veille « grand public ».
Je poste sur les différents réseaux en fonction de l'intérêt qu'il peut y avoir et je rédige chaque jour ma newsletter pour qu'elle soit prête à être envoyée à 9h."

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

"Je crois que la première chose qui me plait c'est d'être pro actif, de me dire que, à mon tout petit niveau, je peux moi aussi apporter ma pierre à l'édifice.
Tous les jours me dire que ce que j'apporte comme aide, comme expertise, comme sensibilisation aux dangers du monde numérique, sert à faire avancer la machine.
J'ai la chance de ne pas exercer un métier mais de vivre un choix que j'ai fait bien avant mes 18 ans qui est celui d'être un militaire.
Je ne sais pas si c'est le cas de beaucoup de corps de métiers.
Ce qui me déplait ?
Que ce soit en ligne ou dans la vraie vie, les gens éternellement négatifs. Ceux qui critiquent ou dénigrent sans apporter la moindre plus-value.
Les pessimistes, qui verront toujours le verre à moitié vide et qui, quoi que vous fassiez ne pourront que voir le mauvais côté des choses.
Ce genre de personnes toxiques dont j'essaie de me tenir éloigné."

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

"Et bien écoute, la première chose qui me vient à l'esprit c'est de te remercier pour ton invitation. Ce n'est jamais facile de parler de soi sans que cela tourne à « ma vie, mon œuvre ! » 😂

Je souhaite une bonne continuation à « Cyber IT » et j'espère que tu ne vas pas t'arrêter en si bon chemin.
Merci Arnaud !"

MATTHIEU BILLAUX
Directeur technique en conseil et R&D

Salut Matthieu, peux-tu me dire en quelques mots, qui tu es ?

"Matthieu, la quarantaine qui approche. Je suis aujourd'hui directeur technique d'une activité de conseil et R&D en sécurité offensive. Je suis également l'ambassadeur français de Hack The Box. On me connaît sous le pseudonyme euz dans pas mal de communautés.

J'adore la sécurité sous toutes ses formes, et je suis un accro aux jeux vidéo accessoirement"

Que dire de ton parcours ?

"Parcours standard au début, moins sur la suite. J'ai commencé l'informatique très jeune. J'ai joué avec un ordi avant même de savoir lire. La passion m'a été communiquée très tôt. Internet à la maison quand j'avais 8-10 ans. L'ADSL à 12 ans. Une autre époque.

Niveau cursus : bac S mention sciences de l'ingénieur obtenu "au talent" (comprendre en ne bossant pas, j'étais trop occupé à jouer ou développer des jeux vidéo). S'en suivent 2 années d'errance scolaires : début de licence d'anglais LLCE puis de droit. Je me décide à bosser, j'entre dans la Marine Nationale où je serai sous-officier dans l'informatique pendant 10 ans. Je découvre la sécurité informatique pendant ce job et je décide d'en faire mon quotidien très vite. Pas possible dans l'armée pour moi à l'époque donc je quitte après 10 ans et commence ma carrière dans le privé. 8 ans plus tard après plusieurs jobs me voici directeur technique"

Quelles sont tes missions quotidiennes ?

"J'interviens sur de nombreux fronts : commerce, avant-vente, encadrement de l'équipe, développement de nos méthodologies et également réalisation d'un quota de missions en tant qu'auditeur.
J'ai également une partie importante de mon temps réservée à la R&D dans le domaine, plutôt côté développement malware et initial access pour les missions red team"

C'est quoi une journée type pour toi ?

"Il n'y en a pas vraiment, mais souvent ça commence par une revue de l'actu cyber (veille) et de ma boîte mail. Ensuite priorisation des tâches pour la journée, puis pas mal de réunions de structuration de l'activité. Si je suis en mission, on embraie sur la réalisation. Le midi après la pause déjeuner, une petite réunion de 15 minutes avec l'équipe pour discuter de tout et de rien et faire le suivi des éventuels points bloquants, puis on repart sur nos missions respectives"

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

"Chaque jour, de nouvelles techniques sont découvertes, c'est à la fois grisant et épuisant de tout suivre.
Les journées ne font que 24 heures malheureusement, c'est le plus gros souci quand il faut être présent sur tous les fronts !
Mais sinon j'adore l'inventivité dont il faut faire preuve pour arriver à nos fins, surtout lors de missions red team, ça demande une vraie vision holistique, et ça, c'est génial"

Merci Matthieu, un petit mot pour la fin ?

"Polypus Pirata Immortalis Est ! (clin d'oeil aux copains qui se reconnaitront)"

Crédit : Halalolo

Article issue du média IT-Connect

Qu'est-ce que le Shadow IT ? Définition, risques et solutions

Dans cet article, nous aborderons un phénomène répandu dans la plupart des entreprises, qui représente un risque tangible et peut les exposer à des cyberattaques : le Shadow IT.

Nous débuterons par définir ce qu'est le Shadow IT, puis nous discuterons des risques qu'il pose pour une organisation. Enfin, la dernière partie de l'article se concentrera sur l'analyse de la surface d'attaque externe d'une organisation pour illustrer l'importance de cette problématique liée au Shadow IT.

Qu'est-ce que le Shadow IT ?

Le Shadow IT, également connu sous le nom de Rogue IT, se traduit en français par "Informatique fantôme" ou "Informatique parallèle". Ce terme désigne l'utilisation de logiciels et d'applications sans l'approbation du service informatique. En d'autres termes, le service informatique n'est pas informé que certains utilisateurs utilisent ces services ou applications. Cela implique que les processus de validation et d'implémentation ont été contournés, que ce soit intentionnellement ou non, par les utilisateurs.

Le Shadow IT inclut également les systèmes oubliés ou non référencés. Par exemple, il peut s'agir d'un PoC (Proof of Concept) mené par le service informatique lui-même, sous forme d'un environnement de test. Ces systèmes de test peuvent rester actifs bien au-delà de la phase d'expérimentation initiale. S'ils ne sont pas correctement isolés de l'environnement de production ou, pire encore, s'ils sont exposés sur Internet, ils peuvent représenter des risques considérables. Les environnements de test non contrôlés peuvent devenir des portes d'entrée pour les cyberattaques, exposant ainsi des vulnérabilités insoupçonnées et compromettant la sécurité globale de l'organisation.

En réalité, le Shadow IT est devenu un phénomène courant en raison de la prolifération des applications et des services accessibles. De nombreux outils modernes sont conçus pour être extrêmement conviviaux, permettant aux utilisateurs de les adopter rapidement sans nécessiter l'intervention du service informatique. Les services Cloud, souvent proposés sous forme de solutions SaaS (Software as a Service), en sont un exemple parfait.

Ces solutions offrent une flexibilité et une facilité d'accès sans précédent, mais cette même facilité peut encourager les utilisateurs à contourner les procédures officielles, créant ainsi des risques invisibles pour l'organisation.

Cependant, le Shadow IT s'accompagne d'une série de risques significatifs, notamment en matière de sécurité, de conformité et de gestion de l'information. Les applications et services non autorisés peuvent ne pas répondre aux normes de sécurité de l'entreprise, introduisant ainsi des vulnérabilités exploitables par des cybercriminels. De plus, l'absence de contrôle centralisé sur ces outils peut compliquer la gestion des données et la conformité réglementaire, entraînant des pénalités potentielles pour l'entreprise. Ces différents aspects du Shadow IT, ainsi que leurs implications pour les organisations, seront examinés en détail dans la prochaine partie de cet article.

Les risques associés au Shadow IT

La sécurité

Par définition, les applications déployées sans l'approbation du service informatique ne respecteront pas les normes de sécurité de l'entreprise. En d'autres termes, elles ne seront ni correctement configurées ni sécurisées, et il est possible que les données ne soient pas sauvegardées de manière adéquate. Avec le temps, si ces applications ne sont pas suivies, elles peuvent devenir vulnérables à une ou plusieurs failles de sécurité. Ces vulnérabilités peuvent être exploitées par des cybercriminels, mettant en péril la sécurité de l'entreprise. Ce risque est particulièrement élevé et critique lorsqu'il s'agit de systèmes exposés sur Internet, où les menaces sont omniprésentes et constamment en évolution.

En outre, l'absence de surveillance et de maintenance régulière de ces applications augmente le risque d'exploitation par des acteurs malveillants. Les mises à jour de sécurité et les correctifs nécessaires peuvent ne pas être appliqués en temps voulu, laissant les systèmes ouverts aux attaques. Cette situation est aggravée par le fait que les utilisateurs non avertis peuvent également mal configurer les applications, créant ainsi des points d'entrée supplémentaires pour les attaques.

En somme, les applications non supervisées constituent une menace sérieuse pour la sécurité informatique de l'entreprise et nécessitent une attention particulière pour minimiser les risques associés.

Il est crucial de comprendre que la sécurité informatique repose sur des protocoles rigoureux et des configurations minutieuses. Les applications non approuvées et déployées de manière autonome échappent à ces contrôles essentiels, exposant l'entreprise à des dangers potentiels. L'importance de suivre et de sécuriser chaque application utilisée au sein de l'organisation ne peut être sous-estimée.

Cela inclut la mise en place de sauvegardes régulières, l'application de mises à jour de sécurité et l'assurance que toutes les configurations respectent les normes de sécurité de l'entreprise. Dans la prochaine partie de cet article, nous explorerons les mesures que les entreprises peuvent prendre pour identifier et gérer les risques associés au Shadow IT.

Les données

Au-delà des risques liés à l'absence de contrôle de sécurité, tels que la configuration inadéquate et le suivi des mises à jour négligé, le Shadow IT pose une menace réelle pour la gestion des données au sein de l'organisation. En effet, les données peuvent être stockées dans des endroits non sécurisés, où des mesures de sécurité adéquates ne sont pas en place. Il peut s'agir de dépôts publics sans authentification, de connexions non chiffrées ou d'une gestion des permissions défaillante.

De plus, l'entreprise peut perdre le contrôle sur les données concernées, ne sachant plus où elles sont stockées ni qui y a accès. À terme, cela peut entraîner une fuite de données si un tiers non autorisé parvient à y accéder. La perte de contrôle sur les données sensibles peut avoir des conséquences graves, tant sur le plan financier que sur la réputation de l'entreprise.

En outre, cela peut également entraîner des violations des réglementations en matière de protection des données, exposant l'organisation à des sanctions légales et à des dommages financiers considérables.

Il est donc impératif pour les entreprises de prendre des mesures pour identifier et contrôler le Shadow IT afin de protéger efficacement leurs données. Cela implique la mise en place de politiques de sécurité claires et l'utilisation d'outils de surveillance avancés pour détecter toute activité non autorisée.

De plus, une sensibilisation accrue des employés aux risques associés au Shadow IT est essentielle pour promouvoir une culture de sécurité au sein de l'organisation.

La conformité et le RGPD

Il existe également un lien étroit entre la notion de conformité et le Shadow IT, notamment en ce qui concerne le RGPD. Pour rappel, le RGPD (Règlement Général sur la Protection des Données) est une législation de l'Union européenne visant à protéger les données personnelles des citoyens de l'UE. Il impose un suivi strict et précis des données personnelles traitées par les entreprises.

Cela signifie que l'organisation doit savoir exactement où les données sont stockées et qui y a accès. Ces exigences sont en totale contradiction avec la problématique du Shadow IT, où les données peuvent être stockées sur des systèmes non approuvés, voire non conformes au RGPD. En cas de violation de données, l'entreprise peut être tenue responsable et se voir infliger des sanctions sévères, y compris des amendes substantielles. La conformité au RGPD implique également la capacité de démontrer que des mesures de protection adéquates sont en place, ce qui est difficile à assurer lorsque des applications non contrôlées sont utilisées.

Outre les obligations liées au RGPD, l'aspect conformité inclut également la gestion des licences et le respect des conditions d'utilisation des services ou applications. Utiliser des logiciels sans licence appropriée ou en violation des termes d'utilisation expose l'entreprise à des risques juridiques et financiers. Le Shadow IT complique cette gestion, car les applications déployées sans l'approbation du service informatique échappent souvent aux contrôles nécessaires pour assurer le respect des licences et des conditions d'utilisation.

Il est crucial pour les entreprises de mettre en place des mesures rigoureuses pour détecter et contrôler le Shadow IT afin de garantir la conformité aux réglementations comme le RGPD. Cela peut inclure l'utilisation d'outils de surveillance pour identifier les applications non autorisées, ainsi que la formation des employés sur les risques et les obligations légales associés à l'utilisation non approuvée de logiciels. Dans la section suivante, nous aborderons les stratégies que les organisations peuvent adopter pour gérer et atténuer les risques liés au Shadow IT tout en assurant leur conformité réglementaire.

L'analyse de la surface d'attaque externe

La sécurité

Compte tenu des risques représentés par le Shadow IT, il est crucial pour les entreprises de prendre les dispositions nécessaires pour protéger leurs données. Au-delà de mettre en place des procédures strictes, une organisation peut adopter un outil d'analyse de la surface d'attaque externe (EASM) afin d'obtenir une cartographie précise des actifs exposés sur Internet. Ces actifs représentent un risque important et peuvent être utilisés comme vecteurs d'attaque initiaux, au même titre que les e-mails de phishing.

L'utilisation de l'EASM offre plusieurs avantages dans la lutte contre le Shadow IT :

Identification des actifs non autorisés : L'analyse effectuée par l'outil EASM permet d'identifier tous les actifs associés à une organisation, qu'ils soient autorisés ou non. En d'autres termes, cette analyse proactive permet de découvrir les systèmes, applications et services utilisés sans l'approbation de la direction informatique. Cela aide à révéler les éléments du Shadow IT et à comprendre leur portée.

Suivi continu : Le processus de découverte régulier de la solution EASM assure une surveillance continue. Cela est crucial pour réduire au maximum le délai entre le moment où un actif est mis en ligne et le moment où il est détecté. Ainsi, l'organisation, par l'intermédiaire de son équipe technique, peut réagir rapidement pour minimiser les risques. La surveillance continue permet de maintenir une visibilité constante sur les nouveaux actifs et de gérer rapidement les problèmes potentiels.

Évaluation des risques : Chaque actif identifié est passé en revue et évalué pour déterminer les risques potentiels qui lui sont associés. Cette évaluation permet d'identifier les faiblesses, notamment les problèmes de configuration et les vulnérabilités, tout comme le ferait un pentester. En connaissant les risques spécifiques associés à chaque actif, l'organisation peut prendre des mesures correctives appropriées pour renforcer la sécurité.

En intégrant une solution EASM, les entreprises peuvent mieux contrôler et sécuriser leur environnement informatique en détectant et en atténuant les risques liés au Shadow IT. L'analyse de la surface d'attaque externe devient alors un outil indispensable pour maintenir la sécurité et la conformité, tout en minimisant les vecteurs d'attaque exploitables par des cybercriminels. Dans la section suivante, nous examinerons les meilleures pratiques pour implémenter et utiliser efficacement une solution EASM afin de protéger les actifs de l'entreprise.

En identifiant les vulnérabilités et les risques associés à chaque système et service exposé, l'outil EASM vous aidera à prendre les mesures nécessaires et à adopter les bonnes décisions. Dans le cas du Shadow IT, cela peut impliquer la désactivation du système non autorisé ou la conservation du système sous réserve que sa configuration soit révisée (par exemple, en renforçant la sécurité du système ou en appliquant des mesures de hardening).

L'outil EASM permet non seulement de repérer les actifs non conformes, mais également de prioriser les actions à entreprendre en fonction du niveau de risque associé à chaque actif. En ayant une vision claire des vulnérabilités, l'organisation peut élaborer un plan de réponse efficace et ciblé. Par exemple, les systèmes les plus critiques ou les plus exposés peuvent être traités en priorité pour réduire rapidement les risques majeurs.

De plus, l'utilisation de l'EASM contribue à améliorer la posture de sécurité globale de l'entreprise en intégrant des pratiques de sécurité robustes et en assurant une surveillance continue. Cette approche proactive permet d'anticiper les menaces et de réduire les surfaces d'attaque potentielles, assurant ainsi une meilleure protection des données et des ressources de l'organisation.

sweepatic SECURITY

En plus de l'analyse de la surface d'attaque externe, les organisations peuvent traquer le Shadow IT grâce à :

La formation des employés pour les informer des risques associés au Shadow IT, mais aussi, pour leur expliquer les processus de validation internes de l'entreprise. Par exemple, la procédure à respecter pour demander l'accès à une application ou un service. Ceci est valable aussi pour le service informatique en lui-même : aucun passe-droit et ils doivent veiller à la bonne application de ces processus.

La gestion des appareils et des autorisations : les outils de gestion des appareils et des applications mobiles peuvent aider à déployer des applications, mais aussi, des politiques pour accorder et refuser certaines actions. Cela peut aussi permettre de contrôler quels appareils et applications ont accès aux données de l'organisation.

La surveillance et audit du réseau et des systèmes pour détecter les flux et les événements inhabituels.

Le dialogue entre le service informatique et les salariés, ainsi que les responsables de service, joue un rôle important, au-delà des solutions techniques. L'origine du Shadow IT peut être lié à un contentieux entre un salarié et le service informatique.

Capture d'écran de l'EASM

Le Shadow IT doit être pris très au sérieux. Il ne faut pas fermer les yeux sur cette informatique déjà dans l'ombre par définition. Au contraire, il est crucial de mettre en lumière les services, les applications et les systèmes utilisés sans l'approbation de l'équipe IT afin de pouvoir prendre les bonnes décisions. La découverte proactive de ces éléments permet d'identifier et de gérer les risques potentiels avant qu'ils ne deviennent problématiques.

En plus de l'identification et de la gestion des actifs non autorisés, il est également important de mettre en place des stratégies pour limiter la tentation des utilisateurs à recourir au Shadow IT. Cela peut être réalisé par le biais de la formation et de la sensibilisation des employés. En informant les utilisateurs sur les risques associés à l'utilisation de logiciels non approuvés et en leur expliquant les procédures à suivre pour obtenir des outils nécessaires, l'organisation peut réduire le recours au Shadow IT.

L'écoute des besoins des utilisateurs est également essentielle. En comprenant pourquoi les employés se tournent vers des solutions non autorisées, l'équipe IT peut trouver des alternatives approuvées qui répondent mieux à leurs besoins. En impliquant les utilisateurs dans le processus de sélection et de validation des outils, l'organisation peut créer un environnement de travail plus sûr et plus collaboratif.

En conclusion, prendre le Shadow IT au sérieux implique une démarche proactive pour identifier et gérer les actifs non autorisés, ainsi qu'une stratégie de sensibilisation et de formation pour limiter son apparition. La prochaine section de cet article examinera les meilleures pratiques pour intégrer ces mesures et gérer efficacement les risques liés au Shadow IT dans votre organisation.

Propos de Florian Burnel

A propos de l'auteur

FLORIAN BURNEL

Ingénieur système et réseau, cofondateur d'IT-Connect et Microsoft MVP "Cloud and Datacenter Management".

Je souhaite partager mon expérience et mes découvertes au travers de mes articles. Généraliste avec une attirance particulière pour les solutions Microsoft et le scripting.

IT-CONNECT FR

La cyber est un marathon pas un sprint !

Source : Europol.europa.eu

Les dessous de l'opération «EndGame» d'Europol

La plus grande opération jamais réalisée contre des botnets

L'opération internationale a permis d'arrêter plusieurs logiciels malveillants

Entre le 27 et le 29 mai 2024, l'opération Endgame, orchestrée depuis le siège d'Europol, a visé des droppers tels que IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee et Trickbot. Les actions avaient pour objectif de perturber les services criminels en arrêtant des cibles de grande valeur, en démantelant les infrastructures illégales et en gelant les revenus illicites.

Cette stratégie a eu un effet mondial sur l'écosystème des droppers. Les logiciels malveillants, dont l'infrastructure a été détruite lors des journées d'action, facilitaient des attaques par ransomware et d'autres types de malwares.

Suite à ces interventions, huit fugitifs liés à ces activités criminelles, recherchés par l'Allemagne, seront ajoutés à la liste des personnes les plus recherchées d'Europe le 30 mai 2024. Ces individus sont accusés de participation à des activités de cybercriminalité grave.

Cette opération est la plus importante jamais réalisée contre les botnets, essentiels au déploiement des ransomwares. Elle a été lancée et dirigée par la France, l'Allemagne et les Pays-Bas, avec le soutien d'Eurojust, et a impliqué le Danemark, le Royaume-Uni et les États-Unis.

L'Arménie, la Bulgarie, la Lituanie, le Portugal, la Roumanie, la Suisse et l'Ukraine ont également participé par diverses actions, telles que des arrestations, des interrogatoires, des perquisitions et la saisie ou suppression de serveurs et de domaines.

De nombreux partenaires privés, tant nationaux qu'internationaux, ont apporté leur soutien, parmi lesquels Bitdefender, Cryptolaemus, Sekoia, Shadowserver, Team Cymru, Prodaft, Proofpoint, NFIR, Computest, Northwave, Fox-IT, HaveIBeenPwned, Spamhaus, DIVD, abuse.ch et Zscaler.

Principaux résultats de l'opération

4 arrestations (1 en Arménie et 3 en Ukraine)

16 perquisitions (1 en Arménie, 1 aux Pays-Bas, 3 au Portugal et 11 en Ukraine)

Plus de 100 serveurs arrêtés ou perturbés en Bulgarie, au Canada, en Allemagne, en Lituanie, aux Pays-Bas, en Roumanie, en Suisse, au Royaume-Uni, aux États-Unis et en Ukraine

Plus de 2 000 domaines placés sous le contrôle des forces de l'ordre

Par ailleurs, les enquêtes ont révélé qu'un des principaux suspects avait gagné au moins 69 millions d'euros en crypto-monnaie en louant des infrastructures criminelles pour le déploiement de ransomwares. Les transactions de ce suspect sont constamment surveillées, et l'autorisation légale de saisir ces actifs lors d'actions futures a déjà été obtenue.

EUROPOL

Qu'est-ce qu'un dropper et comment fonctionne-t-il ?

Les droppers de logiciels malveillants sont des programmes conçus pour installer d'autres malwares sur un système cible. Utilisés au début d'une attaque, ils permettent aux cybercriminels de contourner les mesures de sécurité pour déployer des programmes nuisibles tels que des virus, des ransomwares ou des logiciels espions. Bien que les droppers ne causent pas de dommages directs, ils sont essentiels pour l'infection des systèmes avec des logiciels malveillants.

SystemBC assure la communication anonyme entre un système infecté et des serveurs de commande et de contrôle. Bumblebee, distribué principalement via des campagnes de phishing ou des sites Web compromis, facilite la livraison et l'exécution de charges utiles supplémentaires sur des systèmes compromis. SmokeLoader agit comme un téléchargeur pour installer d'autres logiciels malveillants sur les systèmes qu'il infecte. IcedID (aussi appelé BokBot), initialement un cheval de Troie bancaire, a évolué pour soutenir divers cybercrimes au-delà du vol de données financières.

Pikabot est un cheval de Troie utilisé pour obtenir un accès initial aux ordinateurs infectés, permettant ainsi le déploiement de ransomwares, la prise de contrôle à distance et le vol de données. Tous ces droppers sont utilisés pour déployer des ransomwares et représentent une menace majeure dans la chaîne d'infection.

Salle de réunion de l'opération «EndGame»

La fin du jeu n'est pas encore là

L'opération Endgame ne se clôture pas aujourd'hui. De nouvelles initiatives seront prochainement annoncées sur le site Operation Endgame. De plus, les individus impliqués dans ces botnets ainsi que dans d'autres activités, non encore appréhendés, seront directement appelés à rendre compte de leurs actions.

Phases de fonctionnement des droppers

Infiltration : les droppers peuvent pénétrer dans les systèmes via divers canaux, tels que les pièces jointes d'e-mails, les sites Web compromis, et ils peuvent également être associés à des logiciels légitimes.

Exécution : une fois exécuté, le compte-gouttes installe le malware supplémentaire sur l'ordinateur de la victime. Cette installation se produit souvent à l'insu ou sans le consentement de l'utilisateur.

Évasion : les compte-gouttes sont conçus pour éviter la détection par les logiciels de sécurité. Ils peuvent utiliser des méthodes telles que masquer leur code, l'exécuter en mémoire sans l'enregistrer sur le disque ou usurper l'identité de processus logiciels légitimes.

Livraison de la charge utile : après le déploiement du logiciel malveillant supplémentaire, le dropper peut soit rester inactif, soit se supprimer pour échapper à la détection, laissant la charge utile effectuer les activités malveillantes prévues.

Un centre de commandement à Europol pour coordonner les opérations

Europol a facilité l'échange d'informations et fourni un soutien analytique, de traçage cryptographique et médico-légal à l'enquête. Pour coordonner l'opération, plus de 50 réunions de coordination ont été tenues avec tous les pays participants, ainsi qu'un sprint opérationnel au siège d'Europol.

Plus de 20 agents chargés de l'application des lois du Danemark, de la France, de l'Allemagne et des États-Unis ont soutenu la coordination depuis le centre de commandement d'Europol, avec des centaines d'autres sur le terrain. Un centre de commandement virtuel a également permis une coordination en temps réel entre les officiers arméniens, français, portugais et ukrainiens.

Le centre de commandement d'Europol a facilité l'échange d'informations sur les serveurs saisis, les suspects et le transfert de données, avec des centres de commandement locaux établis dans plusieurs pays. Eurojust a également contribué en mettant en place un centre de coordination pour la coopération judiciaire, soutenant l'exécution des mandats d'arrêt et des décisions d'enquête européens.

EUROJUST

Arnaud Leroy - Juillet/Septembre 2024