Rappel : L'OSINT ou Open Source Intelligence peut être identifiée comme le recueil de renseignements à partir de sources d'information publiques, et cela grâce à des outils spécifiquement développés, soit en interne soit par des sociétés externes. Ces outils qui étaient au départ peu intuitifs et fonctionnels, ont souvent été utilisés par des spécialistes ou des initiés. Ce n'est que dernièrement que les progrès technologiques ont permis d'améliorer, et l'accès aux multiples bases de données en simultané, et les interfaces utilisation / modélisations, cela tout en permettant l'interfaçage avec d'autres sources de renseignements en temps réels. Des sociétés connues comme Palantir proposent des solutions associant Interface Intelligente, Business Intelligence & Intelligence Artificielle pour aller au-delà de l'internet, et incorporer des données comme celles des satellites à côté du renseignement humain et de la dimension Temps réel.

L'exemple d'un outil : Maltego

Un outil comme **Maltego**, par exemple, offre une interface assez agréable afin d'analyser les données qu'il a récolté sous différentes formes dont des graphiques. Mais cette solution permet surtout d'agréger très simplement différentes bases de données externes payantes ou non. Mais il est possible aussi de mentionner d'autres outils comme ceux d'IBM i2 Analyst, CybelAngel.

Quelle est l'utilisation de l'OSINT dans le cadre d'une attaque de Cyber Sécurité ?

Comme expliqué précédemment, l'OSINT permet de récolter des informations se trouvant dans différentes couches, différentes bases de données, ou différents groupes de discussion sur Internet.

Dans le cadre d'une attaque en Cyber Sécurité, ceux qui s'organisent vont dans un premier temps choisir une cible. C'est après avoir choisi la cible, que les recherches et collectes d'informations disponibles sur cette cible vont commencer. Ces recherches vont débuter en fonction du type d'attaque qui est souhaitée, et du type d'information nécessaires.

Exemple 1 :

Si par exemple on souhaite réaliser une campagne d'hameçonnage ou phishing, on va rechercher si une liste d'adresses d'emails de la cible est disponible. Cette liste peut alors avoir été volée précédemment par des hackers et être en vente, ou simplement être disponible gratuitement par la maladresse d'un des employés.

Si l'attaque est une intrusion dans le réseau informatique de la cible, les recherches OSINT vont s'adapter aux types d'informations nécessaires pour le type d'intrusion. Les recherches deviennent alors plus élaborées… Et plus le niveau de défense de la cible est élevé, plus les recherches préparatoires seront aussi importantes.

Exemple 2 :

L'exemple le plus simple d'utilisation d'OSINT pour une tentative d'intrusion sur un réseau informatique d'entreprise est la recherche d'un mot de passe et d'un identifiant. Après avoir sélectionné la cible, il est recherché les extensions d'adresses emails utilisées par l'entreprise. En effet, les adresses emails sont généralement les identifiants utilises par les entreprises pour que les employés s'identifient. Lorsque ces adresse emails sont collectées on va rechercher si des employés se connectent sur des sites externes de réseaux sociaux, e-commerce… avec leur email d'entreprise.

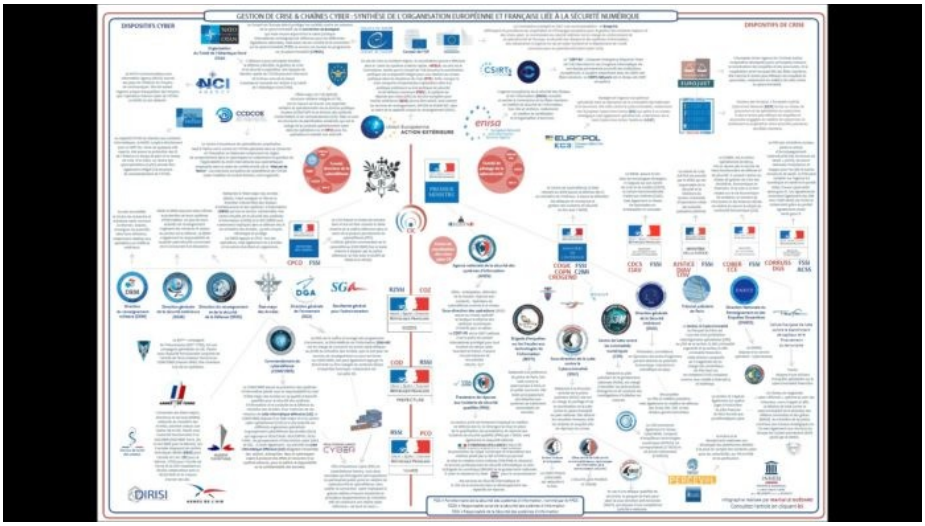
Dans ce cas prenons un employé qui achète régulièrement des billets de trains ou d'avions, et qui se connecte par synchronisation avec son identifiant d'entreprise au site de vente de billets.

Lorsque le ou les employés sont détectés, il va être cherché si des hackers ont volé précédemment des données sur ce site de vente de billets. Lorsque la base de données ou les bases de données volées sont récupérées, on se connecte sur le site de l'entreprise et on teste si le mot de passe synchronisé et utilisé sur le site de vente de billets est bien le même que celui utilisé par le ou les employés sur le réseau de l'entreprise… Après quelques essais, il n'est donc pas étonnant de se connecter au réseau de l'entreprise en usurpant l'identité du ou des employés.

Toutes ces recherches peuvent être effectuées par un outil d'OSINT. Les données disponibles pour la cybersécurité sont nombreuses comme Nom d'utilisateur, adresse email, mot de passe, numéro de téléphone, noms de domaine, adresses IP…

David - Guillaume DENIEL a débuté sa carrière chez KPMG France en 2001 en tant que Responsable des Innovations Métiers Informatiques. Il a ensuite travaillé avec des sociétés internationales en Europe, en Amérique du Nord et au Moyen-Orient. Depuis 2015, il s'est spécialisé dans les Cyber Tools & Cyber Arms. En 2018, Il rejoint un Think Tank Français - Liberté & Prospective - Créé sur les Questions Anti-Terrorisme & Police, il est en charge des Sujets Numériques. Il est diplômé de l'Institut Supérieur de Gestion de Paris, du Manhattan Institute of Management de New York et a étudié à Tokyo.

David - Guillaume DENIEL est joignable sur gdaviddeniel@gmail.com – ou via son profil LinkedIn - www.linkedin.com/in/davidgdeniel



https://nextcloud.inhesj.fr/index.php/s/gDPG5B9SXBJbEmw#pdfviewer

Listes d'outils

BlackHat	http://www.blackhat.com
Center for Internet Security	https://www.cisecurity.org
CNET Security	https://www.cnet.com/topics/security
Common Weakness Enumeration	http://cwe.mitre.org
CSO Online	https://www.csoonline.com
CVE Details	https://www.cvedetails.com
CVE MITRE	http://cve.mitre.org
Dark Reading	https://www.darkreading.com
DShield	https://dshield.org
Exploit Database	https://www.exploit-db.com
HelpNetSecurity	https://www.helpnetsecurity.com
Information Systems Security Association International	https://issa.site-ym.com
Infosec Island	http://www.infosecisland.com
Infosecurity Magazine	https://www.infosecurity-magazine.com
Krebs On Security	https://krebsonsecurity.com
Linux Security	http://www.linuxsecurity.com
McAfee Labs	https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs.html
Microsoft Secure	https://www.microsoft.com/en-us/security/default.aspx
Naked Security	https://nakedsecurity.sophos.com
Network World Security	https://www.networkworld.com/category/security
NIST	https://csrc.nist.gov
Ecole de Guerre Economique	https://www.ege.fr/actualites/ecole-de-guerre-economique-publie-la-cartographie-des-metiers-de-la-cybersecurite-2020.html
Agence Nationale de la Sécurité Informatique	https://www.ssi.gouv.fr
Espace et Cybersécurité	https://www.spacesecurity.info

Prochaine fiche 10 Avril 2022