Quand des RSSI collaborent... (sur une place de marchés d'IOC communautaire)

Emmanuel Mesnard, Damien Berjoan, Fabrice Prigent, Yves Agostini

Quand des RSSI collaborent ... (sur une place de marchés d'IOC communautaire)

Emmanuel Mesnard
Université de Reims Champagne Ardenne
2, avenue Robert Schuman
51100 Reims

Damien Berjoan
ESUP Portail
Université Polytechnique Hauts-de-France
Campus Mont Houy
59313 Valenciennes Cedex 9

Fabrice Prigent
Université Toulouse Capitole
2 rue du Doyen-Gabriel-Marty
31042 Toulouse Cedex 9

Yves Agostini
Université de Lorraine
34 Cours Léopold
54000 NANCY

Résumé

L’état de la menace se fait toujours plus prégnante sur la communauté de l'Enseignement Supérieur et Recherche. Force est de constater que les sources d'incidents cyber touchant notre communauté sont communes. Celles-ci abusent de nos ressources et de la relation de confiance entre nous comme facilitateur de diffusion de la menace.

Chaque RSSI voit, sur son périmètre propre, une forte évolution des incidents en augmentation et une multiplication des outils malveillants (infostealer, dropper, etc.). Les escrocs collaborent et se sont structurés dans le découpage des tâches. ils se partagent ainsi de l'information, se spécialisent et deviennent plus réactifs. Alors pourquoi pas les RSSI !?

Ainsi, des RSSI ont eu la volonté de partager et de mutualiser leurs informations d'incidents, d'IOC, de méthodologies d'attaques, de méthodes de détection, etc. de manière simple, rapide, sécurisée et auprès d'une communauté de confiance.

En complément, nous aborderons l'état de la réponse aux menaces avec une courte présentation des différents outils utilisés dans nos différentes structures ainsi que les méthodologies de détection des incidents. Nous présenterons des retours d'expériences objectifs d'outils en place dans nos structures suivant chaque usage et périmètres spécifiques.

Au fil des échanges, la détection et le partage d’IOC nous est paru indispensable sur une plateforme collaborative de la communauté. Nous présenterons les bénéfices avec quelques chiffres de détections réalisées grâce ce partage d'IOC et nous aborderons des propositions de perspectives à court et moyen terme.

Pour élever le niveau de sécurité de notre communauté, venez partager vos IOC !

Mots-clefs

Menace, phishing, infostealer, droper, IOC, honeypot, NDR, SIEM, brute-force, MISP, …

Introduction

Année après année, l'état de la menace se fait toujours plus prégnant sur la communauté de l'enseignement supérieur et de la recherche (ESR). Ainsi, un premier constat est d'affirmer que les sources d'incidents cyber touchant la communauté sont communes. Maintenant celles-ci abusent des ressources et de la relation de confiance à priori comme facilitateur de diffusion de la menace en interne à la communauté.

Par exemple, les campagnes de phishing affectent très souvent et en même temps plusieurs établissements de la communauté la réactivité de leur signalement devient une nécessité. Chaque RSSI voit, sur son périmètre propre, une forte évolution des incidents à la hausse et une multiplication des outils malveillants avec des fonctionnalités propres (infostealer, dropper, ...). Les escrocs collaborent et se sont structurés dans le découpage des tâches, ils se partagent ainsi de l'information, se spécialisent et deviennent plus réactifs.

Ainsi il est venu le besoin de base et très souvent similaire entre plusieurs RSSI de notre communauté la volonté de partager et de mutualiser nos informations sur des incidents, des indices de compromission (IOCs) récents, des méthodologies d'attaques, des méthodes de détection, ... de manière simple, rapide, sécurisé et auprès d'une communauté de confiance. Cette collaboration nécessite une implication de contribution active des acteurs et non seulement une consommation des informations partagées.

Nous allons maintenant aborder ces points suivant le contexte et l’expérience de quatre structures différentes.

Contexte et Retex de l’université Reims Champagne Ardenne

Le contexte de l’URCA

L’Université de Reims Champagne-Ardenne est une université multidisciplinaire et regroupe 30000 étudiants et 4000 personnels. Elle est répartie sur 5 villes de l’ancienne région Champagne-Ardenne. Son informatique est très centralisée notamment sur Reims qui regroupe quasiment 90 % des serveurs et services. Depuis plusieurs années, la cybersécurité est prise en compte au niveau de la gouvernance et une accélération s’est faite depuis 2022 grâce au plan France Relance Cyber permettant sur les deux phases (Pack initial et Pack relais) d’avoir du budget de l’ANSSI et une impulsion supplémentaire de notre gouvernance à destination des directions métiers. Dans le plan de sécurisation à trois ans qui en a découlé, un gros focus a été fait sur la détection des incidents de sécurité.

Retex de l’URCA

Depuis 2022, le zoom sur la détection des incidents de sécurité a permis, notamment, de centraliser sur différents puits de logs adaptés au contexte (syslog / Windows Event Collector) un maximum d’information de serveurs, de services, d’applications permettant dans un premier temps de répondre à la capacité de répondre à une notification judiciaire ou de revenir en arrière sur un problème/incident.

L’accélération s’est faite sur la mise en place d’une stack Elastic en tant que SIEM. Ainsi, nous passons d’une capacité de stockage et analyse à posteriori à une capacité de corrélation d’événements générés depuis des sources différentes. Des prestations ont été prises pour nous accompagner dans l’écriture de règles d’incidents surtout sur le volet Windows Active Directory et/ou Office 365. Nous continuons à écrire des règles sur des besoins ponctuels et/ou sur une application en particulier (brute-force sur CAS ou la messagerie, …).

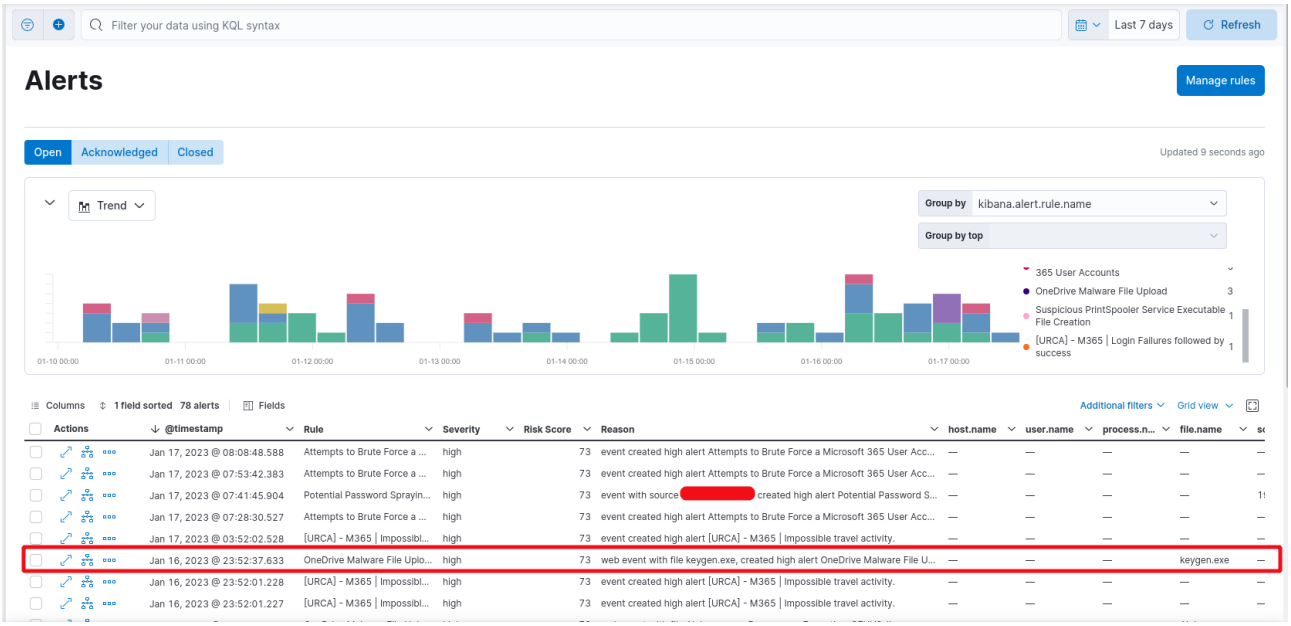

Figure 1: Tableau de bord Elastic

Quand nous détectons des tentatives réussies sur des comptes compromis, nous gardons les IOCs (URL, email, IP, DNS, …) et les communiquons au canal `#SSI-IOC` sur rocket.chat pour les partager aux différentes personnes présentes sur ce canal. Chacun est libre de récupérer ou non ces IOCs et de les tester dans son contexte propre de son organisation. Dans mon cas, ce partage m’a permis de récupérer deux fois des IPs d’attaquants qui avaient compromis un/des compte(s) chez mes collègues de cette présentation et m’ont permis de mettre en évidence également des compromissions de compte chez nous.

Suite à donner

Le partage d’IOC de la manière où nous faisons, reste bien évidemment, très rudimentaire et ne permet pas de revenir sur d’anciens IOCs. Par ailleurs, il faudrait surveiller très régulièrement le canal rocket.chat dédié pour voir de nouveaux IOCs à tester dans son système. Il sera pertinent à plus long terme d’industrialiser et d’uniformiser ce partage d’information entre nous à travers un outil dédié tel que MISP. Un autre point important est sur la confiance à partager de la donnée dite « sensible » puisque les attaques peuvent être en cours. Il faut ainsi éviter qu’un attaquant se sache détecter et par ailleurs, il ne faudrait pas que l’information fuite en dehors de notre communauté.

Contexte et Retex d’ESUP Portail

Contexte d’ESUP Portail

Le Consortium ESUP-Portail est une communauté nationale d'expertise numérique, de coopération et de développement soutenant des solutions open source, créé en 2002 suite à l’appel d’offre du Ministère de l'Enseignement Supérieur pour promouvoir les espaces numériques de travail (ENT).

Transformé en association en 2009 elle regroupe actuellement près d’une centaine d’établissements de l’Enseignement Supérieur et de Recherche (ESR). Elle constitue une communauté structurée pour le développement et la diffusion de services numériques open source en mutualisant les ressources et les moyens de ses adhérents. L’association conduit des projets sur l’évolution des services numériques et leur intégration dans les systèmes d'information (SI) de l’ESR notamment en direction des étudiants ; dont certains services en mode hébergé (SaaS) depuis 2019 comme la plateforme d’échange Rocket-Chat utilisé pour cette place de marché (market place) de partage d’IOC.

Retex d’ESUP Portail

Le retour se fera au travers de mon expérience en tant que RSSI d’une université partagée à la communauté ESUP à l’aide du service Rocket-Chat en mode hébergé. Début 2020 concomitant à la mise en place d’une sonde NDR commerciale sur notre cœur de réseau l’établissement subit plusieurs compromissions par Emotet rapidement identifiées et circonscrites par la sonde. De là régulièrement des IOC externes sont identifiées et leur comportement malveillant est confirmé par la sonde que j’alimente avec des listes d’IOC externes de sites communautaires et de CERTs. De même je mets en place un traitement des phishings permettant d’identifier l’IOC exploitant les comptes compromis. Ainsi je nourris et étoffe une liste d’IOCs dans la sonde NDR qui se charge d’identifier l’activité de celles-ci sur la partie de réseau observé et de confirmer leur activité malveillante ou non. Cette identification en amont d’IOCs hostiles permettra de bloquer en amont les vagues d’Emotet de 2021.

Suite à donner

Reprenant l’adage de l’association ESUP-Portail sur le partage et la mutualisation j’ai initié la diffusion de ces informations en qualifiant des menaces pour notre communauté avec une IOC contextualisée par type de menace (scan, exploitation phishing, compromission compte infostealer, virus, ...) de manière rapide et efficace à une communauté de confiance. Cette diffusion s’effectue au travers d’une politique de partage et d’utilisation des informations à caractère opérationnel de type TLP:AMBER/PAP:GREEN. Pour cela nous utilisons un canal dédié de la plateforme Rocket-Chat ESUP selon une nomenclature permettant d’identifier l’IOC et de caractériser son niveau de malveillance sur les sites de référencement communautaire en la matière. L’objectif étant de pouvoir partager en direct des IOCs chaudes en termes d’activité et de prévenir la communauté permettant d’identifier les compromissions croisées. En effet nous avons constaté qu’une même IOC vecteur d’attaque de tout type (scan, phishing, …) ciblait généralement toute la communauté de l’ESR sur la même période. Alors la rapidité de détection et de partage de cette IOC devient un élément déterminant pour une réponse aux menaces efficaces de et pour notre communauté.

Contexte et Retex à Toulouse Capitole

Contexte de Toulouse Capitole

L'Université Toulouse Capitole regroupe 20 000 étudiants en droit, économie et gestion, avec une petite UFR informatique. Son statut actuel d'établissement expérimental a nécessité de prioriser les ressources informatiques sur une refonte du SI. Son informatique est très centralisée, même si des velléités d'indépendance sont présentes. Pour l'instant, étonnamment préservée des gros incidents de sécurité, les pratiques problématiques sont légion, et la sécurité n'est clairement pas une priorité dans un contexte de mutation toulousain très important.

Retex de Toulouse Capitole

L'université est dotée de nombreux mécanismes de sécurité, dont un honeypot qui aspire les attaquants les plus visibles, que ce soit par du brute force, des scans ou un certain nombre de signatures d'attaque. Des limites en termes d'expéditions de mail, de géolocalisation des authentifications complètent l'ensemble et permettent 1 à 2 fois par mois d'automatiquement neutraliser des comptes, ou d'avertir les utilisateurs en cas de suspicion. Elle a aussi acheté, chez un prestataire israélien, une remontée des comptes volés par infostealer. Ce dernier point a permis de détecter pour l'année 2023-2024 près de 330 comptes, même si 80 % sont en fait des comptes inactivés, les infostealer volant les identifiants conservés sur le navigateur, entre autres. Les utilisateurs sont soumis, très régulièrement, à des campagnes de phishing pédagogiques, ce qui donne d'excellents résultats. Un DNS RPZ, alimenté localement, complète l'ensemble du dispositif en neutralisant certaines infections « connues ».

Figure 2: Quarantaine

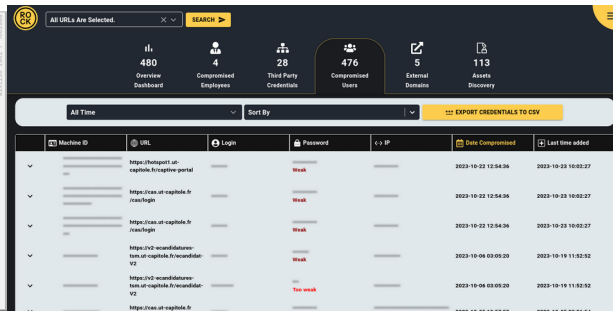

Figure 3: Infostealers

Cependant, malgré cette infrastructure sécurité et 2 antispams, fortement adaptés, certains phishing, en particulier ceux qui « rebondissent » depuis la sphère éducative, passent et ne sont pas toujours repérés, avec en plus, des caractéristiques particulièrement retorses, leur donnant un potentiel nocif très élevé. De même quelques virus, ramenés par des étudiants, ou des personnels en contexte BYOD, ne sont pas toujours bloqués en interne.

Notre contribution au canal #SSI-IOC découle de ce contexte : nous fournissons généralement des exemples de mails retors, et d'adresses IP nocives qui ont « failli » nous piéger. Et notre bénéfice est en miroir : une liste d'adresses mails qui n'auraient pas été détectées, et des traces de compromission réussies avec les IP repérées par les autres membres.

Si jusqu'à présent, les IP que nous récupérons n'ont pas encore donné de résultats vraiment intéressants, les mails nocifs, quant à eux, nous ont permis, à minima, de « corriger » nos antispams, mais en généralement de pouvoir neutraliser, avant visualisation par les victimes potentielles, des

phishing à un rythme quasi hebdomadaire (avec de 5 à 120 utilisateurs touchés, à chaque fois), sans compter les URLs associées. Combien de désastres avons-nous évité ? Impossible de le quantifier.

Suite à donner à Toulouse Capitole

Nous avons commencé à modifier nos procédures pour utiliser immédiatement les remontées du groupe, que ce soit mail ou IP. Sans nous affranchir d'un travail d'analyse, ceci nous rassure fortement de savoir qu'en cas d'intrusions réussies, un certain nombre d'entre elles pourront être repérées par le panoptique que constitue le groupe.

Les discussions afférentes aux diverses méthodes que nous employons les eux et les autres, nous permettent aussi d'entrevoir certaines techniques pertinentes, même si elles ne sont pas toutes adaptables : notre honeypot, par exemple, ne nous permet pas de différencier un brute force, d'un pirate utilisant en série des comptes volés. La plupart des évolutions, qualitative ou quantitative, des apports des membres, sont accompagnées de la technique ou du concept ayant permis de les produire. Une nouvelle manière de s'améliorer.

Contexte et Retex à l'université de Lorraine

Contexte de l'université de Lorraine

L'université de Lorraine est une université pluri-disciplinaire née en 2012 de la fusion des quatre universités lorraines. 60 000 étudiants et 9 000 personnels sont répartis sur deux métropoles, onze villes et agglomérations. La sécurité du système d'information y est prise en compte depuis l'origine de l'établissement en s'appuyant sur les meilleurs pratiques initiées dans les anciens établissements. Elle s'appuie aussi bien sur la volonté de maîtriser les infrastructures et services, le suivi précis de tous les incidents, une organisation d'un réseau de correspondants et le pilotage institutionnel de la sécurité. L'appui politique est fort. Une politique de sécurité de l'établissement (PSSI) a été votée en conseil d'administration dès 2015. La priorité est mise sur la sensibilisation de nos utilisateurs, aussi bien nos personnels que les futurs enseignants, cadres, ingénieurs, médecins que nous formons chaque année.

Aujourd'hui, plus de 100 000 comptes d'étudiants, personnels, vacataires, partenaires accèdent à nos services.

Retex de l'université de Lorraine

L'exploitation de compte volé pour transmettre des tentatives d'escroqueries ou de phishing est, comme pour beaucoup d'organisations, le risque le plus courant. Les conséquences sur la réputation de nos serveurs de mails peut avoir un impact sur le fonctionnement de l'établissement. Nos outils de détections, de blocage automatique mais surtout la formation de nos personnels ont très nettement limité la fréquence des comptes volés par phishing. Un grand nombre de personnels sont désormais capables de les détecter en lisant les URLs douteuses et surtout signalent ces mails douteux.

Pendant longtemps, le second incident le plus courant a été le vol de compte suite à la réutilisation du même mot de passe sur des sites externes à l'établissement. Alors que le phishing vise essentiellement des personnels avec une adresse mail établie depuis plusieurs années, la réutilisation

du mot de passe permet également le vol de comptes d'étudiants. La maîtrise de nos infrastructures nous a permis de mettre en place une analyse en temps réel des traces de connexion[1].

Ces outils de détection ont fait apparaître dès 2020 la nouvelle menace des infostealers. Alors que l'on détectait un à deux comptes certainement volés chaque semaine lorsqu'il s'agissait de mot de passe réutilisé, après le confinement de 2020, nous détections un compte volé chaque jour, puis jusqu'à 3 comptes volés à partir de 2022.

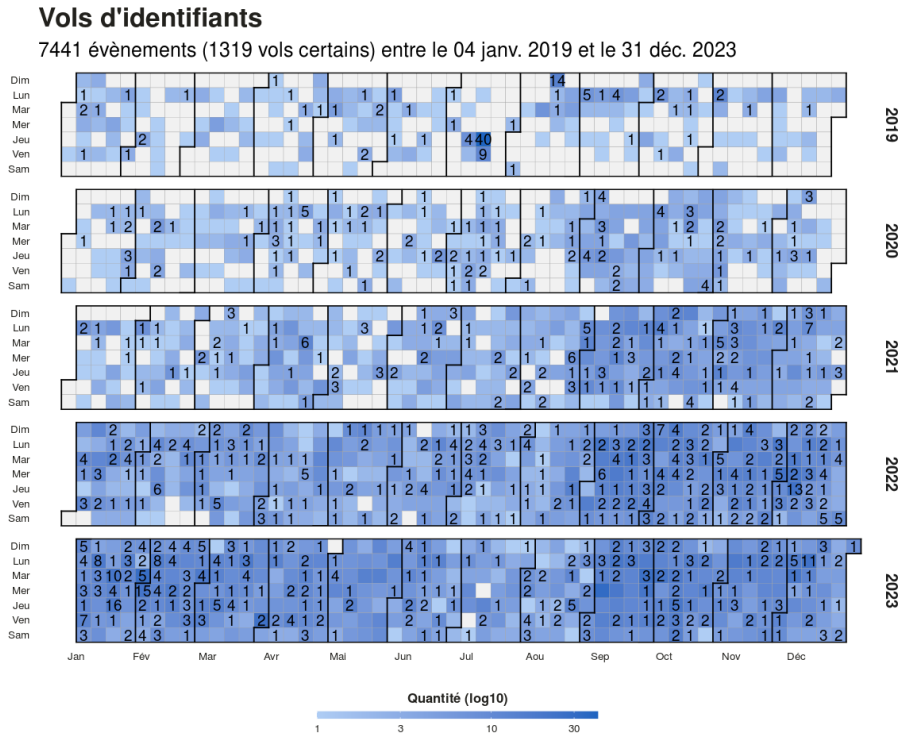

Figure 4: Vols d'identifiants 2019-2024

Fin août 2022, La société Sekoia a parfaitement décrit[2] les techniques de ces groupes de «traffers» : depuis l'achat des applications simples, très variables (et donc rarement détectées par des antivirus), la diffusion depuis de faux cracks ou applications puis le vol des identifiants et cookies de sessions enregistrés dans les navigateurs, applications de mail, vpns, transferts de fichiers, jusqu'au tri et la revente des identifiants volés. Les principaux acheteurs sont les groupes plus organisés qui vont chercher à chiffrer des infrastructures contre demande de rançon (ex : Conti). Les identifiants volés servent de porte d'entrée à nos systèmes.
Ces infostealers sont aujourd'hui une menace majeure aussi bien pour les données personnelles de nos utilisateurs que pour nos établissements.

Actuellement l'établissement verrouille tous les aspects suspects, un informaticien est ensuite chargé de confirmer et sensibiliser l'utilisateur. Un accès depuis un vpn grand public, qui donne un faux sentiment de sécurité, peut masquer un vol d'identifiants personnels.

Suite à donner

Si la formation de nos utilisateurs et nos outils de détections nous permettent de détecter et bloquer un grand nombre de vols d'identifiants, il n'y a pas de garantie absolue de détection. Aujourd'hui alors que les escrocs se partagent des identifiants, des techniques et procédures, la rapidité de réaction est essentielle.
Les éléments de détection sont également sensibles. Il s'agit généralement de données personnelles, mais il est aussi essentiel de les garder secrets pour conserver leur efficacité.

Enfin une classification des éléments de détection doit permettre d'appliquer des mesures spécifiques à chaque politique d'établissement.

État de la réponse aux menaces

Au travers d'une courte présentation des différents outils utilisés dans nos différentes structures (EDR, NDR, XDR, SIEM, ...) ainsi que les méthodologies de détection des menaces propre à chaque contexte et environnement. La multiplication de protection par couche devient une nécessité au vu de l'évolution constante des menaces, un rapide focus par structure sera présenté. Ces différentes méthodologies et protections nous ont amené au besoin de partager et confronter celles-ci ainsi que les IOC récoltées par nos outils respectifs.

La détection et le partage de ces IOC nous sont devenus rapidement indispensables sur une plateforme collaborative de la communauté.

Sur une proposition collégiale nous avons mis en place un canal spécifique (#SSI_IOC) de partage d'IOC sur la plateforme Rocket.Chat d'ESUP-Portail. Cet outil nous permet au quotidien de partager en direct des IOC suivant une Politique de partage et d'utilisation des informations à caractère opérationnel de type TLP:AMBER/PAP:GREEN.

Nous présenterons les bénéfices suivant quelques chiffres de détections réalisées grâce ce partage d'IOC. Les escrocs se partagent bien les comptes compromis pourquoi les RSSI ne partageraient pas les IOC !

L'intérêt de ce partage réside dans la force d'additionner nos outils et nos méthodologies différentes qui deviennent complémentaires. En revanche la réponse sur incident reste propre à chaque établissement dans son contexte et environnement particulier. Nous présenterons des retours d'expériences objectifs d'outils en place dans nos structures suivant chaque usage et périmètres spécifiques. De même, nous partageons nos découvertes et nos ressources librement accessibles qui seront brièvement présentées (liste de ressources par usages et fonctionnalités)

Perspectives

En terme de perspective, nous pouvons nous placer en différentes étapes. En effet, à court terme il peut être intéressant de voir pour ouvrir le canal dédié #SSI_IOC à un public plus large. Mais, il faudra nécessairement prendre le temps de vérifier qui y accède. La notion de confiance doit être omniprésente au vu de la sensibilité des informations échangées et/ou sur des incidents mineurs en cours dans nos organisations. À moyen terme, il pourrait être opportun de réfléchir à la mise en

place d’une instance communautaire de plateforme MISP, ouverture contrôlée de la plateforme de partage d'IOC. Cela permettrait de partager plus proprement des IOCs sur un outil dédié à cet usage et pouvant, éventuellement, alimenter nos propres outils de détections pour gagner du temps à la recherche de compromission potentielle. Enfin, à très long terme, il pourra être envisagé l'expérimentation d'un SOC d'une communauté opérant les outils précédemment décrits. En effet, le bénéfice pour tous en sera d’autant plus grand, que nous n’avons tout simplement pas les moyens d’avoir tous un SOC en interne et/ou externe avec des experts sur ce sujet éminemment complexe. De plus, le partage d’information d’incidents de sécurité permettra de faire grandir la cybersécurité de manière collégiale au sein de notre communauté Éducation.

Bibliographie

[1] Yves Agostini, «Outils statistiques pour la fouille de fichiers de log», JRES, Montpellier - 2015.

[2] https://blog.sekoia.io/fr/traffers-une-plongee-dans-lecosysteme-des-voleurs-dinformations/