Les synthèses du CLUSIF

Le Dark Web : Enjeux et Mesures - *Synthèse de la conférence thématique du CLUSIF du 16 avril 2015.*

L'activité des cybercriminels s'organise majoritairement sur Internet, en utilisant des serveurs, des plus ouverts aux plus fermés, et des réseaux d'anonymisation comme TOR. L'enjeu pour les organisations souhaitant se protéger est double : anticiper des actions ciblées en préparation afin d'éviter la survenance d'un incident et aussi détecter les fuites de données sensibles.

Pour adresser cette problématique, l'objectif du RSSI va être de suivre cette activité cybercriminelle en mettant en place des processus de veille permettant d'analyser le web en y recherchant ce qui concerne son organisation, notamment sur les serveurs fermés et les sites anonymisés. Un tel processus permet ainsi d'anticiper la survenance ou de limiter l'impact d'un incident. Pour cela, il pourra, par exemple, s'appuyer sur des solutions et des services professionnels de surveillance externe qui scannent et fouillent régulièrement l'Internet.

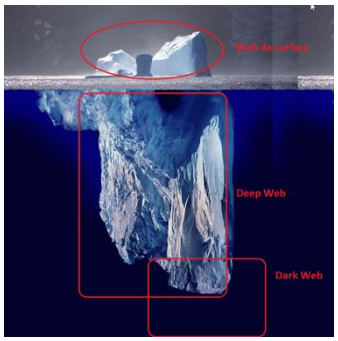
Fort de cet état des lieux, le CLUSIF a souhaité faire un point complet sur ce sujet lors de la conférence du 16 avril 2015. Six intervenants ont partagé leurs expertises et retours d'expérience : Lazaro PEJSACHOWICZ (CLUSIF), François PAGET (Intel Security/ McAfee Labs), Anne SOUVIRA (Commissaire divisionnaire chargée de mission aux questions relatives à la cybercriminalité), Henri CODRON (Responsable de l'Espace RSSI du CLUSIF), Benoit MERCIER et Adrien PETIT (CEIS) et, comme animateur de la table ronde, Jean-Marc GREMY (CLUSIF).

Introduction par le CLUSIF – Lazaro PEJSACHOWICZ.

Dans son introduction, Lazaro PEJSACHOWICZ fait le constat suivant : comme le web sombre est utilisé par les trafiquants, les *hacktivistes* et autres révolutionnaires, il est important pour les entreprises de s'y intéresser. C'est un moyen de mieux se protéger.
En tant que moyen de cacher et de protéger certaines informations le *dark web* peut également être utilisé dans des contextes non criminels liés, Lazaro PEJSACHOWICZ appelle à dissocier le support de l'usage qui en est fait et pose alors la question des limites entre le *bon* Web sombre et le *mauvais*.

Visite guidée du Dark Web – François PAGET (Intel Secuity/McAfee Labs)

François PAGET introduit cette visite guidée en définissant les deux espaces que sont le web invisible (*deep web*) d'une part et le web sombre (*dark web*) d'autre part.[1]
Tout d'abord, le web invisible ou web profond peut être caractérisé par la partie du web accessible en ligne mais non indexée par des moteurs de recherche classiques généralistes.



Le web invisible contient des sites légitimes (bases et banques de données, bibliothèques en ligne gratuites ou payantes, etc..) ainsi que des sites douteux, malsains et criminels. Certaines parties du web invisible ne sont accessibles qu'au travers d'outils spécifiques tels que TOR (The Onion Router) [2], Freenet[3] ou I2P (Invisible Internet Project)[4] qui offrent, de surcroit, un certain anonymat aux visiteurs.

[1] http://davidenewmedia.wordpress.com/workingterms/deep-web/
[2] http://fr.wikipedia.org/wiki/Tor_%28r%C3%A9seau%29
[3] http://fr.wikipedia.org/wiki/Freenet
[4] http://fr.wikipedia.org/wiki/I2P

L'accès au web invisible se fait en modifiant son environnement afin d'anonymiser son poste de travail, par exemple en utilisant des outils tels que TOR ou I2P. Sécurité oblige, il est aussi préconisé de travailler en environnement virtuel (exemple VMWare).

Le web sombre est, en partie, contenu dans le web invisible tout comme il est en partie anonymement accessible via les outils spécifiques précédemment cités. Il ne contient que des sites douteux, malsains et criminels.
Que trouve-t-on sur le web sombre ?

- Des sites où les cybercriminels publient des infos confidentielles et personnelles sur des individus ou des entreprises en représailles à une action menée par ces individus ou ces entreprises qui en sont la victime. (*Doxing*[5]).
- Des boutiques de vente : de cigarettes, de faux papiers, de faux billets, d'armes.
- Des sites de *carding* (vente de *pan* de cartes bancaires volées).
- Des sites permettant de faire appel à des organisations criminelles et d'acheter leurs services. Réelles ou farfelus, on y trouve même des offres pour meurtre et viols.
- Des sites pédopornographiques.
- Des sites de maitres-chanteurs (Par exemple : Rex Mundi) utilisés pour la divulgation de données personnelles et de données d'entreprises, lorsque les intéressés ont refusé le chantage (refus de paiement de la rançon).

En aparté, François PAGET se pose la question de la disponibilité des « produits » offerts sur ces site. Est-on sûr de recevoir ce que l'on a commandé : « Si l'on n'est pas un cybercriminel averti, on a de grandes chances de perdre son argent sans jamais recevoir le produit ou le service espéré ! ».

Deep Web et Dark Web, enjeux et mesures – Anne SOUVIRA (Commissaire divisionnaire chargée de mission aux questions relatives à la cybercriminalité)
En complément de la présentation précédente, Anne SOUVIRA souligne les spécificités du *deep web* et du *dark net*.

Le *dark net* est un ensemble de réseaux privés de petite taille permettant la connexion entre **des** personnes de confiance, ce sont des réseaux privés de partage. Ces réseaux anonymes peuvent être chiffrés (*cipher spaces*) ou accessibles via des outils P2P (Peer to Peer).

Le *deep web* est le web non indexé car certains sites ont un contenu généré de façon dynamique ou pour lesquels les administrateurs ont pris des mesures afin de protéger leurs sites de l'indexation des moteurs de recherche. Ces sites sont protégés par des mots de passe et l'on doit s'y connecter via des ports non standards. Pour obtenir ces mots de passe, il faut être connu, et appartenir à une communauté où la réputation joue un rôle majeur pour avoir accès aux forums et ainsi faire des affaires avec les autres membres.

Ces membres communiquent via des messageries instantanées (*IM*) de type ICQ ou Jabber. Certains sites ont leurs propres serveurs *IM* chiffrés et intègrent des systèmes de transfert de fichiers sécurisés.

Anne SOUVIRA insiste sur la présence de contenu illicite du *deep web* et des *dark net* en particulier au sujet de la pornographie infantile qui s'y échange compliquant la tâche des enquêteurs.

Ensuite l'oratrice aborde le sujet des crypto monnaies et en particulier le *Bitcoin*. Ces monnaies sont échangeables sur les *dark net* alors vecteurs de blanchiment et permettant l'achat de malware type rançongiciel type *crypto locker*. Le Bitcoin est généré (minage) par une chaine cryptée de transactions numériques. Cette monnaie fluctue très significativement vis-à-vis de l'Euro. Elle peut disparaître par hacking ou crash de l'ordinateur qui a permis de la générer.

La création de Bitcoins nécessite une importante puissance de calcul que le particulier ne peut mettre à disposition. Mais en utilisant la puissance de calcul des ordinateurs de ses collègues un utilisateur pourrait *miner* des Bitcoins dans l'entreprise ! D'où l'intérêt pour le RSSI d'en être informé et de s'intéresser à l'usage des postes de travail de son organisation.

[5] http://fr.wikipedia.org/wiki/Doxxing

Enfin, Anne SOUVIRA dresse un état des lieux de la menace :

- la recherche du profit par la vente d'outils (RAT, chevaux de Troie, virus, kits de DDoss), l'utilisation de ces outils pour obtenir des données de valeurs (mot de passe, etc.), de logiciels d'usurpation (spoofing) de numéros de téléphones et d'adresses IP,
- l'exploitation sexuelle des enfants en ligne,
- la fraude massive à la carte bancaire grâce au *phishing*. La collecte de numéros de cartes bancaires ou d'IBAN pour virement rapporte plus que le trafic de stupéfiants selon les études type PwC.

Face aux évènements de janvier 2015 durant lesquelles les organisations ont connu près de trois semaines des défigurations massives de sites web et des photocopieuses crachant de la propagande, nous constatons la fragilité potentielle des cibles de cybermenaces.
Face à cette menace, l'implication des forces de l'ordre est essentielle au maintien des principes démocratiques et au respect des libertés fondamentales.

Pourquoi les RSSI doivent-ils s'intéresser au Dark Web ? – Henri CODRON (Responsable de l'Espace RSSI du CLUSIF).
L'intérêt pour le thème du *dark web* a été mis en avant au sein de l'espace RSSI du CLUSIF.

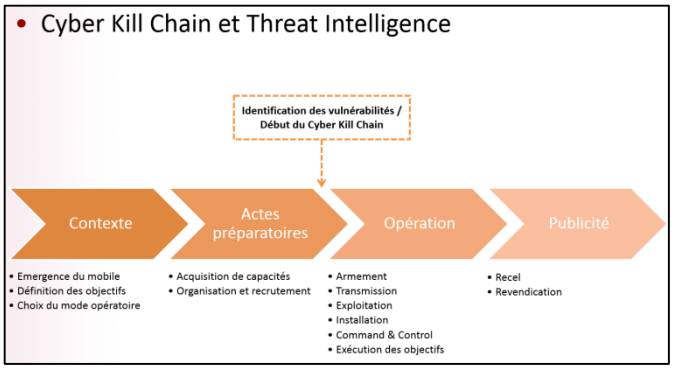
Le RSSI a pour mission de protéger le SI de son organisation. Face aux multiples menaces, les SI ne sont pas toujours protégés et deviennent et peuvent présenter des vulnérabilités. Les entreprises sont ainsi diversement préparées pour faire face à ces risques.

Fort de ce constat, il convient de rechercher des signaux faibles.
Les organisations s'équipent de moyens de surveillance pour détecter ces signaux faibles et identifier si celles-ci sont en cours d'infection ou si elles sont sur le point de devenir une cible potentielle.

L'objectif est de détecter des signes avant-coureurs, par exemple en trouvant des *rootkit*[6] ou des *malware* en préparation, mais également de retrouver les données volées lors d'une attaque précédente.
La question se pose de mettre en place les moyens appropriés à une telle démarche.

Comment réagir, quelles mesures appliquer ? – Benoit MERCIER et Adrien PETIT (CEIS).
Benoit MERCIER et Adrien PETIT présentent un modèle de réponse au besoin de prendre en compte le *dark web* lors de l'élaboration d'un plan de sécurité d'une organisation.

En préambule, les intervenants dressent une cinématique de la menace à laquelle il va être nécessaire de répondre. Cette cinématique commence à la motivation de l'acte pour aller jusqu'à son exécution passant par sa préparation :



Adrien PETIT, présente une étude de cas illustrant le mode opératoire d'une analyse de fuite de données :

- Identification des informations sensibles sur un site de *pasties* - Détection d'un signal faible,
- Identification d'un point de contact ou URL vers un forum du *dark web*,
- Diffusion d'un message du pirate sur un forum indiquant le moyen de le contacter (ICQ, MP, Jabber),
- Selon la demande client, échanges avec le cybercriminel, prise de contact, demande d'informations et enfin négociations,
- Redirection vers un black market pour finaliser l'achat,
- Demande d'un échantillon pour vérification puis acquisition de l'intégralité des documents.

[6] http://fr.wikipedia.org/wiki/Rootkit

Le premier élément de réponse à une telle menace est de se positionner en anticipation et de savoir se mettre à place des cyber-attaquants afin de bien comprendre les motivations et modes opératoires.
Pour cela il est nécessaire de combiner des outils d'analyse autant que des moyens humains : experts en sécurité de l'information et en intelligence économique.

	Technologie	Couverture	Limite des outils	Humain
Web de surface	Outils sur étagère	- Réseaux sociaux - Sites de partage - Sites de diffusion - Sites de stockage - Forums	Flux de données brutes sans analyse	- Présence proactive sur les canaux de communication - Analyse thématique (technique, géopolitique, etc.) - Analyse de tendance - Vision prospective
Deep Web	Outils sur étagère + Développement d'outils spécifiques			
Dark Web	Développement d'outils spécifiques	- Wikis - Forums - IRC - Blackmarkets	Difficultés pour acquérir l'information à forte valeur ajoutée	

L'objectif est de développer une connaissance suffisante des supports utilisés dans le cadre de menaces :

- réseaux sociaux, ex. Rex Mundi,
- bases de données de *pasties* (pastebin.com, justepaste.it),
- Instructions d'attaque DDoS et fuite de données,
- outils de communication traditionnels (channels IRC, Reddit, sites de diffusion),
- outils et services utilisés sur le *dark web* : wiki, moteurs de recherche, forums, IRC, blackmarkets, mails anonymes.

Table Ronde animée par Jean-Marc GREMY.
François PAGET (Intel security/McAfee Labs), Anne SOUVIRA (Commissaire divisionnaire chargée de mission aux questions relatives à la cybercriminalité), Henri CODRON (Responsable de l'Espace RSSI du CLUSIF), Benoit MERCIER et Adrien PETIT (CEIS)

Question - Existe-t-il des moyens de bloquer l'accès au *dark web* ?

On peut rendre l'accès au site difficile voire impossible. Mais dans les faits on ne peut jamais empêcher le site de ressurgir ailleurs.
Il faut être extrêmement prudent et faire attention aux informations que l'on diffuse.

Question - Le *dark web* a-t-il déjà donné des informations utiles en lien avec la sécurité ?

Cela permet :

- de détecter des cibles potentielles
- d'identifier comment évolue la menace (kits d'exploit).
- de réaliser des captures d'écran pour les équipes de marketing !

D'un point de vue technique, la surveillance du *dark web* permet d'opérer une veille sur l'émergence de nouveaux outils. Enfin, cette surveillance permet

- de se tenir au courant des raisons et des motivations des groupes d'hacktivistes,
- d'identifier les tendances,
- de détecter des vulnérabilités,
- de détecter les évolutions technologiques du point de vue du hacking.