1. BESOIN

Ce document a pour but de formaliser les attentes concernant le défi Cyber intitulé « *Investigation à distance des cyberattaques* », annoncé aux start-up, petites et moyennes entreprises (PME) et établissements de taille intermédiaires (ETI) par la ministre des Armées à l'occasion du Forum International de la Cybersécurité (FIC) les 23 et 24 janvier 2018, et qui trouvera sa concrétisation lors de l'édition 2019 du FIC, les 22 et 23 janvier prochains.

1.1. DEFINITION

Le terme EDR (pour *Endpoint Detection & Response*) est un concept désignant une catégorie de logiciels permettant d'accélérer la réponse à un incident cybernétique. Cette capacité repose sur la mise en œuvre d'agents logiciels sur différents équipements du réseau (serveurs, stations de travail, etc.) afin d'effectuer certaines opérations de prélèvement ou d'analyse de manière automatisée à distance.

1.2. OBJECTIFS

Le produit proposé doit répondre au minimum à un des objectifs suivants :

- Permettre de qualifier rapidement l'impact global d'une menace sur un parc informatique.
- Proposer des moyens d'analyse *in vivo* des équipements positionnés sur un réseau.
- Automatiser les tâches d'analyse récurrentes.
- Permettre la conduite d'opérations de *hunting* sur un parc informatique conséquent.
- Synthétiser les éléments présentés.

1.3. CONTRAINTES

Diverses contraintes, inhérentes à l'environnement ciblé, existent et le produit proposé doit en prendre un maximum en compte :

- Travailler sur des réseaux dont le débit est relativement réduit (environ 100 Ko/s), notamment sur les théâtres d'opérations reculés.
- Opérer sur divers systèmes d'exploitation (GNU/Linux, Microsoft Windows, Sun Solaris, BSD, Android, macOS, iOS, etc.).
- Supporter une mise à l'échelle afin de gérer un parc de plusieurs dizaines de milliers de machines.
- Opérer de manière décentralisée afin de ne pas saturer les réseaux de desserte.
- Possibilité d'installer l'agent sur des systèmes contrôlés (signature des agents, etc.).
- La communication entre les agents et les serveurs de contrôle devra être opérée de manière sécurisée (chiffrement des données avec authentification).
- Les agents déployés ne devront pas impacter de manière significative les performances des systèmes hôtes.
- Les agents déployés devront disposer d'un mécanisme de persistance leur permettant d'ignorer ou de résister aux actions suivantes (liste non exhaustive) :
    - Redémarrage intempestif.
    - Extinction de la machine hôte.

- Arrêt brutal du processus de l'agent par l'utilisateur.

1.4. ORGANISMES DEMANDEURS

L'outil proposé disposera d'une interface permettant d'accompagner le travail d'utilisateurs de différents niveaux.

Organisme(s) de niveau 1 (analyse statistique) :

- SOC central (DIRISI).

Organisme(s) de niveau 2 (analyse technique d'envergure) :

- Centre d'Analyse en Lutte Informatique Défensive (CALID).

Organisme(s) de niveau 3 (analyse technique ciblée) :

- SOC d'armée (Armée de l'Air, Marine Nationale).
- SOC de théâtre (Levant).
- Divers acteurs LID du ministère (DGA).

1.5. CAPACITES D'ANALYSE *IN VIVO*

Afin de répondre aux objectifs décrits, l'outil devra disposer de plusieurs fonctionnalités permettant l'investigation numérique à distance.

Le produit présenté devra notamment être en mesure d'effectuer le maximum d'actions suivantes (liste non-exhaustive) :

- Analyse des ruches de la base de registre Windows.
- Analyse de la mémoire vive.
- Permettre de fédérer de manière synthétique les caractéristiques techniques et les performances de la machine hôte.
- Génération de rapports d'analyse dans divers formats.
- Analyse du trafic réseau transitant sur les interfaces physiques et/ou logiques de la machine.
- Recherche d'indicateur de compromission (noms de fichiers, adresses IP, noms de domaine, règles YARA, etc.).
- Téléchargement de fichiers présents sur le poste cible vers un emplacement réseau en vue d'une analyse complémentaire (analyse non-comprise dans le périmètre).
- Administration à distance native en ligne de commande (de type *shell*) au travers de l'agent.
- Génération de *timelines* basées sur les journaux d'évènements du système et des applicatifs.
- Planification d'opérations récurrentes sur un ou plusieurs ensembles de machines définis.
- Navigation au travers de l'arborescence du ou des systèmes de fichiers.
- Blocage d'adresses IP, d'adresses MAC ou de noms de domaines particuliers au niveau des clients.
- Récupération de fichiers effacés et/ou déréférencés.

2. CONTEXTUALISATION

2.1. SCENARIO

Afin de visualiser au mieux les objectifs attendus, le scénario ci-dessous présente le déroulé d'une investigation sur une attaque informatique fictive contre un réseau des armées.

Note : Les points mis en gras soulignent les différentes fonctions reposant sur le produit à développer.

[27/02/2020 14:58] Signalement d'un ralentissement important sur un des systèmes de surveillance aérienne du site de Saint-Dizier en métropole. L'unité en charge de la cyber-surveillance du site ne dénote aucun incident particulier.

[28/02/2020 10:23] Signalement par un partenaire de confiance d'un fichier PE « `dem352.exe` » ainsi que d'un condensat cryptographique SHA-1 « `f161ebd29699d93411cec0915c5133c0f3229a28` » possiblement en lien avec une campagne d'espionnage industriel et de sabotage ciblant la France depuis plusieurs semaines.

[28/02/2020 14:02] Suite à ce signalement, une **recherche globale préventive de ces deux indicateurs** est lancée sur l'intégralité du parc informatique national.

2.1.1 PRIMO-ANALYSE

[28/02/2020 14:51] Au vu des premiers résultats remontés par la recherche, cinq postes de travail semblent être concernés par la présence d'un exécutable ayant le condensat évoqué par le signalement. Les plages d'adresses IP auxquelles appartiennent ces postes indiquent que ces derniers sont **localisés sur des sites géographiques différents.**

[29/02/2020 11:10] Après une **corrélation automatique des résultats finaux** remontés par la recherche, l'isolement d'un indicateur commun souligne un total de huit postes rapportant la présence d'un fichier exécutable au nom variable ayant le condensat cryptographique « `f161ebd29699d93411cec0915c5133c0f3229a28` » donné dans le signalement initial.

[29/02/2020 12:11] Catégorisation et déclenchement d'un incident de lutte informatique défensive au niveau national.

2.1.2 QUALIFICATION DE LA MENACE

[29/02/2020 13:48] Afin de mieux caractériser la menace, une **extraction de tous les moyens de persistance** sur ce groupe de machines est lancée.

[29/02/2020 15:22] L'analyse des moyens de persistance fait remonter la présence de valeurs suspectes pointant vers l'exécutable décelé dans les clés « `HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Run` » de la base de registre Windows de plusieurs profils utilisateurs utilisant les stations victimes. À première vue, le nom de cette valeur semble varier pour chaque hôte impacté.

[29/02/2020 15:35] Afin de délimiter le périmètre de l'incident et de qualifier la probabilité de propagation de la menace, une « **capture du trafic réseau »** des machines impactées est lancée.

[01/03/2020 14:02] Après **corrélation des résultats**, on observe un **pic de requêtes similaires** vers une adresse IP `192.X.Y.65` du réseau interne ainsi que des **requêtes à intervalles réguliers** vers une adresse IP publique `183.X.Y.199` Internet non répertoriée dans les listes noires du MINARM.

[01/03/2020 14:35] Selon les informations récupérées en interne, l'adresse IP `192.X.Y.65` semble appartenir à un plan d'adressage dédié à l'activité opérationnelle du site de Saint-Dizier. Rapprochement de l'incident actuel et du dysfonctionnement du système de surveillance aérienne remonté le 27 février. Déclenchement d'une cellule de crise.

[01/03/2020 16:12] Identification formelle de l'adresse IPv4 `192.X.Y.65` comme étant le serveur applicatif d'un des systèmes de surveillance aérienne du site. Remise en question de l'intégrité du système d'information. Suspension immédiate des vols ordonnée par le commandement.

[01/03/2020 16:18] Une qualification simple de l'adresse IP `183.X.Y.199` permet d'associer cette dernière au nom de domaine `star-shopper.zz` détenu par un site d'*e-shopping* probablement compromis.

[02/03/2020 09:21] **Analyse du trafic réseau et des performances** du serveur possédant l'adresse IP `192.X.Y.65`, observation de nombreux paquets de synchronisation TCP – sans jamais d'acquittement retour de la part du client – en provenance de deux adresses IP différentes, engendrant une charge processeur et réseau importante.

2.1.3 ANALYSE DE LA CHARGE MALVEILLANTE

[02/03/2020 11:11] **Téléchargement des huit fichiers** exécutables dont les condensats SHA-1 correspondent au signalement initial « `f161ebd29699d93411cec0915c5133c0f3229a28` ».

[02/03/2020 11:42] Envoi d'un des fichiers au centre d'analyse pour rétro-ingénierie et caractérisation de la menace.

[02/03/2020 11:45] Parallèlement, une **analyse mémoire** est lancée sur une des machines marquées par la présence de ce fichier. Cette analyse révèle plusieurs descripteurs de fichiers sensibles ouverts dans l'espace mémoire du processus associé au fichier suspect.

[04/03/2020 15:36] Retour du rapport d'analyse du fichier démontrant la dépendance de ce dernier envers deux bibliothèques dynamiques `faj4e.dll` et `netesd.dll`. Le rapport fourni souligne le caractère limité de l'analyse du fait de l'absence des deux fichiers énoncés, et mentionne également la présence des chaines de caractères statiques `.doc`, `.docx`, `.xls` et `.xlsx` dans le code *malware*.

[04/03/2020 16:10] Lancement d'une **recherche de fichiers** sur les huit machines infectées en ciblant les deux bibliothèques dynamiques `faj4e.dll` et `netesd.dll` indiquées dans le rapport d'analyse. La recherche remonte rapidement des correspondances sur deux des huit machines infectées. Au vu des éléments, une recherche est lancée à la demande du commandement sur l'ensemble du parc de machines au niveau national.

[05/03/2020 08:18] Aucun résultat supplémentaire remonté par la recherche globale.

[05/03/2020 08:58] La **comparaison des condensats des fichiers** remontés par cette recherche démontre la présence de deux fichiers distincts ayant pour condensats SHA-1 « `576acc5a01fe3e7b6516e4ebe2d1a74904987abf` » et « `5ab2ab673777572a05f5f21cc5780c4adaf15b8f` ». Le **prélèvement respectif des deux fichiers** `faj4e.dll` et `netesd.dll` est lancé sur une des deux machines en question.

[05/03/2020 09:34] Transmission de ces deux fichiers au centre d'analyse pour complément d'investigation.

[08/03/2020 14:49] Le rapport d'analyse confirme que les deux bibliothèques dynamiques proposent des fonctionnalités réseau, notamment liées à l'envoi de fichiers et à du *SYN flooding*. De plus, deux noms de domaines « `su5req.zz` » et « `star-shopper.zz` » correspondants à deux serveurs de contrôle peuvent être lus dans l'espace mémoire du processus chargeant ces bibliothèques dynamiques. Remise en question de la légitimité du site d'e-shopping « `star-shopper.zz` ».

2.1.4 REMÉDIATION LOCALE

[09/03/2020 09:50] À la demande du commandement et afin de permettre au site de Saint-Dizier de réactiver son dispositif aérien, un **blocage local des adresses IP** des deux postes disposant des bibliothèques dynamiques aux condensats « `576acc5a01fe3e7b6516e4ebe2d1a74904987abf` » et « `5ab2ab673777572a05f5f21cc5780c4adaf15b8f` » est effectué sur le serveur de surveillance aérienne.

2.1.5 RECONSTRUCTION DE L'ATTAQUE

[09/03/2020 11:20] **Génération des *timelines*** basées sur l'intégralité des fichiers journaux des huit machines infectées ainsi que du serveur applicatif appartenant au système de surveillance aérienne impacté.

[09/03/2020 16:01] Compte-rendu de l'escale aérienne de Saint-Dizier constatant le retour en fonctionnement nominal du système.

[11/03/2020 15:32] Le **recoupement des différentes *timelines*** permet de faire corréler l'horaire de début du *SYN flooding* vers le serveur applicatif et la réception des paquets TCP vers ce même serveur. On observe également qu'au moment où les requêtes régulières vers les domaines « `su5req.zz` » et « `star-shopper.zz` » ont été effectuées par les deux machines infectées par les fichiers « `faj4e.dll` » et « `netesd.dll` », des accès à des fichiers disposant des extensions `.docx` et `.xlsx` ont été fait sur ces même machines par le processus du code malveillant initial.

2.1.6 REMÉDIATION GLOBALE

[12/03/2020 10:32] Demande officielle d'ajout de l'adresse IP `183.X.Y.199` ainsi que des noms de domaines « `su5req.zz` » et « `star-shopper.zz` » identifiés comme des serveurs de contrôle dans les listes noires du MINARM.

[12/03/2020 14:58] Sur autorisation du commandement des opérations, **l'élimination de manière centralisée** de tous les exécutables malveillants décelés ainsi que des bibliothèques dynamiques `faj4e.dll` et `netesd.dll` est lancée parallèlement à **l'arrêt centralisé des processus** associés à ces derniers. **Suppression des valeurs de registre** présentes dans les clés « `HKEY_CURRENT_USER/Software/Microsoft/Windows/CurrentVersion/Run` » de chaque utilisateur et pointant vers les exécutables malveillants.

[27/02/2020 14:58] Suite à l'accord du commandement des opérations aériennes du site de Saint-Dizier, le **déblocage local des deux adresses IP** des postes précédemment infectés sur le serveur de surveillance est lancé.

[27/02/2020 14:58] Création d'une **tâche planifiée sur deux semaines de manière journalière** vérifiant que les fichiers identifiés ne soient plus présents sur l'intégralité du parc informatique national, que les

condensats cryptographiques « `f161ebd29699d93411cec0915c5133c0f3229a28` », « `576acc5a01fe3e7b6516e4ebe2d1a74904987abf` » et « `5ab2ab673777572a05f5f21cc5780c4adaf15b8f` » associés à ces fichiers ne soient plus présents sur les systèmes de fichiers des machines du parc.

[27/02/2020 14:58] **Génération automatisée d'un rapport** comportant la *timeline* complète de tous les évènements d'importance pour l'incident ainsi que des éléments permettant de reconstruire l'attaque.

2.1.7 QUALIFICATION DE LA COMPROMISSION

[27/02/2020 14:58] Montée de l'incident au niveau du renseignement et du service de gestion des compromissions afin d'évaluer la criticité de la fuite des documents sensibles exfiltrés.