Agir contre un maliciel

*Fiche à l'attention des **Responsables de la Sécurité des Systèmes d'Information (RSSI)***

1 Confinement

- **Isoler la machine du réseau** sans l'éteindre. Cela peut permettre notamment de retrouver des clés de chiffrement. Si ce n'est pas possible, isoler la machine d'Internet et des autres machines du réseau, en particulier des serveurs de fichiers.
- **Bloquer l'accès de la machine et les utilisateurs compromis** à l'ensemble des services exposés sur internet (RDP, Webmail, VPN, ...)

En cas d'un grand nombre de machines infectées :

- **Déconnecter les sauvegardes** et vérifier leur intégrité avant leur restauration
- Configurer le partage des fichiers **en lecture seule**
- **Fermer les services exposés sur Internet** en connexion direct avec votre réseau : RDP, WEBMAIL, VPN, SSH, ... **Et les possibilités de sortie** : pas de résolution DNS externe directe depuis un serveur/poste, pas de sortie internet directe, obligation de passer par un proxy en mode liste blanche (seulement vers des URL maitrisées, interdire tous les tunnels/RAT). Configurer les serveurs de fichiers (NAS/DFS) en lecture seule.
- **Déconnecter les serveurs critiques potentiellement responsables d'une propagation interne** du maliciel/rançongiciel (Pour l'environnement Windows : AD -> GPO / WSUS -> update / DFS -> file) et **faire un snapshot** pour les serveurs virtuels (RAM et disque)
- **Bloquer les communications** malveillantes identifiées sur vos différents équipements (firewall, proxy, smtp, dns, ...) lors de l'investigation, en surveillant celles qui sont initiées par de nouvelles machines (suspicion de compromission)
- **Configurer vos équipements (firewall, proxy, smtp, dns, ...) pour bloquer** les moyens de l'attaquant (URL, domaine, IP, adresse courriel...)

2 Investigation/Identification

- **Utiliser un outil forensique pour extraire des artefacts** (ORC[ANSSI], FastIR[CERT SEKOIA], Sysinternals, ...) d'un snapshot d'une machine virtuelle. Pour Windows, il faut récupérer les artefacts (autorun, mft, usn, registres, events, RAM ou process+handles, prefetch, taches planifiées, liste des utilisateurs, ...).
- **L'utilisation de ces outils nécessite des droits élevés** (privilégier l'utilisation du compte admin local). Si l'attaquant a des privilèges, il pourrait récupérer les identifiants lors de connexions. **Il est donc indispensable de ne pas reconnecter la machine à Internet pendant et après cette opération**.
- **Récupérer les logs périphériques** en lien avec la machine (Antivirus central, DNS, Firewall, Proxy, Smtp (sortant et courriel entrant vers l'utilisateur), ACL réseau, netflow, IDS ...)
- **Analyser les artefacts** pour :
  a) **Identifier l'origine de l'infection** (patient zéro ou rebond), afin que l'attaquant ne puisse plus compromettre le système avec le même scénario d'attaque.
  b) **Identifier le niveau de privilège de la compromission** (utilisateur ou admin/système), afin d'adapter l'analyse des artefacts. Parfois l'origine n'est pas sur le poste identifié et peut provenir d'un accès à distance VPN, RDP, SSH, RAT par rebond.
- **Vérifier** que les services d'accès à distance sont à jour de patchs et qu'aucun compte n'a été compromis.
- **En cas d'hameçonnage, rechercher si d'autres utilisateurs ont reçu le courriel** et l'ont ouvert.

- **Déclarer l'incident** auprès des autorités compétentes (Ministère de la Santé, ANSSI, CNIL) et **déposer plainte** auprès des services de police ou de gendarmerie (voir la fiche « Réagir à un acte de cybermalveillance »)
- **En cas de crise, informer les utilisateurs** et leur communiquer la conduite à tenir
- Faire une **sensibilisation** à cette menace avec le kit mis à disposition par **cybermalveillance.gouv.fr**
- En cas de **demande de rançon en bitcoin**, **transmettre l'adresse** à https://www.bitcoinabuse.com/

Agir contre un maliciel

2 Identification (suite)

- **Rechercher les canaux de communications utilisés par l'attaquant**, afin de couper les connexions existantes et d'identifier d'autres ressources compromises
- **Identifier le début de la compromission**, afin de pouvoir restaurer le parc avec des sauvegardes intègres
- **Identifier la famille du maliciel** pour connaître les méthodes et l'objectif de l'attaque (rançon, vol de données, crypto-minage...). Cela permet d'adapter la remédiation (communication, changement d'identifiants internes et externes, déclaration CNIL, ...). Identifier ces informations avec https://attack.mitre.org/software/ et rechercher l'existence d'un outil de déchiffrement sur https ://nomoreransom.org/.
- **Identifier les éléments exfiltrés ou la quantité d'informations transmises** vers l'attaquant afin d'avoir une idée de l'ampleur des fuites
- **Identifier l'ensemble des utilisateurs** qui se sont connectés à la machine et leur demander de changer leur mot de passe (si l'accès de l'attaquant était à privilège, il a pu accéder au cache)
- **Rechercher les méthodes de propagation potentielles du maliciel** et vérifier qu'elles n'ont pas été activées
- **Réitérer ces actions** d'investigation sur les nouvelles machines identifiées comme compromises

3 Remédiation/Restauration

- **Corriger les failles à l'origine de l'infection** : mise à jour (par ex: CVE sur VPN, adobe/flash/java/navigateur, ...), revoir la politique d'accès extérieur (politique de mot de passe, fermer RDP, anti brute force, limiter les plages IP, double authentification, segmenter son réseau, arrivée en DMZ spécifique...), amélioration des protections (durcissement général, AppLocker, antivirus, filtrage messagerie et/ou proxy, segmentation réseau, firewall local, ...).
- **Restaurer un système intègre** : changement d'identifiant interne et externe (vol d'identifiant), communication (vol données sensibles), récupération et réinstallation des sauvegardes avant la compromission, reconstruire l'AD (attention très complexe si on ne veut pas repartir de zéro), suppression des fichiers infectés sur le partage réseau/DFS.
- **Bloquer toute possibilité de communication de l'attaquant** : mise en place d'un proxy, interdire les tunnels non standards via le proxy (RAT, ssh, ...), interdire la communication sur les ports non standards, interdire les tunnels DNS, ...
- **Bloquer toute possibilité de reprise de l'infection** : suppression des fichiers infectés du DFS, mise à jour des postes, firewall local, mise en place de filtrage (ACLs) inter VLAN, GPO pour ne permettre les connexions vers un poste en interne que depuis un utilisateur spécifique, ...
- **Installer** "sysmon" pour windows et "auditd" pour linux afin de pouvoir mieux identifier des éléments suspects lors du retour à la normale

4 *Retour à la normale*

- **Renforcer la protection du système contre l'exécution de programmes potentiellement malveillants** (ex: DFS -> FSRM, Applocker, ...)
- **Remettre en service le réseau interne en premier** puis **l'accès vers Internet en ayant bien validé préalablement la mise en œuvre des mesures de remédiation présentés ci-dessus**
- **Surveiller pendant quelques jours** le réseau interne et les connexions vers Internet pour détecter d'éventuels comportements anormaux ou des connexions suspectes (pas d'UA, connexion directe sur IP, port suspect, ...). Si c'est le cas, utiliser les informations de sysmon ou auditd afin d'identifier l'origine et la légitimité de la connexion.
- **Surveiller les marqueurs de l'attaque bloqués** pour vérifier qu'il n'y a plus de machine qui cherche à les utiliser
- **Remettre l'accès des services exposés sur internet** et surveiller qu'il n'y a aucune connexion suspecte réussie (GEOIP, horaire de connexion, useragent spécifique [mac, linux, navigateur qui n'est pas utilisé sur le SI, ...])
- **Investir sur la prévention avec le retour d'expérience** afin de limiter une potentielle nouvelle compromission.