Investigation numérique

1. INTRODUCTION GÉNÉRALE

Sommaire

01

Définitions et concepts fondamentaux

1. Définitions

Investigation numérique ou réponse à incident ?

Analyse forensique :
Pratique construite sur le modèle de la médecine légale et dont le but est la récupération et l'analyse de données techniques issues de différents appareils, souvent dans le contexte d'un crime ou délit

Processus global déployé par une entreprise pour prévenir, détecter, contenir et bloquer les compromissions de données, ainsi que reconstruire le système impacté.

L'investigation numérique peut donc s'inscrire dans le cadre d'une réponse à incident, mais est une activité distincte en soit.

1. Définitions

Récupération

Récupération, sécurisation et reconstruction éventuelles de données brutes afin de pouvoir récupérer des preuves :

- Appareils endommagés
- Fichiers chiffrés ou altérés
- …

Analyse

Collecte, à partir des données brutes, de preuves exploitables dans le cadre de la mission et analyse de ces dernières afin d'apporter des réponses aux questions posées.

Appareils

Tout appareil stockant, utilisant ou transmettant des données numériques :

- Serveur
- Imprimante
- Routeur
- Téléphone
- …

Crime ou délit

Tout crime ou délit impliquant un appareil numérique :

- Intrusion dans un système
- Phishing
- Fraude
- Meurtre
- Kidnapping
- …

2. Objectifs

Les objectifs d'une investigation numérique dépendent nécessairement de son contexte et de la situation ayant exigée une telle investigation.

Dans le cadre d'une réponse à incident :

- Identifier le vecteur d'intrusion et les points de persistance
- Trouver les indicateurs de compromissions
- Comprendre les Techniques, Tactiques et Procédures de l'attaquant
- Détecter des traces d'exfiltration de données
- …

Dans le cadre d'une investigation légale:

- Prouver que le suspect à accédé à tel ou tel site
- Positionner le suspect géographiquement à un moment précis
- Lister les activités réalisées sur un appareil
- …

Les objectifs d'une investigation numérique sont donc très variés, mais dans tous les cas il s'agira de répondre à une ou plusieurs questions à partir des données collectées.

Enfin, les objectifs peuvent évoluer tout au long de l'investigation en fonction des découvertes.

02

Méthodologie générale

2.0 Phases principales d'une investigation

Six grandes phases aboutissant à la rédaction d'un rapport d'investigation:

- Cette décomposition n'est pas absolue.
- En fonction du contexte, il sera parfois difficile voire impossible de réaliser certaines de ces tâches.
- Il sera aussi parfois nécessaire d'appliquer plusieurs itérations d'une ou plusieurs phases, voire du processus complet.

2.1 Récupération et sécurisation des données

Phase de sécurisation de l'environnement de collecte et de récupération des données brutes et des appareils au besoin.

Sécurisation de l'environnement de collecte :

- Inventaire des actions réalisées avant l'arrivée
- Sécurisation du lieu avec interdiction d'accès
- Prise de photos de la scène de crime si approprié

Données brutes :

- Mémoire vive
- Copie bit-à-bit des disques durs
- Récupération des appareils si besoin
- Initialisation de la chaîne de preuve (traçabilité)

Cette étape est absolument primordiale pour les forces de l'ordre qui interviennent sur de vraies scènes de crimes et qui ont besoin de procéder de manière très procédurière pour garantir leurs résultats devant un tribunal. Elle s'applique beaucoup moins dans un cadre privé.

2.2 Définition des objectifs

C'est durant cette phase que l'on définit les objectifs de l'investigation, *i.e* les questions auxquelles on doit répondre, mais également comment et à partir de quels éléments on pense y répondre.

- Monsieur Durand a-t-il appelé Madame Michu au moment du crime ?
- Monsieur Durand a-t-il utilisé la clef USB de Madame Michu ?
- Le binaire lock.exe a-t-il été exécuté sur le poste ?
- Le poste a-t-il été compromis pendant l'incident ?

- Récupérer les données d'appel du téléphone de Monsieur Durand
- Récupérer les EVTX relatifs aux périphériques et la base de registre
- Récupérer tous les artefacts systèmes indiquant une exécution
- Récupérer…. Tout ce qu'on peut ?

- calllog.db, logs.db, …
- Microsoft-Windows-UserPnp%4DeviceInstall.evtx, Microsoft-Windows-Ntfs%4Operational.evtx, SYSTEM, …
- UserAssist, AmCache, AppCompatCache, …
- Artefacts systèmes, journaux réseaux, journaux applicatifs, …

Cette approche est encore une fois très orientée FdO. Vous verrez dans les cas pratiques qu'il est beaucoup moins simple d'avoir cette approche dans un cadre d'investigation privée (type investigation suite au chiffrement du SI).

2.3 Préparation et récupération des artefacts

Cette étape consiste à récupérer, à partir des données brutes collectées, les éléments listés à l'étape d'avant.

Pour chaque artefact à récupérer :

On identifie l'outil adéquat pour récupérer l'artefact

On prépare les données si besoin (déchiffrement de disque, montage de partition, …)

On récupère l'artefact de façon à en garantir l'intégrité et on documente son acquisition

Tous les artefacts collectés doivent être stockés sur un système de fichier accédé en lecture seule pour éviter toute altération.

2.4 Analyse

Etape la plus importante en terme de temps, l'étape d'analyse est celle durant laquelle les artefacts collectés sont étudiés à la recherche d'éléments permettant de répondre aux questions posées.

Le sujet est très vaste en soit mais la phase d'analyse comporte généralement plusieurs étapes dont :

Parsing

Récupération de données lisibles et compréhensibles par l'humain à partir de l'artefact brut

Tri

Classification des informations fournies par l'artefact entre les données pertinentes et non pertinentes

Interprétation

Compréhension et qualification des données relativement au contexte pour en tirer des conclusions

2.5 Consolidation et documentation

Point final de l'investigation, la phase de consolidation est la phase pendant laquelle sont mises en relations toutes les découvertes et conclusions pour répondre à l'ensemble des questions et faire la lumière sur les faits.

Consolidation

- Etablissement d'une chronologie
- Mise en relation des faits pour comprendre le scénario global
- Peut entraîner une requalification des constats ou déboucher sur d'autres questions

Documentation

- Expliquer et vulgariser l'ensemble des constats techniques de manière claire
- Réussir à rendre explicite ce que racontent les faits et comment ils s'articulent afin de saisir le scénario global
- Adapter son discours à la cible

Les productions réalisées pendant cette étape sont les seules que verront les personnes intéressées (clients, FdO, juges, …). Elle sera leur seule vision de votre travail. Il ne faut donc surtout pas la sous-estimer et bien prendre soin à apporter toutes les nuances et précisions possibles afin que vos constats soient parfaitement compris.

2.6 Exemple de rapport

Voici un exemple de modèle de rapport d'investigation (gardez le sous le coude !)

Cet exemple est particulièrement pertinent pour des investigations suite à un incident. Surement beaucoup moins pour une enquête criminelle.

1. Sommaire exécutif
   - Explication des constats et des éléments principaux pour des personnes non techniques
2. Contexte
   - Détails des faits ayant déclenché l'investigation, du contexte technique et organisationnel
   - Liste des éléments collectés
3. Démarche d'investigation
   - Explication de la démarche d'investigation choisie et de la pertinence de celle-ci
4. Constats
   - Liste des faits constatés et vulgarisés de façon à rendre explicite leur intérêt et leur impact
   - Les faits peuvent être regroupés par grandes parties thématiques afin de gagner en clarté et de bien mettre en exergue les différentes phases d'un incident
5. Remédiations
   - Liste des remédiations appliquées pendant l'incident pour mitiger son impact
6. Conclusion
   - Reprise de l'ensemble des constats de manière synthétique
7. Recommandations
   - Liste des recommandations déduites des constats et à mettre en place pour limiter la survenue d'incident du même genre
8. IOCs et TTPs
   - Présentation des indicateurs de compromissions identifiés pendant l'investigation
   - Explication des Tactiques, Techniques et Procédures mises en œuvre par la partie attaquante

Des questions ?