ExaTrack

Trouver et neutraliser l'attaquant

Recherche de compromission

ExaTrack

Sommaire

- Présentation
- Constat de l'existant
- Quand faire une recherche de compromission ?
- Recherche de compromission
  - Méthodologie
  - Collecte des informations
  - Analyse des données
  - Identification d'activité malveillante
- Nos innovations
- Conclusion

ExaTrack

Présentation

Spécialisée dans l'identification de compromissions ciblées **inconnues** (APT)

Stéfan Le Berre

- A travaillé à l'ANSSI comme expert en analyse de codes malveillants
- Découverte de vulnérabilités en noyau Windows
- Plus de 10 ans d'expériences en analyse de malware
- Pratique la rétro-ingénierie depuis 15 ans

Clément Rouault

- Orateur dans de multiples conférences (ex : PacSec)
- Découverte de vulnérabilités en noyau Windows
- Développeur de PythonForWindows
- Pratique la rétro-ingénierie depuis 6 ans

ExaTrack

Constat de l'existant

ExaTrack

Constat de l'existant

Ce n'est pas parce qu'il n'y a pas de preuve d'espionnage qu'il n'y a pas d'espionnage

Les attaques informatiques sont de plus en plus ciblées

ExaTrack

Constat de l'existant

Les anti-virus ne détecteront pas une attaque ciblée (car elle est spécifique à la victime)

Un réseau déconnecté n'arrêtera pas un attaquant déterminé (Stuxnet, Flame, ...)

ExaTrack

Constat de l'existant

"2017 a vu se concrétiser des attaques graves en termes de renseignement, de vol d'informations, avec des attaquants toujours plus forts, toujours plus agiles, et qui ont manifestement des moyens considérables. C'est ce que me disent les industriels : le jour où ils découvrent, sur tel ou tel salon, leur prototype présenté par leur concurrent, ils ont un éclair de lucidité. On est dans un domaine où, contrairement à ce qu'on dit souvent, la meilleure défense, c'est la défense."

ExaTrack

Constat de l’existant

"Ce qui nous préoccupe le plus, ce sont ces attaques sur lesquels on n'a pas les motifs. Ce sont des attaquants de haut niveau, qui prennent pied sur des réseaux sensibles, voire très sensibles, liés à des secteurs d'importance vitale. Ils cartographient ces réseaux, cherchent à comprendre comment ça marche, développent leurs outils. Mais objectivement, je ne sais pas vous dire ce qu'ils préparent."

ExaTrack

Quand faire une recherche de compromission ?

Valider que votre société et ses filiales ne sont pas espionnées informatiquement

ExaTrack

Quand faire une recherche de compromission ?

Lors du rachat d'une société :

- Vérifier que vous ne faites pas entrer un attaquant en même temps que la société
- Des attaques ciblées sont menées sur les filiales entre autres lors d'une annonce de rachat

ExaTrack

Quand faire une recherche de compromission ?

- Pour un rapport d’étonnement

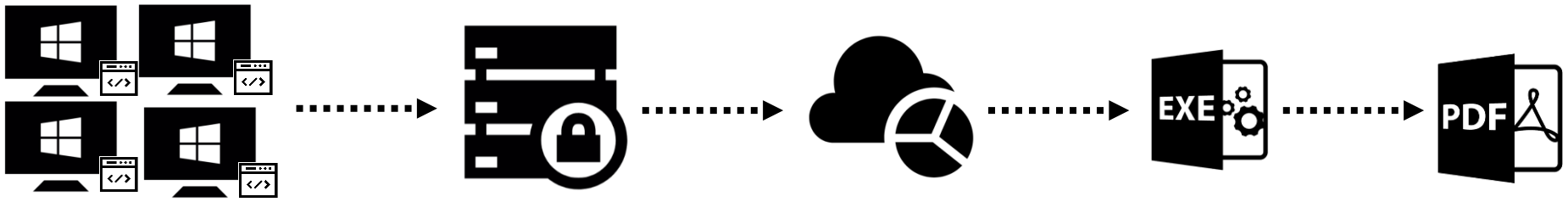
Dès la prise de fonction de RSSI, il est important de vérifier que le SI n'est pas déjà compromis.

Ce rapport peut servir de base aussi bien pour une réponse à incident, en cas de compromission, que pour un durcissement des machines.

ExaTrack

Recherche de compromission

- Identification des machines à analyser
- Collecte des informations sur ces machines
- Analyse des données collectées
- Demande de levée de doutes et rapport final



ExaTrack

Agent de collecte

Type de données collectées :

- Système de fichier
  - Nom des fichiers
  - Hashs
  - Taille
  - Timestamps
  - Signatures

ExaTrack

Agent de collecte

Type de données collectées :

- Registre
  - Nom de clés et valeurs
  - Timestamps
- Fichiers spécifiques
  - Prefetch
  - Lnk
  - Minidumps
  - Etc.

ExaTrack

Agent de collecte

Type de données collectées :

- Processus
  - Modules chargés
  - Espace mémoire
  - Identification de données réécrites
  - Dump de pages mémoires

    Trick : Switch 32/64b
- WMI

ExaTrack

Analyse des données

Plusieurs objectifs :

- Identifier une activité fortement suspecte

  Exemple : un svchost.exe exécuté depuis %temp%

- Corréler et contextualiser les données
- Identifier des altérations mémoires
- Identifier des signaux faibles
- Valider la chaîne de boot

ExaTrack

Analyse des données

DEMO

ExaTrack

Analyse des données

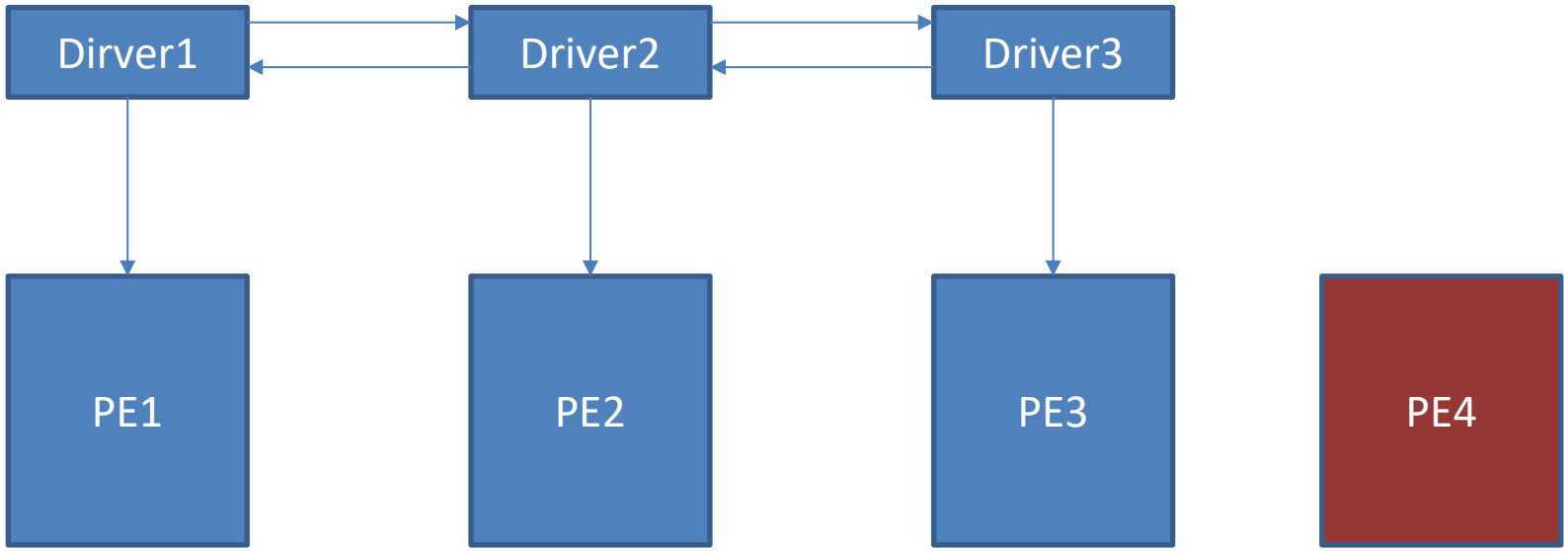
Analyse de dumps mémoires :

- Valider l'intégrité du noyau
  - Drivers chargés
  - Callbacks
  - Device Stack
  - Pug aNd Play
  - Système I/O de la pile réseau
  - Système de filtres (exemple : procmon)
  - Intégrité des drivers
  - Etc.

ExaTrack

Analyse des données

Drivers chargés

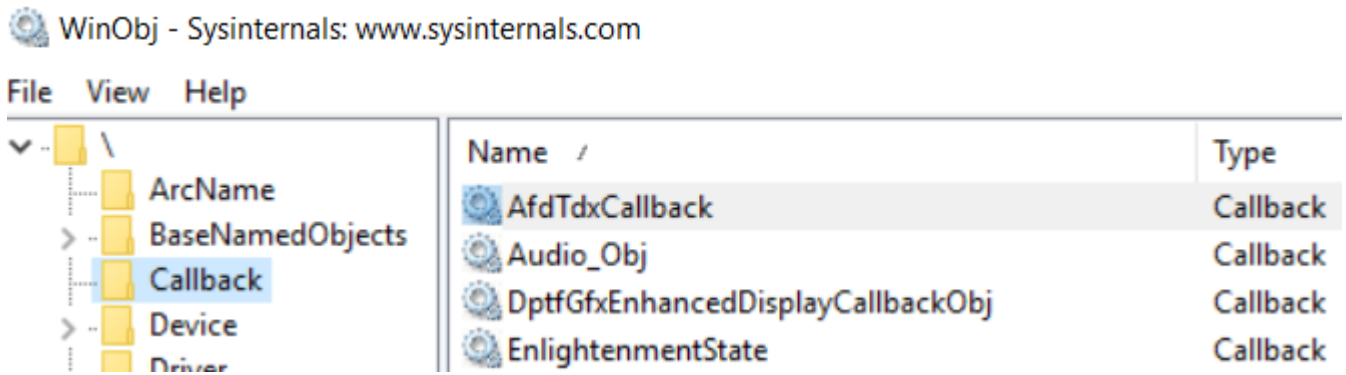


ExaTrack

Analyse des données

Callbacks

- Certaines référencées par l'object manager
- D'autres référencées uniquement par les API (pas dans les symbols)



ExaTrack

Analyse des données

Device Stack

- Chaque « Device » dans WinObj peut avoir d’autres drivers attachés
- Chaque driver de cette pile peut choisir de relayer ou non les packets IRP envoyés

ExaTrack

Analyse des données

PnP

- Arborescence permettant de transmettre les entrées sorties (IO)

Système I/O de la pile réseau

- Majoritairement divisées en deux drivers (avec peu ou pas de symbols) :
  - Ndis (bas niveau)
  - Netio (connexions réseaux)

ExaTrack

Analyse des données

Système de Filtres

- Système utilisé par ProcMon
- Permet d'intercepter les principales communications

Intégrité des drivers

- Vérifier que les drivers critiques ne sont pas réécrits en mémoire

ExaTrack

Analyse des données

DEMO

ExaTrack

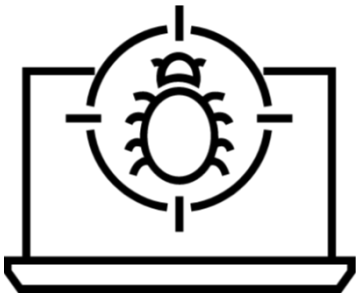
Nos innovations

Tous nos outils sont entièrement développés en interne. Chacun d'eux possède des innovations significatives permettant d'identifier des anomalies complexes.

Nous effectuons une analyse manuelle et en profondeur des données. Ceci permet de contextualiser les anomalies et approfondir les signaux faibles.

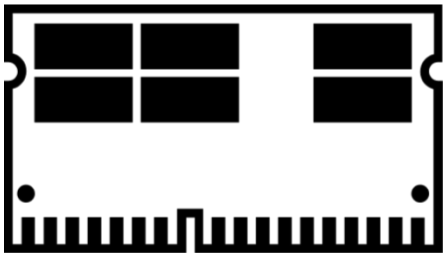
ExaTrack

Nos innovations



Nos outils sont suffisamment performants pour avoir détecté tous les codes malveillants testés, et ce sans avoir recours aux signatures ou IOCs.

Notre outil d'analyse de dump de RAM identifie dynamiquement les structures internes du système pour y dévoiler des rootkits.



ExaTrack

Formations

Windows Internals

Windows Forensics

Malwares Analyze

- Débutant
- Avancé

ExaTrack

Conclusion

La recherche de compromission doit devenir une étape de sécurité normale dans le SI (tout comme effectuer un pentest).

Elle permet également d'estimer la maturité du parc, voir identifier des pratiques non conformes à la PSSI. Dans ce cas elle peut fortement aider à durcir le SI.

Globalement dés que l'on doit gérer un nouveau SI il faut vérifier s'il n'est pas compromis.

ExaTrack

Merci pour votre attention