19 janvier 2015

CERTitude

The Seeker of IOC

Jean MARSAULT
@iansus

Vincent NGUYEN
@nguvin

CERT-solucom

Qui sommes-nous ?

- **Solucom**, 2ème cabinet* de conseil indépendant en France
  - Des clients dans le **top 200** des grandes entreprises et administrations, dans tous les secteurs
  - 1400 collaborateurs dont **250 spécialisés dans la gestion des risques et la cybersécurité**

- Une structure d'expertise : **le CERT-Solucom**
  - **10 analystes**
  - Création en **2013**

Réaction sur attaque ou suspicion	**Lettre CERT-Solucom**	**Exercices de crise**	**Projets internes**

Projets actuels

MISP

MI6

CERTitude

+ outillage audit
(PyKEK, modules Metasploit…)

***Source : PAC 2014**

Conduire une campagne de recherche d'IOC : un besoin en forte augmentation

- La **stratégie de diffusion des IOC** de la part de l'ANSSI introduit une phase cruciale : la **campagne de recherche**
  - Il s'agit de rechercher la présence de marqueurs / IOC sur son système d'information

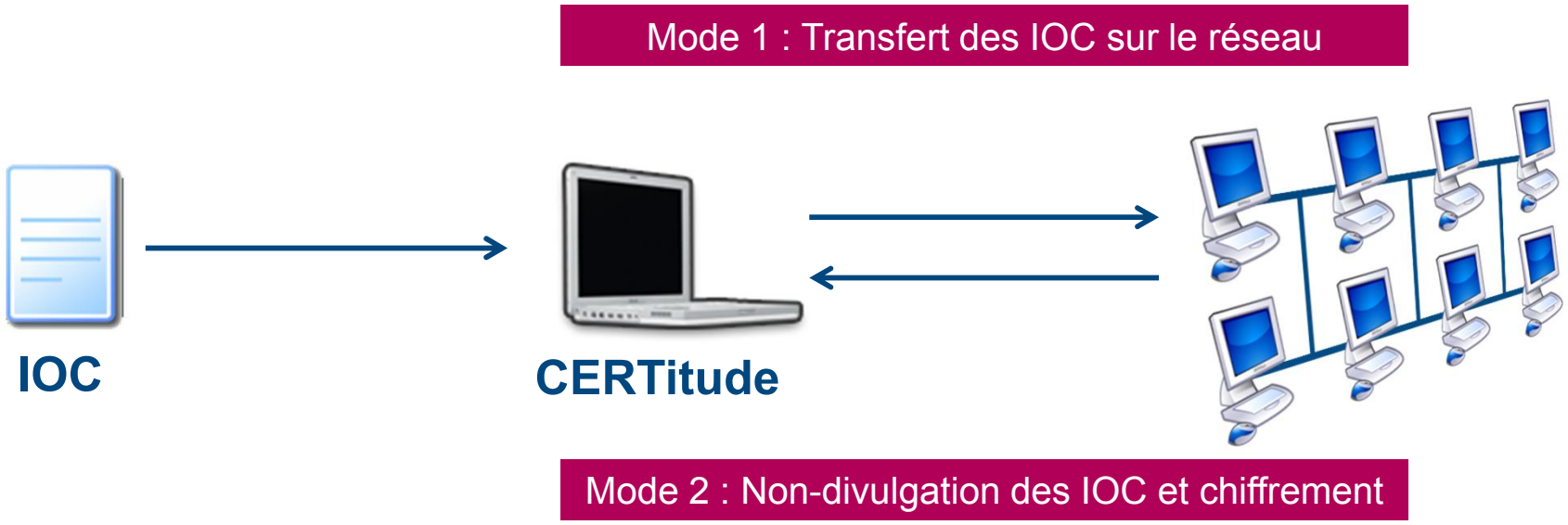
- Lors de nos missions, le CERT-Solucom se retrouve fréquemment confronté au besoin d'**évaluer l'étendue de la compromission** du système d'information

- La plupart des solutions existantes
  - Fonctionnent avec **agent**
  - Transfèrent les IOC recherchés sur le SI : **divulgation à l'attaquant** de la méthode de recherche et identification

CERTitude
The Seeker of IOC

CERTitude : simplifier les campagnes de recherche

- Développement de l'outil **CERTitude** répondant à **deux besoins**
  - Campagne de recherche d'IOC
  - Évaluation du périmètre compromis



Un outil de « scan » sans agent
avec possibilité de non-divulgation des IOC

Extrait du « cahier des charges » de CERTitude

- **Compatibilité** avec un maximum de systèmes d'exploitation Windows
  - Windows XP / Server 2003
  - Windows Vista / 7 / Server 2008
  - Windows 8 / Server 2012
- Impacts faibles sur les **performances systèmes** (transparence utilisateur)
- **Presque aucune trace** laissée sur le poste analysé (i.e. aucun service, processus, fichier après la collecte)
- **Mise à l'échelle** des SI d'entreprise (collecte et analyse)
- **Modularité** du programme pour faire face aux nouvelles familles d'IOC
- Ergonomie…

```
root @ debian-virt ~/CERTitude # _
```

- **Non-divulgation** des IOC recherchés (sur le **réseau** et sur les **postes**), en particulier en cas de périmètre sensible (« Diffusion restreinte » ou plus)
- **Chiffrement** des communications réseaux

Mode 2

Aspects techniques du fonctionnement

Mode 1

Fichiers OpenIOC

CERTitude

SI d'entreprise

Parsing des fichier OpenIOC

Connexion et enregistrement distants

Envoi des scripts de collecte

Collecte des données

Insertion des résultats dans la BDD locale

Création des requêtes pour l'IOC en cours

Requêtes sur la BDD

Analyse des résultats, par poste, par IOC

Récupération des résultats des requêtes

Fin de l'analyse & Résultats

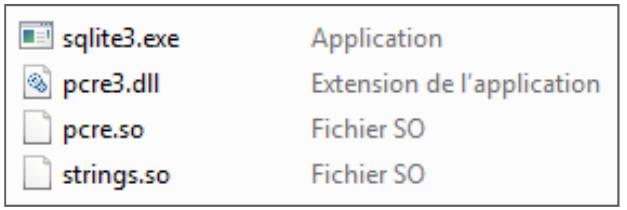
Nettoyage des données

Déroulement de l'analyse en environnement sensible : compatibilité avec les exigences de « Diffusion restreinte »

Mode 2

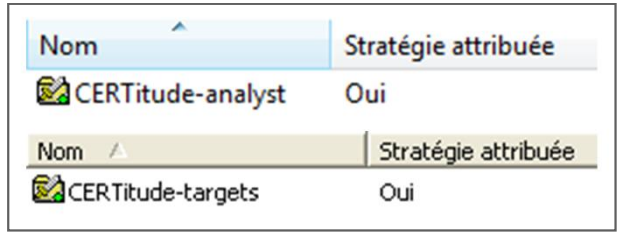
Ne pas diffuser les IOC sur les postes analysés

- La **collecte** des données est toujours effectuée sur le **poste distant**
- Les bases de données créées sont **rapatriées** et les **requêtes** effectuées sur le **poste de l'analyste**



Ne pas faire transiter les données en clair sur le réseau

- Le protocole de **chiffrement** des communications **IPSec** est utilisé en **sous-couche** aux échanges **SMB**
- Des **stratégies de sécurité** IP compatibles sont déployées sur les **postes cibles** et sur le **poste de l'analyste**



Quelques indicateurs pouvant être recherchés par CERTitude

- **Registre**
  - Chemin de la clé
  - Nom de la valeur
- **Fichiers**
  - Chemin du fichier
  - Nom du fichier
  - Extension du fichier
- **Processus en cours**
  - PID et PPID
  - SID et nom d'utilisateur du créateur
  - Nom du processus
  - Chemin de l'exécutable
  - Liste des modules chargés
- **Services**
  - Nom
  - Nom affiché
  - Chemin de l'exécutable
  - Hash MD5 de l'exécutable
  - Statut (*i.e* en cours/ arrête)
  - Mode (*i.e* auto / sur demande / retardé…)
- **Données du Prefetch**
  - Hash du prefetch
  - Nom de l'application
  - Chemin de l'application
  - Taille de l'application (réelle et annoncée)
  - Nombre d'exécutions
- **Connexions réseau**
  - Adresse et port locaux
  - Adresse et port distants
  - Protocole
  - État de la connexion
  - PID du processus à l'origine de la connexion
- **Autres informations réseau**
  - **DnsEntryItem** (Cache DNS)
  - **ArpEntryItem** (Cache ARP)

Focus sur les Prefetch

Pourquoi ?

- Le Prefetch a été initialement mis en place pour accélérer le lancement des exécutables Windows
- Dès qu'un exécutable est lancé, un fichier *.pf* est créé dans le dossier *C:\Windows\Prefetch* contenant des **informations diverses**, notamment sur le chemin d'accès à l'application et les **dates d'exécution**

```
11 00 00 00 28 5D 00 00  .   ...SCCA....(]..
52 00 55 00 4E 00 53 00  A.U.T.O.R.U.N.S.
00 00 00 00 00 00 00 00  ..E.X.E.........
00 00 00 00 00 00 00 00  ....€úÿÿ........
9E 91 4A 03 A8 52 3F B4  .........'J.¨R?´
2C 00 00 00 70 06 00 00  ....ð...,...p...
AA 12 00 00 80 57 00 00  3...ÔD..ª...€W..
```

Comment ?

- Le format utilisé par les fichiers *.pf* est partiellement documenté
- Un **parseur spécifique** a donc été développé pour analyser les fichiers collectés

The file header is 84 bytes of size and consists of:

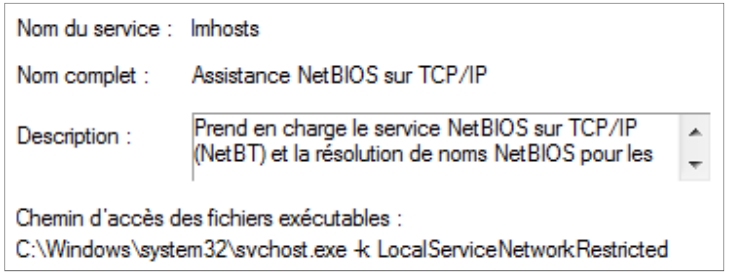
Field	Offset	Length	Type	
H1	0x0000	4	DWORD	Format version (see format version sectio
H2	0x0004	4	DWORD	Signature 'SCCA' (or in hexadecimal repre
H3	0x0008	4	DWORD?	Unknown - Values observed: 0x0F - Windo
H4	0x000C	4	DWORD	Prefetch file size (or length) (sometimes re
H5	0x0010	60	USTR	The name of the (original) executable as a correspond with the one in the prefetch fil

source : http://www.forensicswiki.org

Focus sur les services Windows

Pourquoi ?

- Les services Windows sont un moyen privilégié par les développeurs de malwares puisqu'ils offrent une **présence persistante** sur le système et des **droits** utilisateurs **élevés** à leur démarrage (droits *SYSTEM*)
- De plus, les services peuvent **ne pas apparaître** dans la liste des processus en exécution (via *svchost*)

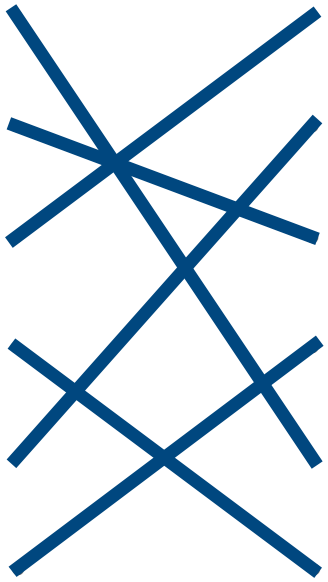


Comment ?

- L'exécutable Windows *sc.exe* permet d'obtenir la **liste des services** (en cours d'exécution ou non).
- Les options *query* et *qc* permettent respectivement d'obtenir **l'état et la configuration avancée** des services.

Problématiques rencontrées lors du développement

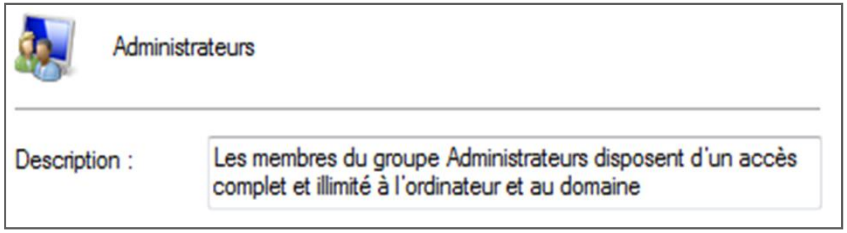
PROBLEMES	SOLUTIONS
Connexion et enregistrement distants	Utilisation de Python
Envoi des données (scripts & requêtes)	~~WMIC~~ Scripts BAT, SH et EXE maisons
Modularité	Protocole SMB
Stockage des résultats de collecte	Nombre limité d'analyses en parallèle
Récupération des données Windows	Portage de PsExec en Python
Surcharge du poste CERTitude / réseau	Base de données SQLite



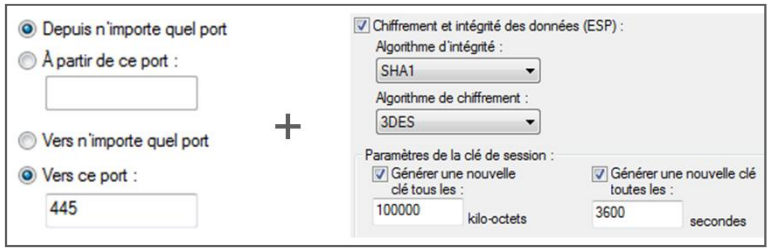
Faites le lien !

Prérequis d'exécution déployables par GPO

Analyste

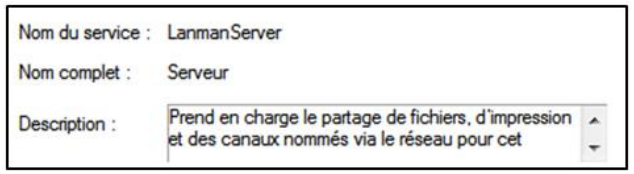


Compte local / de domaine ajouté au groupe « **Administrateurs locaux** » des postes cibles

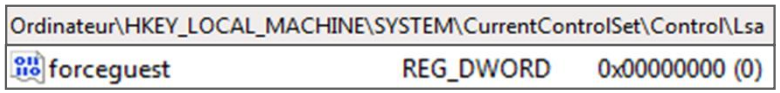


Création de la stratégie de sécurité **IPSec** permettant le **chiffrement des communications**

Postes cibles

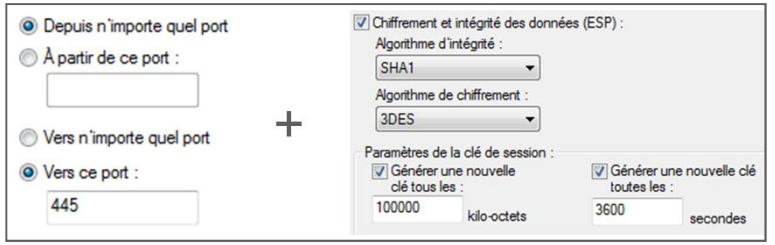


Activation du **partage de fichiers** et des **partages d'administration** par défaut



Désactiver **l'authentification par défaut** comme « **Invité** » pour le compte local

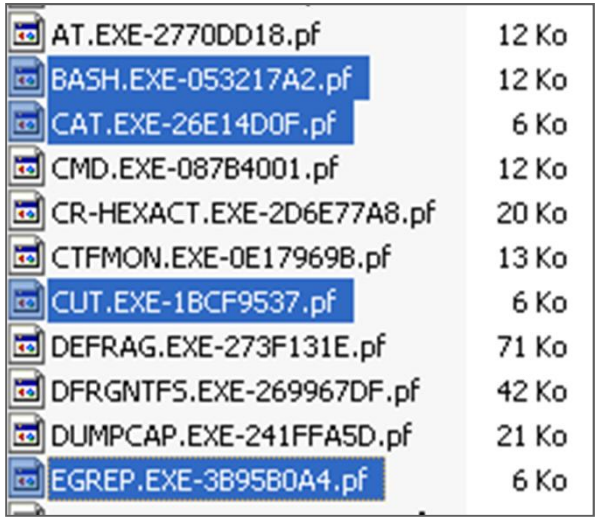
Ouverture des ports TCP **139** et **445**



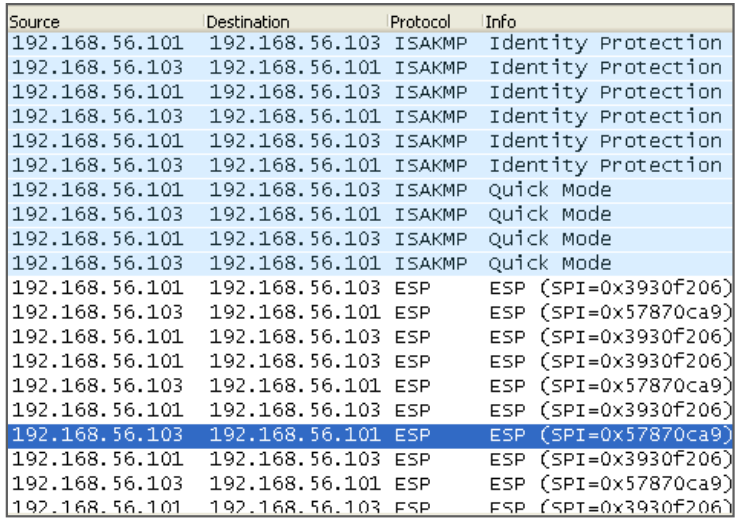
Importation de la stratégie de sécurité **IPSec** permettant le **chiffrement des communications**

Empreinte résiduelle sur le système

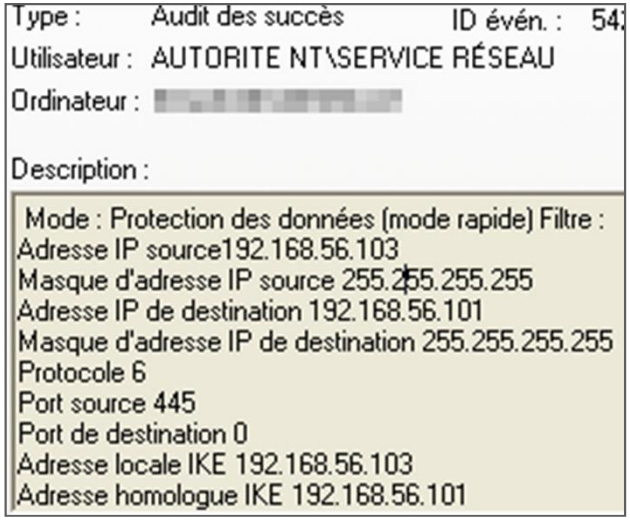
- Le **comportement par défaut** de CERTitude entraîne la **suppression des données** déposées sur le poste (fichiers, service, etc.)
- Cependant, certaines **données système et réseau** persistent malgré cette phase de suppression



Données du Prefetch

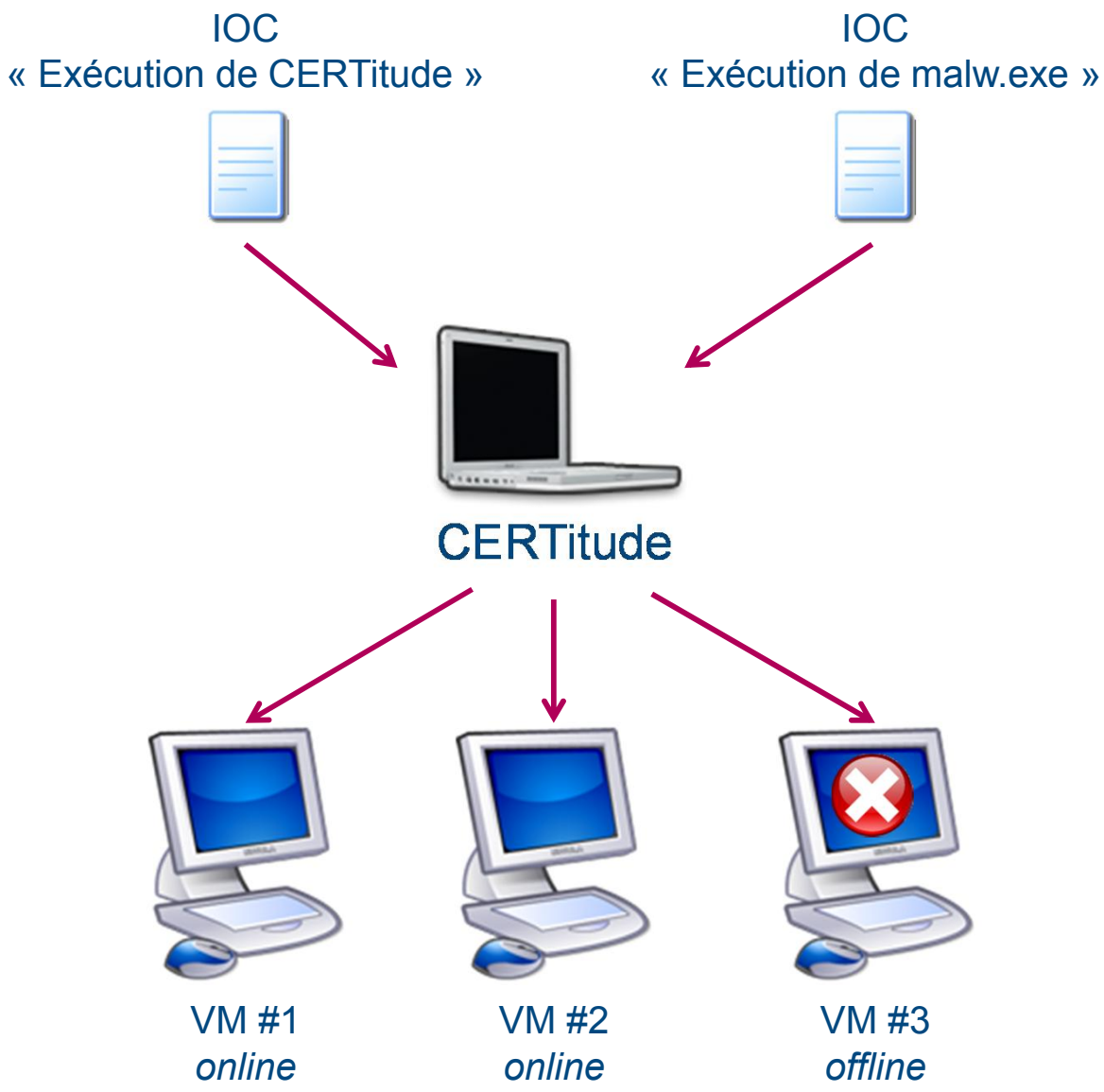


Traces réseau
Journaux d'équipements réseau



Journaux du système

Scénario de la démonstration



Etapes

- Les VM sont **saines** avant la première analyse
- La première analyse donne des **résultats négatifs** pour chaque IOC
- Le fichier « **malw.exe** » est exécuté sur la **VM #2**
- La seconde analyse fournit les résultats
  - **Positifs** pour l'exécution de **CERTitude** sur **toutes les VMs**
  - **Positif** sur la **VM #2** pour l'exécution du fichier « **malw.exe** »

Malw.exe

- Choix d'un nom aléatoire tel que **A9z3-2k09**
- Copie dans **%APPDATA%**
- Clé registre dans **CurrentVersion\Run**
- Enregistrement comme **service Windows**
- Contact de **?.exploit-db.com**

Détail des IOC recherchés

- IOC « Exécution de **CERTitude** »

```
OR
    Prefetch File Executed is RCS.EXE
```

- IOC « Exécution de **malw.exe** »

```
OR
    AND
        AND
            File Name regex ^[a-zA-Z0-9]{4}-[a-zA-Z0-9]{4}\.exe$
            OR
                File Path regex \\Users\\[^\\]+\\AppData\\Roaming
                File Path regex \\Documents and Settings\\[^\\]+\\Application Data
        AND
            Registry Key Path contains HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
            Registry Value Name regex ^[a-zA-Z0-9]{4}-[a-zA-Z0-9]{4}$
        AND
            Service Path MD5 is 214eb6e8b79237f2f0ad6bf12550e649
            Service Name regex ^[a-zA-Z0-9]{4}-[a-zA-Z0-9]{4}$
            OR
                Service mode is 2
                Service Status is 4
        AND
            DNS Record Name contains exploit-db.com
            DNS Record Data Host contains exploit-db.com
        AND
            Process Name regex ^[a-zA-Z0-9]{4}-[a-zA-Z0-9]{4}\.exe$
            OR
                Process Path contains Appplication Data
                Process Path contains AppData
```

Démo de CERTitude

Roadmap

CERTitude v0.8 — 01/2015 – 02/2015

CERTitude v0.9 — 04/2015

CERTitude v1.0 — 06/2015 – 07/2015

CERTitude v0.8

- **Ergonomie**
  - → **Planification avancée** de la campagne de recherche
  - → **Adaptation** au nombre de résultats
  - → Graphe des postes compromis

CERTitude v0.9

- Récupération des **empreintes de fichiers**
  - → MD5 / SHA-1 / SHA-256
  - → Interfaçage avec **agent**
- **Historisation des collectes** et des analyses + nouvelle campagne dans des anciennes collectes

CERTitude v1.0

- **Compatibilité** avec OS plus anciens
  - → Windows NT4 / 98 / 2000
  - → Windows Millenium 
- Gestion avancée des **erreurs**

Ajout de nouveaux modules de recherche

Développement de nouveaux modules en continu : artefacts en mémoire, chaînes de caractères dans les binaires…

By the way, CERTitude est Open Source… et disponible sur GitHub

https://github.com/CERT-Solucom/certitude

cert@solucom.fr

Questions / Propositions ?

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

Contacts

Vincent NGUYEN
CERT-Solucom
KeyID PGP : 0x2C1B028C
Tel : +33 (0)1 49 03 24 90
Mobile : +33 (0)7 62 83 13 61
Mail : vincent.nguyen@solucom.fr

Jean MARSAULT
CERT-Solucom
Tel : +33 (0)1 49 03 86 22
Mail : jean.marsault@solucom.fr