CoRIIN 2022 - Conférence sur la réponse aux incidents et l'investigation numérique 2022

Report of Contributions

Contribution ID: **1** Type: **Présentation courte**

Retour d'expérience sur un Zepplin

Tuesday, June 7, 2022 11:00 AM (25 minutes)

Primary author: CERT, Advens

Co-author: QUESADA, David

Presenter: QUESADA, David

Track Classification: Réponse aux incidents (outre les aspects forensiques évoqués ci-dessus appliqués à la réponse aux incidents):: De la mitigation à la restauration d'un état normal de fonctionnement

Contribution ID: **2** Type: **Présentation courte**

DFIR4vSphere: Investigation numérique sur la solution de virtualisation VMWare vSphere

Tuesday, June 7, 2022 11:30 AM (25 minutes)

VMWare vSphere est une solution de virtualisation composée d'hyperviseurs de type 1 (ESXi) et d'une console de gestion centralisée (VCenter). Selon VMWare, en entreprise près de 80% des environnements virtualisées reposent sur cette technologie. En conséquence c'est une cible de choix pour un attaquant. Dans cette présentation nous allons montrer comment utiliser le module PowerShell DFIR4vSphere pour collecter des journaux et artéfacts forensique aussi bien sur les hôtes ESXi que sur la console VCenter.

Primary author: SAVINA, Léonard (ANSSI)

Presenter: SAVINA, Léonard (ANSSI)

Track Classification: Investigation numérique: Techniques et outils d'analyse de supports numériques (forensic)

Contribution ID: **3** Type: **Présentation courte**

TAPIR : Un parseur d'artefacts pour la réponse aux incidents

Tuesday, June 7, 2022 12:00 PM (25 minutes)

Cette présentation est axée sur deux nouveaux outils de réponse aux incidents : TAPIr et bin2json. Ces deux outils sont basés sur une bibliothèque écrite en rust : TAP (Trustable Artifact Parser), qui fournit différents plugins pour l'analyse d'artefacts (NTFS, MTF, regitry, evtx, prefetch, …), et inclue aussi un moteur de recherche avancé pour filtrer les données générées.
Lors de la présentation nous passerons en revue l'architecture de la bibliothèque TAP, nous verrons quand et comment utiliser TAPIR et bin2json, et enfin nous ferons une démonstration de ces différents outils.

Primary author: JACOB, Solal

Presenter: JACOB, Solal

Track Classification: Investigation numérique: Analyse d'artefacts d'applications, d'activités réseau,…

Contribution ID: **4** Type: **Présentation courte**

RETEX Carrefour SOC

Tuesday, June 7, 2022 12:30 PM (25 minutes)

Bonjour,

Le SOC / CSIRT Carrefour vous propose de presenter un retour d'expérience sur un incident majeur intervenu sur son périmètre en Septembre 2021.

Primary authors: COURTEL, Quentin (Carrefour); GUIGNARD, Thierry (Carrefour)

Presenters: COURTEL, Quentin (Carrefour); GUIGNARD, Thierry (Carrefour)

Track Classification: Réponse aux incidents (outre les aspects forensiques évoqués ci-dessus appliqués à la réponse aux incidents):: De la mitigation à la restauration d'un état normal de fonctionnement

Contribution ID: **5** Type: **Présentation courte**

IOCmite - Quand Suricata rencontre MISP

Tuesday, June 7, 2022 2:00 PM (25 minutes)

Cette conférence a pour but de présenter différents cas d'usage de l'outil opensource IOCmite.

IOCmite permet de créer des datasets d'indicateur de compromission pour permettre la détection en utilisant Suricata, sonde de détection d'intrusion opensource

https://github.com/sebdraven/IOCmite

Primary authors: LEBLOND, Eric (Stamus Network); LARINIER, Sebastien (ESIEA)

Presenters: LEBLOND, Eric (Stamus Network); LARINIER, Sebastien (ESIEA)

Track Classification: Investigation numérique: Analyse d'artefacts d'applications, d'activités réseau,…

Contribution ID: **6** Type: **not specified**

TinyCheck, détection d'implants passive sur smartphones via l'analyse de flux réseau.

Tuesday, June 7, 2022 2:30 PM (25 minutes)

Comment permettre à quiconque de savoir si son smartphone est compromis ? C'est le but de l'outil « TinyCheck ». Développé en premier lieu pour lutter contre le fléau des Stalkerwares, ce projet permet aussi de détecter dans certains cas la présence d'implants plus sophistiqués mis en œuvre par des acteurs malveillants.

Primary author: AIME, Felix

Presenter: AIME, Felix

Contribution ID: **7** Type: **Présentation courte**

Aspects juridiques de la biométrie dans les investigations numériques : Lorsque le corps devient la clef

Tuesday, June 7, 2022 3:00 PM (25 minutes)

Cette contribution visera à analyser la problématique du recours à la biométrie pour déverrouiller des appareils mobiles, supports de données et dossiers de fichiers dans le cadre d'investigations pénales. Elle se consacrera principalement à des problématiques de de procédure pénale et, en particulier, au conflit existant entre de telles méthodes d'enquête et le principe *nemo tenetur se ipsum accusare* selon lequel nul n'est tenu de s'auto-incriminer. L'on analysera ainsi si les données biométriques rattachées à un individu sont couverte par l'interdiction de ne pas s'auto-incriminer. Voir la table des matières provisoires dans le fichier joint.

Primary authors: ZBINDEN, Renaud; Dr TIRELLI, Ludovic (ILCE)

Presenters: ZBINDEN, Renaud; Dr TIRELLI, Ludovic (ILCE)

Track Classification: Aspects juridiques: Aspects juridiques

Contribution ID: **8** Type: **Présentation courte**

L'utilisation du scambaiting à des fins préventives contre les cyberarnaques : le cas des arnaques aux sentiments

Tuesday, June 7, 2022 3:30 PM (25 minutes)

Le projet porte sur l'intérêt du scambaiting à des fins préventives pour lutter contre les cyber-arnaques. Le scambaiting est une technique consistant à appâter des cyberescrocs en se faisant passer pour une victime.

Primary authors: DÉCARY-HÊTU, David (Université de Montréal); BEAUDET-LABRECQUE, Olivier (Institut de lutte contre la criminalité économique); ZBINDEN, Renaud (Institut de lutte contre la criminalité économique)

Presenters: BEAUDET-LABRECQUE, Olivier (Institut de lutte contre la criminalité économique); ZBINDEN, Renaud (Institut de lutte contre la criminalité économique)

Track Classification: Investigation numérique: Investigation sur Internet, sur les réseaux

Contribution ID: **10** Type: **Présentation courte**

La montée en puissance des Initial Access Brokers (IABs) - quels constats faut-il en tirer ?

Tuesday, June 7, 2022 4:30 PM (25 minutes)

Cette présentation reprend les résultats d'une analyse des accès à des systèmes compromis mis en vente sur les espaces d'échanges cybercriminels entre juillet et décembre 2021.

Primary author: TIBIRNA, Livia

Presenter: TIBIRNA, Livia

Track Classification: Investigation numérique: Investigation sur Internet, sur les réseaux

Contribution ID: **11** Type: **Présentation courte**

La mutation de l'hébergement "bulletproof"

Tuesday, June 7, 2022 5:00 PM (25 minutes)

Les hébergeurs bulletproofs sont au coeur de la criminalité sur Internet. Bien que ce terme soit souvent utilisé à outrance en désignant des acteurs du cloud ne répondant pas suffisamment vite aux sollicitations, ce terme désigne véritablement des hébergeurs fournissant un service "premium" à ses clients afin de ne pas subir de coupure de service à la suite d'une plainte, de la résilience en cas d'interruption du service ainsi qu'une non-cooperation avec les forces de l'ordre en cas de sollicitation.
Ces 5 dernières années, une tendance en matière de service bulletproofs semble se dessiner. L'exploitation directe d'un datacentre, et toutes les contraintes associées, laisse la place à des réseaux de revendeurs de services basés sur l'infrastructure de fournisseurs de cloud tout à fait légitimes. L'objectif de cette présentation est de dresser le tableau de ce nouveau modèle en apportant quelques éléments pour reconnaître ces revendeurs de services bulletproofs.

Presenter: MERIOT, Sébastien

Track Classification: Investigation numérique: Investigation sur Internet, sur les réseaux

Contribution ID: **12** Type: **Présentation longue**

Investigations sur un système de fichiers atypiques ou comment voyager dans le temps avec un groupe APT

Tuesday, June 7, 2022 5:30 PM (25 minutes)

Presenter: MINISTÈRE DE L'INTÉRIEUR (Ministère de l'intérieur)

Track Classification: Investigation numérique: Collecte et analyse de mémoire vive