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

mardi 7 juin 2022 - mardi 7 juin 2022

Lille

Recueil des résumés

Contents

1

Retour d'expérience sur un Zepplin

Auteur: Advens CERT[None]

Co-auteur: David Quesada

Auteur correspondant david.quesada@advens.fr

2

DFIR4vSphere: Investigation numérique sur la solution de virtualisation VMWare vSphere

Auteur: Léonard Savina[1]

[1] *ANSSI*

Auteur correspondant leonard.savina@ssi.gouv.fr

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.

3

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

Auteur: Solal Jacob[None]

Auteur correspondant soljacob@cisco.com

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.

4

RETEX Carrefour SOC

Auteurs: Quentin Courtel[1]; Thierry Guignard[1]

[1] *Carrefour*

Auteurs correspondants: thierry_guignard_1@carrefour.com, quentin_courtel@carrefour.com

Bonjour,

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

5

IOCmite - Quand Suricata rencontre MISP

Auteurs: Eric Leblond[1]; Sebastien Larinier[2]

[1] *Stamus Network*

[2] *ESIEA*

Auteurs correspondants: el@stamus-networks.com, sebastien.larinier@esiea.fr

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

6

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

Auteur: Felix Aime[None]

Auteur correspondant felix.aime@gmail.com

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.

7

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

Auteurs: Renaud Zbinden[None]; Ludovic Tirelli[1]

[1] *ILCE*

Auteur correspondant tirelli@penalex.ch

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.

8

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

Auteurs: David Décary-Hêtu[1]; Olivier Beaudet-Labrecque[2]; Renaud Zbinden[2]

[1] *Université de Montréal*

[2] *Institut de lutte contre la criminalité économique*

Auteurs correspondants: olivier.beaudet-labrecque@he-arc.ch, renaud.zbinden@he-arc.ch

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

10

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

Auteur: Livia Tibirna[None]

Auteur correspondant livia.tibirna@sekoia.fr

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.

11

La mutation de l'hébergement "bulletproof"

Auteur correspondant sebastien.meriot@corp.ovh.com

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.

12

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