SSTIC 2016

SSTIC

- Start

- Durées de vente des billets
  - 150 en 2'58
  - 150 en 1'26
  - 70 en 1'07
  - 1 en 25 minutes
- 165 bizuth(e)s

- 37 soumissions au premier appel
- 21 soumissions courtes au second
- 15 articles longs retenus
- 15 présentations courtes retenues
- 476 pages d'actes

Les conférences

KEYNOTE

- **Conférencier : Brad Spengler**
  - Auteur de grsecurity, « un patch »permettant d'ajouter des fonctionnalités de sécurité au noyau Linux.

- **Conférence**
  - Information sur ls update de GRCESCURITY et PAX
    - DENYUSB
    - KSTACKOVERFLOW
  - State of infosec union

How bad assumptions lead to an industry protecting itself from its own “professionals”

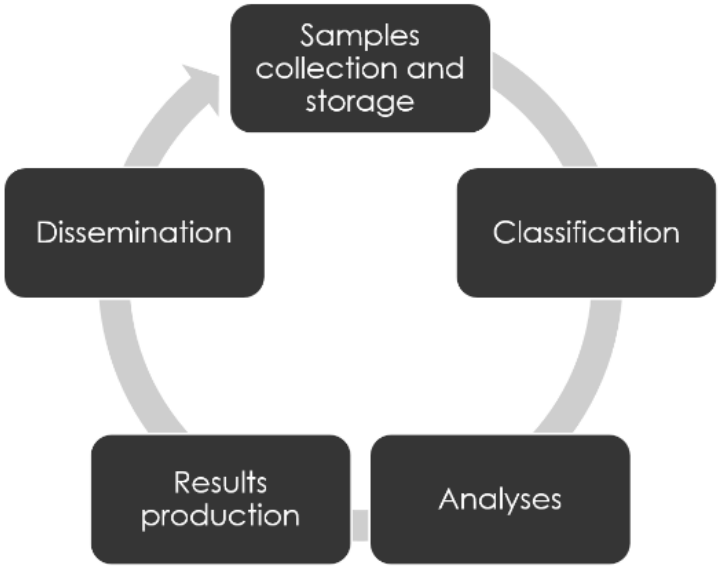
- **Conclusion :**
  - Conférence « austère » au niveau de la forme mais qui en dit long sur le chemin qui conduit au durcissement d’un noyau Linux

- **Quelques sources**
  - https://grsecurity.net/index.php
  - https://grsecurity.net/SSTIC2016.pdf

Démarche d'analyse collaborative de codes malveillants

- **Conférencier : Adrien Chevalier,Stéfan Le Berre,Tristan Pourcelot**

- **Conférence**
  - Un retex sur la mise en place d'un outil collaboratif, permettant à la fois de stocker et d'indexer de l'information sur une analyse de malware et simplifier les futures analyses.
  - nom de code Polimchor : https://github.com/ANSSI-FR/polichombr
  - Un bon complément à VirusTotal pour le stockage de commentaires privés.
  - Utilise comme entrée des samples de codes malicieux (PE, ELF, Shellcode,…)
  - Utilisation possible avec openIOC

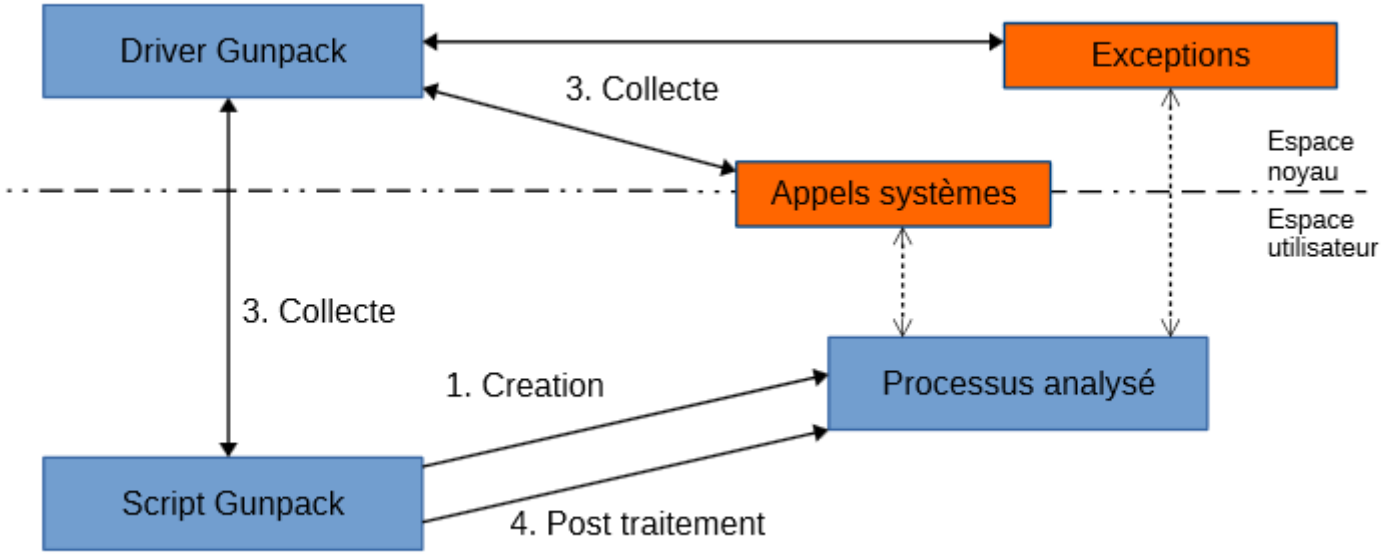


- **Conclusion :**
  - utilisation possible comme input des outils IOC.

Gunpack : un outil générique d'unpacking de malwares

- **Conférencier julien Lenoir**

- **Gunpack**
  - Outil d'unpacking des malware.
  - Le packing est utilisé par les code malicieux pour compresser et /ou chiffrer tout ou partie du code orignal.
  - L'objectif est d'extraite du code « packer » le code viral.

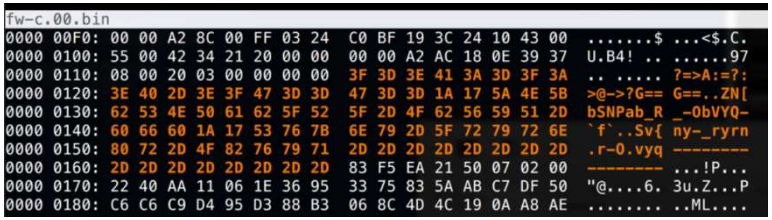


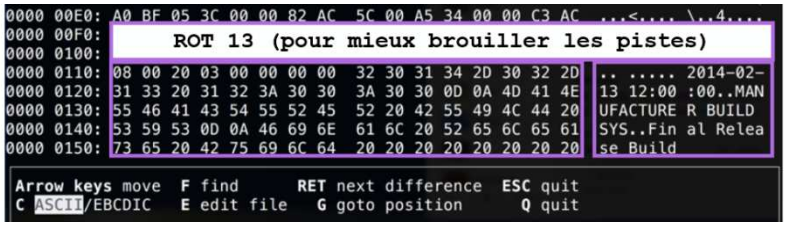
- **Conclusion :**
  - pour réalisation de « forencics viral » voir génération de signature spécifique.

Cryptanalyse en boite noire de chiffrement propriétaire : étude de cas

- **Conférencier Pierre Capillon**
- **La conférence**
  - expose l'état d'esprit d'un attaquant face à un code chiffré
  - évoque les idées suivies et les impasses
  - démontre le faux sentiment de sécurité perçu par les fabricants
  - indique les compétences et les moyens nécessaires pour réaliser ces attaques

- **Exemple**
  - D'un binaire à un code déchiffré





- **Les techniques**

Technique/Idea	Ref.	Comments/Relevance
Finding instruction opcodes	3.1	Unsuccessful attempt at finding executable code
Matching calling conventions	3.1	Unsuccessful attempt at finding code-like patterns in case the encryption kept symbols alike
Bitwise binary differences	3.3	Helped locate bitfields, headers, parameters, etc.
Comparing multiple samples	3.4	Helped identify static data BLOBs, enable statistical analysis, exploit potential similarities
Bruteforce	3.5	Helped recover data without known/identifiable plaintext
Reverse-engineering	3.6	Helped identify and implement the compression algorithm, helped find useful error/corner cases
Binary data fingerprinting	3.7	Unsuccessful attempt at recovering complete files from firmware image

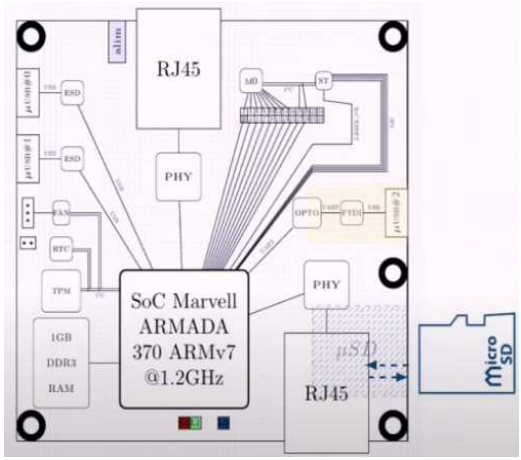
- **Conclusion :**
  - exposé super clair notamment utilisation possible pour des sensibilisations de haut niveau ?????

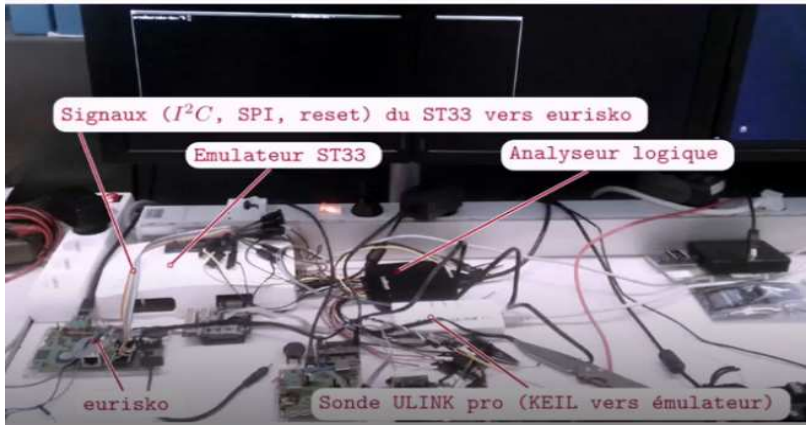
Eurisko : développement d'une carte électronique sécurisée

- **Conférencier**
  - Arnaud Ebalard,Arnaud Fontaine,David Diallo,Jean-Pierre Flori,Karim Khalfallah,Mathieu Renard,Ryad Benadjila

- **Conférence**
  - Un retour d'expérience sur la création d'une carte électronique sécurisée, implémentant des mécanismes garantissant l'intégrité du système qui s'exécute, par une chaine de confiance
  - UIitilisation comme sonde, chiffreur, ……
  - La carte est bâtie autour d'un SOC ARMv7 Armada 370 de chez Marvell. Un microcontrôleur, de la RAM, des I/Os, des ports Ethernet, USB complète la carte.
  - Ajout d'un composant supplémentaire EAL5+ pour « piloter » le chipset.

- **La carte**



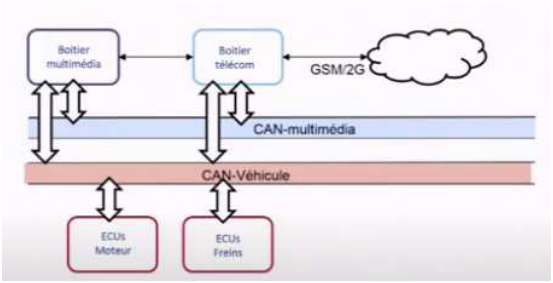


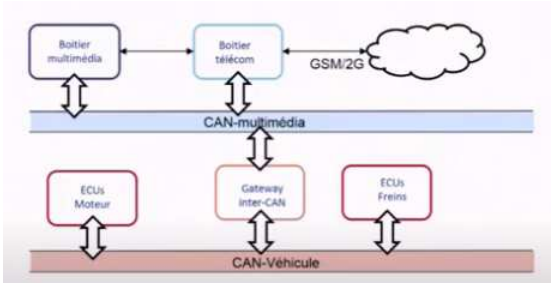
- **Conclusion :**
  - je ne vois pas la plus-value par rapport un RASP => c'est pas sécurisé ☺

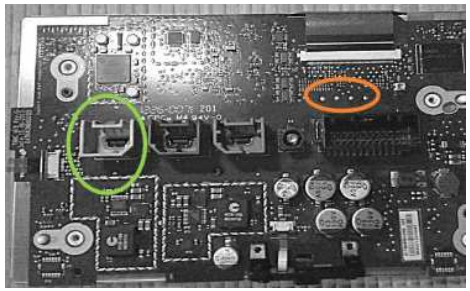
Evolution et dé-évolution des systèmes multimédia embarqués

- **Conférencier François Pollet, Nicolas Massaviol**

- **Conférence**
  - L'étude porte l'analyse des vulnérabilités portées par les BUS CAN embaqués dans les véhicules.
  - Ces bus sont utilisés par le « plan de contrôle », pilotage des freins du moteur mais aussi pour piloter les périphériques multimédia USB WIFI, écran.
  - Deux types d'approche pour gérer ces bus selon les constructeur un bus à plat ou avec une passerelle (ségrégation assurant un meilleur niveau de sécurité)





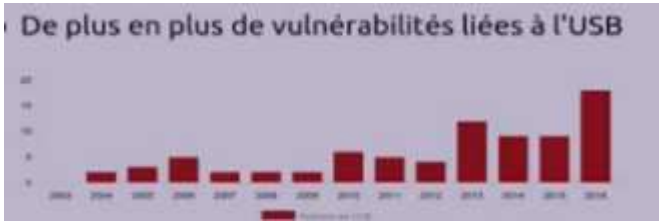


- En conclusion :
  - le conférencier indique que les constructeurs semble prendre conscience du danger, à suivre avec en ligne de mire des homologations ou pas des véhicules ?

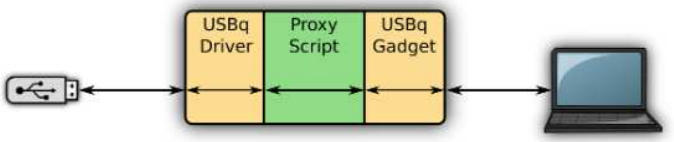
USB Toolkit

- **Conférencier Benoit Camredon**

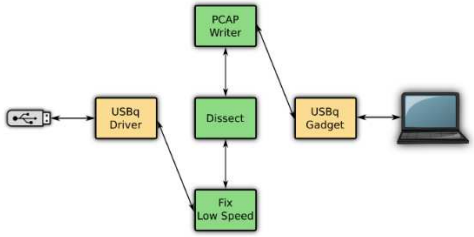
- **Conférence**
  - Visualisation dans un premier temps l'étendu des vulnérabilités qui touchent les périphériques USB

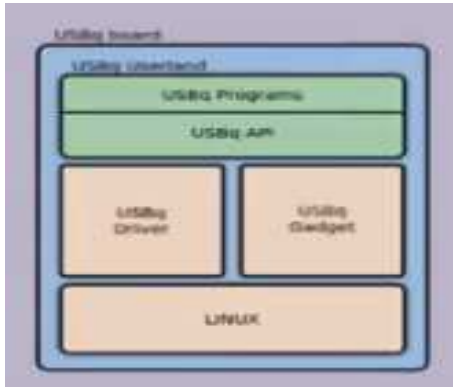


  - Etudes des traces USB sans connaitre l'hôte pour mettre en place un jeu de contre mesure ou d'audit.



  - L'outil développé sur une carte : USBq :
    - disséqueur de paquet USB
    - Firewall USB (autorisation d'un clavier/souris pas d'une clé USB)
    - Analyseur de pcap
    - Fuzzer
    - Fingerprinting hôte





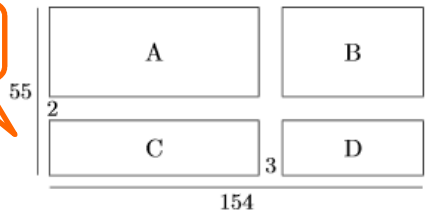
- **En conclusion :**
  - le module Firewall semble pertinent (mode opensource)

Un FizzBuzz pour le cyber

- Conférencier Eric Jaeger,Olivier Levillain (ANSSI)
- Conférence
  - L'ANSSSI présente quelques questions pour recruter ou de sélectionner des candidats.
  - Ce questionnaire est soumis à froid, le candidat ne doit pas utiliser Google, la calculatrice, ….
  - Le questionnaire permet non seulement d'évaluer le niveau des candidats mais aussi de lancer le débat.
  - Quelques questions :

Math

Q Soit un jardin dont la disposition et les dimensions en mètres sont données ci-dessous :



À raison de 17 bulbes par m^2, pour fleurir les parcelles A (de 21 m par 85 m), B, C et D il faut :

- ☐ 134147 bulbes
- ☐ 136051 bulbes
- ☐ 138323 bulbes

Culture

Q L'architecture de Von Neumann c'est...

- ☐ la structuration des données en programmation orientée objet
- ☐ une architecture pour ordinateurs qui ne permet pas de distinguer programmes et données
- ☐ une décomposition des systèmes d'exploitation sous la forme de couches normalisées
- ☐ une alternative à l'architecture Harvard

Q Que pouvez-vous dire du nombre en hexadécimal `0x1616160` ?

- ☐ c'est un nombre pair ;
- ☐ c'est un multiple de 3 ;
- ☐ c'est un multiple de 16 ;
- ☐ c'est un multiple de `0x16` ;
- ☐ c'est un multiple de `0x10101`.

Crypto

Q Un certificat électronique...

- ☐ doit rester secret pour jouer son rôle ;
- ☐ permet l'authentification ;
- ☐ contient la clé utilisée pour déchiffrer les communications ;
- ☐ peut contenir une clé publique ECDSA.

Q Une fonction de chiffrement E prend en entrée une clé et un message clair, et retourne un chiffré. Pour remplir son rôle, E_k doit être...

- ☐ injective
- ☐ surjective
- ☐ déterministe

Shell

Q Quelles commandes *shell* peuvent mener (sans redirection) à la perte de données ?

- ☐ `ls`
- ☐ `rm`
- ☐ `mv`
- ☐ `cat`
- ☐ `cp`

C

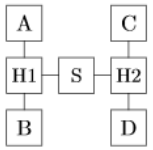
Q Le langage C est un langage...

- ☐ machine
- ☐ de script
- ☐ compilable
- ☐ exécutable par une machine virtuelle

Q On considère un exécutable et son fichier source associé en C qui contient notamment une directive `#define`. Celle-ci est traitée :

- ☐ avant le lancement de l'exécutable
- ☐ au lancement de l'exécutable
- ☐ pendant l'exécution de l'exécutable

Réseau



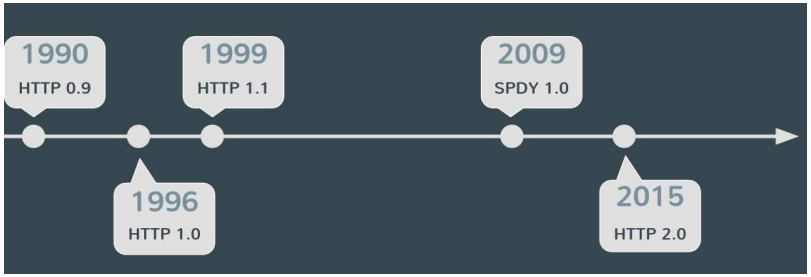
Q Soit le réseau IP ci-dessus, avec A, B, C et D des ordinateurs, $H1$ et $H2$ sont des *hubs* et S est un *switch* correctement configuré

- ☐ Un paquet émis par A à destination de $@_D$ est reçu par D
- ☐ Un paquet émis par C à destination de $@_D$ est reçu par B
- ☐ Un paquet émis par C à destination de $@_B$ est reçu par A
- ☐ A peut émettre un paquet avec $@_B$ en adresse source et $@_D$ en adresse destination, paquet qui sera reçu et traité par D

Comparaisons et attaques sur le protocole hTTP/2

- **Conférencier Georges Bossert**

- **Conférence**
  - Travaux en cours sur le protocole hTTP/2 et comparaison des attaques possible.
  - G Bossert introduit le protocole SPDY (travaux de Google) qui a pour objectifs l'améliorer des temps de latence.
  - Déjà utilisé par Facebook, Google, Twitter, Amazon…



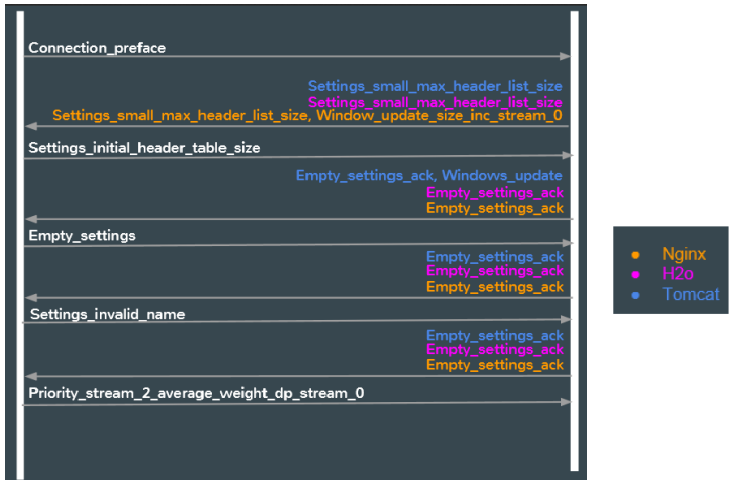
  - Quelques techniques d'attaque :
    - création d'un fuzzer
    - outil de fingerprinting (voir graphe)
    - création de règles pour evader les IDS

La théorie

- Si des serveurs WEB se comportent différement, difficile pour l'IDS de suivre les flux.

En pratique

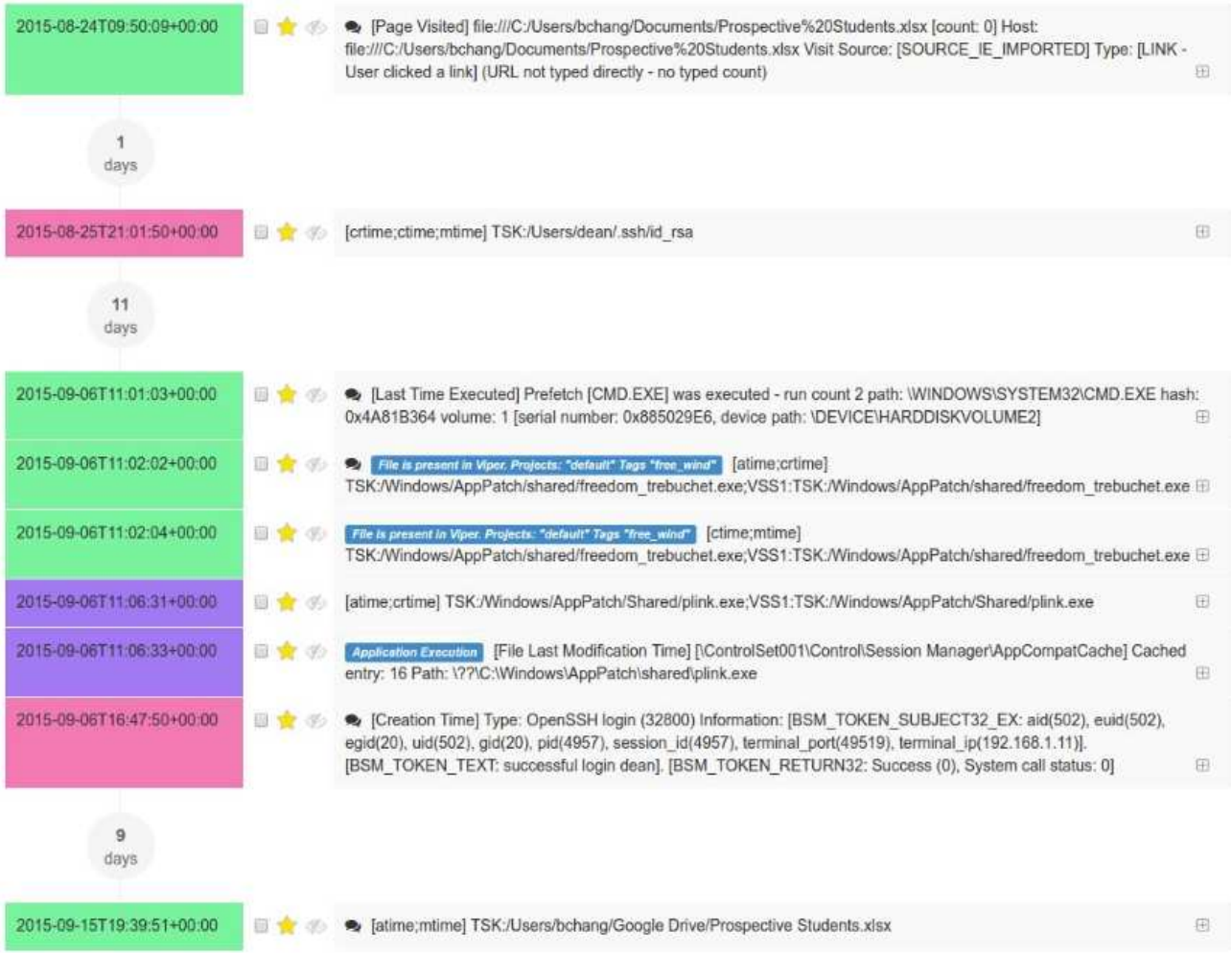
- HTTP/2 pas encore proposé par les principaux IDS
- **MAIS, ça risque d'être compliqué pour les dev. d'IDS !**



- **Conclusion** :
  - http/2 est récent, complexe, avec de nombreuse implémentation et fonctionnalité il reste largement perfectible en matière de sécurité

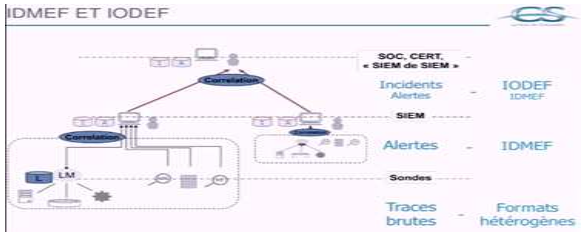
Plaso & Timesketch

- **Conférencier Romain Gayon :** demo https://demo.timesketch.org
- **Conférence**
  - Présentation des outils de forensic Plaso et Timesketch.
  - Plaso outil en Python permet de générer des événements normalisé (log2timeline.py) à partir de d'image RAW, VDI
  - L'outil permet de trier et de filtrer les résultats (psort.py).
  - Il utilisation de préprocesseurs pour déterminer la time zone, l'OS version, le codepage Wondows,……
  - Il s'interface via des pluggins aux outils VirusTotal et Viper (fournit les hash de PE identifié).



Rump

- 3 minutes et 25 Rump au total
- Fuddly : Outil de fuzzing opensource inclus de target reseau
- NFB : Outil de brute force d'une carte de payement RFID (vulnérabilité : crédit stocké en db, UID sur 7 bytes)
- EFI memory &disk dumper : Analyse forensics EFI outil disponible www.tianocore.org/edk2/
- Analyse disque dur :Récupération du code pin d'un disque dur externe USB 3 (AES-260 XTS). Reverse via IDA
- Difficultés de communication sécurisé (Guillaume) Faille remontée et corrigée le 31 mars.
- Appel du python depuis du C Euh pas compris
- ISO live pour analyse de logs avec report basé sur Suricata (IDS), Elasticsearch (Splunk gartuit), Kibana (interface de tableau de bord), Logstash et Scirius disponible en licence GPL
- Réalisation d'une librairie
  - IDEMF basé sur Prélude pour SIEM
  - IODEF basé sur Prélude pour la gestion des incidents
  - Disponible sur gitbub : libidmef et libiodef



- **Vie ma vie** Question ou réponse réelle

« Mais, vous ne voulez quand même pas qu'on suive toutes les CVE qui s'appliquent à notre produit ? »

« A un moment dans un projet, quand le code est mûr, tu as une montée des bugs qui est liée à la maturité du code »

« Vos warnings sont un peu trop inquiétants, ils ont fait peur aux chefs »

Autres

- **Composants logiciels vérifiés en F* : Poly1305**
  - Conférencier Benjamin Beurdouche,Jean Karim Zinzindohoue
  - Exposé
    - Preuve formelle pour vérifier des composants logiciels critiques ou sensibles.
    - Illustration avec une implémentation formellement pour vérifier de TLS.
  - En conclusion :
    - Une application dans la vraie vie semble compliquée

- **Broken Synapse**
  - Conférencier Ivan Kwiatkowski
  - Technique pour lever le brouillard de guerre présent dans je jeux Frozen Synapse.
  - Trois tentatives :
    - analyse via wireshark
    - Décompilation des .cs et .dso via des script python
    - reverse via IDA
  - En conclusion : Mise à part le challenge pas bien vu l'utilité d'une telle conférence.

- **Scapy 2.3.2 : Guillaume Valadon,Pierre Lalet**

- **Windows Error Reporting**
  - Avec Windows XP, Microsoft a fait évoluer Dr. Watson vers un mécanisme plus sophistiqué baptisé WER

- **My friends botnet: How to use your friends to perform Cyber Int ? — Amaury Leroy**

Merci