WAVESTONE

# Bsides LV & DEF CON

## Compte rendu OSSIR

11/09/2018

01

Bsides Las Vegas


- 7 et 8 août 2018
- Tuscany
- 10ème édition
- Gratuit
- 8 tracks de conférence en parallèle

# Serverless infections : Malware just found a new home

- Présenté par Erez YALON
- Serverless, function as a service : intégralité de la plate-forme gérée par le prestataire, seul le code est fourni par le client
- Développer la fonction, la publier, la déclencher puis détruire l'environnement d'exécution
- Extensible et peu cher mais plus lent et dépendant de la plateforme
- Avantages sécurité
  - Fonction lancée dans son propre environnement
  - Environnement détruit en fin d'exécution
- Attaque : contamination du code de la fonction de manière persistante dans un environnement non persistent
  - Utilisation des fonctions AWS-SDK et AWS-CLI pour injecter du code et modifier le code source de la fonction
  - Éléments de configuration par défaut : aucune VPC et container avec un privilège élevé d'exécution, le « lambda execution role »

Other Serverless solutions attacks status

| | AWS Lambda | Google Cloud Function (GCP) | Azure Function (Microsoft) |
|---|---|---|---|
| Access Code via code injection | V | V | V |
| Download Code to hacker server | V (No VPC) | V (Google Firewall block uncommon ports, not IP) | V (Can be blocked by network rules) |
| Modify Function Code | V | No (relevant SDK is not available on runtime) | Yes, but depends on Windows Azure Settings |
| Modify Other Function Code | V (Permissions) | No | Depends on Windows Azure Setting |
| Viral Injection | V | No | No |

# Pacu : Attack and post Exploitation in AWS

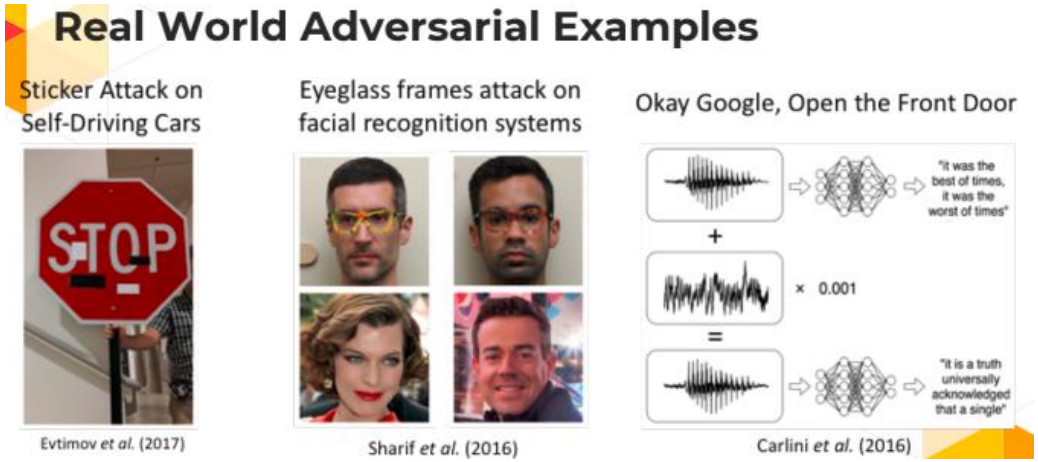
- Présenté par Spencer GIETZEN
- Pacu : outil open source de post exploitation sur AWS
- Constat : facile de faire ses premiers pas sur AWS mais difficile de maitriser en profondeur sa sécurité
- Développement de CloudGoat, un environnement AWS vulnérable par design
  - Dizaine de services AWS mal configurés (EC2, S3, IAM, Lambda, etc.)
  - Plus d'une vingtaine de vecteurs d'attaque
- Coût entre 1 et 3 dollars par jour en fonction de l'utilisation
- Second objectif : outil plus complexe, permettant des attaques en plusieurs étapes, une sorte de Metasploit pour AWS
- Cloudgoat + PACU pour s'entrainer à la sécurité AWS et développer ses exploits pour des environnements plus complexes
  - https://github.com/RhinoSecurityLabs/cloudgoat
  - https://github.com/RhinoSecurityLabs/pacu

# Jarvis nerver saw it coming : Hacking machine learning in speech, text and face recognition & frankly everywhere else

- Présenté par Guy BARNHART-MAGEN et Ezra CALTUM
- Comment attaquer une intelligence artificielle ?
- Structure d'un système de machine learning classique
  - Entrées ➔ Représentation intermédiaire (IR) ➔ Multiplication de matrices ➔ Sorties ➔ Mapping ➔ Prédictions
- Attaque possible lors des différentes étapes du process itératif
  - Attaque de l'infrastructure : IR ou mapping
  - Attaque de l'algorithme : multiplications de matrices
- Top 5 attaques CVSS
  - DoS
  - Erreur de prédiction
  - Perturbation du modèle
  - Vol d'IP
  - Backdoor
- Adversarial attack : manipulation des sorties avec une entrée créée de toute pièce injectée durant la phase d'apprentissage
- Contremesures : réaliser plus de contrôle sur les données et construire une infrastructure plus robuste

# The current state of adversarial machine learning

- Présenté par Heather LAWRENCE
- Adversarial machine learning : secteur de recherche à l'intersection du machine learning et de la sécurité informatique
- Nouveauté : considérer des adversaires qui pourraient manipuler les données injectées afin de compromettre le système de machine learning
- Applications possibles : détection de malware, filtrage de spam, reconnaissance biométrique
- Plusieurs attaques possibles
  - Manipulation des données d'apprentissage avant la phase d'apprentissage
  - Injection d'entrées manipulées dans les données d'apprentissage après la phase d'apprentissage
  - Attaque du classifier
- Adversarial examples : fournir intentionnellement au classifier des données lui faisant prendre la mauvaise décision
- Entrainer et tester un classifier avec des AE permet de réduire le nombre de mauvaises classifications
- Hypothèses des travaux de recherche : white box ou black box
  - Possible de tester son attaque sur son propre classifier et d'ensuite transférer son modèle sur le classifier cible



# All your cloud belong to us : Hunting compromise in Azure

- Présenté par Nate WARFIELD
- Montée du Cloud : de plus en plus de VMs exposées sur Internet et attaquées
  - Comment traquer et trouver des systèmes vulnérables sur Azure ?
- Principal outil : Shodan
  - Développement de modules permettant de détecter les systèmes vulnérables : bases de données NoSQL, services SMBv1, etc.
- Configuration par défaut des VM Azure : exposition de nombreux ports
- 2018 : année des CryptoMiner
- Autre type d'attaques : images IaaS compromises sur les marketplace
- Protections
  - Mettre à jour ses machines après le déploiement
  - Revoir les configurations firewall avant le déploiement
  - Considérer la création de sa propre image IaaS pour les machines sensibles

# SilliVaccine : North Korea's weapon of mass detection

- Présenté par Mark LECHTIK et Michael KAJILOTI
- SiliVaccine : solution antivirus nationale de la Corée du Nord
- Obtention d'une copie rare de cette solution via un journaliste de Bloomberg
- Analyse de l'architecture et des différentes DLL
  - Découverte d'un mécanisme de scan de fichiers de Trend Micro
  - Signatures renommées
  - Mécanisme de liste blanche ➔ future backdoor ?
- Installation de SiliVaccine packagée avec le malware Jaku

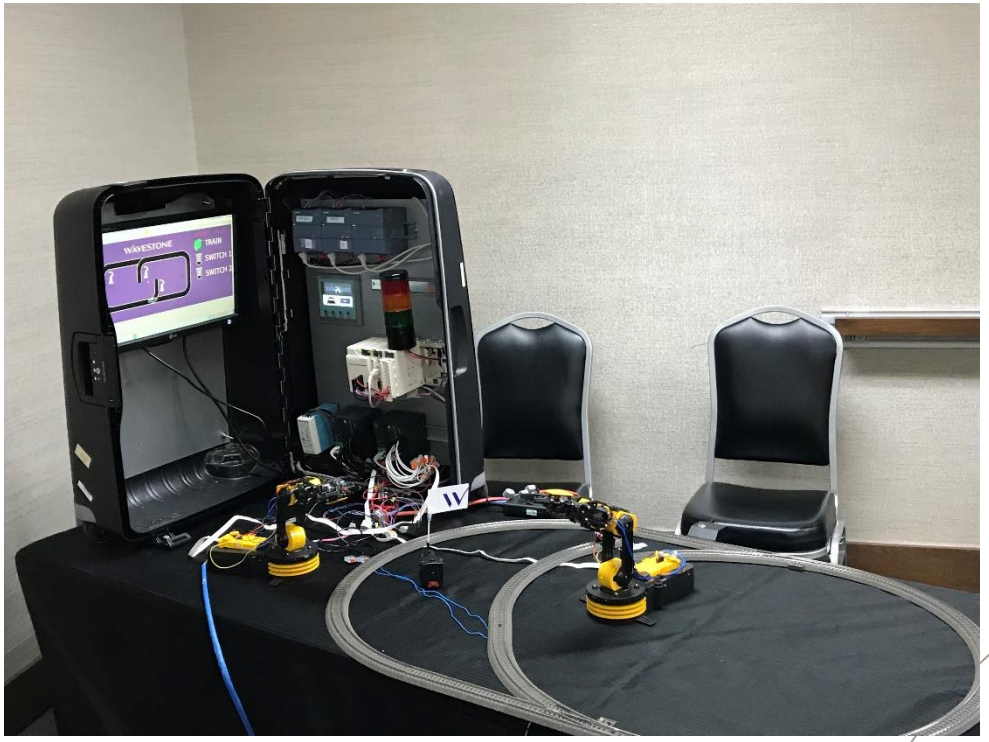
# 02

## DEF CON 26


- 9 au 12 août 2018
- Césars, Flamingo et Linq
- 26ème édition
- 280$ en cash
- 28 000 personnes
- 4 tracks de conférences en parallèle, les skytalks
- Plus d'une quinzaine de villages thématiques : ICS, Car Hacking, IoT, Lockpicking, Wireless, Hardware Hacking, Social Engineering, AI, etc.

# Workshop – Pentesting ICS 101


- Animé par Arnaud SOULLIE et moi-même
- Workshop de 4h sur la sécurité des systèmes industriels
  - Introduction sur les systèmes industriels
  - Familles de vulnérabilités sur les systèmes industriels
  - Programmation d'automates
  - Tests d'intrusion sur automates
  - Capture the flag!
- ~30 participants
- https://tinyurl.com/ics101-dc26

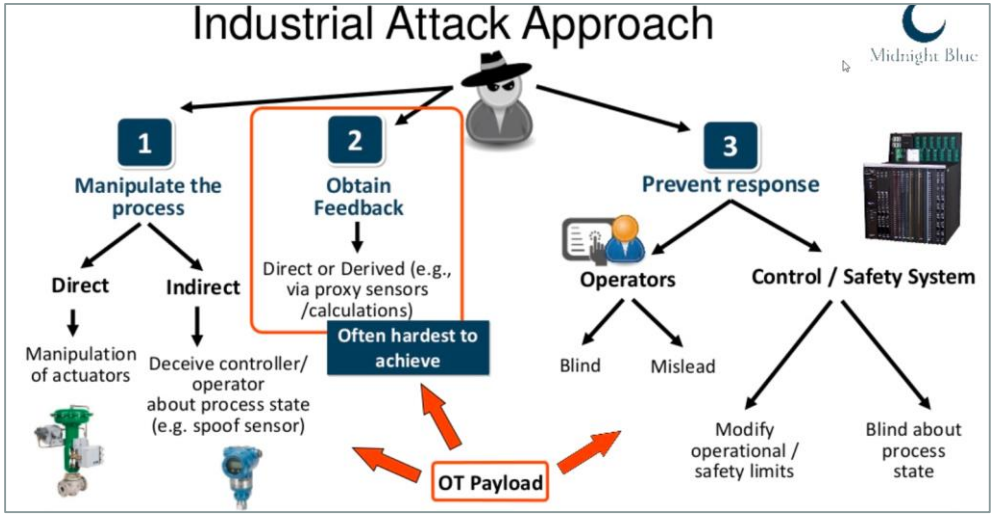


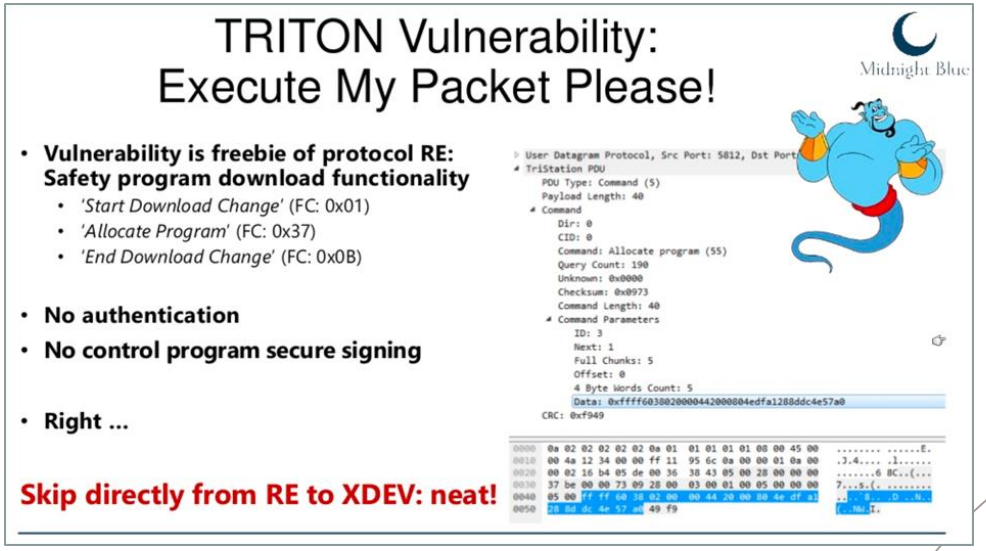
# ICS Village

- Les 10 et 11 août au Flamingo
- CTF Hack the Plan[e]t
  - Organisé par les différents sponsors : Grimm, Dragos, Security Matters, etc.
  - Remporté par la team Dragos #FUZZYSNUGGLYDUCK avec 6600 points
- Conférences dédiées sur les systèmes industriels
  - Espace partagé avec le village Car Hacking


# Through the eyes of the attacker : designing embedded systems exploits for ICS

- Présenté par Marina KROTOFIL et Jos WETZELS
- Construction d'une attaque embarquée sur des systèmes industriels basée sur l'exemple de TRITON
  - Injection d'une backdoor passive et implant de Triconex pour attaquer les SIS
- Approche en trois étapes: manipuler les boucles de contrôle afin d'obtenir un état non sécurisé
- Étapes d'exploitation
  - Obtention du matériel nécessaire
  - Analyse de l'équipement et de sa carte PCB
  - Reverse engineering du logiciel, du protocole et du firmware
  - Découverte de vulnérabilité
  - Développement de l'exploit
- Développement du payload OT
  - Analyse approfondie du firmware
  - Connaissance précise du process SIS



# Analyzing VPNFilter's Modbus module

- Présenté par Patrick DESANTIS et Carlos PACHO
- Campagne de malware depuis 2016, ayant infecté plus de 500 000 postes
- Construction d'un réseau de honeypots avec de vrais équipements afin d'analyser le malware
- 3 composants
  - Le loader persistant
  - La plateforme primaire
  - Les modules et plugins
- Module HTTP et Modbus (sniffer)
  - Boucle parsant les paquets
  - Modbus ➔ vérification de l'IP et création d'un fichier de log
  - HTTP ➔ vérification entête d'authentification et création d'un fichier de log
- Module inoffensif malgré les autres capacités destructrices de l'attaque

# A ACT that teaches : challenging the next generation of ICS ethical hackers

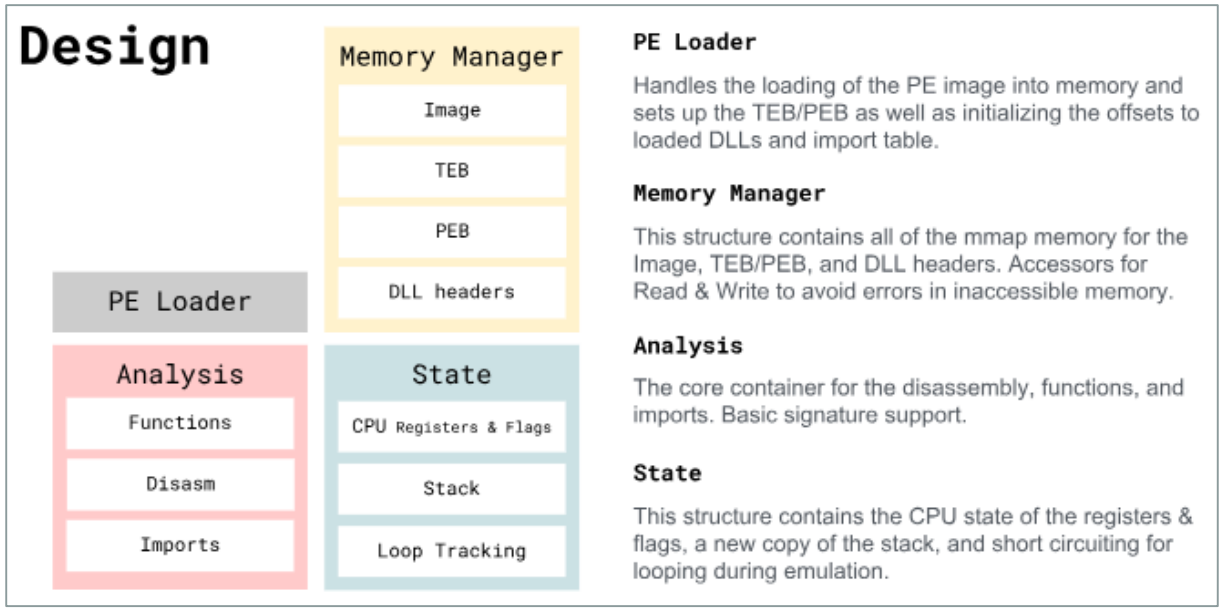
- Présenté par Brandon WORKENTIN
- REX sur l'organisation d'un CTF SI industriel chez Security Matters
- Nombreux problèmes
  - Coût des équipements industriels
  - Multiplicité des OS
  - Transport difficile
  - Difficultés techniques diverses et erreurs humaines
- Limiter les chemins d'attaque
  - Rendre certains vecteurs d'attaque hors-périmètre ou trop difficile à compromettre
- CTF orienté sur l'apprentissage plus que le test
  - Parler avec les participants
  - Poser des questions guidées, donner des indices
- Amélioration continue : collecte des captures réseau

# Reverse engineering physical processes in ICS

- Présenté par Marina KROTOFIL
- Travaux de recherche sur le reverse engineering de procédés industriels
- Il ne suffit pas d'être sur le même réseau que les équipements industriels pour réussir une attaque
- Besoin d'une connaissance approfondie du comportement dynamique du procédé industriel
  - Très difficile à obtenir
- Nouveaux travaux pour créer un système de découverte automatisé des procédés industriels
  - Possible d'obtenir une image d'un procédé industriel
  - Possible de trouver des capteurs et signaux corrélés dans ce procédé
- Aucune approche standard pour le moment

# Finding xori : malware analysis triage with automated disassembly

- Présenté par Amanda ROUSSEAU et Rich SEYMOUR
- Xori : désassembleur automatisé pour l'analyse de malware
- Open source, développé en rust, support des architectures i386 et x86-64, sortie sous format JSON
- Plusieurs modules
  - Un loader de PE
  - Un gestionnaire de mémoire
  - Un module d'analyse, contenant notamment le désassembleur
  - Un module d'état, notamment pour la pile et les registres CPU



# barcOwned : Popping shells with your cereal box

- Présenté par Michael WEST et Colin CAMPBELL
- Code barre = texte
- Scanner : fonctionne comme un clavier tapant les caractères un à un
- Modifier le texte à la volée ? ➔ programmer les scanners
- Règles à ajouter pour déclencher des actions en fonction de critères
  - Possible de modifier du texte, ignorer du texte, ajouter des caractères, ou simplement ne rien faire
- barcOwned : éditeur de payload au format JSON, open source, pour programmer les règles d'un scanner
- Demo
  - Calc.exe
  - Cmd.exe et net user
  - Tetris
  - Désactiver le scanner
- Impossible de se protéger de la programmation
- Règles de protection classiques

**barcOwned** (finally)

- Payload design IDE
  - Payloads in JSON
  - Rapidly develop and test
- Abstracts most complexity
  - No deciphering manuals
- Supports Motorola Symbol
  - Send us scanners?
- Open source

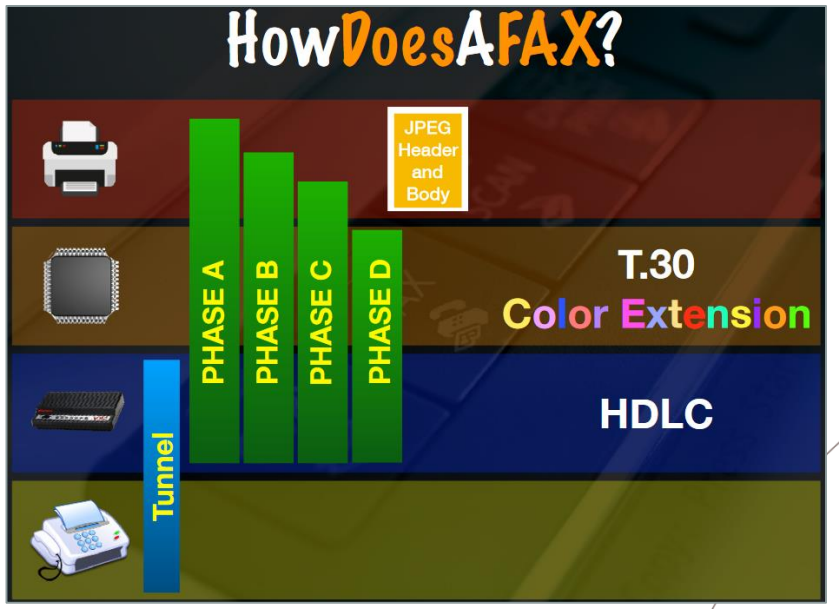
```
{
  "name": "Hello World",
  "description": "Scan hello, get a bonus world!

  "setup": {
    "options": [],
    "rules": [
      {
        "criteria": [
          ["stringatstart", "hello"]
        ],
        "actions": [
          ["sendremaining"],
          ["sendtext", "world"]
        ]
      }
    ]
  },

  "payload": [
    "hello"
  ]
}
```

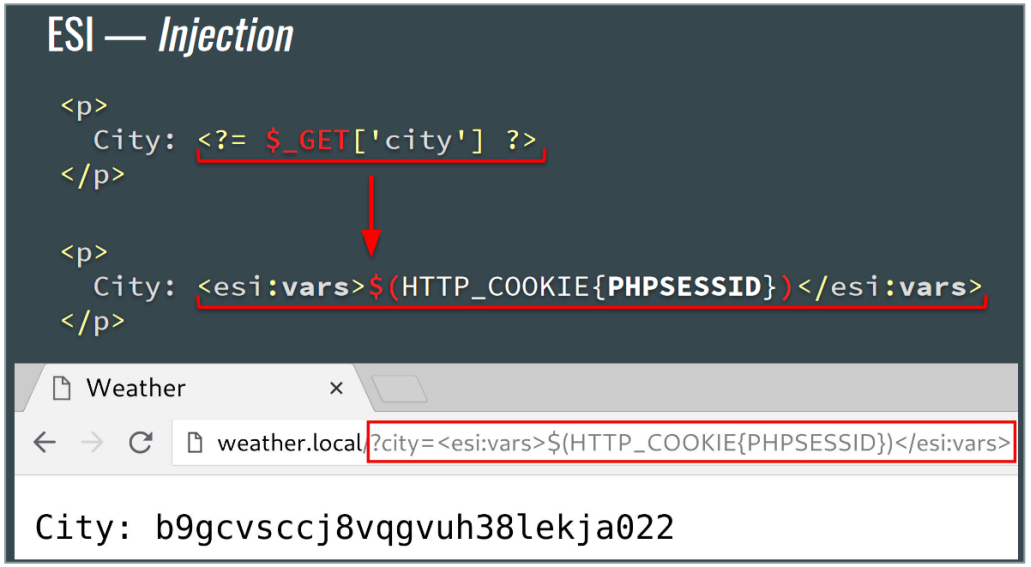
# What the fax ?!

- Présenté par Yaniv BALMAS, Eyal ITKIN
- Fax – équipement à priori obsolète, encore largement utilisé
- Souvent connecté au réseau et donc possible point d'entrée ➔ challenge accepté !
- Démontage des composants hardware pour extraire le firmware
- Compression du firmware avec un algorithme peu robuste, utilisant des sliding window
- Identification des sections : librairies, taches
- Utilisation d'une vulnérabilité publique pour installer leur propre débogueur
- Recherche de vulnérabilités
  - Stack based buffer overflow dans le parser JPEG
- Protection
  - Patcher ses imprimantes
  - Cloisonner du reste du réseau
  - Ne plus utiliser de fax !



# Edge Side Include injection : abusing caching servers into SSRF and transport session hijacking

- Présenté par Louis Dion Marcil
- Edge Side Include (ESI) : classe d'attaques sur les serveurs de cache
- Tags ESI envoyés par les serveurs d'applications dans les réponses HTTP et analysés par les proxy
- Comment le moteur ESI peut savoir si un tag est légitime ou non ?
  - Tag envoyé par le serveur applicatif
  - Tag traité par le proxy
  - ➔ Aucune confiance possible
- Possible de réaliser des injections ESI
  - Récupération des cookies de session
- POC
  - Apache Traffic Server
  - Oracle Web Cache
- Server Side Request Forgery
- Détection manuelle ou automatique




```
FOO<!--esi -->BAR    →    FOOBAR        ✔

FOO<!--foo -->BAR    →    FOO<!--foo -->BAR    ✖
```

WAVESTONE

**Alexandrine TORRENTS**
Consultante

**M** +33 (0)7 63 26 79 87
Alexandrine.torrents@wavestone.com


riskinsight-wavestone.com
@Risk_Insight


securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDON

NEW YORK

HONG KONG

SINGAPORE *

DUBAI *

BRUSSELS

LUXEMBOURG

GENEVA

CASABLANCA

LYON

MARSEILLE

NANTES

* Partenaires stratégiques

WAVESTONE