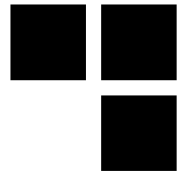
SYNACKTIV
DIGITAL SECURITY

Backdoor TCP/32764

Analyse de *firmwares* et recherche de vulnérabilités

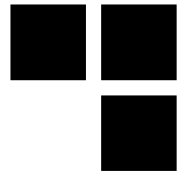
Présenté 08/07/2014
Pour OSSIR Juillet 2014
Par Eloi Vanderbeken

La société Synacktiv



- **Expertise en sécurité des SI**
  - Fondée par des consultants expérimentés & passionnés
- **Offre son expertise aux travers de multiples services**
  - Tests d'intrusion
  - Audits de sécurité
  - Recherche de vulnérabilités
  - Assistance, conseil et R&D
  - Formations
  - Réponse à incident
  - Hébergement sécurisé

Enjeux de cette présentation

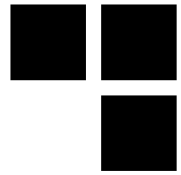


- **Contexte**
  - De plus en plus de systèmes embarqués
  - Souvent connectés
  - Cycles de développement / vie courts
- **Systèmes**
  - *Closed source*
  - (souvent) sans interface de *debug*
- **Cas particulier : les modems routeurs**

Récupération du *firmware*

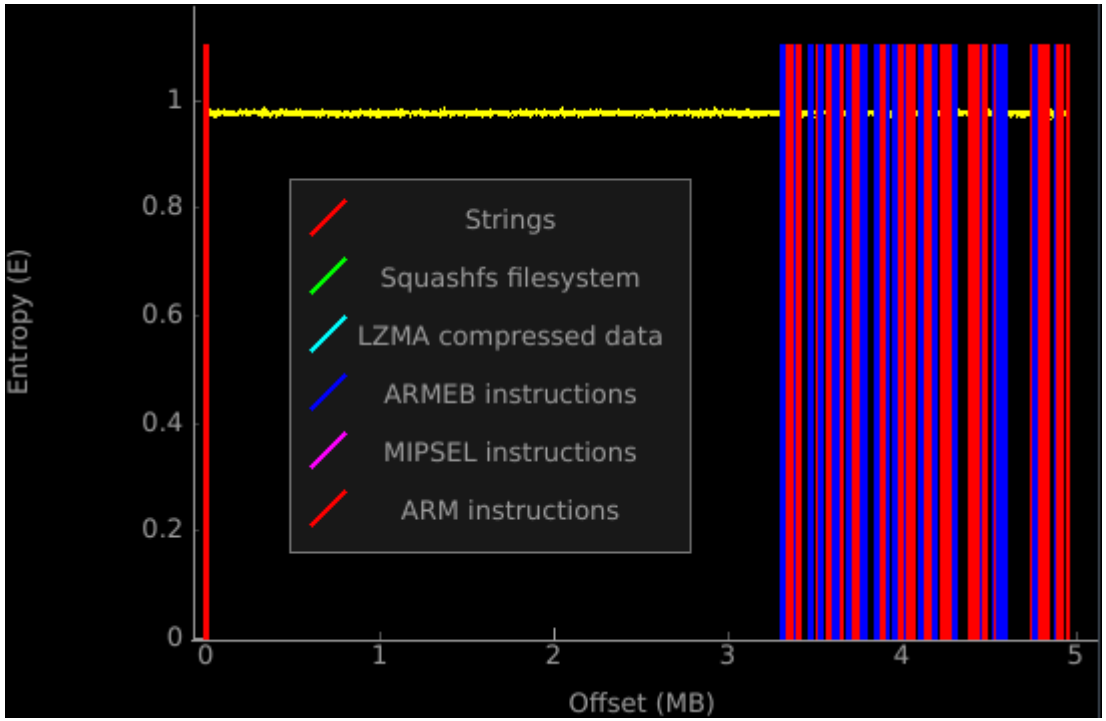
- **Mises à jour**
  - Site de l'éditeur
  - Site tiers : http://www.modem-help.co.uk/
- ***Dump* matériel**
  - Utilisation du port JTAG
  - Nécessite parfois des modifications du matériel
  - Pas l'objet de cette présentation ☺
  - Plus d'informations : http://www.devttys0.com

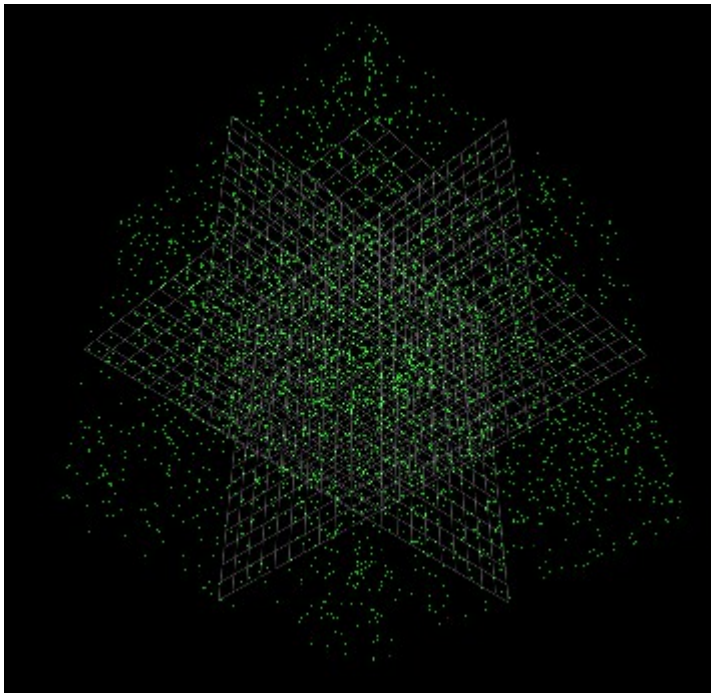
L'outil *binwalk*



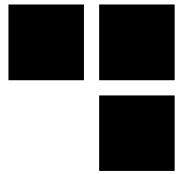
- **http://binwalk.org/**
- **Signatures**
  - Fichiers
  - Système de fichiers
  - Formats spécifiques aux constructeurs
  - Chaînes de copyright
  - Prologues de fonctions dans différents langages assembleurs
  - Etc.
- **Extraction automatique des fichiers reconnus**
- **Visualisation en 2D / 3D**

L'outil *binwalk* - cont'd





Premiers pas



- **Scan des services avec l'outil *nmap***
- **grep !**
  - API : *bind* / *socket* / *system* / fonctions du *firmware* / ...
  - Scripts d'initialisations
  - Messages de l'interface WEB
  - etc.
- **Émulation du périphérique à l'aide de QEMU**
  - Nombreuses architectures disponibles sur http://people.debian.org/~aurel32/qemu/
  - Transfert du système de fichiers
  - *chroot* + exécution des scripts d'initialisation

Cas pratique n°1

Backdoor TCP/32764

Cas pratique n°2

Le retour de la backdoor TCP/32764 !

Quelques ressources...

- **Hors Série n°9 de MISC**
  - Analyse de *firmwares* : cas pratique de la *backdoor* TCP/32764
- **http://www.devttys0.com/**
  - « Dédié à l'exploration, l'exploitation et l'amélioration des équipements embarqués »
- ***Embedded Devices Security And Firmware Reverse Engineering*** **:**
  - BlackHat 2013
- **http://w00tsec.blogspot.com/**

AVEZ-VOUS DES QUESTIONS ?

MERCI DE VOTRE ATTENTION,

SYNACKTIV
DIGITAL SECURITY