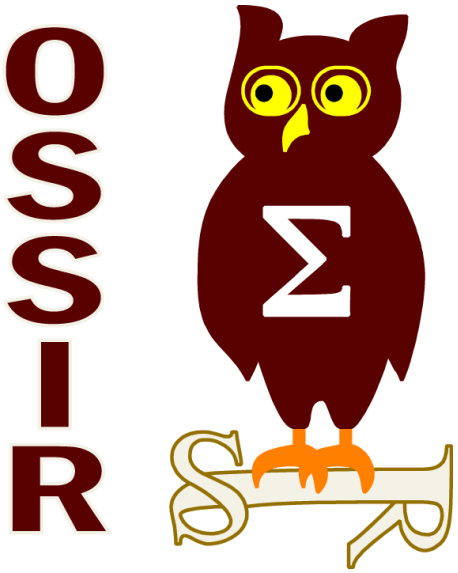
12 Juin 2012



Des risques posés par les imprimantes multifonctions

solucom
management & IT consulting

Agenda

1. Introduction
2. Risques
3. Focus

Note

Cette intervention vise à présenter certains risques liés aux **imprimantes multifonctions** à travers un **retour sur expérience terrain** orienté modèle moyen et haut de gamme sur des audits effectués au sein d'entreprise type CAC 40

Attaque et Sécurisation

Dans **95% des techniques de hacking classiques** sont **suffisantes**

Sinon il est préférable de hacker les processus métier avant d'avoir en dernier lieu recours à des techniques plus avancées

De même la **sécurisation de MFP** est avant tout un **exercice assez classique de durcissement** de la configuration (authentification, contrôle d'accès, chiffrement, mie à jour, etc)

Le problème provient avant tout de la **perception des MFP** : ils sont encore trop souvent **vus comme une imprimante munie d'un disque et connectée** au réseau que comme un **serveur**

Avant de commencer, un petit rappel sur les MFP

MFP (Multi Function Printer)

Dualité

Un **système standard connecté en TCP/IP**, muni d'un disque dur et interagissant avec des protocoles standards

Fax, SCAN, SCAN-to-Folder, etc

Un **système spécifique** à chaque constructeur/modèle

OS : Linux, NetBSD, spécifique (Vxworks)
Tendance globale : de plus en plus de nouveaux modèles sous linux

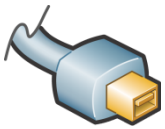
Agenda

1. Introduction
2. Risques
3. Focus

Analyse (très arbitraire) de risques

- **Récupération de documents confidentiels à côté de l'imprimante**
- **Fuite de données**
  - Lors d'une opération de maintenance / mise au rebut
  - Par exploitation de fonctions de la MFP

Souvent pris en compte



- **Récupération de documents confidentiels**
  - Par compromission de l'imprimante
  - Interception de données au niveau réseau

Parfois pris en compte

- **Utilisation du MFP pour l'exfiltration de données**
  - Exfiltration & Outrepassement de système DLP
- **Usurpation d'identité**
- **Intrusion sur le SI en utilisant le MFP comme point d'accès**
  - Télémaintance
  - Interface Wifi / Bluetooth
- **Rebond sur le SI**
  - Récupération d'identifiants administrateurs par interception réseau ou par analyse de l'imprimante

Rarement pris en compte

Les MFP sont le plus souvent perçues comme de simples imprimantes munies d'un disque dur et mises en réseau

Un problème de vision…

Les MFP sont le plus souvent perçues comme de simples imprimantes munies d'un disque et mises en réseau

- Seuls les risques de **fuite de données** liés aux **disques** et à la **récupération de documents** sont pris en compte
- Les systèmes sont laissés dans leur **configuration par défaut**

Cette vision change progressivement, en particulier pour les modèles haut de gamme…

- Mais ce n'est toujours pas le cas pour les **« petites » imprimantes**
- La sécurisation se limite le plus souvent à une **restriction d'accès** au niveau de l'interface

Mais le risque de rebond sur le SI est généralement négligé

- Ce risque restera présent tant que les MFP seront **perçus comme des imprimantes plutôt que comme un serveur**

Agenda

1. Introduction
2. Risques
3. Focus

Audit Physique

Interface intégrée

Tenter les **mots de passe par défaut**

Interface intégrée

- Manuel (site constructeur / souvent scotché derrière l'imprimante)
- Procédure de secours (mise à jour des mots de passe)
- Mode recovery (compte supervisor, reboot en mode recovery)

RETEX

Ricoh : compte supervisor permettant de remettre à zéro le compte administrator et dont le mot de passe pas défaut est rarement changé

Administration via USB

Mesures de sécurité physique

Contrôle d'accès à la salle

Sceau d'intégrité

Badge d'impression

Caméra de surveillance

Positionnement des câbles (positionnement d'un dispositif d'interception physique)

Carton de récupération des impressions ratées / Broyeur

Récupération de données sur les médias de stockages (1/2)

Deux méthodes d'accès

Analyse Online

Utilisation des **fonctions intégrées** (interface Web)

Accès au **FS interne** via PJL (ex JetDirect)

Rooter l'imprimante

RETEX

Accès via l'interface très efficace

- Cas : retrouvé des années de correspondance (Fax) du DG
- Cas : Tous les documents scannés sur les derniers 48h
- Cas Zythom : http://zythom.blogspot.fr/2012/05/watching-you.html

Analyse Offline

Analyse avec des **outils forensics classiques**

Efficacité très variable, en général 2 cas :

- FS standard et données directement accessibles
- FS spécifique ou chiffré (nécessite du reverse)

RETEX

Accès au FS très variable selon les constructeurs

Ricoh : FS « compressé » avec un algorithme maison

Chiffrement mis en place spécifiquement rarement rencontré

Récupération de données sur les médias de stockages (2/2)

Effacement sécurisé

Media de stockage = DD + ∑ε

Medias de stockage

- Ne se limite pas uniquement aux disque durs
- La nvram, des cartes flash ou encore la puce dans certaines cartouches peuvent contenir des données sensibles

Cas de la Maintenance

- Sur des périmètres sensibles, attention à accompagner le technicien lors de son intervention
- Attention aussi au renvoi des imprimantes pour support

Négatifs sur vieux tonners

- Attention aux tonners de certains fax qui contiennent le négatif de tous les documents reçus

RETEX : Italie / Fax sensible

Effacement sécurisé des médias

- Niveau **basique** : fonctions intégrées
- Niveau **intermédiaire** retirer les medias et procéder à un effacement manuel
  - Disques durs : réécriture (surimpression) ex dd, ATA Secure Erase
  - Mémoire flash : réécriture, attention au wear levelling
  - Autre : utiliser les procédures constructeur
- **Sécurisé** : destruction physique
- Cas des **fonctionnalités de chiffrement** proposée par certains constructeurs
  - Une solution pour mitiger les risques sur des périmètres non sensibles
  - Pour les périmètres sensibles, bien que les algorithmes utilisés soient souvent standards (ex AES), la qualité de l'implémentation est difficile à évaluer…
- **Fonction d'effacement sécurisé entre 2 taches** / par 24h si elle est proposée par l'imprimante

Audit Réseau

Telnet

- Donne globalement accès aux **mêmes options que l'interface web**
- Changement **mot de passe de l'interface web != changement sur l'interface telnet**
- **Interception** des mots de passe (classique écoute réseau)

- *Pentest Tip : l'interface étant rarement utilisée, il est possible de déclencher un incident et de filtrer tous les accès sauf l'accès telnet pour forcer les administrateurs à se connecter en Telnet*

RETEX

- ACL par IP défini pour l'interface web
- Changement du mot de passe d'administration via l'interface web. Les administrateurs supposaient que ce changement se répercuteraient sur toutes les interfaces.
- Mot de passe par défaut sur l'interface Telnet ➔ connexion ➔ utilisation de la fonction intégrée de reset des mots de passe ➔ suppression des ACL ➔ accès aux documents scannés

Audit Réseau

```
HP JetDirect
Password is not set

Please type "menu" for the MENU system,
or "?" for help, or "/" for current settings.
> ?
   Help Menu

      Type one "Command" followed by one of its valid "Values".

      Command:          Values:
      ---------------   -------------------------

      ?                 [displays Help menu]
      /                 [Display current values]
      #                 [Comment Line]
      menu              [Enter Menu]
      advanced          [Enable Advanced commands]
      general           [Disable Advanced commands] (default)
      save              [Save settings and exit]
      exit              [exit]
      export            [Export settings to edit and import via Telnet or TFTP

      GENERAL_____________________________________
      passwd            <new-password> <retype-new-password> (16 chars max)
      sys-location      alpha-numeric string (255 chars max)
      sys-contact       alpha-numeric string (255 chars max)
Press RETURN to continue:
```

```
  Enter Selection => e
> advanced
> menu
   ===JetDirect Telnet Configuration===
   HP JetDirect        : J7934G
   Firmware Version    : V.29
   Manufacturing ID    : 2911
   Hardware Address    : 00:1
   System Up Time      : 120:


                  MAIN MENU
  ----------------------------------------
  1. General Settings
  2. TCP/IP Menu
  3. SNMP Menu
  4. IPX/SPX Settings
  5. AppleTalk Settings
  6. DLC/LLC Settings
  7. Other Settings
  8. Support Settings
  ?. Help
  e. Exit Menu
  0. Exit Telnet


  Enter Selection => 1
   ===JetDirect Telnet Configuration===
   HP JetDirect        : J79


              GENERAL SETTINGS
  ----------------------------------------
      Admin Password      : Not Specified
      System Location     : Not Specified
      System Contact      : Not Specified
      SSL state           : 2
```

Audit Réseau

```
nmap -p 1-65535 -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389 172.20[redacted]
Initiating NSE at 15:33
Completed NSE at 15:33, 30.17s elapsed
NSE: Script Scanning completed.
Nmap scan report for 172.20.[redacted]
Host is up (0.00015s latency).
Not shown: 65523 closed ports
PORT      STATE SERVICE    VERSION
21/tcp    open  ftp        HP JetDirect ftpd
|_ftp-bounce: no banner
23/tcp    open  telnet     HP JetDirect printer telnetd (No password)
80/tcp    open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
| robots.txt: has 1 disallowed entry
|_/
| html-title: hp color LaserJet 5550
|_Requested resource was http://172.20.[redacted]/hp/device/this.LCDispatcher
280/tcp   open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
| robots.txt: has 1 disallowed entry
|_/
| html-title: hp color LaserJet 5550
|_Requested resource was http://172.20.[redacted]/hp/device/this.LCDispatcher
443/tcp   open  ssl/http   HP-ChaiSOE 1.0 (HP LaserJet http config)
| robots.txt: has 1 disallowed entry
|_/
|_html-title: Site doesn't have a title.
515/tcp   open  printer
631/tcp   open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
| robots.txt: has 1 disallowed entry
|_/
| html-title: hp color LaserJet 5550
|_Requested resource was http://172.20.[redacted]/hp/device/this.LCDispatcher
7627/tcp  open  http       HP-ChaiSOE 1.0 (HP LaserJet http config)
| html-title: hp color LaserJet 5550
|_Requested resource was http://172.20.[redacted]/hp/device/this.LCDispatcher
9100/tcp  open  jetdirect?
9220/tcp  open  unknown
9290/tcp  open  unknown
14000/tcp open  tcpwrapped
MAC Address: 00:11:0A:[redacted] (Hewlett Packard)
Device type: printer
```

Audit Réseau

HTTP(S)

- **Credentials enregistrés** (parfois accessibles en clair dans le code source de la page)
- **Infoleak** / Logs d'impression (liste de logins) / adresses de serveurs
- **Impression anonymes** / Exfiltration de données
- **Documents scannés ou faxés accessibles**
- **Vulnérabilités liées à l'application web** : XSS, CSRF, Auth bypass, SQLi, etc

RETEX

- REX : des années de correspondances ; pages de garde de fax
- REX Shmoocon 2011 :
  - &page=faxaddr ➔ auth bypass
  - Canon ImageRUNNER, la modifi cation du ACL=1 permet de bypasser l'authentifiation
  - xerox via http://target:8080/cloning.dlm ➔ clone (ACL Bypass)

FTP

- **Impression anonyme**
- **Info leak** (logs d'impression, syslog, stats, etc)

Audit Réseau

SNMP

- Grand **classique** : bruteforce du nom de la communauté avec snmpbrute/ ADMsnmp puis accès via snmpwalk / interception

RETEX

- RETEX IRONGEEK: récupération du mot de passe via SNMP
- RETEX : Réutilisation du nom de la communauté sur d'autres systèmes

JetDirect

- Jetdirect + commandes « commandes » PJL (Printer Job Langage)
- ➔ **impression directe**
- ➔ **accès aux objets PML** ~ SNMP en RW et accès aux disques (via telnet ou Phenoelit Hijitter / PrinterFS)
  - Récupération de **fichiers d'impressions** (permet de bypasser le chiffrement disque), logs de Fax, scans, **codes PIN d'impression sécurisés** ou de changer le message sur l'imprimante (pour du phishing ou pour illustrer le rapport)
  - **FS** : **espace discret pour le stockage** de fichiers (rarement examiné lors d'un analyse forensics)
  - FS: **modification des pages renvoyées par le serveur web** ➔XSS / browser autopwn ; encore mieux si la page est chargée à partir de l'outil de surveillance centralisé

Audit Réseau

JetDirect

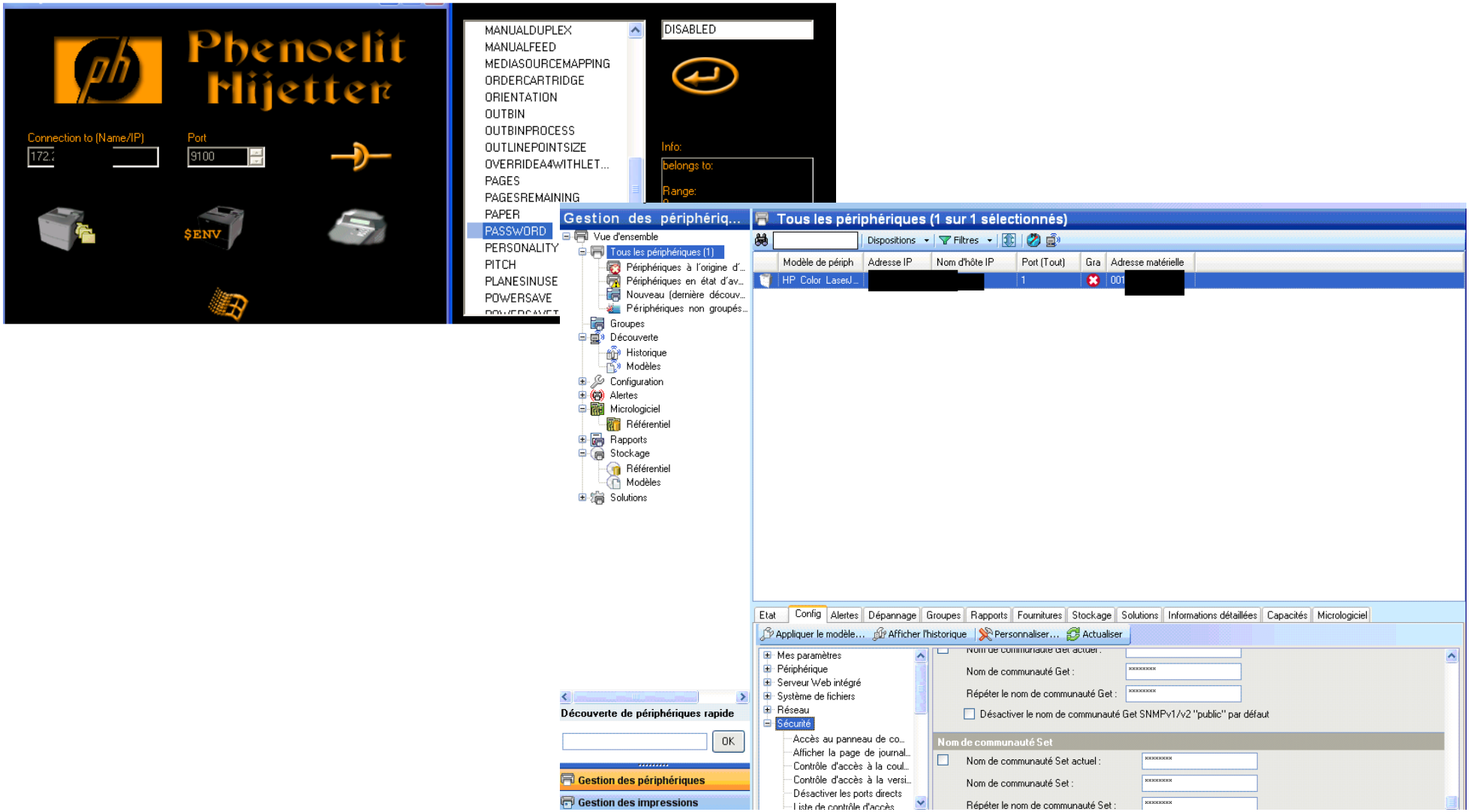
RETEX

- Cas :JetDirect + **Path Trasversal**
  - Accès au FS + Path trasversal (CVE 2010-4107) ➔ root
  - HP Laserjet MFP printer (HP Color LaserJet MFP printer, Laserjet 4100 series, 4200 series, 4300 series, 5100 series, 8150 series, et 9000 series.)
- Cas HP : l'outil d'administration **jet admin** permet d'accéder à plus d'objets PML que via les autres interfaces
- RETEX : **exfiltration de données dans un environnement Citrix isolé**
  - Poste de travail et serveur Citrix ont un accès en 9100 sur l'imprimante qui sert alors de proxy
  - Parfois un mot de passe PJL est défini (cas très rare) : en général un nombre entre 1 et 65535, souvent bruteforçable avec pjlpass

Autres

- LPD / IPP / RSH / SMTP / SMB

Audit Réseau

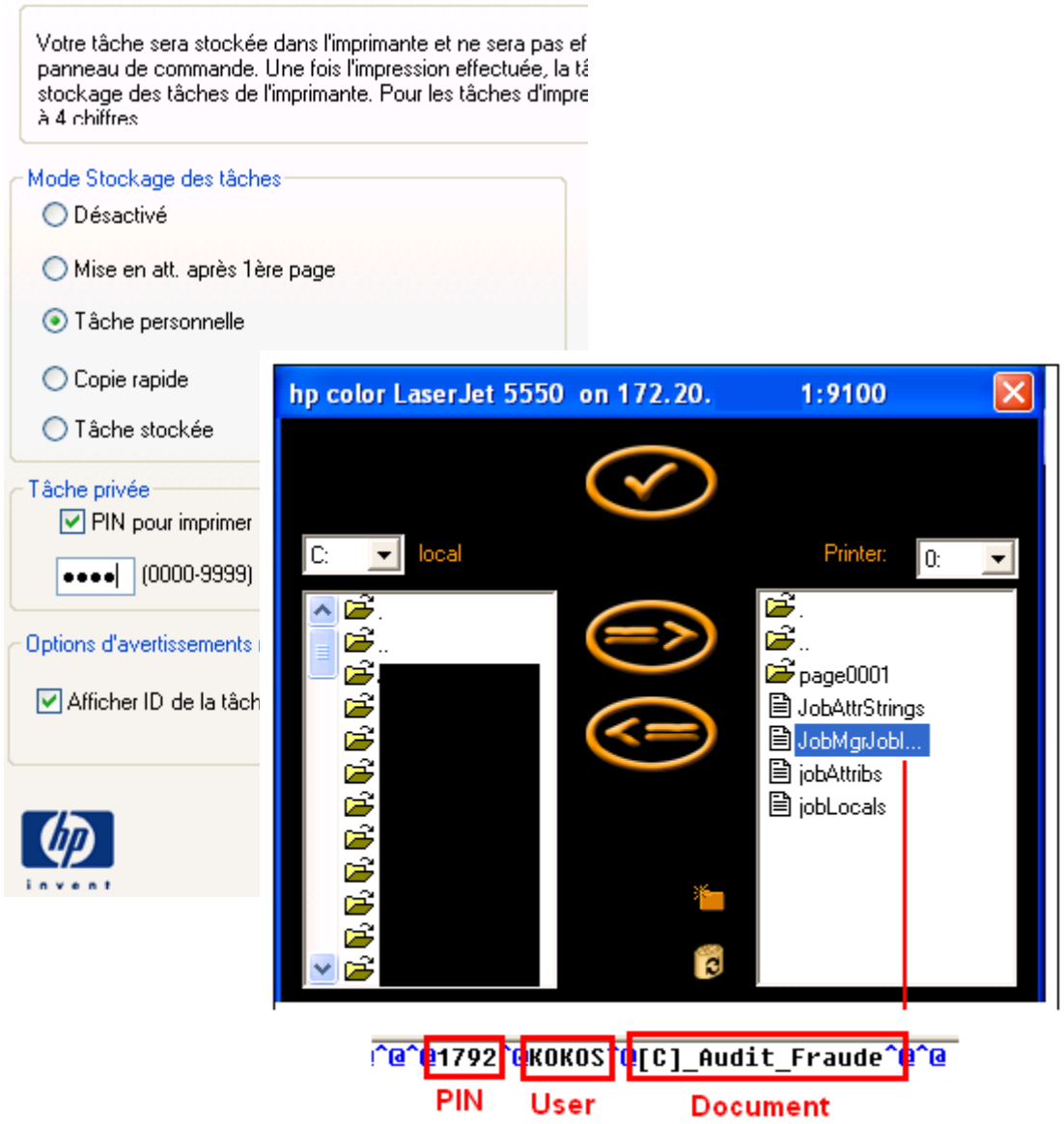


Audit Réseau

Exemple : HP Laser Jet 5550 : Outrepassement de la fonction d'impression « sécurisée »

- De nombreux modèles disposent d'un mode d'**impression « sécurisé »**
  - Un code PIN est nécessaire pour l'impression des données
  - *Note : Les données ne sont pas pour autant nécessairement chiffrées*

- **Cas d'une HP Laserjet 5550**
  - Accès au filesystem over jetdirect (ex : Hijetter)
  - Impossible de récupérer le fichier d'impression mais il est possible d'accéder au fichiers de description : cibler **JobInfo** Savedevice ➔ SavedJobs ➔ Keepjob ➔ Stored job ➔ JobmgrJobInfo
  - Impression du document sans le supprimer
  - L'utilisateur réutilisant souvent son code PIN : PIN Imprimante = PIN téléphone = PIN du token RSA = PIN de la carte à puce, etc)



Interception des communications

Communications

- Les **communications** avec l'imprimante sont **rarement chiffrées** (supporté nativement mais complexe à mettre en place, en particulier sous Windows)
  - Il est donc possible d'intercepter l'échange avec des outils classiques
  - **Interception** des documents échangés (ex ettercap)
  - Interception d'authentifiants (SMTP, LDAP, SNMP, etc)

- Le format PCL (Printer Command Language) est souvent utilisé
- Tip : Si le format n'est pas lisible, tenter de rejouer le code intercepté (rejeu réseau ou via FT¨P)

RETEX

- Cas Pcounter
  - **Communications chiffrées** entre le client et le serveur d'impression
  - **Mais pas entre le serveur d'impression et l'imprimante**
  - Un MITM entre la gateway locale et l'imprimante donne accès à tous les documents

Backdoor logicielles – backdoor physiques

Backdoor Logicielle

- **Difficulté de mise en place très différente selon les modèles**
- **Solution 1 : reverser/rooter** la machine (mais très variable selon les modèles ; parfois il faut bypasser du code signing)
- **Solution 2 : détournement de fonctions intégrées**
  - Ex : support d'applets Java (voir les travaux de Phenoelit)

RETEX

- Solution Keep It Stupid Simple : interface web sur certains modèles équipés de pcounter pour la configuration de l'**option** scan and share. **Non documentée**, elle permet d'adresser une **copie de tous les fax envoyés** à une adresse mail

Backdoor Matérielle

- **Dispositif** d'interception physique (Voir Travaux de NBS)

RETEX

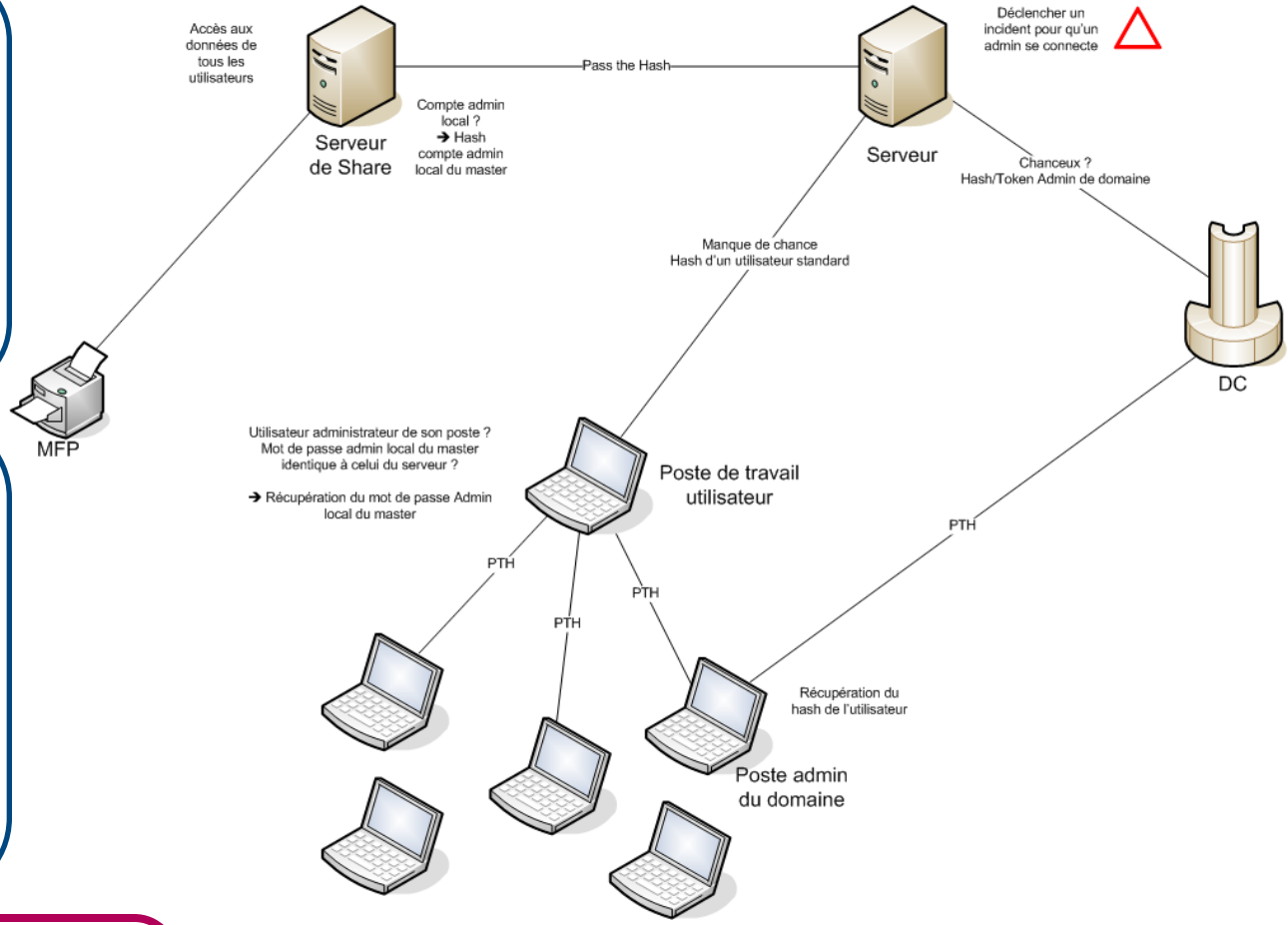
- Solution très simple pour accéder aux données et beaucoup moins dépendant des modèles
  - Ex gumstix + exfiltration Wifi
- Dans l'imprimante (alimentation fournis par l'imprimante)
- Au niveau des câbles
- **RETEX terrain** : dans une entreprise du CAC 40, à l'étage de la direction générale un vendredi après midi, la seule personne qui ait réagit à deux hommes en costume qui démontaient une imprimante a été le directeur de la sureté lorsqu'il est passé par hasard devant le local

Backdoor

Rebond sur le SI, de l'imprimante au domaine

- **MFP interconnectées avec le SI, présentant une double vulnérabilité**
  - Transmission des données ➔ écoute résau
  - Interaction avec le SI : fonctions scan to mail, scan to folder, etc
- Scan to mail / FTP
  - Récupération de credentialspar écoute ➔ accès aux documents sur le serveur FTP

- **Scan to folder (SMB) / compte LDAP**
  - Souvent mal configuré
  - Accès aux documents stockés sur le share, qui peut contenir d'autres documents (en RW)
  - Un compte administrateur (plus simple à configurer pour écrire dans toutes les répertoires utilisateurs)
  - ➔ **accès aux données de tous les utilisateurs**
  - ➔ **Compromission du serveur**
  - ➔ **Rebond sur le domaine**




```
Authentification Id         : 0;417[redacted]
Package d'authentification  : Kerberos
Utilisateur principal       : [redacted]
Domaine d'authentification  : DOMAIN
        msv1_0 :        lm{ 21c1d268a45a9cd2bdb089670571a42 }, ntlm{ 66b20d1b93
1d7b9a20ca6b52b9da0e04 }
        wdigest :       132geom::!!
```

RETEX

- **RETEX shmoocon 2011 :**
  - Logs ➔ noms users ➔ bruteforce (Medusa) ➔ rebond postes de travail et serveurs ➔ token admin de domaine ➔ :)
  - Credentials Share windows dans une interface web ➔ accès au dossier de scan en RW mais aussi au dossier RH

Interfaces de gestion centralisée / DOS

Interface de gestion centralisée

- **SNMP**
- **Iframe** ➔ affichage de l'interface web de chaque imprimante ➔ 1 XSS to rull them all

DOS

- Cas HP : imprimante chauffantes
- **Impression** de grandes quantités de documents (ncat /dev/random sur le port 9100)
- **Verrouillage** / mot de passe

Télé-maintenance… remote root ?

Télé-maintenance

- De nombreux MFP disposent d'un système de **télémaintenance**
  - Attention il peut y avoir plusieurs **systèmes indépendants** : sur l'interface Ethernet, téléphone ou sur la carte Fax
  - Cas des cartes TEL/FAX : D'après les constructeurs elles ne permettent que de modifier certains paramètres « basiques » (vitesse de transmission, état des cartouches, état interne)
  - **Difficulté d'évaluer le risque réel** (reverse au cas par cas ou déclencher volontairement un incident et faire escalader jusqu'au support L3)
  - A défaut la plus grande prudence est de mise et il est préférable d'éviter les interconnexions à deux réseaux simultanés
- Cas des imprimantes directement exposées sur internet

Fuite d'information / Exfiltration de données

Remarque durant la présentation (Hervé S.):

des modems 3G sont de plus en plus intégrés dans les imprimantes (sans forcément que cela soit précisé par le constructeur)

Exfiltration

- Risque présenté par un **pont entre le réseau Ethernet et PSTN**
  - Exfiltration de données
- **Outrepassement d'un système DLP**
  - La solution de DLP couvre-t-elle les Fax envoyée par la passerelle centralisée ?
  - Quid des accès directes ?

- **Stockage de fichiers sur l'imprimante**
- Service **SMTP** configuré sur l'imprimante
- Note :
  - Cas d'imprimante connectées sur un réseau sensible et non sensible : attention au mode de retransmission automatique ne cas d'échec
- Dans certains cas **statistiques** d'utilisation des imprimantes
  - « Boitier magique » contactant le fournisseur en HTTPS
  - Informations stockées dans les puces de certaines cartouches
- Interfaces Wifi / BT

RETEX

- L'équipe sécurité a détecté une interconnexion « sauvage » entre le réseau bureautique et le réseau sensible en principe déconnecté d'internet lors de la réception d'un nombre trop important de cartouches.
- Les imprimantes du réseau bureautique remontent automatiquement au fournisseur l'état des cartouches pour que celui-ci puisse approvisionner en conséquence l'entreprise.
- (Ian Amit): Exfiltration de documents sensibles via fax (en mode rubish)

Serveur d'impression

Cas 1

RETEX

- Tomcat users par défaut ➔ pwn
- Fichiers de configuration
  - Mots de passe LDAP, SMB, SMTP
- Répertoire contenant les spools
- Base spécifique avec association login / card ID
- Mots de passes utilisateurs en clair dans une base

Cas 2

RETEX

- Tous les documents accessibles dans un share…

Sans oublier les aspects contractuels…

Contrat

- Les imprimantes ont-elles été achetées ou sont-elles louées ?
- Une clause de confidentialité est-elle présente ?
- Une clause d'auditabilité (bonus : autorisant à faire de la rétro-ingénierie) est-elle présente ?
- Quelles sont les clauses spécifiques quant à la communication sans délai des vulnérabilités connues par le fournisseur ?
- Quelles sont les conditions spécifiques de maintenance et de télémaintenance ?
- Quelles sont les clauses relatives à l'envoi de statistiques au constructeur ?
- Quelles sont les procédures de contrôle de cette maintenance ?
- Des clauses spéciales de rétention des médias de stockage existent elles en cas de maintenance ou en fin de contrat de location ?

Et quelques autres points

Low Tech Hacking

- Le manuel se trouve souvent dans une pochette fixée à l'arrière de l'imprimante
  - Si le mot de passe administrateur n'y est pas noté, il y a de bonne chance que la procédure de secours soit documentée
    - Ex : compte supervisor sur des imprimantes RICOH
- Modifier les données affichées à l'écran pour piéger l'utilisateur ?
  - Faux numéro de support

Support Spéciaux

- Support d'impression spéciaux ➔ mesures spécifiques
  - Papier spéciaux, chèque de paye

Tracking code

- Micro points jaunes pour assurer la traçabilité des documents (EFF)

Autre

- File d'attente ➔ nom des documents
- Fichiers temporaires d'impression : C:\Documents and Settings\UTILISATEUR\Local Settings\Temp

Éléments de durcissement

Eléments contractuels

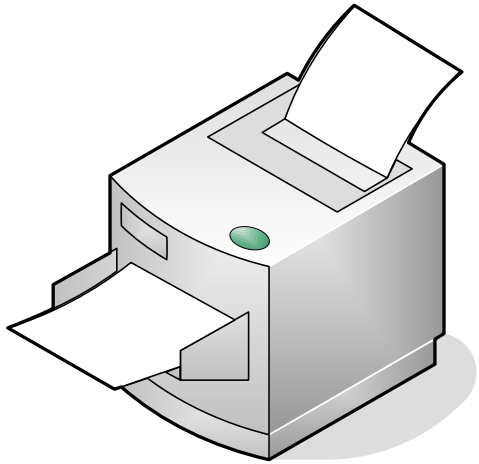
- location/achat
- Clause de confidentialité
- Veille vulnérabilité
- Maintenance - Télémaintenance
- Envoi de statistiques au constructeur
- Contrôle lors de la maintenance
- Clause de foin de vie / contrat (effacement sécurisé des médias)

Installation et administration

- Documentation
- Exposition sur internet
- Modalité d'administration (interface centralisée)
- Authentification
- procédure defin de vie
- Classification des imprimantes

Gestion des incidents

- Procédure de Gestion des incidents



Logging

- Niveau de logging
- Centralisation des logs

Réseau

- Désactivation des piles inutiles
- Configuration du réseau
- VLAN, filtrage ACL
- Interconnexion avec le réseau PSTN
- Restrictions spécifiques sur la copie / fax
- Chiffrement des canaux

Administration

- SNMP
- Mot de passe (dique dur, web, telnet, jetdirect)
- Certificat ? Configuration de la crypto engine
- Mise à joru du firmware

Fonctions stockage / réseau, copie, fax

- Fonctions activées
- Comptes utilisés

Autre

- Accompagnement d'un technicien lors d'une visite
- Périmètre sensible : enclavement, déconnexion, gestion par la sureté
- utilisation d'un bagde à la récupération du document

Questions ?

The power of simplicity
«Ce qui est simple est fort»

www.solucom.fr

Contact

Ary Kokos – Vincent Nguyen

Tel : +33 (0)1 49 03 22 13

Mail : ary.kokos@solucom.fr

RETEX

RETEX communiqué par une des personnes ayant assisté à la présentation

Retour d'exp : Canon C2020i :

- FS EXT3, tout ce qui est scanné/copié/imprimé est stocké en temporaire sur disque avant d'être supprimé immédiatement.
- Puisque c'est de l'ext3, la récupération des fichiers effacés n'est pas triviale (pas aussi facile qu'ext2), mais loin d'être impossible (récup>100 documents).
- Les fonctions d'administration avancées utilisent des mots de passe par défauts qui sont tous listés dans le manuel de service (pas si facile à trouver).

- Contremesures:
  - Il y a un module TPM optionnel pour le chiffrement du disque.
  - Il y a une fonction admin pour écraser le contenu du disque (avant de rendre l'appareil en fin de location).