Brochure

# Comment se protéger contre les attaques ?

## Risques de sécurité dans les films « The Wolf » et solutions HP

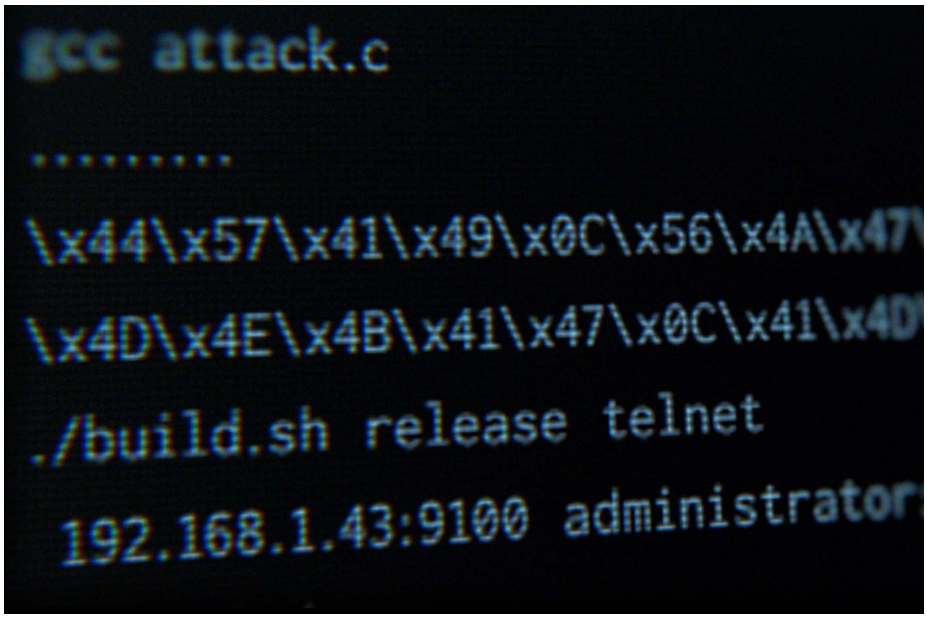
Les pare-feu ne suffisent pas pour résister aux attaques de plus en plus sophistiquées des pirates tels que The Wolf. Il est essentiel de déployer plusieurs couches de protection à chaque point de terminaison de votre infrastructure. Avec les solutions de sécurité proposées par HP, vous pouvez protéger efficacement vos équipements, vos données, vos identités et vos documents.

# Saison 1 The Wolf

Dans le premier film, The Wolf pirate une institution financière mondiale en exploitant ses points de terminaison vulnérables. The Wolf utilise un terminal mobile pour accéder à une imprimante et injecter des logiciels malveillants (ou malwares) capables d'intercepter les données transmises à cette imprimante. Il utilise ensuite un courrier électronique d'hameçonnage (phishing) pour tromper une utilisatrice qui, sans s'en rendre compte, envoie vers une imprimante le code malveillant caché dans son fichier d'impression.

Le programme malveillant ainsi injecté dans l'imprimante franchit le pare-feu et se propage sur les PC de la société. Le code malveillant s'étant incrusté au niveau du BIOS, il peut continuer à injecter ses données malveillantes et même se rétablir en cas de déploiement de défenses réseau.

Enfin, The Wolf découvre un document confidentiel dans le plateau de sortie d'une imprimante multifonction. En raison de la divulgation de ces données sensibles, l'entreprise subit des dégâts considérables, à la fois sur le plan financier et pour la réputation de ses marques.


## Vulnérabilités

- Les fonctionnalités Wi-Fi/Bluetooth® de l'imprimante sont accessibles sans exiger d'authentification de la part des utilisateurs.
- Les fichiers transmis à l'imprimante ne sont pas cryptés.
- Les utilisateurs sont incapables de détecter les courriers électroniques d'hameçonnage ou les fichiers d'impression suspects.
- Les imprimantes et les PC ne disposent d'aucune protection contre les logiciels malveillants.
- Les documents abandonnés dans les bacs de sortie risquent d'exposer des informations sensibles.

## Comment se protéger contre les attaques ?

**Protéger les données** : désactivez les fonctionnalités Wi-Fi/Bluetooth ou imposez une authentification pour les exécuter. Déployez une solution d'authentification et de cryptage pour les mobiles telle que HP JetAdvantage Connect ou HP Access Control.

**Protéger les équipements** : renforcez la sécurité globale de l'entreprise en remplaçant votre parc obsolète et vulnérable par des PC HP Elite et par des équipements d'impression HP Enterprise (imprimantes dédiées et imprimantes multifonctions). Ces modèles sont protégés contre les logiciels malveillants et ils peuvent détecter les attaques, les bloquer et récupérer d'une attaque sans avoir à faire intervenir le département informatique. Par ailleurs, HP Sure Start aide les équipements à s'auto-réparer en redémarrant à partir d'une copie de confiance de leur code BIOS d'origine.

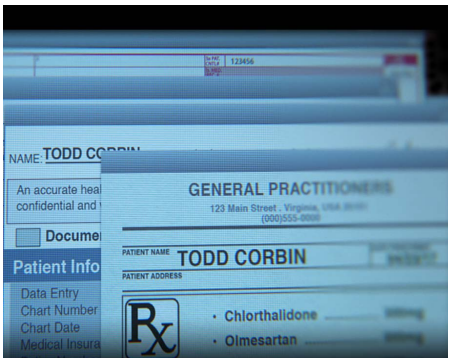
**Protéger les documents** : déployez une solution d'impression à la demande (pull print) telle que HP Access Control ou HP JetAdvantage Secure Print.

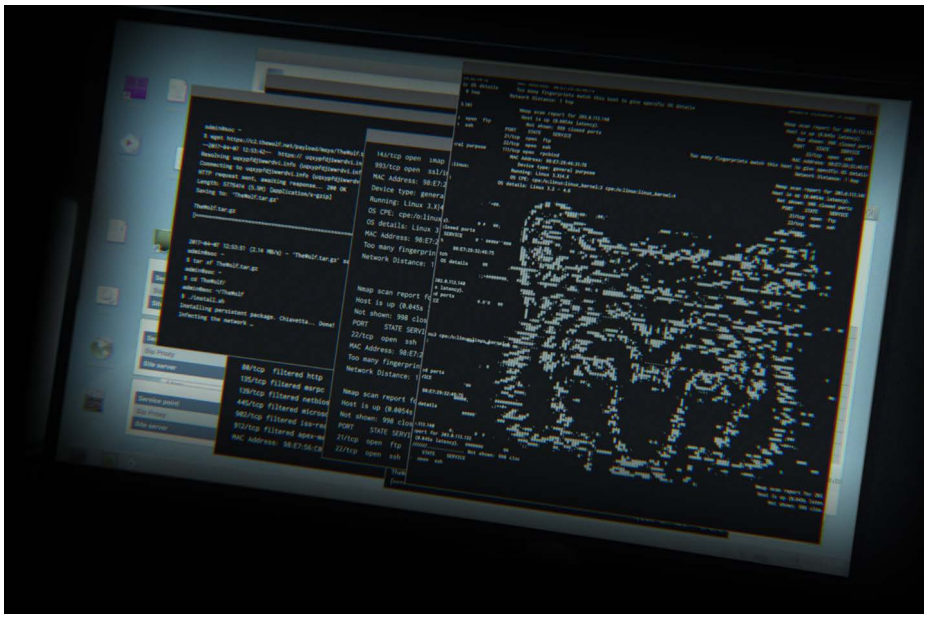
# Saison 2 The Wolf La chasse continue...

Dans le deuxième film, The Wolf cible les dossiers de patients stockés par l'une des plus grandes sociétés de gestion d'enregistrements du monde médical. Dans un hôpital, il pénètre une imprimante en utilisant tout simplement le port USB de celle-ci pour injecter des logiciels malveillants.

Cette imprimante non sécurisée étant connectée au réseau, le logiciel malveillant se trouve déjà derrière le pare-feu et il peut rechercher d'autres équipements connectés à pirater. Et comme cette imprimante appartient à un réseau non segmenté, The Wolf peut accéder à des serveurs connectés à des bases de données qui regorgent d'informations sensibles. Il peut ainsi voler plusieurs millions de dossiers confidentiels de patients.

L'hôpital et la société qui lui fournit les logiciels sont tous deux passibles d'amendes très lourdes, et cet événement risque de nuire à leur réputation.



## Vulnérabilités

- L'utilisateur s'éloigne de son PC sans le verrouiller.
- Le port USB de l'imprimante peut être utilisé sans authentification.
- Les fichiers ne sont pas cryptés.
- Les imprimantes et les PC ne disposent d'aucune protection contre les logiciels malveillants.
- Les imprimantes ne sont pas supervisées de manière à détecter les incidents de sécurité.

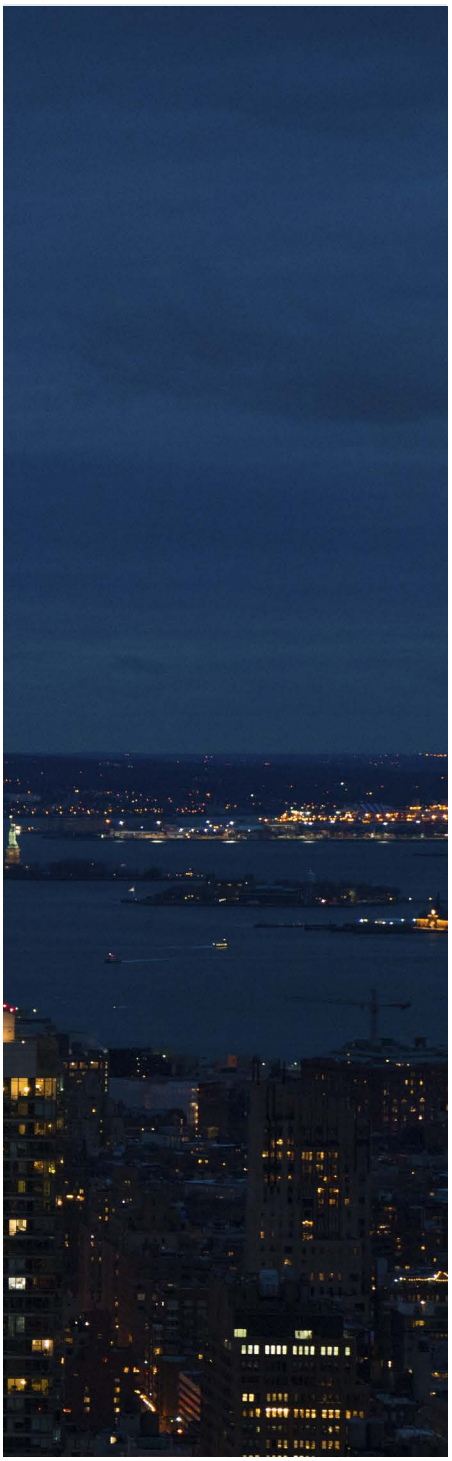
## Comment se protéger contre les attaques ?

**Protéger les identités** : utilisez une authentification multifacteur (disponible sur les PC HP Elite).

**Protéger les données** : déployez une solution d'authentification et de cryptage sur les imprimantes, par exemple HP Access Control. Fermez les ports inutilisés ou contrôlez les accès des utilisateurs aux différents ports. Utilisez des contrôles de cryptage avancés pour toutes les données au repos et en transit.

**Protéger les équipements** : renforcez la sécurité globale de l'entreprise en remplaçant votre parc obsolète et vulnérable par des PC HP Elite et par des équipements d'impression HP Enterprise (imprimantes dédiées et imprimantes multifonctions). Ces modèles sont dotés de protections intégrées contre les logiciels malveillants, ils sont capables de bloquer les attaques, et de s'auto-réparer jusqu'au niveau du BIOS (HP Sure Start).

**Améliorer les pratiques de supervision et d'administration** : déployez HP JetAdvantage Security Manager (sur les imprimantes) et les modules Management Integration Kit[1] (sur les PC) pour configurer automatiquement les politiques de sécurité des équipements dans l'ensemble de votre parc. Configurez les syslogs de manière à enregistrer les détails des événements de sécurité. Connectez les imprimantes à des outils de gestion de la sécurité (SIEM), de manière à bénéficier d'une notification des intrusions en temps réel.



# Protégez vos activités avec les solutions de sécurité HP

### Les imprimantes les mieux sécurisées au monde !²

Avec des fonctionnalités telles que la détection d'intrusion à l'exécution et HP Sure Start, les imprimantes dédiées et les imprimantes multifonctions de la gamme HP Enterprise peuvent détecter les attaques, les bloquer et récupérer d'une attaque sans avoir à faire intervenir le département informatique. Autres protections : disques durs cryptés, microprogramme évolutif et possibilité d'envoyer des alertes de sécurité vers des outils SIEM.
hp.com/go/PrintersThatProtect

### Les PC les mieux sécurisés et les plus faciles à administrer !³

Les PC de la gamme HP Elite protègent vos équipements contre les menaces les plus courantes en appliquant des couches de sécurité au-dessous, au-dessus et à l'intérieur du système d'exploitation. L'authentification multifacteur proposée par HP renforce la protection des identités et l'intégration du module MIK[1] simplifie la gestion de la sécurité dans l'ensemble de votre parc informatique.
hp.com/go/ComputerSecurity

### HP JetAdvantage Connect

Avec cette solution, vous pouvez exploiter plus efficacement les outils et les politiques réseau existants pour superviser l'impression à partir des smartphones et des tablettes en donnant la possibilité aux utilisateurs d'imprimer en toute sécurité aussi facilement qu'à partir d'un PC (aucune application à installer).
hp.com/go/JetAdvantageConnect

### HP Access Control

Avec cette solution, reprenez le contrôle, renforcez la sécurité et réduisez les coûts en déployant des fonctionnalités d'autorisation et d'authentification des demandes d'impression en fonction des rôles et des impressions à la demande (pull print) sécurisées à l'échelle de l'entreprise.
hp.com/go/hpac

### HP JetAdvantage Secure Print

Avec cette solution, protégez les documents sensibles en déployant un système d'impression à la demande (pull print) dans le cloud : les utilisateurs s'authentifient sur l'emplacement d'impression de leur choix pour lancer et imprimer leurs travaux.
hp.com/go/JetAdvantageSecurePrint

### HP JetAdvantage Security Manager

Avec cette solution (le seul outil du marché capable de garantir la conformité de votre sécurité d'impression)[4], réduisez les coûts et les ressources à engager pour garantir la sécurité de votre parc. Définissez des politiques de sécurité à l'échelle du parc, automatisez la correction des paramètres de sécurité de chaque équipement, installez et renouvelez des certificats uniques et générez des rapports de conformité portant sur l'ensemble du parc.
hp.com/go/securitymanager

**Pour plus de détails :**
**hp.com/go/hpsecure**

[1] Le module MIK n'est pas pré-installé, mais vous pouvez le télécharger à partir de la page suivante : hp.com/go/clientmanagement.

[2] Basé sur une enquête comparative HP publiée en 2016 et portant sur les fonctionnalités de sécurité des imprimantes concurrentes de même catégorie. Seul HP propose une telle combinaison de fonctionnalités de sécurité capables de superviser les équipements efficacement, de détecter les attaques, de les bloquer et de valider l'intégrité des logiciels par un redémarrage de confiance. Pour consulter la liste des imprimantes : hp.com/go/PrintersThatProtect. Pour plus de détails : hp.com/go/printersecurityclaims.

[3] Basé sur les capacités de sécurité uniques et complètes proposées sans frais supplémentaires par HP et sur la gestion par le module d'intégration HP Manageability de tous les aspects des PC, notamment la gestion du matériel, du BIOS et des logiciels grâce à Microsoft® System Center Configuration Manager par rapport aux fournisseurs commercialisant, en novembre 2016, plus de 1 million d'unités par an de PC HP Elite équipés de processeurs Intel® Core® de 7e génération, et d'une carte graphique et d'une connexion WLAN Intel® intégrées.

[4] Sur la base de recherches internes HP portant sur les offres des concurrents (Device Security Comparison, janvier 2015) et du rapport Solutions Report on HP JetAdvantage Security Manager 2.1 de Buyers Laboratory LLC (février 2015). Pour plus de détails : hp.com/go/securitymanager.

**Abonnez-vous à notre liste de diffusion :**
**hp.com/go/getupdated**

Partagez ce document avec des collègues



4AA7-0231FRE, juin 2017