

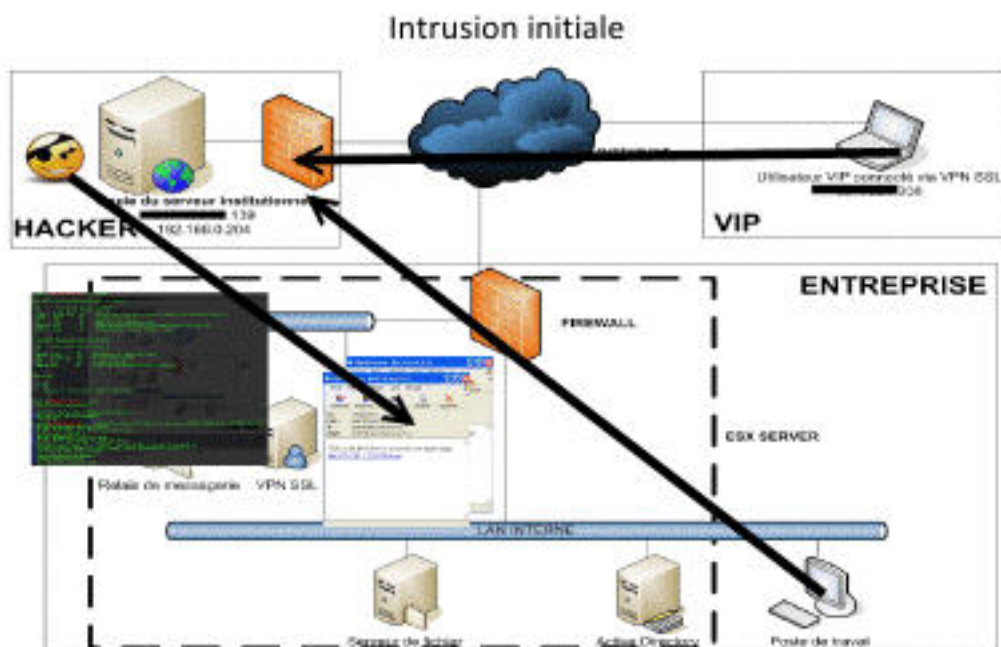
# Fuite des informations les plus sensibles de la société en moins de 45 minutes

Lors des ateliers de la sécurité organisés par CCMBenchmark, un hacker a réalisé une démonstration des fameuses attaques persistantes avancées via l'utilisation d'un trojan spécialement conçu. Son intrusion lui a permis d'accéder aux informations les plus sensibles d'une société en 45 minutes.

Tout commence par la découverte d'une **faille** sur le site Internet d'une grande société. Ce dernier propose d'envoyer, en lien, certaines pages de son catalogue, par mail, au contact de son choix. Problème : il est possible d'inscrire l'adresse de son choix à la fois pour le destinataire mais aussi pour l'émetteur du mail.

C'est ce dont s'aperçoit Nes, société d'**audit en sécurité**, lors d'un **test d'intrusion** commandé par cette "grande société" qui restera, évidemment, anonyme. Les auditeurs ont auparavant reçu la consigne du **RSSI** de mener "le plus loin possible" leur attaque afin d'essayer de "subtiliser le plus d'informations", y compris, et surtout, les plus sensibles. Seuls le RSSI, le DSI, et la DG sont prévenus du test d'intrusion.

[http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/caracteristiques-des-advanced-persistent-threat-apt.shtml?f\\_id\\_newsletter=5060](http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/caracteristiques-des-advanced-persistent-threat-apt.shtml?f_id_newsletter=5060)



Un schéma de l'attaque, avec une capture d'écran authentique. © Nes

## L'intrusion

Après avoir découvert la faille, le hacker employé par Nes commence par copier, intégralement, tout le code du site Internet de l'entreprise visée. Grâce à un logiciel dédié, tout le site est copié sur un serveur de Nes.

Sur 200 mails envoyés, près de 50 destinataires vont cliquer sur le lien piégés

Le hacker, qui a également souhaité rester anonyme, a même pu obtenir un **certificat SSL** par une autorité de certification reconnue, et gratuite. Une seule différence, si le faux site est certifié, ce n'est pas la même autorité qui l'a certifié. Mais les navigateurs et les internautes n'y voient que du feu.

Autre différence, et non des moindres, le site dupliqué est piégé avec une applet Java, contenant une "**backdoor**", une porte dérobée. Ce **cheval de Troie**, qui devra s'installer sur un terminal de la société visée, peut être paramétré afin de ne pas être détecté par les solutions d'antivirus. Son code peut par exemple être mélangé afin de déjouer les bases de signature des **antivirus**. Via des outils **Open Source** rapidement trouvables sur Internet, il est également possible de les configurer pour différentes versions de **Windows**, mais aussi de Linux ou MacOS

## Phishing et social engineering

Ensuite, le hacker, armé de son **code malveillant** dédié, va **hameçonner** les employés de la société visée. Dans le formulaire permettant de partager les pages web du catalogue, il insère comme expéditeur l'adresse mail du directeur général, trouvée tout aussi facilement sur Internet. Dans le corps du message, un texte invitant fortement à cliquer sur un lien, envoyant sur le faux site, piégé, de la société. Sur 200 mails envoyés, près de 50 destinataires vont cliquer sur le lien.

Reste alors à laisser le programme malveillant s'exécuter. Parmi les premiers employés de la société visée à avoir **installé le trojan**, figure un "personnage important", dans la hiérarchie de la société, un "VIP" (voir schéma ci-dessous). "Nous avons eu de la chance" reconnaît le hacker.

L'employé piégé travaille à distance, sur PC portable, mais cela ne change rien à l'attaque : une fois le terminal nomade compromis, sa connexion via **VPN SSL** l'est aussi facilement. En effet, le trojan installé va ensuite pouvoir octroyer les droits pour passer administrateur sur la machine, ou prendre des photos depuis la webcam. Toute la sécurité périmétrique de la société visée (**parefeu, reverse proxy**) est contournée.

Par "chance", l'employé est haut placé dans la société : il a donc de nombreux droits, et les mots de passe qui vont avec. Il peut accéder à de nombreux documents sensibles : fiches de paye, feuille de route de la société pour les prochaines années... Autant de fichiers dont le trojan ne va faire qu'une bouchée, et les envoyer à un serveur distant contrôlé par le hacker.

L'attaque, filmée (voire capture d'écran ci-dessus), a duré moins de 45 minutes. Elle se sera soldée par la **fuite des informations les plus sensibles** de la société.

[http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/?f\\_id\\_newsletter=5060](http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/?f_id_newsletter=5060)<http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/se-protger-contre-les->



[menaces-persistantes-avancees.shtml?f\\_id\\_newsletter=5060](http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/se-protger-contre-les-menaces-persistantes-avancees.shtml?f_id_newsletter=5060)

L'expert Mauro Israel a animé les Ateliers de la sécurité. © CCMBenchmark.

## Menace persistante avancée, le nouveau cauchemar des RSSI

Cette intrusion, menée par Nes à la demande d'un RSSI, et expliquée en détail lors des [Ateliers de la sécurité](#) organisée par CCMBenchmark, n'est pas aussi classique qu'elle n'y paraît. Certes, certains éléments sont connus : **usurpation d'identité, phishing, trojan** etc.

Mais cette attaque était dédiée, elle ne visait qu'une seule société, contrairement au système des **botnets**. Son but n'était pas de corrompre un maximum de machines, juste une suffisait.

Elle ne cherchait d'ailleurs pas à ensuite envoyer de puissante **attaques par déni de service**, mais bien à subtiliser des **informations sensibles**. En outre, elle doit être discrète et rester longtemps sur la machine afin de sortir le plus d'information possible. Ces différences par rapport aux attaques "classiques" font d'elle une **menace persistante avancée**.

### Cauchemar des RSSI

Ce type de menace est le dernier cauchemar des RSSI : ces derniers mois, ce type d'attaque a [mis à genoux RSA](#), la filiale sécurité d'EMC, [Sony et son Playstation Network](#), ou encore [Google, victime d'Aurora](#). [Bercy pourrait également avoir été victime de cette attaque](#), mais les opinions [divergent](#).

L'attaquant va paramétrer son Trojan et même réaliser un malware sur mesure

Pour cibler précisément la société, l'attaque qui repose en grande partie sur **l'ingénierie sociale**, doit être soigneusement préparée. Les pirates doivent collecter un maximum d'informations sur la société.

De nombreux outils, souvent **Open Source**, permettent de connaître les systèmes d'exploitation utilisés par les sociétés, mais aussi leur version, ainsi que celle d'**Adobe** ou encore de **Word** en vigueur dans l'entreprise ciblée... Ces informations permettront très souvent d'obtenir des **vulnérabilités**, notamment si les logiciels ne sont pas tous mis à jour.

"Les entreprises ayant une politique de gestion des mises à jour Adobe, comme Reader, sur tous les postes de travail sont rares", rappelle Raphaël Illouz directeur général de Nes Conseil. Or les failles des versions non patchées sont à la portée du plus grand nombre. Les attaques encore plus sophistiquées peuvent toujours se baser sur des vulnérabilités 0 day.

## **Menace "persistante" et discrète**

Une recherche d'information poussée préalable à l'attaque peut également permettre de connaître les solutions de sécurité, et donc d'antivirus, utilisées par l'entreprise. L'attaquant pourra donc paramétrer son Trojan en fonction, et même réaliser un **malware sur mesure**.

Pour que la menace soit "persistante", le trojan doit également aussi rester le plus longtemps et le plus discrètement actif dans le réseau de l'entreprise. C'est aussi ce qui semble bien s'être passé dans le cas de la fuite d'informations chez Sony. "Dans les forums souterrains, il se dit que l'exfiltration de fichiers .rar appartenant à **Sony** se faisait toutes les quatre heures, pendant 2 mois", explique le hacker de Nes.

# Les parades aux menaces persistantes avancées

Il est possible de se protéger contre les **menaces persistantes avancées**. Outre des "contre-mesures avancées", Nes fait également remarquer que certaines mesures de sécurité élémentaires auraient pu empêcher l'attaque.

## 1) Sensibilisation des utilisateurs.

Les attaques persistantes avancées, comme celle exposée lors de l'atelier, peuvent échouer si les utilisateurs sont correctement sensibilisés. L'**intrusion** n'a été possible que parce qu'un utilisateur a bien voulu exécuter un .exe.

"Il est crucial pour toute organisation de former ces employés critiques, en particulier ceux qui ont accès à des **informations sensibles**, de reconnaître un mail potentiellement suspect" conseille aussi Nes, qui rappelle que l'attaque qu'elle a exposée aurait tout aussi bien pu réussir sans site Internet de **hameçonnage**, mais juste avec un **fichier PDF piégé** envoyé par mail. C'est d'ailleurs [ce qui s'est passé chez RSA](#) et plus précisément sa division dédiée aux tokens, **SecurID**, [victime d'une fuite de donnée](#) il y a quelques semaines.

[http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/caracteristiques-des-advanced-persistent-threat-apt.shtml?f\\_id\\_newsletter=5060](http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/caracteristiques-des-advanced-persistent-threat-apt.shtml?f_id_newsletter=5060)[http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/en-savoir-plus.shtml?f\\_id\\_newsletter=5060](http://www.journaldunet.com/solutions/securite/protection-contre-malware-trojan-et-menace-persistante-avancee-adt/en-savoir-plus.shtml?f_id_newsletter=5060)



Les Ateliers de la sécurité, au Pré Catelan. © CCMBenchmark

## 2) Bien analyser les logs

Les attaques persistantes avancées laissent des traces dans les journaux d'activité tant que le code malicieux est actif à l'intérieur de l'entreprise. "En revanche, il est possible de les effacer ensuite", explique le hacker de Nes et "seul le regard attentif d'un expert pourra détecter l'attaque dans les logs"

### 3) Déployer une solution de DLP ou IPS de nouvelle génération.

Mettre en place une [solution de Data Loss Prevention soit de prévention de fuite de données](#). "Peu évidente à mettre en place" selon l'aveu de Nes, cette solution doit permettre de classer les documents, notamment ceux contenant les informations sensibles, afin de sécuriser les flux sortants. "Les IPS seconde génération ou des règles de firewall sortantes drastiques sont aussi une solution pour empêcher que sortent des informations", rappelle Nes.

### Mettre à jour son parc et auditer les mots de passe

Evidemment, mettre à jour les logiciels utilisés dans un parc, y compris les **antivirus**, empêche les attaques par vulnérabilité connue. Cela concerne aussi **Java et Adobe**. "Aujourd'hui près de la moitié des malwares passent par des failles dans ces solutions", rappelle Nes, qui conseille aussi, évidemment de réaliser souvent des tests d'intrusion et des audits de sécurité. Mais elle reconnaît également qu'il est important de changer d'auditeur pour procéder différemment, et ainsi, mettre éventuellement en lumière d'autres failles.

Selon Nes, les audits doivent également bien se concentrer sur les mots de passe, et notamment ceux des comptes ayant beaucoup de droits. "C'est la première brique de sécurité", rappelle Raphaël Illouz de Nes, qui constate souvent de nombreux **mots de passe mal configurés**, très simples et... très vite cassables.

## En savoir plus

« Revoir

» Les ateliers de la sécurité ont été organisés par CCMBenchmark le 24 mai 2011 au Pré Catelan (Paris). Cette "Démonstration d'attaques persistantes via l'utilisation de trojan dédié" n'était que l'une des sessions. D'autres ateliers pratiques étaient proposés : Gestion de crise, Protection de la navigation dans le "cloud", aspects juridiques de la sécurité liés aux nouveaux usages d'Internet, Menaces liées au Wi-Fi ou sécurité des applications Web entre autres. Un speed consulting donnait aussi aux participants l'occasion de séances privées de consulting en face-à-face avec le consultant de leur choix. La durée de ces entretiens est de 7 minutes.

### En savoir plus

- ▶ **Formation**  
**CCMBenchmark :**  
[Systèmes d'information, informatique](#)
- ▶ **Etude**  
**CCMBenchmark :**  
[Dernières études](#)



### 5 menaces à redouter en 2011

IPv6, réseaux sociaux, smartphones... 2011 ouvre de nouvelles perspectives de nuisances aux pirates. [Lire](#)



### "Deux nouvelles menaces vont marquer 2011 : l'hacktivisme et les menaces persistantes avancées"

Les menaces de sécurité ciblant les smartphones et les réseaux sociaux, ainsi que les attaques politiques devraient se multiplier en 2011. [Lire](#)