MANDIANT
A FireEye® Company

CYBERMENACES : LES CHIFFRES CLÉS

2015 a été l'année de tous les records. Jamais les révélations de compromissions et les groupes de cyberpirates n'ont été aussi nombreux à travers le monde. Dans le même temps, les motivations de ces attaquants se sont diversifiées : infiltration et destruction de systèmes, vol d'informations personnelles, attaque d'équipements réseau, etc. Du côté des victimes, la pression est à son comble avec le stress inhérent à la perte de données et de réputation, l'augmentation du temps et des montants investis dans le rétablissement d'une activité normale, et la multiplication des arguments en faveur d'un renforcement de leur sécurité.

TROIS NOUVELLES TENDANCES EN 2015 :

- Attaques disruptives
- Vols d'informations d'identification personnelle
- Attaques de routeurs et de commutateurs

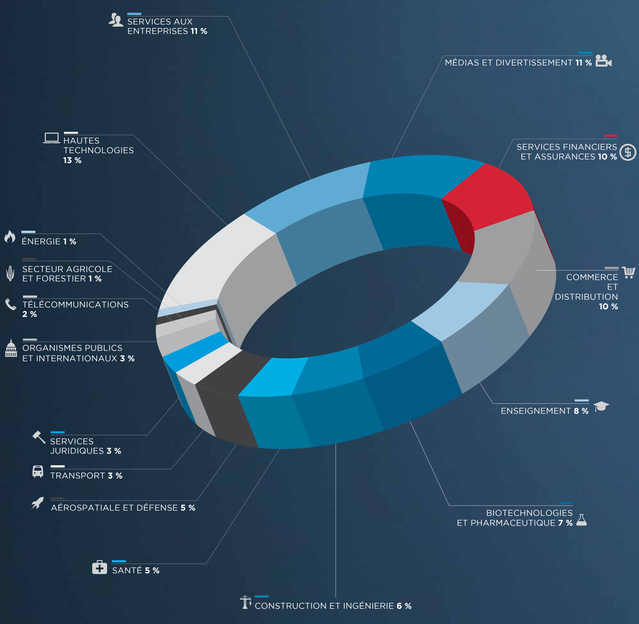
DEUX TENDANCES ANCIENNES QUI PERDURENT :

- Emploi de mécanismes de persistance
- Attaques de fournisseurs de services / sous-traitants pour cibler leurs clients

BILAN DES ATTAQUES EN 2015

SECTEURS D'ACTIVITÉ OÙ MANDIANT A ENQUÊTÉ

Pourcentage du nombre total d'attaques, par secteur



DES ÉVOLUTIONS CONTRASTÉES

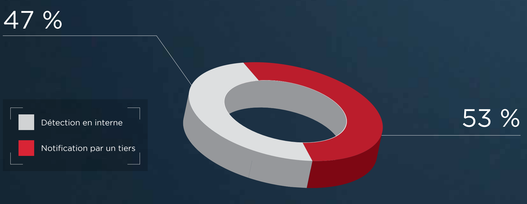
Certains secteurs ont enregistré une hausse des attaques par rapport à 2014 et d'autres, une réduction.

HAUTES TECHNOLOGIES	SERVICES AUX ENTREPRISES
6 % ↑	6 % ↓

PLUS DE COMPROMISSIONS IDENTIFIÉES EN INTERNE

Par rapport à 2014, le nombre d'entreprises qui ont découvert elles-mêmes une compromission a augmenté de 16 %.

16 % ↑



DES ENTREPRISES PLUS VIGILANTES

En 2015, le délai moyen entre la compromission initiale et sa découverte a été réduit de 59 jours (205 jours en 2014).

DÉLAI ENTRE LA COMPROMISSION ET SA DÉCOUVERTE		
MOYENNE	NOTIFICATION PAR UN TIERS	DÉTECTION EN INTERNE
146 JOURS	320 JOURS	56 JOURS

DE NOUVEAUX ENSEIGNEMENTS

Cette année marquée par les attaques par perturbation nous a livré de nouvelles leçons en matière de défense et d'intervention :

1. **Avérez** la compromission effective de votre sécurité.
2. N'oubliez pas que l'attaquant est **un être humain**. Ses réactions peuvent donc être imprévisibles.
3. **Chaque minute compte** : validez et évaluez l'ampleur de la compromission le plus rapidement possible.
4. **Restez concentré** : vous êtes engagé dans une course contre la montre.
5. **Pesez le pour et le contre** avant de communiquer avec l'auteur de l'attaque (voir point 2).
6. Engagez des experts **de manière préventive** pour bénéficier de leur soutien immédiat sur des questions clés (forensique, droit et relations publiques) en cas d'attaque.
7. **Envisagez toutes les éventualités** si une rançon vous est demandée. Vous n'avez aucune garantie de revoir vos données.
8. **Segmentez et contrôlez** efficacement vos sauvegardes.
9. **Une fois l'incident écarté**, concentrez-vous sur un renforcement général de la sécurité.
10. Soyez conscient du fait que **rien n'empêche un pirate expulsé de retenter sa chance**, alors tenez-vous prêt.

EN SAVOIR PLUS Téléchargez le rapport M-Trends 2016 à l'adresse : **fireeye.com/M-Trends-2016.html**

FireEye, France
4, place de la Défense, Paris La Défense Cedex 92974 | +33 1 58 58 01 76 | france@FireEye.com
www.FireEye.fr

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300
www.FireEye.com

FireEye