MANDIANT
A FireEye® Company

M-TRENDS® 2017

Les nouvelles du front

DURÉE D'IMPLANTATION EN RÉGION EMEA

La baisse de la durée d'implantation moyenne dans l'EMEA (469 jours en 2015) s'explique certes par l'augmentation du nombre d'entreprises qui renforcent leur sécurité, mais aussi par une forte recrudescence des attaques visant à être détectées rapidement, à l'image des ransomwares et des attaques d'effacement de données.

PRINCIPAUX SECTEURS DE LA RÉGION EMEA EXPOSÉS AUX CYBERMENACES

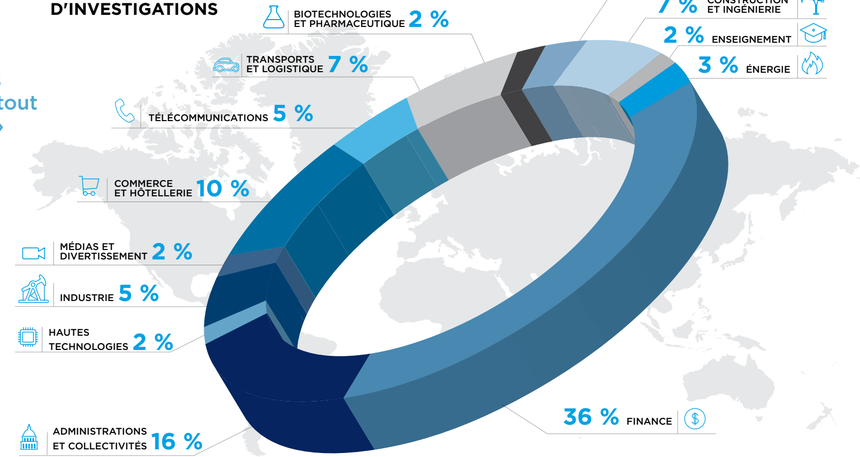
SECTEUR	CIBLE
ÉNERGIE	• Exploration et production pétrolière et gazière • Technologies des énergies propres Systèmes de contrôle industriel
ADMINISTRATIONS ET COLLECTIVITÉS	• Ministères des Affaires étrangères et de la Défense • Opérations internationales • Alliances militaires
SERVICES FINANCIERS	• Banques de détail • Banques d'investissement • Fonds souverains • Identifiants • Données PCI et informations d'identification personnelle
TÉLÉCOMMUNICATIONS	• Opérateurs de réseau cellulaire et mobile • Fournisseurs de services informatiques • Équipements de télécommunications • Opérateurs de satellites

ADAPTATION DES GRANDS PRINCIPES DE DÉFENSE

1 IDENTIFICATION DES ÉLÉMENTS CRITIQUES	2 VISIBILITÉ SUR LE RÉSEAU ET LES TERMINAUX	3 SEGMENTATION RÉSEAU	4 GESTION DES ACCÈS
Identifiez les systèmes internes et les flux de données indispensables à la continuité des activités.	Les frontières du périmètre réseau s'estompent. Il est donc plus essentiel que jamais de surveiller le réseau, les terminaux mobiles, les points de connexion des fournisseurs, les filiales et d'autres interconnexions.	Pourtant essentielle, la segmentation est souvent négligée, ce qui facilite la propagation latérale des attaquants.	Activez l'authentification multifacteur, cloisonnez l'accès par fonction et appliquez le principe du droit d'accès minimal pour limiter la capacité d'un attaquant à accéder aux données à l'aide d'un seul compte compromis.

« La frontière entre certaines attaques financières et les attaques d'acteurs étatiques n'existe tout simplement plus. »

TOTAL DES SECTEURS AYANT FAIT L'OBJET D'INVESTIGATIONS



TENDANCES EN MATIÈRE D'ATTAQUES DANS LE MONDE

Les attaques aux motivations d'ordre financier sont de plus en plus sophistiquées.

L'e-mail est une cible de prédilection. Les attaquants font appel à des méthodes ingénieuses pour parvenir à leurs fins.

Les attaques sont personnalisées. Les auteurs d'attaques à caractère financier personnalisent leurs e-mails de phishing et vont même jusqu'à appeler les victimes pour les « aider ».

TENDANCES EN MATIÈRE D'ATTAQUES DANS L'EMEA

VULNÉRABILITÉ DES INFORMATIONS D'IDENTIFICATION PERSONNELLE

Plusieurs violations de sécurité graves ont compromis la confidentialité d'informations personnelles — documents juridiques, informations de contact, données financières, etc. Ces fuites ont révélé combien il était capital pour les entreprises de toutes tailles de sécuriser la moindre information sur leurs clients.

DES GROUPES DE CYBERPIRATES RUSSES INFLUENCENT LES ÉLECTIONS ET CIBLENT DES RESPONSABLES POLITIQUES ÉTRANGERS

L'Allemagne a annoncé que deux partis politiques avaient été piratés en 2016, sans doute en prélude à d'autres opérations russes visant à influencer les élections dans plusieurs pays de l'Union.

LA CRIMINALITÉ FINANCIÈRE EN HAUSSE

Les établissements financiers au dispositif de sécurité moins abouti représentent une cible plus facile pour des cybercriminels rompus aux compromissions de grands groupes parmi les mieux sécurisés au monde et exploitant les systèmes de messagerie financière vulnérables de la région.

Envie de lire le rapport M-Trends 2017 dans son intégralité ? Lire le rapport complet ici

EN SAVOIR PLUS www.fireeye.com/mtrends

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 | info@fireeye.com | www.FireEye.com

FireEye