LA RÈGLE DE TROIS DES ATTAQUES PAR E-MAIL : TACTIQUES, TECHNIQUES ET CIBLAGE

Chaque jour, les attaquants changent de techniques, de tactiques et de ciblages pour contourner les dispositifs de sécurité des systèmes de messagerie. Fruit de l'analyse de plus de 2,2 milliards d'e-mails échangés entre avril et juin 2019, les données et tendances illustrées dans cette infographie vous aideront à mieux vous préparer aux attaques.

TACTIQUES | LE MODE OPÉRATOIRE DES ATTAQUANTS

Les attaques par e-mail ont considérablement augmenté ces dernières années.

86 %
des attaques par e-mail sont sans malware

14 %
contiennent des malwares

Sans malware = attaques par usurpation, arnaques au président, spear-phishing

L'ART DU TIMING : LES ATTAQUES PAR USURPATION D'IDENTITÉ
(aussi connues sous le nom de compromission de messageries professionnelles (BEC) ou d'arnaque au président)

Les arnaques au président restent un gros problème

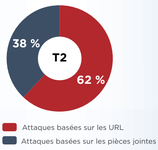
Les attaques sont plus fréquentes en semaine

Pics d'attaques les jeudis et vendredis, surtout en fin de mois

URL : PREMIER VECTEUR D'ATTAQUE

167 %
Augmentation du pourcentage de contenu malveillant hébergé sur des URL HTTPS entre T2 2018 et T2 2019

Blogger™
Utilisé par les attaquants pour donner un air de légitimité à des URL malveillantes



ATTAQUES DE PHISHING : LES UTILISATEURS MICROSOFT EN DANGER

181 %
Augmentation des attaques de phishing usurpant la marque Microsoft entre T1 et T2 2019

68 %
Proportion d'attaques de phishing qui détournent la marque Microsoft

SERVICES CLOUD DÉTOURNÉS DANS LE CADRE D'ATTAQUES DE PHISHING

- Technologies Microsoft grand public
  - Service Office 365 sur le cloud
  - Plateforme et services cloud Microsoft Azure (azurewebsites.net[1], core.windows.net[2], etc.)
- Plateformes d'hébergement de sites web (wixsite.com[3], 000webhostapp.com[4], etc.)
- Liens de prévisualisation de fichiers stockés sur des plateformes de partage comme OneDrive, Dropbox, Box, etc.
- Redirections d'URL de phishing via des plateformes d'e-mailing (SendGrid, MailChimp, etc.)

TECHNIQUES | LES ATTAQUANTS BROUILLENT LES PISTES

Voici un petit aperçu des stratagèmes utilisés pour contourner les systèmes de détection censés bloquer les pièces jointes et les URL malveillantes :

Les attaquants continuent d'utiliser des techniques d'usurpation pour envoyer des e-mails plus vrais que nature

Augmentation du nombre de contournements du captcha dans les attaques de phishing et par macros

Hébergement de contenu malveillant accessible via des identifiants légitimes sur Sharepoint

Utilisation de multiples URL pour masquer le lien malveillant

Techniques de phishing par imbrication d'e-mails avec des pièces jointes msg contenant des URL de phishing

CIBLAGE | LES OBJECTIFS DES ATTAQUANTS

Argent et information

Secteurs les plus visés.

Secteur	Position en T1	Position en T2
Services financiers	1	1
Médias / Divertissement / Hôtellerie	2	2
Industrie	3	3
Fournisseurs de services	4	4
Télécoms	5	5
Collectivités: locales et territoriales	6	6
Services / Conseil	7	7
Assurances	8	8

Plus d'informations sur les évolutions des menaces par e-mail sur **https://www.fireeye.fr/solutions/ex-email-security-products/power-of-one.html**