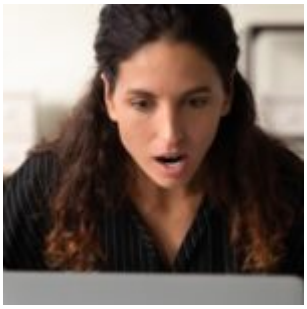
Attention aux pièces jointes HTML malveillantes



Alors que les cyberattaquants multiplient leurs actions et rivalisent d'imagination pour piéger leurs victimes, le groupe Barracuda s'est penché spécifiquement sur les pièces jointes insérées dans les mails pour connaître leur nocivité. Premier constat : 21 % de toutes les pièces jointes HTML analysées étaient malveillantes. Ce type de pièces jointes est souvent utilisé dans les courriers électroniques, notamment dans les rapports générés par le système et qui incluent des liens URL vers le rapport proprement dit. Les attaquants insèrent des pièces jointes HTML frauduleuses dans des e-mails déguisés en rapports hebdomadaires, ce qui incite les utilisateurs à cliquer sur des liens de phishing (hameçonnage).

Des attaques difficiles à détecter

Une fois ouvert, le fichier HTML redirige en effet l'utilisateur vers une machine tierce qui lui demande de saisir ses informations d'identification pour accéder à ses données ou télécharger un fichier pouvant contenir un logiciel malveillant. Ces attaques sont difficiles à détecter car elles n'incluent pas elles-mêmes des logiciels malveillants et utilisent de multiples redirections. En principe, les systèmes de protection des messageries analysent les pièces jointes HTML et peuvent les bloquer. Mais pour limiter les risques, les utilisateurs doivent se méfier des pièces jointes HTML provenant de sources qu'ils n'ont jamais vues auparavant.