Akamai

RAPPORT

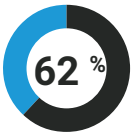
Les petites et moyennes entreprises sont confrontées à de grandes menaces

Introduction

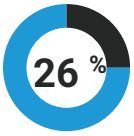
Les cyberattaques contre les grandes entreprises font la une des journaux, mais les petites et moyennes entreprises (PME) sont de plus en plus exposées aux mêmes risques de cybersécurité que les grandes entreprises. Les pirates attaquent actuellement bien souvent sans discriminer, motivés uniquement par l'appât du gain. Ils ne se soucient pas de la taille d'une entreprise s'ils peuvent gagner de l'argent. Les pirates utilisent différentes méthodes pour cibler les employés et leurs terminaux, y compris les terminaux connectés intelligents largement utilisés. Les fournisseurs d'accès à Internet sont bien placés pour aider les PME à se défendre.

Ce bref document décrit certaines des menaces les plus courantes auxquelles les PME sont exposées et leur impact.

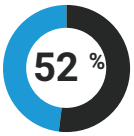
L'enquête Technology and Small Business Survey publiée par la National Small Business Association a mis en évidence un certain nombre de statistiques intéressantes :



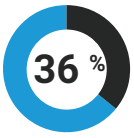
62 % des propriétaires de petites entreprises ont déclaré que la cybersécurité était une préoccupation très importante, 33 % ont déclaré qu'elle était quelque peu importante et seuls 5 % ont déclaré qu'elle n'était pas importante du tout



Seuls 26 % des propriétaires d'entreprise ont déclaré comprendre comment gérer les problèmes de cybersécurité



52 % se disent très préoccupés par la possibilité d'une cyberattaque contre leur entreprise et 44 % quelque peu préoccupés, tandis que 35 % déclarent avoir été victimes d'une cyberattaque



36 % ont déclaré que des informations avaient été faussement envoyées depuis leur domaine ou leur adresse e-mail, 5 % ont déclaré que des informations sensibles avaient été volées, 4 % ont déclaré que des pirates avaient accédé à leurs comptes bancaires et 52 % ont signalé une attaque ayant causé une interruption de service

Aujourd'hui, les menaces Web peuvent être classées en deux grandes catégories : les programmes malveillants et l'hameçonnage. Les botnets sont un sous-ensemble important de programmes malveillants qui méritent une attention particulière.

Les programmes malveillants sont des logiciels sournoisement installés sur les terminaux. Les sites Web compromis peuvent tirer parti de défauts logiciels sur un terminal pour charger des programmes malveillants. Les utilisateurs peuvent également être incités à consulter un site Web malveillant et à cliquer pour charger un fichier malveillant. Certains programmes malveillants peuvent s'activer sur un terminal, puis se propager par eux-mêmes à travers un réseau. Il existe de nombreux types de programmes malveillants qui ciblent les entreprises :

Les mineurs de cryptomonnaie sont des programmes qui utilisent la puissance de traitement d'un terminal sans le consentement de la victime. Les ressources des PME sont ainsi compromises. Ces attaques peuvent être difficiles à détecter, car elles ne contraignent pas les propriétaires des terminaux à payer de l'argent, contrairement aux ransomwares.

Les programmes malveillants spécialisés chargés sur les terminaux de points de vente enregistrent les données des cartes de crédit et les envoient à un pirate, exposant ainsi des chefs d'entreprise.

Les menaces avancées persistantes (APT) accèdent aux réseaux et collectent et extraient des données précieuses. Les APT sont conçues pour être extrêmement discrètes afin de rester actives pendant de longues périodes. Les PME peuvent perdre des données précieuses, ou pire encore, la confiance de leurs clients. Elles peuvent également être soumises à des mesures réglementaires si des données personnelles sont exposées.

Les ransomwares bloquent l'accès à des fichiers en cryptant tout ce qui se trouve sur un terminal ou un serveur. Les pirates proposent alors la clé de déchiffrement contre une somme importante, en encaissant les fonds sans même envoyer la clé dans certains cas. Dans le meilleur des cas, les PME perdent les fonds de la rançon. Dans le pire des cas, elles perdent les fonds *et* des données stratégiques.

Les programmes malveillants peuvent ainsi recueillir des données précieuses de plusieurs manières. **Les logiciels espions** recherchent des données telles que les identifiants de connexion et les données financières et envoient des rapports aux pirates. Les programmes malveillants **d'exfiltration de données** sont spécialement conçus pour localiser, identifier et extraire des données précieuses des ordinateurs. **Les keyloggers** enregistrent les touches utilisées et

peuvent être formés pour permettre aux pirates d'accéder à des comptes financiers, des identifiants de réseaux sociaux ou à d'autres informations précieuses. **Les chevaux de Troie bancaires** surveillent le comportement des utilisateurs pour apprendre les identifiants de connexion et/ou usurpent l'identité des sites bancaires pour voler de l'argent.

Les botnets sont des réseaux de terminaux infectés par le même programme malveillant contrôlés via un canal central (appelé commande et contrôle [C2]) par un seul groupe ou pirate. Les botnets sont souvent disponibles à la location et la plupart peuvent exécuter de nombreuses fonctions différentes, comme celles décrites ci-dessus, pour générer de l'argent.

L'hameçonnage utilise la tromperie, en particulier l'ingénierie sociale, pour inciter les victimes à divulguer des informations qu'un pirate peut monétiser. Par le passé, les attaques par hameçonnage incitaient les utilisateurs à cliquer sur des liens dans des courriers indésirables non sollicités et à divulguer des informations sensibles. Les développeurs d'attaques par hameçonnage ont considérablement diversifié leurs efforts ; ils intègrent désormais également des URL d'hameçonnage dans les publications ou commentaires de réseaux sociaux, ainsi que dans les SMS, sur Skype, Messenger ou dans d'autres services.

Les terminaux mobiles sont des cibles de premier plan pour l'hameçonnage, avec de petits écrans et des utilisateurs qui font plusieurs choses en même temps et peuvent passer à côté d'indices subtils indiquant qu'un lien est malveillant. Pour encore mieux faire passer leur leurre, les experts de l'hameçonnage utilisent des caractères ambigus provenant de différents jeux de caractères pour imiter des noms de domaine légitimes.

Voici quelques exemples réels de chaînes de caractères utilisées :

7eleven.com

Adîdas.com

adidas.com

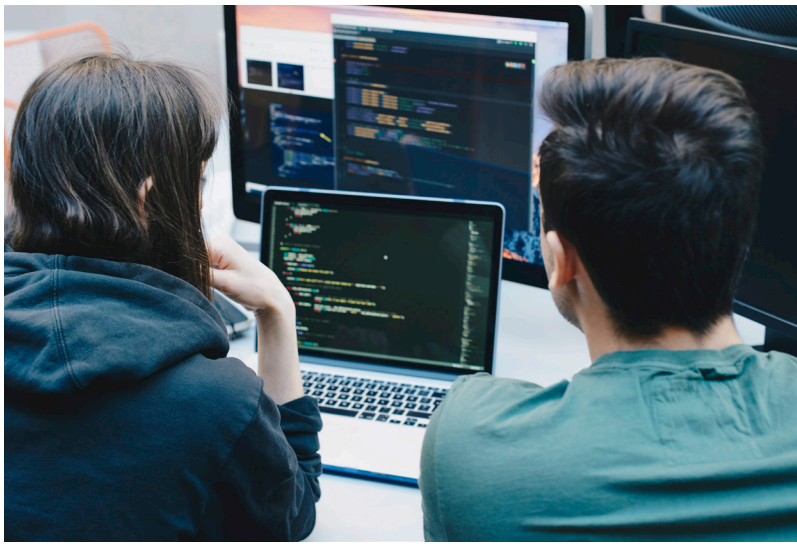
philippineairlines.com

rolex.com

singaporeair.com

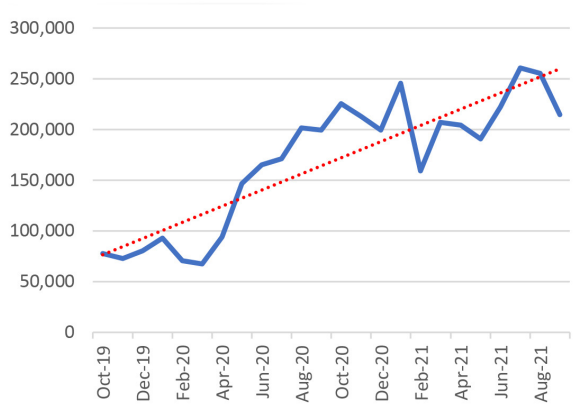
thaiairways.com

L'hameçonnage est dernièrement en hausse. D'après le Phishing Activity Trends Report publié par l'Anti-Phishing Working Group au troisième trimestre 2021,



« L'hameçonnage a atteint un record mensuel au troisième trimestre ; les attaques ont doublé depuis la fin 2019. » Le tableau ci-dessous, extrait de ce rapport, illustre cette tendance. En effet, il peut être plus facile de piéger les utilisateurs que d'exploiter des défauts logiciels.

Attaques par hameçonnage, T4 2019 — T3 2021



Les données recueillies par les équipes d'Akamai de recherche sur la sécurité des opérateurs et des entreprises montrent également que la durée de vie des noms de domaine utilisés pour l'hameçonnage diminue, la médiane passant à environ 1,5 heure en mars 2019. Cela a des conséquences directes sur la protection : les défenses doivent être aussi agiles que les attaques.

Conclusion

Cette liste de menaces Web n'est pas exhaustive. Les pirates évaluent constamment la viabilité de leurs attaques et innovent pour optimiser leur rendement, en changeant la forme et le mode opératoire de leurs attaques. Il existe également d'autres types de programmes malveillants constituant une distraction ou une nuisance plus qu'autre chose, en affichant des publicités ou du contenu indésirables.

Les PME doivent se protéger contre les menaces Web à l'aide de solutions compatibles avec leurs besoins et contraintes uniques. Akamai propose des services Secure Internet Access conçus pour les PME. Ils protègent les PME des types d'attaques décrits dans ce document sans leur imposer de charge de gestion. Chaque terminal et chaque personne sur le lieu de travail, y compris les invités, est automatiquement protégé. Les responsables d'entreprise disposent d'un simple portail graphique leur permettant de voir instantanément ce qui se passe sur leur réseau et quelles menaces ont été repoussées.

Les services Secure Internet Access d'Akamai sont spécialement conçus pour aider les FAI à :

- générer des revenus grâce à une sécurité de niveau professionnel pour les PME
- aller au-delà de la vitesse et de la fiabilité et offrir des services pour PME qui se distinguent par leur sécurité
- réduire les obstacles au déploiement, réduire les coûts et simplifier la prestation de services grâce à une version cloud des services Secure Internet Access

Le service peut être entièrement personnalisé avec un aspect et une apparence conformes à la marque, et l'ensemble de fonctionnalités et les renseignements sur les menaces peuvent également être adaptés aux exigences du marché local.

Toute personne. Tout terminal. À tout moment. Akamai peut vous aider.

Contactez Akamai pour en savoir plus.

Akamai soutient et protège la vie en ligne. Les entreprises leaders du monde entier choisissent Akamai pour concevoir, diffuser et sécuriser leurs expériences digitales, et aident des milliards de personnes à vivre, travailler et jouer chaque jour. Grâce à la plateforme de traitement la plus distribuée au monde, du cloud à la bordure de l'Internet, nos clients peuvent facilement développer et exécuter des applications, tandis que nous plaçons les expériences au plus près des utilisateurs et éloignons les menaces. Pour en savoir plus sur les solutions de sécurité, de traitement et de diffusion d'Akamai, consultez akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur Twitter et LinkedIn. Publication : 06/22.