
netskope
Cloud and Threat Report :
les tendances mondiales en matière de malware cloud et web
DONNÉES FOURNIES PAR
netskope
THREAT LABS

SYNTHÈSE

Dans cette édition du Cloud and Threat Report, nous étudions les téléchargements de malware depuis le Cloud et le web au cours des douze derniers mois. Les chevaux de Troie représentent la grande majorité des téléchargements de malware, grâce aux hackers qui, outre différentes familles de chevaux de Troie, utilisent des techniques d'ingénierie sociale pour cibler leurs victimes. La plupart des téléchargements de malware provenaient de fichiers Windows EXE/DLL ou de documents Microsoft Office, car les hackers continuent de cibler Microsoft Windows, qui reste le système d'exploitation le plus répandu au sein des entreprises.

Nous avons également étudié les sources des téléchargements de malwares : 53 % proviennent de sites web traditionnels et 47 % d'applications cloud. Les téléchargements de malware sur le web sont issus de sites internet de différentes catégories, notamment des sites liés à la technologie et des serveurs de contenu. Les téléchargements malware depuis le Cloud viennent de centaines d'applications différentes, avec en tête les applis de stockage cloud les plus populaires. Ils proviennent généralement de serveurs situés dans les régions où se trouvent leurs victimes.

Enfin, en examinant les sources les plus populaires pour les téléchargements de malwares, nous comprenons mieux certaines des techniques utilisées par les hackers. Les moteurs de recherche sont les principaux référents : les hackers utilisent des techniques de référencement SEO populaires pour se placer dans le haut des résultats de recherches. Les imitations compromises et malveillantes de sites web inoffensifs sont elles aussi des sources populaires pour le téléchargement de malwares.

ÉLÉMENTS CLÉS DU RAPPORT

- **Les chevaux de Troie représentent 77 % de tous des téléchargements cloud et web de malware.** Ils sont utilisés pour s'implanter et diffuser toute une variété de payloads en phases successives, comme des backdoors, des infostealers, ou encore des rançongiciels.
- **47 % des téléchargements de malware proviennent d'applications cloud,** contre 53 % pour les sites web traditionnels, sachant que les hackers continuent d'utiliser un mix cloud et web pour cibler leurs victimes.
- **Les cas de phishing par téléchargement sont en hausse du fait que les hackers utilisent des techniques de référencement SEO** pour faire remonter des fichiers PDF malveillants dans les résultats des moteurs de recherche populaires, comme Google et Bing.
- **Les fichiers EXE et DLL représentent près de la moitié des téléchargements de malware :** les hackers continuent de cibler Microsoft Windows, tandis que les fichiers Microsoft Office malveillants sont en baisse et ont retrouvé leur niveau pre-Emotet.
- **La plupart des téléchargements de malware viennent de serveurs situés dans les mêmes régions que leurs victimes,** car les hackers implantent leur malware dans le monde entier pour échapper aux géobarrières.

À PROPOS DE CE RAPPORT

Netskope offre à des millions d'utilisateurs dans le monde entier une protection des données et contre les menaces. Les informations présentées dans ce rapport se basent sur des données d'utilisation anonymes collectées par la plateforme Security Cloud de Netskope sur un panel de clients Netskope avec leur autorisation préalable. Ce rapport contient des informations sur les détections repérées par le Next Gen Secure Web Gateway (Next Gen SWG) de Netskope, sans tenir compte de l'importance de l'impact de chaque menace individuelle. Les statistiques de ce rapport concernent les douze derniers mois, du 1er avril 2021 au 31 mars 2022.

Netskope Threat Labs

Composé des meilleurs spécialistes en matière de menaces cloud et de malware, le Netskope Threat Labs repère, analyse et conçoit des moyens de défense contre les dernières menaces cloud et data qui touchent les entreprises. Nos spécialistes présentent régulièrement leurs découvertes dans les conférences sur la sécurité les plus prestigieuses comme la DefCon, la BlackHat, et la RSA.

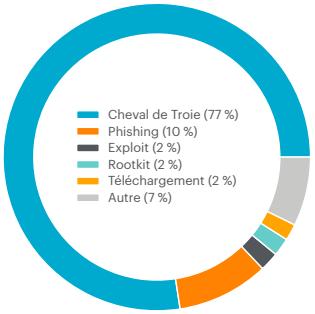
TÉLÉCHARGEMENTS DE MALWARE

Catégories et familles de malware

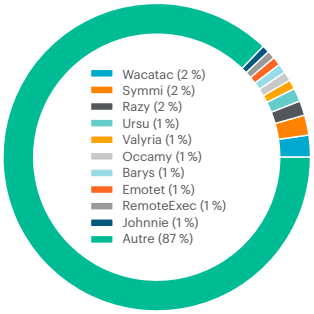
Les chevaux de Troie représentent la majorité (77 %) des téléchargements de malware web et cloud. Ils représentent la première étape d'une cyberattaque, dont le but pour le hacker est de tromper sa victime pour qu'elle télécharge et exécute un logiciel qui permettra au hacker de s'introduire. Ils sont souvent déguisés en logiciels légitimes et utilisés pour tirer parti d'événements importants. Par exemple, de nombreux types de chevaux de Troie COVID-19 ont circulé pendant la pandémie. Les hackers utilisent les chevaux de Troie pour s'implanter et diffuser toute une variété de payloads en phases successives, comme des backdoors, des infostealers ou encore des rançongiciels. Si la majorité des téléchargements de logiciels malveillants sont des chevaux de Troie, aucune famille de chevaux de Troie ne domine pourtant à l'échelle mondiale. Les 10 premières familles de chevaux de Troie représentent seulement 13 % de l'ensemble des téléchargements. Les 87 % restants proviennent d'un large ensemble de familles peu connues.

Les chevaux de Troie représentent la majorité des téléchargements de malware dans toutes les régions du monde à l'exception du Moyen-Orient, où l'incidence des exploits est plus élevée que dans les autres régions. Ici, les fichiers malveillants tirent parti d'un bug ou d'une vulnérabilité lorsqu'ils sont ouverts ou exécutés par la victime. Les cas de phishing par téléchargement, également supérieurs à la moyenne au Moyen-Orient, prédominaient en Afrique. Le phishing par téléchargement diffère des sites web de phishing traditionnels. En général, il s'agit de fichiers PDF qui prennent la forme de faux CAPTCHA, de fausses demandes de partage de fichiers ou de fausses factures, et qui font partie d'une campagne de phishing plus large. Les cas de phishing par téléchargement ont augmenté en novembre 2021, quand les hackers ont réussi à les faire lister sur les moteurs de recherche les plus populaires en utilisant des techniques courantes de référencement SEO (Search Engine Optimization).

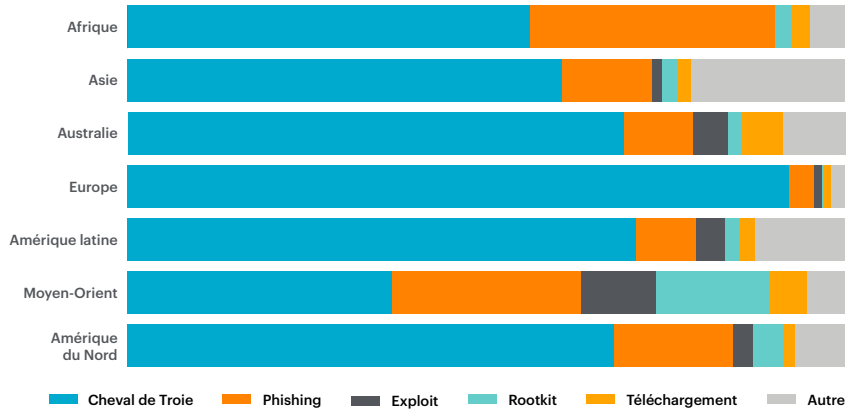
Catégories de malware les plus populaires au cours des 12 derniers mois



Familles de chevaux de Troie les plus répandues au cours des 12 derniers mois

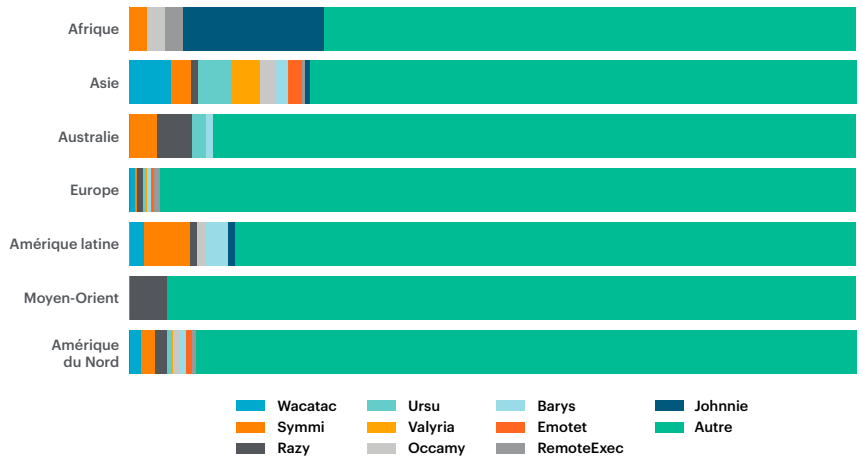


Catégories de malware les plus populaires par région



Les principales familles de chevaux de Troie varient d'une région à l'autre parce que les campagnes de malware ciblent généralement des utilisateurs qui parlent une langue spécifique ou vivent dans un pays donné, ou parce qu'elles sont en lien avec des événements régionaux importants. Certaines familles de chevaux de Troie sortaient du lot dans certaines régions, comme Johnnie en Afrique et Razy au Moyen-Orient. Dans d'autres régions, comme l'Amérique du Nord et l'Asie, la quasi-totalité des familles les plus répandues était présente. En Europe, les familles les plus populaires représentaient un pourcentage plus faible des téléchargements de chevaux de Troie par rapport à toutes les autres régions.

Familles de malware les plus populaires par région

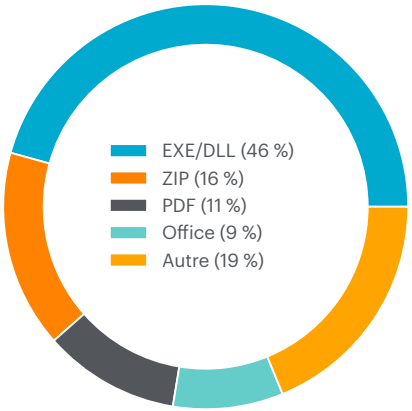


Types de fichiers de malware

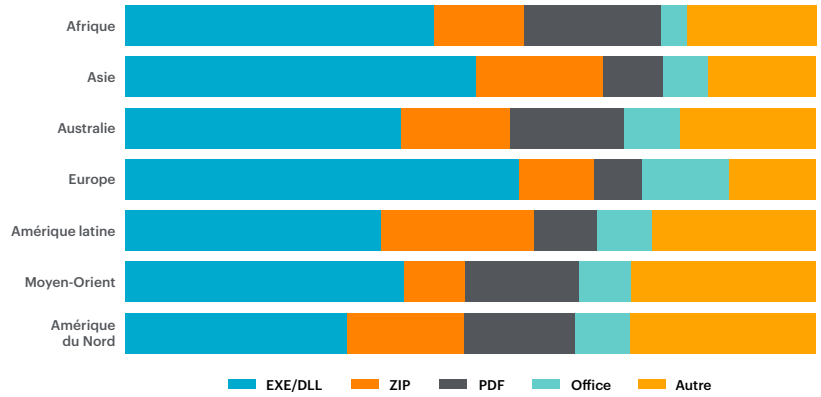
Les fichiers exécutables portables (EXE/DLL), les fichiers Microsoft Office, les fichiers PDF et les fichiers ZIP représentaient 81 % de tous les téléchargements de malware au cours des douze derniers mois. Les documents Office malveillants, qui dominaient davantage en 2020 et début 2021 en raison d'Emotet et de Dridex, sont revenus à leurs niveaux pré-Emotet. Deux changements récents apportés par Microsoft, à savoir le blocage des macros Excel 4.0 et le blocage des macros VBA pour les fichiers téléchargés sur Internet, vont probablement faire baisser davantage ce pourcentage, ce qui obligera les hackers à se tourner vers d'autres stratégies. En plus des PDF de phishing mentionnés plus haut dans ce rapport, les hackers utilisent aussi des PDF malveillants pour rediriger les utilisateurs vers des sites de spams, d'escroquerie et de distribution de malware.

Au niveau régional, on observe peu de variations dans les fréquences propres à chaque type de fichier. Les fichiers EXE/DLL représentent toujours la majorité des téléchargements de malware, suivis par les fichiers PDF, ZIP ou Office. L'Afrique, qui a enregistré le plus fort pourcentage de téléchargements de logiciels malveillants de phishing, a aussi enregistré le plus fort pourcentage de téléchargements de fichiers PDF, ces derniers étant la source de la majorité des téléchargements de malware de phishing.

Fichiers de malware les plus populaires
au cours des 12 derniers mois



Fichiers de malware les plus populaires par région



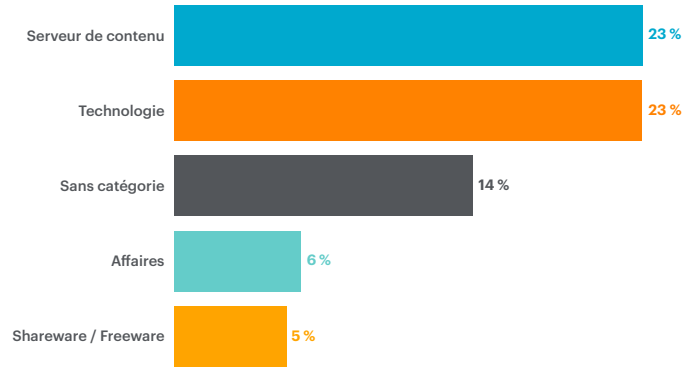
SOURCES DES MALWARES

Téléchargements web de malware

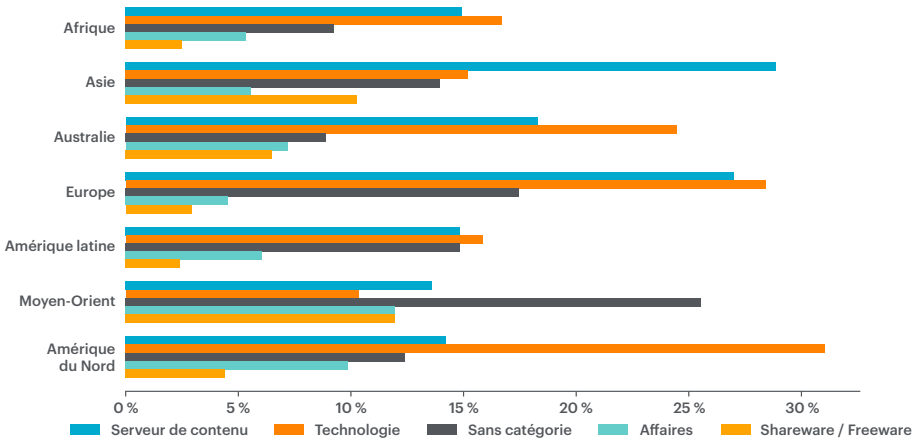
Comparé aux applications cloud, 53 % de tous les téléchargements de malware au cours des douze derniers mois provenaient de sites web traditionnels. Parmi les téléchargements web de malware, certains venaient de sites traditionnellement associés aux malwares. Par exemple, les sites dits « sans catégorie », c'est-à-dire ceux qui ne sont pas assez populaires pour être assignés à une catégorie spécifique, étaient la source de 14 % des téléchargements de malware sur le web. De la même manière, les sites « shareware/freeware », qui distribuent parfois des logiciels groupés avec des logiciels espions et d'autres logiciels malveillants, représentaient 5 % des téléchargements de malware sur le web. Les autres catégories populaires, comme « technologie », « serveur de contenu » et « business », représentent une large part du Web inoffensif et ne peuvent donc pas être facilement filtrées.

Les catégories de sites web les plus populaires pour le téléchargement de malware varient selon les régions. Alors que les sites web dits de « technologie » figuraient en première place dans la plupart des régions, les sites « serveur de contenu » étaient numéro 1 en Asie et les sites « sans catégorie » se trouvaient en tête au Moyen-Orient. En Amérique latine, aucune catégorie ne dominait : les trois premières catégories représentaient chacune environ 15 % de tous les téléchargements de malware.

Catégories web les plus populaires pour le téléchargement de malware au cours des 12 derniers mois

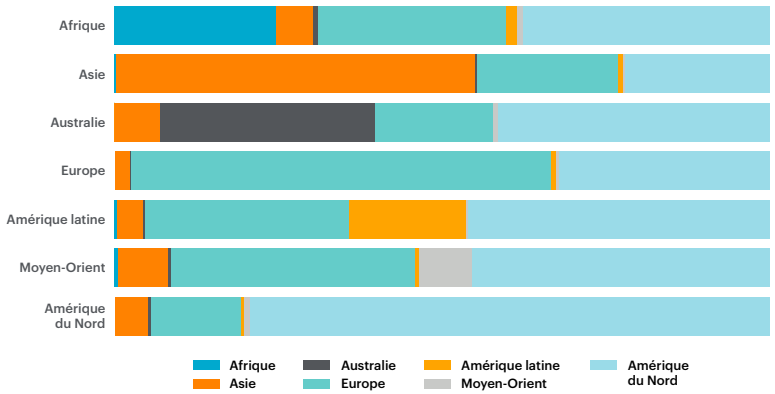


Catégories web les plus populaires pour le téléchargement de malware par région



Les hackers ont également tendance à cibler des victimes situées dans une région spécifique où est hébergé le malware. Dans la plupart des régions, la majorité des téléchargements de malware provenaient de la même région que celle de la victime. C'est particulièrement le cas en Amérique du Nord, où 84 % de tous les téléchargements de malware provenaient de sites web hébergés dans cette même région. À l'inverse, au Moyen-Orient, seulement 7 % des téléchargements de malware proviennent de cette même région, la majorité venant des régions voisines d'Europe et d'Asie. En moyenne, l'Europe était la source de 30 % de tous les téléchargements de malwares toutes régions confondues, contre 42 % pour l'Amérique du Nord.

Région d'origine des téléchargements de malware

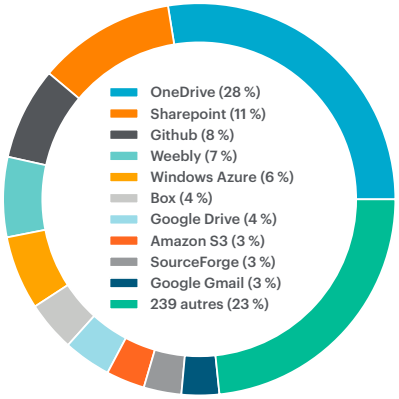


Téléchargements de malware provenant du Cloud

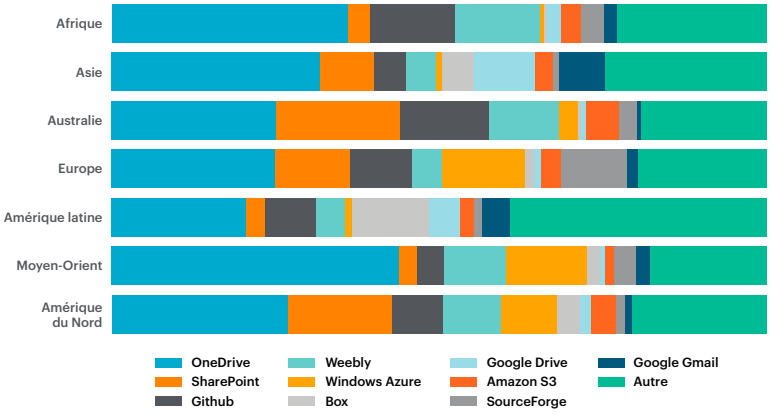
47 % de tous les téléchargements de malware provenaient d'applications cloud plutôt que de sites web traditionnels. Au total, les téléchargements de malware venaient de 257 applications différentes, les dix premières étant à l'origine de 75 % de tous les téléchargements de malware provenant du Cloud. Cela reflète l'activité des hackers et le comportement des utilisateurs : les hackers ont tendance à abuser des applications populaires pour atteindre plus de victimes, et les utilisateurs sont plus susceptibles de télécharger du malware à partir des applications populaires avec lesquelles ils interagissent régulièrement.

Au sein de chaque région, les dix premières applications comptaient pour la majorité des téléchargements de malware provenant du Cloud. Microsoft OneDrive était l'application la plus populaire dans toutes les régions, à des niveaux variables. Certaines applications étaient plus répandues dans certaines régions par rapport à d'autres : Box en Amérique latine, Google Drive en Asie, et Windows Azure Blob Storage au Moyen-Orient. Cela reflète les tactiques des hackers et le comportement des utilisateurs dans chaque région.

Applications les plus populaires pour le téléchargement de malware au cours des 12 derniers mois



Applications les plus populaires pour le téléchargement de malware par région



Origines des téléchargements de malware

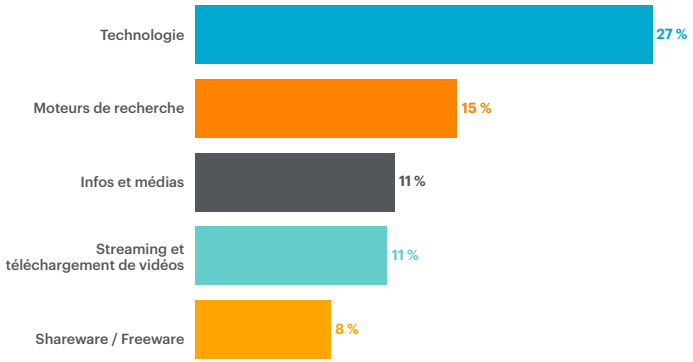
Les téléchargements de malware depuis le Cloud ou le Web ne se font pas spontanément. Pour les chevaux de Troie, les hackers utilisent des techniques d'ingénierie sociale pour tromper leurs victimes et les inciter à télécharger du malware. Les techniques courantes consistent à concevoir des appâts pour tirer parti d'événements majeurs (comme la pandémie de COVID-19), à créer un sentiment d'urgence (comme une facture d'une société de transport à payer) ou à se faire passer pour une application légitime (comme la version gratuite d'un jeu vidéo populaire). Les hackers utilisent aussi des approches techniques comme les exploits logiciels, les téléchargements de type « drive-by » ou la contrebande HTML pour télécharger du malware.

L'en-tête de requête HTTP « referer » donne un aperçu des techniques d'ingénierie sociale utilisées par les hackers pour tromper les utilisateurs et les inciter à télécharger du malware. 14 % des référents étaient issus d'applications cloud contre 86 % pour les sites web traditionnels. Parmi les principaux référents d'applications cloud se trouvaient des applications populaires de stockage, de collaboration et de messagerie — des applications via lesquelles les hackers peuvent envoyer des messages directement à leurs victimes sous de nombreuses formes, comme des e-mails, des messages privés, des commentaires et des partages de documents.

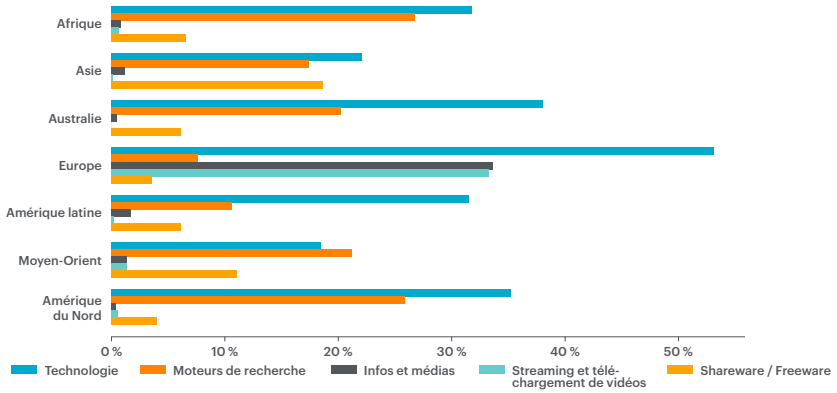
Les principales catégories de référents web contenaient certaines catégories traditionnellement associées au malware, en particulier les sites « shareware/freeware », mais elles étaient dominées par des catégories habituellement considérées comme inoffensives. L'arrivée des « moteurs de recherche » dans cette liste est particulièrement intéressante car elle reflète l'efficacité des techniques de référencement SEO de certains hackers. Les téléchargements de malware référencés par les moteurs de recherche prenaient principalement la forme de fichiers PDF malveillants, dont de nombreux faux CAPTCHA qui redirigeaient les utilisateurs vers des sites de phishing, de spam et d'escroquerie.

Les sites de la catégorie « technologie » étaient en tête des référents de malware dans toutes les régions, mais des différences significatives au sein d'autres catégories ont été identifiées. L'Europe affiche le pourcentage le plus élevé de référents « actualités et médias » et « streaming et téléchargement de vidéos ». C'est en Afrique que dominent les référents « moteur de recherche », et l'Asie a le plus fort pourcentage de référents « shareware/freeware ». Ces différences régionales sont le reflet à la fois des techniques d'ingénierie sociale des hackers et du comportement des utilisateurs.

Catégories de référents les plus populaires pour le téléchargement de malware au cours des 12 derniers mois



Catégories de référents les plus populaires pour le téléchargement de malware par région



RECOMMENDATIONS

Le paysage actuel du malware est dominé par les chevaux de Troie, qui sont diffusés à partir de catégories de sites web et d'applications cloud populaires généralement localisés dans la même région que la victime. Pour atténuer le risque posé par la diffusion de malware sur le Cloud et le Web, Netskope recommande aux entreprises de mettre en œuvre les contrôles suivants :

1. Tout analyser, y compris les voies de circulation des utilisateurs pour le Web, le SaaS managé et non-managé, le shadow IT, le IaaS, et les instances de l'entreprise et personnelles. Éviter de contourner les suites applicatives avec stockage cloud où les téléchargements de malware sont les plus courants. Éviter le contournement ou le blocage par catégorie pour privilégier une approche plus chirurgicale.

2. Déployer une protection multicouche incorporée contre les menaces pour l'ensemble du trafic web et cloud, y compris par l'analyse ML incorporée des fichiers PE (par opposition au sandboxing en arrière-plan), pour pouvoir détecter le malware et l'empêcher d'atteindre les nœuds d'extrémité, et bloquer les communications sortantes du malware.

3. Détecter le malware en arrière-plan via l'analyse pré-exécution, le sandboxing, l'analyse ML, l'émission d'alertes « patient zéro » pour les nouvelles menaces, la rétrospective à l'aide des IOC, et l'analyse MITRE ATT&CK pour une meilleure atténuation des réponses.

4. Tirer parti du Cloud Threat Exchange (CTE) de Netskope pour automatiser le partage bi-directionnel entre les défenses de tout changement au niveau des systèmes de renseignement IOC sur les menaces, gérer la décomposition des IOC et intégrer votre stack sécurité pour le SSE, les nœuds d'extrémité, la sécurité de la messagerie, le SIEM, les XDR et le SOAR.

5. Détecter et interrompre les menaces en bloquant les sites web à risque, et utiliser le RBI pour les sites non catégorisés, les domaines nouvellement enregistrés et les domaines parqués. Utiliser des pare-feux cloud (FWaaS) pour filtrer le trafic de sortie sur tous les ports et protocoles.

6. Réduire les risques liés à vos applications en recommandant des alternatives plus sûres, surveiller et conseiller les utilisateurs pour qu'ils évitent les applications mal notées.

7. Fédérer le SSO/MFA sur vos applications et services cloud, et tirer parti du Zero Trust Network Access (ZTNA) pour les applications et ressources privées. Utiliser l'authentification renforcée dans le cadre de politiques adaptatives basées sur le risque lié à l'application, à l'utilisateur, à l'appareil et à la sensibilité des données, pour appliquer les principes du Zero Trust.

8. Utiliser l'analyse comportementale pour détecter les menaces internes, l'exfiltration de données, les appareils compromis et les informations d'identification compromises dans toutes les voies du trafic utilisateur incorporées, vers les applications privées et vers les applications managées via l'introspection par API.

9. Automatiser les workflows de réponse pour les alertes traitées à l'aide de Netskope Cloud Ticket Orchestrator pour les enquêtes et les réponses, et utiliser le Netskope Cloud Log Shipper pour envoyer les journaux web, cloud et pare-feu vers les XDR, SIEM, et lacs de données.

10. Surveiller en permanence, via l'analyse, les mouvements de données inconnus, les anomalies de comportement, les risques liés aux applications, la duplication des applications, les profils d'initiés et les utilisateurs à risque, et être attentifs aux tableaux de bord courants, y compris votre évaluation des risques liés au Cloud.

EN SAVOIR PLUS

Pour plus d'informations sur les menaces cloud et les dernières découvertes du Netskope Threat Labs, rendez-vous sur **NETSKOPE.COM/FR/NETSKOPE-THREAT-LABS**

Pour plus d'informations sur les méthodes d'atténuation des risques, contactez-nous dès aujourd'hui : **WWW.NETSKOPE.COM/FR/REQUEST-DEMO**

DONNÉES FOURNIES PAR

netskope
THREAT LABS