elastic security labs

Rapport 2022 sur les menaces mondiales

Infographie

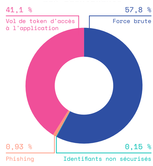
D'où viennent les menaces ?

Le rapport 2022 d'Elastic Security Labs sur les menaces mondiales se base sur des données télémétriques et révèle les phénomènes, les tendances et les recommandations en matière de menaces pour aider les entreprises à se préparer pour l'avenir. En voici les conclusions…

La sécurité du cloud est optimale lorsque les administrateurs ajoutent manuellement des contrôles supplémentaires aux paramètres par défaut

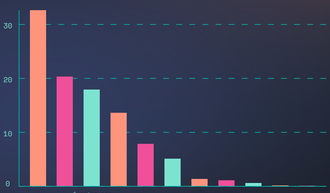
Près de 41 % des alertes liées aux accès protégés par des identifiants concernaient des tentatives de vol des tokens d'accès aux applications plutôt que d'autres éléments justificatifs d'identité.

Techniques d'accès aux identifiants



Pourcentages par techniques MITRE ATT&CK utilisant l'accès aux identifiants

Lorsque les pirates se sont introduits dans votre système, leur priorité est de récupérer des identifiants.



Pourcentages par noms de tactique MITRE ATT&CK pour les alertes de détection basées sur le cloud

Les logiciels commerciaux se transforment en armes

Des malwares conçus pour des simulations d'attaques sont utilisés contre les organisations.

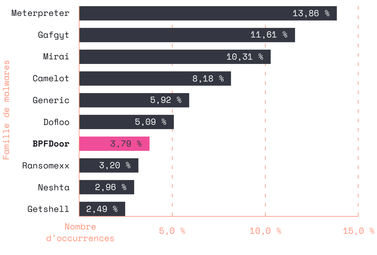
CobaltStrike était la charge utile ou le fichier binaire ciblant le plus largement des points de terminaison Windows à des fins malveillantes, suivi de AgentTesla et RedLineStealer.

Toutes les détections

- CobaltStrike..... 35 %
- AgentTesla..... 25 %
- RedLineStealer..... 10 %

Un logiciel ouvert n'est pas aussi sécurisé que ce que vous pensez

Top 10 des malwares/charges utiles **sur Linux**

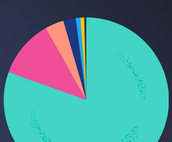


Top 10 des malwares et des charges utiles sur Linux présentant une augmentation de l'activité BPFDoor

Les chevaux de Troie continuent à être la méthode privilégiée pour transformer les livrables en armes

Malwares par catégorie

- Cheval de Troie... 80,5 %
- Mineur de cryptomonnaie..... 11,3 %
- Ransomware..... 3,7 %
- Packer..... 2,4 %
- Porte dérobée..... 0,9 %
- Proxy..... 0,7 %
- Autres..... 0,5 %



Bonne nouvelle : la sécurité aux points de terminaison fonctionne !

Les attaques aux points de terminaison se diversifient pour tenter de contourner les défenses en place. Cette année, nous avons observé 50 techniques d'infiltration aux points de terminaison, qui se sont toutes soldées par un échec.

Technique	Pourcentage de signaux
Masquage	44,29 %
Exécution de proxy binaire	30,00 %
Manipulation des tokens d'accès	12,32 %
Injection de processus	7,02 %
Tâches BITS	4,74 %
Exécution de proxy d'utilitaires de développeur approuvés	0,90 %
Traitement de scripts XSL	0,66 %
Dégradation de défenses	0,65 %
Exploitation de l'évasion par la défense	0,64 %
Exécution système de proxy de script	0,13 %
Modification de registre	0,03 %
Suppression d'indicateur sur l'hôte	0,01 %

Obtenez des informations complètes sur les conclusions des chercheurs d'Elastic Security Labs dans le rapport 2022 sur les menaces mondiales