2025

elastic security labs

RAPPORT DE RECHERCHE SUR LES MENACES MONDIALES

PRÉSENTATION

L'ère des attaques patientes et furtives cède la place à une nouvelle ère de menaces à grande vitesse.

Notre analyse comparative d'une année sur l'autre révèle un changement stratégique clair : les attaquants se réorganisent pour gagner en rapidité, exploitent l'IA pour générer de nouvelles menaces à grande échelle et privilégient l'exécution immédiate plutôt que la furtivité prolongée. Cette accélération oblige les défenseurs à s'adapter à un cycle de vie des attaques qui se mesure en minutes et non plus en mois, où la prise de décisions rapides et contextualisées, fondées à la fois sur des données en temps réel et historiques, est devenue la clé d'une défense efficace.

Le rapport 2025 d'Elastic sur les menaces mondiales publié par Elastic Security Labs analyse ce nouvel environnement.

Sur la base de notre analyse de la télémétrie des menaces mondiales, nous avons identifié les comportements des attaquants et les innovations défensives les plus importantes. Voici un aperçu de ce que vous apprendrez :

#01

Les priorités des pirates sur Windows ont changé

La catégorie tactique **Exécution** représente désormais **32,1 %** des comportements malveillants, soit le double de sa part précédente d'environ 16 %, et dépasse **l'évasion par la défense** en tant que meilleure tactique. Cela rompt avec une tendance observée depuis trois ans et indique un changement stratégique vers le déploiement immédiat de la charge utile plutôt que la furtivité initiale.

2025 **32,1 %**

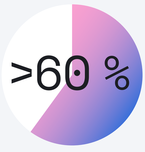
2024 ~16 %

CE QUE CELA SIGNIFIE POUR VOUS

→ Les pirates informatiques n'attendent plus pour se dissimuler ; ils s'efforcent d'exécuter immédiatement un code malveillant dès leur intrusion. La protection de la mémoire d'exécution et la prévention des accès initiaux sont donc plus cruciales que jamais.

#02

La surface d'attaque du cloud est très concentrée



Plus de 60 % de tous les événements de sécurité dans le cloud se résument à seulement trois objectifs adverses :

des objectifs des pirates

/Accès initial
/Persistance
/Accès aux identifiants

CE QUE CELA SIGNIFIE POUR VOUS

→ Sur toutes les principales plateformes cloud, cette attention particulière portée aux **attaques basées sur l'identité** indique clairement que le renforcement des flux d'authentification et la surveillance des accès privilégiés anormaux constituent les moyens les plus efficaces de protéger vos charges de travail dans le cloud.

#03

L'utilisation de l'IA comme une arme est en hausse

+15,5 %

Nous avons constaté une **augmentation de 15,5 % des menaces « génériques »**, une tendance probablement alimentée par les pirates utilisant les LLM pour générer rapidement des chargeurs et outils malveillants simples mais efficaces.

CE QUE CELA SIGNIFIE POUR VOUS

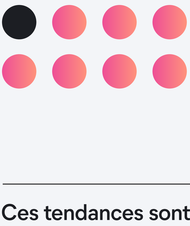
→ La multiplication du nombre de menaces générées par l'IA augmente considérablement le volume et la diversité des logiciels malveillants auxquels vous êtes confronté. Il est donc nécessaire de moins s'appuyer sur les signatures statiques et davantage **sur l'analyse comportementale et la détection basée sur l'IA** pour identifier et bloquer automatiquement le flux de nouvelles menaces à grande échelle.

#04

Le vol d'identifiants de navigateur est une activité florissante

>1 sur 8

conçu pour voler les données du navigateur



Notre analyse de plus de **150 000 échantillons de logiciels malveillants** a révélé que **plus d'un sur huit étaient conçus pour voler les données de navigation**. Il ne s'agit pas d'un usage isolé ; ces identifiants constituent la matière première qui alimente le **marché des brokers d'accès**, fournissant un approvisionnement constant de clés permettant à d'autres pirates de compromettre les comptes cloud des entreprises.

CE QUE CELA SIGNIFIE POUR VOUS

→ Le navigateur constitue une zone de guerre pour les données les plus sensibles de votre organisation. Les voleurs d'informations se sont adaptés aux protections intégrées des navigateurs, ce qui signifie que les contrôles d'identité traditionnels ne suffisent plus.

Ces tendances sont profondément interconnectées.

Des pirates peuvent utiliser un logiciel malveillant généré par l'IA pour voler les identifiants du navigateur, qui sont ensuite utilisés pour obtenir un accès initial à un compte cloud. Une fois à l'intérieur, ils se concentrent immédiatement sur l'exécution pour déployer un ransomware ou voler des données. Ce rapport établit des liens, démontrant comment ces TTP constituent la chaîne d'attaque moderne et, plus important encore, comment la neutraliser à plusieurs niveaux.

Certes, les menaces sont complexes, mais en comprenant le fonctionnement des logiciels malveillants et des menaces et en mettant en place des défenses avancées, les entreprises peuvent considérablement améliorer leur résilience.

ÉTAPE N° 1
se concentrer sur l'exécution

ÉTAPE N° 2
obtenir un accès initial à un compte cloud

ÉTAPE N° 3
utiliser des logiciels malveillants générés par l'IA

ÉTAPE N° 4
voler les identifiants du navigateur

Elastic Security fournit les informations partagées, les fonctionnalités avancées et les connaissances dont vous avez besoin pour faire face aux menaces actuelles et construire un avenir plus sûr.