Les principales menaces de cybersécurité à surveiller en 2026

Les menaces les plus dangereuses ne sont pas toujours les plus bruyantes, mais plutôt celles qui se fondent dans le décor et exploitent les canaux de confiance dans les systèmes. Les adversaires apprennent à déjouer les contrôles les plus stricts et misent de plus en plus sur l'IA. Résultat : des modèles d'attaque qui progressent bien plus vite que les défenses des organisations.

Ingénierie sociale à grande échelle

L'IA générative ouvre la porte à des campagnes de phishing, de vishing et d'usurpation d'identité hautement personnalisées, et donc de plus en plus difficiles à détecter pour les utilisateurs (et les filtres).

- Deepfakes de dirigeants et de fournisseurs
- Appâts contextualisés et entraînés sur des données publiques
- Automatisation des tests et de l'optimisation des campagnes

Pourquoi c'est important : aujourd'hui, la surface d'attaque principale n'est plus la technologie, c'est la confiance.

Intrusions axées sur l'identité

Les adversaires ne cherchent plus à forcer la porte d'entrée d'une organisation, ils préfèrent se connecter en tant qu'employé ou entité connue.

- Lassitude de la MFA et vol de tokens
- Prise de contrôle de comptes SaaS
- Exploitation d'identités avec privilèges

Pourquoi c'est important : les défenses traditionnelles du périmètre et des endpoints ne sont jamais alertées.

Déplacement latéral dans le cloud et l'environnement SaaS

Des identifiants compromis sont utilisés pour passer discrètement d'une application cloud à l'autre, obtenir des accès plus élevés et exfiltrer des données sans utiliser de malware.

- Utilisation abusive de token OAuth
- Expansion du shadow SaaS
- Exfiltration de données à l'aide d'API légitimes

Pourquoi c'est important : les failles prennent l'apparence d'activités utilisateur normales.

Campagnes de ransomware à répétition

Les opérations de ransomware ne se limitent plus au chiffrement : vol de données, harcèlement et pression réglementaire sont désormais de mise.

- Double et triple extorsion
- Ciblage des sauvegardes et des systèmes de restauration
- Fuites de données programmées pour maximiser l'impact

Pourquoi c'est important : la restauration des systèmes ne suffit plus à résoudre l'incident.

splunk> a CISCO company

Attaque de la chaîne d'approvisionnement logicielle

Les adversaires exploitent les logiciels, les mises à jour et les fournisseurs de confiance pour infiltrer les systèmes.

- Dépendances compromises
- Mises à jour malveillantes
- Exploitation d'accès tiers

Pourquoi c'est important : les relations de confiance deviennent des vecteurs d'attaque.

Attaques centrées sur les API

Les API nourrissent les applications et les intégrations modernes, et les pirates savent cibler les méthodes d'authentification faibles et les autorisations laxistes.

- Autorisations non fonctionnelles au niveau de l'objet
- Fuite de tokens
- Exploitation d'endpoints non documentés

Pourquoi c'est important : les API exposent les données et les fonctionnalités à grande échelle.

Exploitation des ressources locales (LotL)

Les acteurs malveillants se fondent dans le décor en exploitant des outils natifs et des utilitaires d'administration.

- Exploitation de PowerShell, de WMI et de l'interface de ligne de commande
- Malwares à empreinte minimale
- Faible visibilité pour les outils d'investigation

Pourquoi c'est important : « Rien de malveillant n'est visible à l'horizon » jusqu'à ce qu'il soit trop tard.

Exploitation de vulnérabilités récemment découvertes

Le délai d'exploitation diminue considérablement.

- Instrumentalisation en quelques heures
- Analyse et exploitation automatisées
- Exploitation à grande échelle des correctifs manquants

Pourquoi c'est important : les délais de détection et de réponse comptent autant que la prévention.

Transformez la sensibilisation aux menaces en action.

Téléchargez la dernière édition des 50 plus grandes menaces de cybersécurité pour découvrir les types d'attaque les plus courants et leurs évolutions pour mieux cibler vos défenses. Et quand viendra le moment de transformer ces informations en actions, Splunk sera là pour apporter clarté et vitesse à vos opérations de sécurité.

splunk> a CISCO company

26_CMP_cheat sheet_Top-cybersecurity-threats_v11_digital