CROWDSTRIKE

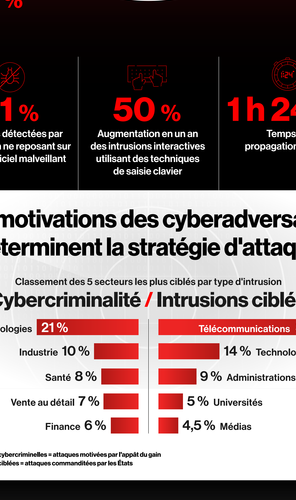
NE LAISSER AUCUNE ÉCHAPPATOIRE

Rapport 2022 sur le Threat Hunting de l'équipe Falcon OverWatch

Comme chaque année, Falcon OverWatch™, l'équipe de Threat Hunting proactif de CrowdStrike, opérationnelle 24 h/24 et 7 j/7, a publié ses conclusions et ses analyses techniques sur les principales nouvelles tactiques utilisées par les cyberadversaires. Elle a également dévoilé les tendances émergentes en matière d'intrusion qu'elle a identifiées entre le 1er juillet 2021 et le 20 juin 2022. Au cours de l'année écoulée, OverWatch a observé des changements spectaculaires dans les modes de conception et de déploiement des cyberattaques.

Intensification des intrusions, renforcement de la complexité

2022



71 %
Menaces détectées par OverWatch ne reposant sur aucun logiciel malveillant

50 %
Augmentation en un an des intrusions interactives utilisant des techniques de saisie clavier

1 h 24 m
Temps de propagation moyen

Les motivations des cyberadversaires déterminent la stratégie d'attaque

Classement des 5 secteurs les plus ciblés par type d'intrusion

Cybercriminalité / Intrusions ciblées

Cybercriminalité		Intrusions ciblées	
Technologies	21 %	Télécommunications	37 %
Industrie	10 %	Technologies	14 %
Santé	8 %	Administrations	9 %
Vente au détail	7 %	Universités	5 %
Finance	6 %	Médias	4,5 %

Intrusions cybercriminelles = attaques motivées par l'appât du gain
Intrusions ciblées = attaques commanditées par les États

Techniques nouvelles et notables

IceApple

Objectifs
Contournement des défenses, accès aux identifiants, exfiltration

Cibles
Serveurs IIS

Caractéristiques
- Framework .NET sophistiqué post exploitation
- Bibliothèques .NET chargées d'exploits depuis la mémoire
- Faible empreinte d'investigation résidant en mémoire

fscan

Objectifs
Découverte

Cibles
Hôte interne, cartographie d'environnement

Caractéristiques
- Outil cybercriminel en hausse fin 2021/début 2022
- Analyseur de vulnérabilité transformé en capteur avancé d'empreintes digitales
- Exploitation par la modification de clé publique, commandes SSH

Sweet Potato

Objectifs
Élévation des privilèges

Cibles
Identifiants Windows, jetons de sécurité

Caractéristiques
- Force l'authentification système pour capturer les identifiants en transit
- Première variante, « Hot Potato », découverte en 2016
- Script automatisé aux multiples variantes (p. ex., Juicy Potato, Lonely Potato, etc.)

Serveur web zero day

Objectifs
Persistance (via webshell), reconnaissance interactive, collecte d'identifiants, exfiltration

Cibles
Serveur Confluence et instances de datacenter

Caractéristiques
- Vulnérabilité permettant l'exécution d'un code distant non authentifié
- Utilisé dans les attaques cybercriminelles et les intrusions ciblées
- Attaque progressive comprenant un déploiement de webshell, une reconnaissance interactive, la collecte d'identifiants et la récupération d'outils à distance

Le Threat Hunting proactif n'est pas un outil, c'est une mission.

Identifiez les techniques.
Cernez vos cyberadversaires.
Menez une traque incessante.

Rapport 2022 sur le Threat Hunting de l'équipe Falcon OverWatch

Télécharger le rapport complet

Pour en savoir plus : https://www.crowdstrike.fr/services/

Suivez-nous

CROWDSTRIKE

We Stop Breaches