Une protection tout au long de la « chaîne d'attaque » avec les solutions de sécurité Cisco

Cisco vous protège tout au long de la « chaîne d'attaque » grâce à sa gamme de solutions simples, ouvertes et automatisées.

La plupart des cyberattaques suivent le schéma suivant :

REPÉRAGE	*Collecter des informations sur une cible.*
PRÉPARATION	*Créer une infrastructure et des outils.*
LANCEMENT	*Établir une connexion initiale avec les utilisateurs.*
ATTAQUE	*Utiliser les vulnérabilités pour prendre le contrôle de l'appareil.*
INSTALLATION	*Installer un malware.*
RAPPEL	*Communiquer avec le point d'origine.*
PROPAGATION	*Propager le malware afin d'atteindre l'objectif final.*

Exemple de la chaîne d'attaque d'un ransomware :

Médias sociaux ou e-mails de phishing

Configurer des serveurs et un kit d'exploit

L'utilisateur clique sur un lien ou sur une publicité malveillante

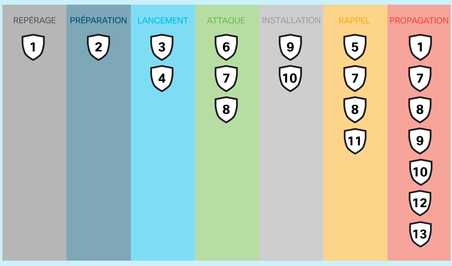
Appel vers une infrastructure malveillante

Le ransomware est installé

Le trafic de type contrôle-commande (C&C) chiffre les fichiers

Les fichiers sont inaccessibles

Les solutions de cybersécurité de Cisco opèrent sur toute la chaîne d'attaque.



1. Cisco Stealthwatch identifie l'activité de reconnaissance.
2. Cisco Talos fournit des données télémétriques ultraprécises sur les menaces à l'échelle mondiale. Il permet d'identifier l'endroit où les attaques sont préparées.
3. La solution Cisco de sécurisation de la messagerie bloque les e-mails malveillants.
4. La solution Cisco de sécurisation du web bloque le contenu malveillant sur le trafic HTTP et HTTPS.
5. Le logiciel Cisco Umbrella bloque le trafic de type contrôle-commande au niveau de la couche DNS ainsi que sur tous les ports et protocoles.
6. Le système de protection contre les intrusions de nouvelle génération (NGIPS) Cisco FirePOWER bloque les exploits avec une grande efficacité.
7. Le pare-feu de nouvelle génération Cisco FirePOWER et Meraki MX peuvent bloquer le trafic de type contrôle-commande (C&C) et l'accès non autorisé aux applications et aux ressources critiques.
8. Le client de la solution de mobilité sécurisée Cisco AnyConnect applique une protection de pare-feu de nouvelle génération (NGFW) aux utilisateurs hors site.
9. Cisco Advanced Malware Protection (AMP) for Endpoints bloque les malwares et permet de restaurer le système en un seul clic.
10. AMP Threat Grid transmet les résultats d'analyse dynamique des malwares à la solution AMP afin de déterminer si un fichier est malveillant.
11. Cisco Cognitive Threat Analytics (CTA) identifie les intrusions en analysant le trafic HTTP et HTTPS de type contrôle-commande (C&C).
12. Cisco ISE (Identity Services Engine) et la solution Cisco TrustSec permettent de contrôler les accès et les identités de manière granulaire.
13. Cisco Cloudlock peut bloquer l'accès non autorisé aux applications cloud et aux données qu'elles hébergent.

Les solutions de sécurité Cisco sont simples, ouvertes et automatisées pour vous permettre d'être plus efficaces.

Simplifiez votre workflow.

- Gérez Cisco AMP et la solution Cisco de sécurisation de la messagerie depuis la même interface.
- Déployez Cisco Umbrella sur tout votre réseau en moins de 5 minutes.

Partagez les informations entre vos produits et les fournisseurs tiers.

- Cisco compte plus de 120 partenaires de sécurité.
- Talos met à jour les produits en temps réel avec des données télémétriques sur les menaces à l'échelle mondiale.

Réagissez automatiquement.

- Supprimez automatiquement un fichier malveillant de toutes les boîtes de réception.
- Bloquez automatiquement une destination malveillante dans Umbrella sur la base des informations sur les menaces provenant d'AMP Threat Grid.

Renforcez votre efficacité.

Avec Cisco, le délai de détection est de **14 heures**, contre **100 à 200 jours** en moyenne dans le secteur.

Rapport annuel Cisco 2017 sur la cybersécurité

Pour en savoir plus, rendez-vous sur cisco.com/go/security.