MANDIANT

Comment bloquer une attaque par ransomware

En cas d'attaque par ransomware, chaque minute compte. Les attaquants opèrent généralement en trois temps : 1. Infiltration du réseau par un backdoor, 2. déplacement latéral pour faire main basse sur des données stratégiques et 3. déploiement du ransomware.

74 % DES ATTAQUES PASSENT INAPERÇUES[1]

Les cybercriminels font preuve d'agilité et frappent en un éclair. Pour les contrer, vos équipes de sécurité doivent être rapides, bien informées et bien entraînées.

ACTIVITÉ DE L'ÉQUIPE DE SÉCURITÉ		ACTIVITÉ/FLUX DE L'ATTAQUANT
	00:00:00	Un utilisateur ouvre un e-mail de phishing
ALERTE DE PRIORITÉ 1 DE LA SOLUTION DE PROTECTION DES TERMINAUX (AV)	00:00:16	Site de phishing visité et fichier .zip téléchargé
	00:00:24	Fichier malveillant extrait et ouvert à partir du fichier .zip
	00:00:26	Appels effectués par les macros intégrées dans le fichier et écriture du malware QAKBOT sur le disque
	00:00:49	Exécution de QAKBOT ; installation des outils de l'attaquant
UN SPÉCIALISTE DU THREAT HUNTING DÉTECTE QAKBOT, L'INVESTIGATION DÉBUTE	00:20:00	
	00:31:26	L'attaquant se connecte au malware et initie la phase de reconnaissance
	00:39:41	Injection et exécution d'un script PowerShell encodé pour les communications CnC sortantes
	00:40:37	L'attaquant poursuit la reconnaissance en identifiant les comptes et systèmes internes
ALERTE DE PRIORITÉ 3 DE LA SOLUTION EDR (ENDPOINT DETECTION AND RESPONSE)	00:41:28	Exfiltration des hachages de mots de passe
	01:07:59	Compromission du compte administrateur du domaine ; déplacement latéral de l'attaquant dans l'environnement de la victime
	01:38:39	Déploiement de Metasploit BEACON
	01:44:26	BLOODHOUND pour la poursuite de la reconnaissance
	01:46:00	Déploiement d'Adfind
	01:59:13	L'attaquant trouve des données d'intérêt, utilise 7zip pour les archiver, puis les exfiltre
	02:55:24	L'attaquant se déplace latéralement en déployant QAKBOT ou BEACON
		L'attaquant poursuit ses déplacements latéraux et ses activités malveillantes sans être repéré
	10 JOURS APRÈS	L'attaquant déploie le ransomware SODINOKIBI

< 1 MINUTE
INSTALLATION DE L'INFRASTRUCTURE D'ATTAQUE

< 45 MINUTES
COMMUNICATIONS CNC SORTANTES OPÉRATIONNELLES

< 1 HEURE
ACQUISITION DES MOTS DE PASSE ADMIN – L'ATTAQUANT SE DÉPLACE LIBREMENT DANS L'ENVIRONNEMENT DE LA VICTIME

< 2 HEURES
EXFILTRATION DES DONNÉES

Posez-vous les bonnes questions pour améliorer vos capacités de détection et de réponse

Pouvez-vous affronter la menace seul ?

- Effectuez-vous une surveillance 24h/7j ?
- Automatisez-vous les processus de routine pour plus de cohérence ?
- Vos ingénieurs sécurité peuvent-ils suivre l'évolution du champ des menaces ?
- Votre SOC est-il aguerri aux combats de première ligne ?

81 %

des professionnels de la sécurité considèrent leur SOC comme très complexe, mais seulement 53 % le trouvent efficace[2]

Votre MSSP est-il efficace ?

- Votre prestataire MSSP vous repasse-t-il sa surcharge de données ?
- Pouvez-vous intégrer vos technologies existantes ?
- Comment votre prestataire surveille-t-il votre infrastructure et vos applications cloud ?
- Votre prestataire gère-t-il l'investigation et la réponse, ou est-ce à vous de vous en charger ?

44 %

des MSSP ignorent certains types d'alertes, faute de recruter plus d'analystes pour gérer les volumes[3]

Faites équipe avec des experts de terrain

Mandiant Managed Defense

- Identifiez les attaquants le plus tôt possible grâce aux connaissances IoC pointues de Mandiant et à ses observations permanentes des activités malveillantes
- Repérez les attaquants avant qu'ils ne frappent en les traquant de façon proactive
- Déterminez rapidement la portée des incidents actifs pour les endiguer sans avoir à faire intervenir une équipe complète de réponse aux incidents
- Renforcez votre équipe avec l'appui des experts en sécurité de Mandiant

99 %

de cas résolus sans processus de réponse aux incidents[4]

Renforcez vos capacités de détection et de réponse

Les services MDR Managed Defense mettent à profit l'expertise et les compétences d'interprétation de nos analystes pour étudier en détail les informations complexes remontées par les technologies de sécurité. Pour vous, c'est la certitude de pouvoir détecter rapidement les incidents critiques, débusquer les attaquants furtifs et réagir avant qu'il ne soit trop tard.

mandiant.fr/advantage/managed-defense

[1] Rapport Mandiant 2020 sur l'efficacité de la cybersécurité, avril 2020
[2] Ponemon Institute, Second Annual Study of Economics of Security Operations Centers: What is the True Cost for Effective Results, janvier 2021
[3] IDC, The Voice of the Analysts Improving Security Operations Center Processes Through Advanced Technologies, janvier 2021
[4] Mandiant Managed Defense 2022

MANDIANT