STORMSHIELD

Threat advisory

Stormshield Endpoint Security Evolution

Votre **entreprise** Grâce à Stormshield Endpoint Security Evolution

est protégée contre les ransomwares

LockBit 2.0

EXFILTRATION ET CHIFFREMENT DES DONNÉES SUR LES MACHINES INFECTÉES

LockBit est un groupe de cyber-attaquants opérant selon un modèle de Ransomware-as-a-Service (RaaS), comme un produit clé en main.

LockBit propose sa plateforme de ransomware à d'autres entités ou individus qui l'utilisent selon un modèle d'affiliation.

LockBit serait le groupe de ransomware le plus actif avec une liste impressionnante de 203 victimes pour le seul 3e trimestre 2021.

Accès initial
Obtention par ingénierie sociale des privilèges élevés pour chiffrer les fichiers et réclamer une rançon.

Cible
Entreprise de toute taille sans une protection efficace contre les ransomwares. En particulier aux États-Unis, Canada et Europe.

Risques
Chiffrement de la donnée (impact intégrité), vol d'informations sensibles (impact confidentialité), perte de productivité (impact disponibilité), etc.

Découvrez notre solution de protection contre les ransomwares

LOCKBIT 2.0

#1

Primo-infection

Phase 1

Le cyber-attaquant **dispose d'un accès à la société cible** soit par l'achat réalisé auprès d'un autre groupe, soit par un phishing qu'il a l'organisé.

*Stormshield Endpoint Security Evolution vous **protège efficacement contre les différentes techniques d'attaques** (les buffer overflow, les packed malware ou encore les process hollowing).*

#2

Latéralisation et recherche de valeur (expansion)

Phase 2

Le cyber-attaquant **s'infiltre en profondeur** pour découvrir le réseau. Ensuite il effectue une **latéralisation** afin d'identifier les machines contenant des informations précieuses.

*Stormshield Endpoint Security Evolution **détecte et neutralise les opérations de type discovery** (par ex., le lancement de commandes pour connaître les adresses IP, les comptes utilisateurs, les serveurs DNS, les partages réseaux, etc.).*

#3

Impact

Phase 3

Exfiltration de données vers l'infrastructure du groupe LockBit

*Stormshield Endpoint Security Evolution **bloque l'accès aux fichiers sensibles** de type mots de passe, clés privées, coffre-fort, credentials, etc.*

Chiffrement des fichiers et publication d'une note de rançon

***Cette étape n'est jamais executée.** Stormshield Endpoint Security Evolution neutralise les malware qui se comportent comme des ransomware, évitant le chiffrement de données.*

Destruction des points de restauration des *Shadow Copies*

*Il **détecte et bloque les tentatives d'altération** de Shadow Copies, arrêtant l'exécution du ransomware.*