KPMG GLD & Associés Monaco

LockBit 3.0

■ **CYBER** ■ ACTUALITÉS

■ *Newsletter N°2*

LockBit 3.0 : Est-ce la chute du plus virulent des groupes de cybercriminels ?

De l'opération Cronos réalisée par les polices de 15 pays à la rébellion du groupe de Ransomwares puis la révélation de l'identité présumée du chef de ce cartel, est-ce la fin du ransomware ?

Histoire

En septembre 2019 naît LockBit (appelé ABCD à ses débuts). Ce groupe de cybercriminels s'est rapidement imposé comme l'un des groupes les plus redoutés dans le monde de la cybersécurité. Il s'infiltre dans les systèmes informatiques, chiffre les données critiques et demande des rançons en échange de la clé de déchiffrement pour récupérer les données.

Ce groupe cible divers secteurs d'activité, y compris les services publics, la santé et les entreprises privées, causant des perturbations massives et des pertes financières colossales. L'impact de LockBit est estimé à plus de 500 millions de dollars sur plus de 2500 victimes [1].

Démantèlement de LockBit : L'opération Cronos

L'opération Cronos est une intervention internationale majeure menée par les forces de l'ordre, notamment Europol, le FBI, la gendarmerie nationale et d'autres forces nationales [2]. Elle a débuté en 2022 par le partage des informations et la coordination des efforts pour traquer les membres de LockBit, en réponse à la menace croissante posée par ce groupe.

Fin 2023, une série de raids coordonnés des forces de l'ordre a eu lieu dans plusieurs pays, aboutissant à l'arrestation de plusieurs membres clés de LockBit. Des équipements informatiques, des serveurs, ainsi que des fonds en cryptomonnaie ont été saisis, perturbant significativement la capacité opérationnelle du groupe de Ransomware.

Le 19 février 2024, dans ce qu'Europol qualifie de « percée significative dans la lutte contre la cybercriminalité », les autorités ont annoncé que l'infrastructure technique de LockBit et son site de fuite de données volées, accessibles publiquement sur le *dark web*, ont été saisis.

La National Crime Agency du Royaume-Uni a remplacé le contenu du site web de LockBit, qui était utilisé pour héberger les données volées aux victimes, par une parodie destinée à ridiculiser les cybercriminels, exposant les opérations et les capacités de LockBit, y compris des clés de déchiffrement et des informations sur deux arrestations.

Début mai 2024, la NCA a révélé l'identité de celui qui pourrait être le cerveau et le développeur du groupe de Ransomware LockBit et du système « Ransomware-as-a-Service » [3] : un russe de 31 ans, originaire de Voronezh, également visé par des sanctions internationales et une offre de récompense américaine de 10 millions de dollars pour des informations menant à son arrestation.

Sûrement à des fins de protection, LockBitSupp, le leader de LockBit, a déclaré dans une interview chiffrée avec « Recorded Future News » [4] que les forces de l'ordre avaient associé la mauvaise personne à son pseudonyme. réaffirme par ailleurs que son objectif reste le même : attaquer 1 million d'entreprises.

Est-ce la fin de LockBit 3.0 ?

L'opération Cronos a porté un coup important au groupe LockBit et souligne l'importance de la coopération internationale dans la lutte contre les cybermenaces.

Malgré cela, Lockbit, même affaibli, continue son activité avec ses affiliés et a mis en ligne un nouveau site vitrine de fuite de données. L'hôpital de Cannes en a d'ailleurs été récemment victime en avril 2024 [5]. Par ailleurs, d'autres groupes de cybercriminels comme Medusa, Akira, RansomHub et d'autres continuent d'opérer et de faire des victimes.

Devant cette menace qui s'adapte, se professionnalise, et renaît sous d'autres formes, les entreprises doivent donc se demander si leur infrastructure est assez sécurisée pour résister à une vague d'attaques, et prendre les mesures nécessaires.

Sources

[1] Russian Hacker Dmitry Khoroshev Unmasked as LockBit Ransomware Administrator (thehackernews.com)

[2] Law enforcement disrupt world's biggest ransomware operation | Europol (europa.eu)

[3] LockBit ransomware admin identified, sanctioned in US, UK, Australia (bleepingcomputer.com)

[4] In interview, LockbitSupp says authorities outed the wrong guy (therecord.media)

[5] Cannes : les hackers ressuscités de LockBit diffusent les données internes de l'hôpital piraté - Le Parisien

Auteurs

Marcel MARSAIS-LACOSTE

Junior • IT Advisory• KPMG Monaco

MMarsais-Lacoste@kpmg.mc

Clément MAILLIOUX

Senior Manager • Advisory • KPMG Monaco

cmaillioux@kpmg.mc

Contactez-nous

Bettina RAGAZZONI
Associé
bragazzoni@kpmg.mc

Stéphane GARINO
Country Senior Partner
sgarino@kpmg.mc

Xavier CARPINELLI
Directeur Associé
xaviercarpinelli@kpmg.mc

Anne-Marie FELDEN
Directeur Associé
afelden@kpmg.mc

Sylvie ROTI
Directeur Associé
sroti@kpmg.mc

Sabina DEBUSSY
Directeur Associé
sdebussy@kpmg.mc

Bernard SQUECCO
Associé
bsquecco@kpmg.mc

2, rue de la Lüjerneta • "Athos Palace" • 98000, Monaco

mc-news@kpmg.mc
www.KPMG.mc
@KPMG_Monaco
+377 977 777 00
@kpmg-monaco
@KPMGMonaco

Abonnez-vous aux Newsletters KPMG Monaco

Les Newsletters de KPMG Monaco vous permettent de recevoir des conseils de nos experts et des actualités pertinentes directement dans votre boîte mail.

Nous nous engageons à vous fournir uniquement des communications pertinentes selon vos centres d'intérêts et de vos besoins professionnels.

Je m'abonne aux Newsletters KPMG Monaco