TLP:GREEN

COMPTE-RENDU D'INFORMATION Le 23/02/2024

CYBER – CERT [ED] N°10

Retour sur le démantèlement de Lockbit – Opération CRONOS

Description

Le *ransomware LockBit*, apparu pour la première fois en septembre 2019, est un *ransomware* qui fonctionne comme un *Ransomware-as-a-Service* (Raas). Largement reconnu comme l'un des *ransomwares* les plus prolifiques au monde, les opérateurs de ce groupe ont développé de nombreuses variantes de LockBit au fil des ans « *causant des milliards d'euros de dommages* », comme l'indique EUROPOL. À ce jour, il s'agit du *ransomware* le plus actif en termes d'incidents, avec près de 2 300 attaques revendiquées publiquement depuis 2020.

L'opération CRONOS, menée avec la coopération de 14 pays, s'est déroulée sur une période de plusieurs mois.

Le 19 février 2024, les autorités impliquées dans l'Operation Cronos ont ainsi publié un message sur le site web de LockBit, indiquant :

« Ce site est désormais sous le contrôle de la National Crime Agency (NCA) du Royaume-Uni, qui travaille en étroite collaboration avec le FBI et le groupe de travail international chargé de l'application de la loi, "Operation Cronos". »

Figure 1 : Capture d'écran du site de LockBit 3.0 après sa saisie par les autorités impliquées dans l'opération CRONOS

Les principales infrastructures de LockBit (34 serveurs à travers le monde) ont ainsi été compromises, mettant fin à leur emprise criminelle. La *National Crime Agency* (NCA) a ainsi indiqué avoir le contrôle total de ce dernier, avec une mainmise sur les données dérobées aux victimes.

Figure 2 : Pays impliqués dans l'opération CRONOS - Source : EUROPOL

Les données acquises au cours de cette opération soutiendront l'effort international de traque des affiliés de cette organisation. Mais plus encore, les développeurs et les membres directs de ce groupe criminel sont également visés par ces investigations.

Ainsi, deux arrestations ont été réalisées en Pologne et en Ukraine à la demande de la justice française, et d'autres mandats d'arrêt ont été émis pour poursuivre cet objectif. Suite à cette opération, les sanctions économiques sont arrivées assez rapidement : 200 comptes de cryptomonnaies liés à cette organisation criminelle ont notamment été gelés. Au final, l'opération Cronos a permis de récupérer plus de 30 000 adresses Bitcoin, dont 500 étaient actives et détenaient plus de 2 200 BTC, soit l'équivalent d'environ 113 000 000 $, provenant de LockBit et de ses affiliés.

En outre, grâce à la coordination d'EUROPOL, la coopération entre la police japonaise, la *National Crime Agency* et le FBI a permis de mettre à disposition des outils de déchiffrement, notamment sur le *portail No More Ransom*.

Selon les données fournies par EUROPOL, cette situation peut être résumée de la manière suivante :

- 10 pays impliqués dans la taskforce CRONOS (AU, CA, FR, DE, JP, NL, UK, USA, SE, CH)
- 4 pays participants (FIN, NZ, PL, UA)
- Prise de contrôle de l'infrastructure technique et du site de LockBit 3.0 par les forces de l'ordre
- Obtention du code source de LockBit et mise à disposition d'un outil de déchiffrement
- 34 serveurs mis hors service
- 14 000 comptes frauduleux fermés
- 3 mandats émis
- 2 arrestations
- 200 comptes de cryptomonnaies gelés

En outre, plusieurs analyses publiées par Redsense et PRODAFT ont permis d'identifier des liens entre LockBit 3.0 et d'anciens membres de Conti et des services de renseignement russes.

Cependant, ce coup de filet pourrait être de courte durée. EUROPOL et les pays contribuant à cette opération ont demandé à tout individu en possession d'informations liées à LockBit 3.0 de se manifester en échange d'une récompense afin de continuer les opérations visant à mettre fin aux agissements des opérateurs de LockBit 3.0. En effet, leurs inquiétudes et leurs besoins semblent justifiés, puisqu'après quelques jours de difficultés majeures, LockBit semble refaire surface avec une nouvelle version appelée " *LockBit-NG-Dev* ", ce qui laisse présager que la version 4.0 sera bientôt disponible pour ses affiliés.

Cette version, sur laquelle le groupe a secrètement travaillé avant son anéantissement présumé, aurait été stockée sur des serveurs non touchés par l'opération CRONOS. Selon le groupe criminel, les serveurs non affectés par la vulnérabilité critique de PHP (CVE-2023-3824) pourraient avoir été laissés à l'écart des actions de la coalition. Toutefois, il est important de préciser que ces informations proviennent de déclarations de comptes liés à LockBit et peuvent donc être considérées comme partiellement fausses.

Outre l'amélioration du fonctionnement global de son programme de chiffrement, l'une des nouveautés les plus intéressantes de cette version est sa capacité à mettre fin au processus si la date indiquée dans le fichier de configuration est dépassée. Cela oblige donc l'affilié à acheter une nouvelle version de son outil de chiffrement. Cette information indique que LockBit n'a très probablement pas l'intention de cesser ses activités et que cette entité est déterminée à poursuivre son ascension au sein de l'écosystème des *ransomwares*

Développements futurs :

- Compte tenu de l'agitation actuelle, on peut s'attendre à une baisse de l'activité mondiale des *ransomwares* au cours des prochains mois ;
- De plus, malgré un probable manque de confiance de la part des affiliés, LockBit pourrait bientôt refaire surface ;
- Au cours des prochains mois, la scène de la cybercriminalité va probablement se réorganiser, avec des affiliés qui rejoindront les programmes de *ransomware* existants ou en créeront de nouveaux ;
- L'humiliation subie par LockBit 3.0 à la suite de cette opération peut également constituer le début d'une réaction agressive de leur part en guise de "revanche" et de démonstration de leur résilience ;

L'efficacité à long terme de cette opération déterminera sans doute les objectifs futurs de la coopération internationale en matière de RaaS.

Sources :

- EUROPOL
- TrendMicro
- Redsense
- PRODAFT
- NoMoreRansom

CERT [ED]