TRIBUNAL JUDICIAIRE
DE PARIS

Liberté
Égalité
Fraternité

PARQUET DE MADAME LA
PROCUREURE DE LA REPUBLIQUE

Paris, le 30 mai 2024

Communiqué de presse

Entre le 27 et le 29 mai 2024, l'opération internationale ENDGAME, coordonnée par EUROJUST et EUROPOL, a eu pour objectif l'entrave de services et outils utilisés par les cybercriminels et a permis l'arrestation de cibles d'intérêt à travers le monde.

L'opération a visé les infrastructures **« Bumblebee » « Pikabot » « Smokeloader » « System BC » « IcedID» et « Trickbot ».** Elle est le résultat d'un travail conjoint entre les autorités allemandes (BKA), néerlandaises (NHTCU), françaises, américaines, anglaises et danoises.

Les opérations menées par les forces de l'ordre se sont déployées sur plusieurs pays et ont mené à **l'interpellation de 4 personnes dont 3 par les autorités françaises**, à 16 perquisitions, à l'interruption d'une centaine de serveurs et à des saisies.

Plus particulièrement s'agissant du volet français, les investigations se sont déroulées sous la direction de la **section de lutte contre la cybercriminalité (J3) du parquet de Paris**, qui a co-saisi l'OFAC, la BL2C et le C3N. Les autorités françaises ont par ailleurs bénéficié de l'assistance de la société privée Sekoia.

Les enquêteurs de **l'OFAC (office central anti-cybercriminalité)**, après avoir identifié l'administrateur de « SystemBC » et cartographié les infrastructures liées à ce dropper avec l'aide de l'ANSSI, ont coordonné le démantèlement de dizaines de serveurs de contrôle. Ils vont désormais alerter des milliers de victimes afin qu'elles puissent se prémunir d'autres attaques de type rançongiciel.

Les enquêteurs de **la BL2C (Brigade de lutte contre la cybercriminalité de la Préfecture de police de Paris)** sont parvenus à identifier l'administrateur du botnet Pikabot. Ils ont procédé à son interpellation et à une perquisition de son domicile, en Ukraine, avec le concours des autorités judiciaires ukrainiennes et du SBU, la police ukrainienne.

Les enquêteurs du **C3N (centre de lutte contre les criminalités numériques, de la gendarmerie)**, en lien avec l'OFAC, ont quant à eux identifié l'un des acteurs principaux du dropper « Bumblebee » et ont procédé à son audition en Arménie, ainsi qu'à des opérations de perquisition. Ont été saisis au domicile du mis en cause, outre son matériel informatique, du numéraire et des cryptomonnaies. L'exécution de ces opérations a été permise dans un délai très court par l'intermédiation des autorités judiciaires (the Investigative Committee) et du ministère des affaires intérieures arméniens.

Contact presse : 06 07 18 42 28
scom.parquet.tj-paris@justice.fr

Cette enquête avait été ouverte le 1er mai 2022, des chefs d'atteintes à un système de traitement automatisé de données (accès et maintien, introduction et modification frauduleuses de données, entrave au fonctionnement), extorsion en bande organisée, blanchiment en bande organisée, association de malfaiteurs, délits faisant encourir 10 ans d'emprisonnement**.** L'opération s'inscrit dans le prolongement des opérations menées par l'OFAC sur le botnet « Emotet » en janvier 2021 et « Qbot » en août 2023.

Le travail des enquêteurs a été de cibler dans un même dossier les infrastructures malveillantes de plusieurs services cybercriminels dit d'« injecteurs » et d'identifier leurs administrateurs et développeurs. Les outils ciblés sont plus connus sous les noms de **« Bumblebee » « Pikabot » « Smokeloader » «SystemBC » « IcedID» et « Trickbot ».**

Un injecteur (ou dropper) est un type spécifique de logiciel malveillant conçu pour être une porte d'entrée à d'autres maliciels sur un système cible, notamment par courriel, servant ainsi de point de départ pour des attaques plus complexes. Il peut être utilisé notamment pour des campagnes d'infection par ransomware (programme qui chiffre les fichiers en demandant une rançon pour les mettre au clair) ou pour voler des données personnelles.

Le déploiement d'un injecteur s'appuie sur une structure complexe et volumineuse de serveurs et d'ordinateurs à travers le monde, dont de nombreux sont compromis et utilisés à l'insu de leur légitime propriétaire. Cette infrastructure internationale permet aux cybercriminels de coordonner leurs attaques et de rester difficiles à détecter.

Ces injecteurs appartiennent au modèle économique dit du « malware as a service ». Leurs administrateurs les proposent à d'autres cybercriminels désireux d'infecter des victimes avec leurs propres programmes malveillants.

En France, les attaques permises par ces outils, centralisées à la section de lutte contre la cybercriminalité (J3) du Parquet de Paris, se comptent par centaines et sont commises au préjudice de sociétés privées, de particuliers, d'administrations publiques y compris d'hôpitaux. Les plaintes déposées à la section J3 en cette matière ont augmenté de 30% entre l'année 2022 et l'année 2023.

Laure BECCUAU,
Procureure de la République

Contact presse : 06 07 18 42 28
scom.parquet.tj-paris@justice.fr