TRIBUNAL JUDICIAIRE
DE PARIS

Liberté
Égalité
Fraternité

PARQUET DE MADAME LA
PROCUREURE DE LA REPUBLIQUE

Paris, le 25 juillet 2024

Communiqué de presse

À la suite d'un signalement de la société Sekoia, la section J3 du parquet de Paris a ouvert une enquête préliminaire, toujours en cours, confiée au C3N (centre de lutte contre les criminalités numériques de la gendarmerie nationale) concernant **un réseau de machines zombies (*botnet*) comptant plusieurs millions de victimes dans le monde, dont plusieurs milliers en France, utilisé notamment à des fins d'espionnage.**

Les machines des victimes avaient été infectées par le *malware* PlugX, un logiciel malveillant de type « RAT » (*Remote Access Trojan*) : après avoir infecté la machine, le logiciel reçoit des ordres d'un serveur central afin d'exécuter des commandes arbitraires et de s'emparer de données présentes sur le système. La contamination était effectuée par toute implantation de clé USB.

Les analystes de la société Sekoia ont identifié et pris possession d'un serveur de commande et de contrôle (C2) à la tête d'un réseau de plusieurs millions de machines infectées, dont 3 000 en France, qui recevaient des requêtes de près de 100 000 machines victimes distinctes par jour. **En lien avec le C3N, la société Sekoia a développé une solution technique permettant de désinfecter à distance** les machines victimes du botnet. La solution de désinfection envisagée a été présentée à des partenaires étrangers de la France, par l'intermédiaire de l'agence Europol.

L'opération de désinfection a été lancée le 18 juillet, et se poursuivra pendant plusieurs mois. Quelques heures après le début du processus, **une centaine de victimes ont déjà pu bénéficier de cette désinfection, majoritairement en France, mais aussi à Malte, au Portugal, en Croatie, en Slovaquie et en Autriche**. À l'issue de l'opération, d'ici à la fin de l'année 2024, les victimes françaises seront individuellement avisées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), au titre de l'article L. 33-14 alinéa 5 du code des postes et des communications électroniques.

La société Sekoia tient à disposition des professionnels une liste d'indicateurs techniques liés au réseau malveillant objet de la présente enquête. Le parquet de Paris rappelle l'importance des mesures de sécurité informatique du quotidien, et recommande notamment l'utilisation d'un logiciel antivirus maintenu à jour.

À la veille de l'ouverture des Jeux olympiques, cette opération démontre **la vigilance des différents acteurs, en France et à l'étranger, mobilisés pour lutter contre toutes les formes de cybercriminalité**, y compris les plus sophistiquées.

Laure BECCUAU,
Procureure de la République

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