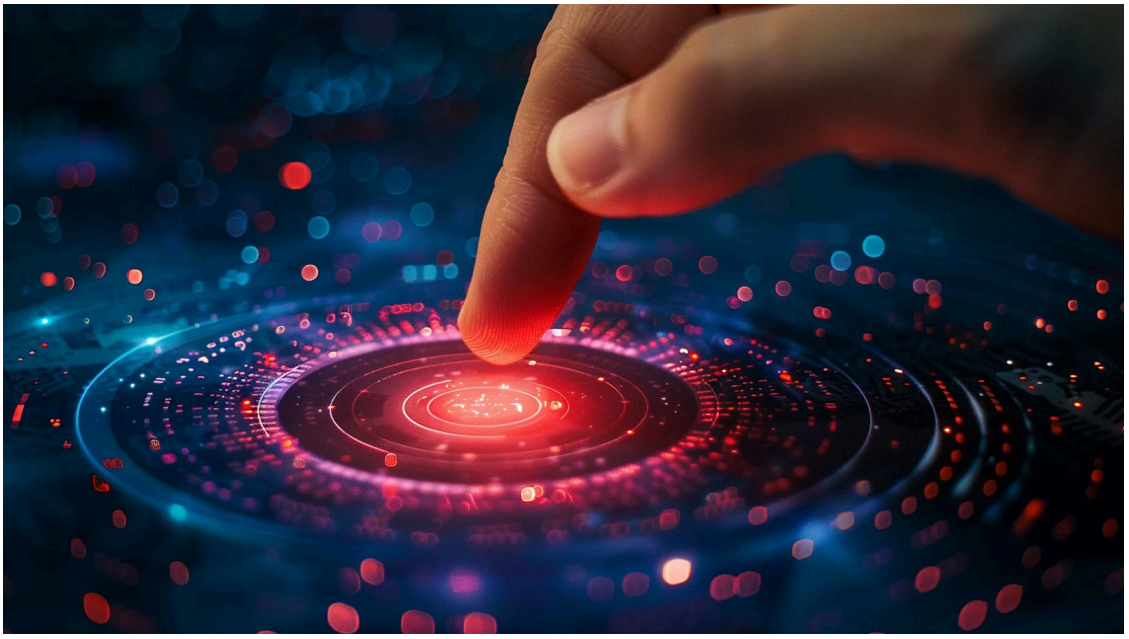
French police push PlugX malware self-destruct payload to clean PCs

By Bill Toulas

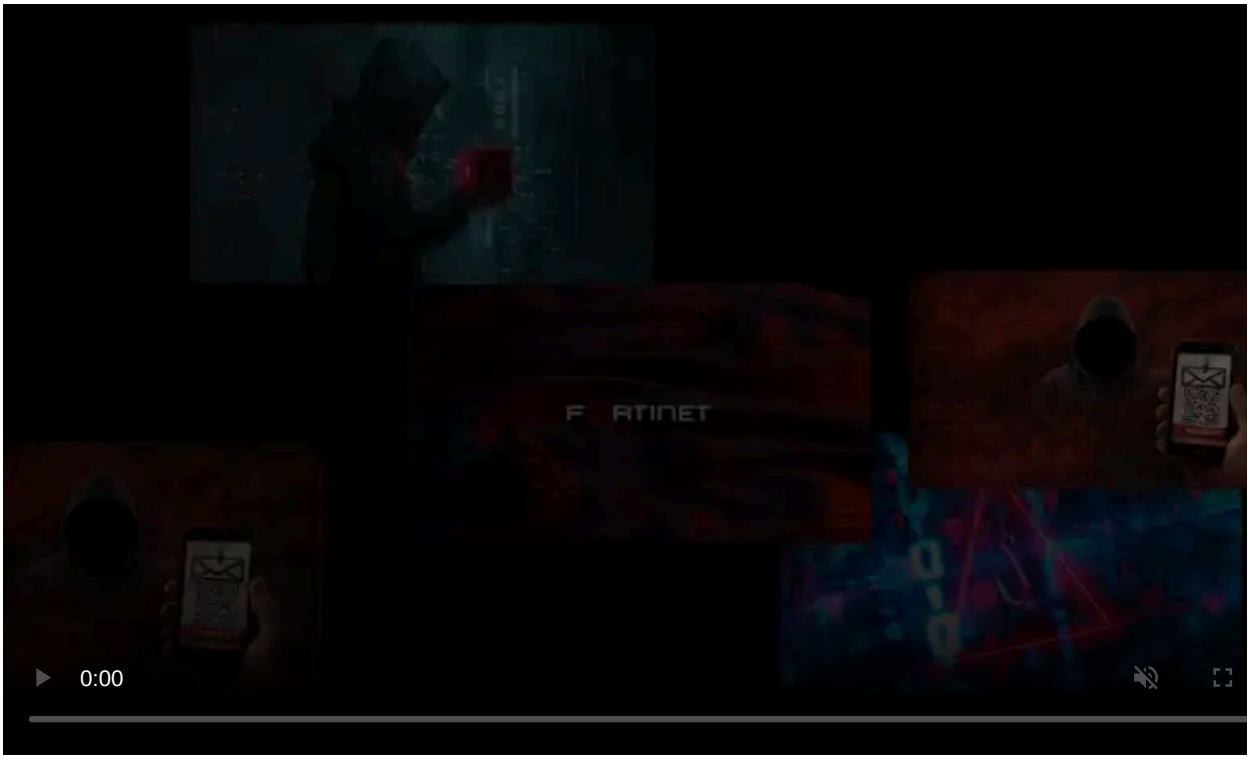
Published: 2024-07-25 · Archived: 2026-04-05 22:33:00 UTC

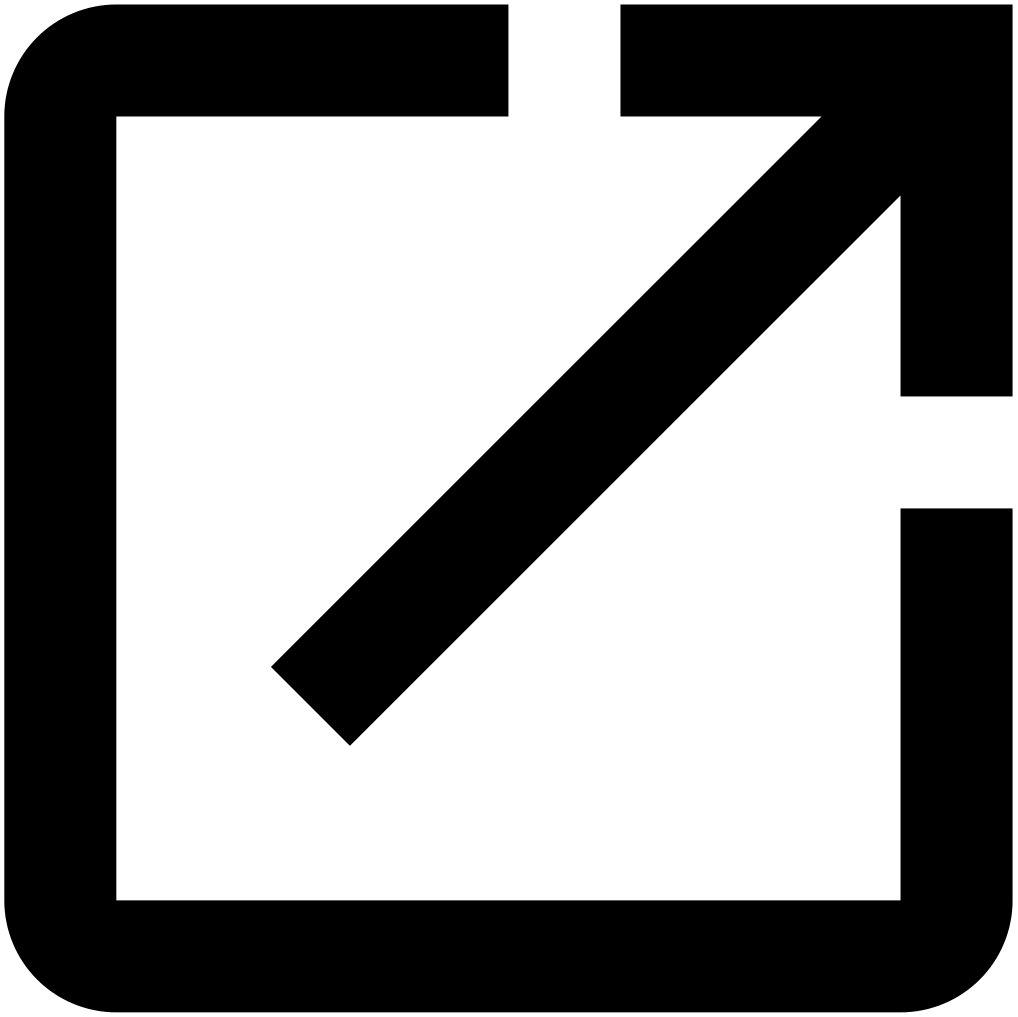


The French police and Europol are pushing out a "disinfection solution" that automatically removes the PlugX malware from infected devices in France.

The operation is conducted by the Center for the Fight Against Digital Crime (C3N) of the National Gendarmerie with assistance by French cybersecurity firm Sekoia, which sinkholed a command and control server for a widely distributed PlugX variant last April.

PlugX is a remote access trojan that has been deployed by multiple Chinese threat actors for a long time. New variants are modified and released according to a malicious campaign's operational needs.


F RTINET
0:00



Cybersecurity firm Sekoia previously reported on a botnet for a PlugX variant that spread through USB flash drives. This botnet was abandoned by its original operator, but it continued to spread independently, infecting almost 2.5 million devices.

Sekoia took control of the abandoned command and control servers, which received up to 100,000 pings from infected hosts daily and had 2,500,000 unique connections from 170 countries over six months.

The security firm sinkholed the PlugX botnet so it could not be used to issue commands to infected devices. However, the malware remained active on people's systems, increasing the risk that malicious actors could take control of the botnet and revive the infections.

Sekoia proposed a clean-up mechanism that uses a custom PlugX plugin pushed to infected devices to issue a self-deletion command that removes the infection.

The researchers also proposed a method to scan connected USB flash drives for the malware and remove it. However, automatically cleaning USB drives could damage the media and prevent access to legitimate files, making the approach risky.

As this approach is intrusive and could lead to legal ramifications, the researchers shared their solution with law enforcement.

"Given the potential legal challenges that could arise from conducting a widespread disinfection campaign, which involves sending an arbitrary command to workstations we do not own, we have resolved to defer the decision on whether to disinfect workstations in their respective countries to the discretion of national Computer Emergency Response Teams (CERTs), Law Enforcement Agencies (LEAs), and cybersecurity authorities," explained Sekoia in their April report.

Cleaning French devices

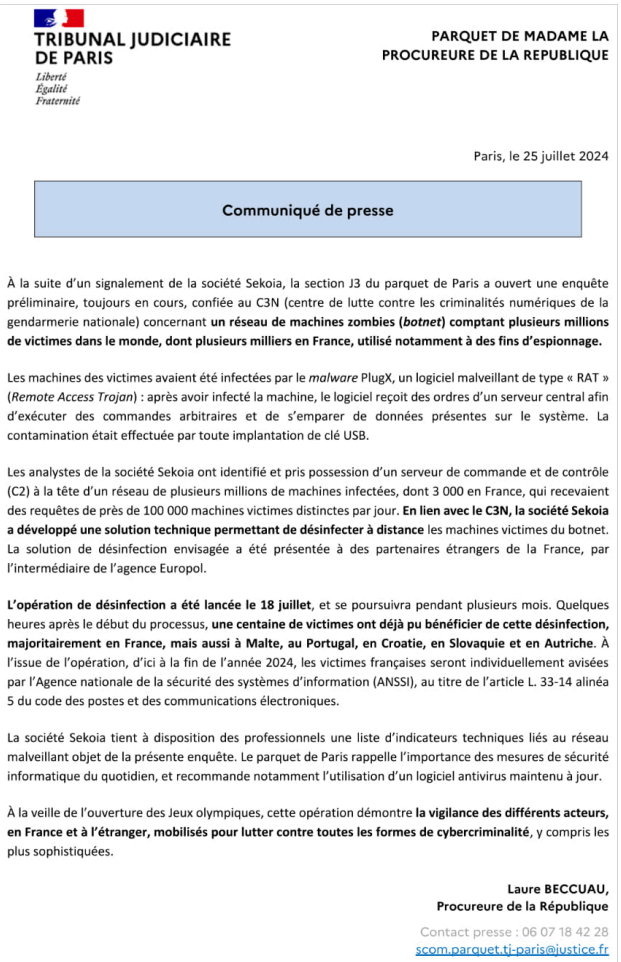
According to C3N, Europol received a disinfection solution from Sekoia, which is being shared with partner countries to remove the malware from devices in their countries.

While Sekoia told BleepingComputer that they could not share details about the solution, it is likely a similar solution to the PlugX module they described in their report.

With the Paris 2024 Olympic Games approaching, the French authorities, including all cybersecurity stakeholders, are on high alert, so the risk of PlugX found in 3,000 systems in France was considered unacceptable.

Hence, PlugX payloads are now being removed from infected systems in France, but also in Malta, Portugal, Croatia, Slovakia, and Austria.

The disinfection operation started on July 18, 2024, and is expected to continue for several months, possibly ending in late 2024.



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

PlugX removal announcement
Source: Parquet de Paris | LinkedIn

The National Agency for the Security of Information Systems (ANSSI) will individually notify victims in France about the clean-up process and how it impacts them.

It's worth noting that this particular PlugX variant spreads via infected USB drives, and it is not known if Sekoia's solution includes the ability to remove the malware from removable media.

People are advised to be cautious when plugging their USB sticks into systems at printing shops and other places that receive many physical connections daily and to scan their devices afterward before connecting them to systems holding sensitive data.

BleepingComputer contacted Europol and the French authorities with questions about the disinfection solution but has not received a reply yet.

Source: https://www.bleepingcomputer.com/news/security/french-police-push-plugx-malware-self-destruct-payload-to-clean-pcs/