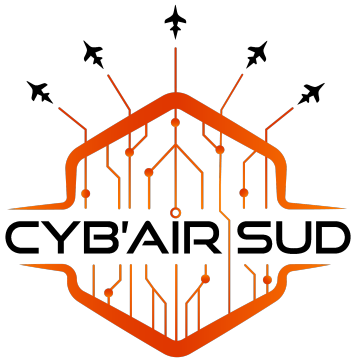


Experience Report: Disinfection Operation of PlugX Worm

CFP 2025 — English Version

Speaker: Charles Meslay

Duration

30 minutes

Short Description

In April 2024, Sekoia.io presented at BotConf "Unplugging PlugX: Sinkholing the PlugX USB Worm Botnet". This talk led to a disinfection campaign conducted in ten countries. Sekoia.io will provide a complete experience report, from botnet sinkholing to the execution of the disinfection campaign.

Detailed Description

In April 2024, we presented at BotConf the talk "Unplugging PlugX: Sinkholing the PlugX USB Worm Botnet", explaining how we had taken control of a PlugX botnet IP and, thanks to malware analysis, discovered that a remote disinfection command could be executed.

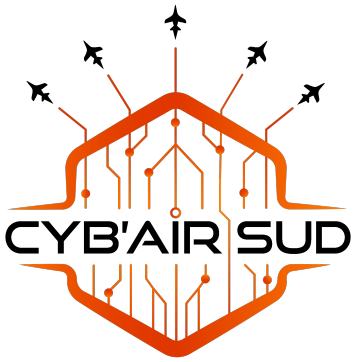
Following this talk, we called on national CERTs to propose a sovereign disinfection operation of this USB worm. More than twenty countries expressed interest, and ten ultimately participated, concluding the campaign in December 2024.

This presentation will cover the full operation:

1. Taking control of the botnet IP
2. Analyzing this PlugX variant and planning disinfection methods
3. Sharing lessons learned regarding organization and results of the disinfection operation

Other Information

— Language: English
— TLP / Recording / Redistribution: no restrictions



Retex sur l'opération de désinfection de PlugX Worm

CFP 2025 — Version Française

Intervenant : Charles Meslay

Durée

30 minutes

Description concise

En avril 2024, Sekoia.io présentait à la BotConf « Unplugging PlugX : sinkholing the PlugX USB Worm Botnet ». Cette conférence a ensuite débouché sur une campagne de désinfection menée dans dix pays. Sekoia.io proposera un retour d'expérience complet, du sinkholing du botnet à la mise en œuvre de la campagne de désinfection.

Résumé détaillé

En avril 2024, nous avons présenté à la BotConf la conférence « Unplugging PlugX : Sinkholing the PlugX USB Worm Botnet », au cours de laquelle nous avons expliqué comment nous avions pris possession d'une adresse IP du botnet PlugX et comment, grâce à l'analyse de ce malware, nous avions pu constater qu'une commande de désinfection pouvait être exécutée à distance.

Lors de cette conférence, nous avons lancé un appel aux CERT nationaux afin de leur proposer une opération de désinfection souveraine de ce ver USB. Plus de vingt pays se sont montrés intéressés et dix d'entre eux ont finalement participé à cette opération, qui s'est achevée en décembre 2024.

Cette présentation retracera l'ensemble de cette opération depuis ses débuts :

1. la prise de possession de l'adresse IP du botnet
2. l'analyse de ce variant de PlugX et les méthodes de désinfection envisagées
3. un retour d'expérience sur l'organisation et les résultats de l'opération de désinfection

Autres informations

— Langue : Français
— TLP / Enregistrement / Rediffusion : normalement aucune restriction