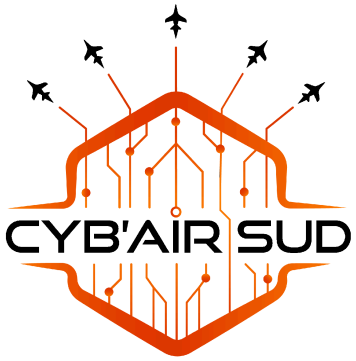


LinkPro — Analysis of a BPF Backdoor

CFP 2025 — English Version

Speaker: Théo Letailleur

Short Description

During a digital investigation following the compromise of an infrastructure hosted on AWS EKS, a stealthy backdoor targeting GNU/Linux systems was discovered. The backdoor notably relies on the installation of two BPF programs — one to hide and the other to enable remote activation using a port-knocking mechanism. This presentation details the malware's capabilities and the infection chain encountered.

Detailed Abstract

The talk will cover:

1. The infection chain observed during the incident investigation;
2. The LinkPro backdoor: capabilities and persistence mechanisms;
3. The BPF implants: architecture, role in stealth and remote activation (port knocking).

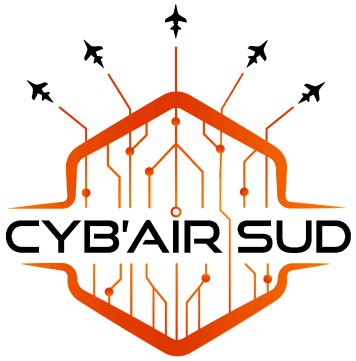
Other Information

— Duration: 30 minutes

— Language: French

Links Synactiv

- LinkedIn
- X (Twitter)
- Bluesky
- Website



LinkPro — Analyse d'une backdoor BPF

CFP 2025 — Version Française

Intervenant : Théo Letailleur

Descriptif

Lors d'une investigation numérique liée à la compromission d'une infrastructure hébergée sur AWS EKS, une backdoor furtive ciblant les systèmes GNU/Linux a été découverte. Cette backdoor présente notamment des fonctionnalités reposant sur l'installation de deux programmes BPF — d'une part pour se dissimuler, d'autre part pour être activée à distance via le mécanisme dit de « port knocking ». Cette présentation détaille les capacités de ce malware et présente la chaîne d'infection rencontrée.

Résumé / Points abordés

1. Chaîne d'infection observée ;
2. Backdoor LinkPro : fonctionnalités, persistance et objectifs ;
3. Implants BPF : architecture, rôle pour la furtivité et activation à distance (port knocking).

Autres Informations

— Durée : 30 minutes

— Langue : Français

Liens Synactiv

- LinkedIn
- X (Twitter)
- Bluesky
- Website