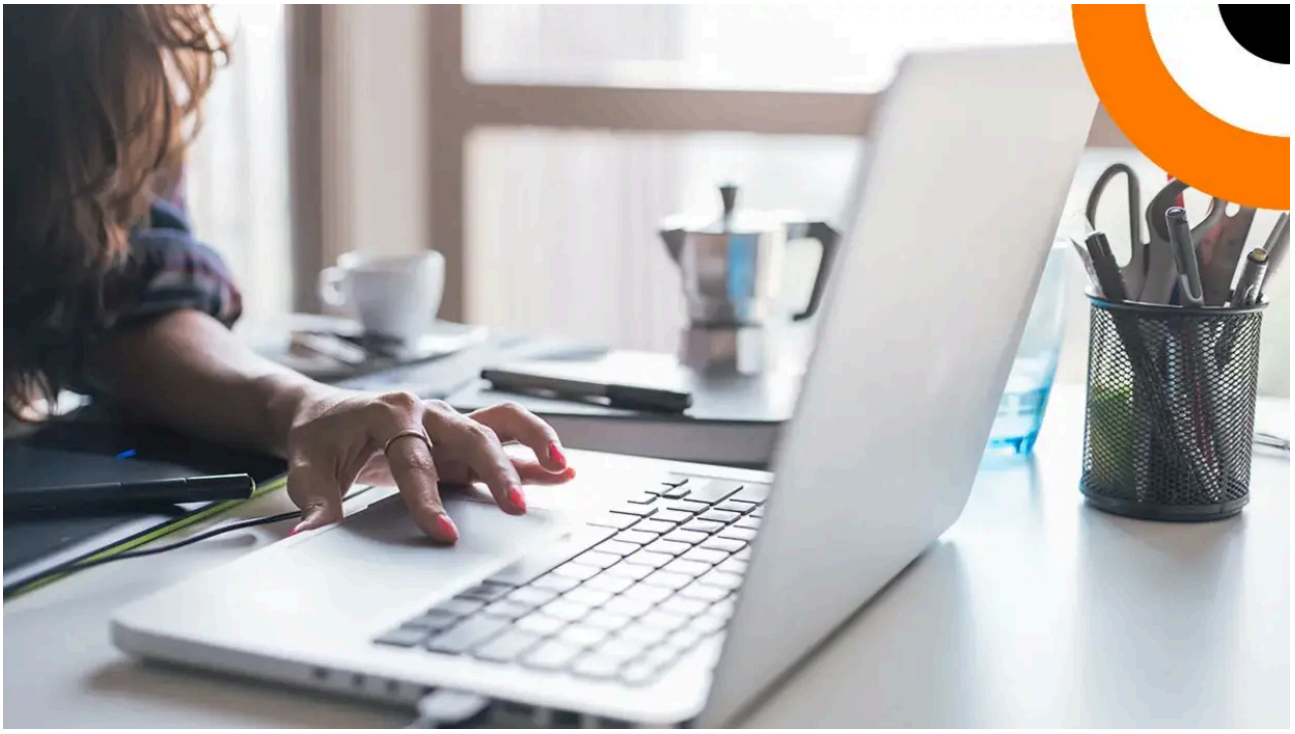
SmokedHam and Qilin Threats | Orange Cyberdefense

Published: 2026-04-15 · Archived: 2026-05-06 02:00:38 UTC

Smoking out an affiliate: SmokedHam, Qilin, a few Google ads and some bossware



TL;DR

- In early 2026, **Orange Cyberdefense** responded to several incidents delivering the SmokedHam backdoor;
- In at least one case, the infection chain resulted in the deployment of the Qilin ransomware;
- We attribute with moderate confidence these activities to the Russian-speaking ransomware affiliate UNC2465, historically associated with DarkSide, LockBit and Hunters International distribution;
- By pivoting on the infrastructure, we identified multiple malicious malvertising domains responsible for delivering SmokedHam typically masqueraded as legitimate utilities like RVTools;
- We identified a relatively high number of SmokedHam variants, with different delivery and persistence techniques, indicating a prolific threat actor iterating on tooling;
- We believe this threat actor to be increasingly targeting European organizations since early 2026.

Introduction

Between early February and early April 2026, **Orange Cyberdefense CERT** was involved in **separate malvertising incidents** affecting three European clients. All three infection chains observed by our analysts

revealed the use of the **SmokedHam** backdoor, delivered through malvertising and masquerading as common utility installers for RVTools or Remote Desktop Manager (RDM).

In one particular incident, the **SmokedHam** infection led to the deployment of **Qilin** ransomware. This case also featured:

- The use of two employee monitoring solutions to further **blend malicious actions into legitimate activity**, as well as legitimate tools and utilities like PuTTy and Kitty SSH clients, Zoho Assist RMM, and Total Commander;
- The use of Cloudflare Workers for domain fronting;
- The use of standard AWS infrastructure endpoints.

The following report delves into the execution chain, malware analysis, and broader infrastructure and adversarial observations. Most notably, we found several overlaps with the Tactics, Techniques and Procedures (TTPs) of **UNC2465**, a known ransomware affiliate historically associated with DarkSide, LockBit and Hunters International distribution.

This report aims at highlighting the evolution of SmokedHam variants, by comparing more than 30 samples retrieved in 2025 and 2026. We also provide IOCs, hunting guidelines, and recommendations at the end.

A version of this investigation was presented during **Botconf 2026** in Reims.

Analysis cut-off date: April 8th, 2026

Indicators of Compromise (IOCs)

IoCs are available here: https://github.com/cert-orangecyberdefense/cti/blob/main/smokedham/iocs

Orange Cyberdefense's Datalake platform provides access to Indicators of Compromise (IoCs) related to this threat, which are automatically fed into our Managed Threat Detection services. This enables proactive hunting for IoCs if you subscribe to our Managed Threat Detection service that includes Threat Hunting.

Orange Cyberdefense's ThreatMap service offers the ability to automatically feed network-related IoCs into your security solutions. To learn more about this service and to find out which firewall, proxy, and other vendor solutions are supported, please get in touch with your Orange Cyberdefense Trusted Solutions representative.

The **Orange Cyberdefense Computer Security Incident Response team** (CSIRT) provides emergency consulting, incident management, and technical advice to help customers handle a security incident from initial detection to closure and full recovery. If you suspect being attacked, do not hesitate to call our Hotline.
