TamperedChef Malware Infects European Endpoints via Fake PDF Editor

COPENHAGEN, DENMARK, September 2, 2025 /EINPresswire.com/ -- Heimdal Security's MXDR team has confirmed infections across European organizations, tied to a stealth malware campaign dubbed TamperedChef.

The attack, first observed in June 2025, spread via a fake PDF editor (AppSuite PDF Editor) promoted through ads and compromised websites.

The malware appeared functional but lay dormant for 56 days, activating on 21 August to exfiltrate browser credentials, cookies, and session tokens.

Infections were found in 0.03% of Heimdal's European customer base. While that percentage appears small, extrapolated across the wider region it represents a significant footprint.

> The golden rule in cybersecurity is that if something is free, then you are the product, or at least you will become one. TamperedChef demonstrates how attackers exploit this behavior"
>
> *Marian Olteanu*

"It's simple," said Marian Olteanu, Heimdal's threat intelligence security analyst.

"A user needs a specific tool not available in their standard software suite, like Adobe Pro which requires an expensive license, so they search online for free alternatives."

Key technical details

- Obfuscation: Code heavily obfuscated and may be AI or LLM generated to evade antivirus detection (Truesec, G DATA)

- Persistence: Registry modifications and scheduled tasks

- Commands used: --install, --fullupdate, --check

- Infrastructure: More than 40 domains, signed by suspicious Malaysian companies (Truesec)

- C2 servers: Confirmed activity at mka3e8.com; Expel also reports links to 5b7crp.com and y2iax5.com

- The campaign is linked to previous operations involving ManualFinder, OneStart Browser, and Epibrowser, suggesting a long-running and organized threat actor.

Recommendations for Organizations

Heimdal advises organizations to:

- Scan endpoints for known indicators of compromise

- Reimage affected devices and reset credentials (manual removal is not a safe remediation step)

- Deploy advanced behavioral monitoring tools

- Restrict installation of unverified software

- Educate employees to install software only from verified vendors, since free or unlicensed tools are a common source of malware

Read the full investigation here: https://heimdalsecurity.com/blog/heimdal-tamperedchef-investigation/

About Heimdal

Established in Copenhagen in 2014, Heimdal empowers CISOs, security teams, and IT administrators to improve their security operations, reduce alert fatigue, and implement proactive measures through a unified command and control platform.

Heimdal®'s award-winning cybersecurity solutions span the entire IT estate, addressing challenges from endpoint to network levels, including vulnerability and patch management, privileged access, Zero Trust implementation, and ransomware prevention.

Daniel Mitchell

Heimdal Security
email us here
Visit us on social media:
LinkedIn
Facebook
YouTube
X
