

Signal & Noise

🕒 INCIDENT SPOTLIGHT

Security Software or Security Risk?

3 "utility" apps in five weeks, each one a Google ad away. One of them was a webcam monitor called Camera Shield AI, and it turned out to be adware: software that earns its operator money by pushing ads and offers at whoever installed it. All three were signed. The one we could trace came from a Google ad on a manual-download site.

Our vSOC got involved when a scheduled scan flagged the document reader sitting in the Downloads folder. That was the only one that got caught. Camera Shield AI had been installed since June, starting on every login and checking in with its operator every day, and nothing had flagged it.

Here's how the delivery works. The ad ran on a site that hosts free PDF manuals and led to a page saying the download was ready. Every visitor gets a unique filename, so there's no single file

to block. They got what they came for, plus a tray app.

The app really does monitor the webcam and microphone. That's the cover. Behind it, a remote server decides which pop-ups to show and when, and the big one asks to switch your browser's search engine to Yahoo through the operator's partner codes. Every redirected search earns them a cut. Part of the code is decrypted and loaded straight into memory, so it never sits on disk where a scanner can read it.

On this machine the pop-up appeared once, the user clicked no, and the search engine stayed Google. No backdoor, no stolen credentials. But the app ships with an updater that downloads and runs whatever the server points it to. It was never used here. That's an install base waiting for a better offer - the same channel could deliver something far worse tomorrow.

IN THIS ISSUE

Incident Spotlight	01
Meet the Analyst	02
Ask an Analyst	02
Eye on the Threatscape	02

🕒 THIS WEEK IN CYBER HISTORY

OCT 12 · 2024 · JAPAN

Two years ago this week, the [Pokémon "Teraleak"](#) hit the internet. Around 1TB stolen from Game Freak in August started spilling online: source code, beta Pokémon designs, and unannounced games. Personal details of 2,606 employees and contractors went with it.

🔍 CASE AT A GLANCE

What fired
Scheduled scan flagged one installer

How it arrived
Google ads aimed at manual searches

What it was
Signed utility apps with daily check-ins

The money
Pop-up offers to hijack search

Response
Removal, domain blocks, custom IOCs

⚠️ WHY THIS MATTERS

Not every threat wants your passwords. Adware like this makes money off the install itself, and signed software from a legit-looking download page **doesn't trip the alarms people expect**. The main app ran for four months without a single detection.

The bigger issue is the updater. An operator with thousands of quiet installs and a way to push code to all of them **can change what that software does overnight**.

MEET THE ANALYST



Maya Douglas
SOC ANALYST II

Maya's security career began during her CS undergrad at CU Boulder and has spanned contracting at Microsoft and running cybersecurity for MSPs. Four years writing for Her Campus means she came into security already knowing how to tell a story.

A Girl Security alum, WiCyS member, and CTF designer, she believes the best defenders come from everywhere. RADICL's focus on the Defense Industrial Base fits her passion for the segment that gets overlooked and underprotected.

“

The companies that get hit hardest are the ones everyone assumes are too small to be a target.

MAYA DOUGLAS, SOC ANALYST II • RADICL

ASK AN ANALYST

CYBERSECURITY AWARENESS MONTH

What's one security myth you wish would die?

"That cybersecurity is someone else's job. Everyone with a login is part of the defense, and a lot of attacks still start with one click on a link that looked harmless enough."

DAKOTA GOULD • SENIOR SOC ANALYST

Dakota is the senior analyst our team goes to when a case gets weird. He's seen enough to know most incidents start with one click from someone who figured security was IT's problem.

EYE ON THE THREATSCAPE

Hackers Turned Up the Heat in Hundreds of French Supermarkets

Overnight on October 11, attackers took control of refrigeration controllers at hundreds of French supermarkets, including Intermarché, Coopérative U, and Carrefour, and forced them into a defrost cycle that didn't set off any alarms. Some fridges hit 122°F, a few caught fire, and stores threw out entire aisles of fresh and frozen food.

The controllers were legacy Danfoss units on outdated firmware that no longer gets security updates. An August research report had already shown how to bypass their login. Nobody has claimed it yet, and ANSSI is investigating.



Your dedicated vSOC & compliance partner. Military-grade managed cybersecurity for the Defense Industrial Base.

radicl.com