WEEKLY THREAT BRIEF

Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 09 · WEEK OF AUG 31, 2026

INCIDENT SPOTLIGHT

A Clean Antivirus Score Is Not a Verdict

Someone plugged a drive into a laptop and opened a shortcut on it eight times in half a minute. What it ran was real antivirus software, properly signed, and 75 engines call it clean. That is exactly why it was chosen.

On a Monday morning, a laptop in a client's overseas office fired nine detections in under eight minutes. Behind all of them was one shortcut on a removable drive, double-clicked **eight times in 32 seconds**.

```
cmd.exe /q /c
"RECYCLER.BIN\1\CEFHelper.exe 567
51"
```

That folder is a costume. Windows never creates a directory called **RECYCLER.BIN**, and the program inside it was living on the drive, not the machine. Its filename was CEFHelper.exe. Its real name, written into the file itself, was **wsc_proxy.exe**: genuine, validly signed Avast antivirus software, sitting where Avast would never put it.

Seventy-five antivirus engines call that file clean, and they are right to. It is authentic vendor code. It is also a known **side-loading carrier**. Based on search order, Windows programs can pull in helper libraries by filename from their own folder first, and they don't check who wrote them. So an attacker writes a malicious library, gives it the name the trusted program expects, and stands the two side by side. The signed program loads it, and the attacker's code runs as that program, under its signature.

The signature checking out is not reassuring. It is the point. Our sensor's cloud verdict on that same hash came back malicious while the public engines saw nothing wrong, and it killed and quarantined the file on all nine detections, every single attempt, without anyone touching a keyboard.

It got as far as creating two empty folders to work out of before our EDR killed the process. Nothing was ever written into them. No outbound connection, no domain lookup, no second program started, no scheduled task, no injection into anything else. Across the client's whole fleet over 14 days, the file shows up on **exactly one machine**.

So the alert is closed and the case is not. The malicious library lived on that drive, and the drive walked out of the building in someone's pocket. **Where it has been plugged in before is the question that actually matters**, and no amount of endpoint telemetry answers it. That is a conversation with a person, and it was the first thing we asked for: recover the drive so we can neutralize the threat at the source.

IN THIS ISSUE

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

THIS WEEK IN CYBER HISTORY

AUG 31 · 2014 · GLOBAL

Hundreds of private celebrity photos hit the open internet, and everyone assumed Apple had been breached. It hadn't. Attackers had spent months phishing individual accounts and guessing security answers off public interviews, then walked in through the front door with valid credentials. No exploit, no malware, just patience.

CASE AT A GLANCE

What fired
9 detections, 8 behavioral plus 1 static, in under 8 minutes

What it was
Signed Avast binary renamed and staged on a removable drive

Technique
DLL side-loading behind a valid signature; VirusTotal 0/75

Verdict
Malicious; no payload written, no traffic, one endpoint

Response
Killed and quarantined on every attempt by policy

WHY THIS MATTERS

Signature checks and antivirus scores look for purely malicious tools, not legitimate tools that can be abused. Attackers pick signed vendor binaries precisely because those tools wave them through, so **the file being legitimate is the attack**. Anything that reads a scan result and stops there was never going to

A USB port is still a working attack path, and device control stops this class of delivery at the vector instead of at execution. **This one never got to run its payload**, and the follow-up is a drive to recover, not damage to undo.

MEET THE ANALYST

Dylan Haase

SOC ANALYST

Dylan spent his early career in military intelligence before earning a computer science degree from the Colorado School of Mines. He is drawn to the full picture of how attackers operate and how defenders catch them.

He brings blue team expertise to RADICL as a SOC Analyst defending Defense Industrial Base contractors, while pursuing red team skills on his own time, pairing both perspectives into a well-rounded security skill set.

> **A valid signature tells you who wrote a file. It doesn't tell you who is using it.**
>
> DYLAN HAASE, SOC ANALYST · RADICL

ASK THE SOC

"What's a red flag most people don't know to look for?" Three analysts answer.

SARAH MENNE

"Validate the sender's address, and read the subject line like you don't trust it."

DYLAN HAASE

"An offer too good to be true. Nobody pays $110k entry level to work from home."

BRENDAN DEWYSE

"If you weren't expecting it, it's probably phishing."

EYE ON THE THREATSCAPE

01 Open the Wrong Folder and Your Coding Agent Runs the Attacker's Code

Manifold Security disclosed eight flaws across seven command-line AI coding agents. A repository's own Git settings can name a command the agent quietly runs, outside its sandbox and with no approval prompt. It works when the repo arrives as raw files with its hidden .git folder intact, which a zip, a shared drive, or a USB stick preserves. Four were unpatched at publication.

02 The White House Is Giving Away Cyber Defense, Starting With Water

Project Watershed 250 launched Aug 31: six months of federal and private-sector cyber help, free, for Texas water and wastewater utilities, run by the National Cyber Director's office and Texas Cyber Command. Abbott cited an Iranian-backed attack on 30 water systems across 12 states. The pilot exists because small providers cannot staff a SOC of their own.

03 284 Million Records, and a Phone Call Is How It Started

McKesson, which delivers roughly a third of the prescription medicines in North America, confirmed data theft after ShinyHunters claimed 284 million records and demanded $55 million. That count is database rows, not unique patients. And the group's way in is usually not an exploit. It is a phone call talking an employee out of their login.

VSOC TIP OF THE WEEK

A signed file in the wrong folder is still an attack. Your antivirus checks who wrote a program, not who put it there or what it loads next, so a real signed tool sitting on a drive in a folder Windows never made is a red flag on its own. Don't run it, don't copy it off, and hand the drive to IT so they can look at what came with it.