

Signal & Noise

🕒 INCIDENT SPOTLIGHT

The Cryptominer in Your Pocket

A USB stick tried to turn a laptop into a crypto mine. Nobody clicked, and we can prove nothing spread.

Almost everyone has done it. A conference giveaway, a stick from the print shop, a colleague's drive. Plug it in, grab the file, move on. A client did exactly that last week, and CrowdStrike quarantined a file off the stick before anything ran. The laptop was offline at the time, so the alert only reached our vSOC once it reconnected.

The infected stick **hides your real files and leaves one shortcut** that looks like your drive. Click it and your files open as usual, so nothing seems wrong. Meanwhile a cryptominer installs itself in a fake Windows folder whose name differs from the real one by a single invisible space. It even pauses when you open Task Manager to see why your laptop is slow.

Analyst Dylan Haase matched the file's behavior to a known USB cryptomining campaign. No published fingerprint matched, so he worked from where the file hid and what it impersonated. It's opportunistic and money-motivated, not aimed at anyone in particular. Then **we proved it didn't spread**. We checked every protected device for any trace of the campaign and found none.

The stick itself still carries the rest of the malware, so it needs a wipe before anyone uses it again. Plug it into another computer without protection and that machine becomes the next miner. The user's real files are fine, hidden in a folder on the stick, and can be recovered on a protected computer.

IN THIS ISSUE

Incident Spotlight	01
Meet the Analyst	01
The Black October Special	02

🕒 THIS WEEK IN CYBER HISTORY

OCT 31 · 2005 · GLOBAL

Researcher Mark Russinovich [found a rootkit on his PC](#) and traced it to a Sony BMG music CD. Copy protection, allegedly. It hid files from antivirus, so malware writers did the obvious thing and hid behind it.

🔍 CASE AT A GLANCE

What it was
USB-spreading Monero cryptominer

How it arrived
Infected USB stick

Response
Quarantined on mount; every device checked

Impact
Nothing ran; no other device touched

👤 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. At RADICL he defends Defense Industrial Base contractors as a SOC Analyst. Off the clock he practices offense, and ranks in the top 1% on TryHackMe.

FOUND A STRAY USB STICK?

Don't plug it in to see what's on it. Hand it to IT, unopened, and tell them where it came from.

vSOC TIP OF THE WEEK

🧠 SPECIAL EDITION

The Black October Special

OCT 2026 • 5 STORIES

WHAT IT IS

Threat actors did the heavy lifting this Cybersecurity Awareness Month. On October 21 alone, emergency fixes dropped for PHP, GitLab, and Google's Brotli, attackers hijacked the AI gateway LiteLLM, and governments took their own websites offline to patch. **Some of the most widely used software online broke in the same week.** The security press started calling it [Black October](#).

WHERE AI COMES IN

AI models flagged two of this month's worst bugs. Calif researchers found php2shell with OpenAI's GPT-5.6 Sol, and OpenAI's own security tools caught the Brotli flaw. Then php2shell's details leaked, and **attacks began before the patch even shipped.**

01 THE BIG ONE

AI Helped Find Two Critical PHP Flaws

On October 21, PHP shipped emergency fixes for two critical flaws, nicknamed php2shell, that let anyone run code on a web server without logging in. They go back to version 5.4. Researchers at Calif found them using OpenAI's GPT-5.6 Sol, and a Wiz team traced the same bugs independently with Google's Gemini. Details leaked before the patch, attacks started almost immediately, and the NSA's advice was refreshingly blunt: update now or unplug.

Wiz also showed working attacks against WordPress, Drupal, and Joomla. If your website runs on PHP, ask your host if it's patched. If it's older than 8.2, that's not a patch conversation. That's a migration. And 8.2 itself reaches end of life December 31.

02 [Eight Broken Certificates, One Exit](#)

Remember last week's weak-key certificate scare? The company behind it is out. On October 22, eMudhra said it was leaving the global SSL/TLS business after browsers stopped trusting it. Hard to sell trust nobody's buying.

04 [GitLab Patches a Remote Code Execution Flaw](#)

Fixes landed October 21 for a flaw that can let an attacker run code on self-managed GitLab servers. GitLab won't say under what conditions, so self-managed instances should update now.

03 [One Old Key, 49,000 Poisoned Downloads](#)

In May, LiteLLM leaked a config file holding a master key, pulled the file, and never revoked the key. An attacker used it to take over every LiteLLM repo, then shipped a poisoned 1.107.0, downloaded about 49,000 times. Installed it? Rotate every credential that machine could reach.

05 [A Compression Bug Hiding Everywhere](#)

Google's Brotli compression library got a fix for a flaw that lets a crafted file crash software, and possibly take it over. It sits inside Node.js, Firefox, and Thunderbird. Chrome isn't on the affected list so far. Regular updates include the fix.



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

radicl.com