WEEKLY THREAT BRIEF

Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 04 · WEEK OF JUL 27, 2026

INCIDENT SPOTLIGHT

Time-Traveling Worm Found Out of Its Natural Habitat

A worm family first seen in 2008 surfaced on a client endpoint this week, contained in seconds and confirmed by analysts who had worked this exact family before. That is the only reason it's a newsletter item and not an incident.

Something that belongs in a museum turned up on a working endpoint this week. A worm whose heyday ended before most of this client's hardware existed arrived on a drive attached to a machine we defend, and it was over in **seconds**.

The file was hiding in a fake recycle bin folder on a secondary drive, under a made-up user ID, with a random eight-letter name and a VMware extension it had no business wearing. Every one of those is a **Conficker** calling card, and our analysts read the path before a single lookup came back. **66 of 70** vendors agreed with them.

That recognition is the whole value. A team seeing this for the first time spends an hour proving what the file is, then another deciding whether the host is on fire. Ours had worked Conficker before and went straight to the only question that mattered: where did this drive come from? Buying a sensor is easy. Having someone on the other end who has already met what it caught can't be licensed.

Conficker infected millions of machines starting in 2008: an old Windows version, weak network shares, and removable drives that auto-ran on the next host they touched. Microsoft patched the flaw within weeks, and Windows killed auto-run years ago.

The file, though, doesn't expire. Copies still circulate on removable media and file shares long after the outbreak ended, and one reached this host. Quarantined in **seconds**, escalated in minutes. It never ran and never spread.

That outcome was not luck. Drop the same drive into the wrong Windows version, auto-run enabled, flat shares, no endpoint coverage, and it does what it did in 2009: **it spreads**. Modern infrastructure closed that door, the endpoint caught what walked up, and analysts who knew this adversary closed it the same hour. Remove any one and this is a different story.

IN THIS ISSUE

THIS WEEK IN CYBER HISTORY

LATE JUL · 2022 · ALBANIA

State-sponsored Iranian actors hit Albania's government infrastructure with a combination of ransomware and data-wiping malware, destroying state records and locking citizens out of critical public services. The collapse was severe enough that Albania cut diplomatic ties with Iran that autumn.

CASE AT A GLANCE

What it was
Conficker / Downadup worm file at rest (jwgkvsq.vmx)

How we caught it
On-sensor machine learning; High severity, 100% confidence

Consensus
66 of 70 vendors flagged the same hash

Verdict
True positive; dormant, non-propagating artifact

Response
Quarantined on detection; no execution or spread

WHY THIS MATTERS

Most SMBs would never have seen this. No sensor on the endpoint, no analyst on the alert, and a known worm gets a foothold nobody notices for months. **Dwell time is the whole game**, and it starts the second the drive goes in.

Detection and expertise are not the same product. Tooling flagged the file; people who had met this adversary before closed it in minutes with no business disruption. That combination is **what a managed vSOC actually buys you**.

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 underserved Defense Industrial Base fits her passion for SMB security: the segment that gets overlooked, underprotected, and increasingly targeted by nation-states.

> **"The companies that get hit hardest are the ones everyone assumes are too small to be a target.**
>
> MAYA DOUGLAS, SOC ANALYST II · RADICL

CASE SPOTLIGHT

TRUE POSITIVE · BRENDAN DEWYSE

A staff member fell for a fake CAPTCHA trick called "ClickFix," pasting a command into Windows' Run box that looked like a routine fix-it step. That paste pulled a file from a remote server and ran it, hiding inside a legitimate process and calling out to attacker infrastructure. It ran roughly three minutes before we caught it, isolated the machine, and confirmed no spread.

TRUE POSITIVE · PAUL PRAWDZIK

An alert flagged a browser reaching actor-controlled domains seconds after a visit to a legitimate supplier site, a technique called EtherHiding where malware reads its next stage from a blockchain instead of the hacked site. The timeline showed the chain stopped there: no download, no execution. Contact confirmed, no compromise.

TRUE POSITIVE · MAYA DOUGLAS

A reported email came from a lookalike domain registered a month ago, impersonating a real defense-robotics manufacturer and borrowing its product language for a credible pretext. One recipient, an unsolicited attachment, a non-standard Message-ID pointing to custom mailing infrastructure. Spear-phish, not cold outreach.

EYE ON THE THREATSCAPE

01 One Town Declared a State of Emergency Over Its Water. Hackers Did It in Two Days.

A coordinated attack hit the control systems of 30+ Minnesota water utilities on July 26 and 27, forcing operators to run plants by hand. Maple Plain declared a state of emergency; Braham banned lawn watering. CISA, the FBI, and the state CISO are all in it, and researchers suspect Iran-linked CyberAv3ngers. These were small, rural utilities. That was the point.

02 An AI Just Broke Crypto We Were Told Would Survive Quantum Computers

Anthropic's Claude Mythos Preview found faster end-to-end key-recovery attacks against post-quantum test schemes like HAWK-256, and sped up attacks on 7-round AES-128. These are research targets, not your VPN. But the assumption that novel cryptanalysis takes a specialist and a decade just got a lot shakier.

03 That $38 Streaming Stick Is Renting Out Your Internet Connection

Cheap generic TV boxes promising unlimited content are known to quietly resell the buyer's bandwidth to strangers. New Bitsight research found they also impersonate phones to click ads on AI-generated sites, defrauding merchants and ad networks at scale. A researcher mapped it by registering a domain it let expire.

VSOC TIP OF THE WEEK

Don't plug in the USB. Not the one from the parking lot, not the one a vendor handed you, not the unlabeled one in the supply drawer. The worm we caught this week arrived on a drive nobody had reason to trust. Unaccounted-for media is unknown until it's scanned. If something feels off, send it our way and we'll run it down.