WEEKLY THREAT BRIEF

Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 03 · WEEK OF JUL 19, 2026

INCIDENT SPOTLIGHT

One Rust Loader, Five Platforms, a Hidden Sliver Implant

RADICL doesn't just watch for alerts, we hunt the threats behind them. Our team uncovered an active malware operation, tracked the group as UNC-RAID-M8280, and turned that research into protection for the clients we defend.

Our analysts found a group running a stealthy, two-part attack. A small first-stage program quietly downloads and unlocks a hidden second program, a modified version of **Sliver**, a legitimate hacking tool that attackers have turned against their targets.

What stood out was the discipline. One toolkit was built to run on **five different systems**, Windows and four flavors of Linux, all from the same template. We traced the group's activity back through **four waves of uploads**, from June 2024 to June 2026.

This wasn't off-the-shelf Sliver, either. The attackers had customized it with their own hidden features, a fingerprint that let us tie every sample back to the same operation.

The clever part was the hosting. Both stages sat inside a **misconfigured cloud storage bucket owned by an unrelated company**, left open to the public. The group got free, trusted hosting and left no infrastructure of its own to trace.

The command channel was hidden the same way, routed through **Cloudflare Tunnel** so the operator's real server never appeared in any public record. Blocking the group means blocking its domains, not chasing shifting IPs.

RADICL got the exposed storage **taken down**, then built detection from what we learned so this tradecraft is caught across every client we protect.

Loader and payload signatures, key-reuse mapping, and full IOCs are published for defenders.

FULL TECHNICAL BREAKDOWN ON OUR BLOG →

IN THIS ISSUE

THIS WEEK IN CYBER HISTORY

JUL 19 · 2024 · CROWDSTRIKE

A faulty CrowdStrike sensor update crashed millions of Windows machines worldwide, grounding flights, halting hospitals and banks, in the largest IT outage in history, no attacker required.

Fun fact: our own Maya worked at Microsoft while this happened. Not a cyberattack, but close enough.

CASE AT A GLANCE

What it was
Two-stage Rust loader delivering a modified Sliver C2 implant

How it arrived
Staged in a misconfigured third-party cloud bucket

Scope
5 platforms, 31 objects, four waves (2024–2026)

Tracked as
UNC-RAID-M8280; custom "FlyFire" Sliver fork

Response
Abused bucket reported and mitigated by the provider

WHY THIS MATTERS

Sliver is legitimate red-team tooling, which is exactly what makes a modified fork dangerous: it blends into the noise and defeats signature-only detection. Borrowed cloud storage and Cloudflare Tunnel mean **there is no attacker-owned infrastructure to block**, and the C2 origin never touches DNS.

This is the intel that stops the next intrusion. We didn't just catalog samples, we published loader and payload signatures, mapped the key-reuse across waves, and got the live delivery point taken down, turning one operation's tradecraft into **detection for everyone we defend**.

MEET THE ANALYST

Will Seligman

RAID TEAM

Will works across security operations at RADICL, including threat intelligence, hunting, detection engineering, incident response, and adversary tradecraft.

He's part of RADICL's RAID team, Research, Adversary Intelligence, and Detections, the unit that hunts attackers, reverse-engineers their tradecraft, and weaponizes what it learns into detections that protect every client. He's automating the path from intelligence to protection.

> **Any tool can block an attack it already knows. The fun part is pulling one adversary apart and figuring out how they got in and where they hid, then building the thing that catches them at the next client before they even start.**
>
> WILL SELIGMAN, RAID · RADICL

CASE SPOTLIGHT

TRUE POSITIVE · DYLAN HAASE

A staff member downloaded a fake "PDF converter" that was really bundled adware, from a lookalike site pushed by a malicious ad. Our sensor quarantined the file the instant it hit disk, before it could run. We confirmed it never executed, checked it hadn't spread to any other machine, and removed it, and the site serving it went dark within a day.

TRUE POSITIVE · PAUL PRAWDZIK

An alert flagged one program injecting code into another, behavior that usually signals an attack. Reviewing the activity around it showed the real cause: a developer's code editor attaching its debugger to a script they were running. Genuine injection, but a legitimate tool, so we confirmed it safe and tuned the alert to stop firing on it.

TRUE POSITIVE · DYLAN HAASE

A reported email was a scam impersonating a company executive, sent from a lookalike Gmail that faked a real reply thread to push a payment. It cleared basic sender checks by riding Google's own mail servers, and was one of several coordinated attempts at different staff. We confirmed it malicious, blocked the senders, and warned the whole company.

EYE ON THE THREATSCAPE

01 Patch Now: CISA Urges Immediate SharePoint Updates After Active Attacks

CISA flagged four SharePoint Server flaws under active exploitation, including a zero-click bug, and added them to its Known Exploited Vulnerabilities catalog. Every supported on-prem version is affected, and federal agencies were ordered to patch on a deadline. Why waiting isn't an option: our blog breaks it down.

02 Rogue AI Agent Hacked a Company On Its Own

The world's largest AI model hub was breached when an autonomous agent ran code via a malicious dataset, stole credentials, and moved across internal systems over a weekend. The twist: OpenAI said the culprit was its own sandbox-escaping models, tested with safety limits reduced.

03 FBI Surveillance System Breached by Chinese Hackers

The FBI disclosed a "major cyber incident" to Congress after one of its surveillance systems was compromised, reportedly exposing phone numbers of wiretap targets. Chinese state hackers are blamed for the breach of the unclassified network, and the fallout is still unfolding.

VSOC TIP OF THE WEEK

A file from a name you trust can still be dangerous. This group hid its malware inside a real company's cloud storage that was accidentally left open to the public, so everything looked legitimate. Two simple habits help: be cautious with anything that downloads and runs on its own, even from a familiar source, and make sure any cloud storage your business uses isn't set to public by mistake. If something feels off, that's what your vSOC is for, send it our way and we'll run it down.