WEEKLY THREAT BRIEF

Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 07 · WEEK OF AUG 17, 2026

CAMPAIGN BRIEF

Attackers Are Getting Smarter: Don't Rely on Reputation Alone

BY SARAH MENNE, SOC ANALYST II

A phishing campaign reached ten of our client tenants this month without spoofing a single sender, compromising a single account, or registering a single new domain. Every reputation check it passed, it passed honestly.

An attacker signed up for a trial account on a legitimate, well-established educational CRM, then used that platform's own notification system to send phishing at scale. No spoofing. No compromise. Every reputation check on the way in came back clean, because the sending infrastructure genuinely is legitimate.

01
THE ACCOUNT
A free trial on a real education platform. No stolen credentials, no compromised mailbox. Just a signup form and a card.

02
THE SENDER
Mail leaves through the platform's own notification system, inheriting a clean shared sending reputation the attacker did nothing to earn.

03
THE LINK
A payload domain roughly a decade old per DNS and WHOIS. Too boring for newly-registered-domain scoring to flag.

04
THE TELL
Subject lines personalized per company. Ten tenants, 47 recipients. This was aimed, not blasted.

WHY THERE'S NO CLEAN BLOCK

The sender domain is legitimate shared infrastructure and the sending IPs sit in a shared mail-provider pool. Block either one and unrelated legitimate mail goes down with it.

Microsoft's own detection flagged the content independently as Phish, Malicious by fingerprint and URL reputation, and auto-quarantined a number of these after delivery. **That native detection, plus client awareness, is the mitigation.**

WHAT ACTUALLY CAUGHT IT

01 **Cross-tenant view.** Isolated, these were low-priority user-reported spam tickets. Correlated, they're one campaign.

02 **The ask, not the sender.** Reputation said clean. What the message wanted did not.

03 **Native quarantine.** Microsoft's post-delivery detection did real work here. Let it run.

04 **User reports.** Every one of these started with somebody hitting the report button.

`The sender was real. The domain was old. The message was still a phish.`

WHY THIS MATTERS

Reputation is a measure of history, not intent. A platform that has sent legitimate mail for years keeps its clean record on the day an attacker rents ten minutes of it. Filters score the infrastructure. They do not score the ask.

You are not expected to audit sender infrastructure. You are expected to notice when a message you did not ask for wants you to log in somewhere. Report it, and let us do the correlating. Looked at one inbox at a time, this never rises above **noise**.

IN THIS ISSUE

THIS WEEK IN CYBER HISTORY

AUG 19, 2003 · SOBIG.F

At its peak, one in every 17 emails on the internet carried it. The worm harvested address books from infected machines and forged its sender line with names recipients already knew. It exploited nothing. It borrowed trust.

HOW IT PASSED INSPECTION

Legitimate sender
Real SaaS platform, real notification system, nothing spoofed

Inherited reputation
A clean sending history the attacker rented rather than built

Aged domain
Roughly ten years of DNS and WHOIS history, so age scoring stayed quiet

Personalized subject
Written per company, not one template sprayed wide

Single-tenant blindness
Low-priority spam reports until somebody looked across all ten

MEET THE ANALYST

Sarah Menne

SOC ANALYST II

Sarah is a SOC Analyst II at RADICL. Before joining the team she spent nearly four years with the National Oceanic and Atmospheric Administration, starting as an IT intern responsible for hardware and applications across ships, aircraft, and ground facilities, along with user accounts, permissions, and access rights.

From there she stepped into an Information Technology Security Specialist role, monitoring and responding to threats across NOAA's systems and working with IT security and compliance teams on detection and escalation. Her path started earlier, in the U.S. Army, where she spent two years as a Signal Support Systems Specialist with postings in Texas, South Korea, and Georgia. That grounding still shows in how she works the floor today.

> **One tenant's noise is ten tenants' campaign. You only see it if you're looking at all of them.**
>
> — SARAH MENNE, SOC ANALYST II · vSOC

CASE SPOTLIGHT

CLEAN TO SCANNERS

A user clicked a link that every automated check called safe. Crawlers fetching the URL got a harmless redirect loop; live fetches from real devices landed on a credential-harvesting page, which sat open about 45 seconds. Nothing ran on the endpoint, and a 27-day sign-in review found no unfamiliar authentication. Credentials rotated, sessions revoked, infrastructure blocked.

UNSIGNED · OPEN INQUIRY

A repackaged, unsigned build of a torrent client with logon persistence ran five days on a machine carrying the customer's EDR sensor. Detonation reached only the vendor's own infrastructure, and a tenant-wide sweep found the file nowhere else. The process was killed; the binary and its autostart entry remain. Whether the device is company-issued or personal decides what happens next.

BENIGN · AI TOOLING

A suspicious JavaScript alert on a developer workstation traced back to an AI coding assistant capturing a debug screenshot from its own scratch folder. Full process ancestry confirmed it, and nothing left the tool's working directory. Closed benign. Even the robots helping write code can set off alarms built to catch actual bad guys.

EYE ON THE THREATSCAPE

01 The Exploit Script Wrote Itself

Five federal agencies issued a joint advisory on Aug 19 warning that attackers are using AI-generated exploitation scripts, dressed up as legitimate OT monitoring tools, against internet-exposed Siemens S7 controllers. The advisory names the Defense Industrial Base among the sectors that could be hit. Their words, not ours: "This is not a theoretical risk." AI didn't invent the attack. It removed the expertise it used to require.

02 Your Org Chart, For Sale

A threat actor is selling employee directories pulled straight out of nine large companies' Microsoft Entra tenants, roughly 3.6 million records. No Azure flaw was involved. Researchers tie the access to credentials harvested by infostealer malware on employee machines. The dumps include job titles, service accounts, and admin identities, which is a target list for the next phishing round.

03 The VPN That Watches

Researchers linked 737 free VPN and proxy extensions in the Chrome Web Store to a single operation, 274 of them impersonating names like NordVPN, Proton VPN, and ExpressVPN. Once connected, they route the entire browser session through the operator's own proxy servers. Google pulled some; hundreds stayed listed. Worth an extension inventory on managed devices.

VSOC TIP OF THE WEEK

If an email asks you to sign in, don't use the link to get there. Open the site the way you normally would, by bookmark or by typing the address, and see whether the same thing is waiting for you. If it isn't, send us the email.