WEEKLY THREAT BRIEF

Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 02 · WEEK OF JUL 12, 2026

INCIDENT SPOTLIGHT

Five Days In, One Analyst Beats the Clock on Live Fraud

A stolen session token had a client mailbox live for days and the fraud emails were already going out. Our SOC read the one signal others miss, pinned the exact account, token, and hidden rule, and shut it down before a single payment moved.

The clock was already running. An administrative-tier mailbox had been live in the attacker's hands for roughly five days, operated from Nebraska-geolocated infrastructure far outside the user's baseline, with fraud emails going out in real time.

The tell was one most tooling would wave off, and our analyst didn't: **concurrency**. The **same session token** was in use from the legitimate user's location and the actor's Nebraska infrastructure at once, a textbook fingerprint of **session token theft (MITRE T1539)**.

That read cracked it open. Inside the mailbox sat a concealment inbox rule: an **obfuscated single-character name**, StopProcessingRules set, filtering external addresses so the fraud replies stayed invisible to the real owner.

From that mailbox the actor was hijacking live conversation threads with **invoice and purchase-order lures** to affiliated-domain recipients, a payment-redirect scheme built to reroute a real payment before anyone noticed.

Because our team had already isolated the exact account, token, and rule, containment was immediate: the client's IT team removed the rule, purged the fraudulent invoices, revoked active sessions, and reset the password in a single coordinated pass. No delegated access or OAuth grants were left behind.

Hardening followed to close the path: **device-compliant Conditional Access** and continuous access evaluation to force re-auth on concurrent-geography token use, plus alerting on high-risk inbox rules.

IN THIS ISSUE

THIS WEEK IN CYBER HISTORY

JUL 12 · 2024 · AT&T

AT&T disclosed that call and text records of nearly every wireless customer were exfiltrated, one of two 2024 breaches exposing over 100 million people.

Fun fact: our own Will was on the security side at AT&T during this breach, leading MDR threat hunting and working with the Central Security Office.

CASE AT A GLANCE

What it was
Business email compromise via stolen session token

How it arrived
Token replay from Nebraska-based infrastructure

Scope
Admin mailbox; ~5-day dwell, no OAuth or delegate grants

Confirmed impact
Payment-redirect fraud via hijacked invoice threads

Response
Rule removed, invoices purged, sessions and password reset

WHY THIS MATTERS

Business email compromise rarely trips an alarm. There is no malware, just a quiet inbox rule and a hijacked invoice thread, and MFA alone won't stop a stolen session token. The only reliable tell is **the same token signing in from two places at once**, which most tooling never surfaces.

That's the difference managed detection and response makes. We didn't just raise an alert, we pinpointed the exact account, token, and rule, stopped the fraud before a payment moved, and hardened conditional access so it can't recur. The outcome our clients get is **a fix, not a ticket.**

MEET THE ANALYST

Dakota Gould

SOC ANALYST 3 · AI SOC OPERATOR

Dakota is a Lead Analyst in RADICL's vSOC, running incident response, threat hunting, and alert triage across a fleet of Defense Industrial Base clients. His path in has been managed services from the start: a degree in Computer Systems Security, then defending Fortune 500 companies from inside an MSP.

What sets the work apart is a builder's instinct: rather than clear alerts one at a time, he builds the automation the whole team runs on, believing DIB suppliers deserve the same defense as the primes they build for.

> **"The real leverage is taking one good investigation and turning it into repeatable tradecraft, codified and automated, so the TTPs we catch at one DIB supplier are ready to detect across the rest before they land. Force multiplication isn't a slogan; it's a requirement.**
>
> DAKOTA GOULD, SOC ANALYST 3 · vSOC

CASE SPOTLIGHT

TRUE POSITIVE · NO IMPACT

An endpoint reached a malicious IP tied to a ClickFix lure, the ploy that tricks users into pasting a PowerShell one-liner. We detonated the script in a sandbox, then hunted the whole environment for irm-based PowerShell and confirmed it never ran. Because the page could also stage an O365 login prompt, we rotated the user's password as a precaution.

TRUE POSITIVE · SHADOW IT

Endpoint telemetry flagged a personal MEGA cloud-storage client installed on a single host. The build was legitimate and we saw no bulk-archiving or staging that would signal data theft, but file transfers did occur. We raised it as an acceptable-use and DLP question; the client moved to ban the app.

TRUE POSITIVE · REMEDIATED

Endpoint telemetry surfaced Advanced IP Scanner running across several hosts, a legitimate tool but a common precursor to lateral movement and a favorite of ransomware crews. We flagged it for confirmation; the client verified it was unapproved and pulled it from every affected device, clearing the recon footprint before it could be abused.

EYE ON THE THREATSCAPE

01 DHS Twice Wrote Off Its Own Breach as a False Positive

A readout shows DHS staff dismissed intruders on the Homeland Security Information Network as harmless twice, letting them dwell for weeks and steal credential files. The network shares sensitive data across partners and is supporting World Cup security.

02 AI Isn't Just Planning the Break-In, It's Doing It

Check Point's 2026 report documents intrusions where AI ran exploitation autonomously, firing thousands of commands with little human direction. Attackers strip safety controls off stolen or open models, and the window from disclosure to working exploit now shrinks to hours.

03 Microsoft's Record 622-CVE Patch Tuesday

July's update was Microsoft's largest ever: 622 CVEs and two exploited zero-days, led by CVE-2026-56164, an unauthenticated, zero-click SharePoint Server flaw found during live attacks. It landed the same day 2016/2019 hit end of support.

VSOC TIP OF THE WEEK

MFA won't stop a stolen token. This intrusion rode a hijacked session token, so no MFA prompt ever fired, the attacker just replayed the session from their own infrastructure. You can't spot this from the inbox, it only shows up in sign-in telemetry, one session appearing from two places at once. That's exactly what the vSOC watches. Ask us to confirm token-aware conditional access is in place: compliant devices required and continuous access evaluation on, so a stolen token forces re-auth instead of walking right in.