WEEKLY THREAT BRIEF

# Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 05 · WEEK OF AUG 3, 2026

INCIDENT SPOTLIGHT

## One User Clicked, Caused More Users to Follow

The alert that opened this case was the least important thing in it: a user clicking a link, eleven hours after the takeover began and hours after the attacker had sent 89 emails and deleted the evidence. Everything that mattered was found working backward from it.

An adversary held a stolen **authentication token**, not a password. Replayed from an unmanaged, non-compliant device, it never triggered a password prompt, an MFA challenge, or a Conditional Access (CA) evaluation. The three controls that stop this were never reached. Eight sessions, **forty hours of dwell**.

The attacker read 55 mail items, built an inbox rule that silently deleted and marked read every inbound message, then mailed 89 recipients "Action Required: Project Documents & Payment Information" and hard-deleted the sent copies.

**Then it started spreading.** The recipient list deliberately included employees' **personal** addresses, outside Safe Links and every corporate control. Three more entered credentials on the phishing page; all three were replayed within minutes, one 87 seconds after the domain resolved. **Every replay hit Conditional Access and was blocked.** Five users touched, one account taken.

**Nailing it down took two analysts working opposite ends.** One reconstructed the 40-hour intrusion, isolating a single session ID and proving token replay from the absence of password and MFA request types, and mapping every downstream credential attempt to a CA block.

The other swept nine endpoints, cleared the fleet, and surfaced one artifact **absent from the identity investigation entirely**: a single host in direct TCP contact with the attacker IP. The sweep also pulled two things *out* of the incident: an unrelated malware host and a credential-tool finding that predated the phish by twenty hours, noise that would have inflated the scope.

The customer got a defined blast radius, a named list of unrotated credentials, and a root cause that rotation alone does not close. Not "you had a breach." Exactly this, exactly this far, and here is what stops it next time.

### IN THIS ISSUE



### THIS WEEK IN CYBER HISTORY

AUG · 2003 · WORLDWIDE

The Blaster worm tore through hundreds of thousands of Windows machines in days, crashing systems on a loop and clogging networks worldwide. It exploited a flaw Microsoft had patched 26 days earlier. Everything Blaster took was sitting behind an update nobody had installed yet.

### CASE AT A GLANCE

**What it was**
AiTM token theft → BEC takeover → internal phishing. No endpoint compromise.

**How we caught it**
One link-click alert, worked backward across two planes

**Blast radius**
1 account taken; 3 harvests, all CA-blocked; 89 recipients; 9 endpoints clean

**Verdict**
True positive; ~40 hours dwell; 23 failed re-entries after containment

**Root cause**
Replayed token accepted from a non-compliant device

### WHY THIS MATTERS

MFA was on, and the attacker got in anyway. It never had to break the lock, it stole a key that was already turned. **Most companies check who comes through the door and never check again after that.**

## MEET THE ANALYST

### Jason Jenkins

DIRECTOR OF INCIDENT RESPONSE

Jason has spent more than two decades finding the truth when the facts aren't immediately visible: the United States Air Force, then a law enforcement career spanning patrol, undercover narcotics, and detective work. Investigations are rarely about a single clue.

He brings that investigative mindset to DFIR, having worked every seat from analyst to leadership. When an organization is facing one of its worst days, incident response is about finding the facts, reducing uncertainty, and restoring confidence.

> **Hackers don't break in. They log in.**
>
> JASON JENKINS, DIRECTOR OF INCIDENT RESPONSE · RADICL

## CASE SPOTLIGHT

BENIGN POSITIVE · DAKOTA GOULD

A retired remote-access tool started up on a laptop at a client who had stopped using that software months earlier. The client asked for an immediate network quarantine. The evidence said it wasn't needed: IT confirmed it was left over from a retired sanctioned deployment, the employee had never launched it or granted anyone access, and telemetry showed the service started, checked in once, and never opened a session. One host, nothing else.

TRUE POSITIVE · BRENDAN DEWYSE

Users at two offices installed WPS Office, a Chinese-made alternative to Microsoft Office, on four laptops without going through IT. The client had ruled it out a week earlier, and it reports usage telemetry to servers in China. Nothing malicious: signed installers, no attacker infrastructure. It arrived one download at a time, which is how unapproved software gets in.

HUNT FINDING · JASON JENKINS

An estate-wide sweep after a cleared alert found encrypted personal webmail on two workstations at a defense contractor. One user opened a ProtonMail mailbox fifteen times over four days; the other once. Nothing shows data leaving, but mail a company cannot see into is a serious problem in an export-controlled environment.

## EYE ON THE THREATSCAPE

### 01 One Subscription Now Buys Three Ways Around Your MFA

The Greatness phishing kit, rented by the month over Telegram, now runs adversary-in-the-middle token theft, device code phishing, and OAuth consent abuse from one operator panel, against Microsoft 365, Google Workspace, and iCloud. Device code is the newest route and the easiest to shut: block the flow in Conditional Access unless a use case needs it.

### 02 CISA Says Attackers Are Already Inside This Build Server Flaw

CVE-2026-63077, a 9.8-severity flaw in on-premise JetBrains TeamCity, is under active exploitation. Build servers hold source code, signing keys, and deploy credentials, which makes them a shortcut into every customer a shop ships to. Patched versions exist. If you run TeamCity yourself, this is a this-week job.

### 03 The Fastest Way Into Your Company This Year Was a Phone Call

ShinyHunters has spent 2026 breaching household names without exploiting much of anything: callers posing as IT, walking employees and help desks through approving access or handing over an MFA code. AI voice tooling now scales the calls. No firewall stops a caller who convinces someone to open the door.

## VSOC TIP OF THE WEEK

**Check every edge device for end-of-life firmware this week.** A joint CISA/NSA/FBI advisory confirms Russian state actors are targeting unpatched routers and firewalls across the DIB as long-term footholds, not smash-and-grab hits.