WEEKLY THREAT BRIEF

Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 19 · WEEK OF NOV 9, 2026

INCIDENT SPOTLIGHT

The Sign-Ins Their Managed Provider Said Were Theirs

An attacker read one employee's mailbox for two weeks and used a lookalike vendor domain to join an invoice thread. The client's managed service provider said the sign-ins were theirs.

While we had the client on the phone, their managed service provider was telling them the sign-ins were routine, since they log in to that account regularly. Then the session signed in again, this time from Poland, and by midday the client agreed it had to be shut down.

The original alert was one sign-in from a UK mobile address, on a session that was already two weeks old. A Python script on Lithuanian hosting had created it, and Dylan Haase, the analyst on the case, found it relaying through three unrelated networks in four minutes.

He traced the start to a seven-minute window on Oct 26: an MFA approval, then two Windows laptops registered to the account, each with a Windows Hello sign-in key. Microsoft's risk engine reset the account's sessions two hours later, but the laptops stayed enrolled and the attacker was back the next morning.

Over the next 14 days they opened 89 emails. When a vendor invoice arrived, they registered a domain one letter off from the vendor's that morning, sent a message into the thread from it, and deleted the sent copy within seconds. Three days later the employee and a colleague replied to the lookalike domain about the invoice.

The attacker also sent a one-word "test" email to a second lookalike domain, and on the day of the alert deleted a shared "Paystub" notification from the inbox. Seven other employees had opened the same email.

No malware was involved. The client **removed the rogue devices**, reset the password, and revoked the unrecognized MFA methods.

IN THIS ISSUE

Incident Spotlight 01
Veterans Day 02

THIS WEEK IN CYBER HISTORY

NOV 2008 · PENTAGON · USA

One infected flash drive put the Agent.btz worm on both classified and unclassified US Central Command networks. This month in 2008, the Pentagon banned removable media across the entire Department of Defense. Officials called it the worst breach of US military computers ever, and the cleanup, Operation Buckshot Yankee, led directly to the creation of US Cyber Command.

CASE AT A GLANCE

What fired
Non-US sign-in via token replay

What it was
M365 account takeover staging a vendor payment redirect

Persistence
Two attacker-registered devices with Windows Hello keys

Dwell time
14 days

Response
Sessions revoked, account disabled; devices removed and MFA reset same day

WHY THIS MATTERS

Resetting a password or forcing a sign-out feels like cleanup. If the attacker registered a device, it isn't. **The device keeps them in** until someone goes into Entra and deletes it, and most SMBs never look there.

When an outside provider shares access to an account, their sign-ins give an attacker cover. **"That was us" needs checking** against the session itself, and any change to where money goes needs a call to a number you already had.

VETERANS DAY SPECIAL · NOV 11

Five RADICL Veterans

Five of the people defending our clients served first. This Veterans Day, we're introducing them.

FEATURED ANALYST · INCIDENT SPOTLIGHT



Dylan Haase

U.S. ARMY HUMINT · SOC ANALYST

Dylan spent four and a half years as an Army Human Intelligence Operator, a job built on getting information from people and testing it against everything else you know. On the page 1 case, he checked the provider's claim against the logs. Outside the SOC he does red team work as a bug bounty hunter, testing real companies' live systems, with permission, and reporting the vulnerabilities he finds.

He worked the account takeover on page 1, and he has contributed to more Signal & Noise investigations than anyone else in the SOC.

ALSO SERVING



Josh Shepard

U.S. AIR FORCE · DIRECTOR OF RAID

Josh has spent his career hunting nation-state hackers. After advising the Air Force CIO, he led the threat hunt team defending Air Force networks and industrial control systems against APTs, then ran intelligence-driven defensive cyber planning for more than 150 specialists across four combatant commands. He holds six GIAC certifications and now directs RAID, RADICL's research, adversary intelligence, and detections team.



Sarah Menne

U.S. ARMY SIGNALS · SOC ANALYST II

Sarah trained as a Signal Support Systems Specialist at Fort Gordon, home of the Signal Corps and Army Cyber Command, served in South Korea through the first year of COVID, and later worked at NOAA. Raised in Annapolis, she now builds the automation behind RADICL's SOC, including the tooling that flags business email compromise.



Jason Jenkins

U.S. AIR FORCE · DIRECTOR OF DFIR

Jason served 12 years in Air Force Security Forces, active and reserve. His 15 years in policing ran from patrol, motors, and undercover narcotics to training new officers, then through the detective bureaus, working crime scenes, homicides, robberies, kidnappings, burglaries, and financial crimes, and finished in the digital forensics and computer crimes bureau. He has since held nearly every role in DFIR and now leads it at RADICL.



Dave Pack

U.S. ARMY · VP, CUSTOMER EXPERIENCE

Pack was a Staff Sergeant and Army intelligence analyst who ran the 3d Armored Cavalry Regiment's analysis and control element during combat in Iraq and led the team pushing top-secret networks to the field by satellite. He went on to build intelligence tools for the Defense Intelligence Agency and DoD counterintelligence before leading SOC teams at IBM and LogRhythm. He now leads cybersecurity operations and compliance at RADICL.

Happy Veterans Day from Signal(s) & Noise.

From the vSOC to every veteran reading this: **thank you for your service.**