CyberHoot

CONFIDENTIAL

ADVISORY CH-TA-2026-0001

THREAT INTELLIGENCE · INCIDENT RESPONSE

Tax-Season "New Client" Lure to Spoofed Teams Link to Fake Device Enrollment (Rippling MDM) & RMM Abuse

Targeting public accounting / CPA firms · 2026 tax season

TLP:AMBER

ADVISORY ID	VERSION
CH-TA-2026-0001	v1.0
DATE	**PREPARED BY**
2026-06-30	CyberHoot, Digital Forensics & Incident Response

HANDLING

Share within your org and with clients/members who need to act; not for public release. Downgrade to TLP:GREEN for ISAC/community distribution at analyst discretion.

1. Executive Summary

In June 2026, a US-based public accounting (CPA) firm was targeted by a patient, multi-week social-engineering operation that maps to the 2026 tax-season campaign wave against accountants that Microsoft, the IRS, and Huntress have documented (see section 7). The attacker posed as a prospective tax client ("Teresa Bair"), made first contact through the firm's public website contact form, built rapport over several weeks, scheduled a "tax meeting," then delivered a Microsoft Teams "Join" link whose displayed URL was spoofed. The visible text read teams.microsoft.com while the real hyperlink resolved to an attacker-controlled fake "Device Enrollment" page. Clicking it enrolled the workstation into an attacker-controlled Rippling MDM tenant, which ran scripts as SYSTEM and tried to install redundant remote-access tooling (a second ScreenConnect instance and FleetDeck).

Outcome at the affected firm: endpoint AV and EDR blocked both remote-access agents. A multi-tool DFIR review found no evidence of data exfiltration and no compromise of the Microsoft 365 identity. This was a device-only compromise, contained to one workstation.

Why this advisory: the Rippling MDM enrollment vector is a newer variant that is not present in current public write-ups, and the specific indicators below are net-new and not yet publicly reported. Sharing them helps peer firms detect and block the same actor.

2. Targeting and Victimology (anonymized)

- Sector and victim: US public accounting (CPA) firm, multi-office, roughly 160 mailboxes.
- Timeframe: initial web-form contact on 2026-04-21; email thread and payload delivery from 2026-06-22 to 06-26.
- Entry point: the firm's public website contact form (free-text Name, Email, and Message; weak anti-bot, a static arithmetic question rather than a real CAPTCHA). The firm's web and marketing vendor relayed the submission to a shared info@ mailbox that auto-forwarded internally.
- Blast radius: one targeted preparer, one workstation. No other mailbox received the lure, confirmed via message trace and content search.

3. Attack Chain

1. First contact (T1566, T1656 Impersonation). The attacker submits the public contact form as a prospective client "Teresa Bair, DO MD," citing a complex tax situation ("requested an extension," "severe health concerns") and asking about fees and "preparation charges." This matches the documented "new client, price-quote" lure.
2. Rapport building (multi-week). An email thread with the targeted preparer, plus a real Outlook calendar invite (a "[Firm] Tax Meeting") to add legitimacy.
3. Delivery, spoofed meeting link (T1566.002, T1204.001, T1036 Masquerading). On meeting day the attacker writes that "the Teams meeting link you sent appears to be inactive, you can join mine," and includes a "Join" link that displays a teams.microsoft.com/meet URL with a plausible Meeting ID and Passcode, but whose real href points to the attacker's fake enrollment page.
4. Fake device enrollment (T1098.005, T1219). The page, branded as a generic "Device Enrollment," enrolls the workstation into an attacker-controlled Rippling MDM tenant using the genuine, signed Rippling agent.
5. Execution as SYSTEM (T1059). The MDM pushes scripts. A bundled python.exe spawns PowerShell, icacls, whoami, net, and similar as SYSTEM, doing recon and permission changes.

6. Redundant RMM (T1219, T1543). The MDM attempts to install a second ScreenConnect instance and FleetDeck, matching the public reporting of deploying two or three remote-access tools for redundancy. Assessment: in this case the second tool was the same RMM product already deployed in the environment. We assess with moderate confidence that this was deliberate, that the actor observed the in-use RMM after landing and matched it so that a lateral instance would blend in with a tool the environment already trusts. Treat a known-good RMM product as safe by instance, not by name: distinguish instances by relay host and instance identifier, because an attacker who matches your RMM will not stand out on a presence-only sweep.
7. Blocked. Endpoint AV blocked both RAT installs, catching them as generic reputation detections (the FleetDeck agent by its binary path, and the second RMM as a reputation detection on the Windows Installer temp file on each attempt), which caused the MSI installs to fail. Note that the AV never identified either tool by name and did not flag the MDM enrollment, the interpreter, or the scripts at all, so log review keyed on named products would miss most of this chain. No hands-on remote session and no data exfiltration were observed.

4. MITRE ATT&CK Mapping

Tactic	Technique	ID
Initial Access	Phishing	T1566
Initial Access / Delivery	Phishing: Spearphishing Link	T1566.002
Execution	User Execution: Malicious Link	T1204.001
Defense Evasion	Masquerading (spoofed link display; signed legit tooling)	T1036
Defense Evasion	Impersonation (fake “new client” persona)	T1656
Persistence / Privilege	Account Manipulation: Device Registration (rogue MDM enrollment)	T1098.005
Execution	Command and Scripting Interpreter (PowerShell as SYSTEM)	T1059
Persistence / C2	Remote Access Software (Rippling MDM, ScreenConnect, FleetDeck)	T1219
Persistence	Create or Modify System Process: Service	T1543

5. Relationship to Known Campaigns

This activity is consistent with the 2026 tax-season wave against accountants and CPA firms:

- The “new client / request for professional tax filing” lure with a complex tax backstory and a price-quote ask (Microsoft, 2026-03-19).
- The IRS “new client” email scam pattern, where the first email is a client request and the second carries a malicious link.
- RMM redundancy, meaning multiple ScreenConnect instances plus a backup RMM (FleetDeck) on one host (Huntress and The Hacker News, February and March 2026).

The newer piece: public reporting describes ScreenConnect, SimpleHelp, Datto, and FleetDeck delivered through malvertising or IRS-document lures. This incident adds a fake “device enrollment” page that enrolls the host into an attacker Rippling MDM tenant, which then runs SYSTEM scripts, delivered through a spoofed Teams meeting link. That vector is not in current public write-ups.

6. Indicators of Compromise

Defanged. A star marks net-new indicators not previously public.

Network and URL:

Type	Value	Notes
URL (star)	hxxps://mahafimpex[.]com/Znroll[.]php	Fake “Device Enrollment” page. Host domain created 2024-07-15 (about two years old), an aged and likely-compromised legitimate website, not a fresh throwaway
Brand string (star)	cnstructer[.]com	Label shown on the fake page. Not a registered domain (no registry record, NXDOMAIN). Alert on the string, but it is not a resolvable or blockable host
Spoofed display URL (star)	hxxps://teams.microsoft[.]com/meet/2870 2700132346?p=w4altvgdyrvzhr1ltx	Fake display text of the malicious “Join” link (the real href was the mahafimpex URL above). Fake Meeting ID 659 862 001 323 46, Passcode Ut3Do7RU

Infrastructure and domain age. The common heuristic that domains under about six months old are likely fraudulent would not have flagged this campaign. The payload was hosted on an aged (about two-year-old) compromised legitimate site (mahafimpex[.]com), and the fake-page brand (cnstructer[.]com) is not even a registered domain. This actor favors abusing established, reputable infrastructure over fresh registrations, which defeats young-domain reputation filtering. Detection should lean on behavior (a display-versus-href link mismatch, rogue MDM or RMM enrollment) rather than domain age alone.

Actor persona and sender:

Type	Value	Notes
Email (star)	bairteresa@outlook[.]com	Display name “Teresa Bair, DO MD” (note the impossible dual DO and MD credential). A genuine, attacker-controlled Outlook.com account
Phone (star)	+1 (628) 246-4880	In the persona signature (628 is a US, San Francisco Bay area code)
Lure subjects	[Firm] Taxes, [Firm] Tax Meeting, web-form Online Inquiry	Subjects incorporate the target firm’s own name plus Tax or Tax Meeting, and will vary per target

Rogue MDM and RMM:

Type	Value	Notes
Rippling MDM tenant (CompanyId, star)	6a39ea1d4447abff347fc13f	Attacker-controlled Rippling tenant the device was enrolled into
FleetDeck deploymentID (star)	50b12ff4-93c9-4967-bffa-7ce7c183338b	Attacker FleetDeck deployment (blocked)
FleetDeck agent SHA-256	f7d793f458450f8da205887757af8496784 8fd42c8be78dfcd00524e6cf2ab65	Legitimate signed FleetDeck RMM, attacker-abused (VirusTotal: PUA/RemoteAdmin)
ScreenConnect instance (attacker, star)	39bb6848f73e769c	Second, redundant ScreenConnect instance pushed to the host (blocked)

Host artifacts (detection markers):

- Registry: HKLM, HKLM
- Windows MDM enrollment: HKLM<GUID>
- Service: rippling-daemon
- Files and paths: C: (including ..._expanded.exe and ...), and a Rippling folder on a user desktop
- FleetDeck: C:Files (x86)Agent_agent_svc.exe and its service
- ScreenConnect: a ScreenConnect Client (*) service whose binary-path relay host (the &h= value) is not your authorized Control or ScreenConnect relay

7. Detection Guidance

- Rogue MDM hunt. Any Rippling registry keys, rippling-daemon service, or C: folder on hosts where your organization does not use Rippling should be treated as a compromise. Surface the enrolled CompanyId and compare it to 6a39ea1d4447abff347fc13f.
- Unauthorized RMM by relay, not by presence. Enumerate ScreenConnect and ConnectWise Control services and parse the &h= relay host from the binary path. Flag any relay that is not your sanctioned one. Also hunt for the FleetDeck agent and service.
- Link-spoof lure. Alert on inbound mail where an anchor’s display text contains teams.microsoft.com or zoom.us but the href domain is different.
- New-client social engineering. Treat unsolicited prospective-client inquiries, especially through web forms, that quickly pivot to “join my meeting” or “open this link” as high risk. Verify identity out of band before clicking.
- MDM enrollment events. Monitor for unexpected Windows MDM enrollment (DMClient) and new device-management service installs.

8. Mitigations

- Block the domains and URLs in section 6 at the mail gateway, web proxy, and EDR. Submit the URL to your email and web vendors and to public blocklists (URLhaus, PhishTank, Google Safe Browsing).
- Block or uninstall unsanctioned RMM and MDM fleet-wide (Rippling, FleetDeck, unauthorized ScreenConnect), and alert on their artifacts.

- Harden public web forms. Replace weak or static anti-bot checks with a real CAPTCHA (reCAPTCHA v3 or hCaptcha) plus a honeypot and rate limiting. Route form mail to a monitored alias and tag form-originated mail as untrusted.
- Reduce standing local admin on workstations with just-in-time elevation, so a single click cannot install remote-access tooling with full rights.
- User awareness. Train staff on the “new client, join my meeting, open this link” tax-season lure and on checking a link’s real destination against its displayed text.

9. Where and How to Report

Group	What to send	Channel
IRS, tax-pro “new client” scam	The lure email and headers; note it targeted a tax preparer	Forward to phishing@irs.gov (subject “New Client Scam”); notify your IRS Stakeholder Liaison if client data is at risk
FBI IC3	Incident summary and IOCs (victim identity included, confidential)	https://www.ic3.gov
CISA	This advisory and IOCs	https://www.cisa.gov/report or report@cisa.gov
Accounting-sector peers	This advisory (TLP:AMBER or GREEN)	AICPA and your state CPA society; FS-ISAC if a member
Microsoft	The abusive @outlook.com account and the phishing message	Report via Outlook “Report phishing”; MSRC or abuse for the consumer account
Rippling (abuse/takedown)	Attacker tenant CompanyId 6a39ea1d…	Rippling Trust and Security abuse contact; request tenant takedown
ConnectWise (ScreenConnect abuse)	Malicious instance 39bb6848…	ConnectWise abuse or trust contact
FleetDeck (abuse/takedown)	deploymentID 50b12ff4…	FleetDeck abuse contact
Host and registrar of mahafimpex[.]com	The compromised page hosting the kit	Notify the site owner and host or registrar abuse; submit to URLhaus, PhishTank, Safe Browsing
Your email security vendor	The message and IOCs	Vendor submission portal

> Confirm exact intake addresses with each group before sending, since some abuse contacts change. Do not include another organization’s internal identifiers when sharing broadly. Keep distribution to the IOCs and TTPs above.

10. References

- Microsoft Security Blog, When tax season becomes cyberattack season (2026-03-19): https://www.microsoft.com/en-us/security/blog/2026/03/19/when-tax-season-becomes-cyberattack-season-phishing-and-malware-campaigns-using-tax-related-lures/

- The Hacker News, Microsoft Warns IRS Phishing Hits 29,000 Users, Deploys RMM Malware (2026-03): https://thehackernews.com/2026/03/microsoft-warns-irs-phishing-hits-29000.html
- Huntress, W-2 Malvertising to Kernel-Mode EDR Kill: https://www.huntress.com/blog/w2-malvertising-to-kernel-mode-edr-kill
- IRS, Tax professionals: Watch out for “new client” email scam: https://www.irs.gov/newsroom/tax-professionals-watch-out-for-new-client-email-scam

Document Changelog

Version	Date	Summary
v1.0	2026-06-30	Initial shareable advisory. Anonymized victimology, attack chain, ATT&CK mapping, campaign linkage, net-new indicators with a domain-age note, detection, mitigations, and reporting destinations.