

[Op Report] Hands-on-Keyboard Intrusion Abusing Multiple RMMs

 blog.deception.pro/blog/hok-intrusion-abusing-multiple-rmms-jan2026

MalBeacon

February 3, 2026

Between January 14 and January 27, 2026, Proofpoint researchers observed a hands-on-keyboard intrusion (interactive attacker activity, not just automated malware) in a Proofpoint-controlled Deception.Pro environment built to resemble a France-based luxury travel organization.

The threat actor abused multiple commercial Remote Monitoring and Management (RMM) tools in tandem. While previous reporting tied this threat actor to Bluetrait and Fleetdeck, this operation expanded the toolset to include Level RMM and MSP360 (formerly CloudBerry)—a meaningful evolution in tradecraft.

The intrusion began with malicious email (malspam) delivering a weaponized PDF lure that led to the installation of Bluetrait RMM, followed by staged deployment of additional RMM agents. Over nearly 15 days, the attacker performed extensive system enumeration, executed non-interactive PowerShell commands, and maintained persistent interactive access—behavior consistent with an engaged threat actor rather than automated malware alone.

This campaign aligns with prior reporting indicating a French-language targeting bias, reinforced here by both victim profiling and threat actor browser activity. No destructive actions or data exfiltration were observed during the window of visibility, but the breadth of RMM tooling and depth of reconnaissance strongly suggest preparation for follow-on activity.



Environment at a Glance

- **Replica Role:** Product Manager, Luxury Travel
- **Replica Organization:** A premier tour operator specializing in bespoke luxury travel
- **Topology:** Microsoft Active Directory environment with **2,000+ endpoints** and **1,500+ users**
- **Replica Location:** France
- **Observed duration:** ~15 days (Jan 14–Jan 27, 2026)

Campaign Background

On **January 13, 2026**, Proofpoint researchers identified an email campaign operated by a known threat actor distributing the **Bluetrait RMM** tool. Proofpoint has tracked this actor since **August 2024**, and other researchers have published analysis on this cluster (links included below).

This actor typically relies on **Bluetrait** or **Fleetdeck** for initial access. Campaigns are generally low-volume (from a few messages to fewer than 500 per campaign). Lures are commonly written in **French, English, Spanish, or German**, and frequently use **payment-related** or **travel-industry** themes. Targeting is broad, with recipients observed across **Europe** and **North Africa**. On limited occasions in 2025, the same cluster also distributed other RMM tools such as **SuperOps** and **Syncro**.

The actor typically uses PDF attachments containing URLs that direct recipients to a **Fleetdeck executable** or a **Bluetrait MSI installer**. Proofpoint has also observed the cluster using Bluetrait to download and install additional RMM tooling after establishing initial access.

For this mid-January campaign, the lure was **French-language** and tied to the **travel industry**. To increase the likelihood the actor would believe they had landed in a realistic corporate environment aligned with their theme, Proofpoint researchers selected a **Deception.Pro** environment tailored to the travel sector and used a **French-geolocated network egress**.

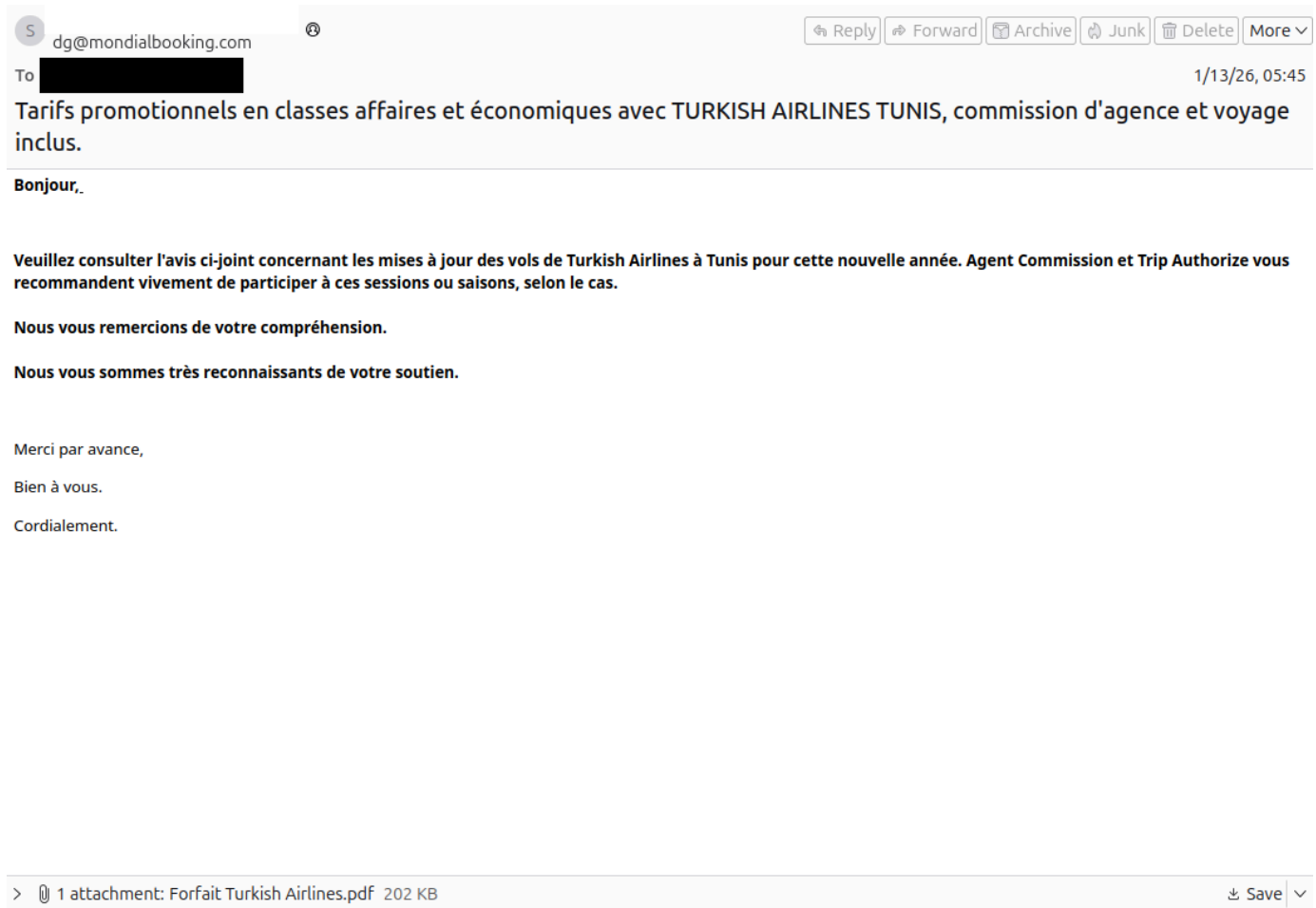


Figure 1: Email (sanitized) received by victims (French-language travel lure).

Initial Lure: “Missing Adobe Plugin” PDF

The email contained a PDF attachment (also written in French) that enticed recipients to click a link to install a fictitious “missing Adobe plugin.” In reality, the link downloaded and installed **Bluetrait RMM**.

Module Adobe turc manquant

Pour consulter le contenu de ce document, vous devez installer le plugin Adobe turc



Figure 2: French PDF lure prompting installation of a “missing Adobe module,” leading to Bluetrait deployment.

Timeline of Observed Activity

January 13 - 14, 2026 — Initial Access

- Malspam delivered to French-speaking recipients with a PDF attachment.
- The PDF contained a link leading to Bluetrait RMM installation (defanged):

hxxps://mactur[.]bluetrait[.]io/simple/msp_download_agent

- Bluetrait RMM successfully installed in Deception.Pro environment.

January 15, 2026 — Expansion and Interactive Access

- Fleetdeck RMM deployed via PowerShell.
- Level RMM installed at approximately 12:43 PM, observed command line:

"C:\Program Files\Level\level.exe" --key <redacted> --action=run

- Hands-on-keyboard activity confirmed.
- Threat actor browser activity observed in Firefox, including visits to:
 - Amazon[.]fr
 - Lemonde[.]fr
- Threat actor installed Mozilla Thunderbird but did not configure it with any email accounts.

January 18–25, 2026 — Persistence and Reconnaissance

- MSP360 backup agent installed:

C:\Program Files\Kalima\Online Backup\Online Backup.exe

- MSP360 Connect agent installed:

C:\Program Files\Connect\Connect.exe

- Extensive enumeration via Level RMM using osquery and PowerShell.

- Repeated polling of:
 - system configuration
 - security posture
 - users and privileges
 - network interfaces

January 27, 2026 — End of Observed Activity

No destructive actions, confirmed lateral movement, or data exfiltration observed prior to session termination.

Total observed duration: 14 days, 20 hours, 15 minutes

Indicators of Compromise

Malicious PDF Attachment

- **File name:** forfeit turkish airlines.pdf
- **SHA256:** 148adc8f253a48d912b040c61625f3addee6695d781ba62aa7a9027cc86aade9
- **Embedded URL** (defanged):

*hxxps://mactur[.]bluetrait[.]io/simple/msp_download_agent?
os=windows&access_key=<redacted>*

RMM Tooling Observed

Bluetrait RMM

- **Executable:** *C:\Program Files (x86)\Bluetrait Agent\Bluetrait MSP Agent.exe*
- **Domains:** bluetrait[.]io

Fleetdeck RMM

- **Executable:** *C:\Program Files (x86)\FleetDeck Agent\fleetdeck_agent.exe*
- **Domains:** fleetdeck[.]io

Level RMM

- **Executable:** *C:\Program Files\Level\level.exe*

- **Domains:**

- agents[.]level[.]io
- downloads[.]level[.]io
- builds[.]level[.]io
- online[.]level[.]io
- global[.]turn[.]twilio[.]com

MSP360 Connect

- **Executable:** *C:\Program Files\Connect\Connect.exe*

- **Domains:**

- mspbackups[.]com
- msp360[.]com
- cloudberrylab[.]com

MSP360 Backup

- **Executable:** *C:\Program Files\Kalima\Online Backup\Online Backup.exe*

- **Domains:**

- mspbackups[.]com
- msp360[.]com
- cloudberrylab[.]com

Network and Detection Telemetry

Emerging Threats Suricata alerts:

- ET INFO Observed RMM Software Domain (bluetrait .io) in TLS SNI
- ET INFO RMM Software Domain in DNS Lookup (bluetrait .io)
- ET INFO Level.io Agent Domain in DNS Lookup (agents .level .io)
- ET INFO Level.io Download Agent Domain in DNS Lookup (downloads .level .io)

- ET INFO Level.io Agent Update Domain in DNS Lookup (builds .level .io)
- ET INFO Level.io Check Connectivity Status in DNS Lookup (online .level .io)
- ET INFO Level.io Agent P2P Connection Domain in DNS Lookup (global .turn .twilio .com)
- ET INFO Observed MSP360 Backup Service Domain (mspbackups .com in TLS SNI)
- ET INFO MSP360 Backup Service Domain in DNS Lookup (mspbackups .com)
- ET INFO Observed Fleetdeck Remote Management Software Domain in TLS SNI (fleetdeck .io)

Assessment and Defender Takeaways

This operation highlights an uncomfortable trend: attackers are increasingly abusing legitimate enterprise tooling as an intrusion framework. The use of **four distinct RMM platforms** is unlikely to be accidental—it provides redundancy, operational flexibility, and resilience against partial remediation.

Key observations:

- **Interactive behavior matters.** Hands-on-keyboard activity differentiated this intrusion from automated malware delivery. The threat actor actively explored the environment, validated regional targeting through browser use, and repeatedly enumerated security controls and user privileges.
- **Toolchain expansion.** The addition of **Level RMM** and **MSP360** suggests an expanding playbook. MSP360's presence is particularly notable: while marketed as a backup solution, its installation raises questions about potential data staging or exfiltration via “legitimate” backup channels (under active forensic investigation). The actor may also have intended to use **Thunderbird** for mailbox persistence, data exfiltration, or sending malicious emails—installing it locally could allow stealthy access from the victim's trusted device and IP.
- **Potential broader targeting.** Sensitive source collection revealed other enrolled RMM devices geolocated in **Tunis, Tunisia**, with source IP addresses associated with **TopNet ISP**. These may represent additional campaign targets, though attribution cannot be confirmed from this visibility alone.

What Defenders Should Watch For

When attackers use “legitimate admin tools,” defenders have to learn the difference between helpdesk noise and hostile intent. Practical detection strategies include:

- Unexpected RMM installations (especially **multiple RMM agents on one endpoint**)

- Silent PowerShell execution, including **execution-policy bypass** patterns
- Redundant management agents co-existing without a valid business justification
- RMM usage patterns inconsistent with known MSP operations (new agents, odd hours, unusual geographies, repeated deep enumeration)

Previous Reporting

- <https://www.proofpoint.com/us/blog/threat-insight/remote-monitoring-and-management-rmm-tooling-increasingly-attackers-first-choice>
- <https://labs.withsecure.com/publications/email-delivered-rmm>

See the Activity the Way an Attacker Sees It

Alerts often flatten intrusions into a handful of “events.” Deception operations, by contrast, show a threat actor’s behavior over time—what they click, what they enumerate, and what they set up for later. To see long-term hands-on-keyboard activity in context—and understand what attackers do once they think no one is watching—reach out to schedule a demo of [Deception.Pro](#).