ANY.RUN Reveals Multi-Stage XWorm Campaign Targeting LATAM Businesses Through Fake Financial Receipts

DUBAI, DUBAI, UNITED ARAB EMIRATES, February 17, 2026 /EINPresswire.com/ -- ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, has uncovered a sophisticated multi-stage malware campaign actively targeting organizations across Latin America (LATAM).

The operation delivers the XWorm remote access trojan (RAT) through deceptive financial receipt lures, combining stealth delivery, fileless execution, and resilient persistence techniques designed to evade early detection and extend attacker dwell time inside corporate environments.

□ □□□□□ □□□□□□□□□□ □□□□□ □□□□□ □□□ □□□□ □□□□□□□□ □□□□□□□□□□□□□

This campaign illustrates how commodity malware is evolving to reach corporate environments across LATAM. Finance-themed social engineering and low-visibility persistence bypass early defenses, delay detection, and increase the risk of credential theft and downstream business impact.

□□□□□□ □□□□□□□□ □□□ □□□□□□□□ □□□□□:

· Finance-themed delivery aligned with real workflows: Fake payment receipts increase execution probability on corporate endpoints.

· Low-visibility execution that delays detection: WMI-spawned PowerShell, steganography, and

fileless loading reduce early security signals.

· Resilient persistence designed for long dwell time: .NET-based scheduled task creation enables continued access after reboot.

· Trusted binary abuse to blend with legitimate activity: Injection into CasPol.exe helps malicious traffic appear normal in endpoint telemetry.

· Identity-driven post-compromise risk: Stolen sessions and credentials can lead to account takeover, fraud, data exposure, or ransomware staging.

To get the full technical breakdown and discover how to cut risk with earlier monitoring and faster triage, visit the ANY.RUN blog.

□□□□□ □□□.□□□

ANY.RUN, a leading provider of interactive malware analysis and threat intelligence solutions, strengthens the SOC operational cycle across Tier 1–3 with live execution visibility, fast IOC enrichment, and continuously updated intelligence. Trusted by □□□,□□□+ □□□□□□□□□ □□□□□□□□□□□□□□ □□ □□,□□□+ □□□□□□□□□□□□□□, it helps teams cut investigation time, reduce unnecessary escalation, and stay ahead of fast-moving phishing and malware campaigns.

The ANY.RUN team
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
LinkedIn
YouTube
X
