EnCyb

Severity: High

Advisory Type: Threat

Abuse of Legitimate RMM Tools via Fake Software Download Websites

Advisory Report

TLP: WHITE

SECURITY THREAT ADVISORY COUNCIL (STAC)

Empowering organizations with cutting-edge cybersecurity strategies to combat emerging digital threats effectively.

EXECUTIVE SUMMARY

Threat actors are distributing legitimate Remote Monitoring and Management (RMM) tools via fake Notepad++ and 7-Zip websites, using them as the initial access vector instead of traditional malware. These signed tools evade antivirus detection, attackers gain persistent remote control and rapidly deploy backdoors, ransomware, and follow-on payloads.

- Active Region: Global
- Affected Sector: Individuals and Enterprises (cross-sector)
- Affected Product: Fake Notepad++ and 7-Zip download websites delivering abused RMM tools such as LogMeIn Resolve, PDQ Connect, and similar utilities
- Severity: High
- Published Date: January 27, 2026

TECHNICAL DETAILS

- **Target:** Individual users, small businesses, and enterprise endpoints—particularly non-admin workstations—where users search for and download commonly used free utilities (e.g., Notepad++, 7-Zip), providing attackers an initial foothold that can later expand into corporate networks.
- **Root Cause:** Lack of robust verification in software acquisition workflows combined with attacker abuse of digitally signed, legitimate RMM tools. Threat actors exploit user trust in well-known brands and the implicit trust security products place in sanctioned IT administration software.
- **Prerequisite For Exploitation:** Successful social engineering leading a user to a spoofed download page (via SEO poisoning, malvertising, or phishing), followed by manual execution of the installer without verifying the source domain, publisher, or digital signature.

IMPACT

- Full remote control of compromised systems by threat actors
- Establishment of persistent unauthorized access via RMM and backdoors
- Credential theft and sensitive data exfiltration
- Lateral movement within enterprise networks
- Deployment of ransomware or additional malware payloads
- Increased dwell time due to evasion of traditional antivirus detection
- Financial loss and compromise of user account integrity

RECOMMENDATIONS

- Download software only from official, verified websites
- Restrict RMM usage to approved IT administrator accounts
- Use EDR/XDR to detect suspicious RMM behaviour (PowerShell, remote sessions)
- Block look-alike domains and malvertising sources
- Conduct regular endpoint audits for unknown remote access tools

REFERENCE

- https://cybersecuritynews.com/threat-actors-using-fake-notepad-and-7-zip-websites/

SECURE, SCALE, SUCCEED WITH

CONFIDENCE

EnCyb

www.encyb.com/contact-us/ EnCyb ✉ soc@encyb.com

www.encyb.com