EINPRESSWIRE

ANY.RUN Reveals Major Cyber Attacks in July: Fake 7-Zip App, New DeerStealer Campaign, and More

DUBAI, DUBAI, UNITED ARAB EMIRATES, July 30, 2025 /EINPresswire.com/ -- ANY.RUN has released its July 2025 cyber threat report. The study highlights the most active malware families, infection techniques, and a growing trend: cybercriminals are increasingly using legitimate Remote Monitoring and Management (RMM) software to attack corporate systems.

□□□ □□□□□□□□ □□□□ □□□□ □□□□

□ DeerStealer campaign: spread via obfuscated .LNK shortcuts. Execution goes through mshta.exe and PowerShell, allowing malware to bypass basic defenses and deliver payloads silently.
□ Fake 7□Zip installer: downloads a malicious archive that extracts Active Directory files, including ntds.dit and the SYSTEM hive. Attackers can use this data for privilege escalation and full domain compromise.
□ Snake Keylogger activity: increased attacks against banking and financial services. The malware uses multiple layers of obfuscation, LOLBins, and registry changes for persistence.

□□□□□□□□ □□□□□□□ □□ □□□□□
□ □□□□□□ □□ □□□ □□□□□□: attackers often rely on tools normally used by IT teams to gain remote access and move inside networks.

□ □□□ □ □□□□□□ □□□ □□□□□□□□□□ (□□ □□□□□): ScreenConnect, UltraVNC, NetSupport, PDQ Connect, Atera.

□ □□□□□□-□□□-□□□-□□□□ □□□□□□□□: cybercriminals increasingly use built-in Windows tools to stay undetected.

□ □□□□□□□□ □□□□□□□□ □□□□□□□: campaigns distributing information□stealers remain among the most common threats, often delivered through phishing emails or fake software installers.

Visit the ANY.RUN blog for more details.

□□□ □□□.□□□ □□□□□□ □□□□□□□□□□□□ □□□□□□□ □□□ □□□□□□□□ □□□□□□
All the threats were identified using ANY.RUN’s malware analysis and threat intelligence solutions that empower companies across finance, healthcare, IT, government, and other industries to catch attacks before they cause damage.

Here’s how ANY.RUN helps companies stay safer:
□ Faster detection of threats and reduced Mean Time to Detect (MTTD)
□ Full visibility into what threats do on the system without any guesswork
□ Immediate access to IOCs for SIEM enrichment and faster response
□ Less manual effort for analysts, thanks to automated analysis
□ Lower risk of breaches, data loss, and business disruption
□ Shareable, detailed reports for internal teams, clients, or compliance needs

□□□□□□ □□□.□□□
ANY.RUN is a provider of cybersecurity solutions. Among its products are Interactive sandbox for analysis of malicious behavior in real time and threat intelligence solutions TI Lookup and TI Feeds suitable for browsing and monitoring emerging and evolving threats targeting over 15,000 companies in sectors like finance, manufacturing, and healthcare.

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