November’s Top Cyber Attacks: XWorm, JSGuLdr, Mobile Threats, and Multi-Stage Campaigns Surge Worldwide

DUBAI, DUBAI, UNITED ARAB EMIRATES, December 1, 2025 /EINPresswire.com/ -- Cyberattacks continued to intensify in November as attackers relied on multi-stage loaders, in-memory execution, and cross-platform payloads. ANY.RUN reports a noticeable rise in loader-driven intrusions, encrypted payload containers, and campaigns targeting Windows, Linux, and Android environments.

The November 2025 Threat Analysis shows how modern attacks blend JavaScript, PowerShell, Linux services, and mobile components to move quietly through enterprise networks, often without leaving traditional executables behind.

□□□-□□□□□ □□-□□□□□□ □□□□□□□: □□□□□ □□□□□□□ □□□□□□□

A new XWorm wave used phishing pages to deliver an obfuscated JavaScript dropper that hid AES-encrypted payloads inside PNG files. By loading the .NET assembly directly in memory, the malware avoided on-disk artifacts and enabled credential theft and remote access attempts inside corporate environments.

□□□□□□□: □□□□□-□□□□□ □□□□□□ □□□□□□□□□□ □□□□□□□□□□□□□□

ANY.RUN analysts identified JSGuLdr, a multi-stage loader that begins with obfuscated JScript and uses COM to launch PowerShell under explorer.exe, making the activity appear routine. PowerShell then downloads and decrypts a payload from Google Drive and executes it, leading

to PhantomStealer being injected into msiexec.exe. This approach enables quiet data theft inside corporate environments with almost no on-disk traces.

For deeper visibility into these threats, including live analyses, key indicators, and detection guidance, explore the ANY.RUN blog.

□□□□□ □□□□□□□ □□□□□□□□□ □□□□□□□□□

· □□□□□□□□□□□□, □□□□□□□□□□□□, □□□□□□□□□: Cross-platform loader and RAT chain enabling access to both corporate endpoints and Linux servers.

· □□□□□□□□□□□□, □□□□□□, □□□□□: Browser hijacking, Tor-based credential theft, and Android trojans targeting employee devices and corporate accounts.

· □□□□□□, □□□□□□□, □□□□□□□□□: Linux ransomware, targeted Windows backdoors, and hybrid RAT–ransomware used for deeper intrusion into enterprise environments.

· □□□□□□□□, □□□□□□□, □□□□□□□□□□: Credential theft, adaptable backdoors, and WhatsApp-based malware spreading through trusted communication channels.

□□□□□ □□□.□□□

ANY.RUN is a leading provider of interactive malware analysis and threat intelligence solutions used by 15,000 organizations and over 500,000 analysts worldwide. The service combines a live Interactive Sandbox, TI Lookup for instant IOC enrichment, and continuously updated Threat Intelligence Feeds to help security teams investigate faster, improve detection logic, and respond to emerging threats with confidence.

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