

ISSUE 55

12/05/2025



Revnext

CYBERSECURITY NEWSLETTER

BY FLAVIA LEPADATU AND SALMA AMGHAR

Modern DDoS Attacks: From Disruptive Tools to Strategic Diversions

by Salma Amghar

DDoS attacks are no longer just blunt-force assaults, they have evolved into sophisticated distractions masking deeper breaches. In today's hybrid-cloud environments, attackers often pair massive traffic floods with stealthy operations like privilege escalation or data exfiltration, exploiting fragmented infrastructures and overwhelming defenders' attention. These hybrid attacks exploit not just technical gaps but human psychology, banking on response teams focusing solely on uptime and ignoring subtler warning signs. As AI-driven threat actors automate this blend of noise and stealth, defenders must assume that every DDoS event could signal a broader intrusion. Experts recommend adopting anomaly detection, improving network segmentation, and conducting multilayered simulation training to prepare teams for these asymmetric threats. Coinciding with this evolving threat landscape, international law enforcement launched Operation PowerOFF, dismantling six DDoS-for-hire services, such as CfxAPI, NeoStress, JetStress, and others, and arresting four individuals in Poland. These so-called "booter" platforms made launching DDoS attacks simple, allowing customers to select targets and attack durations through user-friendly dashboards. The United States seized nine domains, while Dutch authorities contributed by deploying fake booter sites to warn potential users about the illegality of such services. The recent takedown underscores the ongoing efforts of international law enforcement to combat cybercrime and disrupt the infrastructure supporting DDoS-for-hire services. As these services become more accessible, and attackers more strategic, defenders must shift their mindset: DDoS might not just noise, it might be the opening move in a much larger campaign. **Source 1:** [Click here](#) **Source 2:** [Click here](#)



LockBit Leak Exposes Inner Workings, Tactics, and Decline of Ransomware Giant

by Flavia Lepadatu

The LockBit ransomware gang suffered another major blow after an unknown party compromised its leak site. Instead of listing new victims, researchers noticed the Dark Web site displayed a message reading "Don't do crime CRIME IS BAD xoxo from Prague," alongside a link to a zip archive containing a SQL database dump from LockBit's affiliate panel. The leaked data, analyzed by Qualys and Coalition, includes nearly 60,000 Bitcoin addresses, over 4,000 chats with victims, and sensitive information on more than 70 LockBit affiliates and administrators. While the dump lacks decryptors or private keys, it exposes plaintext passwords, affiliate details, and individual ransomware build configurations. The breach follows earlier setbacks, including 2024's Operation Cronos, which seized LockBit infrastructure and led to arrests and sanctions against its alleged leader. Analysts say the new leak offers unprecedented visibility into LockBit's operations. Most victims listed between December 2024 and April 2025 were in Asia-Pacific, with lower-than-usual ransom demands averaging under \$20,000. Qualys also revealed operational tactics, including a preference for Monero over Bitcoin for its privacy features, and instructions to disable backups by targeting specific services and utilities. These findings show the group's methodical approach to maximizing damage and minimizing recovery chances, but also provide a rare look into LockBit's evolving tactics and weakened standing in the ransomware ecosystem. However, experts warn the leak could embolden rival threat actors. **Source:** [Click here](#)

Smishing Triad Expands Global Reach with Sophisticated New Tools

by Flavia Lepadatu

Chinese-linked cybercriminal group the Smishing Triad has intensified global smishing attacks using a revamped toolkit dubbed “Panda Shop,” according to a new report from Resecurity. First identified in 2023, the group now operates within a robust Crime-as-a-Service ecosystem, enabling large-scale impersonation of global brands like DHL, AT&T, Vodafone, and the UK government through SMS, iMessage, and Android RCS. The Panda Shop kit streamlines attacks with interactive Telegram bots, customizable phishing templates, and dashboards for managing stolen data. Some actors reportedly send up to 2 million smishing messages daily, reaching an estimated 60 million victims monthly. The kit’s use of Telegram, instead of Chinese platforms like WeChat, reflects the group’s focus on anonymity and international expansion. Additionally, cybercriminals also exploit telemarketing devices, IP filtering tools, and OTP interception to evade detection. Stolen data is funneled to carding shops or used in NFC-based fraud. Despite rising financial losses, enforcement remains limited. **Source:** [Click here](#)



Israeli spyware giant NSO Group Fined \$168M for WhatsApp Spyware Targeting

by Salma Amghar

A U.S. federal jury has ordered Israeli spyware developer NSO Group to pay WhatsApp approximately \$168 million in damages. The decision follows a December 2024 ruling that found NSO Group violated U.S. laws by exploiting WhatsApp servers to deploy Pegasus spyware, affecting over 1,400 individuals worldwide. NSO was accused of using Pegasus to surveil journalists, human rights activists, and dissidents, such as 456 Mexicans, 100 Indians, 82 Bahrainis, 69 Moroccans, and 58 Pakistanis, among others, spanning 51 countries. The spyware exploited a zero-day vulnerability in WhatsApp’s voice calling feature, allowing attackers to infect devices simply by placing a call. In addition to punitive damages, NSO must pay compensatory damages for the engineering efforts to block the attack. This decision was called a “momentous win in the fight against spyware abuse,” as it sends a clear message to the spyware industry and holds enablers of human rights violations accountable. NSO Group claimed its technology helps prevent crime and terrorism. However, the judge rejected this defense, as NSO cannot distance itself from the consequences of its spyware. **Source 1:** [Click here](#) **Source 2:** [Click here](#)



Trojanized UyghurEdit++ Used in Malware Attack Against World Uyghur Congress Leaders

by Salma Amghar

In a newly uncovered cyber-espionage campaign, senior members of the World Uyghur Congress (WUC) living in exile have been targeted with a Windows-based malware designed to carry out surveillance operations. The attack centered around a weaponized version of UyghurEdit++, an open-source word processing and spell-checking tool built to support the Uyghur language. The attackers impersonated a trusted contact from a partner organization in email messages sent to WUC leaders, which contained links to Google Drive, leading to a password-protected RAR archive. Inside was a tampered copy of UyghurEdit++, which, when launched, began profiling the infected system and transmitting data to an external server. Citizen Lab, a research group based at the University of Toronto, released a detailed report on the incident. According to them, the malware itself lacked technical complexity, but its delivery mechanism was well-crafted. Written in C++, the spyware featured additional capabilities, including downloading and executing further malicious plugins, forming a modular architecture for extended surveillance. However, the precise identity of the attackers remains unconfirmed. **Source 1:** [Click here](#) **Source 2:** [Click here](#)

