ANY.RUN's Q4 Malware Trends Report Reveals Rising Threats and Evolving Cybersecurity Challenges

DUBAI, DUBAI, UNITED ARAB EMIRATES, January 7, 2025 /EINPresswire.com/ -- ANY.RUN, a leading interactive malware analysis platform, has released its highly anticipated Malware Trends Report for Q4 2024, offering in-depth insights into the latest developments in the cybersecurity landscape. The report covers key trends such as the rise of advanced malware strains, emerging attack vectors, and the evolving tactics used by cybercriminals, providing a comprehensive overview of the most pressing cybersecurity challenges businesses face today.

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

Interactive analysis sessions: ANY.RUN users engaged in 1,151,901 public analysis sessions in Q4, a 5.6% increase from Q3. 22.6% of sessions were flagged as malicious, and 6.2% as suspicious, highlighting the rise in cyber threats.

· □□□ □□□□□□□ □□□□□: Stealers led the threat landscape with 25,341 detections. Loaders and RATs remained common, while adware (1,666 detections) emerged in the top ten.

· □□□□□ □□□□□□□ □□□□□□□: Stealc saw a significant rise of 136.3%, from 2,030 detections in Q3 to 4,790 in Q4. Lumma remained the most detected family with 6,982 detections.

· □□□□□□□ □□□□□□□: Phishing-related tasks rose significantly to 82,684, with Storm1747 being the most active group.

· [illegible]: Attackers continued using PowerShell, Windows Command Shell, and various evasion techniques like virtualization and sandbox bypassing.

· [illegible], [illegible], [illegible] ([illegible]): PowerShell and Windows Command Shell remained the top techniques, followed by spearphishing and scheduled tasks, reflecting evolving adversary methods.

For more detailed insights and the full report, visit the ANY.RUN blog.

[illegible]

This report is an important resource for cybersecurity professionals, businesses, and threat analysts looking to stay ahead of emerging threats in 2025. By analyzing trends in malware activity, phishing campaigns, and evolving attack techniques, organizations can enhance their security strategies and better prepare for the challenges ahead.

[illegible]

ANY.RUN is an advanced interactive malware analysis platform designed to empower cybersecurity professionals with real-time insights into emerging threats. Offering tools like a dynamic malware sandbox and Threat Intelligence (TI) lookup, ANY.RUN allows users to analyze suspicious files and URLs, identify malware behavior, and track cybercriminal activity.

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