

ANY.RUN Releases Q3 2024 Malware Trends Report

DUBAI, DUBAI, UNITED ARAB EMIRATES, October 22, 2024 /EINPresswire.com/ -- [ANY.RUN](#), a leading provider of malware analysis and threat intelligence solutions, has released its quarterly report. It covers the most active malware families and types, as well as the emerging tactics used by cybercriminals, providing security professionals with the knowledge needed to stay ahead of the latest threats.

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

In Q3 2024, ANY.RUN sandbox users ran 1,090,457 public interactive analysis sessions, marking a 23.7% increase from Q2 2024.

Of these, 211,770 (19.4%) were identified as malicious. This represents a slight increase in the percentage of malicious sessions from 18.4% in Q2 2024 to 19.4% in Q3 2024.

Users also gathered a total of 570,519,029 IOCs during this period.

□□□ □□□□□□□ □□□□□ □□ □□ □□□□

According to the information collected from ANY.RUN's public database of malware samples:

- In Q3, Stealers became the most detected malware type, regaining the top spot after dropping to fourth in Q2.
- Loaders remained in second place for the second consecutive quarter, showing a 49% increase in detections.
- RATs, which led in Q2, dropped to third, while Trojan and Installer malware saw significant declines.
- Ransomware detections rose by 3,021, highlighting its growing threat.

□□□ □□□□□□□ □□□□□□□□ □□ □□ □□□□

In Q3 2024, the malware landscape shifted significantly.

- Lumma, absent from the Q2 ranking, emerged as the top threat.
- AsyncRAT took the second position in Q3, followed by Remcos, which nearly doubled in

detections.

- Agent Tesla also saw a sharp rise, increasing from 439 to 2,316 detections.
- New malware families such as XWorm and Stealc made their debut this quarter.

For more insights into the Q3 2024 threat landscape, including the most popular MITRE ATT&CK TTPs, visit [ANY.RUN's blog](#).

██████ ███.███

ANY.RUN is trusted by over 500,000 cybersecurity professionals worldwide. The platform provides an interactive sandbox that simplifies malware analysis for both Windows and Linux threats. With its powerful threat intelligence tools, such as TI Lookup, YARA Search, and Feeds, ANY.RUN enables users to quickly identify IOCs and gather critical information to respond to incidents more efficiently.

The ANY.RUN team

ANYRUN FZCO

+1 657-366-5050

[email us here](#)

Visit us on social media:

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/753846829>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.