Key Q1 2024 Malware Trends: Report from ANY.RUN Sandbox

DUBAI, DUBAI, UNITED ARAB EMIRATES, July 11, 2024 /EINPresswire.com/ -- ANY.RUN, a cybersecurity provider of interactive malware analysis sandbox and Threat Intelligence products, has released its latest malware trends analysis for the second quarter of 2024. The report, drawn from 881,466 public analysis sessions conducted by its users, provides a comprehensive overview of the most prominent malware families, types, and tactics, techniques, and procedures (TTPs) observed over the past three months.

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

In Q2 2024, ANY.RUN sandbox users analyzed 881,466 files and links. Of these, 18.4% (162,258) were identified as malicious, and 7.0% (61,619) as suspicious, marking a significant rise from 3.5% in Q1

As a result, users gathered a total of 351,423,662 IOCs during this period, with 73,233,314 (20.8%) unique ones.

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

The report shows that Remote Access Trojans (RATs) dominated the threat landscape in Q2 with 5,868 detections, an increase from 4,956 in Q1 2024. Loaders also saw a rise in detections from 4,770 in Q1 to 5,492 in Q2. Trojans emerged as a significant threat with 4,211 detections.

Stealers dropped from the top position in Q1 (5,799 detections) to fourth place in Q2 (3,640 detections), marking a 37.2% decrease. Ransomware detections also fell by 27.5%, from 4,065 in Q1 to 2,946 in Q2.

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

RedLine surged to the top with 3,411 instances, a 379% increase from Q1. Remcos, which led in Q1, fell to second place with 1,282 instances, a 29.4% decrease. NjRAT maintained its third-place position despite a slight decrease in instances.

New entrants like Qbot and Formbook climbed the ranks, indicating shifting trends in malware prevalence.

□□□□ □□□□□□ □□□□□ □□□&□□ □□□□□□□□□□ □□ □□ □□□□

Email Collection (T1114.001) and Virtualization/Sandbox Evasion (T1497.003) retained their top positions. Scheduled Task/Job (T1053.005) saw a significant increase, rising from 11th to 4th place.

New techniques like Scheduled Task/Job: Cron (T1053.006) entered the top 20, suggesting a change in the tactics used by threat actors.

□□□□□□ □□□□□□□□□□□:

The report is based on data from 881,466 interactive analysis sessions contributed by researchers within the ANY.RUN community. These sessions provide valuable insights into the evolving malware landscape.

For more information, visit ANY.RUN's blog.

□□□□□ □□□.□□□:

ANY.RUN supports over 400,000 cybersecurity professionals globally. The platform simplifies malware analysis for threats targeting both Windows and Linux systems. ANY.RUN’s threat intelligence products, including TI Lookup, Yara Search, and Feeds, enhance the ability to identify and respond to threats efficiently.

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

---

in today's world. Please see our Editorial Guidelines for more information.