# ANY.RUN Exposes Long-Running Phishing Campaign Targeting Italian and US Companies

DUBAI, DUBAI, UNITED ARAB EMIRATES, May 21, 2025 /EINPresswire.com/ -- ANY.RUN, a leader in cybersecurity solutions, has released a new case study exposing a long-running phishing campaign that uses Telegram bots for credential exfiltration. By applying a previously documented message interception technique, analysts uncovered attacker-controlled infrastructure dating back to 2022, targeting Microsoft 365 and PEC users through low-effort phishing pages hosted on platforms like Notion and Glitch.

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

Using Telegram's API, the team was able to intercept and analyze live data exfiltration flows, giving them rare visibility into the attacker's operations. This pivot turned a single sandbox session into a broader investigation, revealing credential theft across multiple regions, repeated bot infrastructure reuse, and signs that the campaign is driven by access brokers rather than highly advanced threat actors.

□□□ □□□□□□□□□□ □□□□□ □□□ □□□□□ □□□□□□

Key insights from this in-depth case study include:

· Telegram bots were used as exfiltration channels, with hardcoded tokens and chat IDs embedded in phishing scripts

· Campaign impersonates Microsoft OneNote, Outlook, and Italy's PEC system

· Hosted on low-cost/free infrastructure: Notion, Glitch, RenderForest, and others

· One of the attacks targeted Italian companies, including A&D, Steelsystem Building, Gruppo Amag, and others.

· Threat activity traced from 2022 to 2025, still active at the time of publication

· Victims span industries like logistics, utilities, finance, and digital identity

· ANY.RUN shares detection assets: IOCs, YARA rules, Suricata rules, and Telegram analysis scripts

· Attribution remains uncertain, but patterns suggest credential resale and access brokering

To explore the full technical analysis, including Telegram bot scripts, victim profiling, and detection recommendations, visit ANY.RUN's blog.

□□□□□ □□□.□□□

ANY.RUN is a cybersecurity provider offering a suite of advanced tools for malware analysis and threat intelligence. Its interactive sandbox supports real-time analysis across Windows, Linux, and Android environments, giving security professionals hands-on visibility into malicious behavior. Trusted by over 15,000 companies worldwide, ANY.RUN also offers comprehensive Threat Intelligence solutions, including TI Lookup, Feeds, and YARA Search, to help teams detect threats faster and respond with confidence.

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