ANY.RUN Unveils Critical Steps for Combating New DHL Phishing Attacks

DUBAI, DUBAI, UNITED ARAB EMIRATES, July 23, 2025 /EINPresswire.com/ -- ANY.RUN, a leading provider of threat analysis and intelligence, has released a detailed case study on phishing attacks exploiting DHL branding. The research uncovers crucial insights into early detection of supply chain attacks and offers practical steps for businesses to identify such threats.

□□□ □□□□□□□□□ □□□□□□□ □□□□□□□□ □□□□□□□ □□□□□□□□□ □□□□□□
In an attack investigated by the team at ANY.RUN, threat actors impersonating DHL targeted Meralco, a major utility company in the Philippines, with deceptive emails designed to steal credentials.

□ □□□□□□□□□□ □□□□□□□□□□□ □□□□□□□□: The email contained a file posing as a shipping invoice. When opened, it displayed a fake DHL-styled login page, prompting the user to enter credentials.

□ □□□□□□□□□□ □□□□□□□□□□□□□ □□□ □□□□□-□□□□□ □□□□□□□□: The login form sent entered data to a legitimate online form handler abused to collect stolen credentials.
□ □□□□□□ □□□□□□□□□□□□□□□ □□□□□□ □□□□□□□□□□: Historical analysis found over 200 phishing samples leveraging the form handling service.

This case study highlights the technical methods used in modern supply chain phishing campaigns, from impersonation and infrastructure abuse to payload delivery and credential capture, and offers valuable indicators of compromise (IOCs) for defenders.

Read the full article on ANY.RUN's blog.

□□□ □□□□□□□□□ □□□ □□□.□□□ □□ □□□□□□□ □□□□□□□ □□□□□□ □□□□□□□□ □□□□□□
Businesses utilizing ANY.RUN's solutions gain a significant edge in identifying and mitigating supply chain attacks, ensuring robust defense against cyber threats.

By safely interacting with suspicious emails, files, and URLs in a controlled sandbox environment, businesses can instantly identify and understand malware and phishing, ensuring they don't spread further.

With access to TI Lookup's searchable database of recent threats, businesses can swiftly verify if artifacts in alerts are linked to specific attacks, enabling rapid response and strengthened security measures.

□□□□□□ □□□.□□□
ANY.RUN is an interactive malware analysis and threat intelligence provider trusted by SOCs, CERTs, MSSPs, and cybersecurity researchers. The company's solutions are leveraged by 15,000 corporate security teams for incident investigations worldwide.

With real-time visibility into malware behavior, a focus on real-time interaction and actionable intelligence, ANY.RUN accelerates incident response, supports in-depth research, and helps defenders stay ahead of evolving threats.

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