EINPRESSWIRE

ANY.RUN Reveals Real-World Tactics Used in Cyberattacks on Government Institutions

DUBAI, DUBAI, UNITED ARAB EMIRATES, June 4, 2025 /EINPresswire.com/ -- Responding to a 51% surge in cyberattacks on public-sector entities in Q1 2025, threat intelligence solution provider ANY.RUN has released a case study spotlighting how advanced phishing campaigns are targeting government institutions, and how security teams can counter them using real-time threat intelligence.

□□□□□□□□□□ □□□□ □□□□□□□□: □□□□ □□□□□□□□

Drawing from actual incidents, the study investigates three major phishing scenarios impersonating government structures to distribute malware and harvest credentials. These include:
□ A phishing email campaign targeting South Carolina's Department of Employment and Workforce using FormBook malware;
□ A fraudulent domain mimicking the U.S. Social Security Administration to deploy remote access tools;
□ A malicious PDF disguised as a South African court summons that lures victims into entering Office 365 credentials.

ANY.RUN's solutions — including its Interactive Sandbox, Threat Intelligence Lookup (TI Lookup), and YARA Search — proved essential in investigating these attacks, revealing tactics, techniques, and procedures (TTPs), and generating actionable indicators of compromise (IOCs).

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

Practical Takeaways for Security Teams
Malware campaigns are increasingly impersonating trusted government institutions, threatening

national infrastructure and public trust. ANY.RUN enables security teams to detect and investigate these threats in real time.

The case study shows how analysts can:
□ Monitor domain-specific phishing trends using YARA rules;
□ Investigate malicious domains targeting government websites;
□ Uncover credential harvesting attempts through dynamic sandbox analysis;
□ Leverage TI Feeds for automated protection.

ANY.RUN encourages government cybersecurity leaders to adopt proactive threat hunting and enhance phishing awareness across agencies. The full case study outlines a step-by-step approach to protecting public institutions from evolving threats.

□□□□□ □□□.□□□
ANY.RUN is a leading malware analysis provider trusted by SOC teams, MSSPs, and cybersecurity professionals globally. With a focus on real-time interaction and actionable intelligence, ANY.RUN accelerates incident response and empowers security teams to defend at scale.

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

This press release can be viewed online at: https://www.einpresswire.com/article/818266089