

ANY.RUN Shares Report on Threats Exploiting Recent CrowdStrike Outage

DUBAI, UNITED ARAB EMIRATES, July 23, 2024 /EINPresswire.com/ -- [ANY.RUN](#), a provider of interactive sandbox and threat intelligence solutions, has released a report detailing the cyber threats exploiting the recent CrowdStrike outage. The report identifies two main sources of threats: fake websites imitating CrowdStrike's official domain name and malware disguised as updates or bug fixes.

████████████████████ ██████████ ████████████████

On July 18, CrowdStrike, a well-known cybersecurity firm, released a faulty update that affected millions of Windows users worldwide. This led to a global outage and significant disruptions, causing users to encounter blue screens of death (BSODs) on their devices.



As users and organizations searched for a solution, cybercriminals seized the opportunity to exploit the situation.

██████ ████████████████ ████████████████████ ████████████████████

Following the outage, many websites were created with domain names similar to CrowdStrike's official domain. While some were harmless, others were used for phishing attempts.

ANY.RUN's data shows that the highest number of newly-created fake domains appeared on the first day after the outage. Using ANY.RUN's Threat Intelligence Lookup service, analysts identified over 60 fake domains, which are listed in their report.

