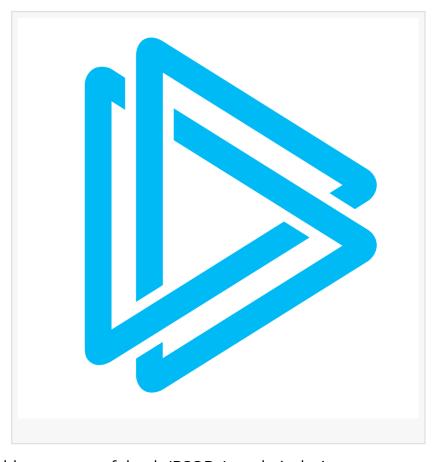


# ANY.RUN Shares Report on Threats Exploiting Recent CrowdStrike Outage

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.

### 

ANY.RUN observed an increase in campaigns spreading malware as updates. One early example was an archive containing Hijackloader, disguised as a CrowdStrike bug fix. When victims opened the file, it installed Remcos, a remote control malware, on their systems.

### 

One of the most sophisticated attacks discovered by ANY.RUN involved a data wiper distributed through a CrowdStrike-themed phishing email and PDF attachment.

The attachment contained an executable that, when launched, asked the user if they wanted to install the update. Upon launching, the wiper erased the system by overwriting files with zero bytes and then reported the successful attack via Telegram.

For the complete report, visit ANY.RUN's blog.

# 000000000000000000

ANY.RUN urges users and organizations to remain cautious and verify all updates or hotfixes before installing them. To ensure accurate information and guidance, it is essential to follow CrowdStrike's official statements.

### 

ANY.RUN is a trusted cybersecurity service used by over 400,000 professionals. It provides an interactive sandbox for simplified malware analysis on Windows and Linux systems, as well as threat intelligence tools like TI Lookup, Yara Search, and Feeds to help users quickly identify IOCs or files, understand threats, and respond to incidents.

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

X

This press release can be viewed online at: https://www.einpresswire.com/article/729814164

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

