مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Phishing Attacks Targeting CrowdStrike Outage

Tracking #:432316074

Date:22-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed phishing emails exploiting the recent CrowdStrike outage. Hackers are attempting to trick recipients into revealing sensitive information or clicking malicious links.

TECHNICAL DETAILS:

In the wake of the recent CrowdStrike global outage, cybercriminals have wasted no time in exploiting the situation by launching phishing scams and creating fake websites to target victims. Hackers are sending phishing emails and making phone calls impersonating CrowdStrike support staff, offering fake recovery solutions and cryptocurrency rewards to lure unsuspecting users into accessing malicious content.

Imposters have posed as independent researchers selling fake recovery solutions, further complicating efforts to resolve the issue.The deceptive domains, including names like crowdstriketoken.com, crowdstrikedown[.]site, and crowdstrike-helpdesk[.]com, have already emerged, targeting individuals desperate to restore their systems. CrowdStrike has published a list of fraudulent domains to help users identify and avoid potential scams.

Indicators of Compromise:
Attached File

RECOMMENDATIONS:

- Be cautious of emails, phone calls, or messages claiming to be from CrowdStrike or Microsoft support. Verify the authenticity of any communication before providing sensitive information or downloading files.
- Avoid clicking on suspicious links or downloading files from untrusted sources. This can lead to email compromise, malware infection, and other scams.
- Ensure that multi-layer phishing mitigations are in place, such as email authentication protocols and employee training on identifying phishing attempts.
- Communicate with official CrowdStrike representatives and adhere to technical advice provided by their support teams. Rely on trusted sources for guidance on resolving the outage.
- Stay vigilant and report any suspicious activity to the appropriate authorities. Collaborate with cybersecurity partners to mitigate the impact of these malicious activities.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.crowdstrike.com/blog/falcon-sensor-issue-use-to-target-crowdstrike-customers/