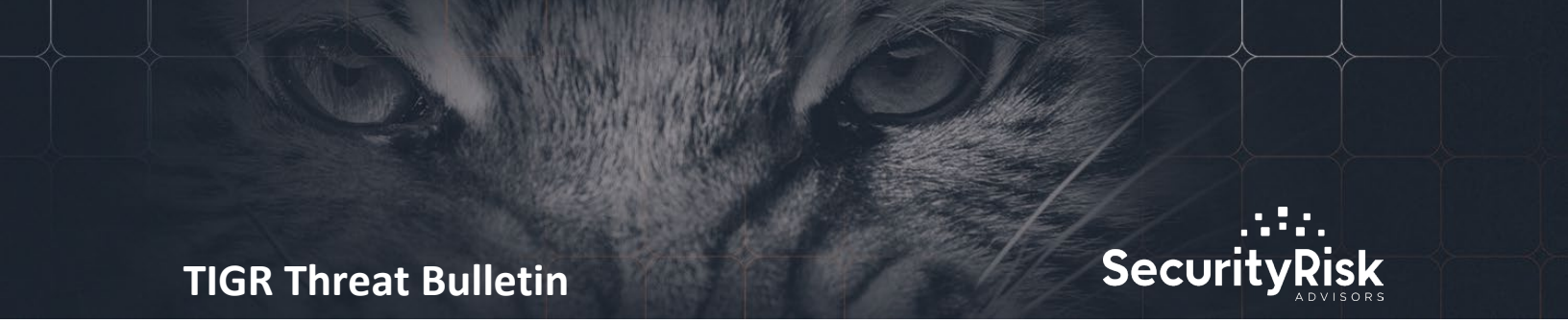

TIGR Threat Bulletin

SecurityRisk ADVISORS

Threat Actors Exploit CrowdStrike Outage with Phishing Campaigns

July 19th, 2024

Executive Summary

Multiple security firms and government organizations have issued warnings regarding threat actors carrying out phishing campaigns and registering malicious domains posing as fake support sites that exploit the disruption caused by the recent CrowdStrike outage. Campaigns have been aimed at both individuals as well as organizations and may be delivered via email or malicious sites. Organizations are advised to only install patches or follow instructions from official CrowdStrike sources such as the crowdstrike.com website and verify the legitimacy of any communications claiming to be from CrowdStrike.

Impact

Installation of a malicious patch or compliance with maliciously crafted instructions could lead to further outages, data theft, unauthorized system access, or a further loss of system stability. This poses a risk to organizations that do not verify the legitimacy of patches or remediation instructions prior to implementing them.

Affected Products

Campaigns are currently targeting CrowdStrike Falcon Sensor customers running Windows machines with the software running on them. Observed campaigns currently include malicious domains that attempt to offer support or patches for the issue and emails claiming to be from “CrowdStrike Support” that are crafted by attackers to gain access to systems.

Safeguards/Recommendations

- Only install patches or follow instructions provided by CrowdStrike via official channels. CrowdStrike's blog post, which has been used to release updates regarding this outage, can be found here.
- Utilize DNS services to block access to newly registered domains to prevent users from accidentally accessing a spoofed domain.
- SRA is actively monitoring XDR / CSOC client environments for known domains and URLs related to malicious CrowdStrike support sites.

References

- https://www.pcmag.com/news/dont-fall-for-it-hackers-pounce-on-crowdstrike-outage-with-phishing-emails
- https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update
- https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/