Communicative Efficacy: The 2024 CrowdStrike Incident and Associated Handling of Remediation

Introduction

A mass computer outage caused by a faulty update to CrowdStrike's Falcon security software caused major interruptance of computer-reliant service on a global scale in July of 2024. Our aim is to analyze and interpret communication from CrowdStrike in this incident. We highlight both potential flaws with the methods of communication, as well as indicate when proper communication occurs. Likewise, both the perceived effectiveness of CrowdStrike's response and those affected are considered to provide a holistic view on the aforementioned effectiveness.

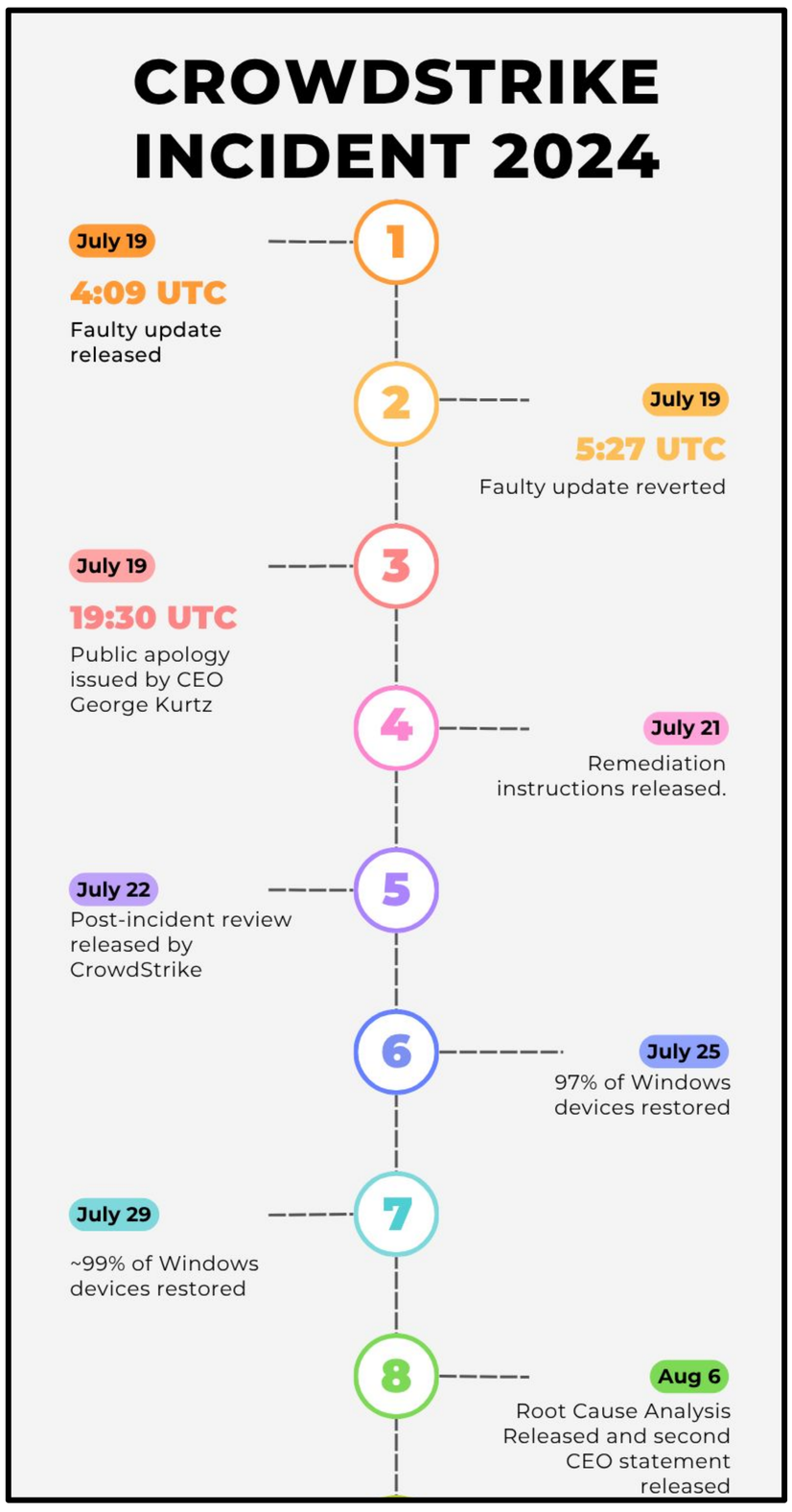
Research Question

Did CrowdStrike release timely and accessible communications that served to alert customers and contain the problem? And how did this responsiveness serve to mitigate/worsen the situation and ensure it doesn't happen again?

Methods

To analyze the communications surrounding the outage, we examined:

- Official reports from CrowdStrike
- News articles reporting on the impact
- Responses from individuals and corporations



Results

The public response from CrowdStrike through their official channels and website was professional and included multi-modal forms of communicating reconciliation steps and procedures, especially within their guidance hub. CrowdStrike directly messaged clients to inform them the outage was caused by a bug in a content update. CrowdStrike acknowledged their mistake with an apology, and took action by having their technical support work closely with customers to get their systems back online quickly. By doing so, CrowdStrike was able to do their best to mitigate the problem, despite the millions of devices impacted and billions in finanical losses. In the aftermath, CrowdStrike released the results of their investigation and a plan for internal actions to prevent similar incidents in the future.

Discussion

We claim that CrowdStrike's response was effective in managing an incident of this scale. CrowdStrike's transparent and collaborative approach to releasing their information provides an insight into how to best handle communication intended to address mass hysteria quickly and effectively. Despite the positives of their response, some recommendations can be made. CrowdStrike should have more clearly admitted the severity of the outage in their apology. Following this, customer frustrations could have been better alleviated with better estimations of when the outage would be resolved. The frustrations caused by the failure to do these things contributed to the erosion of public trust in CrowdStrike.

References