Mason Kotlarz

Jeff Franklin

Cpr E 2340

April 21st 2025

The Largest Global IT Outage In History

On July 19, 2024 Crowdstrike pushed an update to their service including a channel file 291 (C-00000291*.sys) with timestamp 2024-07-19 0409 UTC. This file came with a system logic flaw. This logic flaw would cause falcon, which was the service running on the machines to fail, and due to the importance of teh security and level of access the falcon service needed it ran at the kernel level. As a Windows kernel process the process has the highest level of privileges, giving Falcon the ability to monitor operations in real time across the OS. But this file due to the logic flaw would cause crowdstrikes Falcon to crash leading to the Windows kernel itself to crash. Once the computer had started the update and had the channel file on the system it caused the machine to crash. This led to about 8.5 million Windows devices worldwide to crash.

Of these approximately 8.5 million Windows devices the majority of machines that were crashed were organizations that used crowdstrike system wide. Major airlines like Delta, United, and American Airlines were forced to ground flights due to the crash with the system left inoperable rendered planes unable to fly. Delta alone canceled more than 7,000 flights over five days, affecting approximately 1.3 million passengers (Quinn, Dave, and Becca Longmire). Alongside the airline industry the Healthcare and the Federal Government were hit hard aswell hospitals, emergency services, and public services had to work through the so called “blackout” due to the interconnected IT systems it caused several emergency rooms to revert to manual

processes, delaying patient intake, diagnostics, and even surgeries. The social workers were also hit hard with DMV systems, social services, or law enforcement platforms becoming unassable. Even agencies ranging from the CIA, to the NNSA were rendered disabled. Working for the NNSA this last summer I got to experience firsthand what happened during the outage. With employees being given a day off while the IT staff worked tirelessly to remedy the systems as fast as possible. Thousands of IT teams had to urgently respond, like out working 24–48 hours straight to isolate the issue, patch systems, and restore services.

To respond to the incident, crowdstrike was on calls and immediately interfacing with its customers. The Crowdstrike employees worked almost as tirelessly as the IT staff they were working with and supportiong. The company's technicians and software developers quickly identified the faulty update and released a fix to address the issue, and while the employees were able to guide customers and help service each of their individual organization needs. Crowdstrike was able to deploy a fix for the issue in 79 minutes,however this worked but was very manual. Certain organizations within the healthcare world, and the federal government had the funds for large IT staff and were able to patch the systems much quicker. However larger companies like delta airlines for example were unable to patch systems due the need for IT staff to get their hands on each device manually. Crowdstrike was unable to develop a remote based fix, so each device needed to be repaired manually thus rendering delta airlines struggling to patch machines they have few IT staff able to service. In addition to working closely with companies and organizations around the world, Crowdstrike maintains clear and public communication. CEO of Crowdstrike George Kurtz publicly acknowledged the failure and issued an apology, taking responsibility for the global impact. While having full transparency of what caused the issue and what will be done to prevent such an issue. By publishing a detailed report of the internal audit

and haow the crash was created and pushed out into production without any error checking catching the issue. Crowdstrike partnered with several other companies to help solve the issue further by working with Microsoft to create solutions and solve the issue, and with managed service providers (MSPs) and enterprise clients to assist in large-scale system recovery. Over time with their partnership with different MSPs and microsoft they were able to release scripts and tools to help automate the cleanup and reboot process across networks.

Overall crowdstrike did a realitivlty good job at responding to the incident however CrowdStrike's communication was reactive at first while this was great in all they went straight into manually solving the problem with provided an immediate fix, however they were unable to create a software/automated solution allowing for much quicker patching within a reasonable amount of time. In an ideal world they could've provided a script quicker or immediately to nullify the issue. Along with this change in response publishing recovery playbooks, videos, or templates within hours could have eased recovery for smaller organizations instead of manually going to each organzation to explain the solution and fix. By being more transpart earlier and creating a solution guide with images and video would've been more helpful for organizations who didnt have immediate crowdstrike employees they could go to for advice. These efforts would rebuild trust with clients and stakeholders and demonstrate a commitment to accountability. Lastly a proactive solution would include designing their update system to include failsafes — such as sandbox testing, rollback features, or staged releases. Working to identify potential large scale issues before deployment into world wide production could have prevented this issue entirely.

Ultmatly the crowdstrike falcon channel file will go down in history as one of the first global IT outages ever. Beginning with a single file in a security update leading to a global

shtudown, disrupting air travel, healthcare, government operations, and countless other sectors. While CrowdStrike worked tirelessly along with IT departments around the global and were largely effective lessons about ways critical software updates are tested, deployed, and managed. Moving forward, this event should push companies like CrowdStrike and the industries they serve to invest more in proactive risk mitigation, transparent communication

Work Cited

Kerner, Sean Michael. “Crowdstrike Outage Explained: What Caused It and What’s Next.” WhatIs, TechTarget, 29 Oct. 2024, www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next.

Quinn, Dave, and Becca Longmire. “Global Technology Outage Caused by Failed Software Update Shuts down Flights, Banks and Business.” People.Com, PEOPLE, 19 July 2024, people.com/delta-united-american-airlines-flights-grounded-global-technology-outage-8680613.