CrowdStrike has a new guidance hub for dealing with the Windows outage

The page includes technical information on what caused the outage, what systems are affected, and CEO George Kurtz's statement. It contains links to Bitlocker key recovery processes and to various third-party vendor pages about dealing with the outage, as well.

The page points to a knowledge base article (which only logged-in customers can access) for using a bootable USB key. Microsoft released such a tool yesterday that automatically deletes the problematic channel file that caused machines to blue screen.

CrowdStrike also published a blog yesterday warning that threat actors have been taking advantage of the situation to distribute malware, using "a malicious ZIP archive named crowdstrike-hotfix.zip."

> *The ZIP archive contains a HijackLoader payload that, when executed, loads RemCos. Notably, Spanish filenames and instructions within the ZIP archive indicate this campaign is likely targeting Latin America-based (LATAM) CrowdStrike customers.*

Later in the blog:

> *Following the content update issue, several typosquatting domains impersonating CrowdStrike have been identified. This campaign marks the first observed instance in which a threat actor has capitalized on the Falcon content issue to*

> *distribute malicious files targeting LATAM-based CrowdStrike customers.*

CrowdStrike says organizations should only be working directly with CrowdStrike’s representatives using official channels, and should use only the guidance its support team provides.

https://www.theverge.com/2024/7/21/24202923/crowdstrike-remediation-guidance-hub-windows-bsods-outage-malware