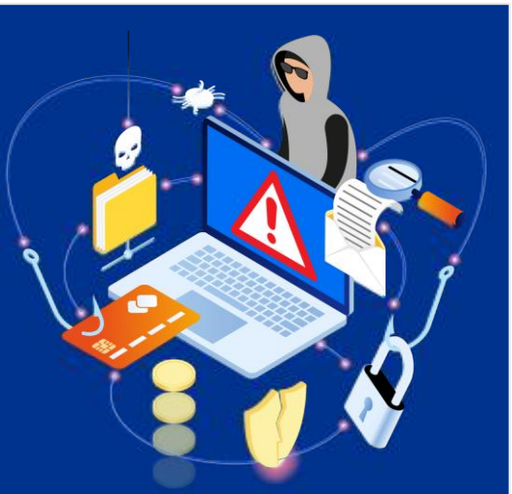
KPMG Cyber Threat Intelligence Platform

CrowdStrike Causing Global Windows Outage



CrowdStrike, a leading cybersecurity platform providing advanced solutions worldwide, is currently experiencing a significant outage affecting users globally. The issue primarily manifests as Blue Screen of Death (BSOD) errors on Windows systems due to a technical error in their main product, Falcon Sensor. The issue, which seemingly affects multiple versions of Windows has been observed following the latest updates of the CrowdStrike agent. This outage has numerous individual users and organizations across countries such as Croatia, Philippines, US, Germany, Mexico, India, and Japan.

CrowdStrike has acknowledged reports of widespread crashes on Windows systems attributed to the Falcon Sensor. Symptoms include hosts experiencing bugchecks and BSOD errors specifically related to 'csagent.sys'. This issue has resulted in extensive disruption, with reports indicating over 3,000 laptops and servers affected across multiple locations in Australia and New Zealand alone, and similar impacts reported globally. Affected users, including defense agencies, banks, payroll services, major retailers, and individual consumers, have been advised by CrowdStrike to refrain from opening support tickets at this time, while the engineering teams are actively working to resolve the issue. While the company is focusing on fixing the underlying problem causing the BSOD errors, concerns regarding the restoration of devices currently stuck in boot loops even after the issue is resolved still remain.

In response CrowdStrike has provided a workaround for users experiencing persistent crashes on their Windows systems due to ongoing issues. If hosts cannot stay online to receive Channel File Changes, users should follow these steps:

- Boot into Safe Mode or Windows Recovery Environment.
- Navigate to C:\Windows\System32\drivers\CrowdStrike.
- Delete the file matching "C-00000291*.sys" or rename it to "C-00000291*.sys.renamed" and reboot the host normally.

File integrity verification may cause issues with this workaround and shall be disabled before performing the above steps. Further, it must be noted that this workaround may not work on LAPS or Bitlocker enabled systems and further fix is awaited.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

CrowdStrike Causing Global Windows Outage