# KPMG Cyber Threat Intelligence Platform

## CrowdStrike Global Windows Outage : An Update on the State of Affairs

On 19 July 2024 at approximately 9:30 AM IST, CrowdStrike released a content deployment for their endpoint security solution Falcon, triggering a worldwide outage of Windows systems in which the product was installed. 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, roots from a single content update and has disproportionately affected individuals and organizations across all sectors throughout the globe, including major countries such as US, Australia, Germany, Mexico, India, and Japan.

Symptoms of the issue include Windows hosts experiencing bugchecks/BSOD error and CrowdStrike has acknowledged reports of this widespread crash and clarified that it is not a cyber attack. Owing to the technicalities of the outage, CrowdStrike has clarified that the issue stems from a 'channel file 291' that is responsible for how named-pipe executions are evaluated by Falcon. The recent update aimed to aid in detection of malicious named pipe techniques has triggered a logic error leading to this global crash. Mac and Linux systems have been reportedly unaffected. This global digital meltdown has struck various sectors including that of critical infrastructure and emergency response alike resulting in airlines operations being grounded, temporary disruption of 911 systems, banking and primary healthcare services.

While as of 19 July 2024 around 11:00 AM IST, CrowdStrike has remediated the channel file and systems brought online after this time are not impacted, difficulty in remediating systems that have already crashed looks arduous. Recovery is projected to cost extensive time and efforts due to manual intervention required to apply this fix on most of the individual hosts.

The situation has also proved to be a playground for attackers who are leveraging various social engineering techniques such as phishing, posing as security researchers or CrowdStrike staff to spread malicious scripts posing as potential fixes etc. A list of IOCs including domains that may be used for malicious purposes and excerpts of recommendation measures shared by CrowdStrike can be found in the upcoming section.

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 Cyber Threat Intelligence Platform

## CrowdStrike Global Windows Outage : An Update on the State of Affairs

### Understanding:

Based on the CrowdStrike communications and public sources we have the following understanding of the situation:

- Initial reports indicate that system crash(es) are occurring on system boot, preventing network-based remediation.
- Deletion of the file "C-00000291*.sys" located at "C:\Windows\System32\drivers\CrowdStrike" remediates the issue, however, due to agent protection, this action must be done via safe mode/pre-boot command line.
- CrowdStrike have issued an update to revert the content deployment.
- BitLocker may complicate the remediation, unless keys are easily accessible for the affected systems.
- Channel file "C-00000291*.sys" with timestamp of 0527 UTC or later is the reverted (good) version.
- Channel file "C-00000291*.sys" with timestamp of 0409 UTC is the problematic version.
- This bad file has a SHA-256 hash of "390c4532761fa80e6823eedfb654b02c3341e251d0df3efcd09e811d93b36b8d".

### What should you do?

- Follow recovery measures and updates through official channels
- Be vigilant about scam websites and phishing emails
- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.

### Recommended Actions:

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. Some of the actions described in this advisory bulletin require Administrative Passwords to be shared in order to execute the recommended action. The sharing of Administrative Passwords should be tracked and reset after the remediation of this incident.

**Systems with the deployment but not yet impacted:**

- Prioritise Update: Implement the update that reverts the content deployment immediately.
- Monitoring: Closely monitor these systems for any signs of instability.
- Backups: Ensure backups are up to date.

**Identifying impacted systems:**

- Use the below query on Falcon portal to identify hosts with the impacted channel file update. The impacted channel file is "C-00000291*.sys" with timestamp of 0409 UTC
    - #event_simpleName=LFODownloadConfirmation | TargetFileName="C-00000291*.sys" | table([timestamp, ComputerName, TargetFileName]) |sort(timestamp)

KPMG

# KPMG Cyber Threat Intelligence Platform

## CrowdStrike Global Windows Outage : An Update on the State of Affairs

**Systems with BitLocker**

- Ensure BitLocker recovery keys are accessible as they are essential for data recovery in the event of a crash. Keys can be checked via the Microsoft Device List. (https://myaccount.microsoft.com/device-list)

### Recommended Actions: Individual Hosts

**If systems are experiencing BSOD, they need manual intervention**

- Boot Windows into Safe Mode or the Windows Recovery Environment.
- Navigate to "%WINDIR%\System32\drivers\CrowdStrike".
- Locate and delete the file matching "C-00000291*.sys".
- Boot the system normally.

**Cloud Systems and Virtual Servers**

- Detach the OS disk volume from the impacted virtual server.
- Create a snapshot or backup of the disk volume.
- Attach/mount the volume to a new virtual server.
- Navigate to "%WINDIR%\System32\drivers\CrowdStrike".
- Delete the file matching "C-00000291*.sys".
- Detach the volume from the new virtual server.
- Reattach the fixed volume to the impacted virtual server.

### Recommended Actions: Cloud Virtual Machines

There are currently two recovery options for the Azure Virtual machines.

**Recovery Option 1:** Relaunch the virtual machine from a snapshot or image taken before 18:30 PM CET.

**Recovery Option 2:**

- Troubleshoot a Windows VM by attaching the OS disk to a repair VM through the Azure portal
- Once the disk is attached, customers can attempt to delete the following file:
- Windows/System32/Drivers/CrowdStrike/C00000291*.sys
- The disk can then be attached and re-attached to the original VM.

There are currently two recovery options for the AWS EC2 instance.

**Recovery Option 1:** Relaunch the EC2 instance from a snapshot or image taken before 18:30 PM CET.

# KPMG Cyber Threat Intelligence Platform

## CrowdStrike Global Windows Outage : An Update on the State of Affairs

**Recovery Option 2:**

- Create a snapshot of the EBS root volume of the affected instance.
- Create a new EBS Volume from the snapshot in the same availability zone.
- Launch a new Windows instance in that availability zone using a similar version of Windows.
- Attach the EBS volume from step (2) to the new Windows instance as a data volume.
- Navigate to \windows\system32\drivers\CrowdStrike\ and delete "C00000291*.sys".
- Detach the EBS volume from the new Windows instance.
- Create a snapshot of the detached EBS volume.
- Replace the root volume of the original instance with the new snapshot. Start the original instance.

## FAQ

Q: How can I access the CrowdStrike Tech Alert for this issue?

A: The Tech Alert is accessible at this link: https://supportportal.crowdstrike.com/s/article/Tech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19. However, it requires an account to be accessed.

Q: Does restoring from a backup resolve the issue?

A: Yes, restoring a system from a backup made before the deployment of the BSOD-causing CrowdStrike update should resolve the issue.

Q: Does the issue impact Mac- or Linux-based systems?

A: No, the issue does not impact Mac- or Linux-based systems.

Q: What can be done to enable employees resume work if their system was affected?

A: In an environment working with a cloud solution such as Microsoft Office 365, you may consider temporarily lifting your conditional access policies for Office 365 to enable staff access their work environment via BYOD. This must be done in consultation with your CISO office and/or Head of Information Security.

Q. How do I protect against scams or phishing campaigns originating as part of this event?

A. We have provided a list of IOCs that you may monitor across the environment. Additionally, stay vigilant against any anomalies of threat actor campaigns that may leverage this event. You may also consider, building more resilient IT processes and test through tabletop and/or purple team exercises. Recovery of systems and/or data loss may be expedited with staff augmentation.

KPMG

# KPMG Cyber Threat Intelligence Platform

## CrowdStrike Global Windows Outage : An Update on the State of Affairs

| Indicators of Compromise: IP Addresses |
|---|
| 104.21.75[.]98 |
| 13.248.243[.]5 |
| 145.131.1[.]37 |
| 212.1.210[.]95 |
| 104.247.81[.]53 |
| 172.67.220[.]94 |
| 198.49.23[.]144 |
| 54.84.104[.]245 |
| 104.18.40[.]47 |
| 185.230.63[.]107 |
| 185.230.63[.]186 |
| 76.223.105[.]230 |
| 89.117.139[.]195 |
| 162.255.119[.]155 |
| 185.230.63[.]171 |
| 198.185.159[.]144 |
| 198.185.159[.]145 |
| 34.149.87[.]45 |

| Indicators of Compromise: Domains | |
|---|---|
| crowdstuck[.]org | whatiscrowdstrike[.]com |
| crowdstrike[.]buzz | crowdstrikereport[.]com |
| crowdstrikefix[.]com | crowdstrikeoutage[.]info |
| crowdstrikefix[.]zip | crowdstrikedoomsday[.]com |
| crowdstrike0day[.]com | crowdstrikeblueteam[.]com |
| crowdstrikebsod[.]com | fix-crowdstrike-bsod[.]com |
| crowdstrikedown[.]com | microsoftcrowdstrike[.]com |
| crowdstrike-bsod[.]com | crowdstrike-helpdesk[.]com |
| crowdstrikeodayl[.]com | crowdstrikebluescreen[.]com |
| crowdstriketoken[.]com | crowdstrike.phpartners[.]org |
| crowdstrikedown[.]site | crowdfalcon-immed-update[.]com |
| crowdstrikeclaim[.]com | fix-crowdstrike-apocalypse[.]com |
| crowdstrikeupdate[.]com | |