**Threat Intel Advisory to proactively prevent Cyber Attacks on unsuspecting users seeking help for the BSOD issue caused by Crowdstrike's faulty update on Windows machines - *SOC Tiger Team and CRS Threat Intel Team***

With recovery activity in full swing across the globe to fix the BSOD issue caused by Crowdstrike's faulty update on Windows machines, and many reaching out for quick fixes and easy workarounds, the hacking community have pounced on the opportunity to Masquerade as Genuine Help and carry out their malicious agenda on unsuspecting users seeking help.
We have been monitoring this situation closely and have created a list of IOCs to help prevent hackers taking advantage of this situation. Please consume as you see fit.

**Suspicious Domains: (Block proactively or keep monitoring on high priority)**

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

**Threat Intel on fake hot fix file named "Crowdstrike-hotfix.zip"**

MD5: 1e84736efce206dc973acbc16540d3e5
SHA-1: fef212ec979f2fe2f48641160aadeb86b83f7b35
SHA-256: c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2

Threat - HijackLoader is a modular malware acting as a vehicle for distributing different types of malicious software on compromised systems. It gained prominence during the summer of 2023 and has since been used in multiple attacks against organizations from various sectors, including hospitality businesses.

For a detailed report, refer: Malware analysis crowdstrike-hotfix.zip Malicious activity | ANY.RUN - Malware Sandbox Online

**Malicious or Misleading Infrastructure Related to CrowdStrike Incident**

Falcon Sensor, a CrowdStrike EDR solution, caused widespread outages affecting numerous Windows systems worldwide, affecting both servers and workstations. Further Insikt Group reporting on the incident can be found in the Validation URLs of this note. In the hours that followed the incident, Insikt Group identified the registration of several malicious, or otherwise misleading, domains likely associated with tech support and cryptocurrency scams.

**Domains:**

crowdstrikedoomsday[.]com
crowdstrikebluescreen[.]com
crowdstriketoken[.]com
fix-crowdstrike-apocalypse[.]com
crowdstrike0day[.]com
crowdstrike-helpdesk[.]com
microsoftcrowdstrike[.]com
crowdstrikebsod[.]com
crowdstrikefix[.]com
whatiscrowdstrike[.]com
supportfalconcrowdstrike[.]com

**IPs:**

212.1.210[.]95
80.78.22[.]84
89.117.139[.]195
145.131.1[.]37

**DOM Hashes:**

21e112db319dbb181376474735a3a893fa9fa32e988ce41688fb5d09be4e1708
1d678ddb7660a10f6a0920f15bf9dfd8639246e1c508f441381a3bff70bcd6eb
9176f14d6bf061e600073d7c4d77d9dc6e06eb877df3949ef778c9d077ee4cdd
d7672d0cfbf67a845b441b5f563bf12f0975943f9e87d67bde48c1964619598d
8359f1b87f1ce8cf27e7ced477d5f4976bb91931067032969ea34532d08471a9
5aa1b6459155cf6950ed7ae019853e598dc81f67395b18b0b22bd9cc182882b7
9c28a02f29ef124ae1947010a2e69c1aaf127262756e63c43bad4017239eee7e

**Cryptocurrency Wallet Addresses:**

0x1AEAe8c6F600d85b3b676ac49bb3816A4eB4455b
0x23512bE6984924F9c39239EE210e16848312CFa9

Reference: https://app.recordedfuture.com/portal/research/insikt/doc:xHcJvV