Threat Intel Advisory 2.0 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 an updated list of IOCs including yesterday's content 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-helpdesk[.]com
crowdstrikebluescreen[.]com
crowdstrike-bsod[.]com
crowdstrikedown[.]site
crowdstrike0day[.]com
crowdstrikedoomsday[.]com
crowdstrikefix[.]com
crashstrike[.]com
crowdstriketoken[.]com
fix-crowdstrike-bsod[.]com
bsodsm8rLIxamzgjedu[.]com
crowdstrikebsodfix[.]blob[.]core[.]windows[.]net
crowdstrikecommuication[.]app
fix-crowdstrike-apocalypse[.]com
crowdstrikeoutage[.]info
clownstrike[.]co[.]uk
whatiscrowdstrike[.]com
clownstrike[.]co
microsoftcrowdstrike[.]com
crowdfalcon-immed-update[.]com
crowdstuck[.]org
failstrike[.]com
winsstrike[.]com
crowdpass[.]
supportfalconcrowdstrikel[.]com
crowdstrikehealthcare[.]com
crowdstrikeclaim[.]com
crowdstrikebug[.]com
crowdstrikeupdate[.]com
crowdstrikefail[.]com
crowdstrikeoopsie[.]com
crowdstrike[.]fail
crowdstrike[.]woccpa[.]com
crowdstrikereport[.]com
crowdstrike-cloudtrail-storage-bb-126d5e[.]s3[.]us-west-1[.]amazonaws[.]com
hoo[.]be/crowdstrike
crowdstrike[.]orora[.]group
supportportal.crowdstrike[.]com/s/login/?mkt_tok=MjgxLU9CUS0yNjYAAAGUa2XCfb6M3jra...

sinkhole-d845c7b471d9adc14942f95105d5ffcf.crowdstrikeupdate[.]com
crowdstrike[.]okta[.]com/app/coupa/exkqmsghe0qkvea070x7/sso/saml
crowdstrike-falcon[.]online
crowdstrikerecovery1[.]blob[.]core[.]windows[.]net
crowdstrikeoutage[.]com
sedo[.]com/search/details/?partnerid=324561&language=es&domain=crowdstrike[.]es&ori...
supportportal[.]crowdstrike[.]com
isitcrowdstrike[.]com
crowdstrike[.]black
crowdstrikefix[.]zip
crowdstrikeold[.]com
crowdstrikeout[.]com
crowdstrike-out[.]com
crowdstrikeoops[.]com
crowdstrikefixer[.]com
crowdstrikesucks[.]com
crowdstrikeclaims[.]com
crowdstrikeglitch[.]com
crowdstrikelawsuit[.]com
crowdstrikesuporte[.]com
crowdstrikezeroday[.]com
crowdstrikerecovery[.]com
crowdstrike-bluescreen[.]com
crowdstrikeclassaction[.]com
crowdstrikewindowsoutage[.]com
crowdstrike.phpartners[.]org
crowdstrikebsod[.]com
crowdstrikeodayl[.]com
crowdstrike[.]buzz
crowdstrikedown[.]com
crowdstrikeblueteam[.]com
supportfalconcrowdstrike[.]com
crowdstrikeupdate.com
crowdstrikefix.zip
crowdstrikereport.com
crowdstrike-helpdesk.com
microsoftcrowdstrike.com
crowdstrikeoutage.info
crowdstrikebsod.com
crowdfalcon-immed-update.com
whatiscrowdstrike.com
fix-crowdstrike-bsod.com
fix-crowdstrike-apocalypse.com
crowdstuck.org
crowdstriketoken.com
crowdstrikefix.com
crowdstrikedoomsday.com
crowdstrikebluescreen.com

crowdstrike0day.com
crowdstrike-bsod.com
crowdstrike-hotfix.zip
crowdstrikeclaim.com

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

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

Additional files with their SHA256 values

File Name	SHA256 Hash
sqlite3.dll	02f37a8e3d1790ac90c04bc50de73cd1a93e27caf833a1e1211b9cc6294ecee5
vclx120.bpl	2bdf023c439010ce0a786ec75d943a80a8f01363712bbf69afc29d3e2b5306ed
instrucciones.txt	4f450abaa4daf72d974a830b16f91deed77ba62412804dca41a6d42a7d8b6fd0
maddisAsm_.bpl	52019f47f96ca868fa4e747c3b99cba1b7aa57317bf8ebf9fcbf09aa576fe006
Setup.exe	5ae3838d77c2102766538f783d0a4b4205e7d2cdba4e0ad2ab332dc8ab32fea9
datastate.dll	6010e2147a0f51a7bfa2f942a5a9eaad9a294f463f717963b486ed3f53d305c2
madexcept_.bpl	835f1141ece59c36b18e76927572d229136aeb12eff44cb4ba98d7808257c299
maidenhair.cfg (HijackLoader configuration)	931308cfe733376e19d6cd2401e27f8b2945cec0b9c696aebe7029ea76d45bf6
rtl120.bpl	b1fcb0339b9ef4860bb1ed1e5ba0e148321be64696af64f3b1643d1311028cb3
vcl120.bpl	b6f321a48812dc922b26953020c9a60949ec429a921033cfaf1e9f7d088ee628
battuta.flv	be074196291ccf74b3c4c8bd292f92da99ec37a25dc8af651bd0ba3f0d020349
RemCos Payload	48a3398bbbf24ecd64c27cb2a31e69a6b60e9a69f33fe191bcf5fddbabd9e184

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
213.5.130[.]58[:]443

DOM Hashes:

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

Cryptocurrency Wallet Addresses:

0x1AEAe8c6F600d85b3b676ac49bb3816A4eB4455b
0x23512bE6984924F9c39239EE210e16848312CFa9

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