Blue Screen Mayhem: When CrowdStrike's Glitch Became Threat Actor's Playground

loginsoft.com/post/blue-screen-mayhem-when-crowdstrikes-glitch-became-threat-actors-playground

Home

/

Blog

July 29, 2024

Profile Icon
Jason Franscisco

Green Plus icon

In the ever-evolving landscape of cybersecurity, even the smallest hiccup can create ripples that turn into tsunamis. The recent Blue Screen of Death (BSOD) outage at Microsoft, caused by a compatibility issue with CrowdStrike, was just such an event. But as we've learned time and time again, where there's chaos, there are opportunists waiting to pounce.

As if managing a major outage wasn't challenging enough, three separate malware campaigns surfaced, exploiting this catastrophe through phishing websites and emails. Apart from these, various CrowdStrike domains have been created for malicious intent; a list of a few domains can be found in the end section.

Figure: Overview of Campaigns Taking Advantage of Microsoft CrowdStrike Outage

Campaign 1: Fake Updates with RemCos RAT

One concerning strategy involved the distribution of misleading updates. Threat actors circulated ZIP files named "crowdstrike-hotfix.zip," ostensibly offering a solution to the BSOD problem. However, these files actually contained the RemCos Remote Access Trojan (RAT), which enables unauthorized remote access to affected systems, potentially leading to data breaches.

In one instance, a phishing website impersonating BBVA bank was used to distribute this malicious ZIP file. When downloaded and run, the file activated HijackLoader, which subsequently installed the RemCos RAT. This case demonstrates how attackers took advantage of the situation to compromise systems by posing as providers of crucial updates.

For intel on the RemCos RAT and HijackLoader, visit Loginsoft's threat profiles:

- RemCos RAT
- HijackLoader

Campaign 2: Daolpu Stealer via Fake Microsoft Recovery Manual

The threat actors behind the Daolpu Stealer delivered the malware via a Word document containing a malicious macro, disguised as a recovery manual. Once the Daolpu Stealer was executed, the following behavior was observed:

- Termination of the Chrome process.
- Collection of credentials from Chrome and Mozilla browsers.
- Exfiltration of data to the command-and-control (C2) server.

Sample: https://tria.ge/240722-q489ga1fnk

For more information about the Daolpu Stealer, visit: https://vi.loginsoft.com/threat-profiles/Daolpu-Malware-Campaign

Campaign 3: The Handala Hacking Hullabaloo

The Handala hacking group utilized the outage to further their political agenda. They claimed to have conducted a wiper malware attack targeting Israeli organizations, disguising it as a CrowdStrike update. This malware was designed to not only disrupt systems but also to permanently delete data, potentially causing significant damage.

This incident illustrates how certain groups may exploit widespread technical issues to carry out targeted attacks, combining cybersecurity threats with political motivations.

Threat Bites

table { border-collapse: collapse; width: 100%; margin: 20px 0; border-radius: 8px; font-family: 'Plus Jakarta Sans', sans-serif; /* Webflow-friendly font */ font-size: 14px; } th, td { padding: 20px 20px; border: 1px solid rgba(255, 255, 255, 0.2); text-align: left; } th { font-weight: bold; /* background-color: rgba(255, 255, 255, 0.12); */ background-color: rgb(26 49 63); color: #FFF; } tr:nth-child(odd) { background-color: rgba(0, 0, 0, 0.05); /* Added subtle banding for visual clarity */ }

Threat Actos	TA544, APT 33, Handala

Malwares	HijackLoader, Remcos RAT, Daolpu Stealer
Targeted Country/Region	Latin America, Israel
Targeted Industry	Banks
First Seen	July 2024
Last Seen	July 2024
LOLBAS	Certutil.exe, Schtasks.exe
Telemetry	Sysmon, Security, PowerShell

Malicious Domains:

crowdstrike-bsod[.]co
crowdstrike-bsod[.]com
crowdstrike-fix[.]zip
crowdstrike-helpdesk[.]com
crowdstrike-out[.]com
crowdstrike[.]blue
crowdstrike[.]bot
crowdstrike[.]cam
crowdstrike[.]ee
crowdstrike[.]es
crowdstrike[.]fail
crowdstrike0day[.]com
crowdstrikebluescreen[.]com
crowdstrikebsod[.]co
crowdstrikebsod[.]com
crowdstrikebug[.]com
crowdstrikeclaim[.]com
crowdstrikeclaims[.]com

References:

- https://www.bleepingcomputer.com/news/security/fake-crowdstrike-fixes-target-companies-with-malware-data-wipers/
- https://www.crowdstrike.com/blog/fake-recovery-manual-used-to-deliver-unidentified-stealer/

- https://www.crowdstrike.com/blog/likely-ecrime-actor-capitalizing-on-falcon-sensor-issues/

Author:

Saharsh Agrawal

29, July 2024