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

By Loginsoft

Published: 2026-02-20 · Archived: 2026-04-05 18:42:12 UTC

Introduction

A polymorphic **Malware** designed to evade detection while stealing sensitive information from infected systems. Similar in behavior and intent to **WASP Stealer**, Discock Stealer leverages obfuscation and frequent code changes to bypass signature-based defenses. The article focuses on its behavior, delivery mechanisms, and why such polymorphic stealers pose a growing challenge for modern security detection.

Key Takeaways

- Blue Screen Mayhem caused widespread system instability across Windows environments.
- CrowdStrike’s Glitch created security blind spots during outage and recovery phases.
- Blue Screen of Death (BSOD) incidents weakened defenses, increasing attacker opportunities.
- Operational failures can amplify threat actor activity if not managed securely

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.

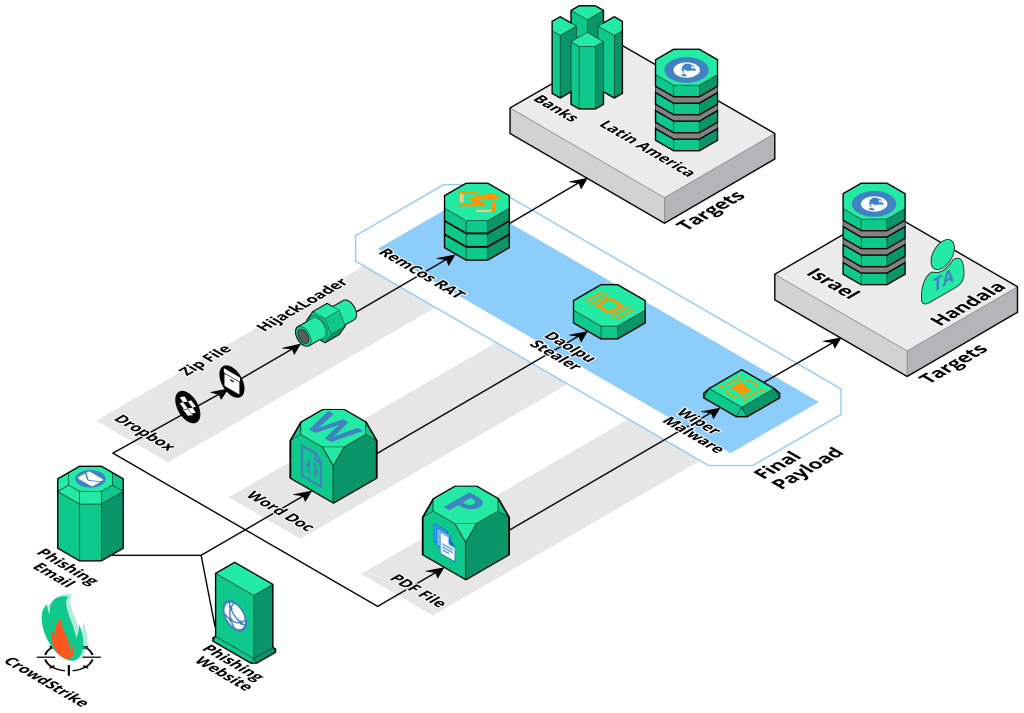

Figure: Overview of Campaigns Taking Advantage of Microsoft CrowdStrike Outage

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: Triage

For more information about the Daolpu Stealer, visit: 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

Threat Actors	TA544, APT33, 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

Conclusion

The blog highlights that **Blue Screen Mayhem** was not just an availability issue but a security concern amplified by scale and timing. **CrowdStrike's Glitch** demonstrated how outages can disrupt defensive controls and open windows of opportunity for attackers, especially during emergency response and remediation. The incident reinforces the need for resilient security architectures, controlled recovery processes, and contingency planning that accounts for both operational and adversarial risks during major system failures.

FAQs

Q1. What is meant by Blue Screen Mayhem?

Blue Screen Mayhem is an informal phrase used to describe large-scale disruption caused when many systems simultaneously crash with the Blue Screen of Death (BSOD). The term became widely used after the global IT outage in July 2024, when a faulty update from CrowdStrike triggered BSODs on millions of Windows devices worldwide. The "mayhem" reflects the massive impact disrupting airlines, banks, hospitals, and businesses across the globe due to widespread system failures.

Q2. How did CrowdStrike's glitch become a security risk?

CrowdStrike's 2024 incident became a major security risk not because of a cyberattack, but due to a flawed update in its Falcon endpoint protection software that triggered widespread Windows Blue Screen of Death (BSOD) crashes. The outage caused massive operational disruption and financial losses, while also creating opportunities for attackers to spread fake fixes and malware during the chaos. A simple logic error in a routine update turned a trusted security tool into a single point of failure highlighting the critical risks of vendor dependency and insufficient update validation.

Q3. Why are BSOD incidents dangerous beyond downtime?

Beyond immediate downtime, Blue Screen of Death (BSOD) incidents are dangerous because they can cause data corruption or loss, signal deeper problems like malware infections or hardware failures, and trigger cascading operational outages across large organizations.

Q4. How can outages become a threat actor's playground?

Outages create a "playground" for attackers by causing chaos, distraction, and urgency. During these moments, security best practices are often overlooked, exposing new vulnerabilities and making organizations and users

more vulnerable to opportunistic attacks.
