CrowdStrike Outage Causes Significant Disruption & Poses Follow-on Social Engineering Threat

July 2024 • SFAR-2024-5

TLP:AMBER

Executive Summary

A widespread IT outage beginning around 1:00 AM Eastern on July 19, 2024 stemming from a defect found in a single CrowdStrike content update, has impacted a significant number of Windows hosts globally, including direct impacts to state, local, tribal, and territorial (SLTT) government entities.[1] In an official statement, CrowdStrike advised they had isolated the issue and deployed a fix.[2] While SLTTs work to maintain critical operations and restore access to Windows-hosted systems running CrowdStrike Falcon sensors, the Center for Internet Security (CIS) Cyber Threat Intelligence (CTI) team has already observed cyber threat actors (CTAs) exploiting the situation to tailor phishing lures and typosquatted[1] domains, posing as CrowdStrike support and legitimate CrowdStrike infrastructure. The CTI team will continue to monitor related threat context and actively disseminate observed typosquatting and phishing indicators of compromise (IOCs) through the MS-ISAC indicator sharing program and the Malicious Domain Blocking and Reporting (MDBR) service.[3]

Substantive Analysis

The MS-ISAC has observed significant disruptions to SLTT members' systems and expects these disruptions to persist while administrators work to effectively deploy CrowdStrike's fix. Thus far, reporting indicates that there are significant disruptions to airlines causing substantial travel delays, railways, healthcare, financial institutions, as well as several reports of 911 centers forced to deploy back up systems to receive emergency calls, along with additional reported impacts to other SLTT subsectors.[4]

The CTI team has identified CTAs standing up infrastructure, such as recently created domains imitating CrowdStrike, that is likely designed for social engineering to take advantage of the urgency and uncertainty of the situation. The newly issued phishing lures and typosquatted domains the CTI team observed follow a common theme of posing as authorized CrowdStrike infrastructure and support. The CTI team assesses that these are likely domains not associated with CrowdStrike and they could be used currently or in the future for malicious purposes. The domains were proactively added to the MDBR service and the MS-ISAC SOC notified several MDBR-enrolled members who forwarded DNS queries to one or more of thee domains. In the past, the CTI team has observed CTAs leveraging chaotic situations and a heightened sense of urgency to socially engineer unsuspecting users into visiting malicious websites and responding to phishing emails that mimic legitimate entities.[5, 6]

Indicators of Compromise

[1] Typosquatting involves the purchase and registration of malicious domains visually similar to an existing domain intended to deceive unsuspecting users into visiting the page. Typosquatters often target high-traffic and/or sensitive websites to exploit the greatest number of users or to gain unauthorized access to restricted information.

The following IOCs include likely malicious domains CIS CTI analysts identified posing as legitimate CrowdStrike infrastructure:

Likely Typosquatted CrowdStrike Domains

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

MITRE ATT&CK Patterns Observed[7]

- T1566 - Phishing
- T1583.001 - Acquire Infrastructure: Domains

Analytic Confidence

Analytic confidence in this assessment is moderate to high, as the CTI team continues to receive updated information on the developing incident. Source reliability is high with minimal conflict among sources. Time was several hours to research this topic and the topic itself was not overly complex. The analyst used a timeline and brainstorming structured method in this analysis, and the analyst worked as part of a small group to complete this product.

For questions or comments, please contact us at intel@cisecurity.org. For further information on our analytic tradecraft, please refer to our blog post outlining these standards.

Recommendations

SLTTs should refer to Crowdstrike's official statement and any ongoing communications.

Additionally, organizations should monitor CTI-published indicators of compromise, as the team continues to identify and share timely and relevant IOCs through STIX/TAXII and the MDBR platform.

SLTT members should be mindful that CTAs are likely to continue to attempt to exploit this incident with social engineering lures. The CTI team advises administrators to advise their organizations to remain vigilant in response to unsolicited email and exercise extra caution when reviewing CrowdStrike support materials.

For further guidance on mitigating the threat of social engineering tactics, refer to:

- Phishing Guidance: Stopping the Attack Cycle at Phase One

References

1. https://apnews.com/live/internet-global-outage-crowdstrike-microsoft-downtime
2. https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/
3. https://www.cisecurity.org/ms-isac/services/mdbr
4. https://apnews.com/live/internet-global-outage-crowdstrike-microsoft-downtime#00000190-caf9-d1bd-abfb-fef9e5a70000
5. https://www.cpomagazine.com/cyber-security/uk-water-supplier-suffered-a-clop-ransomware-attack-during-major-drought-victim-initially-misidentified-as-uks-largest-water-utility/
6. https://thehackernews.com/2020/03/covid-19-coronavirus-hacker-malware.html
7. https://attack.mitre.org/

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061
SOC@cisecurity.org - 1-866-787-4722

Supported via cooperative agreement No. 23CISMSI00003-01-01 - 09/29/2025 awarded through the Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (U.S. DHS). The analysis, findings, and conclusions or recommendations expressed in this document are those of the MS- and EI-ISAC.