AL2024_22 Fake CrowdStrike Fixes Push Malware and Data Wipers (23rd July 2024)

Summary

Threat actors are exploiting the recent disruption caused by CrowdStrike's faulty update to target companies with data wipers and remote access tools. As businesses seek to resolve issues with affected Windows hosts, phishing emails have been observed trying to capitalize on the situation.

Details

Researchers and government agencies have reported an increase in phishing attempts following CrowdStrike's glitchy update that disrupted millions of Windows hosts. These phishing emails impersonate CrowdStrike, offering fake fixes and updates that install malware instead.

In response to the incident, CrowdStrike is assisting affected customers and advises verifying communications through official channels to avoid falling prey to these malicious campaigns. The U.K. National Cyber Security Center (NCSC) has also noted a rise in phishing messages linked to this outage.

Cybersecurity researcher g0njxa identified a campaign targeting BBVA bank customers, promoting a fake CrowdStrike Hotfix that installs the Remcos RAT. The malicious update was distributed via a phishing site mimicking a BBVA Intranet portal.

Automated malware analysis platform AnyRun reported similar campaigns, where fake CrowdStrike updates delivered HijackLoader and Remcos RAT, and a data wiper that overwrites files and reports the activity over Telegram. The pro-Iranian hacktivist group Handala claimed responsibility for distributing the data wiper to Israeli companies.

These phishing emails, sent from the domain 'crowdstrike.com.vc,' contain a PDF with instructions and a link to download a malicious ZIP archive. This archive includes an executable named 'Crowdstrike.exe' that, once executed, launches the data wiper to destroy data on the device.

Indicators of Compromise (IoCs)

Organizations should monitor for the following indicators of compromise:

- Phishing emails claiming to be from CrowdStrike with links to updates or fixes.
- Unexpected behavior or performance issues on systems after installing supposed updates.
- Unusual system activity related to remote access tools and data wiping.

Remediation

To mitigate the risk posed by these fake updates, organizations can:

- Verify communications with CrowdStrike through official channels.
- Educate employees on the dangers of phishing emails and the importance of verifying update sources.
- Implement comprehensive security solutions to detect and block malicious activities.
- Regularly update anti-malware software and configure it to detect and prevent remote access tools and data wipers.
- Monitor network traffic for unusual patterns that may indicate malware activity.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- BleepingComputer. (2024, July 21). Fake CrowdStrike fixes target companies with malware, data wipers. Retrieved from https://www.bleepingcomputer.com/news/security/fake-crowdstrike-fixes-target-companies-with-malware-data-wipers/
- ITPro. (2024, July 22). Hackers are creating fake CrowdStrike recovery resources to trick businesses into loading malware onto their network. Retrieved from https://www.msspalert.com/brief/malicious-payloads-distributed-via-fraudulent-crowdstrike-fixes