ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about potential threats that could arise due to the major Windows system outage caused by Crowdstrike's update.

Summary

Earlier today, 19th July 2024, Crowdstrike pushed out an update to their Falcon EDR solution that caused Windows systems to crash with the well known Blue Screen Of Death (BSOD). With the ongoing outage of Windows systems, maintaining awareness of surrounding threats is important for an organization's security posture.

Threat actors have been quick to start exploiting this global incident, be it by targeting organizations directly affected by this outage or spreading misinformation about it. There are already signs of malicious domains being registered in relation to Crowdstrike Falcon in order to spread misinformation.

This event also highlights the need for the pre and post stages of crisis management. Pre-Crisis preparations such as conducting crisis simulations through tabletop exercises will allow teams to be prepared for when such incidents come about. Likewise, Post-Crisis preparations such as lessons learned discussions will allow organizations to identify their shortcomings during such crises and rectify them.

Alongside crisis management, threat hunting exercises will also prove useful in the coming weeks in order to assess any possible impact that might arise from this incident. These exercises will allow the security teams to determine whether any exploitation of their systems was successfully attempted while attention was given to remediating the outages.

Recommendations

Recommendation #1: Restrict Information Sourcing To Official Sources

ORNA recommends that all readers carefully vet their sources when investigating incidents of this magnitude. For the current Crowdstrike Falcon issue we recommend reading through the official Crowdstrike statement[1].

Recommendation #2: Apply The Official Fix

ORNA recommends that organizations affected by this outage only follow the official guide [1]. Due to the spread of misinformation, sticking to the official guides is important in order to avoid leaving systems vulnerable or compromised.

Recommendation #3: Conduct Threat Hunting Exercises When Possible

ORNA recommends that organizations conduct thorough threat hunting exercises, where possible, in order to assess whether any threat has successfully compromised them.

Recommendation #4: Conduct Regular Crisis Simulation Exercises

ORNA **strongly recommends** that all organizations regularly carry out exercises testing their incident response plans in the form of cyber crisis simulation exercises..

References

1. https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.