Lab 3: CrowdStrike Case Study

CrowdStrike Case Study Report

Anastasiia Tiurina

School of Innovation, Design and Technology Whitireia

IT8x16 Network Design and Management

Supervisor: Dr. Bryce Antony

August 8, 2024

Overview

On 19th of July many companies found that their working machines as well as devices, running on Windows, were down with the BSOD error. The work of airports and hospitals across the world was disrupted due to the same error. The cause of the global outage was a scheduled update of Falcon Sensor software created by CrowdStrike company. Before the CrowdStrike managed to roll back the faulty update the damage has already been done.

What was the function of the CrowdStrike Application effected?

Falcon is the application that received a buggy update which disabled millions machines across the world. According to the official application page it provides an endpoint protection.

What was the business objective / goal that the effected CrowdStrike application addressed?

The goal of the Falcon software is to protect the network of an organization from cyberattacks and malware. It is an implementation of Endpoint Detection and Response (EDR) cybersecurity technology. Endpoint in this context is a device within the network. The activity on an endpoint is constantly monitored by the installed agent – in this case it is a Falcon Sensor, - and, according to the official site of CrowdStrike, the collected data is sent to the monitoring system in the cloud where it is analysed.

So, the business goal of the Falcon is to prevent security breaches and ensure that the company or business that uses Falcon platform follows the CIA triad concept. Such precautions can avoid cases like Latitude breach in Australia.

How did this 'cause' the outage?

Early release and badly tested patch.

Technology-wise, CrowdStrike published a report with the details with Falcon-specific terminology.

Rapid Response Content (RRC) is threat intelligence and it is stored in the cloud.

Falcon Sensor has:

1. Sensor Content: contains rules for threat detection
2. Sensor Detection Engine: acts according to rules and data from RRC
3. Content Interpreter: receives RRC and interprets it through its regex engine and then it goes to Content Validator.

RRC is sent to Interpreter through Channel File that has Template Type.

Before the update Interpreter was accepting 20 parameters. During the update they added one more Template, adding one more parameter. However, there was an error in regex engine that did not parse the parameter correctly. This caused the discrepancy in amount of parameters going through

Channel File and number of parameters the Interpreter reads from. Hence, the Interpreter addressed 21st element in an array of size 20, thus, causing element out-of-bound error.

Why it caused BSOD:

The Falcon Sensor works on the level of kernel drivers (Weston, 2024). And errors in kernel-mode drivers cause crash of operating system (Microsoft, 2023).

The program (third-party software) resides in the critical path of the system. Therefore, if it fails the entire system fails.

As a Network Infrastructure Manager, what could you have changed in the Network Design to mitigate the effects of the outage.

Point of view: CrowdStrike

Adding machines or VMs that can be used for testing of the patch installation.

In case of disaster recovery testing is the most important. And in their Root Cause Analysis CrowdStrike claimed that they tested the fix for the buggy patch and enhanced their testing procedures.

Point of view: Business that uses Falcon

The strategy and disaster recovery plans depends on business goal of the company and understanding the crucial parts.

What protocols / procedures / practices could have been added to enhance resilience in this case study.

Point of view: CrowdStrike

Enhance testing practices.

Point of view: Business that uses Falcon

In this particular case turning the auto-updates off would have helped. However, updating the installed software is important for security reasons. Having emergency/spare machines. Creating restoration images or VM backups.

References:

Microsoft. (2023, December 16). *User Mode and Kernel Mode—Windows drivers*. https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode

Weston, D. (2024, July 27). *Windows Security best practices for integrating and managing security tools*. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2024/07/27/windows-security-best-practices-for-integrating-and-managing-security-tools/