CROWDSTRIKE AND THE BLUE SCREEN OF DEATH

Introduction

On July 19, 2024 , millions of Windows Systems failed to boot and showed the Blue Screen of Death (BSOD). This was at the time Considered as one of the largest IT outage in history (more than 8.5 million Systems) which was triggered by a faulty software update from security vendor (CrowdStrike) of Microsoft.

CrowdStrike

Crowdstrike is a cybersecurity company that provides cloud-based protection for devices or endpoints (laptops, servers, mobile devices). One of their widely used Software is the Falcon Platform (one which caused the outage) that stops breaches by detecting and preventing threats like Malware, ransomware, and exploits, offering Endpoint Detection & Response (EDR), threat intelligence, identity protection and managed services.

Falcon Platform

Falcon is what is known as “Endpoint Detection And Response” (EDR) software. Its Job is to Monitor what is happening on the computers on which it is installed , looking for signs of unusual activity (such as malware). When it detects something fishy, it helps to lock down the threat.

To do this Falcon needs privileged access. This means Falcon is what we call privileged Software. To detect signs of attack, Falcon has to monitor computers in a lot of detail so it has access to lot of internal systems. This includes what communications computers are sending over the internet as well as what programs are running, what files are being opened, and much more.

To do all of this Falcon has been installed at kernel level of Windows. Falcon hooks into the Microsoft OS as a windows kernel process. The process has high privileges, giving Falcon the ability to monitor operations in real time across the OS.

How it Works?

1. **The Kernel Level:** It operates at the "Kernel" level—the very core of the operating system. This gives it a view of everything happening, from keyboard strokes to network connections, allowing it to stop hackers before they can hide.

2. **Behavioural Analysis:** Instead of just looking for known "bad files," it looks for "bad behaviour." For example, if a spreadsheet suddenly starts trying to download encrypted files from the internet, the sensor identifies this as suspicious and kills the process.

What Caused the Outage?

On July 19th, 2024 the Systems running on Windows started showing Blue Screen of Death (BSOD). The Outage was not a Microsoft Windows flaw Directly, but rather a flaw in crowdstrike Falcon that triggered the issue.

As we know falcon needs privilege access, so it is hooked on to Windows OS as a kernel process. There was a logic flaw in Falcon sensor version 7.11 and above, causing it to Crash. Due to crowd-strike falcon's tight integration into the Microsoft Windows kernel, it resulted in a Windows system crash.

The Falcon Platform sensor in regularly updated frequently to provide users with mitigation and threat protection. The flawed update was contained in a file that crowdstrike refers to as "Channel Files", which specifically provide configuration updates for behavioural protections. Channel file 291 is an update that was supposed to help improve how falcon evaluate named pipe (Inter process Communication Mechanism) execution on Microsoft Windows.

With Channel file 291, crowdstrike inadvertently introduced a logic error, causing the Falcon sensor to crash and due to its tight integration to Windows this resuled in Windows Systems showing the Blue Screen of Death (BSOD) screen.

What Happened?

The Falcon uses on-sensor AI and ML Models to protect customer systems by identifying and remediating the latest advanced threats. To do this, the sensor has to be up-to-date and are strengthened with learnings fro the latest threat data from the sensor and human intelligence from the threat detection team. Each sensor has its own local graph store which store the data that tells what kind of meta-data , unusual behaviour of a file/software is considered malicious and should be taken care of. This process of correlating context from its local graph store with live system activity into behaviours and indicators of attack (IOA) is called as refinement.

CROWDSTRIKE AND THE BLUE SCREEN OF DEATH

This refinement process includes a Sensor Detection Engine combining built -in Sensor Content with Rapid Response Content (containing data about possible indicators of a threat) delivered from Cloud.

These Rapid Response Content is delivered through Channel Files and interpreted by the Sensor's Content Interpreter. Each Rapid response Content Channel file is associated with Template Type (structure of the data) built into a sensor release. This Template Type provides the Content Interpreter with activity data and graph context to be matched against the Rapid Response Content.

In the latest release ,the new Inter Process Communication (IPC) Template Type was developed. The new IPC Template type defined 21 input parameter fields, but the integration code that invoked the Content Interpreter with Channel File 291's Template Instance supplied only 20 input values to match against. This "parameter mismatch" caused the Sensor Interpreter to attempt to read memory it wasn't allowed to access which is known as an out-of-bounds memory read.

Because Falcon Operates at the Kernel level, this error caused Windows to immediately crash to protext itself, resulting in the Blue Screen of Death (BSOD).

Why It Happened?

As the Rapid Response Content is viewed as "data configuration" rather than "executable code," it didn't undergo the same rigorous stress testing as the core Falcon Sensor software.

Reasons:

1. Lack of Negative Testing: Most testing at the time was "positive testing" -checking if the update blocked the threats it was supposed to block. They did not perform enough Negative Testing, which involves intentionally feeding the software with "garbage" data to see if it crashes.

2. Bypassing the "Canary" deployment: As these Files were considered data, they were often pushed to all customers at once to ensure everyone was protected from new threats simultaneously. If they had tested it on just 1% of computers first, they would have seen the crashes immediately and stopped the rollout before it hit the other 99%.

3. Flawed Validator: Crowdstrike uses a tool called Content Validator to check updates before they were sent out. The Validator had a bug. It checked the update and essentially cleared it for

deployment, even though the update contained 21 parameters and sensor could only handle 20. Instead of testing how the update actually performed inside real Windows Kernel , they were testing it on their own Software platform.

How Was It Solved?

Crowdstrike:

within an hour of the faulty update's release, Crowdstrike identified the error and "reverted" file on their servers. So any computer that was off or not connected to the internet during that, windows never downloaded the "bad" file and remained safe.

They also enabled a "cloud-based fix" where, if a machine could stay online for a few seconds before crashing, the Falcon sensor would try to "quarantine" its own bad file and replace it

Microsoft:

Microsoft released a special USB recovery Tool, which can be plug into bricked laptop, and the tool would automatically find and delete the bad file.

Manual Workaround:

1. Boot into Safe Mode
2. Navigate to the specific system folder (C:\Windows\System32\drivers\Crowdstrike).
3. Locate and delete the specific File: (C-00000291*.sys)
4. Restart the Computer