Crowdstrike Report

Christian J. Rudder,

November 2024

Contents

This page is left intentionally blank.

1.1 Channel File 291 Incident

Friday July 19, 2024, CrowdStrike, a leading cybersecurity firm, released an update to its Falcon Sensor software designed for Windows-based systems. The update, intending to enhance threat detection single-handedly, disrupted the global IT infrastructure, causing widespread system crashes across various industries (e.g., airlines, healthcare, and banking) [6].

The outage costed fortune **500 companies approximately $5.4 billion** in damages, after an estimated **8.5 million devices** were struck by the blue screen of death (BSoD) [15][9].

1.2 Context and Background

CrowdStrike's Founder and CEO George Kurtz, addressed the public on live TV, stating "That we're deeply sorry for the impact we've caused" [14]. Though this isn't the first time George Kurtz has been caught in the crossfire of a cybersecurity incident. In 2019, George Kurts the customer-facing Field Chief Technology Officer at McAfee, released a faulty update. The update, mistakenly identified a critical Windows system file (svchost.exe) as malware, causing the system to endlessly loop [16].

In a blog posted by CrowdSTrike "as of 8:00 p.m. EDT on July 29, 2024, 99% of Windows sensors were back online" [5]. The incident was said to occur due to a bug which expected 20 input fields instead of 21, causing the software to crash. Channel File 291 was identified the culprit and was removed from the software [5].

1.3 Modern Endpoint Security

First we will break down what exactly the Falcon Sensor is. The Falcon Sensor claims to be a lightweight agent installed on endpoint devices to monitor and record system activity. Ensuring **endpoints** means ensuring devices that connect to a network, such as laptops, desktops, and mobile devices. **Endpoint security** is the process of securing the various points at which a device connects to a network. 90% of successful breaches and 70% of data breaches originate at endpoint, costing companies millions [7].

Since many large scale companies have moved to the cloud, and many working from home, ever more devices are connecting to sensitive data. This means many endpoint solutions constantly monitor and record system activity to detect and prevent threats. This in itself utilizes cloud-based systems to access threat intelligence, providing autonomous real-time protection [3]

Many original anti-viruses signature based, protecting endpoints on a device by scanning for known malware. This relied on a database of known malware signatures. CrowdStrike and many others have opted to use **next-gen anti-virus (NGAV)** machine learning Technology, to aid in detecting newer types of malware that are often fileless, by monitoring system memory [8].

1.4 EPP & EDR Anti-virus Solutions

Endpoint Protection Platforms (EPP) like CrowdStrike may include the following features as defined by IBM [7]:

- **Web control and content filtering**: protects against malicious code in websites and user downloaded content. While providing a whitelist of approved websites.
- **Data classification and data loss prevention (DLP)**: identifies and classifies sensitive data, preventing unauthorized access and data loss.
- **Firewall**: monitors and controls incoming and outgoing network traffic based on configured security rules.
- **Email Gateway**: scans incoming email attachments and links for malicious content.
- **Application control**: restricts the programs that users can run on their devices.

CrowdStrike's **Endpoint Detection and Response (EDR)** solution Falcon Sensor, part of the Falcon Platform, is at the root of the issue. EDRs are a class of security tools that go beyond known threats, to monitor files entering and applications running on a system. These **Correlate Indicators of Compromise (IoC)** systems, aggregate data from various sources—network traffic, unusual user behavior, inconsistent permissions, system configuration changes, unverified software or domains, repetitive file access, and more [11].

These systems aren't just designed to detect threats, but respond to them while an attack is in progress. This incurs IOCs many log based solutions such as **extended detection and response (XDR)**, and **security information and event management (SIEM)** systems to mitigate and isolate threats, going as far as to shut down a system if necessary. These systems typically rely on AI to establish a baseline of normal activity and detect deviations from it [11].

1.5 CrowdStrike Falcon Sensor Distinctions

The immediate reason why CrowdStrike's Falcon Sensor update caused such a widespread outage was due to the software living on at kernel level. These differ from traditional user-mode applications that crash in isolation. Kernel-level applications are more privileged living at the heart of the operating system—if it crashes, the whole system crashes. This process is known as **kernel panic**, which stops the system from potentially corrupting beyond repair [1].

CrowdStrike notes three main kernel-level component features that it complies with from the Microsoft's anti-virus kernel APIs [8]:

- **Kernel Patch Protection (KPP)**: also known as **PatchGuard**, prevents third-party software from modifying the Windows kernel. Available on 64-bit (x64) Window systems, but by-passable on 32-bit (x86) systems, CrowdStrike opts to never patch the kernel. Other anti-virus choose this route, which can lead to system instability if not done correctly [4].
- **Kernel-Mode Code Signing (KMCS)**: that CrowdStrike instead opts to use Microsoft's own driver signing program, to verify its activity at the kernel level. This is a requirement for 64-bit Windows systems, to prevent unsigned drivers from loading [12].

- **Object Callbacks:** a feature that allows CrowdStrike to subscribe to various kernel events, such as file creation, registry access, and network activity. Instead of **kernel hooking**, which intercepts system calls [10][13].

CrowdStrike further justifies its kernel presence to protect against for **Early Boot Protection (EBP)** and which Microsoft supports with its **Early Launch Anti-Malware (ELAM)** driver [8]. This protects against rootkits, which are malware that can hide from the operating system, by loading before the operating system itself. Having this protection in place, stops attackers from sticking USBs into airport kiosks or hotel computers [2].

1.6 Faulty Code and Production Updates:

Bibliography

[1] Rahul Awati. Kernel panic. https://www.techtarget.com/searchdatacenter/definition/kernel-panic. Accessed: November 30, 2024.

[2] Kurt Baker. Rootkit malware. https://www.crowdstrike.com/en-us/cybersecurity-101/malware/rootkits/, November 2023. Accessed: November 30, 2024.

[3] Cisco. What is endpoint security? https://www.cisco.com/c/en/us/products/security/endpoint-security/index.html. Accessed: November 30, 2024.

[4] Wikipedia contributors. Kernel patch protection. https://en.wikipedia.org/wiki/Kernel_Patch_Protection. Accessed: November 30, 2024.

[5] CrowdStrike. Channel file 291 incident - remediation and guidance hub. https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/, August 2024. Page last updated 2024-08-06 2119 UTC.

[6] CrowdStrike. Technical details: Falcon content update for windows hosts, 2024. Executive Viewpoint, published on July 20, 2024.

[7] IBM. What is endpoint security? https://www.ibm.com/topics/endpoint-security. Accessed: November 30, 2024.

[8] Alex Ionescu, Milos Petrbok, Martin O'Brien, and Johnny Shaw. Tech analysis: Crowdstrike's kernel access and security architecture. *CrowdStrike Blog*, August 2024. Executive Viewpoint, Accessed: November 30, 2024.

[9] Sean Michael Kerner. Crowdstrike outage explained: What caused it and what's next. *TechTarget*, October 2024.

[10] Microsoft. Obregistercallbacks function (wdm.h). https://learn.microsoft.com/en-us/windows-hardware/drivers/ddi/wdm/nf-wdm-obregistercallbacks. Accessed: November 30, 2024.

[11] Microsoft. What are indicators of compromise (iocs)? https://www.microsoft.com/en-us/security/business/security-101/what-are-indicators-of-compromise-ioc. Accessed: November 30, 2024.

[12] Microsoft. Kernel-mode code signing requirements. https://learn.microsoft.com/en-us/windows-hardware/drivers/install/kernel-mode-code-signing-requirements--windows-vista-and-later-, June 2022. 5 contributors, Accessed: November 30, 2024.

[13] ReasonLabs. What is kernel-level hooking? https://cyberpedia.reasonlabs.com/EN/kernel-level%20hooking.html. Accessed: November 30, 2024.

[14] Mia Sato. Crowdstrike ceo was working for mcafee in 2010 when there was a global tech outage too. *The Verge*, July 2024. Posted at 9:33 AM EDT, 9 Comments, 9 New.

[15] Joe Tidy. Crowdstrike it outage affected 8.5 million windows devices, microsoft says. *BBC News*, July 2024.

[16] Adrian Volenik. Crowdstrike ceo was working for mcafee in 2010 when there was a global tech outage too. *The Verge*, July 2024. 4 min read.