CrowdStrike Channel File 291 Incident Analysis

Christian J. Rudder, Ivan Khramtchenko, Christopher Min, Ethan Machleder

November 2024

Contents

Contents **1**

1 Crowdstrike Report **3**
1.1 Channel File 291 Incident . . . 3
1.2 Context and Background . . . 3
1.3 Modern Endpoint Security . . . 3
1.4 EPP & EDR Anti-virus Solutions . . . 4
1.5 CrowdStrike Falcon Sensor Distinctions . . . 4
1.6 Faulty Code and Production Updates: . . . 5
1.7 CrowdStrike Incident Report . . . 5
1.8 Windows Kernel Crash Dump Analysis . . . 7
1.9 Legal Issues Raised by CrowdStrike Outage . . . 7
1.10 Ethical Issues Raised by CrowdStrike Outage . . . 9
1.11 Link to Poster . . . 10

Bibliography **11**

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) [10].

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) [29][14].

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" [27]. Though this isn't the first time. In 2010, George Kurts was the Executive Vice President and Chief Technology Officer at McAfee when they released a faulty update, causing a BSoD as it mistakenly identified a critical Windows system file (svchost.exe) as malware [31].

CrowdSTrike announced at "8:00 p.m. EDT on July 29, 2024, 99% of Windows sensors were back online" [8]. The incident occurred due to a file misread, causing systems to crash. The culprit identified—Channel File 291—was removed promptly [8].

1.3 Modern Endpoint Security

CrowdStrike, offers endpoint security through their Falcon solution. Falcon, a lightweight agent securing **endpoints**, meaning, it secures devices that connect to a network, formally known as **endpoint security**. 90% of successful breaches and 70% of data breaches originate at an endpoint, costing millions [12]. Large scale companies are moving to the cloud while employees work from home, ever more devices are connecting to sensitive data. Endpoint solutions have to constantly monitor and record system activity to detect and prevent threats. Endpoint security delivers threat intelligence from the cloud, providing autonomous real-time protection [3]

Many original anti-viruses signature based, protecting endpoints on a device by scanning for known malware—**Indicators of Attack (IOA)**. 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, detecting newer filess and unknown IOAs, by sniffing memory [13]. This is known as **Endpoint Detection and Response (EDR)**.

1.4 EPP & EDR Anti-virus Solutions

Endpoint Protection Platforms (EPP) like CrowdStrike may include the following features [12]:

- **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.

Effectively, 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 [18].

These respond to attacks in in progress. This incurs IOCs and 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 approaches typically rely on AI to establish a baseline of normal activity and detect deviations from it [18].

1.5 CrowdStrike Falcon Sensor Distinctions

The reason why CrowdStrike's Falcon Sensor update caused such a widespread outage was due to the software lived at kernel-level. These differ from traditional user-mode applications that crash in isolation (e.g., skype). Kernel-level applications carry crucial privileges at such layer—if it crashes, the whole system crashes (**kernel panic**). If not, the system could potentially corrupt beyond repair [1].

CrowdStrike notes three main kernel-level component features that it complies with from the Microsoft's kernel APIs [13]:

- **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)**: CrowdStrike complies with Microsoft's KMCS requirements, which ensures that all kernel-mode code obtains a **Extended Validation (EV) Code Signing Certificate** from a trusted **Certificate Authority (CA)** [19][25].
- **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 [17].

CrowdStrike further justifies its kernel presence for **Early Boot Protection (EBP)**, which Microsoft supports with its **Early Launch Anti-Malware (ELAM)** services [13]. This protects against rootkits, malware which hides by loading before the operating system itself. This stops attack via USBs [2].

1.6 Faulty Code and Production Updates:

Despite CrowdStrike Falcon Sensor passing **Windows Hardware Compatibility Program (WHCP)** certifications, and validations through **Windows Hardware Lab Kit (HLK)** testing, the update still slipped through [20]. However, anti-virus software only needs to pass the WHCP and HLK tests once. They only certify that the driver running on the system is stable. Once the driver is installed, CrowdStrike can push updates—**without re-certification**—in a cloud-based process they call **Rapid Response Content (RRC)** [9].

Integrity relies on CrowdStrike's internal deploy and testing pipelines. Typically software companies employ **Continuous Integration/Continuous Deployment (CI/CD)** pipelines to catch issues. CI/CD pipelines are characterized by multiple rounds of manual written tests, peer reviewed code, and automated stress testing to ensure the software compiles safely before deployment [11]. These tests comprise of **unit tests**, **integration tests**, and **end-to-end (E2E) tests** to ensure the software is functioning as expected. Unit tests test individual components of the software, integration tests test how the components interact, and E2E, running the application in production-like environments (e.g., test and development environments before production) in a suite of integration tests to ensure stability. CrowdStrike lacked the CI/CD security to catch Channel File 291, a bug that effectively threw an out-of-bounds error, which would have been caught immediately in E2E tests.

1.7 CrowdStrike Incident Report

Before jumping into CrowdStrike's incident analysis, we must first understand the technical terms used in the analysis [9]:

1. **Falcon OverWatch® and Falcon Complete™**: OverWatch is a 24/7 managed threat hunting service led by human intelligence. Complete is a **managed detection and response (MDR)** service, which is a suite of tools and services including OverWatch, to detect and remediate threats [5][6][7].

2. **Security Telemetry & Graph Store**: Telemetry is the aggregation of data from various sources (e.g., endpoints, servers, network devices) [24]. These analytics are are stored locally on the Falcon Sensor's sensors in a graph database. Graph databases store information in nodes and edges to represent the relationship between data points [22].

Falcon Sensor's interprets relationships in flowing memory to detect possible IOAs.

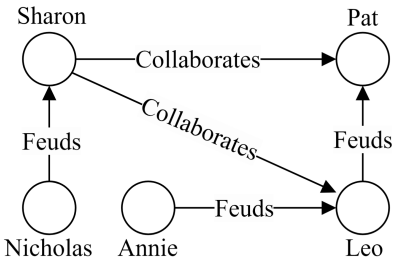

Figure 1.1: Graph Example Depicting Relationships Between Co-workers

3. **Template Types**: Template types push telemetry data to a regular-expression (RegEx) engine Content Interpreter. Template types outline predefined schemas of security criteria to evaluate. **Template Instances** are live configurations, defining parameters, thresholds, and conditions to trigger alerts.

4. **Channel Files**: Each Falcon sensor defines a channel file, which is configured with a template type. RRCs then push threat intelligence to channel files. Template instances then compare the security telemetry to determine IOAs.

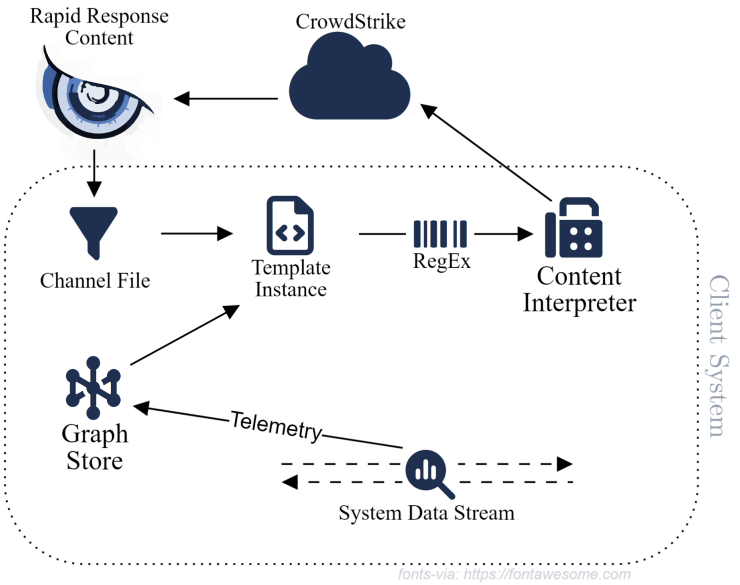

Figure 1.2: RRC & Telemetry Graph Store Data Aggregation for IOA Content Interpreter.

February 2024, CrowdStrike released sensor version 7.11, introducing a new template type. The template type targeted a new IOA vector relating to **Windows Interprocess Communication (IPC)** mechanisms—notably **Named Pipes**. Named pipes facilitate communication between processes on the same or different machines. The exploit enabled an adversary to execute code and impersonation leading to privilege escalation [26].

This release included a new IPC template type. RRC delivers IPC template instances to **Channel File 291**. This new template type defined 21 input fields, while the Content Interpreter still expected 20. This evaded detection as the Content Interpreter identified files based on a wildcard matching pattern.

Listing 1.1: Wildcard Pattern Matching Example

```
*: Matches any sequence
?: Matches any single character
Input: txt = ``abcdef'', pattern = ``a?c*''
Output: true
Reason: `?' matches with `b' and `*' matches with ``def''.
```

(As CrowdStrike has mentioned their use of RegEx before, it is likely that the Content Interpreter used a RegEx pattern to match fields.)

On July 19, 2024, the RRC push two new IPC template instances to channel files—one of which dropped wildcard matching. This required the Content Interpreter to check the 21st field from Channel File 291. However, the Content Interpreter expected 20 fields, causing an out-of-bounds error, crashing the Falcon Sensor. This error caused the BSoD that Friday afternoon affecting 8.5 million devices.

1.8 Windows Kernel Crash Dump Analysis

David Weston, Vice President, Enterprise and OS Security at Microsoft, posted in an incident the kernel crash dump from Channel File 291 [32]. The Microsoft team's **Windows Error Reporting (WER)** kernel crash dumps analysis involved **WinDBG Kernel Debugger**, and several other extensions.

Line 23 (modified to fit page) shows the full file path of Channel File 291, confirming the cause of the crash. The dump shows the crash is due to an out-of-bounds error. While the crash dump is not publicly available, the Microsoft team confirms the out-of-bounds error in the given crash dump. Microsoft quick to confirm Crowdstrike's negligence, as many began pointing fingers at Microsoft.

Despite the fact that this is not Kurtz's first significant security mishap, it would be unfair to place responsibility squarely on his shoulders: each Windows sensor release is certified through extensive testing in Microsoft's HLK and WHQL. Microsoft ought to enforce integrity every step of the way, as who's to say a company switches out its internals after passing its drivers. Nonetheless, CrowdStrike's lack of comprehensive E2E testing introduced a critical error. Such an erroneous mistake raising substantial concerns. In their incident report, they duly noted under the "Findings and Mitigations" section that CrowdStrike need "expand [validation] to include testing within the Content Interpreter" [9]. Even though customers managed to recover from the incident, CrowdStrike faced severe legal repercussions.

1.9 Legal Issues Raised by CrowdStrike Outage

These critical lapses in CrowdStrike's CI/CD practices has led to significant legal action, totalling a $500 million dollar lawsuit filling from Delta Airlines. The lawsuit alleges that CrowdStrike's negligence in testing and deployment erupted the outage. However, the likely hood CrowdStrike walks free seem high, as Delta's lacks the traditional evidence to support such claims in court.

```
!ca ffffde8a870a8290

ControlArea  @ ffffde8a870a8290
  Segment      ffff880ce0689c10  Flink      ffffde8a87267718  Blink        ffffde8a870a7d98
  Section Ref                 0  Pfn Ref                   b  Mapped Views                0
  User Ref                    0  WaitForDel                0  Flush Count                 0
  File Object  ffffde8a879b29a0  ModWriteCount             0  System Views                0
  WritableRefs                0  PartitionId                0
  Flags (8008080) File WasPurged OnUnusedList

      \Windows\System32\drivers\CrowdStrike\C-00000291-00000000-00000032.sys

1: kd> !ntfskd.ccb ffff880ce06f6970
!ntfskd.ccb ffff880ce06f6970

   Ccb: ffff880c`e06f6970
 Flags: 00008003 Cleanup OpenAsFile IgnoreCase
Flags2: 00000841 OpenComplete AccessAffectsOplocks SegmentObjectReferenced
  Type: UserFileOpen
FileObj: ffffde8a879b29a0

(018)  ffff880c`db937370  FullFileName [\Windows\System32\drivers\CrowdStrike\C-00000291-00000000-00000032.sys]
(020) 000000000000004C  LastFileNameOffset
(022) 0000000000000000  EaModificationCount
(024) 0000000000000000  NextEaOffset
(048) FFFF880CE06F69F8  Lcb
(058) 0000000000000002  TypeOfOpen
```

Figure 1.3: Channel File 291 Incident Analysis

Lawyer Ramzy Ladah stated, "It's one thing to claim faulty software caused an outage, he says, but another to prove CrowdStrike didn't take adequate precautions on testing or monitoring" [16].

On top to Delta's lawsuit, CrowdStrike faces a stadium of ready legal repercussions the 8.5 million devices that were affected by the outage. Moreover, it is striking that in the light of such a large scale incident, the government has yet to bat an eye. In contrast, Snowflake, an AI cloud-based data company, was subject to an investigation by the SEC for its cyber breach that posed the threat of data leakage. [15] This raises the question of why CrowdStrike has not faced any legal repercussions from the government despite its severity of the outage. This could be due to the fact that Snowflake had issues regarding the mismanagement of customer data in contrast to CrowdStrike's incident while damaging, did not pose a threat to the data of its customers.

Even if the classification of user data alludes common legal action, CEO George Kurtz McAfee fiasco in conjuntion with this event should raise concern. Considering the frequency of negligent vulnerabilities, there must be an industry/government standard that companies should adhere to. While some frameworks, such as ISO 27001, exist to guide organizations in securing their information systems, there is no universally mandated standard specifically addressing the testing, deployment, and monitoring practices in CI/CD pipelines. This lack of regulation allows companies to cut corners around the thorough testing required to ensure security and stability. It is vital that the United States adheres to a standard, such as the EU's NIS2 Directive that requires companies to meet minimum benchmarks. Some of these benchmarks include rigorous pre-deployment testing and third-party audits. [23] Initiatives like this is what keeps companies in the EU above standard, and until now there have not been any publicly reported cases of companies facing fines under the NIS2 Directive. Considering this, the United States must follow suit such that we can prevent

incidents like CrowdStrike's outage from happening in the future. Aside from the legal aspects of CrowdStrike, there are also various ethical issues that arose from the outage to consider.

1.10 Ethical Issues Raised by CrowdStrike Outage

The scale of the CrowdStrike outage is only matched by the outrageousness of the mistake. Public opinion is divided on how to feel about the issue. Some consumers wonder how a giant corporation could have let such a mistake occur, while others take comfort in the fact that it was only a mistake that could be fixed and not a deliberate attack that could have had more devastating consequences. Ethical questions have arisen as a result.

CrowdStrike provides 25 percent of all enterprise endpoint solutions and has both immense power and responsibility in the cybersecurity space. Following the outage, on September 24th CrowdStrike's Senior VP of Counter Adversary Operations, Adam Meyers, was called to testify in front of the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection. The one-and-a-half-hour hearing underlines the connective-ness between CrowdStrike and governmental institutions and regulatory bodies. Most people wonder if more is necessary.

The startling fact that the error could have been easily detected if the update was run on a secured machine before deployment led to the joke of "testing in production" in the coding space. When consumers expect a company to provide them with a product, they also expect the product to not break as a result of the provider's mistakes. This highlights the issue of consumer trust and confidence in a space where products are proprietary and consumers have very little understanding of the actual moving parts in the products they are purchasing or how they are maintained.

Should the public, as consumers, have to simply trust private enterprises to properly maintain their products and uphold their commitments, or should more control and oversight be put upon them, and is that even possible? It raises the question of whether a government can even provide meaningful oversight that doesn't interfere with a company's development or trample user rights. This train of thought only seems to lead to a loss of consumer confidence.

Another issue is the fact that we had to learn about this error in CrowdStrikes CI/CD pipeline and deployment practices as a result of experience. At the very minimum consumers expect regulatory bodies to have methods and procedures in place to either prevent or spot these errors before they even can affect the real world. An example would be similar to OSHA, which people trust to enforce worker protections and safe practices in the construction space. Now, people are asking where was an OSHA equivalent in the case of preventing the CrowdStrike outage.

In some cases, that already exists in the US with CISA, or the Cybersecurity and Infrastructure Security Agency. A federal agency that is the "operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience". CISA was the federal head of response to the CrowdStrike outage. But why weren't they able to prevent such an outage from occurring in the first place, and why aren't there repercussions on CrowdStrike as a response?

In a statement about the outage CISA Director Jen Easterly called it a "terrible incident" but also "a useful exercise, like a dress rehearsal for what China may want to do to us." This response and subsequent discussion highlighted that the Director was more focused on moving past the incident entirely and more on how it prepared the agency and industry as a whole for the outcomes of the outage. Entirely missing is the fact of how a mistake like this occurred in the first place.

CISA understands the implications of the outage but also understands the position of CrowdStrike in the cybersecurity space. All of this shows that CISA and the US government are satisfied with simply holding a Congressional hearing and receiving CrowdStrike's incident report, which

is federally mandated by the Cyber Incident Reporting for Critical Infrastructure Act of 2022. It would not be out of place to say that the US government understands the position and power of CrowdStrike and as such, cannot take drastic public measures that would drag CrowdStrike's name through the mud and degrade confidence in the company as a whole and the Falcon Sensor as a product. It is somewhat mutually beneficial to leave it at a "do better next time" which preserves the image of CrowdStrike while letting them continue selling a very critical and in-demand product.

Another side issue is the responsibility of Microsoft in all of this. As CrowdStrike deploys its updates to Windows machines through Microsoft, where was their due diligence in the matter? As stated before, Microsoft only certifies the necessary software and drivers once, to make sure they run without difficulties the first time around. Should this have to change as cyber-security software often requires constant communication between cloud-based resources and the driver located on the Windows Kernel? Can Microsoft even be expected to re-certify every update that a third-party vendor intends to push?

In September Microsoft hosted a Windows Endpoint Security Ecosystem Summit on the topic of endpoint security attended by multiple security vendors from the Microsoft Virus Initiative (MVI) as well as government officials from the United States and the European Union. Microsoft has stated that they intend to present more options to vendors for security outside of the kernel and has proposed kernel access restrictions to third parties to permanently avoid issues similar to the Crowdstrike outage from occurring.

As draconian as this might sound, it is a rock-solid solution as Microsoft wouldn't need to potentially re-certify the constant updates required in the ever-evolving cyber-security space. However, this leads to the deduction that Microsoft wants more control over the Windows OS and Kernel as it is related to security. If only Microsoft had access to the Windows Kernel, they would be at a marked advantage over other security vendors that would have to "work from the outside".

Some conclusions have been gained from all of this. Microsoft has endeavored to expand non-kernel measures for vendors, decreasing the likelihood of faulty code resulting in BSoD's. Increasing awareness has been garnered in the CI/CD and deployment practices of cyber-security vendors, especially those with kernel-level access. Hopefully, this awareness will lead to standardized practices and government enforcement and oversight that will prevent significant mistakes that lead to the CrowdStrike outage. [30, 21, 28]

1.11 Link to Poster

CrowdStrike Outage Design on Canva.

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] Cosive. Crowdstrike falcon complete. https://www.cosive.com/capabilities/crowdstrike-falcon-complete. Accessed: November 30, 2024.

[6] CrowdStrike. Falcon complete: Next-gen managed detection and response (mdr). https://www.crowdstrike.com/services/endpoint-security/falcon-complete-next-gen-mdr/. Accessed: November 30, 2024.

[7] CrowdStrike. Falcon overwatch. https://www.crowdstrike.com/platform/threat-intelligence/adversary-overwatch. Accessed: November 30, 2024.

[8] 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.

[9] CrowdStrike. External technical root cause analysis — channel file 291. https://www.crowdstrike.com/wp-content/uploads/2024/08/Channel-File-291-Incident-Root-Cause-Analysis-08.06.2024.pdf, August 2024. Accessed: November 30, 2024.

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

[11] Red Hat. What is ci/cd? https://www.redhat.com/en/topics/devops/what-is-ci-cd, December 2023. Accessed: November 30, 2024.

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

[13] 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.

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

[15] KOVRR. Likely disclosure inconsistencies with massive snowflake data breach. https://www.kovrr.com/blog-post/likely-disclosure-inconsistencies-with-massive-snowflake-data-breach. Accessed: December 4, 2024.

[16] Tamlin Magee. Can delta win its crowdstrike lawsuit? https://www.raconteur.net/technology/delta-crowdstrike-lawsuit. Accessed: December 4, 2024.

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

[18] 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.

[19] 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.

[20] Microsoft. Windows hardware compatibility program certification process. https://learn.microsoft.com/en-us/windows-hardware/design/compatibility/whcp-certification-process, March 2022. Accessed: November 30, 2024.

[21] Committee on Homeland Security. Icymi: Committee examines crowdstrike processes in first congressional hearing on the disastrous july global it outage, 2024. Accessed: 2024-12-06.

[22] Oracle. What is a graph database? https://www.oracle.com/autonomous-database/what-is-graph-database/, November 2024. Accessed: November 30, 2024.

[23] European Parliament. The nis2 directive. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. Accessed: December 4, 2024.

[24] Proofpoint. What is telemetry? telemetry cybersecurity explained. https://www.proofpoint.com/us/threat-reference/telemetry#:~:text=Security%20telemetry%20involves%20data%20collection,%2C%20vulnerabilities%2C%20or%20potential%20breaches. Accessed: November 30, 2024.

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

[26] Carsten Sandker. Offensive windows ipc internals 1: Named pipes. https://csandker.io/2021/01/10/Offensive-Windows-IPC-1-NamedPipes.html, January 2021. Accessed: November 30, 2024.

[27] 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.

[28] SC Media. Crowdstrike outage leads microsoft to plan more 'security capabilities outside of kernel', 2024. Accessed: 2024-12-06.

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

[30] Utility Dive. Crowdstrike snafu was a 'dress rehearsal' for critical infrastructure resiliency, says jen easterly, 2024. Accessed: 2024-12-06.

[31] 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.

[32] David Weston. Windows security best practices for integrating and managing security tools. https://www.microsoft.com/en-us/security/blog/2024/07/27/windows-security-best-practices-for-integrating-and-managing-security-tools/, July 2024. 16 min read, Accessed: November 30, 2024.