CrowdStrike's BSOD Nightmare:

The Hidden Risks of Legacy Detection-Based Endpoint Security

Introduction

On July 19, 2024, a significant global tech outage disrupted airlines, banks, healthcare, and public transit systems. The root cause was traced back to a configuration file that was malformed, which adversely affected Microsoft Windows Operating Systems and caused what is commonly known as Blue Screen of Death ("BSOD").

This incident highlights the vulnerabilities inherent in relying on a detection-based approach to endpoint security, where frequent constant updates are required to keep pace with the overwhelming release of new malware. Kernel updates are particularly sensitive, and reliance on changing Kernel drivers is a recipe for ongoing BSOD events.

This whitepaper examines the root cause of this issue in detail, the failure of detection-based endpoint security solutions in dealing with zero-day threats, as well as providing suggestions for a better approach which improves both security and operational stability.

Why CrowdStrike’s Detection-Based Solution Fails

CrowdStrike’s approach of frequently updating kernel-mode code is inherently risky and disruptive. Kernel-mode code operates at the core of the operating system, managing critical functions and communications with hardware. Frequent updates to this highly sensitive layer can introduce bugs and vulnerabilities that lead to system instability and crashes, such as the Blue Screen of Death (BSOD). The recent BSOD incident caused by a CrowdStrike update is not an isolated case and is unlikely to be the last. This approach creates a constant risk of operational disruptions and undermines system reliability, posing significant challenges for businesses that rely on stable and secure IT environments.

When deploying new kernel-mode code, extensive Quality Assurance (QA) and intensive testing are absolutely necessary. Kernel-mode updates have the potential to cause significant system instability if not meticulously tested. Every new release must undergo rigorous testing phases to ensure compatibility with existing systems and to identify any potential conflicts or bugs. This thorough testing helps prevent issues that could lead to system crashes and ensures that the update performs as expected across various environments. Without adequate QA and testing, the risk of introducing new vulnerabilities or operational disruptions is significantly heightened, making the update process more hazardous than beneficial.

CrowdStrike Violated Microsoft's Approval Process

To maximize client security, CrowdStrike, like other legacy detection-based security providers, continuously updates its software to counter the latest zero-day threats. However, the time required for new code approval by Microsoft can create a conflict between addressing security vulnerabilities and maintaining operational stability. To accelerate their response to zero-day threats, CrowdStrike bypassed Microsoft's approval process. Instead of submitting new driver code for review, which involves rigorous testing for stability, security, and compatibility, CrowdStrike linked its driver update to an external folder providing kernel-code updates, effectively circumventing the approval process.

Understanding the Incident

CrowdStrike's preliminary Post Incident Review (PIR) details the events leading up to the outage. A Rapid Response Content update, intended to gather telemetry on novel threat techniques, caused an out-of-bounds memory read, resulting in a Blue Screen of Death (BSOD) on Windows hosts. This incident affected Windows hosts running sensor version 7.11 and above that were online during the update window.

The Role of the Content Interpreter

CrowdStrike's Falcon platform uses the Content Interpreter to process content configuration updates. According to their PIR, Rapid Response Content updates are designed to perform behavioral pattern-matching operations on the sensor. These updates are stored in a proprietary binary file and are interpreted by the Content Interpreter, enabling the Sensor Detection Engine to observe, detect, or prevent malicious activity.

Despite CrowdStrike's claims that Rapid Response Content is not code or a kernel driver, the very nature of the Content Interpreter suggests otherwise. The term "interpreter" implies that the system is executing instructions or scripts in real-time. This is a crucial point—whatever terminology CrowdStrike uses, the Content Interpreter essentially runs scripts in the kernel, modifying the execution flow.

The Risks of Running Scripts in the Kernel

Running scripts in kernel mode is inherently dangerous. The kernel is the core component of the operating system, managing critical functions like memory management, process scheduling, and hardware interactions. Any errors or vulnerabilities in the kernel can lead to catastrophic system failures, as seen in the July 19 incident.

Moreover, scripts executed in the kernel mode bypass Microsoft's EV Code Signing guidelines. These guidelines are designed to ensure that only trusted, verified code runs in the kernel, preventing malicious code from compromising the system. By using an interpreter to run unvalidated scripts, CrowdStrike undermines this critical security measure, exposing their customers to significant risks.

Extended Validation (EV) Code Signing guidelines represent an industry standard designed to enhance security and trust. EV Code Signing certificates provide the highest level of authentication and undergo a rigorous validation process, ensuring that only verified publishers can distribute software. This process includes comprehensive checks by a trusted Certificate Authority (CA) and provides a cryptographic signature that verifies the legitimacy of the software. Microsoft, among other leading tech companies, has adopted these EV guidelines to reinforce the security of software distributed to users.

CrowdStrike's decision to bypass these EV Code Signing guidelines and Microsoft's stringent approval process highlights a significant deviation from established industry practices. Instead of adhering to the EV guidelines, which ensure stability, security, and compatibility through thorough testing, CrowdStrike linked its driver update to an external folder, thus evading the necessary reviews. This not only violated Microsoft's policies but also compromised the industry standard set by the EV guidelines.

CrowdStrike's struggle to rapidly update kernel code while adhering to Microsoft's stringent approval process and EV guidelines highlights the complexities of balancing security with operational stability These challenges underscore the flaws of a detection-based approach in addressing zero-day threats.

In other words, not only is the detection-based approach not effective in protecting against Zero Day Threats, but the rush to solve them creates operational instability.

What Xcitium Does Differently

Detection-based security does not recognize (and thus protect against) unknowns, including new malware. Unknowns are only discovered and addressed by legacy detection-based endpoint security providers once it has done damage to their clients. Xcitium's Zero Trust Architecture (ZTA) by contrast, automatically detects all unknown executables, and allows them to launch only to a virtualized container where they can do no harm.

Xcitium takes a revolutionary approach to endpoint protection by completely rethinking the traditional architecture. Different from the rest of the industry, which is "detection-based", and thus dependent on constant updates, our strategy is built on containment of all unknown executables, which eliminates the need for constant kernel updates. By identifying and containing all unknown executables in real-time, we protect against known and unknown threats without the need for constant signature and kernel updates, ensuring a stable and secure operating environment. We employ a "Latest and Stable" build concept, allowing customers to choose between the most recent updates and thoroughly tested stable releases. This flexibility minimizes the risk of disruptions.

Additionally, our Adaptive Event Modeling dynamically evolves to address new threats without requiring intrusive code updates. Our approach ensures that only user-mode rules and codes are updated, reducing the impact on system stability and performance. By prioritizing extensive testing and customer control over updates, Xcitium delivers a security solution that is both reliable and resilient, addressing the inherent risks of frequent kernel-mode updates seen in traditional models.

Global Impact

The recent content updates by CrowdStrike, a leading cybersecurity company, included a defect that caused widespread disruptions across multiple sectors.

These updates inadvertently affected the functionality of Microsoft Windows Operating Systems, leading to system crashes, data corruption, and operational paralysis. The outage severely impacted airlines, banks, healthcare facilities, and public transit systems, highlighting the critical vulnerabilities in relying on third-party updates for essential system security.

Impact on Different Sectors:

Banks:

Disruptions: Inaccessibility of online banking services, ATM outages, and transaction failures

Consequences: Customer dissatisfaction, potential security breaches, and financial instability

Healthcare:

Disruptions: System crashes in hospitals, unavailability of patient records, and operational delays

Consequences: Delayed treatments, compromised patient safety, and strained healthcare resources

Public Transit:

Disruptions: Failures in scheduling and ticketing systems, operational delays

Consequences: Commuter chaos, decreased public trust, and economic losses

Airlines:

Disruptions: Flight delays and cancellations, grounded aircraft

Consequences: Passengers stranded, financial losses, and reputational damage

Conclusion

The global tech outage on July 19, 2024, underscores the critical vulnerabilities in relying on frequent kernel updates for detection-based endpoint security, as evidenced by CrowdStrike's defective kernel driver update causing widespread disruptions across various sectors. This incident highlights the inherent risks of a detection-based approach that necessitates constant updates to address new threats. In contrast, Xcitium's zero trust architecture, focusing on containment rather than detection, offers a more stable and secure solution by eliminating the need for frequent kernel updates and prioritizing extensive testing and customer control. This approach ensures system stability and resilience, mitigating the risks of operational disruptions and enhancing overall security.

About Xcitium

Xcitium cybersecurity solutions are used by more than 6,000 organizational customers and partners around the globe. Xcitium was founded with one simple goal – to put an end to cyber breaches. Our patented ZeroDwell technology uses Kernel-level API virtualization to isolate and remove threats like zero-day malware and ransomware before they cause any damage to endpoints. ZeroDwell is the foundation of our Unified Zero Trust (UZT) endpoint and cloud offerings. Since inception, Xcitium has a track record of zero breaches when fully configured; see Xcitium's certified performance record here.

Xcitium's Zero Trust Architecture, preemptively isolates all unknown files and scripts, ensuring they do not compromise the system. This protective, preventive approach significantly reduces the risk of ransomware and zero-day malware attacks.

For more information, visit

xcitium.com