halcyon

Data Sheet

Feature Spotlight: Kernel Guard Protection

Exploiting Vulnerable Drivers to Carry out an Attack

Advancements in endpoint security products have created problems for ransomware adversaries, who must bypass EDR products to carry out their attacks. **An increasingly common technique for disabling security products is loading a signed but vulnerable kernel driver, which allows the attacker to exploit the vulnerability and perform actions in the most privileged domain available: the kernel.**

Halcyon's Kernel Guard Protection combats the use of these signed but vulnerable drivers, ensuring that bad actors cannot exploit this inherent trust to carry out their objectives.

How a Bring Your Vulnerable Driver (BYOVD) Attack Works

Kernel drivers operate at a higher privilege level than admin privileges, allowing them greater control over a system. Given this access, Microsoft Windows only allows valid, cryptographically signed drivers to load. Unfortunately, some of these signed valid drivers contain vulnerabilities that attackers can exploit to use this kernel-level access to set the stage for their ransomware payload deployment.

- **Initial Attack Access:** An attacker first gains access to a compromised computer.
- **Security Tool Identification:** The attacker scans the system to identify security tools (e.g., antivirus, endpoint protection).
- **Exploiting Vulnerable Driver:** If security tools are present, the attacker would load the vulnerable driver to escalate privileges to the kernel level.
- **Disabling Security Measures:** The attacker disables security detection and prevention tools with kernel access.
- **Executing Malicious Actions:** Once security is bypassed, the attacker can perform malicious activities such as deploying ransomware and exfiltrating data.

Halcyon Features

- Always Included 24/7/365 Expert Threat Monitoring and Recovery
- Pre-execution Prevention
- Ransomware Behavior Detection
- Encryption Key Material Intercept
- Data Exfiltration Protection

About Halcyon

Halcyon is the only cybersecurity company that eliminates the business impact of ransomware. Modern enterprises rely on Halcyon to prevent ransomware attacks, eradicating cybercriminals' ability to encrypt systems, steal data, and extort companies. Backed by an industry-leading warranty, the Halcyon Anti-Ransomware Platform drastically reduces downtime, enabling organizations to quickly and easily recover from attacks without paying ransoms or relying on backups.

How Halcyon Kernel Guard Protection Works

1

The Halcyon RISE Team constantly investigates new and exploitable drivers actively used by ransomware operators.

2

When Halcyon detects that a driver is loading that matches Halcyon's vulnerable driver intel, an alert is generated.

3

Halcyon RDR, the 24/7/365 threat monitoring team, included with the platform, investigates the alert and informs the customer(s) of the potential threat.

4

Halcyon RDR will take response actions, as needed, on behalf of the customer to ensure the ransomware actors' operations do not harm the target machine.

How Halcyon Kernel Guard Protection Works with Other Vulnerable Driver Protections

Many endpoint security products, such as CrowdStrike Falcon® or Microsoft Defender®, provide a measure of vulnerable driver protection in their products. However, due to limitations on maintaining an up-to-date knowledge base of all known vulnerable drivers, these protections leave bad actors with many viable options to deliver their attacks. Halcyon's focus on ransomware attacks, with its dedicated research and intelligence teams analyzing how these attacks begin, enables us to provide the most comprehensive coverage against the use of known vulnerable drivers to exploit target systems.

Kernel Guard Protection Benefits

Any security solution aims to stop as many attacks as possible before they begin, limiting potential damage to the organization. With Halcyon Kernel Guard Protection, Halcyon customers have another means to stifle any ransomware attack before it starts. Coupled with Halcyon's pre-execution prevention, ransomware behavior detection, data exfiltration protection, reliable data decryption, ransomware recovery capabilities, and the included 24/7/365 threat monitoring, organizations have the most comprehensive protection against damaging ransomware attacks available without adding staff or additional resources.

See Halcyon in Action

To learn more about Halcyon Kernel Guard Protection or any other aspect of the Halcyon Anti-Ransomware Platform, visit halcyon.ai and schedule a personal demo today with one of our ransomware experts.