

# Reynolds Ransomware

The ultimate EDR killer

Erik Westhovens

19-02-2026



# Cyber Threat Intelligence Report

**Subject:** Reynolds Ransomware & Vulnerable Driver Exploitation (CVE-2025-68947)

**Audience:** SOC, Incident Response, Threat Hunting, Security Leadership

**Date:** February 2026

## 1. Executive Summary

Reynolds is an emerging and highly sophisticated ransomware threat that leverages a Bring-Your-Own-Vulnerable-Driver (BYOVD) technique associated with CVE-2025-68947 to achieve kernel-level execution and disable endpoint security controls prior to initiating encryption. This approach represents a significant evolution in ransomware tradecraft, shifting the focus from post-compromise monetization to pre-encryption stealth and defense neutralization.

Traditional ransomware campaigns typically follow a recognizable progression: initial access, privilege escalation, lateral movement, data exfiltration, and ultimately encryption. Detection opportunities often arise during credential abuse, suspicious PowerShell execution, anomalous SMB activity, or mass file modification events. Reynolds, however, disrupts this detection model by introducing kernel-level defense evasion at an earlier stage in the intrusion lifecycle. By weaponizing a legitimately signed but vulnerable driver, attackers gain the ability to terminate security processes, interfere with endpoint detection and response (EDR) capabilities, and operate beneath user-mode monitoring controls.

The abuse of CVE-2025-68947 enables arbitrary process termination and privileged system manipulation through a trusted driver component. Because the driver is legitimately signed, its presence may not initially appear suspicious in environments that rely heavily on signature-based or reputation-based trust models. Once loaded, the driver exposes functionality that can be exploited to disable or tamper with security software, including antivirus engines, EDR agents, logging components, and other defensive mechanisms. This technique effectively blinds the organization's detection stack before malicious activity escalates to visible stages such as encryption or data staging.

The strategic implication of this approach is substantial. Rather than evading detection during encryption — which often generates high-fidelity alerts due to abnormal file modification rates — Reynolds attempts to eliminate detection capabilities altogether before high-noise behaviors occur. This dramatically reduces the defender's response window. In many cases, by the time encryption begins, monitoring tools may already be impaired or fully disabled. As a result, organizations may experience limited telemetry visibility, incomplete forensic records, and delayed incident recognition.

The use of BYOVD techniques also signals increasing technical maturity within ransomware ecosystems. Kernel-level abuse was historically more common in advanced persistent threat (APT) operations, but it is now becoming normalized within financially motivated ransomware campaigns. This convergence indicates a broader trend: ransomware actors are investing in stealth, resilience, and pre-emptive defense neutralization rather than relying solely on speed and automation.

From a risk perspective, Reynolds must be categorized as a critical enterprise threat. The exploitation of CVE-2025-68947 is not merely a vulnerability management issue; it is an operational enabler for full security bypass. The presence, staging, or execution of the associated driver should not be treated as an isolated misconfiguration or low-risk software artifact. Instead, it should be considered a high-confidence indicator of malicious intent or active compromise. Because driver abuse occurs before traditional behavioral indicators

such as lateral movement bursts or encryption spikes, early detection at the driver level may represent one of the few viable opportunities to contain the attack before business disruption occurs.

Additionally, this technique increases the likelihood of successful double extortion operations. If endpoint monitoring is disabled early, attackers can exfiltrate sensitive data with reduced risk of triggering data loss prevention (DLP) or anomaly detection controls. Organizations may therefore face both operational outage and regulatory exposure, particularly in sectors subject to compliance obligations or breach notification requirements.

Defensive posture must adapt accordingly. Security teams should prioritize detection of vulnerable driver presence, driver load events, and abnormal kernel-level interactions. Monitoring must extend beyond traditional user-mode process behavior and incorporate telemetry capable of identifying suspicious driver installations and exploit patterns. Near-real-time alerting for known vulnerable driver hashes and filenames is strongly recommended, along with strict incident response procedures when detections occur.

In summary, Reynolds represents a shift toward pre-encryption defense dismantling through kernel-level exploitation. By leveraging CVE-2025-68947 in a BYOVD framework, the threat actor minimizes detection exposure, increases the probability of ransomware success, and elevates overall enterprise risk. Any detection of the associated vulnerable driver should be escalated as a high-severity precursor compromise requiring immediate containment and investigation. Early recognition at this stage may be the only practical opportunity to prevent encryption, data loss, and significant business impact.

## 2. Threat Overview

### 2.1 Malware Family

Reynolds is a human-operated ransomware family distinguished by its deliberate focus on defense evasion prior to encryption. Unlike opportunistic or fully automated ransomware strains, Reynolds appears to be deployed in targeted intrusions where attackers maintain hands-on control throughout the compromise lifecycle. This operational style enables adaptive decision-making, environment-specific privilege escalation, and strategic timing of encryption events.

The defining technical characteristic of Reynolds is its ability to achieve kernel-level security bypass through the abuse of a legitimately signed but vulnerable driver associated with CVE-2025-68947. By leveraging a Bring-Your-Own-Vulnerable-Driver (BYOVD) technique, attackers can gain elevated privileges and interfere directly with core operating system components. This allows them to terminate or tamper with endpoint protection platforms before encryption is initiated, significantly reducing the likelihood of detection during critical attack phases.

While full attribution remains limited, the structured intrusion workflow and advanced tradecraft suggest an operational model consistent with Ransomware-as-a-Service (RaaS) ecosystems or affiliate-driven campaigns. In such models, initial access brokers or specialized operators may conduct early-stage compromise activities before deploying the Reynolds payload to monetize the intrusion.

### 2.2 Key Innovation

Reynolds' primary innovation lies in embedding defense neutralization directly within its operational chain rather than relying on separate post-compromise tooling. Traditional ransomware actors often deploy additional utilities to disable EDR, escalate privileges, or manipulate system drivers. Reynolds consolidates these capabilities, integrating kernel-level abuse into the attack sequence itself.

By directly incorporating EDR termination, privilege escalation, and kernel manipulation techniques into its deployment workflow, Reynolds reduces operational noise and limits the number of detectable artifacts left behind. This consolidation streamlines execution and shortens the defensive response window.

This design reflects a broader evolution in ransomware tradecraft toward pre-encryption stealth. Modern ransomware operations increasingly prioritize disabling detection mechanisms before high-visibility actions occur, signaling a shift from reactive evasion to proactive defense dismantling as a standard component of financially motivated cybercrime.

## 3. Vulnerability Details – CVE-2025-68947

### 3.1 Technical Description

CVE-2025-68947 affects a legitimately signed Windows kernel-mode driver that contains insecure functionality allowing improper access to privileged operations. Although the driver is digitally signed and therefore trusted by the Windows operating system, it exposes unsafe input/output control (IOCTL) handlers that can be abused by a local attacker. The presence of a valid signature significantly reduces suspicion during driver loading and allows it to bypass controls that rely solely on signature enforcement or reputation-based trust models.

The vulnerability enables arbitrary process termination by allowing user-supplied input to instruct the driver to interact directly with kernel-level structures. An attacker can leverage this capability to terminate critical security processes, including antivirus engines, EDR agents, logging components, and monitoring services. Because these actions are executed from kernel context, defensive software operating in user mode often cannot prevent or reliably detect the termination.

In addition to process manipulation, exploitation of CVE-2025-68947 facilitates privilege escalation to SYSTEM or full kernel context. This level of access grants the attacker unrestricted control over the operating system, including the ability to modify memory, disable protections, manipulate drivers, and interfere with core security mechanisms. From a defensive standpoint, kernel-level execution represents one of the highest risk states, as it undermines trust in system integrity and limits the reliability of telemetry.

### 3.2 Exploitation Method

In observed attack scenarios, threat actors deploy the vulnerable driver alongside their ransomware tooling as part of a Bring-Your-Own-Vulnerable-Driver (BYOVD) technique. After gaining initial access and establishing administrative privileges, the attacker installs and loads the legitimate driver into the operating system.

Once loaded, the attacker interacts with the driver through its exposed IOCTL interface. By issuing crafted control requests, they can terminate selected security processes, effectively disabling endpoint monitoring and response capabilities. Because the driver operates in kernel space, these termination actions occur outside the reach of many standard user-mode protections.

Following defense neutralization, the attacker maintains kernel-level control to support additional malicious activities. This may include deploying ransomware payloads, establishing persistence, facilitating lateral movement, or staging data for exfiltration. By conducting these operations after security controls have been weakened or disabled, the attacker significantly reduces the probability of detection.

This exploitation technique bypasses traditional user-mode security monitoring and shortens the defender's response window, making early detection of the vulnerable driver's presence or load activity critically important for preventing subsequent ransomware impact.

## **4. Attack Chain Assessment**

### **4.1 Initial Access**

Reynolds operations are consistent with modern human-operated ransomware campaigns that rely on established enterprise intrusion vectors. Initial access is commonly achieved through credential-based compromise rather than zero-day exploitation. Phishing campaigns aimed at harvesting credentials remain a primary entry point, particularly when targeting privileged or IT-associated accounts. Stolen VPN credentials or compromised Microsoft Entra ID accounts also represent high-value access paths, especially in environments lacking strong conditional access enforcement or multifactor authentication resilience.

In some cases, attackers may exploit exposed edge services, vulnerable web applications, or previously deployed web shells to gain footholds within perimeter-facing infrastructure. These methods allow adversaries to establish persistence within externally accessible systems before pivoting internally. Regardless of the entry vector, the defining characteristic of Reynolds intrusions is the rapid transition from access to privilege consolidation.

### **4.2 Post-Access Preparation**

Following initial compromise, operators typically perform structured post-exploitation preparation. This includes establishing persistence mechanisms to ensure continued access even if credentials are reset or sessions are terminated. Persistence may involve scheduled tasks, service modifications, registry alterations, or secondary account creation.

Privilege escalation is a critical objective during this phase. Attackers seek administrative or SYSTEM-level rights to deploy and load the vulnerable kernel driver associated with CVE-2025-68947. Once sufficient privileges are obtained, the vulnerable driver is staged and prepared for execution as part of the defense-evasion sequence.

This preparation phase is often deliberately quiet, minimizing overtly malicious behavior until security controls can be neutralized.

### **4.3 Defense Neutralization**

The core differentiator in the Reynolds attack chain is kernel-level defense neutralization. By loading the vulnerable driver, attackers gain the capability to terminate or interfere with EDR and antivirus processes from kernel context. This not only disables active protection but may also prevent remediation actions such as process blocking, quarantine, or automated containment.

Additionally, disabling or impairing security tooling reduces logging fidelity and forensic visibility, complicating post-incident investigation and timeline reconstruction.

### **4.4 Impact Phase**

Once endpoint protections are weakened or disabled, attackers accelerate toward impact. Lateral movement typically increases in speed and scope, leveraging administrative privileges to propagate across the environment. Sensitive data may be staged and exfiltrated to support double extortion tactics. Finally, encryption is deployed across targeted systems, followed by ransom demands intended to maximize operational and financial pressure.

## 5. Risk Assessment

### 5.1 Severity

Reynolds should be classified as a **Critical / High Enterprise Risk** threat due to its technical sophistication and operational impact potential. Unlike conventional ransomware strains that are detected during lateral movement or encryption bursts, Reynolds introduces stealth at the earliest meaningful stage of compromise. By leveraging a vulnerable but legitimately signed kernel driver, the threat actor can dismantle endpoint defenses before high-noise malicious activity begins.

Pre-encryption stealth significantly alters the defensive equation. Security teams typically rely on behavioral indicators such as mass file modification, suspicious PowerShell execution, credential dumping artifacts, or anomalous authentication patterns to detect ransomware activity. In the Reynolds intrusion model, many of these signals may either never trigger or may trigger too late, after endpoint monitoring has already been impaired. This compressed detection window materially increases the probability of successful attack progression.

Kernel-level control further elevates severity. When attackers operate in kernel context, they gain authority over core operating system functions, including process management, memory interaction, and driver operations. At this level, defensive tools running in user mode may be terminated, manipulated, or blinded. The compromise therefore affects not only confidentiality and availability but also the integrity of system telemetry itself. In practical terms, defenders may lose trust in their visibility and response tooling during the most critical phase of the incident.

Collectively, these factors create a high likelihood of ransomware execution success once the vulnerable driver has been loaded. Detection of the associated driver should therefore be interpreted as a strong precursor indicator of imminent or ongoing ransomware deployment.

### 5.2 Business Impact

The business implications of a successful Reynolds intrusion are substantial. Operational disruption may occur rapidly if core systems, servers, or endpoint fleets are encrypted. Recovery timelines can extend significantly if backups are targeted or if security tooling was disabled before incident containment began.

In addition to availability impact, the likelihood of data exfiltration increases when monitoring controls are neutralized early in the intrusion. Exposure of sensitive customer data, intellectual property, or regulated information can trigger mandatory breach notification obligations under regional and sector-specific regulations. This introduces legal, compliance, and reputational risks beyond the immediate technical disruption.

Financial consequences may include ransom payments, incident response costs, legal expenses, regulatory fines, customer attrition, and long-term brand damage. Given the combination of stealth, privilege depth, and operational intent, Reynolds represents not merely a technical vulnerability but a significant enterprise-level business risk requiring proactive mitigation and rapid-response readiness.

## 6. Detection, Mitigation & Defensive Actions

Effective defense against Reynolds ransomware requires combining early detection capabilities with immediate containment readiness and structural hardening controls. Because the defining characteristic of this threat is pre-encryption defense neutralization, traditional ransomware detection logic alone is insufficient. Security teams must shift focus toward identifying the earliest reliable precursor signal: the presence or execution of the vulnerable driver associated with CVE-2025-68947.

## 6.1 Earliest Reliable Indicator

The most valuable detection point in the Reynolds attack chain is the staging or loading of the vulnerable kernel driver. This event typically occurs before encryption, lateral movement acceleration, or large-scale data exfiltration. As such, it provides a narrow but critical opportunity to contain the intrusion before operational disruption occurs.

Driver presence or execution is a strong indicator of malicious intent in this context. Legitimate enterprise use of this specific vulnerable driver is rare, and its appearance—particularly on servers or endpoints not explicitly requiring it—should be treated as high risk. Because the driver enables kernel-level process termination and security bypass, detection at this stage allows defenders to isolate affected systems before endpoint monitoring is disabled.

## 6.2 Key Telemetry & Monitoring Priorities

Security teams should prioritize telemetry sources capable of identifying:

- Kernel driver load events
- File creation or staging of suspicious driver binaries
- Termination attempts targeting EDR or antivirus processes
- Indicators of privilege escalation to SYSTEM context

Monitoring must include both file-based detection and driver-load visibility. Near-real-time alerting is strongly recommended to reduce response latency.

## 6.3 Advanced Hunting Detection Queries (Microsoft Defender XDR)

### Driver Load Detection (Preferred Signal)

```
DeviceImageLoadEvents
| where SHA256 =~ "206f27ae820783b7755bca89f83a0fe096dbb510018dd65b63fc80bd20c03261"
   or FileName =~ "NSecKrn1.sys"
| project Timestamp, DeviceName, DeviceId, ReportId,
   FileName, FolderPath, SHA256, SHA1,
   InitiatingProcessFileName,
   InitiatingProcessCommandLine,
   InitiatingProcessAccountName
```

### Driver Presence on Disk

```
DeviceFileEvents
| where SHA256 =~ "206f27ae820783b7755bca89f83a0fe096dbb510018dd65b63fc80bd20c03261"
   or FileName =~ "NSecKrn1.sys"
| project Timestamp, DeviceName, DeviceId, ReportId,
   ActionType, FileName, FolderPath,
```

```
SHA256, SHA1,  
InitiatingProcessFileName,  
InitiatingProcessCommandLine,  
InitiatingProcessAccountName
```

These queries should be deployed as Near-Real-Time custom detections across all managed tenants. Any resulting alert must be treated as a high-severity incident requiring immediate triage and potential device isolation.

## 6.4 Indicators of Compromise (IOCs)

### **CVE Reference:**

CVE-2025-68947

### **Driver Filename:**

NSecKrn.sys

### **Known SHA256 Hash:**

206f27ae820783b7755bca89f83a0fe096dbb510018dd65b63fc80bd20c03261

Organizations should continuously validate whether additional hashes or modified variants appear in telemetry and update detection logic accordingly.

## 6.5 Immediate Controls

Across all managed environments, security teams must:

- Deploy near-real-time detections for the identified driver hash and filename
- Confirm Advanced Hunting telemetry availability in each tenant
- Validate that alerts generate properly
- Escalate detections as priority incidents

Any confirmed driver execution should trigger immediate containment actions, including device isolation and privilege review.

## 6.6 Hardening Measures

To reduce exposure to BYOVD-based ransomware techniques, enterprises should:

- Block known vulnerable drivers using policy-based controls
- Enforce tamper protection and EDR self-protection mechanisms
- Monitor and restrict kernel driver installation attempts
- Limit administrative privilege exposure through least-privilege models
- Regularly review driver allowlists and signing trust policies

By integrating early driver-level detection with strong hardening controls, organizations significantly improve their ability to disrupt Reynolds-style ransomware campaigns before encryption and business impact occur.

## 7. Incident Response & Recovery Guidance

Detection of the vulnerable driver associated with CVE-2025-68947 must be treated as a high-confidence precursor to ransomware activity. Because this technique enables kernel-level security bypass, the response should assume that endpoint defenses may already be impaired. Immediate, structured incident handling is essential to prevent escalation to encryption and business disruption.

### 7.1 Immediate Actions

Upon detection, affected device(s) should be isolated from the network without delay. Rapid containment limits lateral movement and prevents the attacker from expanding access while investigation is underway. If automated isolation capabilities are available through the endpoint protection platform, they should be triggered immediately.

Volatile evidence must be preserved before reboot or remediation actions occur. This includes memory capture, active network connections, running processes, and loaded drivers. Since the attacker may have operated in kernel context, volatile data is critical for understanding the scope and technique of compromise.

Formal incident response procedures should be activated at once. This includes notifying the internal incident response team, documenting timelines, preserving logs, and escalating according to organizational playbooks. Early executive awareness may be appropriate depending on the criticality of the affected system.

### 7.2 Investigation Focus

Investigation efforts should prioritize determining the depth and breadth of compromise. Particular attention must be given to credential exposure. If administrative or privileged credentials were used or accessed, assume potential credential theft and plan for resets accordingly.

Lateral movement analysis is essential. Review authentication logs, remote service creation events, SMB activity, and abnormal administrative access patterns. Because defense evasion may have reduced telemetry fidelity, corroborate findings across multiple data sources.

Persistence mechanisms must be identified and eradicated. Examine scheduled tasks, services, registry modifications, newly created accounts, and additional driver installations. Ensure no secondary backdoors or remote access tooling remain active.

Data access and potential exfiltration should be assessed. Review outbound network traffic, cloud storage interactions, and archive creation activity. Even if encryption has not yet occurred, data theft may already have been attempted.

Backup integrity validation is critical. Confirm that backup repositories remain uncompromised, immutable where possible, and free of malicious modification.

### 7.3 Recovery Considerations

The use of BYOVD techniques indicates advanced attacker capability and deliberate defense bypass. Therefore, incident responders should assume the possibility of broader environment compromise beyond the initially detected system. Delayed ransomware execution is also possible if attackers maintain persistence.

Full containment may require network segmentation, temporary service suspension, and comprehensive credential resets across privileged accounts. In high-risk scenarios, rebuilding affected systems from known-good images is strongly recommended.

Ultimately, recovery should prioritize restoring trust in system integrity before resuming normal operations.

## 8. Strategic Outlook & Conclusion

The Reynolds campaign reflects a broader and concerning shift within the ransomware ecosystem. Threat actors are increasingly adopting techniques historically associated with advanced persistent threat (APT) operations, particularly the abuse of kernel-level components to neutralize defenses before executing high-impact actions. The use of a Bring-Your-Own-Vulnerable-Driver (BYOVD) technique tied to CVE-2025-68947 demonstrates how financially motivated groups are integrating low-level system manipulation into their standard operational playbooks.

This evolution marks a transition from reactive evasion to proactive defense dismantling. Rather than attempting to avoid detection during encryption or lateral movement, actors now seek to eliminate or weaken monitoring capabilities at the outset of the intrusion. As a result, signature-based detection and traditional behavior triggers are becoming less reliable as primary safeguards. When endpoint protections are disabled at kernel level, telemetry gaps may emerge, forensic evidence may be incomplete, and detection windows may close before meaningful response can occur.

Organizations must therefore adapt their defensive posture. Greater emphasis should be placed on behavioral detection models that identify abnormal system interactions rather than relying solely on known malware signatures. Driver-level monitoring must become a standard component of enterprise visibility, including detection of vulnerable driver installations, unusual driver loads, and attempts to interact with kernel interfaces. Equally important is the ability to respond quickly and decisively. Rapid containment capabilities—such as automated device isolation and credential revocation—can significantly reduce impact if triggered during early-stage compromise.

In conclusion, Reynolds ransomware, enabled by CVE-2025-68947, represents a high-impact, early-stage defense-evasion threat capable of disabling endpoint protections prior to encryption. Its operational model reduces the effectiveness of conventional detection strategies and increases the probability of successful ransomware deployment and double extortion.

Detection of the associated vulnerable driver must be treated as a confirmed high-risk intrusion precursor. Such alerts require immediate containment, comprehensive investigation, and executive-level awareness where appropriate. Achieving consistent detection coverage across all managed tenants, combined with hardened driver controls and strong incident response readiness, is essential to prevent ransomware execution and the severe operational, financial, and reputational consequences that may follow.

## 10. Our Perspective: How Ransomwared Helps

Modern infostealer operations expose a fundamental weakness in many contemporary security strategies: an overreliance on the assumption that malicious activity will be noisy, persistent, or technically complex. Infostealers deliberately violate that assumption. They are brief, quiet, and designed to disappear before defenders have time to react. Their true impact unfolds later, when stolen credentials, sessions, and tokens are used to access systems in ways that appear legitimate. This is the gap where many organizations lose visibility — and it is precisely the gap Ransomwared was built to address.

At **Ransomwared**, we start from a different premise than most security tools. We assume that initial access will happen. We assume that endpoint defenses may not always see it. And we assume that attackers will increasingly rely on legitimacy rather than malware to achieve their objectives. Instead of asking how to block every possible infostealer variant, we ask a more practical and more urgent question: *How do we detect and respond when stolen access is being prepared for abuse?*

### Seeing What Traditional Tools Miss

Traditional endpoint security solutions are optimized to detect malicious code execution, persistence mechanisms, and exploit behavior. These controls remain essential, but infostealers are explicitly designed to operate beneath their threshold of concern. A short-lived user-context process that reads browser files and exits may never rise above a low-severity alert, if it is flagged at all.

Ransomwared focuses on the *meaning* of that activity rather than its superficial characteristics. A process accessing browser credential stores is not dangerous because it is malware; it is dangerous because it is extracting the very artifacts that grant legitimate access to the enterprise. By treating credential harvesting as a first-class security event rather than a peripheral signal, Ransomwared helps organizations recognize the moment when an environment becomes vulnerable to identity abuse and ransomware staging.

### Bridging Endpoint, Identity, and Behavior

One of the defining challenges of infostealer-driven intrusions is fragmentation of visibility. Endpoint tools see isolated file access. Identity platforms see successful logins. Cloud services see authorized actions. Each system, viewed independently, may show nothing overtly malicious.

Ransomwared is designed to bridge these domains. It correlates endpoint behaviors with identity activity and higher-level behavioral patterns, allowing defenders to see the full narrative of an intrusion rather than disconnected fragments. This correlation is critical in identifying the transition from initial access to pre-impact staging — the phase where attackers prepare for ransomware deployment, data exfiltration, or long-term abuse.

By focusing on patterns rather than signatures, Ransomwared remains effective even as infostealer families change. The specific malware name is less important than the sequence of actions that follows: credential harvesting, session reuse, reconnaissance, and preparation. These patterns are remarkably consistent across campaigns, even as tooling evolves.

### Detecting the Ransomware On-Ramp

Infostealers are rarely the end goal. They are the on-ramp to more destructive activity. Ransomwared is built to identify that on-ramp early, before encryption or extortion occurs.

This includes monitoring for behaviors that commonly precede ransomware deployment, such as unusual enumeration of systems, access to backup infrastructure, and changes to security-relevant configurations. Even

when attackers operate entirely through legitimate interfaces, these preparatory actions create subtle but detectable deviations from normal behavior.

By surfacing these signals early, Ransomward gives organizations time — time to revoke access, contain affected accounts, and disrupt the attack before it reaches the impact stage. In a landscape where minutes or hours can make the difference between a contained incident and a full-scale outage, this early warning capability is decisive.

## **Designed for Resilience, Not Replacement**

Ransomward is not positioned as a replacement for existing security investments. EDR, identity protection, and SIEM platforms remain foundational components of modern defense. However, infostealer-driven attacks demonstrate that no single layer can be relied upon exclusively.

Instead, Ransomward acts as a resilience layer. It assumes that other controls may be bypassed or temporarily blinded and focuses on maintaining visibility when attackers believe they are operating undetected. This philosophy mirrors the reality of modern attacks, where success often depends on exploiting gaps between tools rather than defeating them outright.

In practice, this means Ransomward complements existing telemetry rather than duplicating it. It adds context, correlation, and behavioral insight that help defenders make sense of ambiguous signals and act decisively under uncertainty.

## **Supporting Defenders, Not Overwhelming Them**

Another critical design principle is usability for security teams. Infostealer-driven intrusions generate ambiguity rather than obvious alerts. Analysts are often faced with incomplete information and difficult decisions about whether to escalate or wait.

Ransomward is designed to reduce this uncertainty. By highlighting high-risk behavioral patterns and linking them to likely attacker objectives, it helps analysts prioritize what matters most. The goal is not to generate more alerts, but to generate *clearer* ones — alerts that explain why an event is concerning and what kind of impact it may enable if left unaddressed.

This clarity is especially important in environments with limited SOC resources. When every investigation competes for attention, understanding which signals represent genuine pre-impact activity is essential.

## **Aligning With the Reality of Modern Attacks**

The broader lesson of modern infostealer operations is that attackers are no longer trying to outsmart defenses at the technical level alone. They are exploiting trust, convenience, and architectural assumptions. They are operating where defenders are least likely to look: in successful logins, authorized actions, and legitimate workflows.

Ransomward is built for this reality. It is grounded in the assumption that legitimacy can be abused and that visibility must extend beyond traditional malware indicators. By focusing on behavior, access, and intent rather than code alone, it provides organizations with a fighting chance against threats that are designed to blend in.

## **Keeping the Lights On When Others Go Dark**

Ultimately, the value of Ransomward lies in its ability to maintain visibility when attackers believe they have achieved invisibility. Infostealers create the illusion of normalcy — a quiet environment where everything appears to be functioning as intended until it suddenly is not. Ransomward challenges that illusion by watching for the subtle signs that normal activity has crossed into malicious preparation.

In a threat landscape where infostealers have become the connective tissue between initial compromise and enterprise-scale impact, this capability is no longer optional. It is a requirement for organizations that want to detect attacks before they reach the point of no return.

The reality is clear: modern attacks do not always announce themselves. They often arrive quietly, dressed in legitimacy, and wait patiently for the right moment to strike. Ransomward exists to ensure that even in those moments, defenders are not operating in the dark.