

Threat Spotlight: Storm-0249 Moves from Mass Phishing to Precision EDR Exploitation

 reliaquest.com/blog/threat-spotlight-storm-0249-precision-endpoint-exploitation

December 9, 2025



Key Points:

- Initial access broker (IAB) “Storm-0249” appears to be evolving from a general phishing group to a sophisticated post-exploitation threat, abusing legitimate Endpoint Detection and Response (EDR) processes through sideloading to conceal malicious activity as routine operation.
- While the research within this article focuses predominantly on SentinelOne’s SentinelAgentWorker.exe process, Storm-0249’s observed techniques are easily adaptable to other EDR platforms, making this a cross-industry concern.
- Successful exploitation may allow follow-on reconnaissance, command-and-control (C2) traffic, and persistence activities to go unnoticed. However, legitimate processes within common EDR tools, including SentinelOne, are not exploited, bypassed, evaded, or impaired with the techniques described herein.
- To counter these tactics, organizations must implement automated incident responses and use behavioral analytics to detect and isolate anomalies such as Dynamic Link Library (DLL) sideloading and misuse of Living off the Land binaries (LOLBins) before threats escalate.

ReliaQuest has observed “Storm-0249,” a seasoned initial access broker (IAB), adopting a more targeted and sophisticated approach to enabling ransomware attacks.

Once reliant on mass phishing, this financially motivated threat actor’s playbook now incorporates legitimate signed files, associated with common EDR tools, including SentinelOne’s SentinelAgentWorker.exe, and techniques like Dynamic Link Library (DLL) sideloading, fileless execution, and domain spoofing. These methods allow them attempt bypassing defenses, infiltrate networks, maintain persistence, and operate undetected, raising serious concerns for security teams. ReliaQuest has worked with SentinelOne to finalize this analysis.

Operating within the ransomware-as-a-service (RaaS) ecosystem, Storm-0249 specializes in stealth and persistence. By selling pre-built access to ransomware affiliates, the group accelerates the time-to-impact of attacks and lower the technical barrier for operators, making them a critical enabler of ransomware campaigns.

ReliaQuest GreyMatter is purpose-built to counter advanced tactics. By delivering unified visibility, advanced detection, and automated responses, the platform identifies tactics like DLL sideloading, fileless execution, and suspicious outbound connections originating from trusted processes employed by Storm-0249, empowering security teams to act decisively.

In this report, we’ll explore:

- How Storm-0249 has evolved its tactics with methods like DLL sideloading, Microsoft domain spoofing, and fileless PowerShell execution.
- Why abusing trusted processes like SentinelAgent.Worker.exe creates unique detection challenges.
- What gives these techniques the edge over traditional antivirus and EDR defenses.
- How GreyMatter equips security teams to detect and neutralize these threats before they escalate.

Storm-0249’s New Tactics Weaponize Trusted Processes

Storm-0249 has recently upgraded its arsenal, adding three notable techniques to its playbook:

- **Microsoft domain spoofing** to create fake domains that mimic the structure of legitimate Microsoft URLs, increasing the likelihood of victims clicking malicious links or unwittingly executing harmful code.
- **Curl-to-PowerShell piping** to evade traditional detection methods by weaponizing curl.exe, a legitimate Windows utility commonly used by IT administrators for transferring data from servers.

- **DLL sideloading targeting SentinelOne agents** to exploit the trust inherent in security software relationships, enabling attackers to evade detection with precision.

While these methods are well-known in the threat landscape, their integration into Storm-0249's operations signals an evolution toward the identity-focused and evasion-heavy tactics characteristic of mature RaaS operations.

Before diving further into these new tactics, it's worth noting the starting point of Storm-0249's recent attacks: **ClickFix**. This social engineering method manipulates users into running malicious commands through the Windows Run dialog, under the guise of fixing a legitimate technical issue. In this case, the command appears innocuous but was likely encoded to further obscure its malicious intent from both users and security tools.

Once the adversary has gained access, the attack unfolds in three key steps:

- **Abusing curl.exe:** The attack begins with leveraging curl.exe, which IT teams use daily for tasks like downloading updates or testing APIs. Because curl.exe is a trusted, built-in tool, it rarely raises red flags with security solutions.
- **Spoofed Microsoft Domains:** Attackers host the malicious script on sgcipl[.]com but prepend the URL path with /us.microsoft.com/ to falsely imitate a legitimate Microsoft domain, tricking users and some security tools into believing the content is served from an official Microsoft source.
- **Fileless PowerShell Execution:** Curl then downloads a malicious PowerShell script from the spoofed domain. Instead of saving the script to disk where antivirus might catch it, the command pipes the content directly into PowerShell's memory for immediate execution. By running entirely in memory, traditional signature-based detections miss the activity entirely.

Why This Matters

Storm-0249's ability to seamlessly chain trusted tools like curl.exe and PowerShell with convincing social engineering tactics represents a significant challenge for defenders. This low-barrier entry point bypasses both user-awareness training and traditional antivirus solutions, allowing attackers to establish a foothold with minimal resistance. Organizations relying solely on perimeter defenses or signature-based detection methods are particularly vulnerable, as these techniques leave little forensic evidence behind.

Turning Security Software Against Itself

Storm-0249 has demonstrated the ability to abuse a dangerous trust relationship within security software: By manipulating a legitimate, digitally signed SentinelOne executable to load their malicious code, the attackers made their activity look like normal security software behavior—an effective way to stay under the radar.

```

    "sha1": "3198d49a15f4c8fc0fcaffcc31b6963a512f2b80",
    "size": "262904",
    "fullPath": "C:\\Users\\[REDACTED]\\AppData\\Roaming\\SentinelOne\\SentinelAgentWorker.exe",
    "names": [
      "SentinelAgentWorker.exe"
    ]
  },
  "commandLine": "\"SentinelAgentWorker.exe\"",
  "parentProcess": {
    "pid": "27128",
    "file": {
      "size": "176128",
      "fullPath": "C:\\Windows\\System32\\msiexec.exe",
      "names": [
        "msiexec.exe"
      ]
    }
  }
},
"file": {
  "sha256": "10910179af37ba38786f5a1b59d4dd1c43b6aa512850bbd47fb0feb965b2eb5c",
  "sha1": "07c5599b9bb00feb70c2d5e43b4b76f228866930",
  "size": "3441880",
  "fullPath": "C:\\Users\\[REDACTED]\\AppData\\Roaming\\SentinelOne\\SentinelAgentCore.dll",

```

Figure 1: Legitimate and digitally signed SentinelAgentWorker executable loading a malicious DLL from the same directory.

The attack begins when a user is tricked into running a malicious MSI package downloaded from a phishing URL ([sgcipl\[.\]com/us.microsoft.com/...](http://sgcipl[.]com/us.microsoft.com/...)), which mimics a legitimate Microsoft support portal. The package leverages Windows Installer's SYSTEM privileges—the highest level of access on a Windows machine. With this elevated access, the attackers have the permissions needed to place files in protected locations and execute their malicious code with full system authority.

The MSI package contains a trojanized DLL impersonating a legitimate SentinelOne EDR component, which is strategically dropped into the user's AppData folder, a location often excluded from strict security monitoring to reduce alert noise. The malicious DLL is placed directly alongside the legitimate SentinelOne executable, setting the stage for the next phase of the attack.

When the SentinelOne binary brought along by the attacker launches, it loads the malicious DLL instead of the legitimate one sitting next to it—a technique known as DLL sideloading (Figure 1). The legitimate process does all the work, running the attacker's code, appearing as routine SentinelOne activity to security tools and bypassing detection. Behavioral monitoring is essential to spot when legitimate executables load unexpected files from unusual locations.

Why This Matters

Storm-0249’s ability to weaponize trusted software processes undermines the very security controls organizations rely on. By abusing MSI packages with SYSTEM privileges, attackers can silently deliver malware and establish persistence mechanisms that survive updates and patches. This persistence means that traditional remediation steps, like reinstalling agents or applying fixes, won’t remove their foothold.

Without behavioral monitoring to detect anomalies, attackers can remain hidden for weeks—giving them ample time to escalate their operations, deploy ransomware, and cause significant operational disruption. For CISOs, this means moving beyond reactive defenses and focusing on proactive detection strategies that expose stealthy, persistent threats.

Storm-0249’s Disguised Communication Channels

Storm-0249 has evolved its approach to command-and-control (C2) communications, pivoting away from the more detectable methods it historically used. Previously, its malware—typically dropped via phishing—established direct C2 connections, which were easier to identify because the malicious processes themselves initiated outbound traffic.

Now, the group has shifted to abusing trusted components of SentinelOne’s security software to establish C2 communication. This tactic is particularly concerning because it moves C2 traffic from suspicious, unknown processes to digitally signed, whitelisted security software.

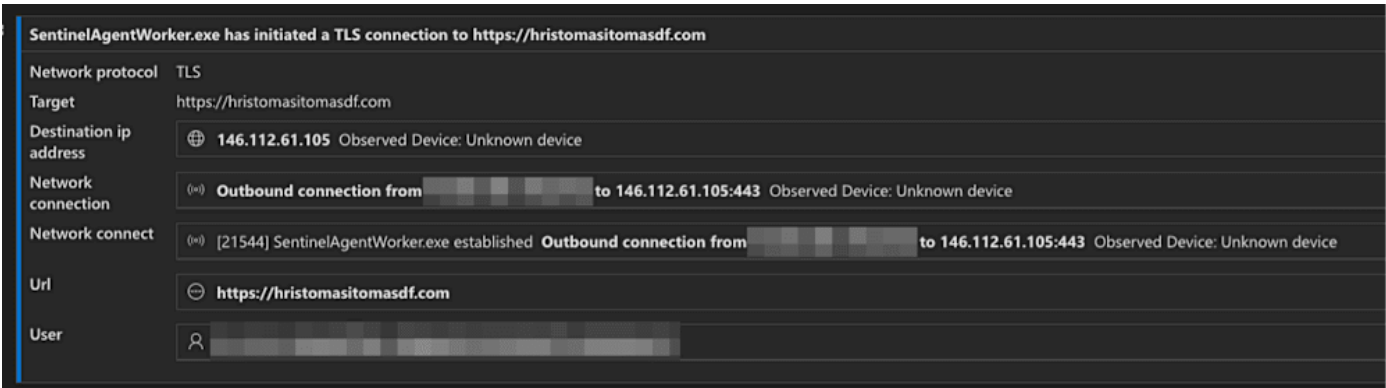


Figure 2: SentinelAgentWorker reaching out to a malicious domain

Once the malicious DLL (SentinelAgentCore.dll) hijacks the legitimate SentinelAgentWorker.exe process through DLL sideloading, Storm-0249 immediately establishes C2 channels. As shown in Figure 2, Microsoft Defender detected the compromised SentinelOne executable connecting to attacker-controlled domains registered within weeks of the attack—but still trusted it. This domain rotation strategy evades static blocklists and reputation-based filtering, which rely on aged domain intelligence.

For security teams, this presents a critical detection opportunity: Implement DNS monitoring that flags connections to newly registered domains (under 30–90 days old) originating from any process, especially trusted executables like EDR agents. Pair this with behavioral analytics that

baselines normal EDR communication patterns—expected destination IPs, connection frequency, and data volume—to surface anomalous C2 activity even when disguised as legitimate security telemetry.

Why This Matters

By funneling encrypted C2 traffic through SentinelAgentWorker.exe, Storm-0249 hides malicious communications in plain sight. To network monitoring tools, it appears as if a trusted, signed process is communicating over standard HTTPS, which is exactly how legitimate EDR telemetry behaves.

The attackers use Transport Layer Security (TLS) encryption to conceal their C2 traffic, making it unreadable to deep packet inspection tools that organizations invest in to catch threats at the perimeter. This neutralizes a significant portion of the security stack, including perimeter defenses, Secure Sockets Layer (SSL) inspection appliances, and threat intelligence feeds—all of which rely on identifying untrusted processes or unencrypted content.

As a result, attackers can securely transmit malware encryption keys and payload instructions without triggering certificate warnings or content inspection alerts. This means they operate with the same level of access and stealth as legitimate security software while exfiltrating data, mapping critical assets, and staging destructive payloads that can halt operations for weeks.

Disguising Reconnaissance as Routine Activity

Storm-0249 has found a way to exploit a critical blind spot in many organizations: Conducting reconnaissance through trusted security processes using legitimate Windows utilities that are nearly impossible to block without disrupting IT operations. Immediately after abusing the SentinelAgentWorker.exe, the attackers ran commands like **reg.exe** and **findstr.exe** to extract system-specific identifiers like **MachineGuid**—a unique hardware-based system ID.

These tools are legitimate Windows administrative utilities used daily by IT teams for system management and troubleshooting, making them an unlikely target for security restrictions. Many organizations focus on locking down PowerShell or cmd.exe but overlook these built-in tools, creating a gap that Storm-0249 strategically exploits.

This isn't just generic reconnaissance—it's preparation for ransomware affiliates. Ransomware groups like “LockBit” and “ALPHV” use MachineGuid to bind encryption keys to individual victim systems. By tying encryption keys to MachineGuid, attackers ensure that even if defenders capture the ransomware binary or attempt to reverse-engineer the encryption algorithm, they cannot decrypt files without the attacker-controlled key. Essentially, Storm-0249 is doing the groundwork, delivering critical intelligence to buyers who will deploy ransomware. This eliminates technical workarounds for victims, leaving payment as the only path to restoration.

The attackers run these commands under the signed EDR process they've brought along, in this case SentinelAgentWorker.exe, abused through DLL sideloading. Because registry queries and string searches are routine EDR operations, security tools see them thousands of times daily. Storm-0249 exploits this noise by running the code under the guise of a signed, trusted process. This approach bypasses behavior-based alerts that would typically flag cmd.exe or powershell.exe executing the same commands.

Why This Matters

Storm-0249's ability to conduct reconnaissance through trusted EDR processes marks a tactical shift across the IAB landscape. By moving beyond monitored Living off the Land binaries (LOLBins) to abusing security software itself, Storm-0249 achieves a new level of stealth.

SentinelAgentWorker.exe constantly generates registry queries as part of its normal operations, creating a noisy environment that forces teams to either tune down alerts or drown in noise. Storm-0249 capitalizes on this noise, using it as a cover to map out critical details, including: MachineGuid for encryption binding, domain membership for lateral movement, and software inventories to identify vulnerabilities.

By delivering pre-profiled targets to ransomware affiliates, Storm-0249 dramatically reduces affiliates' time-to-ransom from weeks to days. This shortens the window for defenders to respond and increases the likelihood that victims will pay a ransom before backups can restore or incident responders mitigate the attack. Traditional process-based detections built around flagging cmd.exe or powershell.exe fail to catch this activity.

How Threat Actor Abuse of EDR Tooling Raises the Stakes

From Phishing to Process Hijacking

Storm-0249 has shifted from noisy, mass phishing campaigns to precision attacks that exploit trusted processes. By using techniques like DLL sideloading, fileless execution, and domain spoofing, the group blends malicious activity into legitimate operations, bypassing traditional defenses. This shift allows ransomware affiliates to infiltrate high-value environments with stealth, prolonging access and increasing the risk of operational disruption. For businesses, this highlights the growing threat of IABs refining their methods to deliver pre-staged access, accelerating attack timelines.

The Danger of Agent Exploitation

Storm-0249's use of DLL sideloading to abuse SentinelOne's SentinelAgentWorker.exe demonstrates how the group is now weaponizing trusted security processes to evade detection. Instead of exploiting software vulnerabilities, this tactic abuses the inherent trust placed in signed,

legitimate processes. Traditional monitoring often excludes these processes from aggressive scrutiny, creating blind spots that groups like Storm-0249 can exploit.

Why Standard Remediation Fails

By using MSI packages with SYSTEM privileges, Storm-0249 ensures its footholds survive routine remediation efforts such as agent reinstalls, patches, and other routine incident response measures. This persistence is foundational to the group's business model, as it allows them to sell ransomware affiliates pre-staged, high-value access that remains intact for weeks. Standard remediation fails because it focuses on surface-level fixes, but Storm-0249's improved tactics exploit deeper trust relationships within systems.

The IAB Multiplier Effect and Cross-Platform Risk

Storm-0249's techniques, like DLL sideloading, are not limited to SentinelOne. They are easily adaptable to other EDR platforms, making this a cross-industry concern. As an IAB, Storm-0249 commoditizes these advanced tactics, selling them to ransomware affiliates who can then focus solely on deploying ransomware. This lowers the technical barrier for attackers and accelerates the spread of ransomware across sectors.

Step Up Your Defenses Against Storm-0249

How ReliaQuest Helps You Stay Ahead

Agentic AI: Traditional signature-based defenses detect malicious files and can't pick up on Storm-0249's abuse of legitimate executables like SentinelAgentWorker.exe or utilities like curl.exe. However, Agentic AI detects malicious **behavior**—such as a trusted EDR process loading an unsigned DLL from AppData, curl.exe piping directly into PowerShell, or legitimate installers retrieving payloads from newly registered domains.

GreyMatter Transit: Storm-0249 uses its initial foothold to establish C2 communication and prepare for ransomware deployment. GreyMatter Transit provides visibility into data as it moves across the network, allowing for real-time detection of anomalous traffic patterns associated with C2 channels to disposable infrastructure like sgcipl[.]com and hristomasitomasdf[.]com, even when disguised as legitimate process traffic from trusted executables.

GreyMatter Digital Risk Protection: Storm-0249 often brokers access to ransomware affiliates through dark-web and cybercriminal forums. GreyMatter Digital Risk Protection (DRP) monitors these forums for discussions about your organization, leaked credentials, and chatter about exploiting specific security tools like SentinelOne. This provides early warning to harden defenses, reset exposed credentials, or update security configurations before Storm-0249 or its ransomware customers strike.

ReliaQuest's detection rules are continuously updated using the latest relevant threat intelligence and research, enabling organizations to defend against sophisticated IAB tactics like those employed by Storm-0249 to evade traditional defenses.

Detection Rule	MITRE ATT&CK ID	Summary
Ransomware Activity - Signature Detected (000129)	TA0002: T1204.002 – Malicious File TA0040: T1486 - Data Encrypted for Impact TA0005: T1480.002 – Mutual Exclusion	IABs provide ransomware operators with pre-established footholds, persistence mechanisms, and reconnaissance data, enabling faster and more efficient attacks by reducing the technical workload for affiliates. This detection rule highlights ransomware activity flagged by endpoint protection or antivirus tools. Even when reported as "cleaned," remnants like persistence mechanisms or secondary payloads may remain, requiring thorough investigation to fully mitigate the threat.
Unmitigated Malware (000123)	TA0002: T1204.002 – Malicious File	Flags cases where antivirus fails to mitigate malicious file activity due to low-confidence antivirus detections, missing files, or the tuning of noisy programs, which allow malware to persist undetected.
Suspicious Registry Activity - Signature Detected (003257)	TA0005: T1112 – Modify Registry TA0006: T1552.002 – Credentials in Registry TA0003: T1547.001 – Registry Run Keys / Startup Folder TA0007: T1012 – Query Registry TA0004: T1547.001 – Registry Run Keys / Startup Folder	Flags the use of the Windows Registry—a hierarchical database that stores critical settings for software, devices, user preferences, and OS configurations—by adversaries like Storm-0249 for persistence or evasion, such as hiding configurations, deleting data, or other tactics for malicious purposes.

Organizations can significantly reduce their mean time to contain (MTTC) threats—from hours to just minutes—and minimize the risk of ransomware deployment by deploying these rules alongside these GreyMatter Automated Response Playbooks:

- **Isolate Host:** Quarantines compromised systems at the first sign of post-exploitation, such as reconnaissance commands or network scans, halting attacker progress before they can establish persistence.

- **Block Domain:** This Playbook can be used to sever communication with attacker infrastructure. Blocking malicious domains associated with Storm-0249's disposable infrastructure prevents C2 communication, payload retrieval, and data exfiltration critical to its attack chain.
- **Ban Hash:** This Playbook can be used to prevent the execution of known malicious files across the environment. Banning file hashes associated with trojanized DLLs like SentinelAgentCore.dll or malicious MSI packages stops Storm-0249's payloads from executing on other systems, preventing spread and persistence.

Your Action Plan

Storm-0249's ability to weaponize trusted processes like SentinelAgentWorker.exe marks a dangerous shift toward stealth and persistence. Security teams must prioritize visibility, control, and rapid response to disrupt these attacks before they escalate.

- Ensure visibility into **trusted processes** to detect suspicious activity like DLL side-loading and unexpected outbound connections. Monitoring these processes closely can help surface anomalies and contain threats before they spread.
- Enforce **strict controls on legitimate tools** like curl.exe and PowerShell to prevent attackers from abusing them for payload delivery or persistence. Limiting these tools to approved workflows reduces opportunities for exploitation.
- Strengthen **DNS monitoring and network segmentation** to counter Storm-0249's use of disposable domains and encrypted C2 traffic. Monitoring for suspicious domains and severing malicious communications reduces the risk of data exfiltration and lateral movement.

Key Takeaways and What's Next

Storm-0249's shift to exploiting trusted tools and processes like SentinelAgentWorker.exe marks a dangerous evolution in IAB tactics. Its use of DLL side-loading, fileless execution, and domain spoofing enables ransomware affiliates to infiltrate networks undetected, creating persistent footholds that are difficult to detect and even harder to remediate.

Looking ahead, these techniques are likely to inspire copycat activity among other IABs, amplifying risks across industries. As RaaS demand grows, these refined methods will spread rapidly, targeting high-value environments and exploiting blind spots in security programs.

To stay ahead, security teams must focus on proactive detection and unified monitoring strategies. The ReliaQuest GreyMatter platform provides the visibility and tools needed to detect anomalies like DLL sideloading and suspicious outbound connections, sever malicious communications, and

isolate compromised systems. With capabilities like DNS monitoring, behavioral analytics, and Automated Response Playbooks, GreyMatter empowers security teams to disrupt attacks early and minimize operational impact.

MITRE ATT&CK TTPs

ID	Tactics and Techniques	ID	Tactics and Techniques
T1566.001	Phishing: Spear Phishing Attachment	T1082	System Information Discovery
T1218	Exploit Public-Facing Application	T1027	Obfuscated Files or Information
T1059.001	Signed Binary Proxy Execution (LOLBins)	T1568.002	Dynamic Resolution: Domain Generation Algorithms
T1203	Exploitation for Client Execution	T1574.002	Hijack Execution Flow: DLL Side-Loading

IOCs

Artifact	Details
07c5599b9bb00feb70c2d5e43b4b76f228866930	Malicious DLL named "SentinelAgentCore"
423f2fcf7ed347ee57c1a3cffa14099ec16ad09c	Spear.msi
krivomadogolyhp[.]com	C2 Domain
hristomasitomasdf[.]com	C2 Domain
hamcore[.]se2	C2 Domain
sgcipl[.]com	C2 Domain
178.16.52[.]145	Malicious IP Address

172.67.206[.]124

Malicious IP Address