HwAudKiller: BYOVD EDR Bypass via Vulnerable Huawei Driver

Tax-Season Malvertising Campaign Delivers Kernel-Mode Security Tool Terminator

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-26

Key Takeaways

- A large-scale malvertising campaign active since at least January 2026 targets U.S. individuals searching for tax-related forms via Google. Fraudulent paid search ads redirect victims through commercial cloaking infrastructure to rogue ConnectWise ScreenConnect installers, ultimately deploying a kernel-mode EDR terminator named HwAudKiller.
- HwAudKiller exploits a previously undocumented vulnerability in `HWAuidoOs2Ec.sys`, a legitimately signed Huawei Device Co. laptop audio driver. By sending a target process ID through a privileged IOCTL handler, it issues `ZwTerminateProcess` from ring-0—a call that bypasses all user-mode EDR protections, including Protected Process Light (PPL).
- The driver was not present in the LOLDrivers community database or Microsoft's recommended driver block list at the time of disclosure. No prior BYOVD weaponization of this specific Huawei component had been documented in either resource, and no CVE had been assigned as of the Huntress publication [1].
- HwAudKiller targets 23 security products, including Microsoft Defender, Kaspersky, and SentinelOne, polling for matching processes every 100 milliseconds and terminating them via the kernel driver [1].
- Huntress identified over 60 instances of malicious ScreenConnect sessions tied to this campaign. Post-EDR-compromise activity includes LSASS credential dumping, network reconnaissance with NetExec, lateral movement, and deployment of redundant remote access tools [1].
- BYOVD has evolved from a capability used primarily by well-resourced threat actors into a widely accessible technique, with commercial EDR-killer offerings now reducing the technical barrier for a broader range of operators. A concurrent ESET analysis found 54 distinct EDR-killer tools exploiting 35 different legitimately signed drivers, suggesting this threat class has expanded well beyond nation-state operators [2].
- Defenders should prioritize enabling Microsoft's Vulnerable Driver Blocklist and Hypervisor-Protected Code Integrity (HVCI), enforcing EDR tamper protection, restricting local administrator rights, and alerting on unexpected kernel driver loads from temporary directories.

Background

The BYOVD Threat Landscape

The bring your own vulnerable driver (BYOVD) technique exploits a fundamental asymmetry in Windows kernel driver security: Microsoft's code signing policy validates that a driver was produced by a known vendor, but it cannot verify that the driver's code is free from exploitable flaws. An attacker who obtains local administrator rights—often through phishing, credential theft, or software exploitation—can load a legitimately signed but vulnerably coded driver. Once running at ring-0, the driver executes without the restrictions applied to user-mode processes, giving the attacker the ability to terminate protected security processes, modify kernel callbacks, or disable system telemetry.

The technique has a documented history stretching back to at least 2021, when groups including Lazarus APT and BlackByte ransomware operators were reported using it against high-value targets [2]. What has changed by 2026 is the broadening of the capability to actors who previously lacked the technical resources to develop or deploy it. A March 2026 ESET study documented 54 distinct EDR-killer tools exploiting 35 legitimately signed drivers, with commercial "EDR-killer-as-a-service" offerings including DemoKiller, ABYSSWORKER, and CardSpaceKiller available to actors without the technical depth to develop their own kernel exploits [2]. Previously weaponized drivers include RTCore64.sys (MSI Afterburner), dbutil_2_3.sys (Dell), and aswArPot.sys (Avast)—each exploited despite carrying a valid digital signature from a well-known vendor [8].

The newly documented HwAudKiller campaign illustrates an additional evolution: BYOVD is no longer confined to targeted intrusion operations. It is now being deployed in opportunistic, large-scale malvertising campaigns operating at the scale of dozens of concurrent victims per week.

The Campaign Operator and Intent

No attribution has been formally established for the HwAudKiller campaign. However, Huntress's investigation of exposed open directory listings on actor-controlled infrastructure revealed JavaScript files containing Russian-language developer comments, suggesting Russian-speaking developers were involved in constructing the tooling [1]. Whether this reflects a Russian-speaking cybercriminal group acting for financial gain, an initial access broker preparing access for sale, or a state-affiliated actor operating under commercial cover has not been established from publicly available evidence. The use of commercial-off-the-shelf RMM tools for initial access and the targeting of U.S. individuals during tax season is broadly consistent with financially motivated criminal activity.

Security Analysis

Stage 1: Malvertising via Google Ads and Commercial Cloaking

The attack chain begins with fraudulent paid search advertisements placed on Google targeting high-intent tax-season search queries, including "W2 tax form" and "W-9 Tax Forms 2026." The ads appear to have bypassed Google's automated review systems through the use of two stacked commercial cloaking services that present entirely different content to security scanners and ad reviewers than to actual victims [1].

The first cloaking layer is Adspect (`rpc.adspect.net`), which injects client-side JavaScript that fingerprints visitor characteristics—browser configuration, IP geolocation, user-agent, and behavioral signals—to classify visitors as either automated crawlers or human targets. The second layer, JustCloakIt (`cdn.justcloakit.com`, `client.justcloakit.com`), provides server-side filtering that gates delivery of the malicious payload based on the classification output from the first layer [1]. Automated scanners that do not pass both filters receive a benign-looking page, making it difficult for Google's ad quality systems to observe the malicious content that human victims encounter. The use of two independent, commercially available cloaking products in sequence—rather than custom-built infrastructure—suggests the campaign operators are sophisticated consumers of the criminal service ecosystem rather than tooling developers themselves.

Victims who pass the cloaking filters are redirected to actor-controlled sites impersonating tax filing portals, including `anukitax.com` and `bringetax.com`. These pages serve a rogue ConnectWise ScreenConnect installer, delivered as a file named `form_w9.msi` [1]. Tax-season targeting of this kind is consistent with a broader pattern of threat actors timing malvertising campaigns to coincide with periods of elevated search activity around common financial topics [10].

Stage 2: Initial Access via Rogue ScreenConnect

ConnectWise ScreenConnect (formerly ConnectWise Control) is a legitimate commercial remote monitoring and management (RMM) tool widely deployed in enterprise environments. The attackers abuse ScreenConnect's free trial tier to spin up multiple actor-controlled relay instances, providing redundancy in case any single instance is blocked or taken down. The use of a legitimate commercial product for remote access likely serves a dual purpose: it blends into environments where ScreenConnect is already in use, and may reduce the likelihood that the initial connection triggers an alert in security tooling that may flag unknown or self-built remote access frameworks more aggressively [1].

Once the rogue installer executes, a ScreenConnect session is established to actor-controlled infrastructure. From this foothold, the attacker delivers subsequent payloads through the active remote session.

Stage 3: Anti-Analysis Crypter

Through the ScreenConnect session, the attacker drops a multi-stage crypter that serves as the loader for HwAudKiller. The crypter employs an unusual anti-analysis technique: it allocates 2 GB of memory, fills it with zeroes, and then frees it. This operation appears designed to exhaust the memory of antivirus sandboxes and emulation engines—which operate with constrained memory environments—before the malicious payload reaches execution. The technique targets the memory limits commonly imposed on automated analysis systems, rather than attempting to detect specific sandbox artifacts [1].

Stage 4: HwAudKiller and the Vulnerable Huawei Driver

Once the crypter completes its anti-analysis routines, it executes HwAudKiller, the kernel-mode EDR terminator that gives the campaign its name. HwAudKiller carries an embedded copy of `HWAuidoOs2Ec.sys`, a legitimate Huawei Device Co. laptop audio driver bearing a valid digital signature. At runtime, HwAudKiller drops this driver to the system's temporary folder under the name `Havoc.sys` and registers it as a kernel service named `Havoc` [1].

The vulnerability in the driver resides in its IOCTL dispatch handler at code `0x2248DC`. When invoked, the handler accepts a 4-byte input buffer containing a process identifier (PID). It copies this value via `memcpy_s` and passes it—without validation—to a kill function that calls `ZwOpenProcess` with `PROCESS_ALL_ACCESS` (`0x1FFFFF`) to obtain a kernel handle to the target process, then immediately calls `ZwTerminateProcess` [1]. Because this call originates from ring-0, no user-mode EDR protection mechanism can intercept or block it. Protected Process Light, which prevents user-mode processes from terminating security products even with administrator rights, has no effect against a call issued from kernel context.

HwAudKiller exploits this handler by running a continuous polling loop that enumerates all running processes every 100 milliseconds. For each process whose name matches any of 23 security product entries on its internal kill list—including Microsoft Defender, Kaspersky, and SentinelOne—it sends the corresponding PID to the driver via IOCTL `0x2248DC` [1]. The driver terminates the process before user-mode defenses can respond. At a 100-millisecond polling interval, HwAudKiller is capable of terminating all 23 targeted security processes within a very short window of its execution, leaving the system without behavioral monitoring.

The driver had not been listed in the LOLDrivers community database, nor in Microsoft's recommended driver block list, prior to Huntress's disclosure [1][3]. No CVE had been assigned to the vulnerability in `HWAuidoOs2Ec.sys` as of the Huntress publication date [1]. This gap between a driver's first documented weaponization and its appearance on defensive blocklists is a recurring challenge in BYOVD defense: the signing and deployment of vulnerable driver code by legitimate vendors can pre-date adversarial discovery by years.

Stage 5: Post-Compromise Activity

With EDR products terminated, the attacker operates on the victim system without behavioral monitoring. Huntress observed a consistent post-compromise pattern across the 60+ ScreenConnect sessions attributed to this campaign: LSASS credential dumping using standard credential extraction techniques, network reconnaissance executed through NetExec, lateral movement to additional hosts on the victim network, and the deployment of multiple additional remote access tools to ensure persistence if any single access vector is discovered and removed [1].

The credential dumping and lateral movement activity is consistent with either a pre-ransomware staging pattern—where access is systematically developed before deployment of a ransomware payload—or with the operational profile of an initial access broker preparing network access for sale to downstream actors. The investigation had not conclusively established which endpoint the campaign was building toward at the time of Huntress's disclosure.

Recommendations

Immediate Actions

Organizations should take the following actions immediately in response to this campaign. First, block the known indicators of compromise at the network perimeter. Malicious domains identified by Huntress include `anukitax.com`, `bringetax.com`, `bjtrck.com`, `fioclouder.com`, `friugrime.com`, `grinvan.com`, `gripsmonga.sbs`, and `jcibj.com`. Cloaking infrastructure that should be blocked includes `cdn.justcloakit.com`, `client.justcloakit.com`, and `rpc.adspect.net` [1].

Second, audit any ConnectWise ScreenConnect deployments for unauthorized trial instances. Huntress specifically recommends treating any ScreenConnect trial instance—particularly those exhibiting `instance-*` relay patterns not matching known corporate deployments—as suspicious [1]. In environments where RMM traffic is pre-approved at the perimeter, it may receive less inspection than other outbound connections—a gap that this campaign explicitly exploits.

Third, hunt for the driver artifact `HWAuidoOs2Ec.sys` dropped as `Havoc.sys` in system temporary directories, and for a kernel service named `Havoc`. File hashes for key campaign samples are documented in Huntress's published indicators [1].

Short-Term Mitigations

Technical controls that operate at the kernel boundary address BYOVD attacks most directly, since the attack itself exploits kernel-mode access. Organizations should verify that Microsoft's Vulnerable Driver Blocklist is active on all Windows endpoints. This policy is enabled by default on Windows 11 22H2 and later but may be disabled by third-party security products or enterprise configuration changes; its status should be confirmed explicitly rather than assumed [4]. The Attack Surface Reduction rule "Block abuse of exploited vulnerable signed drivers" (GUID: `56a863a9-875e-4185-98a7-b882c64b5ce5`) provides an additional layer of defense and should be enabled in block mode where testing confirms it does not disrupt legitimate operations [4][9].

Hypervisor-Protected Code Integrity (HVCI), which uses the Windows hypervisor to restrict kernel-mode code execution to drivers verified against a policy, significantly raises the bar for BYOVD attacks by preventing the loading of drivers not present on the approved list. HVCI should be evaluated for deployment across managed endpoints, with particular priority for systems that handle sensitive credentials or that run security operations infrastructure. Credential Guard should similarly be enabled to protect LSASS from the credential dumping stage that follows EDR termination in this campaign's post-compromise pattern.

EDR tamper protection—the feature that prevents even administrator-privileged processes from stopping or uninstalling the EDR agent—is a necessary but insufficient defense. BYOVD attacks are designed specifically to defeat tamper protection by escalating termination to kernel mode. Tamper protection reduces the attack surface from all privileged actors to only those who can also load kernel drivers, making it valuable, but it should not be treated as a complete defense against this threat class.

Strategic Considerations

The malvertising entry vector in this campaign reflects a broader pattern of threat actors abusing the commercial digital advertising ecosystem to reach victims at scale [10]. Organizations cannot rely solely on user training to mitigate this risk: the fraudulent Google Ads in this campaign appeared in top search results for common, expected queries during tax season, and their malicious nature was invisible to automated systems because of the commercial cloaking stack. DNS-layer filtering and browser-based execution controls reduce exposure to this attack vector independently of user behavior, complementing awareness programs that may not reliably detect sophisticated malvertising.

The campaign's abuse of ScreenConnect's trial tier illustrates the broader challenge posed by legitimate commercial RMM tools. The same software that enables IT operations also provides attackers with a signed, trusted binary for remote access that may not trigger security product alerts. Organizations should maintain an explicit inventory of authorized RMM tools, monitor for any RMM processes connecting to relay infrastructure not matching known corporate deployments, and consider restricting inbound and outbound RMM connections to known-good addresses at the network perimeter.

More broadly, the widespread adoption of BYOVD as documented by the concurrent ESET study warrants treatment as a systemic endpoint security challenge rather than a campaign-specific response item. The LOLDrivers project (loldrivers.io) maintains a community-sourced database of vulnerable drivers that can be integrated into threat hunting workflows and endpoint blocking policies [8]. Security teams should evaluate integrating LOLDrivers signatures into their detection stack as a standing control, not merely in response to individual campaign disclosures.

CSA Resource Alignment

The HwAudKiller campaign implicates several areas of CSA framework guidance that organizations can apply in constructing their response and longer-term defensive posture.

CSA's **AI Control Matrix (AICM)**, as a superset of the Cloud Controls Matrix (CCM), addresses endpoint security controls including requirements for malware protection, tamper resistance, and event logging. The campaign's ability to terminate 23 security products simultaneously underscores the importance of AICM controls in the Threat and Vulnerability Management (TVM) domain, particularly those governing the integrity of security tooling itself. Organizations attesting against AICM should verify that their endpoint protection controls include kernel-level tamper protection verification, not merely user-mode attestation.

CSA's **Zero Trust guidance** is directly applicable to the post-compromise lateral movement phase of this campaign. The Huntress report documents that once EDR was blinded, attackers used NetExec for reconnaissance and moved laterally across victim networks. A Zero Trust architecture that enforces continuous identity verification, micro-segmentation, and least-privilege access to internal resources can limit the blast radius of a successful EDR bypass even when endpoint defenses fail. CSA's Zero Trust Working Group provides implementation guidance on applying these principles to heterogeneous enterprise environments [5].

CSA's **Top Threats to Cloud Computing** report identifies "Insecure Interfaces and APIs" and "Insufficient Identity, Credential, Access, and Key Management" among its top cloud security risks. The credential dumping and lateral movement activity documented in this campaign translates cloud threats into on-premises reality: stolen credentials harvested from LSASS are frequently the mechanism by which attackers escalate from a single endpoint compromise to a network-wide incident, including unauthorized access to cloud management consoles and SaaS services authenticated via enterprise single sign-on [6].

Finally, CSA's guidance on **managing privileged access** directly addresses the precondition that BYOVD exploits: local administrator rights [7]. BYOVD requires that the attacker already holds sufficient privileges to load a kernel driver, which in practice means local administrator access. Organizations that enforce the principle of least privilege and restrict local administrator rights to only those accounts and processes that require them significantly reduce the population of attacker-controlled contexts from which a BYOVD attack could be launched.

References

[1] Anna Pham, "From W-2 to BYOVD: How a Tax Search Leads to Kernel-Mode AV/EDR Kill," Huntress, March 2026. https://www.huntress.com/blog/w2-malvertising-to-kernel-mode-edr-kill

[2] "54 EDR Killers Use BYOVD to Exploit 35 Signed Vulnerable Drivers," The Hacker News, March 2026. https://thehackernews.com/2026/03/54-edr-killers-use-byovd-to-exploit-34.html

[3] "Tax Search Ads Deliver ScreenConnect Malware Using Huawei Driver to Disable EDR," The Hacker News, March 24, 2026. https://thehackernews.com/2026/03/tax-search-ads-deliver-screenconnect.html

[4] "Microsoft Vulnerable Driver Blocklist," Microsoft, 2026. https://learn.microsoft.com/en-us/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules

[5] Cloud Security Alliance, "Zero Trust Working Group," CSA, 2025. https://cloudsecurityalliance.org/research/working-groups/zero-trust/

[6] Cloud Security Alliance, "Top Threats to Cloud Computing: Deep Dive 2025," CSA, May 2025. (URL unavailable at time of review; available via CSA research catalog at cloudsecurityalliance.org)

[7] Cloud Security Alliance, "Managing Privileged Access in the Cloud-First World," CSA, January 2026. (URL unavailable at time of review; available via CSA research catalog at cloudsecurityalliance.org)

[8] "LOLDrivers – Living Off The Land Drivers," Community project, 2026. https://www.loldrivers.io/

[9] "Blocking BYOVD Techniques to Prevent AV/EDR/XDR Bypasses," Halcyon, 2026. https://www.halcyon.ai/blog/blocking-byovd-techniques-to-prevent-av-edr-xdr-bypasses

[10] "When Tax Season Becomes Cyberattack Season: Phishing and Malware Campaigns Using Tax-Related Lures," Microsoft Security Blog, March 19, 2026. https://www.microsoft.com/en-us/security/blog/2026/03/19/when-tax-season-becomes-cyberattack-season-phishing-and-malware-campaigns-using-tax-related-lures/

