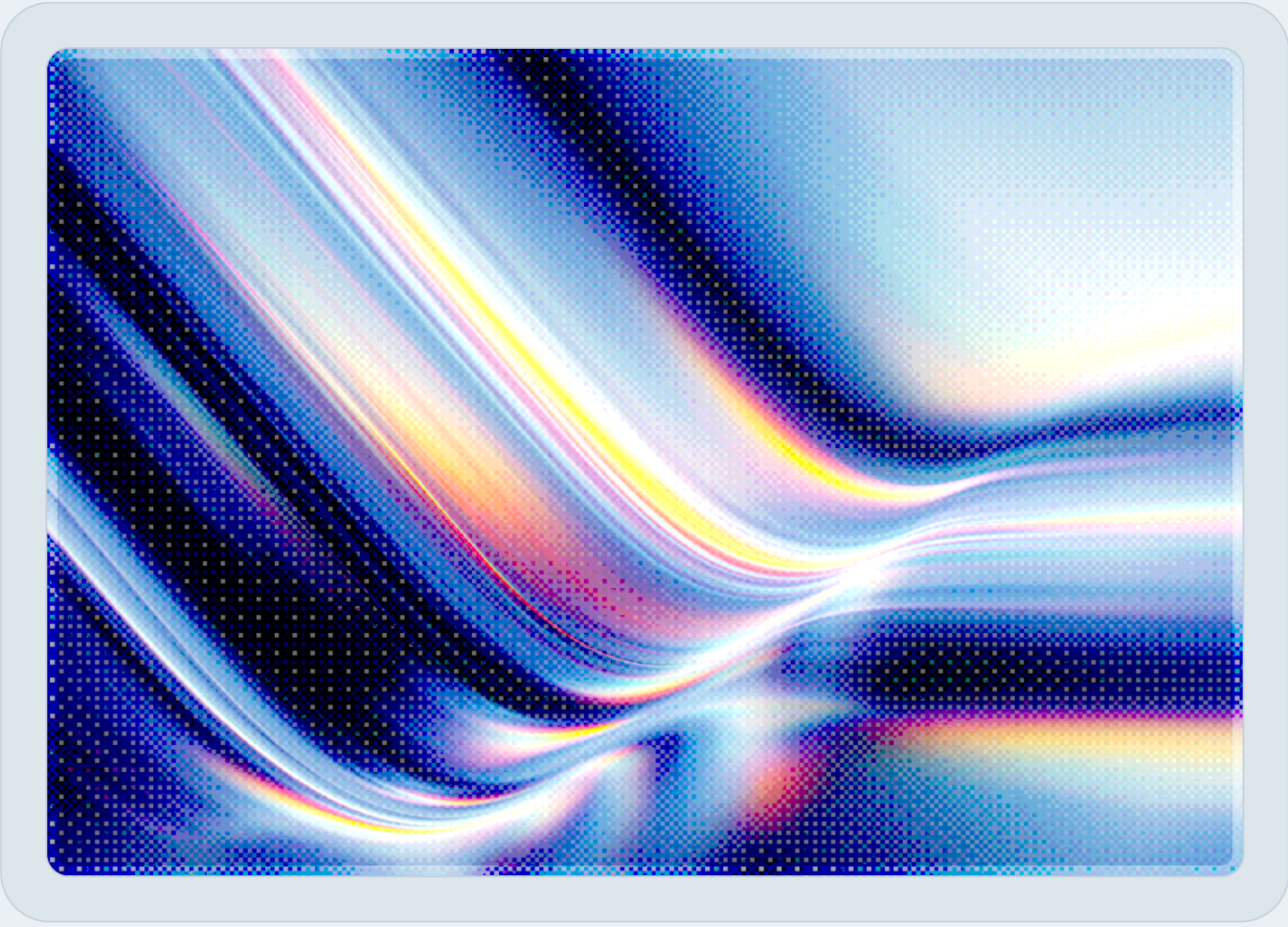
CSAI Foundation | Cloud Security Alliance

Nimbus Manticore's NightLedger Backdoor and Covert Relay Network

2026-07-29

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Kaspersky's Securelist and The Hacker News disclosed on July 28-29, 2026 that Nimbus Manticore — an Iranian, IRGC-linked espionage group tracked under a long list of aliases including UNC1549, Mirage Kitten, Smoke Sandstorm, Subtle Snail, and GalaxyGato — has deployed a previously undocumented Windows backdoor, NightLedger, alongside two custom WebSocket tunneling tools, BridgeHead and ArcBridge [1][2]. NightLedger arrives via DLL side-loading, masquerading as the legitimate Windows library SspiCli.dll and abusing a search-order hijacking flaw in AppVShNotify.exe to execute with the trust of a signed system process [2]. Its command set covers reconnaissance, process control, file exfiltration and staging, screenshot capture, and diagnostic-log collection, communicating with operator infrastructure over HTTPS using a delimiter scheme that Kaspersky describes as similar to the one used by the group's earlier TWOSTROKE backdoor [1][2]. BridgeHead and ArcBridge convert compromised hosts into relay nodes, tunneling operator-issued TCP traffic through the victim's network so that outbound connections appear to originate from the target organization rather than from Nimbus Manticore's own infrastructure [1]. The disclosed victimology — Egypt, government and small-business networks in Jordan and Tanzania, aviation operators in Pakistan, telecommunications firms in Ethiopia, and financial-sector entities in Burkina Faso — extends the group's footprint well beyond the Western aerospace, defense, and telecommunications targets documented in CSA's May 2026 research note on the same actor's MiniFast backdoor [3]. Neither disclosing source has confirmed the initial access method for this specific campaign, though both note the actor's established history of recruitment-themed phishing; organizations in the affected sectors and regions should nonetheless treat DLL search-order anomalies on Windows endpoints, unexpected outbound WebSocket traffic, and recruitment-themed phishing lures as priority hunting leads, consistent with the immediate actions detailed below.

Background

Nimbus Manticore is a long-tracked Iranian threat actor assessed with moderate-to-high confidence across multiple vendors to operate in support of Islamic Revolutionary Guard Corps (IRGC) intelligence objectives. Google's Mandiant division, which tracks the group as UNC1549 and has also used the label Smoke Sandstorm, documented the actor's activity as early as June 2022, when it ran fake recruiting campaigns against aerospace, aviation, defense, and thermal-imaging companies in Israel and the United

Arab Emirates, with secondary targeting in Turkey, India, and Albania [6]. Those early operations relied on convincing fake job portals — sites such as careers-finder[.]com and 1stemployer[.]com — paired with credential-harvesting pages that impersonated Boeing, Teledyne FLIR, and DJI, and the group built out an extensive command-and-control footprint of more than 125 Azure-hosted subdomains designed to blend into legitimate cloud traffic [6]. By 2023 the group's targeting had broadened from a regional Middle East focus to the global aerospace and defense supply chain [6], a pattern consistent with the further geographic diversification documented in this disclosure.

That expansion continued into 2026. CSA's own research documented an escalation between February and April 2026, when Nimbus Manticore deployed a new backdoor, MiniFast, against defense, aerospace, and telecommunications organizations in the United States, Western Europe, and the Middle East — a campaign whose timing coincided with the onset of U.S. and Israeli military operations against Iran on February 28, 2026 [3]. That earlier note flagged coding characteristics in MiniFast consistent with generative-AI-assisted development, including unusually verbose error handling and modular code organization, and situated the finding within a broader pattern of Iranian state threat groups — alongside MuddyWater and Handala Hack — adopting AI tooling to accelerate malware production under operational pressure [3].

The NightLedger disclosure represents a further, and geographically distinct, phase of this activity. Rather than concentrating on Western defense and aerospace targets, the toolset documented by Kaspersky and corroborated by The Hacker News surfaced against government and private-sector organizations across the Middle East, Africa, and South Asia, spanning sectors as varied as aviation, telecommunications, and financial services [1][2]. This pattern suggests Nimbus Manticore is running parallel operational tracks — one directed at high-value Western and Israeli defense-industrial targets, and another sustaining regional espionage against government and commercial targets closer to Iran's immediate sphere of interest — rather than a single, narrowly scoped campaign. The group has relied on tailored recruitment-themed social engineering as a documented initial-access vector since at least 2022, though the exact entry point for the NightLedger campaign itself has not been confirmed by either disclosing source. That the lure category has remained part of the group's toolkit for several years is consistent with its continued effectiveness, though persistence alone does not rule out other explanations, such as lower retooling cost or sufficiency against less-defended regional targets, even as the group's backdoors and infrastructure have evolved considerably.

Security Analysis

NightLedger: A New Windows Backdoor Built for Persistence

NightLedger is delivered through DLL side-loading, a technique that abuses the Windows DLL search order so that a legitimate, signed executable unwittingly loads an attacker-supplied library instead of the genuine system component. Kaspersky's analysis identified the malicious DLL masquerading as SspiCli.dll, a core Windows security support provider library, and found that it is loaded through a search-order hijack of AppVShNotify.exe, a legitimate Microsoft Application Virtualization component [2]. Because the hosting process is a trusted, signed Microsoft binary, this delivery method allows NightLedger to execute with reduced scrutiny from security tooling that whitelists or under-monitors well-known system executables — a persistent challenge for endpoint detection that relies heavily on process reputation rather than behavioral analysis of loaded modules.

Once resident, NightLedger communicates with its command-and-control infrastructure over HTTPS, parsing instructions using a custom delimiter sequence that Kaspersky describes as similar in approach to the scheme used by TWOSTROKE, a backdoor previously attributed to the same actor [1][2]. This structural continuity across backdoor generations is a useful analytic signal: even as Nimbus Manticore retires and replaces individual implants, underlying protocol design choices tend to persist, offering defenders a basis for retrospective hunting once a new tool's C2 grammar is understood. The command set NightLedger supports is broad enough to serve as a general-purpose espionage platform rather than a narrowly scoped implant.

Capability	Description
Host and user reconnaissance	Collects local user identity, hostname, and system information
Process discovery and execution	Enumerates running processes; launches and terminates processes on command
File operations	Downloads, uploads, copies, and deletes files on the compromised host
Directory and drive enumeration	Lists local drives and directory contents for operator situational awareness
Screenshot capture	Captures the victim's display for visual reconnaissance

Capability	Description
Diagnostic log collection	Retrieves NetSetup.log, a Windows domain-join diagnostic file useful for mapping victim network architecture
DLL loading	Loads additional attacker-supplied libraries into memory for follow-on tooling
Beacon interval modification	Adjusts C2 check-in frequency, likely to evade time-based network anomaly detection

Source: [1][2]

BridgeHead and ArcBridge: Turning Victims Into Relay Infrastructure

The second, and arguably more operationally significant, element of this disclosure is Nimbus Manticore's investment in covert tunneling infrastructure. Rather than routing all traffic through infrastructure the group directly owns, BridgeHead and ArcBridge convert compromised endpoints into relay nodes: the operator runs client tools on their own systems, and the resulting TCP traffic is tunneled through the victim's machine so that it appears, to any network observer downstream, to originate from the victim's own network [1]. This model complicates both network-based attribution and defensive response, since traffic destined for a secondary target may transit a compromised but otherwise uninvolved organization's IP space.

BridgeHead, delivered as a DLL named unbcl.dll and observed against targets in Egypt and Pakistan, establishes WebSocket connections over HTTPS and supports Negotiate and NTLM authentication against corporate proxy infrastructure, allowing it to tunnel out through enterprise environments that require proxy authentication for internet access [2]. It implements SOCKS5 proxy functionality over a binary wire protocol supporting connection establishment, data relay, and keepalive messages, and it performs per-target username validation before activating — a straightforward but effective anti-sandbox measure, since automated malware analysis environments rarely replicate a specific victim's actual Windows usernames [2]. ArcBridge, observed in an April 2026 campaign against Middle East targets, serves a similar tunneling function but stores its command-and-control host, port, and implant identifier in an embedded configuration block, and supports operator-issued commands for proxy creation and DNS resolution, with the server rather than the implant initiating tunnel setup [2].

Tool	Delivery	Protocol	Distinguishing Features
BridgeHead	unbcl.dll	WebSocket over HTTPS, SOCKS5	Negotiate/NTLM proxy authentication; per-target username validation
ArcBridge	Standalone WebSocket implant	WebSocket, embedded C2 config	Server-initiated tunnel management; DNS resolution and proxy-creation commands

Source: [1][2]

Infrastructure Evolution and Initial Access

Nimbus Manticore's historical C2 infrastructure leaned heavily on Microsoft Azure, with Mandiant having previously catalogued more than 125 Azure-hosted subdomains used to blend malicious traffic with legitimate cloud services [6]. The NightLedger campaign shows a deliberate shift away from that pattern toward Cloudflare-backed domains, a change that Kaspersky attributes to a desire to complicate attribution while maintaining resilient command-and-control communications [2]; this may also reflect a broader industry pattern of threat actors favoring content-delivery-network fronting over cloud-native subdomains, though neither disclosing source ties this specific shift to prior vendor takedown pressure. The exact initial access method for this campaign has not been confirmed by either source: both Kaspersky and The Hacker News note only that the actor is known to employ recruitment-themed phishing lures impersonating trusted employers and hiring platforms, in this instance potentially paired with lookalike videoconferencing pages that redirect targets to malicious archives hosted on third-party file-sharing services rather than attacker-controlled infrastructure — a pattern that, if used here, would reduce the number of indicators unique to the campaign [1][2]. The disclosure also arrives alongside broader reporting on Iranian threat actors adopting more diverse command-and-control channels, including a framework dubbed Cavern that abuses the Microsoft Graph API for covert communications — a reminder that the tooling documented here represents one strand of a wider and still-evolving Iranian offensive cyber ecosystem rather than an isolated development [1].

Recommendations

Immediate Actions

Security teams, particularly those in aviation, telecommunications, financial services, and government sectors across the Middle East, Africa, and South Asia, should hunt for DLL side-loading indicators associated with AppVShNotify.exe and any unexpected SspiCli.dll instances outside the standard System32 path, since a mismatched file location or hash for either component is a high-confidence signal of compromise. Network defenders should review outbound HTTPS traffic for WebSocket upgrade requests to newly registered or reputation-thin Cloudflare-fronted domains, and should treat any host observed proxying SOCKS5 traffic on behalf of an internal process as a priority incident for investigation. Email security teams should also brief staff involved in hiring, recruitment, and external-facing communications on the actor's documented lure pattern — fake job platforms and lookalike videoconferencing invitations that redirect to archive downloads on third-party file-sharing sites — since this remains the group's best-established historical initial-access vector, even though the confirmed entry point for this specific campaign has not been determined.

Short-Term Mitigations

Because NightLedger's persistence depends entirely on DLL search-order hijacking, organizations should deploy or tune endpoint detection rules that flag DLL loads from non-standard paths by signed system executables, rather than relying solely on signature-based detection of the payload itself, which will change across campaigns. Application control policies that restrict which DLLs a given signed binary is permitted to load — where feasible on Windows environments supporting such controls — directly address this delivery mechanism rather than the downstream backdoor. Organizations with any exposure to the identified victim sectors or regions should also extend logging on proxy authentication events, since BridgeHead's use of Negotiate and NTLM authentication against corporate proxies means successful C2 tunneling may otherwise blend into ordinary authenticated proxy traffic. Retrospective log review for HTTPS sessions containing the delimiter pattern associated with NightLedger and its predecessor TWOSTROKE may surface earlier, undetected compromise.

Strategic Considerations

The relay-node model implemented by BridgeHead and ArcBridge illustrates a broader trend in which compromised victim infrastructure is repurposed as a stepping stone against downstream targets, meaning organizations should not assume that an absence of direct financial or data-theft impact

indicates low severity; a compromised host tunneling traffic on Nimbus Manticore's behalf carries reputational and potential legal exposure even where no data was exfiltrated from the host itself. The group's sustained, multi-year investment in recruitment-themed social engineering — documented since 2022 and the actor's best-established lure pattern, even though the confirmed initial access vector for this specific campaign remains undetermined — argues for treating hiring-process-adjacent phishing as a standing, rather than seasonal, risk category, with dedicated awareness training for HR, recruiting, and any staff who routinely receive unsolicited external communications framed as career opportunities. Finally, the geographic and sectoral broadening documented in this disclosure, set against CSA's earlier reporting on the same actor's Western-focused MiniFast campaign, suggests organizations should not calibrate their threat model for Nimbus Manticore solely on regional or sector-based assumptions; the group has demonstrated the operational capacity to run concurrent campaigns against both high-value Western defense targets and regional government and commercial targets closer to Iran.

CSA Resource Alignment

This disclosure extends CSA's own prior coverage of the same threat actor. CSA's May 2026 research note, "Nimbus Manticore: Iran's AI-Assisted Backdoors Target Western Sectors," documented the group's MiniFast backdoor and the operational pressure that likely drove AI-assisted malware development during the February-April 2026 campaign against Western defense, aerospace, and telecommunications organizations [3]. Read together, the two disclosures show a single, IRGC-linked actor operating parallel toolchains and target sets, and organizations that acted on the endpoint detection and behavioral-monitoring recommendations in the earlier note should extend that same posture to the DLL side-loading and WebSocket-tunneling indicators documented here.

CSA's June 2026 threat intelligence report on VerdantBamboo's deployment of the BRICKSTORM backdoor and its BSD variant offers a directly relevant technical parallel, despite the differing threat actor and nexus [4]. Both campaigns rely on WebSocket-based command-and-control channels and SOCKS5 proxy functionality to tunnel traffic through compromised infrastructure while blending with ordinary HTTPS flows, and that note's mapping of covert relay and tunneling behavior to the MAESTRO threat modeling framework's Layer 1 (Infrastructure and Compute) and to the AI Controls Matrix (AICM) applies with equal force to BridgeHead and ArcBridge. Organizations that have already scoped edge-appliance and relay-node behavior into their MAESTRO threat models following the VerdantBamboo disclosure should extend that scope to endpoint-hosted relay tooling of the kind documented in this note.

Because NightLedger's initial foothold depends on DLL search-order hijacking of a trusted, signed process, the AI Controls Matrix (AICM v1.1) — as the superset of the Cloud Controls Matrix — provides the relevant control baseline for the application-integrity and threat-and-vulnerability-management domains implicated here, including guidance on application allowlisting, integrity monitoring for system binaries, and behavioral endpoint detection that does not rely solely on payload signatures [5]. The confirmed victims in this disclosure are not documented as AI/ML-specific environments, but the underlying control gap — signed-process trust without independent integrity verification — applies equally wherever Windows infrastructure supports AI training, inference, or data pipeline workloads, and organizations extending AICM controls into such on-premises estates should treat this campaign as a concrete illustration of why signed-process trust alone is an insufficient control.

References

[1] The Hacker News. "Nimbus Manticore Deploys NightLedger and Turns Victim Systems Into Covert Relays." The Hacker News, July 28, 2026.

[2] Kaspersky Securelist. "Mirage Kitten's new malware set: NightLedger backdoor and two tunneling tools." Securelist, July 2026.

[3] Cloud Security Alliance. "Nimbus Manticore: Iran's AI-Assisted Backdoors Target Western Sectors." CSA AI Safety Initiative, May 26, 2026.

[4] Cloud Security Alliance. "VerdantBamboo Deploys BRICKSTORM BSD Variant on Linux Appliances." CSA AI-Assisted Rapid Research, June 8, 2026.

[5] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, 2026.

[6] Google Cloud. "When Cats Fly: Suspected Iranian Threat Actor UNC1549 Targets Israeli and Middle East Aerospace and Defense Sectors." Google Cloud Blog, February 2024.