

Mirage Kitten targets Middle East and Africa region with new malware

By Omar Amin, Vasily Berdnikov

Published: 2026-07-28 · Archived: 2026-09-08 02:01:37 UTC

Introduction

Mirage Kitten – also known as UNC1549, Smoke Sandstorm, and Nimbus Manticore – is an advanced persistent threat (APT) group focused on cyber-espionage operations against aerospace, aviation, defense, and telecommunications sectors across the Middle East and Africa, using highly targeted spear-phishing campaigns, fake recruitment portals, and custom multi-stage malware to gain persistent access and exfiltrate sensitive data.

During recent threat research, we identified a previously undocumented malware set developed and used by Mirage Kitten. The toolset includes NightLedger, a new Windows backdoor for reconnaissance, command execution, file operations, process discovery, and screenshot capture; and two custom WebSocket-based tunnelers, ArcBridge and BridgeHead, for covert network access and operator-controlled tunneling.

Technical details

Although the initial access vector remains unclear for most malware samples observed in this activity, we saw BridgeHead being deployed during post-exploitation activities in victim environments in Egypt and at a Pakistan-based aerospace and aviation organization. The deployment followed targeted spear-phishing activity consistent with tradecraft we recently documented as part of our private [threat intelligence reporting service](#) and publicly reported by [Unit 42](#) and [Check Point Research](#), including the use of highly tailored social engineering lures against selected targets. These lures included recruitment-themed content impersonating trusted brands and hiring platforms, as well as lookalike videoconferencing pages that redirected victims to malicious archives hosted on third-party file-sharing services.

NightLedger backdoor

NightLedger is a recently identified Windows backdoor that we attribute to Mirage Kitten based on code and behavioral similarities to the historical implants developed and used by the group. The implant masquerades as `SspiCli.dll` and appears to be designed for DLL search-order hijacking, targeting a legitimate `AppVShNotify.exe` binary. While `AppVShNotify.exe` does not directly import `SspiCli.dll`, it imports `RPCRT4.dll`, which can delay-load `SspiCli.dll` when it invokes an RPC API that requires authentication. This allows a co-located malicious `SspiCli.dll` to be loaded while forwarding expected exports to the legitimate DLL.

When started, the malicious DLL creates the mutex `A8215357-F99A-44FE-BC65-D8F0434B0C03` to enforce a single running instance. If the mutex already exists, it exits immediately.

NightLedger periodically contacts its C2 over HTTPS, issuing an HTTP GET request to the `/edfcvfgbhnjmkqwasderfgg` endpoint at the `realhealthshop[.]com` domain, and uses `tjconsultingservices[.]com` as a fallback C2.

When a valid C2 response is received, the implant tokenizes the payload using the custom delimiter (`#####`) and passes the parsed fields to its command dispatcher. From a development standpoint, this is similar to TWOSTROKE, a backdoor attributed to the same APT and previously documented by [GTIG](#), whose C2 response is hex-encoded and uses (`@##@`) as a field separator.

NightLedger supports the following commands:

Command ID	Description
1	Gather user and host identity information
3	Execute a process/program
17	List directories
20	Download a file to the infected system
25	Gather host and network information
27	Copy a file
30	Update beacon interval
36	Take a screenshot
43	Load a DLL
56	Kill a process
62	Delete a file
69	Terminate thread
70	Upload file to C2 server via POST request to <code>/qasxcdfvgbhnmyuioplkhnj</code>
75	Enumerate logical drives
90	List processes
93	Collect <code>C:\Windows\debug\NetSetup.log</code> together with process-list output. <code>NetSetup.log</code> is a Windows diagnostic log generated under <code>C:\Windows\debug\</code> during domain/workgroup join, unjoin, and related network setup operations.

Command output is returned to the C2 via an HTTP POST request to `/wsdefvbnhyuijklmbgfrtt`.

BridgeHead – a WebSocket tunneler

During our investigation, we encountered a tunnel proxy deployed as `unbcl.dll` in the `%LocalAppData%\Microsoft\VisualStudio` directory on a machine in Egypt. We also identified a similar deployment in a Pakistan-based environment, where the tunneling tool was stored as `C:\program files (x86)\univpn\promote\libwinpthread-1.dll`. The malware dynamically loads `advapi32.dll`, resolves `GetUserNameA`, retrieves the current Windows username, converts it to lowercase, and searches for a specific substring in it. This behavior suggests prior reconnaissance was performed within the internal network and the username check is needed to make sure it runs on a specific machine. This is potentially intended to prevent execution of the standalone malware sample inside virtual analysis systems. If the substring is not found, the function returns silently without activating.

If the username check was successful, the tunneler establishes an HTTPS WebSocket connection as follows:

1	GET /connect HTTP/1.1
2	Host: smartconnect.azurewebsites.net
3	Upgrade: websocket
4	Connection: Upgrade
5	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36 Edg/86.0.622.38

The server responds with HTTP 101 (Switching Protocols) to complete the WebSocket upgrade. After the upgrade, the client sends a binary WebSocket message containing the literal string `"token"` as authentication. The server must respond within 10 seconds, or the connection is dropped and retried with exponential backoff.

The malware's next action depends on the HTTP response returned by the server:

HTTP response	Description
407 (Proxy Auth Required)	Queries supported auth schemes via <code>WinHttpQueryAuthSchemes</code> , selects Negotiate (0x10) or NTLM (0x2) in that exact order, sets Windows SSO credentials (null username/password), retries up to 3 times.
101 (Switching Protocols)	Success. Proceeds to WebSocket upgrade and authentication.
Other	Connection failed. Closes all handles, enters backoff.

This implementation closely mirrors the enterprise proxy traversal logic seen in the backdoor we track internally as Retrograde, which overlaps with tooling publicly reported as [MiniFast/MiniUpdate](#), attributed to the same APT group. The implant is designed to operate through corporate proxy environments by handling HTTP 407

responses, negotiating Windows-integrated proxy authentication with Negotiate preferred over NTLM, retrying with the current user's SSO context, and falling back to exponential C2 connection retry logic capped at 60 seconds.

Once the WebSocket channel is established and authenticated, the implant functions as a full SOCKS5 tunnel proxy. The C2 server initiates all tunnel connections by sending binary commands over the WebSocket; the implant simply forwards traffic between server-specified targets and the WebSocket channel. This makes it a relay node: the operator runs tools server-side, and all resulting TCP traffic is tunneled through the victim's machine as if originating from the victim's network.

All tunnel communication uses a fixed binary wire format:

Offset	Size	Field	Encoding
0	1	type	Message type (1–9)
1	4	connId	Tunnel connection identifier
5	1	flags	Status or error indicator
6	2	dataLen	Payload length
8	var	payload	Message data

Every message is at least 8 bytes. Seven message types are actively used:

Type	Name	Direction	Description
1	CONNECT	Server -> Client	Open a new TCP tunnel to a SOCKS5 target address
2	CONNECT_RESPONSE	Client -> Server	Confirm the connection was established
3	DATA	Bidirectional	Relay TCP traffic through the tunnel
4	DISCONNECT	Bidirectional	Close a tunnel connection
5	PING	Bidirectional	Keepalive probe, sent every 30 seconds by timer
6	PONG	Bidirectional	Keepalive reply
9	FLOWCTRL	Bidirectional	Throttle data flow to prevent buffer overrun

The `CONNECT` payload specifies where the implant should open a TCP connection. The target address is encoded in SOCKS5 format and consists of a single type byte, followed by the address and a 2-byte destination port:

Type byte	Description
0x01	IPv4 address (4 bytes)

0x03	Domain name (1-byte length + string)
0x04	IPv6 address (16 bytes)

Notably, in the process of threat hunting, we detected another variant (MD5: C832ECD135781B11F59E3FFFB3D2B6AC) that shares the same dynamic-resolve stub pattern. This variant communicates with `businessmixture.com/blog` over WSS on port 443, and not through Microsoft Azure. Still, it implements the same technique of limiting execution to a specific username on the infected machine by hardcoding a 3-character control value that must appear as a substring in the lowercased Windows username retrieved via `GetUserNameA` . If the match fails, the implant silently exits, confirming per-target tailoring of each deployed binary.

ArcBridge: another WebSocket tunneling tool

ArcBridge is another WebSocket tunneling tool developed and used by Mirage Kitten. We first identified it in April 2026 in activity targeting victims in the Middle East. The malware creates a mutex named `F56E68DA-4A89-46B4-9AC8-7290A7651000` to enforce single-instance execution. The use of a UUID-like mutex name is consistent with the NightLedger backdoor described earlier. The malware contains an embedded configuration block that stores the C2 host, C2 port, retry or timeout value, SSL flag, and what is highly likely an implant identifier:

1	"<<STARTXX>>"
2	"aecert.org"
3	443
4	5000
5	0
6	"4B8CC395-A26F-41F1-A1DC-8B993D9D41D2"
7	"<<ENDXX>>"

After initialization, ArcBridge communicates over a WebSocket-style channel and waits for server-side control messages. It supports the following commands:

Command	Description
OPEN:	Creates a proxy/tunnel session to a target selected by the operator.
DNS:	Performs hostname or address resolution and returns the result.

Victimology

According to our telemetry, we identified victims across Middle East and African countries including Egypt, SMB and government environments in Jordan and Tanzania, aviation organizations in Pakistan, telecommunication companies in Ethiopia and financial-sector entities in Burkina Faso.

Conclusion

Mirage Kitten continues to evolve its malware arsenal to support targeted cyber-espionage operations across the Middle East and Africa regions. The NightLedger backdoor retains similar core command functionality to TWOSTROKE while introducing additional capabilities, including screenshot capture and collection of the `NetSetup.log` file.

Another notable aspect of the campaign is the group's continued reliance on tunneling utilities as part of its operational toolkit. This aligns with previous public reporting, which documented the group's use of the LIGHTRAIL and POLLBLEND tunnelers. Consistent with this tradecraft, we observed Mirage Kitten continuing to leverage tunneling capabilities alongside a gradual shift away from Microsoft Azure subdomain-style infrastructure in favor of Cloudflare-backed domains in some of its malware, a change likely intended to complicate attribution while maintaining resilient command-and-control communications.

Indicators of compromise

Additional IoCs are available to customers of our [Threat Intelligence Reporting](#) service. For more details, contact us at intelreports@kaspersky.com.

File hashes

NightLedger backdoor

[A239E655709A2518DD0B7BDBED163679](#) – sspicli.dll

ArcBridge WebSocket tunneling tool

[5FA15EF96808EA82F0A6176F0BB4B386](#)

[42F847597109DA2A220391BB09D00676](#)

[AFB1C1583606599C7272CFB33CC6F498](#)

BridgeHead WebSocket tunneling tool

[6038D42AF0AFFD1FB263F470C0956F6B](#) – unbcl.dll

[AE628EFA305387B633DCE82F9364875B](#) – unbcl.dll

[F7D36CC5904A53252D2BB3D21615134F](#) – libwinpthread-1.dll

[C90F0EFADBF322E5EB1C4103A38C30E6](#) – libwinpthread-1.dll

[D09B14A2FE01C7363ECC56F5D046162C](#) – IPHLPAPI.dll

Domains and IPs

[smartconnect\[.\]azurewebsites\[.\]net](#)

[businessmixture\[.\]com](#)

[global-reds\[.\]com](#)

[maadinglobal\[.\]com](#)
[Business-deegital\[.\]com](#)
[business-deegital\[.\]azurewebsites\[.\]net](#)
[businessdeegital\[.\]azurewebsites\[.\]net](#)
[neexportfolio\[.\]azurewebsites\[.\]net](#)
[neexportfolio\[.\]com](#)
[neexportfolio\[.\]eastus\[.\]cloudapp\[.\]azure\[.\]com](#)
[172\[.\]86\[.\]98\[.\]113](#)
[aecert\[.\]org](#)
[realhealthshop\[.\]com](#)
[tjconsultingservices\[.\]com](#)
[thehealth-life\[.\]com](#)
[buisness-central-transportation\[.\]com](#)
[healthcarezoom-central\[.\]azurewebsites\[.\]net](#)
[healthcarezoomcentral\[.\]azurewebsites\[.\]net](#)
[healthcarezoomcentral\[.\]org](#)
[toadreport\[.\]azurewebsites\[.\]net](#)
[business-startup\[.\]azurewebsites\[.\]net](#)
[businessstartup\[.\]azurewebsites\[.\]net](#)

Source: <https://securelist.com/mirage-kitten-new-tools/120811/>