CROWDSTRIKE

Intelligence Alert

CSA-251345

ETHEREAL PANDA Establishes New C2 Infrastructure, Likely Maintains Connections to Victim Entities

Publish Date: 19 December 2025

CROWDSTRIKE INTELLIGENCE

This report is provided for situational awareness and network defense purposes only. DO NOT conduct searches on, communicate with, or engage any individuals, organizations, or network addresses identified in this report. Doing so may put you or your employer at risk and jeopardize any ongoing investigation efforts.

Topic: Espionage || **Adversary:** ETHEREAL PANDA

From June 2025 to October 2025, ETHEREAL PANDA operationalized multiple new command-and-control (C2) infrastructure nodes. CrowdStrike Intelligence identified the adversary leveraging 15 IP addresses and two new domains.

Third-party network telemetry revealed ETHEREAL PANDA likely targeted universities, government energy organizations, and financial institutions across South Asia, East Africa, and Taiwan; this target scope aligns with ETHEREAL PANDA's established targeting patterns.

CrowdStrike Intelligence attributes the activity detailed in this Alert to ETHEREAL PANDA; this assessment is made with high confidence based on the use of known SoftEther VPN TLS certificates, targeting consistent with ETHEREAL PANDA's previous operations, and overlaps with the adversary's Tactics, Techniques, and Procedures (TTPs).

Details

In late October 2025, CrowdStrike Intelligence identified multiple C2 IP addresses that ETHEREAL PANDA operationalized from June 2025 to October 2025 (Table 1). Each IP address displayed one of two TLS certificates that ETHEREAL PANDA has used in previous SoftEther VPN deployments (Table 2) (CSA-250096, CSIT-24181, CSA-241188, CSA-240460, CSIT-23343).

The adversary has used these certificates since creating them, demonstrating ETHEREAL PANDA's sustained reliance on longstanding C2 infrastructure (CSIT-24181, CSA-220901).

X.509 Certificate Fingerprint SHA256 Hash	IP Address	First Observed	Last Observed
d8346e8f61c55e2f484e4a7c4040e20d9f77f8082ce5ae24d8da2a789287a35b	206.238.196[.]237	14 November 2024	14 October 2025
	139.180.187[.]200	10 October 2024	14 October 2025
	156.224.139[.]221	21 March 2025	14 July 2025
	156.224.139[.]245	20 March 2025	14 July 2025
87eb605dfa2c61bc3a1e6c7799b7e3687fe8f6ca7aece227adb0ddf174a88176	108.61.181[.]104	31 December 2024	14 October 2025
	165.154.236[.]234	3 September 2025	14 October 2025
	165.154.230[.]30	1 August 2025	14 October 2025
	212.129.221[.]185	14 April 2025	14 October 2025
	39.107.108[.]124	10 December 2024	10 October 2025
	175.27.158[.]236	26 September 2025	1 October 2025
	45.133.239[.]77	6 September 2025	17 September 2025

	185.216.118[.]101	17 June 2025	31 July 2025
	45.15.8[.]31	17 July 2025	30 July 2025
	103.149.48[.]189	19 June 2025	17 July 2025
	192.83.193[.]82	2 June 2025	2 June 2025

Table 1. ETHEREAL PANDA Certificate-Hosting IP Addresses

X.509 Certificate Fingerprint SHA256 Hash	X.509 Certificate Common Name	Date Created
d8346e8f61c55e2f484e4a7c4040e20d9f77f8082ce5ae24d8da2a789287a35b	CN=vpn217978803.softether[.]net	1 March 2024
87eb605dfa2c61bc3a1e6c7799b7e3687fe8f6ca7aece227adb0ddf174a88176	CN=vpn437972693.sedns[.]cn	26 May 2021

Table 2. ETHEREAL PANDA TLS Certificates

Passive DNS data shows the domains goupdate[.]mywire[.]org and javaup[.]accesscam[.]org resolved to IP addresses 165.154.236[.]234 and 185.216.118[.]101 when these IP addresses displayed ETHEREAL PANDA's SoftEther TLS certificates (Table 3). ETHEREAL PANDA registered both domains using the dynamic DNS (DDNS) registrar Dynu, which they previously used in 2024 (CSIT-24181). Based on the concurrent activity, CrowdStrike Intelligence assesses with moderate confidence that these domains are related to ETHEREAL PANDA's activity.

ETHEREAL PANDA IP Address	Domain	First Observed	Last Observed
165.154.236[.]234	goupdate[.]mywire[.]org	3 August 2025	25 September 2025
185.216.118[.]101	javaup[.]accesscam[.]org	10 July 2025	10 July 2025

Table 3. New ETHEREAL PANDA Domains

From August 2025 to October 2025, third-party network telemetry showed inbound connections to five of the newly attributed ETHEREAL PANDA IP addresses listed in Table 1. The connections originated from entities in Nepal, India, Kenya, and Taiwan via TCP port 443 and multiple ephemeral ports not associated with standard services.

CrowdStrike Intelligence assesses that these connections likely represent compromised hosts beaconing to ETHEREAL PANDA's C2 infrastructure. This assessment is made with moderate confidence based on the connections' directionality and duration as well as ETHEREAL PANDA's previous use of ephemeral ports to relay traffic to hosts displaying SoftEther TLS certificates (CSA-241188, CSIT-24181); however, the nature of the network telemetry precludes a higher confidence assessment.

Source Organization	Destination IP Address (ETHEREAL PANDA C2)	Primary Ports

Kenyan government energy entity	203.91.76[.]102	443, 40016, and 40018
Nepalese retail entity	156.224.139[.]221	11010, 11012
	206.238.196[.]237	
Taiwanese technology entity	203.91.76[.]102	443
Likely Taiwanese technology entity	165.154.230[.]30	443, 40019, and 40025
Taiwanese energy entity	165.154.230[.]30	8322
		40004
Indian construction entity	156.224.139[.]221	11010, 11012
Indian financial entity	156.224.139[.]221	11010, 11012
	206.238.196[.]237	
Indian university entity	139.180.187[.]200	40001
	156.224.139[.]221	11010, 11012
	206.238.196[.]237	443, 40001
		443, 40070
		11010, 11012

Table 4. Third-Party Network Telemetry

On 25 September 2025, third-party network telemetry showed additional connections via TCP port 443 from ETHEREAL PANDA's IP address 206.238.196[.]237 to a likely South Asia-based military entity. CrowdStrike Intelligence assesses that the network telemetry likely reflects ETHEREAL PANDA reconnaissance activity. This assessment is made with moderate confidence based on the connections' directionality and the adversary's known targeting of similar regional entities.

Assessment

CrowdStrike Intelligence attributes the activity detailed in this Alert to ETHEREAL PANDA. This assessment is made with high confidence based on overlaps with ETHEREAL PANDA's infrastructure, including using known SoftEther TLS certificates for extended periods. Additionally, the likely targets—including entities in Taiwan, India, and Kenya—identified in network telemetry are consistent with ETHEREAL PANDA's established target scope, which includes Taiwan and strategic targets in South Asia and East Africa (CSA-221084, CSA-241188, CSA-240460, CSA-231363, CSIT-24181).

ETHEREAL PANDA continues to operationalize new network infrastructure while maintaining longstanding operational tradecraft, including their reuse of TLS certificates and domains across multiple campaigns over extended periods; this pattern likely demonstrates that the adversary's established C2 methodologies are

sufficiently evasive, allowing them to continue their intelligence-collection operations (CSA-241188, CSIT-24181, CSA-250096, CSA-240460, CSIT-23343).

Appendix

Falcon LogScale Query

This Falcon LogScale Query detects the activity described in this report.

```
// hunting rule for indicators (CSA-251345)
case { in("DomainName", values=["goupdate.mywire.org", "javaup.accesscam.org"]);
in("RemoteAddressIP4", values=["103.149.48.189", "108.61.181.104", "139.180.187.200",
"156.224.139.221", "156.224.139.245", "165.154.230.30", "165.154.236.234",
"175.27.158.236", "185.216.118.101", "192.83.193.82", "206.238.196.237",
"212.129.221.185", "39.107.108.124", "45.133.239.77", "45.15.8.31"]) } | table([cid,
aid, #event_simpleName, ComputerName])
```

IOCs

This table details the IOCs related to the information provided in this report.

IOC	Description
goupdate[.]mywire[.]org	ETHEREAL PANDA domain
javaup[.]accesscam[.]org	ETHEREAL PANDA domain
206.238.196[.]237	ETHEREAL PANDA IP address
139.180.187[.]200	ETHEREAL PANDA IP address
156.224.139[.]221	ETHEREAL PANDA IP address
156.224.139[.]245	ETHEREAL PANDA IP address
108.61.181[.]104	ETHEREAL PANDA IP address
165.154.236[.]234	ETHEREAL PANDA IP address
165.154.230[.]30	ETHEREAL PANDA IP address
212.129.221[.]185	ETHEREAL PANDA IP address
39.107.108[.]124	ETHEREAL PANDA IP address
175.27.158[.]236	ETHEREAL PANDA IP address
45.133.239[.]77	ETHEREAL PANDA IP address
185.216.118[.]101	ETHEREAL PANDA IP address

45.15.8[.]31	ETHEREAL PANDA IP address
103.149.48[.]189	ETHEREAL PANDA IP address
192.83.193[.]82	ETHEREAL PANDA IP address