ADVISORY FOR ICM SECTOR

Autumn Dragon targets Southeast Asia government & media sectors using backdoors

Original report published on: November 18, 2025

Executive Summary

On 18 November, CyberArmor reported on a targeted cyber espionage campaign attributed to a threat actor tracked as "Autumn Dragon". The campaign has targeted organisations in Southeast Asia within the South China Sea region, including Singapore, Laos, Cambodia, the Philippines, and Indonesia, with a particular focus on government, media, and news-related entities. The campaign demonstrates characteristics of long-term intelligence collection operations, leveraging spear-phishing and DLL side-loading techniques to establish an initial foothold and maintain persistent access within compromised environments.

Background

Autumn Dragon primarily relied on social engineering and spear-phishing techniques to deliver malicious archive files, exploiting the WinRAR vulnerability (CVE-2025-8088) to automatically extract and execute malicious content once opened by victims.

Following successful initial execution, Autumn Dragon employed a multi-stage malware infection chain utilising DLL side-loading techniques that abused legitimate applications. This approach enabled the threat actor to execute malicious code whilst bypassing security controls that rely on application trust mechanisms. The infection chain facilitated the deployment of multiple backdoors that communicated with command-and-control (C2) infrastructure via Telegram and HTTPS protocols, enabling the exfiltration of sensitive information from compromised systems.

CyberArmor assessed the intent of these activities to be espionage-oriented, targeting sectors of strategic and political interest within the region rather than causing immediate operational disruption.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the Autumn Dragon-related activities identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Deploy tools such as EDR to detect DLL sideloading through behavioural analysis and monitor for suspicious execution of legitimate binaries loading unauthorised DLLs.
- Enhance user awareness on spear-phishing and malicious email attachments.
- Review endpoint logs for abnormal process execution and DLL loading behaviour.
- Implement application control or allow-listing where operationally feasible.
- Ensure timely patching of operating systems and commonly abused software.
- Restrict user privileges to reduce the impact of initial compromise

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A – Indicators of Compromise (IOC)

SHA256 Hash	**Description**
5b64786ed92545eeac013be9456e1ff03d95073910742e45ff6b88a86e91901b	Initial dropper: Proposal_for_Cooperation_3415.05092025.rar
e409736eb77a6799d88c8208eb5e58ea0dcb2c016479153f9e2c4c3c372e3ff6	Batch script: Windows Defender Definition Update.cmd
50855f0e3c7b28cbeac8ae54d9a8866ed5cb21b5335078a040920d5f9e386ddb	Next stage dropper: gs.rar
a3805b24b66646c0cf7ca9abad502fe15b33b53e56a04489cfb64a238616a7bf	2nd stage implant: libcef.dll
5d0d00f5d21f360b88d1622c5cafd42948eedf1119b4ce8026113ee394ad8848	3rd stage loader: opera_elf.dll
fe3fb17140458dc2073d130569f7b45bca681e0557824ee4a042ff7f13d8c977	3rd stage loader: msedge_elf.dll
843fca1cf30c74edd96e7320576db5a39ebf8d0a708bde8ccfb7c12e45a7938c	3rd stage loader: CRClient.dll
2044a0831ce940fc247efb8ada3e60d61382429167fb3a220f277037a0dde438	4th stage encrypted payload: Update.lib
c691f9de944900566b5930f219a55afcfc61eaf4ff40a4f476dd98a5be24b23c	4th stage decrypted payload

Folder	**Description**
C:\Users\Public\Documents\Microsoft\winupdate_v	Staging folder

Domain	**Description**
hxxps[:]//public.megadatacloud[.]com	C2 Domain

IP Address	**Description**
104.234.37[.]45	C2 IP Address

Annex B – MITRE ATT&CK Tactics and Techniques

Tactic	**Technique ID**	**Technique Name**
Initial Access	T1193	Spearphishing Attachment
Execution	T1059.001	Windows Command Shell
	T1203	Exploitation for Client Execution

Persistence	T1547.001	Registry Run Keys / Startup Folder
	T1053.005	Scheduled Task
Defensive Evasion	T1218	Signed Binary Proxy Execution
	T1574	DLL Side-Loading
Discover	T1057	Process Discovery
	T1082	System Information Discovery
	T1012	Query Registry
Collection	T1113	Screen Capture
Command and Control	T1071.001	Web Protocols
	T1573	Encrypted Channel
	T1102.002	Data from Cloud Storage Object
	T1102	Web Service

References

[1] Cyber Armor Report