ADVISORY FOR ICM SECTOR

CL-STA-0048 Group Targets Telecommunications Sector with Customised Tools and Techniques

Original report published on: January 29, 2025[1]

Executive Summary

CL-STA-0048 Group, identified by Unit 42, is suspected to have originated from China and targets South Asian telecommunication organisations and government agencies. The group leverages on Living-off-the-Land Binaries (LOLBin) to evade detection and deliver PlugX and Cobalt Strike. Staged data from an SQL server is then used to exfiltrate sensitive data to their C2 server.

Background

In January 2025, Unit 42 discovered CL-STA-0048 has been conducting cyber-espionage campaigns since May 2024 against South Asian telecommunications organisations. The group exploits vulnerabilities in IIS, Apache Tomcat, and MSSQL Services for initial access, leveraging customised tools and techniques while adapting its methods to bypass defences and achieve its objectives.

PowerShell scripts were used to enumerate running processes and directory contents. Data was exfiltrated using the commonly allowed DNS protocol. LOLBin ('certutil') was used to deploy a PlugX backdoor allowing in-memory execution to evade detection. After establishing a foothold, the attackers employed Hex Staging (incremental encoding of data in hexadecimal format) to evade detection and deliver a Cobalt Strike beacon. The threat group then reconstructed the binary executables or scripts by decoding the hex data back into executable format, using 'certutil'.

The Cobalt Strike beacon was injected into an SQL server process, enabling C2 communication to deliver additional malware such as `Stowaway` and `iox` to tunnel network traffic through compromised systems. A new SQL database user was created for persistence and use for executing SQL commands to search for database of interest. Afterwhich, data was staged and exfiltrated to their C2 server.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention identified in this advisory:

- Scan for Indicators of Compromise to detect threat actor activities (Annex A).
- Refer to the MITRE ATT&CK techniques (Annex B) in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Look for cmd.exe executions with "set /p=" in arguments.

- Look for certutil.exe executions with "-decodehex".
- Add malicious file hashes to blocklist in anti-virus and/or Endpoint Detection & Response (EDR) and Network Detection and Response (NDR) to detect Cobalt Strike activity.
- Monitor for malformed DNS protocol traffic that differs from the usual baseline.
- Keep public facing applications up to date especially IIS, Apache Tomcat and MSSQL.

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

Malware Hash – SHA256	Remark
525540eac2d90c94dd3352c7dd624720ff2119082807e2670785aed77746301d	Cobalt Strike Loaders
af0baf0a9142973a3b2a6c8813a3b4096e516188a48f7fd26ecc8299bce508e1	
3503d6ccb9f49e1b1cb83844d1b05ae3cf7621dfec8dc115a40abb9ec61b00bb	PlugX
0f85b67f0c4ca0e7a80df8567265b3fa9f44f2ad6ae09a7c9b7fac2ca24e62a8	
c5af6fd69b75507c1ea339940705eaf61deadd9c3573d2dec5324c61e77e6098	PotatoSuite
8dfc107662f22cff20d19e0aba76fcd181657255078a78fb1be3d3a54d0c3d46	
336892ff8f07e34d18344f4245406e001f1faa779b3f10fd143108d6f30ebb8a	SspiUacBypass
35da93d03485b07a8387e46d1ce683a81ae040e6de5bb1a411feb6492a0f8435	Winos4.0-based Malware
a09179dec5788a7eee0571f2409e23df57a63c1c62e4b33f2af068351e5d9e2d	Stowaway
edc9222aece9098ad636af351dd896ffee3360e487fda658062a9722edf02185	

Domain	Remark
sentinelones[.]com	Cobalt Strike C2
mail.tttseo[.]com	PlugX C2
h5.nasa6[.]com	C2 Servers
test.nulq5r.ceye[.]io	
web.nginxui[.]cc	

IP Address	Remark
154.201.68[.]57	Winos4.0-based Malware C2
43.247.135[.]106	C2 Servers
38.54.30[.]117	
38.54.56[.]88	
65.20.69[.]103	
52.77.234[.]115	
192.227.180[.]124	
107.174.39[.]125	
18.183.94[.]114	
206.237.0[.]49	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Title
Initial Access	T1190	Exploit Public-Facing Application
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Persistence	T1136.001	Create Account: Local Account
Defense Evasion	T1027	Obfuscated Files or Information
	T1140	Deobfuscate/Decode Files or Information
	T1070.004	Indicator Removal: File Deletion
	T1574.002	Hijack Execution Flow: DLL Side-Loading
Discovery	T1083	File and Directory Discovery
	T1057	Process Discovery
Collection	T1560	Archive Collected Data
Command and Control	T1071.004	Application Layer Protocol: DNS
	T1572	Protocol Tunneling
Exfiltration	T1030	Data Transfer Size Limits
	T1041	Exfiltration Over C2 Channel

References

1. ^ “CL-STA-0048 group targets telecommunications sector with customise tools and techniques”