ADVISORY FOR ICM SECTOR

Squidoor Backdoor Targets Various Organisations for Espionage

Original report published on: February 27, 2025[1]

Executive Summary

In February 2025, Palo Alto Networks Unit 42 identified threat group, CL-STA-0049 targeting various sectors since March 2023 and this includes government, defence, telecommunications, education, and aviation in Southeast Asia and South America. The group aim was to collect sensitive information and profiles of government officials. It employed sophisticated tactics, including web shell entry vector and covert communications channels, using an advanced backdoor called Squidoor on both Windows and Linux. A newly discovered Windows variant of Squidoor reveals its stealthy modular design and unique command and control (C2) communication via Outlook API, DNS tunnelling, and ICMP tunnelling. These protocols are typically permitted in organisations.

Background

Squidoor have been improved to include multiple vectors for Command and Control (C2) communication, such as the Outlook API, DNS tunnelling, and ICMP tunnelling which are largely not monitored.

Initial access to networks is typically gained by exploiting vulnerabilities in Internet Information Services (IIS) servers, followed by the deployment of web shells, which act as persistent backdoors. Four (4) primary web shells were identified: OutlookDC.aspx, Error.aspx (1), Error.aspx (2), and TimeoutAPI.aspx. These web shell share common characteristics, indicating a single origin.

Squidoor's modular design allows it to maintain access, execute commands, and gather intelligence from targeted organisations.

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 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.
- Validate before adding malicious file hashes to blocklist in antivirus and/or Endpoint Detection & Response (EDR) and eXtended Detection and Response (XDR) including servers.

- Monitor DNS, Firewall, Intrusion Detection Systems (IDS) logs for unusual outbound traffic using non-standard ports or protocols (e.g. DNS Tunnelling, Reverse TCP/UDP), that is not used in organisation.
- Monitor web proxy logs for deployment of web shells to IIS web directories, especially .aspx files like OutlookDC.aspx, Error.aspx or TimeoutAPI.aspx that can serve as persistent backdoors.

Annex A - Indicators of Compromise

Malware Hash – SHA256	Remark
f663149d618be90e5596b28103d38e963c44a69a5de4a1be62547259ca9ffd2d	Squidoor – Windows version (config.ini)
83406905710e52f6af35b4b3c27549a12c28a628c492429d3a411fdb2d28cc8c	Squidoor – Linux version
8187240dafbc62f2affd70da94295035c4179c8e3831cb96bdd9bd322e22d029	
fa2a6dbc83fe55df848dfcaaf3163f8aaefe0c9727b3ead1da6b9fa78b598f2b	
3fcfc4cb94d133563b17efe03f013e645fa2f878576282805ff5e58b907d2381	
f45661ea4959a944ca2917454d1314546cc0c88537479e00550eef05bed5b1b9	
9f62c1d330dddad347a207a6a565ae07192377f622fa7d74af80705d800c6096	Associated Web Shells
461f5969b8f2196c630f0868c2ac717b11b1c51bc5b44b87f5aad19e001869cc	
224becf3f19a3f69ca692d83a6fabfd2d78bab10f4480ff6da9716328e8fc727	
6c1d918b33b1e6dab948064a59e61161e55fccee383e523223213aa2c20c609c	
81bd2a8d68509dd293a31ddd6d31262247a9bde362c98cf71f86ae702ba90db4	
7c6d29cb1f3f3e956905016f0171c2450cca8f70546eee56cface7ba31d78970	
c8a5388e7ff682d3c16ab39e578e6c529f5e23a183cd5cbf094014e0225e2e0a	
1dd423ff0106b15fd100dbc24c3ae9f9860a1fcdb6a871a1e27576f6681a0850	
82e68dc50652ab6c7734ee913761d04b37429fca90b7be0711cd33391febff0a	
e8d6fb67b3fd2a8aa608976bcb93601262d7a95d37f6bae7c0a45b02b3b325ad	
2b6080641239604c625d41857167fea14b6ce47f6d288dc7eb5e88ae848aa57f	
33689ac745d204a2e5de76bc976c904622508beda9c79f9d64c460ebe934c192	
5dd361bcc9bd33af26ff28d321ad0f57457e15b4fab6f124f779a01df0ed02d0	
945313edd0703c966421211078911c4832a0d898f0774f049026fc8c9e7d1865	
a7d76e0f7eab56618f4671b5462f5c210f3ca813ff266f585bb6a58a85374156	
265ceb5184cac76477f5bc2a2bf74c39041c29b33a8eb8bd1ab22d92d6bebaf5	

IP Address	Remark
209[.]141[.]40[.]254	Suspected C2
104[.]244[.]72[.]123	
47[.]76[.]224[.]93	

Domain	Remark
support.vmphere[.]com	Suspected C2
update.hobiter[.]com	
microsoft-beta[.]com	
zimbra-beta[.]info	
microsoftapimap[.]com	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique
Initial Access	T1190	Exploit Public Facing Application
Execution	T1059	Command and Scripting Interpreter
Persistence	T1053.005	Scheduled Task / Job: Scheduled Task
	T1505.003	Server Software Component: Web Shell
Defence Evasion	T1027	Obfuscated Files or Information
	T1055	Process Injection
Credential Access	T1552.001	Unsecured Credentials: Credentials in Files
Command and Control	T1071.001	Application Layer Protocol: Web Protocols (HTTP/S)
	T1071.004	Application Layer Protocol: DNS
	T1102	Web Service
	T1568.002	Dynamic Resolution: Domain Generation Algorithms (DGA)
Collection	T1114.002	Email Collection: Remote Email Collection

References

1. ^ “Squidoor: Suspected Chinese Threat Actor's Backdoor Targets Global Organisations”