ADVISORY FOR ICM SECTOR

Eagerbee Backdoor Used to Target ISPs and Governmental Entities in Middle East

Original report published on: January 6, 2025[1]

Executive Summary

Eagerbee is an advanced backdoor malware that has been used in targeted attacks against Internet Service Providers (ISPs) and government entities in the Middle East. It   is designed for stealth and persistence, operating primarily in memory to evade detection. It features a novel service injector, multiple malicious plugins, and command execution capabilities.

Background

Kaspersky researchers recently found EAGERBEE backdoor, a sophisticated malware framework designed to operate in memory, being deployed at ISPs and governmental entities in the Middle East. Eagerbee was first observed in May 2023 targeting East Asia organisations. Kaspersky researchers suspect that this malware is linked to CoughingDown APT, a possible China nexus actor known for cyber espionage campaigns.

The latest version of EAGERBEE features a novel service injector designed to inject the backdoor into a running service, and a slew of previously undocumented plugins that can be deployed after the installation.

Upon installing and running the payload, the service injector targets legitimate windows services such as 'Themes' service, SessionENV, IKEEXT, and MSDTC, to write the backdoor payload in memory via DLL hijacking. EAGERBEE appears on the infected system as "dlloader1x64.dll" and initiates the collection of information such as operating system characteristics and network addresses.

Upon initialisation, it opens a TCP/SSL channel with the C2 server, from which it can execute a payload known as the Plugin Orchestrator with the internal name "ssss.dll". Subsequently, it can inject more plugins, as well as gather and report information to the C2 server. Currently, the initial access vector is still unknown.

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.

- Use Endpoint Detection & Response (EDR) tools to monitor and prevent unauthorised execution of binaries, and privilege escalation attempts.
- Monitor changes to IKEEXT, MSDTC, and SessionEnv Services.
- Review usage of attrib command on files in c:\users\public and system32 folder locations.
- Use firewall rules and intrusion detection systems (IDS) to block communications with C2 servers.

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 - MD5	Remark
c651412abdc9cf3105dfbafe54766c44	EAGERBEE backdoor decompress
9d93528e05762875cf2d160f15554f44	EAGERBEE backdoor compressed file
26d1adb6d0bcc65e758edaf71a8f665d	EAGERBEE backdoor decompress and fix
183f73306c2d1c7266a06247cedd3ee2	Service Injector
35ece05b5500a8fc422cec87595140a7	Plugin Orchestrator
cbe0cca151a6ecea47cfaa25c3b1c8a8	

IP Address	Remark
5[.]34[.]176[.]46	Suspected C2
195[.]123[.]242[.]120	
82[.]118[.]21[.]230	
194[.]71[.]107[.]215	
62[.]233[.]57[.]94	
151[.]236[.]16[.]167	
195[.]123[.]242[.]120	
195[.]123[.]217[.]139	

Domain	Remark
www[.]socialentertainments[.]store	Suspected C2
www[.]rambiler[.]com	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell
Persistence	T1543.003	Create or Modify System Process: Windows Services
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location
Discovery	T1016	System Network Configuration Discovery
	T1049	System Network Connections Discovery
Command and Control	TA0011	Application Layer Protocol: Web Protocols

References

1. ^ “Eagerbee backdoor used to target ISPs and governmental entities in Middle East”