

HiveForce Labs

# THREAT ADVISORY

**ATTACK REPORT**

## Eagerbee Unmasked: Sophisticated Malware Strikes Middle East

Date of Publication

January 7, 2025

Admiralty Code

A1

TA Number

TA2025005

# Summary

**Attack Discovered:** 2025

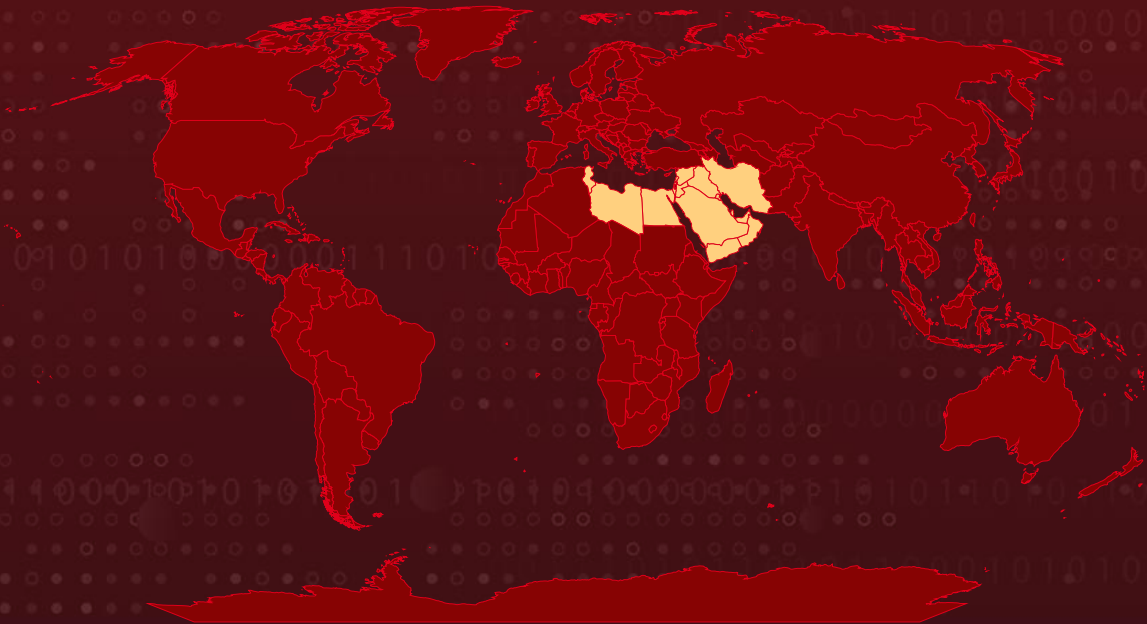
**Targeted Countries:** Middle East

**Targeted Industries:** ISPs and Governmental entities




**Malware:** EAGERBEE backdoor

**Attack:** The Eagerbee malware framework has evolved, with new variants targeting government organizations and internet service providers (ISPs) in the Middle East. Recent investigations uncovered sophisticated components fueling these attacks, including a newly designed service injector. This injector stealthily embeds the backdoor into active system services, enhancing its persistence and evasion capabilities. In addition to the service injector, researchers have identified previously undocumented plugins that are deployed after the backdoor is installed. These plugins enable a wide array of malicious actions, such as deploying additional payloads, probing file systems, executing command shells, and more.

## 🗡️ Attack Regions



Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-26855	ProxyLogon (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server			

# Attack Details

## #1

The Eagerbee malware framework has evolved into a more sophisticated threat, with new variants targeting organizations in the Middle East. Recent investigations have uncovered advanced components fueling these attacks, including a novel service injector designed to stealthily embed the backdoor into active system services, enhancing its persistence and evasion capabilities.

## #2

One key component of the Eagerbee malware framework is a backdoor injector which works alongside a payload file, to target the Themes service process. The injector allocates memory, writes Eagerbee's backdoor code and stub code, decompresses it, and injects it into the service's memory. Triggered by a service control signal, the stub code executes the payload, while the injector cleans up to restore the original state of the service.

## #3

The backdoor collects system information like NetBIOS names, OS details, processor architecture, and network addresses, while maintaining a 24/7 operational capability. It stores its configuration either in a public file directory or hardcoded within the binary and communicates with its C2 server using TCP sockets, with optional SSL encryption for secure transmission.

## #4

Once connected, the backdoor retrieves victim-specific details and downloads a plugin orchestrator, ssss.dll. This orchestrator, injected into memory, gathers additional system and network information, manages plugins, and coordinates their execution. Plugins include modules for file and process management, remote access, service control, and network operations, each tasked with executing specific commands from the orchestrator.

# #5

In East Asia, Eagerbee was deployed through the exploitation of the ProxyLogon vulnerability (CVE-2021-26855) in Exchange servers. Attackers leveraged legitimate Windows services to execute loaders, which introduced the Eagerbee backdoor into memory. The malware's in-memory operation and integration with normal system processes make it highly stealthy and difficult to detect. In East Asian incidents, the attackers' use of consistent service creation patterns and overlapping C2 domains links Eagerbee to the CoughingDown threat group. However, the initial infection vector and the group responsible for deploying Eagerbee in the Middle East remain unknown, underscoring the challenge of attribution in such advanced campaigns.

## Recommendations



**Apply Patch:** Ensure all systems, especially Microsoft Exchange servers, are updated with the latest patches to address vulnerabilities like ProxyLogon (CVE-2021-26855).



**Implement Behavioral Analysis:** Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.



**Limit Privileged Access:** Enforce least-privilege access principles by granting users only the permissions necessary for their roles. Continuously monitor and audit accounts with elevated privileges to detect and respond to any unauthorized or suspicious activity promptly.



**Strengthen Endpoint Defense:** Implement advanced Endpoint Detection and Response (EDR) solutions to effectively detect, analyze, and mitigate in-memory malware activity, ensuring comprehensive protection against sophisticated threats.



# Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0002</u></b> Execution	<b><u>TA0003</u></b> Persistence	<b><u>TA0004</u></b> Privilege Escalation
<b><u>TA0005</u></b> Defense Evasion	<b><u>TA0006</u></b> Credential Access	<b><u>TA0007</u></b> Discovery	<b><u>TA0008</u></b> Lateral Movement
<b><u>TA0011</u></b> Command and Control	<b><u>T1033</u></b> System Owner/User Discovery	<b><u>T1003</u></b> OS Credential Dumping	<b><u>T1543</u></b> Create or Modify System Process
<b><u>T1543.003</u></b> Windows Service	<b><u>T1082</u></b> System Information Discovery	<b><u>T1055</u></b> Process Injection	<b><u>T1505</u></b> Server Software Component
<b><u>T1505.003</u></b> Web Shell	<b><u>T1059</u></b> Command and Scripting Interpreter	<b><u>T1068</u></b> Exploitation for Privilege Escalation	<b><u>T1016</u></b> System Network Configuration Discovery
<b><u>T1083</u></b> File and Directory Discovery	<b><u>T1049</u></b> System Network Connections Discovery	<b><u>T1057</u></b> Process Discovery	<b><u>T1569</u></b> System Services
<b><u>T1569.002</u></b> Service Execution	<b><u>T1021</u></b> Remote Services	<b><u>T1021.001</u></b> Remote Desktop Protocol	<b><u>T1588</u></b> Obtain Capabilities
<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1036</u></b> Masquerading	<b><u>T1095</u></b> Non-Application Layer Protocol	<b><u>T1140</u></b> Deobfuscate/Decode Files or Information
<b><u>T1027</u></b> Obfuscated Files or Information	<b><u>T1124</u></b> System Time Discovery	<b><u>T1070</u></b> Indicator Removal	<b><u>T1070.004</u></b> File Deletion

## Indicators of Compromise (IOCs)

TYPE	VALUE
<b>MD5</b>	183f73306c2d1c7266a06247cedd3ee2, 9d93528e05762875cf2d160f15554f44, c651412abdc9cf3105dfbaf54766c44, 26d1adb6d0bcc65e758edaf71a8f665d, cbe0cca151a6ecea47cfaa25c3b1c8a8, 35ece05b5500a8fc422cec87595140a7

TYPE	VALUE
<b>Domains</b>	www[.]socialentertainments[.]store, www[.]rambiler[.]com
<b>IPv4</b>	62[.]233[.]57[.]94, 82[.]118[.]21[.]230, 194[.]71[.]107[.]215, 151[.]236[.]16[.]167, 5[.]34[.]176[.]46, 195[.]123[.]242[.]120, 195[.]123[.]217[.]139
<b>SHA256</b>	F78065AB91F875C1912595DD9578A6700F246FB6B93ECDBC4BCE4B C374DD187A, 6441DF3EAC5BFCB9BDD84E5D6FCE8EDF146F49EC2C7D4A52FBA096 764D41C29A, 95C31C37B54792B8421AA83F3A93AE4A702E1C2EADE6366692F725 430B5E07A3, 0348A47B5361F725EBDE59C8D81D0EE8E209D2173CEAEC96568691 A0BC764473, 3814E668DFF20F96680CC481E1E48238419DD1013ED18DFB182291 AF64295BA1

## Patch Link

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-26855>

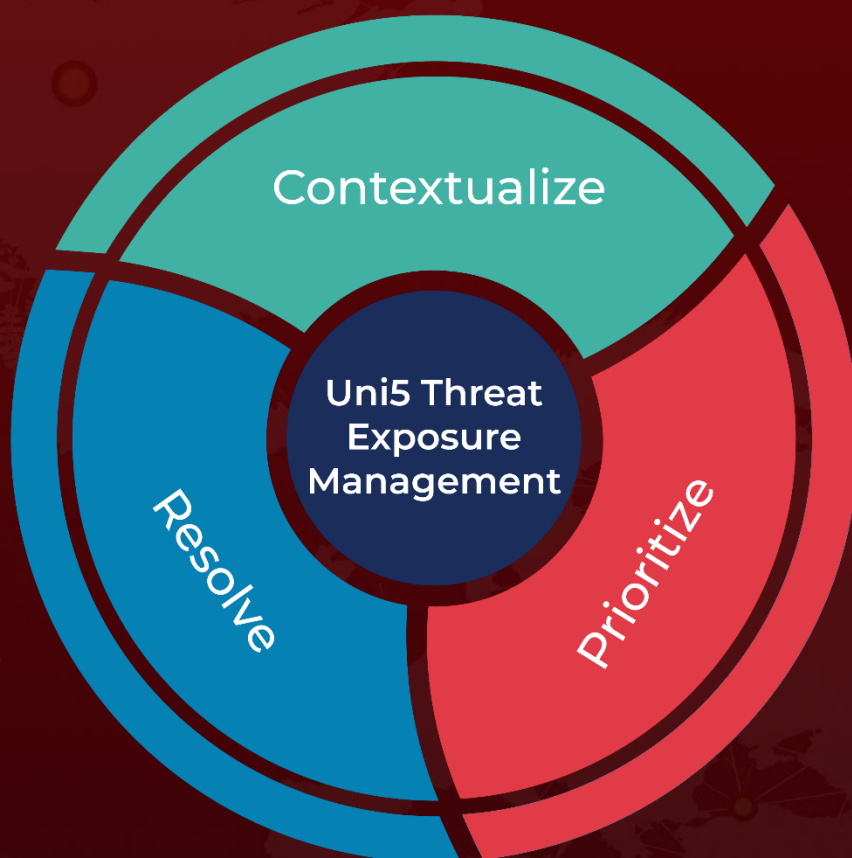
## References

<https://securelist.com/eagerbee-backdoor/115175/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**January 7, 2025 • 5:20 AM**

© 2025 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)