Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

GhostContainer Malware Targets Asian Government Networks

Date of Publication

July 18, 2025

Admiralty Code

A1

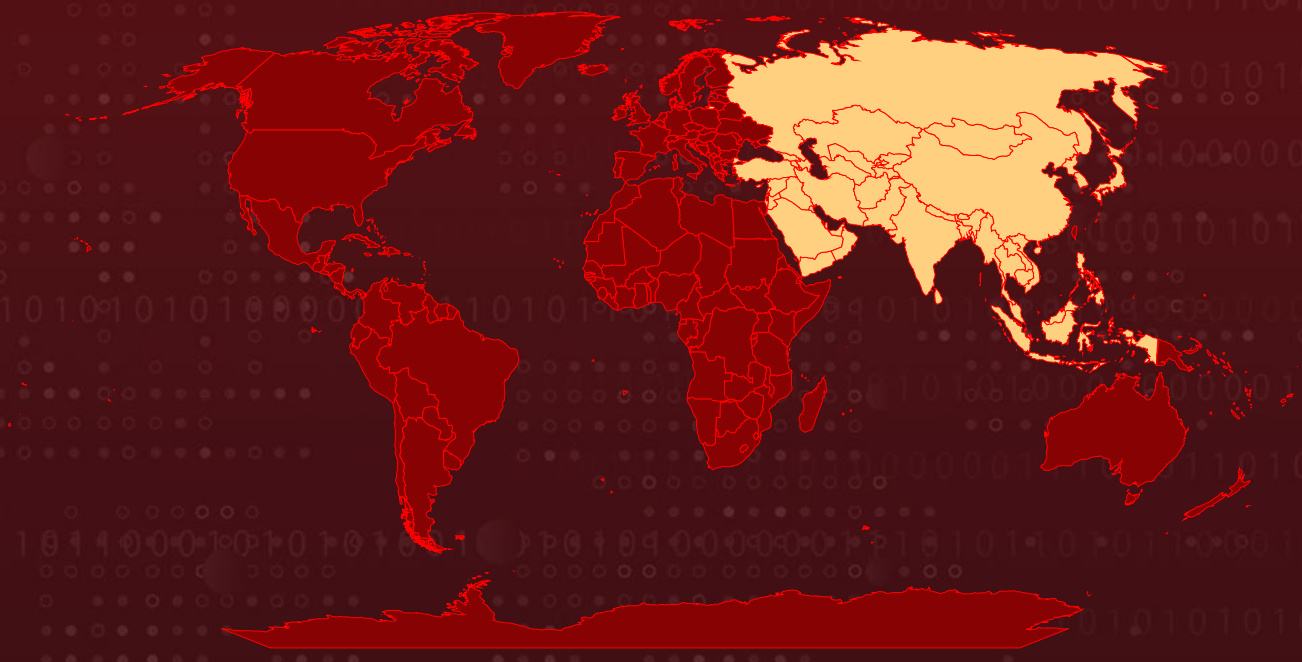
TA Number

TA2025224

Summary

Attack Discovered: July 2025
Targeted Countries: Asia
Affected Industries: Government agency, High-tech
Malware: GhostContainer
Attack: A stealthy and highly sophisticated malware dubbed GhostContainer has been discovered targeting Microsoft Exchange servers in government and high-tech environments across Asia. This backdoor blends seamlessly into normal operations, making it incredibly hard to detect, while allowing attackers to maintain long-term access, all without ever reaching out to an external command-and-control server. By exploiting a known Exchange vulnerability and using open-source tools to create fake web pages for covert communication, the attackers built a custom malware ecosystem tailored for espionage. GhostContainer's ability to bypass security controls, hide in plain sight, and operate without traditional indicators highlights the work of a well-resourced, highly skilled adversary aiming for stealth and persistence.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-0688	Microsoft Exchange Server Validation Key Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓

Attack Details

#1 A stealthy and advanced malware, dubbed GhostContainer, has been discovered targeting Microsoft Exchange servers in sensitive environments, including government agencies and tech companies in Asia. This malware allows attackers to load additional code. GhostContainer can quietly run in the background, blending into normal server activity while acting as a proxy or communication tunnel. This allows attackers to exfiltrate data or gain remote access without triggering obvious alarms.

#2 GhostContainer is a malicious file named App_Web_Container_1.dll, which carries out most of the malware's operations. The main class inside this file, known as Stub, can execute shellcode, download files, run commands, and even load more .NET code as needed. To avoid detection, it uses clever tricks to bypass Windows' security features, like disabling the Antimalware Scan Interface (AMSI) and event logging. It also pulls encryption keys from the server's configuration, allowing it to encrypt its communications with the attacker using AES keeping its activities hidden from prying eyes.

#3 What's particularly interesting is how this malware borrows ideas from publicly available hacking tools. Its command-handling and encryption setup resemble an open-source project created to exploit CVE-2020-0688, a known flaw in Microsoft Exchange. This suggests the attackers are well-versed in both public research and real-world vulnerabilities, repurposing available code to build a more customized, dangerous threat that specifically targets Exchange servers.

#4 A unique aspect of the attack is its use of “ghost pages”, fake virtual pages built using another open-source project called PageLoad_ghostfile.aspx. These pages don’t exist as actual files but are created in memory, making them harder to detect. They serve as a hidden entry point to activate other malware components like the web proxy module, allowing the attacker to send commands and transfer data covertly. Because everything looks like normal web traffic, traditional security tools might completely miss the activity.

#5 The malware’s proxy module acts like a hidden relay parsing incoming requests, forwarding data, and adapting its behavior based on specific headers. It even includes code similar to Neo-reGeorg, a tool used to tunnel traffic through compromised systems. A helper class, StrUtils, supports all this by managing string and XML data behind the scenes.

#6 What makes GhostContainer particularly dangerous is that it doesn’t need a command-and-control (C2) server. Instead, it communicates through ordinary-looking Exchange traffic, making it nearly invisible. The attackers clearly have deep knowledge of Exchange and IIS, and their quiet, tailored approach shows they’re not just experimenting they’re running a sophisticated, targeted espionage campaign.

Recommendations

- **Patch Immediately:** Make sure your Exchange servers are fully up to date with the latest security patches from Microsoft. Attackers often rely on known vulnerabilities like CVE-2020-0688, which have already been fixed in past updates.
- **Look for Suspicious DLLs and Ghost Pages:** Inspect your Exchange and IIS server directories for unusual .dll files or suspicious virtual web pages. GhostContainer uses fake pages and custom DLLs to stay hidden anything out of the ordinary should be investigated.
- **Limit Privileges Where Possible:** Ensure services like IIS and Exchange aren’t running with more privileges than necessary. If malware runs under a low-privilege account, its impact can be greatly reduced.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0008** Lateral Movement	**TA0010** Exfiltration
TA0011 Command and Control	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1553** Subvert Trust Controls
T1553.002 Code Signing	**T1059** Command and Scripting Interpreter	**T1140** Deobfuscate/Decode Files or Information	**T1505** Server Software Component
T1027 Obfuscated Files or Information	**T1203** Exploitation for Client Execution	**T1570** Lateral Tool Transfer	**T1562** Impair Defenses
T1562.001 Disable or Modify Tools	**T1033** System Owner/User Discovery	**T1190** Exploit Public-Facing Application	**T1036** Masquerading
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1090** Proxy	**T1041** Exfiltration Over C2 Channel
T1070 Indicator Removal	**T1070.004** File Deletion		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	01d98380dfb9211251c75c87ddb3c79c
SHA256	87A3AEFB5CDF714882EB02051916371FBF04AF2EB7A5DDEAE4B6B441B2168E36
SHA1	2bb0a91c93034f671696da64a2cf6191a60a79c5
Filename	App_Web_Container_1.dll

Patch Link

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0688

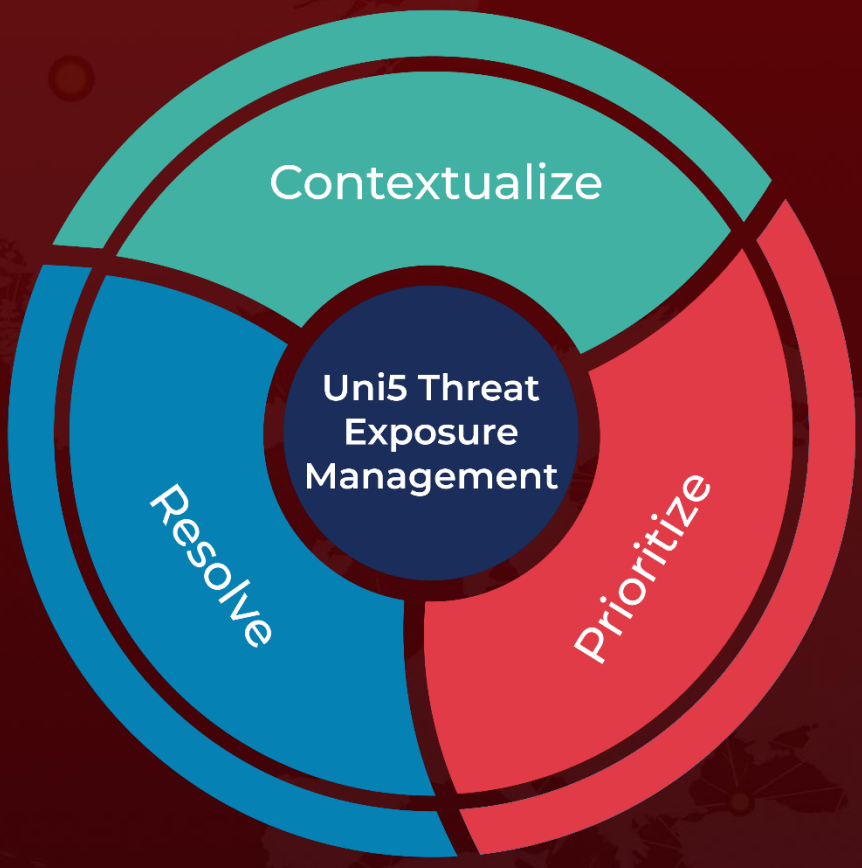
References

https://securelist.com/ghostcontainer/116953/

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

July 18, 2025 . 6:00 AM

More at www.hivepro.com