Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

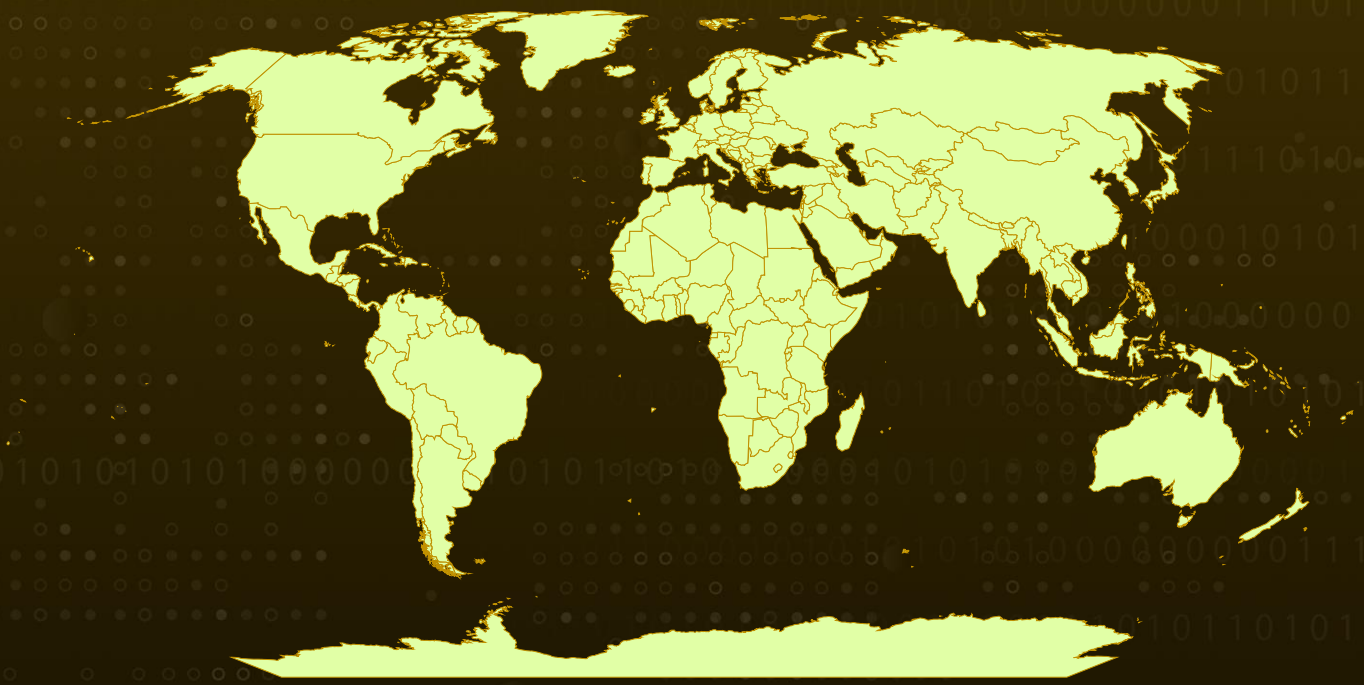
HZ RAT Backdoor Slips into macOS Targeting Enterprise Messaging Apps

Date of Publication	Admiralty Code	TA Number
August 28, 2024	A1	TA2024332

Summary

First Seen: November 2022
Malware: HZ Rat backdoor
Affected Platforms: Windows, macOS
Targeted Region: Worldwide
Attack: HZ RAT is a sophisticated backdoor targeting macOS systems, particularly those using DingTalk and WeChat. This macOS variant mirrors its Windows predecessor but delivers payloads as shell scripts from the attacker's server. The malware's infrastructure includes multiple C2 servers, primarily in China, with some located in the US and the Netherlands.

Attack Regions



Attack Details

#1 HZ RAT is a sophisticated backdoor designed to infiltrate macOS systems, particularly those using the enterprise messaging app DingTalk and the social networking platform WeChat. Discovered in June 2024, this macOS variant closely resembles its Windows counterpart, with the primary distinction being the delivery of payloads as shell scripts from the attacker's server.

#2 Some versions of this backdoor establish connections to command-and-control (C2) servers using local IP addresses, indicating a possible strategy for targeted attacks and lateral movement within the victim's network. Initially identified in November 2022, HZ RAT first emerged targeting Windows systems, where it executed commands via PowerShell scripts.

#3 The macOS variant is distributed within a file named "OpenVPNConnect.pkg," which masquerades as the legitimate "OpenVPN Connect" application. This package contains malicious components that establish a connection to the C2 server, enabling encrypted communication.

#4 HZ RAT is capable of collecting a wide range of data from compromised systems, including system integrity protection status, hardware specifications, and information about Wi-Fi networks. The malware actively seeks to extract WeChat IDs, emails, phone numbers, and detailed organizational data from DingTalk, storing this information in plain text within certain files, making it easily accessible to the attacker.

#5 The infrastructure supporting HZ RAT consists of multiple active C2 servers, predominantly located in China, with some in the US and the Netherlands. The presence of this macOS variant suggests ongoing activity by the threat actors responsible for earlier attacks. Although the malware's current focus is on data exfiltration, its capability for lateral movement within networks hints at the potential for more sophisticated attacks in the future.

Recommendations

Implement Robust Application Security: Only download applications from trusted sources or official app stores. Avoid downloading software from unofficial or suspicious websites. Use tools to check the integrity of installed applications and verify that they have not been tampered with.

Strengthen Network Security Measures: Implement network segmentation to limit the spread of malware within the network. Use firewalls and intrusion detection systems (IDS) to monitor and block malicious traffic.

Configure Application Whitelisting: Apply application whitelisting policies to only allow approved applications and executables to run on systems. This can prevent unauthorized scripts or executables from being executed. Regularly review and update the whitelist to accommodate legitimate applications while blocking potentially harmful ones.

Implement Advanced Threat Detection Technologies: Use behavioral analysis tools to detect deviations from normal system behavior, which can indicate the presence of malware or unauthorized activity. Utilize machine learning algorithms to analyze large volumes of data for patterns indicative of malware activity or emerging threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0007** Discovery
TA0008 Lateral Movement	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1566 Phishing	**T1059** Command and Scripting Interpreter	**T1543** Create or Modify System Process	**T1203** Exploitation for Client Execution
T1027 Obfuscated Files or Information	**T1036** Masquerading	**T1082** System Information Discovery	**T1534** Internal Spearphishing
T1041 Exfiltration Over C2 Channel	**T1573** Encrypted Channel	**T1552.001** Credentials In Files	**T1046** Network Service Discovery
T1135 Network Share Discovery	**T1059.001** PowerShell		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	0c3201d0743c63075b18023bb8071e73, 6cc838049ece4fcb36386b7a3032171f, 6d478c7f94d95981eb4b6508844050a6, 7a66cd84e2d007664a66679e86832202, 7ed3fc831922733d70fb08da7a244224, 9cdb61a758afd9a893add4cef5608914, 287ccbf005667b263e0e8a1ccfb8daec, 7005c9c6e2502992017f1ffc8ef8a9b9, 7355e0790c111a59af377babedee9018, a5af0471e31e5b11fd4d3671501dfc32, da07b0608195a2d5481ad6de3cc6f195, dd71b279a0bf618bbe9bb5d934ce9caa, 8d33f667ca135a88f5bf77a0fab209d4
IPv4	111[.]21[.]246[.]147, 123[.]232[.]31[.]206, 120[.]53[.]133[.]226, 218[.]193[.]83[.]70, 29[.]40[.]48[.]21, 47[.]100[.]65[.]182, 58[.]49[.]21[.]113, 113[.]125[.]92[.]32, 218[.]65[.]110[.]180, 20[.]60[.]250[.]230
File Name	OpenVPNConnect.pkg

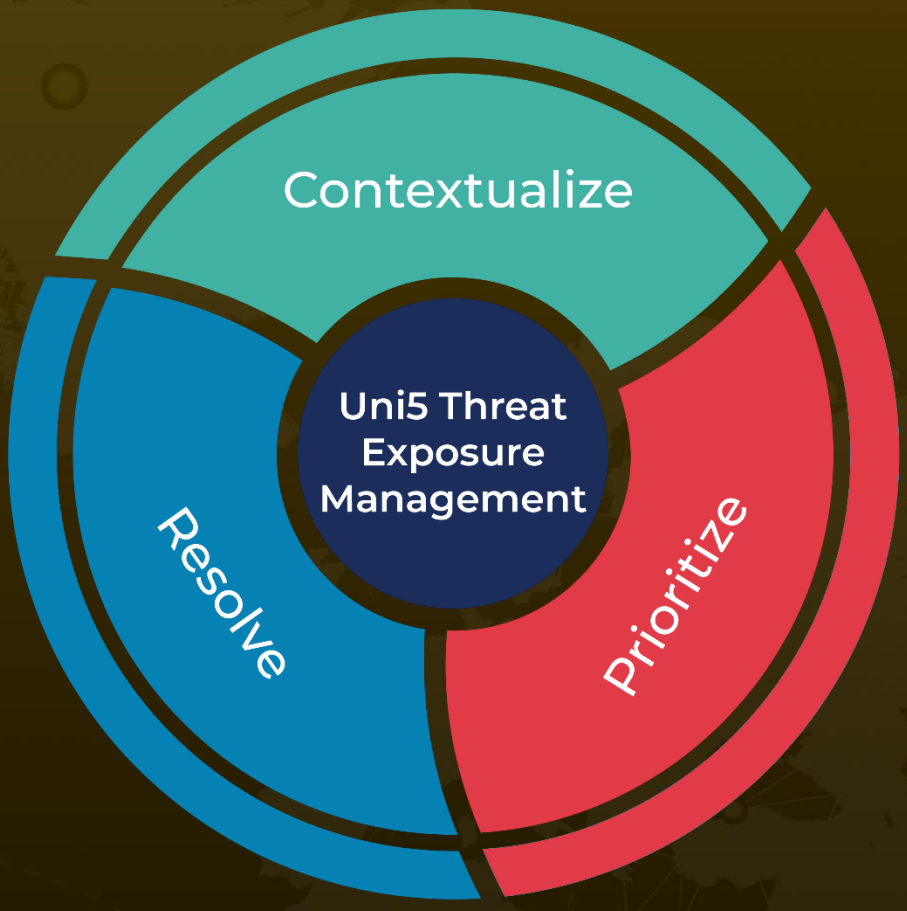
References

https://securelist.com/hz-rat-attacks-wechat-and-dingtalk/113513/

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

August 28, 2024 • 6:30 AM

More at www.hivepro.com