Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

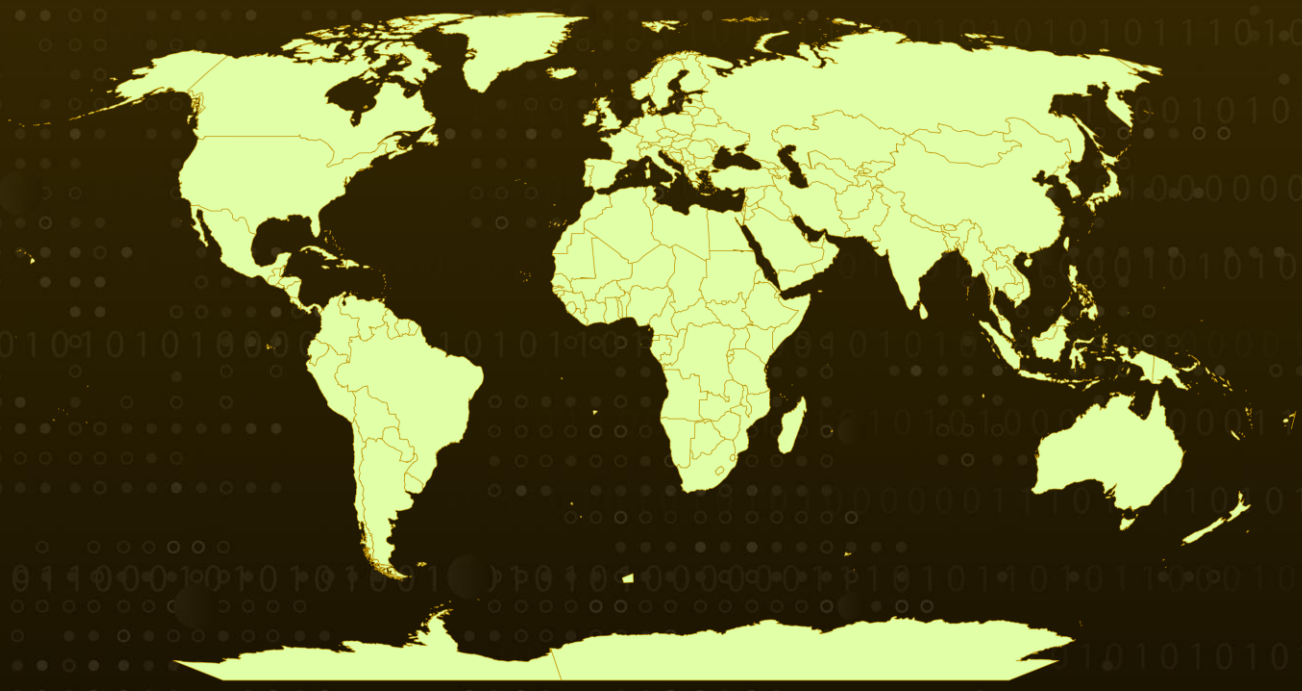
New Variant of Chaes Malware 'Chae$ 4' Targeting Financial and Logistics Sectors

Date of Publication	Admiralty Code	TA Number
September 6, 2023	A1	TA2023356

Summary

First appeared: January 2023
Attack Region: Worldwide
Affected Platform: Mercado Libre, Mercado Pago, WhatsApp Web, Itau Bank, Caixa Bank, and CMS services like WordPress, Joomla, Drupal, and Magento
Malware: Chae$ 4
Targted industries: Financial, Logistics, E-commerce
Attack: A new Chaes malware variant, "Chae$ 4," targeting logistics, finance, and prominent platforms has emerged with enhanced capabilities, including Python-based architecture and an expanded range of targeted services and data theft functions.

Attack Regions



Attack Details

#1

A new and advanced variant of Chaes malware targeting primarily logistics and financial sectors. This Chaes variant, named as "Chae$ 4," is the fourth major iteration, featuring significant changes such as a shift to Python, enhanced encryption, and a focus on targeting platforms like Mercado Libre, Mercado Pago, WhatsApp Web, Itau Bank, Caixa Bank, and CMS services like WordPress, Joomla, Drupal, and Magento. Chaes malware has been active since November 2020, initially targeting e-commerce customers in Latin America.

#2

The Chaes malware is constantly evolving and was first deciphered in November 2020 by Cybereason. Subsequent variants were examined by Avast in January 2022. Remarkably, Chaes malware actors acknowledged Avast's analysis and appreciated their feedback as a means to enhance and advance the malware's capabilities. The threat actor was referred to as 'Lucifer.' Later, in December 2022, Chaes evolved and adopted WMI for system data collection.

#3

Chae$ 4 brings significant transformations, including refined code architecture, increased stealth capabilities, a shift to Python, the adoption of WebSockets for communication, and dynamic resolution of the C2 server's address. The malware starts with a deceptive MSI installer, creating a dedicated folder for its files and deploying the core module, ChaesCore, which is responsible for persistence and communication with the C2 server. Seven independent modules were identified, including an initiation module, an online module, a credential stealer, and others, all with a focus on stealing sensitive information and data.

Recommendations

Implement Advanced Threat Detection: Given the sophisticated nature of Chae$ 4 and its ability to evade traditional security measures, it is crucial to invest in advanced threat detection systems. These systems can employ behavior-based analytics and anomaly detection to identify and respond to the unique characteristics of Chae$ 4 attacks.

Strengthen Web Application Security: Chae$ 4 targets prominent platforms and banks, making web application security paramount. Conduct regular security assessments and penetration testing for web applications, especially if they are linked to financial transactions. Ensure that security patches for web frameworks and content management systems are promptly applied to prevent vulnerabilities that Chae$ 4 can exploit.

Potential MITRE ATT&CK TTPs

TA0011 Command and Control	TA0005 Defense Evasion	TA0003 Persistence	TA0002 Execution
TA0006 Credential Access	TA0010 Exfiltration	T1218 System Binary Proxy Execution	T1053 Scheduled Task/Job
T1053.005 Scheduled Task	T1059.006 Python	T1059 Command and Scripting Interpreter	T1027 Obfuscated Files or Information
T1055.001 Dynamic-link Library Injection	T1555.003 Credentials from Web Browsers	T1555 Credentials from Password Stores	T1055 Process Injection
T1568.002 Domain Generation Algorithms	T1568 Dynamic Resolution	T1041 Exfiltration Over C2 Channel	T1218.007 Msiexec

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	b58161c867b2bd6ac4e2332b951b7897efd2b19f696901b078a395ddcf7d134a, 628b1ba59150a1b66167bec71d16eef23cafc167ffb47c916c69adb2ac372a57, 6d4a7488cb559035d5d06d5a94adc76188cd2dfc6a647f8a77da7565e244898c
Domains	4.q111[.]sbs, <day_domain>[.]mail89[.]us[.]to, <day_domain>[.]ns99[.]uk[.]ms
IPV4	18.228.15[.]16 18.229.122[.]137 13.248.205[.]89 13.248.185[.]41
URLs	hxxp://l-1038939961.sa-east-1.elb.amazonaws[.]com hxxp://l-1038939961.sa-east-1.elb.amazonaws[.]com

TYPE	VALUE
WebSocket URLs	ws://54.233.147[.]24 ws://18.231.31[.]151 ws://18.229.170[.]213 ws://54.94.248.[]242 ws://18.231.70[.]213 ws://18.231.91[.]245 ws://18.230.36[.]203 ws://54.232.236[.]117

References

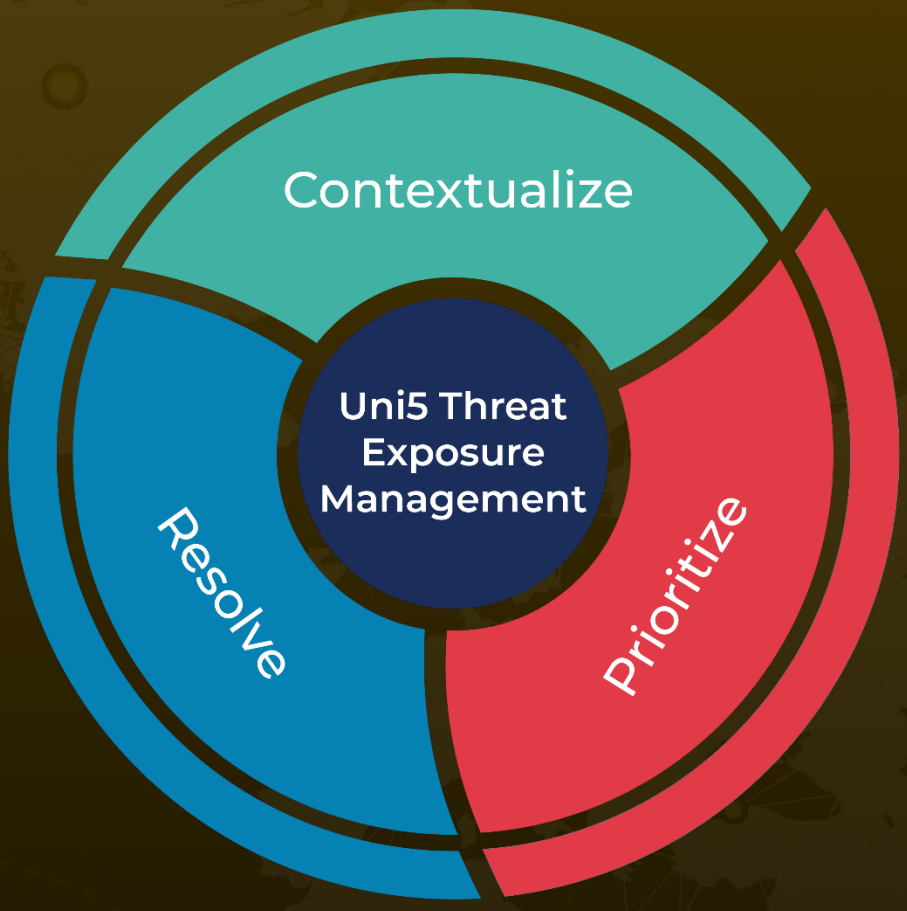
https://blog.morphisec.com/chaes4-new-chaes-malware-variant-targeting-financial-and-logistics-customers

https://www.morphisec.com/hubfs/Morphisec_Chae$4_Threat_Profile.pdf

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

September 6, 2023 • 7:30 AM

More at www.hivepro.com