Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

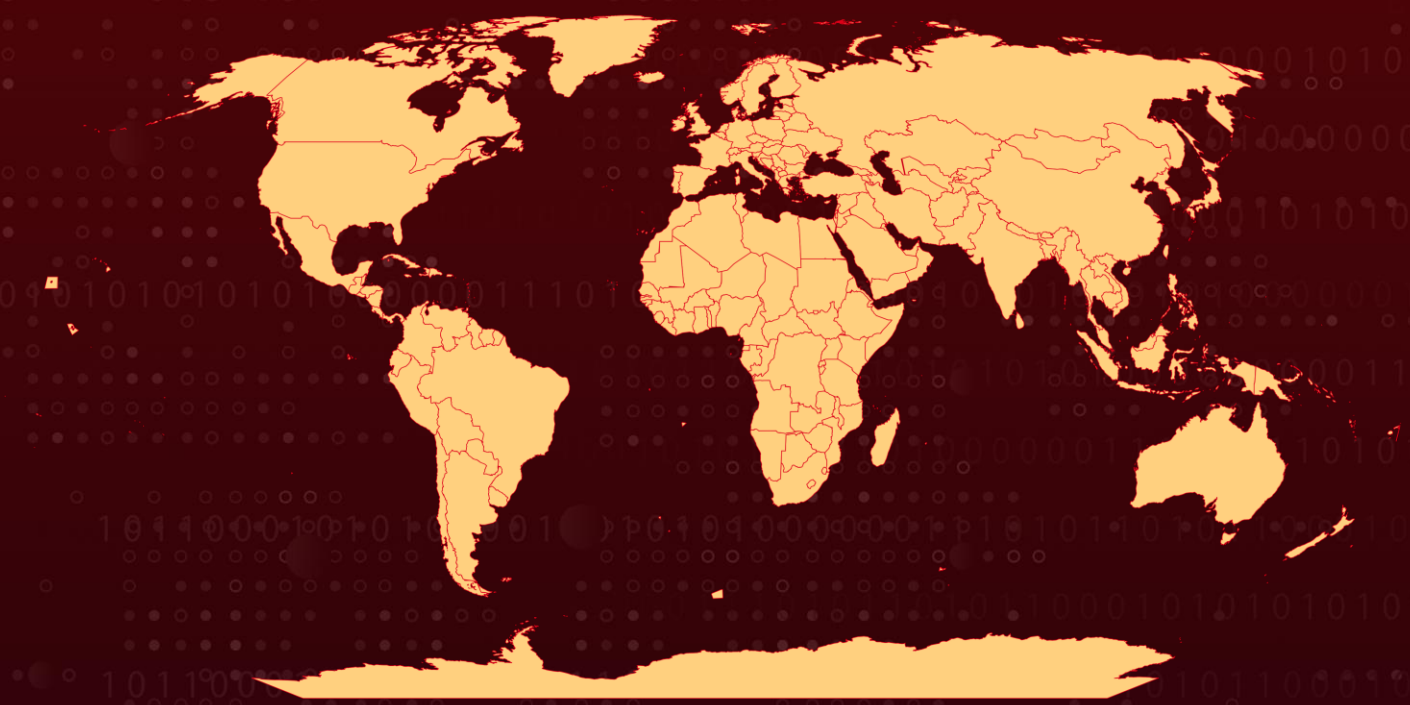
Novel Go-Based Malware Unleashes Coordinated Strikes on macOS and Windows

Date of Publication	Admiralty Code	TA Number
December 21, 2023	A1	TA2023514

Summary

Attack Discovered: July 2023
Affected Platform: Windows and macOS
Attack Region: Worldwide
Malware: JaskaGO
Attack: A recently identified threat known as JaskaGO has surfaced as a new cross-platform information stealer malware. This malware is designed to target and compromise systems running both Windows and Apple macOS operating systems.

Attack Regions



Attack Details

#1 A highly sophisticated malware stealer named JaskaGO poses a significant threat to both Windows and macOS operating systems. Developed using the Go programming language, it exhibits advanced capabilities and the potential for sustained impact. JaskaGO utilizes deceptive strategies, such as disguising itself with file names resembling legitimate applications.

#2 The malware employs a clever tactic of displaying a fake error message box, falsely indicating a missing file, to trick users into believing a code execution error has occurred. It also includes a check to determine if it's operating within a VM, analyzing various machine information parameters. In the Windows version, it searches for VM-related traces in the registry and file system.

#3 After successfully bypassing VM detection, JaskaGO collects information about the victim and establishes a connection to its C&C server. It continuously queries the server for instructions and potential commands to execute on the infected system.

#4 JaskaGO is adept at extracting data from various browsers, including Chrome and Firefox, storing the information in a specified folder. It can adapt to include additional browsers, collecting a comprehensive set of browser-related data, including credentials, browsing history, cookies, password encryption keys, profile files, and login information. The malware can also search for browser crypto wallet extensions and receive a predefined list of wallets for upload to the server.

#5 To achieve persistence on Windows, JaskaGO creates a service and generates a file ("WindowsTerminal_*\LocalState\settings.json") serving as a Windows Terminal profile for automatic execution. On macOS, it executes with root privileges, disables Gatekeeper, duplicates its presence, and creates a LaunchDaemon or LaunchAgent based on successful root access acquisition. These techniques ensure automatic launch during system startup, allowing the malware to embed itself deeply within Windows and macOS environments.

#6 JaskaGO, as a cross-platform threat, challenges the traditional belief in the invulnerability of macOS systems and underscores the vulnerability of both Windows and macOS platforms. With robust persistence mechanisms and advanced stealer capabilities, JaskaGO poses a significant threat by extracting sensitive information from its victims. This highlights the evolving landscape of cyber threats that can impact a wide range of operating systems.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Remain vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0007 Discovery	TA0011 Command and Control
TA0010 Exfiltration	TA0005 Defense Evasion	T1543 Create or Modify System Process	T1543.001 Launch Agent
T1543.003 Windows Service	T1543.004 Launch Daemon	T1082 System Information Discovery	T1057 Process Discovery
T1518 Software Discovery	T1518.001 Security Software Discovery	T1571 Non-Standard Port	T1020 Automated Exfiltration
T1041 Exfiltration Over C2 Channel	T1036 Masquerading		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	7bc872896748f346fdb2426c774477c4f6dcedc9789a44bd9d3c889f778d5c4b, f38a29d96eee9655b537fee8663d78b0c410521e1b88885650a695aad89dbe3f, 6efa29a0f9d112cfbb982f7d9c0ddfe395b0b0edb885c2d5409b33ad60ce1435, f2809656e675e9025f4845016f539b88c6887fa247113ff60642bd802e8a15d2, 85bffa4587801b863de62b8ab4b048714c5303a1129d621ce97750d2a9a989f9, 37f07cc207160109b94693f6e095780bea23e163f788882cc0263cbddac37320, e347d1833f82dc88e28b1baaa2657fe7ecbfe41b265c769cce25f1c0e181d7e0, c714f3985668865594784dba3aeda1d961acc4ea7f59a178851e609966ca5fa6, 9b23091e5e0bd973822da1ce9bf1f081987daa3ad8d2924ddc87eee6d1b4570d, 1c0e66e2ea354c745aebda07c116f869c6f17d205940bf4f19e0fdf78d5dec26, e69017e410aa185b34e713b658a5aa64bff9992ec1dbd274327a5d4173f6e559, 6cdda60ffbc0e767596eb27dc4597ad31b5f5b4ade066f727012de9e510fc186, 44d2d0e47071b96a2bd160aeed12239d4114b7ec6c15fd451501c008d53783cf, 8ad4f7e14b36ffa6eb7ab4834268a7c4651b1b44c2fc5b940246a7382897c98e, 888623644d722f35e4dcc6df83693eab38c1af88ae03e68fd30a96d4f8cbcc01, 3f139c3fcad8bd15a714a17d22895389b92852118687f62d7b4c9e57763a8867, 207b5ee9d8cbff6db8282bc89c63f85e0ccc164a6229c882ccdf6143ccefdcbc

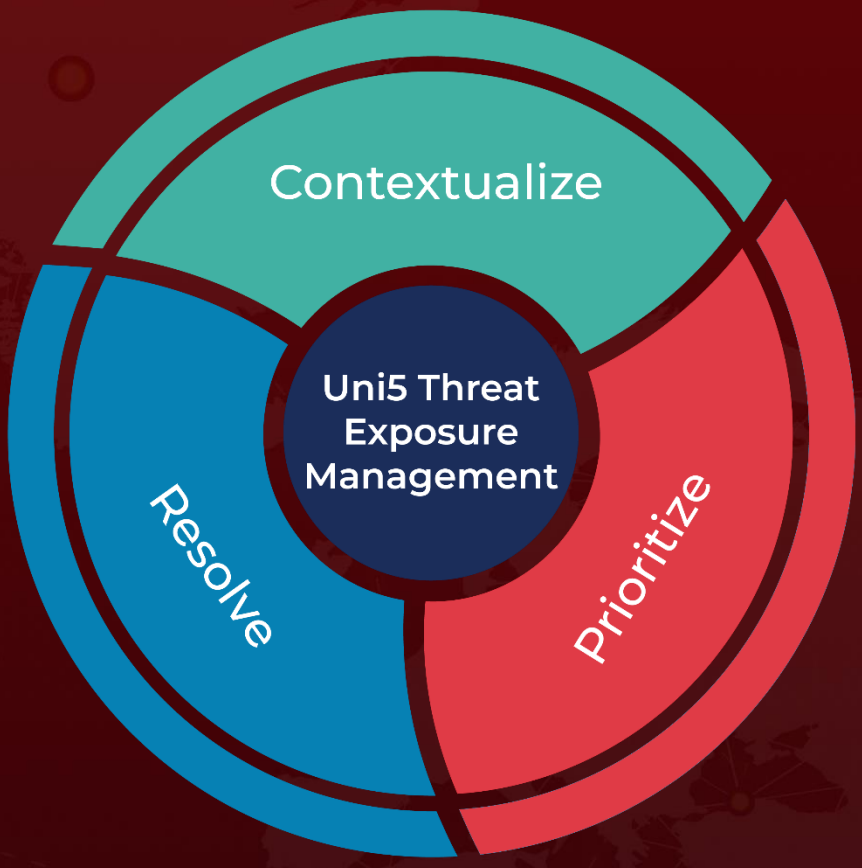
References

https://cybersecurity.att.com/blogs/labs-research/behind-the-scenes-jaskagos-coordinated-strike-on-macos-and-windows

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

December 21, 2023 . 4:10 AM

More at www.hivepro.com