Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

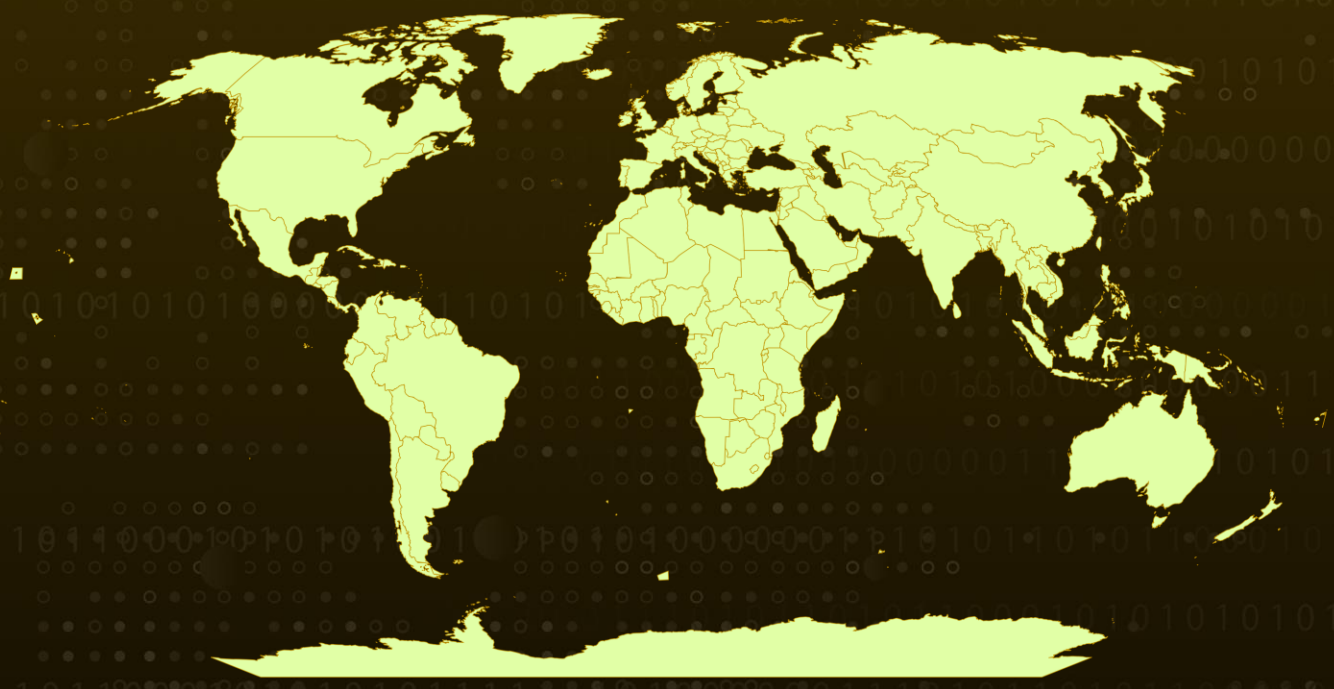
NS-STEALER Utilizes Discord Bots for Covert Exfiltration of Sensitive Data

Date of Publication	Admiralty Code	TA Number
January 23, 2024	A1	TA2024029

Summary

Attack Discovered: Mid-November 2023
Attack Region: Worldwide
Malware: NS-STEALER
Attack: A recently discovered Java-based information stealer, named NS-STEALER, employs a Discord bot channel as an EventListener to exfiltrate sensitive data from compromised hosts. This malware is distributed through ZIP archives that disguise themselves as cracked software.

Attack Regions



Attack Details

#1 In mid-November 2023, a Java-based information stealer was discovered spreading through cracked software ZIP files. It utilizes JDABuilder Classes to create an instance of an EventListener for easy registration, and the stealer uses a Discord bot channel as part of its EventListener functionality.

#2 The NS-STEALER malware, distributed through ZIP archives posing as cracked software, involves a rogue Windows shortcut file ("Loader GAYve") within the ZIP file. This shortcut file serves as a mechanism to deploy a malicious JAR file. Upon execution, the JAR file creates a folder named "NS-<11-digit_random_number>" to store the harvested data.

#3 The NS-STEALER malware, once active, proceeds to save a range of stolen data into the created folder. This includes screenshots, cookies, credentials, autofill data from over number of web browsers, system information, a list of installed programs, Discord tokens, and Steam and Telegram session data. Subsequently, the gathered information is exfiltrated to a Discord Bot channel.

#4 Additionally, the threat actor's malware scans for installed programs on the victim's machine by examining the sub-registry path. After successfully collecting all the targeted information, it is stored in the folder. The malware then initiates a zip operation. Upon completion of the zipping process, the original folder is deleted from the specified location.

#5 The malware, with its sophisticated functionality of acquiring sensitive information and utilizing X509 Certificate for authentication, is adept at swiftly extracting data from victim systems. Moreover, its cost-effective approach of using the Discord Bot channel as an EventListener for data exfiltration makes it a potent tool for threat actors.

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.

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.

Avoid cracked software: It is strongly advised to refrain from using cracked or free software obtained from unofficial sources, as these versions often come with hidden malware. Opt for legitimate and licensed software from official vendors to ensure the integrity and security of your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0010** Exfiltration	**T1566** Phishing
T1059 Command and Scripting Interpreter	**T1036** Masquerading	**T1539** Steal Web Session Cookie	**T1074** Data Staged
T1082 System Information Discovery	**T1124** System Time Discovery	**T1033** System Owner/User Discovery	**T1020** Automated Exfiltration
T1518 Software Discovery	**T1204** User Execution	**T1560** Archive Collected Data	**T1113** Screen Capture

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f02496f4b9da09ae0fbf1b59fbdc4b2193cc9e03134ee4c5e71141bb618fdd0c, 506b40e0f199b32a597bb44aa90343cc14830796f2bf3fd7c3fa281a52ce27c9,

TYPE	VALUE
SHA256	6d6c788c928c1408dd19de83b6dd1a12092c96b179fc17a66414886cf8d1daf0, 90ba262acdb6fd1ead5167a7347a1d66ee0075c24ed18d5b4cb07933a4c42805, a8be7f50b0554e519a8c98ec39d2ba76e0655da133c8795a41d36dc29d9c7433, d5a528f524401a36a6366619f3b2d83efed740801128f527e9dce80e68060922, ded871d290ad309d228c00107d87e88dfadbc9d682ff3e04d9fb63f2c34aa256, ecb4b09bfd34adc671537c98d1b1cd6f662e66077904db0da9f88e2054ef9edd, 85eec9d888d584c33b597d6e40f1a74b4d00db9838d681339b845bb87c14cd10, 3dd8439a4fcc880a5cd5df005e15638be298993c141c200e47c769ef2e3ca1f4, 3dc895e597d503590ef117dd942709a180392c9522c704901e272113bea8310f, 9486f5c47b037e87732c0c7d7d686334d7c3761133735f8b6d65b3aa479ec113, 3013ab2c5c8c8a217e9484f6a46fbacacbce92475dbe7f8d5e3f04d23974de83, eb845853386ca89043ac04ec399e5111a906fd2bcde24ab02494eb035fdd1224, 89665ab4e6ed00809208a4656bc38da81831fd4b8044d7039e5542fe47b81d0e, bcff5e6d151126f0c3691b8c0fc46fb4e586ee5559068ac3acc2bd478c1c9ca1

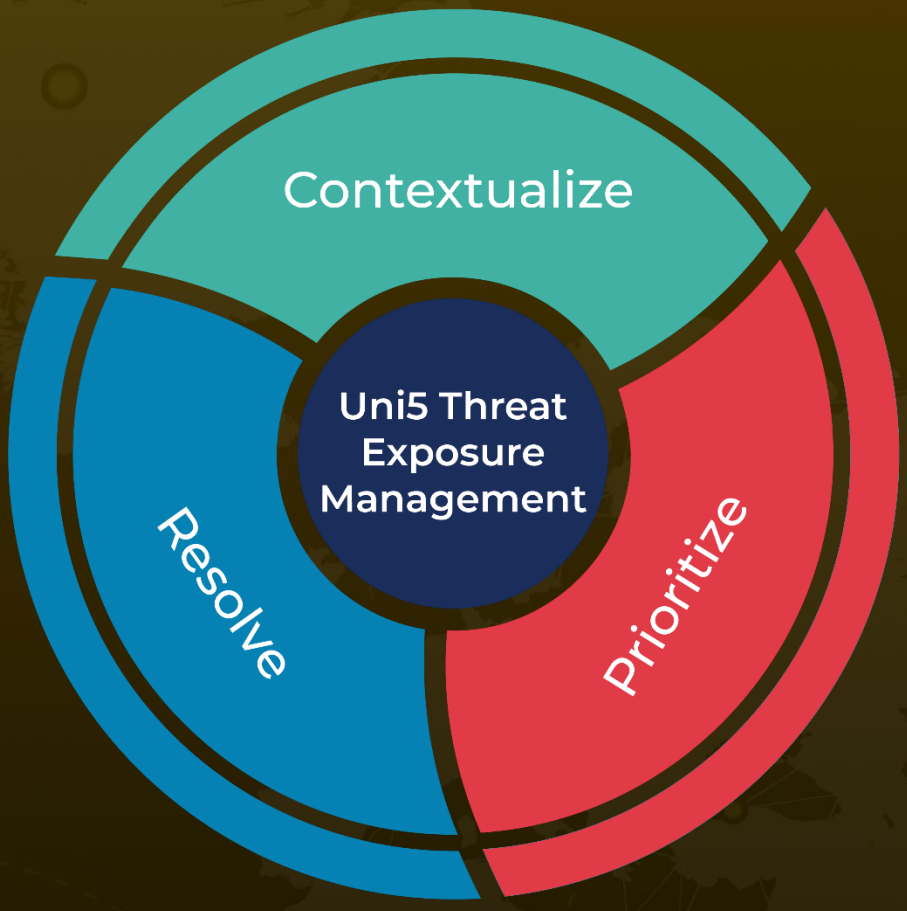
References

https://www.trellix.com/about/newsroom/stories/research/java-based-sophisticated-stealer-using-discord-bot-as-eventlistener/

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 23, 2024 • 4:05 AM

More at www.hivepro.com