Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

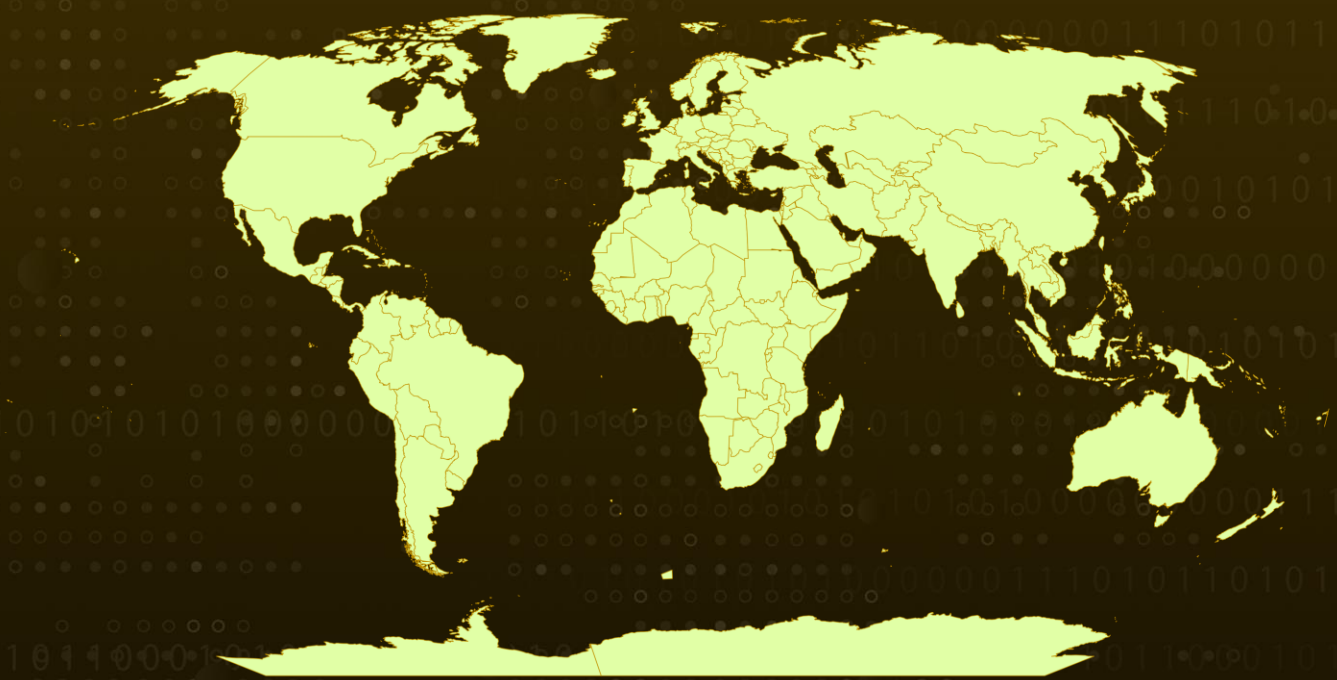
Jellyfish Loader: When Innocent Files Turn Malicious

Date of Publication	Admiralty Code	TA Number
July 23, 2024	A1	TA2024279

Summary

Malware: Jellyfish Loader
Attack Region: Worldwide
Attack: The Jellyfish Loader is a newly discovered .NET-based shellcode loader engineered for malicious purposes. It distinguishes itself by using asynchronous task method builders to execute code, securely gather and transmit system information, and prepare for the execution of additional malicious code delivered by the C&C server.

Attack Regions



Attack Details

#1 The Jellyfish Loader is a newly discovered .NET-based shellcode loader. It uses asynchronous methods to execute code and integrates its dependencies within the executable using tools like Fody and Costura.

#2 The attack chain of the Jellyfish Loader begins by deceiving the user into opening a malicious ZIP file containing a Windows shortcut (.lnk) file. When executed, this .lnk file opens a benign PDF while simultaneously downloading and executing the Jellyfish Loader.

#3 The .lnk file executes JavaScript via mshta.exe, which then retrieves the Jellyfish Loader executable from a remote URL. Once executed, the Jellyfish Loader collects basic system information from the infected machine, encoding this data in JSON format and further obfuscating it with Base64 encoding. This prepares the loader to execute additional malicious code from the C&C server.

#4 Notably, the Jellyfish Loader can send system information upon infection and validate SSL certificates before communicating with its Command and Control (C&C) server. It then sends a shellcode to the infected machine for further malicious actions.

Recommendations

Enhance Email Security Measures: Implement robust email filtering solutions to detect and block malicious attachments, such as ZIP and .lnk files. Educate users about phishing tactics and the dangers of opening attachments from unknown or suspicious sources.

Strengthen Network Security: Utilize Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to identify and block malicious network traffic. Implement network segmentation to limit the spread of malware within the organization.

Utilize Application Control and Whitelisting: Implement application whitelisting to allow only approved applications to run on endpoints. Use application control solutions to monitor and block unauthorized or suspicious applications.

Deploy Secure Web Gateways: Use secure web gateways to block access to known malicious websites and URLs. Monitor and filter outbound network traffic to detect and prevent data exfiltration.

Monitor SSL/TLS Traffic: Inspect SSL/TLS traffic to detect and block malicious communications between infected machines and C&C servers. Ensure that SSL certificates are properly validated to prevent man-in-the-middle attacks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control
TA0010 Exfiltration	**T1204** User Execution	**T1204.001** Malicious Link	**T1036** Masquerading
T1036.008 Masquerade File Type	**T1082** System Information Discovery	**T1573** Encrypted Channel	**T1071.001** Web Protocols
T1071 Application Layer Protocol	**T1041** Exfiltration Over C2 Channel	**T1105** Ingress Tool Transfer	**T1140** Deobfuscate/Decode Files or Information
T1059.007 JavaScript	**T1083** File and Directory Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	ab9c3ef0b8bb1d68d819d569c8276af0, 300b380bf870010f14bfeeeccbdc9729, e577fa8e0491fe027bc4da86a01f64ea

TYPE	VALUE
SHA1	00e0824e139e21fd6e41e2a34c1d6f598d7e4fbe, d4adb79a3809989569fb24aa43c947ef69b8aee1, 9ff473df01487ca59d6426c8fddf77a1c27b2437
SHA256	66d24e2081fcfe3ffdcf80e208553f32b088c7e863668ab3813ba980e1efbc2c, 6d47ce1660eb54a31e7870b170605f9641ec97d756fb865f3a5e357649dc2041, e654e97efb6214bea46874a49e173a3f8b40ef30fd0179b1797d14bcc2c2aa6c
URL	hxxps[:]//ping[.]connectivity-check[.]com/

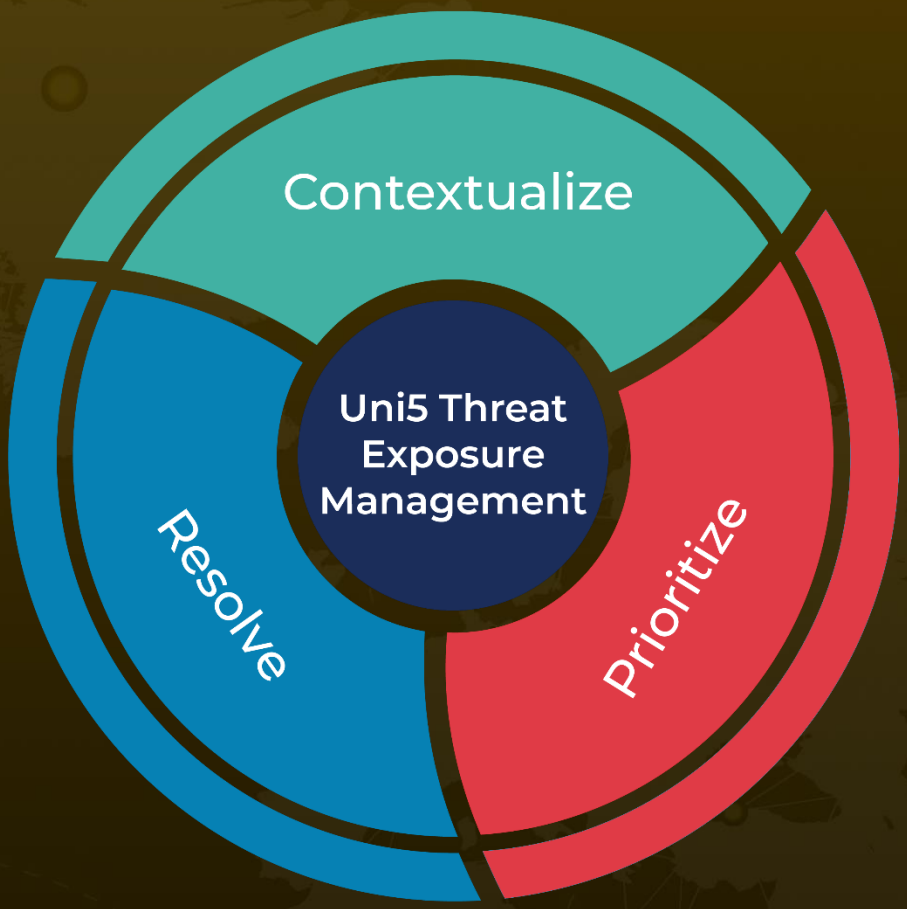
References

https://cyble.com/blog/investigating-the-new-jellyfish-loader/

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 23, 2024 • 3:30 AM

More at www.hivepro.com