

HiveForce Labs

THREAT ADVISORY

 **ATTACK REPORT**

A Fresh Look at the Bumblebee's Comeback Strategies

Date of Publication

February 16, 2024

Admiralty Code

A1

TA Number

TA2024062

Summary

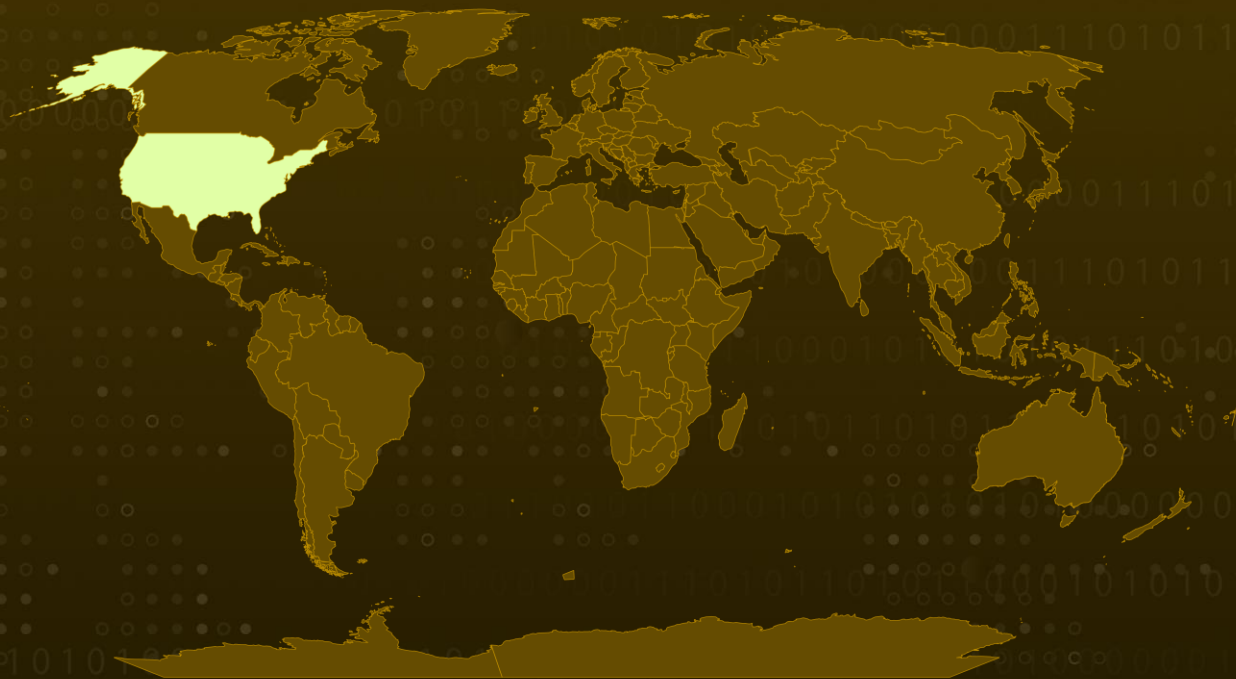
Attack Commenced: February 8, 2024

Malware: Bumblebee

Attack Region: USA




Attack: BumbleBee, a malicious loader discovered in March 2022, resurfaced in the cyber threat landscape on February 8, 2024, after a four-month hiatus. Unlike in previous campaigns, this attack chain diverges from conventional techniques.

Attack Regions



CVEs

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	RARLAB WinRAR			

Attack Details

#1

BumbleBee, a malicious loader identified in March 2022, is coded in C++ and has been employed by various threat actors, potentially serving as an initial access broker. It orchestrates the download and execution of additional payloads until October 2023, only to reemerge in the cyber threat landscape on February 8, 2024, following a four-month break.

#2

The modus operandi for initial access involves phishing emails strategically targeting United States organizations. These emails contain OneDrive URLs that facilitate the download of a Word document, which disguises its malicious intent by posing as correspondence from a renowned consumer electronics company recognized for its AI-driven innovation.

#3

The nefarious document utilizes macros to generate a script file within the Windows temp folder, subsequently employing the "wscript" command to execute the dropped file. This temporary file harbors a PowerShell command designed to retrieve and execute the next stage from a remote server, ultimately downloading and launching the Bumblebee DLL on the victim's system.

#4

In contrast to previous Bumblebee campaigns that employed direct DLL downloads, HTML smuggling, and exploited vulnerabilities like CVE-2023-38831 to deliver the final payload, the current attack chain marks a noteworthy departure from more contemporary techniques.

Recommendations



Continuous Monitoring and Analysis: Establish continuous monitoring and analysis protocols to promptly detect any unusual network behavior, potentially indicating a long-term cyber espionage operation.



Network Segmentation: Employ network segmentation to isolate critical systems and sensitive data, limiting the lateral movement of an attacker within the network in case of a successful infiltration.



Heighten Awareness: Familiarize yourself with common phishing tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

<u>TA0002</u> Execution	<u>TA0003</u> Persistence	<u>TA0004</u> Privilege Escalation	<u>TA0005</u> Defense Evasion
<u>TA0010</u> Exfiltration	<u>TA0011</u> Command and Control	<u>T1059</u> Command and Scripting Interpreter	<u>T1059.001</u> PowerShell
<u>T1070</u> Indicator Removal	<u>T1105</u> Ingress Tool Transfer	<u>T1036</u> Masquerading	<u>T1027</u> Obfuscated Files or Information
<u>T1566.001</u> Spearphishing Attachment	<u>T1566.002</u> Spearphishing Link	<u>T1055</u> Process Injection	<u>T1082</u> System Information Discovery
<u>T1204</u> User Execution	<u>T1068</u> Exploitation for Privilege Escalation	<u>T1211</u> Exploitation for Defense Evasion	<u>T1588.006</u> Vulnerabilities

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//1drv[.]ms/w/s!At-ya4h-odvFe-M3JKvLzB19GQA?e=djPGy, hxxps[:]//1drv[.]ms/w/s!AuSuRB5deTxugQ-83_HzIqbBWuE1?e=9f2plW, hxxp[:]//213[.]139.205.131/update_ver, hxxp[:]//213[.]139.205.131/w_ver.dat
Domain	q905hr35[.]life
IPv4:Port	49[.]13[.]76[.]144:443

TYPE	VALUE
SHA256	0cef17ba672793d8e32216240706cf46e3a2894d0e558906a1782405a8f4decf, 86a7da7c7ed5b915080ad5eaa0fdb810f7e91aa3e86034cbab13c59d3c581c0e, 2bc95ede5c16f9be01d91e0d7b0231d3c75384c37bfd970d57caca1e2bbe730f, c34e5d36bd3a9a6fca92e900ab015aa50bb20d2cd6c0b6e03d070efe09ee689a

Patch Details

Update WinRAR version to 6.23 or later versions

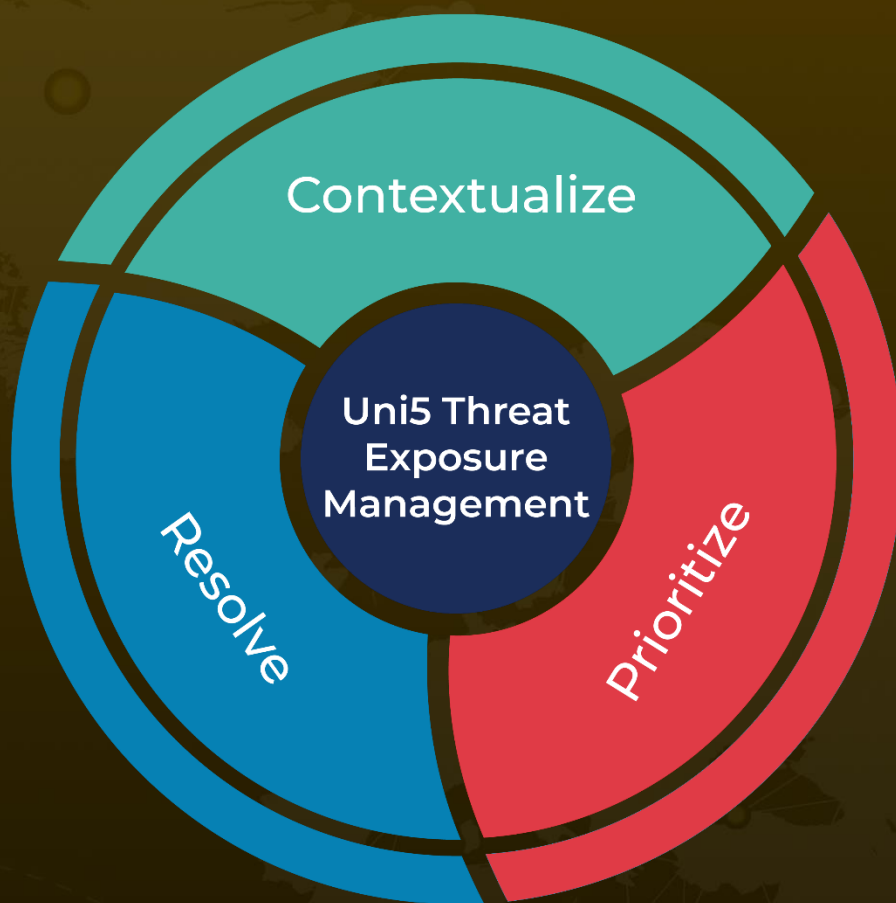
References

<https://www.proofpoint.com/us/blog/threat-insight/bumblebee-buzzes-back-black>

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

February 16, 2024 • 4:30 AM

© 2024 All Rights are Reserved by Hive Pro®



More at www.hivepro.com