Bumblebee malware attacks are back after 4-month break

Date: 14th February 2024 | Severity: High

Summary

The infamous malware loader and initial access broker known as Bumblebee has resurfaced after a four-month absence as part of a new phishing campaign observed in February 2024.

Enterprise security firm Proofpoint said the activity targets organizations in the U.S. with voicemail-themed lures containing links to OneDrive URLs.

"The URLs led to a Word file with names such as "ReleaseEvans#96.docm" (the digits before the file extension varied)," the company said in a Tuesday report. "The Word document spoofed the consumer electronics company Humane."

Attack Vectors

- The Initial Access and Defense Evasion tactics with Phishing (T1566), Process Injection (T1055), and Signed Binary Proxy Execution (T1218) as the primary techniques.
- The infamous malware loader and initial access broker known as Bumblebee has resurfaced after a four-month absence as part of a new phishing campaign observed in February 2024.
- "The URLs led to a Word file with names such as "ReleaseEvans#96.docm" (the digits before the file extension varied)," the company said in a Tuesday report. "The Word document spoofed the consumer electronics company Humane."
- Enterprise security firm Proofpoint said the activity targets organizations in the U.S. with voicemail-themed lures containing links to OneDrive URLs.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	90576eb6754dd1c38fb4cea4bf3f029535900436a02caee891c057c01ca84941 78c5d780b2ca553cbd3fb0140813e0e1fb7c48491090df605f03c309d0086baf 7db1126c80901edbc3be6948f208d4c450a23ea453ecf2e684bb4c8363c60db0 598b792b8231a4d897d71d95437043730fbb423f2863b8261d29a1e5712c9919 422c03f96a72fdd657c2ebca1387bd1f6be6e0b1b30a352827c48ef6fc16995e 9dfb32ed9b5756151623a8049eaa7785bf761601eb6c7165beff489cce31bb08

Recommendation

Submit the File Hash to the Antivirus team to update their database with the file hashes.

Make regular backups of important and critical files.

Avoid browsing the unsafe websites, clicking on suspicious links, or opening unknown email attachments.

Update and Patch operating system, applications, and security software's up to date with latest patches.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

https://www.bleepingcomputer.com/news/security/bumblebee-malware-attacks-are-back-after-4-month-break/

https://www.socinvestigation.com/bumblebee-malware-loader-is-now-active-in-the-wild-detection-response/