BumbleBee: a new trendy loader for Initial Access Brokers

By Quentin Bourgue, Pierre Le Bourhis and Sekoia TDR

Published: 2022-06-13 · Archived: 2026-04-10 03:10:50 UTC

Table of contents

This blog post on BumbleBee malware was originally published as a FLINT report (SEKOIA.IO Flash Intelligence) sent to our clients on June 02, 2022.

BumbleBee is a new malicious loader, first reported by Google TAG in March 2022, that is being used by several **Initial Access Brokers** (IABs) to gain an initial foothold within victims' networks.

In recent weeks, many campaigns distributing BumbleBee have been observed in the wild and the successful compromises often **lead to ransomware attacks**. Indeed, affiliates of several ransomware gangs (Conti, LockBit, AvosLocker, Diavol) were observed delivering BumbleBee in order to **drop another payload** (Cobalt Strike, Meterpreter, Sliver, IcedID, Redline, and more) and deploy ransomware. Furthermore, SEKOIA.IO analysts observed the malware is still **in development** with new features, and improvements. All these reasons make the BumbleBee loader a major threat that companies must deal with at the moment.

SEKOIA.IO analysts have been tracking this threat since early April 2022 and have seen a **significant increase in the number of active BumbleBee C2 servers**, and observed samples. The analysis of multiple BumbleBee samples allowed us to **identify several versions and improvements** made to the product.

Technical Analysis

In this section, we briefly describe the typical infection chain used to deliver the BumbleBee loader. We then share technical details on the modifications made in the latest versions of the malware, and how we track the active C2 server and the malware samples.

Before getting into the technical details, the BumbleBee malware is a sophisticated loader that aims to download and execute a second payload. It implements several defense and evasion techniques to hide from detection systems, and to make it harder for security researchers to analyze the payload.

Typical infection chain

Most of the spearphishing campaigns distributing the BumbleBee loader use the same attack pattern: an email is sent to the victim with a ZIP archive which contains an ISO file. The beginning of the attack chain consists of using an ISO file which contains a Windows link (LNK) used to execute the payload (DLL).

In the following example, the ISO file contains two files:

1. a LNK file `New Folder.lnk`
2. a DLL executed by the LNK file

As shown in the figure below, when the LNK file is executed, it runs the command below to start the malicious DLL using `rundll32.exe` : `C:\\Windows\\System32\\rundll32.exe procsvc.dll,HWgullOFkZ`

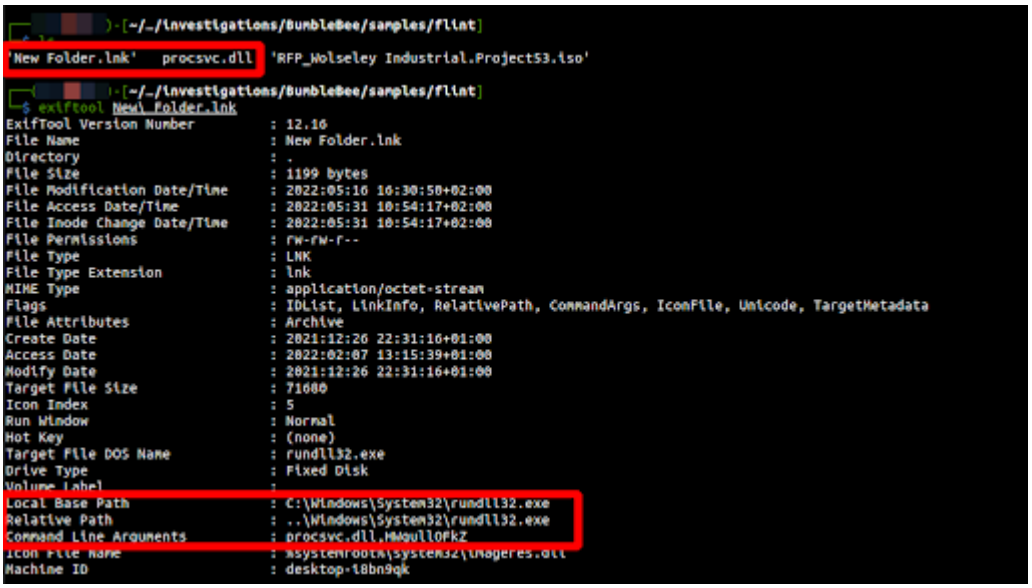

Figure 1. Example of an attachment (uncompressed ISO file) from a spearphishing campaign distributing BumbleBee

This infection vector is more and more used by various actors: APT (such as NOBELIUM) , IABs (to distribute IcedID, BazarLoader, BumbleBee, and more) and other threat actors. This trend appears to be the consequence of the disabling by default of VBA macros in Microsoft Office products, which is one (code execution via Office macros) of the most used techniques by adversaries to get into the network.

Modifications in the latest version

The BumbleBee DLL uses a crypter to deobfuscate another PE that is loaded in a new memory section. This specific section is quickly identifiable: a simple pattern search in a debugger on “DOS mode” can highlight the newly allocated memory with read-write-execute permission.

Once the new section is dumped, the BumbleBee payload can be analyzed. Before anything else, it is worth noting that the malware used almost a full copy/paste of al-khaser github project, as mentioned in others articles or related BumbleBee discussions. The al-khaser code implements several anti-detection techniques. The figure below shows that the main function of the BumbleBee payload avoids execution if one of the anti-virtual environments is spotted.

```
42  if ( check_mac_addr(byte_1CF59B46BB8) )
43    return 1;
44  v1 = 0;
45  if ( GetProcessIdFromName(L"procexp64.exe") )
46    return 1;
47  v2 = sub_1CF59B01540() == 0;
48  if ( !v2 )
49    return 1;
50  ModuleHandleW = GetModuleHandleW(L"kernel32.dll");
51  if ( ModuleHandleW )
52    v4 = GetProcAddress(ModuleHandleW, "wine_get_unix_file_name") != 0i64;
53  else
54    v4 = 0;
55  v5 = v2 & !v4 & (wine_reg_keys() == 0);
56  if ( !v5 )
57    return 1;
58  v6 = v5 & (vbox_reg_key_value() == 0);
59  v7 = (vbox_reg_keys() == 0) & v6;
60  v8 = (vbox_files() == 0) & v7;
61  v9 = v8 & !vbox_dir();
62  if ( !v9 )
63    return 1;
64  v10 = v9 & (check_mac_addr(L"\b") == 0);
65  v11 = (vbox_devices() == 0) & v10;
66  WindowW = FindWindowW(L"VBoxTrayToolWndClass", 0i64);
67  v13 = FindWindowW(0i64, L"VBoxTrayToolWnd");
68  if ( WindowW || (v14 = 0, v13) )
69    v14 = 1;
70  v15 = (v14 ^ 1) & !vbox_network_share() & v11;
71  v16 = (vbox_processes() == 0) & v15;
72  v17 = (vbox_mac_wmi() == 0) & v16;
73  v18 = (vbox_eventlogfile_wmi() == 0) & v17;
```

Figure 2. *Anti-virtual machine checks in the BumbleBee code*

Once the loaded PE is ready and anti-VM checks are passed, the malware decrypts its Command and Control (C2) IP addresses with a key stored in cleartext in the `.data` section using RC4 algorithm. This decryption routine is also used to deobfuscate its campaign ID.

```
1  __int64 __fastcall sub_1CF59AC12A0(unsigned __int8 *input_data, __int64 output_cleartext, int length)
2  {
3    int i; // [rsp+8h] [rbp-28h]
4    unsigned __int8 v5; // [rsp+Ch] [rbp-24h]
5    unsigned __int8 v6; // [rsp+Dh] [rbp-23h]
6    unsigned __int8 v7; // [rsp+Eh] [rbp-22h]
7    unsigned __int8 v8; // [rsp+Fh] [rbp-21h]
8
9    if ( (input_data[258] & 1) != 0 )
10   {
11     v8 = *input_data;
12     v7 = input_data[1];
13     for ( i = 0; i < length; ++i )
14     {
15       v6 = input_data[++v8 + 2];
16       v7 += v6;
17       v5 = input_data[v7 + 2];
18       input_data[v8 + 2] = v5;
19       input_data[v7 + 2] = v6;
20       *(_BYTE *)(output_cleartext + i) = ~input_data[(unsigned __int8)(v5 + v6) + 2] & *(_BYTE *)(output_cleartext + i) | ~*(_BYTE *)(output_cleartext + i) & input_data[(unsigned __int8)(v5 + v6) + 2];
21     }
22     *input_data = v8;
23     input_data[1] = v7;
24   }
25   return input_data[258] & 1;
26 }
```

Figure 3. *Deobfuscation routine in BumbleBee loader*

In most of the payloads we investigate, three blobs of data are obfuscated using RC4:

1. A list of C2 IP addresses with their associated port
2. A campaign identifier, other analysts identify this ID as the botnet ID
3. A number (often 444 or 4444)

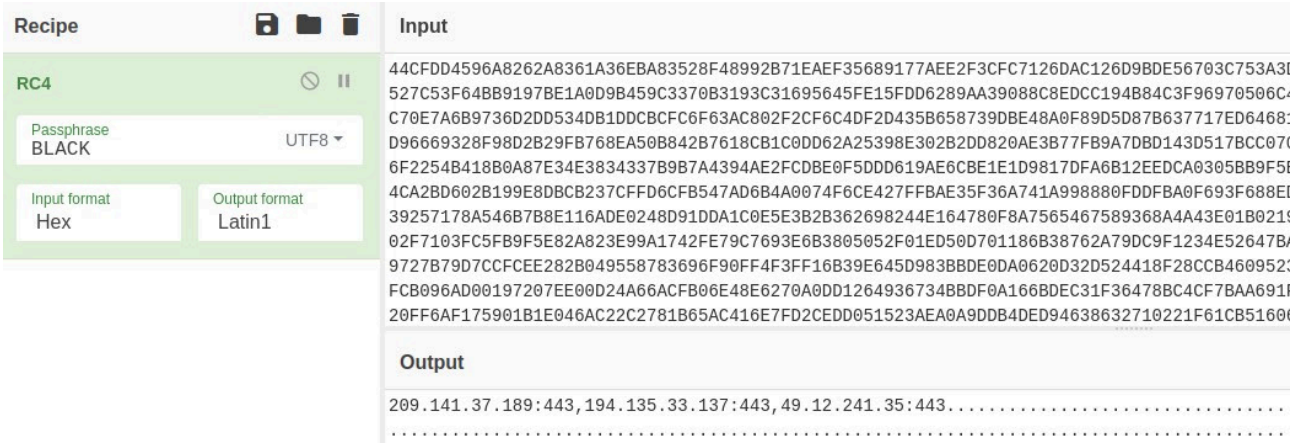

Figure 4. *Recipe in CyberChef to get the obfuscated data*

Once, the C2 IP addresses have been deobfuscated, the malware contacts one of its C2 and then loads the final payload (Meterpreter, Cobalt Strike, or else).

In the initial BumbleBee versions analyzed in April 2022, the malware did not implement any C2 obfuscation: the IP addresses were stored in clear in the PE. This evolution shows that BumbleBee is still under development.

NB: We observed a massive usage of the key “ `BLACK` *” in the dataset of samples we analyzed and also the key “* `iKInPE9WrB` *“.*

Tracking BumbleBee

C2 infrastructure

Tracking the BumbleBee C2 infrastructure is not much different from other botnets such as BazarLoader, Qakbot and IcedID. The SSL certificates used for the BumbleBee C2 server are quite specific. After some analysis of malware samples and thanks to search engines for Internet-connected devices, we were able to identify a common and unique pattern to find the BumbleBee C2 servers. The final heuristic is based on the SSL certificate and the HTTP response.

The heuristic results have increased, from 5 C2 servers at the beginning of April to over 130 at the time of writing this FLINT, as shown by the following figure.

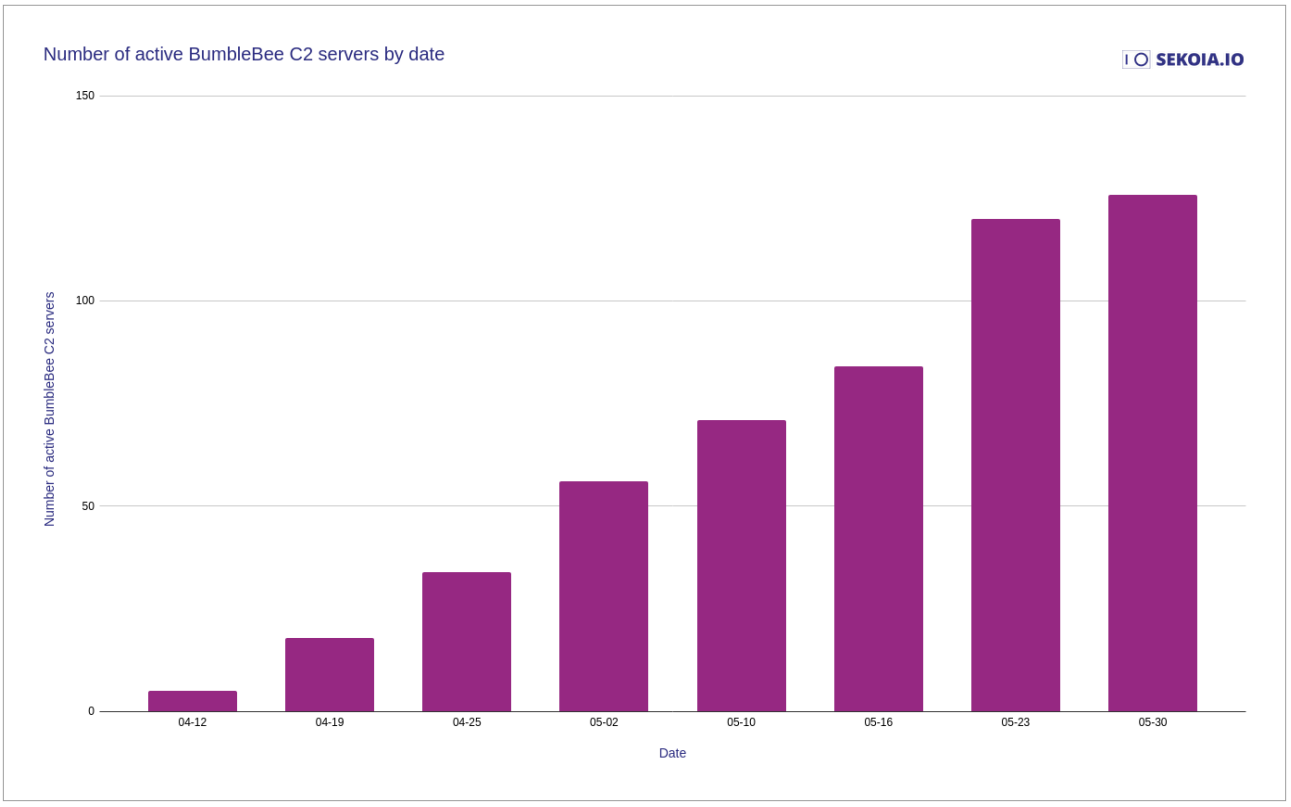

Figure 5. *Number of active BumbleBee C2 servers by date*

This shows that the BumbleBee loader has gained in popularity among the threat actors, particularly for the Initial Access Brokers.

Samples

At the same time, we have written a YARA rule to find BumbleBee samples – it can be found in the section of IOCs & Technical Details. The results of the YARA rule uploaded on a sample sharing platform confirm the trend described previously.

BumbleBee has become in two months a **major threat**, mostly deployed by Initial Access Brokers to gain a foothold within a network and drop a second payload. With the malware being used by affiliates of ransomware gangs, companies need to **monitor this threat** and **protect their assets** from possible BumbleBee compromises.

IOCs & Technical Details

BumbleBee's C2 servers

```
23.82.140[.]133
23.254.217[.]20
23.254.227[.]144
37.120.198[.]248
49.12.241[.]35
51.68.144[.]94
```

```
51.68.146[.]200
51.68.147[.]233
51.75.62[.]99
51.83.251[.]245
51.83.253[.]244
51.83.254[.]164
54.37.130[.]166
54.37.131[.]107
54.38.136[.]187
54.38.137[.]18
54.38.138[.]141
54.38.139[.]20
64.44.101[.]250
64.44.102[.]6
64.44.102[.]150
64.44.135[.]230
64.44.135[.]250
70.34.216[.]103
104.168.156[.]224
145.239.29[.]119
145.239.30[.]26
146.70.95[.]244
146.70.106[.]47
167.235.245[.]35
176.107.177[.]124
192.236.161[.]191
192.236.162[.]127
192.236.194[.]136
193.29.104[.]147
193.233.203[.]156
194.37.97[.]135
209.141.52[.]25
```

BumbleBee's SHA-25

```
e2147cb6039d1b065b0d59d6e60a1e5f526415afefdfddcbbd7b1e8a33194d64
064d21a62fc8718a707c3cf6ca91fddeb2fd407dfee47a923638a91a57b338a4
7140becbc882cab84038ad87e977cd3cb0dc864d2437eb1e2aebab78cc3eb193
0f78561577ce1a5ab8b98634fb9b2ff0392e173fb354e3625f6bab53e0f28b05
94f7bc1e910866c5ed1b06242e82c8d5379d143123ff255b87fc78db98c49ae2
2ca8fcce17d0ca5dc6c260c34b14b969fbc20c4a4520e19aed0a0be23a199243
7b3a33baf89095f9b7d2be8dfa184c274e7f27a05a7e57faf8b32882a60bfe5c
3a2112ed78bbec16929d9f39aca09efe2eb44abb80bbfa765e451a87aef84a99
85019644110b9473b93e3757ed9b324666ac515a1b91afdfbc3b17241b2d9376
873aa6d30e38c79b478eb04a83104bb31fd62989d3cca4b61164065038dadd29
7413426f5afd78b7abc0ca0a3035c2f8578c41e18548ad530ead3ee93f638a3c
```

```
86984171de311b006bc86780e5a415b3698edb864d42e72f851a7d64c2656748
9d6808021c1336763e212c787a669eb0400b089e586457b88373dd87dfcf41c9
ea6690f028157aec343e21484eab136379e35c6296b3e8eab4a7ba7bdfe13e5d
8709e8dfe6bf8b8fdc91c342fc2da948d5b77b05e7a6dba79866f42dfe8ca04b
1389ec4bde4a8970e95d8a48438395578ae81e0649f33c5ca0febe062e56712c
fad36c037c93c48ef5cdf31b8ed31e452a100ad14b75dce88597ef1eea115e9e
```

YARA rule

```
rule loader_win_bumblebee {
  meta:
     version = "1.0"
     malware = "BumbleBee"
     reference = "https://blog.sekoia.io/bumblebee-a-new-trendy-loader-for-initial-access-brokers/"
     source = "SEKOIA.IO"
     classification = "TLP:WHITE"

  strings:
     $str0 = { 5a 00 3a 00 5c 00 68 00 6f 00 6f 00 6b 00 65 00 72 00 32 00 5c 00 43 00 6f 00 6d 00 6d 00 6f 00
     $str1 = "/gates" ascii
     $str2 = "3C29FEA2-6FE8-4BF9-B98A-0E3442115F67" wide

  condition:
     uint16be(0) == 0x4d5a and all of them
}
```

External References

- [Google] Exposing initial access broker with ties to Conti
- [Cynet] Orion Threat Alert: Flight of the BumbleBee
- [Eli Salem's Medium] The chronicles of Bumblebee: The Hook, the Bee, and the Trickbot connection
- [Proofpoint] This isn't Optimus Prime's Bumblebee but it's Still Transforming
- [Github] Al-Khaser v0.81

You can also read our article on:

Chat with our team!

Would you like to know more about our solutions?
Do you want to discover our XDR and CTI products?
Do you have a cybersecurity project in your organization?
Make an appointment and meet us!

Share

CTI Detection Ransomware

Share this post:
