BumbleBee hunting with a Velociraptor

Published: 2023-04-11 · Archived: 2026-04-05 17:40:05 UTC

11.04.2023

research

BumbleBee, a malware which is mainly abused by threat actors in data exfiltration and ransomware incidents, was recently analyzed by Angelo Violetti of SEC Defence - the SEC Consult Digital Forensics and Incident Response team.

During his research, he used several tools and techniques to define ways to detect the presence of BumbleBee on a compromised infrastructure.

The various detection opportunities described in the report can be useful for organizations to detect an infection in its first stages and, therefore, prevent further malicious activity starting from BumbleBee. The detection opportunities rely on open-source tools (e.g., Velociraptor) and rules (e.g., Yara, Sigma) so they can be used by any company or the wider community.

SEC Defence offers Threat Hunting and Incident Response services to support clients in promptly detecting and responding to cyber threats such as BumbleBee. To request immediate support in case of a potential incident or breach, get in touch with SEC Defence.

Introduction

Ransomware attacks, combined with **data exfiltration**, are one of the **most relevant cyber threats** for companies worldwide, as reported by the Enisa Threat Landscape 2022. According to the NIST's Incident Handling guide, the prevention and detection phases of those types of attacks can be crucial to minimize the potential incident's impacts (e.g., operational, legal, etc.).

To gain initial access into a victim’s infrastructure, ransomware operators abuse mostly the following techniques:

- **Phishing campaigns**, also conducted by initial access brokers[1], that deliver malware which acts as a loader for subsequent post-exploitation frameworks like Cobalt Strike or Meterpreter.

- **Exposed vulnerable services** that can be exploited to execute arbitrary commands remotely.
- **Compromised accounts** that allow the threat actor to login into services like VPN.

One of the newest malware families, first discovered by the Google Threat Analysis Group in 2021, and delivered by initial access brokers is called BumbleBee and it has been used by the well-known Russian group *Wizard Spider* which has been linked to ransomware like Conti, Quantum, Royal, etc.

In this article, SEC Defence shows the analysis that has been performed of a BumbleBee sample and provides some threat hunting methods to detect BumbleBee techniques.

BumbleBee

BumbleBee is commonly distributed via malicious ISO images. and abuses thread-hijacking emails to induce the victims to download the ISO file and subsequently open it. When executed, BumbleBee performs mainly the following actions:

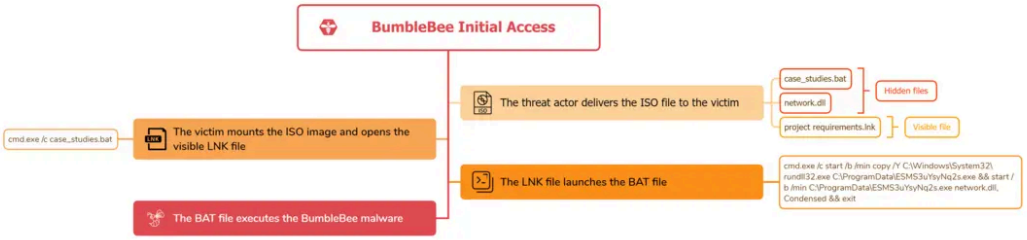
- Verifies if it is running in an analysis or sandboxing environment by performing various checks like enumerating the registry keys and drivers related to VMware or VirtualBox.
- Gathers information about the compromised system through WMI queries.
- Connects to the command and control (C2) servers embedded into the malware configuration that is RC4 encrypted.

Furthermore, BumbleBee can also receive specific commands from the threat actors that can be useful for further malicious actions like achieving persistence and downloading other malware (e.g., Cobalt Strike).

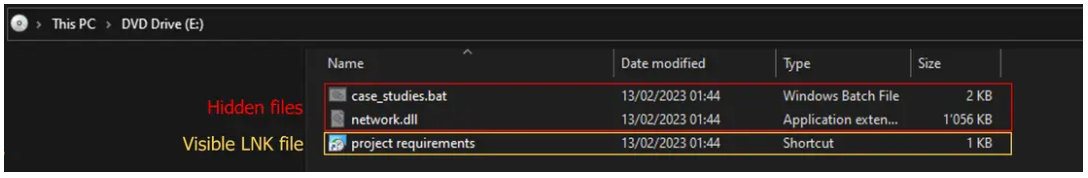
Malware Analysis & Detection

The BumbleBee sample analyzed is the following ISO file, which is available on Malware Bazaar.

File name	Required Documents.img
MD5	016eae588e2e565414259280ba4f6753
SHA1	6983820a0d115bb78290ce9fbd6543623281d3d1
SHA256	127b3506b7da4569cbdf23bb500bb95832e1a8d4fcec5e2ce6ec9e0c973ba36b



BumbleBee Execution Process



The ISO file analyzed contained three files, two hidden and one visible LNK file.

When opened, the LNK file launches cmd.exe to execute the hidden BAT file.

```
C:\Windows\System32\cmd.exe /c case_studies.bat
```

The threat actors slightly obfuscated the BAT file by assigning a unique string to every letter of the alphabet to hide the executed final command.

Obfuscated BAT file:

```
@echo off
:ywthnwxyyek
set ugfmhz=a
:dykxmzumupg
set zjxchb=b
:ibbnmbrapbc
set c=c
:ndtdmdoplmy
set d=d
:gnczycxqkhn
set e=e
:lqupyfuegsj
set f=f
:qslfyhrtbde
set g=g
:vvcvyjohxoa
set h=h
:ofmqjjxjwjp
set i=i
:thdgjluxsul
set j=j
:ykvwjnrlngh
set k=k
:dmmnjqpajrd
set l=l
:wxwivpxbimr
set m=m
:bznyurvpexn
set n=n
:gceoutseaij
set o=o
:leweuwpsvtf
set p=p
:eofagvytuou
set q=q
:jrxqgxviqzq
set r=r
:otoggaswmkl
set s=s
:twgwgcplhwh
set t=t
:lgprrbymgqw
set u=u
:rigirdvaccs
```

```
set v=v
:wlyyrgspyno
set w=w
:bnporipdtyk
set x=x
:txzjdhyestz
set y=y
:yaqzckvtoeu
set z=z
:zogksw
%c%%m%%d%.%e%%x%%e% /%c% %s%%t%%a%%r%%t% /%b% /%m%%i%%n% %c%%o%%p%%y% /Y C:\W%i%%n%%d%%o%%w%%s%\S%y%%s%%t%%e%%m%32\%r%%u%%
```

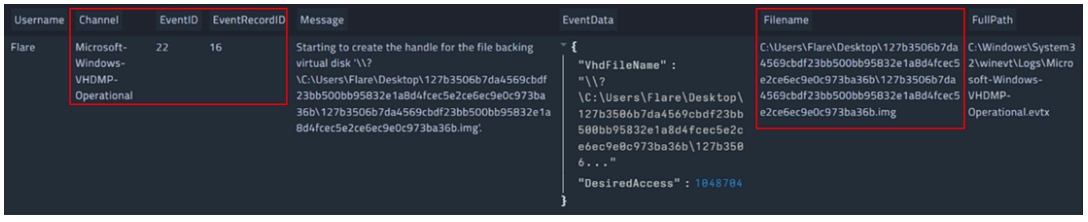
By de-obfuscating the BAT file, it is possible to see that it copies the rundll32 executable into the ProgramData directory and then launches the BumbleBee DLL (network.dll).

De-obfuscated BAT file:

```
cmd.exe /c start /b /min copy /Y C:\Windows\System32\rundll32.exe C:\ProgramData\ESMS3uYsyNq2s.exe && start /b /min C:\Pr
```

Defense Evasion: Mark-of-the-Web Bypass

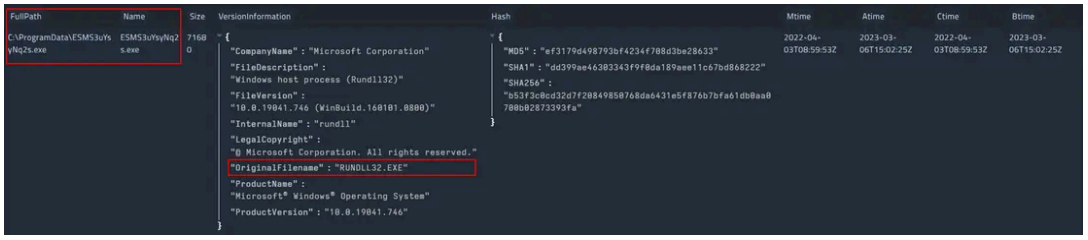
BumbleBee abuses ISO images to evade a Windows mechanism called *Mark-of-the-Web*. Such a mechanism tracks, through a hidden NTFS Alternate Data Stream (ADS) named *Zone.Identifiers*, files downloaded from the Internet which trigger security measures on the tracked files.



Velociraptor

The Velociraptor artifact called *Windows.Detection.ISOMount* can be used to search for ISO files mounted this activity is tracked in the Windows Event Logs with EventID *22*.

The following image shows the identification of the BumbleBee ISO image mounting.



Masquerading: Rename System Utilities Detection

The technique used by the BAT file is called *Rename System Utilities* and consists of copying itself into a specific folder, modifying the name of the executable in order to evade security mechanisms.

Velociraptor

Velociraptor natively offers an artifact named *Windows.Detection.BinaryRename* to hunt for known executables that are copied and re-named by threat actors.

```
SELECT * FROM source(artifact="Windows.Detection.BinaryRename") WHERE VersionInformation.OriginalFilename =~ "rundll32"
```

The following image shows the identification of this technique through Velociraptor.

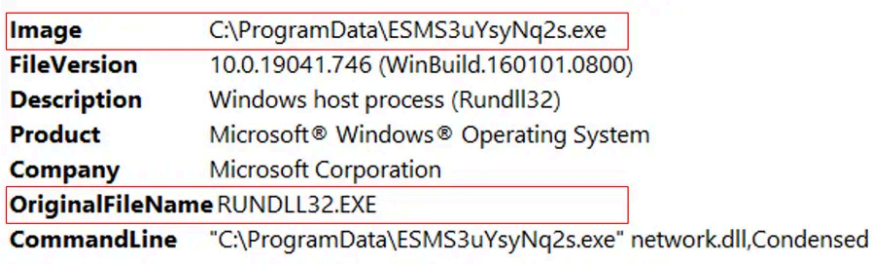


Image	C:\ProgramData\ESMS3uYsyNq2s.exe
FileVersion	10.0.19041.746 (WinBuild.160101.0800)
Description	Windows host process (Rundll32)
Product	Microsoft® Windows® Operating System
Company	Microsoft Corporation
OriginalFileName	RUNDLL32.EXE
CommandLine	"C:\ProgramData\ESMS3uYsyNq2s.exe" network.dll,Condensed

Windows Event Logs

By looking at Sysmon[2] Event ID 1, we notice that the *OriginalFileName* value does not match the executable name specified in the *Image* value.

Therefore, it is possible to hunt for this pattern also through the following Sigma rule:

```
 [···]
detection:
    selection:
        - Description: 'Execute processes remotely'
        - Product: 'Sysinternals PsExec'
        - Description|startswith:
            - 'Windows PowerShell'
            - 'pwsh'
        - OriginalFileName:
            - 'powershell.exe'
            - 'pwsh.dll'
            - 'powershell_ise.exe'
            - 'psexec.exe'
            - 'psexec.c'        # old versions of psexec (2016 seen)
            - 'psexesvc.exe'
            - 'cscript.exe'
            - 'wscript.exe'
            - 'mshta.exe'
            - 'regsvr32.exe'
            - 'wmic.exe'
            - 'certutil.exe'
            - 'rundll32.exe'
            - 'cmstp.exe'
            - 'msiexec.exe'
            - 'reg.exe'
[···]
```

The full Sigma rule can be found here.

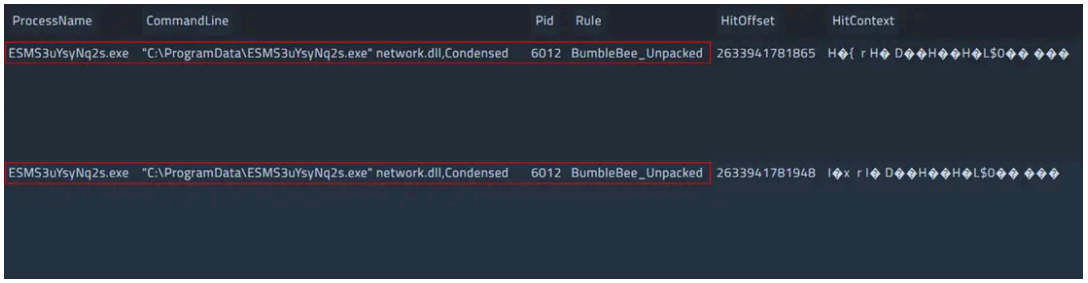
Execution: System Binary Proxy Execution Detection

BumbleBee executes the malicious DLL through Rundll32 with the aim to hide the malware from security applications.

Velociraptor

SEC Defence has created the following Yara rule that can be used to detect running BumbleBee processes through the Velociraptor artifact *Windows.Detection.Yara.Process*.

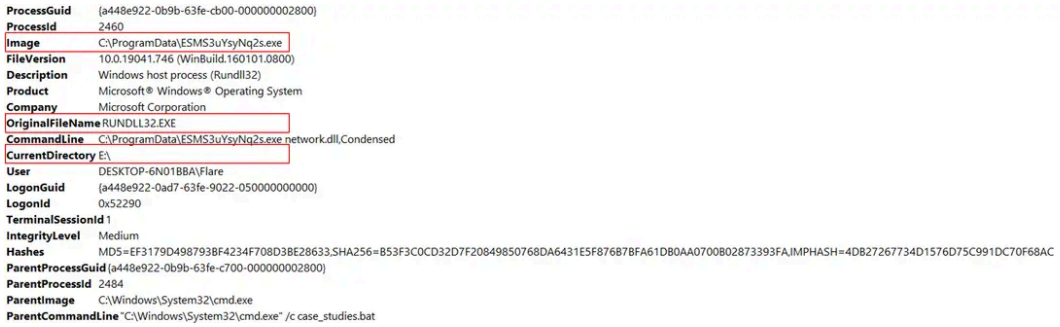
```
 rule BumbleBee_Unpacked{
        meta:
                author = "Angelo Violetti (SEC Consult - SEC Defence)"
                date = "2023-02-23"
                description = "Rule to detect BumbleBee in memory"
                reference = "https://sec-consult.com/incident-response/sec-defence/"

        strings:

                /*
                        $s1

                        mov     rax, [rbx+10h]
                        cmp     qword ptr [rbx+18h], 10h
                        jb      short loc_18000738F
                        mov     rbx, [rbx]
                        mov     r8d, eax
                        mov     rdx, rbx
                        lea     rcx, [rsp+148h+array]
                        call    mw_rc4_ksa_wrapper
                        nop

                        $s2

                        mov     r8d, 0FFFh
                        lea     rdx, mw_encrypted_config
                        lea     rcx, [rsp+148h+array]
                        call    mw_rc4_decrypt_wrapper
                        nop

                        $s3
                        lea     rcx, [rsp+148h+array]
                        call    mw_return
                */

                $s1 = {?? 83 ?? 18 10 72 03 ?? 8B ?? 44 8B ?? 48 8B ?? 48 8D 4C 24 30 E8 ?? ?? FF FF 90}

                $s2 = {48 8D 4C 24 30 E8 ?? ?? FF FF 90}

                $s3 = {48 8D 4C 24 30 E8 ?? ?? FF FF}

        condition:
                all of ($s*)
}
```



ProcessName	CommandLine	Pid	Rule	HitOffset	HitContext
ESMS3uYsyNq2s.exe	"C:\ProgramData\ESMS3uYsyNq2s.exe" network.dll,Condensed	6012	BumbleBee_Unpacked	2633941781865	H◆{ r H◆ D◆◆H◆◆H◆L$0◆◆ ◆◆◆
ESMS3uYsyNq2s.exe	"C:\ProgramData\ESMS3uYsyNq2s.exe" network.dll,Condensed	6012	BumbleBee_Unpacked	2633941781948	I◆x r I◆ D◆◆H◆◆H◆L$0◆◆ ◆◆◆

The Yara rule is based on the operations performed by the malware when decrypts its embedded configuration containing the command and control servers.

The following image shows the identification of BumbleBee processes through SEC Defence Yara rule and Velociraptor.



ProcessGuid	{a448e922-0b9b-63fe-cb00-000000002800}
ProcessId	2460
Image	C:\ProgramData\ESMS3uYsyNq2s.exe
FileVersion	10.0.19041.746 (WinBuild.160101.0800)
Description	Windows host process (Rundll32)
Product	Microsoft® Windows® Operating System
Company	Microsoft Corporation
OriginalFileName	RUNDLL32.EXE
CommandLine	C:\ProgramData\ESMS3uYsyNq2s.exe network.dll,Condensed
CurrentDirectory	E:\
User	DESKTOP-6N01BBA\Flare
LogonGuid	{a448e922-0ad7-63fe-9022-050000000000}
LogonId	0x52290
TerminalSessionId	1
IntegrityLevel	Medium
Hashes	MD5=EF3179D498793BF4234F708D3BE28633,SHA256=B53F3C0CD32D7F20849850768DA6431E5F876B7BFA61DB0AA0700B02873393FA,IMPHASH=4DB27267734D1576D75C991DC70F68AC
ParentProcessGuid	{a448e922-0b9b-63fe-c700-000000002800}
ParentProcessId	2484
ParentImage	C:\Windows\System32\cmd.exe
ParentCommandLine	"C:\Windows\System32\cmd.exe" /c case_studies.bat

Windows Event Logs

Since at time of execution BumbleBee DLL is located on the mounted ISO file, when rundll32.exe is executed, its current directory is set to the external drive, as shown by the following Sysmon Event ID 1.

ESMS3uYsyNq2s.exe (2460) (0x24c02f4b000 - 0x24c02f5f000)

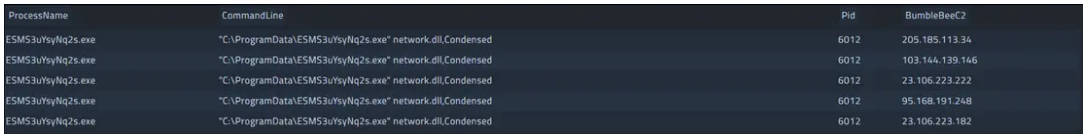
```
00000550 00 00 00 00 00 00 00 00 ca 1a db 13 f0 df 00 10 ................
00000560 31 32 2e 33 32 2e 39 36 2e 31 31 31 00 02 00 00 12.32.96.111....
00000570 0c 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000580 34 32 34 00 00 00 00 00 00 00 00 00 00 00 00 00 424.............
00000590 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
000005a0 32 33 37 2e 32 30 33 2e 35 30 2e 32 30 30 00 00 237.203.50.200..
000005b0 0e 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
000005c0 32 33 36 00 00 00 00 00 00 00 00 00 00 00 00 00 236.............
000005d0 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
000005e0 32 30 35 2e 31 38 35 2e 31 31 33 2e 33 34 00 00 205.185.113.34..
000005f0 0e 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000600 34 34 33 00 00 00 00 00 00 00 00 00 00 00 00 00 443.............
00000610 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000620 34 34 2e 32 31 36 2e 32 31 39 2e 31 37 00 00 00 44.216.219.17...
00000630 0d 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000640 34 33 36 00 00 00 00 00 00 00 00 00 00 00 00 00 436.............
00000650 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000660 32 31 34 2e 37 38 2e 32 31 32 2e 32 33 32 00 00 214.78.212.232..
00000670 0e 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000680 31 33 30 00 00 00 00 00 00 00 00 00 00 00 00 00 130.............
00000690 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
000006a0 32 34 36 2e 35 31 2e 37 2e 38 32 00 00 00 00 00 246.51.7.82.....
000006b0 0b 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
000006c0 33 31 30 00 00 00 00 00 00 00 00 00 00 00 00 00 310.............
000006d0 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
000006e0 31 34 38 2e 32 33 31 2e 31 37 35 2e 33 31 00 00 148.231.175.31..
000006f0 0e 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000700 34 32 38 00 00 00 00 00 00 00 00 00 00 00 00 00 428.............
00000710 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000720 31 30 38 2e 31 36 32 2e 32 30 37 2e 31 39 38 00 108.162.207.198.
00000730 0f 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000740 31 32 30 00 00 00 00 00 00 00 00 00 00 00 00 00 120.............
00000750 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000760 36 30 2e 32 32 35 2e 35 31 2e 31 32 37 00 00 00 60.225.51.127...
00000770 0d 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
00000780 34 36 31 00 00 00 00 00 00 00 00 00 00 00 00 00 461.............
00000790 03 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
000007a0 32 30 36 2e 34 35 2e 32 34 34 2e 34 32 00 00 00 206.45.244.42...
000007b0 0d 00 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 ................
000007c0 32 33 33 00 00 00 00 00 00 00 00 00 00 00 00 00 233.............
```

To detect this behaviour, SEC Defence has defined the following Sigma rule:

```
 title: Suspicious Rundll32 with Current Directory an External Drive
ruletype: Sigma
author: Angelo Violetti (SEC Consult - SEC Defence)
date: 2023/03/01
description: Detects the execution of rundll32.exe and the current directory is not C
reference: sec-consult.com/incident-response/sec-defence/
id: aaff35da-bcee-11ed-afa1-0242ac120002
status: experimental
tags:
    - attack.defenseevasion
    - attack.T1553.005
logsource:
  category: process_creation
  product: windows
detection:
    SELECTION_1:
        OriginalFileName: 'rundll32.exe'
    SELECTION_2:
        CurrentDirectory|startswith: 'C:\\'
    condition: SELECTION_1 and not SELECTION_2
level: medium
```

Command & Control: Application Layer Protocol

After compromising the victim's workstation, BumbleBee contacts the C2 servers that are RC4 encrypted in the binary. By analyzing the process memory, it is possible to notice various IP addresses followed by a destination port, however, only a part of them is associated with port 443 (HTTPS) and are actually used as a C2.



ProcessName	CommandLine	Pid	BumbleBeeC2
ESMS3uYsyNq2s.exe	"C:\ProgramData\ESMS3uYsyNq2s.exe" network.dll,Condensed	6012	205.185.113.34
ESMS3uYsyNq2s.exe	"C:\ProgramData\ESMS3uYsyNq2s.exe" network.dll,Condensed	6012	103.144.139.146
ESMS3uYsyNq2s.exe	"C:\ProgramData\ESMS3uYsyNq2s.exe" network.dll,Condensed	6012	23.106.223.222
ESMS3uYsyNq2s.exe	"C:\ProgramData\ESMS3uYsyNq2s.exe" network.dll,Condensed	6012	95.168.191.248
ESMS3uYsyNq2s.exe	"C:\ProgramData\ESMS3uYsyNq2s.exe" network.dll,Condensed	6012	23.106.223.182

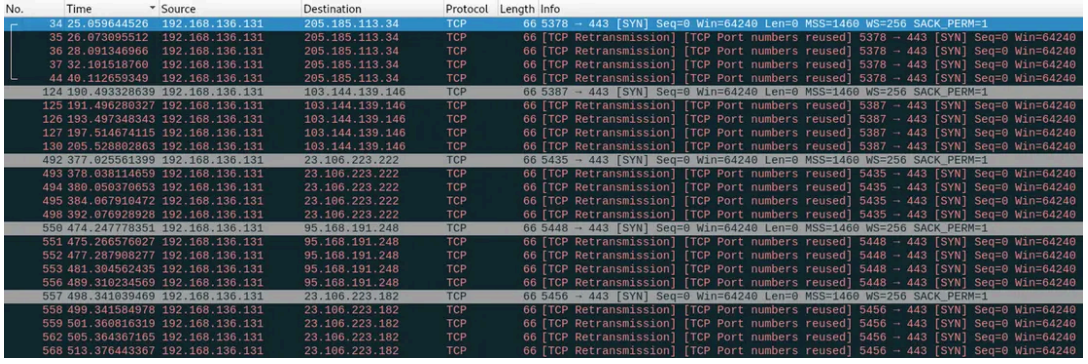
Velociraptor

To automatically extract the C2 server addresses from the malware, SEC Defence created further Velociraptor artifacts that firstly detects BumbleBee processes and secondly extracts the IP addresses which have port 443 associated.

```
 name: Custom.Windows.Carving.BumbleBee
author: "Angelo Violetti (SEC Consult - SEC Defence)"
type: CLIENT
description: |
        This artficat will detect running BumbleBee processes and subsequently extract the command and control servers wit
reference: sec-consult.com/incident-response/sec-defence/
parameters:
  - name: TargetFileGlob
    default:
  - name: PidRegex
    default: .
  - name: ProcessRegex
    default: .
  - name: DetectionYara
    default: |
        rule BumbleBee_Unpacked{
            meta:
                author = "Angelo Violetti @ SEC Defence"
                date = "2023-02-23"

            strings:
                $s1 = {?? 83 ?? 18 10 72 03 ?? 8B ?? 44 8B ?? 48 8B ?? 48 8D 4C 24 30 E8 ?? ?? FF FF 90}
                $s2 = {48 8D 4C 24 30 E8 ?? ?? FF FF 90}
                $s3 = {48 8d 4c 24 30 e8 ?? ?? FF FF}

            condition:
                all of ($s*)
        }

  - name: ExtractIPsYara
    default: |
        rule BumbleBee_IPs{
            meta:
                author = "Angelo Violetti @ SEC Defence"
                date = "2023-02-23"
                description = "Extracts the IP addresses with the destination port equal to 443 from BumbleBee processes"
```

```
            strings:
            $IP = {?? ?? ?? 2e ?? ?? ?? 2e ?? ?? ?? 2e ?? ?? ?? 00 (?? | ?? ??) 00 00 00 00 00 00 00 0f 00 00 00 00 00 00
          condition:
            $IP
        }

sources:
  - precondition:
      SELECT OS From info() where OS = 'windows'

    query: |
        -- Find velociraptor process
        LET me = SELECT Pid
                 FROM pslist(pid=getpid())

        -- Find all processes and add filters
        LET processes = SELECT Name AS ProcessName, CommandLine, Pid
                        FROM pslist()
                        WHERE Name =~ ProcessRegex
                            AND format(format="%d", args=Pid) =~ PidRegex
                            AND NOT Pid in me.Pid

        -- Scan processes in scope with our DetectionYara
        LET processDetections = SELECT * FROM foreach(row=processes,
                                query={
                                    SELECT * FROM if(condition=TargetFileGlob="",
                                        then={
                                            SELECT *, ProcessName, CommandLine, Pid, Rule AS YaraRule
                                            FROM proc_yara(pid=Pid, rules=DetectionYara)
                                        })
                                })

        -- Scan the process for the IP addresses
        LET ipaddressDetections = SELECT ProcessName, CommandLine, Pid, Strings.Data AS IPAddresses FROM foreach(row=proce

        -- Extract the command and control servers
        LET CommandandControlServers = SELECT * FROM foreach(row=ipaddressDetections, query={SELECT ProcessName, CommandLi

        -- Output the command and control servers
        SELECT ProcessName, CommandLine, Pid, str(str=g1) AS BumbleBeeC2 FROM CommandandControlServers
```

The following image shows the output produced by the SEC Defence Velociraptor artifact.



No.	Time	Source	Destination	Protocol	Length	Info
34	25.059644526	192.168.136.131	205.185.113.34	TCP	66	5378 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
35	26.073095512	192.168.136.131	205.185.113.34	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5378 → 443 [SYN] Seq=0 Win=64240
36	28.091346966	192.168.136.131	205.185.113.34	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5378 → 443 [SYN] Seq=0 Win=64240
37	32.101518760	192.168.136.131	205.185.113.34	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5378 → 443 [SYN] Seq=0 Win=64240
44	40.112659349	192.168.136.131	205.185.113.34	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5378 → 443 [SYN] Seq=0 Win=64240
124	190.493328639	192.168.136.131	103.144.139.146	TCP	66	5387 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
125	191.496280327	192.168.136.131	103.144.139.146	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5387 → 443 [SYN] Seq=0 Win=64240
126	193.497348343	192.168.136.131	103.144.139.146	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5387 → 443 [SYN] Seq=0 Win=64240
127	197.514674115	192.168.136.131	103.144.139.146	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5387 → 443 [SYN] Seq=0 Win=64240
130	205.528802863	192.168.136.131	103.144.139.146	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5387 → 443 [SYN] Seq=0 Win=64240
492	377.025561399	192.168.136.131	23.106.223.222	TCP	66	5435 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
493	378.038114659	192.168.136.131	23.106.223.222	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5435 → 443 [SYN] Seq=0 Win=64240
494	380.050370653	192.168.136.131	23.106.223.222	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5435 → 443 [SYN] Seq=0 Win=64240
495	384.067910472	192.168.136.131	23.106.223.222	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5435 → 443 [SYN] Seq=0 Win=64240
498	392.076928928	192.168.136.131	23.106.223.222	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5435 → 443 [SYN] Seq=0 Win=64240
550	474.247778351	192.168.136.131	95.168.191.248	TCP	66	5448 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
551	475.266576027	192.168.136.131	95.168.191.248	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5448 → 443 [SYN] Seq=0 Win=64240
552	477.287908277	192.168.136.131	95.168.191.248	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5448 → 443 [SYN] Seq=0 Win=64240
553	481.304562435	192.168.136.131	95.168.191.248	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5448 → 443 [SYN] Seq=0 Win=64240
556	489.310234569	192.168.136.131	95.168.191.248	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5448 → 443 [SYN] Seq=0 Win=64240
557	498.341039469	192.168.136.131	23.106.223.182	TCP	66	5456 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
558	499.341584978	192.168.136.131	23.106.223.182	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5456 → 443 [SYN] Seq=0 Win=64240
559	501.360816319	192.168.136.131	23.106.223.182	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5456 → 443 [SYN] Seq=0 Win=64240
562	505.364367165	192.168.136.131	23.106.223.182	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5456 → 443 [SYN] Seq=0 Win=64240
568	513.376443367	192.168.136.131	23.106.223.182	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 5456 → 443 [SYN] Seq=0 Win=64240

Network Traffic Analysis

Another method to detect connections to C2 servers is by integrating and constantly updating Cyber Threat Intelligence feeds and detection rules with network security technologies.

In this specific case, the following Proofpoint Emerging Threat Rules were triggered:

- ET CNC Feodo Tracker Reported CnC Server group 1: 103[.]144[.]139[.]146
- ET CNC Feodo Tracker Reported CnC Server group 10: 205[.]185[.]113[.]34
- ET CNC Feodo Tracker Reported CnC Server group 11: 23[.]106[.]223[.]222
- ET CNC Feodo Tracker Reported CnC Server group 25: 95[.]168[.]191[.]248

Suggested Remediation / Other Actions

- Proactively hunt at scale for the subsequent actions that could have been performed by the threat actors after having compromised the patient zero (e.g., discovery, credential access, lateral movement, etc.).
- Isolate, where possible, the compromised systems to contain the incident and prevent the spread of the infection.
- Block the indicators of compromise (IoCs) identified during the analysis and, eventually, insert in blacklists also the indicators reported on OSINT sources like Malware Bazaar, Feodo Tracker, etc.
- If support in handling the incident is needed, contact the incident response team.

Conclusion

By analyzing the tactics, techniques and procedures adopted by BumbleBee, SEC Defence identified and created mechanisms to detect the malware in the early stages of the attack with the aim objective to minimize further potential impacts such as data exfiltration and/or encryption.

As stated by other companies (Mandiant, Intrisec), the threat actors behind BumbleBee have a strong relationship with other malware families like Emotet or IcedID and ransomware groups. Therefore, proactively hunting for BumbleBee activities or applying the right remediation actions in time can prevent the execution of other malicious executables that could cause service unavailability or impact the confidentiality and integrity of data.

[1] *Initial access brokers are cyber-criminals that sell access to compromised infrastructures to other groups with the aim to obtain a financial gain.*
[2] *Sysmon (System Monitor) is a Windows service that allows logging a wide range of activities performed on a system such as process creation, network connections or file changes.*

Repositories:

Sigma: https://github.com/angelovioletti/sigma/blob/master/rules/windows/process_creation/proc_creation_win_rundll32_ext_drive

Velociraptor: https://github.com/Velocidex/velociraptor-docs/blob/d891bf8671230437b2b4497649c28b9a6045252b/content/exchange/artifacts/BumbleBee.yaml

Yara: https://github.com/sec-consult/SD-BumbleBee-Hunting-Rules/blob/main/BumbleBee_Unpacked.yara

This research has been conducted by Angelo Violetti and published on behalf of SEC Defence.

Are you interested in working at SEC Consult?

SEC Consult is always searching for talented security professionals to work in our team.
