SEC Consult
an Eviden business

Home / Blog / BumbleBee hunting with a Velociraptor

BumbleBee hunting with a Velociraptor

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., 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).

Incident?

Malware Analysis & Detection

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

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
```

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
```

```
:twgwgcpinwn
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\
```

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 /mir
```

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 i 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 =~ "rundl
```

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

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 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'
[…]
```

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]
                $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*)
}
```

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.

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 i the external drive, as shown by the following Sysmon Event ID 1.

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
```

Incident?

Command & Control: Application Layer Protocol

with port 443 (HTTPS) and are actually used as a C2.

Velociraptor

```
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 serv
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 proc

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

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(ro

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

    -- 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.

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 compromi 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.

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.yml***

*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.

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

MORE INFORMATION

Back

Incident?