THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

adfind bumblebee cobaltstrike Meterpreter

BumbleBee Zeros in on Meterpreter

November 14, 2022

In this intrusion from May 2022, the threat actors used BumbleBee as the initial access vector from a Contact Forms campaign. We have previously reported on two BumbleBee intrusions (1, 2), and this report is a continuation of a series of reports uncovering multiple TTPs seen by BumbleBee post exploitation operators.

The intrusion began with the delivery of an ISO file that contained an LNK and a DLL. The threat actors leveraged BumbleBee to load a Meterpreter agent and Cobalt Strike Beacons. They then performed reconnaissance, used two different UAC bypass techniques, dumped credentials, escalated privileges using a ZeroLogon exploit, and moved laterally through the environment.

The DFIR Report Services

- Private Threat Briefs: Over 20 private DFIR reports annually.

- Threat Feed: Focuses on tracking Command and Control frameworks like Cobalt Strike, Metasploit, Sliver, etc.
- All Intel: Includes everything from Private Threat Briefs and Threat Feed, plus private events, opendir reports, long-term tracking, data clustering, and other curated intel.
- Private Sigma Ruleset: Features 100+ Sigma rules derived from 40+ cases, mapped to ATT&CK with test examples.
- DFIR Labs: Offers cloud-based, hands-on learning experiences, using real data, from real intrusions. Interactive labs are available with different difficulty levels and can be accessed on-demand, accommodating various learning speeds.

Contact us today for pricing or a demo!

Case Summary

The intrusion started with a contact form on a website. It has been reported that this delivery method has been in use for intrusions since at least 2020. This campaign took place in May, and appears to have run as late as June 2022, based on OSINT data related to similar delivery fingerprints. The contact form gets filled out by the threat actor with a Copyright notice, purporting a violation of the Digital Millennium Copyright Act (DMCA). It then encourages the recipient to download a file showing the purported violation.

Upon the user clicking the link, they arrive at a “Google” storage site on storage.googleapis.com. A zip file is then downloaded to the victim machine and once unzipped the user is presented with an ISO file. The ISO contains a LNK file and a DLL file. When the LNK is double-clicked, the BumbleBee DLL is executed via rundll32. Initially, contact was made with BumbleBee command and control servers but little other early activity was observed.

Approximately 12 hours later, ImagingDevices.exe was launched via WmiPrivse.exe and a Meterpreter agent was injected into the process, like we have observed in previous reports. This process then utilized nltest, net, tasklist, and whoami to perform reconnaissance. About 37 minutes after launching ImagingDevices.exe, the Meterpreter agent migrated to svchost.exe. Upon migrating to the svchost process, there were attempts to bypass UAC and launch a Meterpreter executable.

Several failed attempts to bypass UAC occurred, utilizing the WSReset method, followed by a failed attempt to bypass UAC utilizing the slui hijacking method. Finally, the threat actors succeeded on their final attempt, using the WSReset method. Once UAC was bypassed, Meterpreter's getsystem command was successfully employed. Now in the SYSTEM context, this Meterpreter agent executed a Cobalt Strike Beacon DLL.

The Cobalt Strike Beacon was utilized to perform a second round of reconnaissance and to access credentials. AdFind, nltest, net, and systeminfo were used to facilitate this activity. The Sysinternals tool ProcDump64 was written to disk and used to dump lsass on the beachhead host. Then, the threat actors executed `reg.exe` to save a copy of the `SAM`, `Security`, and `Software` registry hives on the beachhead host. Lateral movement was then performed over SMB, to transfer a Cobalt Strike Beacon DLL's to other workstation's C$\\ProgramData\. These were executed via remote services, but appeared to be there for redundant connections as the threat actors continued to perform their actions on the beachhead workstation.

After a pause of about three hours, 19 hours since initial access, the threat actors launched an exploit against the primary domain controller targeting the Zerologon (CVE 2020 1472) vulnerability. After successfully exploiting the Domain controller, the threat actors used Pass the Hash to begin working in the context of a user who was a member of the Domain Admins group.

From the beachhead host, Invoke-Sharefinder was executed with the output being written to disk. A Cobalt Strike Beacon DLL was then written over SMB to another Domain Controller and executed via a service.

The threat actors were evicted from the environment and no further impact was observed. We assess with medium confidence this intrusion was related to pre-ransomware activity due to the tool set and techniques the actors displayed. As far as impact, one Domain Controller was left broken causing authentication failures across the domain.

Timeline

Analysis and reporting completed by @0xtornado, @samaritan_o, @RoxpinTeddy

Initial Access

The intrusion in this case began with a link to a google domain, storage.googleapis.com. This delivery method has been observed in both thread hijacked email distribution, as well as contact form campaigns. We assess with medium-high confidence that the one observed in our intrusion was likely from a contact form campaign, as the initial access URL was spotted in the wild across various sites, impersonating various companies' legal teams, trying to entice the user to download and review the malicious files.

After clicking the link, the users end up at what, at first glance, may appear to be a legitimate google download site.

Next, a zip file is downloaded to the victim’s system, which when unzipped reveals the ISO image file `StolenImages_Evidence.iso`, once mounted–lures the victim to open a shortcut mimicking a fake documents folder:

The LNK was pointing to the following command, which runs a malicious DLL when the user double clicks on the LNK file:

```
%windir%\system32\cmd.exe /c start rundll32.exe mkl2n.dll,kXlNkCKgFC
```

By extracting LNK metadata using Eric Zimmerman's LECmd tool, we noticed that the initial BumbleBee payload was generated by the same threat actors reported in our previous BumbleBee report:

```
Machine ID: desktop-30fdj39
Mac:eb:33:6a:3b:d0:e3
Creation: 2022-02-11 21:22:11
```

The tracker database block details containing threat actor’s hostname, MAC Address, and other details are the exact same as seen our the last BumbleBee report. However, the payload was slightly modified (name and icon).

Execution

The threat actors dropped and executed multiple payloads reaching out to different C2s. The graph below shows how the threat actors were able to pivot between C2s by either injecting into legitimate processes or dropping and executing new payloads.

Like in our previous BumbleBee report, we see the use of injection into a legitimate Windows executable.

```
C:\Program Files\Windows Photo Viewer\ImagingDevices.exe
```

And likewise, we see BumbleBee spawning these new processes using WmiPrvSE.exe.

The graphic below shows all payloads dropped, executed, or injected by the threat actors. Both Meterpreter and Cobalt Strike payloads were used during this intrusion.

Privilege Escalation

The getsystem module was used to elevate access on the beachhead host.

```
cmd.exe /c echo wafrms > \\.\pipe\wafrms
```

```
C:\Windows\system32\cmd.exe /c echo dec8f35bcbf > \\.\pipe\7fd13a
```

On the second day, a Netlogon spike was observed from the beachhead host to a domain controller.

This spike was made up of various netlogon requests (NetrServerReqChallenge, NetrServerAuthenticate2, NetrServerPasswordSet2) from the beachhead host to the primary domain controller.

A view of the traffic reveals that the threat actors had exploited CVE 2020 1472, otherwise known as ZeroLogon. In the PCAP below, we can see the packet where the exploit succeeds in resetting the credential to all zeros.

On the domain controller, a 4742 event was generated showing the beachhead host changing the password on the domain controller, matching the timestamps to the network data.

After exploiting Zerologon, the threat actors were also seen using Pass the Hash to begin working in the context of a user, who was a member of the Domain Admins group.

Defense Evasion

Process Injection

ImagingDevices.exe injection into “svchost.exe -k UnistackSvcGroup -s WpnUserService” using NtAllocateVirtualMemoryRemoteApiCall. Several other processes were injected into as seen below:

.Pid	.ProcessName	.CommandLine	.Rule
576	winlogon.exe	winlogon.exe	win_cobalt_strike_auto
836	svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p	win_cobalt_strike_auto
616	winlogon.exe	winlogon.exe	win_cobalt_strike_auto
1132	svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService	win_cobalt_strike_auto
6876	svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	win_cobalt_strike_auto
9828	svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	win_cobalt_strike_auto

UAC Bypass

The threat actors were observed bypassing UAC via WSReset and DelegateExecute, spawning new processes at a High integrity level.

While executing this UAC bypass, the threat actors seemed to be running into some kind of trouble during execution, which required them to try the technique several times and tried to kill one of their processes from a prior attempt.

In addition to the WSReset UAC bypass, the threat actors tried a method using slui.exe. The data points to use of the Meterpreter implementation here.[1]

Indicator Removal on Host

The threat actors were also seen deleting a number of their tools which were previously dropped to perform various tactics:

Named Pipe Usage

Throughout the intrusion, the injected Cobalt Strike Processes utilized various named pipes for inter-process communications. Many of these pipes used default Cobalt Strike pipe patterns.

Known Cobalt Strike pipes used:

```
\postex_002d
\postex_67cc
\postex_731d
\postex_a4c1
\postex_c69e
\postex_b6fd
```

```
\postex_5a0d
\postex_d43a
\postex_a820
```

We also saw the unusual named pipes coming from ImagingDevices.exe which was injected with Meterpreter below:

```
\4ae13d6c2cd672ae\pipe\spoolss
\0029482318be6784
\uwjjqz
\vllyad
```

Credential Access

LSASS Dump

The threat actor dropped the Sysinternals executable `procdump64.exe`, which they then used to dump the `lsass` process. The command observed was:

```
procdump64.exe -accepteula -ma lsass.exe C:\ProgramData\lsass.dmp
```

Registry Hives Dump

Using the Cobalt Strike beacon, injected in a svchost.exe process, the threat actors dumped `SAM`, `SECURITY`, and `SYSTEM` hives using the native `reg.exe` utility. Below are the commands that were used:

```
C:\Windows\system32\cmd.exe /C reg.exe save hklm\sam
c:\ProgramData\sam.hive
C:\Windows\system32\cmd.exe C:\Windows\system32\cmd.exe /C reg.exe save
hklm\security c:\ProgramData\security.save
C:\Windows\system32\cmd.exe /C reg.exe save hklm\security
c:\ProgramData\security.save
C:\Windows\system32\cmd.exe C:\Windows\system32\cmd.exe /C reg.exe save
hklm\system c:\ProgramData\system.save
C:\Windows\system32\cmd.exe /C reg.exe save hklm\system
c:\ProgramData\system.save
```

Discovery

The Discovery phase was carried out in this case using both native Windows tools, and external tools such as AdFind and PowerSploit. Initial discovery was performed using various Windows utilities. After dumping the `lsass.exe` process on the beachhead machine, the threat actors then launched `af.exe` (AdFind) to find all user objects and computers in the domain.

```
af.exe -f "(objectcategory=person)" > ad_users.txt
af.exe -f "objectcategory=computer" > ad_computers.txt
```

System utilities used for discovery included:

```
nltest /dclist:DOMAIN
net view /all
net group "Domain Computers" /domain
net group "domain Admins" /domain
whoami
whoami /groups
echo %USERDOMAIN%
ping -n 1 DOMAINCONTROLLER
systeminfo
tasklist
```

Throughout the intrusion, the threat actor kept on trying to view a file named sh.txt.

The file appears to have been the intended output for execution of the `Invoke-ShareFinder` command. Execution of the command was visible in the PowerShell 4103 and 4104 logs.

`Invoke-Sharefoinder` is a module in the [PowerSploit](https://github.com/PowerShellMafia/PowerSploit) framework. This command, in particular, can find (non-standard) shares on hosts in the local domain.

Lateral Movement

The threat actors used the `SMB` protocol to move laterally after compromising the beachhead. They specifically copied the `n23.dll` (Cobalt Strike) file to the `C:\ProgramData` path and then ran it.

We can confirm that the file was copied and then launched via the new service by examining the various host’s system logs for event id 7045.

```
cmd.exe /c rundll32.exe C:\ProgramData\n23.dll,AddProgram
```

Command and Control

Threat actors used multiple command and control servers to interact with the compromised environment.

BumbleBee C2

```
45.153.243.93:443
JA3: 0c9457ab6f0d6a14fc8a3d1d149547fb
JA3s: 61be9ce3d068c08ff99a857f62352f9d
subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
tls.issuerdn : C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
tls.notbefore: May 3, 2022 @ 08:04:39.000
tls.notafter: May 3, 2023 @ 08:04:39.000

213.232.235.199:443
JA3: 0c9457ab6f0d6a14fc8a3d1d149547fb
JA3s: 61be9ce3d068c08ff99a857f62352f9d
subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
tls.issuerdn : C=AU, ST=Some-State, O=Internet Widgits Pty Ltd
tls.notbefore: May 2, 2022 @ 19:09:22.000
tls.notafter: May 2, 2023 @ 19:09:22.000
```

Cobalt Strike

```
cevogesu[.]com at 172.93.201.12:443
JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3s: ae4edc6faf64d08308082ad26be60767
subject: CN=titojukus.com
tls.issuerdn: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited,
CN=Sectigo RSA Domain Validation Secure Server CA
tls.notbefore: Apr 22, 2022 @ 00:00:00.000
tls.notafter: Apr 22, 2023 @ 23:59:59.000

titojukus[.]com at 23.106.215.100:443
JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3s: ae4edc6faf64d08308082ad26be60767
subject: CN=titojukus.com
tls.issuerdn: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited,
CN=Sectigo RSA Domain Validation Secure Server CA
tls.notbefore: Apr 22, 2022 @ 00:00:00.000
tls.notafter: Apr 22, 2023 @ 23:59:59.000
```

Cobalt Strike Server Config:

```
{
  "x64": {
    "sha1": "fa9597b87f78c667cc006aaa1c647d539aa9b827",
    "md5": "ea2c1fa8668812852a77737c4f712ba2",
    "config": {
      "C2 Server": "cevogesu.com,/eo.html,titojukus.com,/eo.html",
      "Polling": 5000,
      "C2 Host Header": "",
      "HTTP Method Path 2": "/fam_newspaper",
      "Watermark": 1580103814,
      "Method 1": "GET",
      "Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
      "Jitter": 23,
      "Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
      "Method 2": "POST",
      "Port": 443,
      "Beacon Type": "8 (HTTPS)"
    },
    "sha256":
"da3c4e2b7768d66ecb6c0e74c6d45e2bcfbc6203b76c7163909bd2061603cef5",
    "time": 1651717062232.1,
    "uri_queried": "/DhpA"
  },
  "x86": {
    "sha1": "785b660537506501e695e46875b02260649b23f7",
    "md5": "5d2a8724dbce65eefb7e74fbb0eceda9",
    "config": {
      "C2 Server": "cevogesu.com,/cs.html,titojukus.com,/cs.html",
      "Polling": 5000,
      "C2 Host Header": "",
      "HTTP Method Path 2": "/posting",
      "Watermark": 1580103814,
      "Method 1": "GET",
      "Spawn To x64": "%windir%\\sysnative\\rundll32.exe",
      "Jitter": 23,
      "Spawn To x86": "%windir%\\syswow64\\rundll32.exe",
      "Method 2": "POST",
      "Port": 443,
      "Beacon Type": "8 (HTTPS)"
    },
    "sha256":
"f7bfde050c81d47d79febdb170f307f447e76253715859727beff889d2a91694",
    "time": 1651717054821.8,
    "uri_queried": "/BiLe"
  }
}
```

Meterpreter

```
ec2-3-16-159-37.us-east-2.compute.amazonaws[.]com at 3.16.159.37:80/443
JA3: ce5f3254611a8c095a3d821d44539877, a0e9f5d64349fb13191bc781f81f42e1
JA3s: ec74a5c51106f0419184d0dd08fb05bc
subject: C=US, ST=DE, O=Hackett LLC, OU=calculate, CN=hackett.llc.com,
Email=calculate@hackett.llc.com
tls.issuerdn: C=US, ST=DE, O=Hackett LLC, OU=calculate,
CN=hackett.llc.com, Email=calculate@hackett.llc.com
tls.ja3.hash
tls.notbefore: Sep 13, 2020 @ 21:43:47.000
tls.notafter: Sep 12, 2027 @ 21:43:47.000
```

Impact

After exploiting Zerologon on the domain controller, the threat actor tried a few more things and then took a break from the hands on keyboard portion of the intrusion. The threat actor was then evicted from the environment. During IR, it was found that the primary domain controller was unresponsive to domain authentication due to the exploit run against it, resulting in domain authentication breaking around the environment.

Indicators

Network

```
 BumbleBee C2
        45.153.243.93:443
        213.232.235.199:443

CobaltStrike
        cevogesu[.]com at 172.93.201.12:443
        titojukus[.]com at 23.106.215.100:443

Meterpreter
```

```
        ec2-3-16-159-37.us-east-2.compute.amazonaws[.]com at
3.16.159.37:80 and 3.16.159.37:44
```

Files

```
documents.lnk
EE7AD5FE821FB9081380DBBF40C4F062
38EEF0CDAA8FAA27C9E2CEDEAFCFE842E2E0E08E
3C600328E1085DC73D672D068F3056E79E66BEC7020BE6AE907DD541201CD167


mkl2n.dll
AEFF99611BABD41D79C3BA7930F00BC1
FA3649B0472BA7FD9B31A22C904B2DE4C008F540
F7C1D064B95DC0B76C44764CD3AE7AEB21DD5B161E5D218E8D6E0A7107D869C1


n23.dll
B3E68AEBE05DC652EC65099E0E98B94E
52D4C0CB9A93E7BC5F1E0C386DCCA3E0AC41B966
65A9B1BCDE2C518BC25DD9A56FD13411558E7F24BBDBB8CB92106ABBC5463ECF


StolenImages_Evidence.iso
FBCAA31456F39F996950511705461639
759688D1245AACD0ED067B0F0388786E911AAF28
4BB67453A441F48C75D41F7DC56F8D58549AE94E7AEAB48A7FFEC8B78039E5CC


wSaAHJzLLT.exe
BD5C8EA8C231BF2775B9C0BA3F7EA867
CCC9E1559B877B04B1D0E7F8920A64B4E35136DA
DF63149EEC96575D66D90DA697A50B7C47C3D7637E18D4DF1C24155ABACBC12
```

Detections

Network

```
ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement
ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
ET POLICY SMB Executable File Transfer
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
```

Sigma

Abused Debug Privilege by Arbitrary Parent Processes

AdFind Usage Detection

Bypass UAC Using DelegateExecute

Bypass UAC via WSReset.exe

UAC Bypass WSReset

Cobalt Strike Named Pipe

Correct Execution of Nltest.exe

Cred Dump Tools Dropped Files

LSASS Memory Access by Tool Named Dump

LSASS Memory Dumping

Malicious PowerView PowerShell Commandlets

Meterpreter or Cobalt Strike Getsystem Service Installation

Meterpreter or Cobalt Strike Getsystem Service Start

Mimikatz Detection LSASS Access

Registry Dump of SAM Creds and Secrets

Shell Open Registry Keys Manipulation

Successful Overpass the Hash Attempt

Suspicious PowerShell Invocations – Specific

Suspicious PowerShell Keywords

Suspicious Rundll32 Without Any CommandLine Params

Suspicious Service Installation

Suspicious Use of Procdump

Suspicious Use of Procdump on LSASS

Yara

```
/*
   YARA Rule Set
   Author: The DFIR Report
   Date: 2022-11-13
   Identifier: Case 13842 Bumblebee
   Reference: https://thedfirreport.com/
*/


/* Rule Set ----------------------------------------------------------------- */



```

```
rule bumblebee_13842_documents_lnk {
    meta:
       description = "BumbleBee - file documents.lnk"
       author = "The DFIR Report via yarGen Rule Generator"
       reference = "https://thedfirreport.com"
       date = "2022-11-13"
       hash1 =
"3c600328e1085dc73d672d068f3056e79e66bec7020be6ae907dd541201cd167"
    strings:
       $x1 = "$..\\..\\..\\..\\Windows\\System32\\cmd.exe*/c start
rundll32.exe mkl2n.dll,kXlNkCKgFC\"%systemroot%\\system32\\imageres.dll"
fullword wide
       $x2 = "C:\\Windows\\System32\\cmd.exe" fullword ascii
       $x3 = "%windir%\\system32\\cmd.exe" fullword ascii
       $x4 = "Gcmd.exe" fullword wide
       $s5 = "desktop-30fdj39" fullword ascii
    condition:
       uint16(0) == 0x004c and filesize < 4KB and
       1 of ($x*) and all of them
 }

 rule bumblebee_13842_StolenImages_Evidence_iso {
    meta:
       description = "BumbleBee - file StolenImages_Evidence.iso"
       author = "The DFIR Report via yarGen Rule Generator"
       reference = "https://thedfirreport.com"
       date = "2022-11-13"
       hash1 =
"4bb67453a441f48c75d41f7dc56f8d58549ae94e7aeab48a7ffec8b78039e5cc"
    strings:
       $x1 = "$..\\..\\..\\..\\Windows\\System32\\cmd.exe*/c start
rundll32.exe mkl2n.dll,kXlNkCKgFC\"%systemroot%\\system32\\imageres.dll"
fullword wide
       $x2 = "C:\\Windows\\System32\\cmd.exe" fullword ascii
       $x3 = "%windir%\\system32\\cmd.exe" fullword ascii
       $x4 = "Gcmd.exe" fullword wide
       $s5 = "pxjjqif723uf35.dll" fullword ascii
       $s6 = "tenant unanimously delighted sail databases princess
```

```
bicyclelist progress accused urge your science certainty dalton databases
h" ascii
       $s7 = "mkl2n.dll" fullword wide
       $s8 = "JEFKKDJJKHFJ" fullword ascii /* base64 encoded string
'$AJ(2I(qI' */
       $s9 = "KFFJJEJKJK" fullword ascii /* base64 encoded string
'(QI$BJ$' */
       $s10 = "JHJGKDFEG" fullword ascii /* base64 encoded string
'$rF(1D' */
       $s11 = "IDJIIDFHE" fullword ascii /* base64 encoded string ' 2H
1G' */
       $s12 = "JHJFIHJJI" fullword ascii /* base64 encoded string '$rE
rI' */
       $s13 = "EKGJKKEFHKFFE" fullword ascii /* base64 encoded string
'(bJ(AG(QD' */
       $s14 = "FJGJFKGFF" fullword ascii /* base64 encoded string
'$bE(aE' */
       $s15 = "IFFKJGJFK" fullword ascii /* base64 encoded string '
QJ$bE' */
       $s16 = "FKFJDIHJF" fullword ascii /* base64 encoded string '(RC
rE' */
       $s17 = "EKFJFdHFG" fullword ascii /* base64 encoded string
'(REtqF' */
       $s18 = "HJFJJdEdEIDK" fullword ascii /* base64 encoded string
'$RItGD 2' */
       $s19 = "KFJHKDJdIGF" fullword ascii /* base64 encoded string
'(RG(2] a' */
       $s20 = "documents.lnk" fullword wide
    condition:
       uint16(0) == 0x0000 and filesize < 13000KB and
       1 of ($x*) and 4 of them
 }

 rule bumblebee_13842_mkl2n_dll {
    meta:
       description = "BumbleBee - file mkl2n.dll"
```

```
        author = "The DFIR Report via yarGen Rule Generator"
        reference = "https://thedfirreport.com"
        date = "2022-11-13"
        hash1 =
"f7c1d064b95dc0b76c44764cd3ae7aeb21dd5b161e5d218e8d6e0a7107d869c1"
    strings:
        $s1 = "pxjjqif723uf35.dll" fullword ascii
        $s2 = "tenant unanimously delighted sail databases princess
bicyclelist progress accused urge your science certainty dalton databases
h" ascii
        $s3 = "JEFKKDJJKHFJ" fullword ascii /* base64 encoded string
'$AJ(2I(qI' */
        $s4 = "KFFJJEJKJK" fullword ascii /* base64 encoded string
'(QI$BJ$' */
        $s5 = "JHJGKDFEG" fullword ascii /* base64 encoded string '$rF(1D'
*/
        $s6 = "IDJIIDFHE" fullword ascii /* base64 encoded string ' 2H 1G'
*/
        $s7 = "JHJFIHJJI" fullword ascii /* base64 encoded string '$rE rI'
*/
        $s8 = "EKGJKKEFHKFFE" fullword ascii /* base64 encoded string
'(bJ(AG(QD' */
        $s9 = "FJGJFKGFF" fullword ascii /* base64 encoded string '$bE(aE'
*/
        $s10 = "IFFKJGJFK" fullword ascii /* base64 encoded string '
QJ$bE' */
        $s11 = "FKFJDIHJF" fullword ascii /* base64 encoded string '(RC
rE' */
        $s12 = "EKFJFdHFG" fullword ascii /* base64 encoded string
'(REtqF' */
        $s13 = "HJFJJdEdEIDK" fullword ascii /* base64 encoded string
'$RItGD 2' */
        $s14 = "KFJHKDJdIGF" fullword ascii /* base64 encoded string
'(RG(2] a' */
        $s15 = "magination provided sleeve governor earth brief favourite
setting trousers phone calamity ported silas concede appearance abate "
ascii
        $s16 = "wK}zxspyuvqswyK" fullword ascii
        $s17 = "stpKspyq~sqJvvvJ" fullword ascii
        $s18 = "ntribute popped monks much number practiced dirty con mid
nurse variable road unwelcome rear jeer addition distract surgeon fall"
ascii
        $s19 = "uvzrquxrrwxur" fullword ascii
        $s20 = "vvvxvsqrs" fullword ascii
    condition:
        uint16(0) == 0x5a4d and filesize < 9000KB and
        8 of them
 }

 rule bumblebee_13842_n23_dll {
    meta:
        description = "BumbleBee - file n23.dll"
        author = "The DFIR Report via yarGen Rule Generator"
        reference = "https://thedfirreport.com"
        date = "2022-11-13"
        hash1 =
"65a9b1bcde2c518bc25dd9a56fd13411558e7f24bbdbb8cb92106abbc5463ecf"
    strings:
        $x1 = "scratched echo billion ornament transportation heedless
should sandwiches hypothesis medicine strict thus sincere fight nourishm"
ascii
        $s2 = "omu164ta8.dll" fullword ascii
        $s3 = "eadlight hours reins straightforward comfortable greeting
notebook production nearby rung oven plus applet ending snapped enquir"
ascii
        $s4 = "board blank convinced scuba mean alive perry character
headquarters comma diana ornament workshop hot duty victorious bye
expres" ascii
        $s5 = " compared opponent pile sky entitled balance valuable list
ay duster tyre bitterly margaret resort valuer get conservative contr"
ascii
        $s6 = "ivance pay clergyman she sleepy investigation used madame
rock logic suffocate pull stated comparatively rowing abode enclosed h"
ascii
```

```
       $s7 = " purple salvation dudley gaze requirement headline
defective waiter inherent frightful night diary slang laurie bugs kazan
annou" ascii
       $s8 = "nced apparently determined among come invited be goodwill
tally crowded chances selfish duchess reel five peaceful offer spirits"
ascii
       $s9 = "scratched echo billion ornament transportation heedless
should sandwiches hypothesis medicine strict thus sincere fight nourishm"
ascii
       $s10 = "s certificate breeze temporary according peach effected
excuse preceding reaction channel bring short beams scheme gosh endless "
ascii
       $s11 = "rtificial poke reassure diploma potentially " fullword
ascii
       $s12 = "led spree confer belly rejection glide speaker wren do
create evenings according cultivation concentration overcoat presume
feed" ascii
       $s13 =
"EgEEddEfhkdddEdfkEeddjgjehdjidhkdkeiekEeggdijhjidgkfigEggdjkhkjkedEigif
efdfhEjgghgEhjkeihifdhEEdgifefgkkEfEijhkhkhidddEdhgidfkE" ascii
       $s14 =
"kgfjjjEEgkdiehfeEjihkfEeididdeEjhggEjedhdfEjiddgEgghejEidEfEEfgfjfhdghfd
dfihfidfEedikfdfjkiffkjiijiiijdhgghekhkegkidkgfjijhkiigg" ascii
       $s15 =
"eekgEeideheghidkkEkkfkjikhiEhiefggdkhifdgEhhdEkkEkgjdEjjeEjhjhihfdgEdEid
igefhhikdgdfEEdjEeggiEdfkdEdiEffdddkgikhhkihigEhjEdehieh" ascii
       $s16 = "eddEfefEEd" ascii
       $s17 =
"hiefgfgkdfhgEdhEEgfhfegiiekgkdheihfjjhdeediefEkekdgeihhdfhhgjjiddjehgEhi
gEkEiEghejfidgjkdjidfkkfjEkfidfdiihkkEdEkEjjkEghfEdiihgE" ascii
       $s18 =
"kfifkfkgdgdfhefdfejjdjigEhghidiiEekeEidEhghijgfkgkkedeeiggeEdhddkdhgigdj
EihjiEjkgjjEefedfhidjkEjfghfjfdfdEjhkjjddjEfdgkEEikifdhE" ascii
       $s19 =
"dedkdeeeeefgdEgfkkiEEfidikkffgighgEfiEEidgehdeiEhhjhjgiEdfkjihEgdgdefgkE
figdfedijhejEgdhkEdifEehifgdhddhfjghjfiifdhiigedggEdikeE" ascii
       $s20 =
"efigfkfkkkfkdifiEhkhjkiejjidgkEfhEfehidhEfekgejgefEjEgdgefgidjjfdkjEfgfE
```

```
igijhidideEEffjefkkkjjeeigggiighdddEddgegjEfEffjjjiddiEk" ascii
    condition:
       uint16(0) == 0x5a4d and filesize < 200KB and
       1 of ($x*) and 4 of them
 }

 rule bumblebee_13842_wSaAHJzLLT_exe {
    meta:
       description = "BumbleBee - file wSaAHJzLLT.exe"
       author = "The DFIR Report via yarGen Rule Generator"
       reference = "https://thedfirreport.com"
       date = "2022-11-13"
       hash1 =
"df63149eec96575d66d90da697a50b7c47c3d7637e18d4df1c24155abacbc12e"
    strings:
       $s1 = "ec2-3-16-159-37.us-east-2.compute.amazonaws.com" fullword
ascii
       $s2 = "PAYLOAD:" fullword ascii
       $s3 = "AQAPRQVH1" fullword ascii
       $s4 = "AX^YZAXAYAZH" fullword ascii
       $s5 = "/bIQRfeCGXT2vja6Pzf8uZAWzlUMGzUHDk" fullword ascii
       $s6 = "SZAXM1" fullword ascii
       $s7 = "SYj@ZI" fullword ascii
       $s8 = "@.nbxi" fullword ascii
       $s9 = "Rich}E" fullword ascii
    condition:
       uint16(0) == 0x5a4d and filesize < 20KB and
       all of them
}
```

MITRE

Malicious File – T1204.002

Windows Command Shell – T1059.003

PowerShell – T1059.001

Process Injection – T1055

File Deletion – T1070.004

LSASS Memory – T1003.001

Exploitation for Privilege Escalation – T1068

Lateral Tool Transfer – T1570

Valid Accounts – T1078

Service Execution – T1569.002

SMB/Windows Admin Shares – T1021.002

Remote System Discovery – T1018

Process Discovery – T1057

Domain Groups – T1069.002

Rundll32 – T1218.011

Domain Account – T1087.002

System Information Discovery – T1082

Security Account Manager – T1003.002

Network Share Discovery – T1135

Pass the Hash – T1550.002

Mark-of-the-Web Bypass – T1553.005

Bypass User Account Control – T1548.002

Web Protocols – T1071.001

Spearphishing Link – T1566.002

Masquerading – T1036

Internal case #13842

« FOLLINA EXPLOIT LEADS TO DOMAIN COMPROMISE

EMOTET STRIKES AGAIN – LNK FILE LEADS TO DOMAIN WIDE RANSOMWARE »

Search … Search

Type your email… Subscribe

Register For Our Next CTF

Reports

Threat Intelligence

Detection Rules

DFIR Labs

Mentoring and Coaching