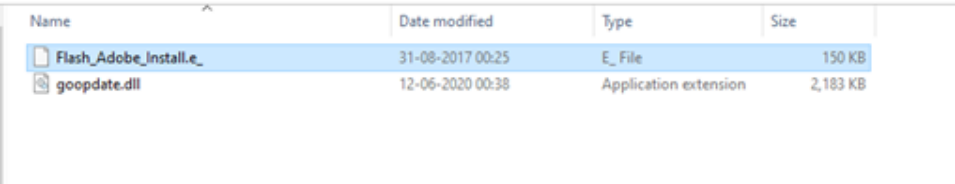
OceanLotus Continues With Its Cyber Espionage Operations

cybleinc.com/2020/11/17/oceanlotus-continues-with-its-cyber-espionage-operations/

November 17, 2020

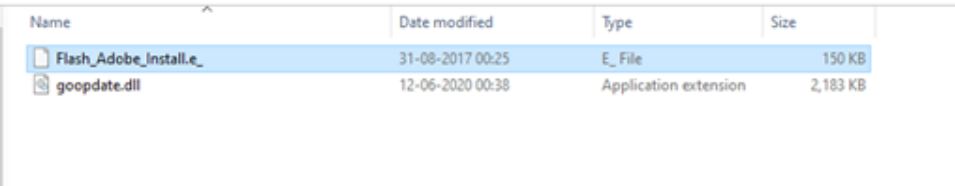


Name	Date modified	Type	Size
Flash_Adobe_Install.e_	31-08-2017 00:25	E_ File	150 KB
goopdate.dll	12-06-2020 00:38	Application extension	2,183 KB

OceanLotus APT group, also known as APT3, Cobalt Kitty, APT-C-00, SeaLotus, Ocean Buffalo, POND LOACH and TIN WOODLAWN, has been active since at least 2014. This threat actor extensively uses the watering-hole attack for compromising social engineering websites to deliver malware payloads. It carries out cyber espionage activities that targets organizations of interest to the Vietnamese Government. In the recent past, the OceanLotus APT group has had strong focus on South East Asian countries like the Philippines, Laos and Cambodia.

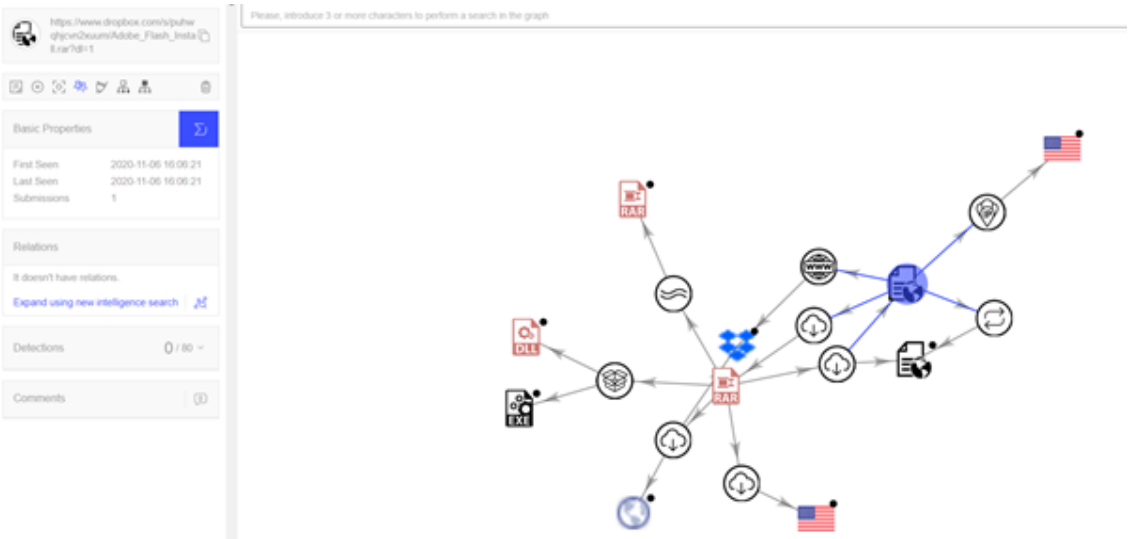
The compromised websites have functionalities like profiling users, redirecting to exploit landing page, and are being leveraged to serve malware payloads for Windows and OSX. As per open source intelligence, it was observed that the OceanLotus APT group has leveraged multiple fake news websites to target users.

In this post we will shed light on one of the latest campaigns of the threat actor with suspected ties to the Vietnamese Government. Cyble discovered that the OceanLotus APT group used an RAR archive named "*Adobe_Flash_Install.rar" to pretend to be an adobe installation, followed by the silent execution of malware payload. The figure below shows the contents of archive file.*



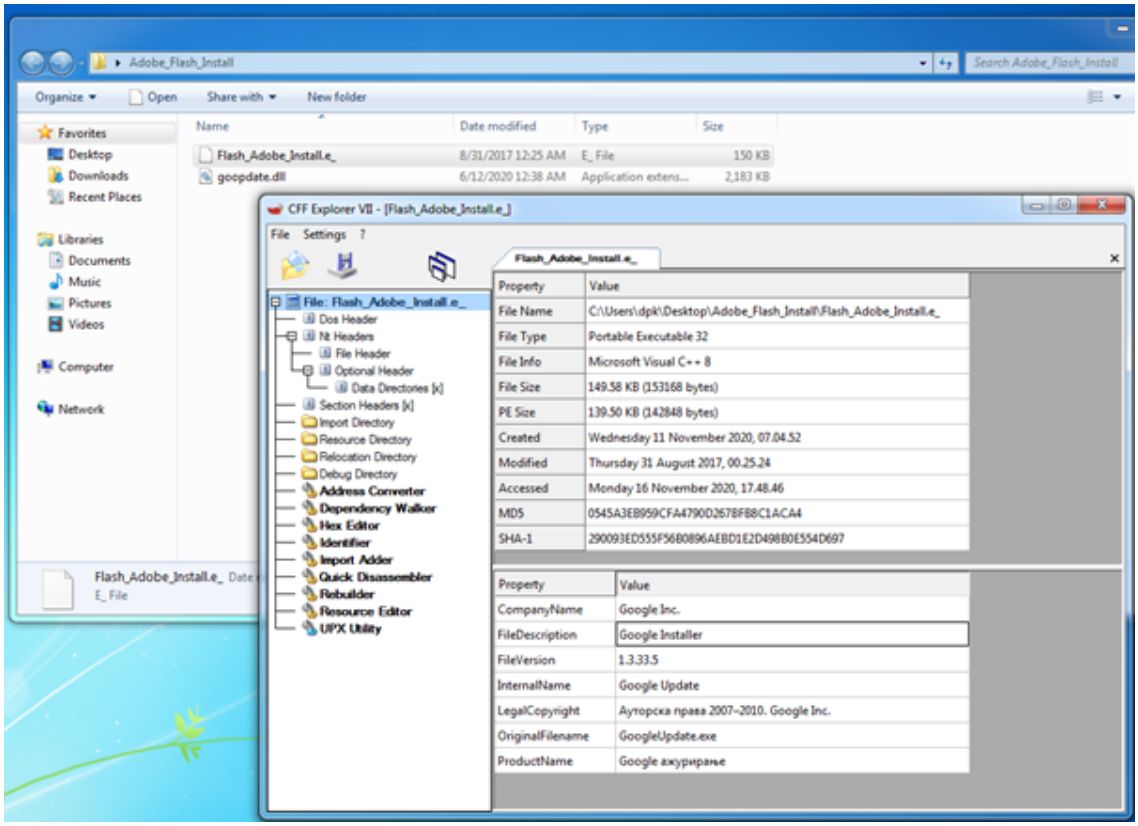
Name	Date modified	Type	Size
Flash_Adobe_Install.e_	31-08-2017 00:25	E_ File	150 KB
goopdate.dll	12-06-2020 00:38	Application extension	2,183 KB

Further research revealed that the threat actor group has used cloud storage like Google Drive to host malware payload files. The Hook diagram below shows that malware payload file is hosted on the dropbox link "hxxps://www.dropbox[.]com/s/puhwqhjcvn2xuum/Adobe_Flash_Install[.]rar?dl=1".

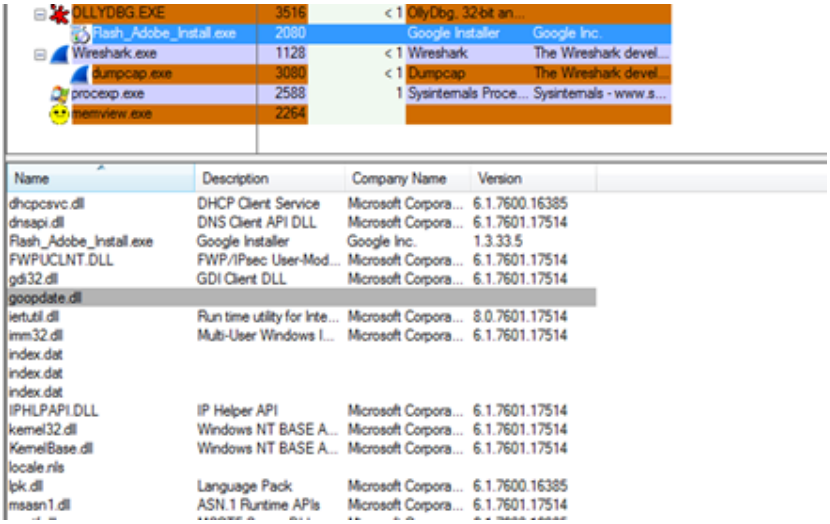


Technical Analysis:

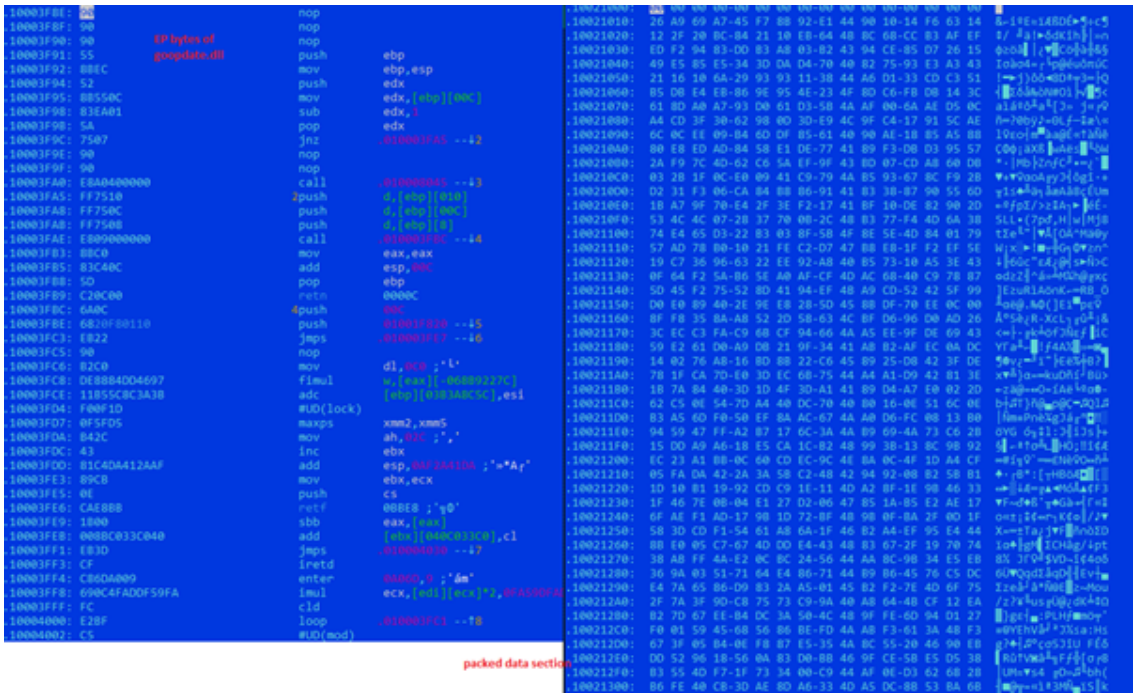
As discussed above, the RAR file contains Adobe_Flash_Install.exe and goopdate.dll. The file named *"Adobe_Flash_Install.exe"* is a legitimate Google update utility used in the side-loading of the malicious dynamic link library named *"goopdate.dll"* from the attacker. The version information of file provides more insight about the Installer, as shown in the figure below.



Upon execution, the installer side-loads and executes the attacker DLL through the search order hijacking method. The process explorer figure below clearly shows the DLL loaded by a legitimate Google Update utility.



The attacker DLL is heavily packed using custom packer as seen in the Hex view of Entry point bytes and data section as depicted in the image below.



The obfuscated attacker DLL is responsible for loading and executing the Cobalt Strike stager into the memory, followed by its execution. This DLL contains several configuration strings encoded with a simple xor encryption, and these strings include C2 url , browser information and cookie detail etc,.

At the time of our analysis, we observed that the Cobalt Strike stager tries to download and execute a shellcode from a remote server that has links to the URL "*summerevent.webhop[.]net/f2JZ". The debugger image attached below shows the hardcoded C2 domain that is decoded during the runtime.*

```
0186F460  773A78CA  CALL to LoadLibraryA from wininet.773A78C4
0186F464  773A79B4  FileName = "urlmon.dll"
0186F468  774399EC  wininet.774399EC
0186F46C  00000000
0186F470  00000000
0186F474  773A787C  RETURN to wininet.773A787C from wininet.773A788E
0186F478  00244890  ASCII "https://summerevent.webhop.net/f2j2"
0186F47C  00244970
0186F480  7739B8F2  RETURN to wininet.7739B8F2 from wininet.7739B879
0186F484  002415C8
0186F488  00244970
0186F48C  00000004
0186F490  7601EAEE  SHELL32.7601EAEE
0186F494  00210000
0186F498  00210000
0186F49C  00000000
0186F4A0  00210000
0186F4A4  00000016
0186F4A8  01010000
```

The payload file has interesting functionalities like the capturing of victim system information as in the debugger view below.

```
Address   Hex dump                                          ASCII
000965E0  1B 26 B8 5C DA 36 00 24 46 50 5F 4E 4F 5F 48 4F  ←&¸\Ú6.$FP_NO_HO
000965F0  53 54 5F 43 48 45 43 4B 3D 4E 4F 00 AB AB AB AB  ST_CHECK=NO.«««««
00096600  AB AB AB AB EE FE EE FE EE FE EE FE EE FE EE FE  «««««ÎþÎþÎþÎþÎþÎþ
00096610  00 00 00 00 00 00 00 00 19 26 B8 5E D4 36 00 1B  ........↓&¸^Ô6.←
00096620  48 4F 4D 45 44 52 49 56 45 3D 43 3A 00 AB AB AB  HOMEDRIVE=C:.«««
00096630  AB AB AB AB AB FE EE FE 00 00 00 00 00 00 00 00  «««««þÎþ........
00096640  1B 26 B8 5C D6 36 00 24 48 4F 4D 45 50 41 54 48  ←&¸\Ö6.$HOMEPATH
00096650  3D 5C 55 73 65 72 73 5C 64 70 6B 00 AB AB AB AB  =\Users\dpk.«««««
00096660  AB AB AB AB EE FE EE FE EE FE EE FE EE FE EE FE  «««««ÎþÎþÎþÎþÎþÎþ
00096670  00 00 00 00 00 00 00 00 15 26 B8 52 D4 36 00 20  ........§&¸RÔ6. 
00096680  4C 4F 43 41 4C 41 50 50 44 41 54 41 3D 43 3A 5C  LOCALAPPDATA=C:\
00096690  55 73 65 72 73 5C 64 70 6B 5C 41 70 70 44 61 74  Users\dpk\AppDat
000966A0  61 5C 4C 6F 63 61 6C 00 AB AB AB AB AB AB AB AB  a\Local.«««««««
000966B0  EE FE EE FE EE FE EE FE 00 00 00 00 00 00 00 00  ÎþÎþÎþÎþ........
000966C0  1B 26 B8 5C DA 36 00 1A 4C 4F 47 4F 4E 53 45 52  ←&¸\Ú6.→LOGONSER
000966D0  56 45 52 3D 5C 5C 57 49 4E 2D 51 42 45 52 45 31  VER=\\WIN-QBERE1
000966E0  34 51 39 50 30 00 AB AB AB AB AB AB AB AB EE FE  4Q9P0.«««««««Îþ
000966F0  00 00 00 00 00 00 00 00 1B 26 B8 5C D4 36 00 21  ........←&¸\Ô6.↑
00096700  4E 55 4D 42 45 52 5F 4F 46 5F 50 52 4F 43 45 53  NUMBER_OF_PROCES
00096710  53 4F 52 53 3D 31 00 AB AB AB AB AB AB AB AB FE  SORS=1.«««««««þ
00096720  EE FE EE FE EE FE EE FE 00 00 00 00 00 00 00 00  ÎþÎþÎþÎþ........
00096730  19 26 B8 5E D4 36 00 1A 4F 53 3D 57 69 6E 64 6F  ↓&¸^Ô6.→OS=Windo
00096740  77 73 5F 4E 54 00 AB AB AB AB AB AB AB AB EE FE  ws_NT.«««««««Îþ
00096750  00 00 00 00 00 00 00 00 01 26 B8 46 D6 36 00 20  ........ ☺&¸FÖ6. 
00096760  50 61 74 68 3D 43 3A 5C 50 72 6F 67 72 61 6D 20  Path=C:\Program 
00096770  46 69 6C 65 73 5C 43 6F 6D 6D 6F 6E 20 46 69 6C  Files\Common Fil
00096780  65 73 5C 4F 72 61 63 6C 65 5C 4A 61 76 61 5C 6A  es\Oracle\Java\j
00096790  61 76 61 70 61 74 68 3B 43 3A 5C 57 69 6E 64 6F  avapath;C:\Windo
000967A0  77 73 5C 73 79 73 74 65 6D 33 32 3B 43 3A 5C 57  ws\system32;C:\W
000967B0  69 6E 64 6F 77 73 3B 43 3A 5C 57 69 6E 64 6F 77  indows;C:\Window
000967C0  73 5C 53 79 73 74 65 6D 33 32 5C 57 62 65 6D 3B  s\System32\Wbem;
000967D0  43 3A 5C 57 69 6E 64 6F 77 73 5C 53 79 73 74 65  C:\Windows\Syste
000967E0  6D 33 32 5C 57 69 6E 64 6F 77 73 50 6F 77 65 72  m32\WindowsPower
000967F0  53 68 65 6C 6C 5C 76 31 2E 30 5C 3B 43 3A 5C 55  Shell\v1.0\;C:\U
00096800  73 65 72 73 5C 64 70 6B 5C 41 70 70 44 61 74 61  sers\dpk\AppData
00096810  5C 4C 6F 63 61 6C 5C 50 72 6F 67 72 61 6D 73 5C  \Local\Programs\
00096820  46 69 64 64 6C 65 72 00 AB AB AB AB AB AB AB AB  Fiddler.«««««««
00096830  EE FE EE FE EE FE EE FE 00 00 00 00 00 00 00 00  ÎþÎþÎþÎþ........
00096840  17 26 B8 50 CE 36 00 1A 50 41 54 48 45 58 54 3D  ↨&¸PÎ6.→PATHEXT=
00096850  2E 43 4F 4D 3B 2E 45 58 45 3B 2E 42 41 54 3B 2E  .COM;.EXE;.BAT;.
00096860  43 4D 44 3B 2E 56 42 53 3B 2E 56 42 45 3B 2E 4A  CMD;.VBS;.VBE;.J
00096870  53 3B 2E 4A 53 45 3B 2E 57 53 46 3B 2E 57 53 48  S;.JSE;.WSF;.WSH
00096880  3B 2E 4D 53 43 00 AB AB AB AB AB AB AB AB EE FE  ;.MSC.«««««««Îþ
```

The network capture depicts multiple connection requests to the attacker C2 server (summerevent.webhop[.]net) as showcased in the Wireshark image below.

udp.stream eq 128

No.	Time	Source	Destination	Protocol	Length	Info
4548	435.411028	192.168.110.128	192.168.110.2	DNS	82	Standard query 0x6a0d A summerevent.webhop.net
4549	436.418535	192.168.110.128	192.168.110.2	DNS	82	Standard query 0x6a0d A summerevent.webhop.net
4550	437.432779	192.168.110.128	192.168.110.2	DNS	82	Standard query 0x6a0d A summerevent.webhop.net
4551	439.444380	192.168.110.128	192.168.110.2	DNS	82	Standard query 0x6a0d A summerevent.webhop.net
4556	443.453705	192.168.110.128	192.168.110.2	DNS	82	Standard query 0x6a0d A summerevent.webhop.net

```
> Frame 4556: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{EBB25827-3410-4600-898A-0685D9A475C7}, id 0
> Ethernet II, Src: VMware_7c:5e:23 (00:0c:29:7c:5e:23), Dst: VMware_f4:26:06 (00:50:56:f4:26:06)
v Internet Protocol Version 4, Src: 192.168.110.128, Dst: 192.168.110.2
    0100 .... = Version: 4

0000  00 50 56 f4 26 06 00 0c  29 7c 5e 23 08 00 45 00   ·PV·&··· )|^#··E·
0010  00 44 0d 65 00 00 80 11  00 00 c0 a8 6e 80 c0 a8   ·D·e···· ····n···
0020  6e 02 f6 ee 00 35 00 30  5e 15 6a 0d 01 00 00 01   n····5·0 ^·j·····
0030  00 00 00 00 00 00 0b 73  75 6d 6d 65 72 65 76 65   ·******s ummereve
0040  6e 74 06 77 65 62 68 6f  70 03 6e 65 74 00 00 01   nt·webho p·net···
0050  00 01                                              ··
```

Conclusion:

The OceanLotus APT group, a threat actor with suspected ties to the Vietnamese Government, continuously evolves with enriched Tactics, Techniques and Procedures (TTP's) as it seeks to target outside of standard spear phishing and leveraging of compromised websites. The threat actor has now created its own fake website to deliver payload, which is a clear indication of its inclination towards organized cyberattacks.

The Cyble Research team is continuously monitoring to harvest the threat indicators/TTP's of emerging APT's in the wild to ensure that targeted organizations are well informed and proactively protected.

Indicators of Compromise(IOC's):

File hashes (SHA- 256) :

230ac0808fde525306d6e55d389849f67fc328968c433a5053d676d688032e6f- Adobe_Flash_Install.rar

7fd58fa4c9f24114c08b3265d30be5aa8f6519ebd2310cc6956eda6c6e6f56f0 – Flash_Adobe_Install.exe(legit Google's Update utility)

69061e33acb7587d773d05000390f9101f71dfd6eed7973b551594eaf3f04193- goopdate.dll(BackDoor.Meterpreter)

cbca9a92a6aa067ff4cab8f1d34ec49ffc9a06c90881f48da369c973182ce06d- Backdoor:Win32/CobaltStrike

URLs:

summerevent.webhop[.]net/f2JZ

About **Cyble**

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the darkweb. Cyble's prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.io.