# Cobalt Strike: Decrypting Obfuscated Traffic – Part 4

blog.nviso.eu/2021/11/17/cobalt-strike-decrypting-obfuscated-traffic-part-4/

November 17, 2021



#### Blogpost series: Cobalt Strike: Decrypting Traffic

Encrypted Cobalt Strike C2 traffic can be obfuscated with malleable C2 data transforms. We show how to deobfuscate such traffic.

This series of blog posts describes different methods to decrypt Cobalt Strike traffic. In <u>part 1</u> <u>of this series</u>, we revealed private encryption keys found in rogue Cobalt Strike packages. In <u>part 2</u>, we decrypted Cobalt Strike traffic starting with a private RSA key. And in <u>part 3</u>, we explain how to decrypt Cobalt Strike traffic if you don't know the private RSA key but do have a process memory dump.

In the first 3 parts of this series, we have always looked at traffic that contains the unaltered, encrypted data: the data returned for a query and the data posted, was just the encrypted data.

This encrypted data can be transformed into traffic that looks more benign, using malleable C2 data transforms. In the example we will look at in this blog post, the encrypted data is hidden inside JavaScript code.

But how do we know if a beacon is using such instructions to obfuscate traffic, or not? This can be seen in the analysis results of the <u>latest version of tool 1768.py</u>. Let's take a look at the configuration of the beacon we started with in <u>part 1</u>:

🕰 @NVISO_Labs		5	– 🗆 X
@NVISO_Labs C:\Demo≻1768.py EbHm.vir			Â
File: EbHm.vir			
xorkey(chain): 0x94t45ttt			
Config found: yorkey h' ' AyAAAAAAAA Aya	aaaaafaf		
0x0001 pavload type	0x0001	0x0002	0 windows-beacon http-reverse http
0x0002 port	0x0001	0x0002	8080
0x0003 sleeptime	0x0002	0x0004	6000
0x0004 maxgetsize	0x0002	0x0004	1048576
0x0005 jitter	0x0001	0x0002	0
0x0007 publickey	0x0003	0x0100	30819f300d06092a864886f70d010101050003818d0030818902818100a738cde7
5f1fbb1c18646c377e03016b162b12ba72bdf7dd	c36b4cd2	e4e9bae	e12205a95c26170bf908105ad7fa4bbccfa798632261bed9870f975f20794e1fe49
95230/1+08a5bCae0315D+0e30bC8a1b38bD03D	/ 8655188	1336056	d325a3500dD2/d/8ad8td13Dba/3D9tD/c3tD4d/a088e323t0/b1865becd83595ta
5782351302030100010000000000000000000000000	000000000000000000000000000000000000000	00000000	20000000000000000000000000000000000000
20000000000000000000000000000000000000	00000000 0v0002	0000000 0v0100	'102 254 70 71 /nti'
0x000e SpawnTo	0x0003	0x00100	(NULL)
0x001d spawnto x86	0x0003	0x0040	'%windir%\\syswow64\\rundll32.exe'
0x001e spawnto_x64	0x0003	0x0040	'%windir%\\sysnative\\rundll32.exe'
0x001f CryptoScheme	0x0001	0x0002	0
0x001a get-verb	0x0003	0x0010	'GET'
0x001b post-verb	0x0003	0x0010	'POST'
0x001c HttpPostChunk	0x0002	0x0004	0
0x0025 license-id	0x0002	0x0004	<pre>0 trial or pirated? - Stats uniques -&gt; ips/hostnames: 434 publicke</pre>
ys: 256	00004	00000	
0x0026 DStageCleanup	0x0001	0x0002	
0X0027 DEFGCaulion	020001	010002	V 'Mazilla/5 A (compatible: MSTE 9 A: Windows NT 6 A: WOW64: Inident
/5.0)'	000000	010100	Notifia, 5.0 (compactore, Hore 5.0, windows whole, mowor, hidene
AxAAAa post uni	0x0003	0x0040	'/submit.php'
0x000b Malleable C2 Instructions	0x0003	0x0100	1
Transform Input: [7:Input,4]			
Print			
0x000c http_get_header	0x0003	0x0200	
Build Metadata: [7:Metadata,3,6:Cookie	e]		
BASE64			
Header Cookie	0,00000	0.0000	
Const header Content Type: application	Voctot-	stpeam	
Build SessionId: [7:SessionId.5:id]	i/ Uccec-	scream	
Parameter id			
Build Output: [7:Output,4]			
Print			
0x0036 HostHeader	0x0003	0x0080	(NULL)
0x0032 UsesCookies	0x0001	0x0002	1
0x0023 proxy_type	0x0001	0x0002	2 IE settings
0x003a	0x0003	0x0080	`\x00\x04`
0x0039	0X0003	080020	
0X0037 AXAA28 killdata	0x0001	020002	
AxAA29 textSectionEnd	0x0002	0x0004	0
0x002b process-inject-start-rwx	0x0001	0x0002	64 PAGE EXECUTE READWRITE
0x002c process-inject-use-rwx	0x0001	0x0002	64 PAGE EXECUTE READWRITE
0x002d process-inject-min_alloc	0x0002	0x0004	0
0x002e process-inject-transform-x86	0x0003	0x0100	(NULL)
0x002f process-inject-transform-x64	0x0003	0x0100	(NULL)
0x0035 process-inject-stub	0x0003	0x0010	'μJþ\x01ìjuíó^\x1aDø%9)'
0x0033 process-inject-execute	0x0003	0x0080	'\x01\x02\x03\x04'
0x0034 process-inject-allocation-method	0x0001	0x0002	0
020000			×

Figure 1: beacon with default malleable C2 instructions

We see for field 0x000b (malleable C2 instructions) that there is just one instruction: Print. This is the default, and it means that the encrypted data is received as-is by the beacon: it does not need any transformation prior to decryption.

And for field 0x000d (http post header), we see that the Build Output is also just one instruction: Print. This is the default, and it means that the encrypted data is transmitted as-is by the beacon: it does not need any transformation after encryption.

Let's take a look at a sample with custom malleable C2 data transforms:

@NVISO_Labs			— C	) ×	:
@NVISO_Labs C:\Demo>1768.py sample.vir					^
File: sample.vir					
length: 0x0c5bb66f					
Config found: xorkey b'.' 0x00000000 0x0	00031e0				
0x0001 payload type	0x0001 0x0002 0 1	windows-beacon_http-reverse_http			
0x0002 port	0x0001 0x0002 80				
0X0003 Sleeptime 0x0004 maxgetsize	0X0002 0X0004 500 0x0002 0x0004 140	00 03644			
0x0005 jitter	0x0001 0x0002 10				
0x0007 publickey	0x0003 0x0100 30	819f300d06092a864886f70d010101050003818d00308189028	18100e2	2be3100	
ad51f228fff4e950a4365aa3cf5dd98d383852cb	b4683702933fbab9	ea621546349ee90c49aafdacc3cf72e26ce6fecbc83b5bf7f43	6e80ba	3494685	
7768bt745e2e5a41c6be2087att5c5bd36503796	c689047b26ee5b770	667ab4+2be69+78a059a+bda+e756c4e7+436e3847ceb57134e	be09965	579b094	
929777278263616661666666666666666666666666666666	888888888888888888888888888888888888888	888888888888888888888888888888888888888	66666666	0000000	
0x0008 server,get-uri	0x0003 0x0100 'ar	nimalszet.com,/jquery-3.3.1.min.js'			
0x0043	0x0001 0x0002 0				
0×0044	0x0002 0x0004 429	94967295			
0x0045	0X0002 0X0004 429 0x0002 0x0004 429	94967295			
0x000e SpawnTo	0x0002 0x0004 423	ULL)			
0x001d spawnto_x86	0x0003 0x0040 '%	windir%\\syswow64\\dllhost.exe'			- 1
0x001e spawnto_x64	0x0003 0x0040 '%	windir%\\sysnative\\dllhost.exe'			
0x001f CryptoScheme	0x0001 0x0002 0				
0x001a get-verb 0x001b post vonb	0X0003 0X0010 G				
0x001c HttpPostChunk	0x0002 0x0004 0	051			
0x0025 license-id	0x0002 0x0004 0	trial or pirated? - Stats uniques -> ips/hostnames:	434 pi	ublicke	
ys: 256					
0x0026 bStageCleanup	0x0001 0x0002 1				
0x0027 bCFGCaution	0x0001 0x0002 0	erille/F Q (Windows NT 6 2, Trident/7 Q, pw11 Q)	ika Car	lko !	
0x0009 useragent	0x0003 0x0100 M	jouery-3 3 2 min is'	IKE Geo	_K0	
0x000b Malleable C2 Instructions	0x0003 0x0100	Jdder y - 5 + 5 + 2 + m 2 m 2 m 2 m 2 m 2 m 2 m 2 m 2 m			
Transform Input: [7:Input,4,1:1522,2:8	4,2:3931,13,15]				
Print					
Remove 1522 bytes from end					
Remove 3931 bytes from begin					
BASE64 URL					
XOR with 4-byte random key	J				
0x000c http_get_header	0x0003 0x0200				
Const_header Accept: text/html,applica	tion/xhtml+xml,ap	pplication/xml;q=0.9,*/*;q=0.8			
Const_header Accent_Encoding: gzin_de	ry.com/ flate				
Build Metadata: [7:Metadata,13,2: cfd	uid=,6:Cookie]				
BASE64 URL					
Prependcfduid=					
Header Cookie	0000 00000				
Const header Accent: text/html.annlica	dx0003 0x0200 tion/xhtml+xml.a	pplication/xml:a=0.9.*/*:a=0.8			
Const header Referer: http://code.jque	ry.com/	pp12cu22017 xm23q=0133 7 3q=010			
Const_header Accept-Encoding: gzip, de	flate				
Build SessionId: [7:SessionId,15,13,5:	cfduid]				
XOR with 4-byte random key					
BASE04 UKL Parameter ofduid					
Build Output: [7:Output,15,13,4]					
XOR with 4-byte random key					
BASE64 URL					
Print	Avaaaa (M				
0x0032 UsesCookies	0x0003 0x0080 (NO				$\downarrow$
					-

Figure 2: beacon with custom malleable C2 instructions

Here we see more than just a Print instruction: "Remove 1522 bytes from end", "Remove 84 bytes from begin", ...

These are instructions to transform (deobfuscate) the incoming traffic, so that it can then be decrypted. To understand in detail how this works, we will do the transformation manually with <u>CyberChef</u>. However, do know that tool <u>cs-parse-http-traffic.py</u> can do these transformations automatically.

This is the network capture for a single GET request by the beacon and reply from the team server (C2):

Wireshark · Follow HTTP Stream (tcp.stream eq 0) · capture.pcapng

```
GET /jquery-3.3.1.min.js HTTP/1.1
                                                                                          ~
Referer: http://code.jquery.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Cookie: cfduid=JD27BB90pAzgeGSJp68qxNUTrMedZK82D4e UYs FcwKlt8zoovN012FCEdSI2d0VAg-
WiJYZsZXGDuLNtgKqozKcHv5MDdvrYG7Id2komJAbFJmBR8SETxypgFwf0ocsumKjy4W1n94o18ZpjdB5npAt
2IaUxNmerKv5kwsBOk
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
Host: animalszet.com
Connection: Keep-Alive
Cache-Control: no-cache
HTTP/1.1 200 OK
Date: Wed, 3 Nov 2021 13:11:19 GMT
Server: NetDNA-cache/2.2
Content-Length: 5628
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
/*! 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,1
={},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?</pre>
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]]:</pre>
[])},end:function(){return this.prevObject||
this constructor()) pushes sorten sort splice n splice wextend-w fn extend-function
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (6407 bytes)
                                                                   Show data as ASCII
                                                                                          \sim
Find:
                                                                                   Find Next
                Filter Out This Stream
                                     Print
                                               Save as...
                                                             Back
                                                                        Close
                                                                                     Help
```

Figure 3: reply transformed with malleable C2 instructions to look like JavaScript code

 $\times$ 

What we see here, is a GET request by the beacon to the C2 (notice the Cookie with the encrypted metadata) and the reply by the C2. This reply looks like JavaScript code, because of the malleable C2 data transforms that have been used to make it look like JavaScript code.

Output

Download CyberChef 4 🖬 🖿 🧻 Input Operations Recipe Search... Favourites To Base64 From Base64 To Hex rom Hex

We copy this reply over to CyberChef in its input field:



The instructions we need to follow, to deobfuscate this reply, are listed in tool 1768.py's output:



instructions

To Hexdump

URL Decode

Entropy

Fork Magic Data format Encryption / Enc Public Key Arithmetic / Logi

Date / Time

So let's get started. First we need to remove 1522 bytes from the end of the reply. This can be done with a CyberChef drop bytes function and a negative length (negative length means dropping from the end):

s 📩 About / Support 🙆

+ 🗅 🗇 🛢 🖬

Length: 5628

length: 5628 lines: 2

(r=e[t])88(l88r88(w.isPlainObject(r)||(i=Array.isArray(r)))?(i?(i=!1,o=n88Array.isArray(n)?n:[]):o=n88w.isPlainObject(n)?

Output "Interview Digitable and the contributors | jquery.org/license \*/iffanction(e,t){'use strict';'05[cct'-+typeof module&"object'-+typeof module&"object'-+typeof module.exports=Acoument'(e,l):'(use strict';'05[cct'-+typeof module&"object'-+typeof module.exports=Acoument'(e,l):'(use strict';'05[cct'-+typeof module&"object'-+typeof dual modurith; (dial-document'):return t(e):t(e):('(undefleed'-typeof use module&'):(e):('(undefleed',e):('(undefleed',e):('(undefleed',e):('(undefleed',e):('(undefleed',e)):'(undefleed',e):('(und

\*/!function(e,t){"use .document?t(e,10):function(e)

Download CyberChef 🛓			Last build: a	build: 2 months ago Options 🏚 About / Support 🕖				0		
Operations	Recipe	í	a 🖿 🕯	Input	length: 5628 lines: 2	+ 🗆	) 🖻 📋	-		
drop	Drop bytes		0 11	<pre>(o[1]=n[1]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return null==e?e+":"object"==typeo e ["function"==typeof e?l[c.call(e)]  "object":typeof e/var b="3.3.1",w=function(e,t){return new</pre>						
RC4 Drop	Start Ø	Length -1522 Apply	y to each line	<pre>w.fn.Init(e,t)},T=/^[\s\wFEFF\xk0]+[\s\wFEFF\xk0]+\$/g;w.fnw.prototype= {jquery:"3.3.1",constructor:w,length:0,toArray:function()(return o.call(this)),get:function(e){return null==e}</pre>						
Drop bytes				<pre>o.call(this):ec0?this[e+this.length]:this[e]],pushStack:function(e){var tww.merge(this.constructor(),e);return t.prevObject-this,t},each:function(e){return w.each(this,e)},map:function(e){return</pre>						
A1Z26 Cipher Encode				<pre>this.publicate(w.asg(this_function(t,n)(return e.call(t,n,t)))).slice:function()(return this.publicate(w.asg)(this_anguments)).first:function()(return this.qub)state(w.asg(t).sate:function()(return this.ge(-1)).ee;function(e)(war t-this.length,m=ere(e0)?e0);return this.publicate(w)=e00(e1)[]])).ee (return this.provbject(This.constructor(t)),publis,sort:norf.gplicar.philos).extended.function( e.t.n,r.io.a=nguments[0][]().et,w=m00(e1);publis.gov=-);sort:splif(e1)=(01)[]=(a)=a=nguments[0]][]().et,w=m00(e1)[]=(a)=a(a)=a(a)=a(a)=a(a)=a(a)=a(a)=a(a)</pre>						
Favourites 📩										
Data format										
Encryption / Encoding				<pre>(r=e[t])&amp;&amp;(l&amp;&amp;r&amp;&amp;(.isPlainObject(r)  (i=Array.isArray(r)))?(i?(i=l1,o=n&amp;&amp;Array.is n:{},a[t]=w.extend(1,o,r)):void 01==r&amp;&amp;(a[t]=r));return a},w.extend({expando:"jQue</pre>	irray(n)?n:[]):o=r 'y"+	n&&w.is₽	<pre>&gt;lainObject(n)</pre>	)?		
Public Key				<pre>("3.3.1"+Hath.random()).replace(/\D/g,""),isReady:!0,error:function(e)(throw new E {},isPlainObject:function(e){var t,n;return((le )"[object Object]" ==c.call(e))88(</pre>	ror(e)},noop:fund	ction()		- 1		
Arithmetic / Logic				<pre>(t=i(e))  'function"==typeof(n=f.call(t, "constructor")&amp;&amp;t.constructor)&amp;&amp;p.call(n)===d)},isEmptyObject:function(e){var t;for(t in e)return 1;return 0},globalEval:function(e){n(e)},each:function(e,t){var n,r=0;if(C(e))</pre>						
Networking				<pre>{for(n=e.length;r<n;r++)if(i1===t.call(e[r],r,e[r]))break)else e)if(i1="e},trim:function(e){return" for(r="" in="" null='e?"":(e+"").replace(T,"")},makeArray:function(e,t&lt;/pre'></n;r++)if(i1===t.call(e[r],r,e[r]))break)else></pre>	:.call(e[r],r,e[r] ){var n=t  [];ret	]))break urn null	c;return 11-e88	- 1		
Language				<pre>(C(Object(e))?w.merge(n."string"==typeof e?[e]:e):s.call(n.e)),n}.inArray:function</pre>	ion(e.t.n){return null==t?					
Utils				Output [{},s++),"object"==typeof a  g(a)  (a={}),s===u&&(a=this,s);s <u;s++)if(null!=(e=a)< th=""><th><pre># lines: 2 /guments[s]))for()</pre></th><th>t in e)r</th><th>) Ltj</th><th></th></u;s++)if(null!=(e=a)<>	<pre># lines: 2 /guments[s]))for()</pre>	t in e)r	) Ltj			
Date / Time				<pre>(r=e[t])&amp;&amp;(l&amp;&amp;r&amp;&amp;(w.isPlainObject(r)  (i=Array.isArray(r)))?(i?(i=!1,o=n&amp;&amp;Array.is n:{},a[t]=w.extend(1,o,r)):void 0!==r&amp;&amp;(a[t]=r));return a},w.extend({expando:"jQue</pre>	urray(n)?n:[]):o=r 'y"+	n&&w.isP	'lainObject(n)	15		
Extractors				<pre>("3.3.1"+Hath.random()).replace(/\D/g,""),isReady:!0,error:function(e)(throw new E {},isPlainObject:function(e){var t,n;return!(!e  "[object Object]"!==c.call(e))88(</pre>	ror(e)),noop:fund	ction()		- 1		
Compression				<pre>(t-i(e))  *function"typeof(n-f.call(t,*constructor")&amp;&amp;t.constructor)&amp;&amp;p.call(n)- t;for(t in e)return1;return10},globalEval:function(e){m(e)},each:function(e,t){va</pre>	<pre>d)),isEmptyObjec * n,r=0;if(C(e))</pre>	ct:funct	don(e){var	- 1		
Hashing				<pre>{for(n=e.length;r<n;r++)if(!1==-t.call(e[r],r,e[r]))break)else e)if(!1="&lt;br" for(r="" in="">e},trim:function(e){return null==e?"":(e+"").replace(T,"")},makeArray:function(e,t</n;r++)if(!1==-t.call(e[r],r,e[r]))break)else></pre>	:.call(e[r],r,e[r] ){var n=t  [];ret	<pre>)))break urn nul]</pre>	cpreturn 11-e88	- 1		
Code tidy				<pre>(C(Object(e))?w.merge(n,"string"==typeof e?[e]:e):s.call(n,e)),n},inArray:function -1:u.call(t,e,n)},merge:function(e,t)(for(var n=+t.length,r=0,i=e.length;r<n;r++)e< pre=""></n;r++)e<></pre>	[i++]=t[r];return	11t?		-1		
Forensics				<pre>e.length=1,e},grep:function(e,t,n){for(var r,1=[],o=0,a=e.length,s=1n;oca;o++)(r=1 i},map:function(e,t,n){var r,1,o=0,s=[];if(C(e))for(r=e.length;o<r;o++)null=(i=t(< pre=""></r;o++)null=(i=t(<></pre>	.(e[o],o))!==s&&1. z[o],o,n))&&s.pusi	.push(e[ h(i);els	o]);return se for(o in	-1		
Multimedia				<pre>e)null=(l=t(e[o],o,n))&amp;ds.push(1);return a.apply([],S)),guld:1,support:n)),"funct (w.fn[Symbol.iterator]-n[Symbol.iterator]),w.each("Boolean Number String Function</pre>	on"==typeor Symbo Array Date RegExp	Object	Error	-1		
Other				<pre>Sympoi.spiit("), function(e,t){[[[object "+t+"]]]=t.toLowerCase()}); function C( e&amp;&amp;e.length,n=x(e);return!g(e)&amp;&amp;!y(e)&amp;&amp;("array"===n  ===t  "number"==typeof t&amp;&amp;&gt;</pre>	j{var t=lle5&"ler H6&t-1 in e)}var	igth~in E=functi	ion(e){var	1		
Flow control	STEP	Z BAKE!	Auto Bake	[:,n,r,j,o,ə,s,u,j,c,r,p,o,n,g,y,v,m,x,o~31214~11mm VBte,yie+.document,1=0,C=0; [return e===t&&(f=18),0;+(=),h=(),h=(),h=(),h=(),h=(),h=(),h=(),h	ae(),K=ae(),S=ae( ice,O=function(e,t qHDoAPuGQ	(),D=fun t){for(v	Ar (e,t)			

# Figure 6: dropping 1522 bytes from the end Then, we need to remove 84 bytes from the beginning of the reply:

Download CyberChef 🛓			ild: 2 months ago Options 🏚 About / Support 🕖						
Operations	Recipe		2 🖿 🕯	Input start: end: Bength:	625 length: 5628 628 lines: 2 + 🗅 🗃 🖬				
drop	Drop bytes 🛇 II			<pre>/*! jQuery v3.3.1   (c) JS Foundation and other contributors   jquery.org/license */!function(e,t){"use strict";"object"==typeof module&amp;@"object"==typeof module.exports?module.exports=e.document?t(e.10):function(e)</pre>					
RC4 Drop	Start Ø	Length -1522	Apply to each line	{if(le.document)throw new Error("jQuery requires a window with a document");retu window:this,function(e,t)("use strict";var n=	<pre>rn t(e)}:t(e)}("undefined"!=typeof window?</pre>				
Drop bytes				[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexC {},c=l.toString,f=l.hasOwnProperty,p=f.toString,d=p.call(Object),h=(),g=function	f,l= e(t){return"function"==typeof				
A1Z26 Cipher Encode	Drop bytes		0 11	<pre>t&amp;&amp;"number"!=typeof t.nodeType},y=function e(t){return null!=t&amp;&amp;t==t.window},v= m(e,t,n){var i,o=(t=t) r).createElement("script");if(o.text=e,n)for(i in v)n[i]8</pre>	<pre>{type:10,src:10,noModule:10};function &amp;</pre>				
Favourites 📩	Start Ø	Length 84	Apply to each line	<pre>(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o)}function x(e){return e  "function"==typeof e?l[c.call(e)] "object":typeof e}var b="3.3.1",w=function</pre>	nulle?e+"":"object"typeof (e,t){return new				
Data format				<pre>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)},</pre>	et:function(e){return null==e?				
Encryption / Encoding				<pre>o.call(this):e&lt;8?this[e+this.length]:this[e]},pushStack:function(e){var t=w.merg t.prevObject=this,t},each:function(e){return w.each(this,e)},map:function(e){ret</pre>	e(this.constructor(),e);return urn				
Public Key				<pre>this.pushStack(w.map(this,function(t,n){return e.call(t,n,t)}))},slice:function( this.pushStack(o.apply(this,arguments))},first:function(){return this.eq(0)},las</pre>	){return t:function(){return				
Arithmetic / Logic				<pre>this.eq(-1)},eq:function(a){var t=this.length,n=+a+(ac001:0);return this.pushStack(n&gt;=0&amp;dinct?[this[n]]:[])},and:function {return this.prev0dybct[[this.constructor()],pushis.portn.sort.pollce:n.splice:n.splice),w.extendw.fn.extend=function{}var e.t,n,r,t,o,a=argument[s][[](.st_ui=uargument.length_i=ifsfor("boolaan"-vrypod a&amp;di_a=argument[s]]] {};s++),~object"=vrypof a[[g(0)][(a=c)],s==ua&amp;dia=dia=dia=dia=dia=dia=dia=dia=dia=dia=</pre>					
Networking									
Language				<pre>((ree[t])86(168n88(w.15P1a1n0b)ect(r)][(1=Array.15Array(r))]/(1/(1=1,0=n86Array. Output 2.</pre>	time: 2ms Jeneth: 4422				
Utils			<pre>ifunction(e,t){"use strict";"object"==typeof module&amp;&amp;"object"==typeof module.exp</pre>	dule.exports?module.exports=e.document?					
Date / Time				<pre>t(e, 0):function(e)[if(le.document)thrue new Front"]Deer requires a undow with a document"):return t(e)):t(e)) ("undefined": "hyperia undowidendowiths, incline(e,1);"und struct struct"; yue new file(");"und struct struct"; yue new file(");"und struct struct"; yue new file(");"und struct struct struct struct yue new file(");"und struct struct struct yue new file(");"und struct struct yue new fi</pre>					
Extractors									
Compression				<pre>t&amp;&amp;"number"!=typeof t.nodeType},y=function e(t){return null!=t&amp;&amp;t==t.window},v= m(e,t,n){var i,o=(t=t) r).createElement("script");if(o.text=e,n)for(i in v)n[i]8</pre>	<pre>{type:!0,src:!0,noModule:!0};function &amp;</pre>				
Hashing				<pre>(o[i]=n[i]);t.head.appendChild(o).parentMode.removeChild(o))function x(e){return null==e?e+":"object"==typ e  "function"==typeof e?l[c.call(e)]  "object":typeof e}var b="3.3.1",w=function(e,t){return new</pre>					
Code tidy				<pre>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)),g</pre>	et:function(e){return nulle?				
Forensics				<pre>o.call(this):e&lt;0?this[e+this.length]:this[e]],pushStack:function(e){var t=w.merg t.prevObject=this,t},each:function(e){return w.each(this,e)},map:function(e){return w.each(this,e)}</pre>	e(this.constructor(),e);return urn				
Multimedia				<pre>this.pushStack(w.map(this,function(t,n){return e.call(t,n,t)}))},slice:function( this.pushStack(o.apply(this,arguments))),first:function(){return this.eq(0)},las</pre>	){return t:function(){return				
Other				<pre>this.eq(-1)},eq:function(e){var t=this.length,n=+e+(e&lt;0?t:0);return this.pushSta {return this.prevObject  this.constructor()},push:s,sort:n.sort,splice:n.splice]</pre>	ck(n>=0&&n <t?[this[n]]:[])},end:function() ,w.extend=w.fn.extend=function(){var</t?[this[n]]:[])},end:function() 				
Flow control	STEP	Z BAKE!	Auto Bake	<pre>e,t,n,r,i,o,a-arguments[0] (),s=1,u-arguments.length,l=l;for("boolean"-etypeof {},s=+),~object"=stypeof a  g(a) (a&lt;}),s==u&amp;&amp;(a+t),s=(s+t)</pre>	<pre>a&amp;&amp;(l-a,a-arguments[s]   arguments[s]))for(t in e)n=a[t],a!== isArray(n)?n:[]):o=n&amp;&amp;w.isPlainObject(n)? uery"+</pre>				

Figure 7: dropping 84 bytes from the beginning And then also dropping 3931 bytes from the beginning:

Download CyberChef 🛓		La	st build: 2	ild: 2 months ago Options 🏚 About / Supp			port 🕜	
Operations	Recipe	8 🖬	Ξ.	Input	length: 5628 lines: 2	+ D		i =
Operations drop RC4 Drop Drop bytes A1226 Cipher Encode Fevourites Cate format	Recipe Drop bytes Start 0 Drop bytes Start 0	Leigh 84 Apply to eac	th line	<pre>imput /*! jQuery v3.3.1   (c) 35 Foundation and other contributors   jquery.org/licess * strict';'object'=-typeof module&amp;d'object'=-typeof module.exports/module.exports/module.exports/ lft(!.document)throw new irror(']Query requires a inflow with a document')return indowrithsi,function(e,t)('use strict':ywn == ],r=e.document,l=0bject.getPrototype0f,onn.slice,a=n.coccat,s=n.push,u=n.inde0f,1 (.c=l.iostring,d'.l.asounProperty p.f-toString,d=p.call(Object).h=().gefunction et &amp;&amp;Touber'!=typeof t.nodelype).y=function et()[return null=t&amp;&amp;Touber].y=function et &amp;&amp;Touber'!=typeof t.nodelype).y=function et()[return null=t&amp;&amp;Touber].y=function et (et,n)(var 1_epicef*]).y=function et()[return null=t&amp;&amp;Touber].y=function et (=[inutcion'=*posef*]](c)[]=(bject';typeof a)[x=0, a)[return(ton(e, .v.fn.int(c,t)),1-/^['tutFFFVad]=['tutFFFVad]=fgur,fnow.prototype= ['guery':3.3.1',ostructore.ukenthe,enthe.better).function eta(b)].gett</pre>	<pre>lines: 2 //function(e,t) ccument?t(e,le) t(e)):t(e)):t(e)):t(e); /return"funct: be:l0,src:l0,nol ll==e?e+"":"obj }(return new function(e)(return</pre>	"use :function Jefined": Module:10 ect"==typ	n(e) !=typeof w peof );functio peof ==e?	rindow?
Encryption / Encoding Public Key Arithmetic / Logic	Start 0	Langth 3931 ‡ Apply to eac	th line	o.call(this):edPthis[ethis].ength):this[d]),pubStack:function(d)(wr tw.merge(t, prev0gtethis),s];eachiruncion(e)(return each(this.e),pubStack(.engt(this.function(e),r(wr neach(this.e),pubStack(.engt(this.function(e),r(wr neach(this.e),pubStack(.engt(this.function((t, nt)))),slice:function((t, nt))),slice:function((t, nt)),slice:function((t, nt)),slice:function((t, nt)),slice:function((t, nt)),slice:function((t, nt)),slice:function((t, nt)),slice:function((t, nt)),slice:function((t, nt)),slice:function((t, nt)),slice),slice:function((t, nt)),slice),slice:function(function(t, nt)),slice),slice:f	nis.constructor aturn unction(){return u>=8&&nct?[this] extend=w.fn.ext0	),e);ret 1 [n]]:[])) end=funct	turn },end:func tion(){var	ction()
Networking Language Utils				<pre>a,t,n,r,1,o,warguments[0] [(),t-1,u-arguments.length,l=11;for("boolaam-"+typed fail(),t-1),t-1;for("boolaam-"+typed fail(),t-1),t-1),t-1,t-1,t-1,t-1,t-1,t-1,t-1,t-1,t-1,t-1</pre>	<pre>&amp;(l=a,a=argument guments[s]))for rray(n)?n:[]):o     time: 2ms     length: 91     lines: 1</pre>	:s[s]   (t in e)r m88w.isP	n=a[t],a!= PlainObjec ] [t] ⊨	:t(n)?
Date / Time Extractors				telvsf=HeCumhCn2KxASeHP2kCAnU3jKshqBhsHpsLF48_1PQ6dbt1QvQxKSkVnch3zVUbezHeFC3nx188wq	(DoAPuGQ			
Compression Hashing Code tidy								
Forensics Multimedia Other								
Flow control	STEP	Z BAKE!	Bake					

Figure 8: dropping 3931 bytes from the beginning

And now we end up with output that looks like BASE64 encoded data. Indeed, the next instruction is to apply a BASE64 decoding instructions (to be precise: BASE64 encoding for URLs):

Download CyberChef 👤		Last buik	build: 2 months ago Options 🏚 About / Support 🌍				
Operations	Recipe	2 🖬 i	Input length lines	5628 + 🗅 🗩 🖬 🖬			
base64	Drop bytes	0 11	/*! jQuery v3.3.1   (c) JS Foundation and other contributors   jquery.org/license */!funct strict":"object"==typeof module&&"object"==typeof module.exports?module.exports?module.exports=e.document	ion(e,t){"use ?t(e,10):function(e)			
To Base64	Start	Length	<pre>strict y ougect ==sypeor mouseas ougect ==cypeor mouse.exports/mouse.exports=c.mocumentr(e,ie);function(e) {if(le.document)inow new Error["]Query requires a window with a document");return t(e)}:t(e)}("undefined"!=typeof w window:the function(e trute="trut</pre>				
From Base64			<pre>[],ree.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l= {),c=1.toString.f=1.hasOwnProperty.p=f.toString.d=p.call(Object),h=(),g=function e(t)(retu</pre>	rn"function"typeof			
Show Base64 offsets	Drop bytes	0 11	<pre>t8&amp;"number" =typeof t.nodeType},y=function e(t){return null =t8&amp;t==t.window},v={type:10,s m(a,t,n){var i_a=(t-t  r).createElement("script");if(o.text=a,n)for(i in v)n[i]&amp;&amp;</pre>	rc:10,noModule:10};function			
Fork	Start Ø	84 Apply to each line	<pre>(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o))function x(e){return null==e?e e  "function"==typeof e?l[c.call(e)]  "object":typeof e}var b="3.3.1",w=function(e,t){return fermions</pre>	++"":"object"typeof unn new			
From Base32	Deve betw	S 11	<pre>w.fn.init(e,t)},T=/^[\s\uFEFF\xA8]+ [\s\uFEFF\xA8]+\$/g;w.fn=w.prototype= {jquery:"3-3-1",constructor:w,length:0,toArray:function(){return o.call(this)},get:function</pre>	n(e){return null==e?			
From Base58	Start	Length -	<pre>o.call(this):e&lt;0?this[e+this.length]:this[e]},pushStack:function(e){var t=w.merge(this.con t.prevObject=this,t},each:function(e){return w.each(this,e)},map:function(e){return</pre>	istructor(),e);return			
From Base85	0	3931 Apply to each line	<pre>e 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</pre>				
Parse SSH Host Key	From Base64	0 11	<pre>this.eq(-1)},eq:function(e){var t=this.length,m=+e+(e&lt;0?t:0);return this.pushStack(n&gt;=08&amp;nct?[this[n]]:[])},end:function {return this.prev0bject[[this.constructor(]),push:s_sort:n.sort,splice:n.splice},w.extend=w.fn.extend=function(){var</pre>				
To Base32	Alphabet		<pre>e,t,n,r,1,o,a-arguments[8]]{;s=1,u=arguments.lengtn,l=1;for("bolean"==typeot ass[1=a,a=arguments[s]] {},s+s+)="object"==typeof a][g(a)][(a=(),s==u&amp;&amp;(a=this,s=);c(u;s+))f(null=(e-arguments[s]))for(the for set of the set of the</pre>				
To Base58	A-28-20-9	Standard (REC 4648): A-7a-z0-9+/=	(r=e[t])86(186n58(w.1sPlainObject(r)  (1=Array.isArray(r)))?(1?(1=11,0=n66Array.isArray(n)))?	ine: 205			
To Base85	Remove non-alphabet c	hars URL safe (RFC 4648 §5): A-20-9	Cantorsyn → Cumput (A.2%)(20.9- ··, 4.8.   ··, 4.8.				
Favourites 🖈		Filename safe: A-Za-z0-9+-= itoa64: ./0-9A-Za-z=					
Data format		XML: A-Za-z0-9					
Encryption / Encoding		y64: A-Za-20-9 z64: 0-9a-zA-Z+/=					
Public Key		Radix-64 (RFC 4880): 0-9A-Za-z+/=					
Arithmetic / Logic		Xxencoding: +-0-9A-Za-z					
Networking		BinHex: !-,-0-689@A-NP-VX-Z['a-fh-mp-r ROT13: N-ZA-Mn-za-m0-9+/=					
Language		UNIX crypt: ./0-9A-Za-z					
Utils							
Date / Time	CTED CONTRACT						
https://gchq.github.io/CyberChel/#	STEP	Auto Bake					

Figure 9: decoding BASE64/URL data

The next instruction is to XOR the data. To do that we need the XOR key. The malleable C2 instruction to XOR, uses a 4-byte long random key, that is prepended to the XORed data. So to recover this key, we convert the binary output to hexadecimal:

Download CyberChef 🛓			Last build:	build: 2 months ago Options 🏚 About / Suppr				port 🕜
Operations	Recipe		2 🖿 🕯	Input	length: 5628 lines: 2	+ 🗅	•	i =
hex	Drop bytes 🛇 11			<pre>/*! jQuery v3.3.1   (c) J5 Foundation and other contributors   jquery.org/license */!function(e,t)("use strict":"object"==typeof module&amp;&amp;"object"==typeof module.exports?module.exports=e.document?t(e,10):function(e)</pre>				
То Нех	Start Ø	Length -1522	Apply to each line	<pre>{if(le.document)throw new Error("jQuery requires a window with a document");return window:this,function(e,t)("use strict";var n=</pre>	t(e)}:t(e)}("und	fined"!=	typeof w	rindow?
From Hex				<pre>[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf, {},c=l.toString,f=l.hasOunProperty,p=f.toString,d=p.call(Object),h={},g=function e</pre>	l= (t){return"function	in"type	of	- 1
Hex to PEM	Drop bytes		0 11	<pre>t8&amp;"number" =typeof t.nodeType},y=function e(t){return null =t8&amp;t===t.window},v={ty m(e,t,n){var i,o=(t=t) r).createElement("script");if(o.text=e,n)for(i in v)n[i]&amp;&amp;</pre>	/pe:10,src:10,noM	dule:10)	;function	n
PEM to Hex	Start Ø	Length 84	Apply to each line	<pre>(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o))function x(e){return nu e  "function"==typeof e?l[c.call(e)]  "object":typeof e}var b="3.3.1",w=function(e, </pre>	ulle?e+"":"obje t){return new	t"type	of	- 1
To Hexdump	Dava hadaa		0.11	<pre>w.fn.init(e,t)},T=/^[\s\uFEFF\x48]+ [\s\uFEFF\x48]+\$/g;w.fn-w.prototype- {jquery:"3.3.1",constructor:w,length:0,toArray:function(){return o.call(this)},get</pre>	function(e){return	n null	ie?	- 1
From Hexdump	Sheet	Length	_	<pre>o.call(this):e&lt;0?this[e+this.length]:this[e]},pushStack:function(e){var t=w.merge( t.prevObject=this,t},each:function(e){return w.each(this,e)},map:function(e){return</pre>	this.constructor()	,e);retu	Inu	- 1
To Hex Content	0	3931	Apply to each line	<pre>this.pushStack(w.map(this,function(t,n){return e.call(t,n,t)}))},slice:function(){r this.pushStack(o.apply(this,arguments))},first:function(){return this.eq(0)},last:</pre>	return function(){return			
From Hex Content	From Base64 🛇 11			<pre>this.eq(-1);eq:function(e)(var t-this.length,m=va(ee02::0);return this.pushStack(n)=e8&amp;ort?[this[1]:]);end=function( {return this.prev0bject][this.constructor());pushis;sortin.sort.splice:n.splice);w.extend=w.fn.extend=function(){var e,tn,r,t,o-arguments[0][(),s=t_u=raguments[.length,l=1;for("boolsam"=rypoor la&amp;(l=a,=raguments[s])] (),s=t_v)=0;bect="stypeof alg(o)]((ac());s==sa&amp;d&amp;(acthis,s=);so((s=t+))f(m)l1=(=raguments[s))]for(t=n=na[t],a]== (=act1)&amp;B(MBMU (splice)act(ac());a=(tac()))f(2(ta());a=(tac()))f(2(ta()));a=(tac())f(2(ta()));a=(tac()))f(2(ta()));a=(tac()))f(2(ta()));a=(tac())f(2(ta()));a=(tac()))f(2(ta()));a=(tac())f(2(t</pre>				
Hex Density chart	Alphabet							
Parse ASN.1 hex string	H 10 10 7 _			Uniterst Uniterst	time: 2ms length: 203	86		
Hex to Object Identifier	Remove non-alphabet chars			b7 85 71 17 e1 e4 0b 09 a1 0a 7d 8a c4 0e 5e 1c fd a4 08 09 d4 26 32 ac 86 a0 4c bi	lines: 1 9 ca 6c 2c 5e 3c -	c 83 d0	19 d3 62	2 89 85
Object Identifier to Hex	To Hex		⊘ 11	00 54 af 54 56 67 21 27 35 54 6d ec c7 59 f7 37 9f 09 7c f3 0a 87 0e 80 0f b8 64				
HTML To Text	Delimiter	Bytes per line						
JPath expression	Space	0						
XPath expression								
Disassemble x86								
Escape string								
Find / Replace								
From Base62								
HASSH Client Fingerprint	STEP	E BAKE!						
https://github.com/gchq/CyberChef/blob/master/CHANGELOG.md	Site		Auto Bake					

Figure 10: hexadecimal representation of the transformed data The first 4 bytes are the XOR key: b7 85 71 17

We use that with CyberChef's XOR command:

Download CyberChef 👲			Last build:	ast build: 2 months ago Options 🏚 About / Support 🕖				upport 🕜
Operations	Recipe		2 🖿 🕯	Input	length: 5628 lines: 2	+ C	- E	î =
hex	Drop bytes		0 11	<pre>/*! jQuery v3.3.1   (c) JS Foundation and other contributors   jquery.org/license */! strict";"object"==typeof module&amp;&amp;"object"==typeof module.exports?module.exports=e.doc</pre>	<pre>function(e,t){' ment?t(e,!0);</pre>	'use functio	n(e)	
То Нех	Start	Length	Apply to each line	{if(le.document)throw new Error("jQuery requires a window with a document");return t( window:this,function(e,t){"use strict";var n=	e)}:t(e)}("unde	fined"	!=typeof	window?
From Hex		. 4344		<pre>[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.push,u=n.indexOf,l= {},c=1.toString,f=1.hasOunProperty,p=f.toString,d=p.call(Object),h=(),g=function e(t)</pre>	return"functio	on"ty	peof	- 1
Hex to PEM	Drop bytes		⊘ 11	<pre>t&amp;&amp;"number" =typeof t.nodeType},y=function e(t){return null!=t&amp;&amp;t==t.window},v={type m(e,t,n){var i_o=(t-t  r).createElement("script");if(o.text=e,n)for(i in v)n[i]&amp;&amp;</pre>	10,src:10,noMc	dule:/	0};functi	ion
PEM to Hex	Start Ø	Length 84	Apply to each line	<pre>(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o))function x(e){return null e  "function"==typeof e?l[c.call(e)] "object":typeof e)var b="3.3.1",w=function(e,t)</pre>	-e?e+"":"objec	:t"ty	peof	
To Hexdump	Dran buter		0.11	<pre>w.fn.init(e,t)},T=/^[\s\uFEF\xA0]+ [\s\uFEF\xA0]+\$/g;w.fn=w.prototype= {jquery:"3.3.1",constructor:w,length:0,toArray:function(){return o.call(this)},get:fu</pre>	iction(e){retur	n null	e?	
From Hexdump	Urop bytes	Length	_	<pre>o.call(this):e&lt;0?this[e+this.length]:this[e]},pushStack:function(e)(var t=w.merge(thi t.prevObject=this,t},each:function(e){return w.each(this,e)},map:function(e){return</pre>	.constructor()	,e);re	turn	
To Hex Content	0	3931	Apply to each line	<pre>this.pushStack(w.map(this,function(t,n){return e.call(t,n,t)}))},slice:function(){ret this.pushStack(o.apply(this,arguments))},first:function(){return this.eq(0)},last:fun</pre>	urn :tion(){return			- 1
From Hex Content	From Base64		⊘ 11	<pre>this.eq(-1)},eq:function(e){var t-this.length,n-+e+(e&lt;0?t:0);return this.pushStack(n&gt; {return this.prevObject][this.constructor()],push's,sort.n.sort,splice.n.splice),wexe</pre>	-0&&nct?[this[r tend=w.fn.exter	)]]:[]) 1d=func	},end:fur tion(){vi	nction() ar
Hex Density chart	Alphabet			<pre>#,t,n,r,1,o,a=arguments[d] {},s=1,u=arguments.length,l=11;for("bolean ==typeor add( {},s++),"object"==typeof a  g(a)  (a={}),s===u&amp;&amp;(a=this,s=-);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(n< td=""><th>nents[s]))for(t</th><td>t in e)</td><td>n=a[t],aí</td><td></td></u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(null=(e=arguments);s<u;s+)if(n<></pre>	nents[s]))for(t	t in e)	n=a[t],aí	
Parse ASN.1 hex string	A-28-20-9			<pre>(r=[t])&amp;&amp;(l&amp;srbs(w.lsplainObject(r)  (l=array.lsarray(r)))/(l/(l=1,0=n&amp;sarray.lsarr Output</pre>	time: 1ms length: 202	B [		ect(n)/
Hex to Object Identifier	Remove non-alphabet	thars		00 00 00 00 56 61 7a 1e 16 8F 0c 0d 73 8b 2F 0b 4a 21 70 1e 63 a3 43 bb 31 25 3d a7 7d e9 5d 49 8b 79 F2 c7 ae 56 13				13 9e bc
Object Identifier to Hex	XOR		⊘ 11	55 25 68 e3 d3 16 36 90 b0 25 7a 5b 42 28 e0 80 1a 78 6b 44 8f f6 19 37 8a c9 73				
HTML To Text	Key		HEX *					
JPath expression	67 85 71 17		TIEX.					
XPath expression	Standard	Null preserving	1					
Disassemble x86	To Hex		0 11					
Escape string	Delimiter	Bytes per line						
Find / Replace	Space	0						
From Base62								
HASSH Client Fingerprint	STED	T BAKE						
HASSH Server Fingerprint	SIEP	A DAKE:	Auto Bake					

#### Figure 11: XORed data

Notice that the first 4 bytes are NULL bytes now: that is as expected, XORing bytes with themselves gives NULL bytes.

And finally, we drop these 4 NULL bytes:

Download CyberChef 👲			Last build:	2 months ago	Options 🔯 About / Support 😰			
Operations	Recipe		2 🖬 🕯	Input	length: 5628 + 🗅 🗃 🗃			
drop	Drop bytes 🚫 II			/*! jQuery v3.3.1   (c) JS Foundation and other contributors   jquery.org/license */!function(e,t){"use strict":"object"=stupped module&&"object"=styped module.exports/amodule.exports/e.l0):function(e)				
RC4 Drop	Start	Length =1522	Apply to each line	{if(le.document)throw new Error("jQuery requires a window with a doc window:this,function(e,t){"use strict";var n=	ument");return t(e)}:t(e)}{"undefined"!=typeof window?			
Drop bytes	0		2	[],r=e.document,i=Object.getPrototypeOf,o=n.slice,a=n.concat,s=n.pus {},c=1.toString,f=1.hasOumProperty,p=f.toString,d=p.call(Object),h=(	h,u=n.indexOf,l= ),g=function e(t){return"function"==typeof			
A1226 Cipher Encode	Drop bytes		0 11	<pre>t&amp;&amp;"number" =typeof t.nodeType},y=function e(t){return null =t&amp;&amp;t=== m(e,t,n){var i,o=(t=t  r).createElement("script");if(o.text=e,n)for(</pre>	<pre>t.window},v={type: 0,src: 0,noModule: 0};function i in v)n[i]&amp;&amp;</pre>			
Favourites 📩	Start Ø	Length 84	Apply to each line	<pre>(o[i]=n[i]);t.head.appendChild(o).parentNode.removeChild(o))function e  "function"==typeof e?l[c.call(e)] "object":typeof e}var b="3.3.1</pre>	<pre>x(e){return null==e?e+"":"object"==typeof ",w=function(e,t){return new</pre>			
Data format			0.0	<pre>w.fn.init(e,t)},T=/^[\s\uFEFF\x40]+ [\s\uFEFF\x40]+\$/g;w.fn-w.protot {jquery:"3.3.1",constructor:w,length:0,toArray:function(){return o.c</pre>	<pre>ype- all(this)},get:function(e){return null==e?</pre>			
Encryption / Encoding	Drop bytes		0 "	<pre>o.call(this):e&lt;8?this[e+this.length]:this[e]},pushStack:function(e){ t.prev0bject=this,t},each:function(e){return w.each(this,e)},map:fun</pre>	var t=w.merge(this.constructor(),e);return action(e){return			
Public Key	Ð	3931	Apply to each line	<pre>this.pushStack(w.map(this,function(t,n)(return e.call(t,n,t)))),sli this.pushStack(o.apply(this,arguments))),first:function(){return thi</pre>	ce:function(){return s.eq(0)},last:function(){return			
Arithmetic / Logic	From Base64		⊘ 11	<pre>this.eq(-1)},eq:function(e){var t=this.length,n=+e+{e&lt;0?t:0};return this.pushStack(n&gt;=0&amp;&amp;nct?[this[n]]:[])},end:function() {return this.prevObject  this.constructor()},push:s,sort:n.sort,splice:n.splice},w.extend=w.fn.extend=function(){var</pre>				
Networking	Alphabet			<pre>e,t,n,r,i,o,a=arguments[0]  {},s=1,u=arguments.length,l=!1;for("boolean"=typeof a&amp;&amp;(l=a,a=arguments[s]   {},s++),"object"==typeof a  g(a)  (a=(}),s==u&amp;a(a=this,s==);s<u;s++)if(null=(e=arguments[s]))for(t e)n="a[t],a!==&lt;/pre" in=""></u;s++)if(null=(e=arguments[s]))for(t></pre>				
Language	A-Za-z0-9			(r=e[t])88(188r88(w.1sPlainObject(r)))((1=array.1sarray(r)))/(1?(1=:1,0=n86array.1sarray(n)?n:[]):0=n86w.1sPlainObject start: 101 time: 205				
Utils	Remove non-alphabet	chars		56 61 7a 1e 16 8f 8c 9d 73 8b 2f 8b 4a 21 79 1e 63 a3 43 bb 31 25 3d	ar 7d e9 5d 49 8b 79 f2 c7 ae 56 13 9e bc 55 25 b8 e3			
Date / Time	XOR		0 11	d3 10 36 90 b0 25 7a 5b 42 28 e0 80 1a 78 6b 44 8f f6 19 37 8a c9 73				
Extractors	Key		LIEV -					
Compression	b7 85 71 17		HEA *					
Hashing	Standard	Null preservin	g					
Code tidy	Drop bytes		0 11					
Forensics	Start	Length	_					
Multimedia	0	4	Apply to each line					
Other	To Hex		⊘ 11					
Flow control	STEP	💆 BAKE!	Auto Bake					

# Figure 12: fully transformed data

What we end up with, is the encrypted data that contains the C2 commands to be executed by the beacon. This is the result of deobfuscating the data by following the malleable C2 data transform. Now we can proceed with the decryption using a process memory dump, just like we did in <u>part 3</u>.



Figure 13: extracting the cryptographic keys from process memory Tool <u>cs-extract-key.py</u> is used to extract the AES and HMAC key from process memory: it fails, it is not able to find the keys in process memory.

One possible explanation that the keys can not be found, is that process memory is encoded. Cobalt Strike supports a feature for beacons, called a sleep mask. When this feature is enabled, the process memory with data of a beacon (including the keys) is XOR-encoded while a beacon sleeps. Thus only when a beacon is active (communicating or executing commands) will its data be in cleartext.

We can try to decode this process memory dump. Tool <u>cs-analyze-processdump.py</u> is a tool that tries to decode a process memory dump of a beacon that has an active sleep mask feature. Let's run it on our process memory dump:

@NVISO_Labs - cs-analyze-processdump.py rundll32.exe_211103_141122.dmp	_	×
		^
@NVISO_Labs_C:\Demo>cs-analyze-processdump.py_rundll32.exe_211103_141122.dmp		
Hile: rundli32.exe_211103_141122.dmp		
Error: Would read over segment boundaries!		
Error: Would read over segment boundaries!		
Error: Would read over segment boundaries!		
Error: Would read over segment boundaries!		
Error: Would read over segment boundaries!		
Error: Would read over segment boundaries!		
Error: would read over segment boundaries!		
Error: Would read over segment boundaries:		
Error: Would read over segment boundaries!		
Error: Would read over segment boundaries:		
Error: Would read over segment boundaries:		
Error, Would read over segment boundaries:		
Error, Would read over segment boundaries:		
Error, Would read over segment boundaries:		
Error, Would read over segment boundaries:		
Error, Would read over segment boundaries:		
Error: Would read over segment boundaries:		
Error: Would read over segment boundaries:		
Error: Would read over segment boundaries!		
Erron, Would read over segment boundaries. France, Memory snare		
Segment 2576000 size 44000		
Potential keys = 49421		
Probable keys:		
0 3001 h'\xr7\xa518\xh5(.\xd9\xf2\xa50\xe80' h'c7a56a38h5282ed9f2a56fe86f' 82.000000		
Trving probable key 0:		
		~

Figure 14: analyzing the process memory dump (screenshot 1)



Figure 15: analyzing the process memory dump (screenshot 2)

The tool has indeed found a 13-byte long XOR key, and written the decoded section to disk as a file with extension .bin.

This file can now be used with cs-extract-key.py, it's exactly the same command as before, but with the decoded section in stead of the encoded .dmp file:



Figure 16: extracting keys from the decoded section And now we have recovered the cryptographic keys.

Notice that in figure 16, the tool reports finding string sha256\x00, while in the first command (figure 13), this string is not found. The absence of this string is often a good indicator that the beacon uses a sleep mask, and that tool cs-analyze-processdump.py should be used prior to extracting the keys.

Now that we have the keys, we can decrypt the network traffic with tool <u>cs-parse-http-traffic.py</u>:



Figure 17: decrypting the traffic fails

This fails: the reason is the malleable C2 data transform. Tool cs-parse-http-traffic.py needs to know which instructions to apply to deobfuscate the traffic prior to decryption. Just like we did manually with CyberChef, tool cs-parse-http-traffic.py needs to do this automatically. This can be done with option -t.

Notice that the output of tool 1768.py contains a short-hand notation of the instructions to execute (between square brackets):

0x000b Malleable\_C2 Instructions 0x0003 0x0100 Transform Input: [7:Input,4,1:1522,2:84,2:3931,13,15] Print Remove 1522 bytes from end Remove 84 bytes from begin Remove 3931 bytes from begin BASE64 URL XOR with 4-byte random key 0x000c http\_get\_header 0x0003 0x0200 Const header Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 Const\_header Referer: http://code.jquery.com/ Const\_header Accept-Encoding: gzin. deflate Build Metadata: [7:Metadata,13,2:\_\_cfduid=,6:Cookie] BASE64 URL Prepend \_\_cfduid= Header Cookie 0x0003 0x0200 0x000d http\_post\_header Const\_header Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 Const\_header Referer: http://code.jquery.com/ Const\_header Accent\_Encoding: grin\_deflate Build SessionId: [7:SessionId,15,13,5:\_\_cfduid] XOR with 4-byte handom key BASE64 URL Parameter cfduid Build Output: [7:Output,15,13,4] XOR with 4-byte random key BASE64 URL Print

Figure 18: short-hand notations of malleable C2 instructions For the tasks to be executed (input), it is:

7:Input,4,1:1522,2:84,2:3931,13,15

And for the results to be posted (output), it is:

7:Output, 15, 13, 4

These instructions can be put together (using a semicolon as separator) and fed via option -t to tool cs-parse-http-traffic.py:

@NVISO_Labs	_		×	١
@NVISO_Labs C:\Demo>cs-parse-http-traffic.py -t 7:Input,4,1:1522,2:84,2:3931,13,15;7:Output,15,13,4 -k dbe32 9b67e52a5bad695:eeee0d3b24b0cc2c969b9483ccf66404 capture.pcapng Packet number: 45 HTTP response (for request 33 GET) Length raw data: 5628 Timestamp: 1635945079 20211103-131119 Data size: 29 Command: 6 DATA_JITTER Length random data = 21	22c2ee	ad03f	16	
Packet number: 88 HTTP response (for request 80 GET) Length raw data: 5692 Timestamp: 1635945085 20211103-131125 Data size: 74 Command: 6 DATA_JITTER Length random data = 66				
Packet number: 119 HTTP response (for request 111 GET) Length raw data: 5628 Timestamp: 1635945090 20211103-131130 Data size: 39 Command: 6 DATA_JITTER Length random data = 31				
Commands summary: 6 DATA_JITTER: 3 @NVISO_Labs C:\Demo>				

# Figure 19: decrypted traffic

And now we finally obtain decrypted traffic. There are no actual commands here in this traffic, just "data jitter": that is random data of random length, designed to even more obfuscate traffic.

# Conclusion

We saw how malleable C2 data transforms are used to obfuscate network traffic, and how we can deobfuscate this network traffic by following the instructions.

We did this manually with CyberChef, but that is of course not practical (we did this to illustrate the concept). To obtain the decoded, encrypted commands, we can also use cs-parse-http-traffic.py. Just like we did in <u>part 3</u>, where we started with an unknown key, we do this here too. The only difference, is that we also need to provide the decoding instructions:



Figure 20: extracting and decoding the encrypted data And then we can take one of these 3 encrypted data, to recover the keys.

Thus the procedure is exactly the same as explained in <u>part 3</u>, except that option -t must be used to include the malleable C2 data transforms.

# About the authors

Didier Stevens is a malware expert working for NVISO. Didier is a SANS Internet Storm Center senior handler and Microsoft MVP, and has developed numerous popular tools to assist with malware analysis. You can find Didier on <u>Twitter</u> and <u>LinkedIn</u>.

You can follow NVISO Labs on <u>Twitter</u> to stay up to date on all our future research and publications.