Excel 4.0 Makro (XLM) Analizi

written by Mert SARICA | 1 June 2021
If you are looking for an English version of this article, please visit here.

2017 yılında başlayan DDE tabanlı oltalama saldırıları, 2020 yılı itibariyle yerini Excel 4.0 Makro (XLM) oltalama saldırılarına bıraktı. Ufak bir araştırma yaptığınızda XLM makrolarının hayatımıza girişinin 1992 yılında Microsoft Excel 4.0'ın yayınlanması ile olduğunu görebilirsiniz. Tehdit aktörleri tarafından sıklıkla kötüye kullanılan VBA makroları ise Excel 5.0 ile duyurulması ile hayatımıza girmiş ve günümüzde de en güncel Microsoft Office sürümünde hala desteklenmektedir.

Yanlış anımsamıyorsam XLM makroları ile ilgili ofansif güvenlik üzerine okuduğum ilk teknik makale Outflank firmasına ait bu blog yazısıydı. XLM makrolarını VBA makroları gibi tespit edip, analiz etmenin pek de kolay olmadığı XLM makrolarına yönelik yapılan güvenlik araştırmaları ile ortaya çıkmaya başladıktan sonra her zaman olduğu gibi ofansif güvenlik uzmanlarının yanı sıra tehdit aktörlerinin de dikkatini çekmeye başladı. Aradan çok zaman geçmeden de kurumlar XLM makro içeren oltalama saldırıları ile karşılaşmaya başladılar.

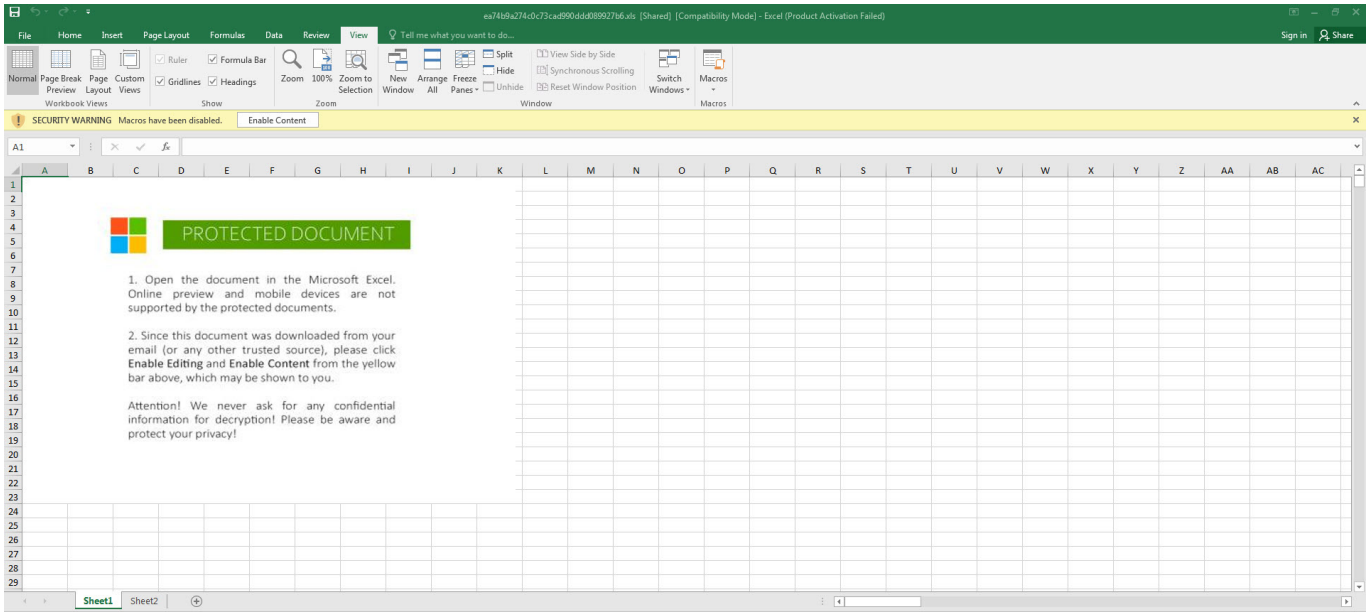
XLM makro içeren bir Office dosyasını analiz etmenin zorluğu, Microsoft Office Makro Analizi başlıklı blog yazımda belirttiğimin aksine Office'nin arayüzünden kolaylıkla görüntülenememesinden (view macro) kaynaklanmaktadır. Durum böyle olunca da zararlı XLM makro içeren Office dosyalarının tecrübesiz siber güvenlik uzmanlarının dikkatinden kaçma ihtimali ("Bu Office dosyası bozuk", "Makro içermiyor" gibi) artmaktadır. Ben de hem siber güvenlik analisletlerine XLM makro içeren Microsoft Office dosyalarının nasıl analiz edilebileceğini göstermek hem de XLM makro içeren Microsoft Office dosyalarına karşı farkındalık yaratmak adına gerçek bir olaydan yola çıkarak bir blog yazısı yazmaya karar verdim.

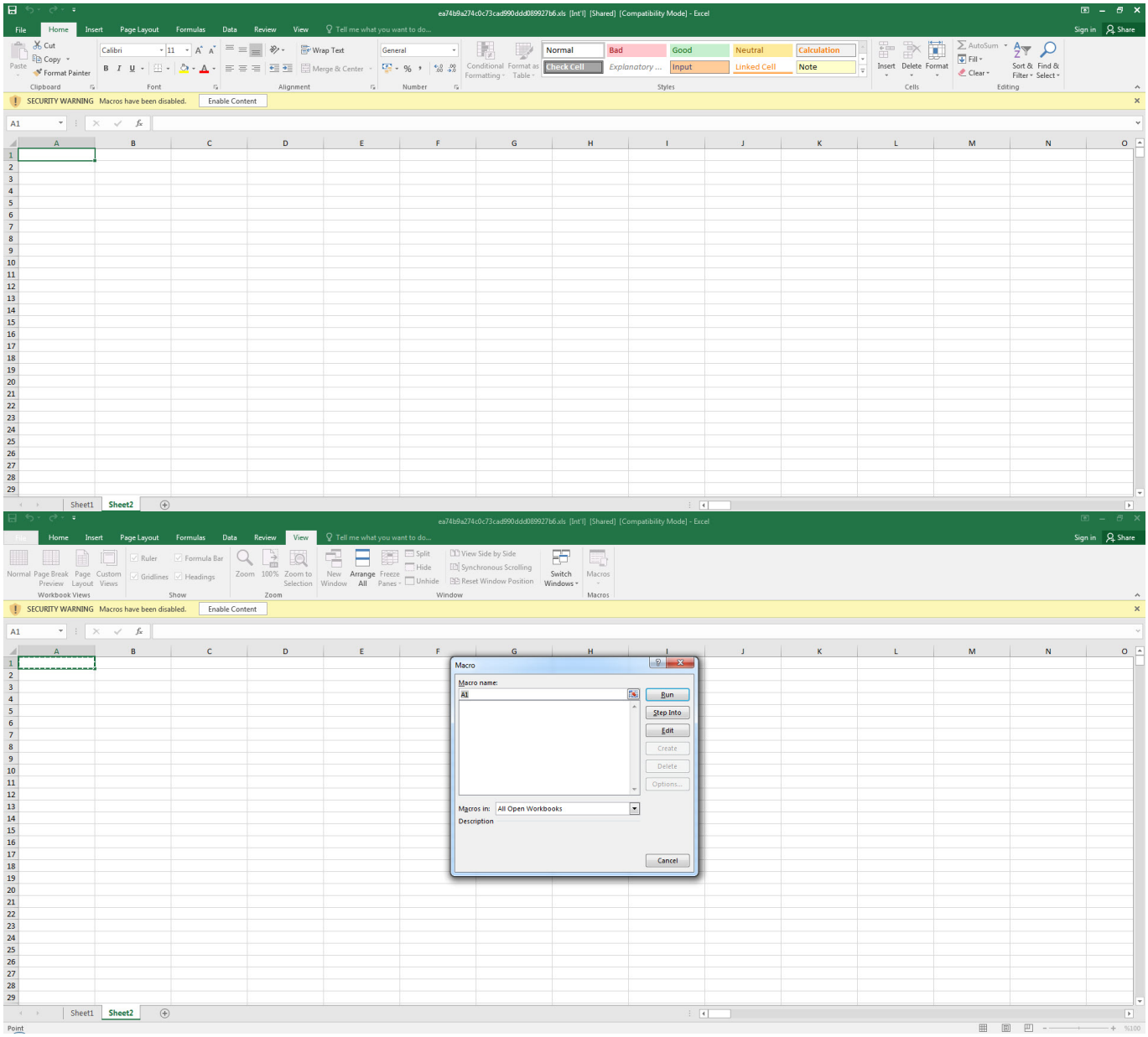
2020 yılının Mayıs ayında çok sayıda SMTP ip adresinden gönderilen ve gönderici adresi @wp.pl uzantılı olan yüzlerce e-posta için güvenlik sistemlerinde engellendiğine dair alarmlar üremeye başladı. E-postalar incelendiğinde eklerinde rastgele isimle oluşturulmuş XLS uzantılı Excel dosyaları bulunuyordu. Bu gibi durumlarda siber güvenlik analistlerinin

yapması gereken en önemli adımlardan biri zararlı doküman içinde yer alan komuta kontrol merkezine ait adreslerini tespit etmek, web trafiği kayıtlarında aramak ve kurum genelinde erişimi engellemektedir.

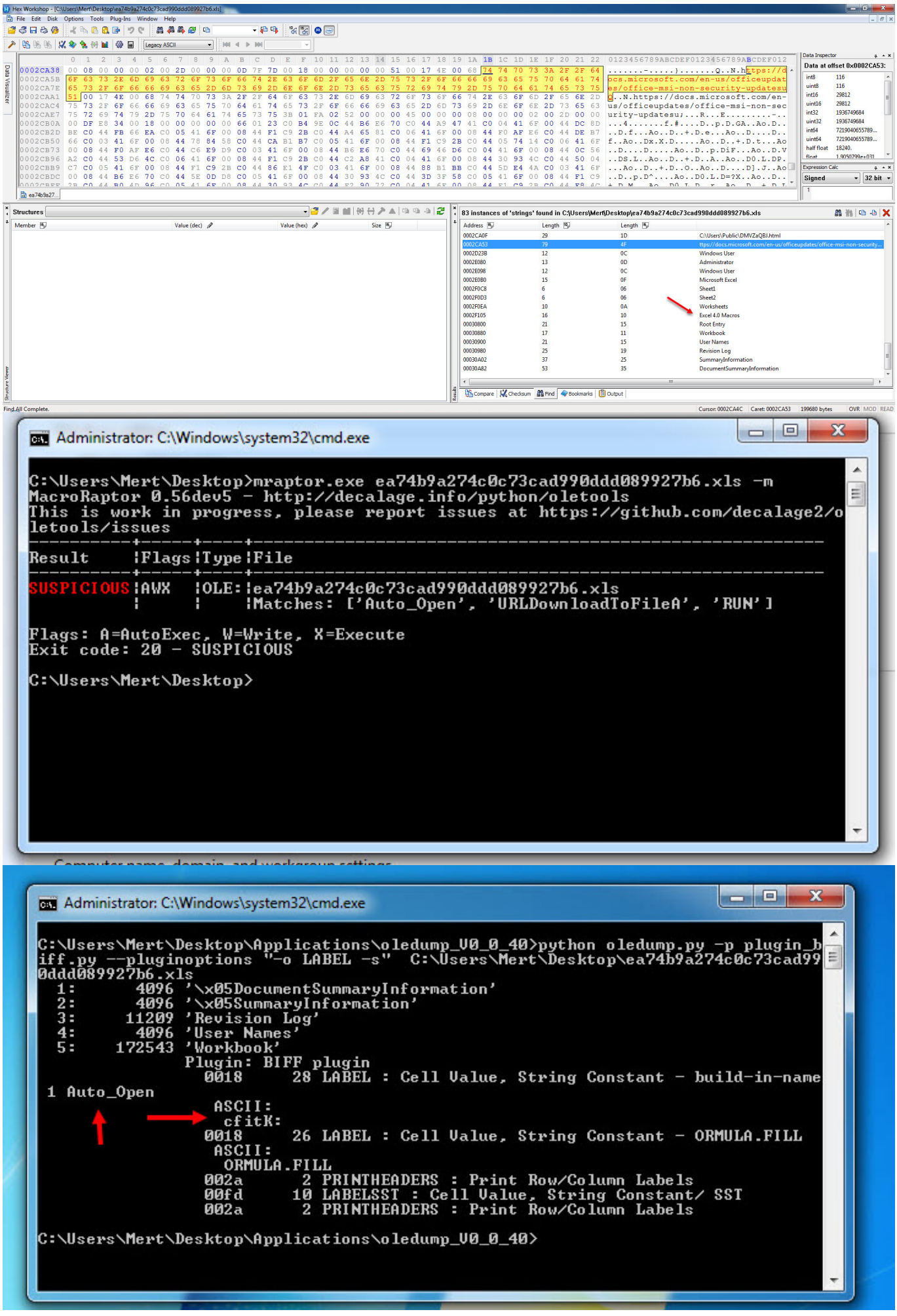
Tabii mevzu bahis XLM makro içeren Office dosyası olduğunda statik ve dinamik analiz yapan kum havuzu (sandbox) sistemlerinin anti kum havuzu yöntemleri karşısında yetersiz kaldığı durumlar söz konusu (Örnek: Kum Havuzu Tespiti) olabilmektedir. Alarma konu olan zararlı Excel dosyası da tam da bu şekilde kum havuzunda çalıştığını anlamaya yönelik kontroller gerçekleştirdiği için komuta kontrol merkezinin adresi bu analizler (VirusTotal, Hybrid-Analysis) esnasında ortaya çıkmamaktadır. Bu durumda siber güvenlik analistinin yapması gereken iş bu zararlı Excel dosyasını alıp zararlı yazılımı analizi amacıyla oluşturduğu sanal sistemine kopyalamak ve orada analiz etmek olmalıdır.

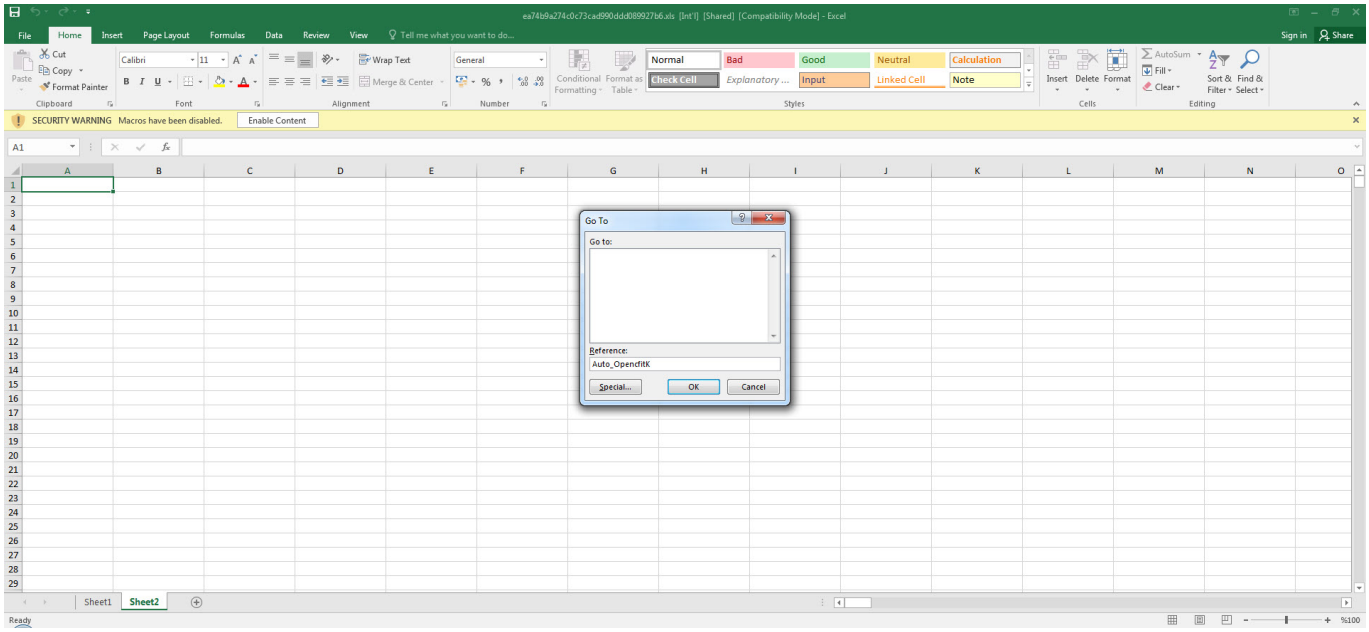
Excel dosyasını sanal sistemde çalıştırdığımızda karşımıza iki tane sayfa (Sheet1 & Sheet2) çıkmaktadır. Birinci sayfada kötü emellerini gerçekleştirebilmek için makroyu aktif hale getirmemiz gerektiğini belirten sahte bir resim/mesaj, ikinci sayfada ise bomboş hücreler (aslında boş değil :)) karşımıza çıkmaktadır. Her ne kadar Excel bize bu dosyada makro olduğuna dair uyarı verse de dosyada yer alan makroyu görüntülediğimizde içinin boş olduğu görünmektedir.



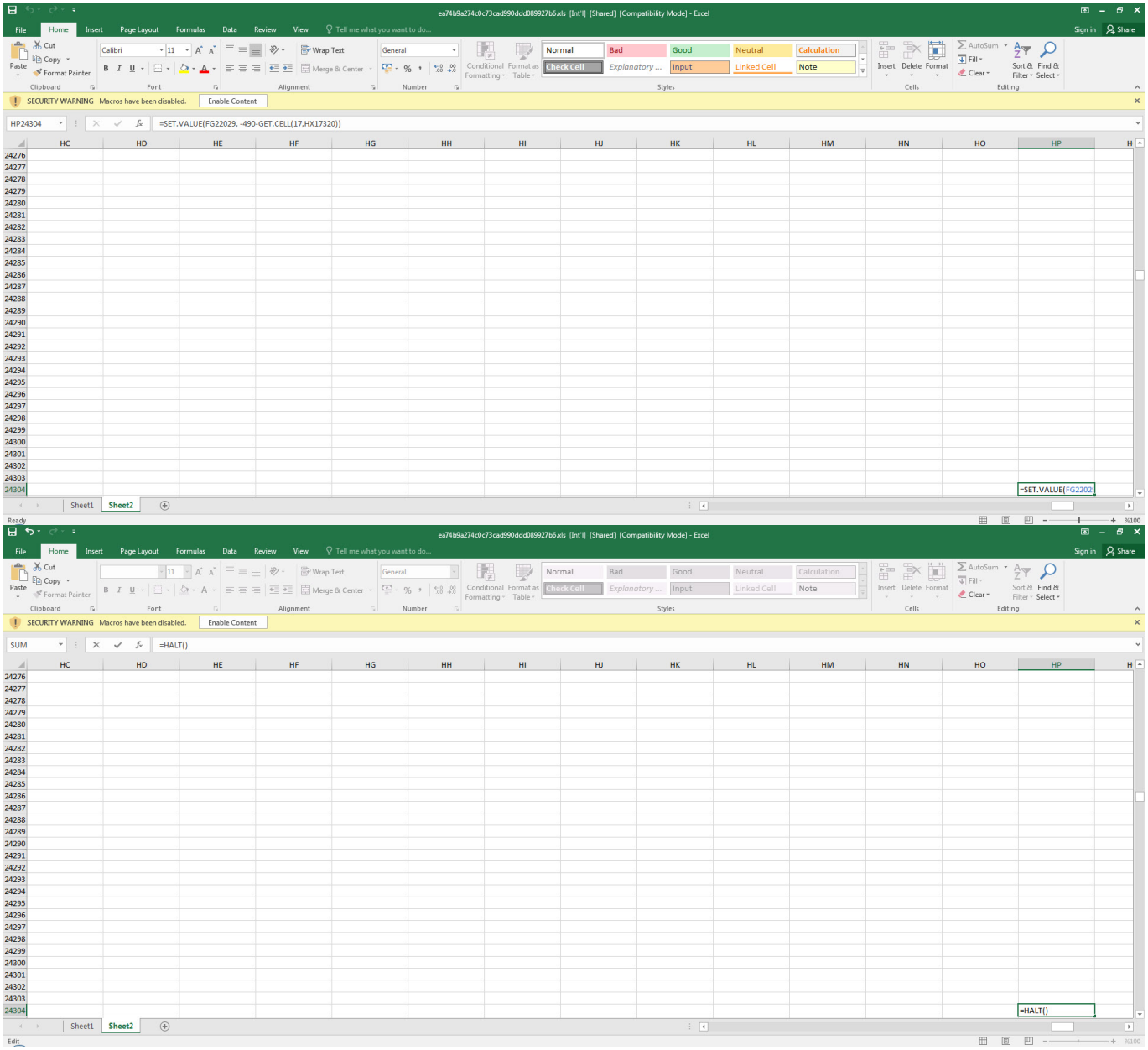


Dosyayı herhangi bir hex editörü ile açıp içinde yer alan karakter dizilerine (strings) baktığımızda Excel 4.0 Macros dizisinden şüphe ettiğimiz gibi bunun XLM makrosu içerdiğini görebiliyoruz. Dosyanın içinde makro olduğundan emin olmak için dosyayı mraptor aracı ile analiz ettiğimizde dosyada makro olduğu ve otomatik olarak çalışabilmesi adına Auto_Open isminde (VBA makrosundaki AutoOpen() fonksiyonu gibi) bir hücreye (cell) sahip olduğu anlaşılıyordu. Bu hücrenin adını öğrenip görüntülemek ve analiz etmek için ise Didier STEVENS'ın oledump aracından faydalanarak (oledump.py -p plugin_biff.py –pluginoptions "-o LABEL -s" C:\Users\Mert\Desktop\ea74b9a274c0c73cad990ddd089927b6.xls) ilk çalıştırılan hücrenin Auto_OpencfitK adına sahip olduğunu gördüm. Analistin Excel üzerinden Go To (CTRL-G) ile Auto_Open ismine sahip hücreye giderek analize başlayacağını bilen zararlı kod geliştiricisi akıllılık yaparak adını bu hücrenin adını Auto_OpencfitK olarak değiştirmiştir.


Hex Workshop - [C:\Users\Mert\Desktop\ea74b9a274c0c73cad990ddd089927b6.xls]
Structures
83 instances of 'strings' found in C:\Users\Mert\Desktop\ea74b9a274c0c73cad990ddd089927b6.xls
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop>mraptor.exe ea74b9a274c0c73cad990ddd089927b6.xls -m
MacroRaptor 0.56dev5 - http://decalage.info/python/oletools
This is work in progress, please report issues at https://github.com/decalage2/oletools/issues
Result | Flags | Type | File
SUSPICIOUS | AWX | OLE: | ea74b9a274c0c73cad990ddd089927b6.xls
Matches: ['Auto_Open', 'URLDownloadToFileA', 'RUN']
Flags: A=AutoExec, W=Write, X=Execute
Exit code: 20 - SUSPICIOUS
C:\Users\Mert\Desktop>
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop\Applications\oledump_V0_0_40>python oledump.py -p plugin_biff.py --pluginoptions "-o LABEL -s" C:\Users\Mert\Desktop\ea74b9a274c0c73cad990ddd089927b6.xls
1: 4096 '\x05DocumentSummaryInformation'
2: 4096 '\x05SummaryInformation'
3: 11209 'Revision Log'
4: 4096 'User Names'
5: 172543 'Workbook'
Plugin: BIFF plugin
0018 28 LABEL : Cell Value, String Constant - build-in-name
1 Auto_Open
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_V0_0_40>

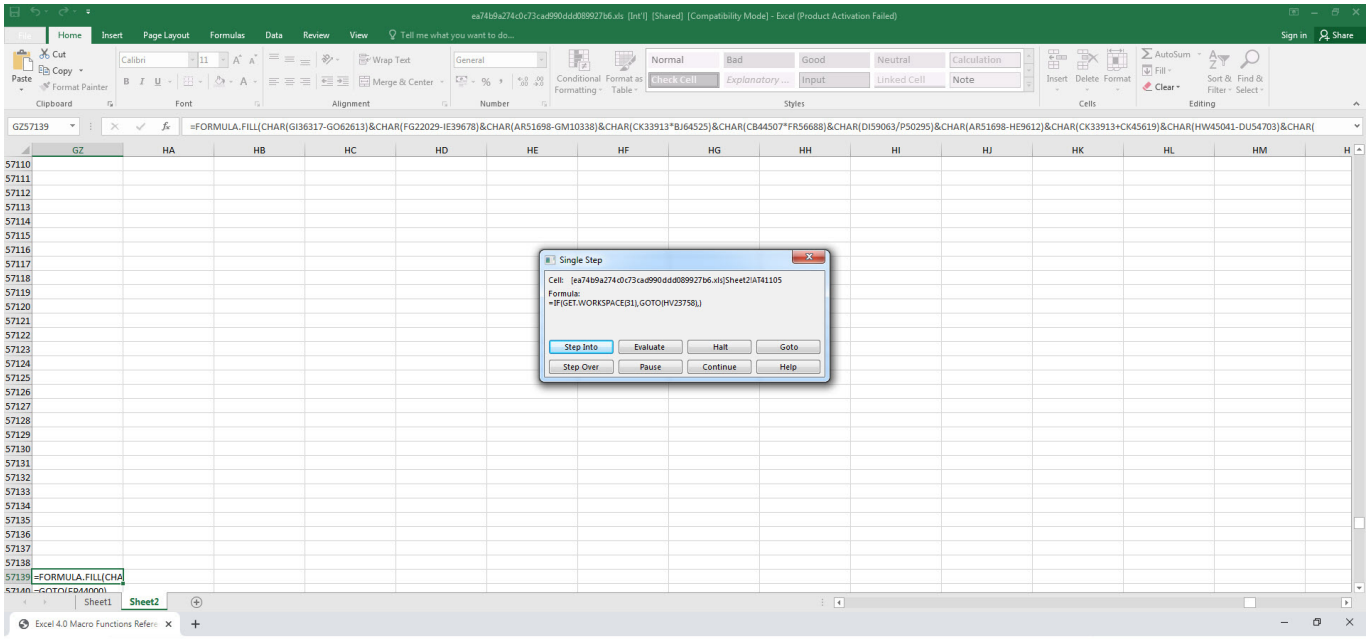


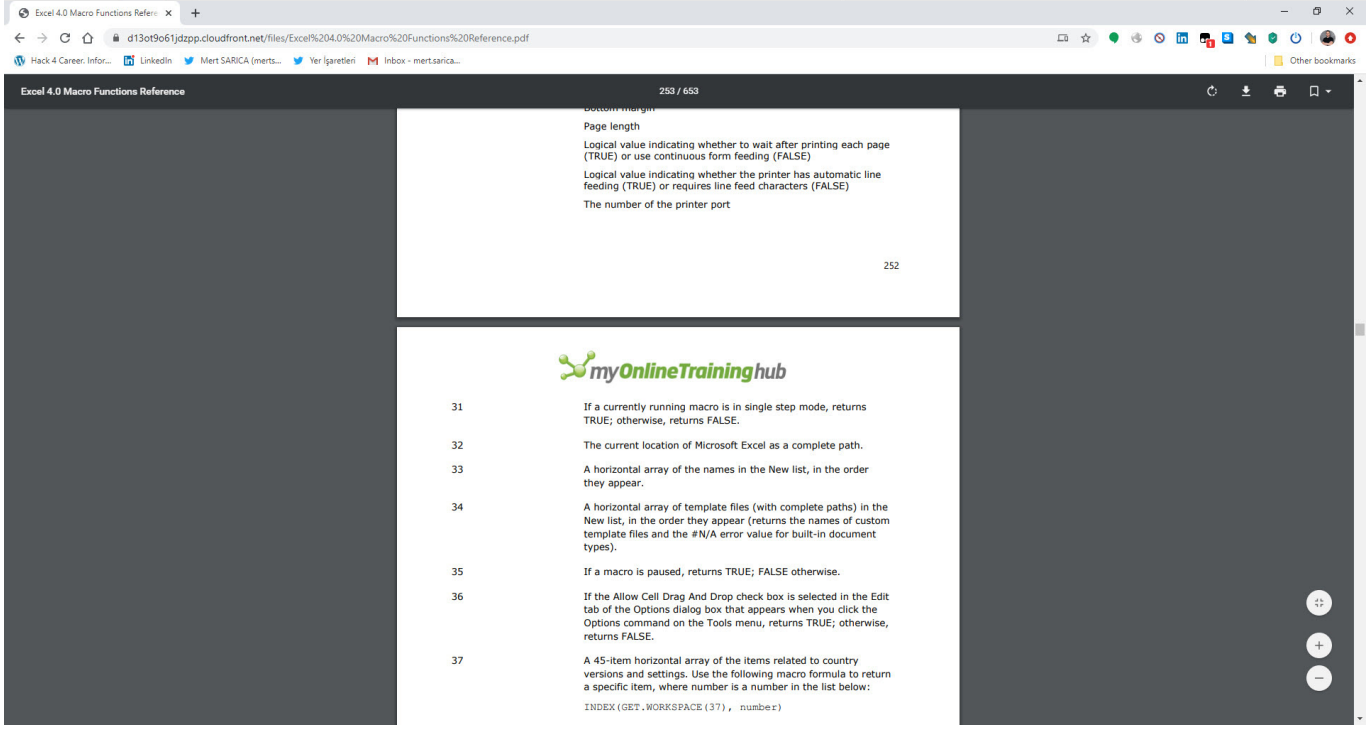
Başlangıç hücresine gittikten ve dosya genelinde 42 tane FORMULA ifadesi ve CHAR fonksiyonundan oluşan gizlenmiş (obfuscated) bir makro olduğunu öğrendikten sonra her birini teker teker çözmek ve analiz etmek bir hayli zaman alacağı için hata ayıklaması (debugging) ile ilerlemeye karar verdim. Auto_OpencfitK hücresine gidip ALT + F8 kısa yoluna bastıktan sonra Step Into butonuna bastığımda haliylen Excel beni devam etmek için makro çalıştırmaya izin vermemi ve ardından dosyayı kapatıp açmamı istedi. Dosyayı açar açmaz Excel hızlıca Auto_OpencfitK hücresinden ilerleyeceği için bu adımı kaçırmamak için bu hücrede yer alan =SET.VALUE(FG22029, -490-GET.CELL(17,HX17320)) formülünü =HALT() ile değiştirerek makronun sonlanmasını sağladım. Ardından =HALT() formülünü =SET.VALUE(FG22029, -490-GET.CELL(17,HX17320)) ile değiştirip bu hücre üzerinde ALT + F8 kısa yoluna bastığımda sorunsuz bir şekilde ilk hücreden makroyu dinamik olarak analiz etmeye başlayabildim.

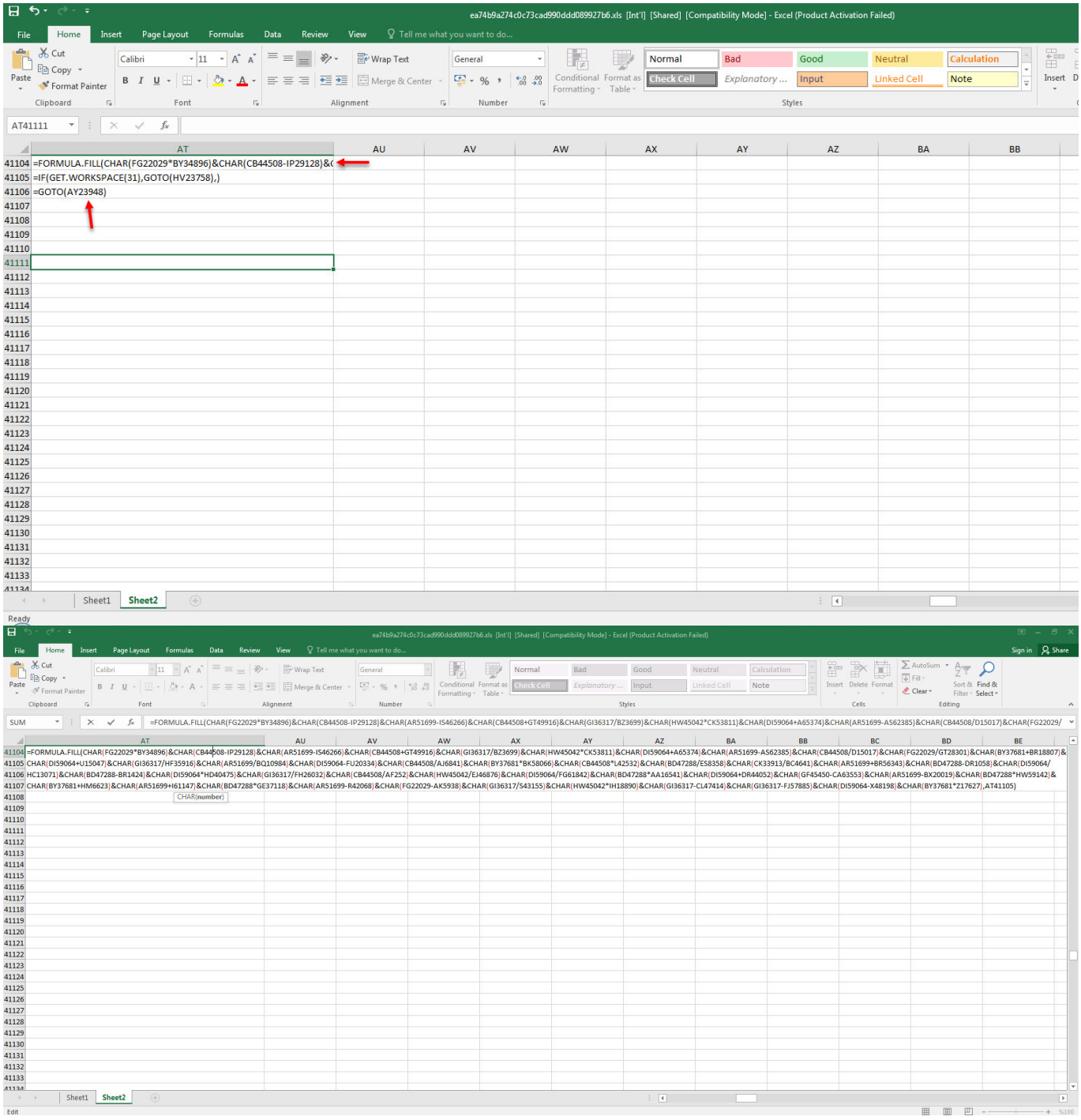


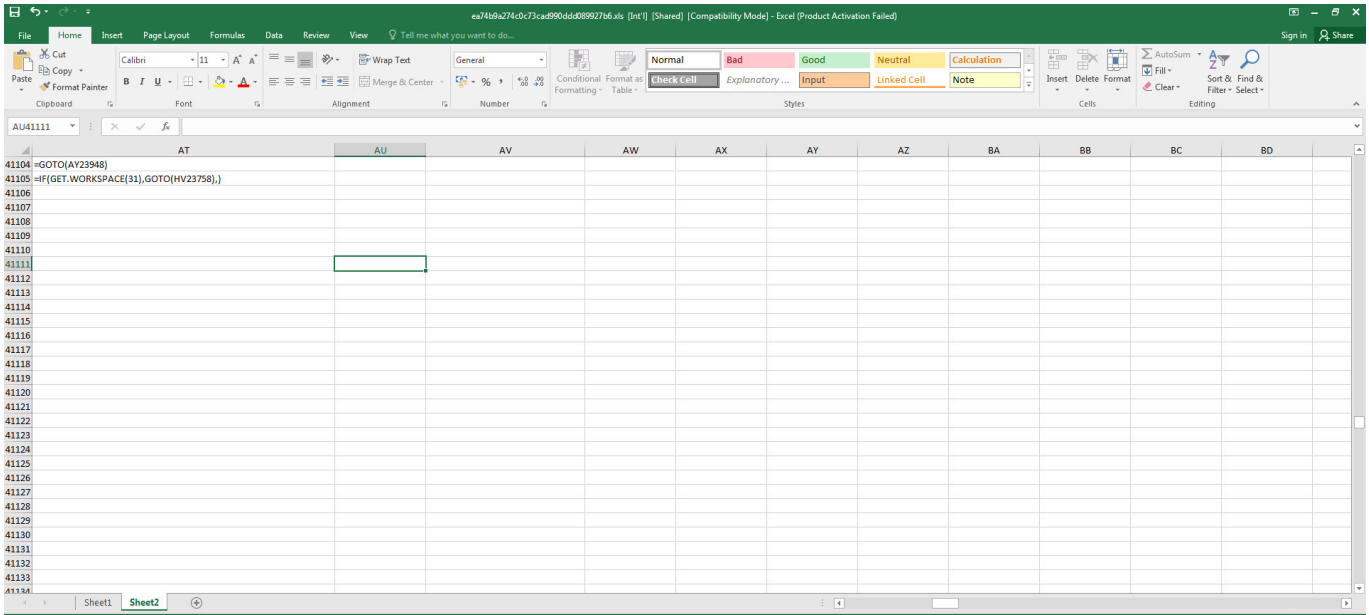
Step Into ve Evaluate butonlarından faydalanarak gizlenmiş hücrelerin çözülmesi ile analize devam ettikçe Excel 4.0 Macro Functions Reference belgesinden faydalanarak makronun hata ayıklamaya ve kum havuzuna karşı çeşitli kontroller gerçekleştirdiğini gördüm. Hata ayıklama kontrolü yapan AT41104 hücresine geldiğimde bu kontrolü atlatmak için hata ayıklama tespit edilememesi durumunda devam ettiği hücredeki =GOTO(AY23948) değerini AT41104 hücresine kopyaladım.

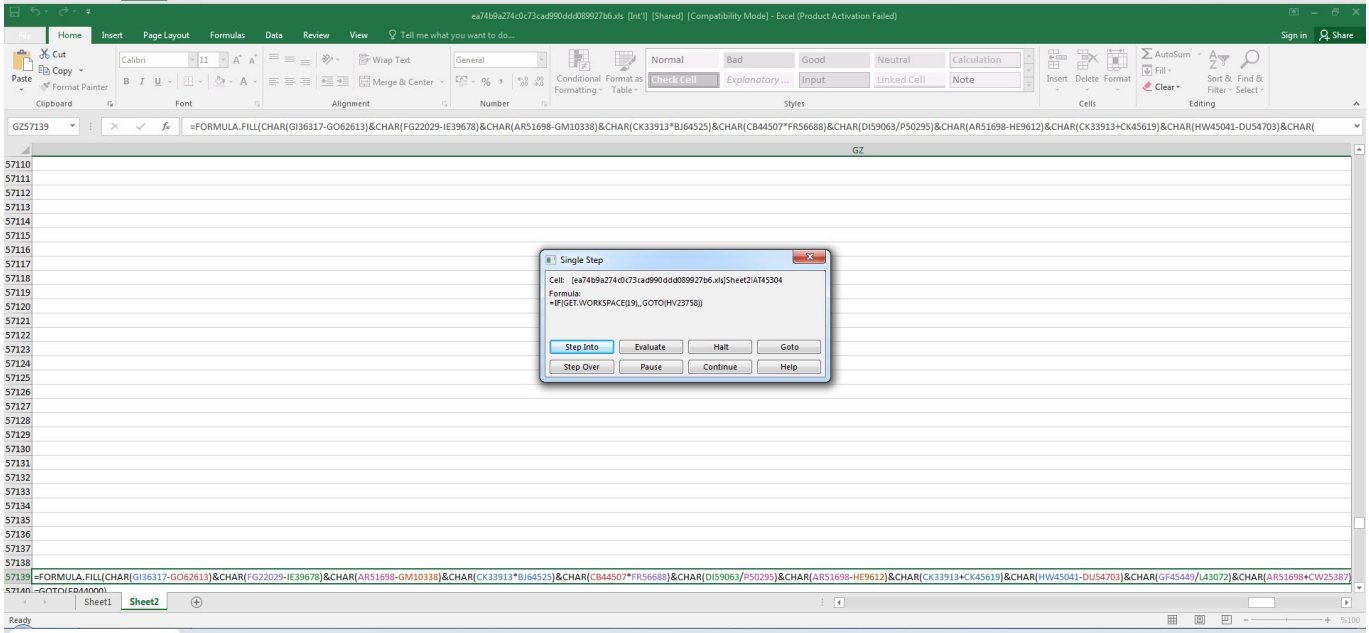
=IF(GET.WORKSPACE(31),GOTO(HV23758),) Makro hata ayıklama modunda mı ? (Anti-debugging)
=IF(GET.WORKSPACE(19),,GOTO(HV23758),) Sistemde fare var mı ? (Anti-sandbox)
=IF(GET.WORKSPACE(42),,GOTO(HV23758),) Ses dosyası çalınabiliyor mu ? (Anti-sandbox)

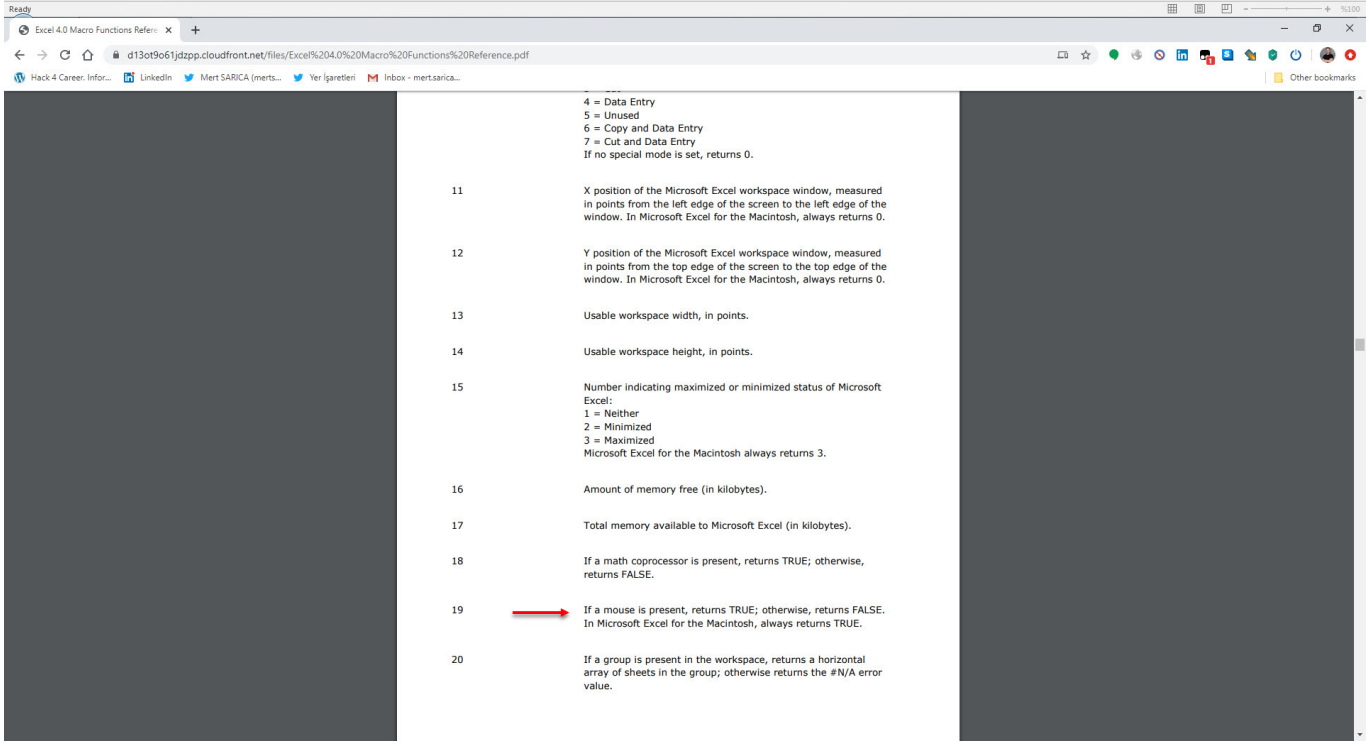

ea74b9a274c0c73cad990ddd089927b6.xls [Int'l] [Shared] [Compatibility Mode] - Excel (Product Activation Failed)
Home
Insert
Page Layout
Formulas
Data
Review
View
Tell me what you want to do...
Sign in
Share
Paste
Cut
Copy
Format Painter
Clipboard
Calibri
11
Font
Wrap Text
Merge & Center
Alignment
General
Number
Conditional Formatting
Format as Table
Normal
Bad
Good
Neutral
Calculation
Check Cell
Explanatory ...
Input
Linked Cell
Note
Styles
Insert
Delete
Format
Cells
AutoSum
Fill
Clear
Sort & Filter
Find & Select
Editing
GZ57139
=FORMULA.FILL(CHAR(GI36317-GO62613)&CHAR(FG22029-IE39678)&CHAR(AR51698-GM10338)&CHAR(CK33913*BJ64525)&CHAR(CB44507*FR56688)&CHAR(DI59063/P50295)&CHAR(AR51698-HE9612)&CHAR(CK33913+CK45619)&CHAR(HW45041-DU54703)&CHAR(
GZ
HA
HB
HC
HD
HE
HF
HG
HH
HI
HJ
HK
HL
HM
57139 =FORMULA.FILL(CHA
57140 =GOTO(ERA4000)
Sheet1
Sheet2
Single Step
Cell: [ea74b9a274c0c73cad990ddd089927b6.xls]Sheet2!AT41105
Formula:
=IF(GET.WORKSPACE(31),GOTO(HV23758),)
Step Into
Evaluate
Halt
Goto
Step Over
Pause
Continue
Help

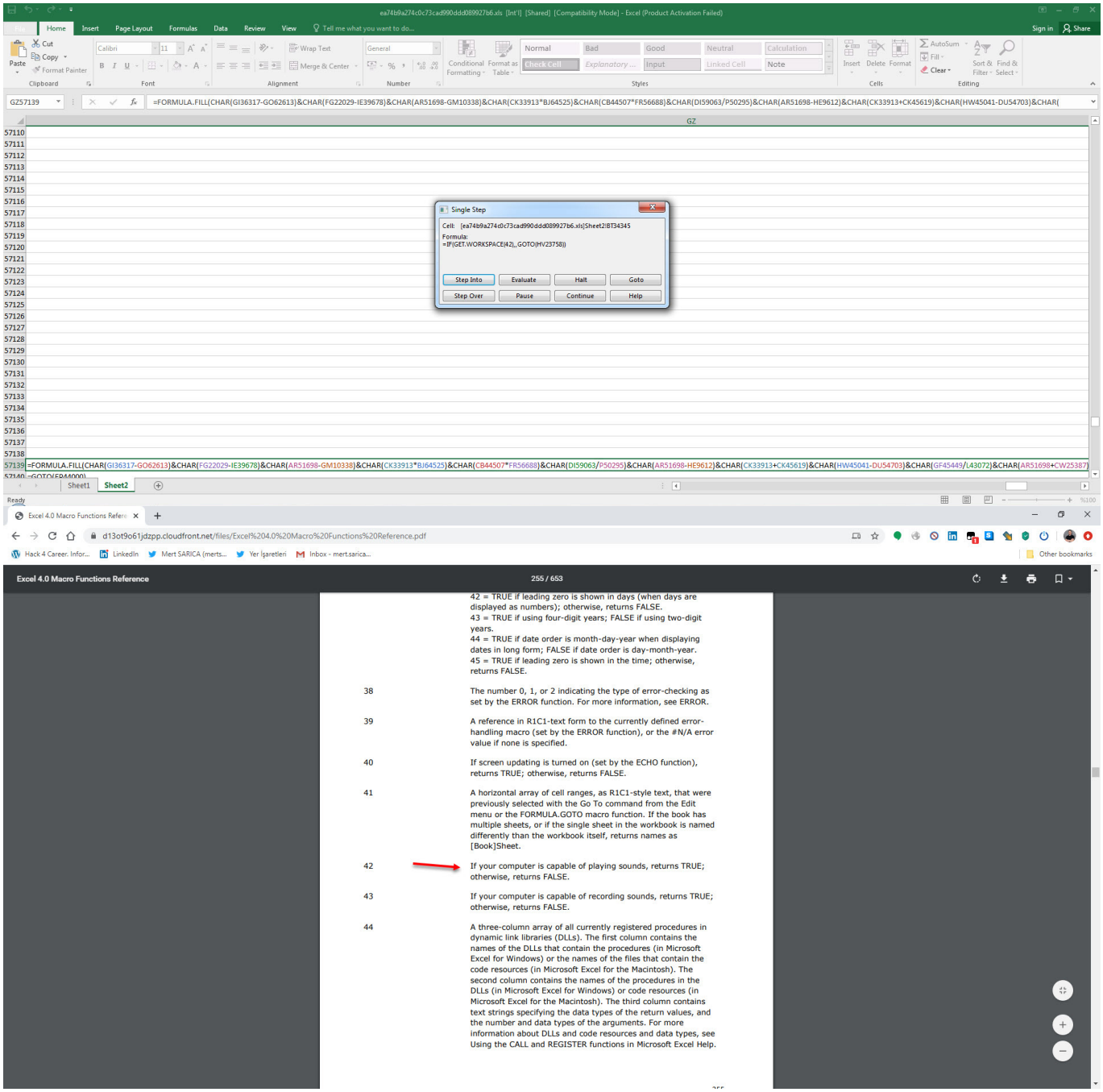

Excel 4.0 Macro Functions Refere
d13ot9o61jdzpp.cloudfront.net/files/Excel%204.0%20Macro%20Functions%20Reference.pdf
Hack 4 Career. Infor...
LinkedIn
Mert SARICA (merts...
Yer işaretleri
Inbox - mert.sarica...
Other bookmarks
Excel 4.0 Macro Functions Reference
253 / 653
Page length
Logical value indicating whether to wait after printing each page (TRUE) or use continuous form feeding (FALSE)
Logical value indicating whether the printer has automatic line feeding (TRUE) or requires line feed characters (FALSE)
The number of the printer port
252
myOnlineTraininghub
31 If a currently running macro is in single step mode, returns TRUE; otherwise, returns FALSE.
32 The current location of Microsoft Excel as a complete path.
33 A horizontal array of the names in the New list, in the order they appear.
34 A horizontal array of template files (with complete paths) in the New list, in the order they appear (returns the names of custom template files and the #N/A error value for built-in document types).
35 If a macro is paused, returns TRUE; FALSE otherwise.
36 If the Allow Cell Drag And Drop check box is selected in the Edit tab of the Options dialog box that appears when you click the Options command on the Tools menu, returns TRUE; otherwise, returns FALSE.
37 A 45-item horizontal array of the items related to country versions and settings. Use the following macro formula to return a specific item, where number is a number in the list below:
INDEX(GET.WORKSPACE(37), number)


ea74b9a274c0c73cad990ddd089927b6.xls [Int'l] [Shared] [Compatibility Mode] - Excel (Product Activation Failed)
AT41111
=FORMULA.FILL(CHAR(FG22029*BY34896)&CHAR(CB44508-IP29128)&(
=IF(GET.WORKSPACE(31),GOTO(HV23758),)
=GOTO(AY23948)
Sheet1
Sheet2
Ready
SUM
=FORMULA.FILL(CHAR(FG22029*BY34896)&CHAR(CB44508-IP29128)&CHAR(AR51699-IS46266)&CHAR(CB44508+GT49916)&CHAR(GI36317/BZ3699)&CHAR(HW45042*CK53811)&CHAR(DI59064+A65374)&CHAR(AR51699-AS62385)&CHAR(CB44508/D15017)&CHAR(FG22029/
CHAR(number)
Edit

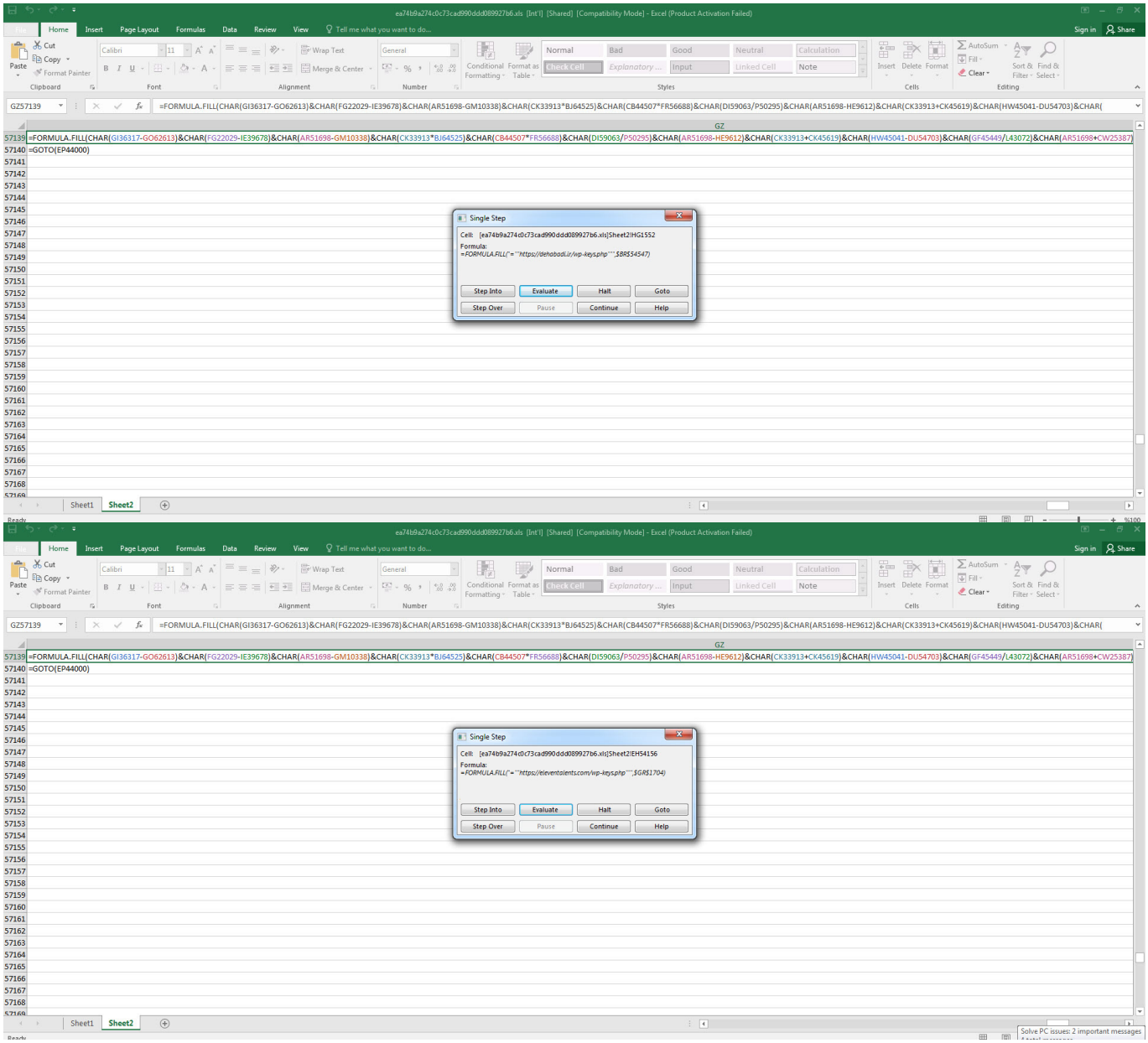

ea74b9a274c0c73cad990ddd089927b6.xls [Int'l] [Shared] [Compatibility Mode] - Excel (Product Activation Failed)
AU41111
AT
AU
AV
AW
AX
AY
AZ
BA
BB
BC
BD
41104 =GOTO(AY23948)
41105 =IF(GET.WORKSPACE(31),GOTO(HV23758),)
Sheet1
Sheet2


ea74b9a274c0c73cad990ddd089927b6.xls [Int'l] [Shared] [Compatibility Mode] - Excel (Product Activation Failed)
GZ57139
=FORMULA.FILL(CHAR(GI36317-GO62613)&CHAR(FG22029-IE39678)&CHAR(AR51698-GM10338)&CHAR(CK33913*BJ64525)&CHAR(CB44507*FR56688)&CHAR(DI59063/P50295)&CHAR(AR51698-HE9612)&CHAR(CK33913+CK45619)&CHAR(HW45041-DU54703)&CHAR(
GZ
Single Step
Cell: [ea74b9a274c0c73cad990ddd089927b6.xls]Sheet2!AT45304
Formula:
=IF(GET.WORKSPACE(19),,GOTO(HV23758))
Step Into
Evaluate
Halt
Goto
Step Over
Pause
Continue
Help
57139 =FORMULA.FILL(CHAR(GI36317-GO62613)&CHAR(FG22029-IE39678)&CHAR(AR51698-GM10338)&CHAR(CK33913*BJ64525)&CHAR(CB44507*FR56688)&CHAR(DI59063/P50295)&CHAR(AR51698-HE9612)&CHAR(CK33913+CK45619)&CHAR(HW45041-DU54703)&CHAR(GF45449/L43072)&CHAR(AR51698+CW25387)
Sheet1
Sheet2
Ready

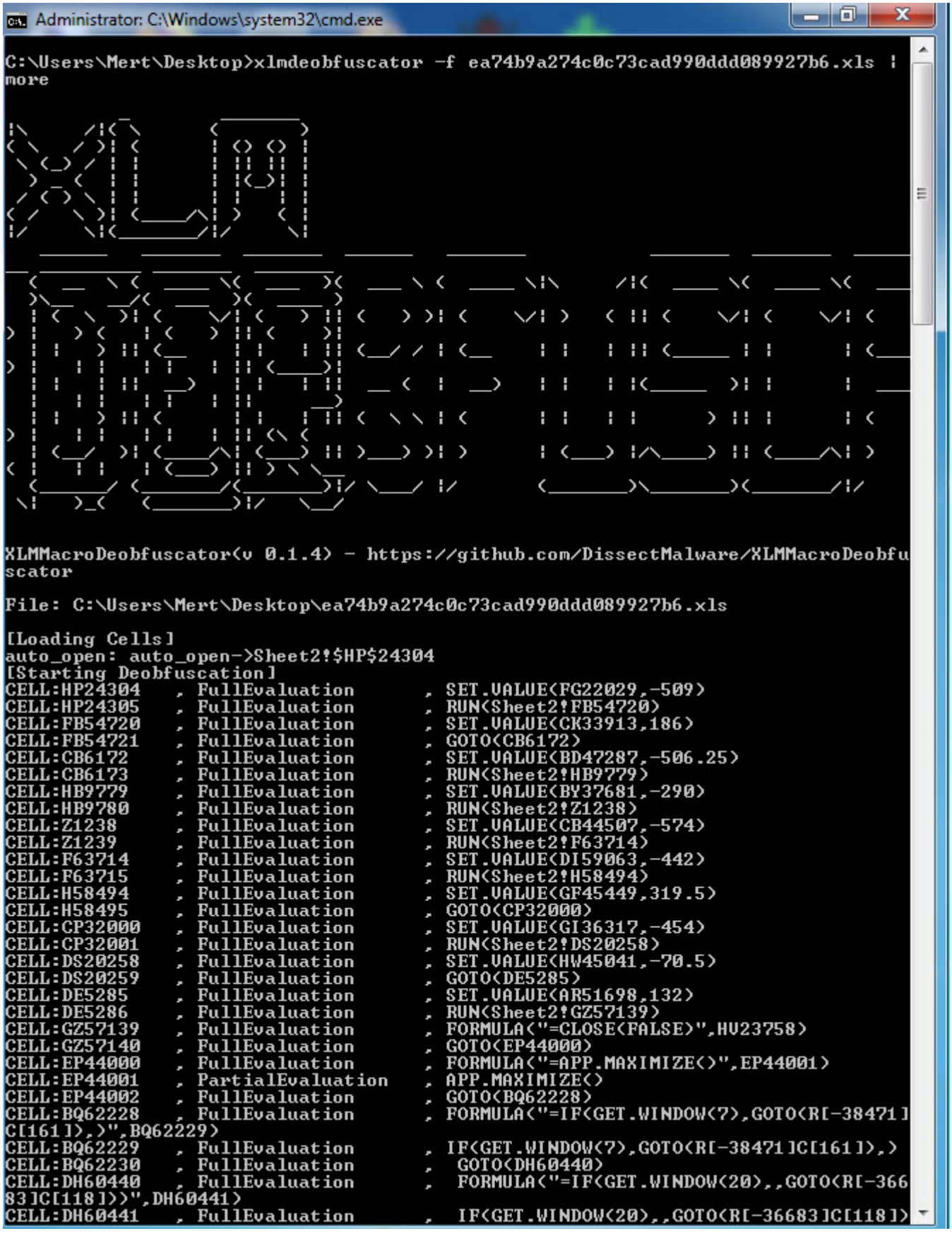

Excel 4.0 Macro Functions Refere
d13ot9o61jdzpp.cloudfront.net/files/Excel%204.0%20Macro%20Functions%20Reference.pdf
4 = Data Entry
5 = Unused
6 = Copy and Data Entry
7 = Cut and Data Entry
If no special mode is set, returns 0.
11 X position of the Microsoft Excel workspace window, measured in points from the left edge of the screen to the left edge of the window. In Microsoft Excel for the Macintosh, always returns 0.
12 Y position of the Microsoft Excel workspace window, measured in points from the top edge of the screen to the top edge of the window. In Microsoft Excel for the Macintosh, always returns 0.
13 Usable workspace width, in points.
14 Usable workspace height, in points.
15 Number indicating maximized or minimized status of Microsoft Excel:
1 = Neither
2 = Minimized
3 = Maximized
Microsoft Excel for the Macintosh always returns 3.
16 Amount of memory free (in kilobytes).
17 Total memory available to Microsoft Excel (in kilobytes).
18 If a math coprocessor is present, returns TRUE; otherwise, returns FALSE.
19 If a mouse is present, returns TRUE; otherwise, returns FALSE. In Microsoft Excel for the Macintosh, always returns TRUE.
20 If a group is present in the workspace, returns a horizontal array of sheets in the group; otherwise returns the #N/A error value.

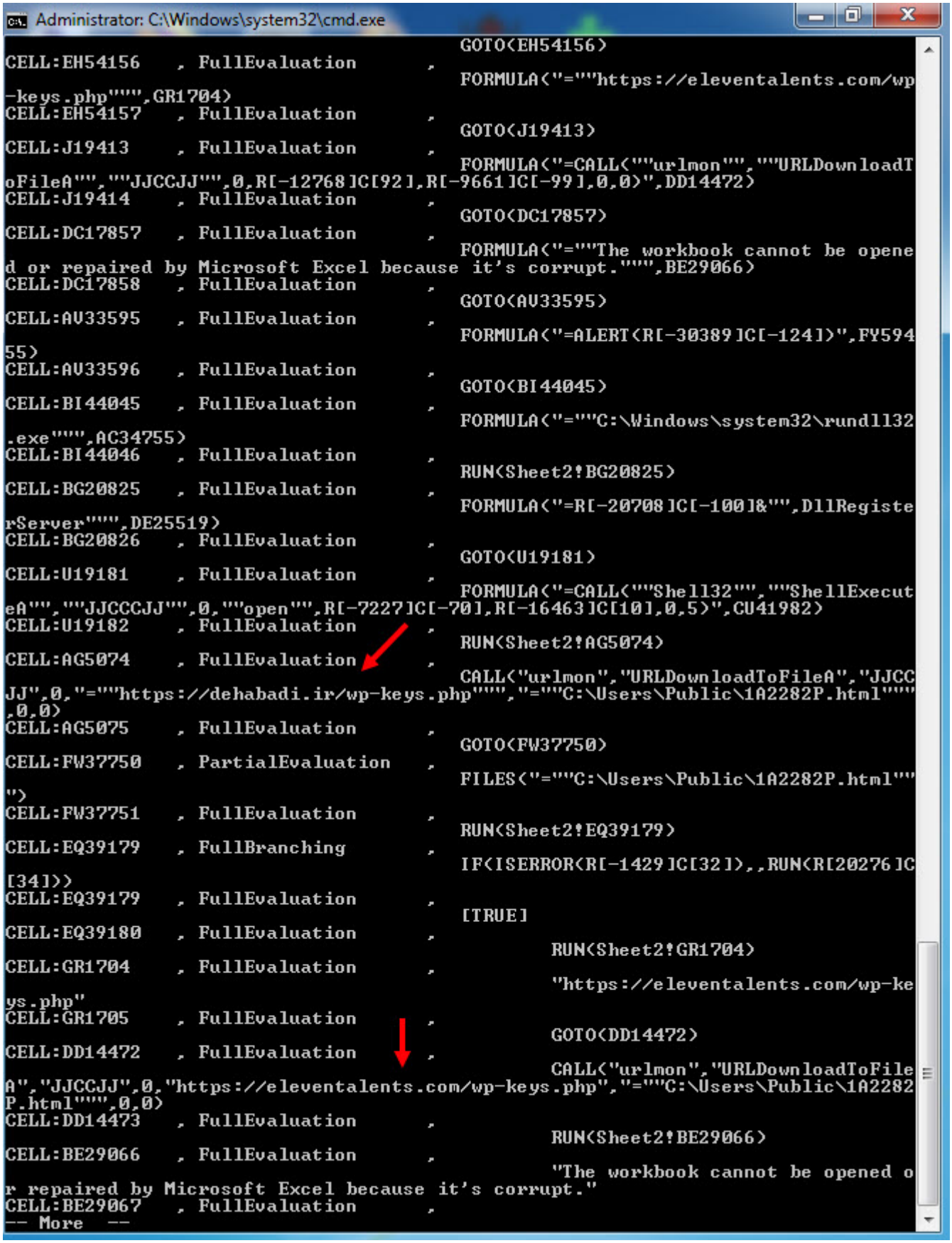


Hata ayıklamaya devam ettiğimde internet bağlantısını kontrol etmek için https://docs.microsoft.com/en-us/officeupdates/office-msi-non-security-updates web adresine bağlandığını ve hata alması durumunda çalışmayı durdurduğunu farkettim. Kayıt defteri (registery) üzerinden sistemde makro kullanımına izin verilip verilmediğini de kontrol ettikten sonra https://dehabadi[.]ir/wp-keys[.]php ve https://eleventalents[.]com/wp-keys[.]php adresleri ile iletişim kurmaya çalıştığını gördüm. Analiz esnasında bu iki adres de aktif olmadığı için analize devam edememiş olsam da yapmış olduğum araştırmalar sonucunda Zloader zararlı yazılımına ait komuta kontrol merkezleri olduğunu tahmin ettiğim bu adresleri ortaya çıkararak başarıyla amacıma ulaşmış oldum.



Bu yazı ile işin temelini öğrendiğinize göre bundan sonra XLMMacroDeobfuscator gibi bir araç ile gizlenmiş XLM makroyu hızlıca çözebilir ve zamandan tasarruf edebilirsiniz. :) Bu yazının XLM makro analizi yapmak isteyen analistlere ışık tutacağını ümit ederek bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.


Administrator: C:\Windows\system32\cmd.exe
C:\Users\Mert\Desktop>xlmdeobfuscator -f ea74b9a274c0c73cad990ddd089927b6.xls | more
XLMMacroDeobfuscator(v 0.1.4) - https://github.com/DissectMalware/XLMMacroDeobfuscator
File: C:\Users\Mert\Desktop\ea74b9a274c0c73cad990ddd089927b6.xls
[Loading Cells]
auto_open: auto_open->Sheet2!HP24304
[Starting Deobfuscation]
CELL:HP24304 , FullEvaluation , SET.VALUE(FG22029,-509)
CELL:HP24305 , FullEvaluation , RUN(Sheet2!FB54720)
CELL:FB54720 , FullEvaluation , SET.VALUE(CK33913,186)
CELL:FB54721 , FullEvaluation , GOTO(CB6172)
CELL:CB6172 , FullEvaluation , SET.VALUE(BD47287,-506.25)
CELL:CB6173 , FullEvaluation , RUN(Sheet2!HB9779)
CELL:HB9779 , FullEvaluation , SET.VALUE(BY37681,-290)
CELL:HB9780 , FullEvaluation , RUN(Sheet2!Z1238)
CELL:Z1238 , FullEvaluation , SET.VALUE(CB44507,-574)
CELL:Z1239 , FullEvaluation , RUN(Sheet2!F63714)
CELL:F63714 , FullEvaluation , SET.VALUE(DI59063,-442)
CELL:F63715 , FullEvaluation , RUN(Sheet2!H58494)
CELL:H58494 , FullEvaluation , SET.VALUE(GF45449,319.5)
CELL:H58495 , FullEvaluation , GOTO(CP32000)
CELL:CP32000 , FullEvaluation , SET.VALUE(GI36317,-454)
CELL:CP32001 , FullEvaluation , RUN(Sheet2!DS20258)
CELL:DS20258 , FullEvaluation , SET.VALUE(HW45041,-70.5)
CELL:DS20259 , FullEvaluation , GOTO(DE5285)
CELL:DE5285 , FullEvaluation , SET.VALUE(AR51698,132)
CELL:DE5286 , FullEvaluation , RUN(Sheet2!GZ57139)
CELL:GZ57139 , FullEvaluation , FORMULA("=CLOSE(FALSE)",HV23758)
CELL:GZ57140 , FullEvaluation , GOTO(EP44000)
CELL:EP44000 , FullEvaluation , FORMULA("=APP.MAXIMIZE()",EP44001)
CELL:EP44001 , PartialEvaluation , APP.MAXIMIZE()
CELL:EP44002 , FullEvaluation , GOTO(BQ62228)
CELL:BQ62228 , FullEvaluation , FORMULA("=IF(GET.WINDOW(7),GOTO(R[-38471]C[161]),)",BQ62229)
CELL:BQ62229 , FullEvaluation , IF(GET.WINDOW(7),GOTO(R[-38471]C[161]),)
CELL:BQ62230 , FullEvaluation , GOTO(DH60440)
CELL:DH60440 , FullEvaluation , FORMULA("=IF(GET.WINDOW(20),,GOTO(R[-36683]C[118]))",DH60441)
CELL:DH60441 , FullEvaluation , IF(GET.WINDOW(20),,GOTO(R[-36683]C[118])



Not: XLM makro analizine dair daha fazla kaynak arayanlara şu yazılara da (#1, #2, #3, #4, #5) göz atmalarını tavsiye edebilirim.