2023

SECURITY REPORT

Malware Document Analysis

github.com/Abdibimantara

abdibimantara.github.io

Daftar Isi

Eksekutif Summary

Pada bulan maret 2023, terdapat *sample* baru yang terindentifikasi sebagai *malware*. *Malware* tersebut berasal dari file *berekstensi*.xls dan .doc dan dikenal dengan nama “Bank Slip.xls”. Aktivitas *malware* tersebut memiliki hubungan dengan kerentanan yang dikenal dengan id CVE-2017-11882 dan CVE-2018-0802.

Tools yang digunakan

Dalam melakukan proses identifikasi malware tersebut, kami menggunakan beberapa tools yaitu :

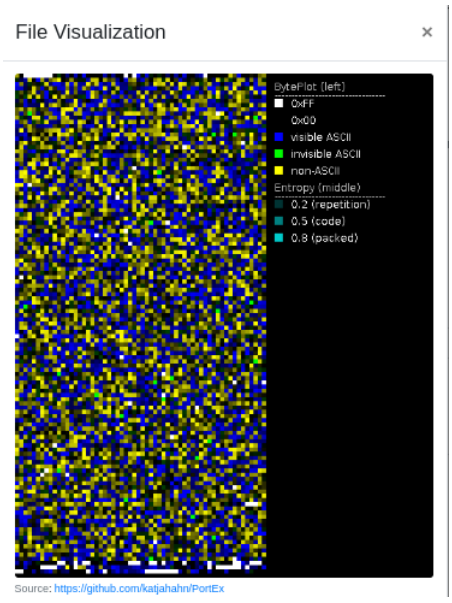
- AnyRun (Sandbox)
- Triage (Sanbox)
- Oledump.py

Identifikasi Sample Malware

Diawal tahun 2023 ini, kami kembali menemukan salah satu document berbahaya yang menggunakan format .xls. File tersebut merupakan salah satu file yang berasal dari produk terkenal yaitu Microsoft excel. File tersebut memiliki nama “Bank Slip.xls”. Secara kasat mata, mungkin orang awam hanya berfikir bahwa file tersebut hanyalah slip tranksaski perbankan seperti pada umumnya. Namun disini kami akan memberikan informasi mengenai file tersebut kami kategorikan sebagai malware.

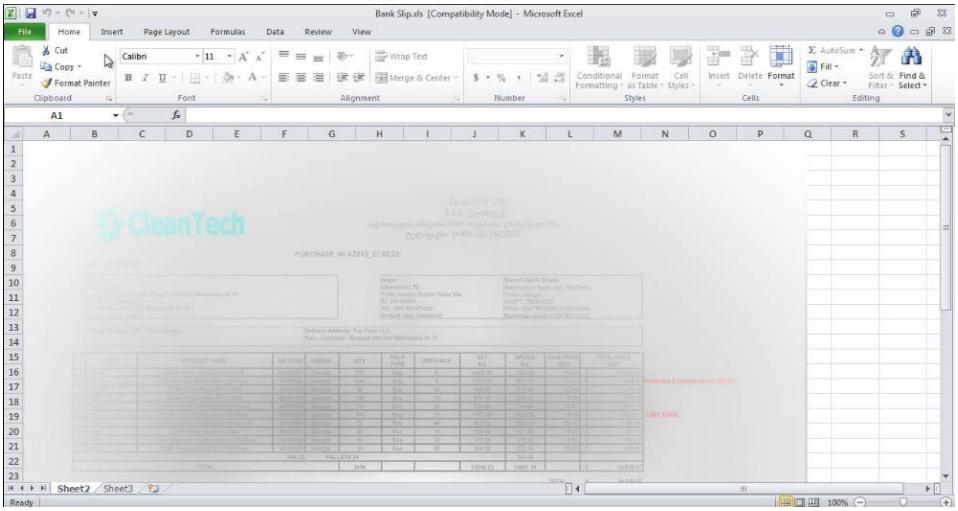
Berikut detail sample file yang berhasil kami dapatkan :

- Nama : “Bank Slip.xls”
- Size : 432 KB
- MD5 : 85c490912e285bd5d94e0a426f04a9d6
- SHA1 : 6a571ed2b4c58522eabd1bd00e3fc7a7a3b26635
- SHA-256 : f15fda356c604aa1819c7d45cc556f8fb796471a - 7c13e8bdea4be2f3a984c923
- SHA512 : 479fcd2889c9f10668c51191a9f2c3654e69e3d - 686fe2d2e82b5aa9775f63d311e1012f13f0c51c - bfed3dde4a8fee6da3a58416688dce46d75f6f505 - 0f9e680b
- SSDEEP : 12288:KIoQbGFJX8EVSD4iJ9UHqthcULSH - v1tfKawyxh5s:tOJXhV1iXU0cUej7xs
- Application : Microsoft Excel
- Content-Type : application/vnd.ms-excel
- Entropy : 8.0



Gambar 1. Visualisasi file Bank Slip.xls“

Analisa file “Bank Slip.xls” dimulai dengan membuka file tersebut degan menggunakan bantuan dari tools sandbox free online yaitu **hatching malware sandbox.**



Gambar 2. Tampilan saat membuka file “Bank Slip.xls“

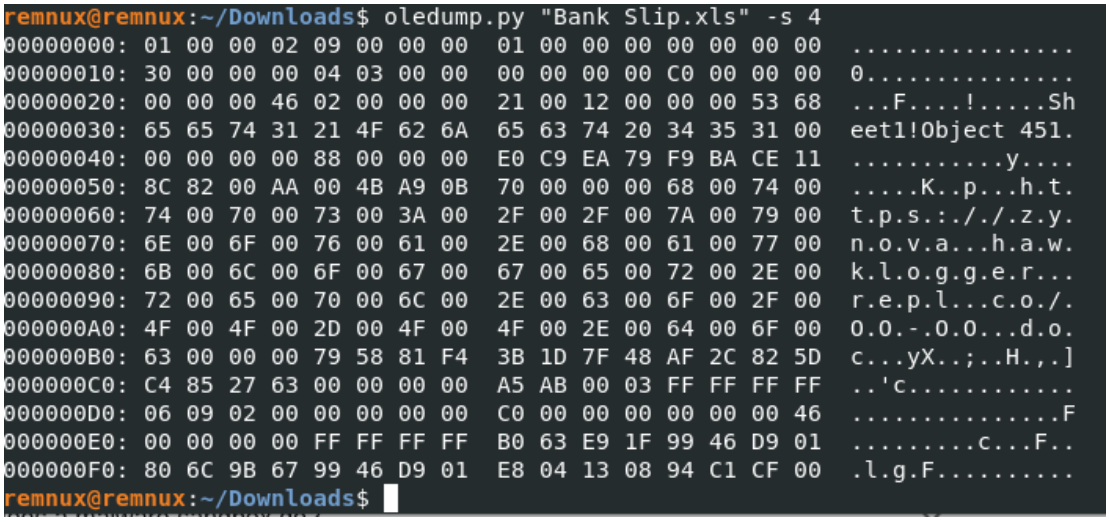
Terlihat bahwa file tersebut tampak tidak menampilkan sesuatu yang berbahaya dan hanya terdapat suatu foto atau gambar yang membuat informasi transaksi perbankan. Disini kami berinisiatif untuk melakukan pengcekkan lebih mendetail yaitu melihat apakah ada suatu perintah atau command yang tertanama dalam file tersebut yang disebut dengan *macro.*

Untuk membantu kami dalam menganalisis *macro* dalam file “Bank Slip.xls” tersebut, kami menggunakan tools oledump yang dibuat oleh Didier Stevens. Melalui tools tersebut kami akan mencoba melalukan dump pada object yang *terlinking* dan *terembedding*.

```
remnux@remnux:~/Downloads$ oledump.py "Bank Slip.xls"
  1:       114 '\x01CompObj'
  2:       244 '\x05DocumentSummaryInformation'
  3:       200 '\x05SummaryInformation'
  4:       256 'MBD011DAFF2/\x01Ole'
  5:    425747 'Workbook'
  6:       526 '_VBA_PROJECT_CUR/PROJECT'
  7:       104 '_VBA_PROJECT_CUR/PROJECTwm'
  8: m     977 '_VBA_PROJECT_CUR/VBA/Sheet1'
  9: m     977 '_VBA_PROJECT_CUR/VBA/Sheet2'
 10: m     977 '_VBA_PROJECT_CUR/VBA/Sheet3'
 11: m     985 '_VBA_PROJECT_CUR/VBA/ThisWorkbook'
 12:      2644 '_VBA_PROJECT_CUR/VBA/_VBA_PROJECT'
 13:       553 '_VBA_PROJECT_CUR/VBA/dir'
remnux@remnux:~/Downloads$
```

Gambar 3. Identifikasi macro “Bank Slip.xls”

Berdasarkan pengecekkan, kami tidak menemukan macro dalam file “Bank Slip.xls” tersebut. Namun disini file tersebut memiki sebanyak 13 stream, sehingga kami berinisiatif untuk melakukan pengcekkan satu demi satu.



Gambar 4. Hasil dump stream 4 “Bank Slip.xls”

Pada pengecekkan yang dilakukan di stream ke 4, kami menemukan sesuatu yang ganjil. Dimana tampak seperti link url yang tertanam pada document tersebut. Untuk lebih detail dapat dilihat pada gambar dibawah :

Gambar 5. Hasil dump stream 4 “Bank Slip.xls” bagian kedua

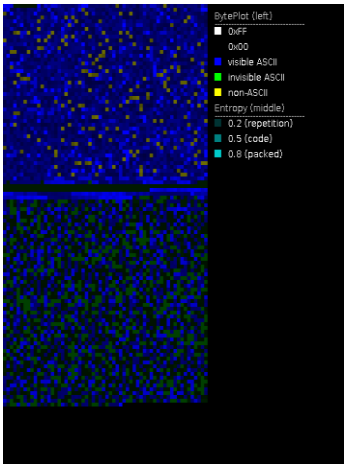
Disini kami mengetahui bahwa file “Bank Slip.xls” setelah dibuka oleh user, akan mencoba terhubung dengan url tersebut dan akan mencoba mendownload file baru yaitu “OO-OO.doc”.

Berikut detail file “OO-OO.doc” yang berhasil kami dapatkan :

- Nama : “OO-OO.doc”
- Size : 12,26 KB
- MD5 : f769da2607ed96e6a3a3faf2812efabe
- SHA1 : 180a581b8bb14e4959e235711785b6e8409aac6e
- SHA-256 : c054af2f2e1ece3e68889a77c04e6d21675-

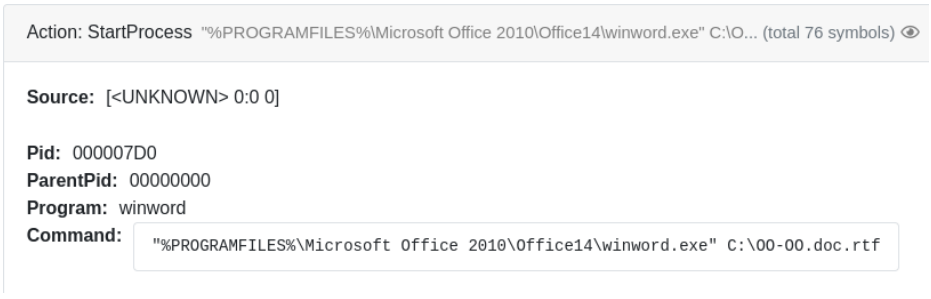
646b0c5a2b5815633ed2dc1089942

- SHA512 : 6444f305933c4daecf5680f49f15448eb92 bdc7e0e0df39a45d9658529d6c994b-343577ff42b386c65ee113e1de298c4cdd237-88b4dda21aecbf61dae8f5980
- SSDEEP : 384:DmjkZenlHY8zYK6+8S4RmWvirtT-PcnNfT9fSp:DmjKIlLzMo4RnNZTpSp

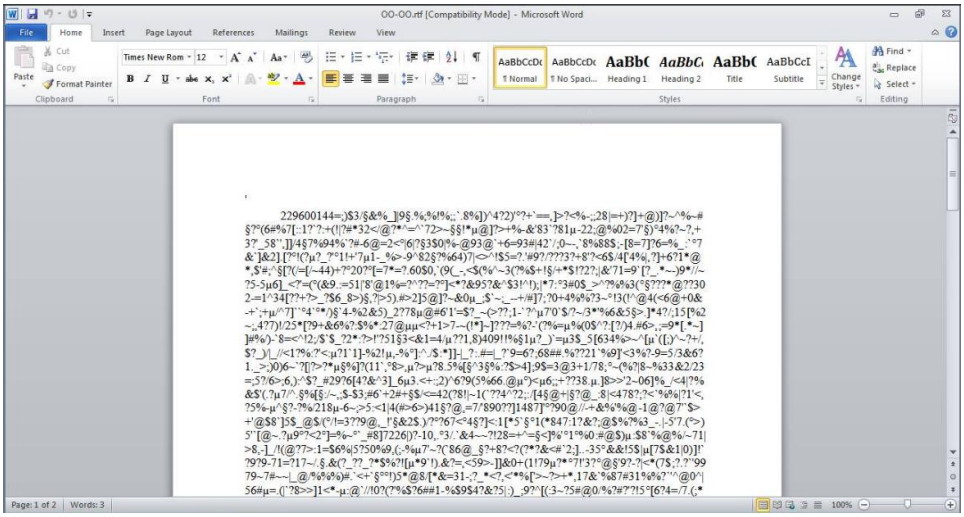


Gambar 6. Visualisasi File “OO-OO.doc”

Diketahui bahwa file “OO-OO.doc” juga merupakan salah satu file Microsoft word. Ketika kami membuka file tersebut, kami hanya mendapati bahwa file tersebut memiliki double ektension yaitu .doc dan .rtf.



Gambar 7. Double Extention File “OO-OO.doc”



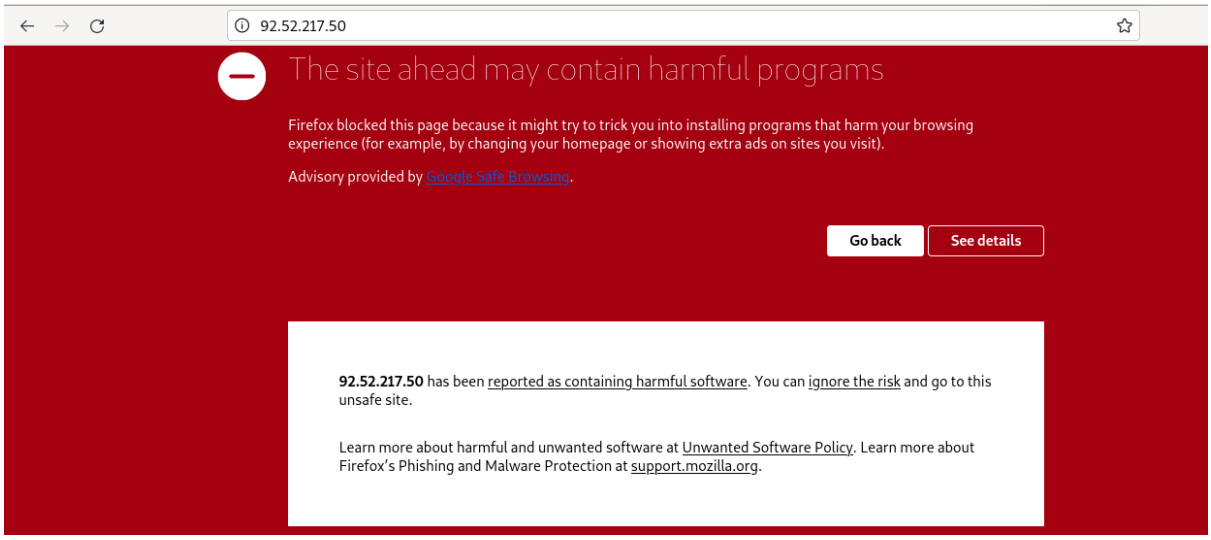
Gambar 8. Tampilan saat membuka file “OO-OO.doc”

Berdasarkan hasil dari percobaan membuka file “OO-OO.doc” tersebut kami menemukan bahwa file tersebut berisi beberapa string yang tidak beraturan. Disini kami berusaha menyelidiki string tersebut, namun kami tidak mendapatkan informasi yang kami inginkan.

Namun dari hasil aktivitas open file tersebut kami menangkap aktivitas anomali yaitu :

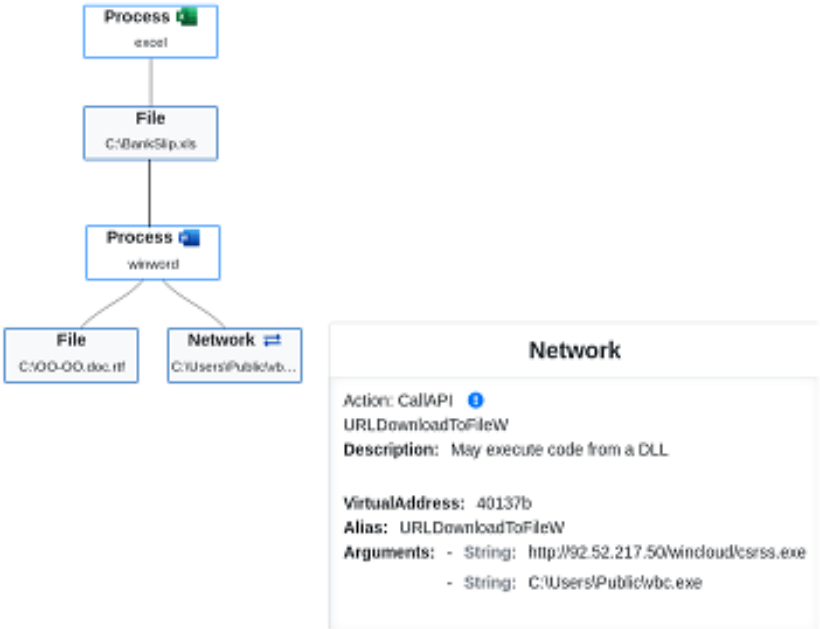
- Found action EmbedEquation (May contain an exploit due to the presence of equation OLE objects)
- Found action GetProcAddress (May execute code from a DLL)
- Found action LoadLibraryW (May execute code from a DLL)
- Found action URLDownloadToFileW (May execute code from a DLL)
- Found action ExpandEnvironmentStringsW (May execute code from a DLL)

Dimana dari beberapa aktivitas tersebut menunjukkan bahwa terdapat adanya usaha untuk menjalin konektivitas terhadap ip eksternal yaitu **92(.)52(.)217(.)50** yan bersal dari negara Hongaria. Dimana disaat user telah berhasil terhubung dengan ip tersebut maka secara otomatis mendownload file yang Bernama **“csrss.exe”** yang kami yakini telah dimodifikasi pada direktori wincloud. Dimana disini adalah file csrss.exe berfungsi sebagai “**controls many critical functions on your operating system**” sehingga sangat berbahaya jika attacker berhasil mendapatkan akses tersebut. Sayangnya kami tidak bisa mendapatkan sample file tersebut dikrenakan ip eksternal tersebut sudah nonaktifikan dikarenakan terindikasi sebagai phising.



Gambar 9. Tampilan saat mengakses ip csrss.ex”

Berikut adalah grafik hubungan yang terjadi antara file “Bank Slip.xls” dan file “OO-OO.doc” dalam membantu attacker menjalankan aksinya.



Gambar 10. Diagram alur aktivitas malware

Tactic dan Technique

Berdasarkan hasil pengecekkan yang kami lakukan diketahui bahwa file “Bank Slip.xls” terdeteksi menggunakan tactic Execution dengan technique Command and Scripting Interpreter sedangkan pada file “OO-OO.doc” terdeteksi menggunakan tactic Execution dengan technique Exploitation for Client Execution.

Table 1. Tactic dan Technique

Files	Tactic	Technique	CVE Related
Bank Slip.xls	Execution	Command and Scripting Interpreter	-
	Execution	Exploitation for Client Execution	Related to CVE-2017-11882 or CVE-2018-0802

Indicator of Compromise (IoC)

Berdasarkan hasil pengecekkan yang kami lakukan juga didapet bebera Indicator of Compromise (IoC) yang berasal dari Kedua file tersebut

IoC File “Bank Slip.xls”

- URL : https://zynova(.)hawklogger(.)repl(.)co/OO-OO.doc
- Domain : zynova(.)hawklogger.()repl(.)co
- MD5 : 3f98d7e0e33566331bf8eae6480a9b84
- SHA1 : 050dd851fe2af90b9749ad5e9e0583792ff190ca
- SHA256 : 7be46bdc7bdc8f96d32dbd966ff6f46fc51 762b3f287318c18ca3a8807cd2465
- SHA512 : 024f5ebc27664d19fd2a3ca25d539b0 e2c67bea05bdfe7dcb57f6a3cf1f210ce 392f596d3397e76588956ab67b618865eb

f274deed138d281fa183f4edcdc23f

- IP Address : 34(.)160(.)67(.)231 (United States)

IoC File “OO-OO.doc”

- URL : http://92.52.217.50/wincloud/csrss.exe
- MD5 : 74b4ebf7ab889024341b49a476232fc2
- SHA1 : 6d573661d8b7950aacf3c818ea938b0cf1bc7194
- SHA256 : eeb57c0fa42e066b0dda567cd12c53
  53345b048d87b41e19419e3b0958fc5ce3
- SHA512 : 946a2f229e3986263bd3f571c425 -
  f2fc57122988aee38d0ca81c8e20d0
  f9881ed102e1997625d631055
  13a62ad2f52625585c245958a6b6b9c00a6ae6de33890
- IP Address : 92(.)52(.)217(.)50 (Hongaria)

Tips agar Terhindari dari Malware

1. Malware tersebut umumnya berasal dari pesan atau email, sehingga hindari membuka file yang berasal dari seseorang atau sumber tidak dikenal
2. Segera nonaktifkan koneksi internet jika sudah terlanjut membuka file tersebut
3. Selalu Update Sistem operasi serta antivirus yang digunakan
4. Segera laporkan insiden atau indikasi anomaly jika mencurigan pada tim Cybersecurity