Advanced Malware VBA Stomping

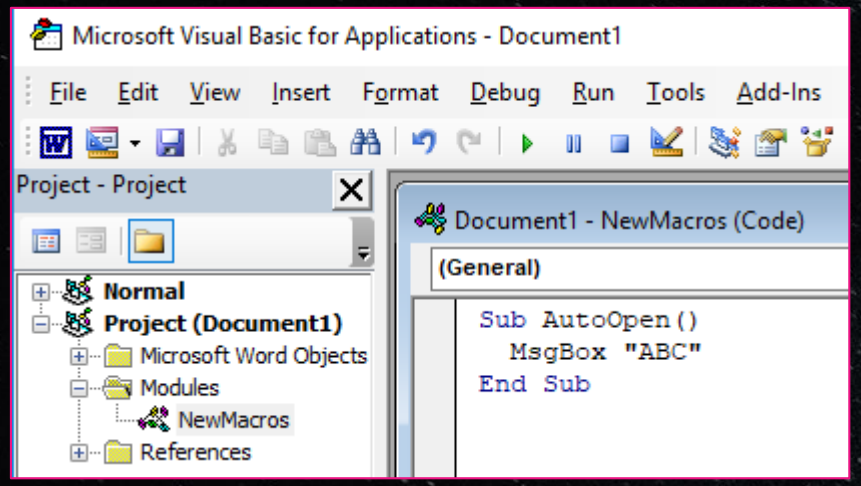
What's New in 2019

Kirk Sayre @bigmacjpg
Carrie Roberts @OrOneEqualsOne

Recap: DerbyCon 2018

- Macro Storage (VBA) stored as:
  - Source Code - the original code as entered by the programmer (compressed)
  - P-Code - a compiled Pseudo-code ← This is what executes most of the time
- Dr. Vesselin Bontchev https://github.com/bontchev/pcodedmp

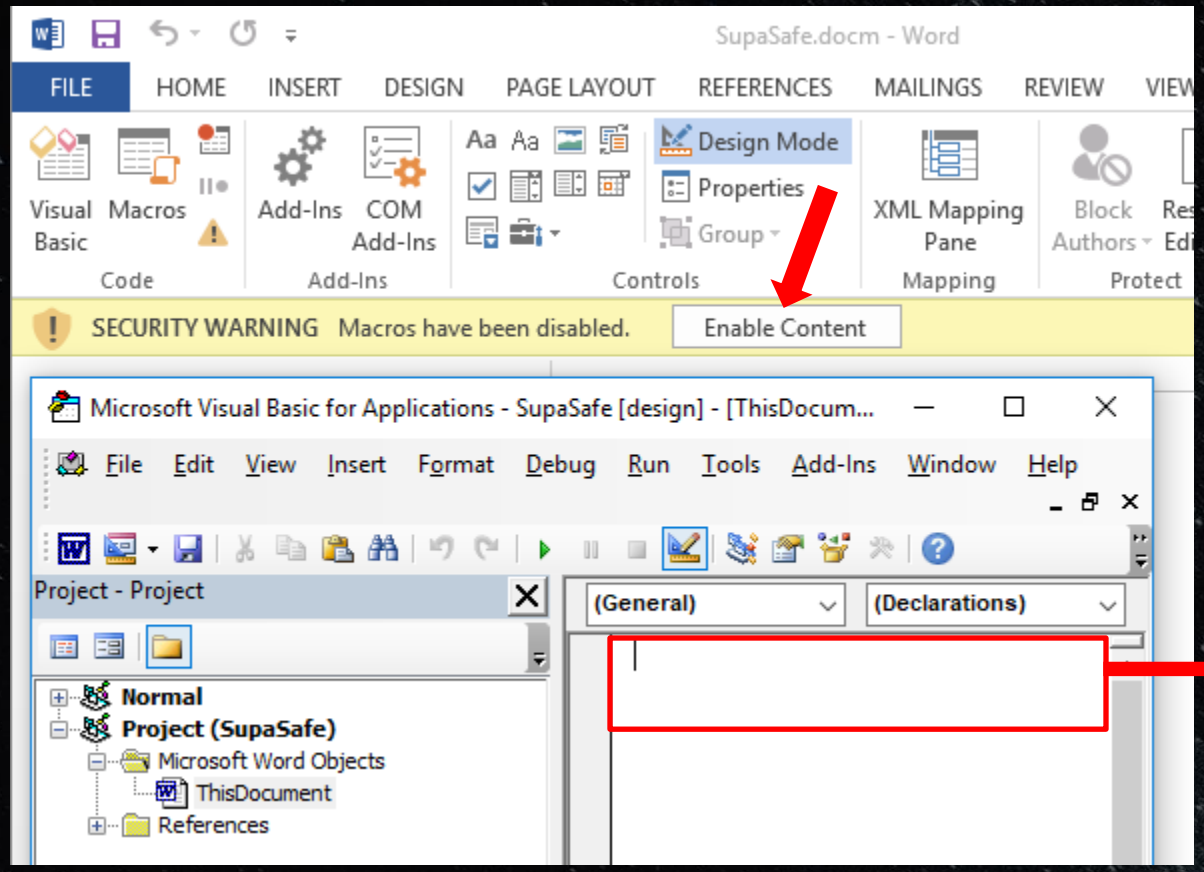
Source Code

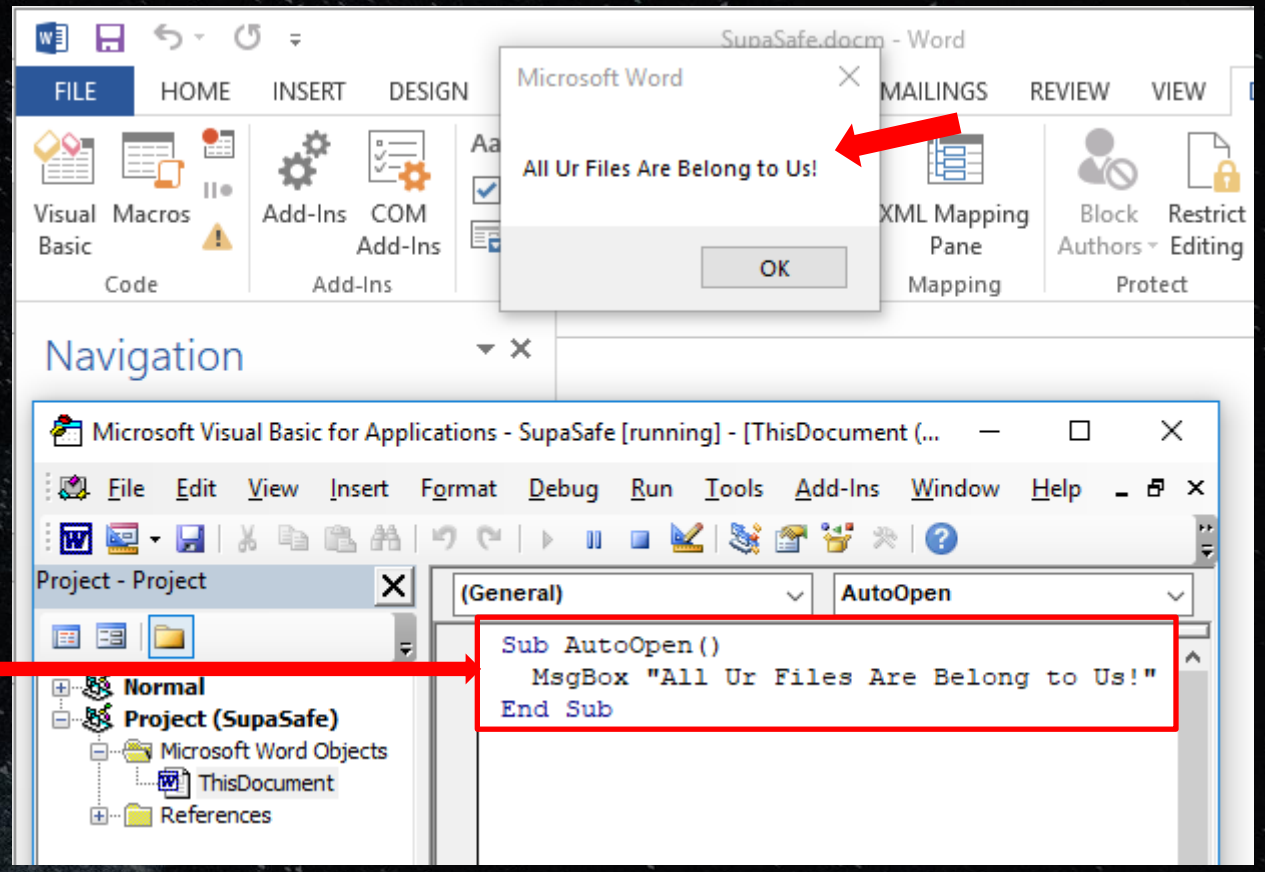


P-Code

```
Line #0:
        FuncDefn (Sub AutoOpen())
Line #1:
        LitStr 0x0003 "ABC"
        ArgsCall MsgBox 0x0001
Line #2:
        EndSub
```

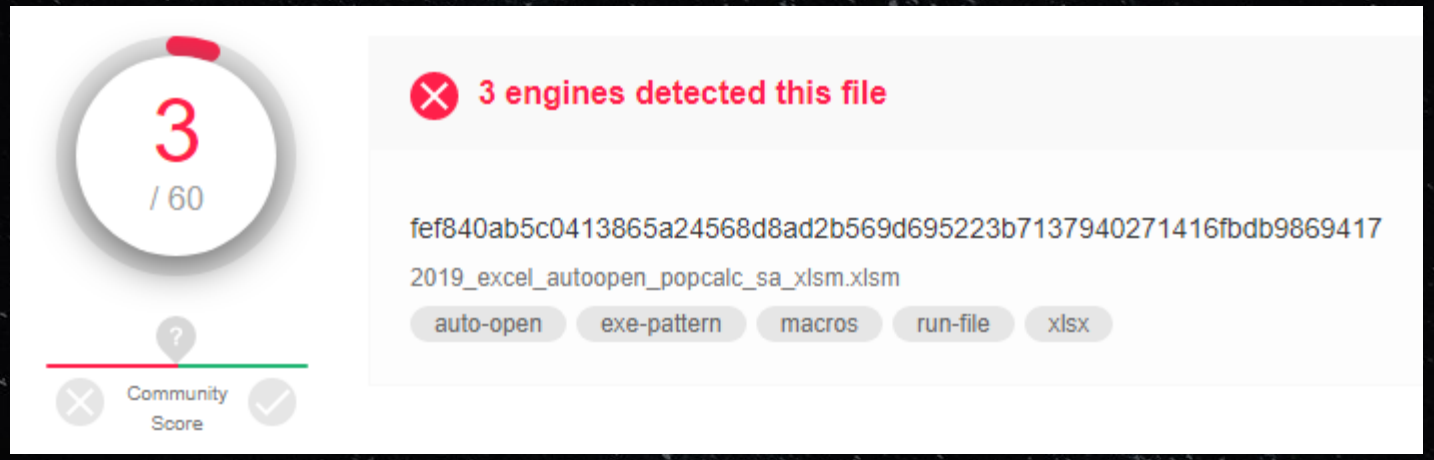
VBA Stomp Demo

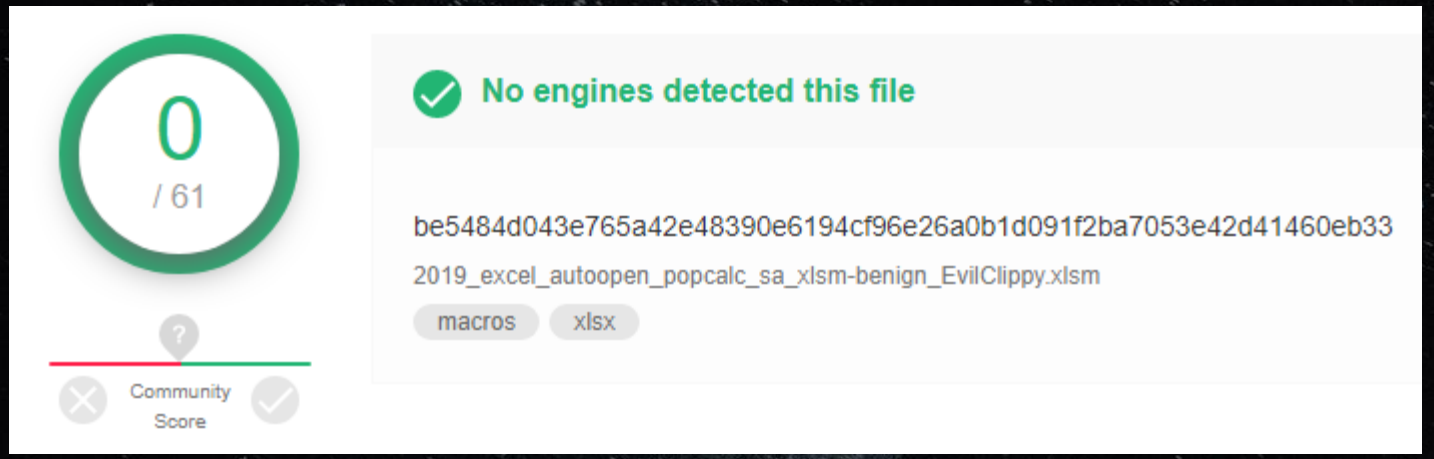




sparkcon
Save Data. Hack Better.

VirusTotal Results after VBA Stomp





fef840ab5c0413865a24568d8ad2b569d695223b7137940271416fbdb9869417
be5484d043e765a42e48390e6194cf96e26a0b1d091f2ba7053e42d41460eb33

sp4rkcon
Save Data. Hack Better.

VBA Stomping: What's New in 2019

2018	2019
Manual Stomping	Automated Stomping
Stomp Source Code	Replace Source Code
Office Version Dependency	Dynamic Version Support
	Lock VBA Project
	Yara Rule for Detection

sp4rkcon
Save Data. Hack Better.

Automated VBA Stomping Tools

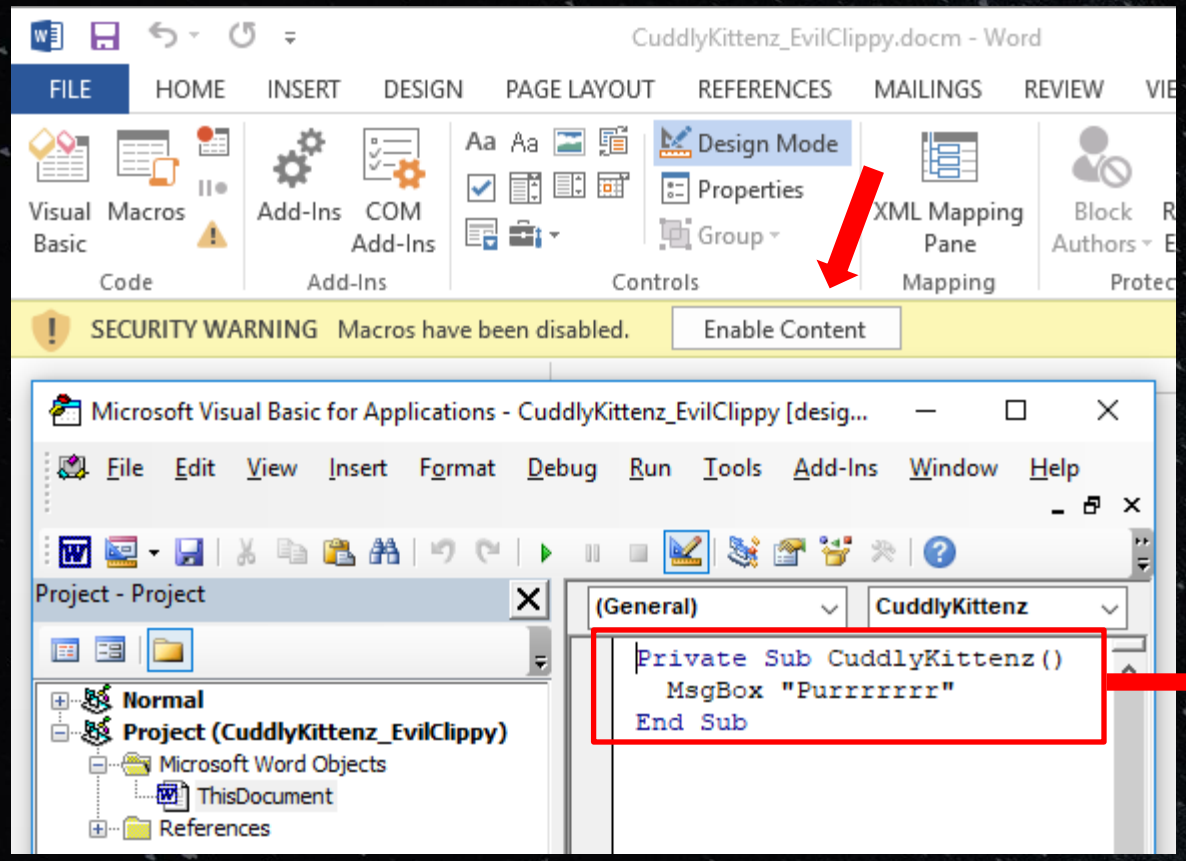
- Automated Document Builder (ADB)
  - Python tool by Harold Ogden and Kirk Sayre
  - https://github.com/haroldogden/adb
- Evil Clippy
  - Cross-Platform Binary by Stan Hegt (@StanHacked) from Outflank
  - https://github.com/outflanknl/EvilClippy

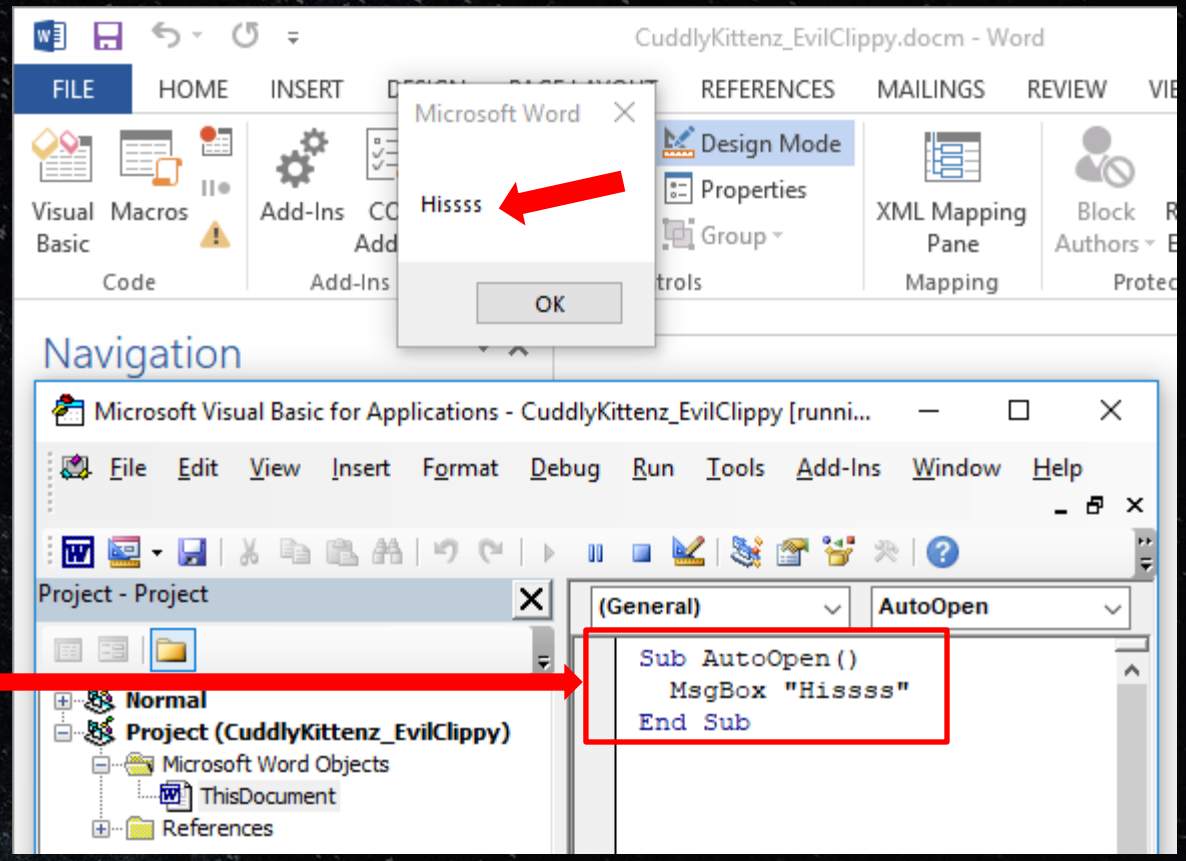
Evil Clippy - Automated VBA Stomping

- Replace vs Stomp
- Deliver version matched document template to victim
- Lock VBA Source (make it unviewable)
- Many more tricks included

sp4rkcon
Save Data. Hack Better.

Evil Clippy Replace VBA Source





sp4rkcon
Save Data. Hack Better.

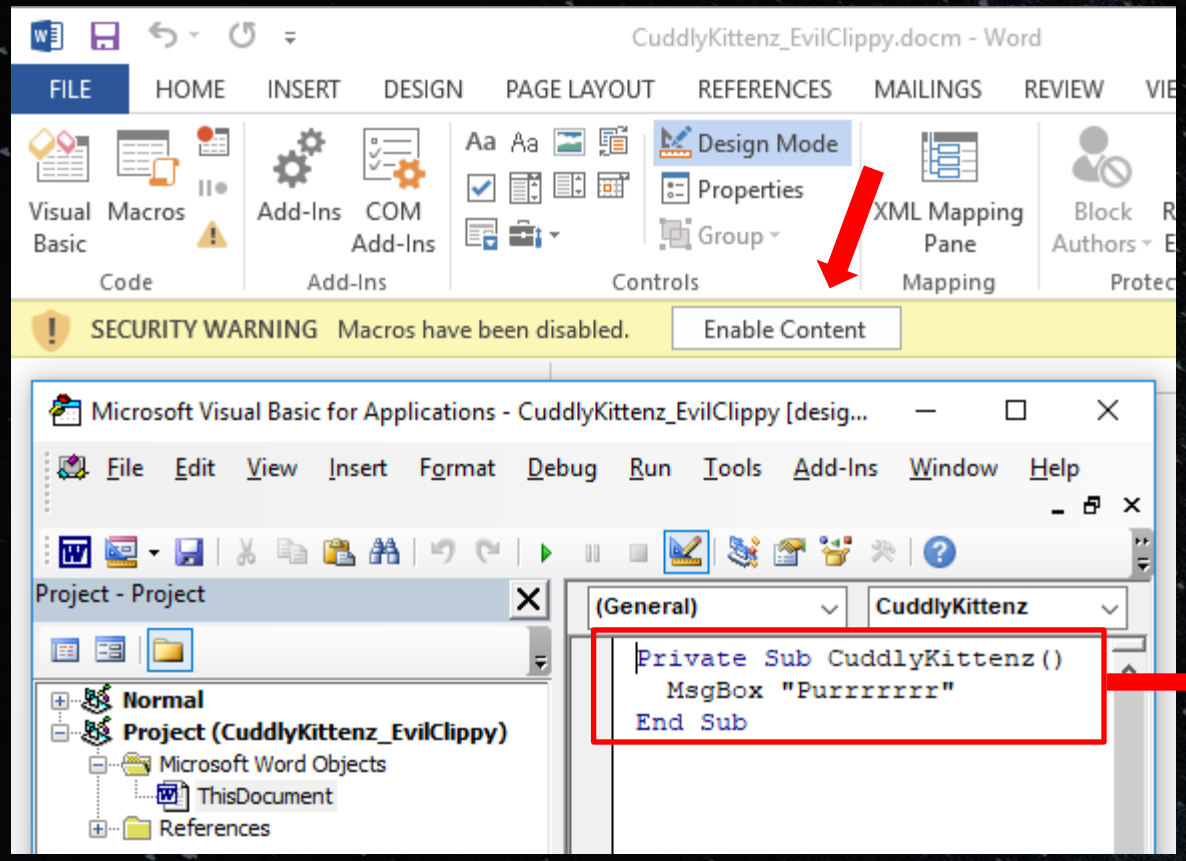
Version Matched Document Template

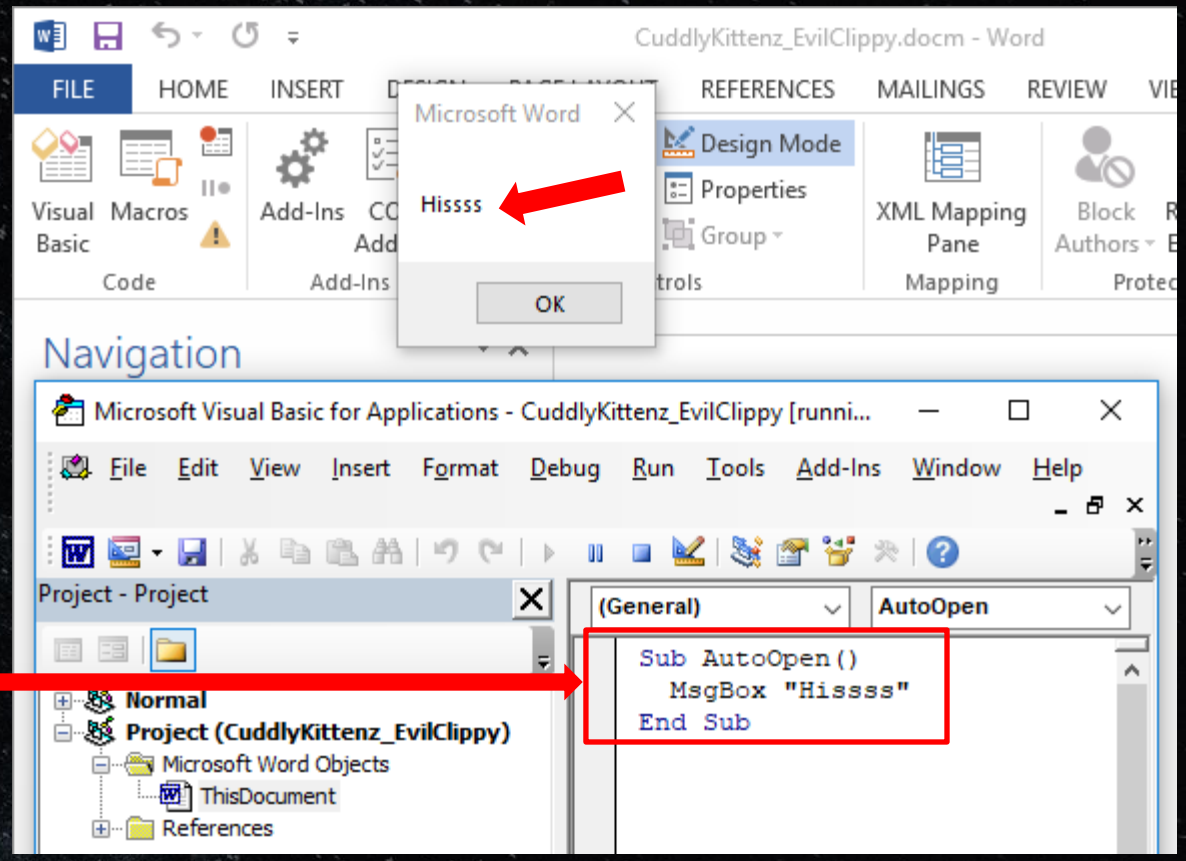
- Compiled P-Code will only run in specific Office versions.
- P-Code version information is stored in bytes 2-3 of the _VBA_PROJECT OLE stream.
- EvilClippy can set these bytes to allow VBA stomped documents to execute under different versions of Office.
- EvilClippy can also run as a web server to automatically serve out the correct document versions based on the connecting user agent.

Serve Out Version Matched Documents

```
victim:~/Software/EvilClippy> ./EvilClippy.exe --webserver=1343 -s test.vbs test_doc.doc
Now stomping VBA code in module: ThisDocument
Webserver starting on port 1343. Press a key to quit.
Webserver running...
Serving request from 10.4.137.6:56836 with user agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win64; x64; Trid
0C; Microsoft Outlook 15.0.5023; ms-office; MSOffice 16)
Targeting pcode on Office version: 2016x64
Serving out file 'test_doc_EvilClippy.doc'
Serving request from 10.4.137.6:56842 with user agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win32; x32; Trid
0C; Microsoft Outlook 15.0.5023; ms-office; MSOffice 16)
Targeting pcode on Office version: 2016x86
Serving out file 'test_doc_EvilClippy.doc'
Serving request from 10.4.137.6:56846 with user agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; Win32; x32; Trid
0C; Microsoft Outlook 15.0.5023; ms-office; MSOffice 15)
Targeting pcode on Office version: 2013x86
Serving out file 'test_doc_EvilClippy.doc'
```

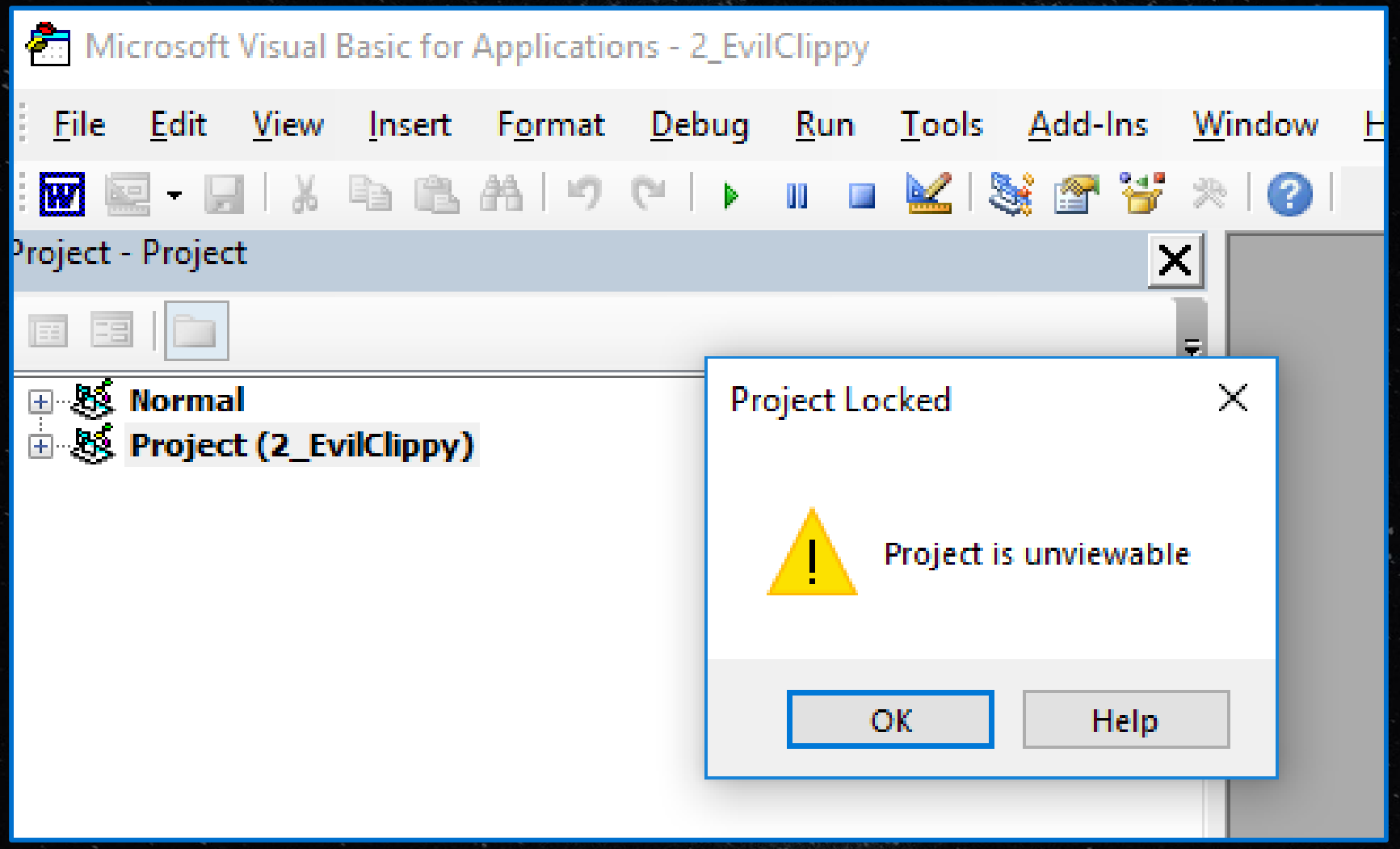
Evil Clippy Replace VBA Source





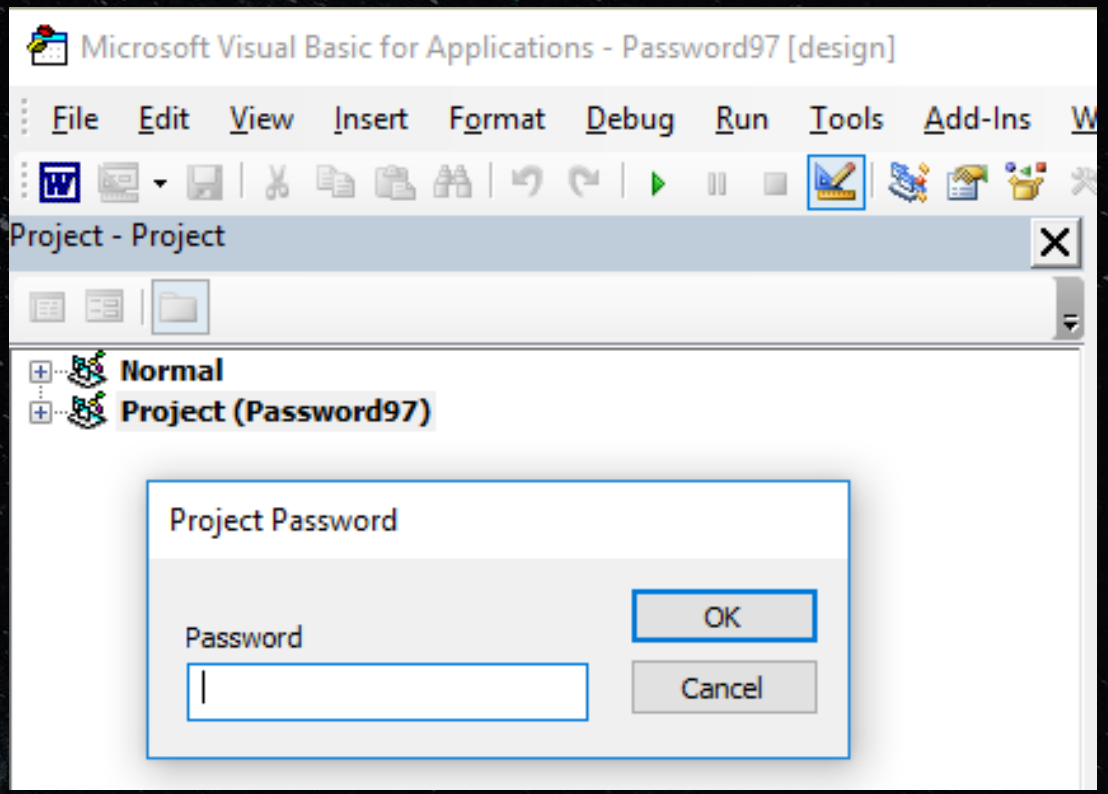
sp4rkcon
Save Data. Hack Better.

Lock VBA Source (make it unviewable)



Unlock VBA Project

- Evil Clippy can also remove Locked/Unviewable Setting
  - Previously considered irreversible
- Bonus: Also removes password protection



https://medium.com/walmartlabs/vba-project-locked-project-is-unviewable-4d6a0b2e7cac

VBA Stomp Detection

- Zipped by MS Office?

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0x0000	Signature				Version		Flags		Compression		Mod Time		Mod Date		Crc-32	
0x0010	Crc-32				Compressed Size				Uncompressed Size				File Name Len		Extra Field Len	
0x0020	File Name (variable size)															
0x0030	Extra Field (variable size)															

Extra Field Len != 0 for MS Office

Yara Rule For Detection

```
rule unusual_office_zip_header
{
        meta:
          description = "MS Office Open_XML document with unusual zip header"
          weight  = 90
          author = "Carrie Roberts - Walmart Information Security"
          date = "2019-04-02"

        strings:
          // Headers of files to look for
          $header_pkzip_with_zero_extra_field_length = { 50 4b 03 04 [24] 00 00} //PK zip header
          $office_openxml="[Content_Types].xml" nocase
          $has_macros = "/vbaProject.bin" nocase

        condition:
          ($header_pkzip_with_zero_extra_field_length at 0) and $office_openxml and $has_macros
}
```

VBA Stomp Summary

- Deterrent to Anti-Virus Detection and Reverse Engineering
- Easily Automated with Evil Clippy
- Some Detections Available
- See ***vbastomp.com*** for More Information

Kirk Sayre @bigmacjpg
Carrie Roberts @OrOneEqualsOne
https://vbastomp.com