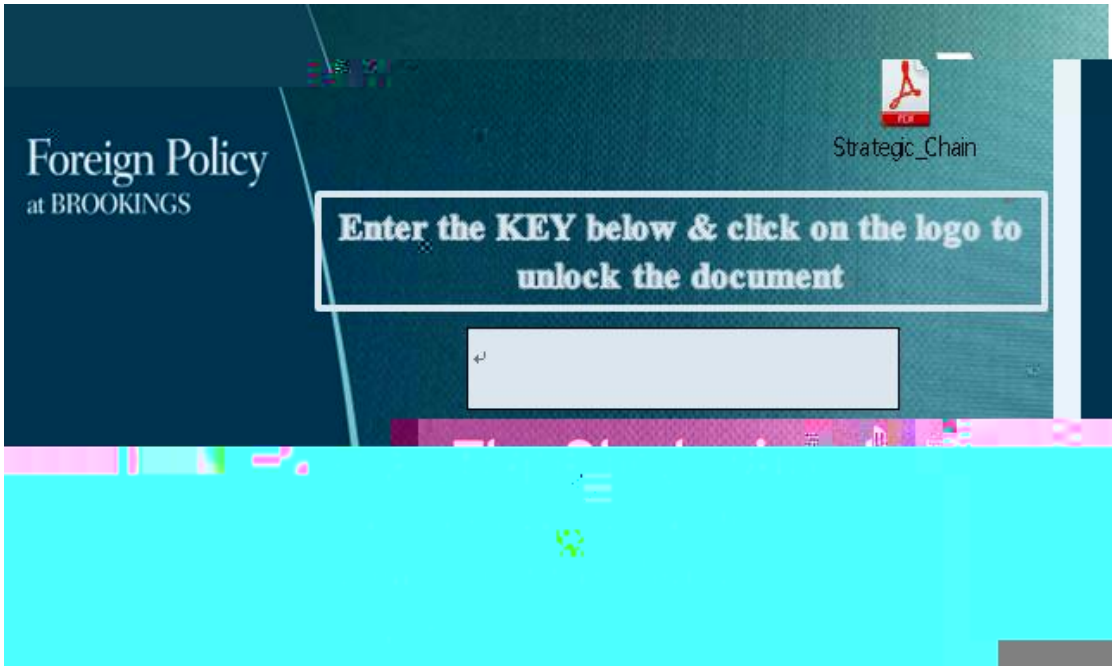
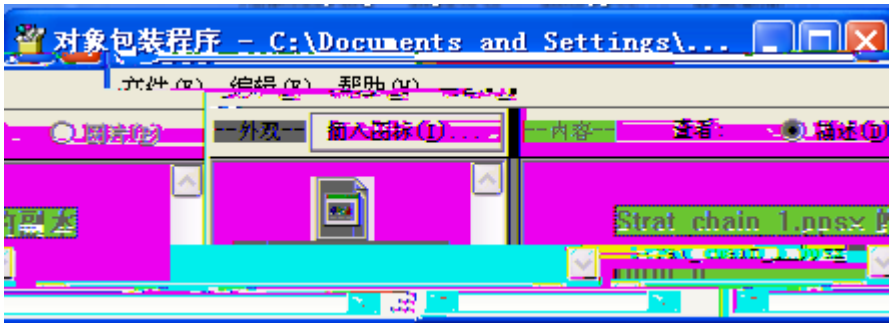
VenusEye



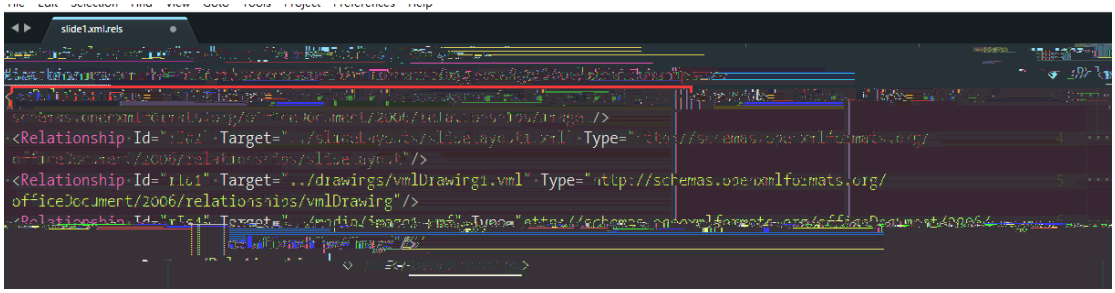

www.venusdental.com.cn




3. 圧縮 OLE パッケージ Start_chain_1 と ppsx ファイル ppt スライドショー ppt

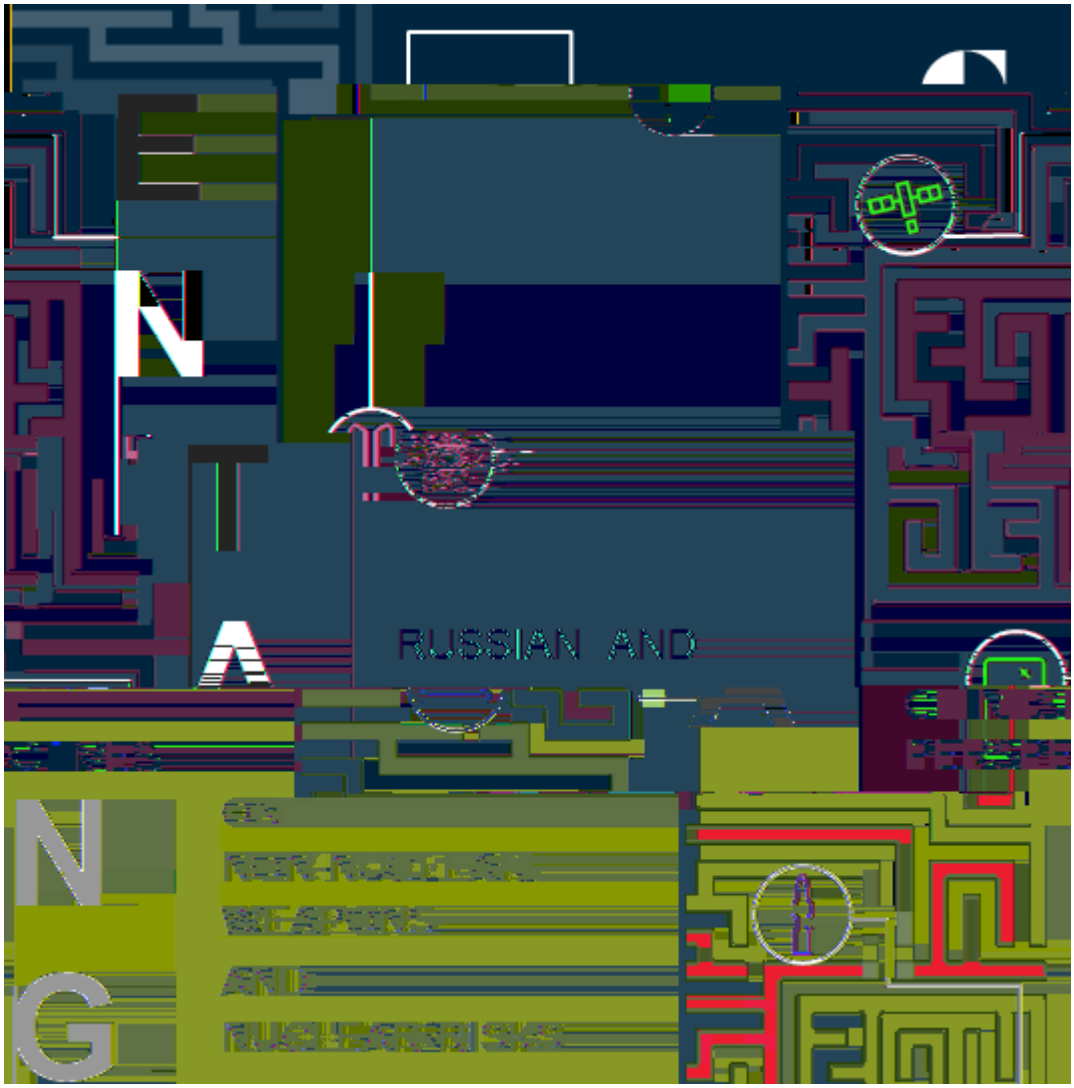



4. B ppsx ファイル+X CVE-2017-0199 パッチ適用 ppt ファイル sct フォルダ




5. sct フォルダ内 B3+X Powershell ウィンドウ putty.exe 実行 - Strategic_Chain.pdf ファイル X 実行

6. L[illegible]01j= Entanglement ppsx
[illegible]X CVE-2017-0199 %[illegible]

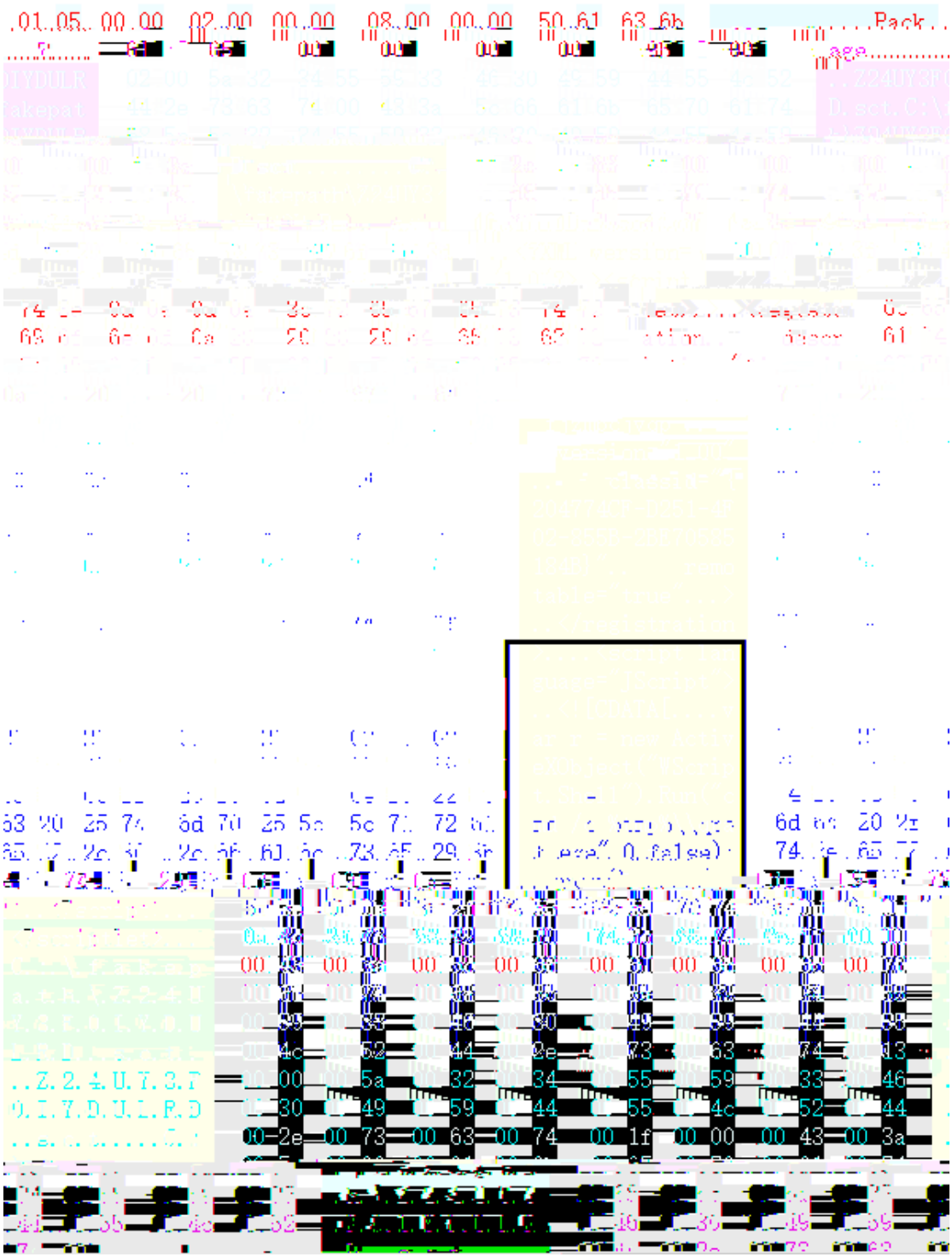



2018 3

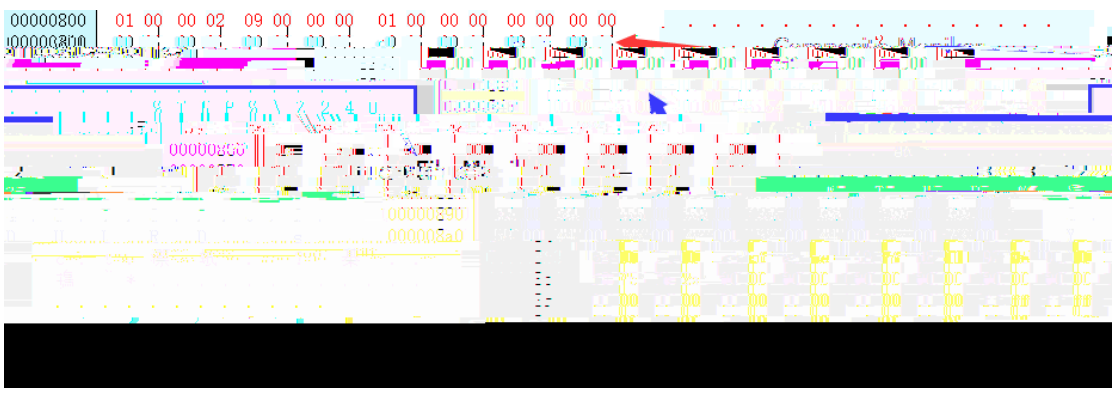
CVE-2017-8570


www.venusdental.com.cn


www.venusdental.com.cn



OLE CVE-2017-8570 Scriptlet Moniker -sct



%N4G-G qrat

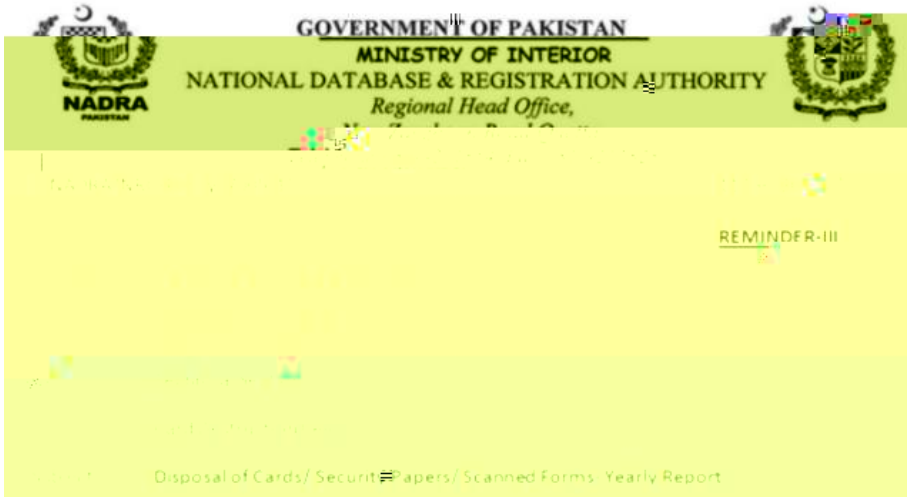
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | 0123456789ABCDEF |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00h: | AD | AE | 10 | 00 | 02 | 00 | 71 | 72 | 61 | 74 | 2E | 65 | 78 | 65 | 00 | 43 | -®....qrat.exe.C |
| 10h: | 3A | 5C | 66 | 61 | 6B | 65 | 70 | 61 | 74 | 68 | 5C | 71 | 72 | 61 | 74 | 2E | :\fakepath\qrat. |
| 20h: | 65 | 78 | 65 | 00 | 00 | 00 | 03 | 00 | 15 | 00 | 00 | 00 | 43 | 3A | 5C | 66 | exe.........C:\f |
| 30h: | 61 | 6B | 65 | 70 | 61 | 74 | 68 | 5C | 71 | 72 | 61 | 74 | 2E | 65 | 78 | 65 | akepath\qrat.exe |
| 40h: | 00 | 00 | AE | 10 | 00 | 4D | 5A | 90 | 00 | 03 | 00 | 00 | 00 | 04 | 00 | 00 | ..®..MZ..... |
| 50h: | 00 | FF | FF | 00 | 00 | B8 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 40 | 00 | 00 | .ÿÿ..¸.......@.. |
| 60h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 70h: | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | ..... |
| 80h: | 00 | 80 | 00 | 00 | 00 | 0E | 1F | BA | 0E | 00 | B4 | 09 | CD | 21 | B8 | 01 | .€.....°..´.Í!¸. |
| 90h: | 4C | CD | 21 | 54 | 68 | 69 | 73 | 20 | 70 | 72 | 6F | 67 | 72 | 61 | 6D | 20 | LÍ!This program |
| A0h: | 63 | 61 | 6E | 6E | 6F | 74 | 20 | 62 | 65 | 20 | 72 | 75 | 6E | 20 | 69 | 6E | cannot be run in |
| B0h: | 20 | 44 | 4F | 53 | 20 | 6D | 6F | 64 | 65 | 2E | 0D | 0D | 0A | 24 | 00 | 00 | DOS mode....$.. |
| C0h: | 00 | 00 | 00 | 00 | 00 | 50 | 45 | 00 | 00 | 4C | 01 | 04 | 00 | F0 | 09 | 74 | .....PE..L...ð.t |
| D0h: | 5A | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | E0 | 00 | 0E | 01 | 0B | 01 | 06 | Z.........à..... |
| E0h: | 00 | 00 | 98 | 10 | 00 | 00 | 12 | 00 | 00 | 00 | 00 | 00 | 00 | 8E | B7 | 10 | ..˜..........Ž·. |
| F0h: | 00 | 00 | 20 | 00 | 00 | 00 | C0 | 10 | 00 | 00 | 00 | 40 | 00 | 00 | 20 | 00 | .. ...À....@.. . |

CVE-2015-2545  CVE-2017-0261 %N&%N

&/Nv F k

7-y -%NG\ BADNEWS 3+G

XP

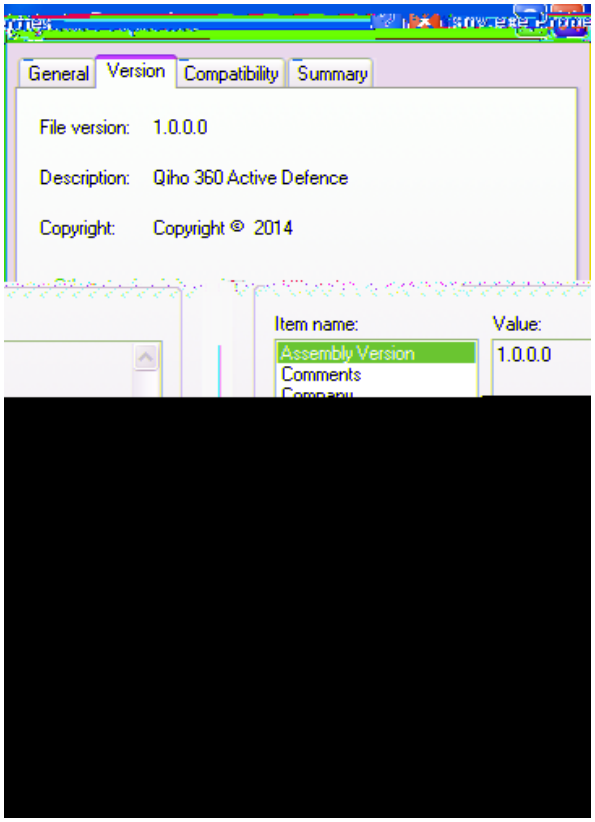


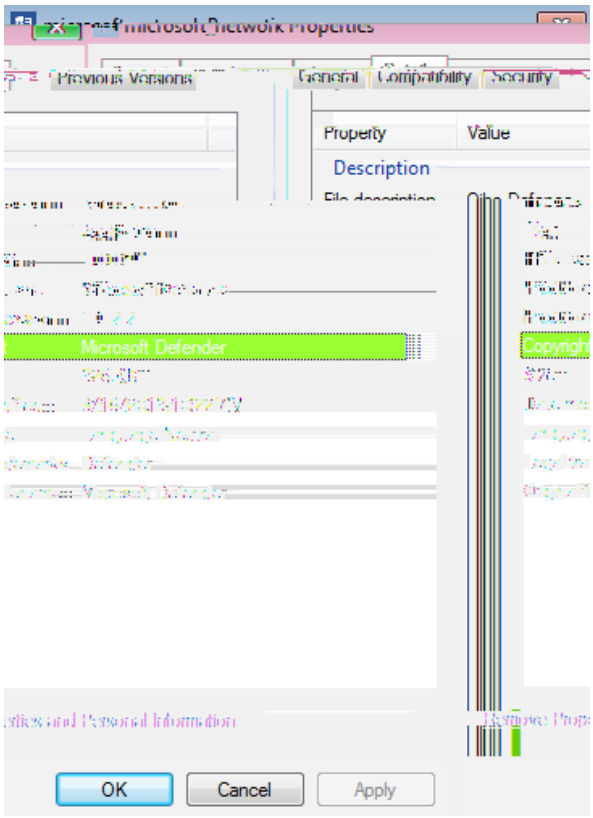

QuasarRAT  BADNEWS

/

A [illegible] B [illegible] QuasarRAT

1. [illegible] Qiho 360 1y



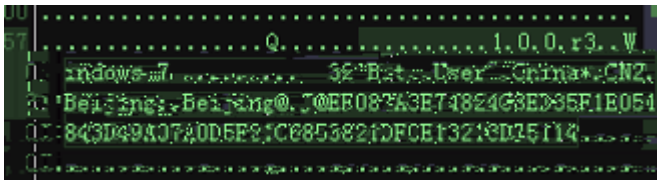



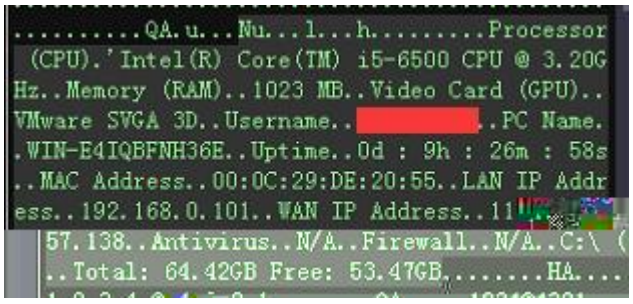
维纳星辰
www.venusdc.com.cn



6. 0> 6fLö C&C








C BADNEWS

1.

%PROGRAMDATA%\Microsoft\DeviceSync\VMwareCplLauncher.exe
%PROGRAMDATA%\Microsoft\DeviceSync\vmtools.dll
%PROGRAMDATA%\Microsoft\DeviceSync\MSBuild.exe

VMwareCplLauncher.exe vmtools.dll




o¢¤` PÍÚÁPA x à ã ä s @ Å ! ’ Î ¶




7. [illegible] dat

8. [illegible] dat [illegible] AES [illegible] +base64 5F.1[illegible]

[illegible] v [illegible] F 1 [illegible] . [illegible] 5 F . 1 [illegible]
\e3e7e71a0b28b5e96cc492e636722f73\4sVKAOvu3D\UYEfgEpXAOE.php

[illegible]

!

[illegible]

brokings.org
crazywomen-dating.com
ifenngnews.com
209.58.185.37
mail.ifenngnews.com
chinapolicyanalysis.org

C&C 
94.242.249.203
209.58.183.33

VenusEye H

Locky

18

Sage 2.0

18 Office

