SILIVACCINE

NORTH KOREA'S WEAPON OF MASS DETECTION

Check Point
SOFTWARE TECHNOLOGIES LTD.

ABOUT US

@_marklech_ @kajilot

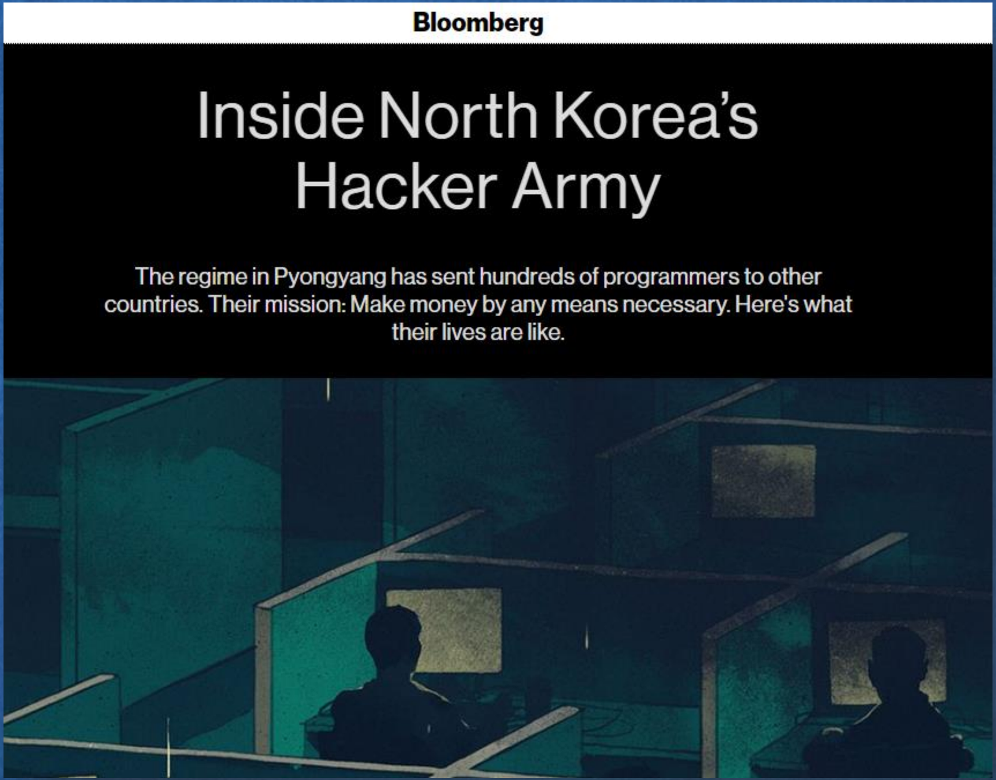
MARK LECHTIK MICHAEL KAJILOTI

CAPTIALIST PIG RESEARCHERS FROM THE MIDDLE EAST

who work at:

Check Point
SOFTWARE TECHNOLOGIES LTD.

THE STORY BEGINS WITH …

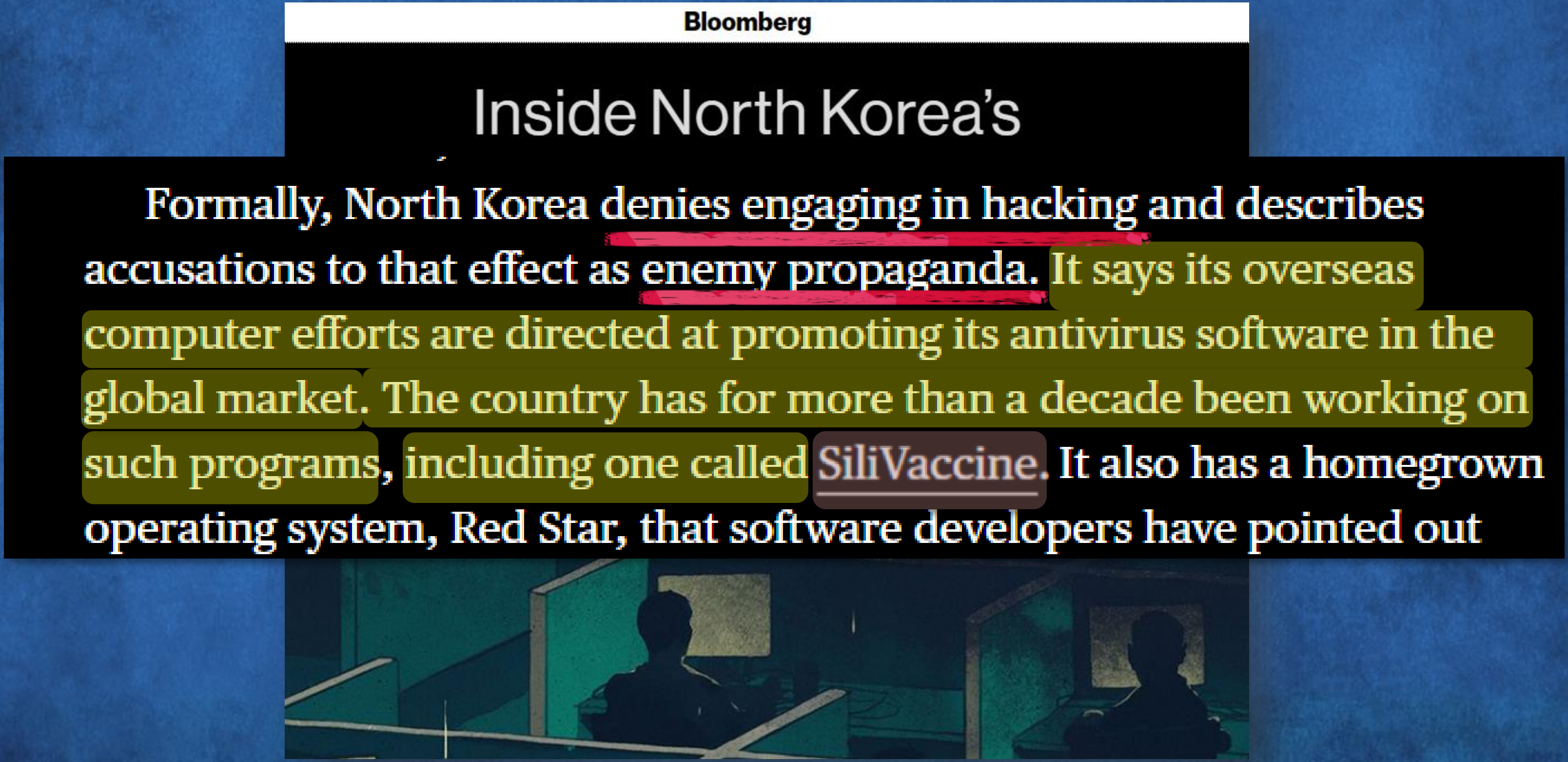


Bloomberg

Inside North Korea's Hacker Army

The regime in Pyongyang has sent hundreds of programmers to other countries. Their mission: Make money by any means necessary. Here's what their lives are like.

THE STORY BEGINS WITH …



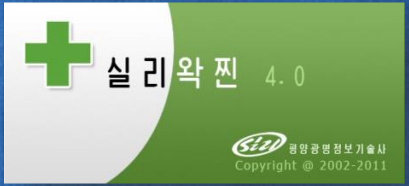
Bloomberg

Inside North Korea's

Formally, North Korea denies engaging in hacking and describes accusations to that effect as enemy propaganda. It says its overseas computer efforts are directed at promoting its antivirus software in the global market. The country has for more than a decade been working on such programs, including one called SiliVaccine. It also has a homegrown operating system, Red Star, that software developers have pointed out

WHAT IS SILIVACCINE?

- anti-virus developed and used exclusively in north korea
- very rare and hard to find outside the DPRK
- actively developed since 2003
- the version we researched is 4.0 – from 2013
  - we are in possession of another one from 2005



실리왁찐 4.0

평양광명정보기술사

Copyright @ 2002-2011

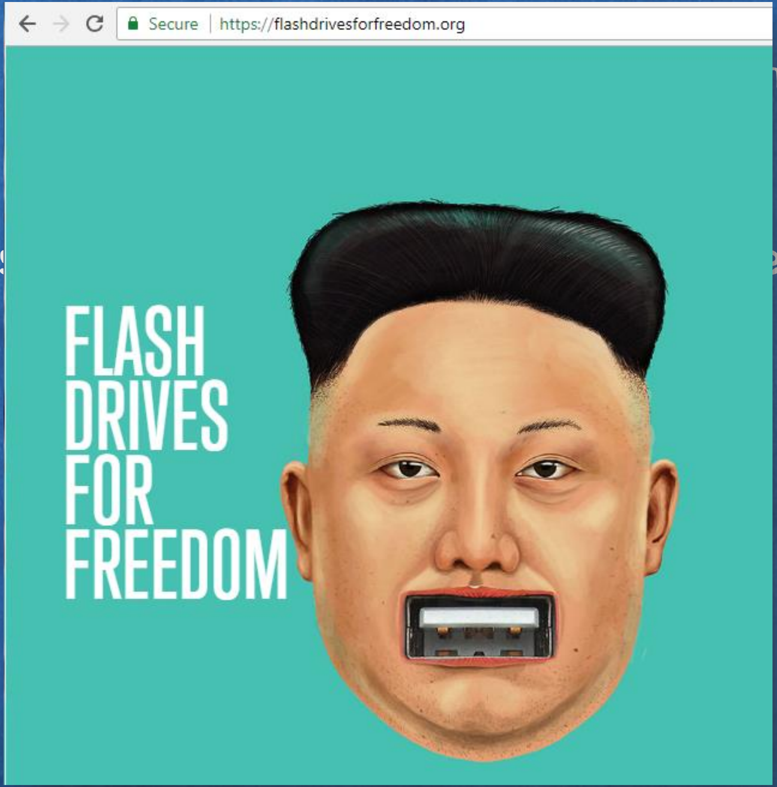
NORTH KOREAN AV?

- there is no internet for citizens in the **DPRK**, only intranet
  - so why use an anti-virus?

- possibly, used to protect against smuggled media

NORTH KOREAN AV?

- there is no
  - so why
- possibly, us



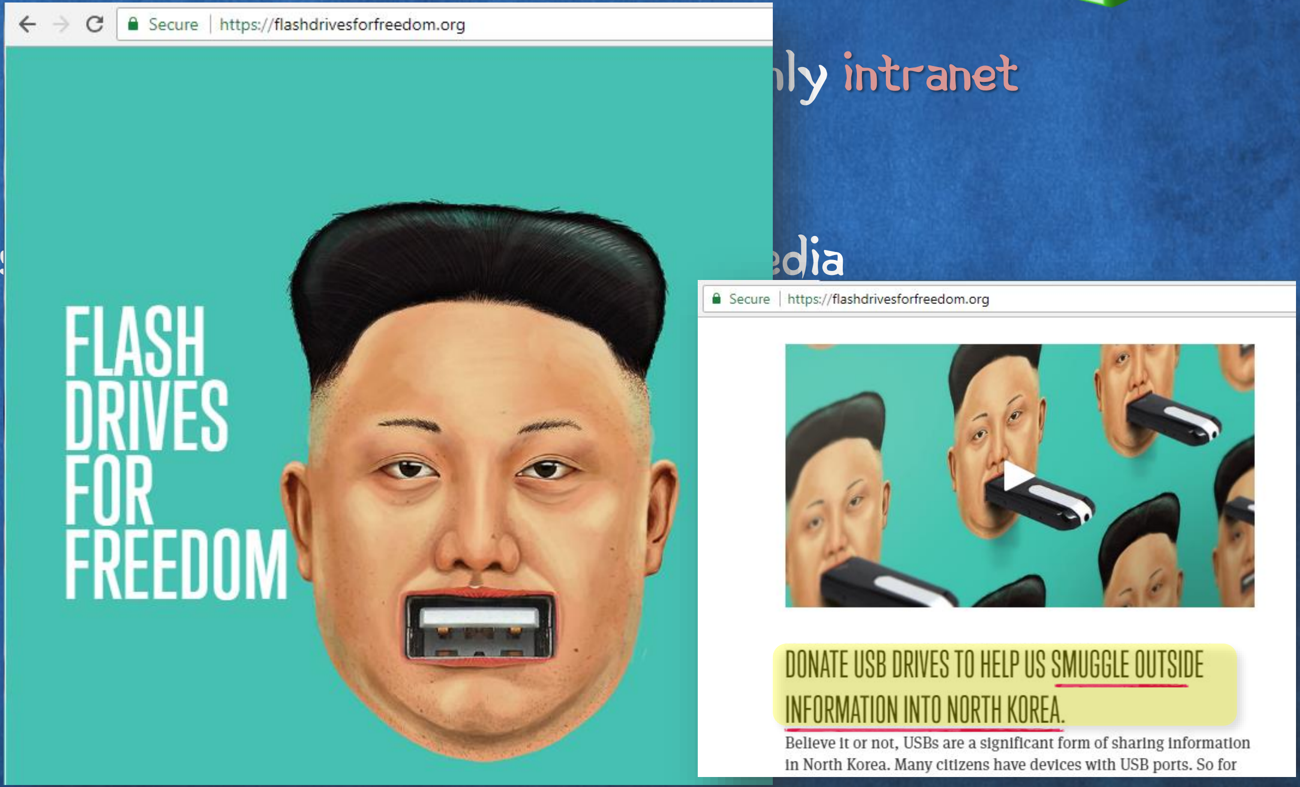
Secure | https://flashdrivesforfreedom.org

nly intranet

edia

NORTH KOREAN AV?

- there is no … nly intranet
  - so why
- possibly, us … edia



Secure | https://flashdrivesforfreedom.org

FLASH DRIVES FOR FREEDOM

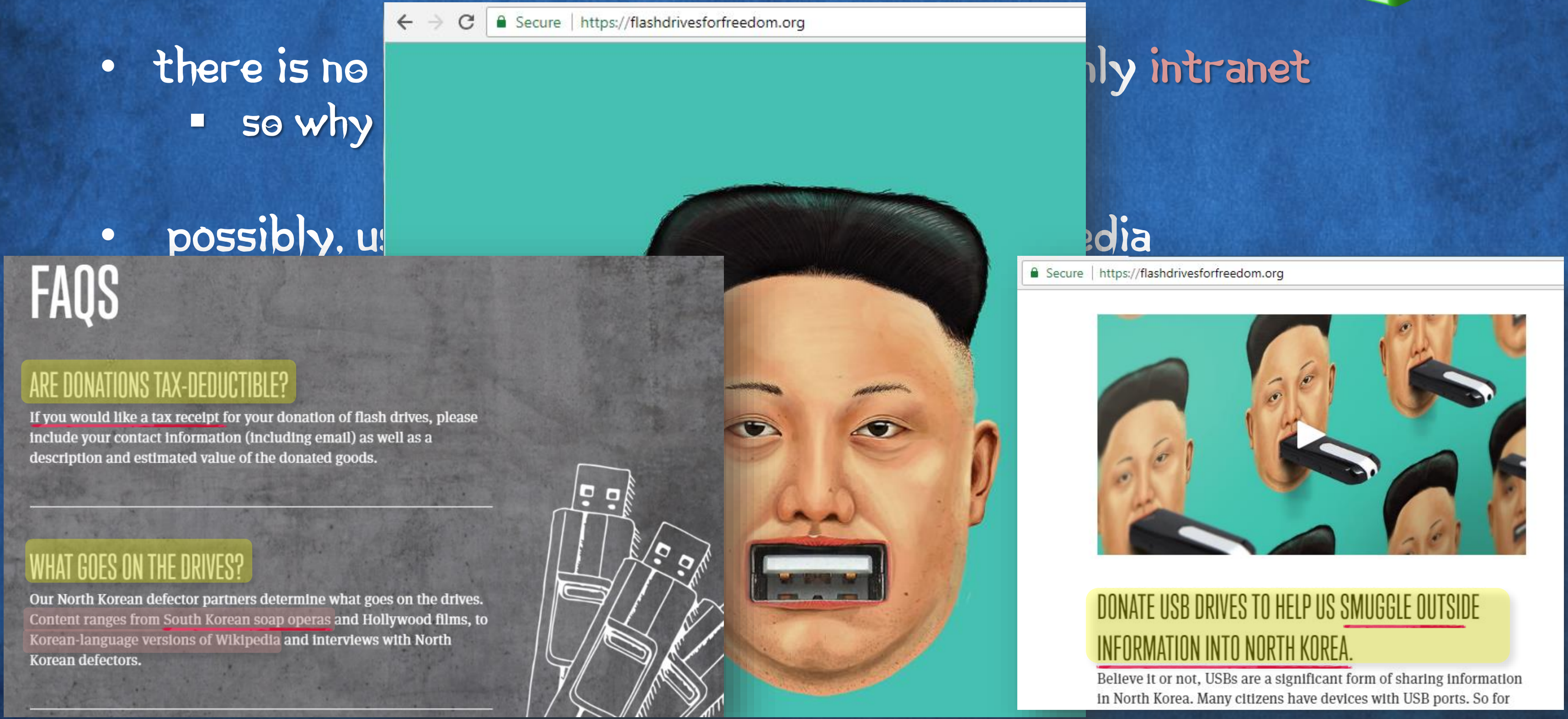
Secure | https://flashdrivesforfreedom.org

DONATE USB DRIVES TO HELP US SMUGGLE OUTSIDE INFORMATION INTO NORTH KOREA.

Believe it or not, USBs are a significant form of sharing information in North Korea. Many citizens have devices with USB ports. So for

NORTH KOREAN AV?

- there is no nly intranet
  - so why
- possibly, u edia



Secure | https://flashdrivesforfreedom.org

FAQS

ARE DONATIONS TAX-DEDUCTIBLE?

If you would like a tax receipt for your donation of flash drives, please include your contact information (including email) as well as a description and estimated value of the donated goods.

WHAT GOES ON THE DRIVES?

Our North Korean defector partners determine what goes on the drives. Content ranges from South Korean soap operas and Hollywood films, to Korean-language versions of Wikipedia and interviews with North Korean defectors.

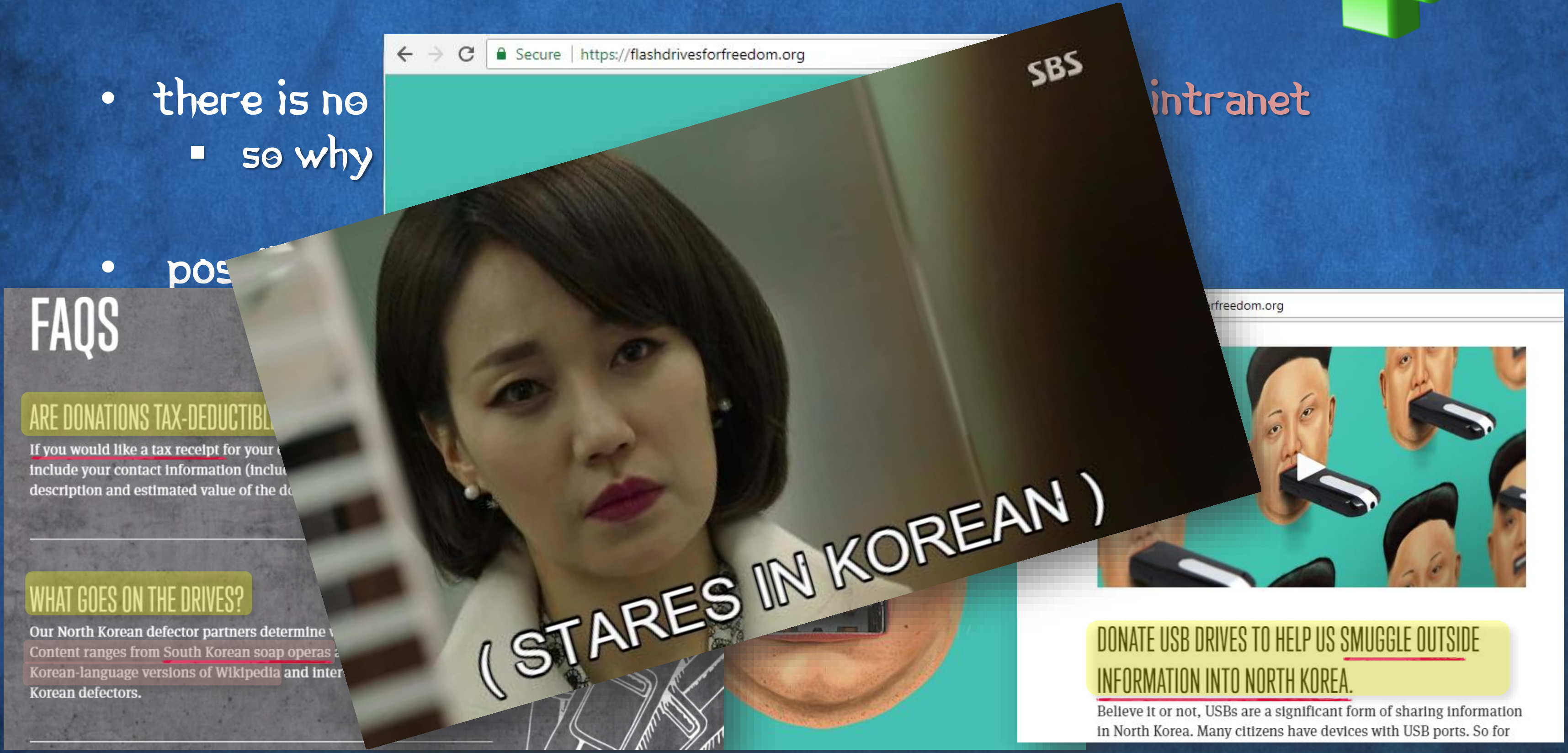
Secure | https://flashdrivesforfreedom.org

DONATE USB DRIVES TO HELP US SMUGGLE OUTSIDE INFORMATION INTO NORTH KOREA.

Believe it or not, USBs are a significant form of sharing information in North Korea. Many citizens have devices with USB ports. So for

NORTH KOREAN AV?

- there is no intranet
  - so why
- pos



FAQS

ARE DONATIONS TAX-DEDUCTIBL

If you would like a tax receipt for your
include your contact information (inclu
description and estimated value of the d

WHAT GOES ON THE DRIVES?

Our North Korean defector partners determine
Content ranges from South Korean soap operas a
Korean-language versions of Wikipedia and inter
Korean defectors.

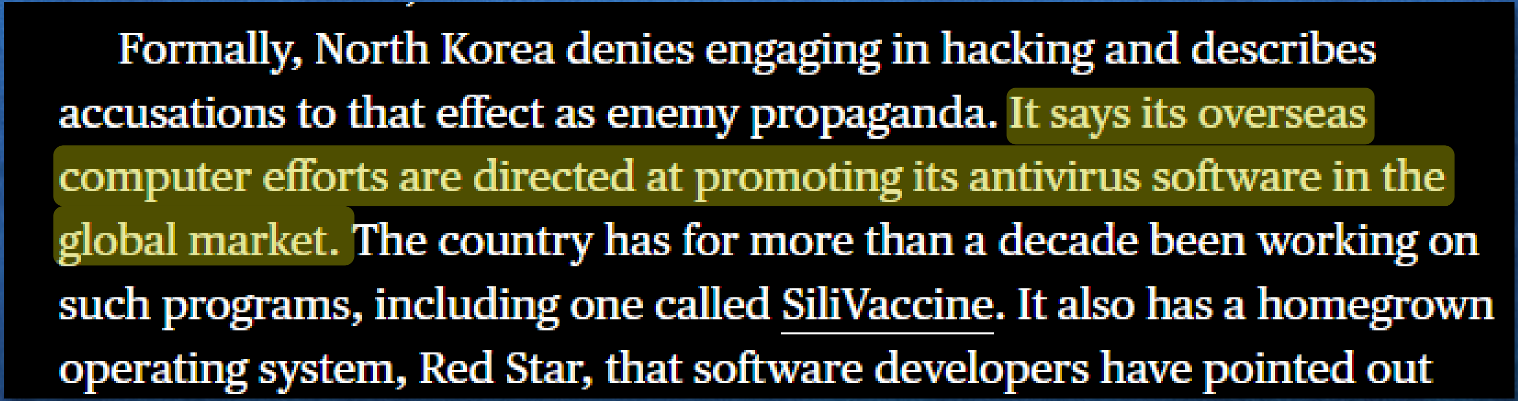
DONATE USB DRIVES TO HELP US SMUGGLE OUTSIDE INFORMATION INTO NORTH KOREA.

Believe it or not, USBs are a significant form of sharing information in North Korea. Many citizens have devices with USB ports. So for

NORTH KOREAN AV?

- there is no internet for citizens in the **DPRK**, only intranet
  - so why use an anti-virus?

- another option - meant to be sold as a product to other countries

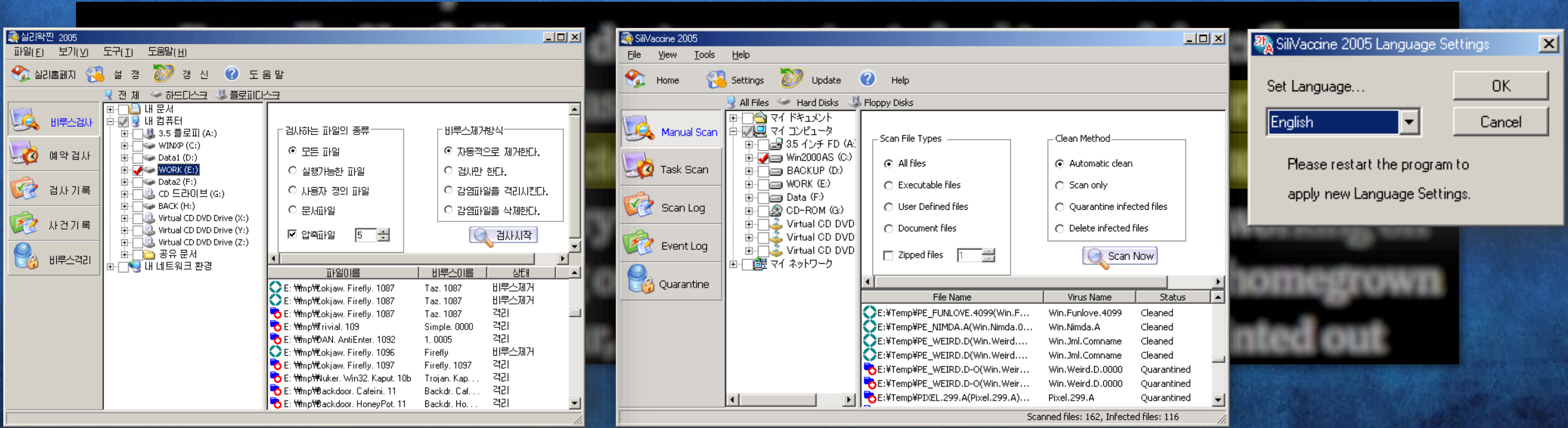


Formally, North Korea denies engaging in hacking and describes accusations to that effect as enemy propaganda. It says its overseas computer efforts are directed at promoting its antivirus software in the global market. The country has for more than a decade been working on such programs, including one called SiliVaccine. It also has a homegrown operating system, Red Star, that software developers have pointed out

NORTH KOREAN AV?

- there is no internet for citizens in the DPRK, only intranet
  - so why use an anti-virus?

- in fact, the 2005 version was written both in korean and english
  - possible evidence that it was aimed towards global markert



검사하는 파일의 종류
- ● 모든 파일
- ○ 실행가능한 파일
- ○ 사용자 정의 파일
- ○ 문서파일
- ☑ 압축파일 5

비루스제거방식
- ● 자동적으로 제거한다.
- ○ 검사만 한다.
- ○ 감염파일을 격리시킨다.
- ○ 감염파일을 삭제한다.

파일이름	비루스이름	상태
E: ₩mp₩Lokjaw. Firefly. 1087	Taz. 1087	비루스제거
E: ₩mp₩Lokjaw. Firefly. 1087	Taz. 1087	비루스제거
E: ₩mp₩Lokjaw. Firefly. 1087	Taz. 1087	격리
E: ₩mp₩Trivial. 109	Simple. 0000	격리
E: ₩mp₩DAN. AntiEnter. 1092	1. 0005	격리
E: ₩mp₩Lokjaw. Firefly. 1096	Firefly	비루스제거
E: ₩mp₩Lokjaw. Firefly. 1097	Firefly. 1097	격리
E: ₩mp₩Nuker. Win32. Kaput. 10b	Trojan. Kap. . .	격리
E: ₩mp₩Backdoor. Cafeini. 11	Backdr. Caf. . .	격리
E: ₩mp₩Backdoor. HoneyPot. 11	Backdr. Ho. . .	격리

Scan File Types
- ● All files
- ○ Executable files
- ○ User Defined files
- ○ Document files
- □ Zipped files 1

Clean Method
- ● Automatic clean
- ○ Scan only
- ○ Quarantine infected files
- ○ Delete infected files

File Name	Virus Name	Status
E:¥Temp¥PE_FUNLOVE.4099(Win.F...	Win.Funlove.4099	Cleaned
E:¥Temp¥PE_NIMDA.A(Win.Nimda.0...	Win.Nimda.A	Cleaned
E:¥Temp¥PE_WEIRD.D(Win.Weird....	Win.Jml.Comname	Cleaned
E:¥Temp¥PE_WEIRD.D(Win.Weird....	Win.Jml.Comname	Cleaned
E:¥Temp¥PE_WEIRD.D-O(Win.Weir...	Win.Weird.D.0000	Quarantined
E:¥Temp¥PE_WEIRD.D-O(Win.Weir...	Win.Weird.D.0000	Quarantined
E:¥Temp¥PIXEL.299.A(Pixel.299.A)...	Pixel.299.A	Quarantined

Scanned files: 162, Infected files: 116

Set Language... English

Please restart the program to apply new Language Settings.

HOW DID WE OBTAIN IT?

- bloomberg article links to a blog post by martyn williams
- he got the av by e-mail as a potential story lead from an unknown user
- agreed to share it with us for deeper analysis
- thank you martyn!

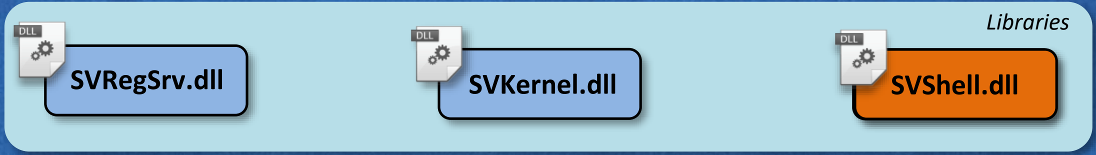
@martyn_williams

MOTIVATION

- understand how the program is built
- observe some of north korea's coding and engineering practices
- find any abnormal behavior \ "undocumented" features
- find potential backdoor

anti-virus components overview

Software Architecture

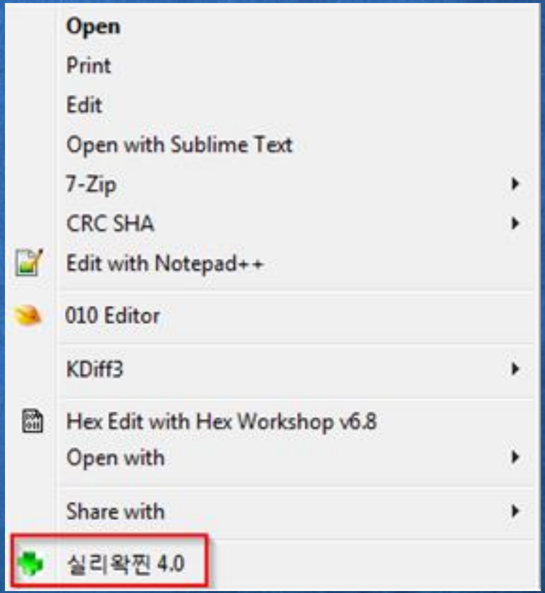


Libraries

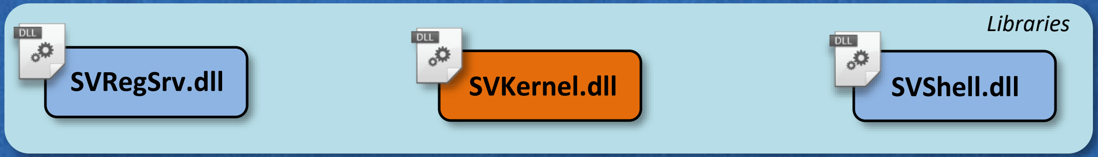
SVRegSrv.dll

SVKernel.dll

SVShell.dll

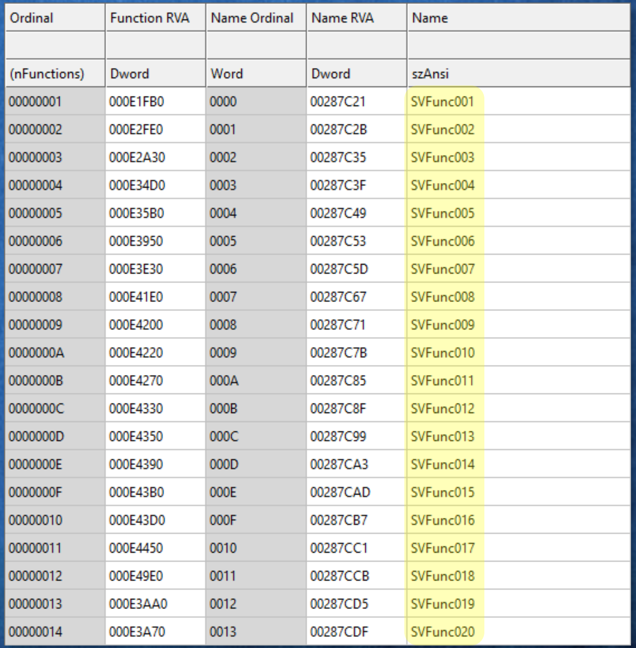


SOFTWARE ARCHITECTURE



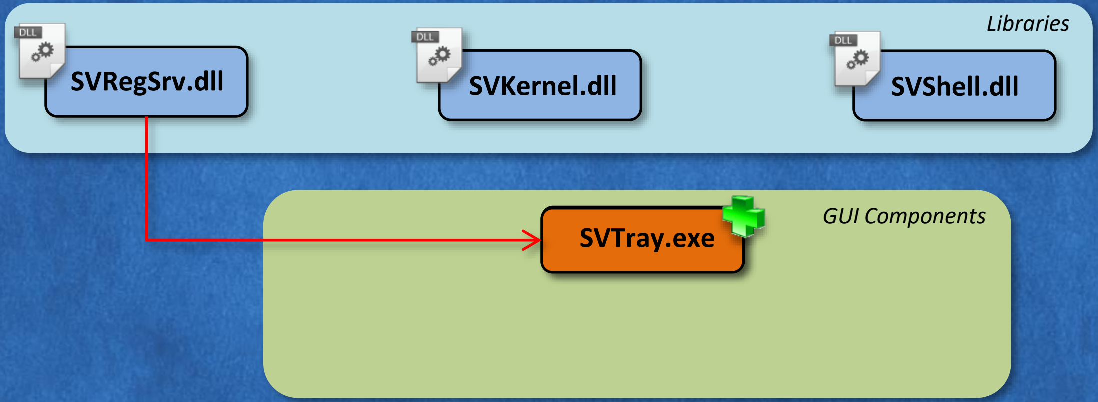
Libraries

- file scanning engine
- contains core functionality to detect if a file is malicious or not
- exposes 20 export functions
- verdict is based on search of malicious patterns

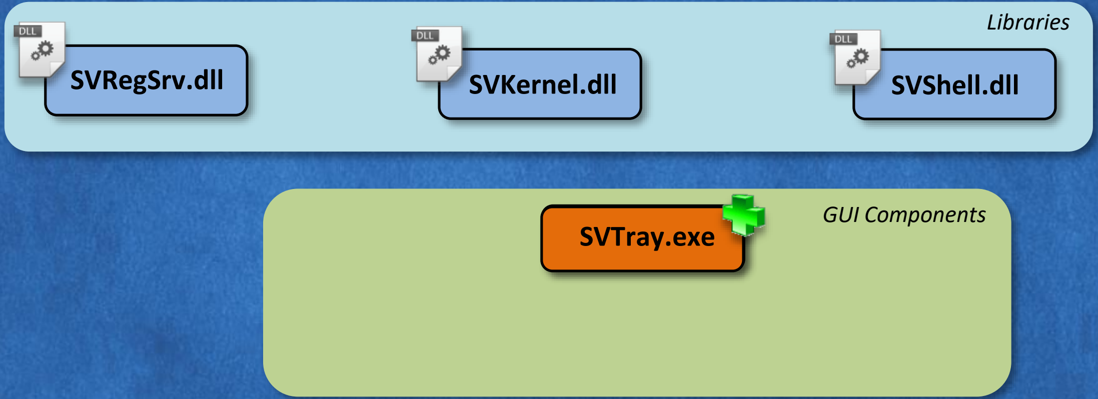


Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	000E1FB0	0000	00287C21	SVFunc001
00000002	000E2FE0	0001	00287C2B	SVFunc002
00000003	000E2A30	0002	00287C35	SVFunc003
00000004	000E34D0	0003	00287C3F	SVFunc004
00000005	000E35B0	0004	00287C49	SVFunc005
00000006	000E3950	0005	00287C53	SVFunc006
00000007	000E3E30	0006	00287C5D	SVFunc007
00000008	000E41E0	0007	00287C67	SVFunc008
00000009	000E4200	0008	00287C71	SVFunc009
0000000A	000E4220	0009	00287C7B	SVFunc010
0000000B	000E4270	000A	00287C85	SVFunc011
0000000C	000E4330	000B	00287C8F	SVFunc012
0000000D	000E4350	000C	00287C99	SVFunc013
0000000E	000E4390	000D	00287CA3	SVFunc014
0000000F	000E43B0	000E	00287CAD	SVFunc015
00000010	000E43D0	000F	00287CB7	SVFunc016
00000011	000E4450	0010	00287CC1	SVFunc017
00000012	000E49E0	0011	00287CCB	SVFunc018
00000013	000E3AA0	0012	00287CD5	SVFunc019
00000014	000E3A70	0013	00287CDF	SVFunc020

Software Architecture



SOFTWARE ARCHITECTURE



Libraries

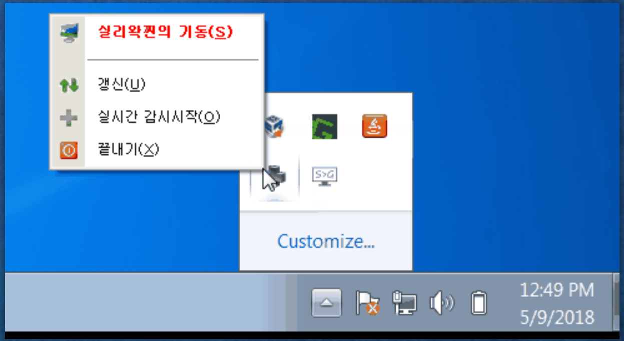
SVRegSrv.dll

SVKernel.dll

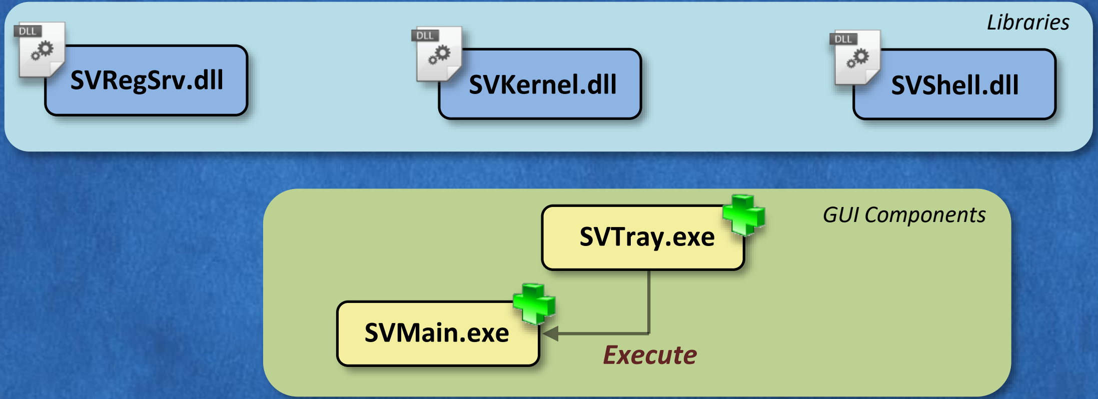
SVShell.dll

GUI Components

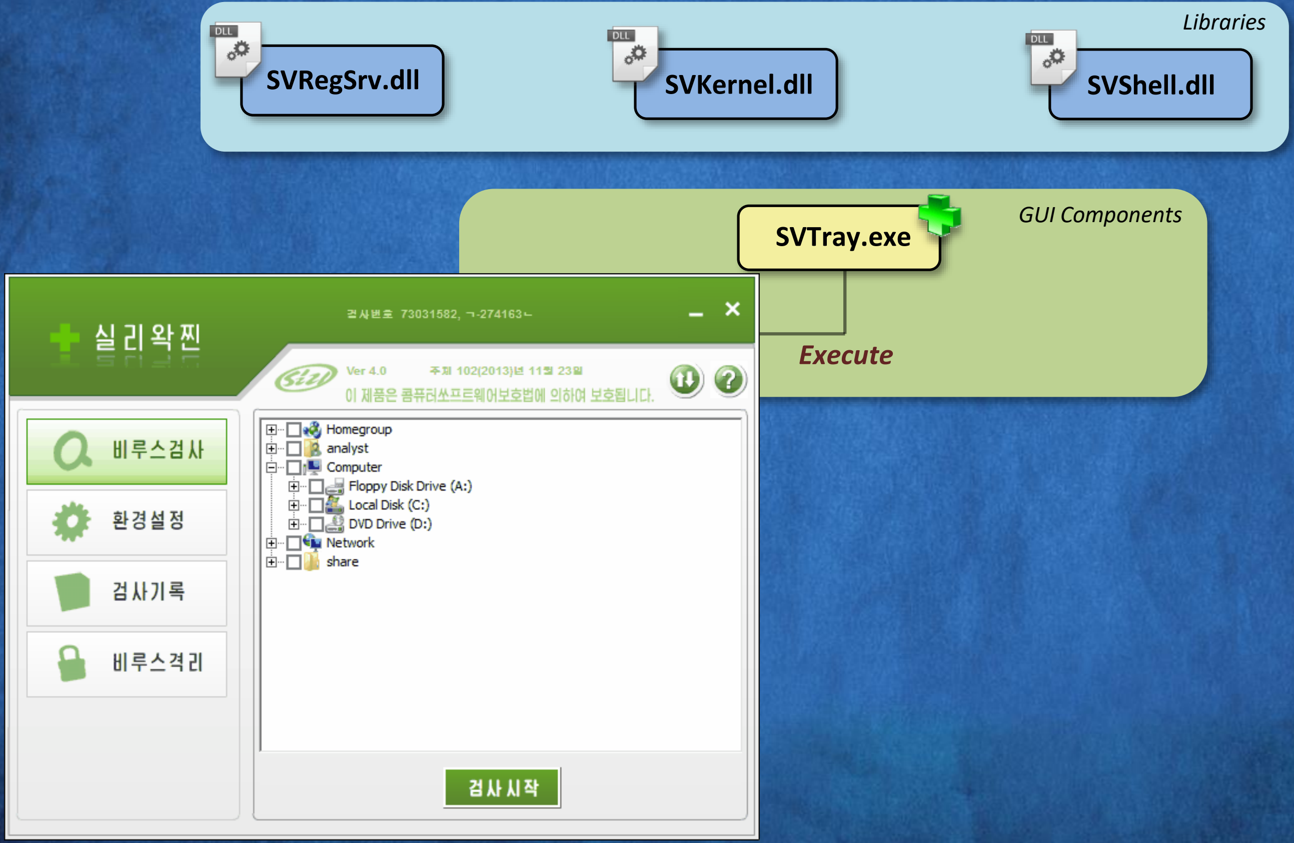
SVTray.exe



Software Architecture



Software Architecture



Libraries

SVRegSrv.dll

SVKernel.dll

SVShell.dll

GUI Components

SVTray.exe

Execute

실리왁찐

검사번호 73031582, ㄱ-274163ㄴ

Ver 4.0 주체 102(2013)년 11월 23일

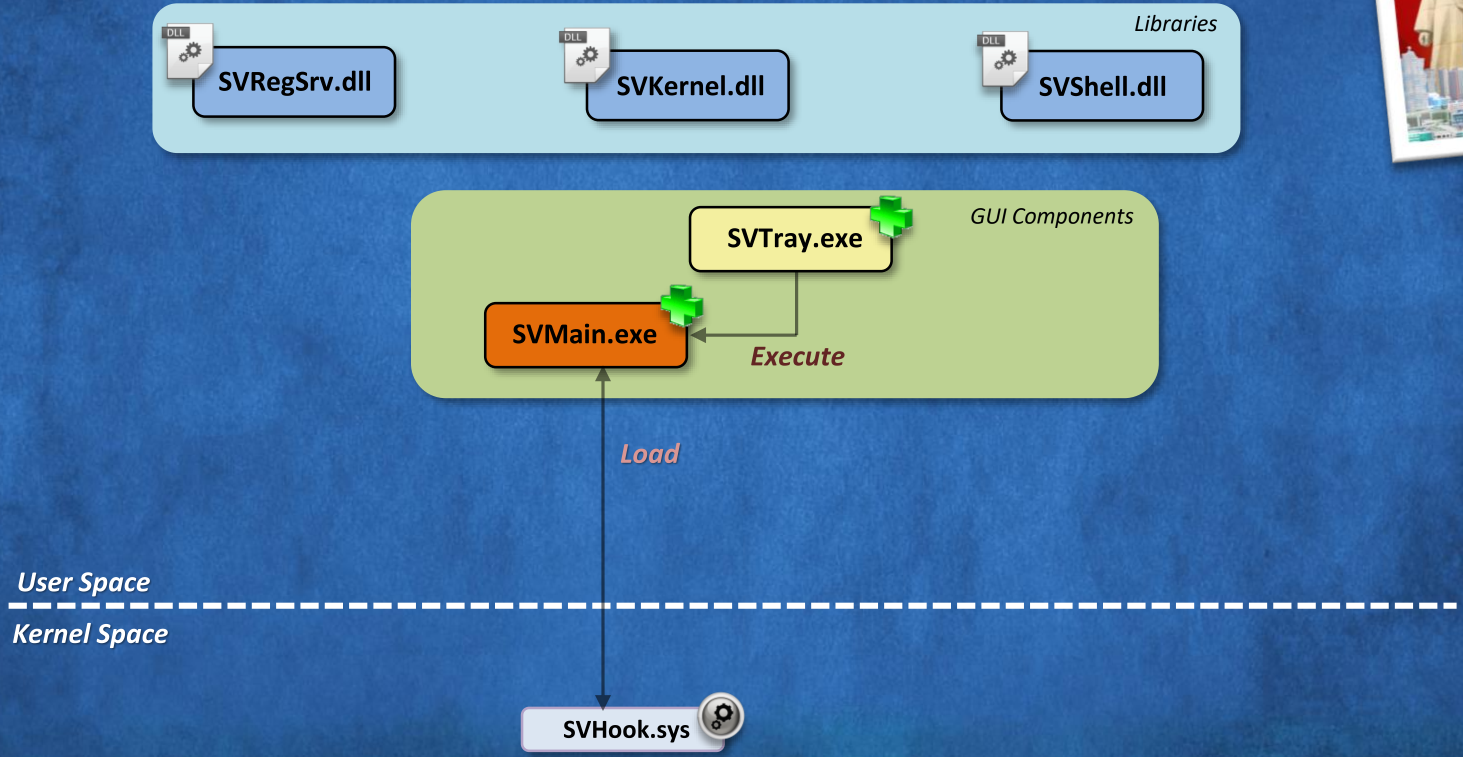
이 제품은 콤퓨터쏘프트웨어보호법에 의하여 보호됩니다.

- 비루스검사
- 환경설정
- 검사기록
- 비루스격리

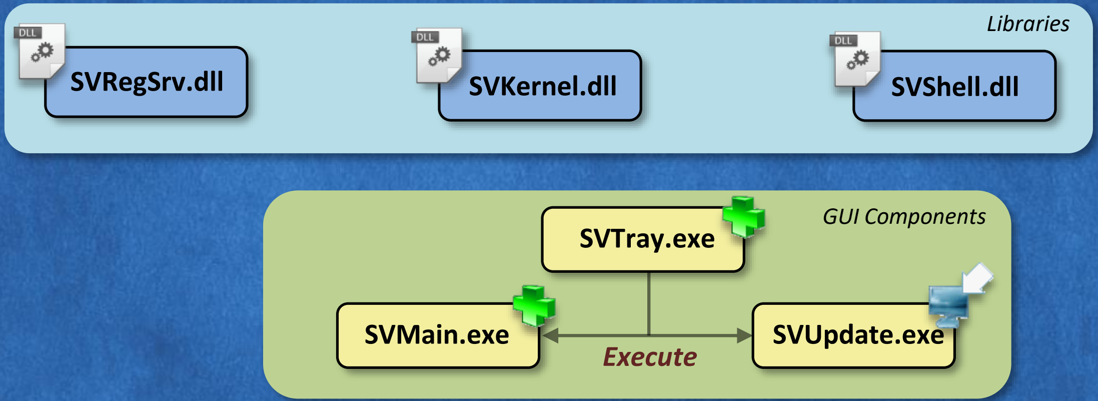
```
⊞ □ Homegroup
⊞ □ analyst
⊟ □ Computer
   ⊞ □ Floppy Disk Drive (A:)
   ⊞ □ Local Disk (C:)
   ⊞ □ DVD Drive (D:)
⊞ □ Network
⊞ □ share
```

검사시작

SOFTWARE ARCHITECTURE



SOFTWARE ARCHITECTURE



Libraries

SVRegSrv.dll

SVKernel.dll

SVShell.dll

GUI Components

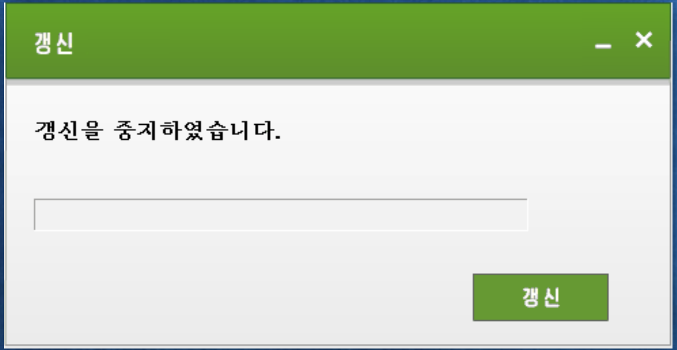
SVTray.exe

SVMain.exe

Execute

SVUpdate.exe

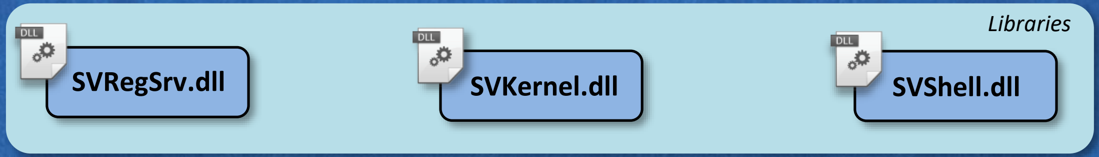
Integrity Checker

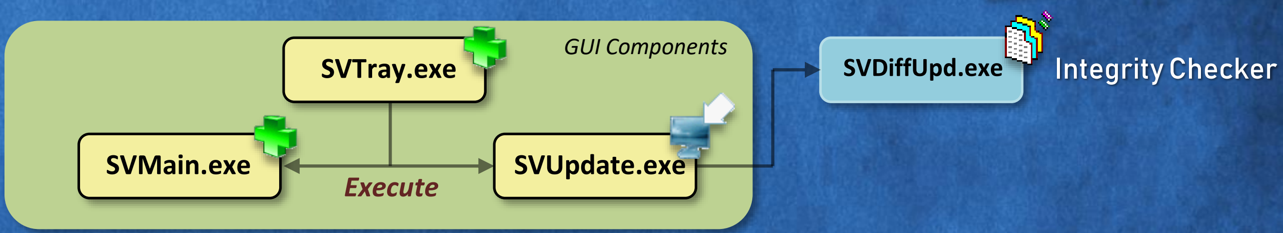


갱신

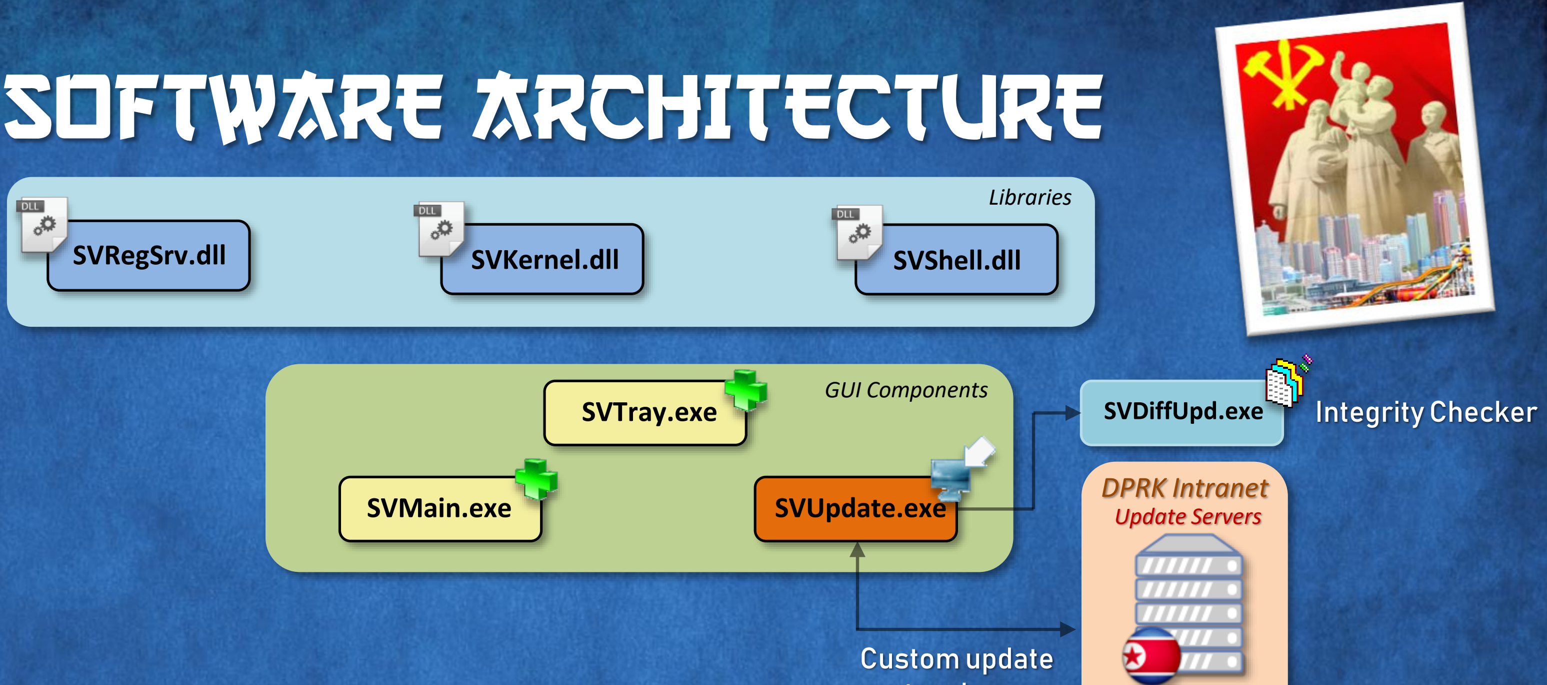
갱신을 중지하였습니다.

SOFTWARE ARCHITECTURE

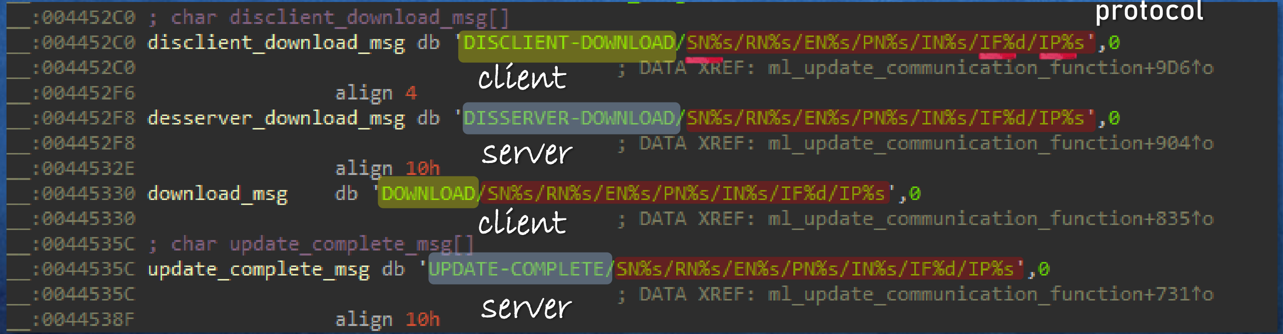




SOFTWARE ARCHITECTURE

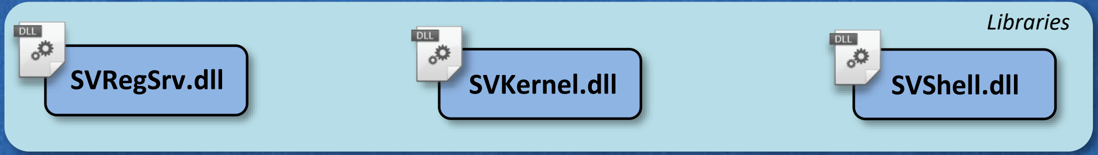


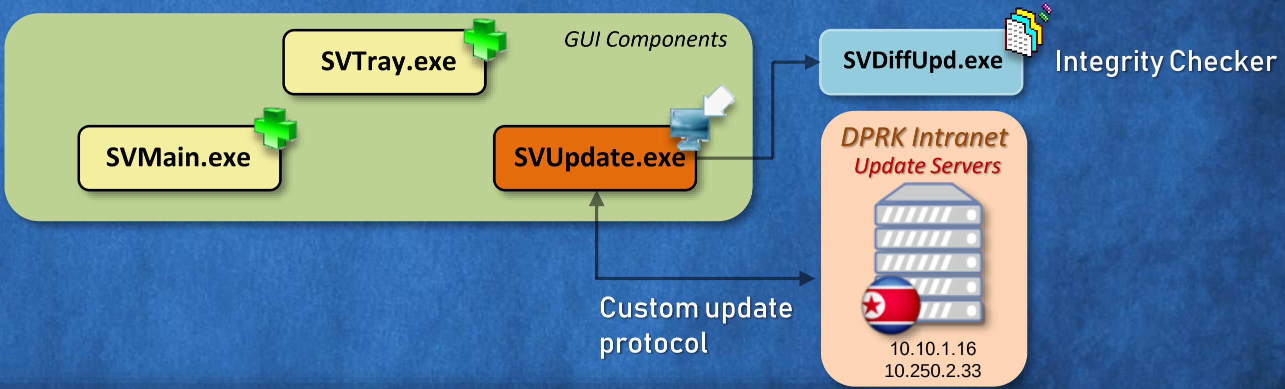
10.10.1.16
10.250.2.33

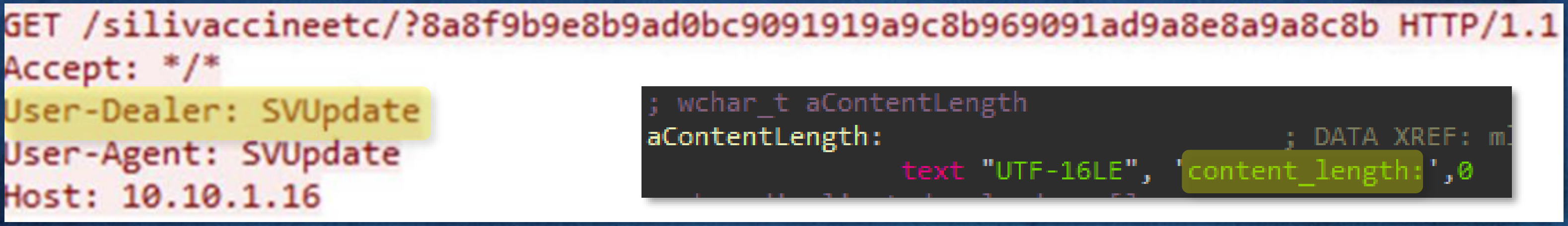


```
:004452C0 ; char disclient_download_msg[]
:004452C0 disclient_download_msg db 'DISCLIENT-DOWNLOAD/SN%s/RN%s/EN%s/PN%s/IN%s/IF%d/IP%s',0
:004452C0                                              ; DATA XREF: ml_update_communication_function+9D6↑o
:004452F6                 align 4
:004452F8 desserver_download_msg db 'DISSERVER-DOWNLOAD/SN%s/RN%s/EN%s/PN%s/IN%s/IF%d/IP%s',0
:004452F8                                              ; DATA XREF: ml_update_communication_function+904↑o
:0044532E                 align 10h
:00445330 download_msg    db 'DOWNLOAD/SN%s/RN%s/EN%s/PN%s/IN%s/IF%d/IP%s',0
:00445330                                              ; DATA XREF: ml_update_communication_function+835↑o
:0044535C ; char update_complete_msg[]
:0044535C update_complete_msg db 'UPDATE-COMPLETE/SN%s/RN%s/EN%s/PN%s/IN%s/IF%d/IP%s',0
:0044535C                                              ; DATA XREF: ml_update_communication_function+731↑o
:0044538F                 align 10h
```

SOFTWARE ARCHITECTURE



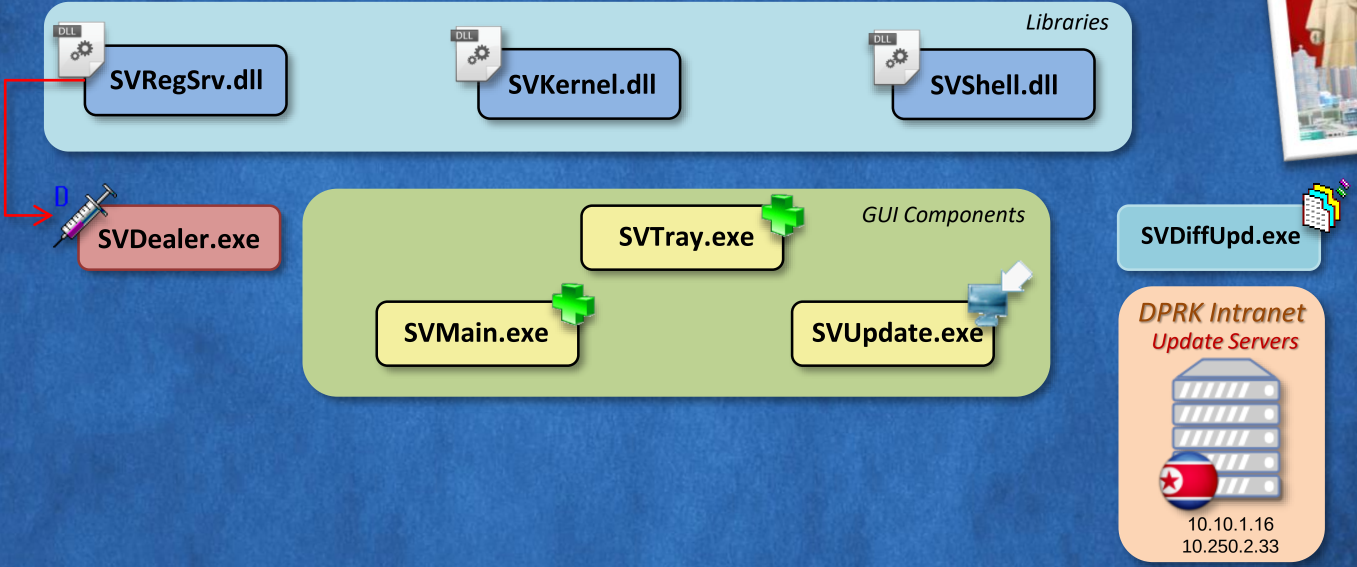




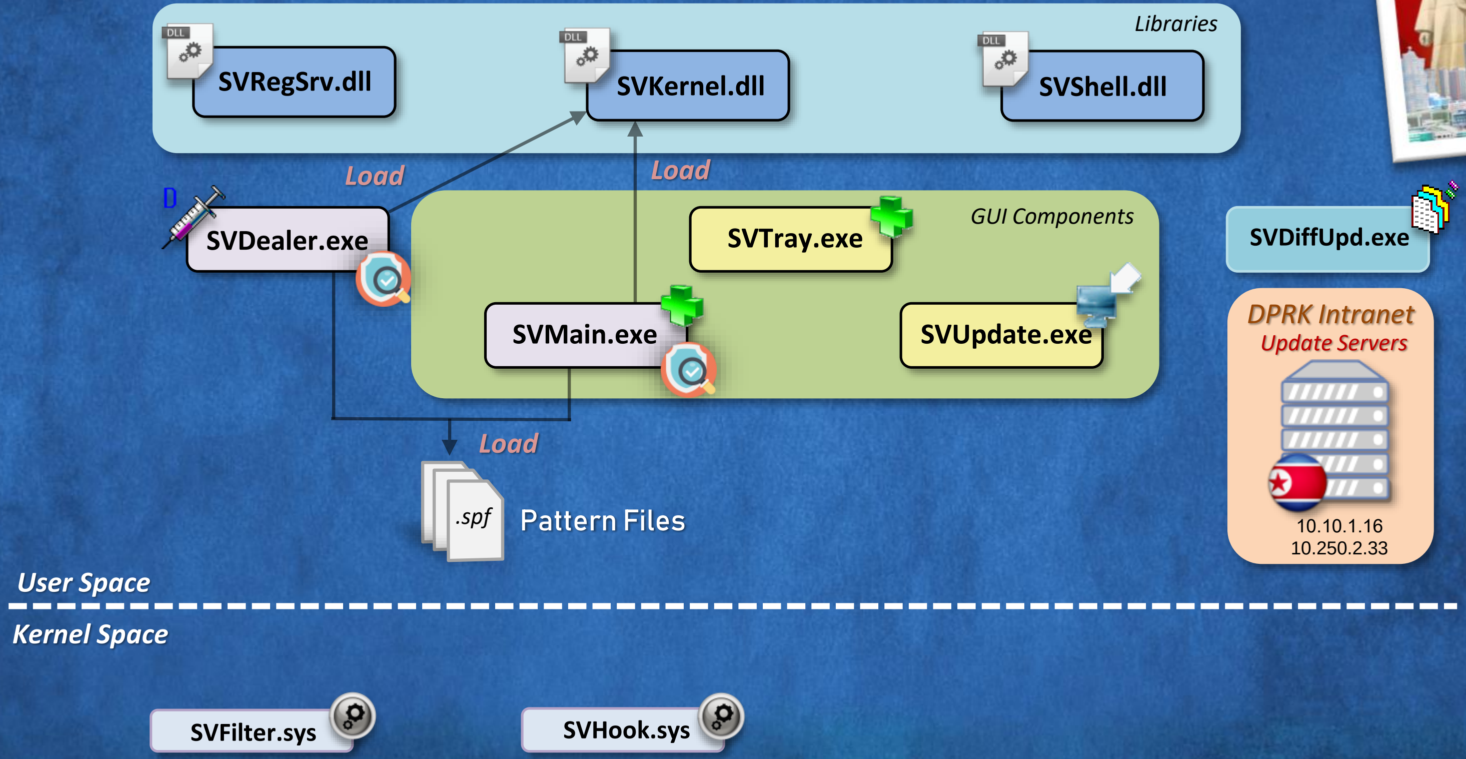
```
GET /silivaccineetc/?8a8f9b9e8b9ad0bc9091919a9c8b969091ad9a8e8a9a8c8b HTTP/1.1
Accept: */*
User-Dealer: SVUpdate
User-Agent: SVUpdate
Host: 10.10.1.16
```

```
; wchar_t aContentLength
aContentLength:                               ; DATA XREF: m
                  text "UTF-16LE", 'content_length:',0
```

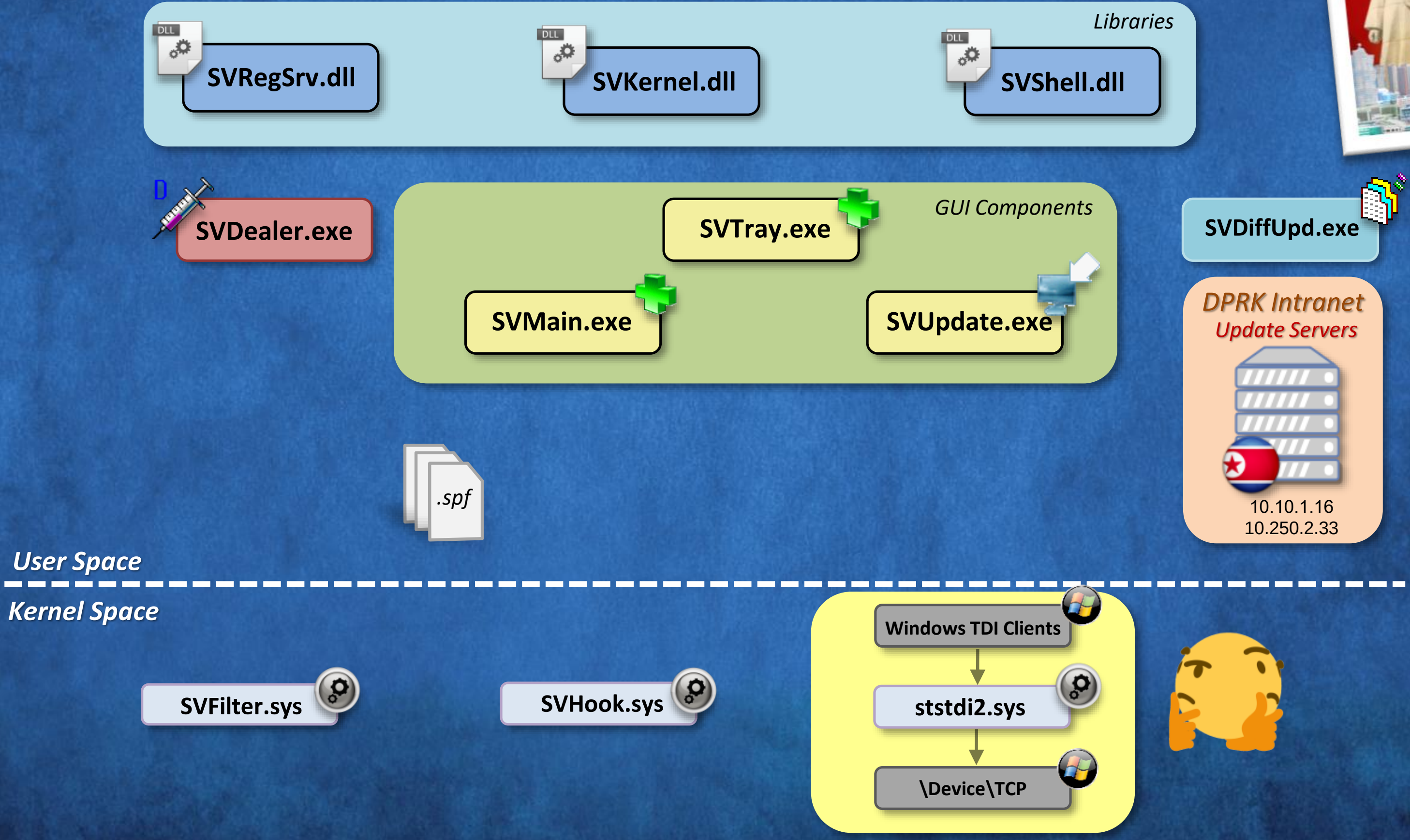
SOFTWARE ARCHITECTURE



SOFTWARE ARCHITECTURE



Software Architecture



Libraries

SVRegSrv.dll

SVKernel.dll

SVShell.dll

SVDealer.exe

GUI Components

SVTray.exe

SVMain.exe

SVUpdate.exe

SVDiffUpd.exe

DPRK Intranet
Update Servers
10.10.1.16
10.250.2.33

.spf

User Space

Kernel Space

SVFilter.sys

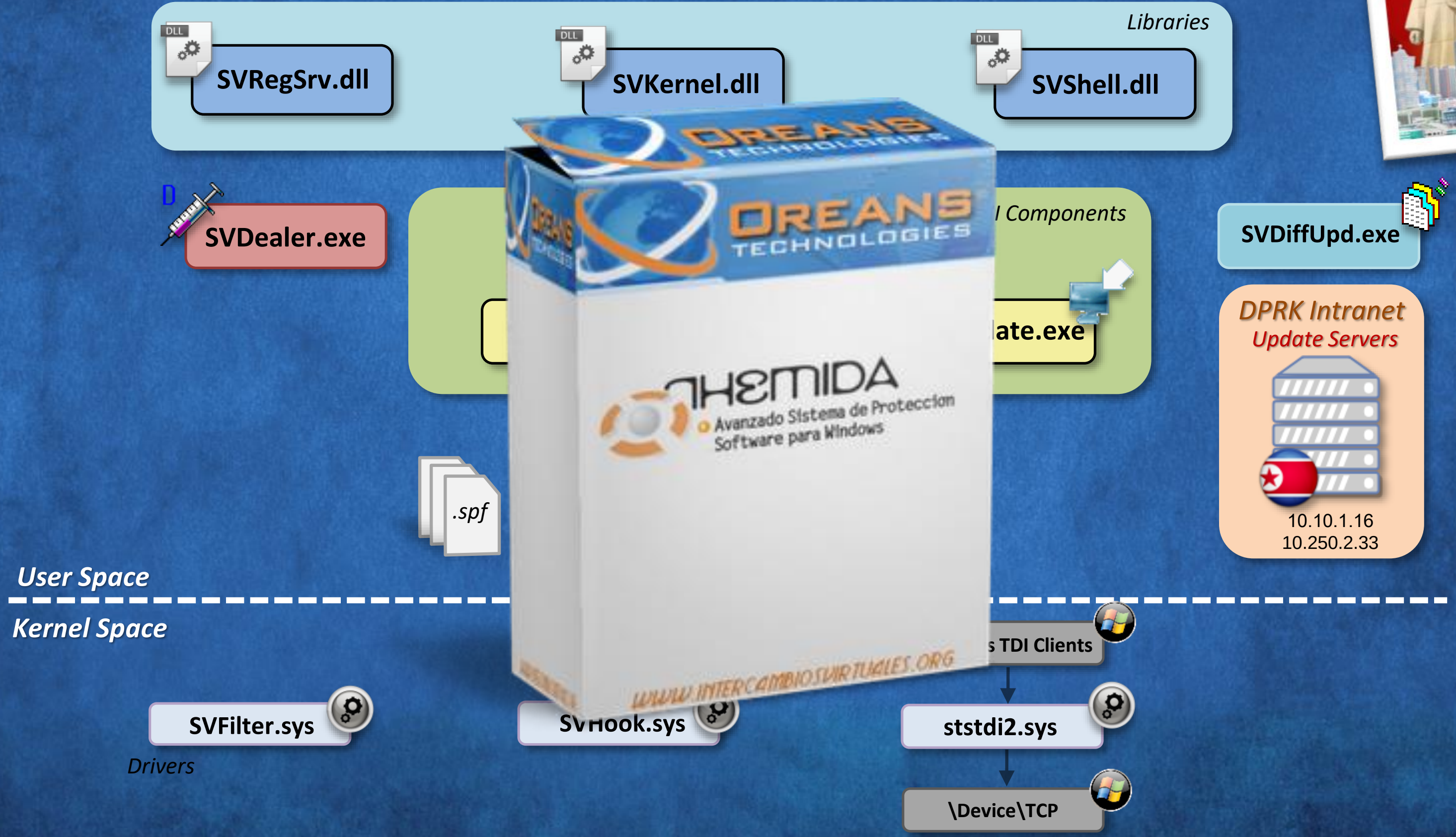
SVHook.sys

Windows TDI Clients

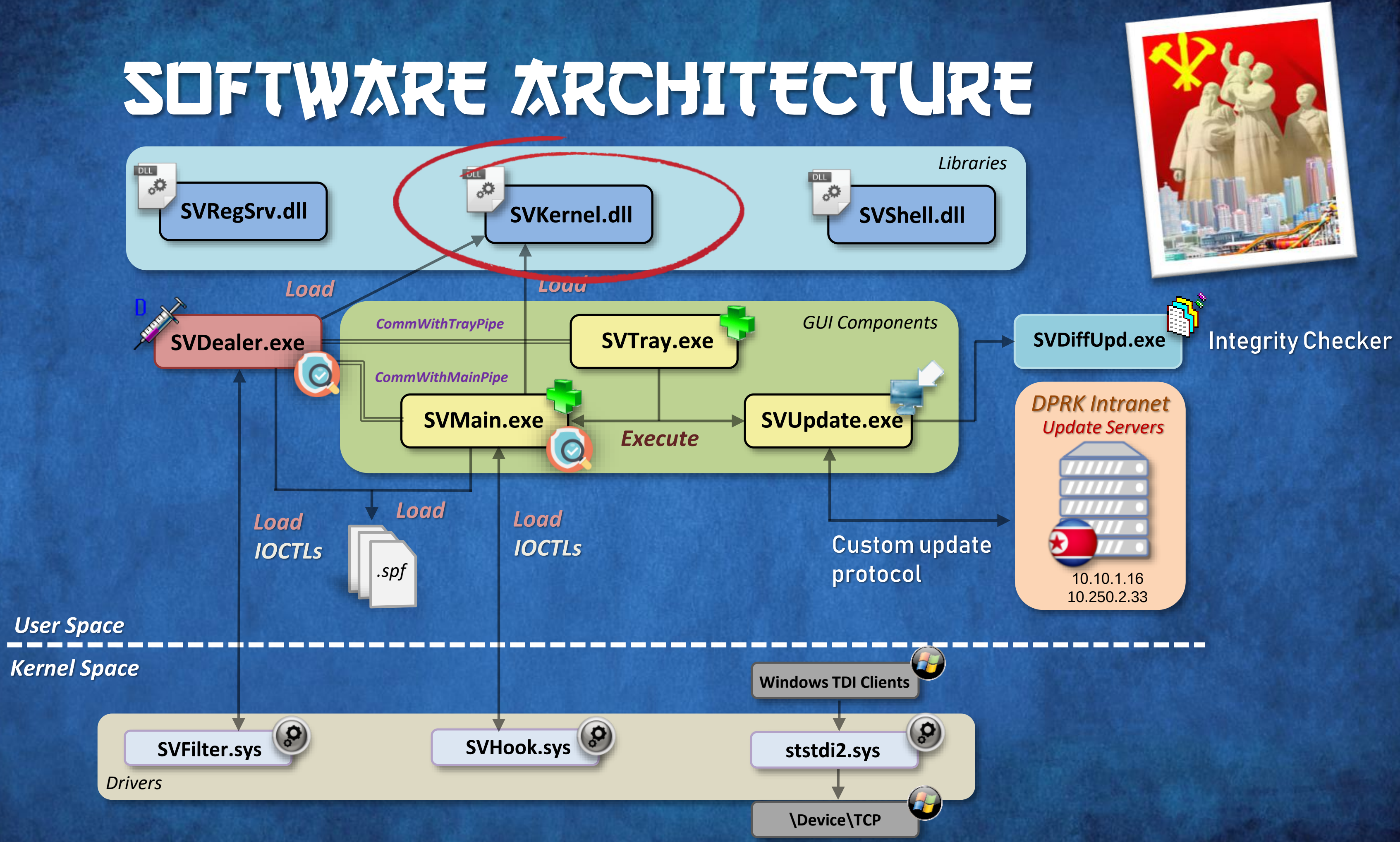
ststdi2.sys

\Device\TCP

SOFTWARE ARCHITECTURE



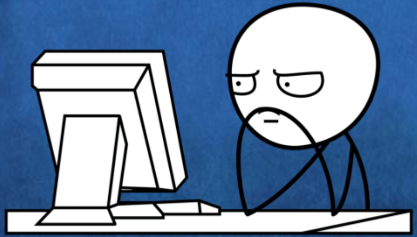
SOFTWARE ARCHITECTURE

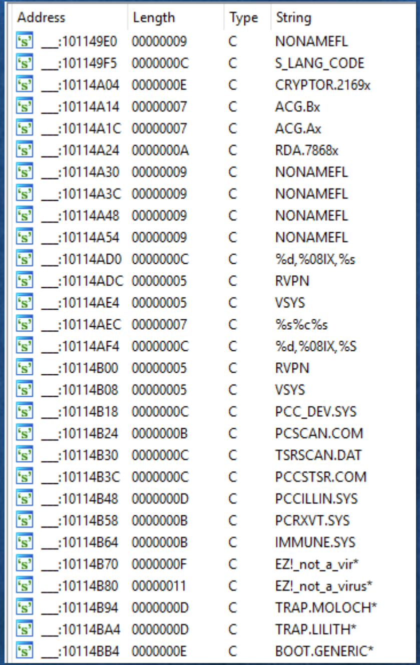


deep dive into svkernel.dll

STRINGS

- we observe some of the strings in svkernel.dll
- simple search of those strings brings us to a file named vsapi32.dll
- file scanning engine! TREND MICRO
- does this mean silivaccine uses a trend micro dll?

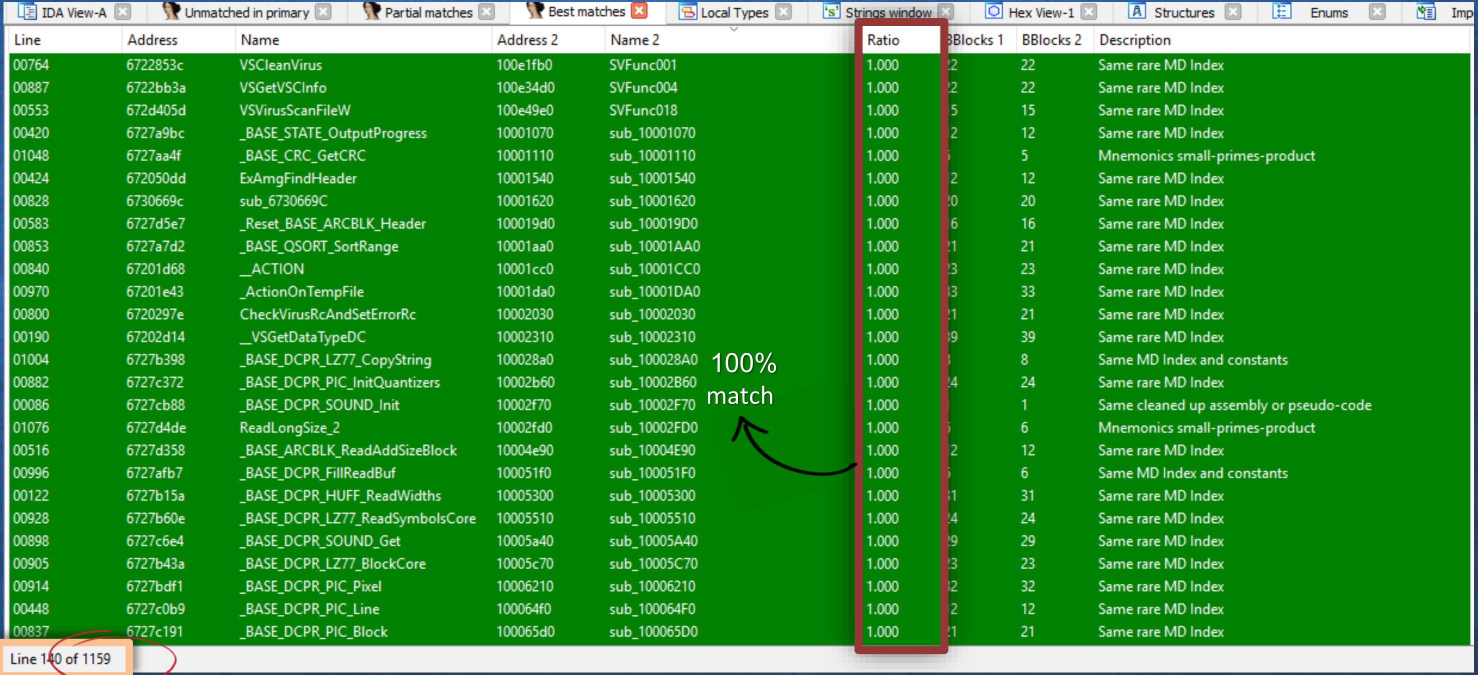




Address	Length	Type	String
___:101149E0	00000009	C	NONAMEFL
___:101149F5	0000000C	C	S_LANG_CODE
___:10114A04	0000000E	C	CRYPTOR.2169x
___:10114A14	00000007	C	ACG.Bx
___:10114A1C	00000007	C	ACG.Ax
___:10114A24	0000000A	C	RDA.7868x
___:10114A30	00000009	C	NONAMEFL
___:10114A3C	00000009	C	NONAMEFL
___:10114A48	00000009	C	NONAMEFL
___:10114A54	00000009	C	NONAMEFL
___:10114AD0	0000000C	C	%d,%08lX,%s
___:10114ADC	00000005	C	RVPN
___:10114AE4	00000005	C	VSYS
___:10114AEC	00000007	C	%s%c%s
___:10114AF4	0000000C	C	%d,%08lX,%S
___:10114B00	00000005	C	RVPN
___:10114B08	00000005	C	VSYS
___:10114B18	0000000C	C	PCC_DEV.SYS
___:10114B24	0000000B	C	PCSCAN.COM
___:10114B30	0000000C	C	TSRSCAN.DAT
___:10114B3C	0000000C	C	PCCSTSR.COM
___:10114B48	0000000D	C	PCCILLIN.SYS
___:10114B58	0000000B	C	PCRXVT.SYS
___:10114B64	0000000B	C	IMMUNE.SYS
___:10114B70	0000000F	C	EZ!_not_a_vir*
___:10114B80	00000011	C	EZ!_not_a_virus*
___:10114B94	0000000D	C	TRAP.MOLOCH*
___:10114BA4	0000000D	C	TRAP.LILITH*
___:10114BB4	0000000E	C	BOOT.GENERIC*

CODE SIMILARITY

TREND MICRO

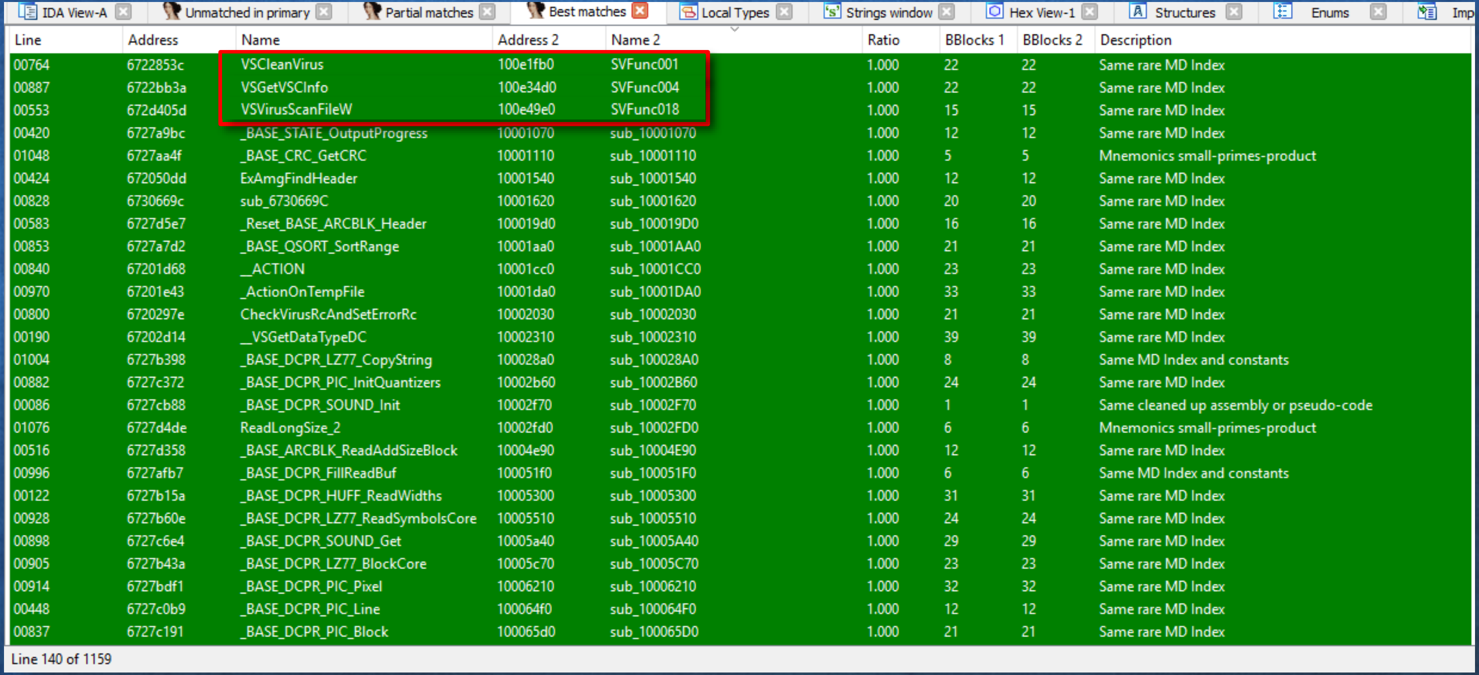


Line	Address	Name	Address 2	Name 2	Ratio	BBlocks 1	BBlocks 2	Description
00764	6722853c	VSCleanVirus	100e1fb0	SVFunc001	1.000	2	22	Same rare MD Index
00887	6722bb3a	VSGetVSCInfo	100e34d0	SVFunc004	1.000	2	22	Same rare MD Index
00553	672d405d	VSVirusScanFileW	100e49e0	SVFunc018	1.000	5	15	Same rare MD Index
00420	6727a9bc	_BASE_STATE_OutputProgress	10001070	sub_10001070	1.000	2	12	Same rare MD Index
01048	6727aa4f	_BASE_CRC_GetCRC	10001110	sub_10001110	1.000	5	5	Mnemonics small-primes-product
00424	672050dd	ExAmgFindHeader	10001540	sub_10001540	1.000	2	12	Same rare MD Index
00828	6730669c	sub_6730669C	10001620	sub_10001620	1.000	0	20	Same rare MD Index
00583	6727d5e7	_Reset_BASE_ARCBLK_Header	100019d0	sub_100019D0	1.000	6	16	Same rare MD Index
00853	6727a7d2	_BASE_QSORT_SortRange	10001aa0	sub_10001AA0	1.000	1	21	Same rare MD Index
00840	67201d68	__ACTION	10001cc0	sub_10001CC0	1.000	3	23	Same rare MD Index
00970	67201e43	_ActionOnTempFile	10001da0	sub_10001DA0	1.000	3	33	Same rare MD Index
00800	6720297e	CheckVirusRcAndSetErrorRc	10002030	sub_10002030	1.000	1	21	Same rare MD Index
00190	67202d14	__VSGetDataTypeDC	10002310	sub_10002310	1.000	9	39	Same rare MD Index
01004	6727b398	_BASE_DCPR_LZ77_CopyString	100028a0	sub_100028A0	1.000	8	8	Same MD Index and constants
00882	6727c372	_BASE_DCPR_PIC_InitQuantizers	10002b60	sub_10002B60	1.000	4	24	Same rare MD Index
00086	6727cb88	_BASE_DCPR_SOUND_Init	10002f70	sub_10002F70	1.000		1	Same cleaned up assembly or pseudo-code
01076	6727d4de	ReadLongSize_2	10002fd0	sub_10002FD0	1.000	6	6	Mnemonics small-primes-product
00516	6727d358	_BASE_ARCBLK_ReadAddSizeBlock	10004e90	sub_10004E90	1.000	2	12	Same rare MD Index
00996	6727afb7	_BASE_DCPR_FillReadBuf	100051f0	sub_100051F0	1.000	6	6	Same MD Index and constants
00122	6727b15a	_BASE_DCPR_HUFF_ReadWidths	10005300	sub_10005300	1.000	1	31	Same rare MD Index
00928	6727b60e	_BASE_DCPR_LZ77_ReadSymbolsCore	10005510	sub_10005510	1.000	4	24	Same rare MD Index
00898	6727c6e4	_BASE_DCPR_SOUND_Get	10005a40	sub_10005A40	1.000	9	29	Same rare MD Index
00905	6727b43a	_BASE_DCPR_LZ77_BlockCore	10005c70	sub_10005C70	1.000	3	23	Same rare MD Index
00914	6727bdf1	_BASE_DCPR_PIC_Pixel	10006210	sub_10006210	1.000	2	32	Same rare MD Index
00448	6727c0b9	_BASE_DCPR_PIC_Line	100064f0	sub_100064F0	1.000	2	12	Same rare MD Index
00837	6727c191	_BASE_DCPR_PIC_Block	100065d0	sub_100065D0	1.000	1	21	Same rare MD Index

100% match

Line 140 of 1159

CODE SIMILARITY



Line	Address	Name	Address 2	Name 2	Ratio	BBlocks 1	BBlocks 2	Description
00764	6722853c	VSCleanVirus	100e1fb0	SVFunc001	1.000	22	22	Same rare MD Index
00887	6722bb3a	VSGetVSCInfo	100e34d0	SVFunc004	1.000	22	22	Same rare MD Index
00553	672d405d	VSVirusScanFileW	100e49e0	SVFunc018	1.000	15	15	Same rare MD Index
00420	6727a9bc	_BASE_STATE_OutputProgress	10001070	sub_10001070	1.000	12	12	Same rare MD Index
01048	6727aa4f	_BASE_CRC_GetCRC	10001110	sub_10001110	1.000	5	5	Mnemonics small-primes-product
00424	672050dd	ExAmgFindHeader	10001540	sub_10001540	1.000	12	12	Same rare MD Index
00828	6730669c	sub_6730669C	10001620	sub_10001620	1.000	20	20	Same rare MD Index
00583	6727d5e7	_Reset_BASE_ARCBLK_Header	100019d0	sub_100019D0	1.000	16	16	Same rare MD Index
00853	6727a7d2	_BASE_QSORT_SortRange	10001aa0	sub_10001AA0	1.000	21	21	Same rare MD Index
00840	67201d68	__ACTION	10001cc0	sub_10001CC0	1.000	23	23	Same rare MD Index
00970	67201e43	_ActionOnTempFile	10001da0	sub_10001DA0	1.000	33	33	Same rare MD Index
00800	6720297e	CheckVirusRcAndSetErrorRc	10002030	sub_10002030	1.000	21	21	Same rare MD Index
00190	67202d14	__VSGetDataTypeDC	10002310	sub_10002310	1.000	39	39	Same rare MD Index
01004	6727b398	_BASE_DCPR_LZ77_CopyString	100028a0	sub_100028A0	1.000	8	8	Same MD Index and constants
00882	6727c372	_BASE_DCPR_PIC_InitQuantizers	10002b60	sub_10002B60	1.000	24	24	Same rare MD Index
00086	6727cb88	_BASE_DCPR_SOUND_Init	10002f70	sub_10002F70	1.000	1	1	Same cleaned up assembly or pseudo-code
01076	6727d4de	ReadLongSize_2	10002fd0	sub_10002FD0	1.000	6	6	Mnemonics small-primes-product
00516	6727d358	_BASE_ARCBLK_ReadAddSizeBlock	10004e90	sub_10004E90	1.000	12	12	Same rare MD Index
00996	6727afb7	_BASE_DCPR_FillReadBuf	100051f0	sub_100051F0	1.000	6	6	Same MD Index and constants
00122	6727b15a	_BASE_DCPR_HUFF_ReadWidths	10005300	sub_10005300	1.000	31	31	Same rare MD Index
00928	6727b60e	_BASE_DCPR_LZ77_ReadSymbolsCore	10005510	sub_10005510	1.000	24	24	Same rare MD Index
00898	6727c6e4	_BASE_DCPR_SOUND_Get	10005a40	sub_10005A40	1.000	29	29	Same rare MD Index
00905	6727b43a	_BASE_DCPR_LZ77_BlockCore	10005c70	sub_10005C70	1.000	23	23	Same rare MD Index
00914	6727bdf1	_BASE_DCPR_PIC_Pixel	10006210	sub_10006210	1.000	32	32	Same rare MD Index
00448	6727c0b9	_BASE_DCPR_PIC_Line	100064f0	sub_100064F0	1.000	12	12	Same rare MD Index
00837	6727c191	_BASE_DCPR_PIC_Block	100065d0	sub_100065D0	1.000	21	21	Same rare MD Index

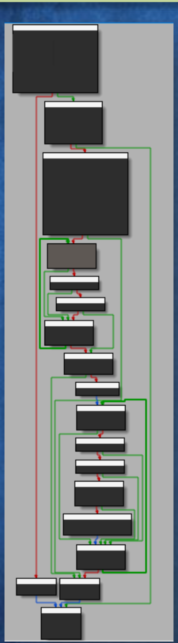
Line 140 of 1159

CODE SIMILARITY

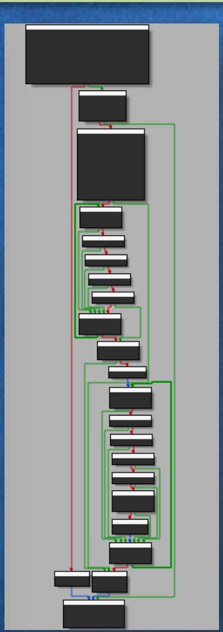
Trend Micro	SiliVaccine
VSCleanVirus	SVFunc001
VSDecompressFile	SVFunc002
VSGetPaternPath	SVFunc003
VSGetVSCInfo	SVFunc004
VSInit	SVFunc005
VSQuit	SVFunc006
VSReadPatternInFile	SVFunc007
VSSetCharacterEnvType	SVFunc008
VSSetConfFlag	SVFunc009
VSSetConfig	SVFunc010
Unknown	SVFunc011
Calls VSSetConfFlag	SVFunc012
VSSetLogFilePath	SVFunc013
Calls VSSetConfFlag	SVFunc014
Calls VSSetConfFlag	SVFunc015
VSSetProcessFileCallbackFunc	SVFunc016
Calls VSSetConfFlag	SVFunc017
VSVirusScanFileW	SVFunc018

CODE SIMILARITY

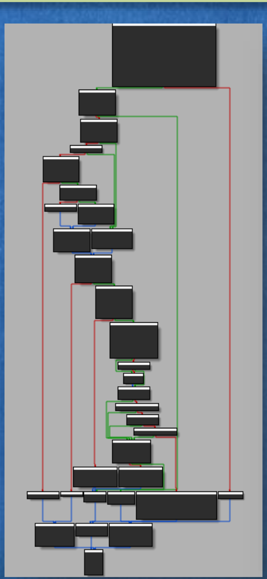
VSGetVSCInfo



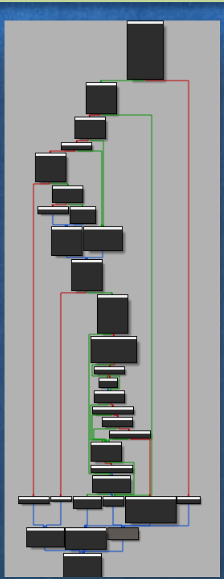
SVFunc004



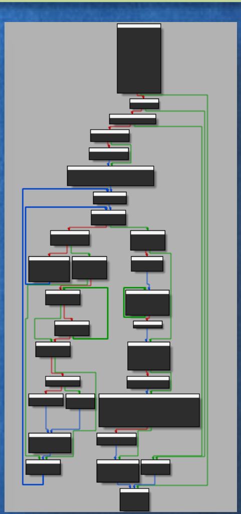
VSInit



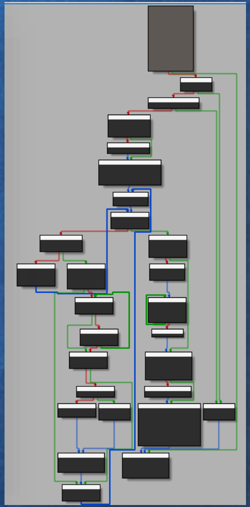
SVFunc005



VSQuit



SVFunc006



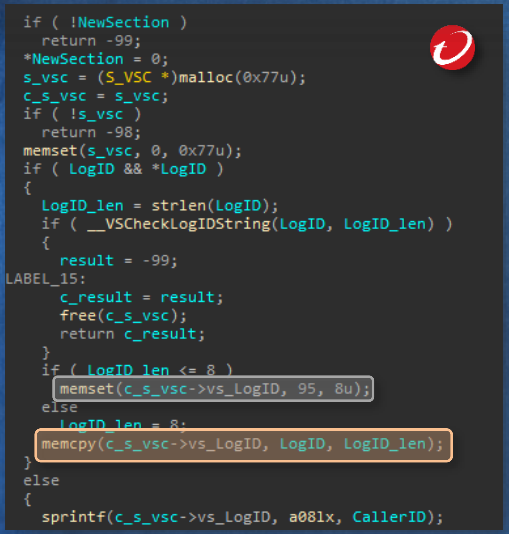
CODE DIFFERENCE

Trend Micro	SiliVaccine
VSCleanVirus	SVFunc001
VSDecompressFile	SVFunc002
VSGetPaternPath	SVFunc003
VSGetVSCInfo	SVFunc004
VSInit	SVFunc005
VSQuit	SVFunc006
VSReadPatternInFile	SVFunc007
VSSetCharacterEnvType	SVFunc008
VSSetConfFlag	SVFunc009
VSSetConfig	SVFunc010
Unknown	SVFunc011
Calls VSSetConfFlag	SVFunc012
VSSetLogFilePath	SVFunc013
Calls VSSetConfFlag	SVFunc014
Calls VSSetConfFlag	SVFunc015
VSSetProcessFileCallbackFunc	SVFunc016
Calls VSSetConfFlag	SVFunc017
VSVirusScanFileW	SVFunc018

CODE DIFFERENCE

VSInit

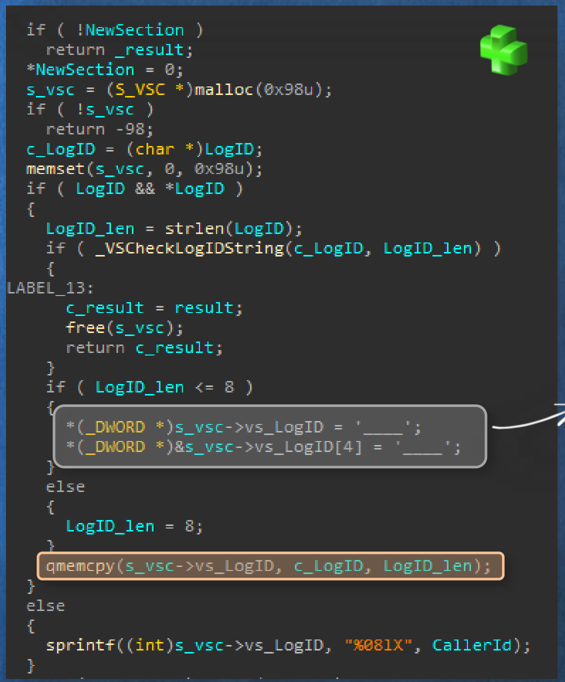
```
int __stdcall VSInit(int CallerID, char *LogID, int OldCfgSection, int *NewSection)
{
```



```
  if ( !NewSection )
    return -99;
  *NewSection = 0;
  s_vsc = (S_VSC *)malloc(0x77u);
  c_s_vsc = s_vsc;
  if ( !s_vsc )
    return -98;
  memset(s_vsc, 0, 0x77u);
  if ( LogID && *LogID )
  {
    LogID_len = strlen(LogID);
    if ( __VSCheckLogIDString(LogID, LogID_len) )
    {
      result = -99;
LABEL_15:
      c_result = result;
      free(c_s_vsc);
      return c_result;
    }
    if ( LogID_len <= 8 )
      memset(c_s_vsc->vs_LogID, 95, 8u);
    else
      LogID_len = 8;
    memcpy(c_s_vsc->vs_LogID, LogID, LogID_len);
  }
  else
  {
    sprintf(c_s_vsc->vs_LogID, a08lx, CallerID);
```

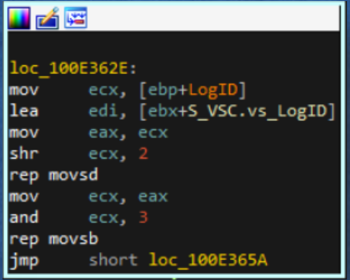
SVFunc005

```
signed int __stdcall SVFunc005(int CallerId, const char *LogID, S_VSCONF *OldCfgSection, _DWORD *NewSection)
{
```



```
  if ( !NewSection )
    return _result;
  *NewSection = 0;
  s_vsc = (S_VSC *)malloc(0x98u);
  if ( !s_vsc )
    return -98;
  c_LogID = (char *)LogID;
  memset(s_vsc, 0, 0x98u);
  if ( LogID && *LogID )
  {
    LogID_len = strlen(LogID);
    if ( _VSCheckLogIDString(c_LogID, LogID_len) )
    {
LABEL_13:
      c_result = result;
      free(s_vsc);
      return c_result;
    }
    if ( LogID_len <= 8 )
    {
      *(_DWORD *)s_vsc->vs_LogID = '____';
      *(_DWORD *)&s_vsc->vs_LogID[4] = '____';
    }
    else
    {
      LogID_len = 8;
    }
    qmemcpy(s_vsc->vs_LogID, c_LogID, LogID_len);
  }
  else
  {
    sprintf((int)s_vsc->vs_LogID, "%08lX", CallerId);
  }
```

function inlining



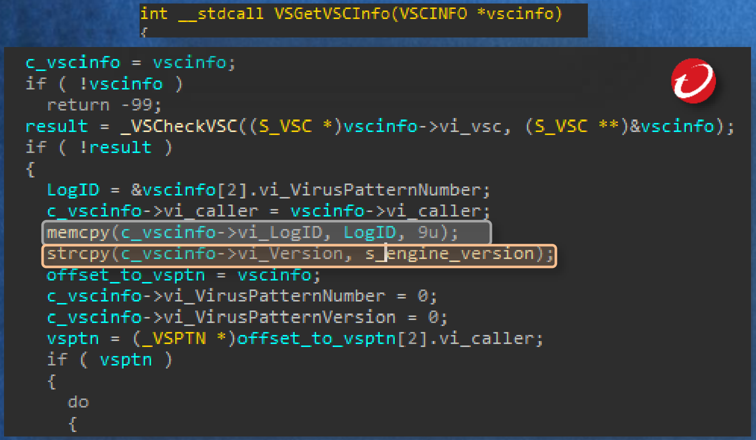
```
loc_100E362E:
mov     ecx, [ebp+LogID]
lea     edi, [ebx+S_VSC.vs_LogID]
mov     eax, ecx
shr     ecx, 2
rep movsd
mov     ecx, eax
and     ecx, 3
rep movsb
jmp     short loc_100E365A
```

CODE DIFFERENCE

Trend Micro	SiliVaccine
VSCleanVirus	SVFunc001
VSDecompressFile	SVFunc002
VSGetPaternPath	SVFunc003
VSGetVSCInfo	SVFunc004
VSInit	SVFunc005
VSQuit	SVFunc006
VSReadPatternInFile	SVFunc007
VSSetCharacterEnvType	SVFunc008
VSSetConfFlag	SVFunc009
VSSetConfig	SVFunc010
Unknown	SVFunc011
Calls VSSetConfFlag	SVFunc012
VSSetLogFilePath	SVFunc013
Calls VSSetConfFlag	SVFunc014
Calls VSSetConfFlag	SVFunc015
VSSetProcessFileCallbackFunc	SVFunc016
Calls VSSetConfFlag	SVFunc017
VSVirusScanFileW	SVFunc018

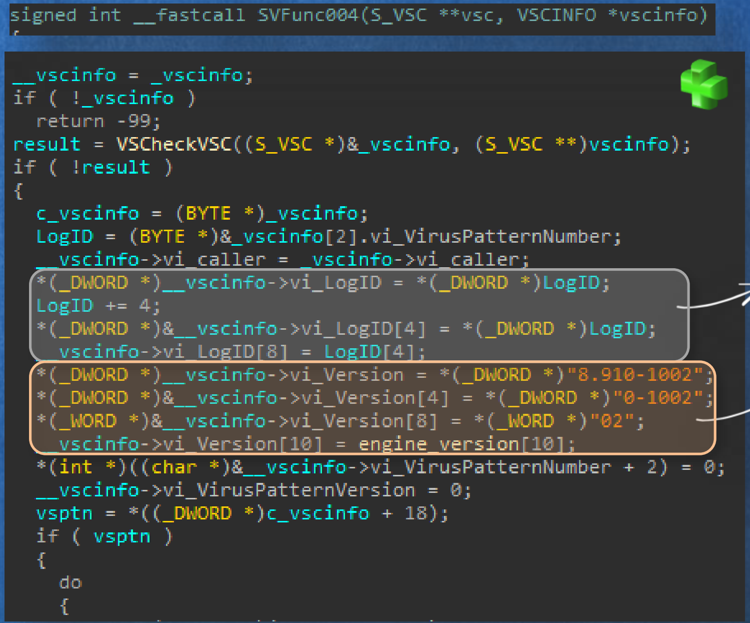
CODE DIFFERENCE

VSGetVSCInfo



```
int __stdcall VSGetVSCInfo(VSCINFO *vscinfo)
{
  c_vscinfo = vscinfo;
  if ( !vscinfo )
    return -99;
  result = _VSCheckVSC((S_VSC *)vscinfo->vi_vsc, (S_VSC **)&vscinfo);
  if ( !result )
  {
    LogID = &vscinfo[2].vi_VirusPatternNumber;
    c_vscinfo->vi_caller = vscinfo->vi_caller;
    memcpy(c_vscinfo->vi_LogID, LogID, 9u);
    strcpy(c_vscinfo->vi_Version, s_engine_version);
    offset_to_vsptn = vscinfo;
    c_vscinfo->vi_VirusPatternNumber = 0;
    c_vscinfo->vi_VirusPatternVersion = 0;
    vsptn = (_VSPTN *)offset_to_vsptn[2].vi_caller;
    if ( vsptn )
    {
      do
      {
```

SVFunc004



```
signed int __fastcall SVFunc004(S_VSC **vsc, VSCINFO *vscinfo)
{
  __vscinfo = _vscinfo;
  if ( !_vscinfo )
    return -99;
  result = VSCheckVSC((S_VSC *)&_vscinfo, (S_VSC **)vscinfo);
  if ( !result )
  {
    c_vscinfo = (BYTE *)_vscinfo;
    LogID = (BYTE *)&_vscinfo[2].vi_VirusPatternNumber;
    __vscinfo->vi_caller = _vscinfo->vi_caller;
    *(_DWORD *)__vscinfo->vi_LogID = *(_DWORD *)LogID;
    LogID += 4;
    *(_DWORD *)&__vscinfo->vi_LogID[4] = *(_DWORD *)LogID;
    __vscinfo->vi_LogID[8] = LogID[4];
    *(_DWORD *)__vscinfo->vi_Version = *(_DWORD *)"8.910-1002";
    *(_DWORD *)&__vscinfo->vi_Version[4] = *(_DWORD *)"0-1002";
    *(_WORD *)&__vscinfo->vi_Version[8] = *(_WORD *)"02";
    __vscinfo->vi_Version[10] = engine_version[10];
    *(int *)((char *)&__vscinfo->vi_VirusPatternNumber + 2) = 0;
    __vscinfo->vi_VirusPatternVersion = 0;
    vsptn = *((_DWORD *)c_vscinfo + 18);
    if ( vsptn )
    {
      do
      {
```

again,
function inlining

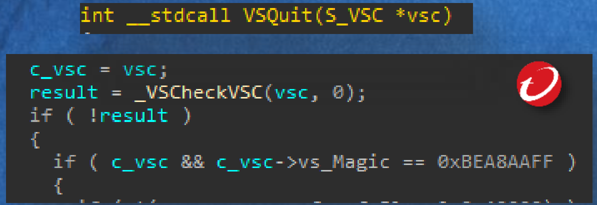
engine version:
8.910-1002

CODE DIFFERENCE

Trend Micro	SiliVaccine
VSCleanVirus	SVFunc001
VSDecompressFile	SVFunc002
VSGetPaternPath	SVFunc003
VSGetVSCInfo	SVFunc004
VSInit	SVFunc005
VSQuit	SVFunc006
VSReadPatternInFile	SVFunc007
VSSetCharacterEnvType	SVFunc008
VSSetConfFlag	SVFunc009
VSSetConfig	SVFunc010
Unknown	SVFunc011
Calls VSSetConfFlag	SVFunc012
VSSetLogFilePath	SVFunc013
Calls VSSetConfFlag	SVFunc014
Calls VSSetConfFlag	SVFunc015
VSSetProcessFileCallbackFunc	SVFunc016
Calls VSSetConfFlag	SVFunc017
VSVirusScanFileW	SVFunc018

CODE DIFFERENCE

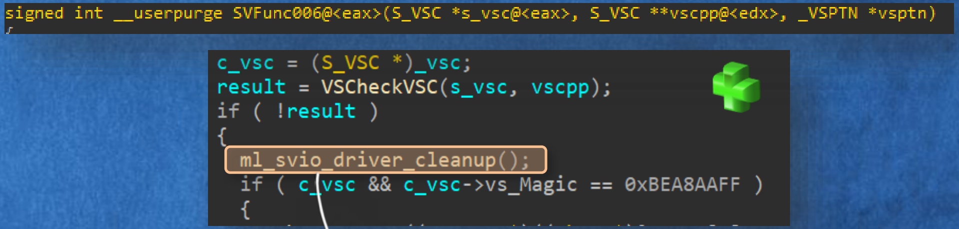
VSQuit



```
int __stdcall VSQuit(S_VSC *vsc)
```

```
  c_vsc = vsc;
  result = _VSCheckVSC(vsc, 0);
  if ( !result )
  {
    if ( c_vsc && c_vsc->vs_Magic == 0xBEA8AAFF )
    {
```

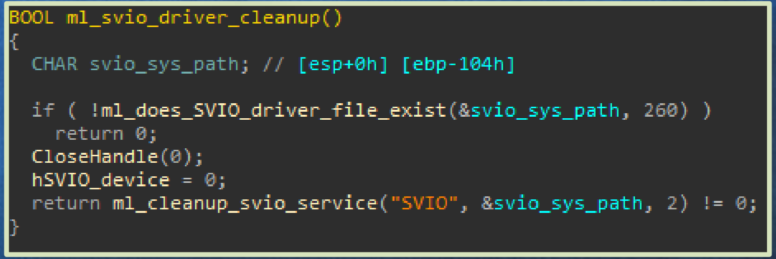
SVFunc006



```
signed int __userpurge SVFunc006@<eax>(S_VSC *s_vsc@<eax>, S_VSC **vscpp@<edx>, _VSPTN *vsptn)
```

```
  c_vsc = (S_VSC *)_vsc;
  result = VSCheckVSC(s_vsc, vscpp);
  if ( !result )
  {
    ml_svio_driver_cleanup();
    if ( c_vsc && c_vsc->vs_Magic == 0xBEA8AAFF )
    {
```

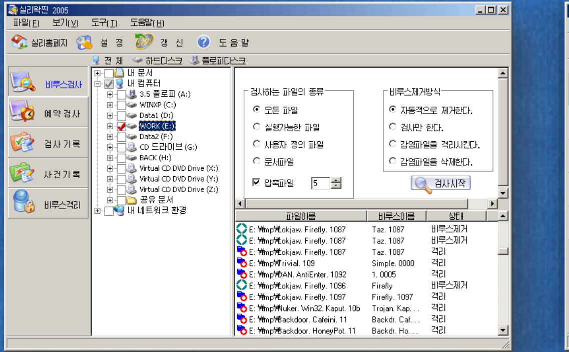
silivaccine proprietary function



```
BOOL ml_svio_driver_cleanup()
{
  CHAR svio_sys_path; // [esp+0h] [ebp-104h]

  if ( !ml_does_SVIO_driver_file_exist(&svio_sys_path, 260) )
    return 0;
  CloseHandle(0);
  hSVIO_device = 0;
  return ml_cleanup_svio_service("SVIO", &svio_sys_path, 2) != 0;
}
```

AN ONGOING PRACTICE

- remember the 2005 version of silivaccine?



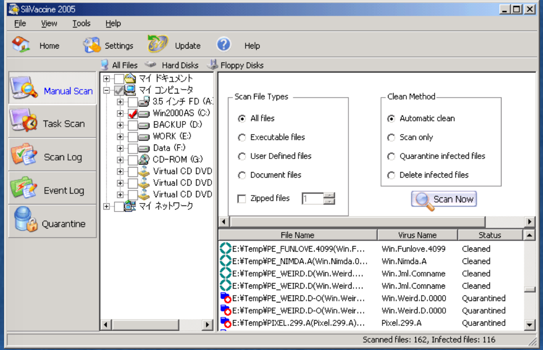
검사하는 파일의 종류

● 모든 파일
○ 실행가능한 파일
○ 사용자 정의 파일
○ 문서파일
☑ 압축파일 5

비루스제거방식

● 자동적으로 제거한다.
○ 검사만 한다.
○ 감염파일을 격리시킨다.
○ 감염파일을 삭제한다.

파일이름	비루스이름	상태
E: ₩tmp₩Lokjaw. Firefly. 1087	Taz. 1087	비루스제거
E: ₩tmp₩Lokjaw. Firefly. 1087	Taz. 1087	비루스제거
E: ₩tmp₩Lokjaw. Firefly. 1087	Taz. 1087	격리
E: ₩tmp₩Trivial. 109	Simple. 0000	격리
E: ₩tmp₩DAN. AntiEnter. 1092	1. 0005	격리
E: ₩tmp₩Lokjaw. Firefly. 1096	Firefly	비루스제거
E: ₩tmp₩Lokjaw. Firefly. 1097	Firefly. 1097	격리
E: ₩tmp₩Nuker. Win32. Kaput. 10b	Trojan. Kap. . .	격리
E: ₩tmp₩Backdoor. Cafeini. 11	Backdr. Caf. . .	격리
E: ₩tmp₩Backdoor. HoneyPot. 11	Backdr. Ho. . .	격리



Scan File Types

● All files
○ Executable files
○ User Defined files
○ Document files
☐ Zipped files 1

Clean Method

● Automatic clean
○ Scan only
○ Quarantine infected files
○ Delete infected files

File Name	Virus Name	Status
E:¥Temp¥PE_FUNLOVE.4099(Win.F...	Win.Funlove.4099	Cleaned
E:¥Temp¥PE_NIMDA.A(Win.Nimda.0...	Win.Nimda.A	Cleaned
E:¥Temp¥PE_WEIRD.D(Win.Weird....	Win.Jml.Comname	Cleaned
E:¥Temp¥PE_WEIRD.D(Win.Weird....	Win.Jml.Comname	Cleaned
E:¥Temp¥PE_WEIRD.D-O(Win.Weir...	Win.Weird.D.0000	Quarantined
E:¥Temp¥PE_WEIRD.D-O(Win.Weir...	Win.Weird.D.0000	Quarantined
E:¥Temp¥PIXEL.299.A(Pixel.299.A)...	Pixel.299.A	Quarantined

Scanned files: 162, Infected files: 116

- guess what... it also uses a trend micro component
    - instead of using vsapi32.dll (user mode), authors used tmfilter.sys (kernel mode)
- this is not a one time thing.

TREND MICRO'S RESPONSE

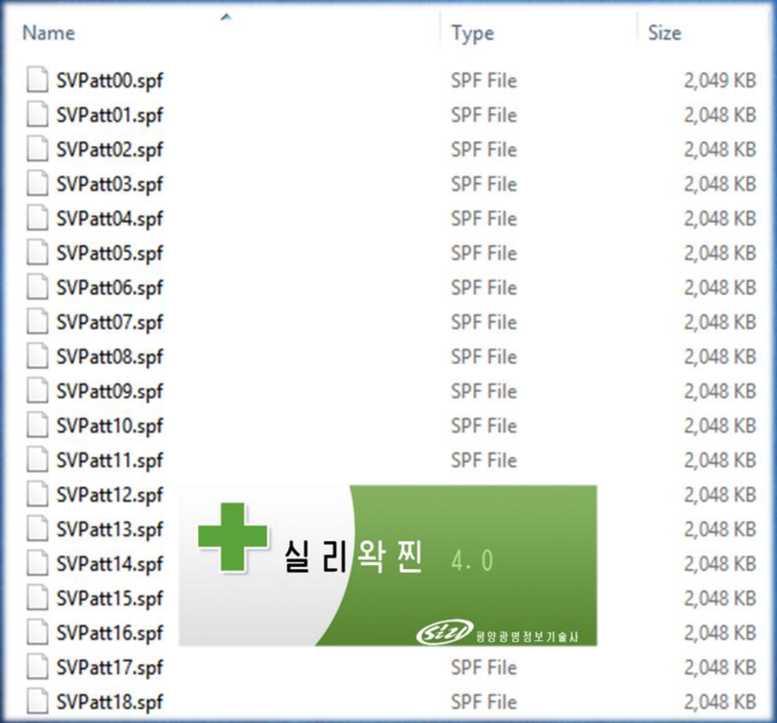
"Trend Micro is aware of the research by Check Point on the 'SiliVaccine' North Korean anti-virus product, and Check Point has provided us with a copy of the software for verification. While we are unable to confirm the source or authenticity of that copy, ***it apparently incorporates a module based on a 10+ year-old version of the widely distributed Trend Micro scan engine*** *used by a variety of our products.*

Trend Micro has never done business in or with North Korea*. We are confident that any such usage of the module is entirely unlicensed and illegal, and we have seen no evidence that source code was involved. The scan engine version at issue is quite old and has been widely incorporated in commercial products from Trend Micro and third party security products through various OEM deals over the years.*

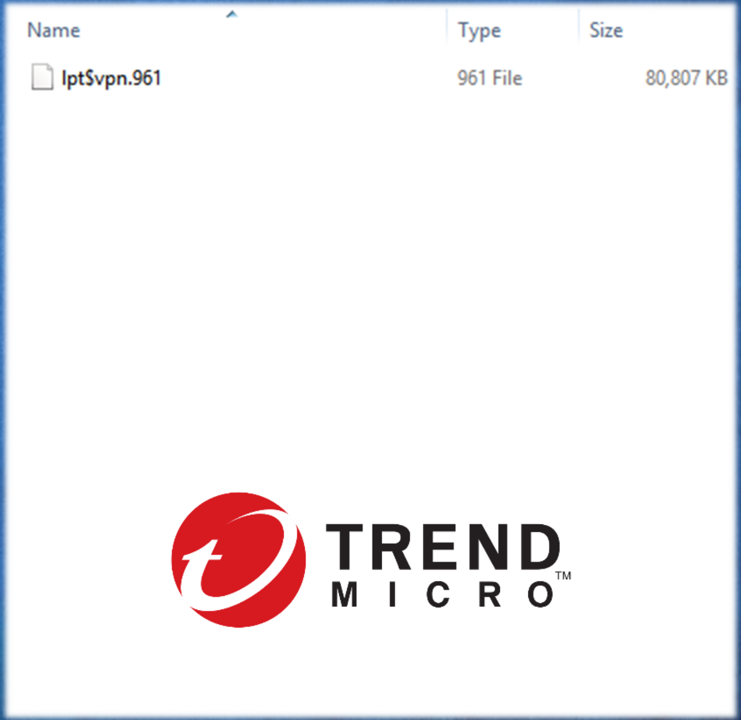
The specific means by which it may have been obtained by the creators of SiliVaccine is unknown. *Trend Micro takes a strong stance against software piracy, however legal recourse in this case would not be productive. We do not believe that the infringing use at issue poses any material risk to our customers."*

hiding the trend
micro components

SAME ENGINE.. SAME SIGNATURES?

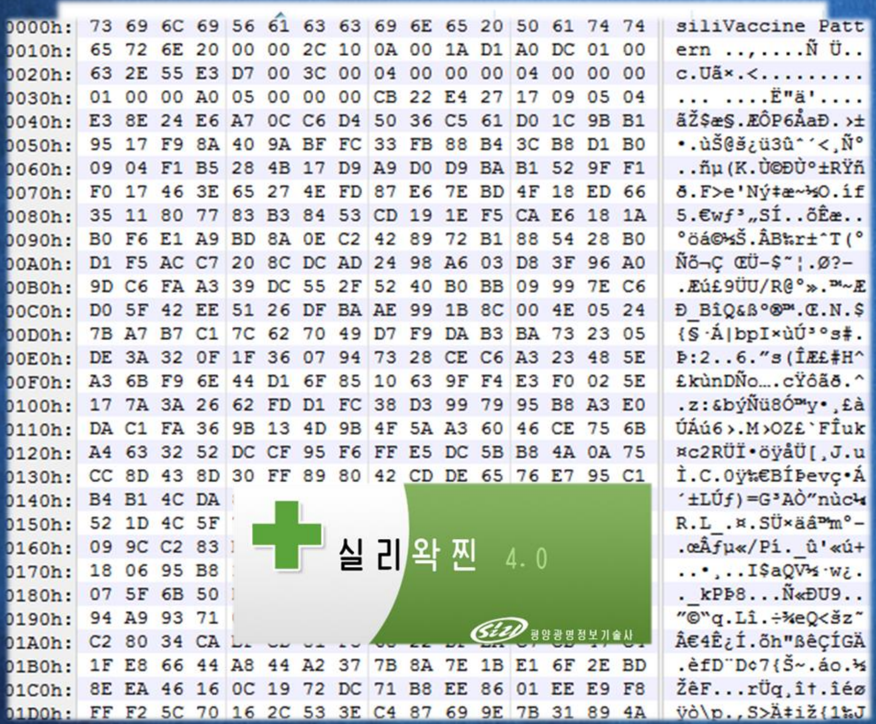


Name	Type	Size
SVPatt00.spf	SPF File	2,049 KB
SVPatt01.spf	SPF File	2,048 KB
SVPatt02.spf	SPF File	2,048 KB
SVPatt03.spf	SPF File	2,048 KB
SVPatt04.spf	SPF File	2,048 KB
SVPatt05.spf	SPF File	2,048 KB
SVPatt06.spf	SPF File	2,048 KB
SVPatt07.spf	SPF File	2,048 KB
SVPatt08.spf	SPF File	2,048 KB
SVPatt09.spf	SPF File	2,048 KB
SVPatt10.spf	SPF File	2,048 KB
SVPatt11.spf	SPF File	2,048 KB
SVPatt12.spf		2,048 KB
SVPatt13.spf		2,048 KB
SVPatt14.spf		2,048 KB
SVPatt15.spf		2,048 KB
SVPatt16.spf		2,048 KB
SVPatt17.spf	SPF File	2,048 KB
SVPatt18.spf	SPF File	2,048 KB

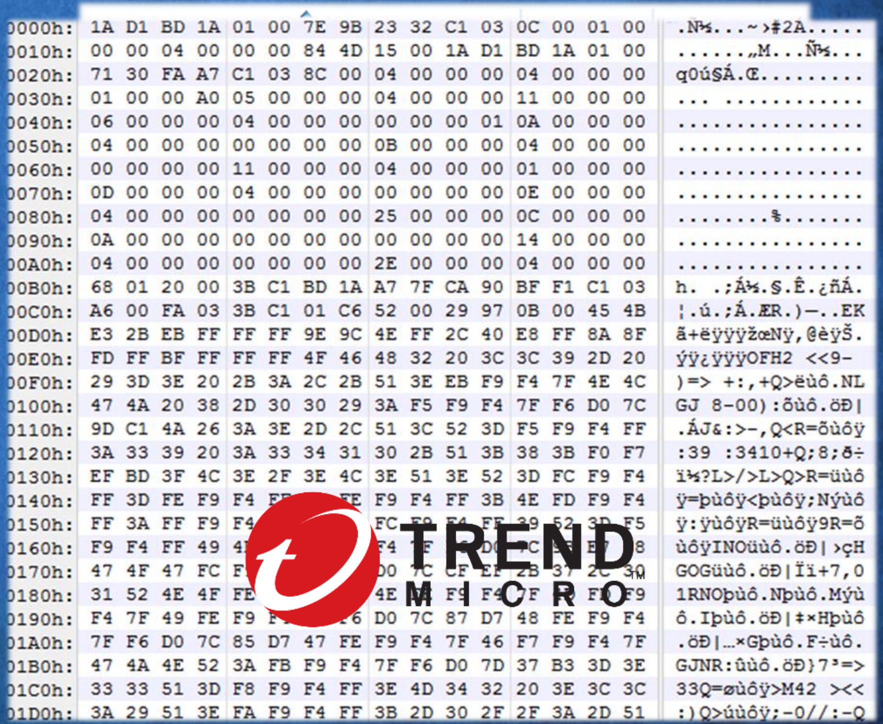


Name	Type	Size
lpt$vpn.961	961 File	80,807 KB

SAME ENGINE.. SAME SIGNATURES?

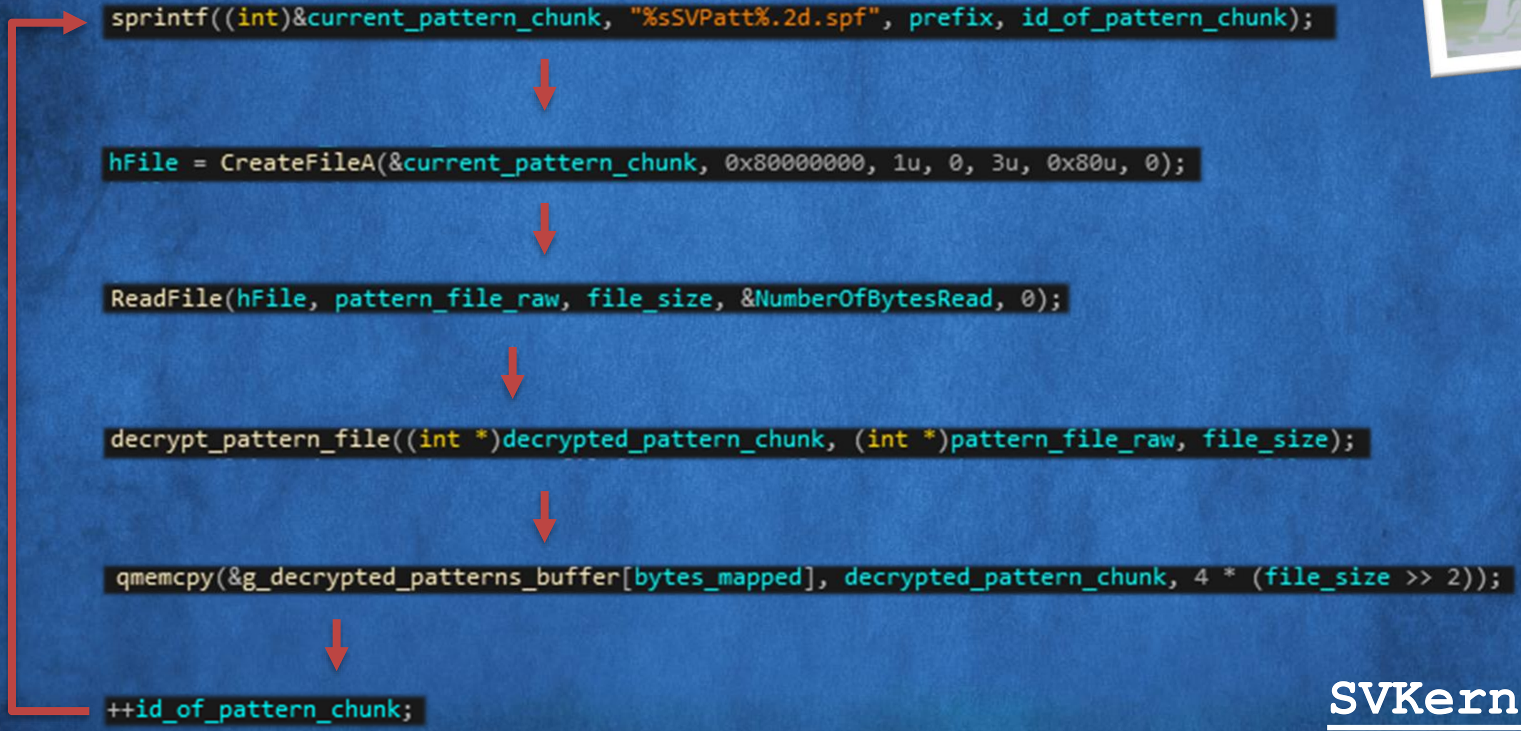


```
0000h: 73 69 6C 69 56 61 63 63 69 6E 65 20 50 61 74 74  siliVaccine Patt
0010h: 65 72 6E 20 00 00 2C 10 0A 00 1A D1 A0 DC 01 00  ern ..,....Ñ Ü..
0020h: 63 2E 55 E3 D7 00 3C 00 04 00 00 00 04 00 00 00  c.Uã×.<.........
0030h: 01 00 00 A0 05 00 00 00 CB 22 E4 27 17 09 05 04  ... ....Ë"ä'....
0040h: E3 8E 24 E6 A7 0C C6 D4 50 36 C5 61 D0 1C 9B B1  ãŽ$æ§.ÆÔP6ÅaÐ.›±
0050h: 95 17 F9 8A 40 9A BF FC 33 FB 88 B4 3C B8 D1 B0  •.ùŠ@š¿ü3ûˆ´<¸Ñ°
0060h: 09 04 F1 B5 28 4B 17 D9 A9 D0 D9 BA B1 52 9F F1  ..ñµ(K.Ù©ÐÙº±RŸñ
0070h: F0 17 46 3E 65 27 4E FD 87 E6 7E BD 4F 18 ED 66  ð.F>e'Ný‡æ~½O.íf
0080h: 35 11 80 77 83 B3 84 53 CD 19 1E F5 CA E6 18 1A  5.€wƒ³„SÍ..õÊæ..
0090h: B0 F6 E1 A9 BD 8A 0E C2 42 89 72 B1 88 54 28 B0  °öá©½Š.ÂB‰r±ˆT(°
00A0h: D1 F5 AC C7 20 8C DC AD 24 98 A6 03 D8 3F 96 A0  Ñõ¬Ç ŒÜ$˜¦.Ø?– 
00B0h: 9D C6 FA A3 39 DC 55 2F 52 40 B0 BB 09 99 7E C6  .Æú£9ÜU/R@°».™~Æ
00C0h: D0 5F 42 EE 51 26 DF BA AE 99 1B 8C 00 4E 05 24  Ð_BîQ&ßº®™.Œ.N.$
00D0h: 7B A7 B7 C1 7C 62 70 49 D7 F9 DA B3 BA 73 23 05  {§·Á|bpI×ùÚ³ºs#.
00E0h: DE 3A 32 0F 1F 36 07 94 73 28 CE C6 A3 23 48 5E  Þ:2..6.”s(ÎÆ£#H^
00F0h: A3 6B F9 6E 44 D1 6F 85 10 63 9F F4 E3 F0 02 5E  £kùnDÑo….cŸôãð.^
0100h: 17 7A 3A 26 62 FD D1 FC 38 D3 99 79 95 B8 A3 E0  .z:&býÑü8Ó™y•¸£à
0110h: DA C1 FA 36 9B 13 4D 9B 4F 5A A3 60 46 CE 75 6B  ÚÁú6›.M›OZ£`FÎuk
0120h: A4 63 32 52 DC CF 95 F6 FF E5 DC 5B B8 4A 0A 75  ¤c2RÜÏ•öÿåÜ[¸J.u
0130h: CC 8D 43 8D 30 FF 89 80 42 CD DE 65 76 E7 95 C1  Ì.C.0ÿ‰€BÍÞevç•Á
0140h: B4 B1 4C DA                                      ´±LÚf)=G³AÒ”nùc¼
0150h: 52 1D 4C 5F                                      R.L_.¤.SÜ×äâ™m°–
0160h: 09 9C C2 83                                      .œÂƒµ«/Pí._û'«ú+
0170h: 18 06 95 B8                                      ..•¸..I$aQV½·w¿.
0180h: 07 5F 6B 50                                      ._kPÞ8...Ñ«ÐU9..
0190h: 94 A9 93 71                                      ”©“q.Lî.÷¾eQ<šz˜
01A0h: C2 80 34 CA                                      Â€4Ê¿Í.õh"ßêÇÍGÄ
01B0h: 1F E8 66 44 A8 44 A2 37 7B 8A 7E 1B E1 6F 2E BD  .èfD¨D¢7{Š~.áo.½
01C0h: 8E EA 46 16 0C 19 72 DC 71 B8 EE 86 01 EE E9 F8  ŽêF...rÜq¸î†.îéø
01D0h: FF F2 5C 70 16 2C 53 3E C4 87 69 9E 7B 31 89 4A  ÿò\p.,S>Ä‡iž{1‰J
```



```
0000h: 1A D1 BD 1A 01 00 7E 9B 23 32 C1 03 0C 00 01 00  .Ñ½...~›#2Á.....
0010h: 00 00 04 00 00 00 84 4D 15 00 1A D1 BD 1A 01 00  ......„M...Ñ½...
0020h: 71 30 FA A7 C1 03 8C 00 04 00 00 00 04 00 00 00  q0ú§Á.Œ.........
0030h: 01 00 00 A0 05 00 00 00 04 00 00 00 11 00 00 00  ... ............
0040h: 06 00 00 00 04 00 00 00 00 00 00 01 0A 00 00 00  ................
0050h: 04 00 00 00 00 00 00 00 0B 00 00 00 04 00 00 00  ................
0060h: 00 00 00 00 11 00 00 00 04 00 00 00 01 00 00 00  ................
0070h: 0D 00 00 00 04 00 00 00 00 00 00 00 0E 00 00 00  ................
0080h: 04 00 00 00 00 00 00 00 25 00 00 00 0C 00 00 00  ........%.......
0090h: 0A 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00  ................
00A0h: 04 00 00 00 00 00 00 00 2E 00 00 00 04 00 00 00  ................
00B0h: 68 01 20 00 3B C1 BD 1A A7 7F CA 90 BF F1 C1 03  h. .;Á½.§.Ê.¿ñÁ.
00C0h: A6 00 FA 03 3B C1 01 C6 52 00 29 97 0B 00 45 4B  ¦.ú.;Á.ÆR.)—..EK
00D0h: E3 2B EB FF FF FF 9E 9C 4E FF 2C 40 E8 FF 8A 8F  ã+ëÿÿÿžœNÿ,@èÿŠ.
00E0h: FD FF BF FF FF FF 4F 46 48 32 20 3C 3C 39 2D 20  ýÿ¿ÿÿÿOFH2 <<9- 
00F0h: 29 3D 3E 20 2B 3A 2C 2B 51 3E EB F9 F4 7F 4E 4C  )=> +:,+Q>ëùô.NL
0100h: 47 4A 20 38 2D 30 30 29 3A F5 F9 F4 7F F6 D0 7C  GJ 8-00):õùô.öÐ|
0110h: 9D C1 4A 26 3A 3E 2D 2C 51 3C 52 3D F5 F9 F4 FF  .ÁJ&:>-,Q<R=õùôÿ
0120h: 3A 33 39 20 3A 33 34 31 30 2B 51 3B 38 3B F0 F7  :39 :3410+Q;8;ð÷
0130h: EF BD 3F 4C 3E 2F 3E 4C 3E 51 3E 52 3D FC F9 F4  ï½?L>/>L>Q>R=üùô
0140h: FF 3D FE F9 F4       FE F9 F4 FF 3B 4E FD F9 F4  ÿ=þùôÿ<þùôÿ;Nýùô
0150h: FF 3A FF F9 F4          FC F9 F4 FF 39 52 3D F5  ÿ:ÿùôÿR=üùôÿ9R=õ
0160h: F9 F4 FF 49                                      ùôÿINOüùô.öÐ|›çH
0170h: 47 4F 47 FC             D0 7C CF EF 2B 37 2C 30  GOGüùô.öÐ|Ïï+7,0
0180h: 31 52 4E 4F FE          4E    F9 F4 7F    FD F9  1RNOþùô.Nþùô.Mýù
0190h: F4 7F 49 FE F9       F6 D0 7C 87 D7 48 FE F9 F4  ô.Iþùô.öÐ|‡×Hþùô
01A0h: 7F F6 D0 7C 85 D7 47 FE F9 F4 7F 46 F7 F9 F4 7F  .öÐ|…×Gþùô.F÷ùô.
01B0h: 47 4A 4E 52 3A FB F9 F4 7F F6 D0 7D 37 B3 3D 3E  GJNR:ûùô.öÐ}7³=>
01C0h: 33 33 51 3D F8 F9 F4 FF 3E 4D 34 32 20 3E 3C 3C  33Q=øùôÿ>M42 ><<
01D0h: 3A 29 51 3E FA F9 F4 FF 3B 2D 30 2F 2F 3A 2D 51  :)Q>úùôÿ;-0//:-Q
```

LOOKING DEEPER



```
sprintf((int)&current_pattern_chunk, "%sSVPatt%.2d.spf", prefix, id_of_pattern_chunk);
```

```
hFile = CreateFileA(&current_pattern_chunk, 0x80000000, 1u, 0, 3u, 0x80u, 0);
```

```
ReadFile(hFile, pattern_file_raw, file_size, &NumberOfBytesRead, 0);
```

```
decrypt_pattern_file((int *)decrypted_pattern_chunk, (int *)pattern_file_raw, file_size);
```

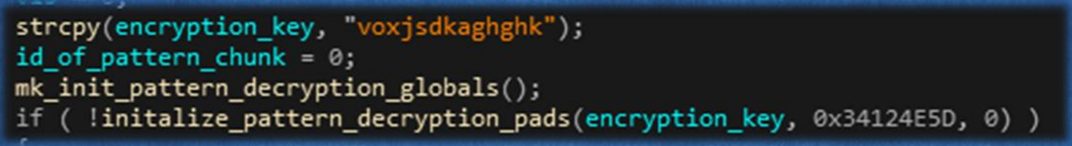
```
qmemcpy(&g_decrypted_patterns_buffer[bytes_mapped], decrypted_pattern_chunk, 4 * (file_size >> 2));
```

```
++id_of_pattern_chunk;
```

SVKernel.dll

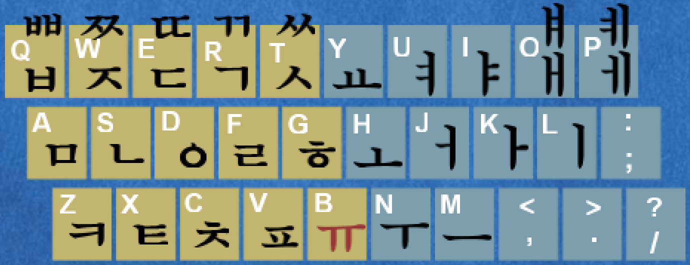
SVFunc019

THE ENCRYPTION KEY

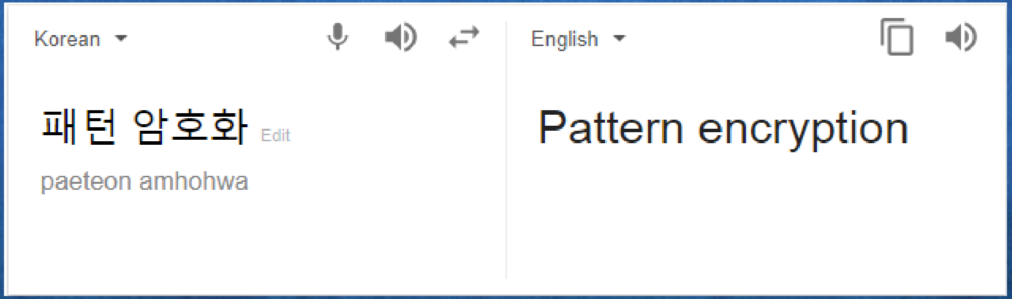


```
strcpy(encryption_key, "voxjsdkaghghk");
id_of_pattern_chunk = 0;
mk_init_pattern_decryption_globals();
if ( !initalize_pattern_decryption_pads(encryption_key, 0x34124E5D, 0) )
```

패턴 암호화



voxjsdkaghghk

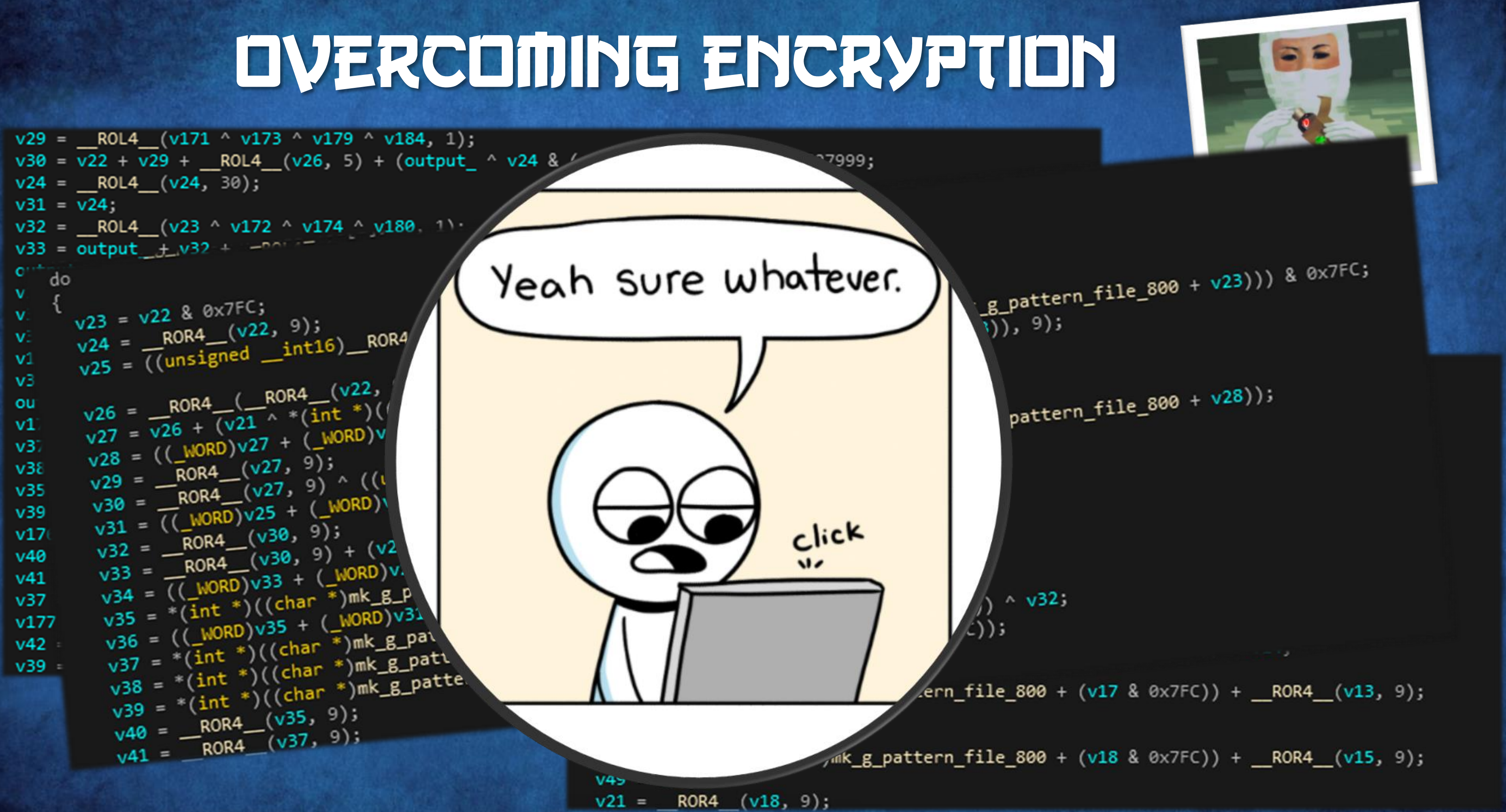


패턴 암호화

paeteon amhohwa

Pattern encryption

OVERCOMING ENCRYPTION

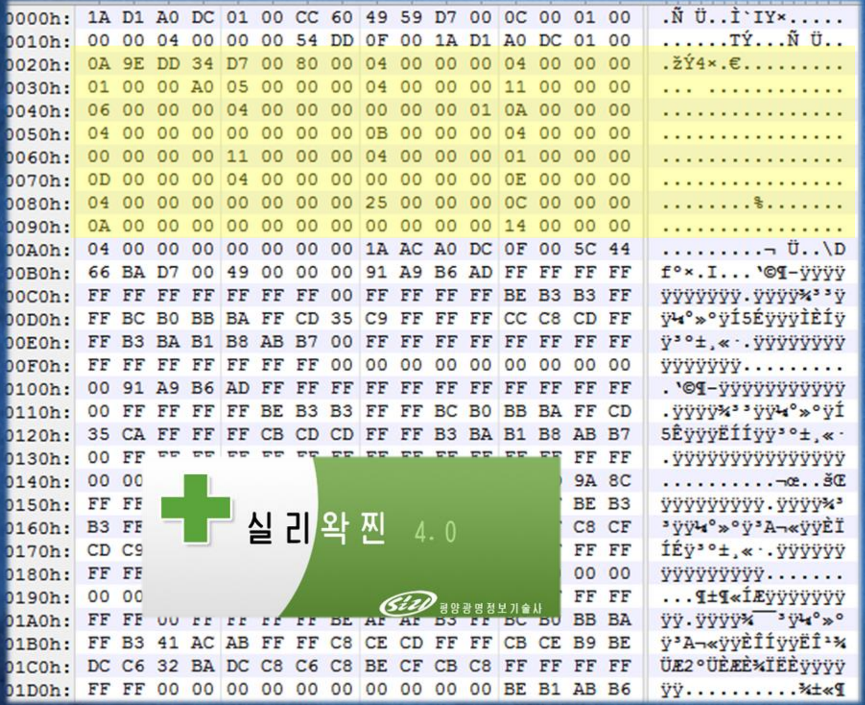


```
v29 = __ROL4__(v171 ^ v173 ^ v179 ^ v184, 1);
v30 = v22 + v29 + __ROL4__(v26, 5) + (output_ ^ v24 &
v24 = __ROL4__(v24, 30);
v31 = v24;
v32 = __ROL4__(v23 ^ v172 ^ v174 ^ v180, 1);
v33 = output_ + v32 +
```

```
do
{
  v23 = v22 & 0x7FC;
  v24 = __ROR4__(v22, 9);
  v25 = ((unsigned __int16)__ROR4

  v26 = __ROR4__(__ROR4__(v22,
  v27 = v26 + (v21 ^ *(int *)(
  v28 = ((_WORD)v27 + (_WORD)v
  v29 = __ROR4__(v27, 9);
  v30 = __ROR4__(v27, 9) ^ ((u
  v31 = ((_WORD)v25 + (_WORD)v
  v32 = __ROR4__(v30, 9);
  v33 = __ROR4__(v30, 9) + (v2
  v34 = ((_WORD)v33 + (_WORD)v
  v35 = *(int *)((char *)mk_g_p
  v36 = ((_WORD)v35 + (_WORD)v3
  v37 = *(int *)((char *)mk_g_pa
  v38 = *(int *)((char *)mk_g_patt
  v39 = *(int *)((char *)mk_g_patte
  v40 = __ROR4__(v35, 9);
  v41 = __ROR4__(v37, 9);
```

```
_g_pattern_file_800 + v23))) & 0x7FC;
)), 9);

pattern_file_800 + v28));

) ^ v32;
C));

tern_file_800 + (v17 & 0x7FC)) + __ROR4__(v13, 9);

mk_g_pattern_file_800 + (v18 & 0x7FC)) + __ROR4__(v15, 9);

v21 = __ROR4__(v18, 9);
```

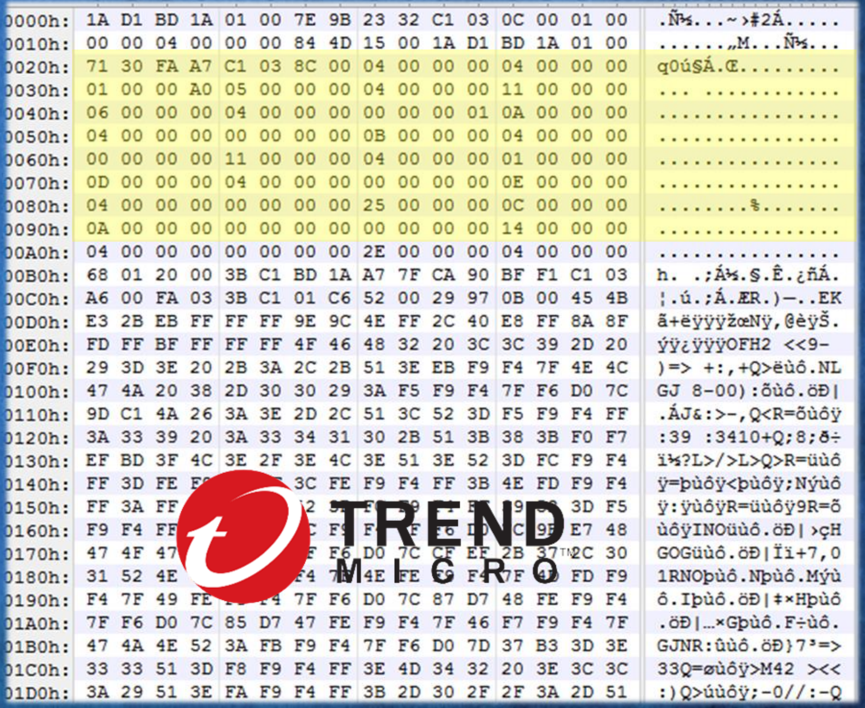
DUMPED AND DECRYPTED



```
0000h: 1A D1 A0 DC 01 00 CC 60 49 59 D7 00 0C 00 01 00  .Ñ Ü..Ì`IY×.....
0010h: 00 00 04 00 00 00 54 DD 0F 00 1A D1 A0 DC 01 00  ......TÝ...Ñ Ü..
0020h: 0A 9E DD 34 D7 00 80 00 04 00 00 00 04 00 00 00  .žÝ4×.€.........
0030h: 01 00 00 A0 05 00 00 00 04 00 00 00 11 00 00 00  ... ............
0040h: 06 00 00 00 04 00 00 00 00 00 00 01 0A 00 00 00  ................
0050h: 04 00 00 00 00 00 00 00 0B 00 00 00 04 00 00 00  ................
0060h: 00 00 00 00 11 00 00 00 04 00 00 00 01 00 00 00  ................
0070h: 0D 00 00 00 04 00 00 00 00 00 00 00 0E 00 00 00  ................
0080h: 04 00 00 00 00 00 00 00 25 00 00 00 0C 00 00 00  ........%.......
0090h: 0A 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00  ................
00A0h: 04 00 00 00 00 00 00 00 1A AC A0 DC 0F 00 5C 44  .........¬ Ü..\D
00B0h: 66 BA D7 00 49 00 00 00 91 A9 B6 AD FF FF FF FF  f°×.I...‘©¶-ÿÿÿÿ
00C0h: FF FF FF FF FF FF FF 00 FF FF FF FF BE B3 B3 FF  ÿÿÿÿÿÿÿ.ÿÿÿÿ¾³³ÿ
00D0h: FF BC B0 BB BA FF CD 35 C9 FF FF FF CC C8 CD FF  ÿ¼°»°ÿÍ5ÉÿÿÿÌÈÍÿ
00E0h: FF B3 BA B1 B8 AB B7 00 FF FF FF FF FF FF FF FF  ÿ³°±¸«·.ÿÿÿÿÿÿÿÿ
00F0h: FF FF FF FF FF FF FF 00 00 00 00 00 00 00 00 00  ÿÿÿÿÿÿÿ.........
0100h: 00 91 A9 B6 AD FF FF FF FF FF FF FF FF FF FF FF  .‘©¶-ÿÿÿÿÿÿÿÿÿÿÿ
0110h: 00 FF FF FF FF BE B3 B3 FF FF BC B0 BB BA FF CD  .ÿÿÿÿ¾³³ÿÿ¼°»°ÿÍ
0120h: 35 CA FF FF FF CB CD CD FF FF B3 BA B1 B8 AB B7  5ÊÿÿÿËÍÍÿÿ³°±¸«·
0130h: 00 FF                                     FF FF  .ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
0140h: 00 00                                     9A 8C  ..........¬œ..šŒ
0150h: FF FF                                     BE B3  ÿÿÿÿÿÿÿÿÿÿ.ÿÿÿÿ¾³
0160h: B3 FF                                     C8 CF  ³ÿÿ¼°»°ÿ³A¬«ÿÿÈÏ
0170h: CD C9                                     FF FF  ÍÉÿ³°±¸«·.ÿÿÿÿÿÿ
0180h: FF FF                                     00 00  ÿÿÿÿÿÿÿÿÿÿ......
0190h: 00 00                                     FF FF  ...¶±¶«ÍÆÿÿÿÿÿÿÿ
01A0h: FF FF 00 FF FF FF FF BE AF AF B3 FF BC B0 BB BA  ÿÿ.ÿÿÿÿ¾¯¯³ÿ¼°»°
01B0h: FF B3 41 AC AB FF FF C8 CE CD FF FF CB CE B9 BE  ÿ³A¬«ÿÿÈÎÍÿÿËÎ¹¾
01C0h: DC C6 32 BA DC C8 C6 C8 BE CF CB C8 FF FF FF FF  ÜÆ2°ÜÈÆÈ¾ÏËÈÿÿÿÿ
01D0h: FF FF 00 00 00 00 00 00 00 00 00 00 BE B1 AB B6  ÿÿ..........¾±«¶
```

실리왁찐 4.0

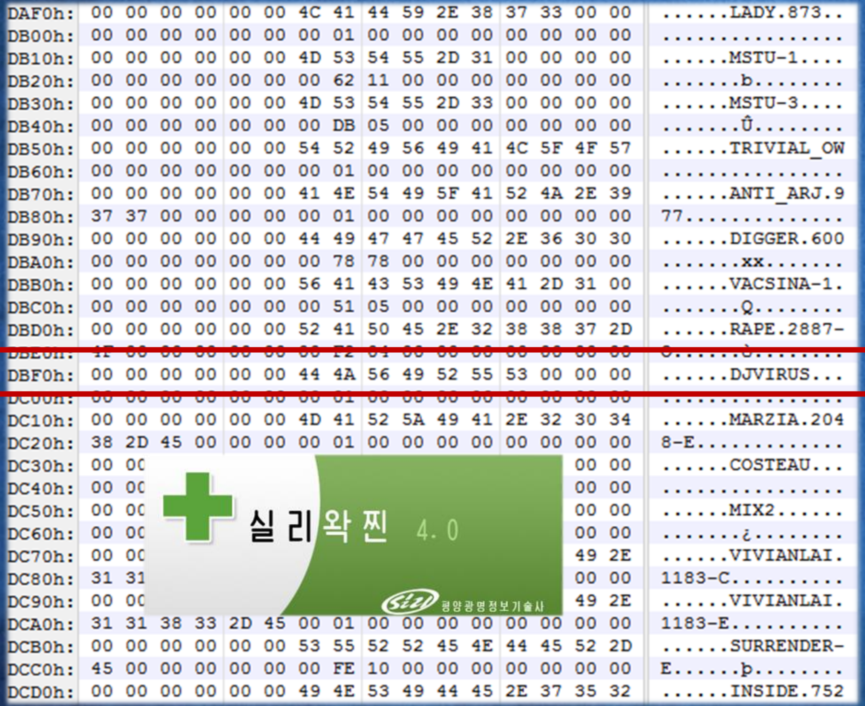
평양광명정보기술사



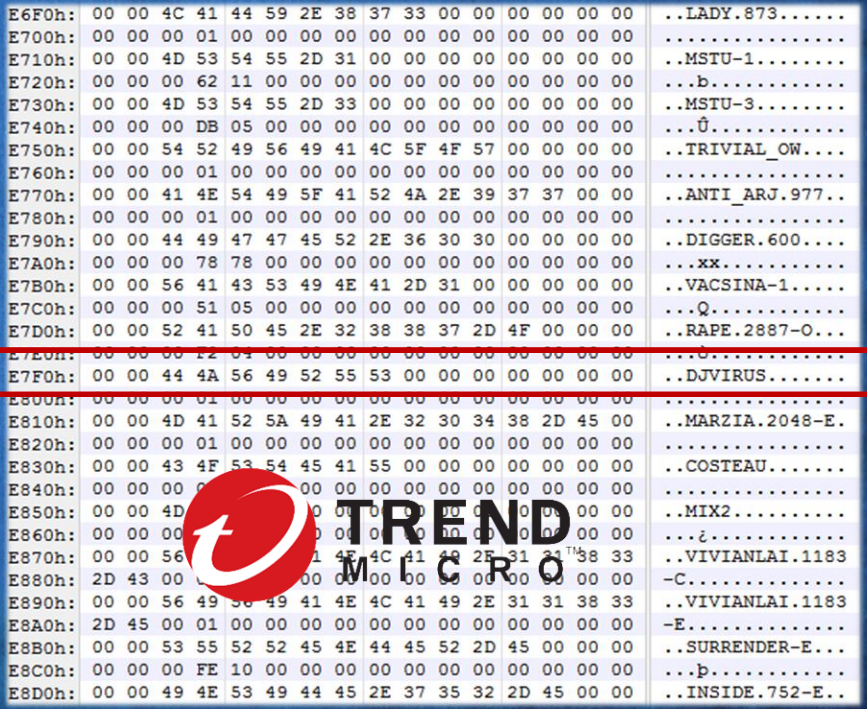
```
0000h: 1A D1 BD 1A 01 00 7E 9B 23 32 C1 03 0C 00 01 00  .Ñ½...~›#2Á.....
0010h: 00 00 04 00 00 00 84 4D 15 00 1A D1 BD 1A 01 00  ......„M...Ñ½...
0020h: 71 30 FA A7 C1 03 8C 00 04 00 00 00 04 00 00 00  q0ú§Á.Œ.........
0030h: 01 00 00 A0 05 00 00 00 04 00 00 00 11 00 00 00  ... ............
0040h: 06 00 00 00 04 00 00 00 00 00 00 01 0A 00 00 00  ................
0050h: 04 00 00 00 00 00 00 00 0B 00 00 00 04 00 00 00  ................
0060h: 00 00 00 00 11 00 00 00 04 00 00 00 01 00 00 00  ................
0070h: 0D 00 00 00 04 00 00 00 00 00 00 00 0E 00 00 00  ................
0080h: 04 00 00 00 00 00 00 00 25 00 00 00 0C 00 00 00  ........%.......
0090h: 0A 00 00 00 00 00 00 00 00 00 00 00 14 00 00 00  ................
00A0h: 04 00 00 00 00 00 00 00 2E 00 00 00 04 00 00 00  ................
00B0h: 68 01 20 00 3B C1 BD 1A A7 7F CA 90 BF F1 C1 03  h. .;Á½.§.Ê.¿ñÁ.
00C0h: A6 00 FA 03 3B C1 01 C6 52 00 29 97 0B 00 45 4B  ¦.ú.;Á.ÆR.)—..EK
00D0h: E3 2B EB FF FF FF 9E 9C 4E FF 2C 40 E8 FF 8A 8F  ã+ëÿÿÿžœNÿ,@èÿŠ.
00E0h: FD FF BF FF FF FF 4F 46 48 32 20 3C 3C 39 2D 20  ýÿ¿ÿÿÿOFH2 <<9-
00F0h: 29 3D 3E 20 2B 3A 2C 2B 51 3E EB F9 F4 7F 4E 4C  )=> +:,+Q>ëùô.NL
0100h: 47 4A 20 38 2D 30 30 29 3A F5 F9 F4 7F F6 D0 7C  GJ 8-00):õùô.öÐ|
0110h: 9D C1 4A 26 3A 3E 2D 2C 51 3C 52 3D F5 F9 F4 FF  .ÁJ&:>-,Q<R=õùôÿ
0120h: 3A 33 39 20 3A 33 34 31 30 2B 51 3B 38 3B F0 F7  :39 :3410+Q;8;ð÷
0130h: EF BD 3F 4C 3E 2F 3E 4C 3E 51 3E 52 3D FC F9 F4  ï½?L>/>L>Q>R=üùô
0140h: FF 3D FE             3C FE F9 F4 FF 3B 4E FD F9 F4  ÿ=þùôÿ<þùôÿ;Nýùô
0150h: FF 3A FF                                  3D F5  ÿ:ÿùôÿR=üùôÿ9R=õ
0160h: F9 F4 FF                                  E7 48  ùôÿINOüùô.öÐ|>çH
0170h: 47 4F 47             F6 D0 7C CF EF 2B 37 2C 30  GOGüùô.öÐ|Ïï+7,0
0180h: 31 52 4E                                  FD F9  1RNOþùô.Nþùô.Mýù
0190h: F4 7F 49 FE          7F F6 D0 7C 87 D7 48 FE F9 F4  ô.Iþùô.öÐ|‡×Hþùô
01A0h: 7F F6 D0 7C 85 D7 47 FE F9 F4 7F 46 F7 F9 F4 7F  .öÐ|…×Gþùô.F÷ùô.
01B0h: 47 4A 4E 52 3A FB F9 F4 7F F6 D0 7D 37 B3 3D 3E  GJNR:ûùô.öÐ}7³=>
01C0h: 33 33 51 3D F8 F9 F4 FF 3E 4D 34 32 20 3E 3C 3C  33Q=øùôÿ>M42 ><<
01D0h: 3A 29 51 3E FA F9 F4 FF 3B 2D 30 2F 2F 3A 2D 51  :)Q>úùôÿ;-0//:-Q
```

TREND MICRO™

I SEE A PATTERN EMERGING

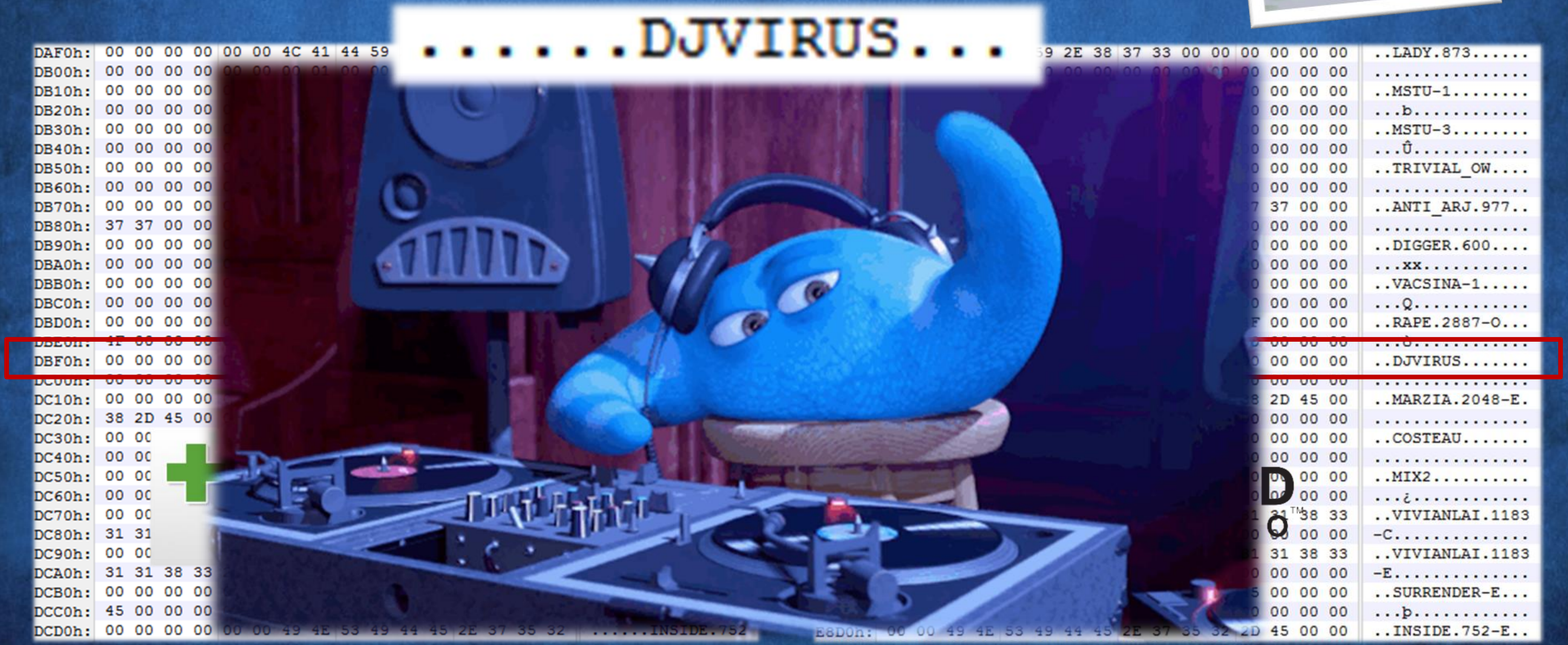


```
DAF0h: 00 00 00 00 00 00 4C 41 44 59 2E 38 37 33 00 00   ......LADY.873..
DB00h: 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00   ................
DB10h: 00 00 00 00 00 00 4D 53 54 55 2D 31 00 00 00 00   ......MSTU-1....
DB20h: 00 00 00 00 00 00 00 62 11 00 00 00 00 00 00 00   .......b........
DB30h: 00 00 00 00 00 00 4D 53 54 55 2D 33 00 00 00 00   ......MSTU-3....
DB40h: 00 00 00 00 00 00 00 DB 05 00 00 00 00 00 00 00   .......Û........
DB50h: 00 00 00 00 00 00 54 52 49 56 49 41 4C 5F 4F 57   ......TRIVIAL_OW
DB60h: 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00   ................
DB70h: 00 00 00 00 00 00 41 4E 54 49 5F 41 52 4A 2E 39   ......ANTI_ARJ.9
DB80h: 37 37 00 00 00 00 00 01 00 00 00 00 00 00 00 00   77..............
DB90h: 00 00 00 00 00 00 44 49 47 47 45 52 2E 36 30 30   ......DIGGER.600
DBA0h: 00 00 00 00 00 00 00 78 78 00 00 00 00 00 00 00   .......xx.......
DBB0h: 00 00 00 00 00 00 56 41 43 53 49 4E 41 2D 31 00   ......VACSINA-1.
DBC0h: 00 00 00 00 00 00 00 51 05 00 00 00 00 00 00 00   .......Q........
DBD0h: 00 00 00 00 00 00 52 41 50 45 2E 32 38 38 37 2D   ......RAPE.2887-
DBE0h: 4F 00 00 00 00 00 00 F2 04 00 00 00 00 00 00 00   O......ò........
DBF0h: 00 00 00 00 00 00 44 4A 56 49 52 55 53 00 00 00   ......DJVIRUS...
DC00h: 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00   ................
DC10h: 00 00 00 00 00 00 4D 41 52 5A 49 41 2E 32 30 34   ......MARZIA.204
DC20h: 38 2D 45 00 00 00 00 01 00 00 00 00 00 00 00 00   8-E.............
DC30h: 00 00                                     00 00   ......COSTEAU...
DC40h: 00 00                                     00 00   ................
DC50h: 00 00                                     00 00   ......MIX2......
DC60h: 00 00                                     00 00   .......¿........
DC70h: 00 00                                     49 2E   ......VIVIANLAI.
DC80h: 31 31                                     00 00   1183-C..........
DC90h: 00 00                                     49 2E   ......VIVIANLAI.
DCA0h: 31 31 38 33 2D 45 00 01 00 00 00 00 00 00 00 00   1183-E..........
DCB0h: 00 00 00 00 00 00 53 55 52 52 45 4E 44 45 52 2D   ......SURRENDER-
DCC0h: 45 00 00 00 00 00 00 FE 10 00 00 00 00 00 00 00   E......þ........
DCD0h: 00 00 00 00 00 00 49 4E 53 49 44 45 2E 37 35 32   ......INSIDE.752
```



```
E6F0h: 00 00 4C 41 44 59 2E 38 37 33 00 00 00 00 00 00   ..LADY.873......
E700h: 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00   ................
E710h: 00 00 4D 53 54 55 2D 31 00 00 00 00 00 00 00 00   ..MSTU-1........
E720h: 00 00 00 62 11 00 00 00 00 00 00 00 00 00 00 00   ...b............
E730h: 00 00 4D 53 54 55 2D 33 00 00 00 00 00 00 00 00   ..MSTU-3........
E740h: 00 00 00 DB 05 00 00 00 00 00 00 00 00 00 00 00   ...Û............
E750h: 00 00 54 52 49 56 49 41 4C 5F 4F 57 00 00 00 00   ..TRIVIAL_OW....
E760h: 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00   ................
E770h: 00 00 41 4E 54 49 5F 41 52 4A 2E 39 37 37 00 00   ..ANTI_ARJ.977..
E780h: 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00   ................
E790h: 00 00 44 49 47 47 45 52 2E 36 30 30 00 00 00 00   ..DIGGER.600....
E7A0h: 00 00 00 78 78 00 00 00 00 00 00 00 00 00 00 00   ...xx...........
E7B0h: 00 00 56 41 43 53 49 4E 41 2D 31 00 00 00 00 00   ..VACSINA-1.....
E7C0h: 00 00 00 51 05 00 00 00 00 00 00 00 00 00 00 00   ...Q............
E7D0h: 00 00 52 41 50 45 2E 32 38 38 37 2D 4F 00 00 00   ..RAPE.2887-O...
E7E0h: 00 00 00 F2 04 00 00 00 00 00 00 00 00 00 00 00   ...ò............
E7F0h: 00 00 44 4A 56 49 52 55 53 00 00 00 00 00 00 00   ..DJVIRUS.......
E800h: 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00   ................
E810h: 00 00 4D 41 52 5A 49 41 2E 32 30 34 38 2D 45 00   ..MARZIA.2048-E.
E820h: 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00   ................
E830h: 00 00 43 4F 53 54 45 41 55 00 00 00 00 00 00 00   ..COSTEAU.......
E840h: 00 00 00          00 00 00 00 00 00 00 00 00 00   ................
E850h: 00 00 4D                               00 00 00   ..MIX2..........
E860h: 00 00 00                               00 00 00   ...¿............
E870h: 00 00 56             4C 41    2E 31 31 38 33      ..VIVIANLAI.1183
E880h: 2D 43 00          00                      00 00   -C..............
E890h: 00 00 56 49    49 41 4E 4C 41 49 2E 31 31 38 33   ..VIVIANLAI.1183
E8A0h: 2D 45 00 01 00 00 00 00 00 00 00 00 00 00 00 00   -E..............
E8B0h: 00 00 53 55 52 52 45 4E 44 45 52 2D 45 00 00 00   ..SURRENDER-E...
E8C0h: 00 00 00 FE 10 00 00 00 00 00 00 00 00 00 00 00   ...þ............
E8D0h: 00 00 49 4E 53 49 44 45 2E 37 35 32 2D 45 00 00   ..INSIDE.752-E..
```

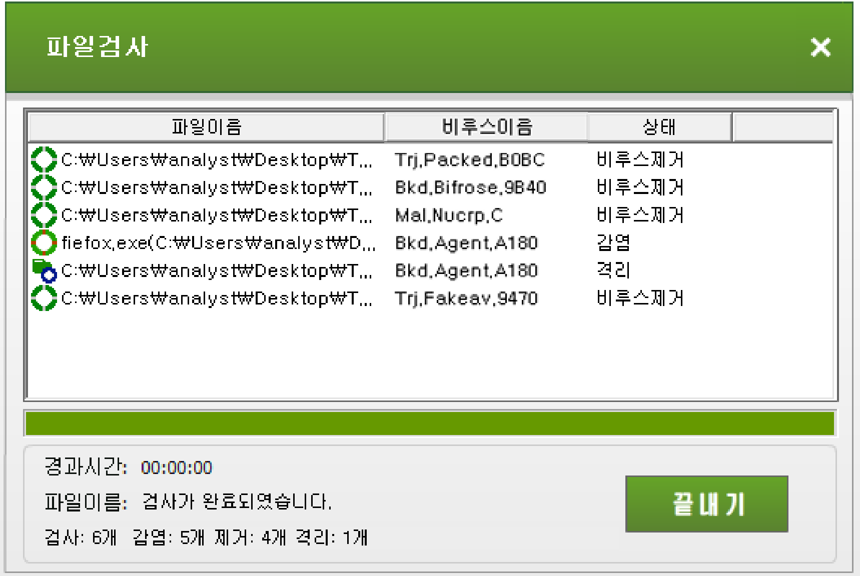
I SEE A PATTERN EMERGING



......DJVIRUS...

```
DAF0h: 00 00 00 00 00 00 4C 41 44 59   59 2E 38 37 33 00 00 00 00 00 00  ..LADY.873......
DB00h: 00 00 00 00 00 00 00 01 00 00   00 00 00 00 00 00 00 00 00 00 00  ................
DB10h: 00 00 00 00                                             0 00 00 00  ..MSTU-1........
DB20h: 00 00 00 00                                             0 00 00 00  ...b............
DB30h: 00 00 00 00                                             0 00 00 00  ..MSTU-3........
DB40h: 00 00 00 00                                             0 00 00 00  ...Û............
DB50h: 00 00 00 00                                             0 00 00 00  ..TRIVIAL_OW....
DB60h: 00 00 00 00                                             0 00 00 00  ................
DB70h: 00 00 00 00                                             7 37 00 00  ..ANTI_ARJ.977..
DB80h: 37 37 00 00                                             0 00 00 00  ................
DB90h: 00 00 00 00                                             0 00 00 00  ..DIGGER.600....
DBA0h: 00 00 00 00                                             0 00 00 00  ...xx...........
DBB0h: 00 00 00 00                                             0 00 00 00  ..VACSINA-1.....
DBC0h: 00 00 00 00                                             0 00 00 00  ...Q............
DBD0h: 00 00 00 00                                             F 00 00 00  ..RAPE.2887-O...
DBE0h: 4F 00 00 00                                             0 00 00 00  ...Ò............
DBF0h: 00 00 00 00                                             0 00 00 00  ..DJVIRUS.......
DC00h: 00 00 00 00                                             0 00 00 00  ................
DC10h: 00 00 00 00                                             8 2D 45 00  ..MARZIA.2048-E.
DC20h: 38 2D 45 00                                             0 00 00 00  ................
DC30h: 00 00                                                   0 00 00 00  ..COSTEAU.......
DC40h: 00 00                                                   0 00 00 00  ................
DC50h: 00 00                                                   0 00 00 00  ..MIX2..........
DC60h: 00 00                                                   0 00 00 00  ...¿............
DC70h: 00 00                                                   1 31 38 33  ..VIVIANLAI.1183
DC80h: 31 31                                                   0 00 00 00  -C..............
DC90h: 00 00                                                   1 31 38 33  ..VIVIANLAI.1183
DCA0h: 31 31 38 33                                             0 00 00 00  -E..............
DCB0h: 00 00 00 00                                             5 00 00 00  ..SURRENDER-E...
DCC0h: 45 00 00 00                                             0 00 00 00  ...þ............
DCD0h: 00 00 00 00 00 00 49 4E 53 49 44 45 2E 37 35 32  ......INSIDE.752
E8D0h: 00 00 49 4E 53 49 44 45 2E 37 35 32 2D 45 00 00  ..INSIDE.752-E..
```

LET ME SEE THOSE NAMES



파일검사 ✕

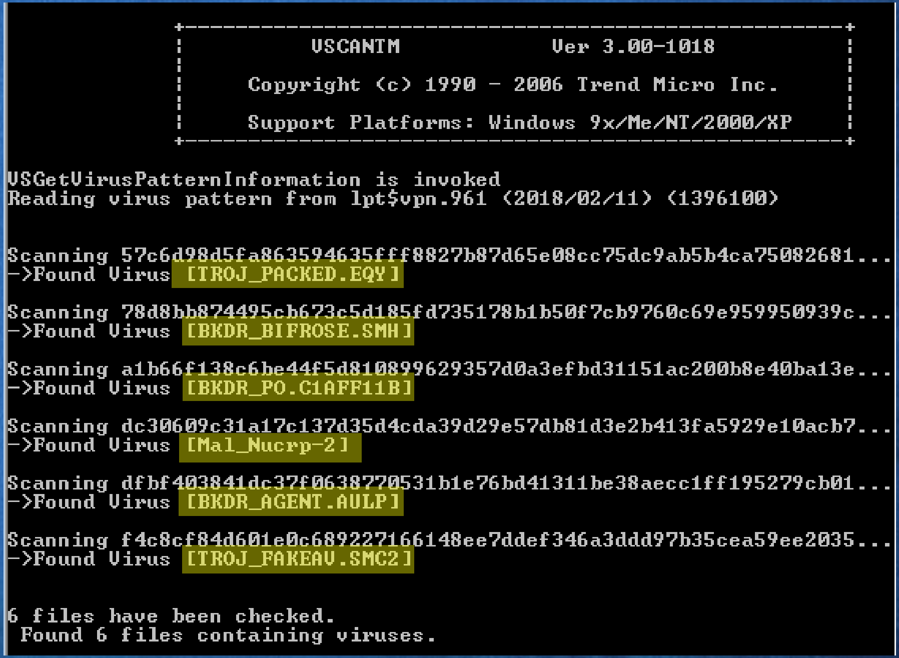
파일이름	바이러스이름	상태
C:₩Users₩analyst₩Desktop₩T...	Trj.Packed.B0BC	바이러스제거
C:₩Users₩analyst₩Desktop₩T...	Bkd.Bifrose.9B40	바이러스제거
C:₩Users₩analyst₩Desktop₩T...	Mal.Nucrp.C	바이러스제거
fiefox.exe(C:₩Users₩analyst₩D...	Bkd.Agent.A180	감염
C:₩Users₩analyst₩Desktop₩T...	Bkd.Agent.A180	격리
C:₩Users₩analyst₩Desktop₩T...	Trj.Fakeav.9470	바이러스제거

경과시간: 00:00:00

파일이름: 검사가 완료되었습니다.

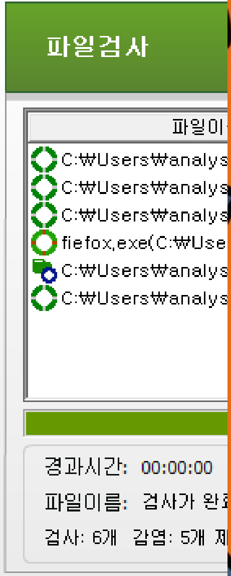
검사: 6개 감염: 5개 제거: 4개 격리: 1개

끝내기



```
          +-----------------------------------------------------+
          |           VSCANTM                  Ver 3.00-1018     |
          |                                                      |
          |       Copyright (c) 1990 - 2006 Trend Micro Inc.     |
          |                                                      |
          |       Support Platforms: Windows 9x/Me/NT/2000/XP    |
          +-----------------------------------------------------+

VSGetVirusPatternInformation is invoked
Reading virus pattern from lpt$vpn.961 (2018/02/11) (1396100)


Scanning 57c6d98d5fa863594635fff8827b87d65e08cc75dc9ab5b4ca75082681...
->Found Virus  [TROJ_PACKED.EQY]

Scanning 78d8bb874495cb673c5d185fd735178b1b50f7cb9760c69e959950939c...
->Found Virus  [BKDR_BIFROSE.SMH]

Scanning a1b66f138c6be44f5d810899629357d0a3efbd31151ac200b8e40ba13e...
->Found Virus  [BKDR_PO.C1AFF11B]

Scanning dc30609c31a17c137d35d4cda39d29e57db81d3e2b413fa5929e10acb7...
->Found Virus  [Mal_Nucrp-2]

Scanning dfbf403841dc37f0638770531b1e76bd41311be38aecc1ff195279cb01...
->Found Virus  [BKDR_AGENT.AULP]

Scanning f4c8cf84d601e0c689227166148ee7ddef346a3ddd97b35cea59ee2035...
->Found Virus  [TROJ_FAKEAV.SMC2]


6 files have been checked.
 Found 6 files containing viruses.
```

LET ME SEE THOSE NAMES

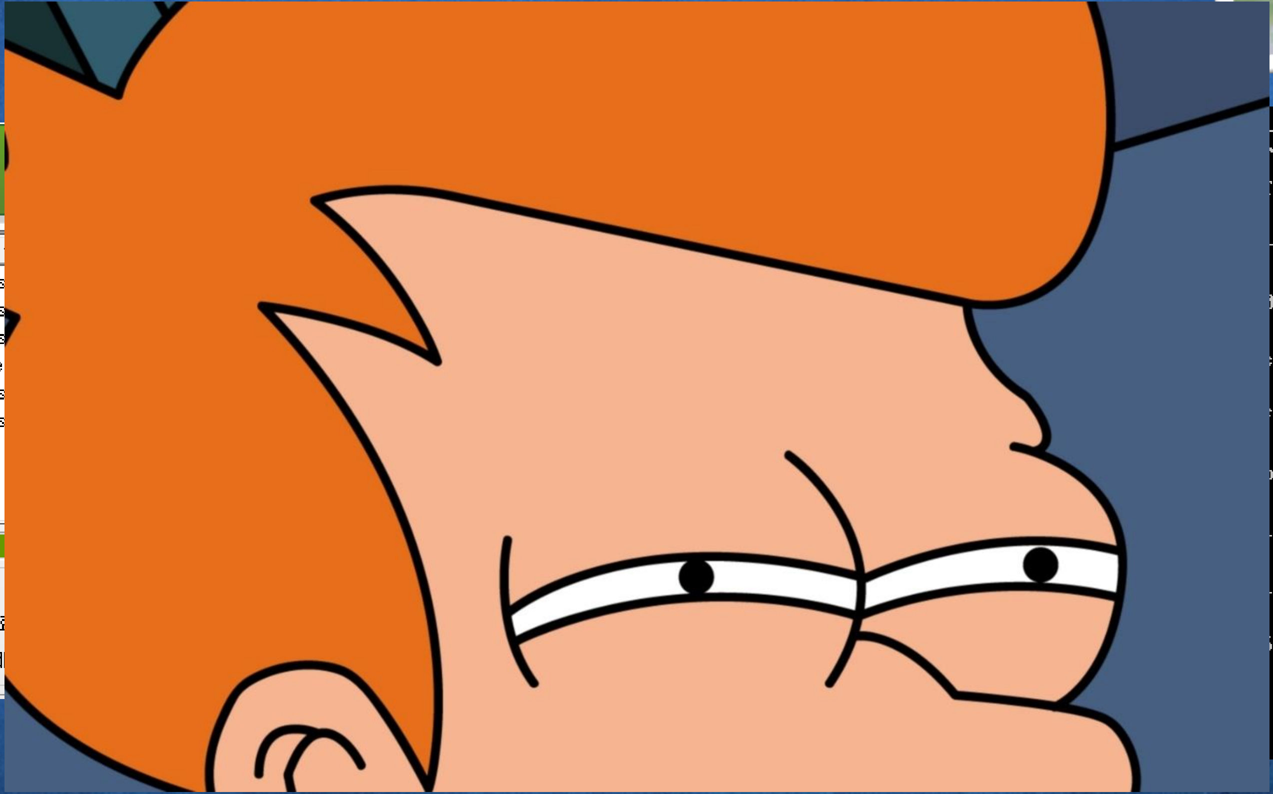


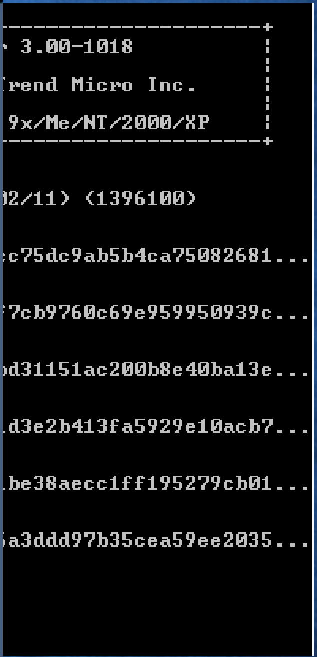
파일검사

파일이

C:₩Users₩analys
C:₩Users₩analys
C:₩Users₩analys
fiefox.exe(C:₩Use
C:₩Users₩analys
C:₩Users₩analys

경과시간: 00:00:00
파일이름: 검사가 완
검사: 6개 감염: 5개 제





```
-------------------------------+
 3.00-1018                     |
Trend Micro Inc.               |
 9x/Me/NT/2000/XP              |
-------------------------------+

02/11) (1396100)

c75dc9ab5b4ca75082681...

f7cb9760c69e959950939c...

bd31151ac200b8e40ba13e...

1d3e2b413fa5929e10acb7...

1be38aecc1ff195279cb01...

5a3ddd97b35cea59ee2035...
```

RENAMING IS EASY

TREND MICRO TROJ_STEAL-1

실리왁찐 4.0 Trj.Steal.B 😉

HOW DO YOU SAY BKDR IN SILI?

prefixes

PE	→	W32
WORM	→	Wrm
BKDR	→	Bkd
Cryp	→	Crp
TROJ	→	Trj
TSPY	→	Spy
Possible	→	Poss
Html	→	Htm

suffixes

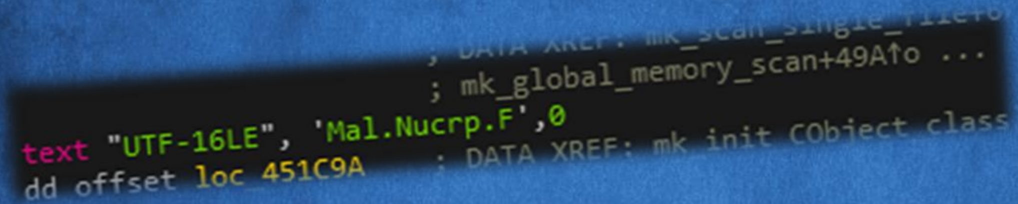
0 - 9	→	A - J
O	→	Org
All Else*	→	Random Hex

HIDING SOMETHING?

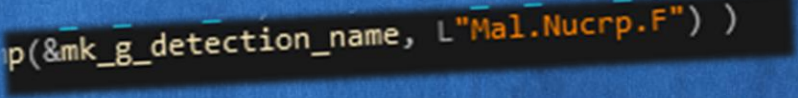
- ✓ files are protected with themida
- ✓ pattern files are encrypted
- ✓ malware signatures are renamed in real time

the ignored signature

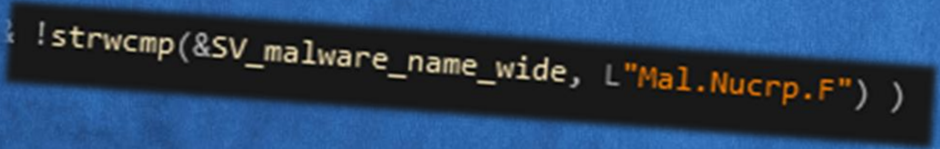
WHAT'S WITH THIS STRING?



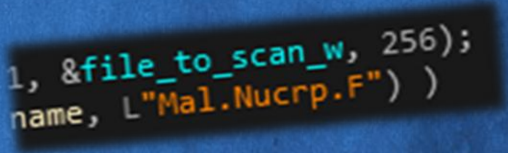
```
                          ; DATA XREF: mk_scan_single_fileto
                          ; mk_global_memory_scan+49A↑o ...
text "UTF-16LE", 'Mal.Nucrp.F',0
dd offset loc_451C9A      ; DATA XREF: mk_init CObject class
```



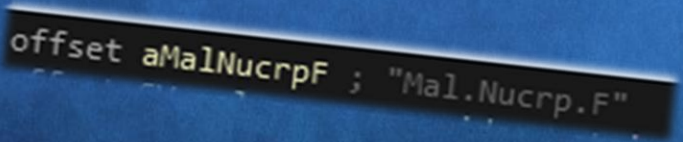
```
p(&mk_g_detection_name, L"Mal.Nucrp.F") )
```



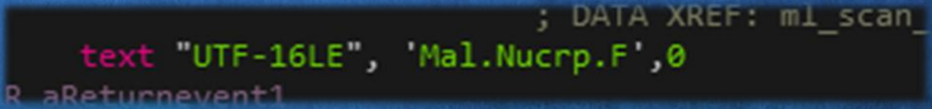
```
!strwcmp(&SV_malware_name_wide, L"Mal.Nucrp.F") )
```



```
1, &file_to_scan_w, 256);
name, L"Mal.Nucrp.F") )
```



```
offset aMalNucrpF ; "Mal.Nucrp.F"
```



```
                            ; DATA XREF: ml_scan_
  text "UTF-16LE", 'Mal.Nucrp.F',0
R aReturnevent1
```

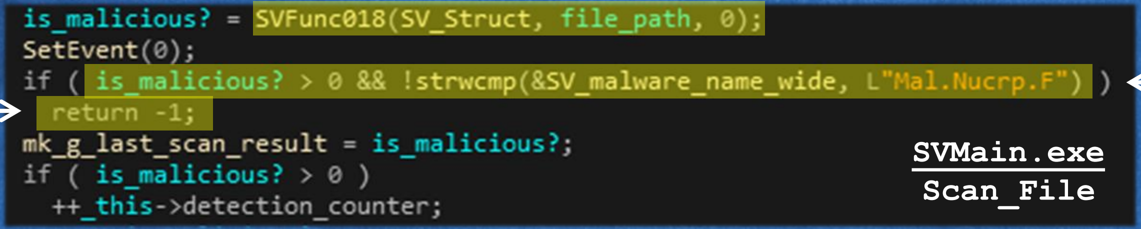
TRANSLATION PLEASE!

TREND MICRO MAL_NUCRP-5

실리왁찐 4.0 Mal.Nucrp.F

WHAT IS GOING ON HERE?

scan file



```
is_malicious? = SVFunc018(SV_Struct, file_path, 0);
SetEvent(0);
if ( is_malicious? > 0 && !strwcmp(&SV_malware_name_wide, L"Mal.Nucrp.F") )
  return -1;
mk_g_last_scan_result = is_malicious?;
if ( is_malicious? > 0 )
  ++_this->detection_counter;
```

SVMain.exe

Scan_File

check if

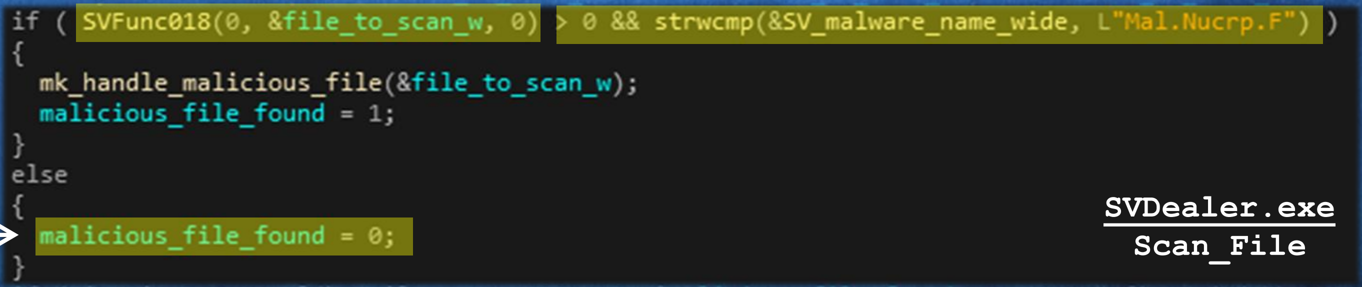
Mal.Nucrp.F

ignore!

scan file

check if not

Mal.Nucrp.F



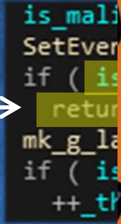
```
if ( SVFunc018(0, &file_to_scan_w, 0) > 0 && strwcmp(&SV_malware_name_wide, L"Mal.Nucrp.F") )
{
  mk_handle_malicious_file(&file_to_scan_w);
  malicious_file_found = 1;
}
else
{
  malicious_file_found = 0;
}
```

ignore!

SVDealer.exe

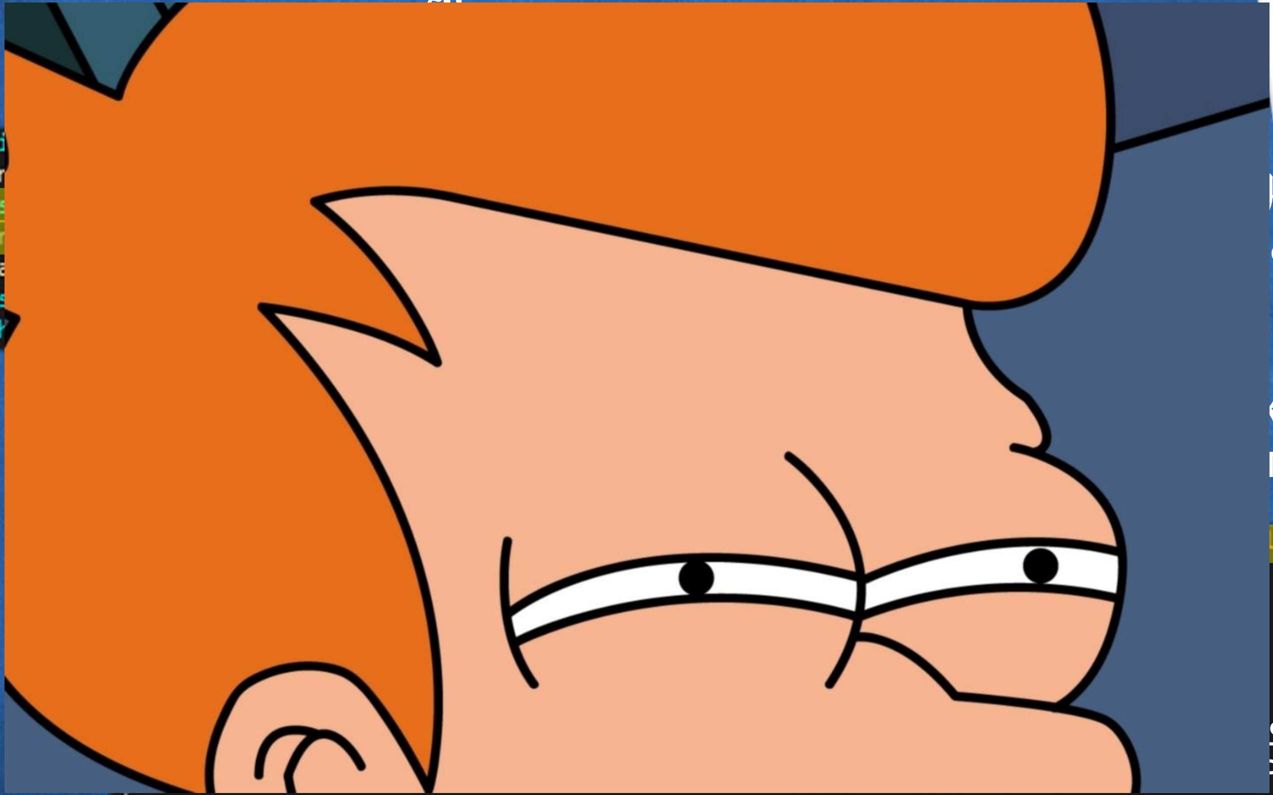
Scan_File

WHAT IS GOING ON HERE?



```
is_mali
SetEver
if ( is
  retur
mk_g_la
if ( is
  ++_th
```

ignore!



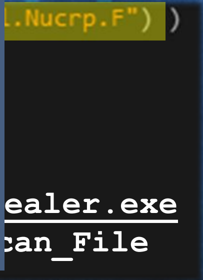
ignore!

k if

crp.F

k if not

Nucrp.F

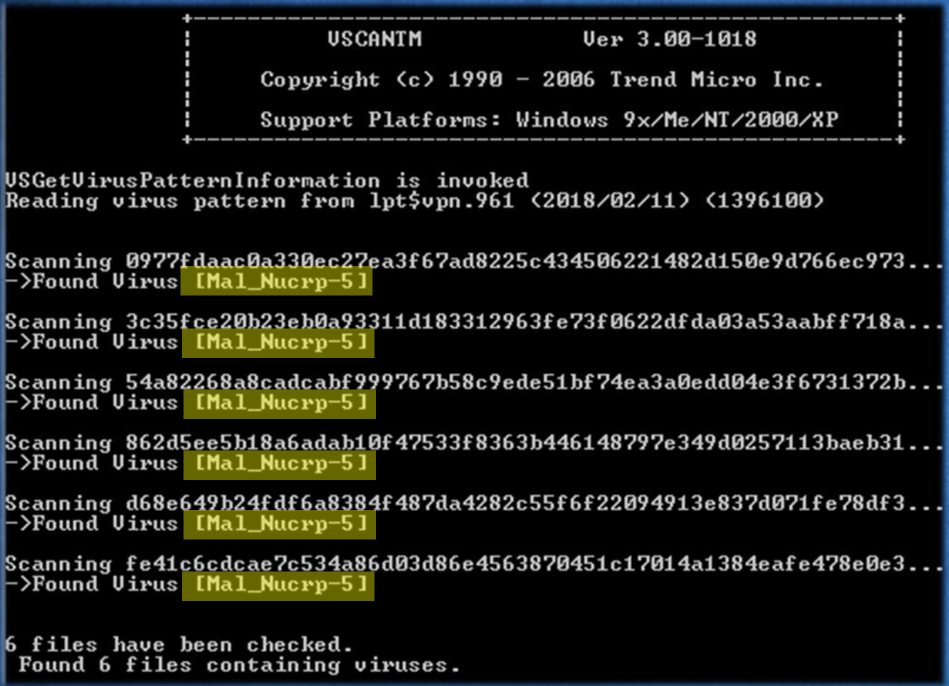


```
.Nucrp.F") )
```

ealer.exe

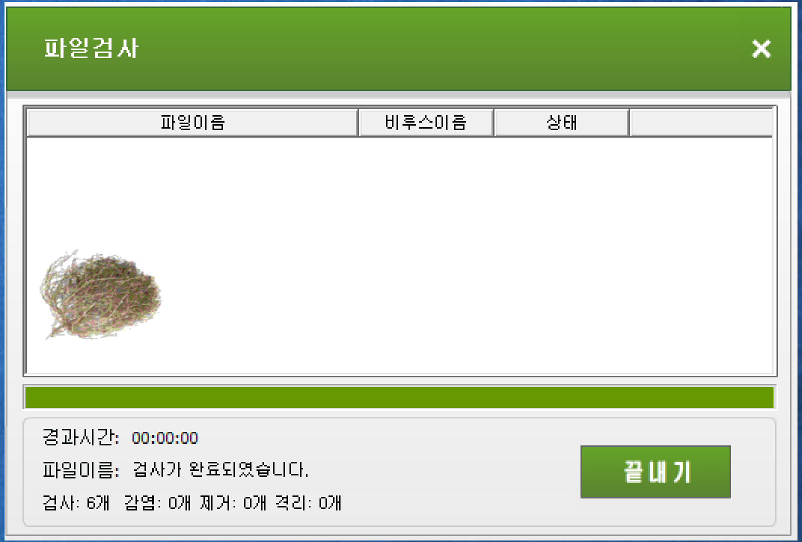
can_File

Scanning: 6 samples



```
          +------------------------------------------------------------+
          |      VSCANTM                Ver 3.00-1018                   |
          |                                                            |
          |    Copyright (c) 1990 - 2006 Trend Micro Inc.              |
          |                                                            |
          |    Support Platforms: Windows 9x/Me/NT/2000/XP             |
          +------------------------------------------------------------+

VSGetVirusPatternInformation is invoked
Reading virus pattern from lpt$vpn.961 (2018/02/11) (1396100)


Scanning 0977fdaac0a330ec27ea3f67ad8225c434506221482d150e9d766ec973...
->Found Virus [Mal_Nucrp-5]

Scanning 3c35fce20b23eb0a93311d183312963fe73f0622dfda03a53aabff718a...
->Found Virus [Mal_Nucrp-5]

Scanning 54a82268a8cadcabf999767b58c9ede51bf74ea3a0edd04e3f6731372b...
->Found Virus [Mal_Nucrp-5]

Scanning 862d5ee5b18a6adab10f47533f8363b446148797e349d0257113baeb31...
->Found Virus [Mal_Nucrp-5]

Scanning d68e649b24fdf6a8384f487da4282c55f6f22094913e837d071fe78df3...
->Found Virus [Mal_Nucrp-5]

Scanning fe41c6cdcae7c534a86d03d86e4563870451c17014a1384eafe478e0e3...
->Found Virus [Mal_Nucrp-5]


6 files have been checked.
 Found 6 files containing viruses.
```

6 / 6 Detections



경과시간: 00:00:00

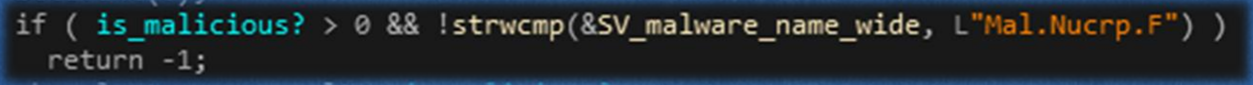
파일이름: 검사가 완료되였습니다.

검사: 6개 감염: 0개 제거: 0개 격리: 0개

0 / 6 Detections

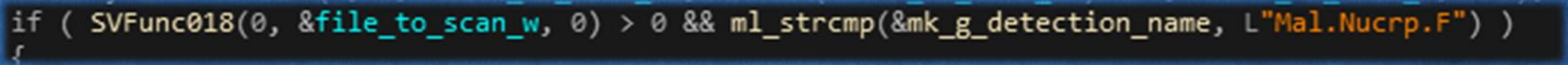
WHITELISTING QA

✓



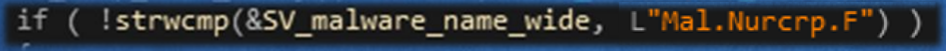
```
if ( is_malicious? > 0 && !strwcmp(&SV_malware_name_wide, L"Mal.Nucrp.F") )
  return -1;
```

✓



```
if ( SVFunc018(0, &file_to_scan_w, 0) > 0 && ml_strcmp(&mk_g_detection_name, L"Mal.Nucrp.F") )
{
```

✗

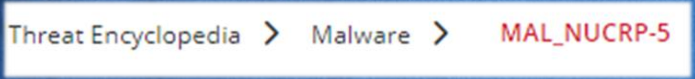


```
if ( !strwcmp(&SV_malware_name_wide, L"Mal.Nurcrp.F") )
```

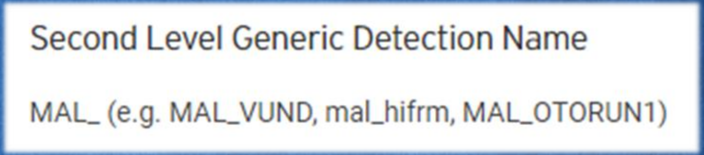
← woops! a typo ☺

NUCRP?

TREND MICRO

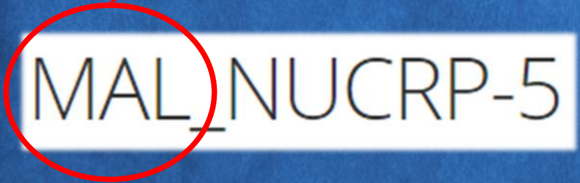


Threat Encyclopedia > Malware > MAL_NUCRP-5

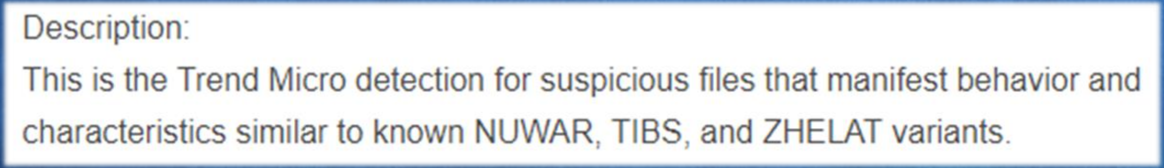


Second Level Generic Detection Name

MAL_ (e.g. MAL_VUND, mal_hifrm, MAL_OTORUN1)



MAL_NUCRP-5



Description:

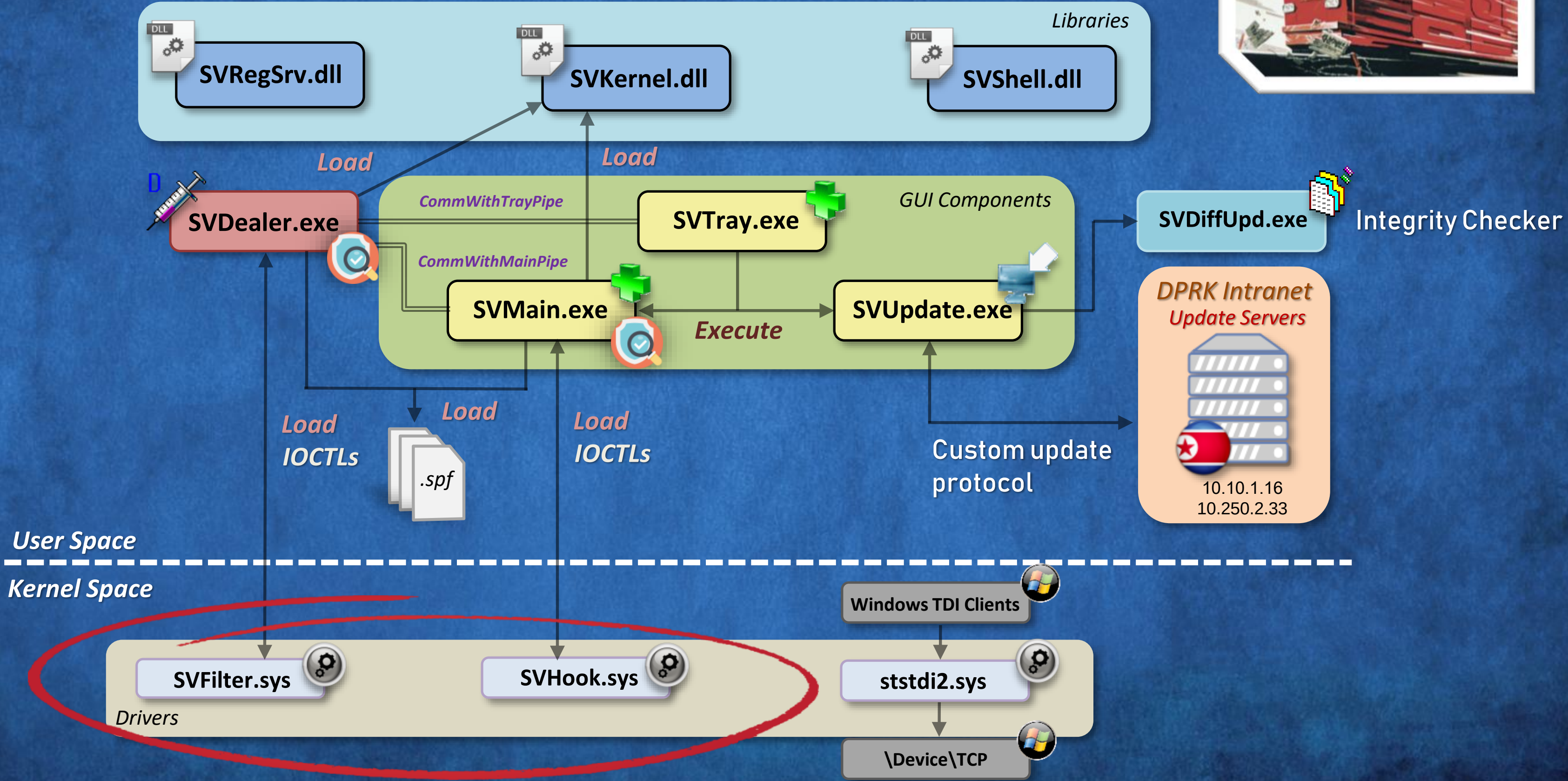
This is the Trend Micro detection for suspicious files that manifest behavior and characteristics similar to known NUWAR, TIBS, and ZHELAT variants.

WHY WHITELIST?

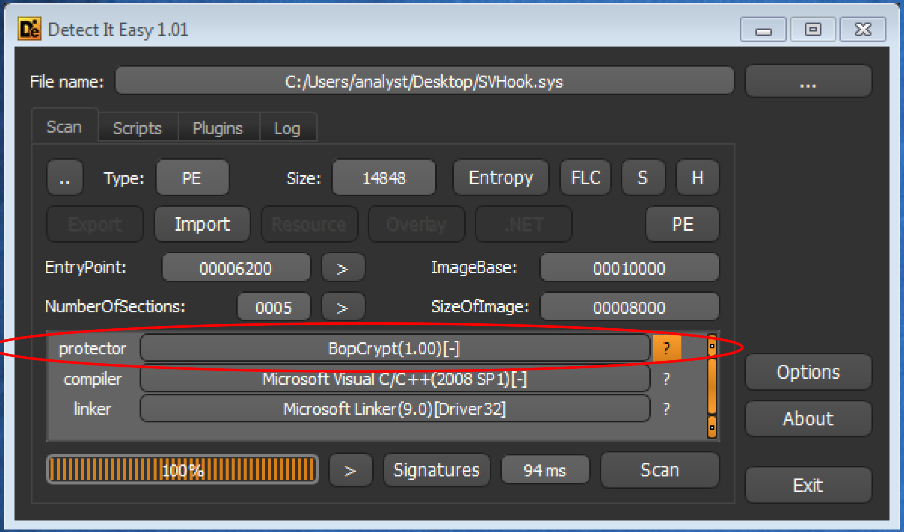
- existing north korean tool ?
- possible future backdoor ?
- detection of a silivaccine component ?
- false positive ☺ ?

the kernel side of silivaccine

A STORY ABOUT 3 DRIVERS



SNOOPING AROUND



File name: C:/Users/analyst/Desktop/SVHook.sys

Type: PE

Size: 14848

EntryPoint: 00006200

ImageBase: 00010000

NumberOfSections: 0005

SizeOfImage: 00008000

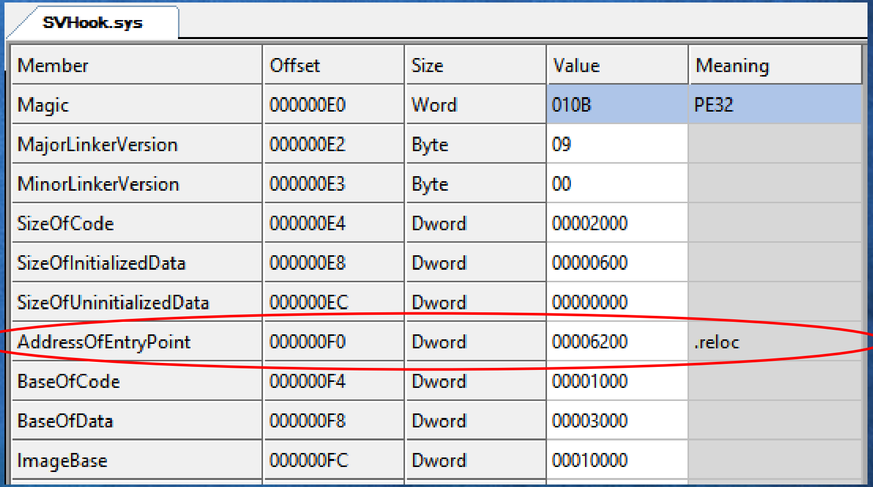
protector BopCrypt(1.00)[-] ?

compiler Microsoft Visual C/C++(2008 SP1)[-] ?

linker Microsoft Linker(9.0)[Driver32] ?

100%

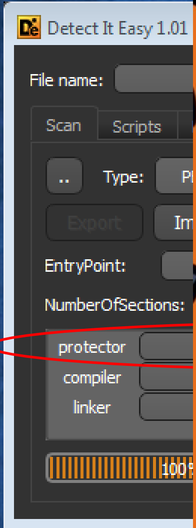
94 ms

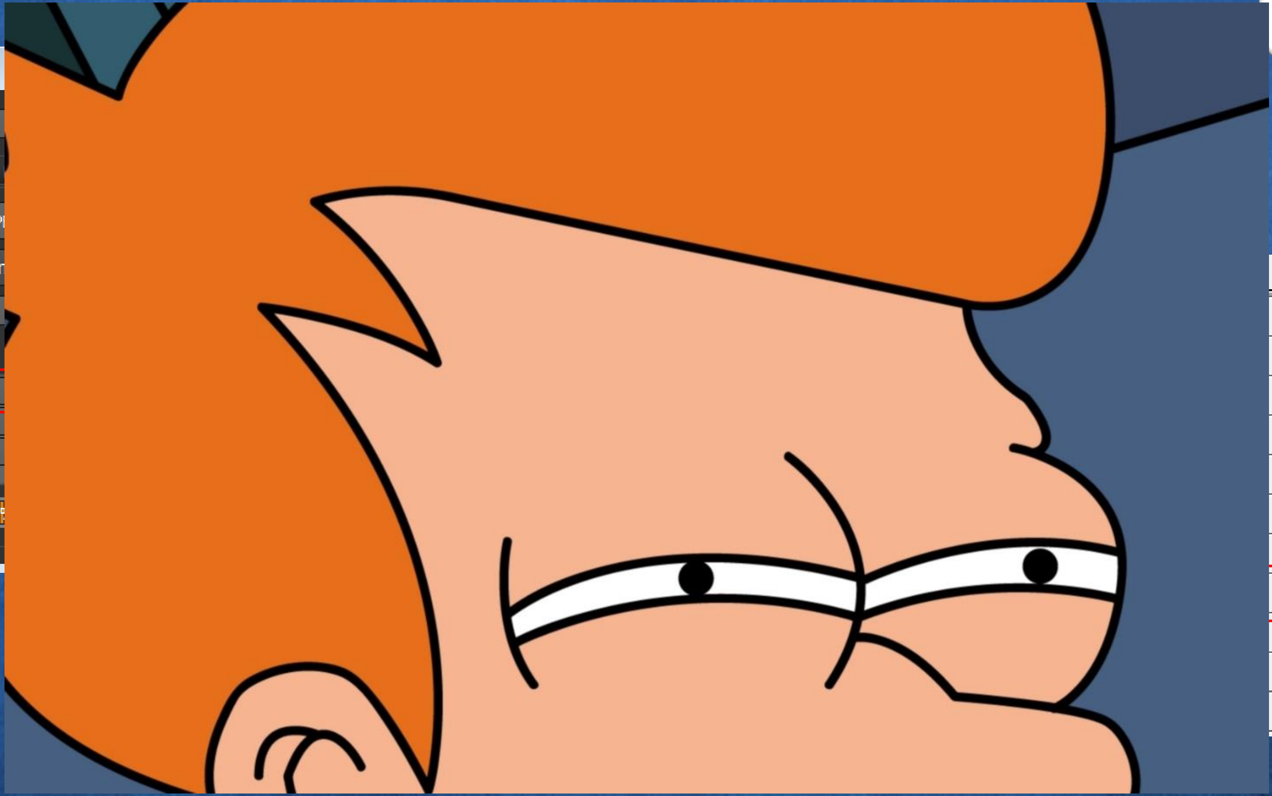


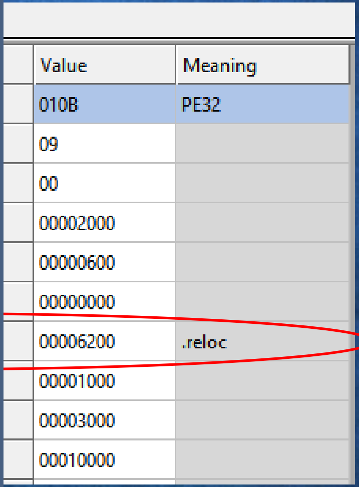
SVHook.sys

Member	Offset	Size	Value	Meaning
Magic	000000E0	Word	010B	PE32
MajorLinkerVersion	000000E2	Byte	09	
MinorLinkerVersion	000000E3	Byte	00	
SizeOfCode	000000E4	Dword	00002000	
SizeOfInitializedData	000000E8	Dword	00000600	
SizeOfUninitializedData	000000EC	Dword	00000000	
AddressOfEntryPoint	000000F0	Dword	00006200	.reloc
BaseOfCode	000000F4	Dword	00001000	
BaseOfData	000000F8	Dword	00003000	
ImageBase	000000FC	Dword	00010000	

SNOOPING AROUND

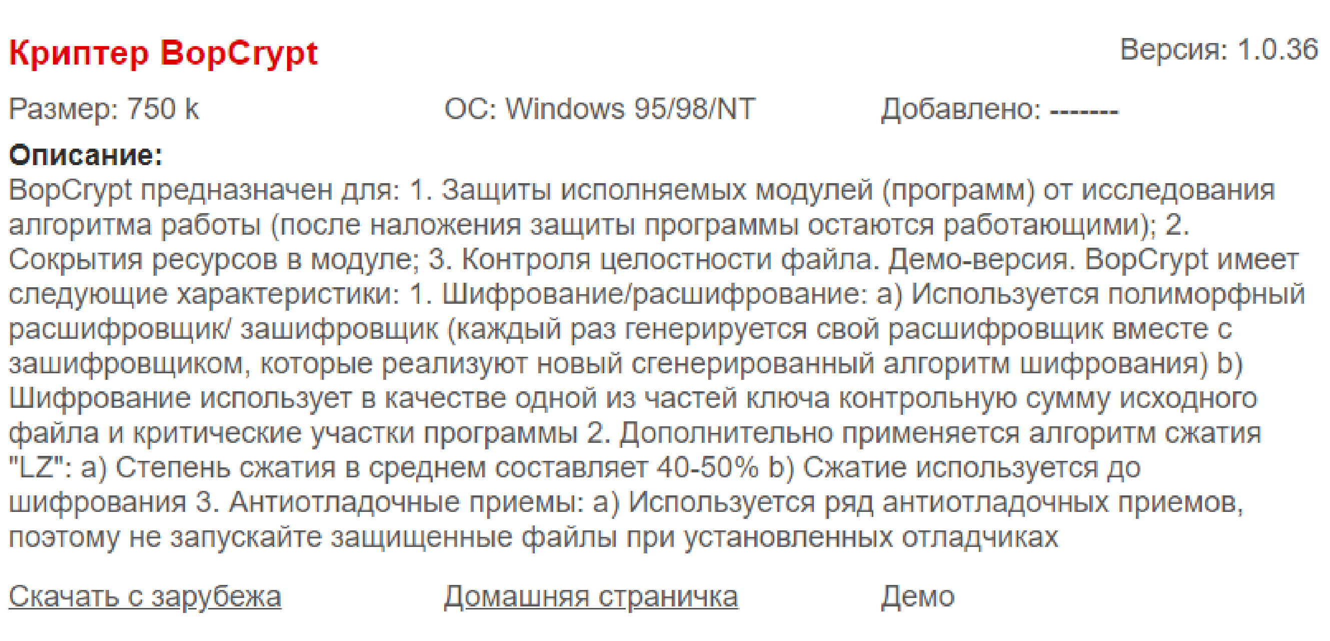






Value	Meaning
010B	PE32
09	
00	
00002000	
00000600	
00000000	
00006200	.reloc
00001000	
00003000	
00010000	

BOPCRYPT?



Криптер BopCrypt

Версия: 1.0.36

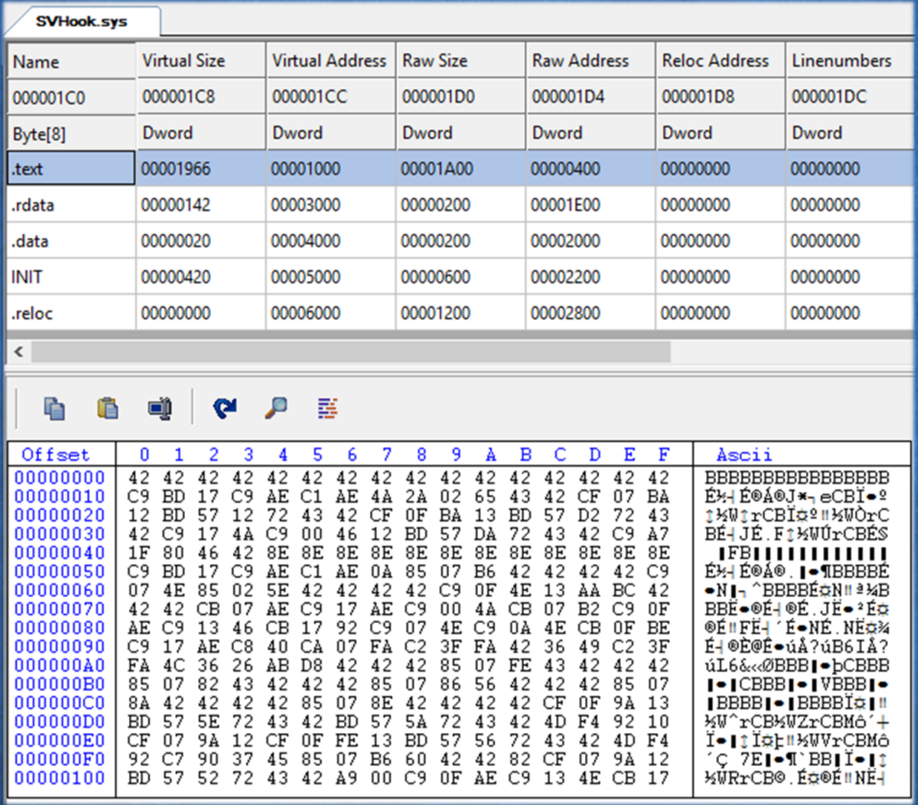
Размер: 750 k   ОС: Windows 95/98/NT   Добавлено: -------

Описание:

BopCrypt предназначен для: 1. Защиты исполняемых модулей (программ) от исследования алгоритма работы (после наложения защиты программы остаются работающими); 2. Сокрытия ресурсов в модуле; 3. Контроля целостности файла. Демо-версия. BopCrypt имеет следующие характеристики: 1. Шифрование/расшифрование: a) Используется полиморфный расшифровщик/ зашифровщик (каждый раз генерируется свой расшифровщик вместе с зашифровщиком, которые реализуют новый сгенерированный алгоритм шифрования) b) Шифрование использует в качестве одной из частей ключа контрольную сумму исходного файла и критические участки программы 2. Дополнительно применяется алгоритм сжатия "LZ": a) Степень сжатия в среднем составляет 40-50% b) Сжатие используется до шифрования 3. Антиотладочные приемы: a) Используется ряд антиотладочных приемов, поэтому не запускайте защищенные файлы при установленных отладчиках

Скачать с зарубежа   Домашняя страничка   Демо

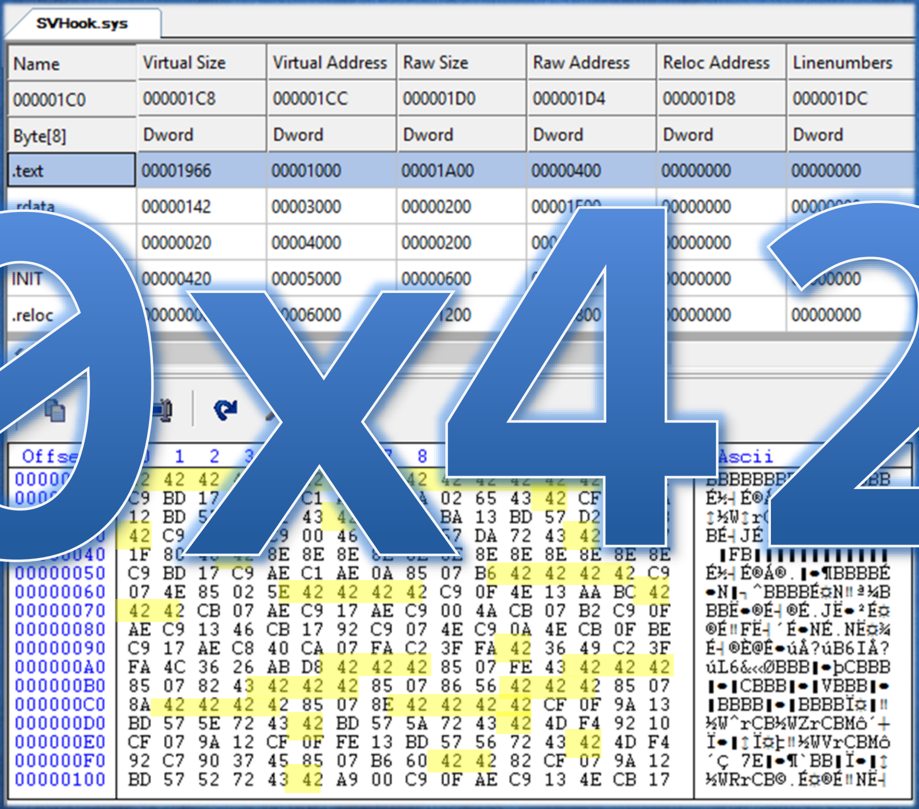
WHAT IS THE ANSWER???



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers
000001C0	000001C8	000001CC	000001D0	000001D4	000001D8	000001DC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
.text	00001966	00001000	00001A00	00000400	00000000	00000000
.rdata	00000142	00003000	00000200	00001E00	00000000	00000000
.data	00000020	00004000	00000200	00002000	00000000	00000000
INIT	00000420	00005000	00000600	00002200	00000000	00000000
.reloc	00000000	00006000	00001200	00002800	00000000	00000000

```
Offset     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    Ascii
00000000  42 42 42 42 42 42 42 42 42 42 42 42 42 42 42 42    BBBBBBBBBBBBBBBB
00000010  C9 BD 17 C9 AE C1 AE 4A 2A 02 65 43 42 CF 07 BA    É½┤É®Á®J*┐eCBÏ•º
00000020  12 BD 57 12 72 43 42 CF 0F BA 13 BD 57 D2 72 43    ↕½W↕rCBÏ¤º‼½WÒrC
00000030  42 C9 17 4A C9 00 46 12 BD 57 DA 72 43 42 C9 A7    BÉ┤JÉ.F↕½WÚrCBÉ§
00000040  1F 80 46 42 8E 8E 8E 8E 8E 8E 8E 8E 8E 8E 8E 8E     ▌FB▌▌▌▌▌▌▌▌▌▌▌▌
00000050  C9 BD 17 C9 AE C1 AE 0A 85 07 B6 42 42 42 42 C9    É½┤É®Á®.▌•¶BBBBÉ
00000060  07 4E 85 02 5E 42 42 42 42 C9 0F 4E 13 AA BC 42    •N▌┐^BBBBÉ¤N‼ª¼B
00000070  42 42 CB 07 AE C9 17 AE C9 00 4A CB 07 B2 C9 0F    BBË•®É┤®É.JË•²É¤
00000080  AE C9 13 46 CB 17 92 C9 07 4E C9 0A 4E CB 0F BE    ®É‼FË┤´É•NÉ.NË¤¾
00000090  C9 17 AE C8 40 CA 07 FA C2 3F FA 42 36 49 C2 3F    É┤®È@Ê•úÂ?úB6IÂ?
000000A0  FA 4C 36 26 AB D8 42 42 42 85 07 FE 43 42 42 42    úL6&«ØBBB▌•þCBBB
000000B0  85 07 82 43 42 42 42 85 07 86 56 42 42 42 85 07    ▌•▌CBBB▌•▌VBBB▌•
000000C0  8A 42 42 42 42 85 07 8E 42 42 42 42 CF 0F 9A 13    ▌BBBB▌•▌BBBBÏ¤▌‼
000000D0  BD 57 5E 72 43 42 BD 57 5A 72 43 42 4D F4 92 10    ½W^rCB½WZrCBMô´┼
000000E0  CF 07 9A 12 CF 0F FE 13 BD 57 56 72 43 42 4D F4    Ï•▌↕Ï¤þ‼½WVrCBMô
000000F0  92 C7 90 37 45 85 07 B6 60 42 42 82 CF 07 9A 12    ´Ç 7E▌•¶`BB▌Ï•▌↕
00000100  BD 57 52 72 43 42 A9 00 C9 0F AE C9 13 4E CB 17    ½WRrCB©.É¤®É‼NË┤
```

WHAT IS THE ANSWER???



SVHook.sys

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers
000001C0	000001C8	000001CC	000001D0	000001D4	000001D8	000001DC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword
.text	00001966	00001000	00001A00	00000400	00000000	00000000
.rdata	00000142	00003000	00000200	00001E00	00000000	[illegible]
[illegible]	00000020	00004000	00000200	[illegible]	[illegible]	[illegible]
INIT	00000420	00005000	00000600	[illegible]	[illegible]	[illegible]
.reloc	[illegible]	00006000	[illegible]	[illegible]	00000000	00000000

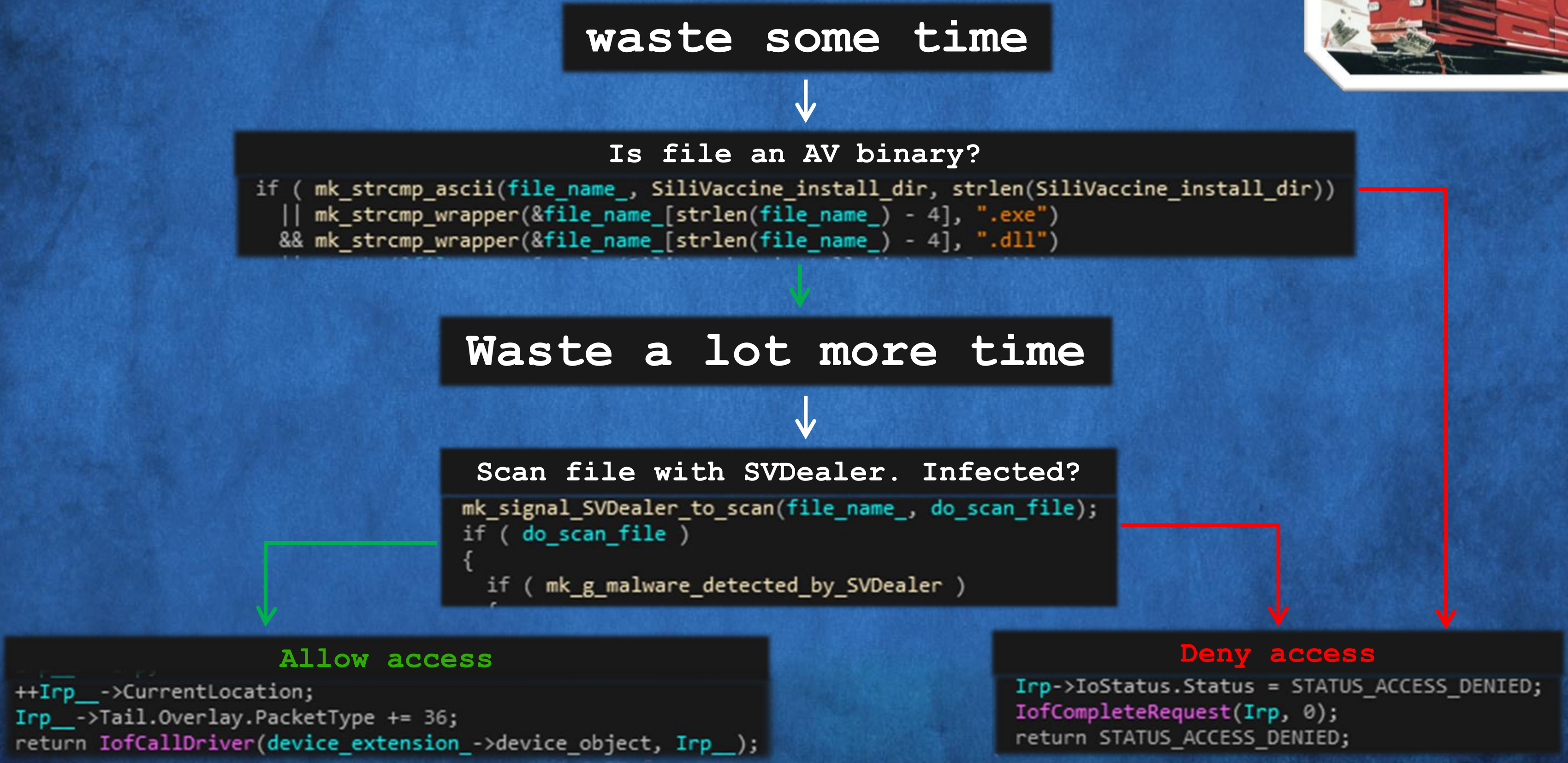
```
Offset    0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   Ascii
00000050  C9 BD 17 C9 AE C1 AE 0A 85 07 B6 42 42 42 42 C9  É½┤É®Á®.▌•¶BBBBÉ
00000060  07 4E 85 02 5E 42 42 42 42 C9 0F 4E 13 AA BC 42  •N▌¬^BBBBÉ☼N‼ª¼B
00000070  42 42 CB 07 AE C9 17 AE C9 00 4A CB 07 B2 C9 0F  BBË•®É┤®É.JË•²É☼
00000080  AE C9 13 46 CB 17 92 C9 07 4E C9 0A 4E CB 0F BE  ®É‼FË┤´É•NÉ.NË☼¾
00000090  C9 17 AE C8 40 CA 07 FA C2 3F FA 42 36 49 C2 3F  É┤®È@Ê•úÂ?úB6IÂ?
000000A0  FA 4C 36 26 AB D8 42 42 42 85 07 FE 43 42 42 42  úL6&«ØBBB▌•þCBBB
000000B0  85 07 82 43 42 42 42 85 07 86 56 42 42 42 85 07  ▌•▌CBBB▌•▌VBBB▌•
000000C0  8A 42 42 42 42 85 07 8E 42 42 42 42 CF 0F 9A 13  ▌BBBB▌•▌BBBBÏ☼▌‼
000000D0  BD 57 5E 72 43 42 BD 57 5A 72 43 42 4D F4 92 10  ½W^rCB½WZrCBMô´┼
000000E0  CF 07 9A 12 CF 0F FE 13 BD 57 56 72 43 42 4D F4  Ï•▌↕Ï☼þ‼½WVrCBMô
000000F0  92 C7 90 37 45 85 07 B6 60 42 42 82 CF 07 9A 12  ´Ç 7E▌•¶`BB▌Ï•▌↕
00000100  BD 57 52 72 43 42 A9 00 C9 0F AE C9 13 4E CB 17  ½WRrCB©.É☼®É‼NË┤
```

0x42

SVFILTER.SYS

- file system filter driver
- loaded and utilized by `SVDealer.exe`
- 2 main functionalities:
  - real time scanning on file access
  - protection of anti virus binaries

SVFILTER.SYS IN A NUTSHELL



waste some time

Is file an AV binary?

```
if ( mk_strcmp_ascii(file_name_, SiliVaccine_install_dir, strlen(SiliVaccine_install_dir))
  || mk_strcmp_wrapper(&file_name_[strlen(file_name_) - 4], ".exe")
  && mk_strcmp_wrapper(&file_name_[strlen(file_name_) - 4], ".dll")
```

Waste a lot more time

Scan file with SVDealer. Infected?

```
mk_signal_SVDealer_to_scan(file_name_, do_scan_file);
if ( do_scan_file )
{
  if ( mk_g_malware_detected_by_SVDealer )
```

Allow access

```
++Irp__->CurrentLocation;
Irp__->Tail.Overlay.PacketType += 36;
return IofCallDriver(device_extension_->device_object, Irp__);
```

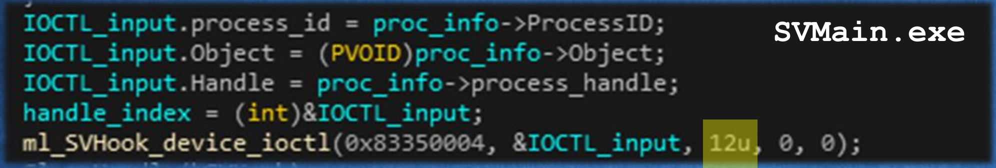
Deny access

```
Irp->IoStatus.Status = STATUS_ACCESS_DENIED;
IofCompleteRequest(Irp, 0);
return STATUS_ACCESS_DENIED;
```

SVHOOK.SYS

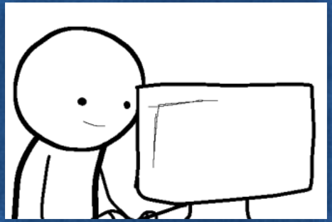
- loaded and utilized by SVMain.exe
- doesnt actually hook anything
- used to query object metadata from kernel
- odd and confusing...
  - contains 13 ioctls, only 3 are ever used
  - very buggy

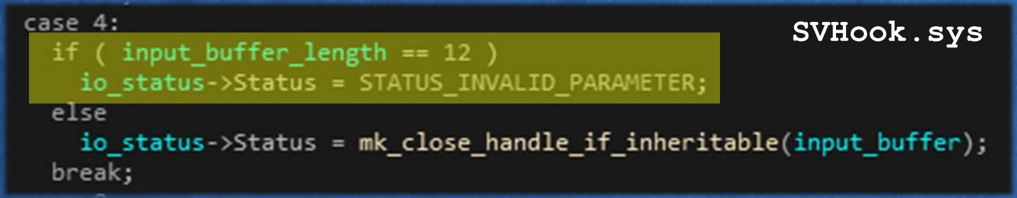
YOU COPY?



SVMain.exe

```
IOCTL_input.process_id = proc_info->ProcessID;
IOCTL_input.Object = (PVOID)proc_info->Object;
IOCTL_input.Handle = proc_info->process_handle;
handle_index = (int)&IOCTL_input;
ml_SVHook_device_ioctl(0x83350004, &IOCTL_input, 12u, 0, 0);
```

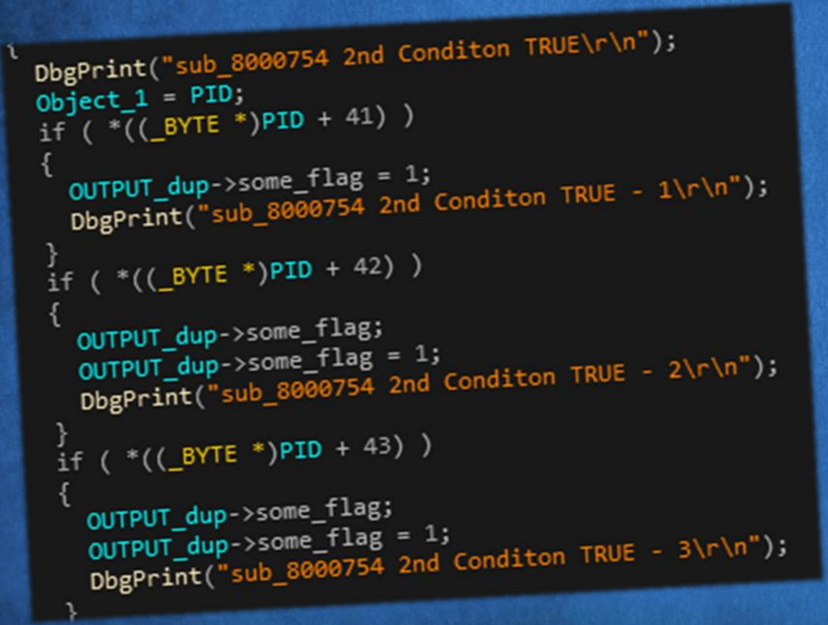




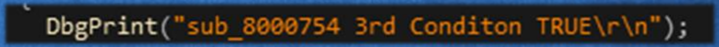
SVHook.sys

```
case 4:
  if ( input_buffer_length == 12 )
    io_status->Status = STATUS_INVALID_PARAMETER;
  else
    io_status->Status = mk_close_handle_if_inheritable(input_buffer);
  break;
```

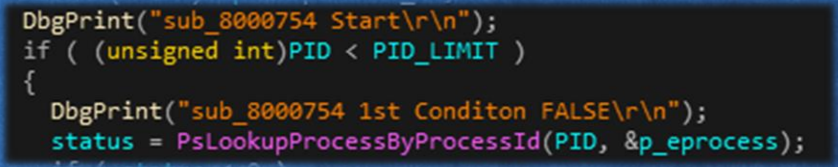
OH YES I COPY



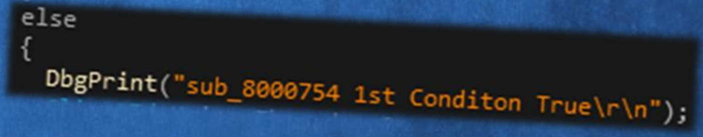
```
{
  DbgPrint("sub_8000754 2nd Conditon TRUE\r\n");
  Object_1 = PID;
  if ( *((_BYTE *)PID + 41) )
  {
    OUTPUT_dup->some_flag = 1;
    DbgPrint("sub_8000754 2nd Conditon TRUE - 1\r\n");
  }
  if ( *((_BYTE *)PID + 42) )
  {
    OUTPUT_dup->some_flag;
    OUTPUT_dup->some_flag = 1;
    DbgPrint("sub_8000754 2nd Conditon TRUE - 2\r\n");
  }
  if ( *((_BYTE *)PID + 43) )
  {
    OUTPUT_dup->some_flag;
    OUTPUT_dup->some_flag = 1;
    DbgPrint("sub_8000754 2nd Conditon TRUE - 3\r\n");
  }
```



```
  DbgPrint("sub_8000754 3rd Conditon TRUE\r\n");
```

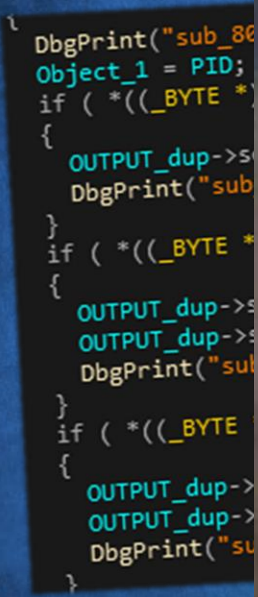


```
DbgPrint("sub_8000754 Start\r\n");
if ( (unsigned int)PID < PID_LIMIT )
{
  DbgPrint("sub_8000754 1st Conditon FALSE\r\n");
  status = PsLookupProcessByProcessId(PID, &p_eprocess);
```

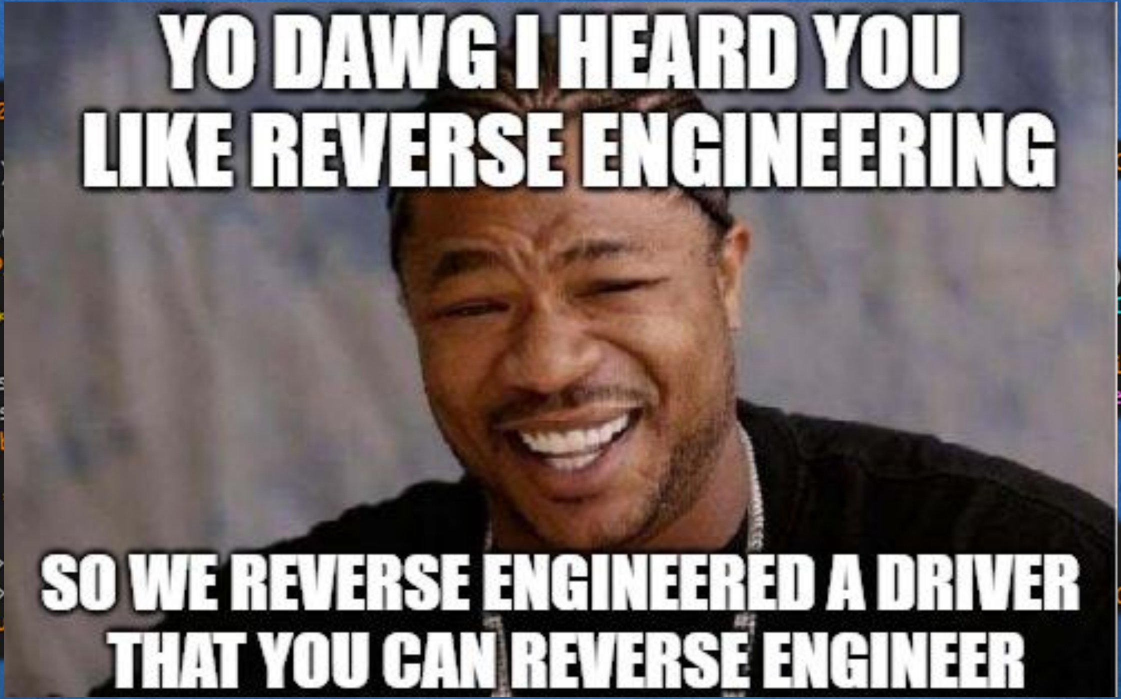


```
else
{
  DbgPrint("sub_8000754 1st Conditon True\r\n");
```

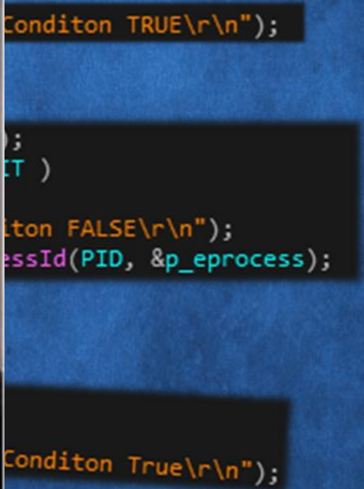
OH YES I COPY



```
{
  DbgPrint("sub_80
  Object_1 = PID;
  if ( *((_BYTE *)
  {
    OUTPUT_dup->s
    DbgPrint("sub
  }
  if ( *((_BYTE *
  {
    OUTPUT_dup->s
    OUTPUT_dup->s
    DbgPrint("sub
  }
  if ( *((_BYTE
  {
    OUTPUT_dup->
    OUTPUT_dup->
    DbgPrint("su
  }
```



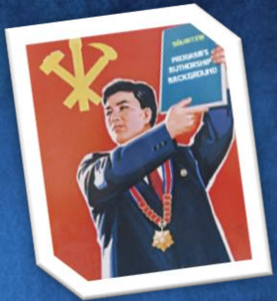
YO DAWG I HEARD YOU LIKE REVERSE ENGINEERING
SO WE REVERSE ENGINEERED A DRIVER THAT YOU CAN REVERSE ENGINEER

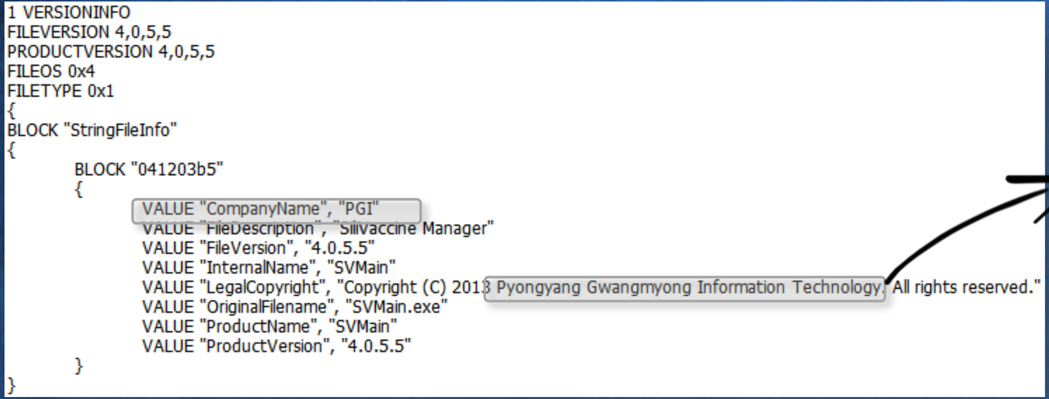


```
Conditon TRUE\r\n");

);
IT )

iton FALSE\r\n");
essId(PID, &p_eprocess);

Conditon True\r\n");
```

who is behind silivaccine?

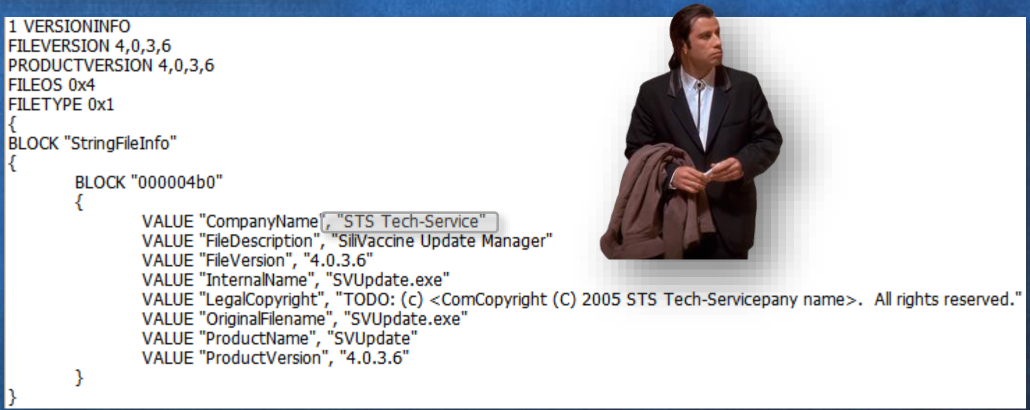
VERSION INFO





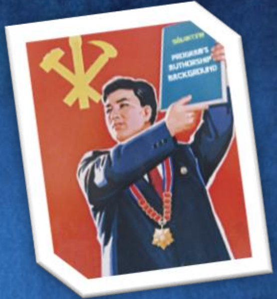
```
1 VERSIONINFO
FILEVERSION 4,0,5,5
PRODUCTVERSION 4,0,5,5
FILEOS 0x4
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
        BLOCK "041203b5"
        {
                VALUE "CompanyName", "PGI"
                VALUE "FileDescription", "Silivaccine Manager"
                VALUE "FileVersion", "4.0.5.5"
                VALUE "InternalName", "SVMain"
                VALUE "LegalCopyright", "Copyright (C) 2013 Pyongyang Gwangmyong Information Technology. All rights reserved."
                VALUE "OriginalFilename", "SVMain.exe"
                VALUE "ProductName", "SVMain"
                VALUE "ProductVersion", "4.0.5.5"
        }
}
```

- North korean establishment
- Appeared as author of other technological developments in DPRK
  - Specializes in network security software

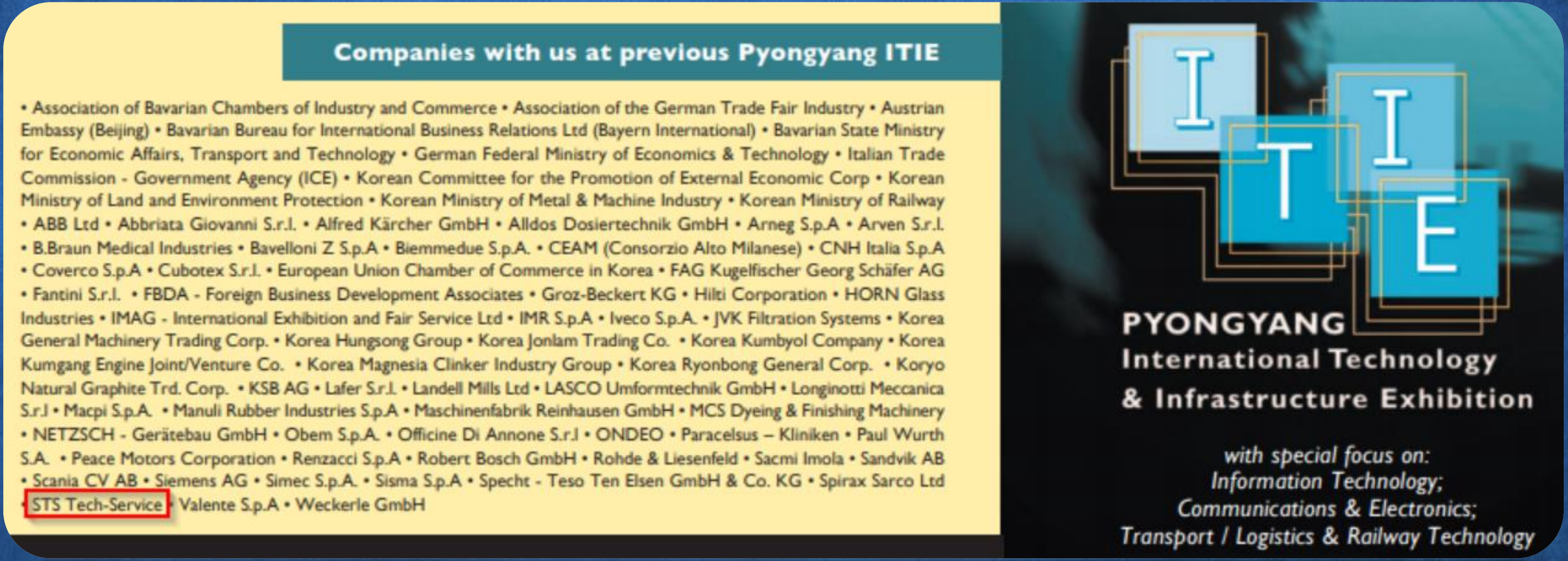


```
1 VERSIONINFO
FILEVERSION 4,0,3,6
PRODUCTVERSION 4,0,3,6
FILEOS 0x4
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
        BLOCK "000004b0"
        {
                VALUE "CompanyName", "STS Tech-Service"
                VALUE "FileDescription", "SiliVaccine Update Manager"
                VALUE "FileVersion", "4.0.3.6"
                VALUE "InternalName", "SVUpdate.exe"
                VALUE "LegalCopyright", "TODO: (c) <ComCopyright (C) 2005 STS Tech-Servicepany name>.  All rights reserved."
                VALUE "OriginalFilename", "SVUpdate.exe"
                VALUE "ProductName", "SVUpdate"
                VALUE "ProductVersion", "4.0.3.6"
        }
}
```

WHO'S STS TECH-SERVICE?



- based in the dprk



Companies with us at previous Pyongyang ITIE

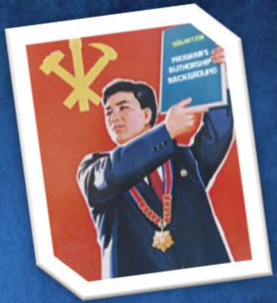
• Association of Bavarian Chambers of Industry and Commerce • Association of the German Trade Fair Industry • Austrian Embassy (Beijing) • Bavarian Bureau for International Business Relations Ltd (Bayern International) • Bavarian State Ministry for Economic Affairs, Transport and Technology • German Federal Ministry of Economics & Technology • Italian Trade Commission - Government Agency (ICE) • Korean Committee for the Promotion of External Economic Corp • Korean Ministry of Land and Environment Protection • Korean Ministry of Metal & Machine Industry • Korean Ministry of Railway • ABB Ltd • Abbriata Giovanni S.r.l. • Alfred Kärcher GmbH • Alldos Dosiertechnik GmbH • Arneg S.p.A • Arven S.r.l. • B.Braun Medical Industries • Bavelloni Z S.p.A • Biemmedue S.p.A. • CEAM (Consorzio Alto Milanese) • CNH Italia S.p.A • Coverco S.p.A • Cubotex S.r.l. • European Union Chamber of Commerce in Korea • FAG Kugelfischer Georg Schäfer AG • Fantini S.r.l. • FBDA - Foreign Business Development Associates • Groz-Beckert KG • Hilti Corporation • HORN Glass Industries • IMAG - International Exhibition and Fair Service Ltd • IMR S.p.A • Iveco S.p.A. • JVK Filtration Systems • Korea General Machinery Trading Corp. • Korea Hungsong Group • Korea Jonlam Trading Co. • Korea Kumbyol Company • Korea Kumgang Engine Joint/Venture Co. • Korea Magnesia Clinker Industry Group • Korea Ryonbong General Corp. • Koryo Natural Graphite Trd. Corp. • KSB AG • Lafer S.r.l. • Landell Mills Ltd • LASCO Umformtechnik GmbH • Longinotti Meccanica S.r.l • Macpi S.p.A. • Manuli Rubber Industries S.p.A • Maschinenfabrik Reinhausen GmbH • MCS Dyeing & Finishing Machinery • NETZSCH - Gerätebau GmbH • Obem S.p.A. • Officine Di Annone S.r.l • ONDEO • Paracelsus – Kliniken • Paul Wurth S.A. • Peace Motors Corporation • Renzacci S.p.A • Robert Bosch GmbH • Rohde & Liesenfeld • Sacmi Imola • Sandvik AB • Scania CV AB • Siemens AG • Simec S.p.A. • Sisma S.p.A • Specht - Teso Ten Elsen GmbH & Co. KG • Spirax Sarco Ltd • STS Tech-Service • Valente S.p.A • Weckerle GmbH

ITIE

PYONGYANG
International Technology
& Infrastructure Exhibition

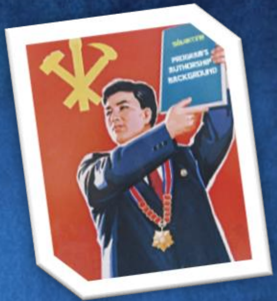
with special focus on:
Information Technology;
Communications & Electronics;
Transport / Logistics & Railway Technology

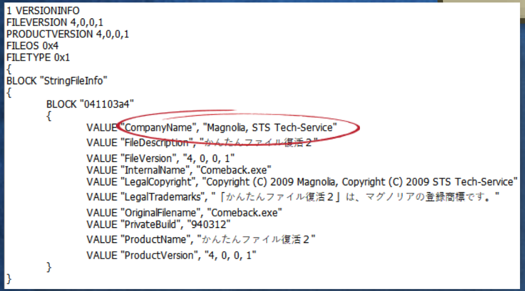
WHO'S STS TECH-SERVICE?



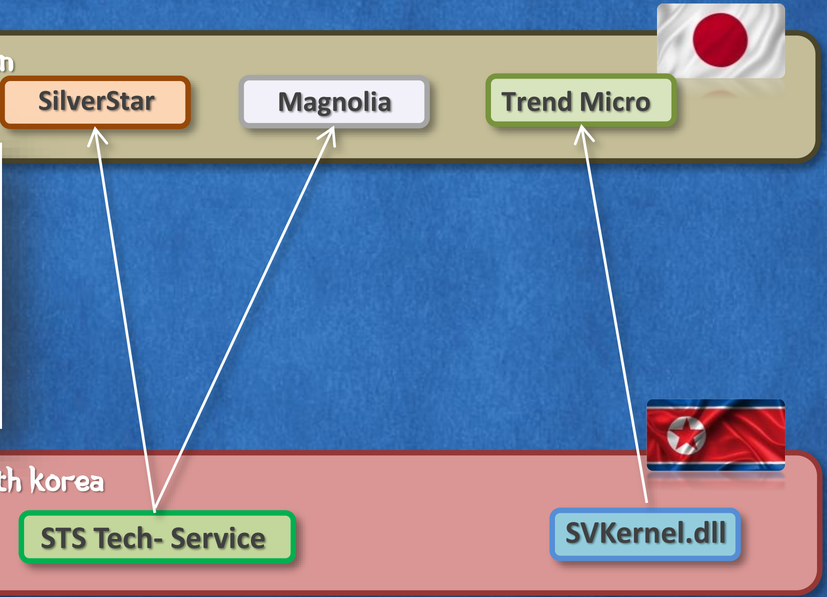
- based in the dprk
  - government entity? or private company?
- according to a source: subdivision of the kpa
  - korea peoples army
- trend micro states engine leaked from a 3rd party
  - is the company connected with other companies outside dprk?

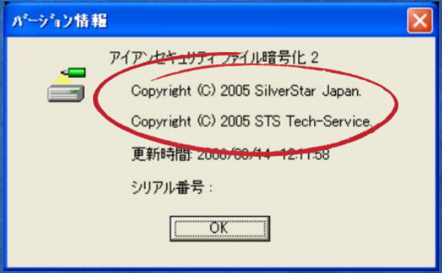
THE JAPANESE CONNECTION





```
1 VERSIONINFO
FILEVERSION 4,0,0,1
PRODUCTVERSION 4,0,0,1
FILEOS 0x4
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
        BLOCK "041103a4"
        {
                VALUE "CompanyName", "Magnolia, STS Tech-Service"
                VALUE "FileDescription", "かんたんファイル復活２"
                VALUE "FileVersion", "4, 0, 0, 1"
                VALUE "InternalName", "Comeback.exe"
                VALUE "LegalCopyright", "Copyright (C) 2009 Magnolia, Copyright (C) 2009 STS Tech-Service"
                VALUE "LegalTrademarks", "「かんたんファイル復活２」は、マグノリアの登録商標です。"
                VALUE "OriginalFilename", "Comeback.exe"
                VALUE "PrivateBuild", "940312"
                VALUE "ProductName", "かんたんファイル復活２"
                VALUE "ProductVersion", "4, 0, 0, 1"
        }
}
```





アイアンセキュリティ ファイル暗号化 2

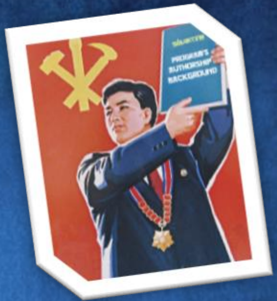
Copyright (C) 2005 SilverStar Japan.

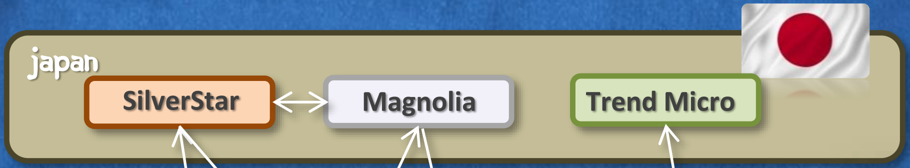
Copyright (C) 2005 STS Tech-Service.

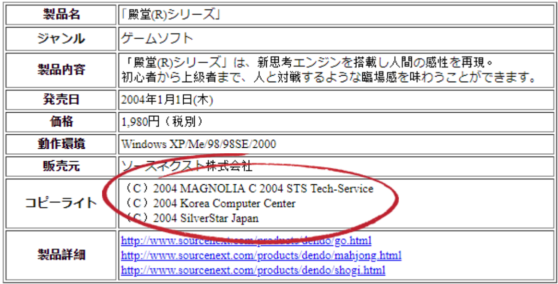
更新時間: 2006/08/14 12:11:58

シリアル番号 :

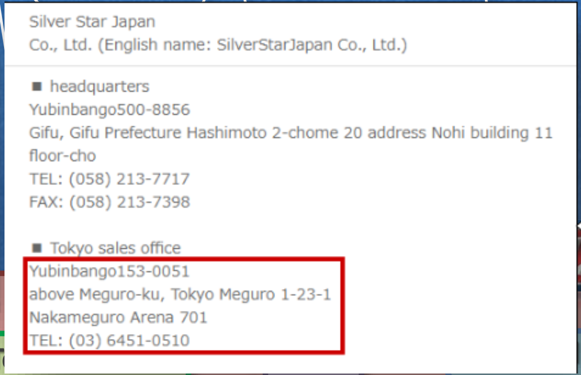
THE JAPANESE CONNECTION







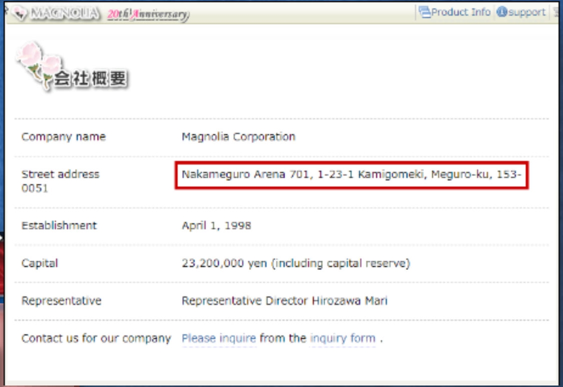
製品名	「殿堂(R)シリーズ」
ジャンル	ゲームソフト
製品内容	「殿堂(R)シリーズ」は、新思考エンジンを搭載し人間の感性を再現。 初心者から上級者まで、人と対戦するような臨場感を味わうことができます。
発売日	2004年1月1日(木)
価格	1,980円（税別）
動作環境	Windows XP/Me/98/98SE/2000
販売元	ソースネクスト株式会社
コピーライト	（C）2004 MAGNOLIA C 2004 STS Tech-Service （C）2004 Korea Computer Center （C）2004 SilverStar Japan
製品詳細	http://www.sourcenext.com/products/dendo/go.html http://www.sourcenext.com/products/dendo/mahjong.html http://www.sourcenext.com/products/dendo/shogi.html



Silver Star Japan
Co., Ltd. (English name: SilverStarJapan Co., Ltd.)

■ headquarters
Yubinbango500-8856
Gifu, Gifu Prefecture Hashimoto 2-chome 20 address Nohi building 11 floor-cho
TEL: (058) 213-7717
FAX: (058) 213-7398

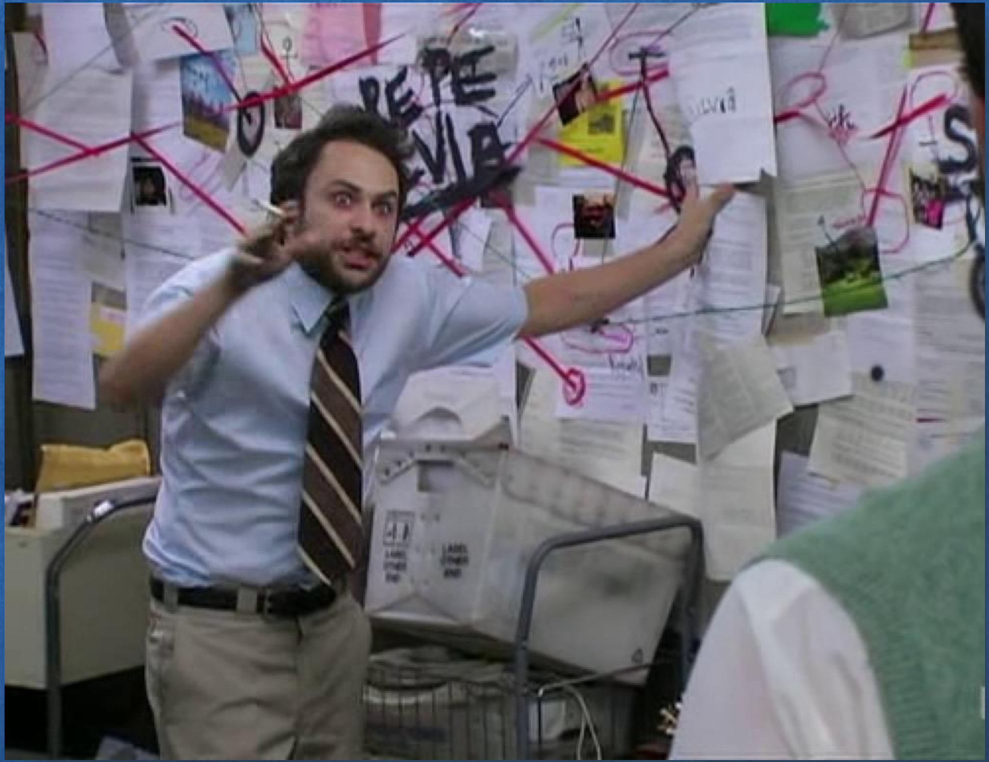
■ Tokyo sales office
Yubinbango153-0051
above Meguro-ku, Tokyo Meguro 1-23-1
Nakameguro Arena 701
TEL: (03) 6451-0510

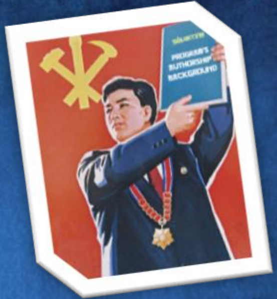


会社概要

Company name	Magnolia Corporation
Street address 0051	Nakameguro Arena 701, 1-23-1 Kamigomeki, Meguro-ku, 153-
Establishment	April 1, 1998
Capital	23,200,000 yen (including capital reserve)
Representative	Representative Director Hirozawa Mari
Contact us for our company	Please inquire from the inquiry form .

THE JAPANESE CONNECTION

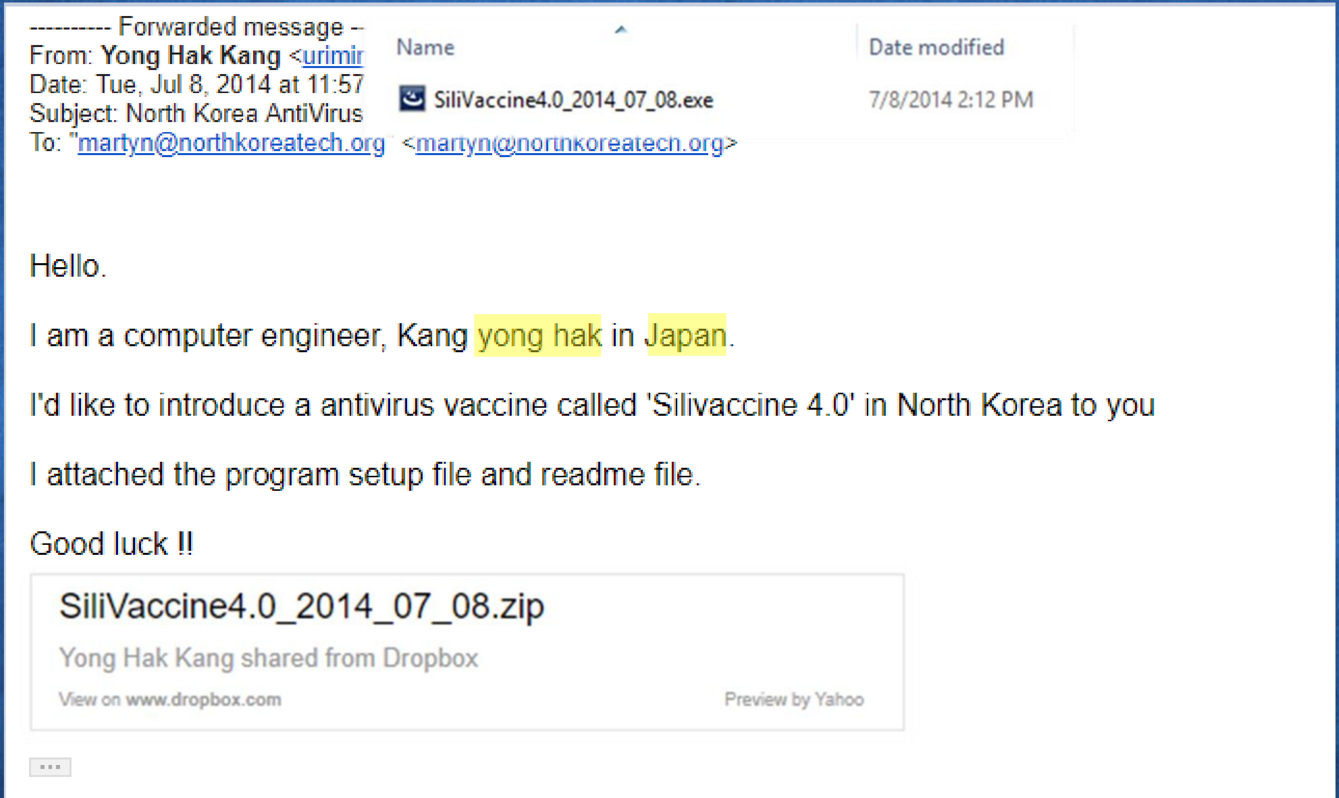




examining the package

NO BACKDOOR...?

Examining the Package



---------- Forwarded message --
From: **Yong Hak Kang** <urimir
Date: Tue, Jul 8, 2014 at 11:57
Subject: North Korea AntiVirus
To: "martyn@northkoreatech.org" <martyn@northkoreatech.org>

Name	Date modified
SiliVaccine4.0_2014_07_08.exe	7/8/2014 2:12 PM

Hello.

I am a computer engineer, Kang yong hak in Japan.

I'd like to introduce a antivirus vaccine called 'Silivaccine 4.0' in North Korea to you

I attached the program setup file and readme file.

Good luck !!

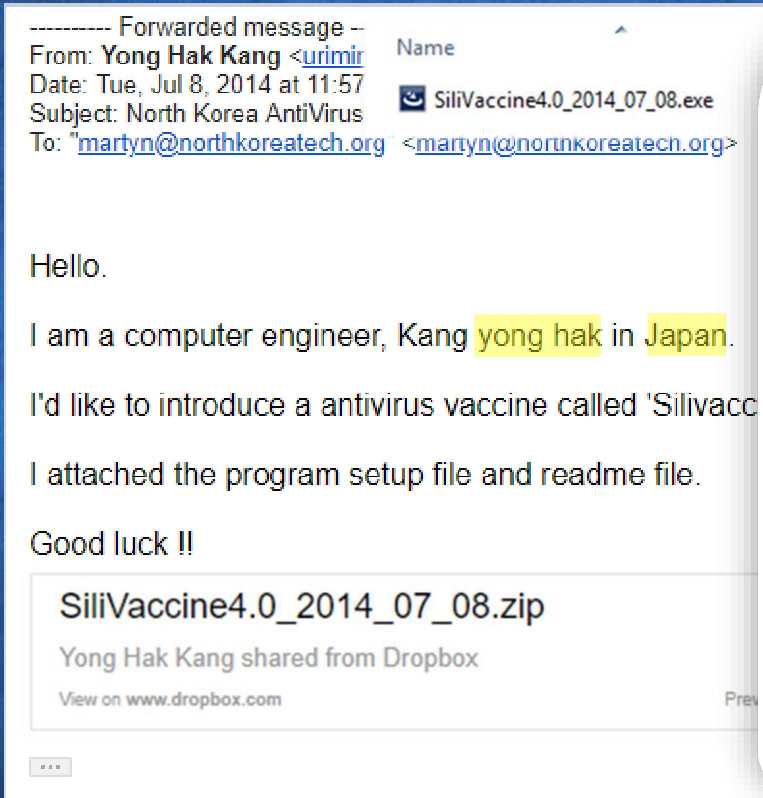
SiliVaccine4.0_2014_07_08.zip

Yong Hak Kang shared from Dropbox

View on www.dropbox.com

Preview by Yahoo

EXAMINING THE PACKAGE



---------- Forwarded message --
From: **Yong Hak Kang** <urimir
Date: Tue, Jul 8, 2014 at 11:57
Subject: North Korea AntiVirus
To: "martyn@northkoreatech.org" <martyn@northkoreatech.org>

Name

SiliVaccine4.0_2014_07_08.exe

Hello.

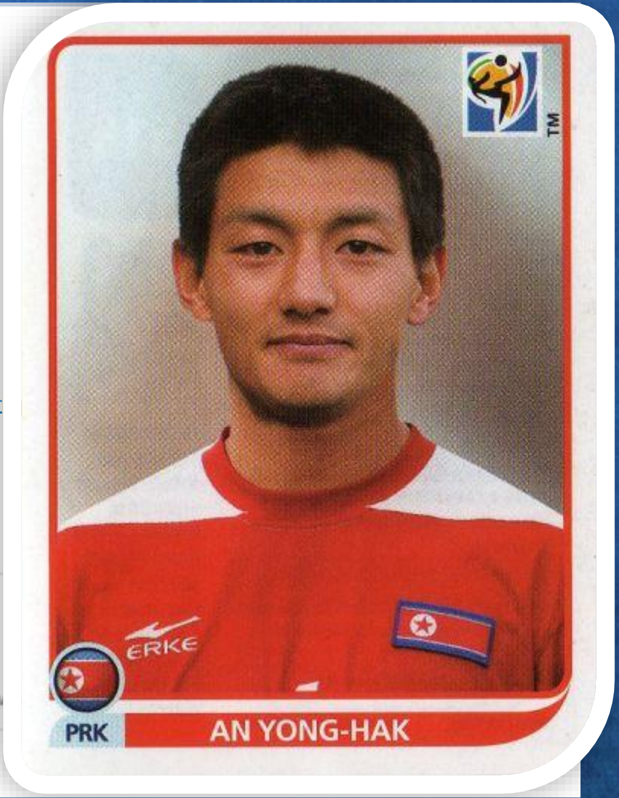
I am a computer engineer, Kang yong hak in Japan.

I'd like to introduce a antivirus vaccine called 'Silivacc

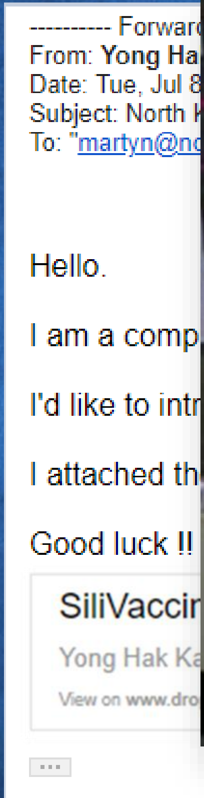
I attached the program setup file and readme file.

Good luck !!

SiliVaccine4.0_2014_07_08.zip
Yong Hak Kang shared from Dropbox
View on www.dropbox.com



EXAMINING THE PACKAGE



---------- Forward
From: Yong Ha
Date: Tue, Jul 8
Subject: North K
To: "martyn@no

Hello.

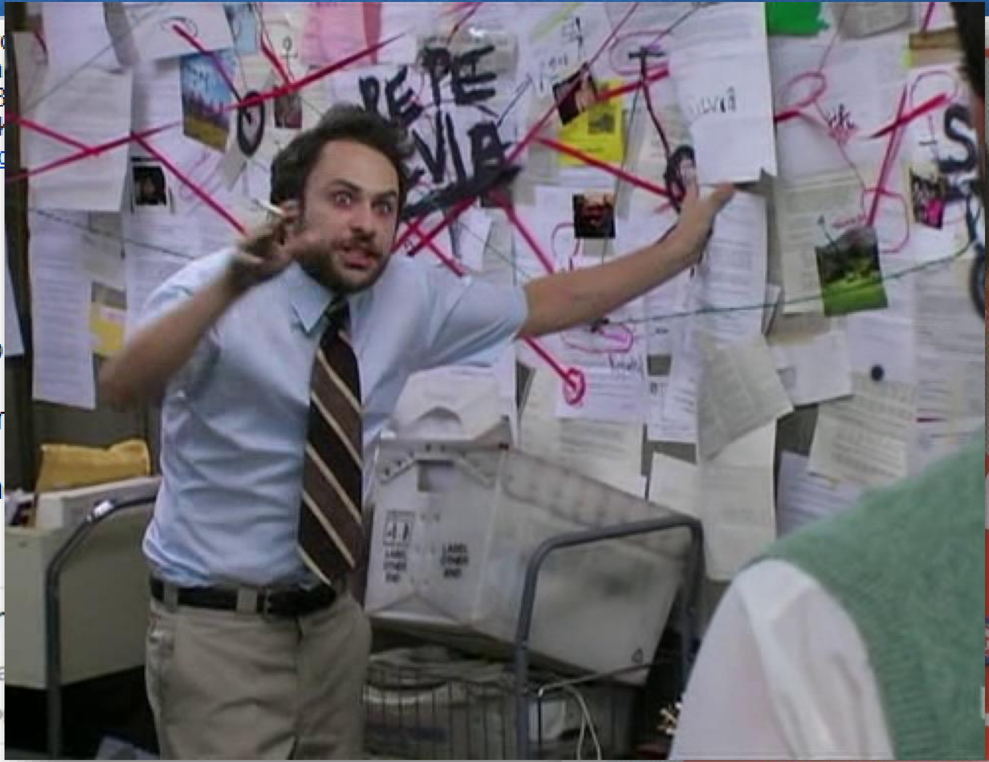
I am a comp

I'd like to intr

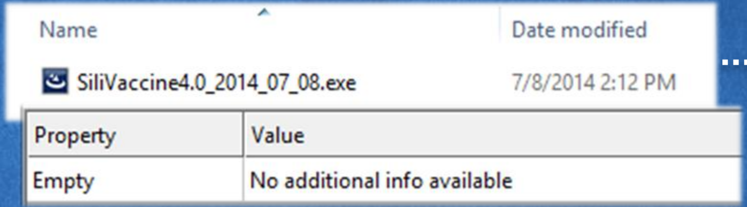
I attached th

Good luck !!

SiliVaccin
Yong Hak Ka
View on www.dro

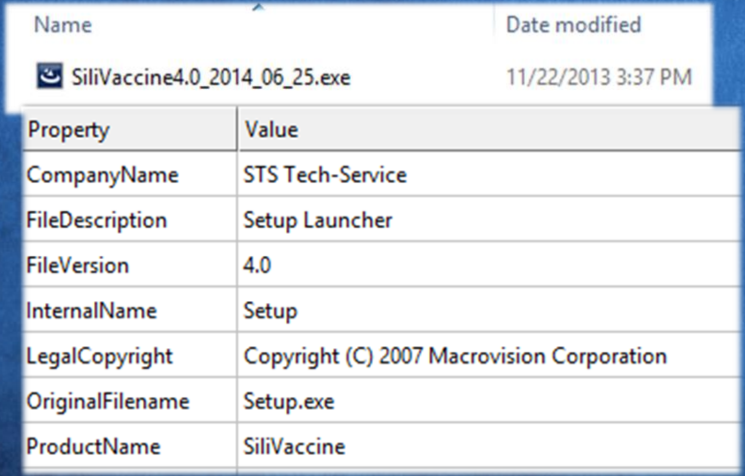


EXAMINING THE PACKAGE



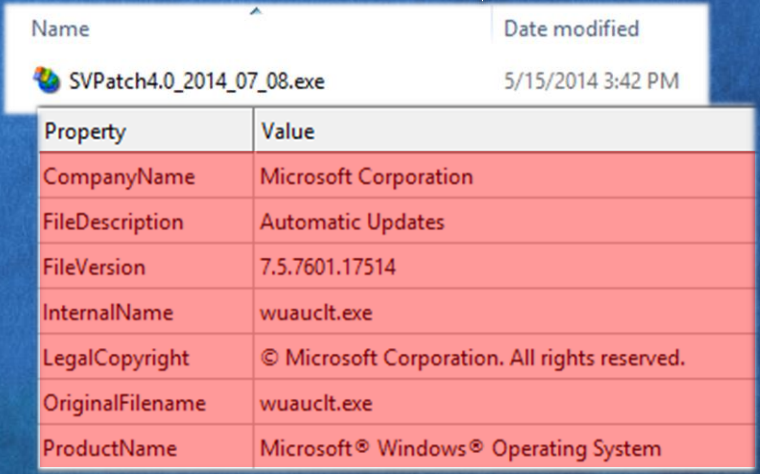
Name	Date modified
SiliVaccine4.0_2014_07_08.exe	7/8/2014 2:12 PM

Property	Value
Empty	No additional info available



Name	Date modified
SiliVaccine4.0_2014_06_25.exe	11/22/2013 3:37 PM

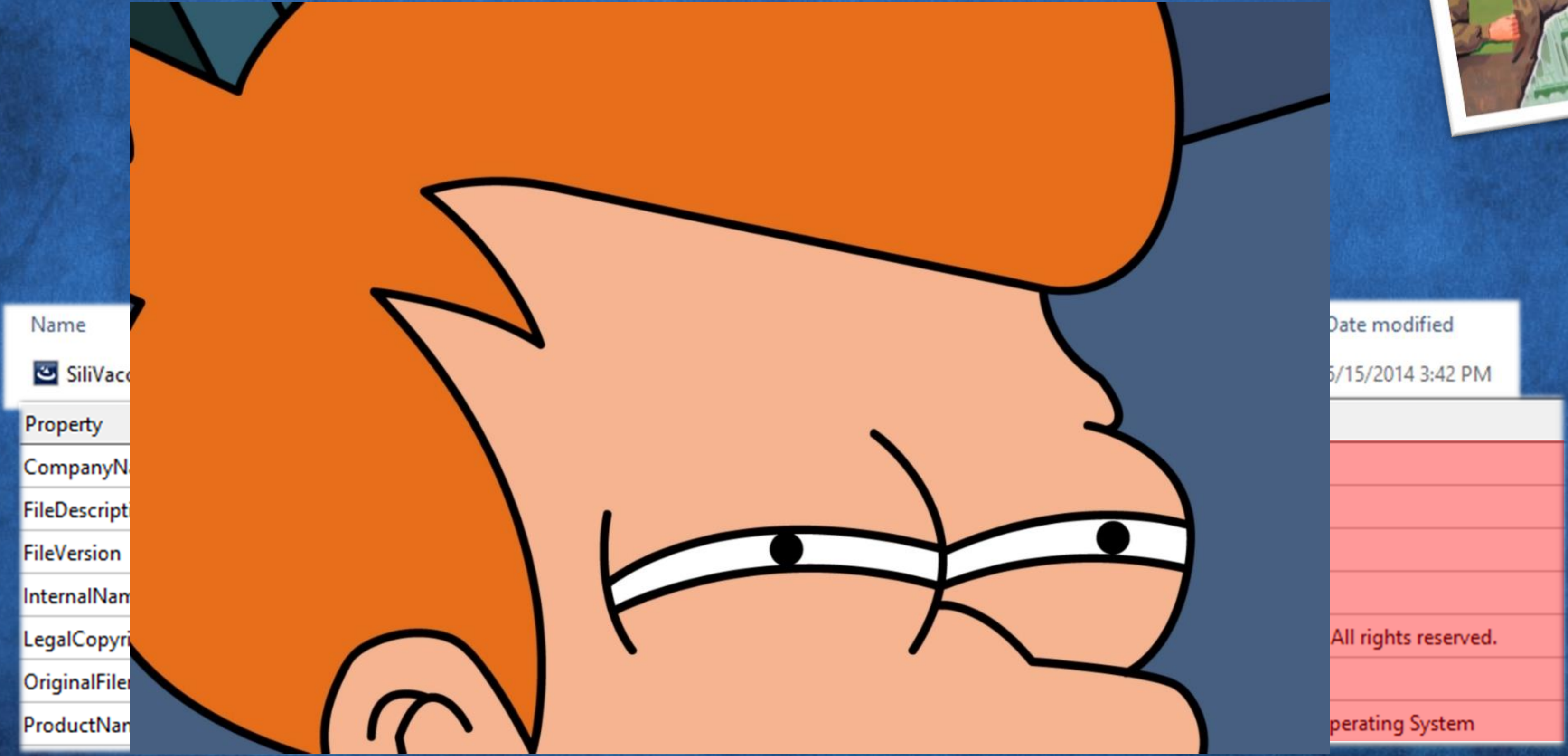
Property	Value
CompanyName	STS Tech-Service
FileDescription	Setup Launcher
FileVersion	4.0
InternalName	Setup
LegalCopyright	Copyright (C) 2007 Macrovision Corporation
OriginalFilename	Setup.exe
ProductName	SiliVaccine



Name	Date modified
SVPatch4.0_2014_07_08.exe	5/15/2014 3:42 PM

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Automatic Updates
FileVersion	7.5.7601.17514
InternalName	wuauclt.exe
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	wuauclt.exe
ProductName	Microsoft® Windows® Operating System

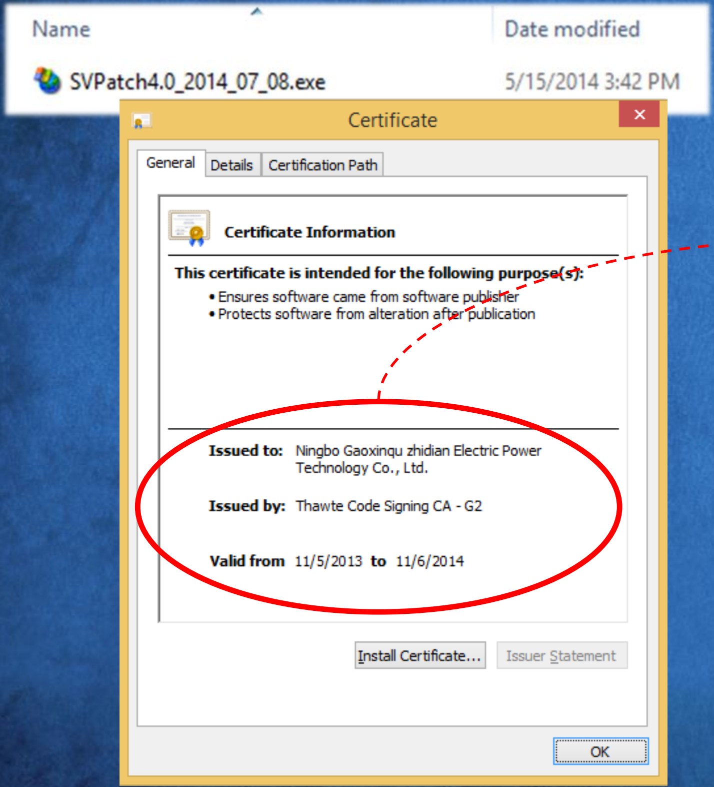
Examining the Package



Name	Date modified
SiliVac	/15/2014 3:42 PM

Property	
CompanyN	
FileDescripti	
FileVersion	
InternalNam	
LegalCopyri	All rights reserved.
OriginalFile	
ProductNam	perating System

LOOKS SUSPICIOUS



Name	Date modified
SVPatch4.0_2014_07_08.exe	5/15/2014 3:42 PM

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Ningbo Gaoxinqu zhidian Electric Power Technology Co., Ltd.

Issued by: Thawte Code Signing CA - G2

Valid from 11/5/2013 **to** 11/6/2014

Install Certificate...
Issuer Statement
OK

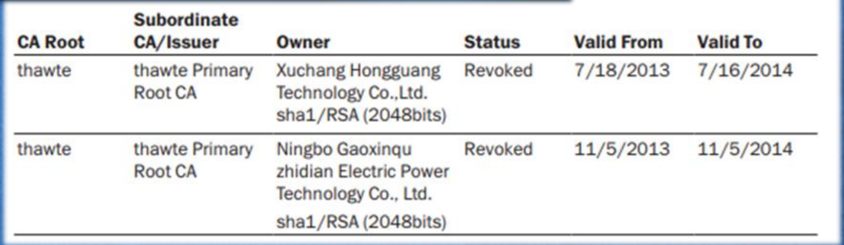
THE DARKHOTEL APT

A STORY OF UNUSUAL HOSPITALITY

Version 1.1

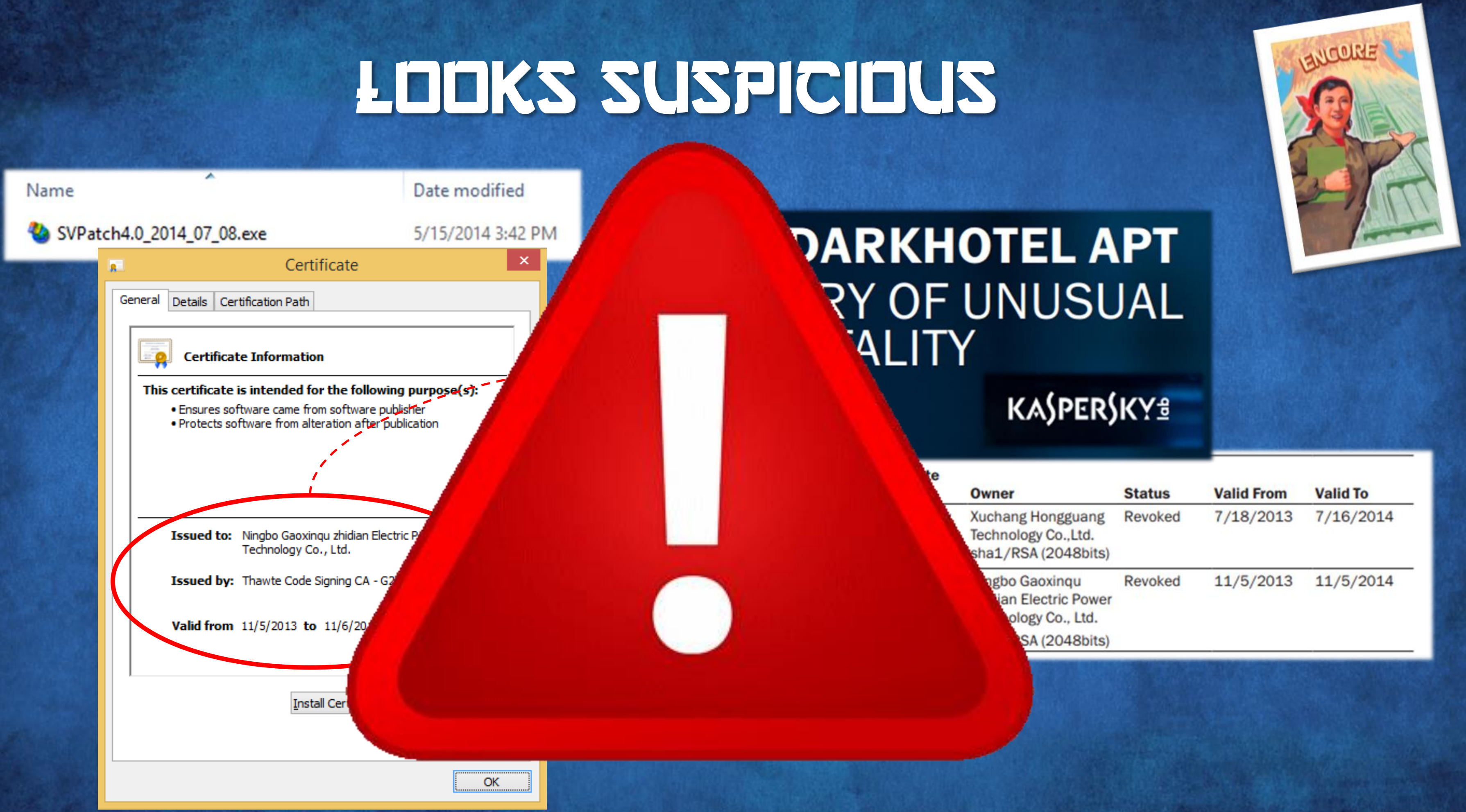
November, 2014

KASPERSKY lab



CA Root	Subordinate CA/Issuer	Owner	Status	Valid From	Valid To
thawte	thawte Primary Root CA	Xuchang Hongguang Technology Co.,Ltd. sha1/RSA (2048bits)	Revoked	7/18/2013	7/16/2014
thawte	thawte Primary Root CA	Ningbo Gaoxinqu zhidian Electric Power Technology Co., Ltd. sha1/RSA (2048bits)	Revoked	11/5/2013	11/5/2014

LOOKS SUSPICIOUS



Name	Date modified
SVPatch4.0_2014_07_08.exe	5/15/2014 3:42 PM

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Ningbo Gaoxinqu zhidian Electric P
Technology Co., Ltd.

Issued by: Thawte Code Signing CA - G2

Valid from 11/5/2013 **to** 11/6/20

Install Cer

OK

DARKHOTEL APT

RY OF UNUSUAL

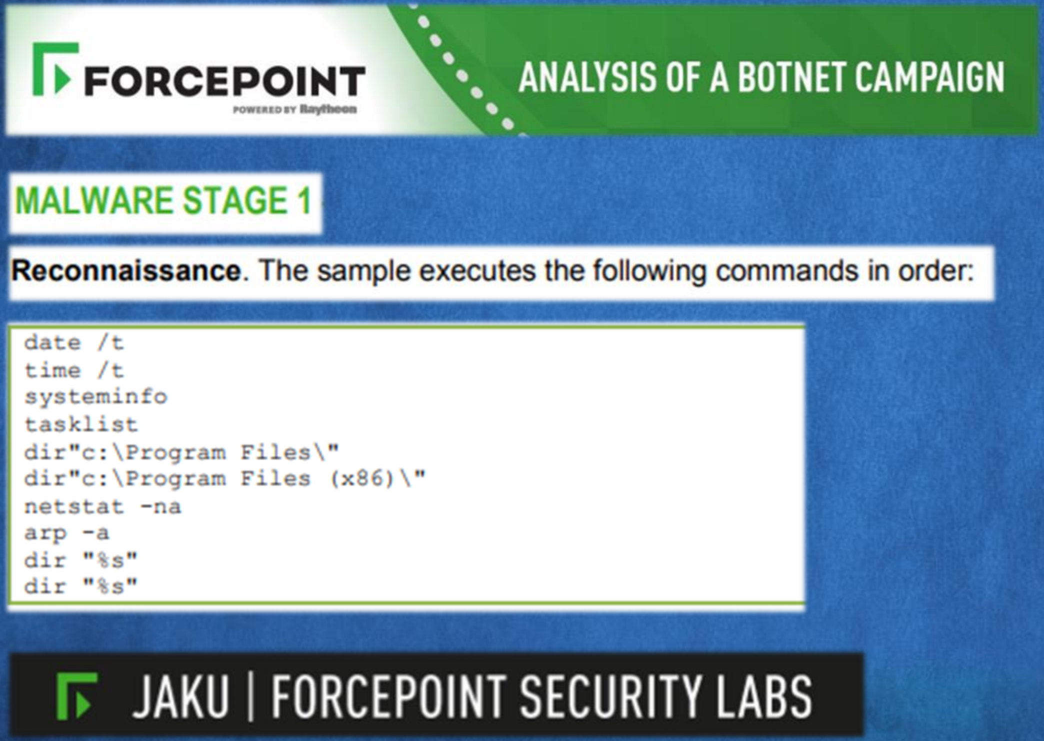
ALITY

KASPERSKY lab

te

Owner	Status	Valid From	Valid To
Xuchang Hongguang Technology Co.,Ltd. sha1/RSA (2048bits)	Revoked	7/18/2013	7/16/2014
ngbo Gaoxinqu ian Electric Power ology Co., Ltd. SA (2048bits)	Revoked	11/5/2013	11/5/2014

DIGGING DEEPER



FORCEPOINT

POWERED BY Raytheon

ANALYSIS OF A BOTNET CAMPAIGN

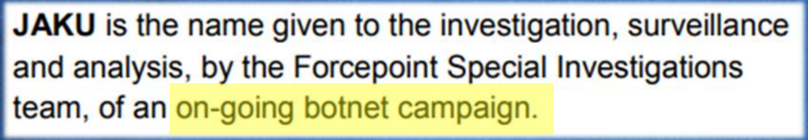
MALWARE STAGE 1

Reconnaissance. The sample executes the following commands in order:

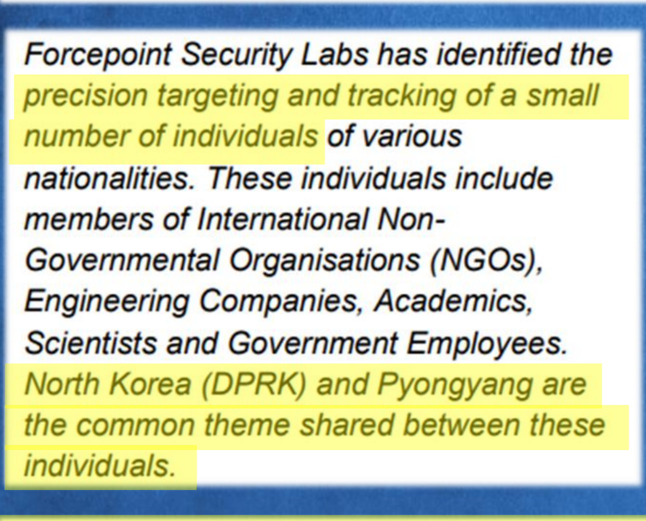
```
date /t
time /t
systeminfo
tasklist
dir"c:\Program Files\"
dir"c:\Program Files (x86)\"
netstat -na
arp -a
dir "%s"
dir "%s"
```

JAKU | FORCEPOINT SECURITY LABS

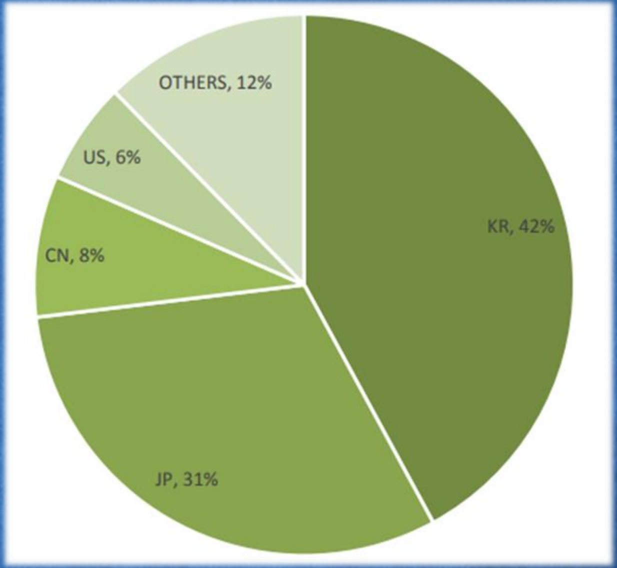
JAKU?

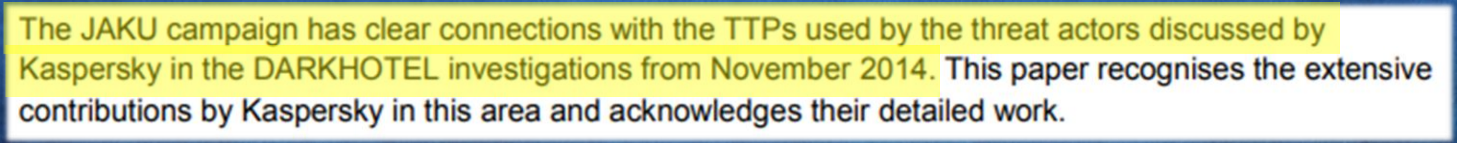


JAKU is the name given to the investigation, surveillance and analysis, by the Forcepoint Special Investigations team, of an on-going botnet campaign.



Forcepoint Security Labs has identified the precision targeting and tracking of a small number of individuals of various nationalities. These individuals include members of International Non-Governmental Organisations (NGOs), Engineering Companies, Academics, Scientists and Government Employees. North Korea (DPRK) and Pyongyang are the common theme shared between these individuals.





The JAKU campaign has clear connections with the TTPs used by the threat actors discussed by Kaspersky in the DARKHOTEL investigations from November 2014. This paper recognises the extensive contributions by Kaspersky in this area and acknowledges their detailed work.

TARGET?

WAIT… IS THIS…?

final words

conclusion

✓ silivaccine has been illegally using trend micros engine for years, over multiple versions

✓ silivaccine authors tried to hide this fact

✓ silivaccine explicitly whitelists a specific signature

✓ installation comes bundled with jaku malware

UNANSWERED QUESTIONS

- ✓ how did silivaccine authors obtain access to trend micros proprietary components?
- ✓ what is the exact purpose of the whitelisting?
- ✓ is jaku part of silivaccine or was martyn the target?

THANK YOU!

@ _marklech_ @kajilot

QUESTIONS?

@ _marklech_ @kajilot

MARK LECHTIK MICHAEL KAJILOTI

CAPTIALIST PIG RESEARCHERS FROM THE MIDDLE EAST

who work at:

Check Point
SOFTWARE TECHNOLOGIES LTD.