

# 악성코드 포렌식



*JK Kim*

*@pr0neer*

*forensic-proof.com*

*proneer@gmail.com*

## 악성코드 분석 케이스

### 1. 보안 HW/SW에 의해 악성코드가 탐지된 경우

- 발견된 악성코드를 기준으로 분석
- 발견된 악성코드 이외의 **추가적인 악성코드를 탐지 못할 가능성**

### 2. 서비스의 비정상적인 행위로 악성코드 감염이 의심되는 경우

- 비정상 행위가 발생한 시점을 기준으로 분석
- 빠른 대응을 하지 못하는 경우 **악성코드를 탐지 못할 가능성**

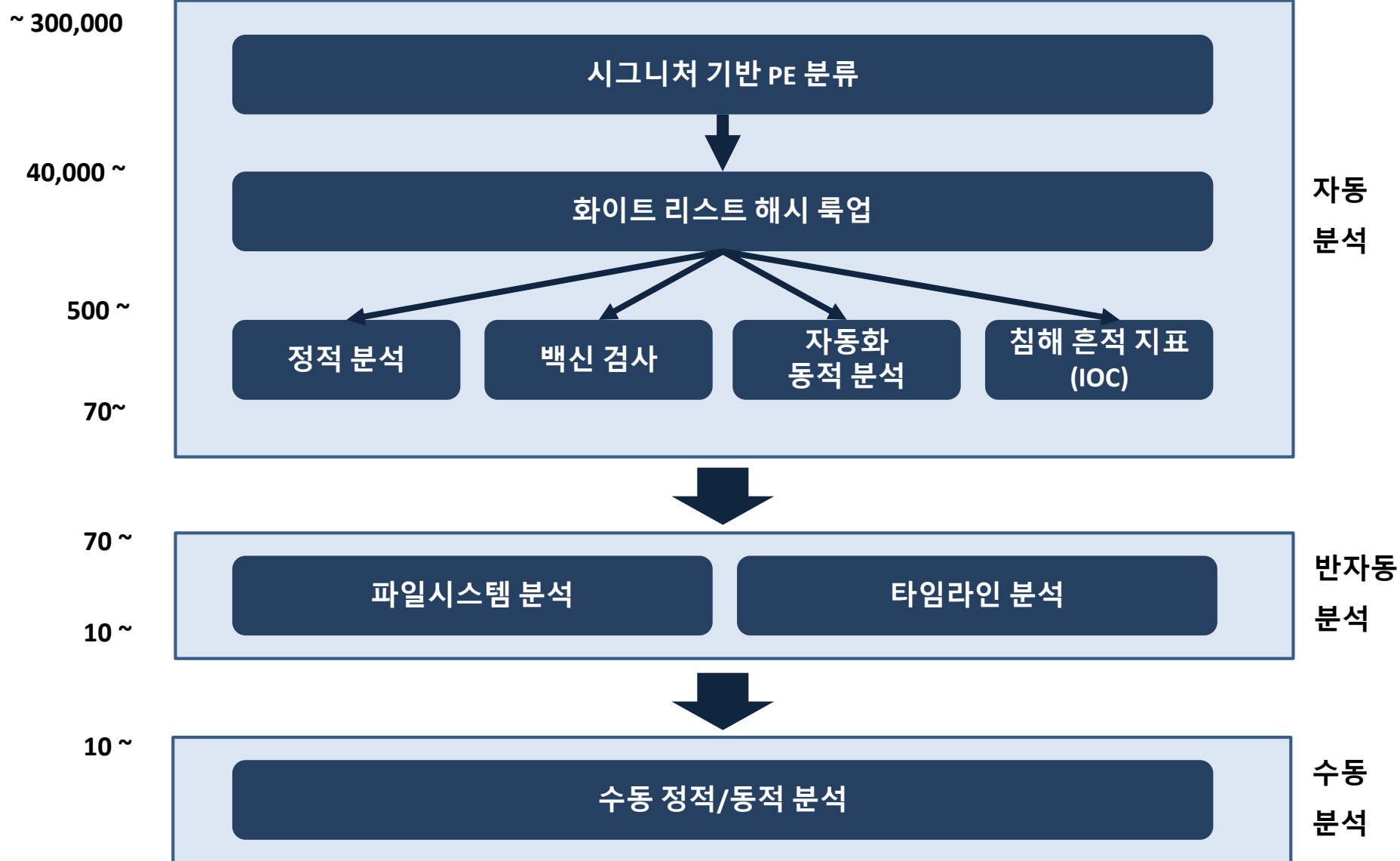
➔ 악성코드가 발견된 경우 다양한 보안 위협에 대한 고려가 필요

➔ 체계적인 분석을 통해 악성코드의 근원과 영향을 분석하고 대응해야 함

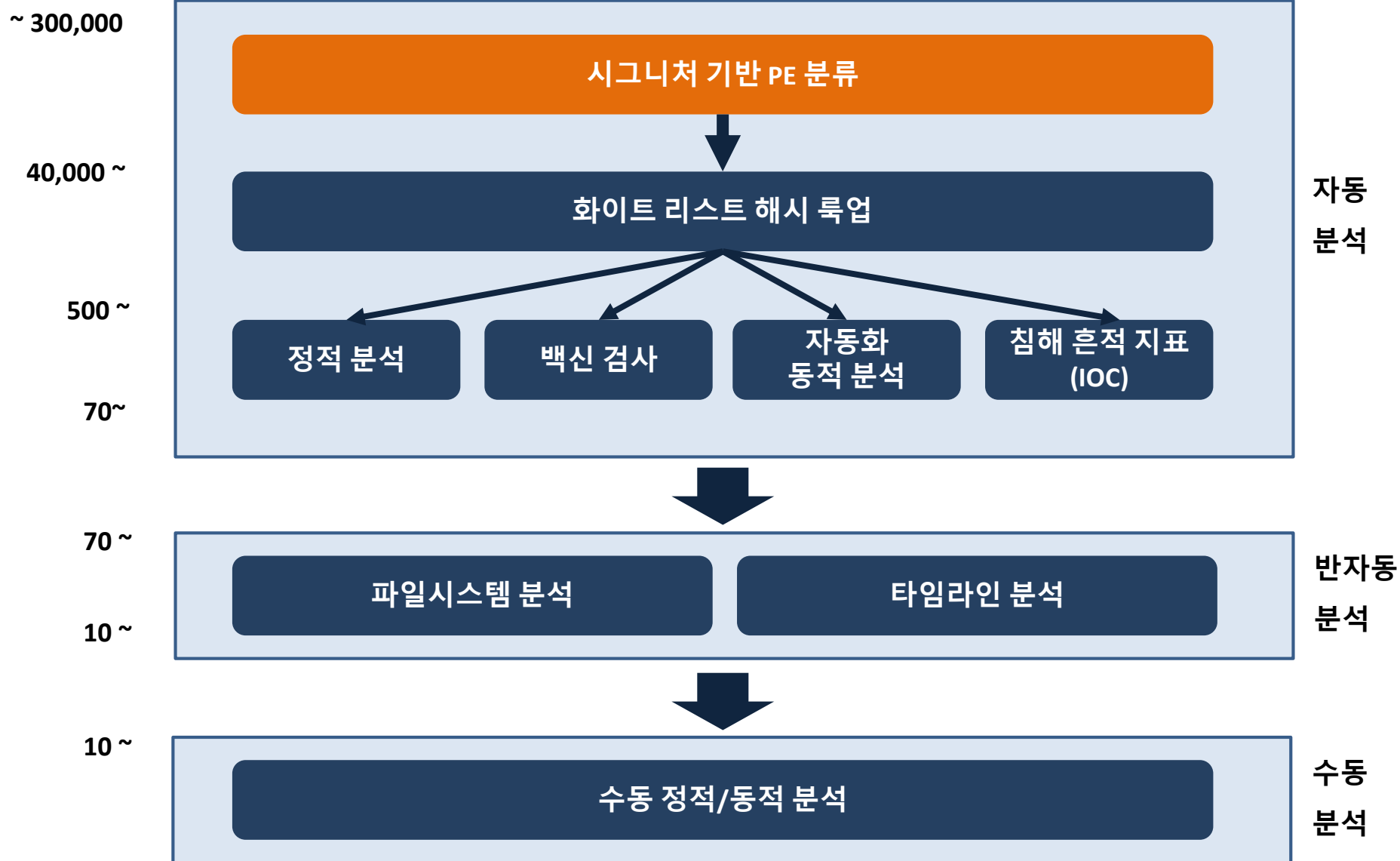
# 악성코드 분석 프레임워크

*Security is a people problem...*

# 악성코드 분석 프레임워크



# 악성코드 분석 프레임워크



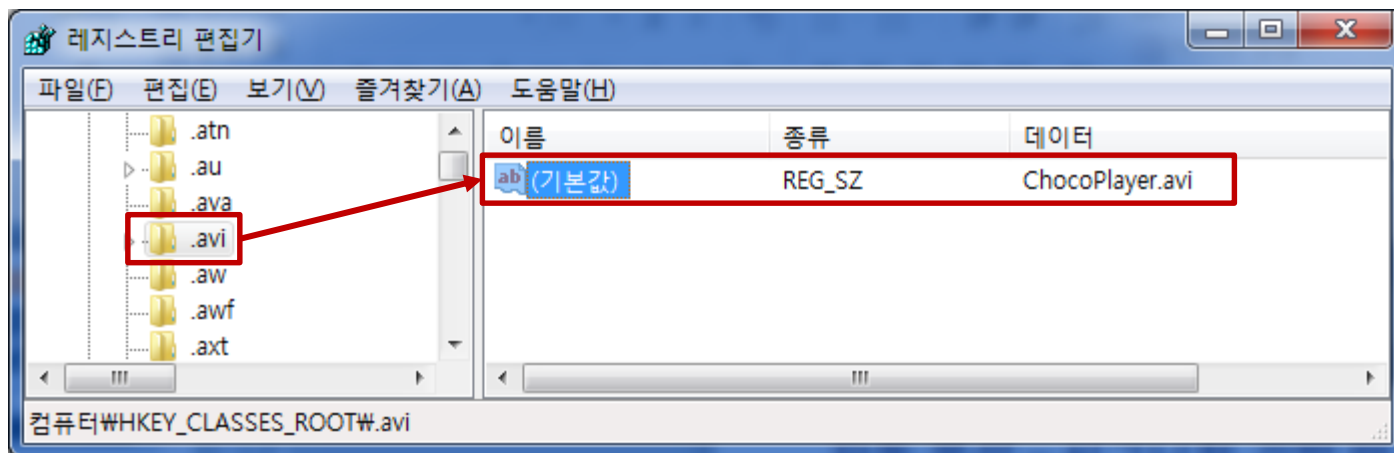
## 자동 분석 – 시그니처 기반 PE 분류 (1/4)

- **PE (Portable Executable) 포맷**
  - 유닉스 COFF(Common Object File Format)을 기반으로 윈도우 3.1 부터 지원된 실행 파일 형식
- **PE 파일 종류**
  - **EXE** – 일반 실행 파일
  - **DLL** – 동적 링크 파일
  - **SYS** – 드라이버 파일
  - **SCR** – 화면보호기 파일
  - **VXD** – 드라이버 파일
  - **OCX** – 객체 제어, Active X 컨트롤 파일
  - **CPL** – 윈도우 시스템 환경 설정 파일 (제어판 기능 추가)
- **VXD 와 SYS의 차이점은?**

## 자동 분석 – 시그니처 기반 PE 분류 (2/4)

- 확장자 분류의 문제점

- 원도우는 기본적으로 확장자 기반의 애플리케이션 바인딩 사용
- .AVI → 윈도우 미디어 플레이어 (기본) → 곰플레이어 설치 후?
- .JPG → 윈도우 사진 뷰어 → 꿀뷰, 알씨 설치 후?
- 애플리케이션 바인딩 정보는 레지스트리(HKEY\_CLASSES\_ROOT)에 저장
- 유로2012 미녀.src, 야구동영상.(exe).avi



# 악성코드 분석 프레임워크

## 자동 분석 – 시그니처 기반 PE 분류 (3/4)

- PE 시그니처

notepad.exe																																																	
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3	0	1	2	3	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0	1	2	3					
0000h:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	B8	00	00	00	MZ	.....	ÿÿ	.....																									
0014h:	00	00	00	00	40	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....	@	.....																										
0028h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....																												
003Ch:	E8	00	00	00	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	è	....	°	..	´	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	!	
0050h:	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	74	20	62	65	is	program	cannot	be																									
0064h:	20	72	75	6E	20	69	6E	20	44	4F	53	20	6D	6F	64	65	2E	0D	0D	0A	run	in	DOS	mode	....																								
0078h:	24	00	00	00	00	00	00	00	83	C2	32	29	C7	A3	5C	7A	C7	A3	5C	7A	\$	.....	f	Å	2	)	Ç	£	\	z	Ç	£	\	z															
008Ch:	C7	A3	5C	7A	CE	DB	D8	7A	C6	A3	5C	7A	CE	DB	C9	7A	C5	A3	5C	7A	Ç	£	\	z	Î	Û	0	z	Æ	£	\	z	Î	Û	É	z	Å	£	\	z									
00A0h:	CE	DB	CF	7A	DA	A3	5C	7A	C7	A3	5D	7A	33	A3	5C	7A	CE	DB	DF	7A	Î	Û	î	z	Û	£	\	z	Ç	£	\	z	3	£	\	z	Î	Û	ß	z									
00B4h:	D3	A3	5C	7A	CE	DB	D5	7A	CC	A3	5C	7A	CE	DB	C8	7A	C6	A3	5C	7A	Ó	£	\	z	Î	Û	Ö	z	Î	£	\	z	Î	Û	È	z	Æ	£	\	z									
00C8h:	CE	DB	CD	7A	C6	A3	5C	7A	52	69	63	68	C7	A3	5C	7A	00	00	00	00	Î	Û	î	z	Æ	£	\	z	Rich	Ç	£	\	z	....															
00DCh:	00	00	00	00	00	00	00	00	00	00	00	00	50	45	00	00	64	86	06	00	.....	PE	..	dt	..																								
00F0h:	B3	C9	5B	4A	00	00	00	00	00	00	00	00	F0	00	22	00	0B	02	09	00	³	É	[	J	.....	8	."	.....																					
0104h:	00	A8	00	00	00	58	02	00	00	00	00	00	70	35	00	00	00	10	00	00	.	...	X	.....	p	5	.....																						

- IMAGE\_DOS\_HEADER

- MZ 시그니처 – “MZ” (0x4D5A)

- IMAGE\_NT\_HEADER

- PE 시그니처 – “PE ” (0x50450000)



## 자동 분석 – 시그니처 기반 PE 분류 (4/4)

- 야구동영상을 이용한 악성코드 배포 유형

1. 다운로드 프로그램

- 웹하드(파일공유) 사이트마다 고유의 다운로드 프로그램 사용

2. 확장자 변경

- 9회말 2아웃.(exe).avi
- 정상 동영상 파일 앞부분에 악성파일 삽입, 리소스 변경을 이용해 아이콘 변경

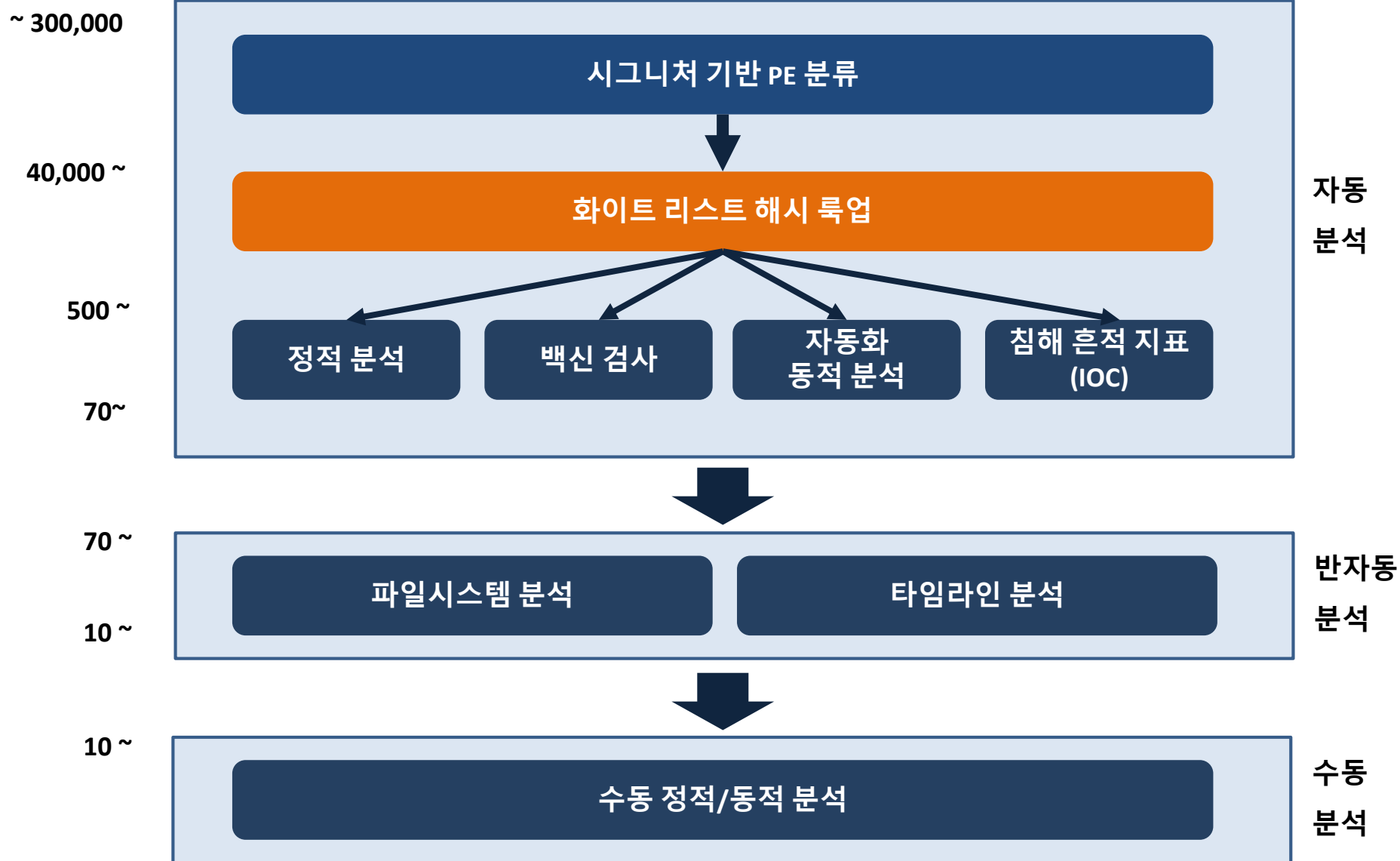
3. 자체 압축 풀림(self-extracting archive, SFX)

- 9회말 2아웃.exe

4. 동영상 플레이어 취약점

- 플레이어의 취약점을 이용해 동영상 포맷 구성

# 악성코드 분석 프레임워크



## 자동 분석 – 화이트 리스트 해시 록업 (1/3)

- **화이트 리스트 해시**
  - 알려진 정상 파일에 대한 해시 (MD5, SHA-1, SHA-256)
  - RDS (Reference Data Set)를 활용
- **NSRL(National Software Reference Library by NIST) RDS**
  - 미국국립표준원에서 지원하는 화이트리스트 해시 프로젝트
  - 1년에 4번 분기말에 배포 (3월, 6월, 9월, 12월)
  - 2012년 6월 기준, 26,911,012 개의 유일한 해시값 배포
  - 운영체제 서비스팩/패치 별로 해시값 계산 ➔ RDS 포맷으로 배포
  - RDS 이외에 EnCase, Hashkeeper, Vagon 형식으로도 배포

## 자동 분석 - 화이트 리스트 해시 록업 (2/3)

- NSRL 프로젝트 (<http://www.nsrl.nist.gov/>)

Information Technology Laboratory  
**National Software Reference Library**

NIST  
National Institute of Standards and Technology

### Welcome to the National Software Reference Library (NSRL) Project Web Site.

This project is supported by the U.S. Department of Justice's National Institute of Justice (NIJ), federal, state, and local law enforcement, and the National Institute of Standards and Technology (NIST) to promote efficient and effective use of computer technology in the investigation of crimes involving computers. Numerous other sponsoring organizations from law enforcement, government, and industry are providing resources to accomplish these goals, in particular the FBI who provided the major impetus for creating the NSRL out of their ACES program.

The National Software Reference Library (NSRL) is designed to collect software from various sources and incorporate file profiles computed from this software into a Reference Data Set (RDS) of information. The RDS can be used by law enforcement, government, and industry organizations to review files on a computer by matching file profiles in the RDS. This will help alleviate much of the effort involved in determining which files are important as evidence on computers or file systems that have been seized as part of criminal investigations.

The RDS is a collection of digital signatures of **known, traceable software applications**. There are application hash values in the hash set which may be considered malicious, i.e. steganography tools and hacking scripts. **There are no hash values of illicit data, i.e. child abuse images.**

The National Software Reference Library is a project in [Software and Systems Division](#) supported by [The Office of Law Enforcement Standards](#).

#### NSRL RDS Annual Release Schedule

The NSRL RDS is released four times each year - in March, June, September and December - according to the schedule below.

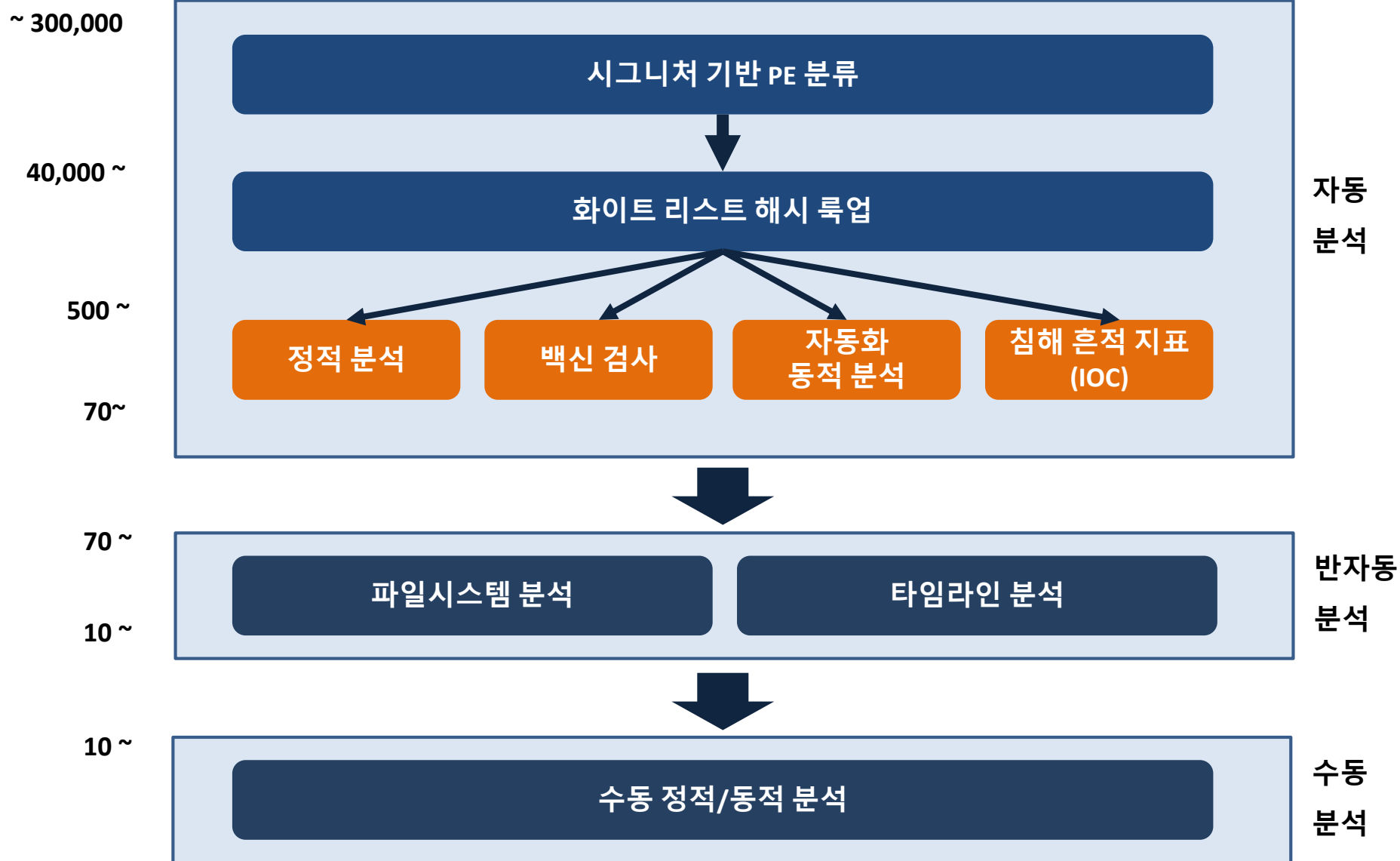
**Current Release: June 2012 RDS 2.37 containing 26,911,012 unique hash values.**

Date	Task	Notes
Feb 16-28	Build and QC of master RDS	Software arriving now goes in next release
Mar 1	Deliver master RDS to NIST SRD contact	SRD duplicates and mails the RDS
Apr 1	Subscribers should receive RDS in mail	
Apr 28	ISO images of RDS available as <a href="#">free downloads</a>	
May 16-28	Build and QC of master RDS	Software arriving now goes in next release
Jun 1	Deliver master RDS to NIST SRD contact	SRD duplicates and mails the RDS

## 자동 분석 – 화이트 리스트 해시 록업 (3/3)

- **NSRL RDS 지원 기관**
  - **Adobe** Systems Incorporated, **U.S. Air Force**, **Faronics** Incorporated, **Federal Bureau of Investigation**
  - **U.S. Food and Drug Administration**, **Microsoft**, **Netherlands Forensic Institute**, **NIST**, **Oracle** Corporation
  - **Sanderson** Forensics, **G. Sherwood**, **Summitsoft** Corporation, **WetStone** Technologies, Inc.
- **NSRL RDS 의 한계**
  - 다국어 운영체제에 대한 지원 미흡
  - 국내 소프트웨어에 대한 미지원
- **국내형 RDS 필요**
  - 지속적인 업데이트와 관리를 위해 국가연구기관에서 주도하는 것이 필요
  - 특수 목적만을 위한 것이 아닌 공개형으로 개발

# 악성코드 분석 프레임워크



# 악성코드 분석 프레임워크

## 자동 분석 – 정적 분석 (1/4)

- PE 파일 포맷 분석

- PE 파일에서 악성파일이 주로 사용하는 값의 설정 여부를 검증 → 가중치

OLLYDBG.EXE															
0 1 2 3 4 5 6 7 8 9 A B C D E F 0 1 2 3 0123456789ABCDEF0123															
030Ch:	00	06	00	00	00	00	00	00	00	00	00	00	00	20	00 00 60
0320h:	2E	64	61	74	61	00	00	00	00	B0	05	00	00	00	0B 01 00
0334h:	00	EE	0A	00	00	00	00	00	00	00	00	00	00	40	00 00 C0
Template Results - EXETemplate2.bt															
Name		Value		Start		Size		Color		Comment					
▷ struct IMAGE_DOS_HEADER dos_header				0h		40h		Fg: Bg:							
▷ UCHAR doscode[448]				40h		1C0h		Fg: Bg:							
▷ struct IMAGE_NT_HEADERS nt_headers				200h		F8h		Fg: Bg:							
▲ struct IMAGE_SECTION_HEADER sections_table[8]				2F8h		140h		Fg: Bg:							
▲ struct IMAGE_SECTION_HEADER sections_table[0]		.text		2F8h		28h		Fg: Bg:							
▷ BYTE Name[8]		.text		2F8h		8h		Fg: Bg:							
DWORD VirtualSize		716800		300h		4h		Fg: Bg:							
DWORD VirtualAddress		1000h		304h		4h		Fg: Bg:							
DWORD SizeOfRawData		714752		308h		4h		Fg: Bg:							
DWORD PointerToRawData		600h		30Ch		4h		Fg: Bg:							
DWORD NonUsedPointerToRelocations		0		310h		4h		Fg: Bg:							
DWORD NonUsedPointerToLinenumbers		0		314h		4h		Fg: Bg:							
WORD NonUsedNumberOfRelocations		0		318h		2h		Fg: Bg:							
WORD NonUsedNumberOfLinenumbers		0		31Ah		2h		Fg: Bg:							
▷ struct SECTION_FLAGS Characteristics		Code Executable Readable		31Ch		4h		Fg: Bg:							
▷ struct IMAGE_SECTION_HEADER sections_table[1]		.data		320h		28h		Fg: Bg:							
▷ struct IMAGE_SECTION_HEADER sections_table[2]		.tls		348h		28h		Fg: Bg:							
▷ struct IMAGE_SECTION_HEADER sections_table[3]		.rdata		370h		28h		Fg: Bg:							
▷ struct IMAGE_SECTION_HEADER sections_table[4]		.idata		398h		28h		Fg: Bg:							
▷ struct IMAGE_SECTION_HEADER sections_table[5]		.edata		3C0h		28h		Fg: Bg:							
▷ struct IMAGE_SECTION_HEADER sections_table[6]		.rsrc		3E8h		28h		Fg: Bg:							
▷ struct IMAGE_SECTION_HEADER sections_table[7]		.reloc		410h		28h		Fg: Bg:							
▷ BYTE textsection[714752]				600h		AE800h		Fg: Bg:							
▷ BYTE datasection[119296]				AEE00h		1D200h		Fg: Bg:							
▷ BYTE tlssection[512]				CC000h		200h		Fg: Bg:							
▷ BYTE rdatasection[512]				CC200h		200h		Fg: Bg:							
▷ BYTE idatasection[7680]				CC400h		1E00h		Fg: Bg:							

# 악성코드 분석 프레임워크

## 자동 분석 – 정적 분석 (2/4)

- 엔트로피 계산

- PE 파일의 각 섹션별 엔트로피를 계산하여 패킹 및 암호화 탐지

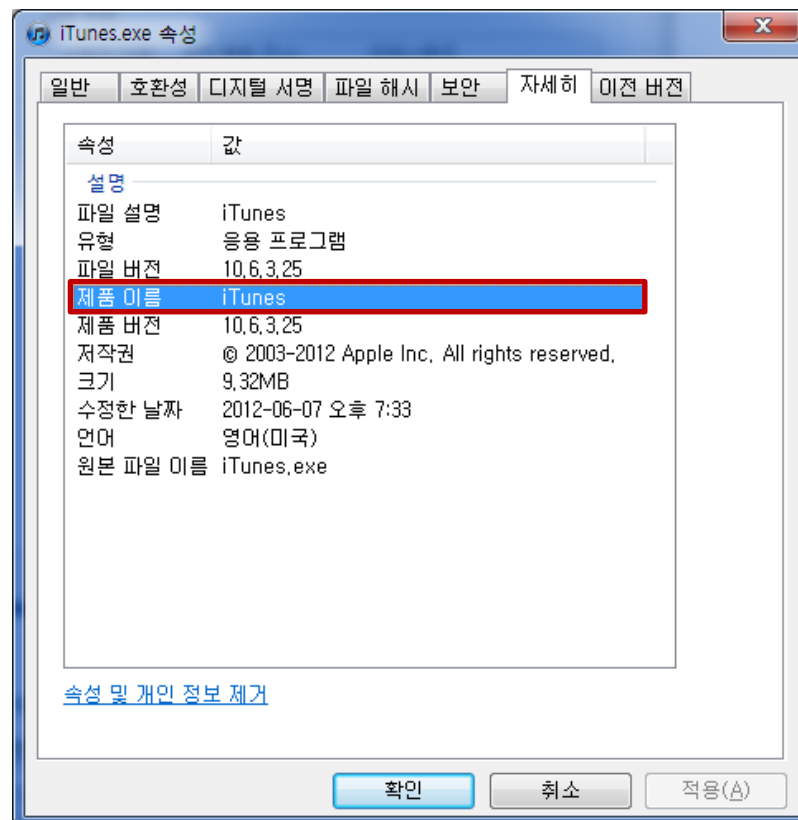
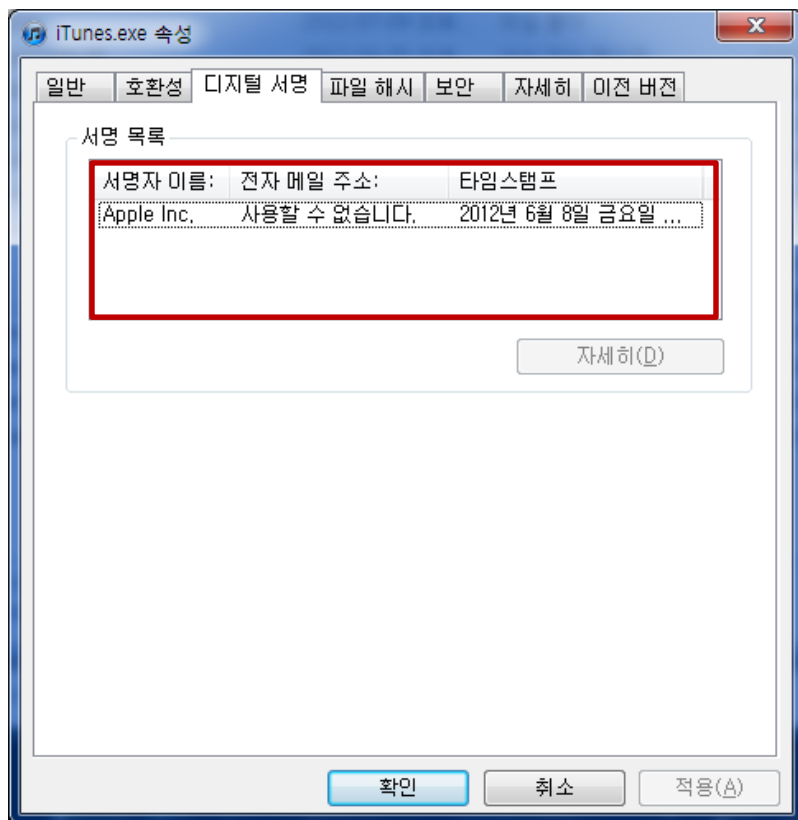
UPX.exe																
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
03C0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
03D4h:	00	00	00	00	00	00	00	31	2E	32	35	00	55	50	58	21
03E8h:	F4	62	F5	C4	42	72	6B	2E	C7	47	04	00	75	E4	01	00
03FCh:	26	0B	00	64	FF	E5	FD	FF	55	8B	EC	83	7D	0C	00	75
0410h:	5D	C3	15	08	14	6A	26	68	74	C1	42	00	6D	69	FF	DB
0424h:	0B	01	BA	33	83	C4	0C	FF	75	04	08	10	20	66	FB	FF
0438h:	74	69	18	56	83	CE	FF	48	48	0F	84	88	00	01	7B	59
044Ch:	70	05	58	40	28	10	68	A0	81	9B	79	7F	3F	00	09	EC
0460h:	E9	6A	00	85	14	97	94	7C	6A	6F	90	74	2C	EB	67	29
0474h:	53	F2	29	F9	70	6C	EB	3D	6E	8C	EB	28	6C	F8	07	A7
0488h:	6B	2C	63	14	8B	F0	8B	C6	5E	FE	FF	C1	27	6D	B8	6C
049Ch:	AC	A1	B0	05	44	00	83	8D	F8	FF	FB	FF	FF	F2	7C	F0
04B0h:	89	45	FC	7F	FF	7F	68	E8	DC	57	B0	FD	03	56	57	6A
04C4h:	4E	68	FF	D2	50	7A	F7	BE	FF	F6	0C	8B	75	24	34	85
04D8h:	09	59	8D	BD	3A	F3	A5	29	28	23	79	EF	43	FB	75	06
04ECh:	8B	B7	83	A5	2E	00	0D	D8	F6	FF	77	FF	8D	47	FF	89
0500h:	45	1C	83	F8	02	89	7E	14	C7	46	18	01	A2	7B	F0	FF
0514h:	0A	7F	30	83	C0	FE	6A	03	99	59	F7	F9	85	D2	79	C7
0528h:	FF	DB	20	3A	EB	22	33	C0	83	FA	01	0F	95	C0	8D	04
053Ch:	35	EB	DE	FE	A7	E1	0B	68	C0	C7	8B	4D	20	83	F9	01
0550h:	75	61	83	BD	7C	B0	FD	CF	77	75	5D	3B	C7	72	59	39
0564h:	51	C5	1C	02	75	37	DC	D0	14	8E	FC	50	47	57	43	89
0578h:	1C	A9	F8	56	03	04	52	05	0F	85	FB	FB	01	B3	DB	D2
058Ch:	D0	D7	03	7F	11	83	61	F2	35	9B	83	4C	DC	FF	1F	56
05A0h:	D7	0C	32	4C	7F	40	57	06	19	92	E5	BD	FF	0F	2B	2A
05B4h:	E7	65	14	0A	7F	0F	0A	3F	00	DE	2B	FE	DE	59	7C	22
05C8h:	56	0F	50	51	45	18	5E	7E	9F	08	2B	81	1C	EB	25	4D



## 자동 분석 - 정적 분석 (3/4)

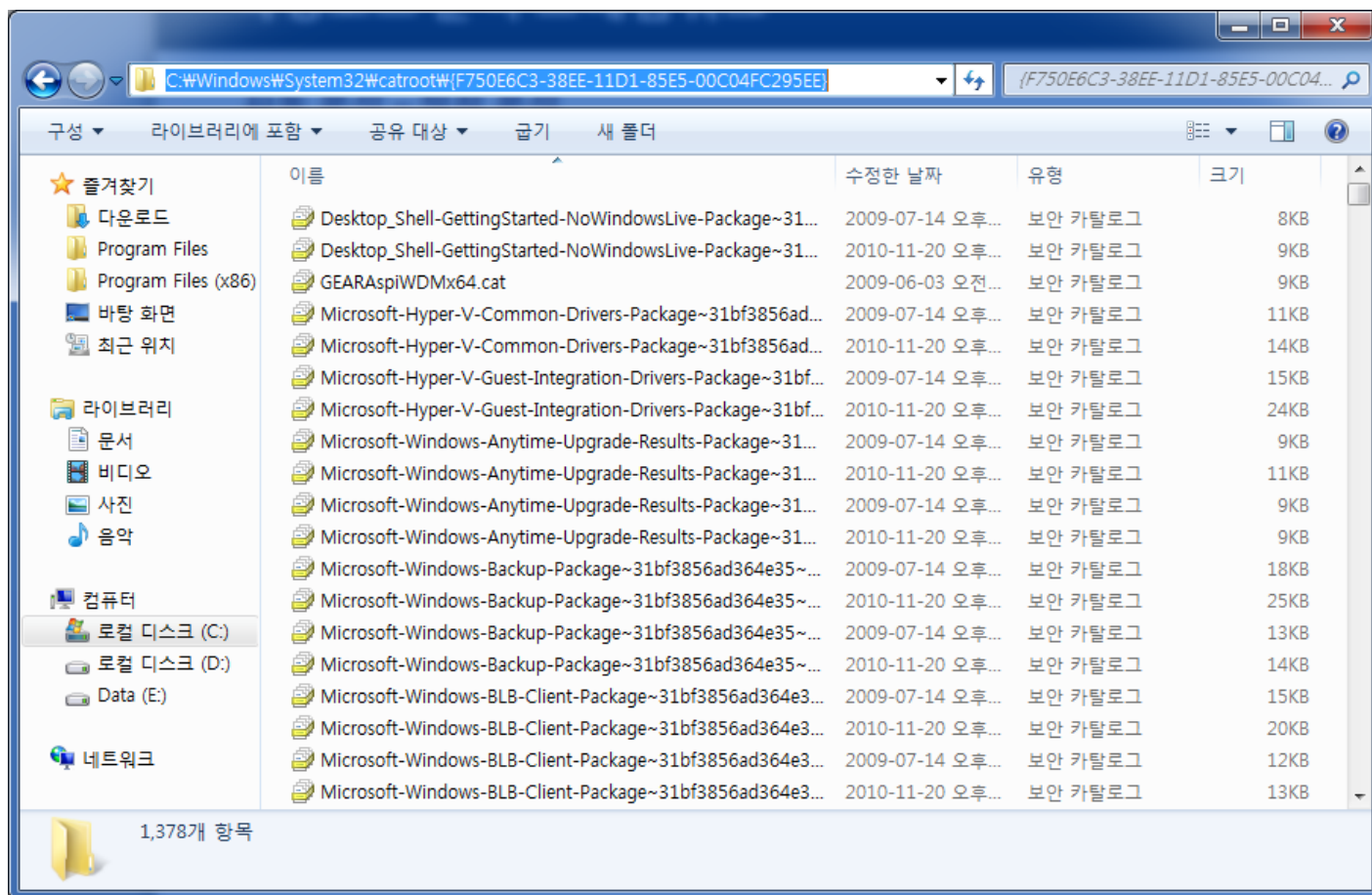
- 서명 검증

- 파일의 디지털 서명이 유효한지, 제품명/제조사와 디지털 서명이 같은 지 검사



## 자동 분석 - 정적 분석 (4/4)

- 카탈로그 해시 비교
  - 윈도우 카탈로그 해시 데이터베이스 값 비교




## 자동 분석 – 백신 검사 (1/2)

- 2개 이상의 백신 중복 검사
  - 국내 백신 중 1개
    - 안랩 v3, 하우리 바이로봇
  - 국외 백신 중 1개
    - 카스퍼스키, 어베스트, 아비라, AVG, 마이크로소프트, ESET, 시만텍, 맥아피, 트렌드마이크로, 비트디펜더, 소포스, ...
- 백신 순위
  - AV-TEST (<http://www.av-test.org/en/tests/>)
  - VB100 (<http://www.virusbtn.com/vb100/index>)
  - AV-Comparatives (<http://www.av-comparatives.org/comparativesreviews>)

## 자동 분석 – 백신 검사 (2/2)

- 악성파일 시그니처 DB에 질의
  - Virus Total – <https://www.virustotal.com/>
  - Jotti – <http://virusscan.jotti.org/>





SHA256: be051b6498077ee0fbeca54417b41a98493ebde86b4f33754dc1512817025ab3

File name: smona\_be051b6498077ee0fbeca54417b41a98493ebde86b4f33754dc1512817025ab3.bin

Detection ratio: 11 / 42

Analysis date: 2012-07-18 09:59:52 UTC ( 1주, 5일 ago )



 More details

Antivirus	Result	Update
AhnLab-V3	-	20120718
AntiVir	-	20120718
Antiy-AVL	Trojan/win32.agent	20120717
Avast	-	20120718
AVG	-	20120718
BitDefender	-	20120718
ByteHero	-	20120716
CAT-QuickHeal	Trojan.Genome.adzfy	20120718

## 자동 분석 – 자동화 동적 분석 (1/2)

- 동적 분석 방법

- 분석 대상 실행 파일을 가상화 환경에서 실행한 후 행위 모니터링

- 동적 행위

- 프로세스 모니터링
- 파일 생성/읽기 모니터링
- 로드한 DLL 모니터링
- 레지스트리 생성/읽기 모니터링
- 네트워크 연결 모니터링
- ... ..

## 자동 분석 – 자동화 동적 분석 (2/2)

- 동적 분석 도구

- Anubis – <http://anubis.iseclab.org/>



The screenshot displays the Anubis web application interface. At the top, the title "Anubis: Analyzing Unknown Binaries" is centered, flanked by two Anubis head icons. Below the title is a navigation menu with links: Home, Advanced Submission, Clustering, News, About, Sample Reports, and Links (with sub-links for register and login). The main content area is titled "Task Overview" and contains a table of analysis details. To the right of the table is a "Save Report:" button with icons for HTML, XML, PDF, and Text. The footer of the interface identifies the organization as the International Secure Systems Lab and provides the contact email anubis@iseclab.org.

<b>Task ID:</b>	1f17c9f911c6a6b24315d05876f588df0
<b>File Name:</b>	Procmon.exe
<b>MD5:</b>	a94445ae49d456b997ad551f759fa9e9
<b>Analysis Submitted:</b>	2012-07-29 17:50:24
<b>Analysis Started:</b>	2012-07-29 17:50:24
<b>Analysis Ended:</b>	2012-07-29 17:53:14
<b>Created New Analysis Report:</b>	Yes
<b>Available Report Formats:</b>	HTML  XML  PDF  Text

International Secure Systems Lab  
Contact: anubis@iseclab.org

- CWSandbox – <http://www.gfi.com/malware-analysis-tool>
- Norman Sandbox – [http://www.norman.com/security\\_center/security\\_tools/](http://www.norman.com/security_center/security_tools/)
- Joebox – <http://www.joesecurity.org/>

## 자동 분석 – 침해 흔적 지표(IOC) 확인 (1/2)

- **침해 흔적 지표 (IOC, Indicators Of Compromise)**
  - 침해 사고를 의심하거나 판단할 수 있는 시스템 흔적
  - 알려진 지표를 이용해 분석 대상 시스템을 점검
  - 대표적으로 맨디언트(Mandiant)의 OpenIOC
- **OpenIOC**
  - 현재 맨디언트의 주도 하에 많은 기관이 참여하고 있지 않음
  - 국내 표적형 악성파일에 대한 데이터 부족
- **국내 IOC 데이터의 활용 방안이 필요**

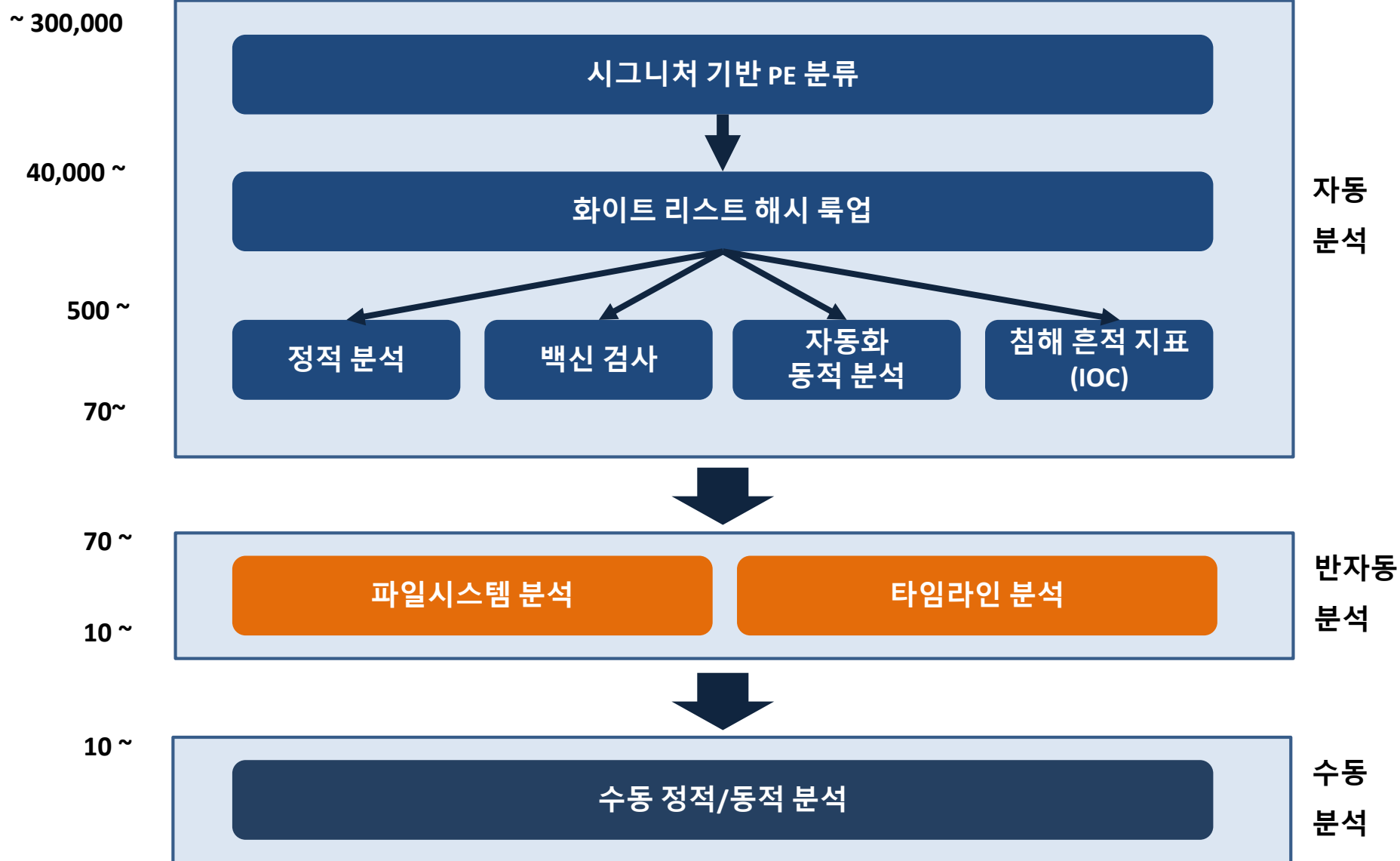
## 자동 분석 – 침해 흔적 지표(IOC) 확인 (2/2)

- IOC Example : Stuxnet

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="ea3cab0c-72ad-40cc-abbf-90846fa4afec"
last-modified="2011-11-04T19:35:05" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>STUXNET VIRUS (METHODOLOGY)</short_description>
  <description>Generic indicator for the stuxnet virus. When loaded, stuxnet spawns lsass.exe in a suspended state. The malware then maps in its
own executable section and fixes up the CONTEXT to point to the newly mapped in section. This is a common task performed by malware and allows the
malware to execute under the pretense of a known and trusted process.</description>
  <keywords>methodology</keywords>
  <authored_by>Mandiant</authored_by>
  <authored_date>0001-01-01T00:00:00</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="73bc8d65-826b-48d2-b4a8-48918e29e323">
      <IndicatorItem id="b9ef2559-cc59-4463-81d9-52800545e16e" condition="contains">
        <Context document="FileItem" search="FileItem/PEInfo/Sections/SectionName" type="mir" />
        <Content type="string">.stub</Content>
      </IndicatorItem>
      <IndicatorItem id="156bc4b6-a2a1-4735-bfe8-6c8d1f7eae38" condition="contains">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">mdmcpq3.PNF</Content>
      </IndicatorItem>
      <IndicatorItem id="e57d9a5b-5e6a-41ec-87c8-ee67f3ed2e20" condition="contains">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">mdmeric3.PNF</Content>
      </IndicatorItem>
      <IndicatorItem id="63d7bee6-b575-4d56-8d43-1c5eac57658f" condition="contains">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">oem6C.PNF</Content>
      </IndicatorItem>
      <IndicatorItem id="e6bfff12a-e23d-45ea-94bd-8289f806bea7" condition="contains">
        <Context document="FileItem" search="FileItem/FileName" type="mir" />
        <Content type="string">oem7A.PNF</Content>
      </IndicatorItem>
      <Indicator operator="AND" id="422ae9bf-a1ae-41f2-8e54-5b4c6f3e1598">
        <IndicatorItem id="e93f1610-daa1-4311-bcf3-3aecef8271c0" condition="contains">
          <Context document="DriverItem" search="DriverItem/DeviceItem/AttachedToDriverName" type="mir" />
          <Content type="string">fs_rec.sys</Content>
        </IndicatorItem>
      </Indicator>
    </definition>
  </ioc>
```

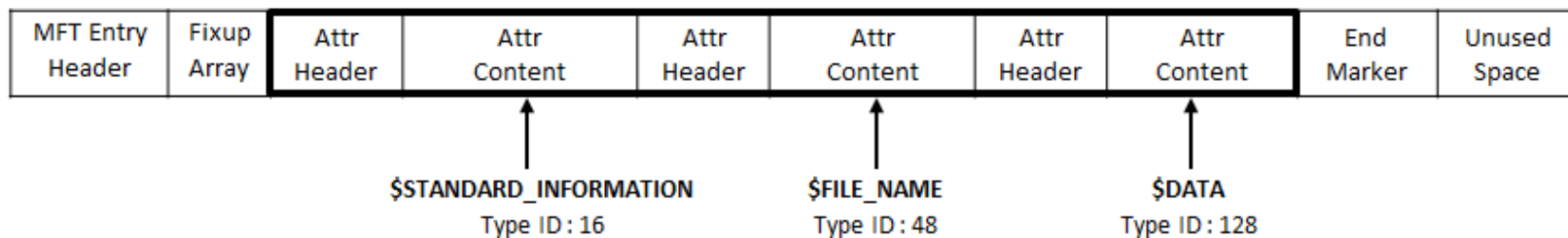


# 악성코드 분석 프레임워크



## 반자동 분석 – 파일시스템 분석 (1/7)

- 파일시스템 시간 변조



- \$SIA (STANDARD\_INFORMATION ATTRIBUTE), \$FNA (FILE\_NAME ATTRIBUTE)
  - 생성 시간 (Created Time)
  - 수정 시간 (Written Time)
  - 접근 시간 (Last Accessed Time)
  - MFT 수정 시간 (MFT Modified Time)
- API를 통해 생성, 수정, 접근 시간만 수정 가능 → MFT 수정 시간을 통해 시간 변조 탐지

## 반자동 분석 – 파일시스템 분석 (2/7)

- 행위에 따른 파일시스템 시간 흔적 (GUI)

\$STANDARD_INFO	생성	수정	접근	삭제	복사	로컬이동	볼륨이동	이름변경
Created	✓				✓			
Written	✓	✓						
Accessed	✓	✓	✓		✓		✓	
MFT Modified	✓			✓	✓	✓	✓	✓

\$FILE_NAME	생성	수정	접근	삭제	복사	로컬이동	볼륨이동	이름변경
Created	✓				✓		✓	
Written	✓			✓	✓	✓	✓	
Accessed	✓				✓		✓	
MFT Modified	✓			✓	✓	✓	✓	

# 악성코드 분석 프레임워크

## 반자동 분석 - 파일시스템 분석 (3/7)

### 파일시스템 시간 변조

- 시스템 폴더 중요 파일의 생성/수정/접근 시간을 얻어온 후 자신의 시간 정보 수정
- MFT 수정 시간이나 생성 시간 정렬을 이용해 악성 의심 파일 검출 가능

Drive C:

Windows\System32 21 days ago

Name	Ext.	Size	Created ^	Modified	Accessed	Record update	Attr.	1st sector
PSHED.DLL	DLL	56.1 KB	2009-07-14 08:19:28	2009-07-14 10:45:45	2009-07-14 08:19:28	2012-03-04 10:07:36	A	185792
clfs.sys	dll	77.5 KB	2009-07-14 08:19:34	2009-07-14 10:40:15	2009-07-14 08:19:34	2012-03-04 10:06:59	A	139017...
clfs.sys	dll	11.5 KB	2009-07-14 08:19:38	2009-07-14 10:41:55	2009-07-14 08:19:38	2012-03-04 10:07:44	A	8168856
services.exe	exe	321 KB	2009-07-14 08:19:46	2009-07-14 10:39:37	2009-07-14 08:19:46	2012-03-04 10:07:39	A	226920
csrss.exe	exe	7.5 KB	2009-07-14 08:19:49	2009-07-14 10:39:02	2009-07-14 08:19:49	2012-03-04 10:07:00	A	119760
smss.exe	exe	110 KB	2009-07-14 08:19:50	2009-07-14 10:39:41	2009-07-14 08:19:50	2012-03-04 10:07:41	A	436696
clfs.sys	sys	359 KB	2009-07-14 08:19:59	2009-07-14 10:52:31	2009-07-14 08:19:59	2012-03-04 10:06:59	A	367256
api-ms-win-security-lsal...	dll	3.5 KB	2009-07-14 08:20:47	2009-07-14 10:24:53	2009-07-14 08:20:47	2012-03-04 10:06:55	HA	110636...
api-ms-win-security-sdd...	dll	3.0 KB	2009-07-14 08:20:47	2009-07-14 10:24:53	2009-07-14 08:20:47	2012-03-04 10:06:55	HA	110666...
sechost.dll	dll	111 KB	2009-07-14 08:20:52	2009-07-14 10:41:53	2009-07-14 08:20:52	2012-03-04 10:07:39	A	332464
cryptbase.dll	dll	43.0 KB	2009-07-14 08:20:54	2009-07-14 10:40:24	2009-07-14 08:20:54	2012-03-04 10:07:00	A	94720
profapi.dll	dll	43.0 KB	2009-07-14 08:20:57	2009-07-14 10:41:53	2009-07-14 08:20:57	2012-03-04 10:07:36	A	134208
netevent.dll	dll	18.5 KB	2009-07-14 08:20:58	2009-07-14 10:30:47	2009-07-14 08:20:58	2012-03-04 10:07:19	A	144538...
nsi.dll	dll	13.5 KB	2009-07-14 08:21:05	2009-07-14 10:41:53	2009-07-14 08:21:05	2012-03-04 10:07:33	A	103296
RpcEpMap.dll	dll	65.5 KB	2009-07-14 08:21:05	2009-07-14 10:41:53	2009-07-14 08:21:05	2012-03-04 10:07:37	A	133952
winnsi.dll	dll	25.5 KB	2009-07-14 08:21:08	2009-07-14 10:41:56	2009-07-14 08:21:08	2012-03-04 10:07:48	A	176744
dhcpcsvc6.dll	dll	53.0 KB	2009-07-14 08:21:09	2009-07-14 10:40:28	2009-07-14 08:21:09	2012-03-08 08:32:33	A	192704
dhcpcsvc.dll	dll	85.0 KB	2009-07-14 08:21:09	2009-07-14 10:40:28	2009-07-14 08:21:09	2012-03-08 08:32:33	A	151104
dhcpcore6.dll	dll	219 KB	2009-07-14 08:21:13	2009-07-14 10:40:28	2009-07-14 08:21:13	2012-03-08 08:32:33	A	447512
IPHLAPI.DLL	DLL	143 KB	2009-07-14 08:21:13	2009-07-14 10:41:10	2009-07-14 08:21:13	2012-03-04 10:07:11	A	276512
dhcpcore.dll	dll	307 KB	2009-07-14 08:21:15	2009-07-14 10:40:28	2009-07-14 08:21:15	2012-03-04 10:07:02	A	446896
api-ms-win-core-ums-l1...	dll	3.0 KB	2009-07-14 08:21:15	2009-07-14 10:24:53	2009-07-14 08:21:15	2012-03-04 10:06:55	HA	110257...
shimeng.dll	dll	6.5 KB	2009-07-14 08:21:19	2009-07-14 10:41:54	2009-07-14 08:21:19	2012-03-08 08:32:37	A	8033728

## 반자동 분석 – 파일시스템 분석 (4/7)

- **시스템 폴더에 파일 생성**

- 파일명을 시스템 파일과 동일하게 생성하여 은닉 (다른 경로, Windows ➔ System32)
- 시스템 파일을 패치(정상 동작)하여 자신을 은닉
- 파일명을 랜덤으로 생성하여 은닉

- **비정상적인 경로에 파일 생성**

- 최근에는 APT 공격을 위해 최종 목적을 이루기 위한 시스템을 찾을 때까지 자신의 흔적을 은닉하면서 이동
- 시스템 폴더보다는 비정상적인 경로에 파일 생성
  - %SystemDrive%\\$Extend
  - %SystemDrive%\\$Recycle.Bin
  - %SystemDrive%\ProgramData
  - %SystemDrive%\System Volume Information

## 반자동 분석 – 파일시스템 분석 (5/7)

- **슬랙 영역 사용**
  - 슬랙 영역 – 논리적인 구조와 물리적인 구조의 차이로 생기는 낭비되는 공간
  - MFT 슬랙
  - INDX 슬랙
  - 램 슬랙
  - 드라이브 슬랙
  - 파일 슬랙
  - 파일시스템 슬랙
  - 볼륨 슬랙

# 악성코드 분석 프레임워크

## 반자동 분석 – 파일시스템 분석 (6/7)

- 슬랙 영역 사용 예

- MBR 루트킷의 경우 MBR 슬랙을 주로 이용
- TDL3/4 루트킷의 경우 동적디스크를 위해 예약된 파티션되지 않은 영역 사용

Hard disk 1								
Partitioning style: MBR								
Name	Ext.	Size	Created ^	Modified	Accessed	Record update	Attr.	1st sector
Partition 1	NTFS	199 GB						2048
Partition 2	NTFS	0.7 TB						417523712
Start sectors		1.0 MB						0
Unpartitionable space		1.7 MB						1953521664

```
40955 MB Disk 0 at Id 0 on bus 0 on atapi [MBR]
C: Partition1 [New <Raw>] 40947 MB < 40946 MB free>
  Unpartitioned space      8 MB

ENTER=Install D=Delete Partition F3=Quit
```

## 반자동 분석 – 파일시스템 분석 (7/7)

- **파일 카빙**

- 최근 APT 공격이 증가하면서 목적을 달성하기 전까지 흔적을 삭제
- 단순 파일 삭제 ➔ 완전 삭제(wiping) 기법 사용
- 파일 삭제 시 파일 카빙을 통한 복구 필요
- 레코드 단위의 카빙 필요

- **확장자 변조**

- 외부 감염된 사이트에 올려둔 파일을 내려받을 때 확장자 변조 주로 사용



## 반자동 분석 – 타임라인 분석 (1/2)

- **이상 징후 발견 시 해당 징후를 기준으로 타임라인 분석이 필요**
  - 악성코드 행위 확인
  - 추가적인 악성코드 발견
  - 감염 경로 확인
- **타임라인 데이터**
  - 파일시스템 시간 정보
  - 레지스트리 시간 정보
  - 인터넷 익스플로러/파이어폭스/크롬/사파리 시간 정보
  - 이벤트 로그 시간 정보
  - 아파치/IIS 시간 정보
  - 링크 파일 시간 정보
  - 프리/슈퍼패치 시간 정보
  - PCAP 시간 정보
  - EXIF 시간 정보
  - 휴지통 시간 정보
  - 복원지점/볼륨 새도우 복사본 시간 정보
  - ... ..

# 악성코드 분석 프레임워크

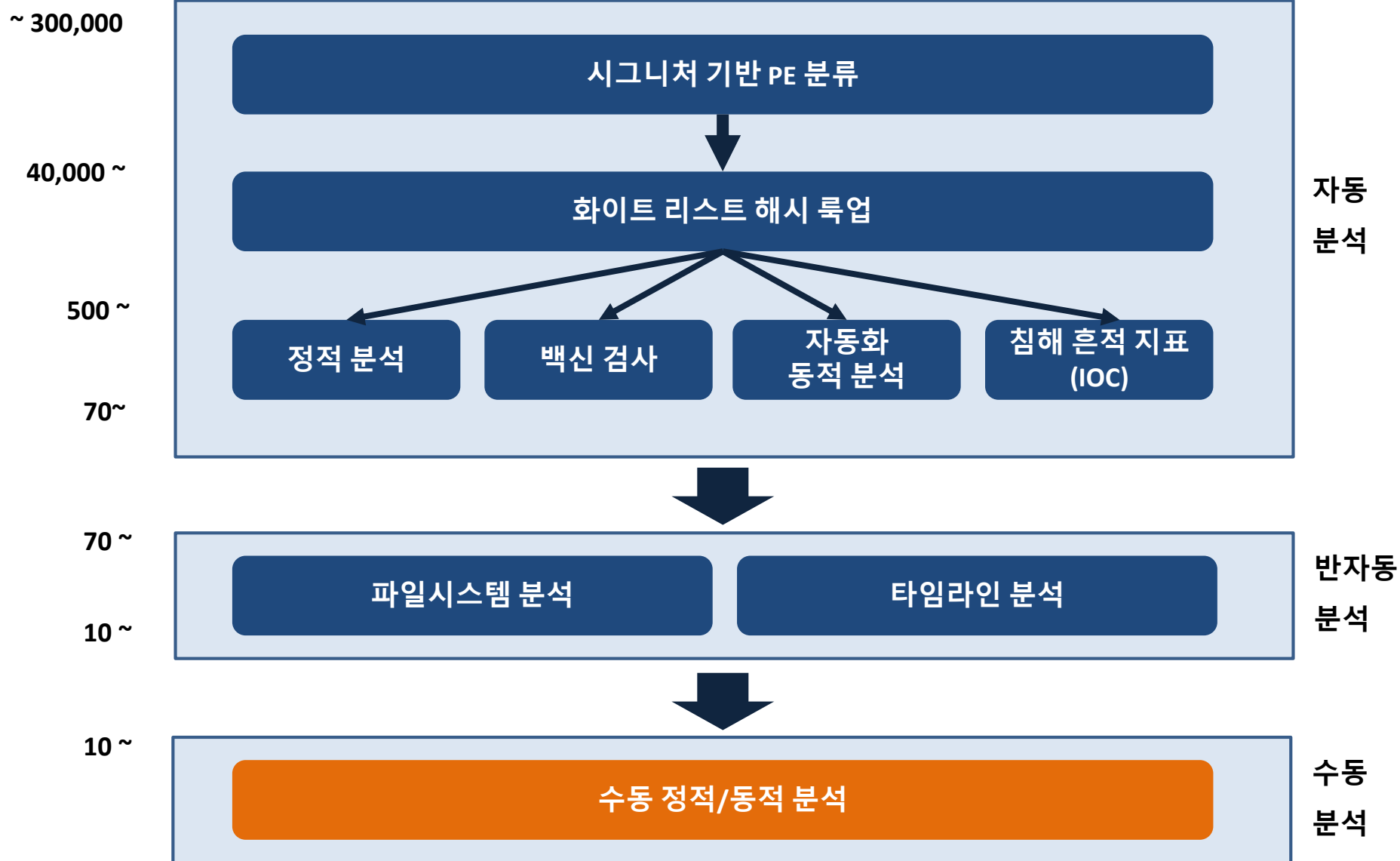
## 반자동 분석 – 타임라인 분석 (2/2)

- 타임라인 도구 – log2timeline (<http://log2timeline.net/>)
  - 슈퍼 타임라인 분석

A	B	C	D	E	F	G	J
date	time	timezone	MAC	source	sourcetype	type	short
6/18/2009	22:30:26	ESTSEDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/DRIVERS/msiscsi.sys[MofResource](Thu Jun 18 22:30:26 2009.29992 Entry in log file: C:/Windows/
6/18/2009	22:30:26	ESTSEDT	MACB	LOG	WMIprov Log file	Time Written	C:/Windows/system32/drivers/ndis.sys[MofResourceName](Thu Jun 18 22:30:26 2009.2998 Entry in log file: C:/Windows/
6/18/2009	22:36:15	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	LOGON.SCR-7C80CA1C.pf: LOGON.SCR was executed
6/18/2009	22:41:26	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] SYSTEM
6/18/2009	22:41:54	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DEFRAG.EXE-738093E8.pf: DEFRAG.EXE was executed
6/18/2009	22:41:54	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	DFRGNTFS.EXE-4F838A89.pf: DFRGNTFS.EXE was executed
6/18/2009	22:41:59	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] emRoot/System32/Config/SOFTWARE
6/18/2009	23:33:57	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/00000000/
6/18/2009	23:33:57	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/00000000/
6/18/2009	23:33:57	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/00000000/
6/18/2009	23:33:57	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/00000000/
6/18/2009	23:34:09	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	PKMAILER.EXE-83FAD500.pf: PKMAILER.EXE was executed
6/18/2009	23:34:35	ESTSEDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Stats
6/18/2009	23:34:36	ESTSEDT	MACB	REG	NTUSER key	Last Written	Software/Google/GoogleToolbarNotifier/Temp
6/18/2009	23:34:50	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	IPODSERVICE.EXE-FE1A6FF7.pf: IPODSERVICE.EXE was executed
6/18/2009	23:34:59	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	RUNDLL32.EXE-2E65B341.pf: RUNDLL32.EXE was executed
6/18/2009	23:34:59	ESTSEDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Windows/system32/rundll32.exe
6/18/2009	23:35:05	ESTSEDT	MACB	LSO	Flash Cookie	LSO created	Flash Cookie: site ui/preferences
6/18/2009	23:35:07	ESTSEDT	MACB	REG	NTUSER key	Last Written	Software/Microsoft/InternetExplorer/LowRegistry/Audio/PolicyConfig/PropertyStore/5447cc
6/18/2009	23:35:38	ESTSEDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:Mozilla Firefox.Ink
6/18/2009	23:35:39	ESTSEDT	MACB	REG	UserAssist key	Time of Launch	UEME_RUNPATH:C:/Program Files/Mozilla Firefox/firefox.exe
6/18/2009	23:35:39	ESTSEDT	MACB	PRE	Vista/Win7 Prefetch	Last run	FIREFOX.EXE-E60C0AA7.pf: FIREFOX.EXE was executed
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000003/
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/0000000E/
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/00000008/
6/18/2009	23:41:36	ESTSEDT	MACB	REG	Deleted Registry	Last Written	[DELETED] ???/{83da6326-97a6-4088-9453-a1923f573b29}/00000003/

<http://blogs.sans.org/computer-forensics/files/2012/01/NewPicture034.jpg>

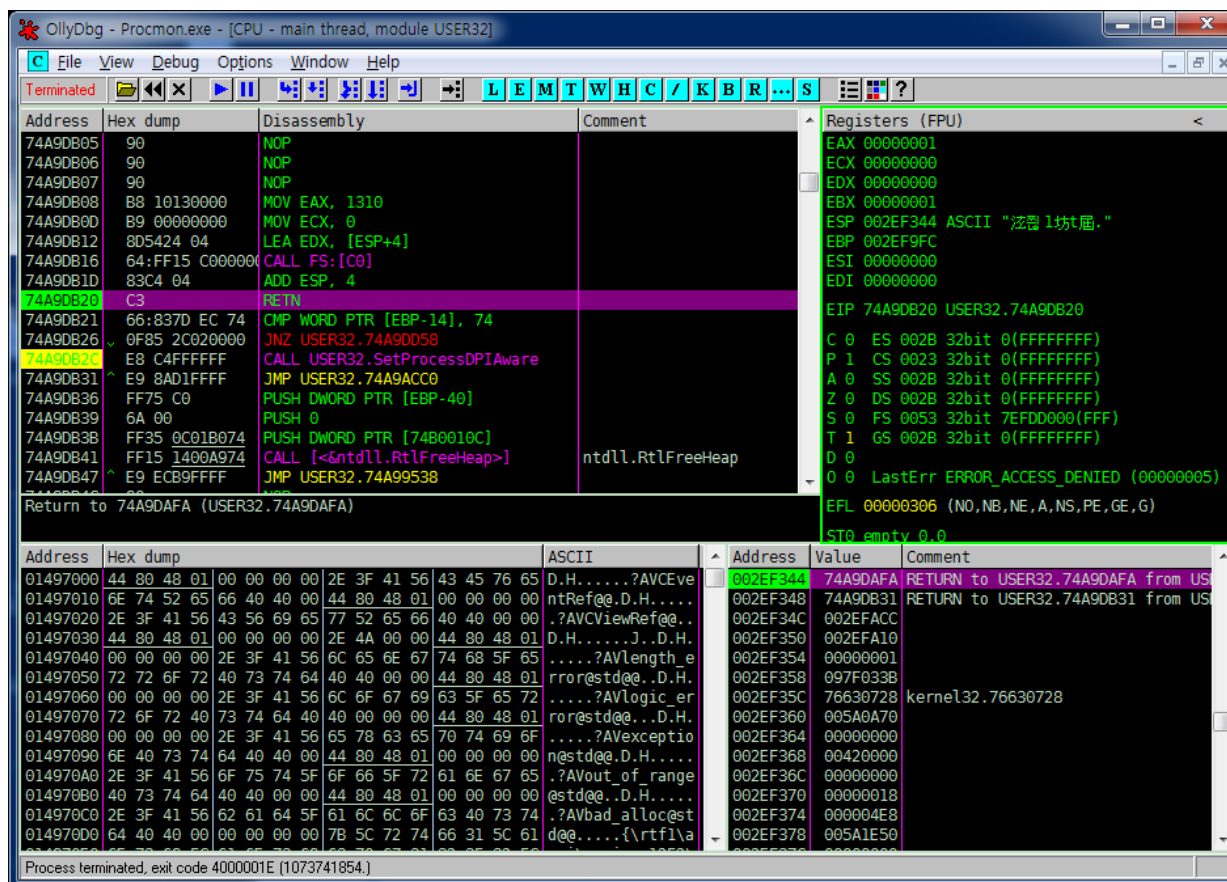
# 악성코드 분석 프레임워크



# 악성코드 분석 프레임워크

## 수동 분석 - 수동 정적/동적 분석

- 디버거를 이용한 분석
  - 정적/동적 디버거 - OllyDbg, IDA



# 악성코드 분석 프레임워크

## 수동 분석 - 수동 정적/동적 분석

- 가상화 환경에서 의심 악성코드 실행 후 메모리 분석
  - Volatility, Responder Pro, Redline, ...

```
C:\> 관리자: C:\Windows\system32\cmd.exe
C:\Users\proneer\Desktop\volatility-2.0\volatility-2.0>vol.py psscan -f "Windows XP Professional-8baf3bf4.vmem" --profile=WinXPSP3x86
Volatile Systems Volatility Framework 2.0
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)

Offset      Name                PID      PPID     PDB              Time created      Time exited
-----
0x01fde020  vmacthlp.exe        852      684      0x0e5400c0       2012-07-31 00:22:21
0x02023da0  services.exe        684      640      0x0e540080       2012-07-31 00:22:20
0x0212c4d8  svchost.exe         232      684      0x0e5402a0       2012-07-31 00:22:41
0x021cc3d0  winlogon.exe        640      392      0x0e540060       2012-07-31 00:22:20
0x021cd988  smss.exe            392       4       0x0e540020       2012-07-31 00:22:19
0x021d4558  msmgs.exe          1804     1504     0x0e540260       2012-07-31 00:22:24
0x021d4b58  vmtoolsd.exe        508      684      0x0e5402e0       2012-07-31 00:22:41
0x02209da0  ctfmon.exe         1816     1504     0x0e540280       2012-07-31 00:22:24
0x02220880  svchost.exe         864      684      0x0e5400e0       2012-07-31 00:22:21
0x02226a68  svchost.exe        1052     684      0x0e540120       2012-07-31 00:22:21
0x0229db20  svchost.exe         948      684      0x0e540100       2012-07-31 00:22:21
0x022e2da0  csrss.exe           616      392      0x0e540040       2012-07-31 00:22:19
0x02376ae8  WgaTray.exe        1488     640      0x0e5401c0       2012-07-31 00:22:22
0x023b0528  svchost.exe         444      684      0x0e5402c0       2012-07-31 00:22:41
0x023b41d8  WinCloud.exe        604      684      0x0e540300       2012-07-31 00:22:41
0x023c65b8  svchost.exe        1136     684      0x0e540160       2012-07-31 00:22:22
0x02446e8  VMwareTray.exe     1780     1504     0x0e540220       2012-07-31 00:22:24
0x0246a020  explorer.exe       1504     1464     0x0e5401e0       2012-07-31 00:22:22
0x0246b020  userinit.exe       1464     640      0x0e5401a0       2012-07-31 00:22:22
0x02489720  spoolsv.exe        1624     684      0x0e540200       2012-07-31 00:22:23
0x024a7a60  svchost.exe        1096     684      0x0e540140       2012-07-31 00:22:21
0x024d5a98  lsass.exe           696      640      0x0e5400a0       2012-07-31 00:22:20
0x024deda0  VMwareUser.exe     1788     1504     0x0e540180       2012-07-31 00:22:24
0x024f2710  lsass.exe          1796     1504     0x0e540240       2012-07-31 00:22:24
0x025c8830  System              4         0       0x00319000
```

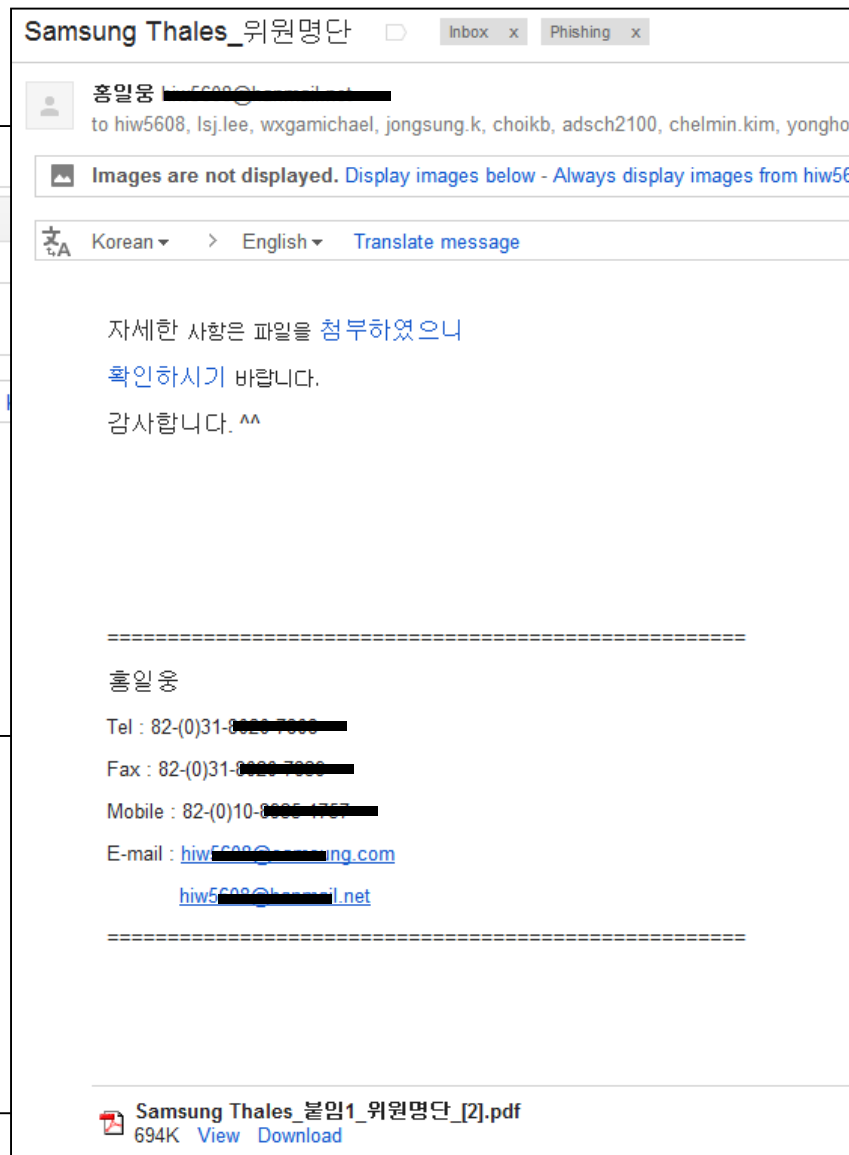
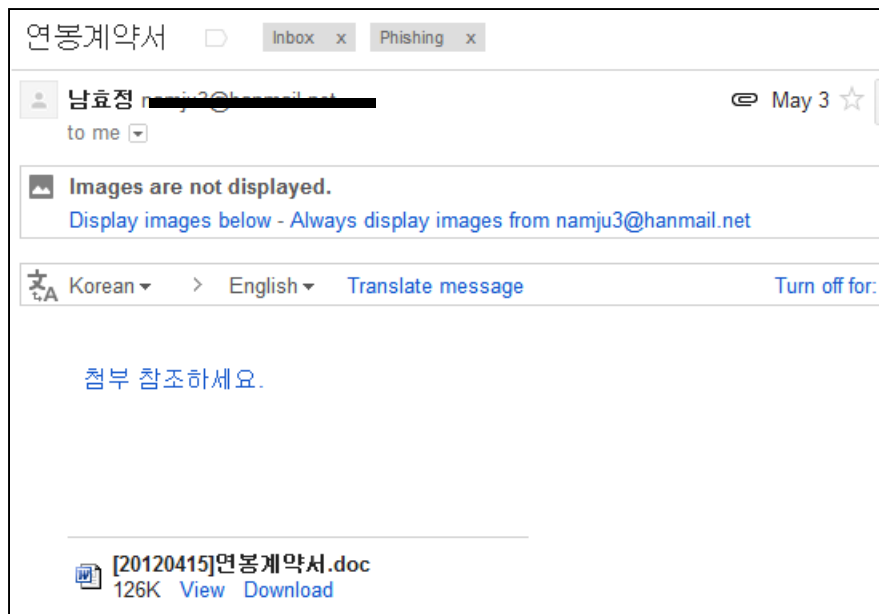
# 최근 악성코드 위협

*Security is a people problem...*

# 최근 악성코드 흐름

## 스피어-피싱 위협

- 연봉 계약서





- **금융권 피싱 사이트**
  - 개인의 사이트 아이디/비번, 보안카드 번호 탈취 목적
  - PC와 모바일을 모두 지원하는 피싱 사이트





# 최근 악성코드 흐름

## 애플리케이션 취약점 위협

뉴스  
토픽

### 제로보드 XE에서 XSS 취약점 발견...사용자 주의!

등록 : 12-07-31 05:31 , 데일리시큐 김민권기자 , mkgil@dailysecu.com

embed와 object 활용한 XSS 취약점...KISA에 전달

NHN(대표 김상헌)이 운영하는 제로보드XE(Xpress Engine)에서 XSS 취약점이 발견됐다. 이로 진행된 테스트에서 모두 XSS 취약점이 발견됐다. 이번 취약점은 26일 최진웅씨에게 발견됐고 KISA(한국인터넷진흥원)와 데일리시큐에 전달됐다.

최씨는 "embed와 object 활용한 XSS이고 embed의 경우엔 구형 브라우저에서 먹히지 않" "IE9, Chrome에서 테스트를 완료했다"고 밝혔다. 아래는 테스트 스크린샷이다.

```
84 </div>
85
86 <div class="readBody">
87 <div class="content">
```

뉴스  
토픽

### 네이버 영화리뷰 제목에 XSS 취약점 발견!

등록 : 12-07-31 04:55 , 데일리시큐 김민권기자 , mkgil@dailysecu.com

### 자바스크립트 실행 취약점으로 악성코드 배포 위험...패치 완료



뉴스  
토픽

### HWP 제로데이 취약점 이용한 신규 APT 공격

등록 : 12-06-21 04:45 , 데일리시큐 김민권기자 , mkgil@dailysecu.com

### 북핵 내용으로 위장...최신 버전 한컴오피스 사용자도 위험!

### 정부부처 및 기관, 국방, 기업 등 표적으로 한 APT 공격 예상

"북핵해결 3대 전략", "삼위일체의 북핵전략" 등의 내용을 가지고 있는 한컴오피스 파일을 이용한 악성파일이 발견됐다. 해당 악성파일이 사용한 보안취약점은 트가 공식 배포되고 있지 않은 Zero-Day 취약점이기 때문에 최신 버전의 직접적인 위협에 노출될 가능성이 매우 높은 상황이다.

잉카인터넷 대응팀 관계자는 "최근 연속해서 HWP 한글 문서 취약점을 이용한 등 국가안보와 관련된 정치적인 키워드를 포함한 악성 파일이 연속해서 발견될 수" "특정할 수는 없지만, 정부부처 및 기관, 국방, 기업 등을 표적으로 한 지능형 공격이" "이용되고 있을 것으로 예상된다"며 "한컴오피스 제품군 이용자들은 최신 업데이트" "이와 유사한 문서파일 열람을 가급적 자제하고 신뢰할 수 있는 보안서버" "에서 열람을 하는 것"을 당부했다.

뉴스  
토픽

### 어도비 플래시 취약점 악용한 타깃공격 발생!

등록 : 12-05-08 16:50 , 데일리시큐 김민권기자 , mkgil@dailysecu.com

### 이메일 첨부파일에 악의적 조작된 MS워드 파일 첨부해 공격진행

한국 시각으로 지난 5월 4일 저녁 시만텍(Symantec)에서는 블로그 "Targeted Attacks Using Confusion(CVE-2012-0779)"을 통해 Adobe Flash Player에 존재하는 CVE-2012-0779 취약점을 악용한 타깃 공격(Targeted Attack)이 발생하였음을 공개하였다.

이와 관련해 Adobe에서도 보안 권고문 "Security update available for Adobe Flash Player"을 통해 Flash Player에 CVE-2012-0779 취약점이 존재하며, 해당 취약점을 제거하기 위한 보안 패치를 공개하였다.

이 번에 공개된 해당 CVE-2012-0779 취약점은 Adobe Flash Player 11.2.202.233와 그 이전 버전의 모든 영향을 받는 것으로 밝혀지고 있다.

# 최근 악성코드 흐름

## 스마트폰 악성코드 위험



<http://image.ahnlab.com/comm/info/1203026626222985.jpg>

## 이벤트형 악성코드 위협

엔터프라이즈

[illegible]

글자 + -      

특히 오는 6월 개최되는 2010 남아공 월드컵 관련 내용의 메일로 위장해 어도비 아크로벳 2의 특정 이미지(TIFF) 파싱(Parsing, 구문분석) 관련 취약점 악용하는 악성코드 유포 사례가 외에서 보고 됐다. 악의적인 PDF는 기존에 알려진 CVE-2010-0188 취약점을 갖고 있다.

[illegible]

## /소셜결기자

# 최근 악성코드 흐름

## 위장형 악성코드 위험

### 통신사 요금명세서 위장 악성코드 주의보

[연립] 입력 2012-07-05 11:01:00 | 수정 2012-07-05 11:01:33

Like 0 Tweet 0 +1 0

f t p 기사보내기

음성듣기

통신사 요금명세서로 위장한 악성코드 파일이 발견됐다.

보안업체인 안랩[053800]은 최근 통신사 요금명세서로 위장해 유포되는 악성코드 파일이 발견돼 사용자들의 주의가 필요하다고 5일 밝혔다.

이 파일은 일반적으로 받는 요금명세서 형태지만 메일에 '\*\*\*email201205\_html 첨부파일이 있다.

### 국회의원 메일 위장, 악성 한글파일 발견

손경호 기자 sontech@zdnet.co.kr 2012.07.11 / PM 03:28 하우리, 국회의원 위장 악성코드 악성코드, 악성코드

- ▶ 밥먹고 OO마시면 살이 찍찍빠져!
- ▶ [단독공개] -10kg 가장
- ▶ 부부관계 오래하면 뭘해?얕은데...
- ▶ 당뇨는 내 몸을 바꿔야

정부가 등을 겨냥해 국회의원에게 발송한 것철 위장된 악성 한글파일 발견되고 있는 것으로 확인됐다.

하우리(대표 김희천)는 11일 '민중평등자문회의.hwp'라는가 첨부파일이 이메일을 통해 발송됐으며, 사용자가 열람할 경우 '한반도의 평화정착과 공동번영을 위하여'라는 제목의 문서가 열리면서 악성코드가 실행된다고 밝혔다.

해당 악성코드에 감염되면 ▲사용자 PC 이름 ▲사용자 IP Address ▲

forensic-proof.com

NEWS

**페이스북 친구위장 악성코드 등장, SNS 주의 요망**  
 조회1836 | 트위터노출 586989 | 추천0 | 스크랩0 | 11.11.03 12:04 | 조우성

뉴스 본문

수정 / 본문 함께쓰기 | 함께는 히스토리(1)

OPM t f p

0 1

Print +1

찾아다

페이스북 친구위장 악성코드 등장, SNS 주의 요망

11.11.03 12:04 | 조우성

3

- 이용자 PC에 악성코드 설치, 개인정보 빼가고 좀비 PC로 만들어 악용
- 아이패드 저가판매, 로또 당첨금 수령 등 광고성 스팸메일도 급증

스팸메일 차단 솔루션 개발 업체인 지란지교소프트가 국내 200여개 사의 이메일 데이터를 분석한 '3/4분기 스팸메일 동향 분석 보고서'에 따르면 바이러스 메일이 2/4분기 대비 무려 78%가 급증했으며, 페이스북 친구 요청 메일로 위장한 악성코드 메일이 새롭게 등장해 SNS이용자들의 주의가 요망된다고 밝혔다.

### 악성코드가 '디도스용 백신'으로 위장

다음 카페 등에서 가짜 '알약' 유포...사용자 주의 필요

2011.03.07월칠 19:07 입력

[마감임박] 5개월 100만원의 실용적 MBA!

글자 + -

t p f C +

안철수연구소  
 PC주치의의를 아시나요?  
 만족도 100% 도전!  
 PC주치의의 사용자 생성 릴레이

AL VacRemovalTool(3000x0S\_20110306\_1630) 등록 정보

파일 형식: 응용 프로그램  
 설명: AL VacRemovalTool(3000x0S\_20110306\_1630)  
 위치: H:\sample  
 크기: 1,17KB (1,236,752 바이트)  
 디스크 할당 크기: 1,17KB (1,236,752 바이트)  
 만든 날짜: 2011년 3월 7일 오후 11:40:29  
 수정한 날짜: 2011년 3월 7일 오후 11:40:32  
 액세스한 날짜: 2011년 3월 7일 오후  
 특성: ☐ 읽기 전용(☐ 숨김(☐ 보안(☐

DDOS용\_백신

파일 형식: 응용 프로그램  
 설명: DDOS용\_백신  
 위치: H:\sample  
 크기: 17KB (179,181 바이트)  
 디스크 할당 크기: 17KB (180,224 바이트)  
 만든 날짜: 2011년 3월 7일 오후 1:26:44  
 수정한 날짜: 2011년 3월 7일 오후 1:26:50  
 액세스한 날짜: 2011년 3월 7일 오후  
 특성: ☐ 읽기 전용(☐ 숨김(☐ 보안(☐

◇디지털 서명이 있는 정품(왼쪽)과 가짜 알약 [사진=미스트소프트]

## 고급 안티포렌식 기법 사용

- **파일 삭제**
  - 자신의 목적을 달성한 후 은닉을 위해 파일 삭제
  - 일반 삭제 → 완전 삭제(wiping), 시스템 파일로 여러 번 덮어쓰기
- **이벤트 로그 중지/삭제**
  1. 이벤트 로그에 흔적을 남기지 않기 위해 이벤트 로그 서비스를 중지 시킨 후 악성 행위
  2. 악성 행위 후 이벤트 로그를 초기화
- **네트워크 탐지 솔루션 우회를 위해 인코딩 기법 사용**
  - 특정 바이트나 패턴으로 XOR
- **포렌식 분석 데이터의 조작**

