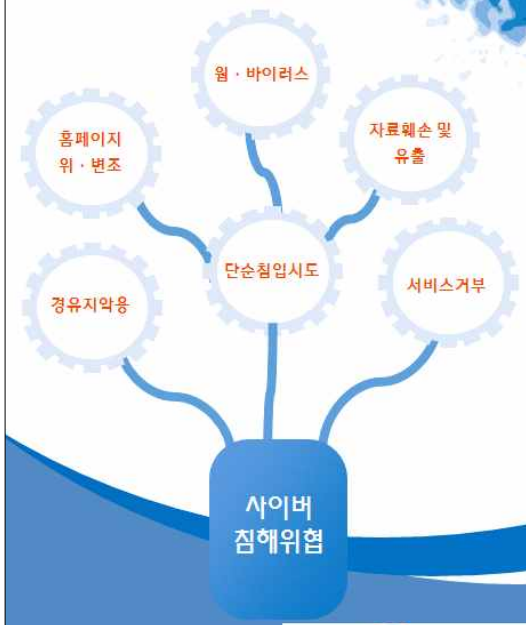
ISBN : 000-00-000-0000-0

사이버 침해위협 유형별 대응 매뉴얼



2015.11

KiSTi 한국과학기술정보연구원
www.kisti.re.kr
Korea Institute of Science and Technology Information

이 매뉴얼은 「한국과학기술정보연구원 보안업무규정」을 근거로 「과학기술분야」 사이버 침해위협 발생 시 정보보호담당자(또는 서버 · 네트워크 담당자)가 적용할 세부 대응요령 및 제반 조치사항 등을 규정하고 있음.

Ⅰ 개요

Ⅱ 유형별 대응요령

매뉴얼 활용을 위한 일러두기

<코드체계>

☐ 사이버 침해위협 유형별 대응 매뉴얼 코드체계

< 코드체계 구성 및 의미 >

▶ 코드체계 구성

코드체계	WV	01
	▲	▲
코드의미	사이버 침해위협 유형	작업
코드구분	WV : 웜·바이러스 DL : 자료훼손 및 유출 HH : 홈페이지 위·변조 MU : 경유지 악용 DA : 서비스 거부 SA : 단순침입시도	각 단계별 활동에 대해 01부터 1단위로 번호 부여

▶ 코드설명

코드구분	코드설명
WV	웜·바이러스(Worm Virus)
DL	자료훼손 및 유출(Data Leakage)
HH	홈페이지 위·변조(Homepage Hacking)
MU	경유지 악용(Malicious URL)
DS	서비스 거부(Denial of Service)
SA	단순침입시도(Simple Attack)

I

개요

KISTI
한국과학기술정보연구원

Ⅰ. 개요

1 목적

□ 본 매뉴얼은 과학기술분야 핵심 연구정보자원을 웜·바이러스 및 해킹 등과 같은 사이버 침해위협으로부터 보호하기 위하여,

□ 사이버 침해위협 유형별 대응요령을 정보보호 대상기관 및 첨단연구그룹 보안담당자들에게 제공함으로써 침해사고를 체계적·효율적으로 대응하고, 이에 따른 피해를 최소화하고자 한다.

< 사이버 침해위협 >

▶ 웜·바이러스, 홈페이지 위·변조, 서비스거부 공격 등으로 정보시스템의 정상적인 동작이 불가능한 상황이 발생되었거나 발생될 가능성이 있는 경우를 말한다.

2 매뉴얼 구성체계

□ 본 매뉴얼은 사이버 침해위협 유형별 대응을 위한 절차와 방법을 제공하며, 다음과 같은 내용으로 구성되어 있다. 본장에서는 사이버 침해위협 유형별 대응 매뉴얼에 대한 목적, 적용대상 및 범위, 관련법규 등에 대해 설명한다.

□ 2장에서는 각급 기관의 정보보호 담당자가 사이버 침해위협 유형별 대응 업무를 수행하는데 필요한 절차와 단계별 수행내용에 대해 설명한다.

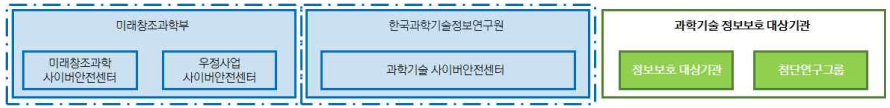
□ 각 유형은 웜·바이러스, 자료훼손 및 유출, 홈페이지 위·변조, 경유지 악용, 서비스거부, 단순침입시도로 6가지로 구성되며, 각 유형별 프로세스와 프로세스 하위에 존재하는 세부 프로세스는 다음의 항목에 따라 구성된다.

1) 설명 : 해당 유형에 대한 정의와 개념 설명
2) 대응요령 : 해당 유형에 대한 일반적인 절차 흐름과 이에 대한 주요내용
3) 특이사항 : 해당 절차를 수행하는데 참고해야 하는 사항

※ 단순침입시도에 대한 대응요령은 실업무에서 처리하는 경우가 없으므로 내용을 생략한다.

3 적용대상 및 범위

□ 본 매뉴얼의 적용대상은 과학기술분야 보안관제서비스를 제공받는 정보보호 대상기관 및 첨단연구그룹 대상이며, 적용범위는 사이버 침해위협 상황 발생 시 적용한다.



【 그림 Ⅰ.3 (1) 】 사이버 침해위협 유형별 대응 매뉴얼 적용대상

4 관련법규

□ 「국가사이버안전관리규정」(대통령훈령 제316호)

□ 「국가정보보안기본지침」

□ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(대통령훈령 제13014호)

□ 「미래창조과학부 정보보안기본지침」(미래창조과학부훈령 제25호)

Ⅱ

유형별 대응요령

KISTI
한국과학기술정보연구원

Ⅱ. 유형별 대응요령

1 개요

1.1 유형별 대응요령 구성내용

□ 사이버 침해위협 대응을 위해 필요한 작업을 웜·바이러스, 자료훼손 및 유출, 홈페이지 위·변조, 경유지 악용, 서비스거부로 구분하여 각 유형별 세부작업에 따른 상세 대응요령을 제공한다.

□ 각 유형별 정의, 절차, 절차별 방법 등 대응활동 전반에 걸친 제반 고려사항과 특이사항을 제공한다.

1.2 유형별 대응요령 공통 프로세스

□ 사이버 침해위협에 대한 피해를 최소화하기 위한 표준 대응 프로세스는 사고인지, 초동대응, 정밀분석, 재발방지 4단계로 운영한다.

< 사이버 침해위협 표준 대응 프로세스>

※ 상세한 분석이 필요한 경우에는 「3단계 정밀분석」을 실시한다.

1.3 단계별 수행활동 코드표

□ 사이버 침해위협 발생 시 유형별로 아래의 코드를 확인하여 점검한다.

【 표 Ⅰ.1.3 (1) 】 단계별 수행활동 코드표

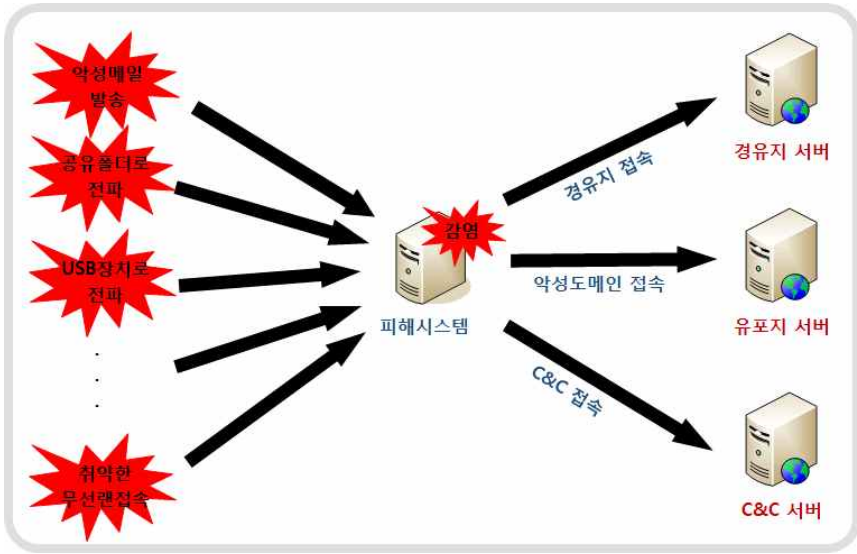
구분	단계	수행활동	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부
1단계	사고인지	메일·유선으로 피해사실인지	WV-01	DL-01	HH-01	MU-01	DA-01
		피해시스템 식별 (실 사용IP 확인)	WV-02	DL-02		MU-02	DA-02
		삽입(변조)된 페이지확인			HH-02		
2단계	초동조치	피해시스템의 네트워크 케이블 분리	WV-03	DL-03	HH-03	MU-03	
		보안장비에서 내·외부 유입경로차단	WV-04	DL-04	HH-04	MU-04	DA-03
		보안장비에서 자료훼손 및 유출여부확인		DL-05			
		백신 점검	WV-05	DL-06		MU-05	
		삽입(변조)된 파일경로확인			HH-05		
		삽입(변조)된 페이지 채증하여 별도보관			HH-06		
		삽입(변조)된 파일삭제 및 원본파일로 복구			HH-07		
		장비별 임계치 조정					DA-04
		조치 완료	WV-06	DL-07	HH-08	MU-06	DA-05
3단계	정밀분석	사용하지 않는 계정 및 숨겨진 계정확인	WV-07	DL-08	HH-09	MU-07	
		시스템로그의 변조유무확인	WV-08	DL-09	HH-10	MU-08	
		최근 변경된 파일·프로그램·서비스 확인	WV-09	DL-10	HH-11	MU-09	
		숨겨진 프로세스 및 비정상프로세스확인	WV-10	DL-11	HH-12	MU-10	
		비정상포트 및 외부연결확인	WV-11	DL-12	HH-13	MU-11	
		취약한 프로그램의 최신버전 설치여부확인		DL-13			
		웹로그에서 MOVE, PUT메소드 공격 여부확인			HH-14		
		웹서버에서 취약한 서비스 활성화여부확인			HH-15		
		네트워크장비에서 트래픽유발 IP주소 확인					DA-06
		보안장비에서 차단 트래픽량 및 세션수 확인					DA-07
		서버에서 트래픽량 및 세션수 등 확인					DA-08
4단계	재발방지	보완조치 및 재발방지조치	WV-12	DL-14	HH-16	MU-12	DA-09
		서비스 정상화	WV-13	DL-15	HH-17	MU-13	DA-10

2 웜·바이러스

2.1 설명

□ 웜·바이러스 피해란 컴퓨터 바이러스, 웜 등이 사용자의 동의 없이 컴퓨터에 설치되어 사용자의 정보가 탈취되거나 컴퓨터를 오동작하고 네트워크를 마비시킬 수 있는 악의적인 행위를 당하는 피해를 말한다.

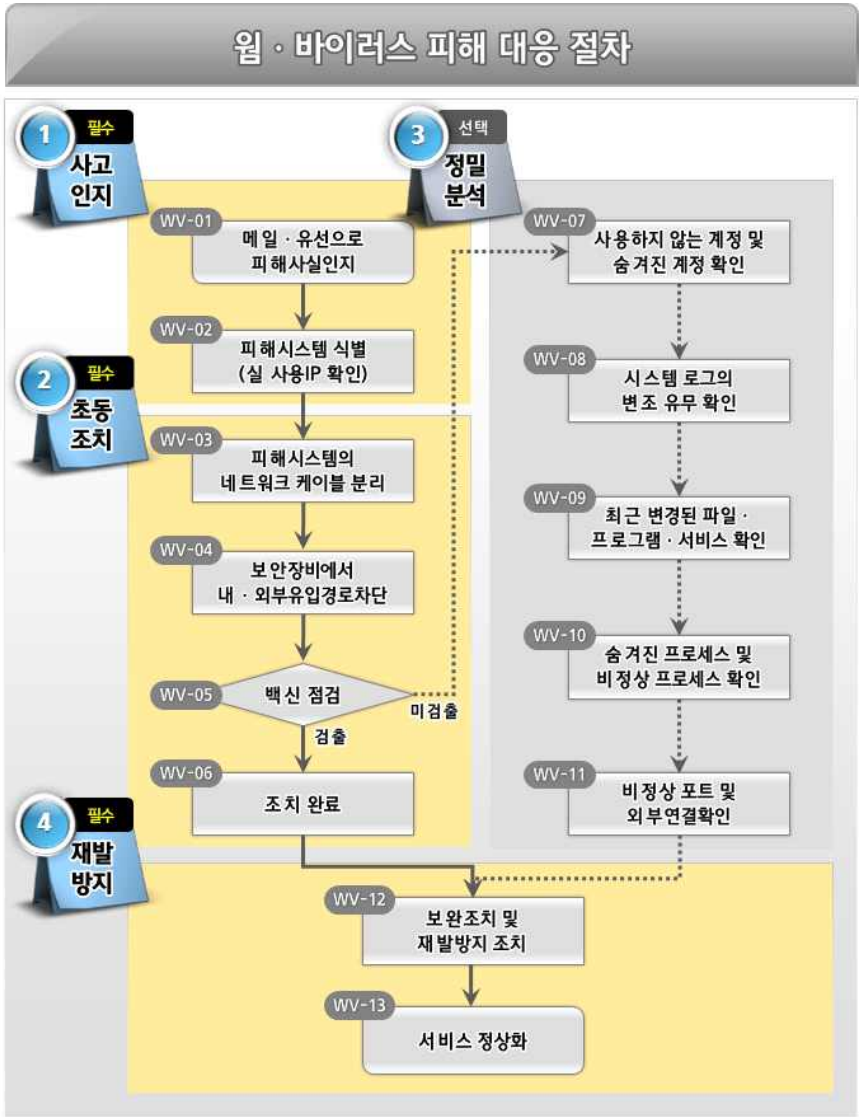
□ 웜·바이러스 피해 개요도



【 그림 Ⅱ.2.1 (1) 】 웜·바이러스 피해 개요도

2.2 대응요령

□ 웜·바이러스 피해 대응요령은 사고인지, 초동조치, 재발방지의 필수 절차와 정밀분석의 선택절차로 구성하여 운영한다.



【 그림 Ⅱ.2.2 (1) 】 웜·바이러스 피해 대응절차

2.2.1 사고인지

WV-01 메일 또는 유선으로 피해사실 인지

○ 자체 사고 탐지 및 과학기술사이버안전센터(S&T-SEC), NCSC 등으로부터 이관된 메일(유선)을 통해 피해사실을 인지한다.

WV-02 피해시스템 식별 (실 사용IP 확인)

○ 자체 사고 탐지 및 메일(유선)로 통보된 피해시스템 IP주소를 네트워크 장비 또는 방화벽 확인 등을 통해 실제 사용하는 IP주소를 확인하여 감염된 시스템을 식별한다.

2.2.2 초동조치

WV-03 피해시스템의 네트워크 케이블 분리

○ 감염된 호스트가 식별되면 해당 호스트를 네트워크에서 격리하여 2차 감염 확산을 방지한다.

WV-04 보안장비에서 내·외부유입경로차단

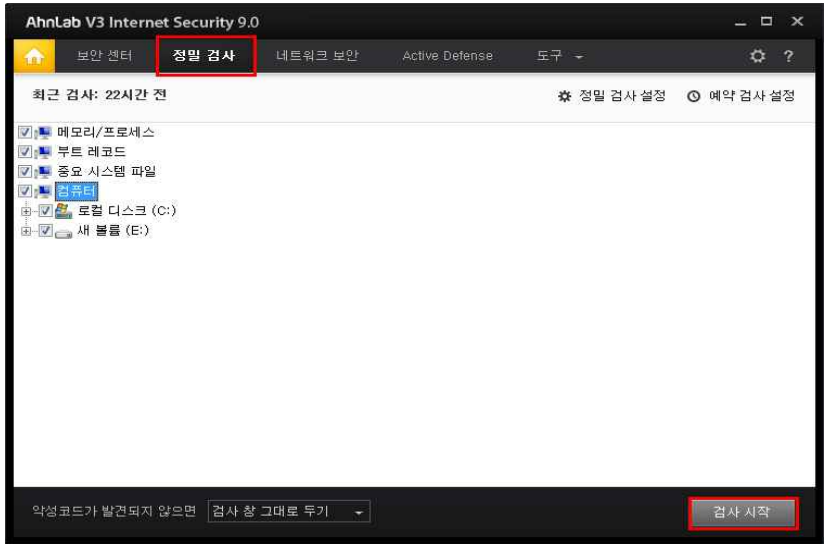
○ 웜·바이러스가 내부 네트워크로 접속 시도한 경우, 침입차단시스템, 스위치 또는 라우터의 차단규칙을 설정하여 내부 네트워크의 유입을 차단한다.

○ 내부 피해 시스템의 웜·바이러스가 외부 시스템으로 연결을 시도하는 경우 라우터나 침입차단시스템의 차단규칙을 이용하여 해당 연결 시도를 차단한다.

WV-05 백신 점검

○ 윈도우 시스템의 경우 안전모드로 부팅하여 백신프로그램을 실행 후 전체파일에 대해 정밀검사를 실시한다.

- 아래 그림은 Windows에서 백신프로그램(V3)으로 정밀검사를 실행하는 예시화면이다.



【 그림 Ⅱ.2.2 (2) 】 백신프로그램 정밀검사 실행화면 예시

○ 백신점검을 통해 악성코드가 검출될 경우 백신치료를 실시한다.

○ 백신점검 후 포맷조치 또는 추가 분석이 필요할 경우에는『 3. 정밀분석』 절차대로 분석을 실시한다.

WV-06 조치 완료

○ 백신프로그램으로 검출된 웜·바이러스를 제거 또는 치료한다.

2.2.3 정밀분석

WV-07 사용하지 않는 계정 및 숨겨진 계정 확인

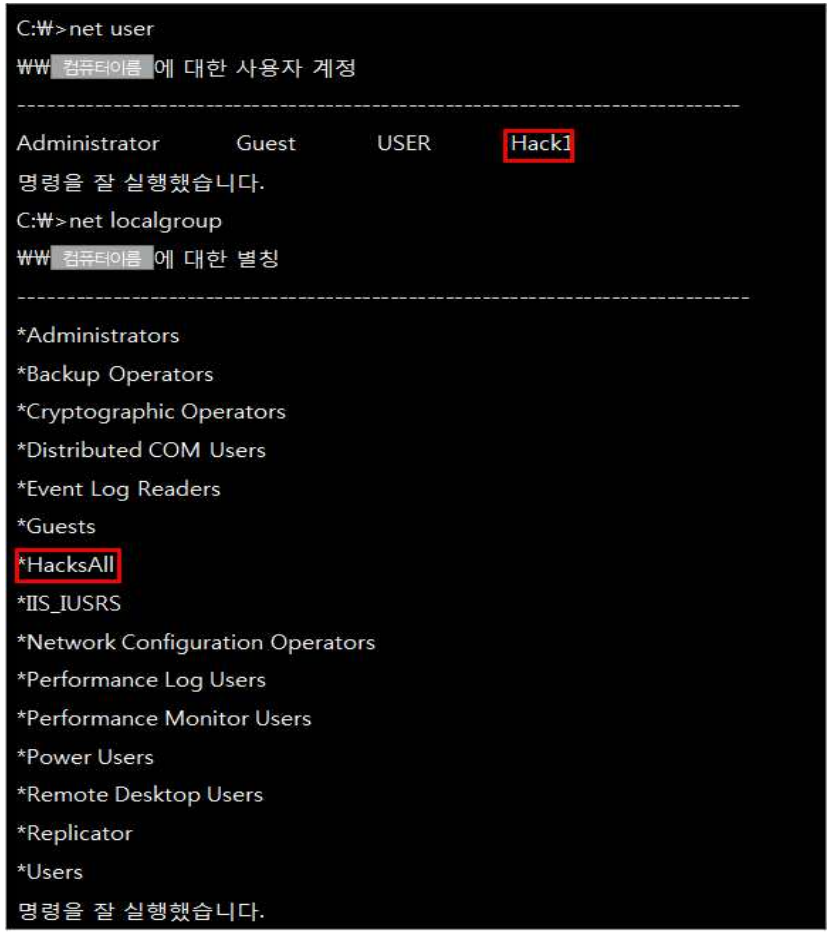
○ 불법적으로 등록된 사용자나 권한이 상승된 계정 및 그룹이 없는지 아래와 같은 방법으로 확인한다.

가. Windows

【 표 Ⅱ.2.2 (1) 】 Windows 사용자·그룹 정보 확인 명령어

명령어	설명	다운로드
net user	시스템에 존재하는 계정정보 출력	Windows
net localgroup	시스템에 존재하는 그룹정보 출력	Windows

- 아래 그림은 위의 명령어 실행을 통해 시스템의 계정정보 명령어를 실행한 화면이다.



【 그림 Ⅱ.2.2 (3) 】 Windows 시스템 계정정보 명령어 실행화면

- Hack1이란 불법계정이 생성되어있으며, HacksAll이란 불법그룹이 생성되어 있음을 알 수 있다. 그리고 내장된 guest 계정이 '사용 안함' 으로 되어 있는지 점검한다.

나. UNIX / LINUX

【 표 Ⅱ.2.2 (2) 】 UNIX 사용자 · 그룹 정보 확인 명령어

명령어	설명	다운로드
cat /etc/passwd	시스템에 존재하는 계정정보 출력	Unix/Linux

- /etc/passwd파일에서 UID=0인 계정은 root만이 가지고 있으므로 일반 계정에서 uid=0인 계정의 존재여부를 반드시 확인해야 한다.
- 아래 내용은 /etc/passwd파일의 내부 파일의 일부 화면과 설명이다.

```
root:x:0:0:root:/root:/bin/bash
user1:x:0:0::/home/user1:/bin/bash
```

【 그림 Ⅱ.2.2 (4) 】 /etc/passwd파일 내부화면

- user1이란 불법계정의 UID=0인 것을 확인할 수 있다.
- /etc/passwd파일의 구조는 아래와 같다.

【 표 Ⅱ.2.2 (3) 】 /etc/passwd파일 구조

root	:x	:0	:0	:root	:/root	:/bin/bash
❶	❷	❸	❹	❺	❻	❼

<참고설명>

❶ : 사용자 계정 이름(대부분 ID라고 부른다)
❷ : 사용자 비밀번호(x로 되어 있는 것은 섀도우 패스워드 시스템에 의해 /etc/shadow에 암호화된 형태로 저장 되어있음)
❸ : 사용자 UID(모든 정보는 수치 값으로 저장 되어 있음 root -> 0(UID))
❹ : 사용자 소속 그룹 GID(모든 정보는 수치 값으로 저장 되어 있음 root -> (GID))
❺ : 사용자 정보(계정이름)
❻ : 사용자 계정 디렉터리(계정 홈 디렉터리)
❼ : 사용자 로그인 쉘 (리눅스 : bash Shell, 유닉스 : Korn Shell 등등)

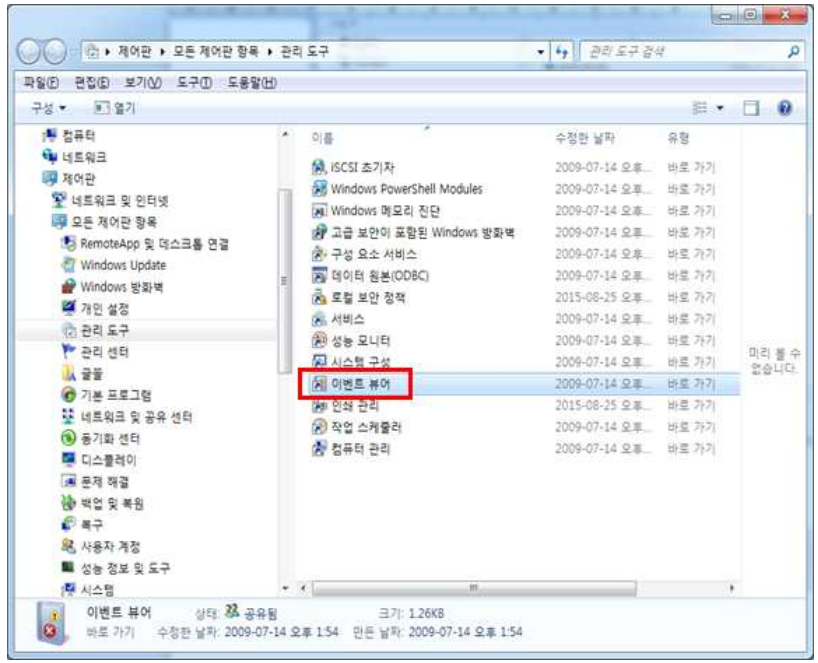
WV-08 시스템 로그의 변조 유무 확인

○ 시스템을 비인가된 방법으로 접근한 공격자들은 시스템에 흔적을 남기게 된다. 이러한 흔적 및 활동 정보를 찾아내기 위해서는 로그 분석이 필요하다.

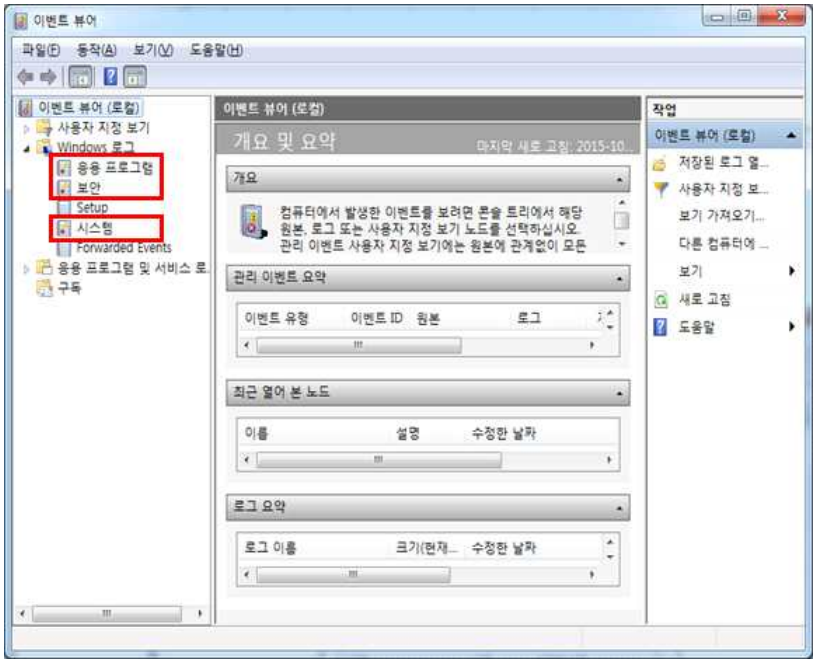
가. Windows

1) 이벤트뷰어

- 윈도우 시스템에서는 하드웨어, 소프트웨어 및 시스템 문제를 이벤트 로그에 저장하므로 이벤트 뷰어 실행을 통해 확인이 필요하다.
- 위치 : 제어판➜관리도구➜컴퓨터관리➜이벤트 뷰어



【 그림 Ⅱ.2.2 (5) 】 Windows 이벤트 뷰어 경로화면



【 그림 Ⅱ.2.2 (6) 】 Windows 이벤트 뷰어 실행화면

- 아래의 표를 참고하여 이벤트 로그ID로 공격과 관련된 이벤트를 분석한다.

【 표 Ⅱ.2.2 (4) 】 특징별 이벤트 로그

특징	이벤트 설명	이벤트 ID
로컬 로그온 시도 실패	사용자 이름과 패스워드를 조합하여 로그온 시도 했을 때 생성되는 이벤트	529, 530, 531, 532, 533, 534, 537
계정의 잘못된 사용	입력된 사용자 계정/패스워드에는 문제가 없지만 다른 제한에 의해 로그온 실패 시 생성되는 이벤트	530, 531, 532, 533
계정 잠김	계정 잠금 정책에 의해 사용자 계정이 잠겼을 때 발생하는 이벤트	539
터미널 서비스 공격	터미널 서비스 연결 후 완전히 세션을 종료하지 않았거나 다시연결 했을 때 이벤트 발생	683, 682
사용자 계정 생성	사용자 계정이 만들어진 시간과 활성화된 시간으로 공격자에 의한 사용자 계정 생성 인지를 확인	624, 626
사용자 계정 패스워드	사용자 이외의 계정에 의해 패스워드가 변경되었을 경우 공격자에 의해 해당 사용자 계정이 탈취당한 경우	627, 628

나. UNIX / LINUX

1) secure파일

- secure파일은 보안과 관련된 중요한 로그를 남기며, 사용자 인증 관련된 로그를 포함하고 있다.
- secure파일은 syslog데몬에 의해 남겨지는데, 텍스트 형태의 파일이므로 cat등을 이용하여 확인할 수 있다.

```
# cat /var/log/secure
Nov 28 16:37:11 insecure in.telnetd[6317] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.ftpd[4258] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.rlogind[4168] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.rshd[6328] : conncet from 192.168.10.17
Nov 28 16:40:35 insecure login: LOGIN ON 1 BY Hack1 FROM Hack1
```

【 그림 Ⅱ.2.2 (7) 】 secure파일 열람화면

- 위의 그림에서 "Nov 28 16:37:11"에 192.168.10.17로부터 telnet, ftp, rlogin, rsh 등에 대한 접속시도가 있었음을 알 수 있다. 일반적으로 한 사용자가 짧은 시간에 이들 서비스 요청을 수동으로 할 수는 없으므로, 이 로그를 통해 192.168.10.17로부터 단순침입시도 공격이 있었음을 알 수 있다.

2) messages파일

- 시스템 에러, 재부팅 메시지, 로그인 실패 등의 많은 정보를 포함하고 있는 로그파일로써, 시스템 관리자가 시스템 장애 원인 또는 공격으로부터 남는 흔적을 찾아내기 위해서도 messages 파일을 점검한다.

```
# more /var/log/messages
Nov  12 13:44:12 msd1 su: 'su root' failed for aster on /dev/pts/1
Nov  12 14:22:30 msd1 rsh[10103]: connection from bad port
Nov  12 14:28:15 msd1 su: 'su root' failed for aster on /dev/pts/2
Nov  12 14:29:41 msd1 last message repeated 1 time
Nov  12 15:39:29 msd1 su: 'su root' failed for aster on /dev/pts/1
Nov  12 15:57:52 msd1 syslogd: going down on signal 15
```

【 그림 Ⅱ.2.2 (8) 】 messages파일 열람화면

<참고설명>

- 'root'권한으로의 불법적인 로그인 시도가 있었는지를 살펴본다.
- 'su'명령을 이용한'root'또는 특정 권한의 사용자로의 의심스러운 전환 시도가 있었는지를 살펴본다.
- 유효한 사용자로부터의 반복적인 실패한 로그인 시도가 있었는지를 살펴본다.

WV-09 최근 변경된 파일 · 프로그램 · 서비스 확인

○ 공격자들은 공격 성공 후 악성 파일 및 프로그램들을 레지스트리 뿐만 아니라, 서비스, 스케줄러 등에 등록해 놓기 때문에, 이러한 부분을 반드시 점검 하여야 한다.

가. Windows

1) MAC TIME 분석

- 일반적인 파일시스템은 디렉터리나 파일과 관련된 아래와 같은 시간 속성을 갖는다.

<참고설명>

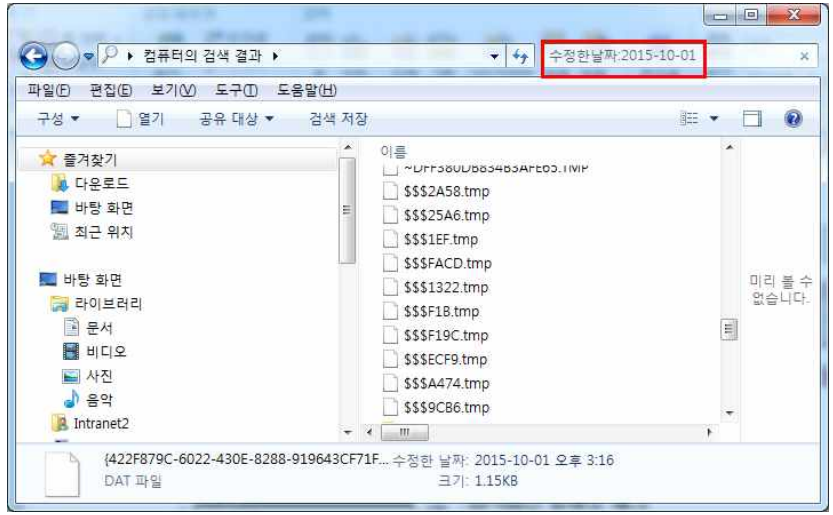
- MTIME : 파일을 생성 및 최근 수정한 시간
- ATIME : 최근 파일을 읽거나 실행시킨 시간
- CTIME : 파일 속성이 변경된 시간

- 이러한 시간 정보를 MAC time 이라 하며 분석을 통해 공격자가 파일 시스템에서 어떠한 행동을 했는지에 대해 판단 할 수 있는 정보를 제공한다.

<참고설명>

- 감염시점으로 MTIME, ATIME 검색
- 검출된 악성코드 MTIME, ATIME 검색

- 위치 : 시작-검색-파일 및 폴더-검색옵션-날짜



【 그림 Ⅱ.2.2 (9) 】 윈도우즈 MAC TIME으로 검색

<참고설명>

- 검색옵션은 날짜로 체크
- 찾고자 하는 MAC TIME 지정
  - 수정된 파일(MTIME)
  - 마지막으로 엑세스한 파일(ATIME)
  - 만든파일(CTIME)

- 감염 날짜를 기준으로 "마지막 엑세스 파일" 을 검사하게 되면 감염 후 실행됐던 파일들을 검색할 수 있다.

2) 설치 프로그램 점검

- 사고분석을 위해서는 피해시스템의 기본적인 정보가 필요하다. psinfo는 OS의 기본정보 및 보안 업데이트 정보 등을 제공하며 설치된 소프트웨어 정보 또한 알려준다. 이러한 보안 업데이트 정보는 시스템 취약점을 통해 어떻게 공격했는지에 대한 정보를 얻을 수 있기 때문에 최종 업데이트 날짜를 확인해야 한다.

【 표 Ⅱ.2.2 (5) 】 시스템 정보 확인 명령어

명령어	설명	다운로드
psinfo -h -s	설치된 핫픽스 및 소프트웨어 목록 정보	sysinternals

- 아래의 그림은 핫픽스 및 소프트웨어 목록을 확인한 화면이다.

```
C:₩Tools₩PSTools>psinfo -h -s

PsInfo v1.77 - Local and remote system information viewer
Copyright (C) 2001-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for ₩₩ 컴퓨터이름:
Uptime:                 7 days 8 hours 56 minutes 19 seconds
Kernel version:         Windows 7 Professional, Multiprocessor Free
Product type:           Professional
Product version:        6.1
Service pack:           0
Kernel build number:    7601
Registered organization:
Registered owner:       ????4
IE version:             9.0000
System root:            C:₩Windows
Processors:             8
Processor speed:        3.9 GHz
Processor type:         Intel(R) Core(TM) i7-4790K CPU @
Physical memory:        2616 MB
Video driver:           NVIDIA GeForce GTX 960

Installed     HotFix
n/a           Internet Explorer - 0
Applications:
Adobe Flash Player 18 ActiveX 18.0.0.232
Adobe Reader X (10.1.15) MUI 10.1.15
AhnLab Policy Agent 4.6 4.6
```

【 그림 Ⅱ.2.2 (10) 】 핫픽스 및 소프트웨어 목록 확인 명령어 실행화면

3) 서비스 점검

- 현재 윈도우에서 실행되고 있는 서비스 정보를 수집한다. 제어판의 서비스메뉴에서 설정할 수 있다. 대다수의 불법 서비스 항목은 윈도우 기본 서비스 이름과 유사한 이름을 사용하기 때문에 분석자는 윈도우 기본 서비스 항목과 불법 프로세스를 명확히 구분할 수 있어야 한다.

【 표 Ⅱ.2.2 (6) 】 서비스 정보 확인 명령어

명령어	설명	다운로드
net start	동작중인 서비스의 목록정보	Windows

- 아래의 그림은 동작중인 서비스 목록을 확인한 화면이다.

```
C:₩>net start
다음과 같은 Windows 서비스가 시작되었습니다.

   Adobe Acrobat Update Service
   AhnLab V3 Service
   ASUS Com Service
   Background Intelligent Transfer Service
   Base Filtering Engine
   CNG Key Isolation
   COM+ Event System
   Cryptographic Services
   DCOM Server Process Launcher
   Desktop Window Manager Session Manager
   DHCP Client
   Diagnostic Policy Service
   Diagnostic Service Host
   Diagnostics Tracking Service
   Distributed Link Tracking Client
   DNS Client
   Function Discovery Provider Host
   Group Policy Client
   Human Interface Device Access
   IKE and AuthIP IPsec Keying Modules
   Intel(R) Content Protection HECI Service
   Intel(R) HD Graphics Control Panel Service
   Intel(R) PROSet Monitoring Service
   IP Helper
```

【 그림 Ⅱ.2.2 (11) 】 서비스 목록 확인 명령어 실행화면

나. UNIX / LINUX

1) MAC TIME 분석

- 최근에 수정되거나 새롭게 생성된 파일을 찾는 명령어로 공격자가 시스템 파일의 변조를 숨기기 위해 시간을 수정하는 경우가 있으므로 이러한 경우에 대비하여 inode 변경시간을 점검한다.
- 아래의 그림은 최근 10일 동안 수정되거나 생성된 파일을 찾아서 파일로 저장하는 화면이다.

```
#find / -ctime -10 -print -xdev >/var/cime_10.txt
```

【 그림 Ⅱ.2.2 (12) 】 최근 10일 동안 수정 및 생성된 파일을 저장하는 화면

2) 설치 프로그램 점검

- setuid를 가지는 실행 프로그램은 실행도중에 슈퍼유저(root)의 권한을 가지고 실행되므로 find를 이용하여 setuid나 setgid 파일이 있는지 확인한다.

```
#find / -user root -perm -4000 -print>setuid.txt
#find / -user root -perm -2000 -print>setgid.txt
```

【 그림 Ⅱ.2.2 (13) 】 root권한을 가지고 실행하는 파일을 저장하는 화면

WV-10 숨겨진 프로세스 및 비정상 프로세스 확인

○ 일반적인 시스템들은 많은 실행 프로세스들을 가지고 있으며, 이러한 프로세스 중에는 공격자가 실행시켜놓은 프로세스가 실행되고 있거나 흔적이 남아 있을 수 있으니 자세히 확인해 볼 필요가 있다.

가. Windows

- 윈도우에서 프로세스를 점검할 수 있는 도구로는 pslist가 있다. 이 도구는 sysinternals에서 제공하며, 현재 구동 중인 프로세스 목록을 출력해준다.

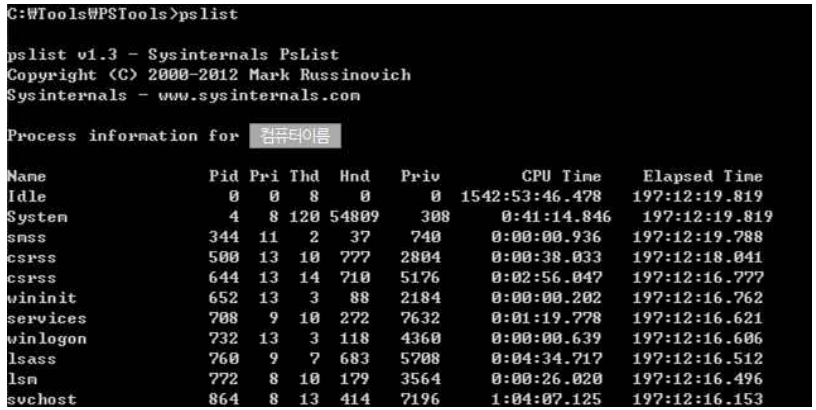
【 표 Ⅱ.2.2 (7) 】 프로세스 정보 확인 명령어

명령어	설명	다운로드
pslist	현재 프로세스 리스트 출력	sysinternals

- 프로세스 정보 확인시 주의해서 보아야 할 정보는 아래와 같다

<참고설명>

- 실행 프로세스명
- 프로세스 실행파일 위치
- 프로세스 커맨드 라인
- 프로세스 실행시간
- 프로세스가 참조중인 DLL 및 파일
- pslist : 현재 구동중인 프로세스 목록을 출력해 준다. 옵션을 하지 않으면 프로세스가 실행된 시간을 자세히 확인할 수 있는데 이러한 시간은 또 한 uptime에서 확인했던 부팅시간 이후에 악성프로그램이 언제 실행되었는지 확인 가능하다. -t 옵션을 사용하면 프로세스를 트리구조로 어떤 프로세스에서 실행되었는지 확인할 수 있다.



【 그림 Ⅱ.2.2 (14) 】 윈도우 프로세스 목록 정보 실행화면

나. UNIX / LINUX

- 프로세스 확인은 "ps -ef" 명령어를 통해 확인 할 수 있는데, process 실행자, PID, 실행일시, 프로세스명 등을 확인할 수 있다.

```
# ps -ef|more
UID    PID    PPID  C     STIME   TTY    TIME  CMD
root     1       0  0   May 22   ?        0:44/etc/init -r
root     2       0  0   May 22   ?        0:00pageout
root   339       1  0   May 22   ?        0:00/usr/openwin/bin/fbconsole -d :0
root    53       1  0   May 22   ?        0:00/usr/lib/devfsadm/devfseventd
root    57       1  0   May 22   ?        0:00/usr/lib/devfsadm/devfsadmd
root   138       1  0   May 22   ?        0:00/usr/sbin/keyserv
root   236       1  0   May 22   ?        0:00/usr/lib/power/powerd
root 25743       1  0    Jun 5   ?        0:03/usr/sbin/inetd -s
root   136       1  0   May 22   ?        0:07/usr/sbin/rpcbind
root   190       1  0   May 22   ?        0:00/usr/sbin/cron
root   176       1  0   May 22   ?        0:02/usr/lib/autofs/automountd
root   189       1  0   May 22   ?        0:04/usr/sbin/syslogd
root   204       1  0   May 22   ?        0:50/usr/sbin/nscd
root   296       1  0   May 22   ?        0:00/usr/dt/bin/dtlogin -daemon
root   297       1  0   May 22   ?        0:00/usr/lib/nfs/mountd
root   262       1  0   May 22   ?        0:00/usr/lib/sendmail -bd -q15m
root   316       1  0   May 22   ?        0:00/usr/lib/saf/sac  -t 300
root   371       1  0   May 22   ?        0:00/usr/openwin/bin/speckeysd
root   299       1  0   May 22   ?        0:00/usr/lib/nfs/nfsd  -a 16
root   337     305  0   May 22   ?        9:53mibiisa -r -p 32781
root   322     296  0   May 22   ?        0:00/usr/dt/bin/dtlogin -daemon
root   367     357  0   May 22   ?        0:00/usr/openwin/bin/fbconsole
root   390     357  0   May 22   ?        0:00/usr/openwin/bin/htt -nosm
root   433     431  0   May 22   ?        0:11dtwm
root   431     414  0   May 22   pts/2    0:45/usr/dt/bin/dtsession
```

【 그림 Ⅱ.2.2 (15) 】 유닉스 프로세스 목록 정보 실행화면

WV-11 비정상 포트 및 외부연결확인

○ 현재 열려있는 포트를 어떠한 응용 프로그램이 사용하는지에 대한 정보를 수집한다. 이는 피해시스템에서 특정 포트를 사용하는 백도어나 트로이목마를 찾기 위한 중요한 정보가 된다.

가. Windows

- “netstat -an” 명령어를 통해 프로토콜 상태, IP 기반 네트워크 연결 정보 등을 확인해서 현재 열려 있는 포트와 포트에 연결되어 있는 IP 정보를 확인해야 한다.

【 표 Ⅱ.2.2 (8) 】 네트워크 정보 확인 명령어

명령어	설명	다운로드
netstat -an	서비스 중인 포트 정보 및 연결된 아이피 정보	Windows

- 아래 명령어 수행결과에서 보면 시스템이 사용하지 않는 30451 포트가 LISTENING 상태로 열려 있는 것을 확인할 수 있다.

```
C:₩>netstat -an

활성 연결

프로토콜  로컬 주소          외부 주소          상태
TCP     0.0.0.0:135        0.0.0.0:0          LISTENING
TCP     0.0.0.0:445        0.0.0.0:0          LISTENING
TCP     0.0.0.0:1026       0.0.0.0:0          LISTENING
TCP     0.0.0.0:1027       0.0.0.0:0          LISTENING
TCP     0.0.0.0:1028       0.0.0.0:0          LISTENING
TCP     0.0.0.0:3371       0.0.0.0:0          LISTENING
TCP     0.0.0.0:30451      0.0.0.0:0          LISTENING
UDP     0.0.0.0:445        0.0.0.0:0          LISTENING
```

【 그림 Ⅱ.2.2 (16) 】 네트워크 정보 실행화면

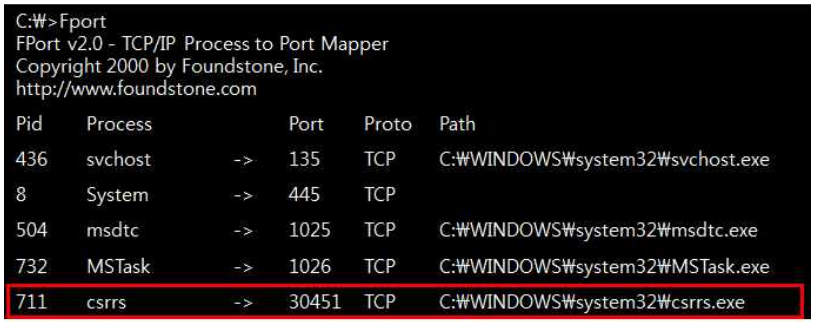
- 아래의 도구를 사용하여 열려있는 포트의 정보를 수집한다.

【 표 Ⅱ.2.2 (9) 】 포트별 서비스 정보 확인 명령어

명령어	설명	다운로드
fport	서비스 중인 포트를 열고 있는 프로그램 정보	foundstone.com

• fport 명령어는 어떠한 응용 프로그램이 어떤 포트를 사용하는지에 대한 정보를 보여준다.

<참고설명>
/p : 포트별 정렬
/a : 응용프로그램 이름순 정렬
/l : 프로세스 ID 정렬
/ap : 응용 프로그램 디렉토리 순 정렬



【 그림 Ⅱ.2.2 (17) 】 fport 실행화면

나. UNIX / LINUX

• netstat는 현재 시스템의 네트워크 연결상태를 알려주는 명령어로 어떤 포트가 열려있는 지 발신지 주소는 어떻게 되는지 등을 확인할 수 있다.

【 그림 Ⅱ.2.2 (18) 】 네트워크 정보 실행화면

2.2.4 재발방지

WV-12 보완조치 및 재발방지 조치

○ 사용하지 않는 계정과 숨겨진 계정 삭제

○ 외부 네트워크와 연결된 백도어 포트 발견 시 방화벽을 통해 해당포트로의 접근 제한 정책 적용

○ 백도어 포트 서비스를 실행중인 파일 확인 및 삭제

○ 그 외 공격자 흔적 제거

- 공격자의 모든 활동과 피해 흔적을 100% 분석한 경우는 이를 찾아서 복구하면 되나, 그렇지 않은 경우는 시스템 재설치

○ 비밀번호 교체

- 웜 · 바이러스 공격으로 인해 비밀번호가 유출되었을 가능성이 있으므로 피해 시스템 뿐만 아니라 관련된 시스템의 비밀번호 교체 실시

○ 백업 복구

- 웜 · 바이러스 공격 이후 파일이 변조되었을 가능성이 있으므로 감염 이전의 백업된 기록을 갖고 피해시스템을 복구

○ 취약점 제거 및 보안조치

- 침입의 원인이 된 취약점을 제거하고 웜 · 바이러스 공격과 관련된 보안패치를 포함하여 기존에 설치되지 않았던 모든 보안 패치를 설치
- 만약 보안패치가 없다면 취약점을 임시적으로 제거할 수 있는 수단을 강구해야 함
- 피해시스템의 안전한 운영을 위해 보안설정을 점검

WV-13 서비스 정상화

○ 시스템을 주기적으로 모니터링 하여 서비스 정상여부를 확인한다.

2.3 특이사항

☐ Mass SQL Injection 공격 대응방안

○ Mass SQL Injection에 피해를 입은 사이트에 접속을 한 경우 피해를 받지 않기 위해서 웹브라우저의 보안설정을 한다.

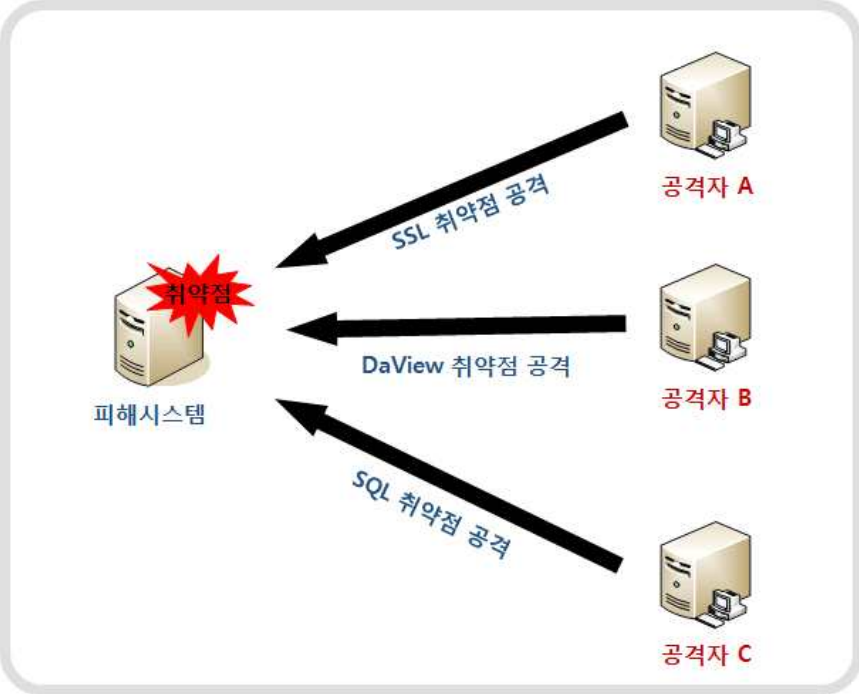
- Internet Explorer 에서는 보안 설정에 자바스크립트를 비활성화를 시켜서 사용할 수 있지만, 선별 기능이 없어 제약이 따른다.
- 파이어폭스는 애드온 중에 NoScript(자바 스크립트 방지) 라는 기능을 통하여 악성코드의 실행을 막을 수 있다.

3 자료훼손 및 유출

3.1 설명

☐ 자료훼손 및 유출 피해란 시스템에 설치된 소프트웨어에 취약점을 이용하여 시스템에 정보를 절취·훼손하는 일체의 공격 행위로 인한 피해를 말한다.

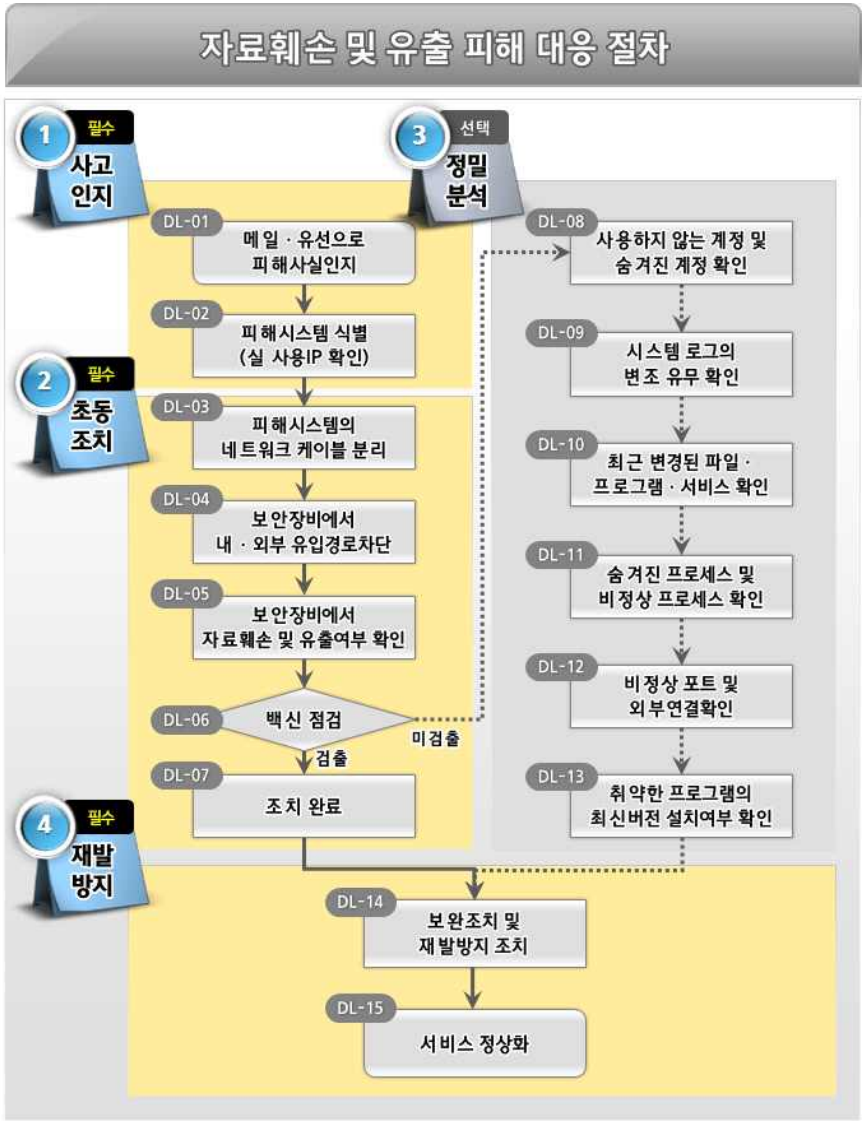
☐ 자료훼손 및 유출 피해 개요도



【 그림 Ⅱ.3.1 (1) 】 자료훼손 및 유출 피해 개요도

3.2 대응요령

□ 자료훼손 및 유출 피해 대응요령은 사고인지, 초동조치, 재발방지의 필수절차와 정밀분석의 선택절차로 구성하여 운영한다.



【 그림 Ⅱ.3.2 (1) 】 자료훼손 및 유출 피해 대응절차

3.2.1 사고인지

DL-01 메일 또는 유선으로 피해사실 인지

○ 자체 사고 탐지 및 과학기술사이버안전센터(S&T-SEC), NCSC 등으로부터 이관된 메일(유선)을 통해 피해사실을 인지한다.

DL-02 피해시스템 식별 (실 사용IP 확인)

○ 자체 사고 탐지 및 메일(유선)로 통보된 피해시스템 IP주소를 네트워크 장비 또는 방화벽 확인 등을 통해 실제 사용하는 IP주소를 확인하여 감염된 시스템을 식별한다.

3.2.2 초동조치

DL-03 피해시스템의 네트워크 케이블 분리

○ 감염된 호스트가 식별되면 해당 호스트를 네트워크에서 격리하여 2차 감염 확산을 방지한다.

DL-04 보안장비에서 내 · 외부유입경로차단

○ 악성코드가 내부 네트워크로 접속 시도한 경우, 침입차단시스템, 스위치 또는 라우터의 차단규칙을 설정하여 내부 네트워크의 유입을 차단한다.

○ 내부 피해 시스템의 악성코드가 외부 시스템으로 연결을 시도하는 경우 라우터나 침입차단시스템의 차단규칙을 이용하여 해당 연결 시도를 차단한다.

DL-05 보안장비에서 자료훼손 및 유출여부 확인

○ 기관에서 운영 중인 정보보호시스템(자료유출 탐지시스템, DB접근제어 등)에서 자료훼손 및 유출여부를 확인한다.

DL-06 백신 점검

○ 윈도우 시스템의 경우 안전모드로 부팅하여 백신프로그램을 실행 후 전체파일에 대해 정밀검사를 실시한다.

- 아래 그림은 Windows에서 백신프로그램(V3)으로 정밀검사를 실행하는 예시화면이다.

【 그림 Ⅱ.3.2 (2) 】 백신프로그램 정밀검사 실행화면 예시

○ 백신점검을 통해 악성코드가 검출될 경우 백신치료를 실시한다.

○ 백신점검 후 포맷조치 또는 추가 분석이 필요할 경우에는『 3. 정밀분석』 절차대로 분석을 실시한다.

DL-07 조치 완료

○ 백신프로그램으로 검출된 악성코드를 제거 또는 치료한다.

3.2.3 정밀분석

DL-08 사용하지 않는 계정 및 숨겨진 계정 확인

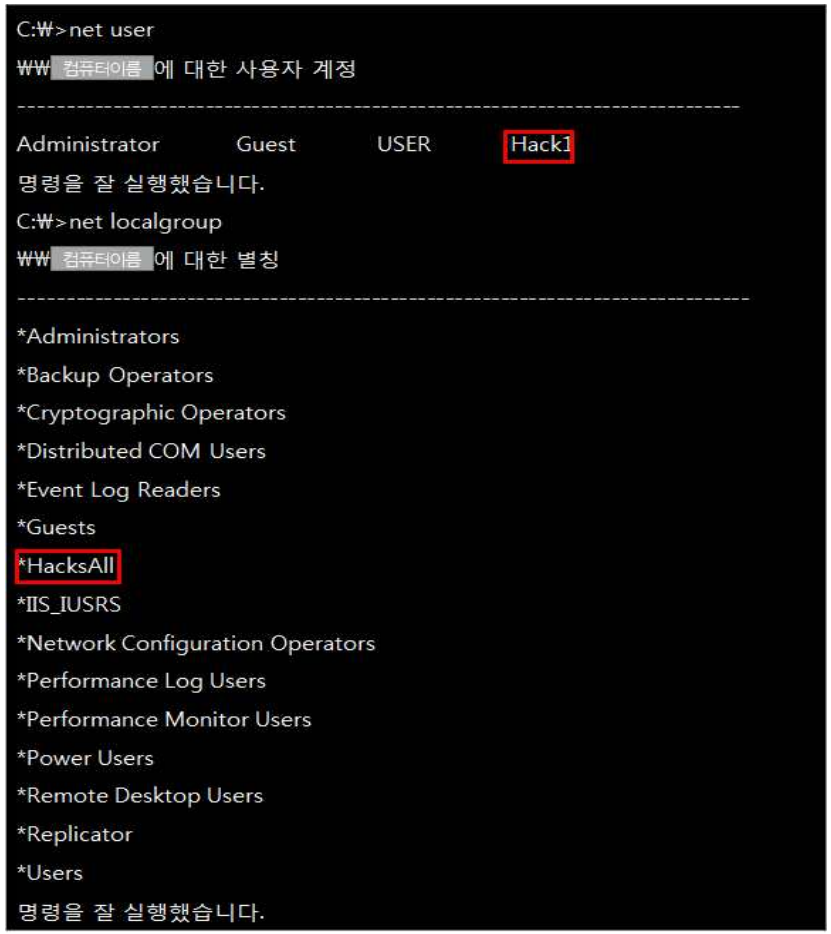
○ 불법적으로 등록된 사용자나 권한이 상승된 계정 및 그룹이 없는지 아래와 같은 방법으로 확인한다.

가. Windows

【 표 Ⅱ.3.2 (1) 】 Windows 사용자·그룹 정보 확인 명령어

명령어	설명	다운로드
net user	시스템에 존재하는 계정정보 출력	Windows
net localgroup	시스템에 존재하는 그룹정보 출력	Windows

- 아래 그림은 위의 명령어 실행을 통해 시스템의 계정정보 명령어를 실행한 화면이다.



【 그림 Ⅱ.3.2 (3) 】 Windows 시스템 계정정보 명령어 실행화면

- Hack1이란 불법계정이 생성되어있으며, HacksAll이란 불법그룹이 생성되어 있음을 알 수 있다. 그리고 내장된 guest 계정이 '사용 안함' 으로 되어 있는지 점검한다.

나. UNIX / LINUX

【 표 Ⅱ.3.2 (2) 】 UNIX 사용자 · 그룹 정보 확인 명령어

명령어	설명	다운로드
cat /etc/passwd	시스템에 존재하는 계정정보 출력	Unix/Linux

- /etc/passwd파일에서 UID=0인 계정은 root만이 가지고 있으므로 일반 계정에서 uid=0인 계정의 존재여부를 반드시 확인해야 한다.
- 아래 내용은 /etc/passwd파일의 내부 파일의 일부 화면과 설명이다.

【 그림 Ⅱ.3.2 (4) 】 /etc/passwd파일 내부화면

- user1이란 불법계정의 UID=0인 것을 확인할 수 있다.
- /etc/passwd파일의 구조는 아래와 같다.

【 표 Ⅱ.3.2 (3) 】 /etc/passwd파일 구조

root	:x	:0	:0	:root	:/root	:/bin/bash
❶	❷	❸	❹	❺	❻	❼

<참고설명>

❶ : 사용자 계정 이름(대부분 ID라고 부른다)
❷ : 사용자 비밀번호(x로 되어 있는 것은 섀도우 패스워드 시스템에 의해 /etc/shadow에 암호화된 형태로 저장 되어있음)
❸ : 사용자 UID(모든 정보는 수치 값으로 저장 되어 있음 root -> 0(UID))
❹ : 사용자 소속 그룹 GID(모든 정보는 수치 값으로 저장 되어 있음 root -> (GID))
❺ : 사용자 정보(계정이름)
❻ : 사용자 계정 디렉터리(계정 홈 디렉터리)
❼ : 사용자 로그인 쉘 (리눅스 : bash Shell, 유닉스 : Korn Shell 등등)

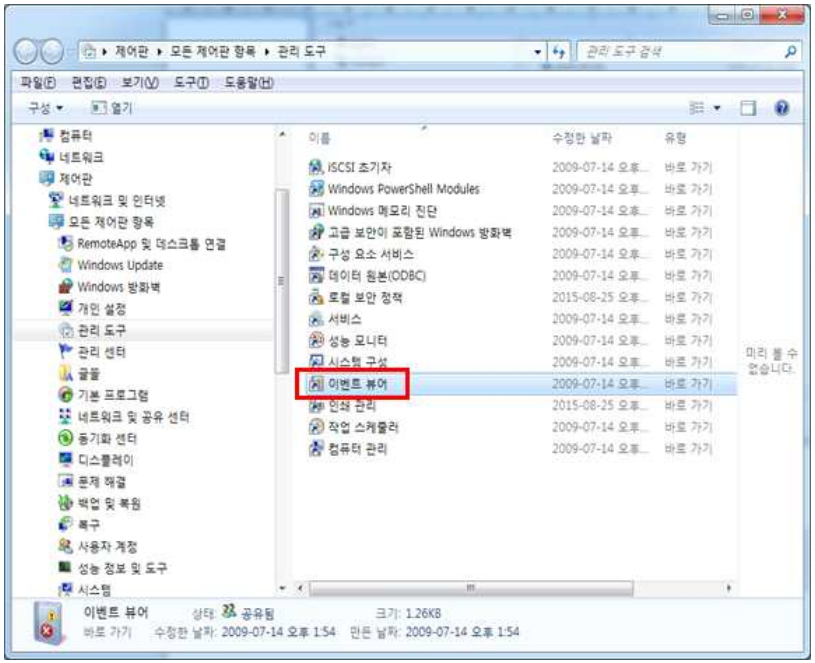
DL-09 시스템 로그의 변조 유무 확인

○ 시스템을 비인가된 방법으로 접근한 공격자들은 시스템에 흔적을 남기게 된다. 이러한 흔적 및 활동 정보를 찾아내기 위해서는 로그 분석이 필요하다.

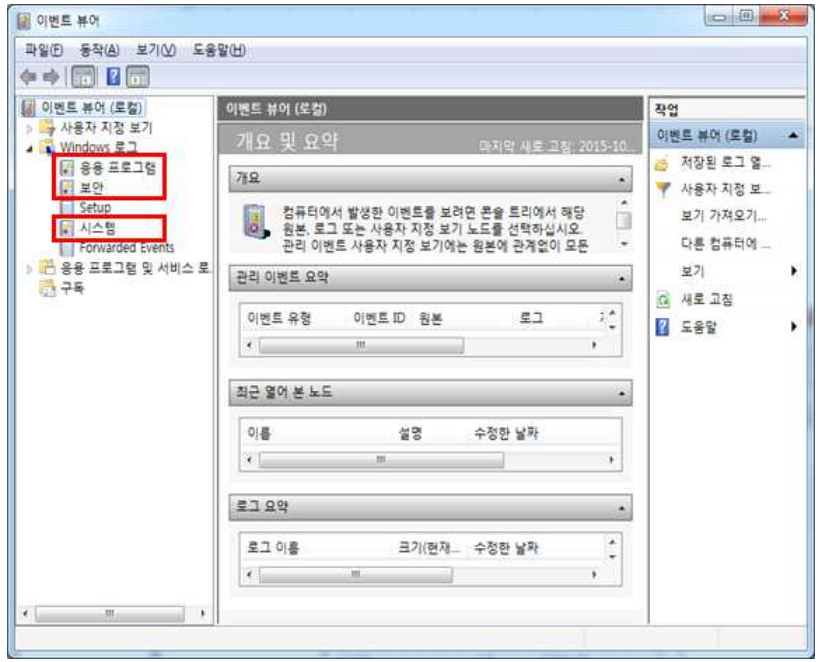
가. Windows

1) 이벤트뷰어

- 윈도우 시스템에서는 하드웨어, 소프트웨어 및 시스템 문제를 이벤트 로그에 저장하므로 이벤트 뷰어 실행을 통해 확인이 필요하다.
- 위치 : 제어판➜관리도구➜컴퓨터관리➜이벤트 뷰어



【 그림 Ⅱ.3.2 (5) 】 Windows 이벤트 뷰어 경로화면



【 그림 Ⅱ.3.2 (6) 】 Windows 이벤트 뷰어 실행화면

- 아래의 표를 참고하여 이벤트 로그ID로 공격과 관련된 이벤트를 분석한다.

【 표 Ⅱ.3.2 (4) 】 특징별 이벤트 로그

특징	이벤트 설명	이벤트 ID
로컬 로그온 시도 실패	사용자 이름과 패스워드를 조합하여 로그온 시도 했을 때 생성되는 이벤트	529, 530, 531, 532, 533, 534, 537
계정의 잘못된 사용	입력된 사용자 계정/패스워드에는 문제가 없지만 다른 제한에 의해 로그온 실패 시 생성되는 이벤트	530, 531, 532, 533
계정 잠김	계정 잠금 정책에 의해 사용자 계정이 잠겼을 때 발생하는 이벤트	539
터미널 서비스 공격	터미널 서비스 연결 후 완전히 세션을 종료하지 않았거나 다시연결 했을 때 이벤트 발생	683, 682
사용자 계정 생성	사용자 계정이 만들어진 시간과 활성화된 시간으로 공격자에 의한 사용자 계정 생성인지를 확인	624, 626
사용자 계정 패스워드	사용자 이외의 계정에 의해 패스워드가 변경되었을 경우 공격자에 의해 해당 사용자 계정이 탈취당한 경우	627, 628

나. UNIX / LINUX

1) secure파일

- secure파일은 보안과 관련된 중요한 로그를 남기며, 사용자 인증 관련된 로그를 포함하고 있다.
- secure파일은 syslog데몬에 의해 남겨지는데, 텍스트 형태의 파일이므로 cat등을 이용하여 확인할 수 있다.

```
# cat /var/log/secure
Nov 28 16:37:11 insecure in.telnetd[6317] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.ftpd[4258] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.rlogind[4168] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.rshd[6328] : conncet from 192.168.10.17
Nov 28 16:40:35 insecure login: LOGIN ON 1 BY Hack1 FROM Hack1
```

【 그림 Ⅱ.3.2 (7) 】 secure파일 열람화면

- 위의 그림에서 "Nov 28 16:37:11"에 192.168.10.17로부터 telnet, ftp, rlogin, rsh 등에 대한 접속시도가 있었음을 알 수 있다. 일반적으로 한 사용자가 짧은 시간에 이들 서비스 요청을 수동으로 할 수는 없으므로, 이 로그를 통해 192.168.10.17로부터 단순침입시도 공격이 있었음을 알 수 있다.

2) messages파일

- 시스템 에러, 재부팅 메시지, 로그인 실패 등의 많은 정보를 포함하고 있는 로그파일로써, 시스템 관리자가 시스템 장애 원인 또는 공격으로부터 남는 흔적을 찾아내기 위해서도 messages 파일을 점검한다.


```
# more /var/log/messages
Nov  12 13:44:12 msd1 su: 'su root' failed for aster on /dev/pts/1
Nov  12 14:22:30 msd1 rsh[10103]: connection from bad port
Nov  12 14:28:15 msd1 su: 'su root' failed for aster on /dev/pts/2
Nov  12 14:29:41 msd1 last message repeated 1 time
Nov  12 15:39:29 msd1 su: 'su root' failed for aster on /dev/pts/1
Nov  12 15:57:52 msd1 syslogd: going down on signal 15
```

【 그림 Ⅱ.3.2 (8) 】 messages파일 열람화면

<참고설명>

- 'root'권한으로의 불법적인 로그인 시도가 있었는지를 살펴본다.
- 'su'명령을 이용한'root'또는 특정 권한의 사용자로의 의심스러운 전환 시도가 있었는지를 살펴본다.
- 유효한 사용자로부터의 반복적인 실패한 로그인 시도가 있었는지를 살펴본다.

DL-10 최근 변경된 파일 · 프로그램 · 서비스 확인

○ 공격자들은 공격 성공 후 악성 파일 및 프로그램들을 레지스트리 뿐만 아니라, 서비스, 스케줄러 등에 등록해 놓기 때문에, 이러한 부분을 반드시 점검 하여야 한다.

가. Windows

1) MAC TIME 분석

- 일반적인 파일시스템은 디렉터리나 파일과 관련된 아래와 같은 시간 속성을 갖는다.

<참고설명>

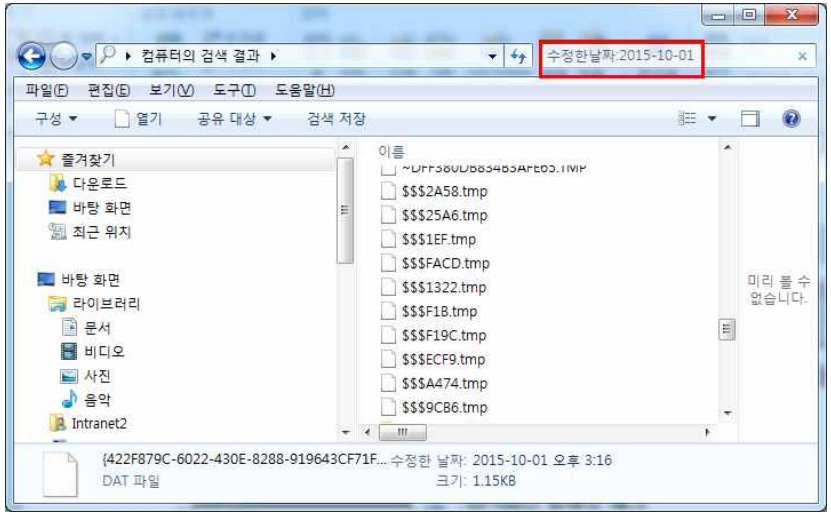
- MTIME : 파일을 생성 및 최근 수정한 시간
- ATIME : 최근 파일을 읽거나 실행시킨 시간
- CTIME : 파일 속성이 변경된 시간

• 이러한 시간 정보를 MAC time 이라 하며 분석을 통해 공격자가 파일 시스템에서 어떠한 행동을 했는지에 대해 판단 할 수 있는 정보를 제공한다.

<참고설명>

- 감염시점으로 MTIME, ATIME 검색
- 검출된 악성코드 MTIME, ATIME 검색

• 위치 : 시작-검색-파일 및 폴더-검색옵션-날짜



【 그림 Ⅱ.3.2 (9) 】 윈도우즈 MAC TIME으로 검색

<참고설명>

- 검색옵션은 날짜로 체크
- 찾고자 하는 MAC TIME 지정
  - 수정된 파일(MTIME)
  - 마지막으로 엑세스한 파일(ATIME)
  - 만든파일(CTIME)

• 감염 날짜를 기준으로 “마지막 엑세스 파일” 을 검사하게 되면 감염 후 실행됐던 파일들을 검색할 수 있다.

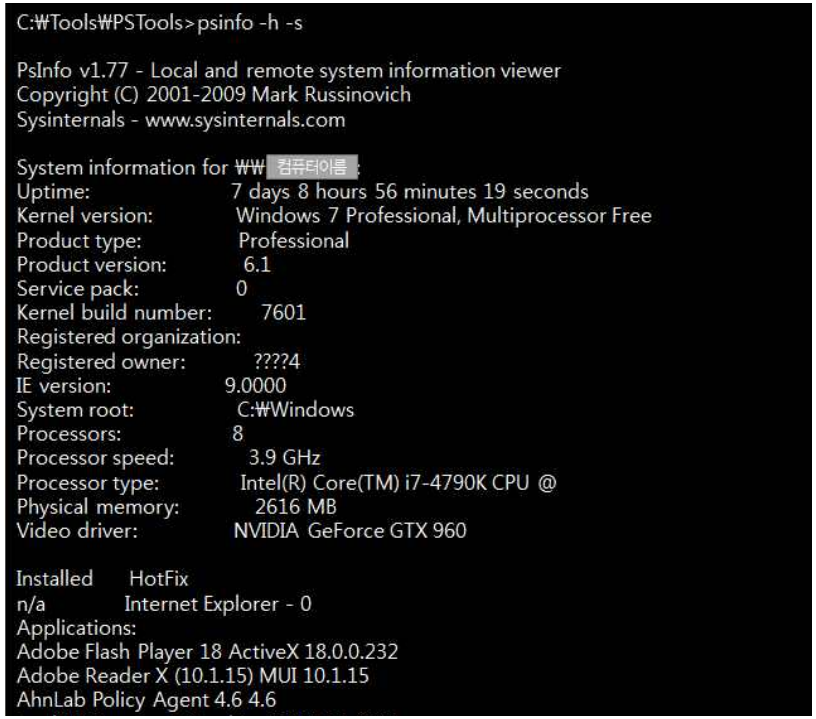
2) 설치 프로그램 점검

• 사고분석을 위해서는 피해시스템의 기본적인 정보가 필요하다. psinfo는 OS의 기본정보 및 보안 업데이트 정보 등을 제공하며 설치된 소프트웨어 정보 또한 알려준다. 이러한 보안 업데이트 정보는 시스템 취약점을 통해 어떻게 공격했는지에 대한 정보를 얻을 수 있기 때문에 최종 업데이트 날짜를 확인해야 한다.

【 표 Ⅱ.3.2 (5) 】 시스템 정보 확인 명령어

명령어	설명	다운로드
psinfo -h -s	설치된 핫픽스 및 소프트웨어 목록 정보	sysinternals

• 아래의 그림은 핫픽스 및 소프트웨어 목록을 확인한 화면이다.



【 그림 Ⅱ.3.2 (10) 】 핫픽스 및 소프트웨어 목록 확인 명령어 실행화면

3) 서비스 점검

- 현재 윈도우에서 실행되고 있는 서비스 정보를 수집한다. 제어판의 서비스메뉴에서 설정할 수 있다. 대다수의 불법 서비스 항목은 윈도우 기본 서비스 이름과 유사한 이름을 사용하기 때문에 분석자는 윈도우 기본 서비스 항목과 불법 프로세스를 명확히 구분할 수 있어야 한다.

【 표 Ⅱ.3.2 (6) 】 서비스 정보 확인 명령어

명령어	설명	다운로드
net start	동작중인 서비스의 목록정보	Windows

- 아래의 그림은 동작중인 서비스 목록을 확인한 화면이다.

```
C:₩>net start
다음과 같은 Windows 서비스가 시작되었습니다.

   Adobe Acrobat Update Service
   AhnLab V3 Service
   ASUS Com Service
   Background Intelligent Transfer Service
   Base Filtering Engine
   CNG Key Isolation
   COM+ Event System
   Cryptographic Services
   DCOM Server Process Launcher
   Desktop Window Manager Session Manager
   DHCP Client
   Diagnostic Policy Service
   Diagnostic Service Host
   Diagnostics Tracking Service
   Distributed Link Tracking Client
   DNS Client
   Function Discovery Provider Host
   Group Policy Client
   Human Interface Device Access
   IKE and AuthIP IPsec Keying Modules
   Intel(R) Content Protection HECI Service
   Intel(R) HD Graphics Control Panel Service
   Intel(R) PROSet Monitoring Service
   IP Helper
```

【 그림 Ⅱ.3.2 (11) 】 서비스 목록 확인 명령어 실행화면

나. UNIX / LINUX

1) MAC TIME 분석

- 최근에 수정되거나 새롭게 생성된 파일을 찾는 명령어로 공격자가 시스템 파일의 변조를 숨기기 위해 시간을 수정하는 경우가 있으므로 이러한 경우에 대비하여 inode 변경시간을 점검한다.
- 아래의 그림은 최근 10일 동안 수정되거나 생성된 파일을 찾아서 파일로 저장하는 화면이다.

```
#find / -ctime -10 -print -xdev >/var/cime_10.txt
```

【 그림 Ⅱ.3.2 (12) 】 최근 10일 동안 수정 및 생성된 파일을 저장하는 화면

2) 설치 프로그램 점검

- setuid를 가지는 실행 프로그램은 실행도중에 슈퍼유저(root)의 권한을 가지고 실행되므로 find를 이용하여 setuid나 setgid 파일이 있는지 확인한다.

```
#find / -user root -perm -4000 -print>setuid.txt
#find / -user root -perm -2000 -print>setgid.txt
```

【 그림 Ⅱ.3.2 (13) 】 root권한을 가지고 실행하는 파일을 저장하는 화면

WO-11 숨겨진 프로세스 및 비정상 프로세스 확인

○ 일반적인 시스템들은 많은 실행 프로세스들을 가지고 있으며, 이러한 프로세스 중에는 공격자가 실행시켜놓은 프로세스가 실행되고 있거나 흔적이 남아 있을 수 있으니 자세히 확인해 볼 필요가 있다.

가. Windows

- 윈도우에서 프로세스를 점검할 수 있는 도구로는 pslist가 있다. 이 도구는 sysinternals에서 제공하며, 현재 구동 중인 프로세스 목록을 출력해준다.

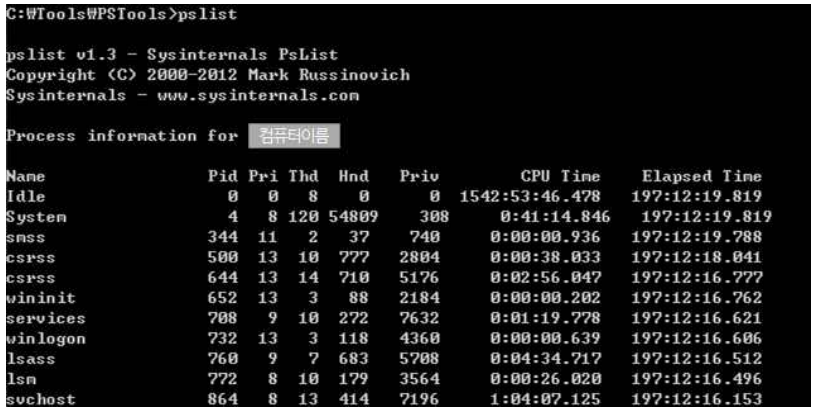
【 표 Ⅱ.3.2 (7) 】 프로세스 정보 확인 명령어

명령어	설명	다운로드
pslist	현재 프로세스 리스트 출력	sysinternals

• 프로세스 정보 확인시 주의해서 보아야 할 정보는 아래와 같다

<참고설명>

- 실행 프로세스명
- 프로세스 실행파일 위치
- 프로세스 커맨드 라인
- 프로세스 실행시간
- 프로세스가 참조중인 DLL 및 파일
- pslist : 현재 구동중인 프로세스 목록을 출력해 준다. 옵션을 하지 않으면 프로세스가 실행된 시간을 자세히 확인할 수 있는데 이러한 시간은 또 한 uptime에서 확인했던 부팅시간 이후에 악성프로그램이 언제 실행되었는지 확인 가능하다. -t 옵션을 사용하면 프로세스를 트리구조로 어떤 프로세스에서 실행되었는지 확인할 수 있다.



```
C:₩Tools₩PSTools>pslist

pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for 컴퓨터이름:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   8    0      0 1542:53:46.478   197:12:19.819
System                4   8 120 54809    308    0:41:14.846   197:12:19.819
smss                344  11   2   37    740    0:00:00.936   197:12:19.788
csrss               500  13  10  777   2804    0:00:38.033   197:12:18.041
csrss               644  13  14  710   5176    0:02:56.047   197:12:16.777
wininit             652  13   3   88   2184    0:00:00.202   197:12:16.762
services            708   9  10  272   7632    0:01:19.778   197:12:16.621
winlogon            732  13   3  118   4360    0:00:00.639   197:12:16.606
lsass               760   9   7  683   5708    0:04:34.717   197:12:16.512
lsm                 772   8  10  179   3564    0:00:26.020   197:12:16.496
svchost             864   8  13  414   7196    1:04:07.125   197:12:16.153
```

【 그림 Ⅱ.3.2 (14) 】 윈도우 프로세스 목록 정보 실행화면

나. UNIX / LINUX

• 프로세스 확인은 "ps -ef" 명령어를 통해 확인 할 수 있는데, process 실행자, PID, 실행일시, 프로세스명 등을 확인할 수 있다.

```
# ps -ef|more
UID    PID    PPID  C    STIME    TTY    TIME  CMD
root     1       0  0   May 22    ?      0:44/etc/init -r
root     2       0  0   May 22    ?      0:00pageout
root   339       1  0   May 22    ?      0:00/usr/openwin/bin/fbconsole -d :0
root    53       1  0   May 22    ?      0:00/usr/lib/devfsadm/devfseventd
root    57       1  0   May 22    ?      0:00/usr/lib/devfsadm/devfsadmd
root   138       1  0   May 22    ?      0:00/usr/sbin/keyserv
root   236       1  0   May 22    ?      0:00/usr/lib/power/powerd
root 25743       1  0    Jun 5    ?      0:03/usr/sbin/inetd -s
root   136       1  0   May 22    ?      0:07/usr/sbin/rpcbind
root   190       1  0   May 22    ?      0:00/usr/sbin/cron
root   176       1  0   May 22    ?      0:02/usr/lib/autofs/automountd
root   189       1  0   May 22    ?      0:04/usr/sbin/syslogd
root   204       1  0   May 22    ?      0:50/usr/sbin/nscd
root   296       1  0   May 22    ?      0:00/usr/dt/bin/dtlogin -daemon
root   297       1  0   May 22    ?      0:00/usr/lib/nfs/mountd
root   262       1  0   May 22    ?      0:00/usr/lib/sendmail -bd -q15m
root   316       1  0   May 22    ?      0:00/usr/lib/saf/sac -t 300
root   371       1  0   May 22    ?      0:00/usr/openwin/bin/speckeysd
root   299       1  0   May 22    ?      0:00/usr/lib/nfs/nfsd -a 16
root   337     305  0   May 22    ?      9:53mibiisa -r -p 32781
root   322     296  0   May 22    ?      0:00/usr/dt/bin/dtlogin -daemon
root   367     357  0   May 22    ?      0:00/usr/openwin/bin/fbconsole
root   390     357  0   May 22    ?      0:00/usr/openwin/bin/htt -nosm
root   433     431  0   May 22    ?      0:11dtwm
root   431     414  0   May 22    pts/2  0:45/usr/dt/bin/dtsession
```

【 그림 Ⅱ.3.2 (15) 】 유닉스 프로세스 목록 정보 실행화면

DL-12 비정상 포트 및 외부연결확인

○ 현재 열려있는 포트를 어떠한 응용 프로그램이 사용하는지에 대한 정보를 수집한다. 이는 피해시스템에서 특정 포트를 사용하는 백도어나 트로이목마를 찾기 위한 중요한 정보가 된다.

가. Windows

- “netstat -an” 명령어를 통해 프로토콜 상태, IP 기반 네트워크 연결 정보 등을 확인해서 현재 열려 있는 포트와 포트에 연결되어 있는 IP 정보를 확인해야 한다.

【 표 Ⅱ.3.2 (8) 】 네트워크 정보 확인 명령어

명령어	설명	다운로드
netstat -an	서비스 중인 포트 정보 및 연결된 아이피 정보	Windows

- 아래 명령어 수행결과에서 보면 시스템이 사용하지 않는 30451 포트가 LISTENING 상태로 열려 있는 것을 확인할 수 있다.

```
C:₩>netstat -an

활성 연결

  프로토콜  로컬 주소          외부 주소          상태
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3371           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:30451          0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            0.0.0.0:0              LISTENING
```

【 그림 Ⅱ.3.2 (16) 】 네트워크 정보 실행화면

- 아래의 도구를 사용하여 열려있는 포트의 정보를 수집한다.

【 표 Ⅱ.3.2 (9) 】 포트별 서비스 정보 확인 명령어

명령어	설명	다운로드
fport	서비스 중인 포트를 열고 있는 프로그램 정보	foundstone.com

- fport 명령어는 어떠한 응용 프로그램이 어떤 포트를 사용하는지에 대한 정보를 보여준다.

<참고설명>

/p : 포트별 정렬
/a : 응용프로그램 이름순 정렬
/l : 프로세스 ID 정렬
/ap : 응용 프로그램 디렉토리 순 정렬

```
C:₩>Fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process          Port  Proto  Path
436   svchost    ->    135   TCP    C:₩WINDOWS₩system32₩svchost.exe
8     System     ->    445   TCP
504   msdtc      ->    1025  TCP    C:₩WINDOWS₩system32₩msdtc.exe
732   MSTask     ->    1026  TCP    C:₩WINDOWS₩system32₩MSTask.exe
711   csrrs      ->    30451 TCP    C:₩WINDOWS₩system32₩csrrs.exe
```

【 그림 Ⅱ.3.2 (17) 】 fport 실행화면

나. UNIX / LINUX

- netstat는 현재 시스템의 네트워크 연결상태를 알려주는 명령어로 어떤 포트가 열려있는 지 발신지 주소는 어떻게 되는지 등을 확인할 수 있다.

```
# netstat -an | more
Active Internet connections (including servers)
Proto  Recv-Q  Send-Q  Local Address          Foreign Address        State
tcp        0       0 0.0.0.0:7777           0.0.0.0:*              LISTEN
tcp        0       0 0.0.0.0:8000           0.0.0.0:*              LISTEN
tcp        0       0 0.0.0.0:8817           0.0.0.0:*              LISTEN
tcp        0       0 0.0.0.0:21             0.0.0.0:*              LISTEN
tcp        0       0 0.0.0.0:22             0.0.0.0:*              LISTEN
tcp        0       0 0.0.0.0:80             0.0.0.0:*              LISTEN
tcp        0       0 0.0.0.0:8080           0.0.0.0:*              LISTEN
tcp        0       0 0.0.0.0:6000           0.0.0.0:*              LISTEN
```

【 그림 Ⅱ.3.2 (18) 】 네트워크 정보 실행화면

DL-13 취약한 프로그램의 최신버전 설치여부 확인

○ 자료훼손 및 유출 공격 별로 설치된 소프트웨어의 버전을 확인한다.

○ 아래의 방법은 대표적인 소프트웨어에 대한 버전 확인하는 방법이다.

① DaView 버전 확인 방법

- DaView프로그램을 실행하여 도움말을 이용하여 버전정보를 확인한다.

② OpenSSL 취약점 노출 여부 확인 방법

- 명령어를 통한 OpenSSL 버전 정보 확인

. openssl이 설치된 시스템에서 아래 명령어를 입력하여 취약점에 영향 받는버전을 사용하는지 확인

```
root@server:~# openssl version –a
OpenSSL 1.0.1 14 May 2012
```

【 그림 Ⅱ.3.2 (19) 】 openssl 버전확인 명령어 실행화면

3.2.4 재발방지

DL-14 보완조치 및 재발방지 조치

○ 사용하지 않는 계정과 숨겨진 계정 삭제

○ 외부 네트워크와 연결된 백도어 포트 발견 시 방화벽을 통해 해당포트로의 접근 제한 정책 적용

○ 백도어 포트 서비스를 실행중인 파일 확인 및 삭제

○ 그 외 공격자 흔적 제거

- 공격자의 모든 활동과 피해 흔적을 100% 분석한 경우는 이를 찾아서 복구하면 되나, 그렇지 않은 경우는 시스템 재설치

○ 비밀번호 교체

- 악성코드로 인해 비밀번호가 유출되었을 가능성이 있으므로 피해 시스템 뿐만 아니라 관련된 시스템의 비밀번호 교체 실시

○ 백업 복구

- 악성코드 피해 이후 파일이 변조되었을 가능성이 있으므로 감염 이전의 백업된 기록을 갖고 피해시스템을 복구

○ 취약점 제거 및 보안조치

- 침입의 원인이 된 취약점을 제거하고 악성코드 피해와 관련된 보안 패치를 포함하여 기존에 설치되지 않았던 모든 보안 패치를 설치

- 만약 보안패치가 없다면 취약점을 임시적으로 제거할 수 있는 수단을 강구해야 함

- 피해시스템의 안전한 운영을 위해 보안설정을 점검

DL-15 서비스 정상화

○ 시스템을 주기적으로 모니터링 하여 서비스 정상여부를 확인한다.

3.3 특이사항

☐ OpenSSL Heartbleed Vulnerability 대응방안

○ OpenSSL 하트비트(HeartBeat) 활성화 여부 확인

- 취약한 버전의 OpenSSL을 사용하는 시스템 중 HeartBeat 기능 사용 여부 확인 방법은 아래와 같다 (단, 패치된 최신 버전(1.0.1g)은 활성화 여부를 확인할 필요 없음)

```
root@server:~# openssl s_client –connect domain.com:443 –tlsextdebug –debug
–state | grep -i heartbeat
```

【 그림 Ⅱ.3.3 (1) 】 openssl HeartBeat 기능사용여부 확인 실행화면

※ 명령어 실행 방법 : domain.com에 점검 대상 URL 정보로 수정

- HeartBeat 기능이 활성화되어 있는 경우 heartbeat 문자열이 검색된다.

```
TLS server extension "heartbeat" (id=15), len=1
0000 - 01                                               .
read from 0x95cb888 [0x95d0e33] (5 bytes => 5 (0x5))
0000 - 16 03 02 0b cc                                   .....
read from 0x95cb888 [0x95d0e38] (3020 bytes => 3020 (0xBCC))
0000 - 0b 00 0b c8 00 0b c5 00-05 9d 30 82 05 99 30 82  ..........0...0.
0010 - 04 81 a0 03 02 01 02 02-08 11 bb ec db 00 00 39  ...............9
0020 - d0 30 0d 06 09 2a 86 48-86 f7 0d 01 01 05 05 00  .0...*.H........
0030 - 30 5e 31 0b 30 09 06 03-55 04 06 13 02 4b 52 31  0^1.0...U....KR1
0040 - 12 30 10 06 03 55 04 0a-0c 09 43 72 6f 73 73 43  .0...U....CrossC
```

【 그림 Ⅱ.3.3 (2) 】 openssl HeartBeat 문자열 검색된 화면

- HeartBeat 기능이 활성화되지 않은 경우 heartbeat 문자열이 검색되지 않는다.

```
TLS server extension "session ticket" (id=35), len=0
read from 0x9349888 [0x934ee33] (5 bytes => 5 (0x5))
0000 - 16 03 02 13 6f                                   ....o
read from 0x9349888 [0x934ee38] (4975 bytes => 4975 (0x136F))
```

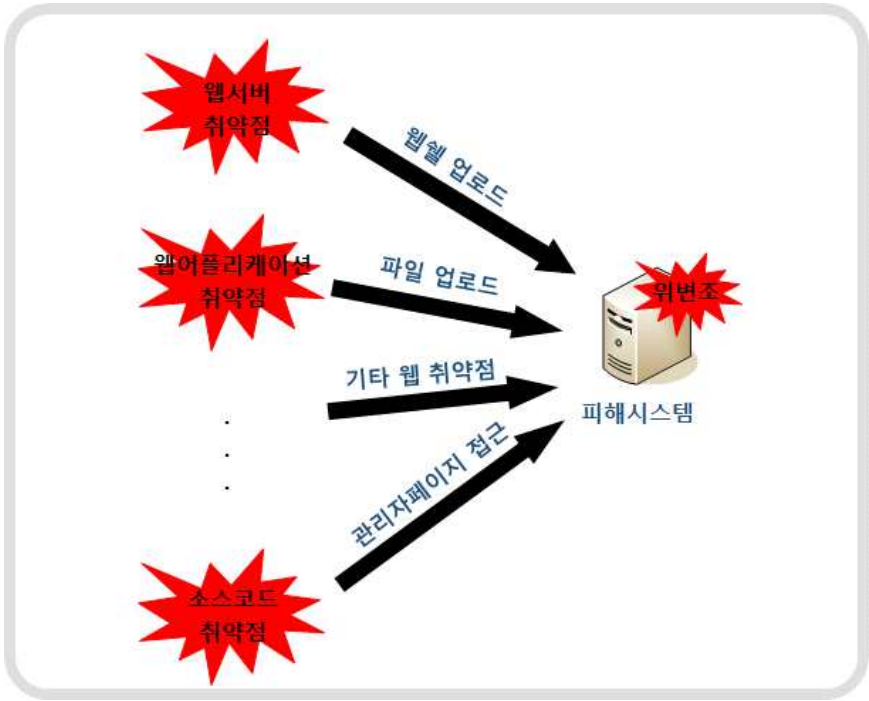
【 그림 Ⅱ.3.3 (2) 】 openssl HeartBeat 문자열 검색되지 않은 화면

4 홈페이지 위·변조

4.1 설명

□ 홈페이지 위·변조 피해란 시스템에 설치된 소프트웨어에 취약점을 이용하여 시스템에 정보를 절취·훼손하는 일체의 공격 행위로 인한 피해를 말한다.

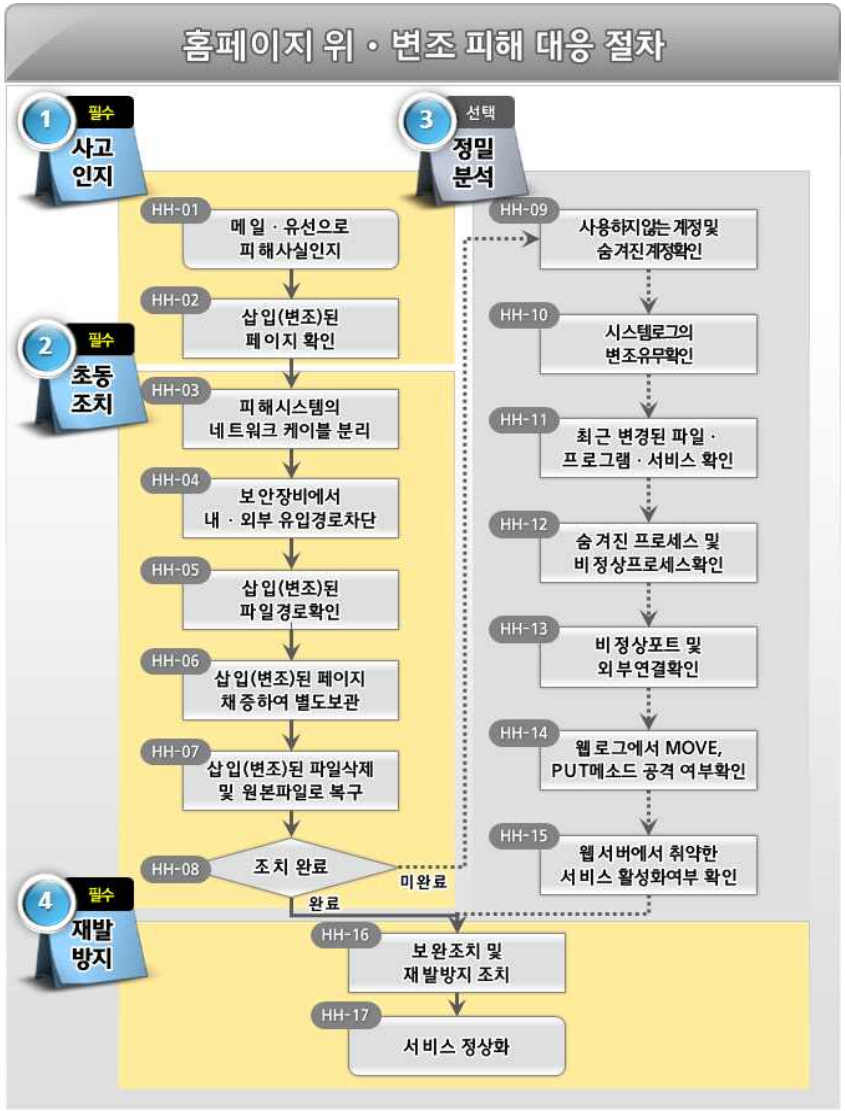
□ 자료훼손 및 유출 피해 개요도



【 그림 Ⅱ.4.1 (1) 】 홈페이지 위·변조 피해 개요도

4.2 대응요령

□ 홈페이지 위·변조 피해 대응요령은 사고인지, 초동조치, 재발방지의 필수절차와 정밀분석의 선택절차로 구성하여 운영한다.



【 그림 Ⅱ.4.2 (1) 】 홈페이지 위·변조 피해 대응절차

4.2.1 사고인지

HH-01 메일 또는 유선으로 피해사실 인지

○ 자체 사고 탐지 및 과학기술사이버안전센터(S&T-SEC), NCSC 등으로부터 이관된 메일(유선)을 통해 피해사실을 인지한다.

HH-02 삽입(변조)된 페이지확인

○ 자체 사고 탐지 및 메일(유선)로 통보된 홈페이지의 삽입(변조) 여부를 확인한다.

4.2.2 초동조치

HH-03 피해시스템의 네트워크 케이블 분리

○ 위·변조된 홈페이지가 식별되면 해당 홈페이지를 네트워크에서 격리하여 2차 확산을 방지한다.

※ 홈페이지가 이중화 되어 있거나 동일한 서비스가 가능한 시스템이 있을 경우 네트워크에서 격리하는 것을 권장하나, 그렇지 않을 경우 내부 검토 후 격리여부를 판단한다.

HH-04 보안장비에서 내·외부유입경로차단

○ 공격자IP를 침입차단시스템과 웹방화벽의 차단규칙을 이용하여 해당 연결 시도를 차단한다.

HH-05 삽입(변조)된 파일경로 확인

○ 피해시스템에 접속하여 홈페이지에 업로드 된 파일을 찾는다. 즉, 피해서버에 업로드 된 파일을 검색한다.

HH-06 삽입(변조)된 페이지 채증하여 별도보관

○ 삽입(변조)된 파일은 반드시 별도의 디렉토리에 보관하여 사고처리 종료 시 과학기술사이버안전센터(S&T-SEC)에 결과보고와 함께 채증한

파일을 첨부하여 발송한다.

HH-07 삽입(변조)된 파일삭제 및 원본파일로 복구

○ 삽입(변조)된 파일 삭제 후 최근 백업한 원본파일로 복구한다.

HH-08 조치 완료

○ 원본파일로 복구 후 서비스 여부를 확인한다.

4.2.3 정밀분석

HH-09 사용하지 않는 계정 및 숨겨진 계정 확인

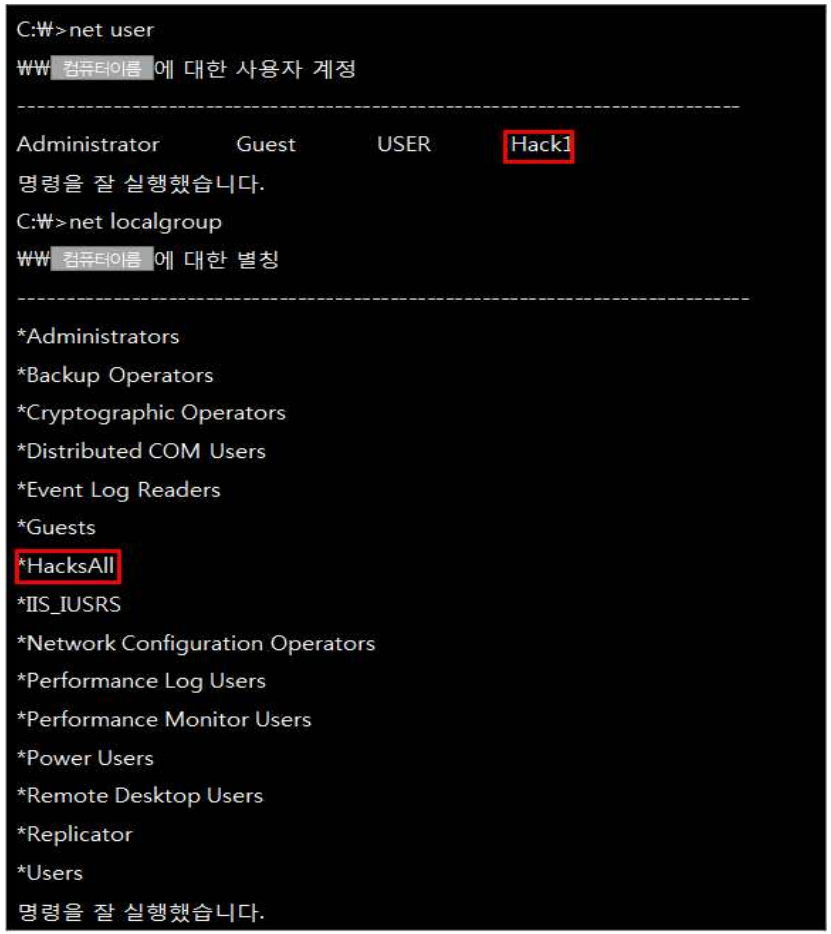
○ 불법적으로 등록된 사용자나 권한이 상승된 계정 및 그룹이 없는지 아래와 같은 방법으로 확인한다.

가. Windows

【 표 Ⅱ.4.2 (1) 】 Windows 사용자·그룹 정보 확인 명령어

명령어	설명	다운로드
net user	시스템에 존재하는 계정정보 출력	Windows
net localgroup	시스템에 존재하는 그룹정보 출력	Windows

- 아래 그림은 위의 명령어 실행을 통해 시스템의 계정정보 명령어를 실행한 화면이다.



【 그림 Ⅱ.4.2 (2) 】 Windows 시스템 계정정보 명령어 실행화면

- Hack1이란 불법계정이 생성되어있으며, HacksAll이란 불법그룹이 생성되어 있음을 알 수 있다. 그리고 내장된 guest 계정이 '사용 안함' 으로 되어 있는지 점검한다.

나. UNIX / LINUX

【 표 Ⅱ.4.2 (2) 】 UNIX 사용자・그룹 정보 확인 명령어

명령어	설명	다운로드
cat /etc/passwd	시스템에 존재하는 계정정보 출력	Unix/Linux

- /etc/passwd파일에서 UID=0인 계정은 root만이 가지고 있으므로 일반 계정에서 uid=0인 계정의 존재여부를 반드시 확인해야 한다.
- 아래 내용은 /etc/passwd파일의 내부 파일의 일부 화면과 설명이다.

```
root:x:0:0:root:/root:/bin/bash
user1:x:0:0::/home/user1:/bin/bash
```

【 그림 Ⅱ.4.2 (3) 】 /etc/passwd파일 내부화면

- user1이란 불법계정의 UID=0인 것을 확인할 수 있다.
- /etc/passwd파일의 구조는 아래와 같다.

【 표 Ⅱ.4.2 (3) 】 /etc/passwd파일 구조

root	:x	:0	:0	:root	:/root	:/bin/bash
❶	❷	❸	❹	❺	❻	❼

<참고설명>

❶ : 사용자 계정 이름(대부분 ID라고 부른다)
❷ : 사용자 비밀번호(x로 되어 있는 것은 섀도우 패스워드 시스템에 의해 /etc/shadow에 암호화된 형태로 저장 되어있음)
❸ : 사용자 UID(모든 정보는 수치 값으로 저장 되어 있음 root -> 0(UID))
❹ : 사용자 소속 그룹 GID(모든 정보는 수치 값으로 저장 되어 있음 root -> (GID))
❺ : 사용자 정보(계정이름)
❻ : 사용자 계정 디렉터리(계정 홈 디렉터리)
❼ : 사용자 로그인 쉘 (리눅스 : bash Shell, 유닉스 : Korn Shell 등등)

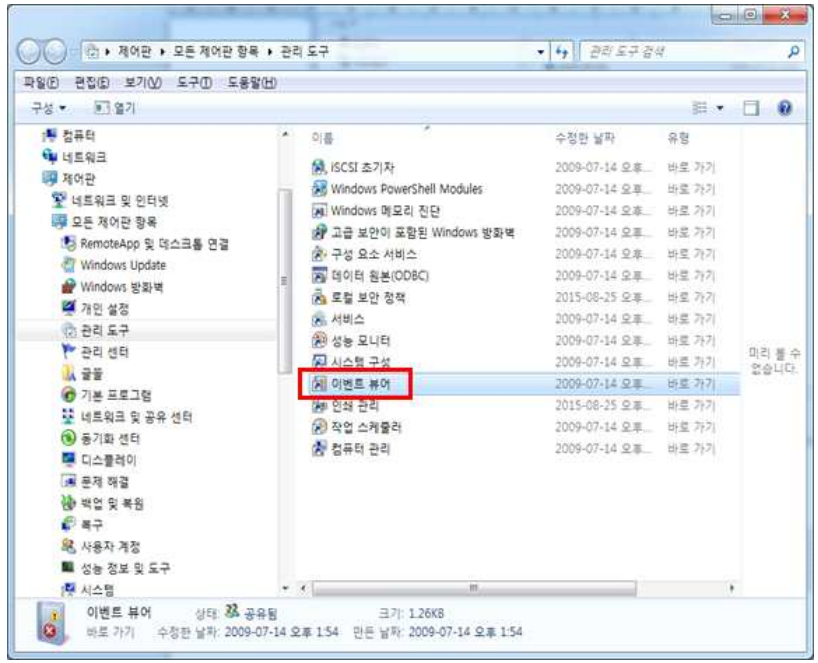
HH-10 시스템 로그의 변조 유무 확인

○ 시스템을 비인가된 방법으로 접근한 공격자들은 시스템에 흔적을 남기게 된다. 이러한 흔적 및 활동 정보를 찾아내기 위해서는 로그 분석이 필요하다.

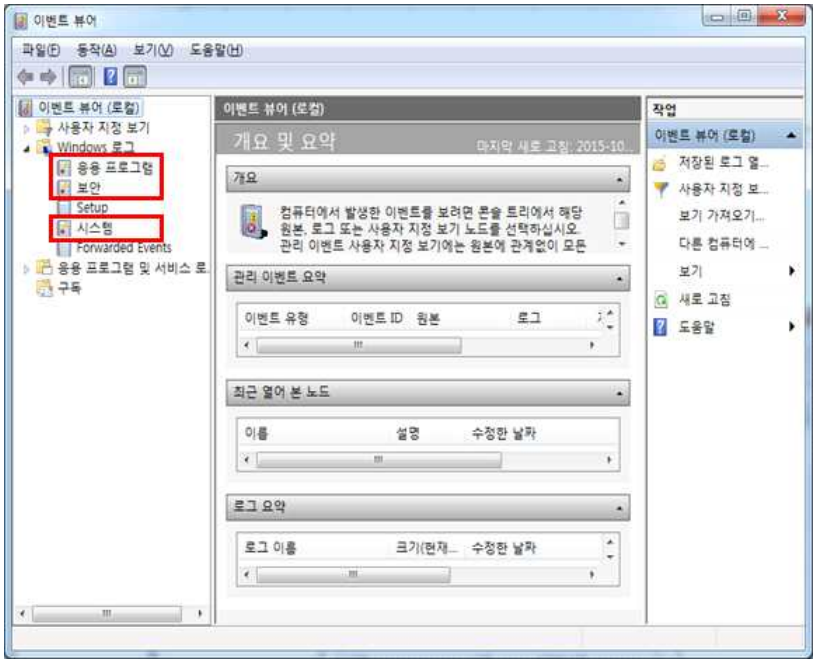
가. Windows

1) 이벤트뷰어

- 윈도우 시스템에서는 하드웨어, 소프트웨어 및 시스템 문제를 이벤트 로그에 저장하므로 이벤트 뷰어 실행을 통해 확인이 필요하다.
- 위치 : 제어판➜관리도구➜컴퓨터관리➜이벤트 뷰어



【 그림 Ⅱ.4.2 (4) 】 Windows 이벤트 뷰어 경로화면



【 그림 Ⅱ.4.2 (5) 】 Windows 이벤트 뷰어 실행화면

• 아래의 표를 참고하여 이벤트 로그ID로 공격과 관련된 이벤트를 분석한다.

【 표 Ⅱ.4.2 (4) 】 특징별 이벤트 로그

특징	이벤트 설명	이벤트 ID
로컬 로그온 시도 실패	사용자 이름과 패스워드를 조합하여 로그온 시도 했을 때 생성되는 이벤트	529, 530, 531, 532, 533, 534, 537
계정의 잘못된 사용	입력된 사용자 계정/패스워드에는 문제가 없지만 다른 제한에 의해 로그온 실패 시 생성되는 이벤트	530, 531, 532, 533
계정 잠김	계정 잠금 정책에 의해 사용자 계정이 잠겼을 때 발생하는 이벤트	539
터미널 서비스 공격	터미널 서비스 연결 후 완전히 세션을 종료하지 않았거나 다시연결 했을 때 이벤트 발생	683, 682
사용자 계정 생성	사용자 계정이 만들어진 시간과 활성화된 시간으로 공격자에 의한 사용자 계정 생성 인지를 확인	624, 626
사용자 계정 패스워드	사용자 이외의 계정에 의해 패스워드가 변경되었을 경우 공격자에 의해 해당 사용자 계정이 탈취당한 경우	627, 628

나. UNIX / LINUX

1) secure파일

• secure파일은 보안과 관련된 중요한 로그를 남기며, 사용자 인증 관련된 로그를 포함하고 있다.

• secure파일은 syslog데몬에 의해 남겨지는데, 텍스트 형태의 파일이므로 cat등을 이용하여 확인할 수 있다.

```
# cat /var/log/secure
Nov 28 16:37:11 insecure in.telnetd[6317] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.ftpd[4258] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.rlogind[4168] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.rshd[6328] : conncet from 192.168.10.17
Nov 28 16:40:35 insecure login: LOGIN ON 1 BY Hack1 FROM Hack1
```

【 그림 Ⅱ.4.2 (6) 】 secure파일 열람화면

• 위의 그림에서 "Nov 28 16:37:11"에 192.168.10.17로부터 telnet, ftp, rlogin, rsh 등에 대한 접속시도가 있었음을 알 수 있다. 일반적으로 한 사용자가 짧은 시간에 이들 서비스 요청을 수동으로 할 수는 없으므로, 이 로그를 통해 192.168.10.17로부터 단순침입시도 공격이 있었음을 알 수 있다.

2) messages파일

• 시스템 에러, 재부팅 메시지, 로그인 실패 등의 많은 정보를 포함하고 있는 로그파일로써, 시스템 관리자가 시스템 장애 원인 또는 공격으로부터 남는 흔적을 찾아내기 위해서도 messages 파일을 점검한다.

```
# more /var/log/messages
Nov  12 13:44:12 msd1 su: 'su root' failed for aster on /dev/pts/1
Nov  12 14:22:30 msd1 rsh[10103]: connection from bad port
Nov  12 14:28:15 msd1 su: 'su root' failed for aster on /dev/pts/2
Nov  12 14:29:41 msd1 last message repeated 1 time
Nov  12 15:39:29 msd1 su: 'su root' failed for aster on /dev/pts/1
Nov  12 15:57:52 msd1 syslogd: going down on signal 15
```

【 그림 Ⅱ.4.2 (7) 】 messages파일 열람화면

<참고설명>

- 'root'권한으로의 불법적인 로그인 시도가 있었는지를 살펴본다.
- 'su'명령을 이용한'root'또는 특정 권한의 사용자로의 의심스러운 전환 시도가 있었는지를 살펴본다.
- 유효한 사용자로부터의 반복적인 실패한 로그인 시도가 있었는지를 살펴본다.

HH-11 최근 변경된 파일 · 프로그램 · 서비스 확인

○ 공격자들은 공격 성공 후 악성 파일 및 프로그램들을 레지스트리 뿐만 아니라, 서비스, 스케줄러 등에 등록해 놓기 때문에, 이러한 부분을 반드시 점검 하여야 한다.

가. Windows

1) MAC TIME 분석

- 일반적인 파일시스템은 디렉터리나 파일과 관련된 아래와 같은 시간 속성을 갖는다.

<참고설명>

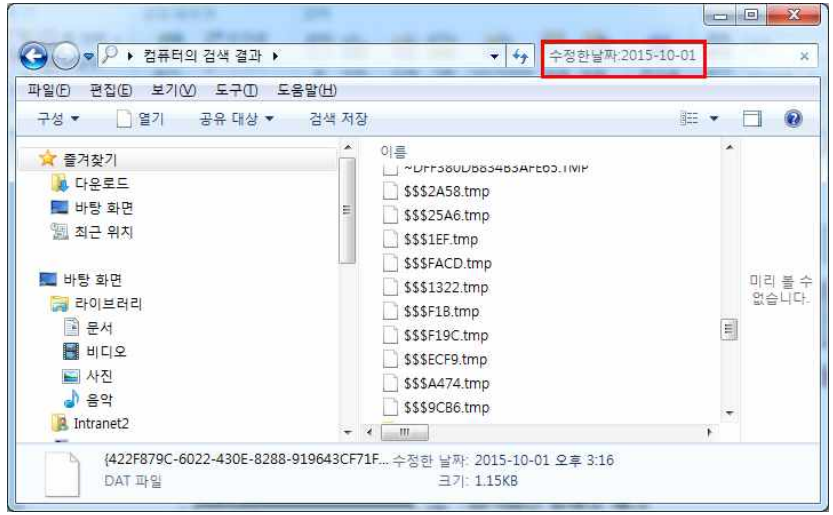
- MTIME : 파일을 생성 및 최근 수정한 시간
- ATIME : 최근 파일을 읽거나 실행시킨 시간
- CTIME : 파일 속성이 변경된 시간

- 이러한 시간 정보를 MAC time 이라 하며 분석을 통해 공격자가 파일 시스템에서 어떠한 행동을 했는지에 대해 판단 할 수 있는 정보를 제공한다.

<참고설명>

- 감염시점으로 MTIME, ATIME 검색
- 검출된 악성코드 MTIME, ATIME 검색

- 위치 : 시작-검색-파일 및 폴더-검색옵션-날짜



【 그림 Ⅱ.4.2 (8) 】 윈도우즈 MAC TIME으로 검색

<참고설명>

- 검색옵션은 날짜로 체크
- 찾고자 하는 MAC TIME 지정
  - 수정된 파일(MTIME)
  - 마지막으로 엑세스한 파일(ATIME)
  - 만든파일(CTIME)

- 감염 날짜를 기준으로 "마지막 엑세스 파일" 을 검사하게 되면 감염 후 실행됐던 파일들을 검색할 수 있다.

2) 설치 프로그램 점검

- 사고분석을 위해서는 피해시스템의 기본적인 정보가 필요하다. psinfo는 OS의 기본정보 및 보안 업데이트 정보 등을 제공하며 설치된 소프트웨어 정보 또한 알려준다. 이러한 보안 업데이트 정보는 시스템 취약점을 통해 어떻게 공격했는지에 대한 정보를 얻을 수 있기 때문에 최종 업데이트 날짜를 확인해야 한다.

【 표 Ⅱ.4.2 (5) 】 시스템 정보 확인 명령어

명령어	설명	다운로드
psinfo -h -s	설치된 핫픽스 및 소프트웨어 목록 정보	sysinternals

- 아래의 그림은 핫픽스 및 소프트웨어 목록을 확인한 화면이다.

```
C:₩Tools₩PSTools>psinfo -h -s

PsInfo v1.77 - Local and remote system information viewer
Copyright (C) 2001-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for ₩₩ 컴퓨터이름:
Uptime:                 7 days 8 hours 56 minutes 19 seconds
Kernel version:         Windows 7 Professional, Multiprocessor Free
Product type:           Professional
Product version:        6.1
Service pack:           0
Kernel build number:    7601
Registered organization:
Registered owner:       ????4
IE version:             9.0000
System root:            C:₩Windows
Processors:             8
Processor speed:        3.9 GHz
Processor type:         Intel(R) Core(TM) i7-4790K CPU @
Physical memory:        2616 MB
Video driver:           NVIDIA GeForce GTX 960

Installed     HotFix
n/a           Internet Explorer - 0
Applications:
Adobe Flash Player 18 ActiveX 18.0.0.232
Adobe Reader X (10.1.15) MUI 10.1.15
AhnLab Policy Agent 4.6 4.6
```

【 그림 Ⅱ.4.2 (9) 】 핫픽스 및 소프트웨어 목록 확인 명령어 실행화면

3) 서비스 점검

- 현재 윈도우에서 실행되고 있는 서비스 정보를 수집한다. 제어판의 서비스메뉴에서 설정할 수 있다. 대다수의 불법 서비스 항목은 윈도우 기본 서비스 이름과 유사한 이름을 사용하기 때문에 분석자는 윈도우 기본 서비스 항목과 불법 프로세스를 명확히 구분할 수 있어야 한다.

【 표 Ⅱ.4.2 (6) 】 서비스 정보 확인 명령어

명령어	설명	다운로드
net start	동작중인 서비스의 목록정보	Windows

- 아래의 그림은 동작중인 서비스 목록을 확인한 화면이다.

```
C:₩>net start
다음과 같은 Windows 서비스가 시작되었습니다.

   Adobe Acrobat Update Service
   AhnLab V3 Service
   ASUS Com Service
   Background Intelligent Transfer Service
   Base Filtering Engine
   CNG Key Isolation
   COM+ Event System
   Cryptographic Services
   DCOM Server Process Launcher
   Desktop Window Manager Session Manager
   DHCP Client
   Diagnostic Policy Service
   Diagnostic Service Host
   Diagnostics Tracking Service
   Distributed Link Tracking Client
   DNS Client
   Function Discovery Provider Host
   Group Policy Client
   Human Interface Device Access
   IKE and AuthIP IPsec Keying Modules
   Intel(R) Content Protection HECI Service
   Intel(R) HD Graphics Control Panel Service
   Intel(R) PROSet Monitoring Service
   IP Helper
```

【 그림 Ⅱ.4.2 (10) 】 서비스 목록 확인 명령어 실행화면

나. UNIX / LINUX

1) MAC TIME 분석

• 최근에 수정되거나 새롭게 생성된 파일을 찾는 명령어로 공격자가 시스템 파일의 변조를 숨기기 위해 시간을 수정하는 경우가 있으므로 이러한 경우에 대비하여 inode 변경시간을 점검한다.

• 아래의 그림은 최근 10일 동안 수정되거나 생성된 파일을 찾아서 파일로 저장하는 화면이다.

```
#find / -ctime -10 -print -xdev >/var/cime_10.txt
```

【 그림 Ⅱ.4.2 (11) 】 최근 10일 동안 수정 및 생성된 파일을 저장하는 화면

2) 설치 프로그램 점검

• setuid를 가지는 실행 프로그램은 실행도중에 슈퍼유저(root)의 권한을 가지고 실행되므로 find를 이용하여 setuid나 setgid 파일이 있는지 확인한다.

```
#find / -user root -perm -4000 -print>setuid.txt
#find / -user root -perm -2000 -print>setgid.txt
```

【 그림 Ⅱ.4.2 (12) 】 root권한을 가지고 실행하는 파일을 저장하는 화면

WO-12 숨겨진 프로세스 및 비정상 프로세스 확인

○ 일반적인 시스템들은 많은 실행 프로세스들을 가지고 있으며, 이러한 프로세스 중에는 공격자가 실행시켜놓은 프로세스가 실행되고 있거나 흔적이 남아 있을 수 있으니 자세히 확인해 볼 필요가 있다.

가. Windows

• 윈도우에서 프로세스를 점검할 수 있는 도구로는 pslist가 있다. 이 도구는 sysinternals에서 제공하며, 현재 구동 중인 프로세스 목록을 출력해준다.

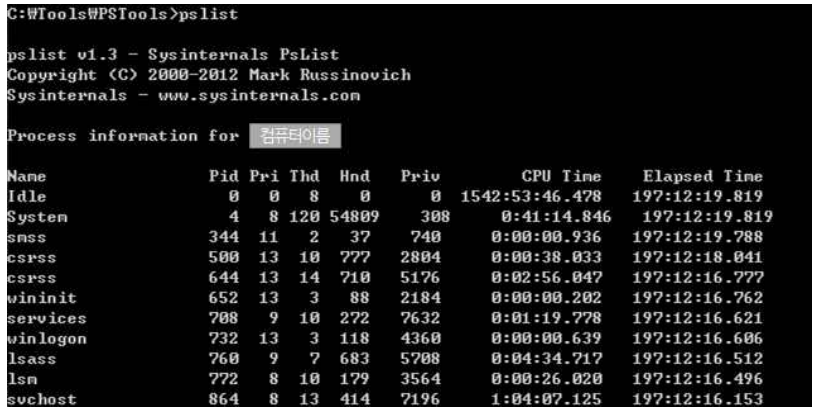
【 표 Ⅱ.4.2 (7) 】 프로세스 정보 확인 명령어

명령어	설명	다운로드
pslist	현재 프로세스 리스트 출력	sysinternals

• 프로세스 정보 확인시 주의해서 보아야 할 정보는 아래와 같다

<참고설명>

- 실행 프로세스명
- 프로세스 실행파일 위치
- 프로세스 커맨드 라인
- 프로세스 실행시간
- 프로세스가 참조중인 DLL 및 파일
- pslist : 현재 구동중인 프로세스 목록을 출력해 준다. 옵션을 하지 않으면 프로세스가 실행된 시간을 자세히 확인할 수 있는데 이러한 시간은 또 한 uptime에서 확인했던 부팅시간 이후에 악성프로그램이 언제 실행되었는지 확인 가능하다. -t 옵션을 사용하면 프로세스를 트리구조로 어떤 프로세스에서 실행되었는지 확인할 수 있다.



```
C:₩Tools₩PSTools>pslist

pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for 컴퓨터이름

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   8    0      0 1542:53:46.478   197:12:19.819
System                4   8 120 54809    308    0:41:14.846   197:12:19.819
smss                344  11   2   37    740    0:00:00.936   197:12:19.788
csrss               500  13  10  777   2804    0:00:38.033   197:12:18.041
csrss               644  13  14  710   5176    0:02:56.047   197:12:16.777
wininit             652  13   3   88   2184    0:00:00.202   197:12:16.762
services            708   9  10  272   7632    0:01:19.778   197:12:16.621
winlogon            732  13   3  118   4360    0:00:00.639   197:12:16.606
lsass               760   9   7  683   5708    0:04:34.717   197:12:16.512
lsm                 772   8  10  179   3564    0:00:26.020   197:12:16.496
svchost             864   8  13  414   7196    1:04:07.125   197:12:16.153
```

【 그림 Ⅱ.4.2 (13) 】 윈도우 프로세스 목록 정보 실행화면

나. UNIX / LINUX

- 프로세스 확인은 "ps -ef" 명령어를 통해 확인 할 수 있는데, process 실행자, PID, 실행일시, 프로세스명 등을 확인할 수 있다.

```
# ps -ef|more
UID    PID    PPID  C     STIME   TTY    TIME  CMD
root     1       0  0   May 22   ?        0:44/etc/init -r
root     2       0  0   May 22   ?        0:00pageout
root   339       1  0   May 22   ?        0:00/usr/openwin/bin/fbconsole -d :0
root    53       1  0   May 22   ?        0:00/usr/lib/devfsadm/devfseventd
root    57       1  0   May 22   ?        0:00/usr/lib/devfsadm/devfsadmd
root   138       1  0   May 22   ?        0:00/usr/sbin/keyserv
root   236       1  0   May 22   ?        0:00/usr/lib/power/powerd
root 25743       1  0    Jun 5   ?        0:03/usr/sbin/inetd -s
root   136       1  0   May 22   ?        0:07/usr/sbin/rpcbind
root   190       1  0   May 22   ?        0:00/usr/sbin/cron
root   176       1  0   May 22   ?        0:02/usr/lib/autofs/automountd
root   189       1  0   May 22   ?        0:04/usr/sbin/syslogd
root   204       1  0   May 22   ?        0:50/usr/sbin/nscd
root   296       1  0   May 22   ?        0:00/usr/dt/bin/dtlogin -daemon
root   297       1  0   May 22   ?        0:00/usr/lib/nfs/mountd
root   262       1  0   May 22   ?        0:00/usr/lib/sendmail -bd -q15m
root   316       1  0   May 22   ?        0:00/usr/lib/saf/sac  -t 300
root   371       1  0   May 22   ?        0:00/usr/openwin/bin/speckeysd
root   299       1  0   May 22   ?        0:00/usr/lib/nfs/nfsd  -a 16
root   337     305  0   May 22   ?        9:53mibiisa -r -p 32781
root   322     296  0   May 22   ?        0:00/usr/dt/bin/dtlogin -daemon
root   367     357  0   May 22   ?        0:00/usr/openwin/bin/fbconsole
root   390     357  0   May 22   ?        0:00/usr/openwin/bin/htt -nosm
root   433     431  0   May 22   ?        0:11dtwm
root   431     414  0   May 22   pts/2    0:45/usr/dt/bin/dtsession
```

【 그림 Ⅱ.4.2 (14) 】 유닉스 프로세스 목록 정보 실행화면

HH-13 비정상 포트 및 외부연결확인

○ 현재 열려있는 포트를 어떠한 응용 프로그램이 사용하는지에 대한 정보를 수집한다. 이는 피해시스템에서 특정 포트를 사용하는 백도어나 트로이목마를 찾기 위한 중요한 정보가 된다.

가. Windows

- "netstat -an" 명령어를 통해 프로토콜 상태, IP 기반 네트워크 연결 정보 등을 확인해서 현재 열려 있는 포트와 포트에 연결되어 있는 IP 정보를 확인해야 한다.

【 표 Ⅱ.4.2 (8) 】 네트워크 정보 확인 명령어

명령어	설명	다운로드
netstat -an	서비스 중인 포트 정보 및 연결된 아이피 정보	Windows

- 아래 명령어 수행결과에서 보면 시스템이 사용하지 않는 30451 포트가 LISTENING 상태로 열려 있는 것을 확인할 수 있다.

```
C:₩>netstat -an

활성 연결

프로토콜  로컬 주소          외부 주소          상태
TCP     0.0.0.0:135        0.0.0.0:0          LISTENING
TCP     0.0.0.0:445        0.0.0.0:0          LISTENING
TCP     0.0.0.0:1026       0.0.0.0:0          LISTENING
TCP     0.0.0.0:1027       0.0.0.0:0          LISTENING
TCP     0.0.0.0:1028       0.0.0.0:0          LISTENING
TCP     0.0.0.0:3371       0.0.0.0:0          LISTENING
TCP     0.0.0.0:30451      0.0.0.0:0          LISTENING
UDP     0.0.0.0:445        0.0.0.0:0          LISTENING
```

【 그림 Ⅱ.4.2 (15) 】 네트워크 정보 실행화면

- 아래의 도구를 사용하여 열려있는 포트의 정보를 수집한다.

【 표 Ⅱ.4.2 (9) 】 포트별 서비스 정보 확인 명령어

명령어	설명	다운로드
fport	서비스 중인 포트를 열고 있는 프로그램 정보	foundstone.com

• fport 명령어는 어떠한 응용 프로그램이 어떤 포트를 사용하는지에 대한 정보를 보여준다.

<참고설명>
/p : 포트별 정렬
/a : 응용프로그램 이름순 정렬
/l : 프로세스 ID 정렬
/ap : 응용 프로그램 디렉토리 순 정렬

```
C:₩>Fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process          Port  Proto  Path
436   svchost    ->    135   TCP    C:₩WINDOWS₩system32₩svchost.exe
8     System     ->    445   TCP
504   msdtc      ->    1025  TCP    C:₩WINDOWS₩system32₩msdtc.exe
732   MSTask     ->    1026  TCP    C:₩WINDOWS₩system32₩MSTask.exe
711   csrrs      ->    30451 TCP    C:₩WINDOWS₩system32₩csrrs.exe
```

【 그림 Ⅱ.4.2 (16) 】 fport 실행화면

나. UNIX / LINUX

• netstat는 현재 시스템의 네트워크 연결상태를 알려주는 명령어로 어떤 포트가 열려있는 지 발신지 주소는 어떻게 되는지 등을 확인할 수 있다.

```
# netstat -an | more
Active Internet connections (including servers)
Proto  Recv-Q  Send-Q  Local Address      Foreign Address    State
tcp        0       0  0.0.0.0:7777       0.0.0.0:*          LISTEN
tcp        0       0  0.0.0.0:8000       0.0.0.0:*          LISTEN
tcp        0       0  0.0.0.0:8817       0.0.0.0:*          LISTEN
tcp        0       0  0.0.0.0:21         0.0.0.0:*          LISTEN
tcp        0       0  0.0.0.0:22         0.0.0.0:*          LISTEN
tcp        0       0  0.0.0.0:80         0.0.0.0:*          LISTEN
tcp        0       0  0.0.0.0:8080       0.0.0.0:*          LISTEN
tcp        0       0  0.0.0.0:6000       0.0.0.0:*          LISTEN
```

【 그림 Ⅱ.4.2 (17) 】 네트워크 정보 실행화면

HH-14 웹로그에서 MOVE, PUT메소드 공격 여부확인

○ 공격자는 취약점을 이용하여 악성파일 또는 공격자의 소스 코드를 업로드 하게 되는데. 이러한 경우 웹-로그에 아래와 같은 내용이 기록된다.

```
2015-10-26  23:59:48  88.229.138.31  201  PUT  210.104.140.167 80 /paro.htm
```

【 그림 Ⅱ.4.2 (18) 】 웹로그 PUT 메소드 성공화면

○ 여기에서 주의해서 보아야 할 점은 Method부분과, 상태코드 부분이다. 공격자는 PUT Method를 이용하여 paro.htm 파일을 업로드 시켰으며, 상태코드는 201로 업로드는 성공한 것으로 나타난다.

○ 하지만, 상태코드가 성공한 것으로 나타난다 하더라도, 성공여부는 반드시 웹 브라우져를 이용하여, 확인하고, 실제 서버에 해당 파일이 존재하는지 여부를 확인해야 한다.

○ 보안이 고려되어 잘 개발된 홈페이지에서는 오류 발생시 오류페이지로 Redirect 시킴으로 인해 로그상에는 200으로 남아있는 경우가 있다.

○ 웹 브라우저를 통해 확인한 결과 paro.htm 파일이 업로드 되어 있다면, PUT Method를 이용한 파일 업로드 공격이 성공한 것이다.

HH-15 웹서버에서 취약한 서비스 활성화여부확인

○ 윈도우 IIS 또는 Apache에서 WebDAV가 활성화 되어 있다면, 원격에서 파일 업로드가 가능하므로 서비스 활성화 여부를 확인한다.

4.2.4 재발방지

HH-16 보완조치 및 재발방지 조치

○ 윈도우 IIS 웹서버의 WebDAV가 활성화 되어 있을 경우 사용 중지

○ 리눅스 아파치 웹서버의 설정파일에서 사용하지 않는 HTTP 메소드에 대해 허용 금지

○ IIS 웹서버 또는 아파치 웹서버의 설정이 변경되었을 경우 관리자계정 변경 필수

○ 웹페이지 내용이 변경되었을 경우 휘슬을 통해 웹쉘 감염여부를 확인하고 발견될 경우 삭제 조치

○ 웹쉘이 발견될 경우 웹 접속로그를 통해 웹쉘에 접근한 IP를 확인하고 방화벽을 통해 접근 제한 정책 적용

○ 사용하지 않는 계정과 숨겨진 계정 삭제

○ 그 외 공격자 흔적 제거

- 공격자의 모든 활동과 피해 흔적을 100% 분석한 경우는 이를 찾아서 복구하면 되나, 그렇지 않은 경우는 시스템 재설치

○ 비밀번호 교체

- 홈페이지 위·변조 피해로 인해 비밀번호가 유출되었을 가능성이 있으므로 피해 시스템 뿐만 아니라 관련된 시스템의 비밀번호 교체 실시

○ 백업 복구

- 홈페이지 위·변조 피해 이후 파일이 변조되었을 가능성이 있으므로 감염 이전의 백업된 기록을 갖고 피해시스템을 복구

○ 취약점 제거 및 보안조치

- 침입의 원인이 된 취약점을 제거하고 웜·바이러스 공격과 관련된 보안패치를 포함하여 기존에 설치되지 않았던 모든 보안 패치를 설치

- 만약 보안패치가 없다면 취약점을 임시적으로 제거할 수 있는 수단을 강구해야 함

- 피해시스템의 안전한 운영을 위해 보안설정을 점검

HH-17 서비스 정상화

○ 시스템을 주기적으로 모니터링 하여 서비스 정상여부를 확인한다.

4.3 특이사항

□ 웹쉘 대응방안

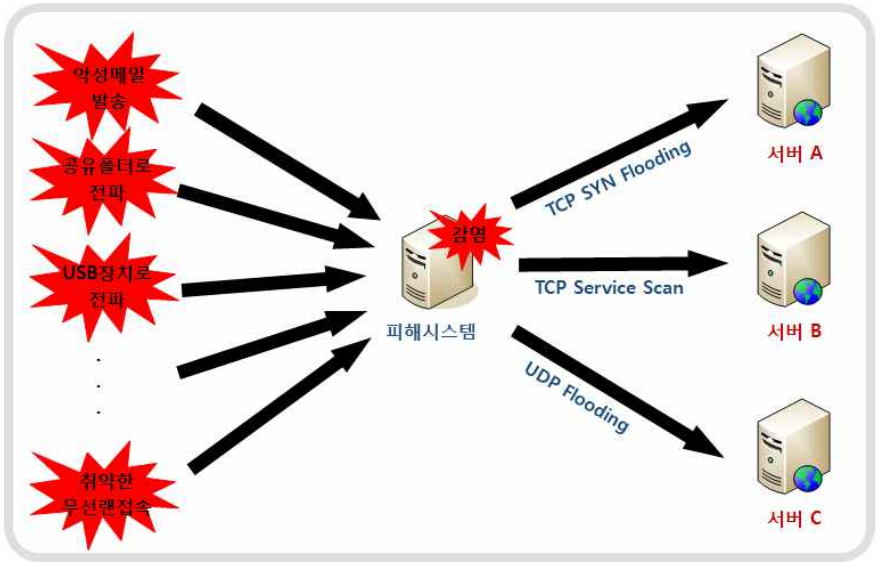
○ 파일 업로드가 불필요한 게시판의 경우는 업로드의 기능을 완전히 제거하고 필요한 경우에는 파일의 확장자를 체크한다. 확장자를 체크하는 루틴은 javascript 같이 html 파일 내에 포함되어서는 안되고 반드시 서버 사이드에서 실행되는 CGI 파일 등에 존재해야 한다.

5 경유지 악용

5.1 설명

□ 경유지 악용 피해란 컴퓨터 바이러스, 웜 등이 사용자의 동의 없이 컴퓨터에 설치되어 사용자의 정보가 탈취되거나 컴퓨터를 오동작 하고 네트워크를 마비시킬 수 있는 악의적인 행위를 당하는 피해를 말한다.

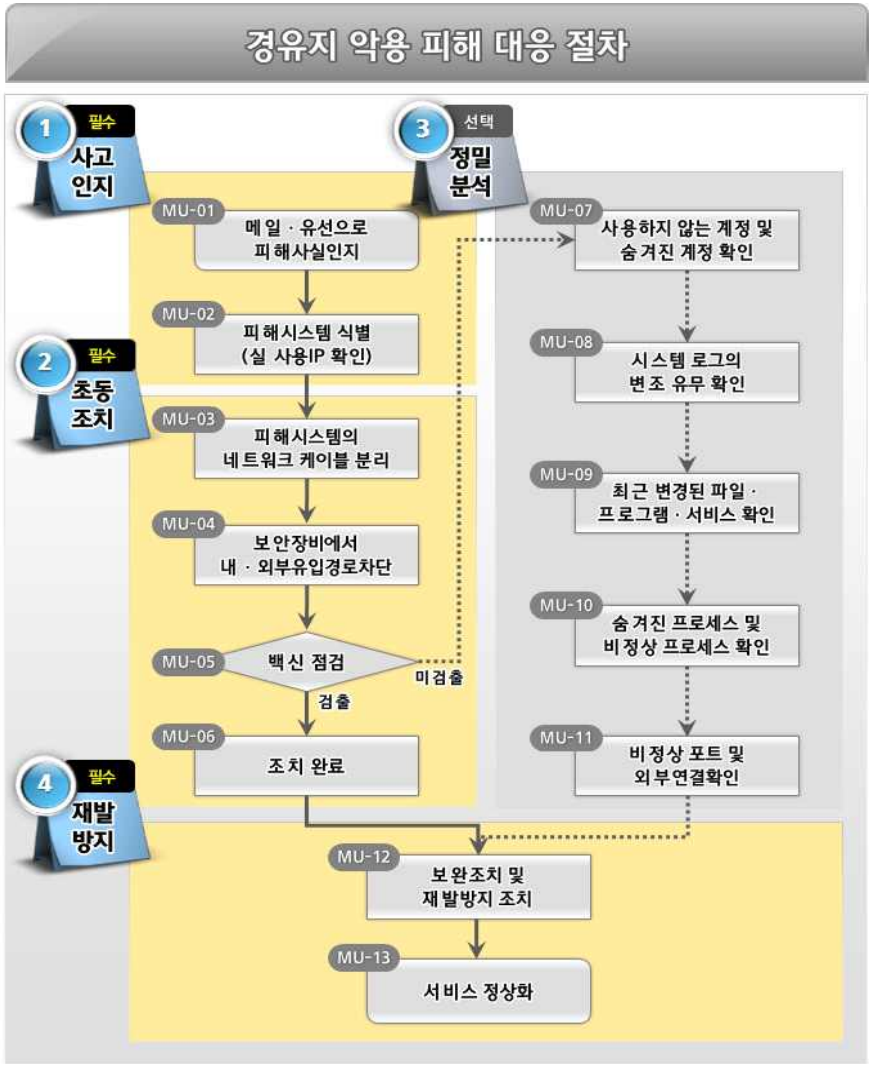
□ 경유지 악용 피해 개요도



【 그림 Ⅱ.5.1 (1) 】 경유지 악용 피해 개요도

5.2 대응요령

□ 경유지 악용 피해 대응요령은 사고인지, 초동조치, 재발방지의 필수절차와 정밀분석의 선택절차로 구성하여 운영한다.



【 그림 Ⅱ.5.2 (1) 】 경유지 악용 피해 대응절차

5.2.1 사고인지

MU-01 메일 또는 유선으로 피해사실 인지

○ 자체 사고 탐지 및 과학기술사이버안전센터(S&T-SEC), NCSC 등으로부터 이관된 메일(유선)을 통해 피해사실을 인지한다.

MU-02 피해시스템 식별 (실 사용IP 확인)

○ 자체 사고 탐지 및 메일(유선)로 통보된 피해시스템 IP주소를 네트워크 장비 또는 방화벽 확인 등을 통해 실제 사용하는 IP주소를 확인하여 감염된 시스템을 식별한다.

5.2.2 초동조치

MU-03 피해시스템의 네트워크 케이블 분리

○ 감염된 호스트가 식별되면 해당 호스트를 네트워크에서 격리하여 2차 감염 확산을 방지한다.

MU-04 보안장비에서 내 · 외부유입경로차단

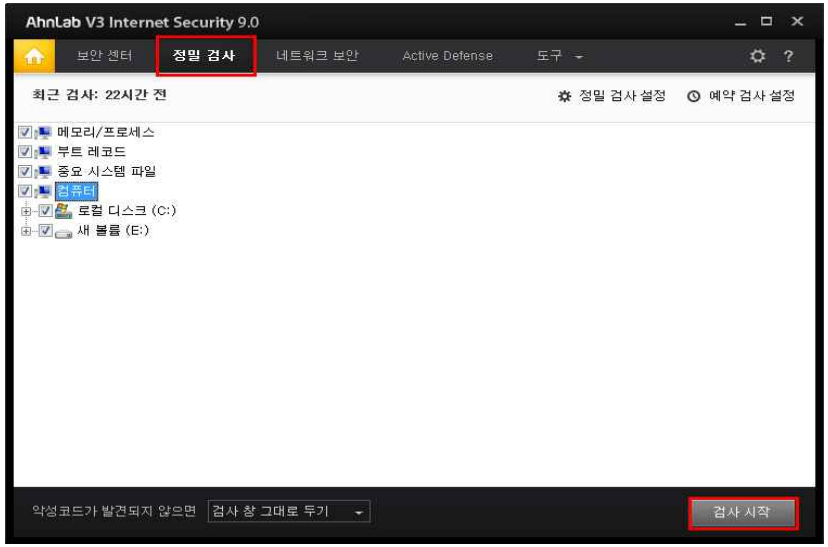
○ 악성코드가 내부 네트워크로 접속 시도한 경우, 침입차단시스템, 스위치 또는 라우터의 차단규칙을 설정하여 내부 네트워크의 유입을 차단한다.

○ 내부 피해 시스템의 악성코드가 외부 시스템으로 연결을 시도하는 경우 라우터나 침입차단시스템의 차단규칙을 이용하여 해당 연결 시도를 차단한다.

MU-05 백신 점검

○ 윈도우 시스템의 경우 안전모드로 부팅하여 백신프로그램을 실행 후 전체파일에 대해 정밀검사를 실시한다.

- 아래 그림은 Windows에서 백신프로그램(V3)으로 정밀검사를 실행하는 예시화면이다.



【 그림 Ⅱ.5.2 (2) 】 백신프로그램 정밀검사 실행화면 예시

○ 백신점검을 통해 악성코드가 검출될 경우 백신치료를 실시한다.

○ 백신점검 후 포맷조치 또는 추가 분석이 필요할 경우에는『 3. 정밀분석』 절차대로 분석을 실시한다.

MU-06 조치 완료

○ 백신프로그램으로 검출된 악성코드를 제거 또는 치료한다.

5.2.3 정밀분석

MU-07 사용하지 않는 계정 및 숨겨진 계정 확인

○ 불법적으로 등록된 사용자나 권한이 상승된 계정 및 그룹이 없는지 아래와 같은 방법으로 확인한다.

가. Windows

【 표 Ⅱ.5.2 (1) 】 Windows 사용자・그룹 정보 확인 명령어

명령어	설명	다운로드
net user	시스템에 존재하는 계정정보 출력	Windows
net localgroup	시스템에 존재하는 그룹정보 출력	Windows

- 아래 그림은 위의 명령어 실행을 통해 시스템의 계정정보 명령어를 실행한 화면이다.

```
C:₩>net user
₩₩ 컴퓨터이름 에 대한 사용자 계정
-------------------------------------------------------------------------------
Administrator            Guest                    USER                     Hack1
명령을 잘 실행했습니다.
C:₩>net localgroup
₩₩ 컴퓨터이름 에 대한 별칭
-------------------------------------------------------------------------------
*Administrators
*Backup Operators
*Cryptographic Operators
*Distributed COM Users
*Event Log Readers
*Guests
*HacksAll
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Replicator
*Users
명령을 잘 실행했습니다.
```

【 그림 Ⅱ.5.2 (3) 】 Windows 시스템 계정정보 명령어 실행화면

- Hack1이란 불법계정이 생성되어있으며, HacksAll이란 불법그룹이 생성되어 있음을 알 수 있다. 그리고 내장된 guest 계정이 '사용 안함' 으로 되어 있는지 점검한다.

나. UNIX / LINUX

【 표 Ⅱ.5.2 (2) 】 UNIX 사용자・그룹 정보 확인 명령어

명령어	설명	다운로드
cat /etc/passwd	시스템에 존재하는 계정정보 출력	Unix/Linux

- /etc/passwd파일에서 UID=0인 계정은 root만이 가지고 있으므로 일반 계정에서 uid=0인 계정의 존재여부를 반드시 확인해야 한다.
- 아래 내용은 /etc/passwd파일의 내부 파일의 일부 화면과 설명이다.

```
root:x:0:0:root:/root:/bin/bash
user1:x:0:0::/home/user1:/bin/bash
```

【 그림 Ⅱ.5.2 (4) 】 /etc/passwd파일 내부화면

- user1이란 불법계정의 UID=0인 것을 확인할 수 있다.
- /etc/passwd파일의 구조는 아래와 같다.

【 표 Ⅱ.5.2 (3) 】 /etc/passwd파일 구조

root	:x	:0	:0	:root	:/root	:/bin/bash
❶	❷	❸	❹	❺	❻	❼

<참고설명>

❶ : 사용자 계정 이름(대부분 ID라고 부른다)
❷ : 사용자 비밀번호(x로 되어 있는 것은 섀도우 패스워드 시스템에 의해 /etc/shadow에 암호화된 형태로 저장 되어있음)
❸ : 사용자 UID(모든 정보는 수치 값으로 저장 되어 있음 root -> 0(UID))
❹ : 사용자 소속 그룹 GID(모든 정보는 수치 값으로 저장 되어 있음 root -> (GID))
❺ : 사용자 정보(계정이름)
❻ : 사용자 계정 디렉터리(계정 홈 디렉터리)
❼ : 사용자 로그인 쉘 (리눅스 : bash Shell, 유닉스 : Korn Shell 등등)

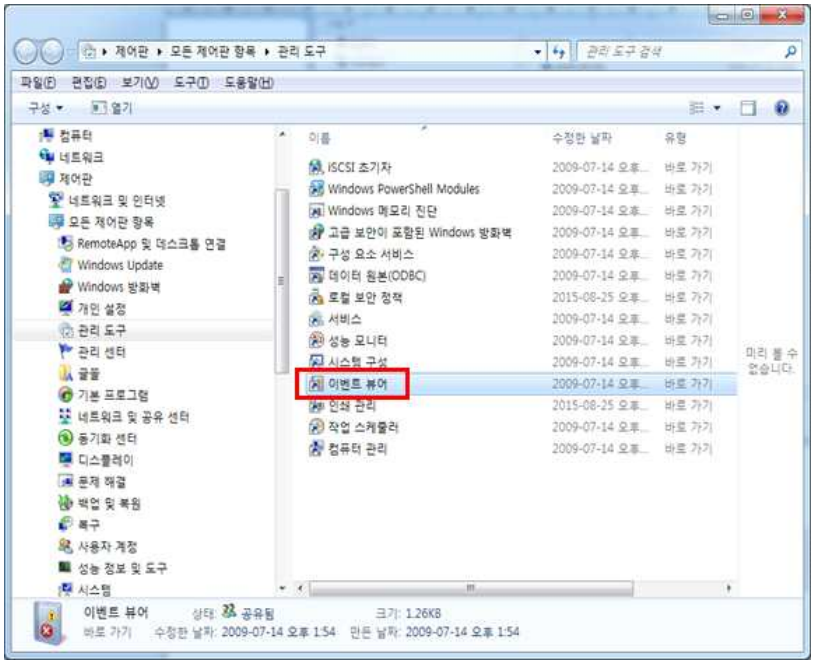
MU-08 시스템 로그의 변조 유무 확인

○ 시스템을 비인가된 방법으로 접근한 공격자들은 시스템에 흔적을 남기게 된다. 이러한 흔적 및 활동 정보를 찾아내기 위해서는 로그 분석이 필요하다.

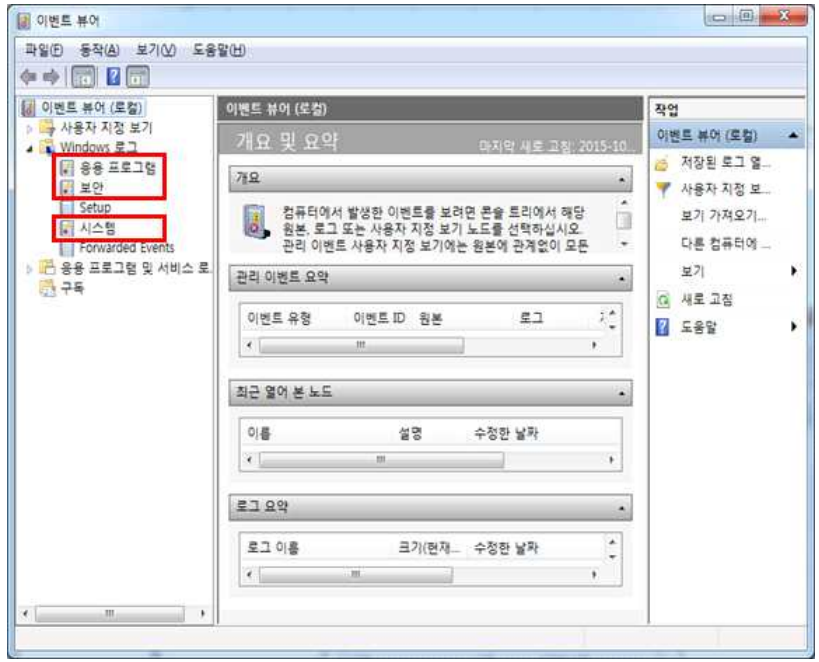
가. Windows

1) 이벤트뷰어

- 윈도우 시스템에서는 하드웨어, 소프트웨어 및 시스템 문제를 이벤트 로그에 저장하므로 이벤트 뷰어 실행을 통해 확인이 필요하다.
- 위치 : 제어판➜관리도구➜컴퓨터관리➜이벤트 뷰어



【 그림 Ⅱ.5.2 (5) 】 Windows 이벤트 뷰어 경로화면



【 그림 Ⅱ.5.2 (6) 】 Windows 이벤트 뷰어 실행화면

- 아래의 표를 참고하여 이벤트 로그ID로 공격과 관련된 이벤트를 분석한다.

【 표 Ⅱ.5.2 (4) 】 특징별 이벤트 로그

특징	이벤트 설명	이벤트 ID
로컬 로그온 시도 실패	사용자 이름과 패스워드를 조합하여 로그온 시도 했을 때 생성되는 이벤트	529, 530, 531, 532, 533, 534, 537
계정의 잘못된 사용	입력된 사용자 계정/패스워드에는 문제가 없지만 다른 제한에 의해 로그온 실패 시 생성되는 이벤트	530, 531, 532, 533
계정 잠김	계정 잠금 정책에 의해 사용자 계정이 잠겼을 때 발생하는 이벤트	539
터미널 서비스 공격	터미널 서비스 연결 후 완전히 세션을 종료하지 않았거나 다시연결 했을 때 이벤트 발생	683, 682
사용자 계정 생성	사용자 계정이 만들어진 시간과 활성화된 시간으로 공격자에 의한 사용자 계정 생성인지를 확인	624, 626
사용자 계정 패스워드	사용자 이외의 계정에 의해 패스워드가 변경되었을 경우 공격자에 의해 해당 사용자 계정이 탈취당한 경우	627, 628

나. UNIX / LINUX

1) secure파일

- secure파일은 보안과 관련된 중요한 로그를 남기며, 사용자 인증 관련된 로그를 포함하고 있다.
- secure파일은 syslog데몬에 의해 남겨지는데, 텍스트 형태의 파일이므로 cat등을 이용하여 확인할 수 있다.

```
# cat /var/log/secure
Nov 28 16:37:11 insecure in.telnetd[6317] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.ftpd[4258] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.rlogind[4168] : conncet from 192.168.10.17
Nov 28 16:37:11 insecure in.rshd[6328] : conncet from 192.168.10.17
Nov 28 16:40:35 insecure login: LOGIN ON 1 BY Hack1 FROM Hack1
```

【 그림 Ⅱ.5.2 (7) 】 secure파일 열람화면

- 위의 그림에서 "Nov 28 16:37:11"에 192.168.10.17로부터 telnet, ftp, rlogin, rsh 등에 대한 접속시도가 있었음을 알 수 있다. 일반적으로 한 사용자가 짧은 시간에 이들 서비스 요청을 수동으로 할 수는 없으므로, 이 로그를 통해 192.168.10.17로부터 단순침입시도 공격이 있었음을 알 수 있다.

2) messages파일

- 시스템 에러, 재부팅 메시지, 로그인 실패 등의 많은 정보를 포함하고 있는 로그파일로써, 시스템 관리자가 시스템 장애 원인 또는 공격으로부터 남는 흔적을 찾아내기 위해서도 messages 파일을 점검한다.


```
# more /var/log/messages
Nov  12 13:44:12 msd1 su: 'su root' failed for aster on /dev/pts/1
Nov  12 14:22:30 msd1 rsh[10103]: connection from bad port
Nov  12 14:28:15 msd1 su: 'su root' failed for aster on /dev/pts/2
Nov  12 14:29:41 msd1 last message repeated 1 time
Nov  12 15:39:29 msd1 su: 'su root' failed for aster on /dev/pts/1
Nov  12 15:57:52 msd1 syslogd: going down on signal 15
```

【 그림 Ⅱ.5.2 (8) 】 messages파일 열람화면

<참고설명>

- 'root'권한으로의 불법적인 로그인 시도가 있었는지를 살펴본다.
- 'su'명령을 이용한'root'또는 특정 권한의 사용자로의 의심스러운 전환 시도가 있었는지를 살펴본다.
- 유효한 사용자로부터의 반복적인 실패한 로그인 시도가 있었는지를 살펴본다.

MU-09 최근 변경된 파일 · 프로그램 · 서비스 확인

○ 공격자들은 공격 성공 후 악성 파일 및 프로그램들을 레지스트리 뿐만 아니라, 서비스, 스케줄러 등에 등록해 놓기 때문에, 이러한 부분을 반드시 점검 하여야 한다.

가. Windows

1) MAC TIME 분석

- 일반적인 파일시스템은 디렉터리나 파일과 관련된 아래와 같은 시간 속성을 갖는다.

<참고설명>

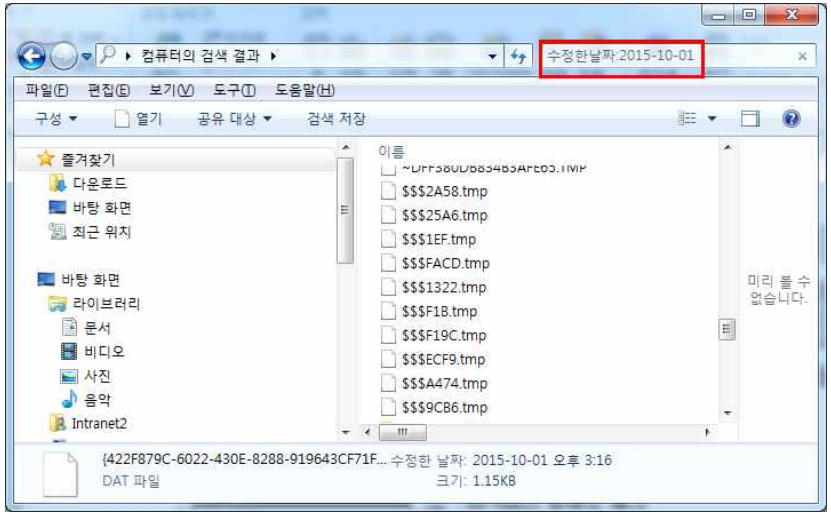
- MTIME : 파일을 생성 및 최근 수정한 시간
- ATIME : 최근 파일을 읽거나 실행시킨 시간
- CTIME : 파일 속성이 변경된 시간

• 이러한 시간 정보를 MAC time 이라 하며 분석을 통해 공격자가 파일 시스템에서 어떠한 행동을 했는지에 대해 판단 할 수 있는 정보를 제공한다.

<참고설명>

- 감염시점으로 MTIME, ATIME 검색
- 검출된 악성코드 MTIME, ATIME 검색

• 위치 : 시작-검색-파일 및 폴더-검색옵션-날짜



【 그림 Ⅱ.5.2 (9) 】 윈도우즈 MAC TIME으로 검색

<참고설명>

- 검색옵션은 날짜로 체크
- 찾고자 하는 MAC TIME 지정
  - 수정된 파일(MTIME)
  - 마지막으로 엑세스한 파일(ATIME)
  - 만든파일(CTIME)

• 감염 날짜를 기준으로 “마지막 엑세스 파일” 을 검사하게 되면 감염 후 실행됐던 파일들을 검색할 수 있다.

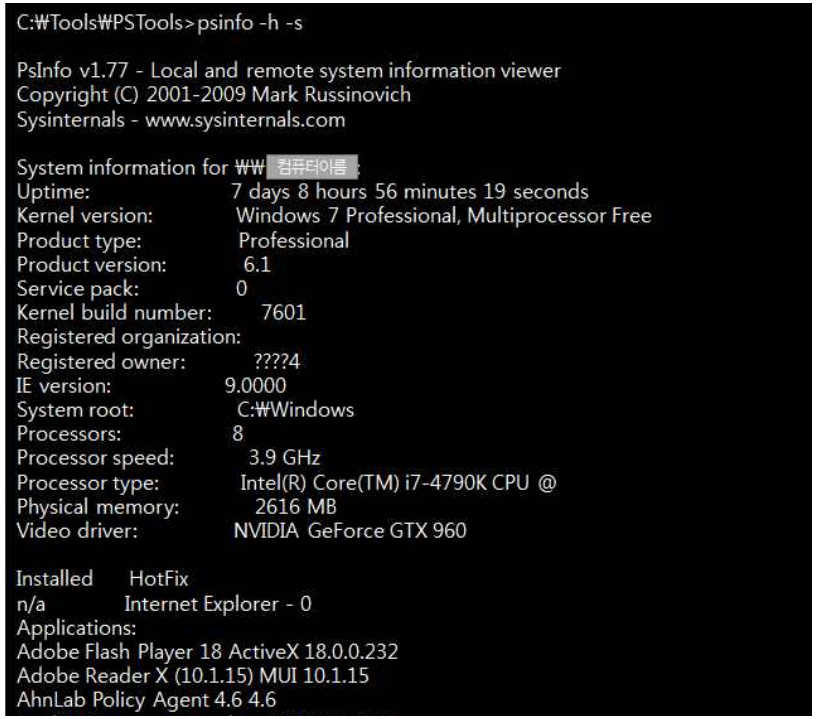
2) 설치 프로그램 점검

• 사고분석을 위해서는 피해시스템의 기본적인 정보가 필요하다. psinfo는 OS의 기본정보 및 보안 업데이트 정보 등을 제공하며 설치된 소프트웨어 정보 또한 알려준다. 이러한 보안 업데이트 정보는 시스템 취약점을 통해 어떻게 공격했는지에 대한 정보를 얻을 수 있기 때문에 최종 업데이트 날짜를 확인해야 한다.

【 표 Ⅱ.5.2 (5) 】 시스템 정보 확인 명령어

명령어	설명	다운로드
psinfo -h -s	설치된 핫픽스 및 소프트웨어 목록 정보	sysinternals

• 아래의 그림은 핫픽스 및 소프트웨어 목록을 확인한 화면이다.



【 그림 Ⅱ.5.2 (10) 】 핫픽스 및 소프트웨어 목록 확인 명령어 실행화면

3) 서비스 점검

- 현재 윈도우에서 실행되고 있는 서비스 정보를 수집한다. 제어판의 서비스메뉴에서 설정할 수 있다. 대다수의 불법 서비스 항목은 윈도우 기본 서비스 이름과 유사한 이름을 사용하기 때문에 분석자는 윈도우 기본 서비스 항목과 불법 프로세스를 명확히 구분할 수 있어야 한다.

【 표 Ⅱ.5.2 (6) 】 서비스 정보 확인 명령어

명령어	설명	다운로드
net start	동작중인 서비스의 목록정보	Windows

- 아래의 그림은 동작중인 서비스 목록을 확인한 화면이다.

```
C:₩>net start
다음과 같은 Windows 서비스가 시작되었습니다.

   Adobe Acrobat Update Service
   AhnLab V3 Service
   ASUS Com Service
   Background Intelligent Transfer Service
   Base Filtering Engine
   CNG Key Isolation
   COM+ Event System
   Cryptographic Services
   DCOM Server Process Launcher
   Desktop Window Manager Session Manager
   DHCP Client
   Diagnostic Policy Service
   Diagnostic Service Host
   Diagnostics Tracking Service
   Distributed Link Tracking Client
   DNS Client
   Function Discovery Provider Host
   Group Policy Client
   Human Interface Device Access
   IKE and AuthIP IPsec Keying Modules
   Intel(R) Content Protection HECI Service
   Intel(R) HD Graphics Control Panel Service
   Intel(R) PROSet Monitoring Service
   IP Helper
```

【 그림 Ⅱ.5.2 (11) 】 서비스 목록 확인 명령어 실행화면

나. UNIX / LINUX

1) MAC TIME 분석

- 최근에 수정되거나 새롭게 생성된 파일을 찾는 명령어로 공격자가 시스템 파일의 변조를 숨기기 위해 시간을 수정하는 경우가 있으므로 이러한 경우에 대비하여 inode 변경시간을 점검한다.
- 아래의 그림은 최근 10일 동안 수정되거나 생성된 파일을 찾아서 파일로 저장하는 화면이다.

```
#find / -ctime -10 -print -xdev >/var/cime_10.txt
```

【 그림 Ⅱ.5.2 (12) 】 최근 10일 동안 수정 및 생성된 파일을 저장하는 화면

2) 설치 프로그램 점검

- setuid를 가지는 실행 프로그램은 실행도중에 슈퍼유저(root)의 권한을 가지고 실행되므로 find를 이용하여 setuid나 setgid 파일이 있는지 확인한다.

```
#find / -user root -perm -4000 -print>setuid.txt
#find / -user root -perm -2000 -print>setgid.txt
```

【 그림 Ⅱ.5.2 (13) 】 root권한을 가지고 실행하는 파일을 저장하는 화면

MU-10 숨겨진 프로세스 및 비정상 프로세스 확인

○ 일반적인 시스템들은 많은 실행 프로세스들을 가지고 있으며, 이러한 프로세스 중에는 공격자가 실행시켜놓은 프로세스가 실행되고 있거나 흔적이 남아 있을 수 있으니 자세히 확인해 볼 필요가 있다.

가. Windows

- 윈도우에서 프로세스를 점검할 수 있는 도구로는 pslist가 있다. 이 도구는 sysinternals에서 제공하며, 현재 구동 중인 프로세스 목록을 출력해준다.

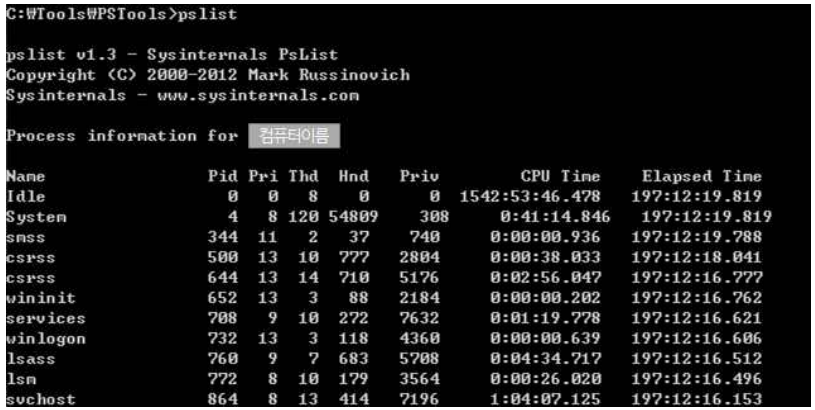
【 표 Ⅱ.5.2 (7) 】 프로세스 정보 확인 명령어

명령어	설명	다운로드
pslist	현재 프로세스 리스트 출력	sysinternals

• 프로세스 정보 확인시 주의해서 보아야 할 정보는 아래와 같다

<참고설명>

- 실행 프로세스명
- 프로세스 실행파일 위치
- 프로세스 커맨드 라인
- 프로세스 실행시간
- 프로세스가 참조중인 DLL 및 파일
- pslist : 현재 구동중인 프로세스 목록을 출력해 준다. 옵션을 하지 않으면 프로세스가 실행된 시간을 자세히 확인할 수 있는데 이러한 시간은 또 한 uptime에서 확인했던 부팅시간 이후에 악성프로그램이 언제 실행되었는지 확인 가능하다. -t 옵션을 사용하면 프로세스를 트리구조로 어떤 프로세스에서 실행되었는지 확인할 수 있다.



```
C:₩Tools₩PSTools>pslist

pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for 컴퓨터이름:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   8    0      0 1542:53:46.478   197:12:19.819
System                4   8 120 54809    308    0:41:14.846   197:12:19.819
smss                344  11   2   37    740    0:00:00.936   197:12:19.788
csrss               500  13  10  777   2804    0:00:38.033   197:12:18.041
csrss               644  13  14  710   5176    0:02:56.047   197:12:16.777
wininit             652  13   3   88   2184    0:00:00.202   197:12:16.762
services            708   9  10  272   7632    0:01:19.778   197:12:16.621
winlogon            732  13   3  118   4360    0:00:00.639   197:12:16.606
lsass               760   9   7  683   5708    0:04:34.717   197:12:16.512
lsm                 772   8  10  179   3564    0:00:26.020   197:12:16.496
svchost             864   8  13  414   7196    1:04:07.125   197:12:16.153
```

【 그림 Ⅱ.5.2 (14) 】 윈도우 프로세스 목록 정보 실행화면

나. UNIX / LINUX

• 프로세스 확인은 "ps -ef" 명령어를 통해 확인 할 수 있는데, process 실행자, PID, 실행일시, 프로세스명 등을 확인할 수 있다.

```
# ps -ef|more
UID    PID    PPID  C    STIME    TTY    TIME  CMD
root     1       0  0   May 22    ?       0:44/etc/init -r
root     2       0  0   May 22    ?       0:00pageout
root   339       1  0   May 22    ?       0:00/usr/openwin/bin/fbconsole -d :0
root    53       1  0   May 22    ?       0:00/usr/lib/devfsadm/devfseventd
root    57       1  0   May 22    ?       0:00/usr/lib/devfsadm/devfsadmd
root   138       1  0   May 22    ?       0:00/usr/sbin/keyserv
root   236       1  0   May 22    ?       0:00/usr/lib/power/powerd
root 25743       1  0    Jun 5    ?       0:03/usr/sbin/inetd -s
root   136       1  0   May 22    ?       0:07/usr/sbin/rpcbind
root   190       1  0   May 22    ?       0:00/usr/sbin/cron
root   176       1  0   May 22    ?       0:02/usr/lib/autofs/automountd
root   189       1  0   May 22    ?       0:04/usr/sbin/syslogd
root   204       1  0   May 22    ?       0:50/usr/sbin/nscd
root   296       1  0   May 22    ?       0:00/usr/dt/bin/dtlogin -daemon
root   297       1  0   May 22    ?       0:00/usr/lib/nfs/mountd
root   262       1  0   May 22    ?       0:00/usr/lib/sendmail -bd -q15m
root   316       1  0   May 22    ?       0:00/usr/lib/saf/sac -t 300
root   371       1  0   May 22    ?       0:00/usr/openwin/bin/speckeysd
root   299       1  0   May 22    ?       0:00/usr/lib/nfs/nfsd -a 16
root   337     305  0   May 22    ?       9:53mibiisa -r -p 32781
root   322     296  0   May 22    ?       0:00/usr/dt/bin/dtlogin -daemon
root   367     357  0   May 22    ?       0:00/usr/openwin/bin/fbconsole
root   390     357  0   May 22    ?       0:00/usr/openwin/bin/htt -nosm
root   433     431  0   May 22    ?       0:11dtwm
root   431     414  0   May 22    pts/2   0:45/usr/dt/bin/dtsession
```

【 그림 Ⅱ.5.2 (15) 】 유닉스 프로세스 목록 정보 실행화면

MU-11 비정상 포트 및 외부연결확인

○ 현재 열려있는 포트를 어떠한 응용 프로그램이 사용하는지에 대한 정보를 수집한다. 이는 피해시스템에서 특정 포트를 사용하는 백도어나 트로이목마를 찾기 위한 중요한 정보가 된다.

가. Windows

- “netstat -an” 명령어를 통해 프로토콜 상태, IP 기반 네트워크 연결 정보 등을 확인해서 현재 열려 있는 포트와 포트에 연결되어 있는 IP 정보를 확인해야 한다.

【 표 Ⅱ.5.2 (8) 】 네트워크 정보 확인 명령어

명령어	설명	다운로드
netstat -an	서비스 중인 포트 정보 및 연결된 아이피 정보	Windows

- 아래 명령어 수행결과에서 보면 시스템이 사용하지 않는 30451 포트가 LISTENING 상태로 열려 있는 것을 확인할 수 있다.

```
C:₩>netstat -an

활성 연결

프로토콜  로컬 주소          외부 주소          상태
TCP    0.0.0.0:135      0.0.0.0:0      LISTENING
TCP    0.0.0.0:445      0.0.0.0:0      LISTENING
TCP    0.0.0.0:1026     0.0.0.0:0      LISTENING
TCP    0.0.0.0:1027     0.0.0.0:0      LISTENING
TCP    0.0.0.0:1028     0.0.0.0:0      LISTENING
TCP    0.0.0.0:3371     0.0.0.0:0      LISTENING
TCP    0.0.0.0:30451    0.0.0.0:0      LISTENING
UDP    0.0.0.0:445      0.0.0.0:0      LISTENING
```

【 그림 Ⅱ.5.2 (16) 】 네트워크 정보 실행화면

- 아래의 도구를 사용하여 열려있는 포트의 정보를 수집한다.

【 표 Ⅱ.5.2 (9) 】 포트별 서비스 정보 확인 명령어

명령어	설명	다운로드
fport	서비스 중인 포트를 열고 있는 프로그램 정보	foundstone.com

- fport 명령어는 어떠한 응용 프로그램이 어떤 포트를 사용하는지에 대한 정보를 보여준다.

<참고설명>
/p : 포트별 정렬
/a : 응용프로그램 이름순 정렬
/l : 프로세스 ID 정렬
/ap : 응용 프로그램 디렉토리 순 정렬

```
C:₩>Fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process          Port  Proto  Path
436   svchost    ->    135   TCP    C:₩WINDOWS₩system32₩svchost.exe
8     System     ->    445   TCP
504   msdtc      ->    1025  TCP    C:₩WINDOWS₩system32₩msdtc.exe
732   MSTask     ->    1026  TCP    C:₩WINDOWS₩system32₩MSTask.exe
711   csrrs      ->    30451 TCP    C:₩WINDOWS₩system32₩csrrs.exe
```

【 그림 Ⅱ.5.2 (17) 】 fport 실행화면

나. UNIX / LINUX

- netstat는 현재 시스템의 네트워크 연결상태를 알려주는 명령어로 어떤 포트가 열려있는 지 발신지 주소는 어떻게 되는지 등을 확인할 수 있다.

```
# netstat -an | more
Active Internet connections (including servers)
Proto  Recv-Q  Send-Q  Local Address      Foreign Address    State
tcp        0       0 0.0.0.0:7777       0.0.0.0:*          LISTEN
tcp        0       0 0.0.0.0:8000       0.0.0.0:*          LISTEN
tcp        0       0 0.0.0.0:8817       0.0.0.0:*          LISTEN
tcp        0       0 0.0.0.0:21         0.0.0.0:*          LISTEN
tcp        0       0 0.0.0.0:22         0.0.0.0:*          LISTEN
tcp        0       0 0.0.0.0:80         0.0.0.0:*          LISTEN
tcp        0       0 0.0.0.0:8080       0.0.0.0:*          LISTEN
tcp        0       0 0.0.0.0:6000       0.0.0.0:*          LISTEN
```

【 그림 Ⅱ.5.2 (18) 】 네트워크 정보 실행화면

2.2.4 재발방지

MU-12 보완조치 및 재발방지 조치

○ 윈도우 서버의 RRAS 서비스가 실행중일 경우 해당 서비스 중지

○ 윈도우 서버의 이벤트 로그를 통해 RRAS 서비스를 실행시킨 이력 및 IP를 확인하고 해당 IP에 대한 접근 제한 정책 적용

○ 유닉스 · 리눅스 서버의 PPTP 서비스가 실행중일 경우 해당 프로세스 중지

○ 유닉스 · 리눅스 서버의 시스템 로그를 통해 PPTP 서비스를 실행시킨 이력 및 IP를 확인하고 해당 IP에 대한 접근 제한 정책 적용

○ 사용하지 않는 계정과 숨겨진 계정 삭제

○ 외부 네트워크와 연결된 백도어 포트 발견 시 방화벽을 통해 해당포트로의 접근 제한 정책 적용

○ 백도어 포트 서비스를 실행중인 파일 확인 및 삭제

○ 그 외 공격자 흔적 제거

- 공격자의 모든 활동과 피해 흔적을 100% 분석한 경우는 이를 찾아서 복구하면 되나, 그렇지 않은 경우는 시스템 재설치

○ 비밀번호 교체

- 경유지 악용 공격으로 인해 비밀번호가 유출되었을 가능성이 있으므로 피해 시스템 뿐만 아니라 관련된 시스템의 비밀번호 교체 실시

○ 백업 복구

- 악성코드 공격 이후 파일이 변조되었을 가능성이 있으므로 감염 이전의 백업된 기록을 갖고 피해시스템을 복구

○ 취약점 제거 및 보안조치

- 침입의 원인이 된 취약점을 제거하고 경유지 악용 공격과 관련된 보안패치를 포함하여 기존에 설치되지 않았던 모든 보안 패치를 설치

- 만약 보안패치가 없다면 취약점을 임시적으로 제거할 수 있는 수단을 강구해야 함

- 피해시스템의 안전한 운영을 위해 보안설정을 점검

MU-13 서비스 정상화

○ 시스템을 주기적으로 모니터링 하여 서비스 정상여부를 확인한다.

5.3 특이사항

□ 봇넷 C&C 대응방안

○ 외부 네트워크와 연결된 백도어 포트 발견 시 방화벽을 통해 해당 포트로의 접근 제한 정책 적용한다.

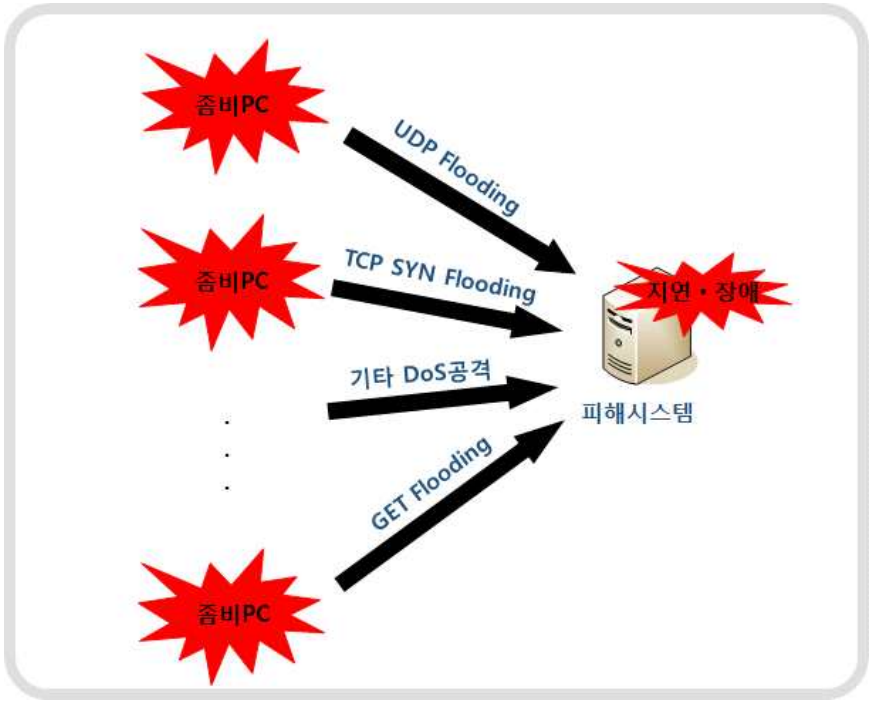
○ 백도어 포트 서비스를 실행중인 파일 확인 및 삭제한다.

6 서비스 거부

6.1 설명

□ 서비스 거부 피해란 다수의 악성코드 감염PC를 이용, 대량의 접속 트래픽을 일시에 특정 사이트 또는 시스템에 전송하여 과부하를 유발시킴으로써 정상적인 정보시스템서비스를 할 수 없도록 하는 사이버 공격으로 발생한 피해를 말한다.

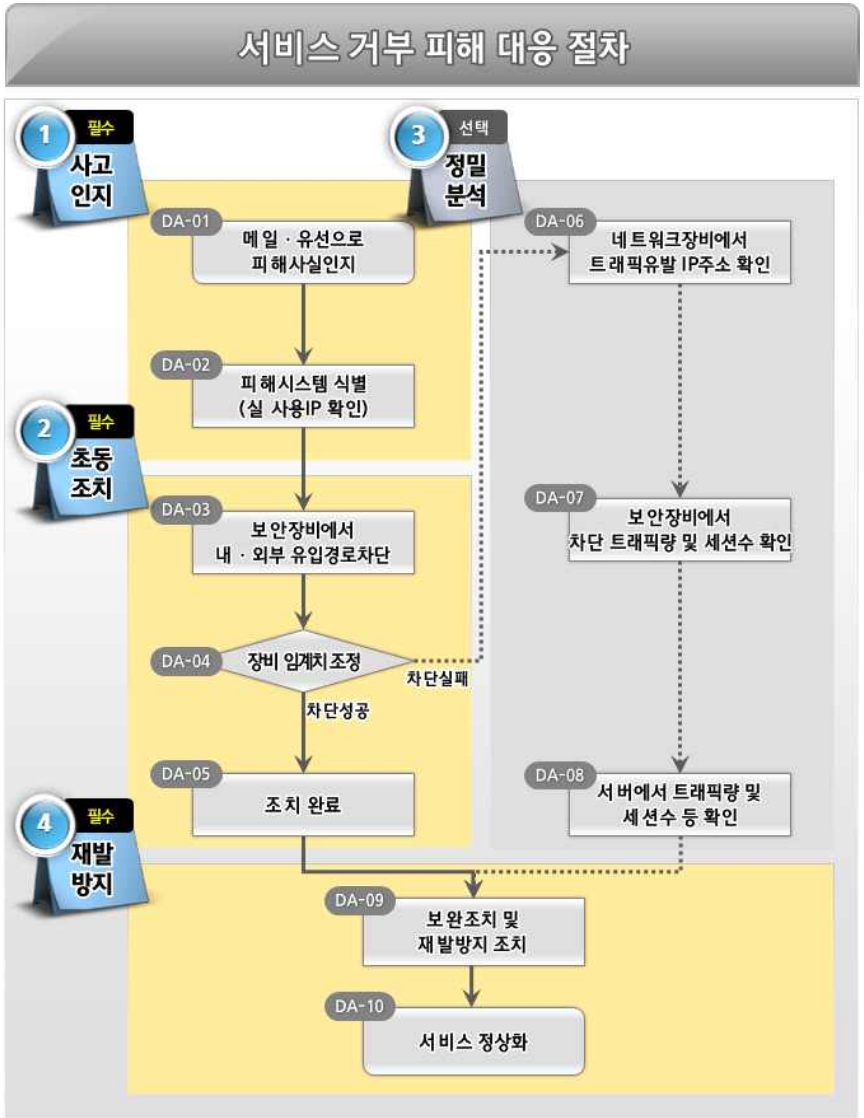
□ 서비스 거부 피해 개요도



【 그림 Ⅱ.6.1 (1) 】 서비스 거부 피해 개요도

6.2 대응요령

□ 서비스 거부 피해 대응요령은 사고인지, 초동조치, 재발방지의 필수절차와 정밀분석의 선택절차로 구성하여 운영한다.



【 그림 Ⅱ.6.2 (1) 】 서비스 거부 피해 대응절차

6.2.1 사고인지

DA-01 메일 또는 유선으로 피해사실 인지

○ 자체 사고 탐지 및 과학기술사이버안전센터(S&T-SEC), NCSC 등으로부터 이관된 메일(유선)을 통해 피해사실을 인지한다.

DA-02 피해시스템 식별 (실 사용IP 확인)

○ 자체 사고 탐지 및 메일(유선)로 통보된 피해시스템 IP주소를 네트워크장비 또는 방화벽 확인 등을 통해 실제 사용하는 IP주소를 확인하여 피해 시스템이 부하 발생여부를 확인한다.

6.2.2 초동조치

DA-03 보안장비에서 내 · 외부유입경로차단

○ 라우터 ACL 설정을 통해 공격IP주소, 특정 프로토콜에 대한 트래픽 차단한다.

○ 공격 IP 주소가 실존하지 않는 스푸핑 된 IP 주소인 경우는 회선사업자, 라우터 또는 방화벽에서 차단한다.

DA-04 장비 임계치 조정

○ 유입되는 트래픽을 침입차단시스템, 스위치 또는 라우터의 차단규칙의 대역폭 임계치를 조정하여 초과되는 트래픽은 차단한다.

○ 별도의 예비 서버를 이용하여 URL Redirection을 적용한다.

○ 미 존재 페이지 요청, 상대적으로 많은 페이지 요청 등의 IPS/IDS에서 비정상 행위 연결 차단한다.

DA-05 조치 완료

○ 서비스 거부 공격 대응 장비별 차단 된 트래픽을 확인한다.

6.2.3 정밀분석

DA-06 네트워크장비에서 트래픽유발 IP주소 확인

○ 네트워크 장비에서 가장 많은 트래픽을 유발하는 IP 주소를 정렬하여 실시간으로 모니터링 한다.

DA-07 보안장비에서 차단 트래픽량 및 세션수 확인

○ 유입되는 트래픽량과 세션수를 보안장비에서 확인 한다.

DA-08 서버에서 트래픽량 및 세션수 등 확인

○ 피해 서버에서 정의한 최대 세션 개수 초과 여부 확인, 평균 세션 개수와 비교한다.

6.2.4 재발방지

DA-09 보완조치 및 재발방지 조치

○ 불 필요한 UDP/ICMP 서비스 차단

○ 통신량 한계 초과 공격의 경우에는 네트워크 상단 (회선사업자, IDC, 라우터 등)에서 처리하는 것이 네트워크 장비 및 보안장비의 부하를 줄이는 데 효과적임

○ 세션을 관리하는 장비에서 동일 IP 주소에 대한 동시 접속량 제한 및 차단

※ 예 : 동일 IP 주소에서 동시 접속 회수가 10회 이상인 경우 300초 동안 차단

○ L4 라우터에서 트래픽 임계치를 설정 후 초과되는 트래픽은 Drop처리

○ L7 라우터에서 IP마다 요청횟수에 임계치 설정 후 초과되는 트래픽은 Drop처리

○ 별도의 예비 서버를 이용하여 URL Redirection을 적용

○ 미존재 페이지 요청, 상대적으로 많은 페이지 요청등의 IPS/IDS에서 비정상 행위 연결 차단 설정

○ L7 라우터에서 HTTP 헤더의 cache-Control에 CC공격패턴(no-store, no-cache, must-revalidate, max-age=0)을 포함시 Drop처리

○ IPS/IDS에서 CC공격 패턴 차단 규칙 설정

○ 수신 Timeout 값을 낮게 설정, mod-antiloris설치, snort rule 적용 등의 Apache 설정 변경 및 모듈 설치

○ IPS/IDS에서 Slowloris패턴(HTTP헤더의 끝이 /0d0a0d0a/로 끝나지 않는 패킷)이 탐지되고 일정시간동안 다음 패킷으로 완전한 헤더 내용이 전달되지 않는다면 연결을 차단

○ URL이 아닌HTTP Request의 HOST필드값에 대해 임계치 설정

○ 서비스별 트래픽의 대역폭을 제한하고, 사용하지 않는 서비스를 사전에 차단

○ 웹서버의 Connection Timeout과 Keep alive timeout 임계치 설정

○ 웹서버의 Request Read Timeout(mod_reqtimeout) 임계치 설정

○ 일반적인 웹서버의 POST파라미터 개수 제한, POST메시지 크기제한 설정

○ Tomcat에서는 maxRarameterCount, maxPostSize 임계치 설정

○ PHP에서는 5.4.0 RC4이상 버전으로 업데이트하고 max_input_var 임계치 설정

○ 홈페이지에 검색서비스 구현 시, SQL의 'like' 구문을 사용하는 유사 검색 서비스는 지양

○ 와일드 카드 및 특수기호 검색을 차단하기 위해 웹방화벽에서 사용자 입력값 필터링

○ 정보제공이 주기능이며 검색 요청이 많은 경우, 자주 요청되는 내용은 검색 결과를 파일로 저장하고 인덱싱(indexing) 방식으로 결과를 제공하며 DB서버를 이중화하여 로드밸런싱(load balancing) 수행

○ IIS 웹서버를 최신버전으로 업데이트

○ SNMP서비스가 불필요한 시스템은 각 벤더별 설정에 따라 해당 서비스를 중지

○ 보안이 강화된 SNMP최신 버전(V3)을 사용하도록 시스템을 패치

○ SNMP를 사용하지 않을 경우 기관의 내부 네트워크에서 외부 네트워크로 나가는 트래픽 중 SNMP서비스에서 사용하는 포트를 차단하여 내부 서버가 다른 서버를 공격하는 경우를 사전 차단

○ 백업 복구

- 서비스거부 공격 이후 파일이 변조되었을 가능성이 있으므로 피해 이전의 백업된 기록을 갖고 피해시스템을 복구

○ 취약점 제거 및 보안조치

- 침입의 원인이 된 취약점을 제거하고 서비스 거부 공격과 관련된 보안 패치를 포함하여 기존에 설치되지 않았던 모든 보안 패치를 설치
- 만약 보안패치가 없다면 취약점을 임시적으로 제거할 수 있는 수단을 강구해야 함
- 피해시스템의 안전한 운영을 위해 보안설정을 점검

DA-10 서비스 정상화

○ 시스템을 주기적으로 모니터링 하여 서비스 정상여부를 확인한다.

6.3 특이사항

□ 특이사항 없음