제 3 장 | 침해사고 분석 기술

제1절 윈도우 사고분석

최근 윈도우 서버나 개인 사용자 PC를 겨냥한 해킹뿐 아니라 웜, 바이러스, 봇을 통한 해킹사고 또한 급증하고 있어 관리자나 사용자들을 위한 윈도우 침해사고 분석 기술이 요구되고 있다.

윈도우 사고분석에 있어 포렌식 측면에서 봤을 때 피해시스템에 영향을 주지 않고 필요한 정보를 얻어야 한다. 하지만 그렇게 하기 위해서는 전문적인 포렌식 기술과 도구들이 있어야 하므로 본 안내서에서는 라이브(live)에서 직접 피해시스템을 쉽고 빠르게 분석 할 수 있는 방법에 대해 알아보도록 한다.

1. 초기분석

침해사고를 정확히 분석하기 위해서는 현재 구동중인 프로세스 정보나 네트워크 상태 정보 등 휘발성 증거를 수집해야 한다. 그리고 현재 피해시스템의 상황을 빠른 시간 안에 파악할 수 있는 방법이 필요하므로 윈도우 커맨드에서 실행되는 명령어들을 이용해 프로세스, 네트워크, 로그인 정보들을 수집해야 한다. 분석자는 이러한 정보들을 이용해 최대한 빨리 시스템의 변경내용이나 공격자의 흔적을 파악해야 한다.

가. 시스템 시간 확인

모든 시스템들이 시간을 동기화 시켜놓지 못하기 때문에 각 시스템별로 운영되는 고유의 시간이 있다. 이러한 시간이 파악되어야만 시스템 로그 시간을 연관 지어 확인 할 수 있다. 또한 공격자들은 관리자들의 분석에 혼란을 주기위해 시스템 시간을 변경해 놓는 경우가 있으므로 시스템 현재 시간을 확인해야 한다.

'date'와 'time'은 cmd.exe 프로그램에 내장되어 있고 시스템 시간을 기록하는데 사용한다. 그리고 uptime은 시스템의 부팅 시간 정보를 보여주는 명령어로 사고 시간을 결정하는데 필요하기 때문에 중요한 정보이다. 도구는 'http://www.sysinternals.com'에서 무료로 다운받을 수 있다.

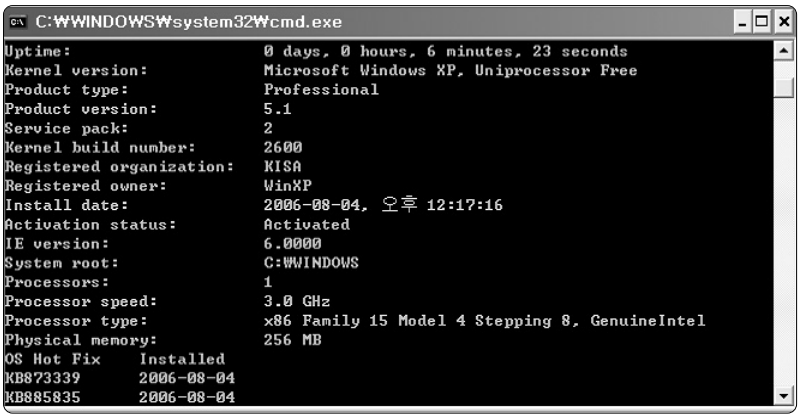
명령어	설 명	다운로드
date /T	시스템 날짜를 알려주는 명령어 ex)2006-10-23	OS
time /T	시스템 시간을 알려주는 명령어 ex)오전 09:48	OS
uptime	부팅된 시간 정보를 알려주는 명령어	sysinternals

※ OS : 윈도우 시스템에서 기본적으로 제공하는 명령어

나. 시스템 정보

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.

아래 그림은 psinfo 명령어를 통해 시스템의 정보를 확인한 화면이다.



〈그림 3-1〉 psinfo 실행 화면

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

다. 프로세스 정보 확인

대부분의 윈도우즈 시스템들은 많은 실행 프로세스들을 가지고 있다. 이러한 프로세스 중에는 공격자가 실행시켜놓은 악성프로그램이 실행되고 있거나 흔적이 남아 있을 수 있으니 자세히 확인해 볼 필요가 있다. 관심 있게 확인해 봐야 될 프로세스 정보는 다음과 같다.

- 실행 프로세스명
- 프로세스 실행파일 위치
- 프로세스 커맨드 라인
- 프로세스 실행시간
- 프로세스가 참조중인 DLL 및 파일

프로세스를 점검할 수 있는 도구로는 pslist가 있다. 이 도구는 'http://www.

sysinternals.com' 에서 다운 받을 수 있으며 현재 구동중인 프로세스 목록을 출력해준다. 옵션을 하지 않으면 프로세스가 실행된 시간을 자세히 확인할 수 있는데 이러한 시간은 또한 uptime에서 확인했던 부팅시간 이후에 악성프로그램이 언제 실행되었는지 확인 가능하다. -t 옵션을 사용하면 프로세스를 트리구조로 어떤 프로세스에서 실행되었는지 확인할 수 있다.

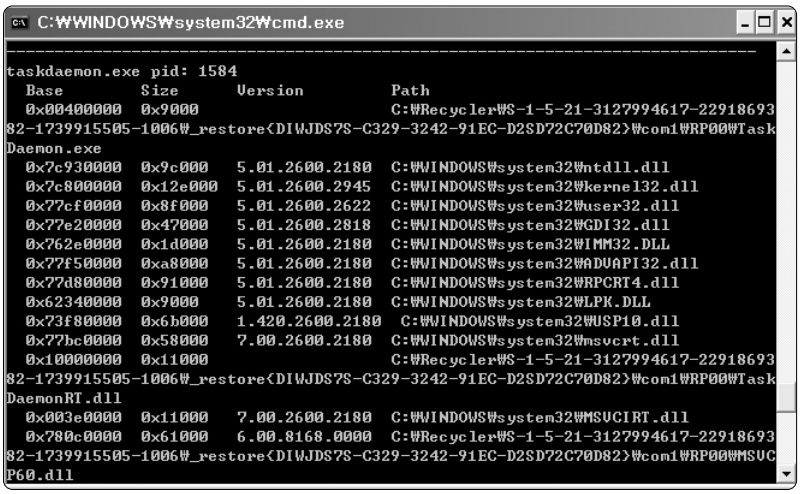
```
C:\Forensic\>pslist -t
```

Name	Pid	Pri	Thd	Hnd	VM	WS	Priv
Idle	0	0	1	0	0	16	0
System	8	8	36	57	5824	272	32
smss	160	11	6	33	5380	376	1084
csrss	184	13	10	392	33144	4068	1576
winlogon	204	13	17	379	37520	4796	5740
services	232	9	30	495	32472	4812	2340
svchost	416	8	8	305	22984	3416	1344
iexplore	332	8	6	197	49496	5772	3412
mdm	1228	8	3	90	21304	2420	700
SPOOLSV	444	8	11	131	26240	3528	2232
msdtc	472	8	18	203	31324	5004	1628
svchost	564	8	18	345	39264	7560	4100
sqlservr	624	8	32	281	318796	10432	12372
rsmss	704	8	2	38	11072	1264	484
lsass	244	9	14	258	31784	4744	2296
Explorer	1040	8	14	315	49492	3868	4432
Internat	1204	8	1	28	15944	1628	340
sqlmangr	1248	8	3	99	27544	3772	1160
atjob	1324	8	1	10	5696	552	124
sysAnalyzer	1548	8	3	151	52064	7852	3636
conime	1404	8	1	23	14728	1296	300

위 명령어 실행결과에서 보면 백도어 프로그램인 rsmss가 "winlogon-services"의 자식 프로세스로 실행된 것을 확인할 수 있어 윈도우 서비스에 의해 실행된 것을 확인할 수 있다.

at.job이라는 악성프로그램 같은 경우는 윈도우에서 흔히 보지 못한 프로그램이 실행되고 있어 어렵지 않게 찾아낼 수 있지만 정상 파일처럼 위장하여 악성프로그램을 실행하는 경우가 있으므로 실행파일 위치를 찾아서 정상 프로그램의 위치와 맞는지 확인해야 한다.

또한 프로그램들이 사용하는 동적라이브러리 (DLL, Dynamic Link Libraries)정보를 수집해야 한다. 악성 프로그램은 시스템 DLL 뿐만 아니라 자체 제작한 DLL을 사용할 수도 있으므로 자세한 점검이 필요하다. listdlls은 모든 프로세스가 사용하고 있는 DLL 정보를 보여주고, 경로, 사이즈, 버전까지도 알 수 있다. 아래 그림은 정상적인 프로그램처럼 위장한 악성프로그램인 TaskDaemon.exe 프로그램을 listdlls로 확인한 화면이다. 이 악성프로그램은 자체 제작한 TaskDaemonRT.dll 등을 사용하는 것을 확인할 수 있다.



〈그림 3-2〉 listdlls 실행결과

또한 악성프로그램들은 자신들의 실행과 관련된 설정파일들이 있고 특히 악성 봇 프로그램 같은 경우 설정파일에 있는 서버에 접속을 하고 명령어들을 실행하기 때문에 자세한 조사가 필요하다. 프로세스들이 어떠한 파일들을 참조하고 있는지 확인할 수 있는 방법은

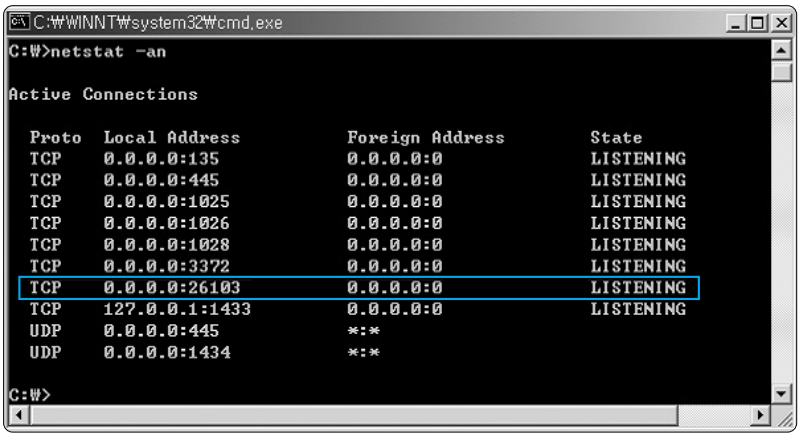
'http://www.sysinternals.com' 에서 제공하는 handle 프로그램을 이용해서 확인할 수 있다.

명령어	설 명
pslist	현재 프로세스 리스트 출력
listdlls	프로세스들이 사용하는 DLL 출력
handle	프로세스들이 참조하는 파일 리스트 출력

다. 네트워크 정보 확인

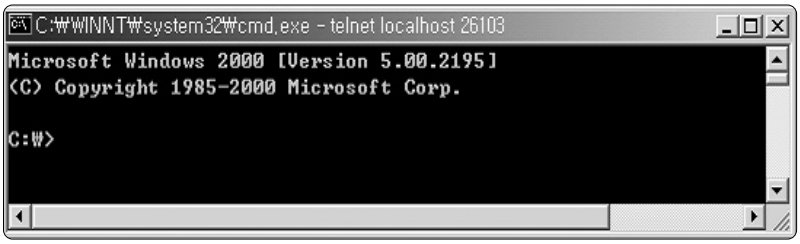
현재 피해시스템 네트워크 정보, 서비스를 열고 있는 응용프로그램 정보, 서비스에 연결되어 있는 세션 정보 등은 공격자의 흔적을 추적 할 수 있는 중요한 역할을 한다.

"netstat -an" 명령어를 통해 프로토콜 상태, IP 기반 네트워크 연결 정보 등을 확인해서 현재 열려 있는 포트와 포트에 연결되어 있는 IP 정보를 확인해야 한다. 아래 명령어 수행 결과에서 보면 시스템이 사용하지 않는 26103 포트가 LISTENING 상태로 열려 있는 것을 확인할 수 있다.



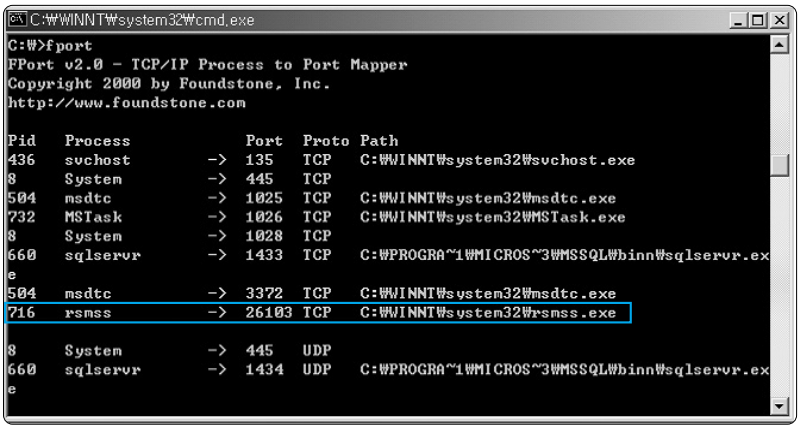
〈그림 3-3〉 netstat 실행 화면

이와 같은 26103포트에 telnet이나 nc로 접속하여 어떤 응용 어플리케이션이 구동중인지 확인해야 한다. 확인 결과 윈도우 command를 실행할 수 있게 해주는 백도어 포트임을 아래 그림처럼 확인할 수 있었다.



〈그림 3-4〉 telnet으로 접속한 화면

위의 26103 백도어 포트를 열고 있는 프로세스를 확인해야 하는데 fport 라는 'http://www.foundstone.com' 에서 제공한 명령어를 사용하여 다음과 같이 확인할 수 있다.



〈그림 3-5〉 fport 실행 화면

해킹 사고가 발생하면 네트워크 인터페이스 카드(NIC)가 promisc 모드로 동작중인지 확인해야 한다. 공격자는 스니핑 공격을 통해 시스템으로 송수신되는 모든 네트워크 트래픽을 모니터링 할 수 있는데 이 경우에 네트워크 인터페이스 카드가 promisc 모드로 동작하게

되므로 반드시 점검이 필요하다.

명령어	설 명	다운로드
ipconfig /all	시스템의 아이피 정보 수집	OS
netstat -an	서비스 중인 포트 정보 및 연결된 아이피 정보	OS
fport	서비스 중인 포트를 열고 있는 프로그램 정보	sysinternal
promiscdetect	NIC 가 promisc 모드로 동작중인지 확인	tsecurity.nu

라. 사용자/그룹 확인

공격자에 의해 추가된 사용자나 그룹이 없는지 다음과 같은 명령어로 확인한다.

명령어	설 명	다운로드
net user	시스템에 존재하는 계정정보 출력	OS
net localgroup	시스템에 존재하는 그룹정보 출력	OS

마. 공유, 로그인 정보 확인

시스템에서 제공되는 "net" 명령어를 사용해 현재 시스템에 공유된 정보, 현재 로그인되어 있는 사용자 정보를 확인해야 한다. 그리고 NBT(Net bios)에 연결된 정보가 있는지 nbtstat 명령어를 사용해 확인할 필요가 있다. 또한 시스템의 감사 정책이 설정되어 있다면 'http://www.foundstone.com' 에서 제공하는 ntlast 명령어를 통해 로그인/로그오프에 대한 성공 실패 여부를 확인할 수 있다.

명령어	설 명	다운로드
net share	시스템 공유 정보 출력	OS
net session	공유 자운에 접속한 컴퓨터 정보 출력	OS
nbtstat -c	NBT에 연결된 세션 정보 출력	OS
ntlast -f	원격접속 로그 정보 출력	foundstone.com

바. 분석 스크립트

앞서 설명한 프로그램들을 하나씩 실행해 분석 할 수도 있지만 초기분석을 효율적으로 수행하기 위해서는 휘발성 데이터를 빠르게 수집해서 분석해야 한다. 빠르게 수집하고 분석하기 위해서는 배치파일로 위의 명령어를 수행하고 결과는 파일로 저장해야 한다.

```
echo off
@echo =========초기 분석 점검 날짜==========
date /t
@echo =========초기분석 점검 시간==========
time /t
@echo =========시스템 기본 정보(psinfo)==========
psinfo -h -s -d
@echo =========부팅시간정보(uptime)==========
uptime
@echo =========IP정보 (ipconfig /all)==========
ipconfig /all
@echo =========세션 정보 (net sess)==========
net sess
@echo =========포트 정보(netstat -na)==========
netstat -na
@echo =========로그온 사용자 정보(ntlast)==========
ntlast -f
@echo =========포트별 서비스 정보(fport /i)==========
fport /i
@echo =========Promiscuous 모드 정보(promiscdetect)==========
promiscdetect
@echo =========로컬 서비스 정보(net start)==========
net start
@echo =========프로세스 기본 정보(pslist -t)==========
pslist -t
@echo =========DLL 정보(listdll)==========
listdlls
@echo =========핸들 정보(handle)==========
```

```
handle
@echo =========공유 정보(net share)==========
net share
@echo =========사용자정보(net user)==========
net user
@echo =========도메인 그룹 정보(net group)==========
net group
@echo =========로컬 그룹 정보(net localgroup)==========
net localgroup
@echo =========관리자 그룹 정보==========
net localgroup administrators
```

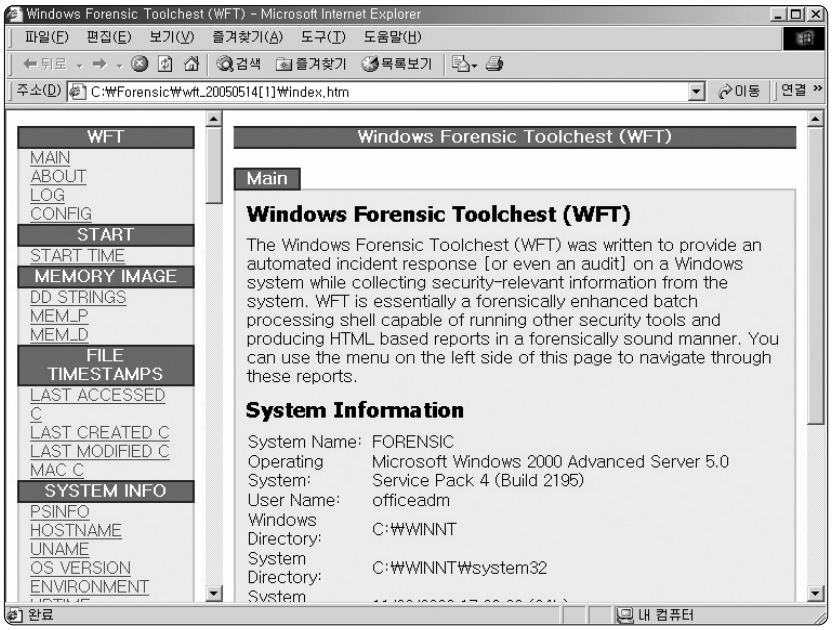
사. 자동화 도구

자동화된 스크립트의 사용 이외에도 윈도우 피해시스템 초기 분석을 위해 앞서 설명한 공개용 도구를 이용해 정보를 자동으로 수집해 주는 도구를 사용할 수 있다. 그중에서도 수집된 정보를 아래 그림처럼 브라우저로 확인할 수 있는 기능을 제공하는 WFT(Windows Forensic Toolchest) 사용을 추천한다. 사용방법은 다음과 같다.

- 먼저 WFT와 분석에 필요한 명령어들을 다운받는다.
- 명령어 "wft.exe"를 실행한다.
- 시스템에 따라 5분 정도 기다리면 index.html 파일이 생성된다.
- index.html 파일을 열어 관련정보를 확인한다.

※ dd 명령어를 수행하다 프로그램이 끝나는 경우가 발생할 수 있으므로 관련 실행 부분을 wft.cfg 파일에서 주석 처리해 준다. 또한 hfind, streams 명령어 수행시간이 상당히 길어질 수 있기 때문에 이 부분도 주석 처리하길 권장한다.

- 다운로드 : http://www.foolmoon.net/security/



〈그림 3-6〉 WFT 실행 화면

WFT 도구에서 사용한 명령어는 다음과 같다.

arp.exe	hunt.exe	ntlast.exe	reg.exe
attrib.exe	ipconfig.exe	openports.exe	regdmp.exe
auditpol.exe	iplist.exe	pclip.exe	RootkitRevealer.exe
autorunsc.exe	ipxroute.exe	promiscdetect.exe	route.exe
cmd.exe	listdlls.exe	ps.exe	sc.exe
cmdline.exe	mac.exe	psfile.exe	servicelist.exe
dd.exe	mdmchk.exe	psinfo.exe	sniffer.exe
drivers.exe	mem.exe	pslist.exe	streams.exe
dumpel.exe	nbtstat.exe	psloggedon.exe	strings.exe
efsinfo.exe	net.exe	psloglist.exe	tlist.exe
fport.exe	netstat.exe	psservice.exe	uname.exe
handle.exe	netusers.exe	pstat.exe	uptime.exe
hfind.exe	now.exe	psuptime.exe	whoami.exe
hostname.exe	ntfsinfo.exe	pulist.exe	

– 기타 도구

WFT외 공개된 자동화 도구는 다음과 같다.

• Biatchux(F.I.R.E)
http://biatchux.dmzs.com/

• IRCR(Incident Response Collection Report)
http://packetstormsecurity/Win/IRCR.zip

2. 루트킷 점검

루트킷(RootKit)이란 “시스템에 탐지되지 않도록 하는 코드, 프로그램의 집합”, “시스템 관리자 권한을 획득하기 위한 프로그램”이라 할 수 있다. 최근 윈도우 해킹동향은 공격에 성공한 후 시스템에 다운로드 된 악성프로그램(Bot, 백도어 등)파일 및 실행된 악성 네트워크, 프로세스 정보를 숨기기 위해 루트킷을 연동하고 있다.

가. 루트킷 기능

대부분의 루트킷은 사용자 모드와 커널 모드의 루트킷으로 구분할 수 있다. 사용자 모드는 파일 교체 즉 특정 프로세스에 사용한 DLL 파일들을 교체하거나 IAT(Import Address Table) 후킹, API 엔트리 패치 방법들을 사용해서 원하는 정보를 숨기는 루트킷들이다. 하지만 커널 모드 루트킷은 윈도우 운영체제 레벨인 윈도우 Native API(ntdll.dll, Kernel32.dll, User32.dll 등) 커널 드라이브와 Win32 응용프로그램 간의 데이터를 조작함으로써 공격자의 흔적을 감춘다.

이러한 루트킷들의 기능은 다음과 같다.

- 프로세스/스레드 감추기
- 프로세스 보안설정 변경 및 제거
- 파일/폴더 감추기
- 레지스트리/서비스 감추기
- 네트워크 정보 감추기
- 스니핑 및 시스템 제어

현재까지 외부에 공개된 루트킷들은 다음과 같으며 최근 피해시스템에서 발견된 것들은 대부분 아래 루르킷들의 변종이라 볼 수 있다.

〈표 3-1〉 윈도우 루트킷 종류

루트킷 명	특 징
Hacker Defender	현재 가장 광범위하게 사용되며 다양한 변종이 존재 프로세스, 네트워크, 시작프로그램, 레지스트리, 서비스 등을 숨기는 가장 많은 기능을 제공하고 있다.
FU	"EPROCESS"의 링크 조작을 통한 프로세스 숨기는 기능 제공
Vanquish	DLL 인젝션 기법을 사용한 루트킷 프로세스, 네트워크, 레지스트리, 서비스를 숨기는 기능 및 로그인 정보 또한 기록할 수 있는 기능 제공
AFX rootkit	코드 인젝션과 API 후킹을 사용하는 루트킷 으로 프로세스, 모듈, 핸들, 파일, 포트, 레지스트리 등을 숨길 수 있는 기능 제공
NT Rootkit	초기 윈도우즈 루트킷으로 현재까지 업데이트가 없는 상태이다.

나. 루트킷 탐지

루트킷을 탐지하기 위한 방법으로 시스템에 설치되어 있는 안티바이러스 프로그램을 이용할 수도 있겠지만 커널 레벨 까지 검사를 하는 프로그램은 극히 드물다. 또한 루트킷은 악성 프로그램이나 공격자의 흔적을 숨기고 있으므로 이러한 숨겨진 정보를 통해 중요한 정보들을 찾아낼 수 있으므로 반드시 전문 프로그램을 활용해야 한다.

아래 표는 루트킷 탐지 전문 프로그램의 기능을 분석한 표로써 분석자에게 적절한 프로그램을 찾아서 분석하면 된다.

〈표 3-2〉 루트킷 탐지 프로그램 종류 및 기능 분석

기 능	Procexp	Rootkit Revelear	BlackLight	Gmer	Anti-Rootkit	IceWord	Archon
숨겨진 프로세스	X	X	O	O	O	O	O
숨겨진 프로세스 (FU Rootkit)	X	X	O	O	O	O	O
숨겨진 레지스트리	X	O	O	O	O	O	O
숨겨진 파일	X	O	O	O	O	O	O
DLL Injection	X	X	X	X	X	X	O
모듈 점검	X	X	X	O	X	O	O
시스템콜 후킹	X	X	X	O	X	O	O
API 후킹	X	X	X	X	X	X	O

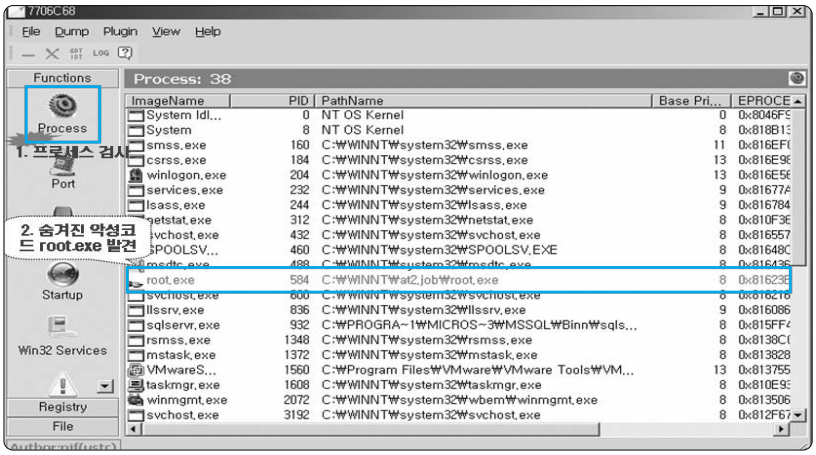
다. IceSw●rd 도구를 사용한 탐지

IceSword는 개인이 개발한 프리웨어 도구로 기능이나 사용자를 위한 인터페이스 측면에서 가장 쉽게 사용할 수 있게 구현되어 있다.

• 다운로드 : http://www.blogcn.com/user17/pjf/index.html

- 프로세스 검사

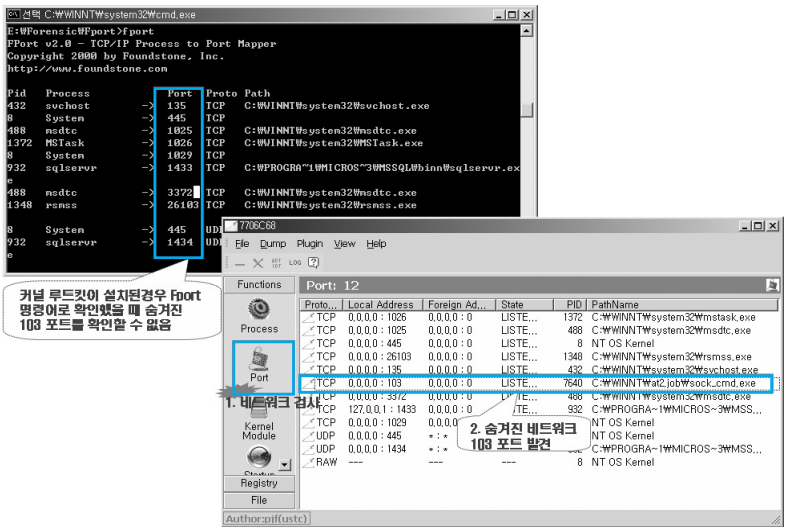
아래 그림을 보면 실제 피해시스템에서 숨겨진 프로세스를 찾은 화면이다. 숨겨진 root.exe의 실행경로를 통해 악성프로그램들의 홈 디렉터리인 "c:\winnt\at2.job\"을 확인할 수 있다. 이 디렉터리는 루트킷에 의해 숨겨져 있으므로 IceSword 도구의 "File"을 통해 확인해야 한다.



〈그림 3-7〉 IceSw●rd를 통한 프로세스 정보 확인 화면

– 네트워크 점검

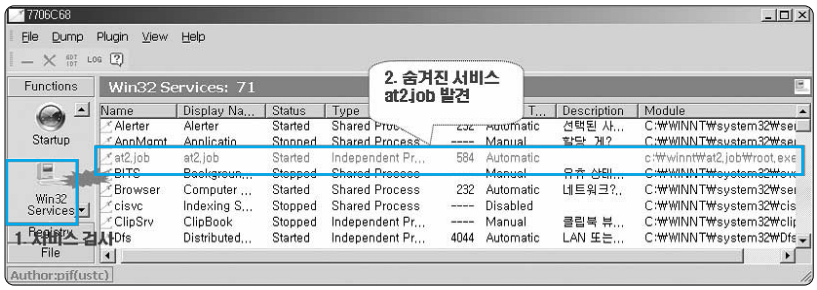
다음 그림은 fport 명령어를 통해선 103번 포트의 백도어를 확인할 수 없지만 IceSword 네트워크 정보를 확인하면 루트킷에 숨겨진 백도어 포트를 확인할 수 있다.



〈그림 3-8〉 숨겨진 백도어 포트 검출 화면

– 서비스 점검

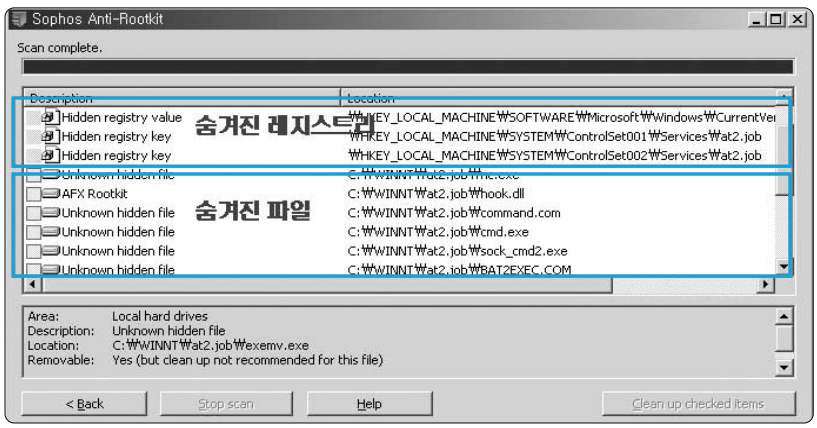
대부분의 커널 루트킷들은 서비스로 모듈을 로딩하게 되므로 루트킷을 실행하는 서비스를 숨기게 된다. 아래 그림은 루트킷에 의해 숨겨졌던 서비스를 검출한 화면이다. 이 서비스를 Disable로 하고 Stop으로 상태를 변경해서 시스템을 재부팅하면 루트킷이 실행되는 것을 막을 수 있다.



〈그림 3-9〉 숨겨진 서비스 검출 화면

– 숨겨진 레지스트리/파일 검사

IceSword로 숨겨진 레지스트리를 찾을 경우 수동으로 점검해야 하는 불편함이 있으므로 루트킷에 의해 숨겨진 파일과 레지스트리를 자동으로 찾아서 검출해 주는 "Anti-Rootkit" 도구로 확인할 수 있다.



〈그림 3-10〉 Anti-R●●tkit의 사용 예

3. 상세분석

가. 레지스트리 분석

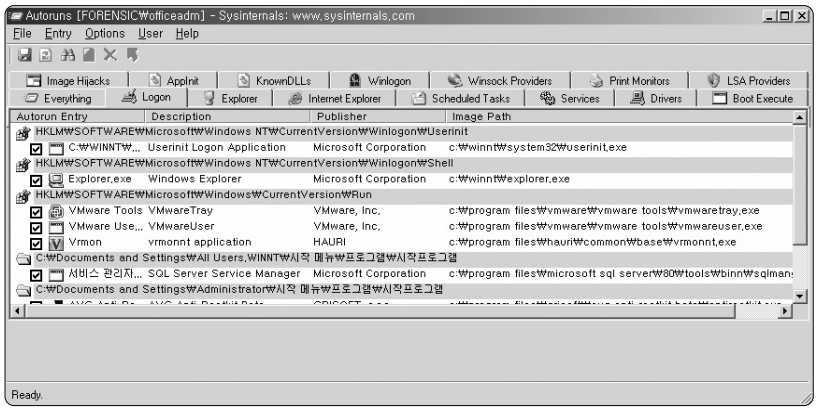
윈도우 레지스트리는 시스템이 운영되는데 필요한 정보를 담고 있다. 설치된 소프트웨어 정보부터 환경설정, 임시 저장값까지 시스템에 거의 모든 정보를 담고 있으므로 사고분석에 있어 공격자의 중요한 흔적을 찾을 수 있다.

– 시작 프로그램

아래 레지스트리 목록은 윈도우 시작 시 자동으로 실행하는 프로그램을 등록하는 레지스트리들이다. 공격자들은 악성프로그램을 등록하여 시스템 재부팅 시 자동으로 실행되도록 하므로 자세한 분석이 필요하다.

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
HKLM\Software\Microsoft\Windows\CurrentVersion\Windows\Load
HKLM\Software\Microsoft\Windows\CurrentVersion\Windows\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\Userinit
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
```

윈도우 시작과 관련된 레지스트리 정보는 sysinternals에서 제공하는 Autoruns 프로그램을 통해 아래와 같이 확인할 수 있다.

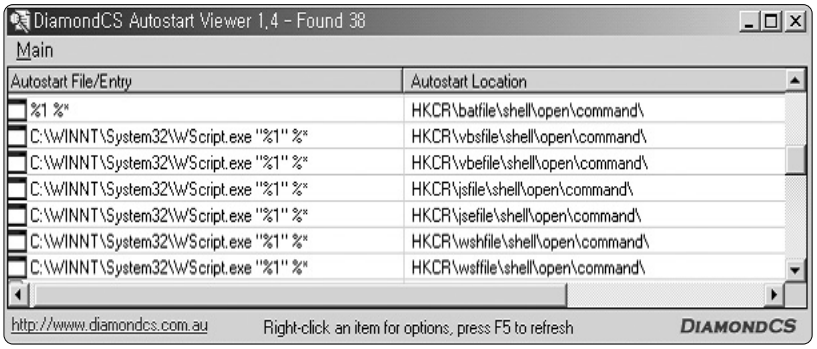


〈그림 3-11〉 Aut●runs를 이용하여 시작 레지스트리 점검 화면

아래 레지스트리 키들은 디폴트로 %1%* 값을 갖는데 이들을 "server.exe %1%*"로 변경할 경우 exe, com, bat, hta, pif 파일들의 실행 시 매번 server.exe 파일을 자동으로 실행되도록 할 수 있다.

```
[HKEY_CLASSES_ROOT\exefile\shell\open\command] @=""%1" %*"
[HKEY_CLASSES_ROOT\comfile\shell\open\command] @=""%1" %*"
[HKEY_CLASSES_ROOT\batfile\shell\open\command] @=""%1" %*"
[HKEY_CLASSES_ROOT\htafile\Shell\Open\Command] @=""%1" %*"
[HKEY_CLASSES_ROOT\piffile\shell\open\command] @=""%1" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\ open\command] @=""%1" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\ open\command] @=""%1" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\ open\command] @=""%1" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\htafile\Shell\ Open\Command] @=""%1" %*"
[HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\ open\command] @=""%1" %*"
```

위와 같은 레지스트리들은 'http://www.diamondcs.com.au'에서 제공하는 "Autostart Viewer"를 통해 확인할 수 있다.



〈그림 3-12〉 Autostart Viewer 실행 화면

– 공격자가 남긴 레지스트리 정보 수집

- 최근 사용한 문서 목록
  HKCU\Software\Microsft\windows\CurrentVersion\Explorer\Recentdocs
- 터미널 서비스 접속 목록
  HKCU\Software\Microsft\Terminal server Client\Default
- 설치된 소프트웨어 목록
  HKCU\Software\
- 열어본 파일 목록
  HKCU\Software\Microsft\windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

나. 자동실행 점검

– 서비스 점검

공격자는 윈도우 서비스에 자신의 악성프로그램을 등록 시켜 시스템이 재부팅 되더라도 해당 서비스 (등록된 악성프로그램)을 자동으로 재시작할 수 있다. 이러한 방법은 대부분의 공격자들이나 악성프로그램들이 행하고 있는 유형이기 때문에 분석자는 반드시 서비스를 점검할 필요가 있다.

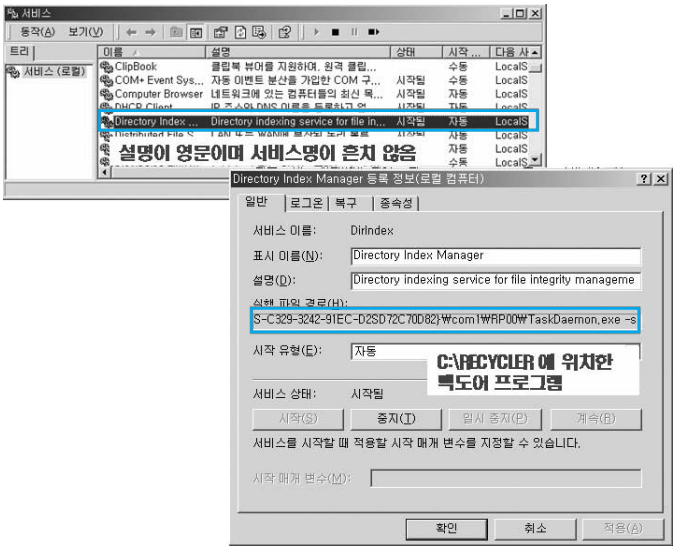
악성 프로그램을 실행하는 서비스를 예상할 수 있는 방법은 다음과 같다.

- 생소한 이름의 서비스
- "Description" 내용이 비어있는 서비스
- "Description" 내용이 영문인 서비스

하지만 대부분의 공격자 프로그램이 정상적인 서비스 이름으로 가장하고 있기 때문에 찾기 쉽지는 않지만, 현재 시작된 서비스 항목이 어떤 것이며 실행파일 경로가 올바른지 확인해야 한다. 다음은 악성프로그램이 관리자가 혼동하도록 주로 사용하는 서비스명이며 실제 서비스명과 유사하다.

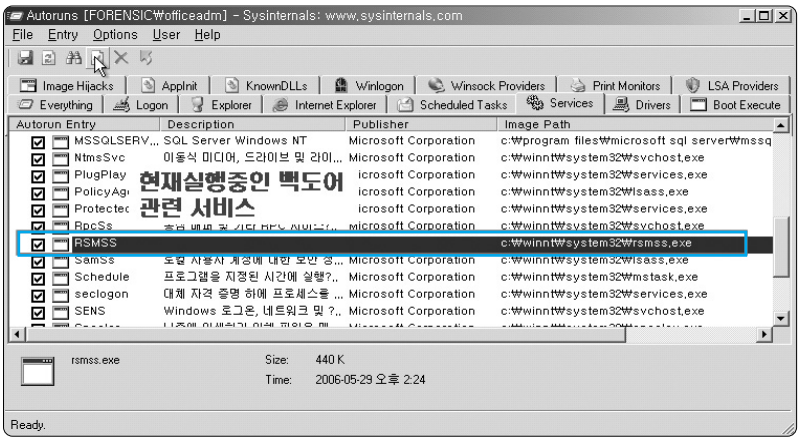
- Backup System
- Remote Administrator Service
- System Spooler Host
- Windows Management Drivers
- Universal Serial Bus Control Components

다음 그림은 공격자에 의해 등록된 서비스를 시스템에서 제공하는 "관리도구-서비스"에서 확인한 화면이다.



〈그림 3-13〉 수상한 서비스 검출 화면

Autoruns는 현재 구동중인 서비스와 실행된 프로그램을 한눈에 확인할 수 있는 기능을 제공하며 아래 그림은 "Services" 탭을 실행해 백도어 관련 서비스를 확인한 화면이다. 아래 백도어 관련 서비스는 설명 부분이 비어 있어 쉽게 찾을 수 있다.

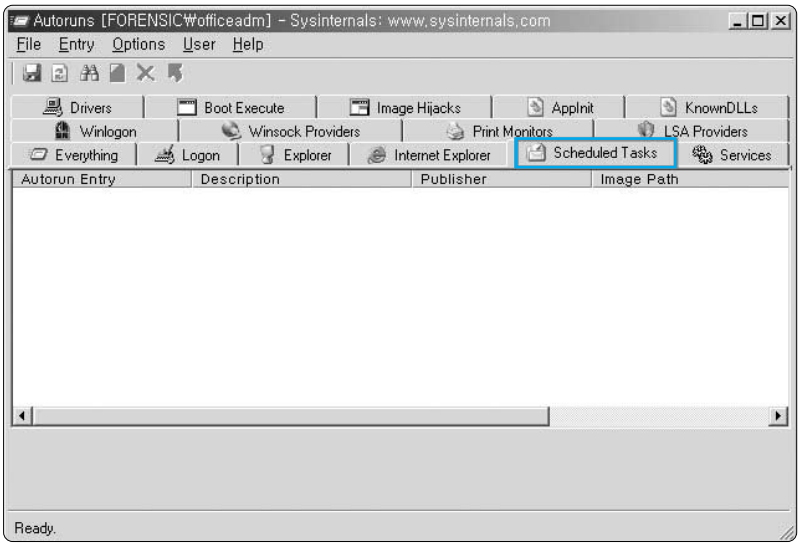


〈그림 3-14〉 Autoruns 도구를 이용하여 수상한 서비스 검출 화면

– 스케쥴된 작업 확인

시스템은 필요한 작업을 원하는 시간에 예약할 수 있는 기능이 존재 한다. 공격자들은 이러한 기능을 이용해 시스템이 재부팅 되더라도 악성 프로그램이 시작될 수 있도록 할 수 있으므로 점검이 필요하다.

Autoruns의 Scheduled Tasks 기능을 통해 쉽게 확인할 수 있다.



〈그림 3-15〉 스케쥴된 작업 확인 화면

– 자동시작 폴더 점검

윈도우의 재시작 시 이 폴더 안에 있는 모든 프로그램들은 자동으로 실행된다. 윈도우에서 이러한 자동 시작 폴더는 다음과 같다.

- C:\Documents and Settings\Administrator\시작 메뉴\프로그램\시작프로그램
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders

Autoruns의 Logon 기능을 통해 쉽게 확인 가능하다.

- Winlogon Notification DLL

Winlogon Notification DLL은 NT 서비스에 비해 적은 코드만으로 구현이 가능하며 안전모드에서도 원하는 코드의 실행이 가능한 장점이 있다. Winlogon.exe에서 발생하는 이벤트 핸들러를 작성하여 Logon, Logoff, Startup, Shutdown, Startscreensaver, Stopscreensaver 등의 이벤트가 발생할 때마다 원하는 코드를 실행할 수가 있다. 관련 레지스트리는 다음과 같다.

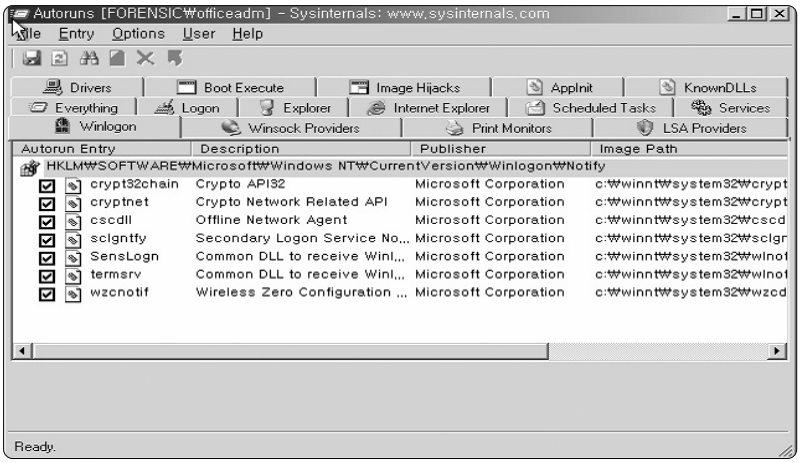
```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\
Winlogon\Notify\
```

※ Troj/Haxdoor-DI 악성프로그램 예

arprmdg0.dll에 의해 삽입된 코드를 동작시키기 위해 아래 레지스트리가 생성된다.

```
CurrentVersion\Winlogon\Notify\arprmdg0
DllName=arprmdg0.dll
Startup=arprmdg0
Impersonate=1
```

Autoruns의 Winlogon 기능을 통해 점검 할 수 있으며 설명부분이 비워져 있거나 생소한 이름의 dll이 실행되었는지 확인이 필요하다.

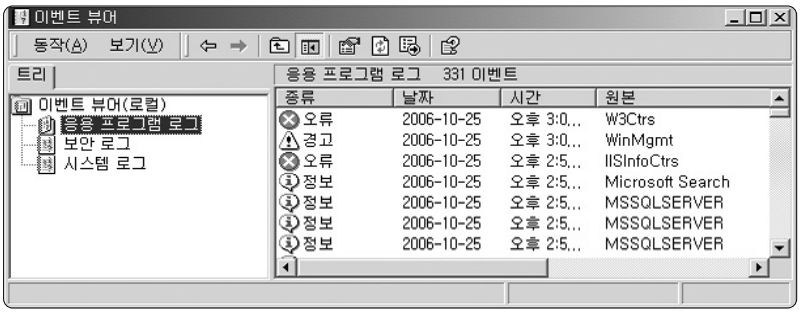


〈그림 3-16〉 Winlogon 확인 화면

다. 이벤트 로그분석

공격자의 흔적 및 활동 정보를 찾아내기 위해서는 로그분석이 필요하다. 윈도우 시스템에서는 하드웨어, 소프트웨어 및 시스템 문제를 이벤트로그에 저장하므로 이벤트 뷰어를 통해 확인이 필요하다.

- 관리도구 ⇨ 이벤트 뷰어
- 실행 ⇨ eventvwr.msc



〈그림 3-17〉 이벤트 뷰어 화면

하지만 공격자는 자신들의 흔적을 지우기 위해 'ClearEvent' 같은 프로그램들을 이용해 이벤트 로그를 모두 삭제할 수도 있기 때문에 만약 어떠한 로그도 남아있지 않다면 공격자가 흔적을 지운 것으로 이해해야 한다.

아래 표는 이벤트 점검 시 주의 깊게 살펴봐야 할 것들이다.

〈표 3-3〉 공격과 관련된 이벤트 로그

특 징	설 명	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

라. MAC time 분석

대부분의 파일시스템은 모든 디렉터리나 파일과 관련된 다음과 같은 시간 속성을 갖는다.

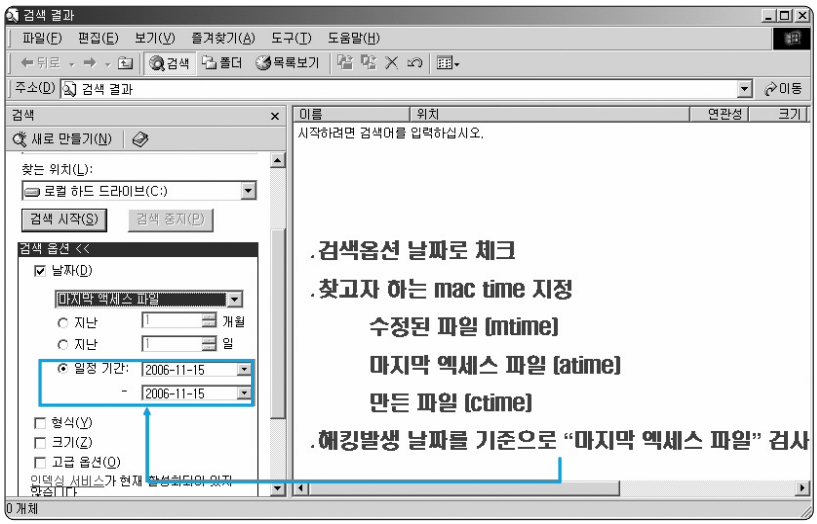
- mtime : 파일을 생성 및 최근 수정한 시간
- atime : 최근 파일을 읽거나 실행시킨 시간
- ctime : 파일 속성이 변경된 시간

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

- 해킹시점으로 mtime, atime 검색
- 검출된 악성코드 mtime, atime 검색

위와 같은 정보로 검색 후 시간대를 중심으로 정렬해서 시간 흐름에 따라 어떠한 파일이 생성, 수정, 실행됐는지를 분석해야 한다. mac time은 윈도우즈 기능 중 "파일 및 폴더 찾기" 기능을 통해 확인할 수 있고 점검 방법은 아래 그림과 같다.

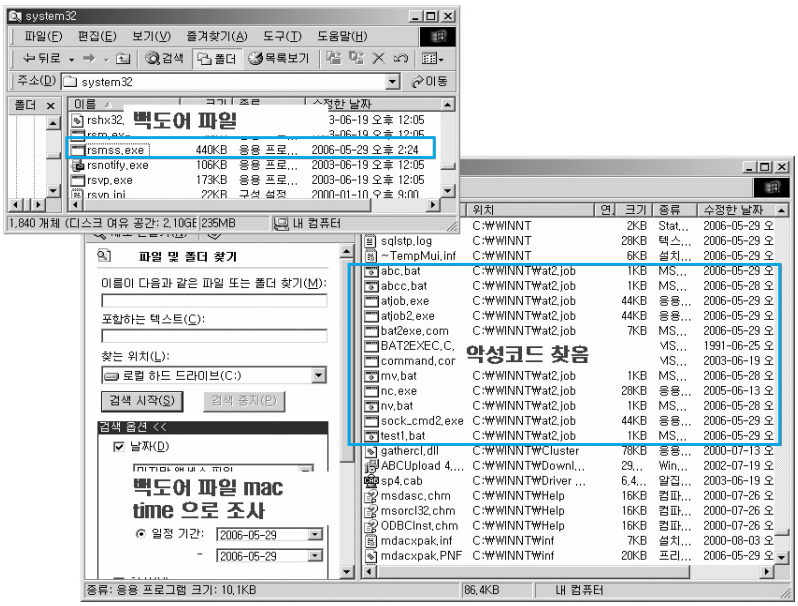
- 위치 : 시작 – 검색 – 파일 및 폴더 – 검색옵션 – 날짜



〈그림 3-18〉 윈도우즈 파일 mac time 분석 방법

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

아래 그림은 발견된 백도어파일 rsmss.exe의 mtime을 통해 윈도우-파일찾기 기능에서 그때 실행됐던 파일들을 조사한 결과 악성프로그램들을 찾을 수 있었다.



〈그림 3-19〉 mac time을 이용 악성코드 찾는 화면

마. 침입방법 분석

공격자가 어떻게 시스템에 침입할 수 있었는지에 대한 분석 또한 피해시스템 분석에서 매우 중요하다. 관리자들은 이러한 해킹 원인분석을 하지 않고 사고에 따른 조치만 취하게 되면 이후에 또다시 같은 취약점으로 해킹을 당할 수 있기 때문에 원인 분석을 통해 반드시 패치를 수행해야 한다.

윈도우즈 서버에서 해킹사고가 발생할 수 있는 경우는 크게 다음과 같이 분류할 수 있다.

- 윈도우 취약점
  - 시스템 취약점 (보안 업데이트 미실시)
  - 패스워드 취약점
  - 잘못된 공유설정

- 웹 어플리케이션 취약점
  - SQL Injection
  - 파일업로드 등

- MS-SQL 취약점
  - 디폴트 패스워드 사용
  - 패치 미실시

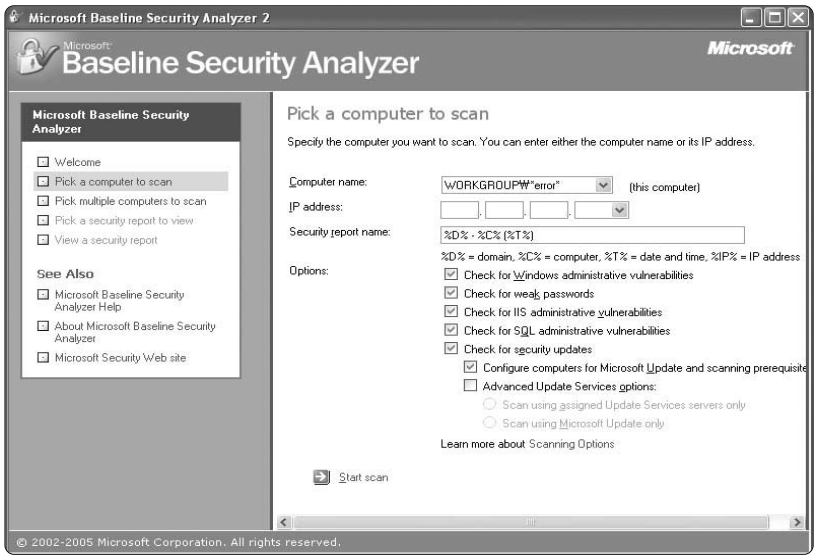
먼저 시스템에 어떤 어플리케이션이 운영 중인지 확인해야 한다. 하지만 대다수의 해킹 사고는 시스템 보안 업데이트 미 실시로 인한 윈도우 취약점이나 웹 서비스 공격을 통해 발생한다.

웹 서비스가 구동 중인 경우는 해킹 발생 시점에 발생한 로그 분석을 통해 공격 여부 및 방법을 대부분 확인할 수 있다.

- IIS 로그 위치 : C:\WINNT\system32\LogFiles\W3SVC1

윈도우 취약점의 경우는 최종 보안 업데이트 날짜를 파악 하는 게 중요하다. 최종 보안 업데이트 이후 발표됐던 취약점 중 리모트에서 공격 가능한 취약점이 있었는지 파악하고 관련 서비스가 오픈 되어 있는지 확인해야 한다.

Microsoft에서 제공하는 Microsoft Baseline Security Analyzer를 이용하여 보안 패치 상태, IIS, SQL 보안 상태를 점검할 수 있다.



〈그림 3-20〉 MBSA를 이용한 보안상태 확인

바. 인터넷 임시파일 분석

인터넷 익스플로러를 통해 특정 사이트에 접속하게 되면 관련 사이트의 페이지는 임시파일에 저장되며 접속한 흔적이 히스토리에 남으며 또한 사용되었던 쿠키도 디스크에 저장한다. 이러한 임시파일들을 통해 공격자가 방문한 특정 사이트들을 확인할 수 있다.

〈표 3-4〉 인터넷 임시파일 종류

종 류	위 치
임시 인터넷 객체	%SystemRoot%Downloaded ProgramFiles
임시 인터넷 파일	%USERPROFILE%Local Settings\Temporary Internet Files
열어본 페이지	%USERPROFILE%Local Settings\History
임시 쿠키 파일	%USERPROFILE%Local Settings\COOKIES