

작성자 : 기술지원부 조 태 준 tedcho@nextline.net

IceSword (숨겨진 프로세스 탐지 프로그램)

사용 방법

IceSword.exe의 functions의 기능 중 가장 많이 사용되는 process / port / win32 service 의 3개의 기능에 대하여 설명을 드리겠습니다.

IceSword.exe를 실행시키고 process, services, port, startup, kernel module 등의 항목에 붉게 표시된 것이 있는지 확인합니다.

Process / services 등의 항목에서 문제의 process와 service를 종료(terminate/stop)합니다.

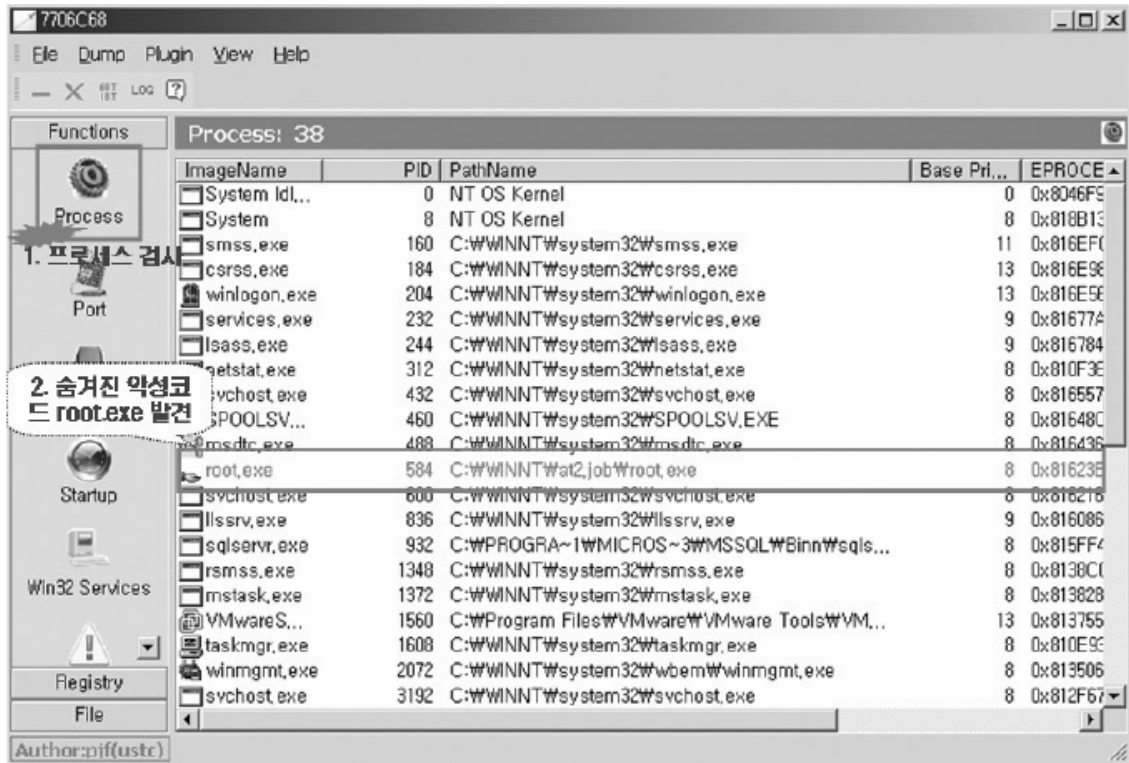
만약 문제되는 process가 explorer.exe, winlogon.exe, svchost.exe와 같은 윈도우의 정상 프로세스라면 dll injection을 의심해 보아야 합니다. IsHelf.exe로 문제를 야기한 dll을 확인한 후 (sysinternals의 process explorer로도 제조사, 버전 등의 파일특성을 통해 확인이 가능) process explorer로 해당 프로세스를 정지(suspend)시킨 후 IceSword.exe로 해당 dll을 프로세스에서 제거(unload)합니다. 그 후에 IceSword.exe의 file 항목에서 찾아 직접 삭제합니다. 정지시킨 프로세스는 process explorer로 다시시작 resume)합니다. (유감스럽게도 process explorer에는 프로세스를 정지시키는 기능은 있지만 dll을 프로세스에서 제거하는 기능은 없고, IceSword.exe는 그 반대입니다.)

문제되는 윈도우의 정상프로세스가 2개 이상이라면 프로세스가 서로 연동되어 있을 수 있으므로 해당 프로세스를 모두 정지시킨 후 위 설명에 따릅니다.

IceSword.exe의 file과 registry 항목에서 확인된 파일과 레지스트리를 찾아 직접 삭제 (오른쪽 마우스 클릭)합니다

1. 프로세스 검사

아래 그림을 보면 실제 피해시스템에서 숨겨진 프로세스를 찾은 화면 입니다. 숨겨진 root.exe 의 실행경로를 통해 악성프로그램들의 홈디렉터리인 “c:\Wwinnt\Wat2.job\” 을 확인할수 있습니다. 이 디렉터리는 루트킷에 의해 숨겨져 있으므로 IceSword도구의 “File” 을 통해 확인해야 합니다.



2. 네트워크 점검

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

Kernel 루트킷에 설치된 경우 fport 명령어로 확인했을 때 숨겨진 103 포트를 확인할 수 없음

| Pid | Process | Port | Proto | Path |
|------|----------|-------|-------|--|
| 432 | svchost | 135 | TCP | C:\WINNT\system32\svchost.exe |
| 8 | System | 445 | TCP | |
| 488 | msdtc | 1025 | TCP | C:\WINNT\system32\msdtc.exe |
| 1372 | MS Task | 1026 | TCP | C:\WINNT\system32\MSTask.exe |
| 8 | System | 1029 | TCP | |
| 932 | sqlservr | 1433 | TCP | C:\PROGRA~1\MICROS~3\MSSQL~3\Binn\sqlservr.exe |
| 488 | msdtc | 3372 | TCP | C:\WINNT\system32\msdtc.exe |
| 1348 | rsms | 26103 | TCP | C:\WINNT\system32\rsms.exe |
| 8 | System | 445 | UDP | |
| 932 | sqlservr | 1434 | UDP | |

| Proto | Local Address | Foreign Ad... | State | PID | PathName |
|-------|----------------|---------------|----------|------|--|
| TCP | 0.0.0.0:1025 | 0.0.0.0:0 | LISTE... | 488 | C:\WINNT\system32\msdtc.exe |
| TCP | 0.0.0.0:1026 | 0.0.0.0:0 | LISTE... | 1372 | C:\WINNT\system32\MSTask.exe |
| TCP | 0.0.0.0:445 | 0.0.0.0:0 | LISTE... | 8 | NT OS Kernel |
| TCP | 0.0.0.0:26103 | 0.0.0.0:0 | LISTE... | 1348 | C:\WINNT\system32\rsms.exe |
| TCP | 0.0.0.0:135 | 0.0.0.0:0 | LISTE... | 432 | C:\WINNT\system32\svchost.exe |
| TCP | 0.0.0.0:103 | 0.0.0.0:0 | LISTE... | 7640 | C:\WINNT\at2job\at2jobcmd.exe |
| TCP | 0.0.0.0:3372 | 0.0.0.0:0 | LISTE... | 488 | C:\WINNT\system32\msdtc.exe |
| TCP | 127.0.0.1:1433 | 0.0.0.0:0 | LISTE... | 932 | C:\PROGRA~1\MICROS~3\MSSQL~3\Binn\sqlservr.exe |
| TCP | 0.0.0.0:1029 | 0.0.0.0:0 | LISTE... | 8 | NT OS Kernel |
| UDP | 0.0.0.0:445 | * | * | 8 | NT OS Kernel |
| UDP | 0.0.0.0:1434 | * | * | 932 | C:\PROGRA~1\MICROS~3\MSSQL~3\Binn\sqlservr.exe |
| RAW | --- | --- | --- | 8 | NT OS Kernel |

1. 네트워크 검사

2. 숨겨진 네트워크 103 포트 발견

3. 서비스 점검

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

2. 숨겨진 서비스 at2job 발견

| Name | Display Na... | Status | Type | T... | Description | Module |
|---------|----------------|---------|-------------------|------|-------------|--------------------------|
| Alerter | Alerter | Started | Shared Proc... | 232 | Automatic | 선택된 사... |
| AppMgmt | Applicatio... | Stopped | Shared Process | --- | Manual | 항당 계? |
| at2job | at2job | Started | Independent Pr... | 584 | Automatic | c:\winn\at2.job\root.exe |
| BITS | Backgroun... | Stopped | Shared Process | --- | Manual | 유휴 상태... |
| Browser | Computer ... | Started | Shared Process | 232 | Automatic | 네트워크?.. |
| clsv | Indexing S... | Stopped | Shared Process | --- | Disabled | |
| ClipSrv | ClipBook | Stopped | Independent Pr... | --- | Manual | 클립북 뷰... |
| Dfs | Distributed... | Started | Independent Pr... | 4044 | Automatic | LAN 또는... |

1. 서비스 검사