1. IceSword란? 루트킷 제거를 목적으로 만들어진 툴로서 북경 과학기술 대학교(USTC)의 pjf 출품작이기도 합니다. 중국어 버전과 영어버전을 제공하고 현재까지 나온버전은 1.22버전까지 있으며, 비스타용도 따로 존재 합니다 .제작자의 공식 블로그는 http://www.blogcn.com/user17/pjf/index.htm 이며, 다운로드가 가능합니다. 별도의 설치 없이 IceSword.exe를 실행하면 실행됩니다.

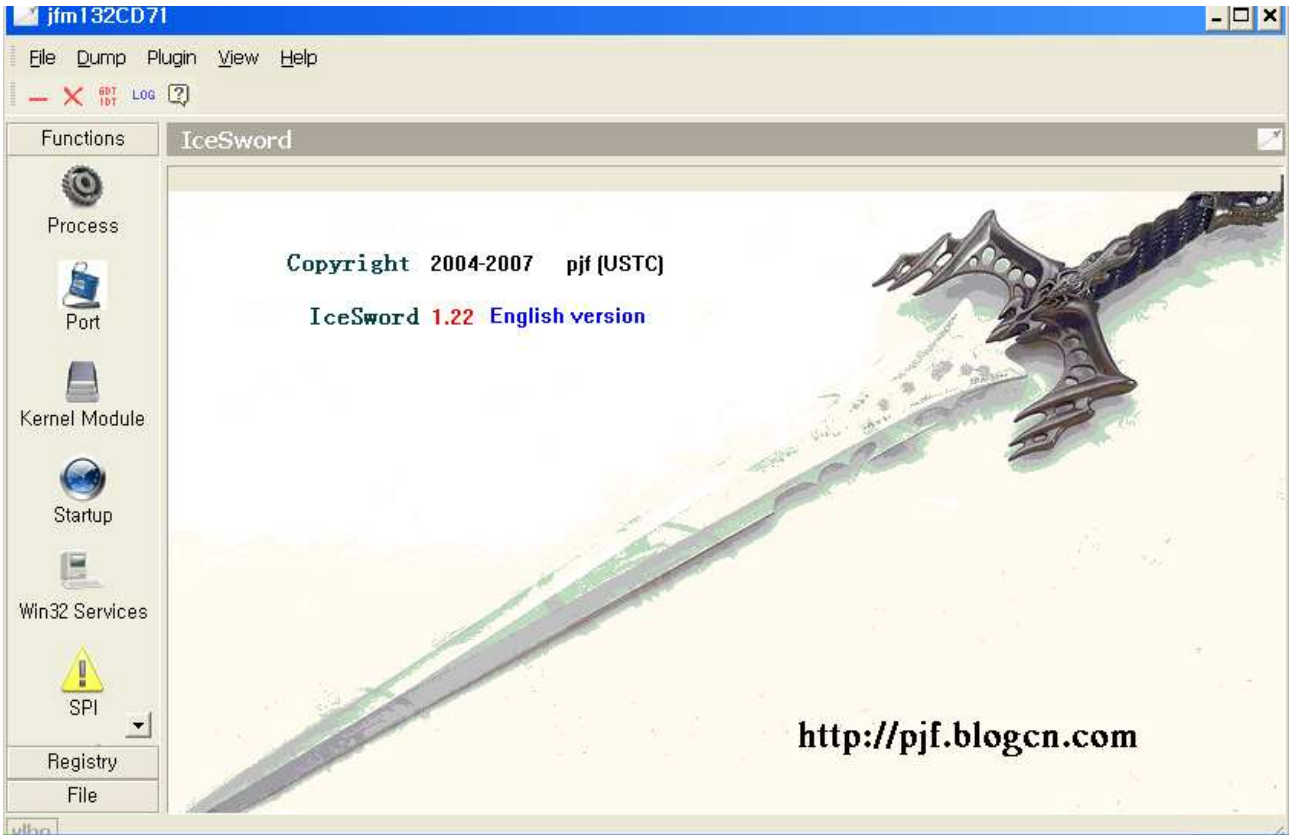


그림 1 프로그램의 초기 구동 화면

IceSword는 루트킷 시스템의 분석을 목적으로 만들어졌기에 타 업체에서 만든 루트킷과는 다른 성격을 가지고 있습니다. 다른 안티루트킷 제품이 주로 스캔하는 기능을 가지고 있지만, IceSword는 타 안티루트킷과는 달리 파일을 스캔하는 과정이 없습니다. 대신에 다양한 시스템 상태 보기를 제공함으로써 루트킷의 제거를 유도합니다. 물론 이걸 다 알고 처리하기 위해서는 많은 학습이 선행되어야 합니다. 그리고, 별도의 백업을 하는 방법이 존재하지 않기 때문에 특히 더 많은 주의가 필요합니다.

IceSword만의 특징으로는 대부분 process explorer (sysinternal.com에서 만든 리소스 관리 프로그램) 류의 툴은 모두 Windows의Toolhlp32, psapi, ZwQuerySystemInformation 등의 시스템 콜을 이용한 것입니다. ApiHook를 쓰면 쉽게 그것들을 제거 할 수 있으며 backdoor는 더욱 손쉽게 제거가 가능합니다. 대부분의 툴은 Kernel thread scheduling 구조로 프로세스들을 조회하는데 이런 방식은 버전별로 업그레이드를 해야 한다던 지 패치를 해야 하기 때문에 요즘 이렇게 찾는 방법을 변경할 것을 제안한 사람이 있습니다.

그러나 IceSword의 프로세스 조회 방법은 유일한 것이며 backdoor들이 할 수 있는 은폐기능에 대해서도 충분히 고려한 것이므로 현재 거의 모든 숨겨진 프로세스들을 찾아낼 수 있습니다.

기본적으로 사용자의 스레드 방식과 커널 스레드 방식이 있는데 IceSword 의 경우 독자적인 방식으로 조회를 합니다.

2. IceSword의 각 메뉴 설명

IceSword의 각 메뉴를 간략하게 설명하도록 하겠습니다.

2-1. Process

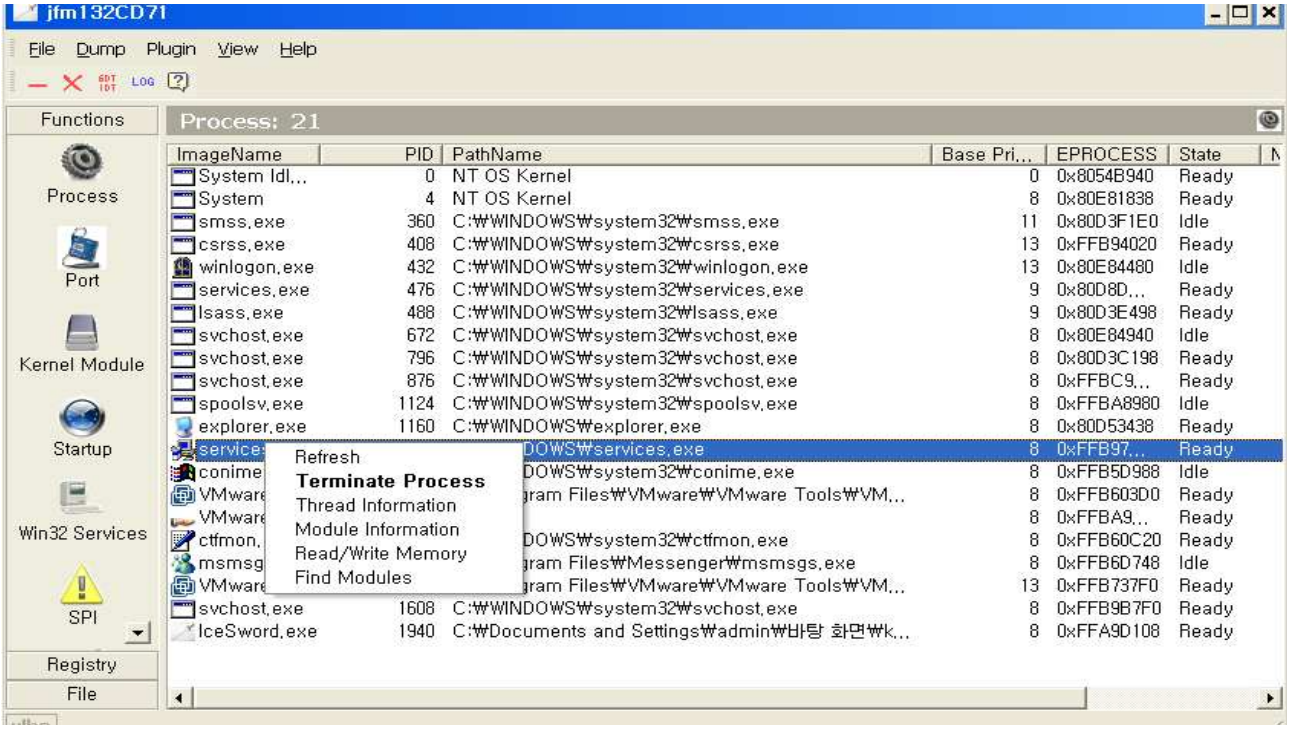


그림 2 Process메뉴를 선택한 모습

현재 실행 중인 프로세스 목록을 보여줍니다. 실행 중인 모든 프로세스를 보여주며, 장치관리자에서는 볼 수 없는 숨겨진 프로세스까지 보여줍니다. 대부분 루트킷이 실행된 경우, 작업관리자와 이 목록을 비교하여 쉽게 실행되고 있는 여부를 찾아낼 수 있습니다.

- Terminate Porcess : 프로세스를 강제로 제거합니다.
- Thread Information : 프로세스의 Thread정보를 표시합니다.

그림 3 Thread 정보 창

- Module Information : 프로세스의 Module정보를 표시합니다.

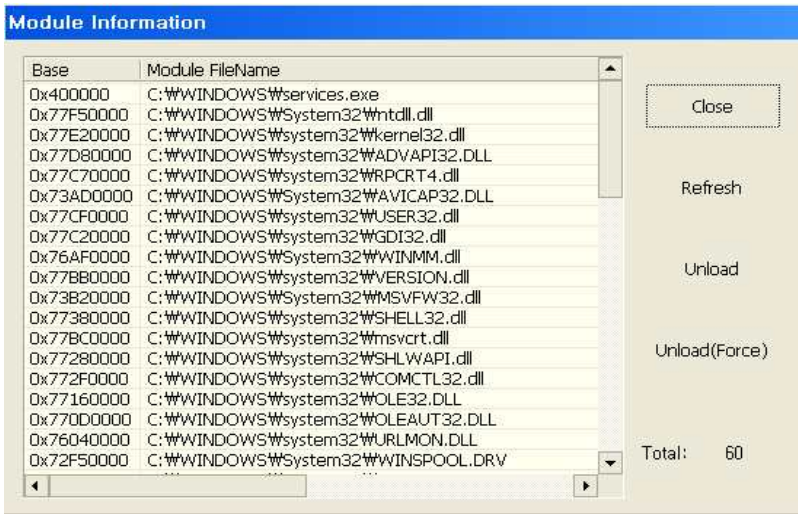


그림 4 Module 정보 창

- Read/Write Memory : 프로세스의 읽기/쓰기 메모리를 표시합니다.

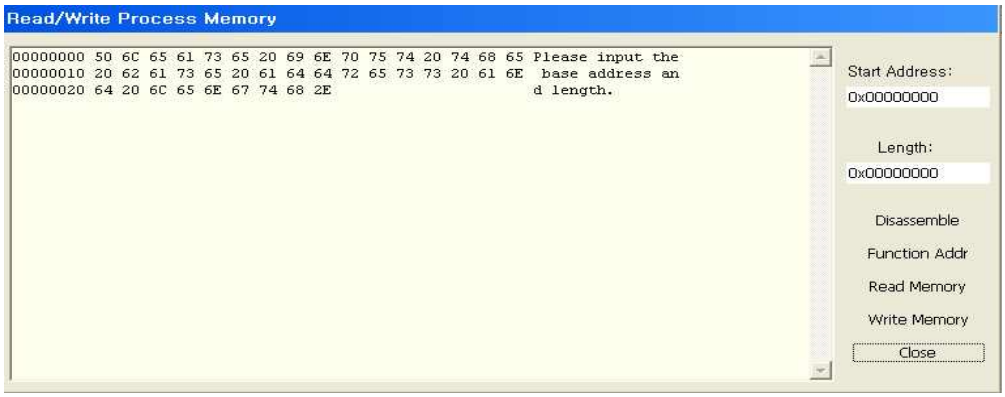


그림 5 Read/Write Memory 정보 창

- Find Module : 문자열을 입력해 모듈을 검색합니다.

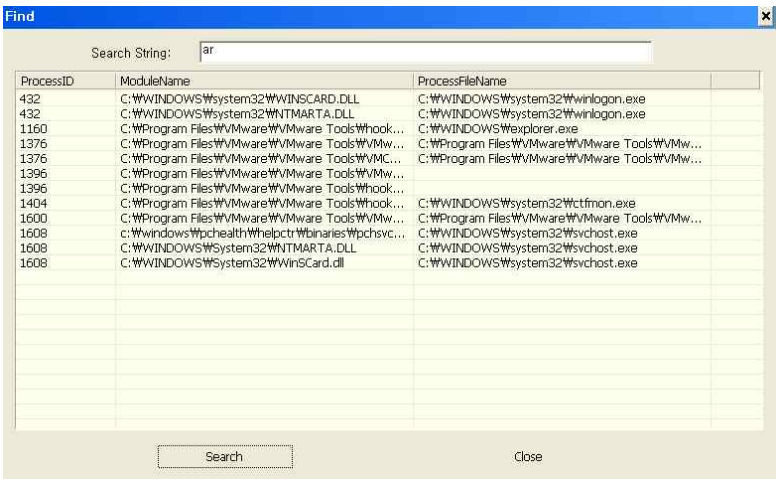


그림 6 ar이라는 문자열로 검색한 결과

2-2. Port

네트워크의 접근 현황을 보여줍니다. 내 컴퓨터와 원격지에 연결된 상태를 보여주며, 연결된 경우 해당 프로세스를 보여주지는 않지만 PID를 통해 Process에서 해당 프로세스를 찾을 수 있습니다. 기본적으로 허용한 포트가 아니라면, 이를 통해 어느 위치에 있는지 찾아 낼 수 있습니다.

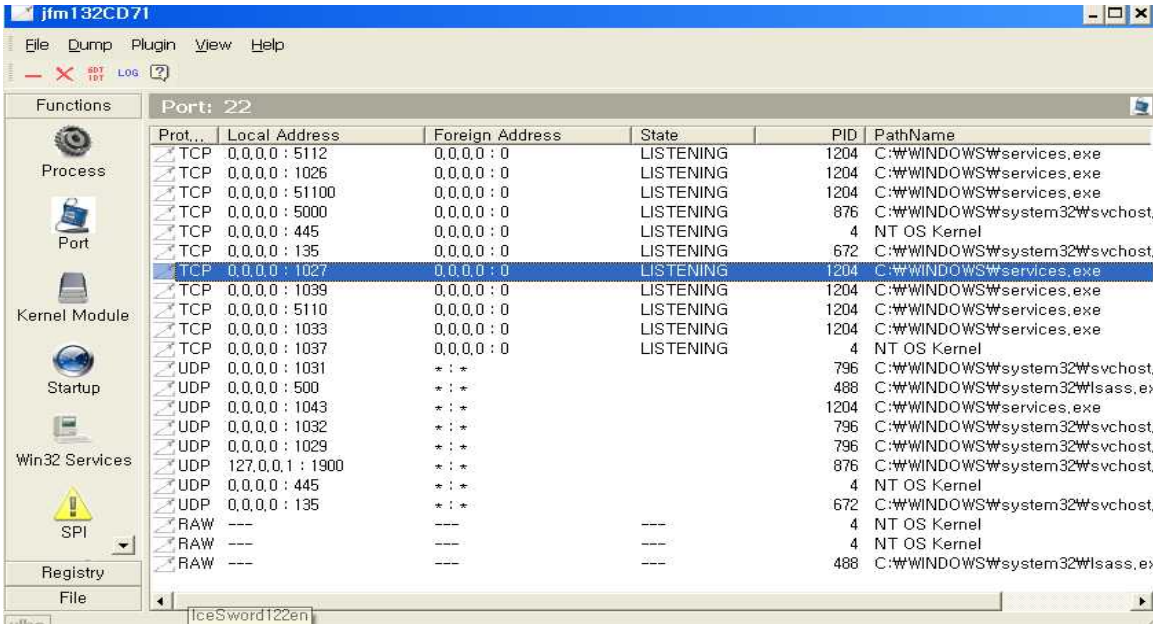


그림 7 Port 화면

2-3. Kernel Module

실행 파일에 의해 로드된 시스템 파일(.SYS)이나 동적 라이브러리 파일(.DLL)의 목록을 보여줍니다. 대부분의 루트킷은 자신을 은폐하기 위해 SYS나 DLL파일을 몇 개 심는데, 그 목록을 볼 수 있게 해줍니다. 다만, 여기에 있는 파일이 정상적인지 여부를 따지지 않고 강제로 내리는 경우 시스템이 바로 블루스크린을 보여주게 되며, 심각한 경우 다시 부팅이 이뤄지지 않을 수도 있습니다.

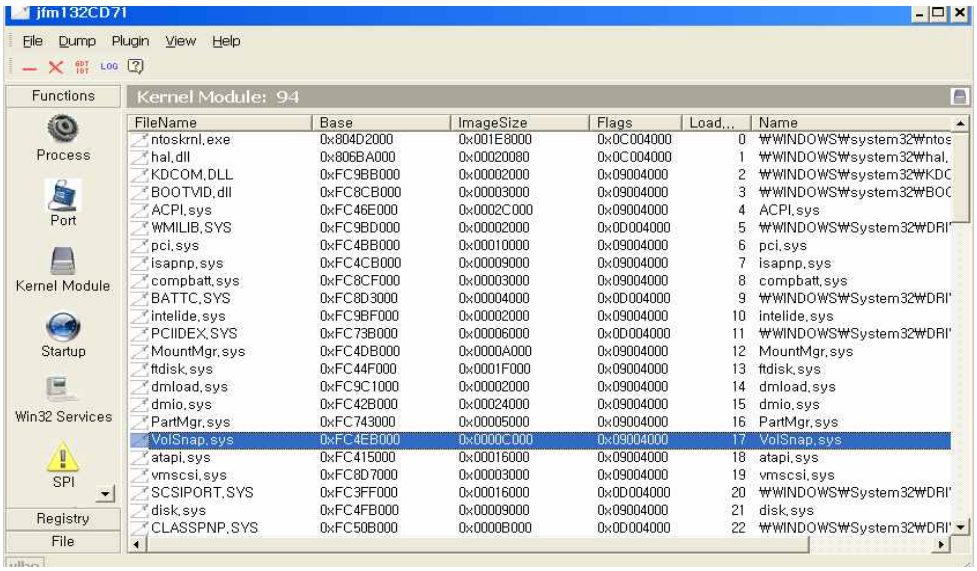


그림 8 Kernel Module화면

2-4. Startup

실행 파일에 있는 목록을 보여줍니다. 시작 지점에 있는 레지스트리의 목록을 정리해주는 것으로 로그온 시 시작되는 레지스트리의 위치를 모두 알고 있다면, 이 목록을 구태여 사용할 필요는 없습니다. 삭제기능이 없으며 검사밖에 할 수 없습니다.

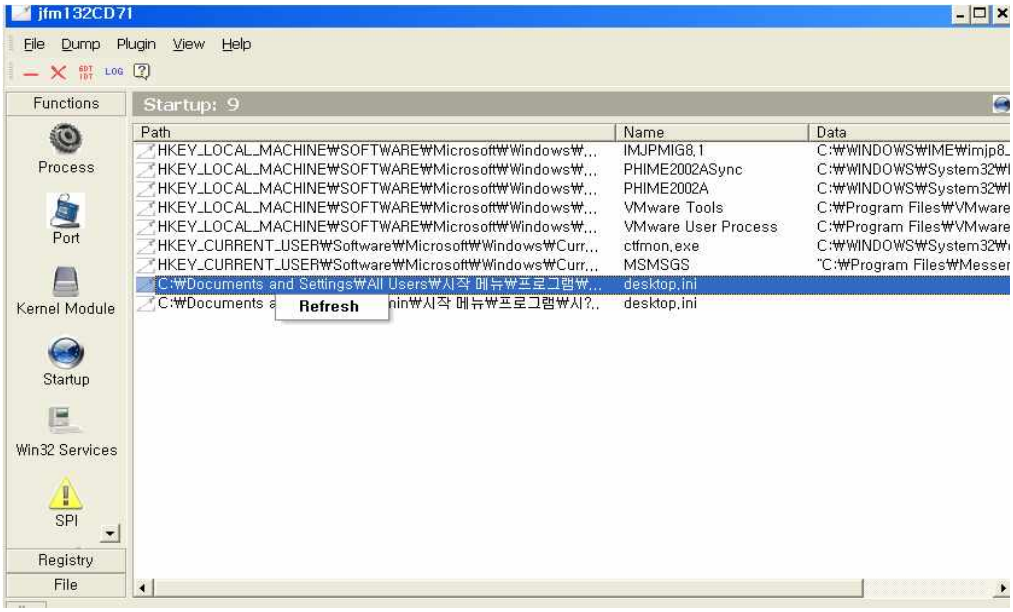


그림 9 Startup 화면

2-5. Win32 Services

서비스로 실행되는 프로세스 목록을 보여줍니다. 유명한 루트킷의 경우에는 IceSword가 자동으로 빨간색으로 강조해줍니다만, 일부 루트킷의 경우는 일반적인 검은 색 글씨로 보여 구분지을 수 있습니다. 또 한, 시스템중의 숨겨졌거나 혹은 숨겨져 있지 않는 서비스를 검사 하는데 숨겨져 있는 서비스는 빨간색으로 나타내며, 서비스에 대한 부팅, 정지, 사용금지 등을 제공합니다.

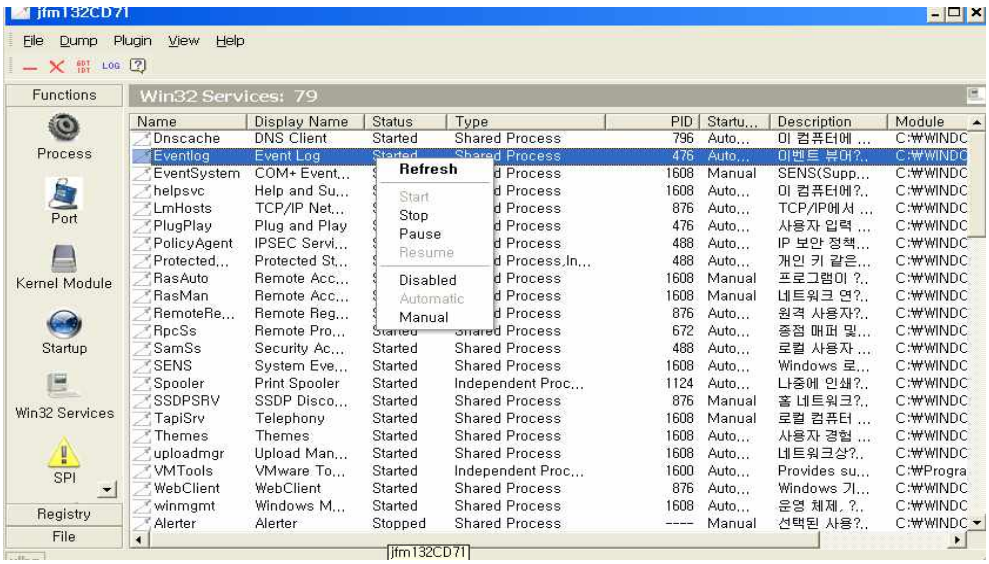


그림 10 개체를 선택해 마우스 오른쪽 버튼을 누른 화면

- Start : 선택한 서비스를 사용을 시작합니다.
- Stop : 선택한 서비스를 사용을 정지합니다.
- Pause : 선택한 서비스를 잠시 정지합니다.
- Resume : 잠시 정지된 서비스를 다시 시작합니다.
- Disable : 선택한 서비스의 사용을 금지합니다.
- Automatic : 선택한 서비스를 자동으로 시작하게 바꿉니다.
- Manual : 선택한 서비스를 수동으로 시작하게 바꿉니다.

2-6. SPI (Service Provider Interface)

SPI는 서비스 인터페이스를 제공합니다. 즉, 모든 Windows의 네트워크조작은 모두 이 인터페이스를 통하여 데이터 패킷을 받거나 보냅니다. 이를 통해 네트워크 드라이버에 로딩되거나 영향을 미치는 부분을 보여줍니다. 이러한 이유로 많은 악성프로그램들은 이 dll을 바꾸어버립니다. 이렇게 되면 사용자가 네트워크를 방문한 모든 패킷을 감시할 수 있으며 그것에 대하여 광고를 넣을 수 있게됩니다. 만약 분명하지 않은 상황에서 이, dll을 삭제하면 네트워크를 사용 할 수 없게 되어 인터넷에 접속할 수 없게 됩니다. 이와는 다르게 일부 루트킷의 경우 Winsock을 이용하여 특정 네트워크 패킷을 캡춰하는 기능을 갖고 있기 때문에 이에 대한 점검 방법으로 사용할 수 있습니다. ARP가 이상한 시스템의 경우 대부분 이 곳에 문제가 있는 시스템이 많습니다. 검사하는 기능밖에 제공하지 않기 때문에 직접 제거를 해야 합니다.

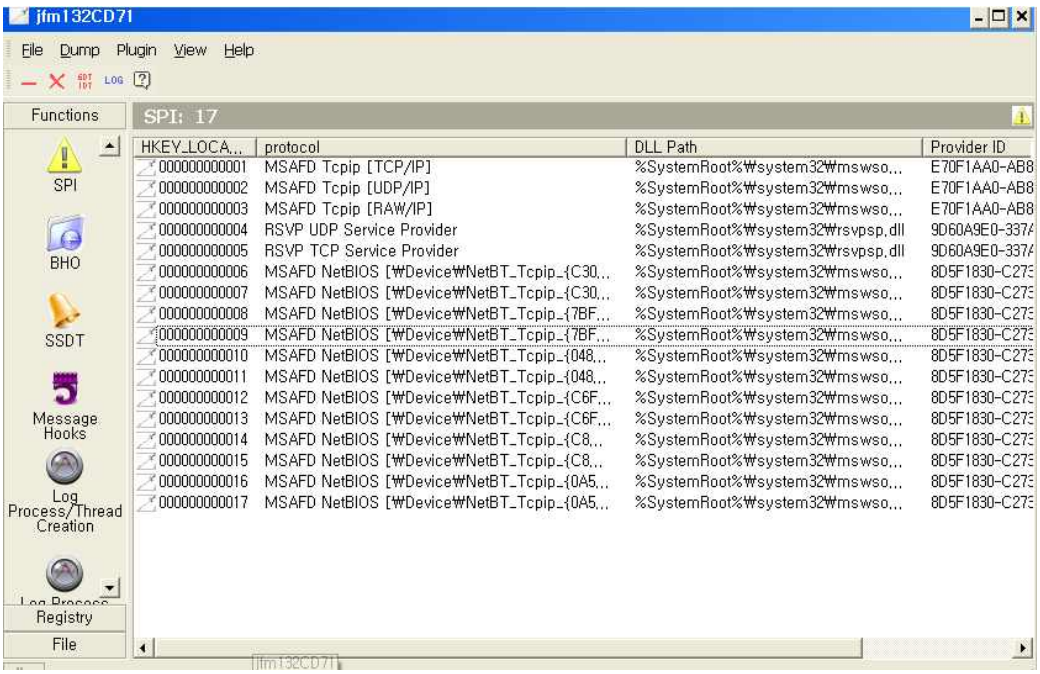


그림 11 SPI 화면

2-7. BHO (Browser Helper Object)

브라우저나 시스템의 쉘 실행시 로딩되는 DLL들의 목록입니다. 이 부분은 IceSword가 아닌 다른 툴로도 비슷한 결과를 얻을 수 있습니다. (예 : HijackThis, Autoruns) 검사하는 기능 밖에 제공하지 않으므로 직접 삭제해야 합니다.

2-8. SSDT (System Service Descriptor Table)

시스템의 메모리를 참고 할 수 있게끔 하는 부분입니다. 이미 다른 곳에서 결과를 얻을 수 있기 때문에, 자주 볼 필요는 없습니다만, 위에서 나열한 모든 기능으로 잡을 수 없는 경우 이곳에 실행 중인 메모리를 봄으로써 답을 찾을 수 있습니다.

보안 적인 측면으로 보면, SSDT상에서 컴퓨터 시스템의 서비스함수를 획득하기 위하여 kernel backdoor는 가능한 한 이 서비스리스트를 수정합니다. 특히 일부 오래된 rootkit, hook를 통하여 로그온리스트를 수정합니다. 수정된 값은 빨간색으로 나타내게 되는데 일분 보안프로그램도 빨간색으로 표시가 됩니다. 예를 들면 Regmon같은 프로그램이 빨간색으로 표시됩니다. 물론 일부 보안프로그램도 빨간색으로 표시가 됩니다.

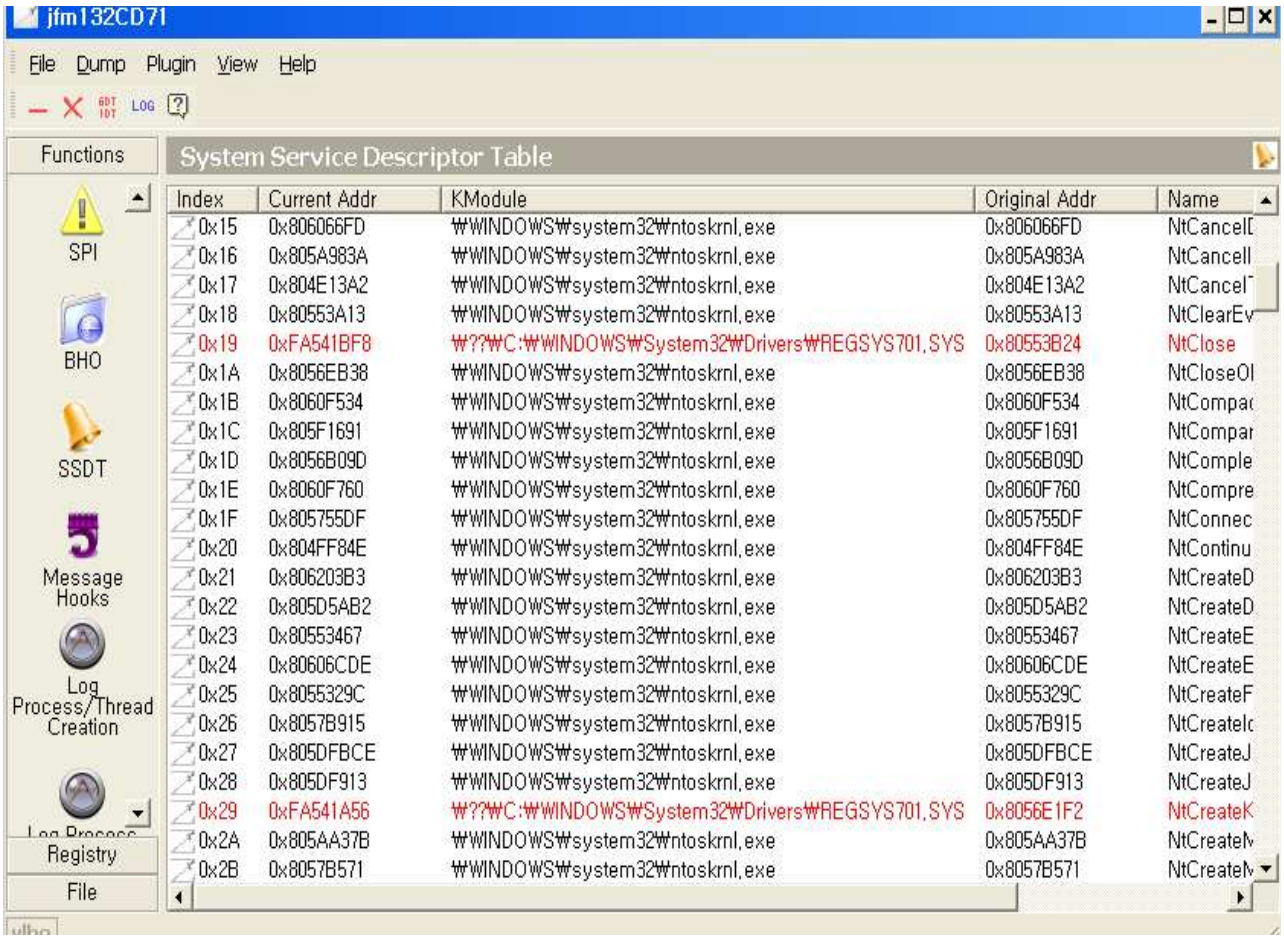


그림 12 SSDT 화면

2-9. Message Hooks

키보드 입력 값, 마우스 좌표 등이 필요한 경우 Win32 API를 호출하게 됩니다. 이를 이용해 프로그램 동작 시 입출력 장치의 반응을 보여줍니다. 어떤 프로그램들이 이를 이용하는지에 대한 값들이 표시가 되며 검사만 가능합니다. 키로거가 의심되는 경우 이곳에서 손쉽게 잡을 수 있습니다.

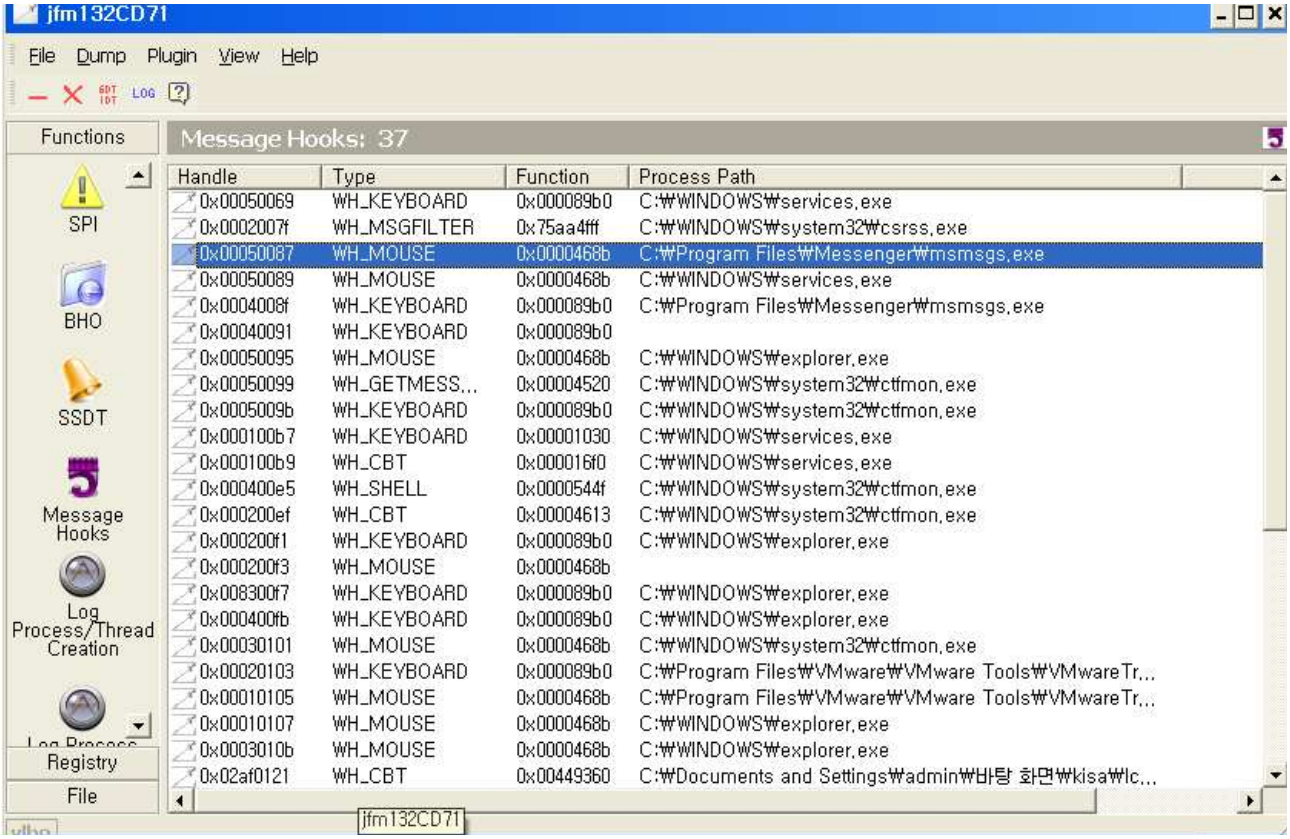


그림 13 Message Hooks 화면

2-10. Log Process/Thread Creation

어떤 프로세스가 어떤 것을 실행했는지를 보여주는 부분입니다. IceSwrod가 실행 중인 기간 동안 프로세스 Thread 생성을 기록 합니다. 주로 주기적인 프로그램이 돈다고 의심될 때 이 부분을 확인하면, 해결책이 나옵니다. 예를 들어 트로이목마는 바이러스 진행과정을 실행할 때, 백신프로그램이 같은 진행과정에 있는 가를 검사해본 뒤, 있다면 백신프로그램을 삭제합니다. 만약 IceSword가 실행되고 있다면 이런 과정들은 기록되어 어느 진행과정이 백신들을 지우는지 찾을 수 있습니다. 이를 이용해 트로이목마 혹은 바이러스들의 진행과정을 발견하고 지울 수 있습니다. 그리고 트로이목마 혹은 바이러스가 다중 Thread보호기술로 진행과정을 Stop한 후에 또 다시 시작되는 것을 발견하였을 때 IceSwrod는 어떤 Thread가 이 프로세스들을 생성하였는가를 발견하고, 그것들을 한 번에 제거할 수 있습니다.

[File] -> [Setting] -> [Forbid all process/thread creating]을 체크. 이렇게 하면 시스템 프로세스 혹은 thread를 생성할 수 없게 됩니다. 이 때 의심스러운 프로세스나 thread를 제거한 후 멈춘 것을 취소하면 됩니다.

2-11. Log Process Termination

Log Process/Thread Creation와 비슷하나, 프로세스/쓰레드가 언제 종료되었는지를 기록해 줍니다. Log Process/Thread Creation와 함께 사용하여 프로그램의 동작 기록을 남길 때 유용합니다.

2-12. Scan Modules Hooks

모듈을 검사합니다. 특정 프로세스나 파일을 모니터링 하기 위해서 사용합니다. 이 기능을 사용하면, 꽤 많은 부하가 있으므로 사용에 주의하시기 바랍니다.

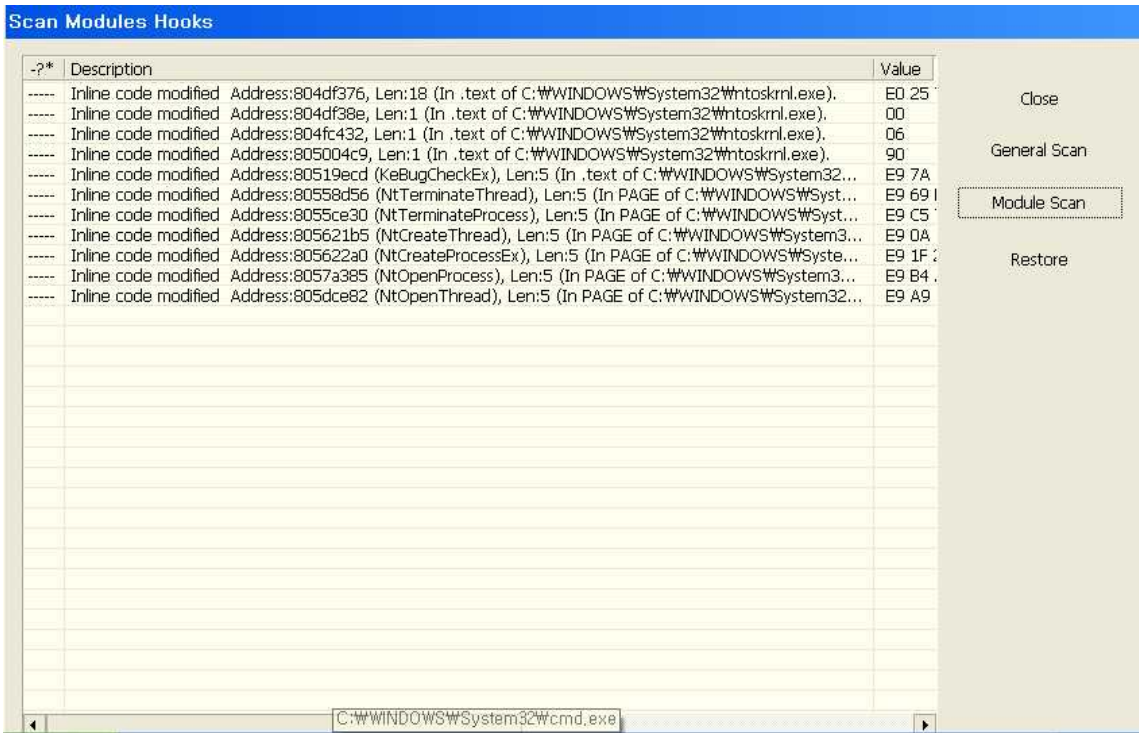
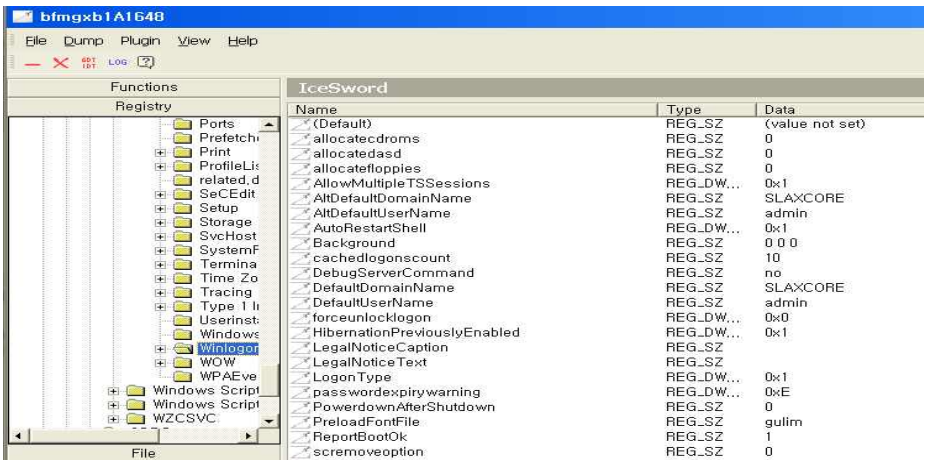


그림 14 커널 모듈 모니터링 화면

2-13. Registry

관리자라면 한번쯤은 사용해보셨을 레지스트리 편집기입니다. 윈도우의 Regedit로는 접근 할 수 없는 부분까지 아무런 제재 없이 접근과 삭제가 가능합니다. 따라서 사용 시 주의가 요구되는 기능입니다.



2-14. File

윈도우의 탐색기와 같은 기능을 가집니다. 하지만 윈도우 탐색기처럼 편한 기능은 제공하지 않습니다. 탐색기와 결정적으로 다른 점은 숨김 파일을 찾고 보호모드의 파일들을 보호 할 수 없게 하는 기능이 있습니다. 그리고 systme32₩config₩SAM등의 파일은 카피 할 수도 열 수도 없지만 IceSword는 직접 카피 할 수 있습니다.

또한 CNNIC의 cdnport.sys이 파일은 현재 IceSword만이 직접 삭제 할 수 있습니다. 기타 삭제프로그램인 unlocker, CopyLock, KillBox 같은 프로그램이 제거하지 못하는 것도 IceSword로는 제거가 가능합니다. 이러한 기능을 가진 툴인 만큼 사용상의 주의가 필요합니다.

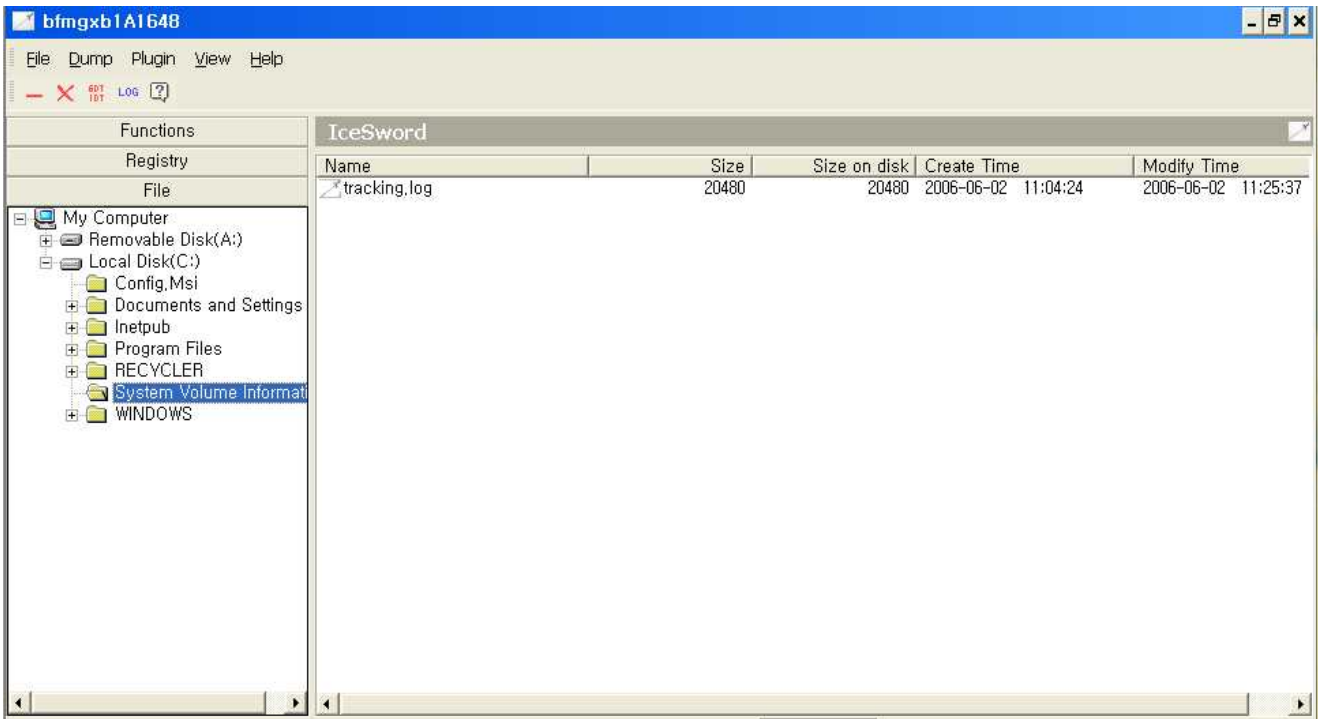


그림 16 System Volume Information 폴더에 쉽게 접근한 화면

3. IceSword의 수 많은 기능을 알아보았습니다. 루트킷 제거용으로 만들어진 강력한 툴인 만큼 사용자의 주의가 요구되는 프로그램입니다. 대다수의 루트킷과 악성코드들은 IceSword로도 제거가 가능합니다. 하지만 몇몇 악성코드는 IceSword로도 제거가 힘든 것이 많습니다. 계속해서 공격자는 진화하는 만큼 방어자들도 그에 맞춰 진화하는 모습을 보여줘야 한다고 생각합니다.

4. 참고자료

http://www.ntfaq.co.kr/4039
SKinfosec IceSword 분석 매뉴얼 한상흠

작성자 : 중부대학교 SCP회장 정혜성