

	중국 보안 동향 분석 보고서	Document No.
		SKInfosec-CHR-010

IceSword 분석 매뉴얼



한 상 흠
(m4gichack@gmail.com)

SK Infosec Co., Inc
MSS BIZ Security Center

기술 문서	IceSword 분석 매뉴얼	Document No.
중국보안동향		SKInfosec-CHR-010

Table of Contents

1. 개요	3
2. IceSword 분석	4
2.1. 컴퓨터에 문제점이 생긴다	4
2.2. IceSword의 장점	4
1) 특징	4
2) process environment block	5
3) 프로세스 삭제	5
4) 포트	5
2.3. IceSword 의 주요 기능	7
1) 프로세스 검사	7
2) 포트 검사	8
3) kernel 모듈	9
4) 부팅 그룹	10
5) Services	11
6) SPI , BHO	12
7) SSDT (System Service Descriptor Table)	13
8) Message Hook	14
9) Log Process / Thread creation	15
10) Regedit	16
11) File 탐색기	17
3. 마치며	18
4. 참고자료	19

기술 문서	IceSword 분석 매뉴얼	Document No.
중국어보안동향		SKInfosec-CHR-010

1. 개요

윈도우 루트킷을 가장 쉽고 빠르게 찾을 수 있는 툴을 추천하라고 하면 대부분의 보안전문가들은 IceSword를 추천 할 것이다.

얼음 칼이라고 해석이 되는 이 툴은 간단하게 IS 라고 불리기도 하며 북경 과학기술 대학교 (USTC)의 pjf 출품작이기도 하다. 시스템 진단 및 악성프로그램들을 제거 한다는 의미로 sword 라는 이름을 붙였을 것이다. 악성 프로그램한테 이 툴이야 말로 자신을 제거시킬 수 있는 강력한 무기인 것이다.

최근 Vista 버전까지 release 된 IceSword가 왜 이렇게 예리한 무기로 불리는지 이제부터 알아보도록 하겠다.

제작자의 공식적인 블로그는 <http://www.blogcn.com/user17/pjf/index.html> 이다

en ver. http://202.38.64.10/~jfpan/download/IceSword120_en.zip

vista ver. http://202.38.64.10/~jfpan/download/is120en_vista.zip

기술 문서	IceSword 분석 매뉴얼	Document No.
중국어보안동향		SKInfosec-CHR-010

2. IceSword 분석

2.1. 컴퓨터에 문제점이 생기다

- 삭제할 수 없는 파일
- 수정 할 수 없는 로그인 리스트
- 삭제할 수 없는 프로세스
- 알 수 없는 프로세스
- 일부 프로그램들의 숨겨진 포트들
- 탐색기로도 찾을 수 없는 루트킷 프로그램들

이런 상황들이 자신의 컴퓨터에 혹은 서버 시스템에서 일어나고 있다면 끔찍할 것이다. 우리는 얼음 칼을 이용하여 이런 문제점들을 제거할 것이다.

2.2. IceSword의 장점

1) 특징

대부분 process explorer (sysinternal.com에서 만든 리소스 관리 프로그램) 류의 툴은 모두 Windows의Toolhlp32, psapi, ZwQuerySystemInformation 등의 시스템 콜을 이용한 것이다.

ApiHook를 쓰면 쉽게 그것들을 제거 할 수 있으며 backdoor들은 더 말할 것 없다.

대부분의 툴은 Kernel thread scheduling 구조로 프로세스들을 조회하는데 이런 방식은 버전 별로 업그레이드를 해야 한다던 지 패치를 해야 하기 때문에 요즘 이렇게 찾는 방법을 변경 할 것을 제안한 사람이 있다.

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

기본적으로 사용자의 스레드 방식과 커널 스레드 방식이 있는데 IceSword 의 경우 독자적인 방식으로 조회한다는 것을 알 수 있다

기술 문서	IceSword 분석 매뉴얼	Document No.
중국어보안동향		SKInfosec-CHR-010

2) process environment block

대부분 툴도 Toolhelp32, psapi를 통하여 프로세스 이름 등을 찾는다. 앞의 것은 RtlDebug***함수를 call하여 목표점에 remote thread를 주입한 것이고 뒤에 것은 api을 디버그 하여 목표 메모리를 읽어서 얻는 것인데 본질적으로 모두 process environment block (이하 PEB) 에서 하나하나 센 것 이다.

PEB를 수정 하는 것을 통하여 쉽게 이 툴 들을 우회할 수 있게 된다. 그러나IceSword의 핵심적인 방법으로 인하여 경로를 하나도 빠뜨리지 않고 상세하게 보여주며 프로그램이 실행될 때 잘라 내어 기타 경로에 가져 간 것도 나타나게 된다.

3) 프로세스 삭제

IceSword의 프로세스 제거는 편리하며 강력하다. 당연히 위험하기도 하다. 선택된 여러 개의 프로세스들을 쉽게 없앨 수 있다. 기타 프로세스의 경우도 쉽게 제거 할 수 있으며 물론 일부 프로세스들을 (ex.winlogon) 제거 한다면 시스템이 crash 될 것이다.

4) 포트

포트 툴에 관한 것은 인터넷에 확실히 아주 많다. 하지만 인터넷에 포트를 숨기는 방법도 아주 많다. IceSword가 있다면 이런 툴들은 무용지물이 된다. 사실 방화벽 상태를 가지고 찾으려고 하지만 너무 범위를 넓게 만들고 싶지 않다. 여기 포트는windows의 IPv4 Tcpip 프로토콜 스택에 속하는 포트를 가리키며 제3의 프로토콜Stack 또는 IPv6 Stack은 지원하지 않는다.

기술 문서	IceSword 분석 매뉴얼	Document No.
중국보안동향		SKInfosec-CHR-010

일부 악성 프로그램들이 사용하는 방법들에 대해 설명을 하자면 Thread주입, 프로세스 숨기기, 파일 숨기기, 부팅 보호 등이 있다. 일반 사용자가 이 파일을 삭제하거나 진행과정을 찾으려면 아주 어렵고 이런 상황들을 보았을 때 제거할 수 없어서 답답해 한다.

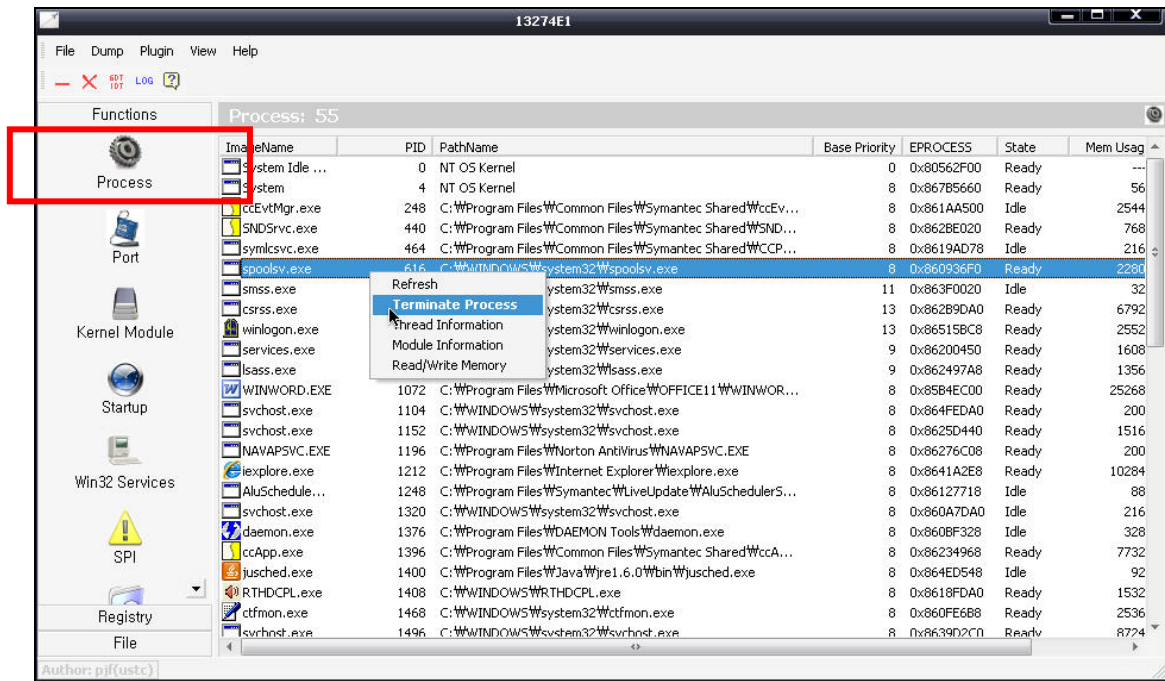
정말 삭제가 안되면 다른 시스템으로부터 이 파일을 삭제해야 할지도 모른다. 예를 들면 부팅보호를 하고 있는 rootkit 프로그램인 CNNIC이 Assistant.sys 를 부팅 추가 할 때 그것은 파일과 로그온리스트를 우회하여 직접적으로 true값으로 되돌아가며 Windows는 파일을 제거하였다고 제시한다. 그러나 다시 확인해 보면 그것은 여전히 그곳에 있다. 일부 unclocker과 같은 삭제 툴은 효과가 없다. IceSword는 현재 유일하게 직접적으로 이미 추가된 부팅리스트와 로그온 리스트보호를 할 수 있는 툴 이다. CNNIC와 같은 rootkit프로그램을 제거하려면 재 부팅 하지 않고도 제거 할 수 있다.

2.3. IceSword 의 주요 기능

IS는 새롭고 많은 핵심 기술들이 있는 프로그램이다. 프로그램을 만든 핵심 기술 들은 설명 하지 않겠고 이것을 이용하는 사용자의 각도에서 주요 기능을 설명하겠다.

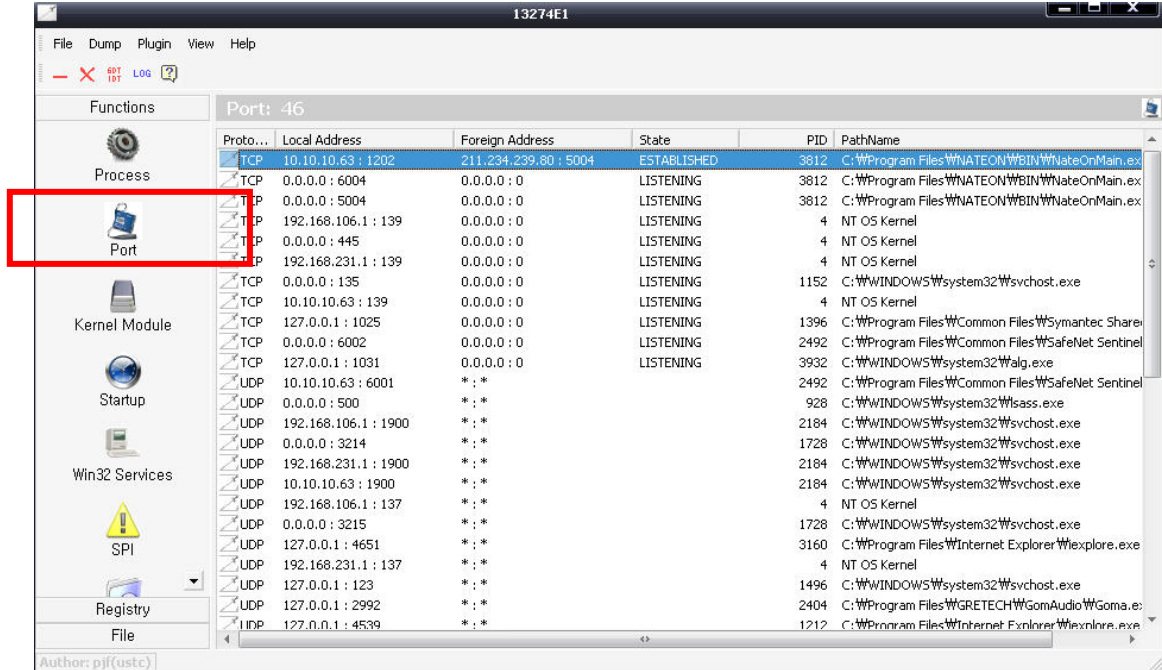
1) 프로세스 검사

실행 프로세스의 파일주소, 여러 가지 숨겨있는 프로세스 들이 나타내 진다. 이것을 사용하면 쉽게 Task Manager, Procexp등 툴들이 제거 할 수 없는 프로세스들을 쉽게 제거 할 수 있다. 그리고 또 프로세스들의 thread, 모듈정보 등을 검사 할 수 있다.



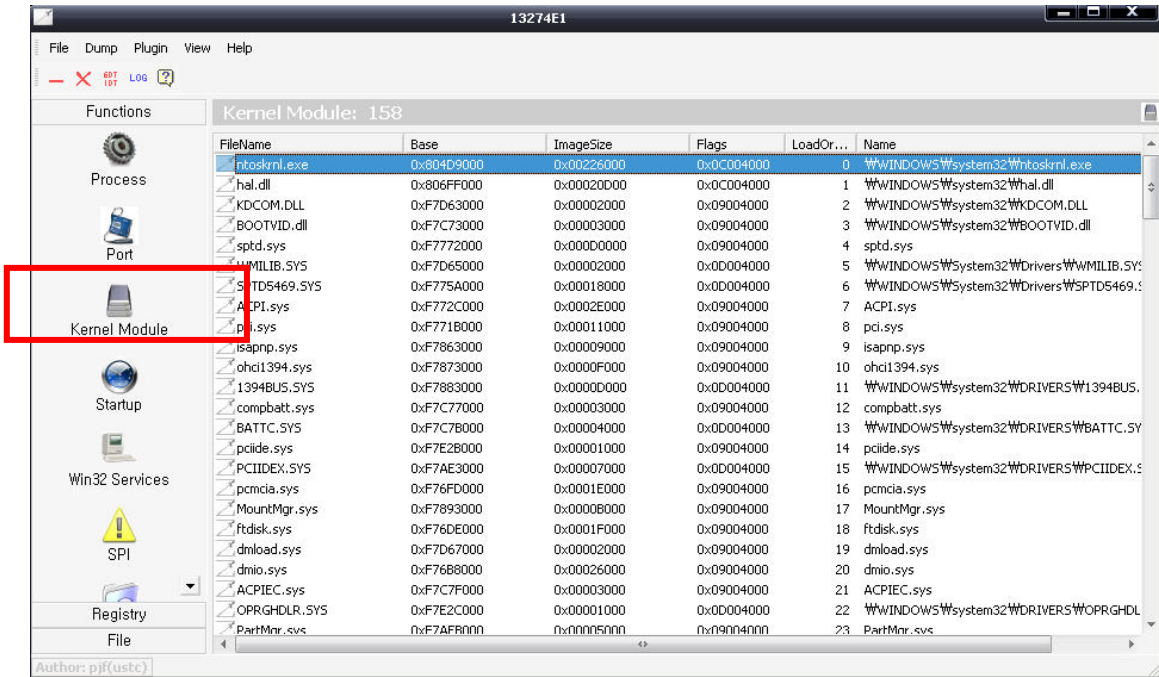
2) 포트 검사

cport, ActivePort와 같은 툴은 현재 열어놓은 포트 및 상응되는 응용프로그램주소, 이름을 나타낸다. 여러 가지 수단을 사용해서 포트를 숨긴 툴을 포함하여 그의 아래에서 모두 볼 수 있다.



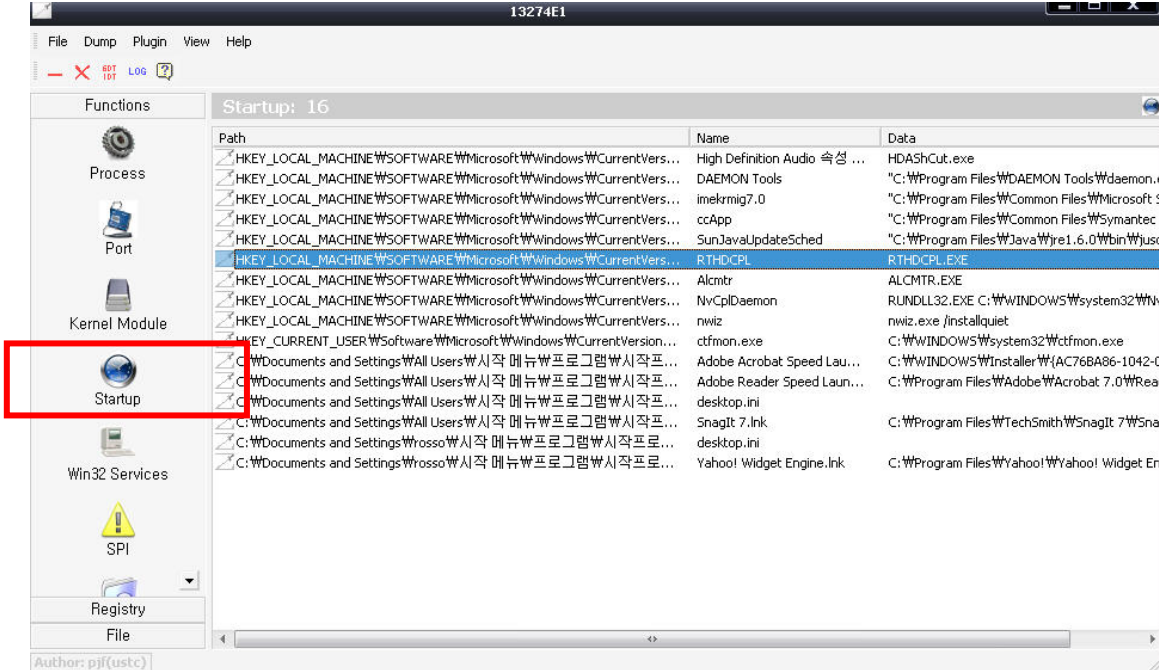
3) kernel 모듈

시스템과 공간에 추가한 PE모듈은 일반적으로 모두 부팅프로그램이며 추가된 부팅부분 등을 볼 수 있다. 일부 숨겨있는 부팅 파일을 포함 하여, 예를 들면 IS자신의 IsDrv118.sys, 이것은 탐색기에서 볼 수 없다.



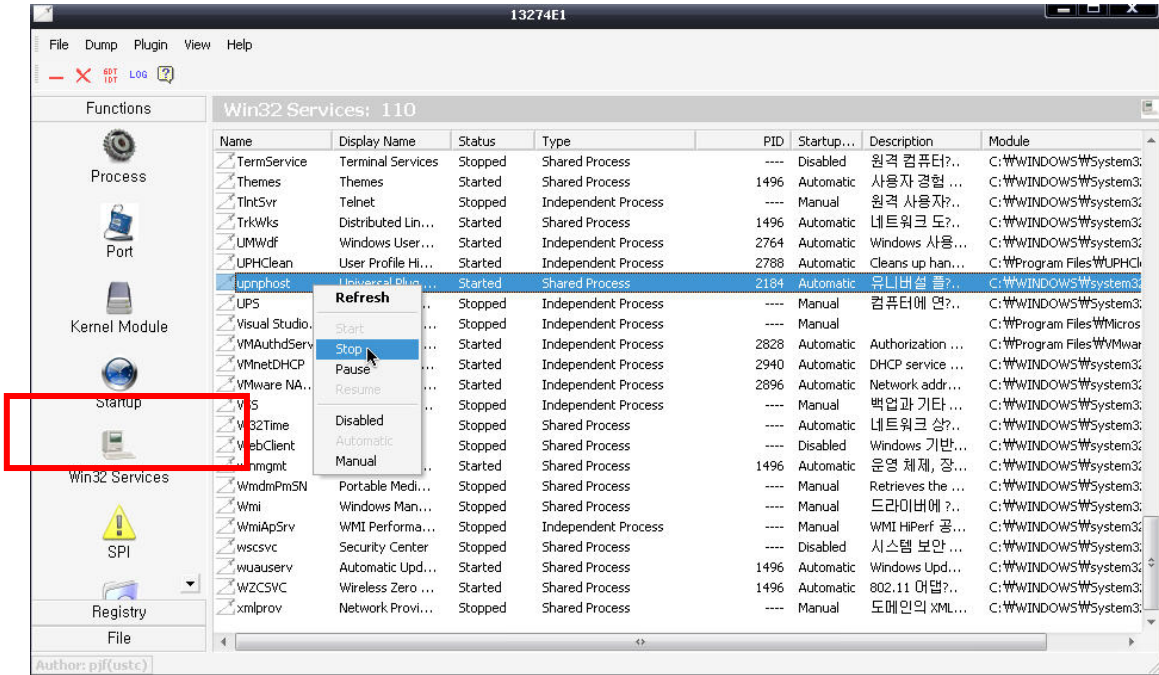
4) 부팅 그룹

Windows 부팅 그룹 안의 관련방식은 좀 쉽게 이해 할 수 있다. 그러나 아쉬운 것은 삭제 기능은 없으며 검사밖에 할 수 없다.



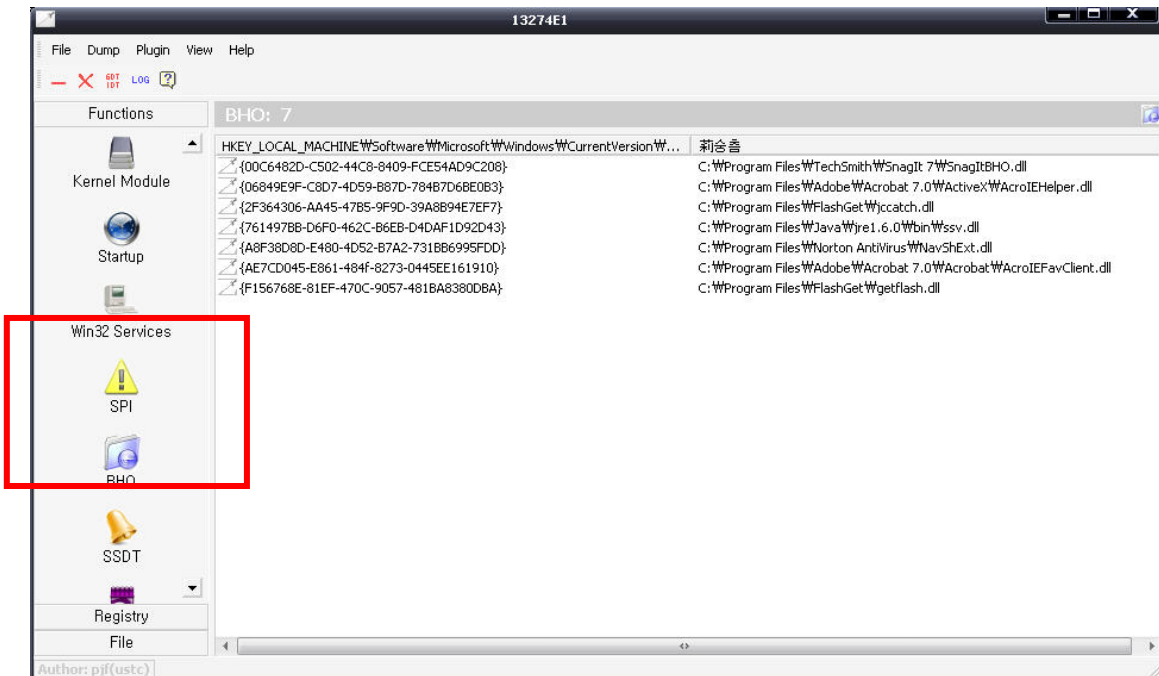
5) Services

시스템중의 숨겨졌거나 혹은 숨겨져 있지 않는 서비스를 검사 하는데 숨겨져 있는 서비스는 빨간색으로 나타난다. 서비스에 대한 부팅, 정지, 사용금지 등을 제공한다.



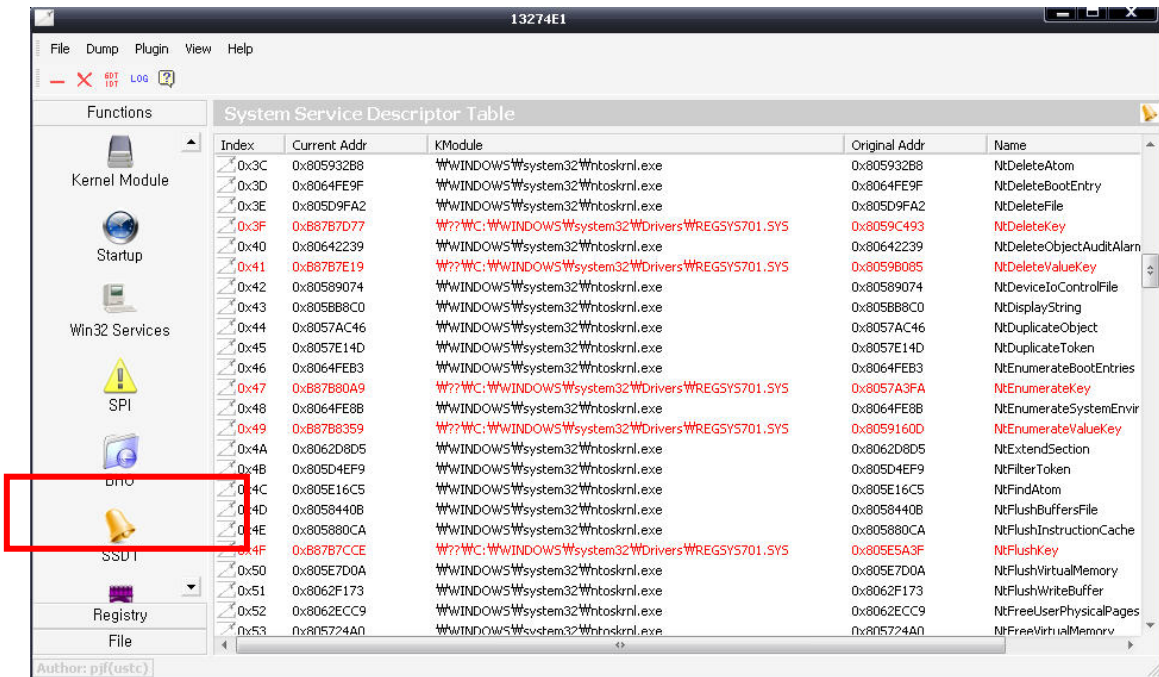
6) SPI , BHO

SPI는 서비스 인터페이스를 제공한다. 즉 모든Windows의 네트워크조작은 모두 이 인터페이스를 통하여 데이터 패킷을 받거나 보낸다. 많은 악성프로그램들은 이 dll를 바꾸어버린다. 이렇게 되면 사용자가 네트워크를 방문한 모든 패킷을 감시할 수 있으며 그것에 대하여 광고를 넣을 수 있다. 만약 분명하지 않는 상황에서 이. dll를 삭제하면 네트워크를 사용할 수 없게 되어 인터넷에 접속할 수 없게 된다. LSPFix등 툴은 이 기능에 대한 것이다. BHO는 더 말할 것도 없고, 브라우저의 보조 프로그램, 사용자가 브라우저를 부팅 할 때 그것은 자동적으로 부팅하여 광고 창 등이 튀어 나오게 된다. 이 두 가지는 검사하는 기능밖에 제공하지 않는다.



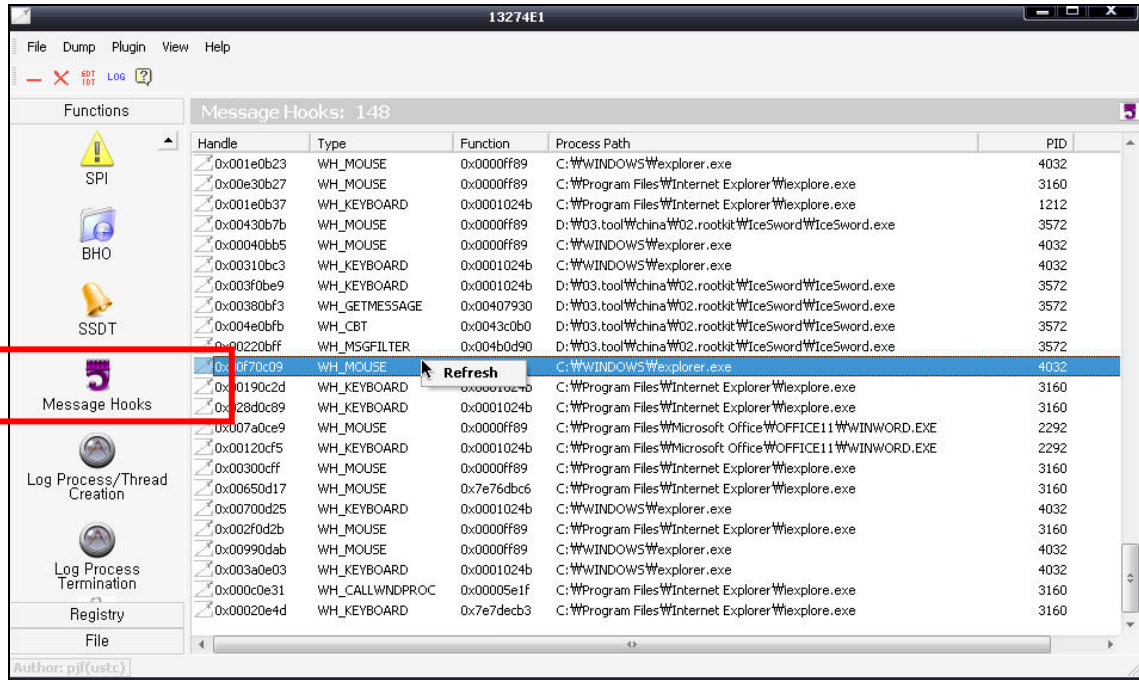
7) SSDT (System Service Descriptor Table)

System Service Descriptor 리스트, 당신의 시스템의 서비스함수를 획득하기 위하여 kernel backdoor는 가능한 한 이 서비스리스트를 수정한다. 특히 일부 오래된 rootkit, 위에서 말한 것처럼 이런 hook를 통하여 로그온리스트를 수정한다. 수정된 값은 빨간색으로 나타내며 물론 일부 보안프로그램도 빨간색으로 표시가 된다. 예를 들면 regmon같은 프로그램이 빨간색으로 표시 된다.



8) Message Hook

키보드 입력 값, 마우스 좌표 등이 필요한 경우 Win32 API를 호출 하게 된다. 어떤 프로그램들이 이를 이용 하는지에 대한 값들이 표시가 되며 검사만 가능하다

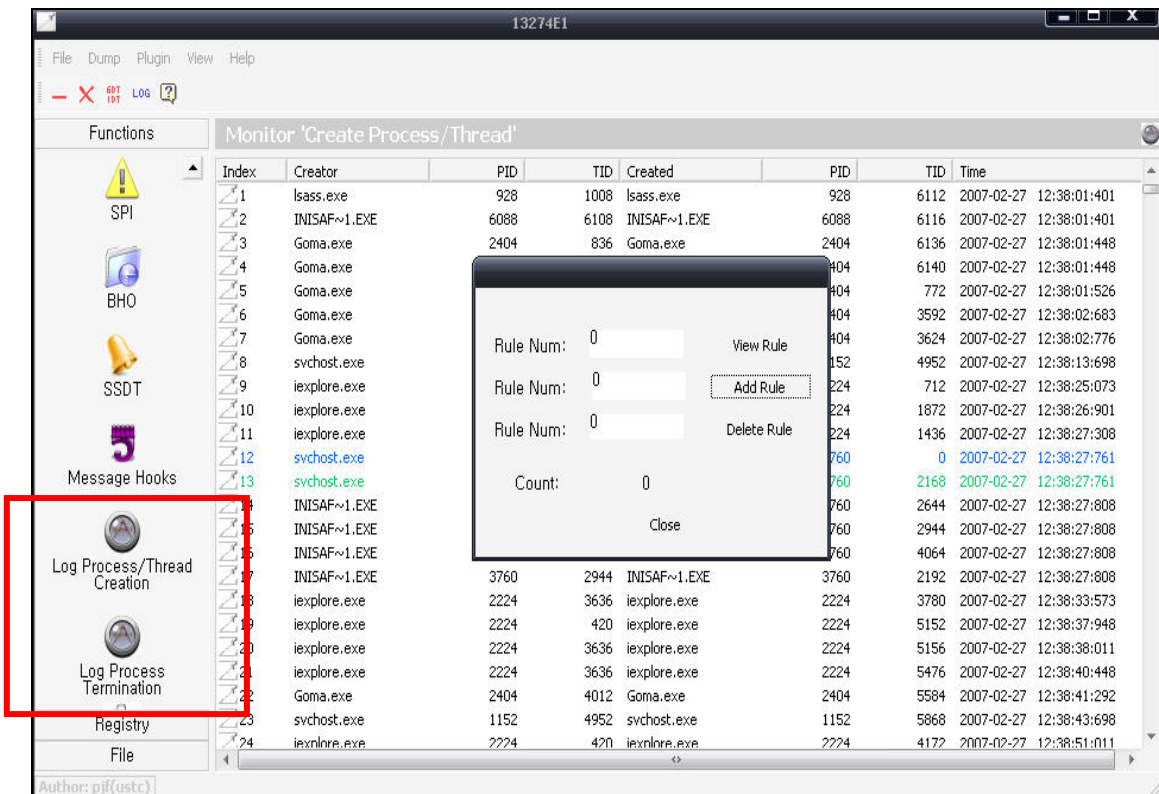


9) Log Process / Thread creation

Log Process 와 thread creation 은 IceSword 실행 기간의 프로세스 thread 생성을 기록할 수 있다.

예를 들어 트로이목마나 바이러스 진행과정을 실행할 때 바이러스를 없애는 프로그램들이 같은 진행과정이 있는가를 검사해본다. 있으면 없애버린다. 만약 IceSword이 실행되고 있다면 이런 과정들은 기록되어 어느 진행과정이 백신들을 지우는지 찾을 수 있다.

때문에 트로이목마 혹은 바이러스들의 진행과정을 발견하고 지울 수 있다. 그리고 트로이목마 혹은 바이러스가 다중 thread보호기술로 이상한 진행과정 등을 stop한 후에 또 다시 시작되는 것을 발견하였을 때 IceSword는 어떤 thread가 이 프로세스들을 생성 하였는가를 발견하고 그것 들을 한번에 제거할 수 있다. 메뉴 ->설치 대화상자에서 “process thread creation”을 선택한다 이때는 시스템 프로세스 혹은 thread를 생성할 수 없으며 의심스러운 프로세스 thread를 제거한 후 stop시킨 것을 취소하면 된다.

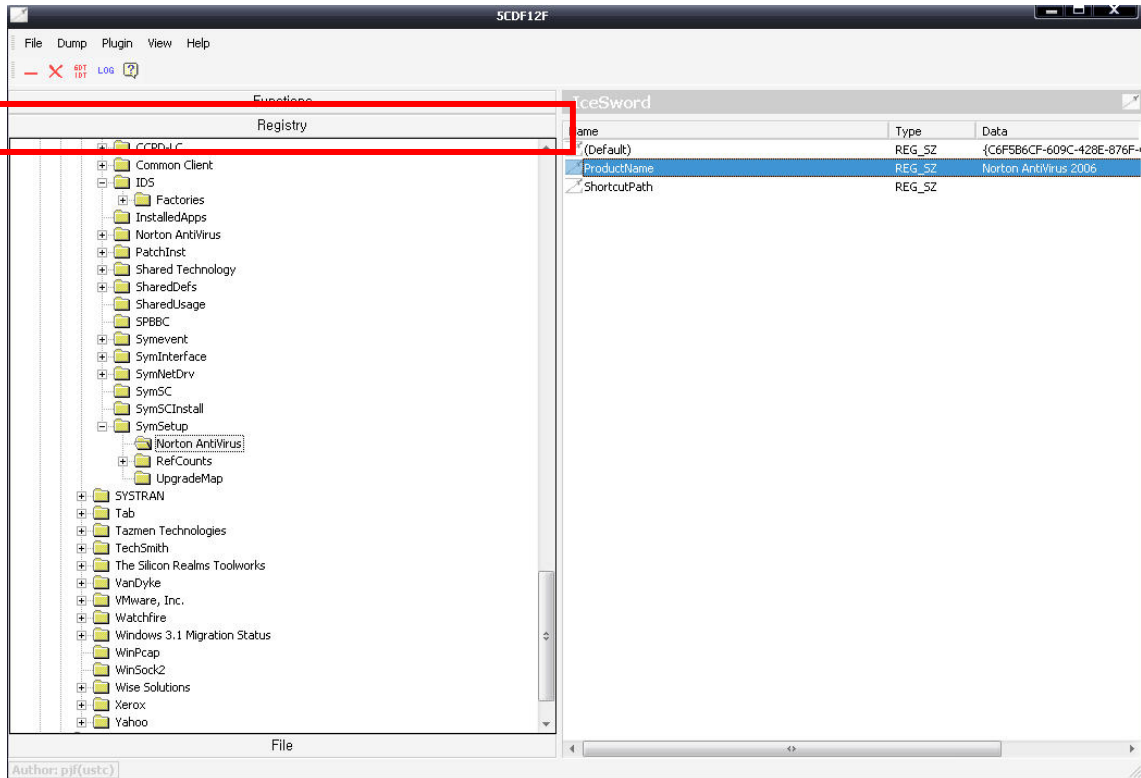


10) Regedit

윈도우의 Regedit는 너무 부족한 게 많다. 예를 들면 명칭 길이의 제한으로 하여 전 경로 이름의 길이가 255바이트를 초과하는 경우 Sub-item을 만들고 이 항목 그 뒤에 있는 sub-key가 regedit중에서 나타나지 않는 것을 볼 수 있다. (이 경우 프로그램을 작성하거나 혹은 기타 툴을 사용한다. 예를 들면regedt32) 그리고 또 일부러 프로그램으로 생성한 특수캐릭터가 있는 경우 regedit 는 열 수 없다.

IceSword에서 로그인 리스트편집을 추가하는 것은 위의 문제를 해결하기 위한 것이 아니라 이미 Regedit을 대체할 수 있는 좋은 툴이 많기 때문이다. IceSword중의 “로그인 리스트”항목은 트로이목마나 backdoor 에 의해 숨겨진 로그인 리스트를 찾기 위해 쓴 것이다. 현재 로그인 리스트를 숨기는 방법에 속아 넘어가지 않으면서 진정 믿을만한 것은 당신이 직접 로그인 리스트의 실제 내용을 보는 것이다.

예를 들면 CNNIC이 추가한 HKLM\SYSTEM\CurrentControlSet\Services\ndport 키 값, 바로 이것을 통하여 cndport.sys이 부팅파일을 추가한 것이다. Regedit을 통하여 당신은 삭제하지만 감염된 근본은 삭제할 수 없다. 그러나 IS를 사용하면 쉽게 제거할 수 있다.



11) File 탐색기

IS의 파일탐색기는 윈도우 탐색기와 비슷하다. 그렇게 편리하지 않다. 그러나 그것의 독특한 기능이 있는데 숨긴 파일들을 찾고 보호모드의 파일들을 보호 할 수 없게 하는 기능이 있다.

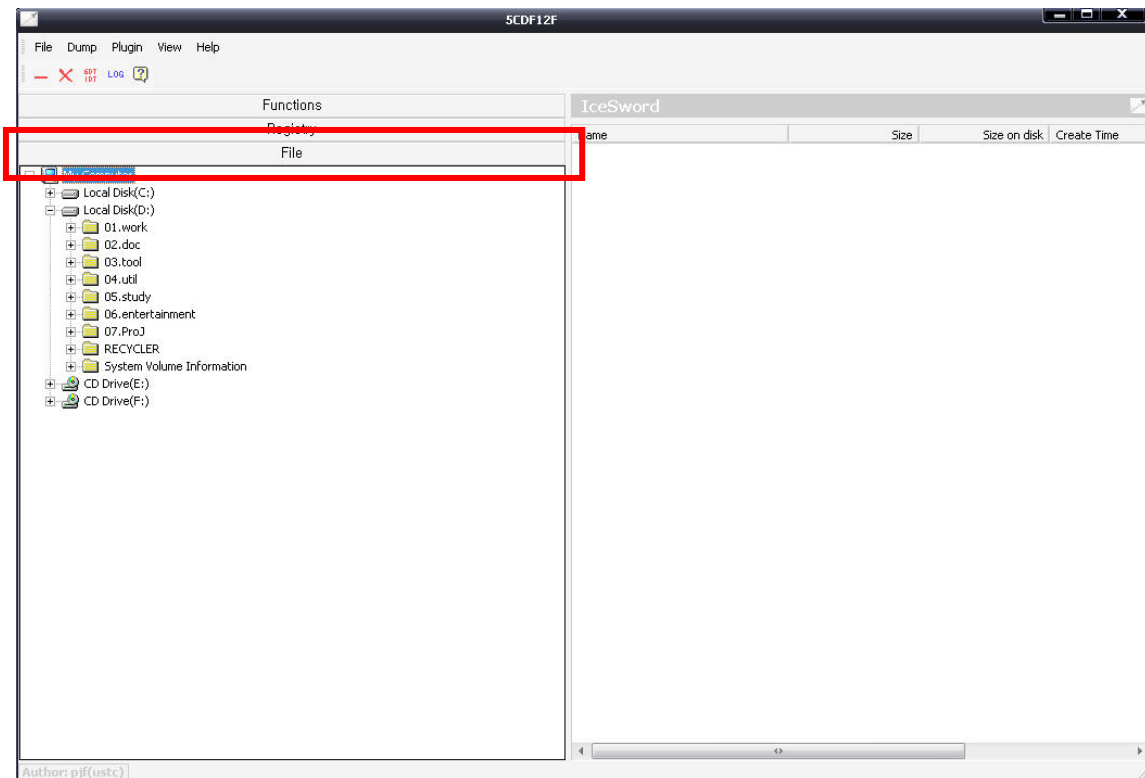
그리고 또한 system32\config\WSAM등의 파일은 카피 할 수도 열수도 없지만 IceSword는 직접 카피 할 수 있다.

또한 CNNIC의 cdnport.sys이 파일은 현재 IS만이 직접 그것을 삭제 할 수 있습니다.기타 어떤 방식이든지 모두 자신의 보호권한을 제거 할 수 없다.

대다수 unlocker, CopyLock, KillBox 같은 프로그램들은 모두 효과가 없다. Windows의 시스템이 완전히 추가한 삭제 메커니즘을 이용하고

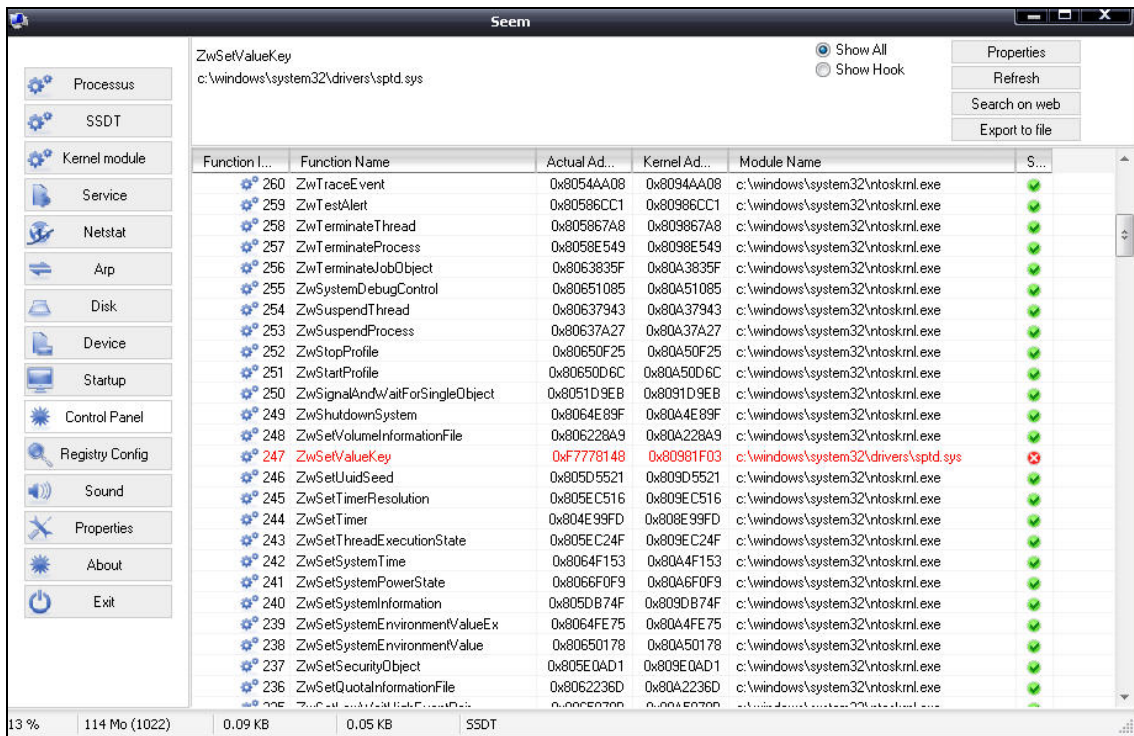
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager하에서

PendingFileRenameOperations을 증가하는 모든 완전한 파일을 삭제하는 파일 툴은 IS 뿐이다.



3. 마치며

이것으로 IceSword 의 기능을 살펴 보았다. 시스템 리소스 분석을 함에 있어 강력한 기능을 구사하고 있음을 알 수 있다. IceSword 내부 기능의 강력함도 확인하였다. 여러분들은 기능이 비슷한 소프트웨어를 사용해 보았을 것이다. 실제로 IceSword 와 거의 같은 기능이 있는 seem 라는 툴도 있다.



지금의 커널backdoor 기능은 점점 강해지며 일반적으로 쉽게 프로세스, 포트, 로그인 리스트, 파일 정보를 숨길 수 있으며 일반적인 툴은 근본적으로 발견 할 수 없다. IceSword은 많은 새로운 kernel 기술을 사용하여 backdoor로 하여금 IceSword를 피할 수 없게 한다.

IceSword의 많은 새로운 기술을 적용하여 보통의 프로세스 툴과 구별이 된다. 예를 들면 IceSword은 Idle진행과정, System진행과정, csrss진행과정 이 세 개 과정 외의 모든 프로세스들을 삭제 할 수 있다. 이 것은 다른 소프트웨어는 할 수 없을 것이다. 물론 일부 진행과정도 마음대로 삭제할 수 있는 것은 아니다. 예를 들면 시스템의 winlogon.exe 프로세스들을 없애버리면 시스템이 crash된다. 이런 것들을 주의 해야 한다.

기술 문서	IceSword 분석 매뉴얼	Document No.
중국보안동향		SKInfosec-CHR-010

이런 시스템 리소스 툴을 완벽히 이해하려면 윈도우 내부구조 등을 숙지한 후에 이용을 하면 이해하기 쉬울 것이다. 현재 악성프로그램 들은 우리와 시스템을 속이고 보안프로그램들은 또 악성프로그램들을 속이고 있는 상황들의 연속이다. “눈뜨고 코 베어 간다”라는 속담도 있듯이 자신의 시스템 구조를 모르면 악성프로그램들은 언제든지 자신의 코를 베어갈지도 모른다.

4. 참고자료

- Original article: <http://hackbase.com/>