

sysinternals 도구 모음

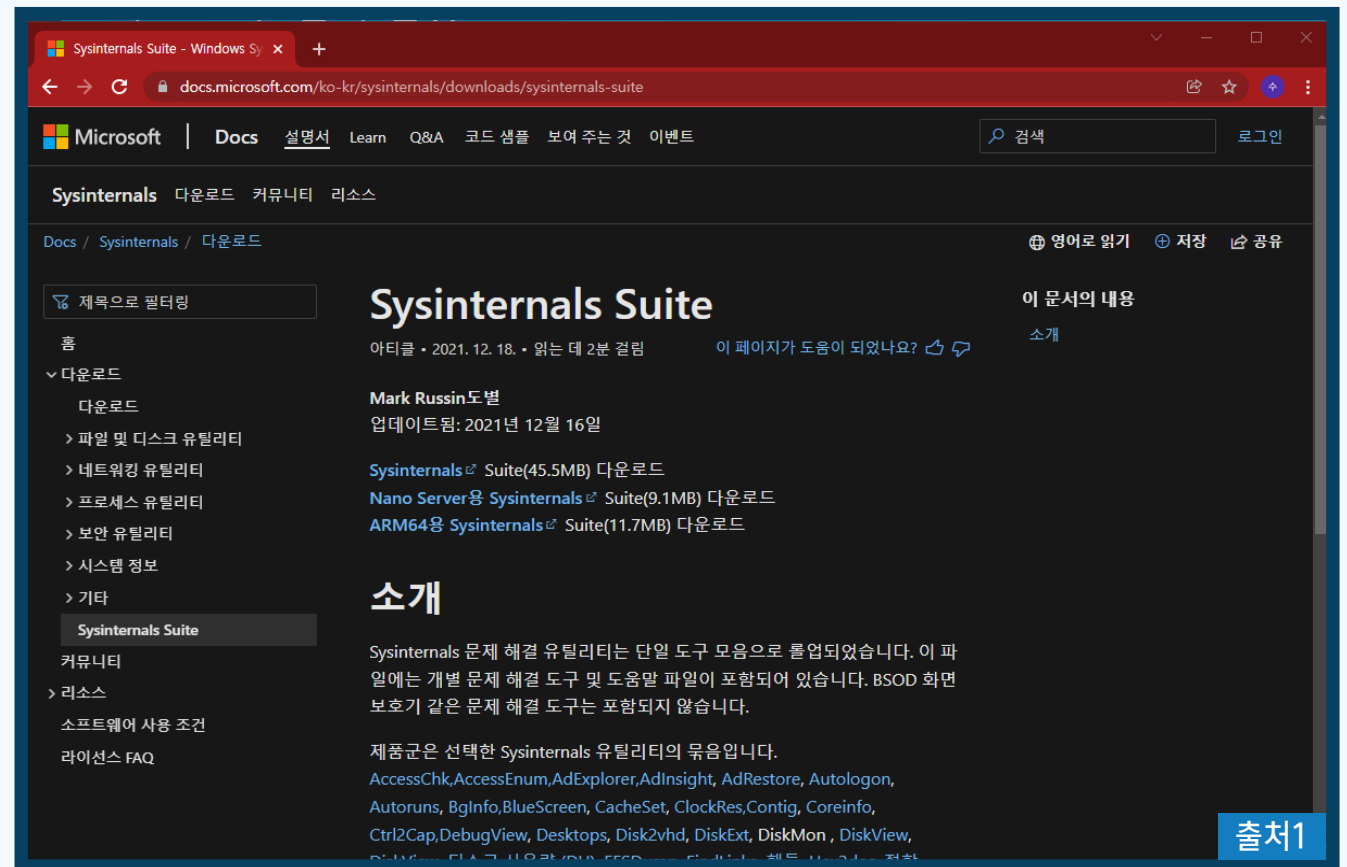
1 sysinternals suite 다운로드

⚙️ 다음의 웹 사이트에서 다운로드 가능함

<https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>



⚙️ 다운로드 후 압축을 풀면 TCP view, Autoruns, process explorer, process monitor 등 여러 가지 유용한 툴들이 모여 있음



2 TCP view

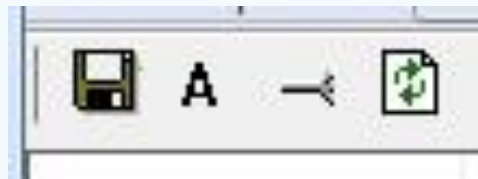
⚙️ 다음의 웹 사이트에서 다운로드 가능함

<https://technet.microsoft.com/en-us/sysinternals/bb897437.aspx>



⚙️ TCP view는 특정 프로세스에서 사용하는 포트번호와 네트워크 관련 행위들의 분석이 가능함

- 디스크 모양의 옵션은 현재 상태를 텍스트 파일로 저장함
- A 옵션은 로컬 및 원격지 주소를 IP 주소 또는 호스트 이름으로 설정함
- 오른쪽에 화살 같은 모양의 옵션은 현재 연결된 상태 또는 열린 모든 프로그램을 볼 수 있도록 설정함
- 마지막은 새로 고침



2 TCP view

TCP view 실행화면

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Process]	0	TCP	15-6600k	11852	61.111.62.149	http	TIME_WAIT				
[System Process]	0	TCP	15-6600k	11853	61.111.62.149	http	TIME_WAIT				
avgnsa.exe	7824	UDP	15-6600k	53788	*	*					
avgsvca.exe	2644	TCP	15-6600k	11327	212.4.153.164	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11405	nrt04s10-in-f19.1e100.net	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11478	203.133.172.30	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11494	m1.daumcdn.net	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11497	175.126.170.134	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11502	110.45.229.81	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11503	110.45.215.107	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11514	175.126.170.134	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11543	59.18.49.89	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11549	59.18.34.246	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11551	59.18.44.187	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11554	59.18.46.49	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11555	59.18.46.49	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11558	59.18.49.152	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11559	59.18.49.152	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11560	59.18.49.152	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11564	59.18.49.158	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11565	59.18.49.158	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11579	59.18.45.45	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11582	59.18.34.50	https	CLOSE_WAIT				
chrome.exe	7216	TCP	15-6600k	11591	59.18.46.49	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11594	59.18.44.187	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11603	59.18.49.152	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11604	59.18.49.152	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11607	cache.google.com	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11613	59.18.34.118	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11760	23.101.184.206	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11763	65.52.103.106	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11764	65.52.103.106	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11772	68.232.45.201	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11773	23.33.152.253	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11776	23.33.152.253	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11777	23.33.152.253	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11778	23.33.152.253	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11784	23.33.152.253	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11785	68.232.45.201	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11786	23.43.8.36	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11798	104.74.184.188	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11801	134.170.185.125	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11806	137.116.171.195	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11809	168.63.242.221	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11815	23.43.8.36	https	ESTABLISHED				
chrome.exe	7216	TCP	15-6600k	11820	68.232.45.201	https	ESTABLISHED				

Endpoints: 179 Established: 52 Listening: 34 Time Wait: 38 Close Wait: 1

출처2

② TCP view

⚙️ 출력 정보 설명

🔵 항목별 설명

process	실행 중인 프로세스
protocol	프로토콜(TCP 또는 UDP) 이름
local address	사용 중인 로컬 PC의 IP 주소와 포트 번호
remote address	소켓이 연결된 원격 PC의 IP 주소와 포트 번호

2 TCP view

⚙️ 출력 정보 설명

🔵 정보 색상에 따른 의미

- 1 초록색 : 정상적으로 연결이 되었을 때
- 2 노란색 : 연결이 바뀌었을 때
- 3 빨간색 : 연결이 끊기거나 종료되었을 때

Proc...	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
[System Pr...	0	TCP	mahanaim-pc.k...	9973	110.45,229.135	http	TIME_WAIT				
AppleMobil...	2028	TCP	mahanaim-PC	1028	localhost	5354	ESTABLISHED				
AppleMobil...	2028	TCP	mahanaim-PC	1028	localhost	5354	ESTABLISHED				
AppleMobil...	2028	TCP	mahanaim-PC	27015	mahanaim-PC	0	LISTENING				
AppleMobil...	2028	UDP	mahanaim-PC	64548	*	*					
AppleMobil...	2028	UDP	mahanaim-PC	64549	*	*					
ASDSvc.exe	2636	TCP	mahanaim-PC	1235	mahanaim-PC	0	LISTENING				
ASDSvc.exe	2464	TCP	mahanaim-PC	1297	mahanaim-PC	0	LISTENING				
ASDSvc.exe	2636	TCP	mahanaim-pc.k...	9937	211.115.106.202	http	CLOSE_WAIT	1	329	2	2,626
ASDSvc.exe	2636	TCP	mahanaim-pc.k...	9958	211.115.106.210	http	CLOSE_WAIT	1	841	2	704
ASDSvc.exe	2636	TCP	mahanaim-pc.k...	9966	211.115.106.201	http	CLOSE_WAIT	1	329	2	2,626
ASDSvc.exe	2636	TCP	mahanaim-pc.k...	9969	211.115.106.201	http	CLOSE_WAIT	1	841	2	704
ASDSvc.exe	2636	TCP	mahanaim-pc.k...	9970	211.115.106.201	http	CLOSE_WAIT	1	841	2	704
chrome.exe	5488	UDP	mahanaim-PC	57543	*	*		20	851	21	1,228
chrome.exe	5488	TCP	mahanaim-pc.k...	9974	nr13s97-in-f229...	https	ESTABLISHED	6	916	4	902
chrome.exe	5488	TCP	mahanaim-pc.k...	10013	cache.google.c...	https	ESTABLISHED	9	3,760	4	1,512
DaumSAM.e...	2160	TCP	mahanaim-PC	3927	mahanaim-PC	0	LISTENING				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	9956	110.45,229.135	http	ESTABLISHED	12	5,000	192	358,648
ieexplor.e...	6612	TCP	mahanaim-pc.k...	9957	114.108.157.76	http	ESTABLISHED	4	1,596	4	892
ieexplor.e...	6612	TCP	mahanaim-pc.k...	9962	110.45,243.149	http	ESTABLISHED	4	1,584	4	892
ieexplor.e...	6612	TCP	mahanaim-pc.k...	9967	175.126.170.134	http	ESTABLISHED	4	3,856	8	1,568
ieexplor.e...	6612	TCP	mahanaim-pc.k...	9969	175.126.170.134	http	ESTABLISHED	4	3,788	8	1,568
ieexplor.e...	6612	TCP	mahanaim-pc.k...	9971	61.111.62.175	https	ESTABLISHED	6	6,851	9	9,410
ieexplor.e...	6608	TCP	mahanaim-pc.k...	9972	110.45,229.135	http	ESTABLISHED	4	940	4	1,365
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10016	61.111.62.151	http	CLOSE_WAIT	1	401	1	248
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10016	61.111.62.151	http	CLOSE_WAIT	1	401	1	248
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10017	ns2.daum.net	http	CLOSE_WAIT	1	694	3	620
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10018	ns1.daum.net	http	CLOSE_WAIT	1	561	1	328
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10019	61.111.62.151	http	CLOSE_WAIT	1	1,595	4	934
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10020	ns2.daum.net	http	CLOSE_WAIT	1	1,141	3	626
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10021	113.29.189.10	http	CLOSE_WAIT	1	1,400	3	660
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10022	ns1.daum.net	http	CLOSE_WAIT	1	443	1	223
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10023	61.111.62.151	http	CLOSE_WAIT	1	411	1	246
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10024	ns2.daum.net	http	CLOSE_WAIT	1	1,136	3	626
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10025	113.29.189.10	http	CLOSE_WAIT	1	1,388	3	660
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10026	ns2.daum.net	http	CLOSE_WAIT	1	561	1	327
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10027	ns2.daum.net	http	CLOSE_WAIT	1	1,564	4	846
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10028	113.29.189.10	http	CLOSE_WAIT	1	1,396	3	660
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10029	61.251.98.132	http	CLOSE_WAIT	1	573	1	226
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10030	ns2.daum.net	http	CLOSE_WAIT				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10031	113.29.189.10	http	CLOSE_WAIT	3	1,413	3	666
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10032	113.29.189.10	http	CLOSE_WAIT				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10033	61.111.62.151	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10034	ns2.daum.net	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10035	ns1.daum.net	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10036	61.111.62.151	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10037	ns2.daum.net	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10038	113.29.189.10	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10039	61.111.62.151	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10040	ns1.daum.net	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10041	ns2.daum.net	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10042	ns2.daum.net	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10043	113.29.189.10	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10044	61.111.62.151	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10045	ns2.daum.net	http	ESTABLISHED				
ieexplor.e...	6612	TCP	mahanaim-pc.k...	10046	ns2.daum.net	http	ESTABLISHED				

Endpoints: 137 Established: 32 Listening: 33 Time Wait: 1 Close Wait: 23

출처3

2 TCP view

⚙️ 출력 정보 설명

🔵 연결 상태 표시

state	
CLOSE_WAIT	원격의 연결 요청을 받고 연결이 종료되기를 기다리는 상태
CLOSED	server 완전히 연결이 종료된 상태
ESTABLISHED	서로 연결이 되어 있는 상태
FIN_WAIT_1	소켓이 닫히고 연결이 종료되고 있는 상태
FIN_WAIT_2	로컬이 원격으로부터 연결 종료 요구를 기다리는 상태
LAST_ACK	연결은 종료되었고 승인을 기다리는 상태
LISTEN	데몬이 요청을 받을 수 있도록 연결 요구를 기다리는 상태 즉, 포트가 열려있음을 의미
SYN_RECEIVED	원격으로부터 연결 요청을 받은 상태
SYN_SEND	로컬에서 원격으로 연결 요청(SYN 신호를 보냄)을 시도한 상태
TIMED_WAIT	연결은 종료되었으나 원격의 수신 보장을 위해 기다리고 있는 상태

3 Actoruns

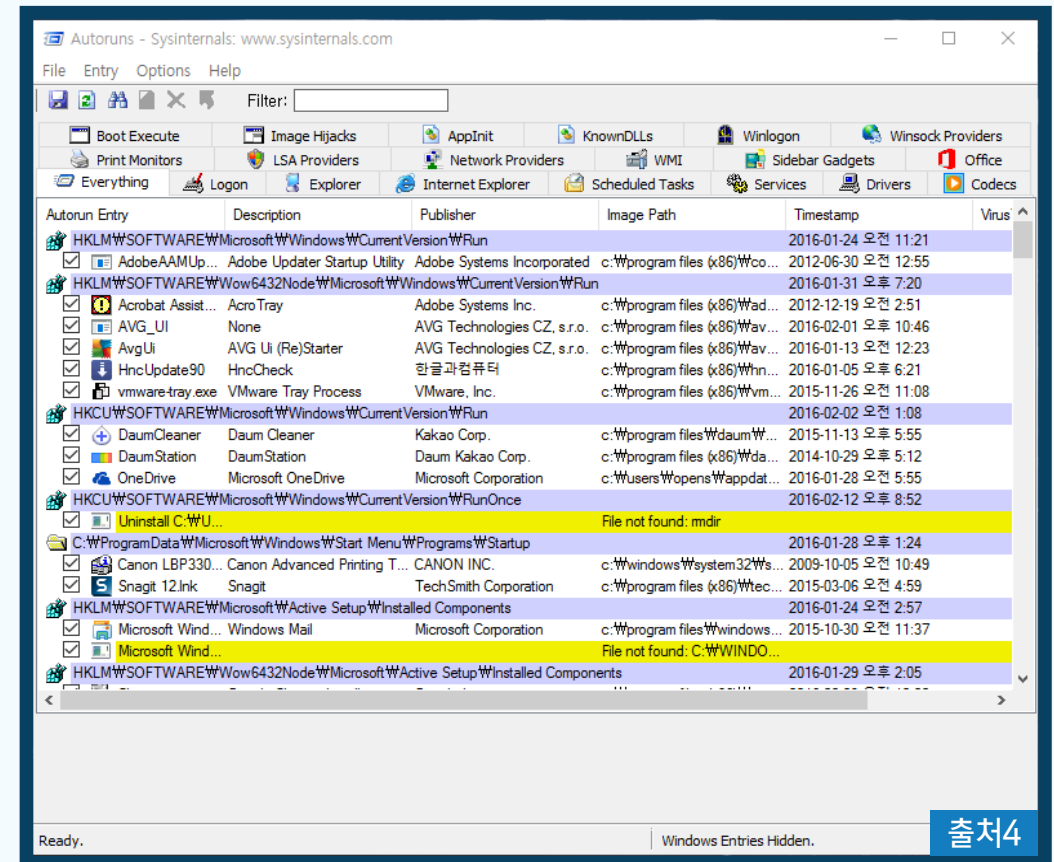
⚙️ 다음의 웹 사이트에서 다운로드 가능함

<https://technet.microsoft.com/ko-kr/sysinternals/bb963902>



⚙️ Autoruns를 이용하면 악성코드가 사용자 몰래 등록하는 시작프로그램을 확인할 수 있음

⚙️ 추가적인 기능으로 악성코드가 실행되기 전 저장해둔 자동 실행 파일 목록이 있다면 악성코드가 실행된 후 내용과 비교해서 새로 추가되거나 변경된 내용을 알려줌



4 process explorer

⚙ Mark Russinovich가 만든 프로세스 관리 유틸리티로 Microsoft에 인수됨

Process	CPU	Private Byt...	Working Set	PID	Description	Company Name
System Idle Process	86,61	0 K	4 K	0		
System	1,77	624 K	28,244 K	4		
Interrupts	0,54	0 K	0 K	n/a	Hardware Interrupts and...	
smss.exe		356 K	1,144 K	416		
csrss.exe		1,460 K	5,616 K	952		
wininit.exe		1,220 K	5,856 K	1060		
services.exe	< 0,01	3,196 K	7,148 K	1180		
svchost.exe	0,01	8,068 K	6,536 K	1292	Host Process for Windo...	Microsoft Corporation
RuntimeBroker.exe		12,476 K	9,440 K	6840	Runtime Broker	Microsoft Corporation
ShellExperienceHo...	Sus...	16,296 K	360 K	5168	Windows Shell Experien...	Microsoft Corporation
SearchUI.exe	Sus...	42,340 K	428 K	6156	Search and Cortana ap...	Microsoft Corporation
SettingSyncHost.e...		6,128 K	12,828 K	3696	Host Process for Sett...	Microsoft Corporation
CSISYN~1.EXE		11,412 K	3,180 K	6992	Microsoft Office Docum...	Microsoft Corporation
MSOSYNC.EXE		13,020 K	4,292 K	4472	Microsoft Office Docum...	Microsoft Corporation
SkypeHost.exe	Sus...	15,076 K	352 K	860	Microsoft Skype	Microsoft Corporation
explorer.exe		29,736 K	43,336 K	1592	Windows 탐색기	Microsoft Corporation
POWERPNT.EXE	< 0,01	186,580 K	177,592 K	4728	Microsoft PowerPoint	Microsoft Corporation
Tcpview.exe	1,46	10,080 K	10,640 K	2088		
procexp.exe		2,796 K	10,084 K	2288	Sysinternals Process E...	Sysinternals - www.s...
procexp64.exe	0,17	13,600 K	35,136 K	7052	Sysinternals Process E...	Sysinternals - www.s...
svchost.exe	0,02	6,492 K	6,060 K	1356	Host Process for Windo...	Microsoft Corporation
svchost.exe		24,256 K	20,036 K	1464	Host Process for Windo...	Microsoft Corporation
sihost.exe		4,720 K	4,136 K	3176	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe	< 0,01	6,300 K	4,728 K	7996	Windows 작업을 위한 호...	Microsoft Corporation
svchost.exe	< 0,01	12,116 K	9,924 K	1484	Host Process for Windo...	Microsoft Corporation
svchost.exe	0,01	14,244 K	10,768 K	1596	Host Process for Windo...	Microsoft Corporation
svchost.exe	0,01	11,476 K	10,756 K	1612	Host Process for Windo...	Microsoft Corporation
svchost.exe		4,284 K	3,788 K	1704	Host Process for Windo...	Microsoft Corporation
svchost.exe	0,04	13,792 K	8,812 K	1752	Host Process for Windo...	Microsoft Corporation
dashHost.exe		5,552 K	2,668 K	2928		

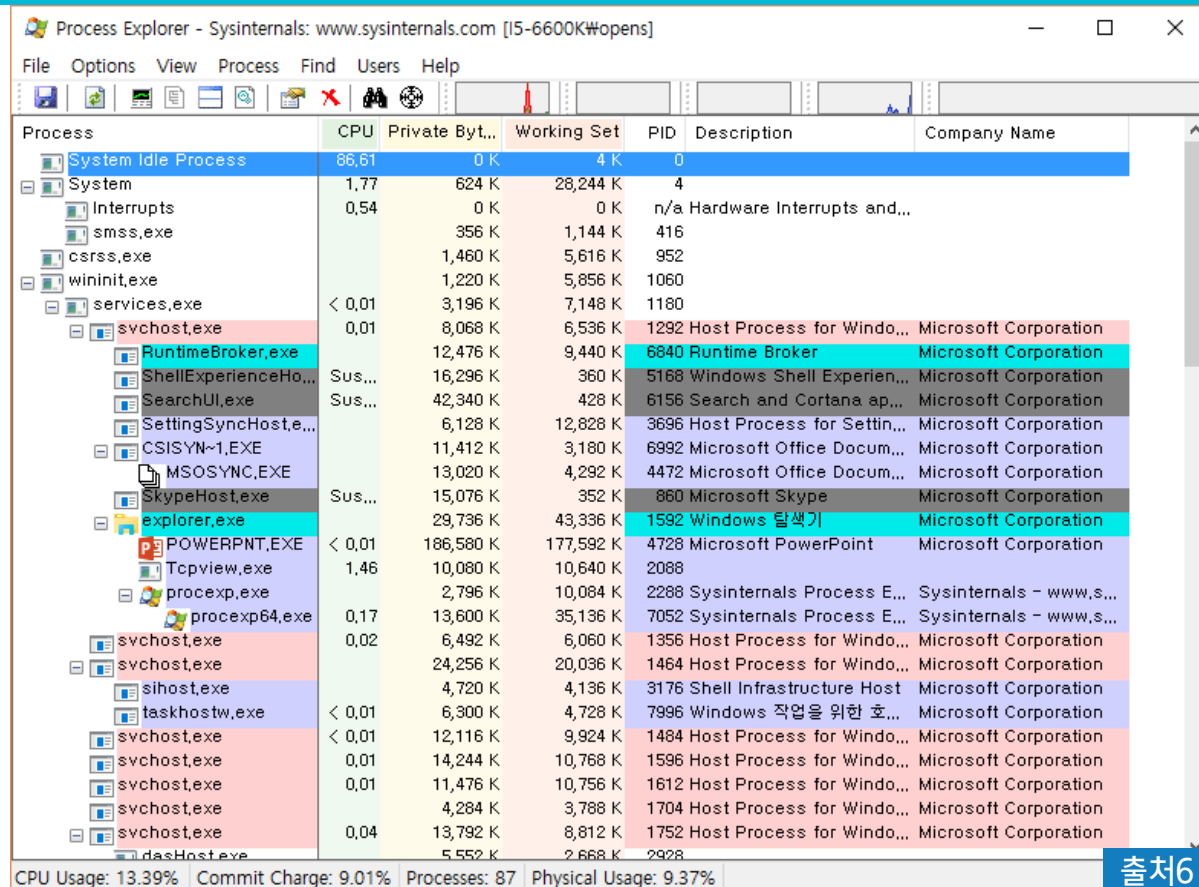
CPU Usage: 13.39% Commit Charge: 9.01% Processes: 87 Physical Usage: 9.37%

출처5

4 process explorer

process explorer의 화면에 출력되는 주요 기능

- 1 parent/child 프로세스 트리 구조 표시
- 2 프로세스 실행/종료 시 각각의 색깔(초록/빨강)로 표시
- 3 프로세스 suspend 기능
→ 실행 중지
- 4 프로세스 종료(kill) 기능
→ kill process tree 기능 지원
- 5 DLL/Handle 검색
→ 프로세스에 인젝션 된 DLL 검색 또는 특정 파일을 오픈한 프로세스 검색



Process Explorer - Sysinternals: www.sysinternals.com [I5-6600K#opens]

File Options View Process Find Users Help

Process	CPU	Private Byt...	Working Set	PID	Description	Company Name
System Idle Process	86,61	0 K	4 K	0		
System	1,77	624 K	28,244 K	4		
Interrupts	0,54	0 K	0 K	n/a	Hardware Interrupts and...	
smss.exe		356 K	1,144 K	416		
csrss.exe		1,460 K	5,616 K	952		
wininit.exe		1,220 K	5,856 K	1060		
services.exe	< 0,01	3,196 K	7,148 K	1180		
svchost.exe	0,01	8,068 K	6,536 K	1292	Host Process for Windo...	Microsoft Corporation
RuntimeBroker.exe		12,476 K	9,440 K	6840	Runtime Broker	Microsoft Corporation
ShellExperienceHo...	Sus...	16,296 K	360 K	5168	Windows Shell Experien...	Microsoft Corporation
SearchUI.exe	Sus...	42,340 K	428 K	6156	Search and Cortana ap...	Microsoft Corporation
SettingSyncHoste...		6,128 K	12,828 K	3696	Host Process for Settin...	Microsoft Corporation
CSISYN~1.EXE		11,412 K	3,180 K	6992	Microsoft Office Docum...	Microsoft Corporation
MSOSYNC.EXE		13,020 K	4,292 K	4472	Microsoft Office Docum...	Microsoft Corporation
SkypeHost.exe	Sus...	15,076 K	352 K	860	Microsoft Skype	Microsoft Corporation
explorer.exe		29,736 K	43,336 K	1592	Windows 탐색기	Microsoft Corporation
POWERPNT.EXE	< 0,01	186,580 K	177,592 K	4728	Microsoft PowerPoint	Microsoft Corporation
Tcpview.exe	1,46	10,080 K	10,640 K	2088		
procexp.exe		2,796 K	10,084 K	2288	Sysinternals Process E...	Sysinternals - www.s...
procexp64.exe	0,17	13,600 K	35,136 K	7052	Sysinternals Process E...	Sysinternals - www.s...
svchost.exe	0,02	6,492 K	6,060 K	1356	Host Process for Windo...	Microsoft Corporation
svchost.exe		24,256 K	20,036 K	1464	Host Process for Windo...	Microsoft Corporation
sihost.exe		4,720 K	4,136 K	3176	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe	< 0,01	6,300 K	4,728 K	7996	Windows 작업을 위한 호...	Microsoft Corporation
svchost.exe	< 0,01	12,116 K	9,924 K	1484	Host Process for Windo...	Microsoft Corporation
svchost.exe	0,01	14,244 K	10,768 K	1596	Host Process for Windo...	Microsoft Corporation
svchost.exe	0,01	11,476 K	10,756 K	1612	Host Process for Windo...	Microsoft Corporation
svchost.exe		4,284 K	3,788 K	1704	Host Process for Windo...	Microsoft Corporation
svchost.exe	0,04	13,792 K	8,812 K	1752	Host Process for Windo...	Microsoft Corporation
dashHost.exe		5,552 K	2,668 K	2928		

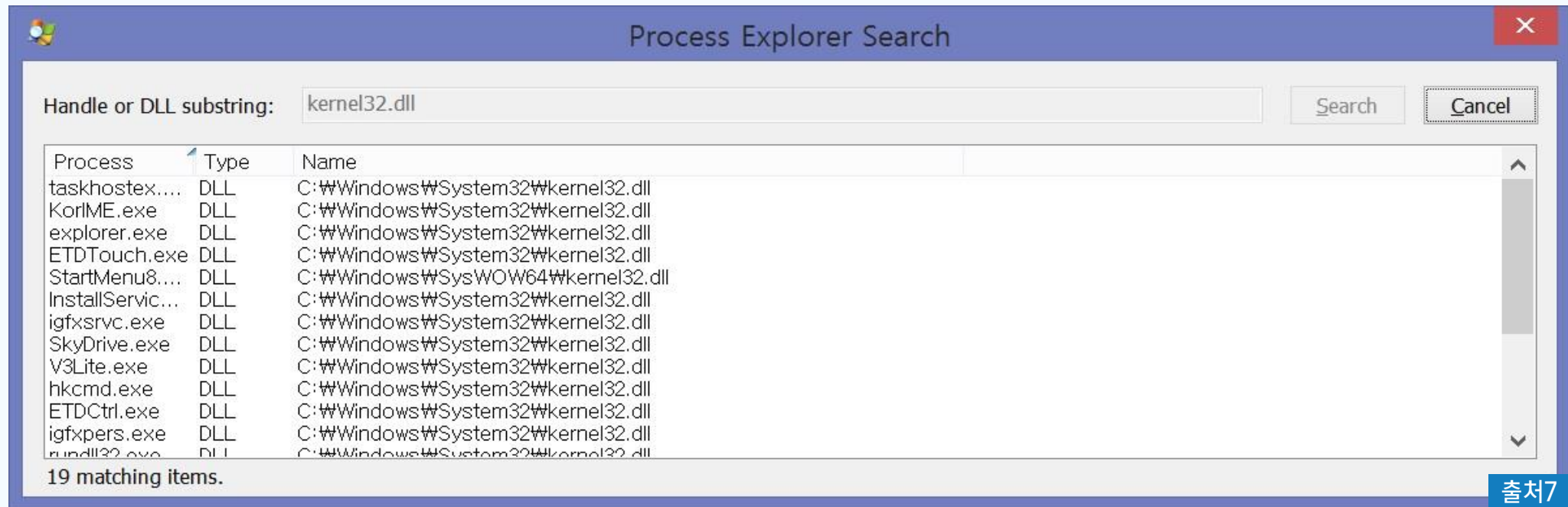
CPU Usage: 13.39% Commit Charge: 9.01% Processes: 87 Physical Usage: 9.37%

출처6

4 process explorer

프로세스 익스플로러의 **find** 기능을
이용하면 특정 모듈을 불러온
프로세스들도 확인할 수 있음

이는 DLL과 같은 악성코드를
실행한 프로세스를 찾는 데 용이함



1 sysinternals 도구 모음

⑤ process monitor

process monitor

시스템에서 동작 중인 프로세스의 모든 행위를 모니터링하는 도구



5 process monitor

02

process monitor의 주요 6가지 기능

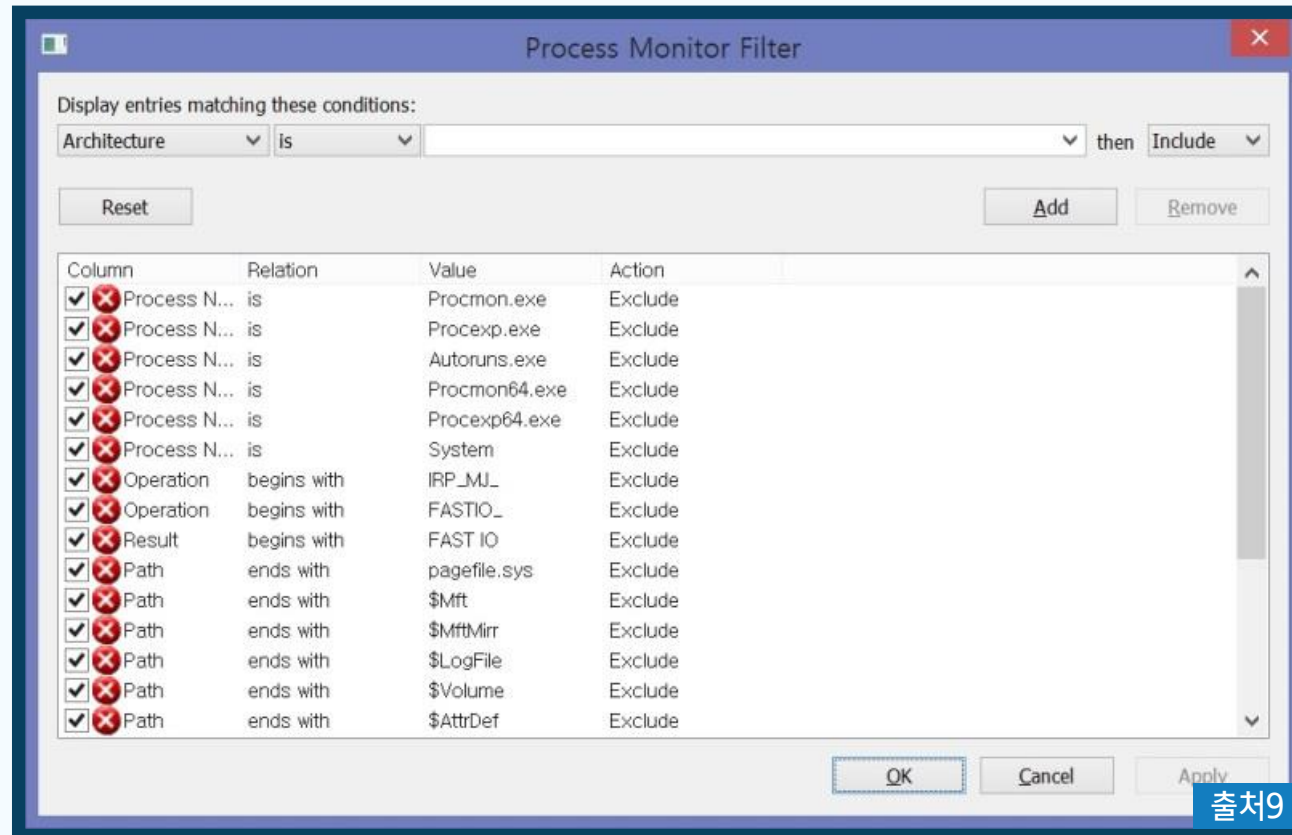


- 1 레지스트리 활동 모니터링(show registry activity)
- 2 파일 시스템 활동 모니터링(show file system activity)
- 3 네트워크 활동 모니터링(show network activity)
- 4 프로세스 종료(kill) 기능(kill process tree 기능 지원)
- 5 프로세스와 스레드 활동 모니터링(show process and thread activity)
- 6 이벤트 프로파일링(show profiling events)

5 process monitor

03

enable advanced output을 켜면 파일 시스템 활동을 관찰할 때 각 디스패치 루틴정보를 출력함

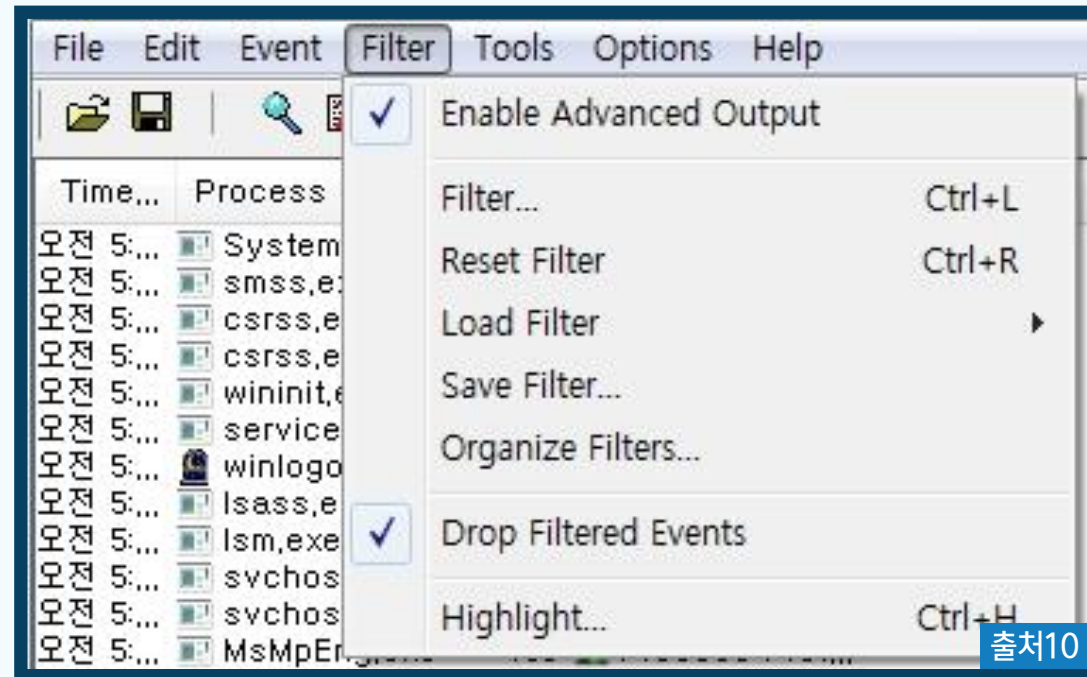


출처9

5 process monitor

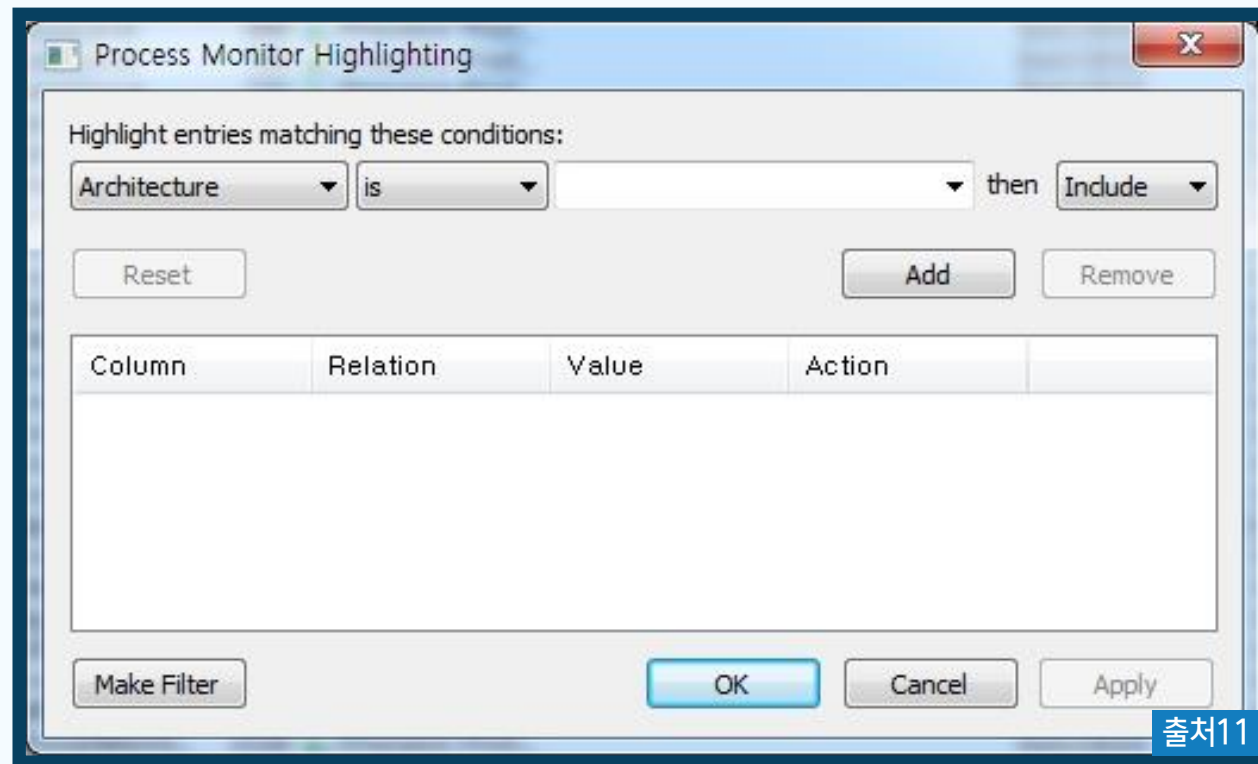
04

advanced output 옵션을 사용하지 않는다면 일반 응용 프로그래머들에게 좀 더 익숙한 Win32 인터페이스 이름으로 출력됨



5 process monitor

05 highlight 기능은 로그를 쉽게 보는 데 도움을 줌





5 process monitor

process and thread
activity 내용 분석

file system
activity

registry
activity

- 프로세스, 스레드와 관련된 오퍼레이션은 다음과 같음
 - process/thread create : 프로세스/스레드를 생성함
 - process/thread start : 프로세스/스레드를 시작함
 - load image : 이미지를 읽음

Operation	
	Load Image
	Load Image
	Thread Exit
	Thread Create
	Load Image
	Load Image
	Load Image
	Load Image
	Load Image
	Load Image
	Thread Exit
	Load Image
	Load Image
	Load Image
	Load Image
	Load Image
	Load Image
	Thread Create
	Load Image
	Load Image
	Thread Create

5 process monitor

process and
thread activity

file system activity
내용 분석

registry
activity

CreateFile

- 파일을 만들거나 이미 만들어져 있는 파일을 옴
- 파일뿐만 아니라 파이프, 메일 슬롯, 콘솔 등의 오브젝트를 만들거나 열기도 함

WriteFile

- 파일에 데이터를 씀

ReadFile

- 파일에서 데이터를 읽음

CopyFile

- 파일을 복사함

MoveFile

- 파일을 이동함

DeleteFile

- 파일을 삭제함

CloseFile

- 파일을 닫음

LockFile

- 바이트 범위로 지정된 파일을 잠금

Operation
CloseFile
CreateFile
CreateFile
CreateFile
CreateFile
CreateFile
CreateFile
QueryBasicInformationFile
CreateFileMapping
DeviceIoControl
CreateFile
FileSystemControl
CloseFile
CreateFileMapping
CloseFile
QueryStandardInformationFile
CreateFileMapping
CreateFileMapping
CreateFile
CreateFile
CreateFile
FileSystemControl
FileSystemControl
CloseFile
CloseFile
CreateFileMapping
QueryStandardInformationFile
CreateFileMapping
QueryStandardInformationFile

출처13

(1/3)

5 process monitor

process and
thread activity

file system activity
내용 분석

registry
activity

CreateFileMapping

- MMF(Memory Mapped File) 생성
- 일반적으로 실행 파일(EXE, DLL)들이 실행되면 MMF가 됨

UnlockFileSingle

- 바이트 범위로 잠금된 파일을 해제(unlock)함

FileSystemControl

- 지정된 파일 시스템이나 파일 시스템 필터 드라이버에 직접 제어 코드를 보내어, 해당 드라이버가 지정된 작업을 수행하게 함

QueryNameInformationFile

- 파일 객체에 대한 정보를 반환
- 이름의 형식에 대한 자세한 정보를 반환함

5 process monitor

process and
thread activity

file system activity
내용 분석

registry
activity

QueryStandardInformation
File

- 파일 객체에 대한 정보를 반환
- 바이트 단위 파일 할당 크기, 바이트 오프셋의 파일 위치의 끝, 파일에 대한 하드링크 수, 파일 객체가 디렉토리인지의 정보를 나타냄

QueryInformationVolume

- 특정 파일, 디렉토리, 저장장치 또는 볼륨과 연결된 볼륨에 대한 정보를 검색함

QueryDirectory

- 기존 디렉토리를 오픈
- 디렉토리 개체에 쿼리를 액세스함

5 process monitor

process and
thread activity

file system
activity

registry activity
내용 분석

RegOpenKey	지정한 위치의 키를 오픈
RegCloseKey	열어놓은 키 핸들을 닫음
RegDeleteKey	지정한 키의 서브키를 지움
RegSetValue	지정한 키의 기본 값을 설정함
RegCreateKey	지정한 키의 서브키로 새 키를 만들
RegEnumKey	지정한 키의 서브 키들을 조회함
RegQueryValue	지정한 키의 기본 값을 가져옴
RegEnumValue	지정한 키가 가지고 있는 모든 값의 이름들을 가져옴
RegGetValue	지정한 이름을 갖는 값을 가져옴
RegDeleteValue	지정된 이름을 갖는 값을 제거함

Operation
 RegCloseKey
 RegQueryKey
 RegEnumKey
 RegQueryKey
 RegOpenKey
 RegQueryKey
 RegOpenKey
 RegOpenKey
 RegCloseKey
 RegOpenKey
 RegEnumKey
 RegOpenKey
 RegQueryKey
 RegOpenKey
 RegQueryKey

출처14

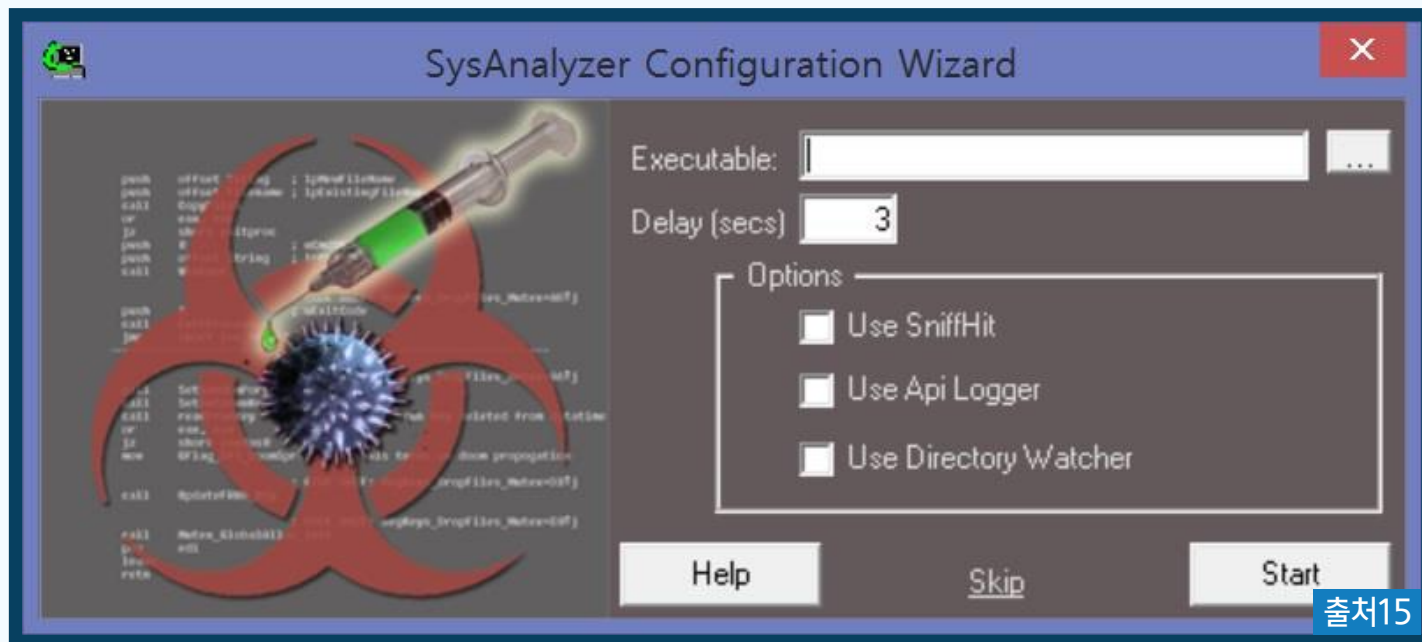
1 SysAnalyzer

- ⚙️ 다음의 웹 사이트에서 다운로드 가능함

<http://sysanalyzer.software.informer.com/1.0/>



- ⚙️ SysAnalyzer는 분석 프로그램이 직접 악성코드를 실행시켜 체크한 사항을 출력해줌
- ⚙️ 실행된 프로세스, 사용 포트, 사용한 DLL, 악성코드가 사용한 API 등의 정보를 출력해줌



출처15

② CaptureBAT

⚙️ 다음의 웹 사이트에서 다운로드 가능함

<https://www.honeynet.org/projects/old/capture-bat/>



기능

- CLI 기반의 도구로 커널 레벨에서 정보를 수집하는 점과 삭제되는 파일들을 저장해 놓는 점
- 네트워크 패킷을 캡처하는 등

② CaptureBAT

실행

- 실행하기 위해서는 VC++ 2005 재배포 패키지 및 WinPcap의 설치가 필요함



프로그램의 실행은 cmd에서 `CaptureBAT.exe -c -n -l c:\wresult.txt` 명령어를 사용함

옵션

- `-c` : 수정되거나 삭제된 파일을 캡처함
- `-n` : 네트워크 활동을 캡처함
- `-l` : 위치에 결과를 저장함