VBS.Autorun.7474
상세 분석 보고서

최초 작성 : 2011년 11월 24일
작성자 : 김부성
홈페이지 : http://www.chosik.com
이메일 : kbs6880@gmail.com

▣기본 정보

종류	Worm	위험도	낮음
감염경로	이동식 디스크	증상	시스템 설정 변경
플랫폼	Windows	크기	7,474byte
암호화 여부	비암호화	팩킹	
MD5	A45D0F681A149DAA3B8E8B556B7462C6		
SHA1	CC024E6C8697D7665829AA50E58C8868AA617AA6		

▣VirusTotal 정보

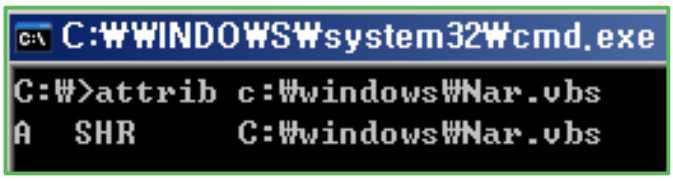
Antivirus	Version	Result
AhnLab- V3	2011.11.24.00	VBS/Solow.worm
AntiVir	7.11.18.59	VBS/RunAuto.Q
Antiy- AVL	2.0.3.7	Worm/Win32.AutoRun
Avast	6.0.1289.0	VBS:AutoRun- gen [Wrm]
AVG	10.0.0.1190	VBS/Worm
BitDefender	7.2	Generic.ScriptWorm.51607B57
ByteHero	1.0.0.1	-
CAT- QuickHeal	12.00	VBS/Autorun.CAJ
ClamAV	0.97.3.0	Worm.VBS.Autorun.Nar
Commtouch	5.3.2.6	VBS/Autorun.S
Comodo	10786	Worm.Win32.AutoRun.nsf
DrWeb	5.0.2.03300	Win32.HLLW.Autoruner.2851
Emsisoft	5.1.0.11	Worm.Win32.AutoRun!IK
eSafe	7.0.17.0	-
eTrust- Vet	37.0.9585	VBS/SillyAutorunScript.L
F- Prot	4.6.5.141	VBS/Autorun.S
F- Secure	9.0.16440.0	Generic.ScriptWorm.51607B57
Fortinet	4.3.370.0	VBS/AutoRun.NSF!worm
GData	22	Generic.ScriptWorm.51607B57
Ikarus	T3.1.1.109.0	Worm.Win32.AutoRun
Jiangmin	13.0.900	VBS/Autorun.a
K7AntiVirus	9.119.5525	EmailWorm
Kaspersky	9.0.0.837	Worm.Win32.AutoRun.nsf
McAfee	5.400.0.1158	VBS/Autorun.worm.k
McAfee- GW- Edition	2010.1D	VBS/Autorun.worm.k
Microsoft	1.7801	Worm:VBS/Autorun.W
NOD32	6656	VBS/AutoRun.S
Norman	6.07.13	AutoRun.JFQ
nProtect	2011- 11- 24.02	Generic.ScriptWorm.51607B57
Panda	10.0.3.5	VBS/Autorun.ADB
PCTools	8.0.0.5	-
Prevx	3.0	-
Rising	23.85.03.02	Worm.Script.VBS.Autorun.cb
Sophos	4.71.0	VBS/Sasan- Fam
SUPERAntiSpyware	4.40.0.1006	-
Symantec	20111.2.0.82	VBS.Runauto
TheHacker	6.7.0.1.347	-
TrendMicro	9.500.0.1008	VBS_AUTORUN.CAJ
VBA32	3.12.16.4	Worm.Win32.AutoRun.nsf
VIPRE	11135	Trojan.VBS.Autorun.a (v)
ViRobot	2011.11.24.4791	VBS.Autorun.7474
VirusBuster	14.1.82.0	VBS.Autorun.EZH

▣요약

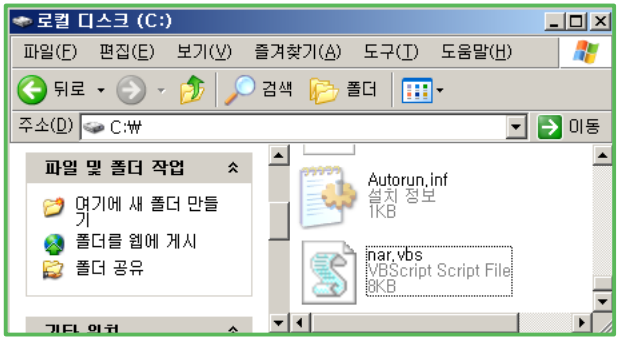
이 악성코드는 이동식 디스크를 통해 자신을 전파하며, 윈도우 폴더와 각 논리 드라이브의 최상위 디렉토리에 자기 자신을 복사하고 Autorun 파일을 생성하며 CD-ROM 및 이동식 디스크가 자동 실행되지 않도록 레지스트리 정보를 수정한다.

▣상세 정보

①악성코드가 실행되면 파일의 위치를 확인하고, 자기 자신을 windows 폴더에 Nar.vbs라는 파일명으로 복사하고 System, Hidden, Read 속성을 설정한다.



②논리 드라이브들의 최상위 디렉토리에 nar.vbs와 Autorun.inf 파일을 생성한다.



③다음 레지스트리를 등록한다.

▶HKLM₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩nar (c:₩windows₩nar.vbs)

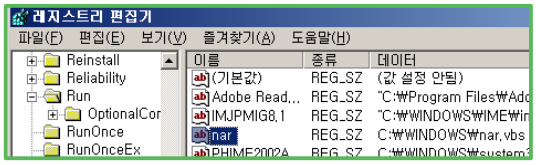
▶HKLM₩SYSTEM₩CurrentControlSet₩Services₩Cdrom₩AutoRun (0)

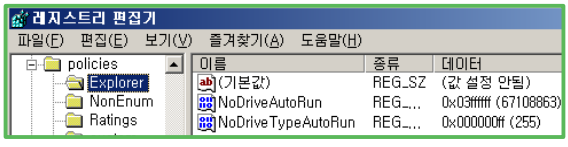
▶HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩policies₩Explorer₩NoDriveTypeAutoRun (255)

▶HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩policies₩Explorer₩NoDriveAutoRun (67108863)

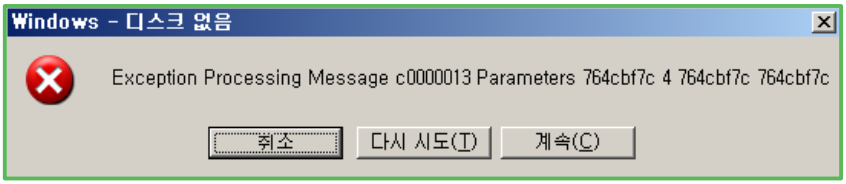
▶HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer₩NoDriveAutoRun (67108863)

▶HKU₩.DEFAULT₩Software₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer₩NoDriveAutoRun (67108863)

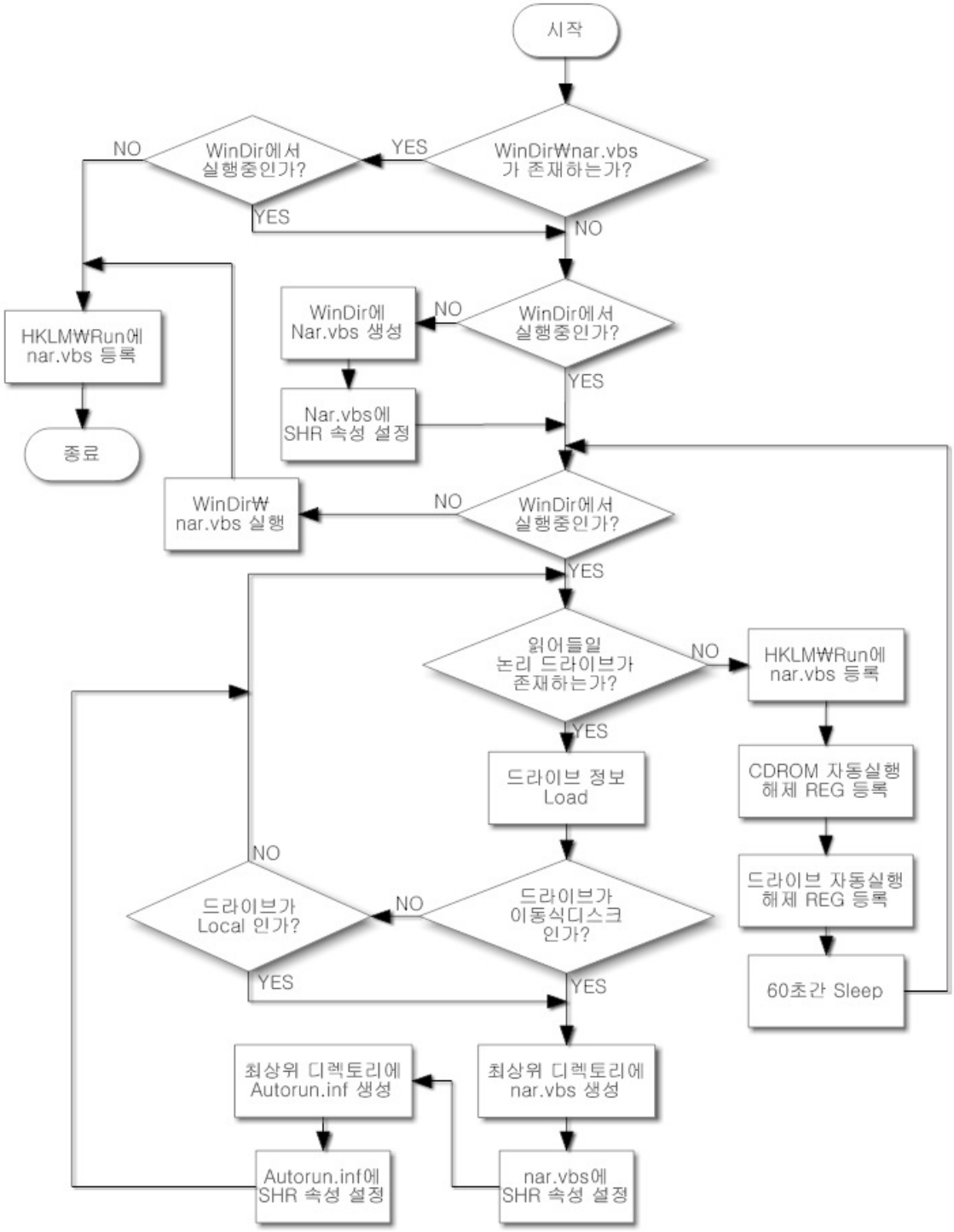




④에러 처리 미흡으로 인해 특정 시스템에서 에러 메시지를 유발한다.



▣실행 순서도



▣마무리

이 악성코드는 이동식 디스크의 자동실행을 방지하도록 레지스트리를 변경하고 기존의 nar.vbs, autorun.inf 파일을 자기 자신으로 덮어쓰는 행위 이외에 다른 행위를 하지 않는 것으로 보아 White Worm 으로써 동작하려고 했던 것으로 보인다. 하지만 코딩이 미흡하여 주기적으로 에러창을 띄우고 과도한 동작으로 인해 좋은 의도마저 묻히는 경향을 보였다.

▣부록

◆분석 메모

※개인적으로 악성코드를 분석하면서 간단하게 메모했던 자료로써, 내용이 지저분하고 뒤죽박죽일 수 있으니 참고용으로만 사용하시기 바랍니다.

7~15 변수 세팅
19~24 현재 실행중인 디렉토리 확인
27 WinDir₩nar.vbs 파일이 존재하지 않거나 현재 윈도우 디렉토리에서 실행중이라면
29 autorun 문자열 저장
30 현재 파일 스트림 오픈
31~34 현재 파일의 내용을 narsource 변수에 저장
37 현재 윈도우 디렉토리에서 실행중이 아니라면
38 윈도우 디렉토리의 Nar.vbs 파일 객체를 얻어온 뒤
39 Archive 속성을 설정하고
40 윈도우 디렉토리에 Nar.vbs 파일을 unicode 형식으로 생성한다.
41 narsource 변수의 내용을 생성한 Nar.vbs 파일에 저장한다.
44 Nar.vbs에 Archive&System&Hidden&ReadOnly 속성을 설정한다.

47 현재 윈도우 디렉토리에서 실행중인 동안
49 disk_Drive 변수에 드라이브 정보를 차례대로 읽어와서
50 읽어들인 드라이브 타입이 이동식디스크이거나 로컬디스크인 경우
52~58 드라이브 최상위 디렉토리에 Nar.vbs을 생성하고 Archive&System&Hidden&ReadOnly 속성을 설정하고
60~66 Autorun.inf 파일을 생성하고 Archive&System&Hidden&ReadOnly 속성을 설정한다.

71 부팅시 Nar.vbs가 자동실행되도록 레지스트리에 등록
72 CDRom이 자동실행되지 않도록 레지스트리 값 변경
73~76 드라이브가 자동 실행되지 않도록 레지스트리 값 변경
79 1분 단위로 실행하기 위해 1분간 Sleep
83 현재 윈도우 디렉토리에서 실행중이 아니라면
85 윈도우 디렉토리의 nar.vbs를 실행
88 부팅시 Nar.vbs가 자동실행되도록 레지스트리에 등록