Win32.Xema.Worm.307200.E
일반 분석 보고서

최초 작성 : 2012년 1월 10일
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	307,200byte
암호화 여부	비암호화	팩킹	
MD5	72C7A16B32B651E08A1B32525340C29C		
SHA1	AF0C2239DB59BE5CE2C05AE93FC2C51D3B07622D		

▣VirusTotal 정보

Antivirus	Version	Result
AhnLab- V3	2012.01.09.00	Win32/Xema.worm.307200.E
AntiVir	7.11.20.203	TR/Crypt.XPACK.Gen
Antiy- AVL	2.0.3.7	Trojan/win32.agent
Avast	6.0.1289.0	Win32:Virut
AVG	10.0.0.1190	I- Worm/VB.TY
BitDefender	7.2	Trojan.Downloader.VB.VMF
ByteHero	1.0.0.1	-
CAT- QuickHeal	12.00	W32.Virut.D
ClamAV	0.97.3.0	W32.Virut.ci
Commtouch	5.3.2.6	W32/Worm.TQT
Comodo	11225	Virus.Win32.Virut.~Q
DrWeb	5.0.2.03300	BackDoor.Generic.1706
Emsisoft	5.1.0.11	Virus.Win32.VB.JED!IK
eSafe	7.0.17.0	Win32.Virut.Ci
eTrust- Vet	37.0.9671	Win32/Virut!corrupt
F- Prot	4.6.5.141	W32/Worm.TQT
F- Secure	9.0.16440.0	Trojan.Downloader.VB.VMF
Fortinet	4.3.388.0	W32/Generic.A@mm
GData	22.342/22.634	Trojan.Downloader.VB.VMF
Ikarus	T3.1.1.109.0	Virus.Win32.VB.JED
Jiangmin	13.0.900	Trojan/VB.dki
K7AntiVirus	9.124.5897	EmailWorm
Kaspersky	9.0.0.837	Email- Worm.Win32.generic
McAfee	5.400.0.1158	W32/Generic.worm.h
McAfee- GW- Edition	2010.1E	W32/Generic.worm.h
Microsoft	1.7903	Worm:Win32/Autorun.CD
NOD32	6780	Win32/AutoRun.ZB
Norman	6.07.13	-
nProtect	2012- 01- 09.01	Dropped:Trojan.Downloader.VB.VMF
Panda	10.0.3.5	Trj/Sinowal.WRE
PCTools	8.0.0.5	-
Prevx	3.0	-
Rising	23.92.00.02	Trojan.Win32.Undef.fky
Sophos	4.73.0	W32/VB- DZU
SUPERAntiSpyware	4.40.0.1006	-
Symantec	20111.2.0.82	W32.Evolym
TheHacker	6.7.0.1.373	W32/Generic
TrendMicro	9.500.0.1008	WORM_VB.GAC
TrendMicro- HouseCall	9.500.0.1008	WORM_VB.GAC
VBA32	3.12.16.4	Win32.AutoRun.ZB
VIPRE	11375	Virus.Win32.Virut.b (v)
ViRobot	2012.1.9.4871	Worm.Win32.Autorun.307392

▣요약

이 악성코드는 이동식 디스크를 통해 자신을 전파하며, 시스템 디렉토리에 자기 자신을 복사하며 레지스트리를 수정한다.

▣상세 정보

①다음 디렉토리에 다음과 같은 이름으로 자기 자신을 복사한다.

▶C:₩Windows₩system32₩autochl.exe

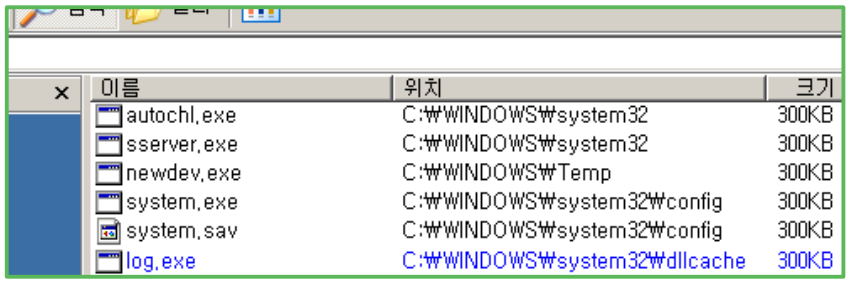
▶C:₩Windows₩system32₩sserver.exe

▶C:₩Windows₩system32₩config₩system.exe

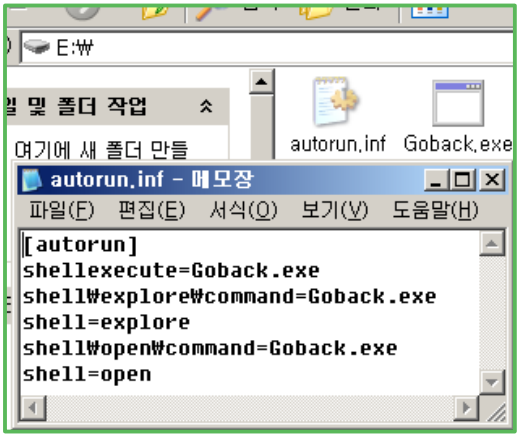
▶C:₩Windows₩system32₩config₩system.sav

▶C:₩Windows₩Temp₩newdev.exe

▶C:₩Windows₩system32₩dllcache₩log.exe



②이동식 디스크에 자기 자신을 복사하고 Autorun.inf 파일을 생성한다.



③다음 레지스트리를 등록한다.

▶HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Policies₩Explorer₩NoDriveTypeAutoRun (145)

▶HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩Advanced₩Folder₩Hidden₩SHOWALL₩CheckedValue (0)

▶HKLM₩SOFTWARE₩Microsoft₩Windows NT₩CurrentVersion₩Winlogon₩shell (explorer.exe c:windows₩system32₩sserver.exe)