Win32.FlyStudio.Worm.1289331
일반 분석 보고서

최초 작성 : 2012년 3월 5일

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	1,289,331byte
암호화 여부	비암호화	팩킹	
MD5	2166A3F7687F8CE2A812F171891D3C45		
SHA1	6C66D61BCE7A96FA12509047E0E7AB0298D7533C		

▣VirusTotal 정보

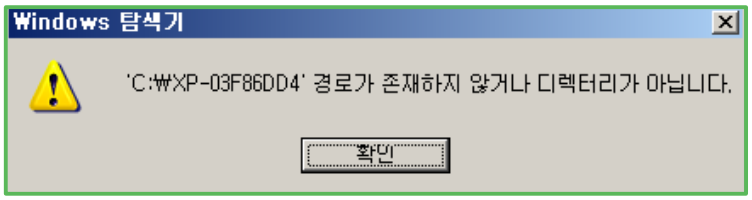
Antivirus	Result	Update
AhnLab- V3	-	20120305
AntiVir	TR/Drop.Agent.qsc	20120305
Antiy- AVL	-	20120305
Avast	Win32:AutoRun- BPV [Drp]	20120305
AVG	Citem_c.CLT	20120305
BitDefender	Worm.Generic.43288	20120305
ByteHero	-	20120305
CAT- QuickHeal	Win32.TrojanDropper.Silly_P2P.B.6	20120305
ClamAV	Trojan.Dropper- 2514	20120305
Commtouch	W32/Nuj.A.gen!Eldorado	20120304
Comodo	ApplicUnsaf.Win32.HackTool.FlySky.AC	20120305
DrWeb	Trojan.DownLoad.28634	20120305
Emsisoft	Trojan- Spy.Win32.FlyStudio!IK	20120305
eSafe	Win32.TRDrop.Agent.Q	20120305
eTrust- Vet	Win32/Nuj.A	20120305
F- Prot	W32/Nuj.A.gen!Eldorado	20120304
F- Secure	Trojan- Downloader:W32/VB.BUE	20120305
Fortinet	W32/BDoor.DRV!tr	20120305
GData	Worm.Generic.43288	20120305
Ikarus	Trojan- Spy.Win32.FlyStudio	20120305
Jiangmin	TrojanDownloader.VB.adh	20120301
K7AntiVirus	Riskware	20120302
Kaspersky	Worm.Win32.FlyStudio.bf	20120305
McAfee	W32/Autorun.worm.dq	20120305
McAfee- GW- Edition	W32/Autorun.worm.dq	20120304
Microsoft	Worm:Win32/Nuj.A	20120305
NOD32	Win32/AutoRun.FlyStudio.AG	20120305
Norman	W32/Obfuscated.H!genr	20120304
nProtect	Worm.Generic.43288	20120305
Panda	W32/FlySky.AD	20120305
Rising	Worm.Win32.Autorun.eyr	20120305
Sophos	W32/AutoRun- MO	20120305
Symantec	W32.SillyFDC	20120305
TheHacker	Trojan/Downloader.FlyStudio.ho	20120305
TrendMicro	WORM_FLYSTUDI.IQ	20120304
TrendMicro- HouseCall	WORM_FLYSTUDI.IQ	20120305
VBA32	Trojan.HLLW.Erun.507	20120305
VIPRE	Trojan.Win32.Generic!BT	20120305
ViRobot	Worm.Win32.S.FlyStudio.1289331.B	20120305

▣요약

이 악성코드는 이동식 디스크를 통해 자신을 전파하며, 시스템 디렉토리 및 임시폴더에 자기 자신을 복사하며 특정 사이트에 접근을 시도한다.

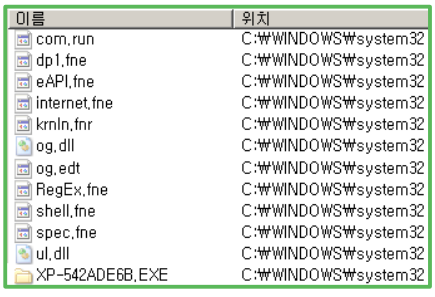
▣상세 정보

①실행하면 다음과 같은 대화창을 띄운다.

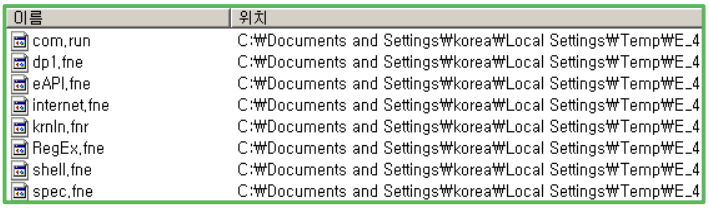


②다음 디렉토리에 다음 파일을 생성한다.

▶C:₩Doc~1₩User₩Local Settings₩Temp₩E_4₩krnln.fnr
▶C:₩Doc~1₩User₩Local Settings₩Temp₩E_4₩shell.fne
▶C:₩Doc~1₩User₩Local Settings₩Temp₩E_4₩eAPI.fne
▶C:₩Doc~1₩User₩Local Settings₩Temp₩E_4₩internet.fne
▶C:₩Doc~1₩User₩Local Settings₩Temp₩E_4₩spec.fne
▶C:₩Doc~1₩User₩Local Settings₩Temp₩E_4₩RegEx.fne
▶C:₩Doc~1₩User₩Local Settings₩Temp₩E_4₩dp1.fne
▶C:₩Doc~1₩User₩Local Settings₩Temp₩E_4₩com.run
▶C:₩Windows₩system32₩XP-(랜덤8자).exe
▶C:₩Windows₩system32₩RegEx.fne
▶C:₩Windows₩system32₩com.run
▶C:₩Windows₩system32₩dp1.fne
▶C:₩Windows₩system32₩eAPI.fne
▶C:₩Windows₩system32₩internet.fne
▶C:₩Windows₩system32₩krnln.fnr
▶C:₩Windows₩system32₩shell.fne
▶C:₩Windows₩system32₩spec.fne
▶C:₩Windows₩system32₩ul.dll
▶C:₩Windows₩system32₩og.dll
▶C:₩Windows₩system32₩og.edt



이름	위치
com.run	C:₩WINDOWS₩system32
dp1.fne	C:₩WINDOWS₩system32
eAPI.fne	C:₩WINDOWS₩system32
internet.fne	C:₩WINDOWS₩system32
krnln.fnr	C:₩WINDOWS₩system32
og.dll	C:₩WINDOWS₩system32
og.edt	C:₩WINDOWS₩system32
RegEx.fne	C:₩WINDOWS₩system32
shell.fne	C:₩WINDOWS₩system32
spec.fne	C:₩WINDOWS₩system32
ul.dll	C:₩WINDOWS₩system32
XP-542ADE6B.EXE	C:₩WINDOWS₩system32



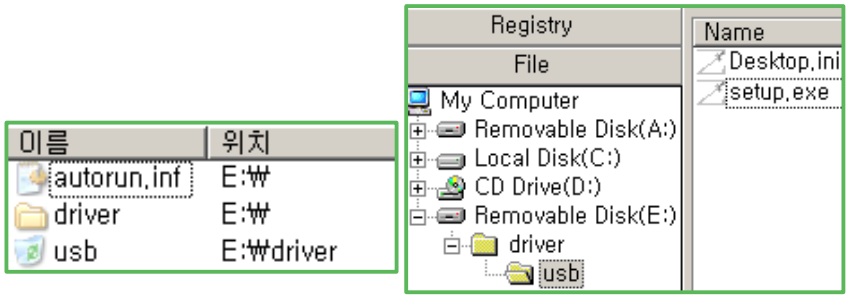
이름	위치
com.run	C:₩Documents and Settings₩korea₩Local Settings₩Temp₩E_4
dp1.fne	C:₩Documents and Settings₩korea₩Local Settings₩Temp₩E_4
eAPI.fne	C:₩Documents and Settings₩korea₩Local Settings₩Temp₩E_4
internet.fne	C:₩Documents and Settings₩korea₩Local Settings₩Temp₩E_4
krnln.fnr	C:₩Documents and Settings₩korea₩Local Settings₩Temp₩E_4
RegEx.fne	C:₩Documents and Settings₩korea₩Local Settings₩Temp₩E_4
shell.fne	C:₩Documents and Settings₩korea₩Local Settings₩Temp₩E_4
spec.fne	C:₩Documents and Settings₩korea₩Local Settings₩Temp₩E_4

③이동식 디스크에 다음 파일을 생성한다.

▶₩autorun.inf

▶₩driver₩usb₩Desktop.ini

▶₩driver₩usb₩setup.exe



④시작 프로그램에 빈 문자열의 파일명으로 자신을 등록한다.

⑤다음 도메인 네임을 질의 하고 접속을 시도한다.

▶www.microsoft.com

▶www.google.com

▶hi.baidu.com

▶www.baihe.googlepages.com

▶www.bloguser.googlepages.com

▶sites.google.com

Protocol	Info
DNS	Standard query A www.microsoft.com
DNS	Standard query response CNAME toggle.www.ms.akadns.net CNAME g.
DNS	Standard query A hi.baidu.com
DNS	Standard query response CNAME hi.n.shifen.com A 123.125.115.35
DNS	Standard query A www.baihe.googlepages.com
DNS	Standard query response CNAME www3.l.google.com A 74.125.235.69
DNS	Standard query A www.bloguser.googlepages.com
DNS	Standard query response CNAME www3.l.google.com A 74.125.235.98
DNS	Standard query A sites.google.com
DNS	Standard query response CNAME www3.l.google.com A 74.125.235.13