Win32.Trojan.Pearmor.416768
일반 분석 보고서

최초 작성 : 2012년 3월 8일

작성자 : 김부성

홈페이지 : http://www.chosik.com

이메일 : kbs6880@gmail.com

▣기본 정보

종류	Trojan	위험도	낮음
감염경로	이동식 디스크	증상	시스템 설정 변경
플랫폼	Windows	크기	416,768byte
암호화 여부	비암호화	팩킹	ASPack 2.12
MD5	2F450D4CF7E655AF0DDFF5B928C17FE0		
SHA1	B7D53FD7DA65B86937E4AB2E765195DC2F4AE858		

▣VirusTotal 정보

Antivirus	Result	Update
AhnLab- V3	Win- Trojan/Pearmor.416768	20120308
AntiVir	TR/Crypt.ASPM.Gen	20120308
Antiy- AVL	-	20120305
Avast	Win32:Pakes- TH [Trj]	20120308
AVG	Win32/Kenfa	20120307
BitDefender	Backdoor.Hupigon.41550	20120307
ByteHero	-	20120305
CAT- QuickHeal	(Suspicious) - DNAScan	20120307
ClamAV	PUA.Packed.ASPack	20120307
Commtouch	W32/Troj_Obfusc.N.gen!Eldorado	20120307
Comodo	TrojWare.Win32.Trojan.Agent.Gen	20120307
DrWeb	Win32.HLLW.Autoruner.1267	20120307
Emsisoft	Backdoor.Win32.Hupigon!IK	20120308
eSafe	Win32.TRCrypt.Aspm	20120305
F- Prot	W32/Troj_Obfusc.N.gen!Eldorado	20120307
F- Secure	Backdoor.Hupigon.41550	20120307
GData	Backdoor.Hupigon.41550	20120307
Ikarus	Backdoor.Win32.Hupigon	20120308
Jiangmin	Backdoor/Hupigon.cdqv	20120301
K7AntiVirus	Riskware	20120307
Kaspersky	Worm.Win32.Runfer.dvu	20120307
McAfee	Artemis!2F450D4CF7E6	20120307
McAfee- GW- Edition	Heuristic.LooksLike.Win32.EPO.C	20120307
Microsoft	Backdoor:Win32/Hupigon.DF	20120308
NOD32	probably a variant of Win32/Fujacks	20120307
Norman	W32/Packed_PEArmor.C	20120304
nProtect	Worm/W32.Runfer.416768	20120307
Panda	Bck/Hupigon.LNX	20120308
PCTools	Backdoor.Graybird	20120228
Rising	Backdoor.Win32.ShangXing.kf	20120307
Sophos	Mal/DSpy- B	20120308
Symantec	Backdoor.Graybird!Gen	20120305
TheHacker	W32/Runfer.ads	20120308
TrendMicro	TROJ_GEN.R47CRAC	20120308
TrendMicro- HouseCall	TROJ_GEN.R47CRAC	20120308
VBA32	Backdoor.Win32.Hupigon.bafb	20120307
VIPRE	Trojan.Win32.Generic!BT	20120308
ViRobot	Backdoor.Win32.Hupigon.416768.C	20120308
VirusBuster	Packed/PE- Armor	20120308

▣요약

이 악성코드는 이동식 디스크를 통해 자신을 전파하며, 시스템 디렉토리 및 루트 디렉토리에 자기자신을 복사한다.

▣상세 정보

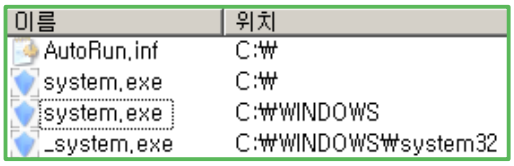
①다음 디렉토리에 다음 파일을 생성한다.

▶c:₩windows₩system.exe

▶c:₩windows₩system32₩_system.exe

▶[루트 디렉토리]:₩autorun.inf

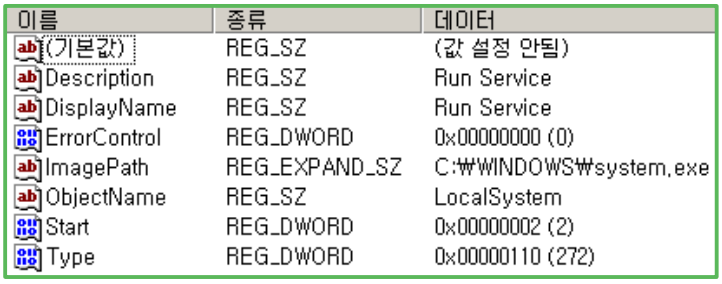
▶[루트 디렉토리]:₩system.exe



이름	위치
AutoRun.inf	C:₩
system.exe	C:₩
system.exe	C:₩WINDOWS
_system.exe	C:₩WINDOWS₩system32

②다음 레지스트리를 등록한다.

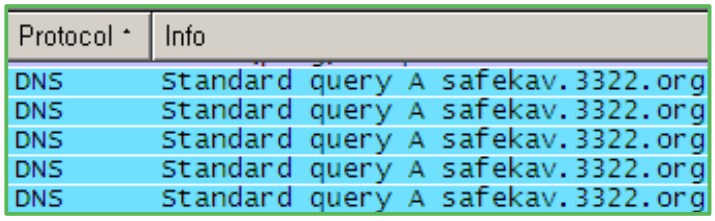
▶HKLM₩SYSTEM₩CurrentControlSet₩Services₩Run Service



이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안됨)
Description	REG_SZ	Run Service
DisplayName	REG_SZ	Run Service
ErrorControl	REG_DWORD	0x00000000 (0)
ImagePath	REG_EXPAND_SZ	C:₩WINDOWS₩system.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000110 (272)

③다음 도메인 네임을 질의 하고 접속을 시도한다.

▶safekv.3322.org



Protocol	Info
DNS	Standard query A safekav.3322.org
DNS	Standard query A safekav.3322.org
DNS	Standard query A safekav.3322.org
DNS	Standard query A safekav.3322.org
DNS	Standard query A safekav.3322.org