Win32/Backdoor.Worm.IRCBot.23552
상세 분석 보고서

최초 작성 : 2011년 05월 09일
1차 수정 : 2011년 05월 23일
작성자 : 김부성
홈페이지 : http://www.choslk.com
이메일 : kbs6880@gmail.com

▣기본 정보

종류	Backdoor	위험도	높음
감염경로	이동식 디스크, 보안 취약점	증상	원격 코드 실행
플랫폼	Windows	크기	23,552byte
암호화 여부	문자열 암호화	팩킹	kkrunchy
MD5	21FB327E99105F1D2816CE9731770695		
SHA1	5EA7693143A2F66BC64213DE21CB939C216EF03B		

▣VirusTotal 정보

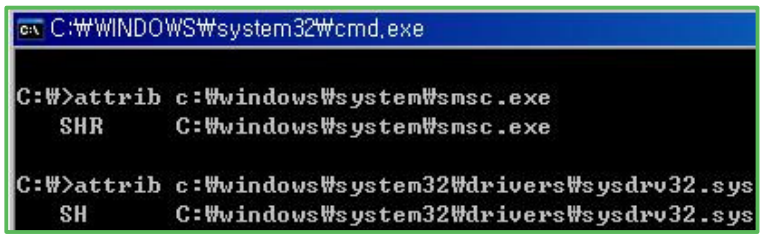
Antivirus	Version	Result
AhnLab- V3	2011.05.09.00	Win32/IRCBot.worm.23552.G
AntiVir	7.11.7.179	TR/Dropper.Gen
Antiy- AVL	2.0.3.7	Backdoor/Win32.IRCBot.gen
Avast	4.8.1351.0	Win32:IRCBot- DMJ
Avast5	5.0.677.0	Win32:IRCBot- DMJ
AVG	10.0.0.1190	IRC/BackDoor.SdBot4.RAY
BitDefender	7.2	IRC- Worm.Generic.5032
CAT- QuickHeal	11.00	Backdoor.IRCBot.jhz
ClamAV	0.97.0.0	Trojan.IRCBot- 3783
Commtouch	5.3.2.6	W32/Ircbot.ABZ
Comodo	8631	-
DrWeb	5.0.2.03300	BackDoor.IRC.Sdbot.4844
eSafe	7.0.17.0	Win32.TRCrypt.XPACK
eTrust- Vet	36.1.8312	Win32/IRCBot.MG
F- Prot	4.6.2.117	W32/Ircbot.ABZ
Fortinet	4.2.257.0	W32/IRCBot.JHZ!tr.bdr
GData	22	IRC- Worm.Generic.5032
Ikarus	T3.1.1.103.0	Net- Worm.Win32.Kolab
Jiangmin	13.0.900	Backdoor/IRCBot.fpl
K7AntiVirus	9.102.4584	Backdoor
Kaspersky	9.0.0.837	Net- Worm.Win32.Kolab.dww
McAfee	5.400.0.1158	W32/Sdbot.dr!ADA37D45
McAfee- GW- Edition	2010.1D	W32/Sdbot.dr!ADA37D45
Microsoft	1.6802	Worm:Win32/Neeris.AU
NOD32	6105	Win32/IRCBot.AMC
Norman	6.07.07	W32/Smalltroj.dam
Panda	10.0.3.5	W32/Ircbot.CNJ.worm
PCTools	7.0.3.5	Backdoor.Sdbot!sd6
Prevx	3.0	High Risk System Back Door
Rising	23.56.06.05	Trojan.Win32.Generic.11ED3EE4
Sophos	4.65.0	W32/IRCbot- AEL
SUPERAntiSpyware	4.40.0.1006	Trojan.Agent/Gen.Process
Symantec	20101.3.2.89	W32.Spybot.Worm
TheHacker	6.7.0.1.191	W32/Kolab.dww
TrendMicro	9.200.0.1012	WORM_NEERIS.SM
TrendMicro- HouseCall	9.200.0.1012	WORM_NEERIS.SM
VBA32	3.12.16.0	Malware- Cryptor.General.6
VIPRE	9229	Backdoor.IRCBot
ViRobot	2011.5.9.4451	Backdoor.Win32.IRCBot.23552.P
VirusBuster	13.6.343.0	Backdoor.IRCBot.ADZR

▣요약

이 악성코드는 이동식 디스크와 네트워크를 통해 자신을 전파하며, 시스템 폴더에 자신을 복사하고 레지스트리를 조작하여 시작 프로그램과 방화벽 정책을 수정한다. 또한, 특정 서버에 접속을 시도하며 서버의 원격 명령을 수행한다.

▣상세 정보

①악성코드가 실행되면 파일의 위치를 확인하고, 자신을 %system% 폴더에 smsc.exe라는 파일명으로 복사하고 System, Hidden, Read 속성을 설정한다.

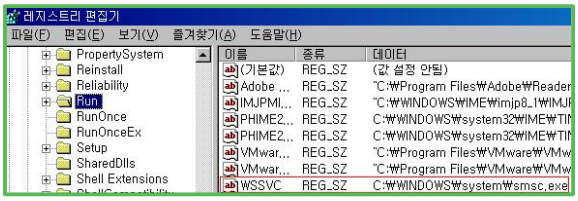


②다음 레지스트리를 등록한다.

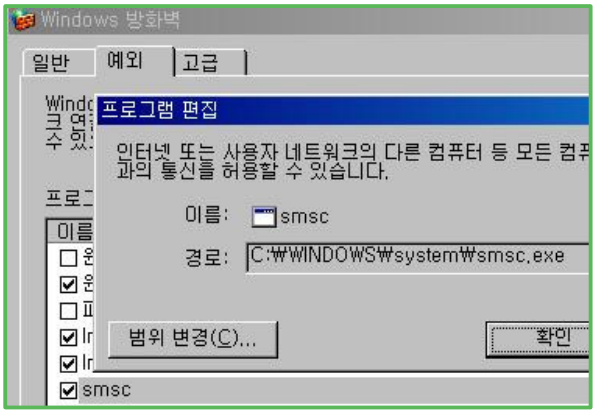
▶HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run₩WSSVC(c:₩windows₩system₩smsc.exe)

▶HKLM₩SYSTEM₩CurrentControlSet₩Control₩SafeBoot₩Minimal₩SVCWINSPOOL₩Default(Service)

▶HKLM₩SYSTEM₩CurrentControlSet₩Control₩SafeBoot₩Network₩SVCWINSPOOL₩Default(Service)

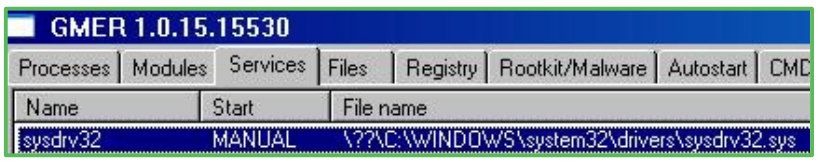


③방화벽에 자신을 예외 등록한다.

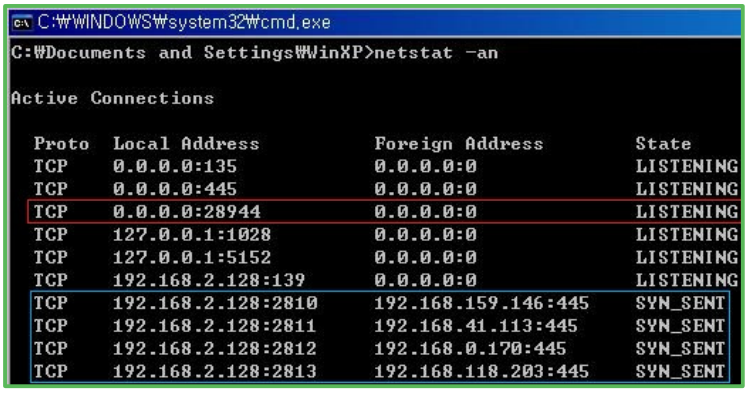


④%system32%폴더에 sysdrv32.sys 파일을 생성하고 System, Hidden 속성을 설정한다.

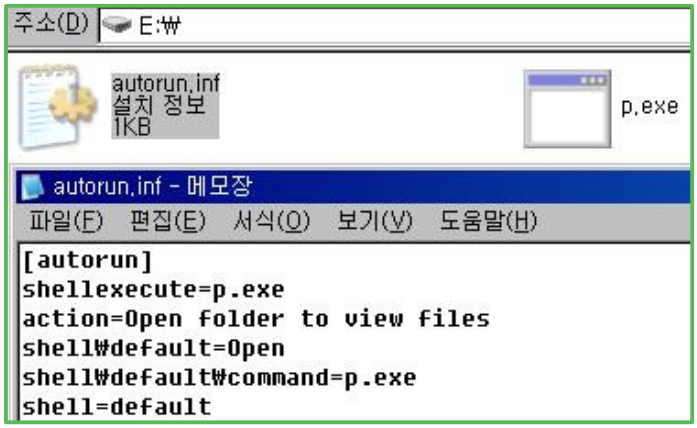
⑤sysdrv32 서비스를 등록한다.



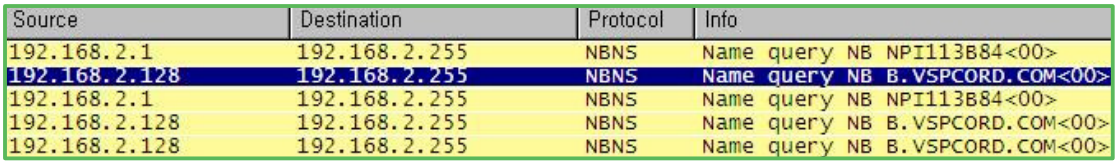
⑥임의의 포트를 열고 자기 자신을 배포할 준비를 한다.
⑦같은 네트워크대역의 취약 호스트를 탐색하고 감염시킨다.



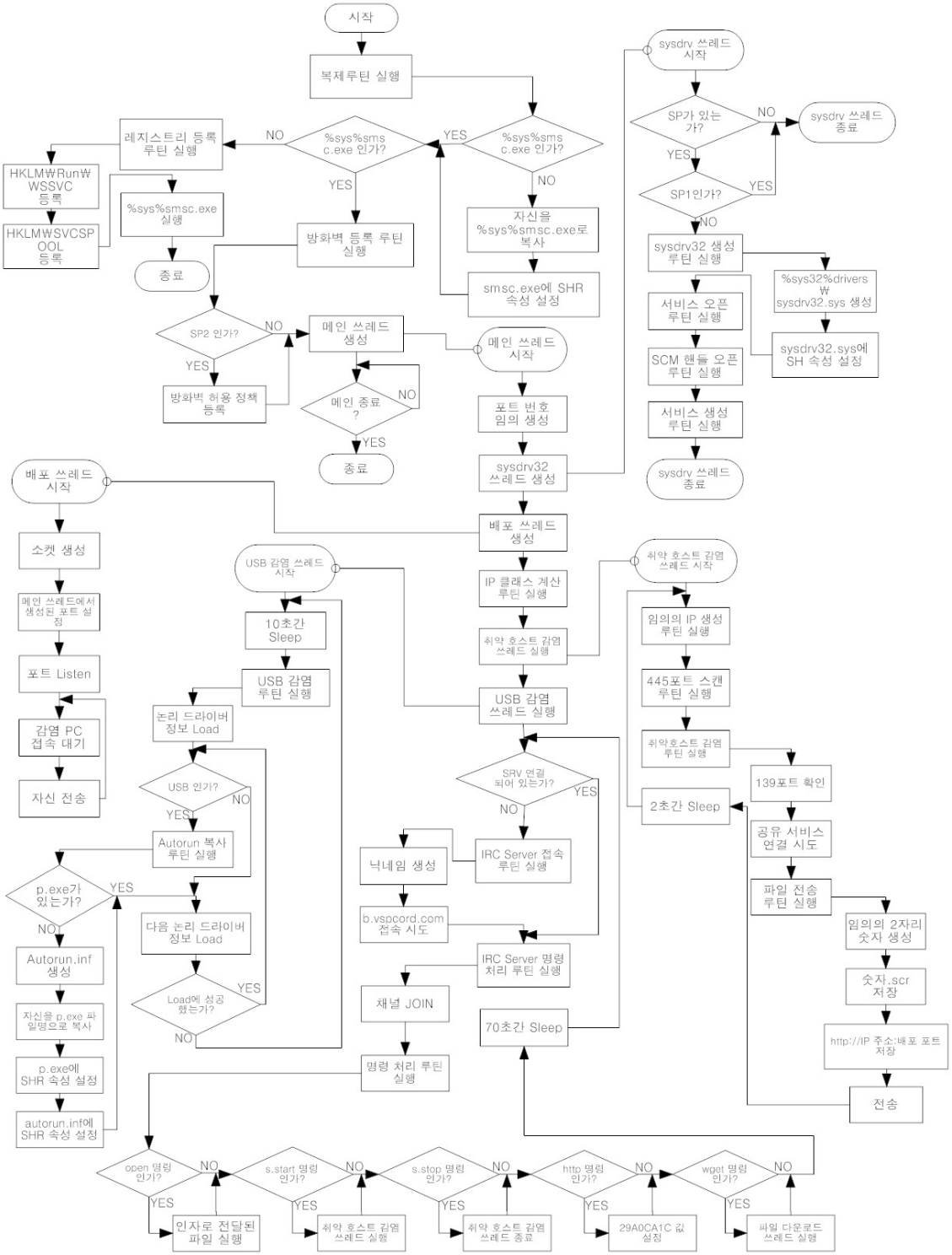
⑧이동식 디스크 연결시 자기 자신을 p.exe라는 파일명으로 감염시키고 autorun.inf 파일을 생성한 뒤 System, Hidden, Read 속성을 설정한다.



⑨IRC Server(b.vspcord.com)에 접속하고 해커의 명령을 기다린다.



▣실행 순서도


시작
복제루틴 실행
%sys%sms c.exe 인가?
YES
NO
레지스트리 등록 루틴 실행
HKLM₩Run₩WSSVC 등록
HKLM₩SVCSPOOL 등록
%sys%smsc.exe 실행
종료
방화벽 등록 루틴 실행
%sys%sms c.exe 인가?
자신을 %sys%smsc.exe로 복사
smsc.exe에 SHR 속성 설정
SP2 인가?
방화벽 허용 정책 등록
메인 쓰레드 생성
메인 종료 ?
메인 쓰레드 시작
포트 번호 임의 생성
sysdrv32 쓰레드 생성
sysdrv 쓰레드 시작
SP가 있는가?
sysdrv 쓰레드 종료
SP1인가?
sysdrv32 생성 루틴 실행
%sys32%drivers₩sysdrv32.sys 생성
서비스 오픈 루틴 실행
SCM 핸들 오픈 루틴 실행
sysdrv32.sys에 SH 속성 설정
서비스 생성 루틴 실행
sysdrv 쓰레드 종료
배포 쓰레드 시작
배포 쓰레드 생성
소켓 생성
메인 쓰레드에서 생성된 포트 설정
포트 Listen
감염 PC 접속 대기
자신 전송
USB 감염 쓰레드 시작
10초간 Sleep
USB 감염 루틴 실행
논리 드라이버 정보 Load
USB 인가?
Autorun 복사 루틴 실행
p.exe가 있는가?
다음 논리 드라이버 정보 Load
Load에 성공 했는가?
Autorun.inf 생성
자신을 p.exe 파일명으로 복사
p.exe에 SHR 속성 설정
autorun.inf에 SHR 속성 설정
USB 감염 쓰레드 실행
IP 클래스 계산 루틴 실행
취약 호스트 감염 쓰레드 실행
취약 호스트 감염 쓰레드 시작
임의의 IP 생성 루틴 실행
445포트 스캔 루틴 실행
취약호스트 감염 루틴 실행
2초간 Sleep
139포트 확인
공유 서비스 연결 시도
파일 전송 루틴 실행
임의의 2자리 숫자 생성
숫자.scr 저장
http://IP 주소:배포 포트 저장
전송
SRV 연결 되어 있는가?
IRC Server 접속 루틴 실행
닉네임 생성
b.vspcord.com 접속 시도
IRC Server 명령 처리 루틴 실행
채널 JOIN
명령 처리 루틴 실행
70초간 Sleep
open 명령인가?
인자로 전달된 파일 실행
s.start 명령인가?
취약 호스트 감염 쓰레드 실행
s.stop 명령인가?
취약 호스트 감염 쓰레드 종료
http 명령인가?
29A0CA1C 값 설정
wget 명령인가?
파일 다운로드 쓰레드 실행

▣Server 정보

①요약 정보

서버 작동 여부	미작동			
기본정보	서버 종류	IRC Server	도메인	b.vspcord.com
	IP 주소	211.233.91.10	Port 번호	988
추가정보	패스워드	h4xg4ng	채널명	#lox

②명령의 실행

감염 PC의 명령실행은 접속된 IRC Server의 채널 TOPIC 값을 전달받음으로써 실행된다.

③명령의 입력

해커는 IRC Server의 채널에 접속하여 TOPIC 값을 **$dec(!명령)**의 포맷으로 입력하여 감염 PC에게 명령을 전달한다.

ex:)/TOPIC #lox $dec(!s.start 10 5 3 -r -e)

④명령표

명령 포맷	설명	
open [파일명]	파일을 백그라운드로 실행한다.	
r3	SVCWINSPOOL 서비스를 실행한다.	
s.start [0-128] [1-60] [1-3] [-r | -s] [-e]	취약 호스트 탐색 쓰레드를 실행한다.	
	옵션	설명
	[0-128]	쓰레드 갯수
	[1-60]	탐색 텀 (초 단위)
	[1-3]	감염 IP 네트워크 대역 (A,B,C 클래스)
	[-r]	네트워크 호스트 대역을 x로 저장
	[-s]	네트워크 호스트 대역을 0으로 저장
	[-e]	네트워크 대역 계산에 사용할 IP 주소에 공인 IP 주소를 이용한다. (미설정시 사설 IP)
s.stop	취약 호스트 탐색 쓰레드를 종료한다.	
http [stop]	stop 인자가 전달되면 29A0CA1C 위치의 메모리 값을 0으로 세팅한다. (정확한 동작은 미확인)	
wget [URL주소] [-n]	URL 주소로부터 파일을 내려받아 실행시킨다.	
	옵션	설명
	[-n]	IRC Server 접속을 종료한다.

▣마무리

리버싱을 흥미를 가지고 공부하면서 저를 괴롭히던 이 악성코드를 직접 분석해내고 말겠다는 각오 아래 부족한 실력으로 분석을 시작했습니다.

첫 리버싱 결과물이고 부족한 점이 많아 잘못된 분석이 많이 있을지도 모르지만 저처럼 리버싱을 시작하고자 하는 분들에게 조금이나마 도움이 되는 자료가 되었으면 좋겠습니다.

추가1 > 많은 분들이 처음 작성된 보고서 내용에 대해 관심을 가지고 지적해주셨던 부분에 대하여 미약하게나마 보완하여 수정된 보고서를 작성하였습니다. 역시나 제 실력이 미약하여 IRC Server의 명령 처리에 대해 완벽하게 알아내지는 못하였지만 어설프게나마 명령표도 작성되었습니다. 보고서에 대한 지적 사항 또는 추가 사항은 제 블로그에 남겨주시면 감사히 받아들이겠습니다.

▣부록

◆리버싱 분석 메모(Unpacked)

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

==========최초 실행 파일==========

29A05F7D 최초 메인 루틴

29A0607E　　자기 복제 루틴을 실행한다.(29A068F0)
29A06091　　현재 실행되고 있는 프로세스가 c:₩windows₩system₩smsc.exe인지 확인하고 맞다면 복제파일 실행 루틴으로 점프한다.
29A0609F　　레지스트리 등록 루틴을 실행한다.(29A066E9)
29A060ED　　c:₩windows₩system₩smsc.exe를 실행한다.
29A0612C　　자기자신을 종료한다.

29A068F0 (최초 자기 복제 루틴) 실행폴더->SYSTEM폴더₩smsc.exe

29A06990　　현재 실행되고 있는 프로세스가 c:₩windows₩system₩smsc.exe인지 확인하고 맞다면 파일 복사 루틴을 건너뛴다.
29A069AE　　c:₩windows₩system₩smsc.exe이 존재하는지 확인하고 존재하면 파일 속성을 일반파일로 변경한다.
29A069D8　　자기자신을 c:₩windows₩system₩smsc.exe로 복사한다.
29A06A1D　　c:₩windows₩system₩smsc.exe 파일에 읽기전용,숨김,시스템파일 속성을 설정한다.

29A066E9 (레지스트리 등록 루틴)

29A06755　　윈도우 시작시 자동실행이 되도록 HKLM₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Run에 WSSVC라는 이름으로 c:₩windows₩system₩smsc.exe를 등록
29A06820　　HKLM₩SYSTEM₩CurrentControlSet₩Control₩SafeBoot₩Minimal에 SVCWINSPOOL라는 이름으로 서브키를 생성한다.
29A06848　　HKLM₩SYSTEM₩CurrentControlSet₩Control₩SafeBoot₩Minimal₩SVCWINSPOOL의 기본값을 Service로 설정한다.
29A068AB　　HKLM₩SYSTEM₩CurrentControlSet₩Control₩SafeBoot₩Network에 SVCWINSPOOL라는 이름으로 서브키를 생성한다.
29A068D3　　HKLM₩SYSTEM₩CurrentControlSet₩Control₩SafeBoot₩Network₩SVCWINSPOOL의 기본값을 Service로 설정한다.

==========c:₩windows₩system₩smsc.exe==========

29A06132 복제 파일 실행 루틴

29A06140 방화벽 추가 루틴을 실행한다.(29A0705A)
29A0615B 메인 루틴 쓰레드를 생성한다.(29A0617F)
29A0616A 메인 루틴이 종료되기를 기다린다.(29A0617F)
29A06171 핸들을 종료하고 프로세스 실행을 종료한다.

29A0705A (방화벽 추가 루틴)

29A070EF 현재 운영체제가 WinXP SP2인지 확인한다. (SP2가 아니면 루틴 종료)
29A07164 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩SharedAccess₩Parameters₩FirewallPolicy₩StandardProfile₩AuthorizedApplications₩List에 자기자신을 추가하여 방화벽에 예외처리한다.
(값 : C:₩WINDOWS₩system₩smsc.exe:*:Microsoft Enabled)

29A0617F 메인 루틴

29A062BE 파일 배포 쓰레드에서 Listen 포트로 사용할 값을 랜덤으로 생성한다.
29A062EB sysdrv32.sys 관련 쓰레드를 생성한다.(29A01000)
29A062FF 파일 배포 쓰레드를 생성한다.(29A01CA4)
29A0632F 네트워크 대역 계산 루틴을 실행한다.(29A027E7)
29A0636E 취약 호스트 탐색&감염 쓰레드 실행 쓰레드를 생성한다.(29A025B7)
29A0639F USB 감염(메인) 쓰레드를 생성한다.(29A034F4)
29A063C5 IRC Server 접속 루틴을 실행한다.(29A04A39)
29A063D0 IRC Server 응답 처리 루틴(?)을 실행한다.(29A04E37)

29A01000 sysdrv32.sys 관련 쓰레드

29A0108F 서비스팩이 없는지 확인한다.
29A010A3 서비스팩1인지 확인한다.
29A010EE sysdrv32.sys 생성 루틴을 실행한다.(29A01159)
20A010FF 서비스 오픈 루틴을 실행한다.(29A0139E)
29A01104 SCM 핸들 오픈 루틴을 실행한다.(29A011AB)
29A0111B 서비스 생성 루틴을 실행한다.(29A011F9)

29A01159 sysdrv32.sys 생성 루틴

29A01185 system32₩drivers 폴더에 sysdrv32.sys 파일을 생성한다.
29A01196 sysdrv32.sys 파일에 숨김,시스템 파일 속성을 설정한다.
29A011A1 5초간 Sleep 한다.

29A0139E 서비스 오픈 루틴

29A013BF　　sysdrv32 서비스를 오픈한다.

　　서비스명:sysdrv32

　　접근권한:ALLUSERSPROFILE=C:₩Documents and Settings₩All Users

29A011AB SCM 핸들 오픈 루틴

29A011B8　　SCM 핸들을 오픈한다.

29A011F9 서비스 생성 루틴

29A0124D　　sysdrv32 서비스를 오픈한다.

29A012A9　　sysdrv32 서비스를 생성한다.

　　ServiceName = "sysdrv32"

　　DisplayName = "Play Port I/O Driver"

　　DesiredAccess = SERVICE_QUERY_STATUS|SERVICE_START|SERVICE_STOP|10000

　　ServiceType = SERVICE_KERNEL_DRIVER

　　StartType = SERVICE_DEMAND_START

　　ErrorControl = SERVICE_ERROR_NORMAL

　　BinaryPathName = "C:₩WINDOWS₩system32₩drivers₩sysdrv32.sys"

　　LoadOrderGroup = "SST wanport drivers"

　　pTagId = NULL

　　pDependencies = NULL

　　ServiceStartName = NULL

　　Password = NULL

29A012F2 서비스 실행 루틴

29A0131A　　sysdrv32 서비스를 오픈한다.

29A0136A　　sysdrv32 서비스를 실행한다.

29A01CA4 (파일 배포 쓰레드)

29A01CDE　　소켓을 생성한다.

29A01CF7　　소켓에 SO_REUSEADDR 속성을 설정한다.

29A01D19　　인자로 넘어온 랜덤 값을 이용하여 포트를 설정한다.

29A01D2A　　소켓을 바인딩한다.

29A01D3B　　설정된 포트로 Listen 한다.

29A01D82 application/octet-stream 값을 저장한다.
29A01DA2 현재 파일명을 읽어와서 EBP-430(E6FB84)에 저장한다.
29A01DBA 읽어들인 파일명을 이용하여 GENERIC_READFILE_SHARE_READ,OPEN_EXISTING 모드로 오픈한다.
29A01DD2 파일의 크기를 읽어온다.
29A01DD9 파일의 크기를 EBP-20(E6FF94)에 저장한다.
29A01DDC 오픈한 파일의 핸들을 종료한다.
29A01DF8 날짜 포맷을 EBP-24(E6FE90)에 저장한다.
29A01E45 감염 PC의 접속을 기다린다.
29A01F04 패킷을 읽어들인다.
29A01F6C 패킷의 내용에 "GET "이 포함되는지 확인한다.
29A01FEC 응답 패킷 문자열을 생성하여 EBP-19C0(E6E5F4)에 저장한다.

```
HTTP/1.0 200 OK
Server: private
Cache-Control: no-cache,no-store,max-age=0
pragma: no-cache
Content-Type: application/octet-stream
Content-Length: 23552
Accept-Ranges: bytes
Date: Thu, 07 Apr 2011 16:30:12 GMT
Last-Modified: Th"...
```

29A0200F 생성한 패킷을 전송한다.
29A02032 자기자신을 GENERIC_READFILE_SHARE_READ,OPEN_EXISTING 모드로 오픈한다.
29A0204A 파일의 크기를 구한다.
29A02092 파일을 읽어들인다.
29A020A6 데이터를 전송한다.
29A020CE 파일핸들을 종료한다.
29A020DF 소켓을 종료한다.
29A020E5 다시 새로운 접속을 기다리기 위해 29A01E23으로 점프한다.

29A027E7 네트워크 대역 계산 루틴
첫번째 인자 : Host IP 주소
두번째 인자 : 1=나머지 x 채움
0=나머지 0 채움
세번째 인자 : 네트워크 대역

29A0280E EBP-2C(B6FC68)에 현재 PC의 IP 주소 저장한다.
29A02824 저장한 IP주소를 클래스별로 분할한다.
29A02829 EBP-1C(B6FC78)에 A클래스 값 저장한다.
29A02841 D클래스까지 반복하면서 각 클래스 값을 저장한다.
EBP-18(B6FC7C):B클래스, EBP-14(B6FC80):C클래스,
EBP-10(B6FC84):D클래스

29A025B7 취약 호스트 탐색&감염 쓰레드 실행 쓰레드

29A02653 취약 호스트 탐색&감염 쓰레드를 생성한다.(29A02509)

29A02509 취약 호스트 탐색&감염 쓰레드
쓰레드 인자 : IP 대역

29A02560 랜덤 IP 생성 루틴을 실행하여 접속을 시도할 IP주소를 랜덤으로 생성한다.(29A02454)
29A02574 445 포트 스캔 루틴을 호출하여 생성된 IP주소의 445포트가 열려있는지 확인한다.(29A026E5)
29A02581 생성된 IP를 변환한다.
29A02588 취약 호스트 감염 루틴을 호출하여 찾아낸 취약한 IP를 감염시킨다.(29A02784)
29A02593 속도 조절을 위하여 2초간 Sleep 한다.
29A025A3 29A0C5F4가 0일때까지 계속 반복한다.

29A026E5 445 포트 스캔 루틴
첫번째 인자 : 연결할 IP 주소
두번째 인자 : select 응답 대기 시간

29A026FD 소켓 생성
29A02725 445번 포트 설정
29A02740 연결
29A02769 응답 대기
29A02772 연결 해제

29A02454 랜덤 IP 생성 루틴
첫번째 인자 : 네트워크 대역
두번째 인자 : 현재 몇번째 IP 인지

11AFF4C A클래스 변수(EBP-C)
11AFF50 B클래스 변수(EBP-8)
11AFF54 C클래스 변수(EBP-4)
11AFF48 D클래스 변수(EBP-10)

29A024DA 첫번째 rand 결과를 C클래스 변수(EBP-4)에 저장한다.
29A024DD D클래스 변수 값을 EAX에 저장한다.
29A024E0 D클래스 변수가 비었는지 확인한다.
29A024E2 비어있지 않으면 rand 건너뛴다.
29A024E6 두번째 rand 결과를 좌측 8번 시프트

29A024E9　　시프트한 두번째 결과와 첫번째 결과 더한다.
29A024EC　　ECX에 A클래스 값 로드한다.
29A024F0　　결과 더한값을 다시 좌측 8번 시프트
29A024F3　　시프트한 값에 B클래스 값 더한다.
29A024F6　　다시 좌측 8번 시프트
29A024F9　　시프트한 값에 ECX에 저장해두었던 A클래스값 더한다.

29A0C5F0에 랜덤 IP주소를 저장

29A02784　　취약 호스트 감염 루틴

29A02794　　139번 포트가 열렸는지 확인하고 연결을 시도한다.(29A0147A)
29A027A1　　공유폴더에 연결을 시도한다.(29A02196)
29A027A8　　파일 전송 루틴을 실행한다. (29A02AF4)

29A02196　　공유관련 작업을 함

29A02217　　₩₩IP주소₩IPC$ 문자열 저장
29A0229A　　₩₩IP주소₩pipe₩spoolss 바인딩
29A022C1　　ncacn_cp:192.168.2.100[₩₩pipe₩₩spoolss]

29A02AF4　　파일 전송 루틴

29A02DFC　　랜덤으로 생성된 두자리 숫자.scr 저장
29A02E69　　"http://IP주소:29A01CA4에서 오픈한 포트/x" 문자열 저장

29A034F4　　USB 감염 (메인)

29A0352B　　10초간 대기한다.
29A03538　　USB 감염 루틴을 실행한다.(29A03760)
29A0353E　　반복 감염을 위하여 Sleep 함수 부분으로 점프한다.

29A03760　　USB 감염 루틴

29A03771　　논리 드라이버들의 정보를 얻어온다.
29A0378F　　이동식 디스크인 경우 파일을 복사한다.
29A037BA　　Autorun & 자기자신 파일 복사 루틴을 실행한다.(29A03540)
29A037C8　　다음 논리 드라이버를 읽어들인다.

29A03540 Autorun & 자기자신 파일 복사 루틴
첫번째 인자 : 원본 파일 경로
두번째 인자 : 복사 위치

29A035F6 이동식 디스크에 p.exe 파일이 존재하는지 확인한다.
29A03612 이동식 디스크에 autorun.inf 파일을 생성한다.
autorun.inf파일에 다음 내용을 입력
29A03636 [autorun]
29A03667 shellexecute=p.exe
29A0368F action=Open folder to view files
29A036B0 shell₩default=Open
29A036DE shell₩default₩command=p.exe
29A0370C shell=default
29A0372C 자기 자신을 이동식 디스크에 p.exe 라는 파일명으로 복사한다.
29A03741 p.exe파일에 읽기전용&숨김&시스템 파일 속성을 설정한다.
29A0374C autorun.inf파일에 읽기전용&숨김&시스템 파일 속성을 설정한다.

29A04A39 IRC Server 접속 루틴

29A04A77 29A056ED 루틴에서 [00-KOR-XP-3312752] 생성
29A04AFB b.vspcord.com의 IP 주소 질의
29A04B20 988 포트 설정
29A04B39 서버 연결
29A04C30 IRC 명령 전송 루틴을 실행하여 패스워드를 전달한다.(29A04DE2)
PASS h4xg4ng
29A04C6A IRC 명령 전송 루틴을 실행하여 닉네임을 전달한다.(29A04DE2)
NICK 생성된 닉네임
29A04CAA IRC 명령 전송 루틴을 실행하여 유저정보를 전달한다.(29A04DE2)
USER 유저 정보

29A04DE2 IRC 명령 전송 루틴
첫번째 인자 : IRC 명령 포맷
나머지 인자 : 포맷에 들어갈 문자열

29A04DFF 두 인자를 합쳐서 하나의 문자열로 만든다.
29A04E28 완성된 명령을 IRC Server로 전송한다.

29A04E37 IRC Server 명령 수신 루틴

29A04E60 서버의 응답을 수신한다.
29A04E8D 응답이 정상적으로 수신되었으면 패킷 처리 루틴을 실행한다.(29A050A1)

29A050A1 패킷 처리 루틴

29A050C3 처리할 데이터가 남아있지 않으면 종료한다.
29A050CD 데이터 처리 루틴을 실행한다.

29A050E1 데이터 처리 루틴

29A053B1 IRC 명령 전송 루틴을 실행하여 채널에 접속한다.(29A04DE2)
JOIN #lox
29A05462 TOPIC 명령 처리 루틴을 실행한다.(29A04E9F)

29A04E9F TOPIC 명령 처리 루틴
첫번째 인자 : 서버에서 전달된 문자열(명령)
두번째 인자 : 명령 전송자 닉네임
세번째 인자 : 1

29A04F3B 전달된 문자열에서 채널명을 제외한 명령 코드를 추출한다.
29A04F93 $dec() 안의 내용을 추출한다.
29A0508D 서버 명령 처리 루틴을 실행한다.(29A039E1)

29A039E1 서버 명령 처리 루틴
첫번째 인자 : 명령 문자열
두번재 인자 : B6F7EC

29A03A62 실제 서버 명령 처리 루틴을 실행한다.(29A03A75)

29A03A75 실제 서버 명령 처리 루틴

29A03A91 전달된 명령이 open 명령인지 확인한다.
29A03AB4 open이라면 인자로 전달된 파일을 숨김 속성으로 실행한다.
29A03B04 전달된 명령이 s.start 명령인지 확인한다.
29A03C61 전달된 인자를 참조하여 취약 호스트 탐색&감염 쓰레드 실행 쓰레드를 실행한다.(29A025B7)
29A03C98 전달된 명령이 s.stop 명령인지 확인한다.
29A03CA2 쓰레드 종료 루틴을 실행하여 실행중인 취약 호스트 탐색&감염 쓰레드 실행 쓰레드를 모두 종료한다.(29A033EC)
29A03CBE 전달된 명령이 http 명령인지 확인한다.
29A03CE6 전달된 인자가 stop인지 확인한다.
29A03CFA 전달된 인자가 stop이면 29A0CA1C를 0으로 설정하고 아니면 1로 설정한다.

29A03D3E　　전달된 명령이 wget인지 확인한다.
29A03DD6　　파일 다운로드 & 실행 쓰레드을 실행한다.

29A06D06　　파일 다운로드 & 실행 쓰레드

29A06D76　　다운로드 받은 파일을 저장할 Temp 폴더 경로를 저장한다.
29A06DF0　　를 실행하여 인자로 전달된 url로 부터 파일을 다운로드 받는다.
29A06DB6　　Temp 폴더 경로와 랜덤함수를 실행하여 얻은 파일명을 합하여 최종적으로 다운로드받은 파일 위치를 저장한다.
29A06DF0　　URL로부터 파일을 다운로드 받는다.
29A06E1E　　정상적으로 다운로드 받았으면 다운로드 받은 파일을 실행한다.
29A06E60　　-n 옵션이 설정되어 있으면 IRC Server 접속을 종료한다.