

ASEC Annual Report 2003

® ASEC Report 2003. 12

AhnLab Security E-response Center Annual Report 2003

ASEC

Annual Report

2003

ASEC Report 2003. 12

(AhnLab Security E-response Center)

가

ASEC Annual Report ()

ASEC

2003

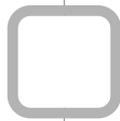
Ahn AhnLab

Ah AhnLab

Abn



I.	2003	4
	1. 2003	4
	2.	Top 20	5
II.	2003	12
III.	2003	19
IV.	2003	25
	1.	25
	2.	29
	3.	32
	4.	34
V.	2003	35
	1.	35
	2.	42



2003

: (jsjung@ahnlab.com)

1. 2003

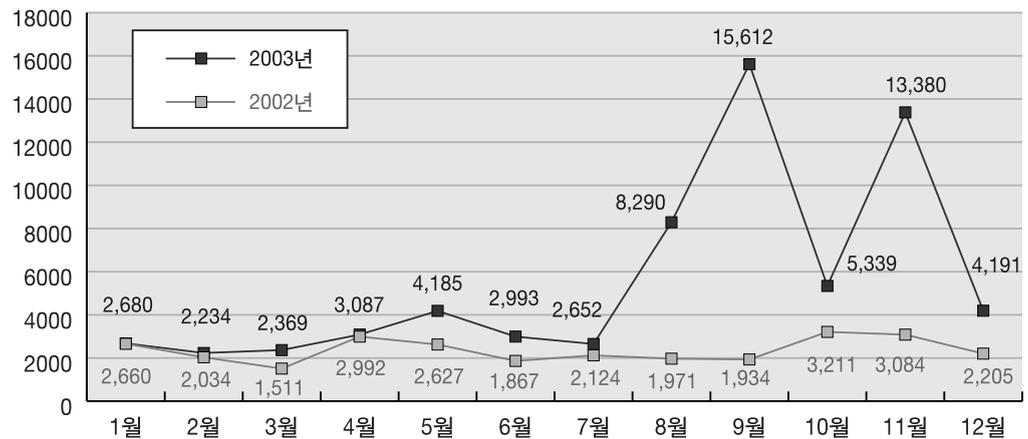
2003년 1월 1일부터 12월 31일까지 발생한 SQL_Overflow () 8건
 (Win32/Blaster.worm.6176) , F(Win32/Sobig.worm.F)
 2002년 1월 1일부터 12월 31일까지 발생한 피해건수

	1	2	3	4	5	6	7	8	9	10	11	12
2002	2660	2034	1511	2992	2627	1867	2124	1971	1934	3211	3084	2205
2003	2680	2234	2369	3087	4185	2993	2652	8290	15612	5339	13380	4191

[1] 2002, 2003년 12월 10일 기준

[1] 2003년 12월 31일 기준 67,012건 (2002년 12월 31일 기준 22,050건) 증가

피해건수



[1] 2002, 2003년 12월 31일 기준

가 가
 1 SQL_Overflow, 5 (Win32/LovGate.worm.
 107008), 8 (Win32/Blaster.worm.6176) , F(Win32/Sobig.
 worm.F) , (Win32/Dumaru.worm.9234) , (Win32/Mimail.worm)

2. Top 20

2002
 [2], [3]

Win32/Klez.worm.H	4,650
Win32/Nimda	4,400
Win32/FunLove.4099	3,637
Win32/Opasoft.worm.28672	994
Win95/Spaces.1445	850
Win32/Elkern.B	838
Win32/Nimda.B	719
Win32/Winevar.worm	584
Win32/Weird	509
Win95/CIH	493
Win32/Yaha.worm.27648	471
I-Worm/Wininit	417
Win32/Nimda.eml.79225	402
Win32/Parite.B	388
Win32/Opasoft.worm.24064	370
Win32/Datom.worm.54784	330
Win32/Nimda.B.eml.79232	328
Win32/Gop.worm.60313	288
Win32/Sircam.worm	285
Win32/Opasoft.worm.28672.B	260

[2]2002 Top20

Top 20

Win32/Sobig.worm.F	14,949
Win32/Dumaru.worm.9234	14,741
Win32/Blaster.worm.6176	4,901
Win32/Yaha.worm.45568.B	4,732
Win32/LovGate.worm.107008	1,571
Win32/Parite	1,174
Win32/Parite.B	1,000
Win32/FunLove.4099	899
Win32/Welchia.worm.10240	819
Win32/Valla.2048	803
JS/Fortnight	728
Win95/Spaces.1445	725
Win32/Klez.worm.H	682
MIRC/Stde9	608
Win32/Yaha.worm.27648	544
HTML/Redlof	538
Win32/Nimda	499
Win32/Opasoft.worm.28672	489
Win32/Elkern.B	443
Win32/Yaha.worm.45568	436

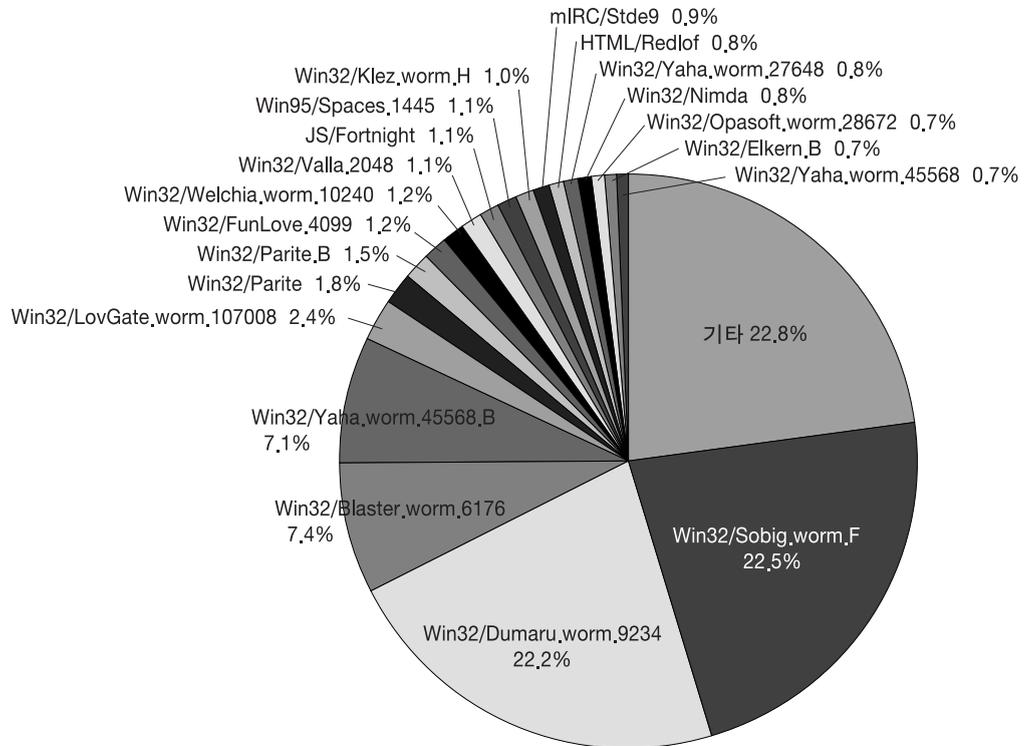
[3] 2003 Top 20
 * 2003 2003 12 10

[1] 가 가 가

[3] Top 5

- Win32/Sobig.worm.F
- Win32/Dumaru.worm.9234
- Win32/Blaster.worm.6176
- Win32/Yaha.worm.45568.B
- Win32/LovGate.worm.107008

1, 2 44% 3 가 8 가 , , 가 , 가 8 가
 2003 , 가 가 8 가
 F , 가 가 8 가
 . [3] Top 20 [2] .



[2] 2003 Top 20

[2] 가 . 5 4 (Mass Mailer)

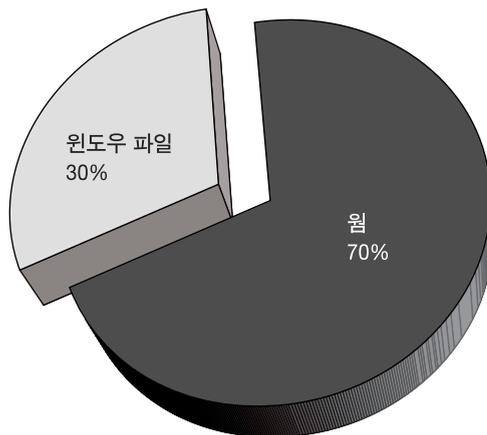
SQL_Overflow
NT

가 .

2002 , 2003 Top 20

2002 , 2003 Top 20

[3],[4] .

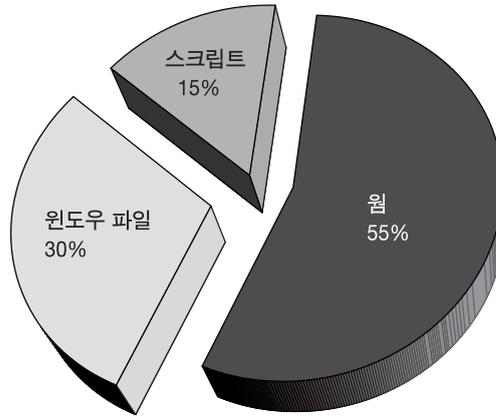


[3] 2002 Top 20

2002

Win32
Mass Mailer
(Win32/Nimda),
(Win32/Opasoft.worm)

9x NetBIOS
H(Win32/Klez.worm.H) 2001
9x



[4]2003 Top 20

2003
(JS/Fortnight)

가
(HTML/Redlof)

가

가

2002 , 2003

Top 20

2003

2002 2003

Top 20

[5], [6]

가

가

가

가

-

- ()

- (NetBIOS)

-

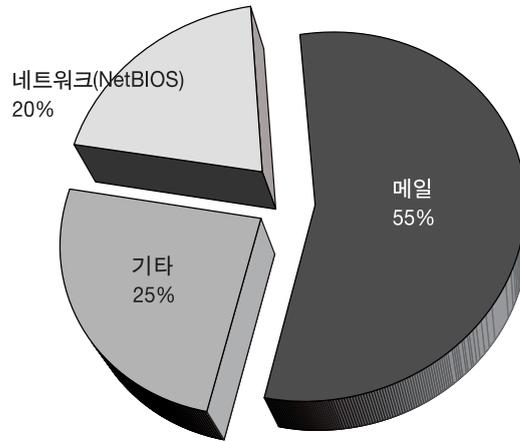
NetBIOS

2003

(

)

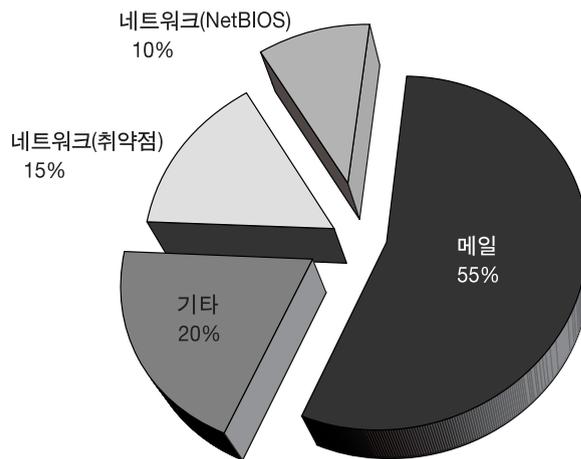
가



[5]2002 Top 20

[5] 2002 가 가

, B(Win32/Elkren.B), B(Win32/Parite.B) 가 2003



[6]2003 Top 20

2003

가 . 8 RPC

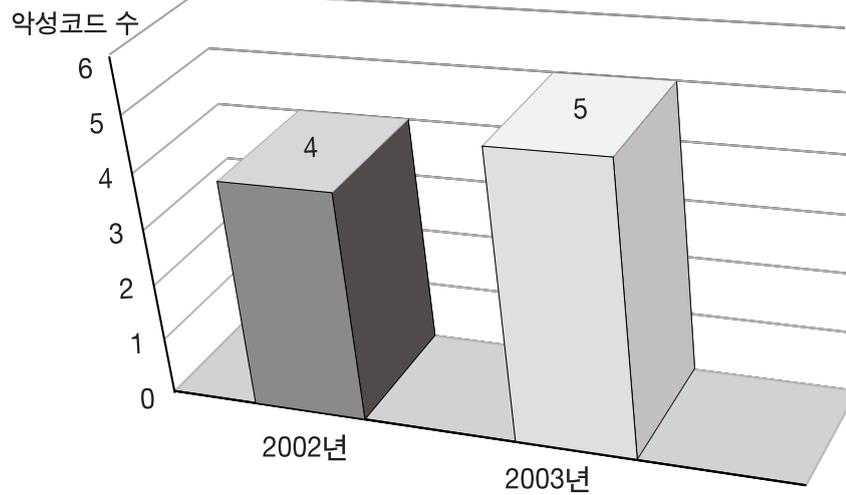
DCOM

(null session)

가
가 Dropper/MircPack
Win32/Valla.2048, Win32/Parite B

TCP

2002 2003 Top 20 가 가



[7] 2002 , 2003 가

[7] 2002 Top 20 20% , 2003 25% 가

가 가 가 가 가 가

- (SMTP, MAPI)
- ()
- (,)
- (, MSN, Yahoo Messenger)
- P2P (P2P)

2002 , 2003

2002

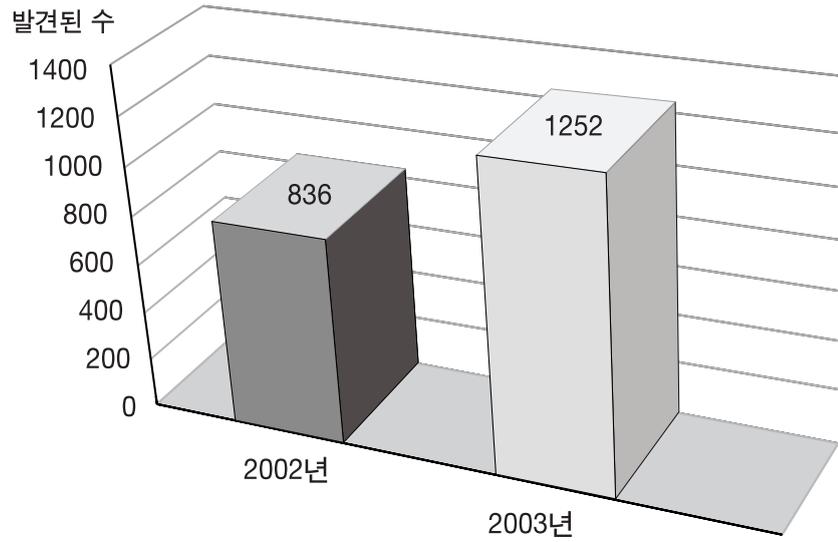
/ 가

. 2003

2002 2003

142%

가 가
가



[8] 2002 , 2003

[8]

2003

가

66%

가

가

Top 20

가

가



2003

: (jsjung@ahnlab.com)

2003 1 1 12 10 1,133 , 2002
277 4 가 가 [1], [2] .

										/
1	0	1	2	0	4	0	3	0	10	
2	0	0	8	2	2	0	3	0	15	
3	0	2	8	0	3	0	2	0	15	
4	0	4	6	0	1	0	4	0	15	
5	0	1	10	3	1	0	2	0	17	
6	0	2	7	4	4	0	0	0	17	
7	0	4	13	2	9	0	0	0	28	
8	0	0	1	2	1	0	1	0	5	
9	0	0	10	0	2	0	3	0	15	
10	0	7	24	6	7	0	0	0	40	
11	0	15	27	8	10	0	0	0	60	
12	0	5	21	5	5	0	0	0	36	
	0	41	137	32	49	0	18	0	277	

[1]2002

										/
1	0	7	54	18	3	8	0	0	0	90
2	0	2	80	15	3	13	1	1	0	115
3	2	3	76	24	1	12	0	0	0	118
4	0	1	46	11	3	11	0	0	0	72
5	0	4	44	14	2	14	0	0	0	78
6	0	2	52	6	4	21	0	0	0	85
7	0	3	59	4	1	10	0	0	0	77
8	0	2	93	13	3	20	0	0	0	131
9	0	1	78	7	2	28	0	0	0	116
10	0	0	59	3	0	30	0	0	0	92
11	0	0	50	1	2	58	0	0	0	111
12	0	0	30	3	0	15	0	0	0	48
	2	25	721	119	24	240	1	1	0	1133

[2]2003

3] 가 ([

88	89	90	91	92	93	94	95	96	97	98	99	2000	2001	2002	2003	
1	6	28	21	17	34	76	128	226	256	276	379	572	435	277	1133	3865

[3]1998 ~ 2003 (2003 12 10)

- 가

-

- 가

-

DoS () 가 IRCBot DoS
 (Win32/Dumaru.worm.9234) (Win32/LovGate.worm.107008)
 가 DoS

DoS

가 가

가

가

가

IRCBot

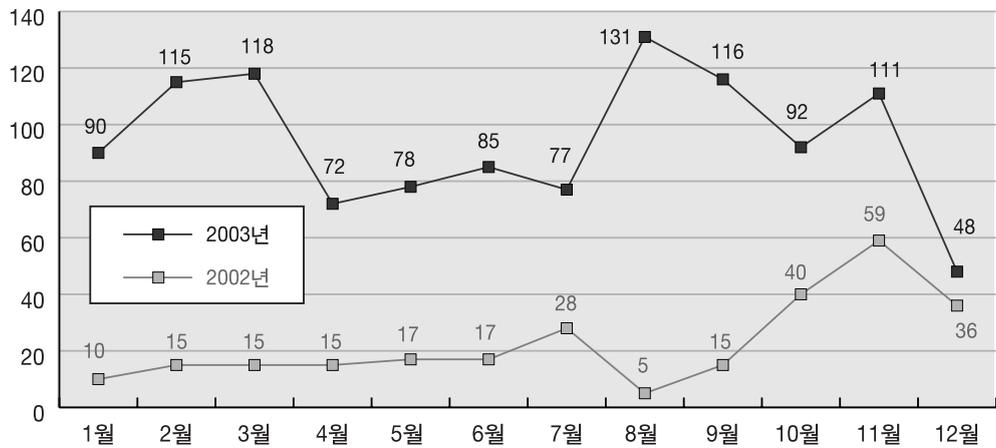
?

[2]

IRCBot

가 IRCBot
 가

발견건수



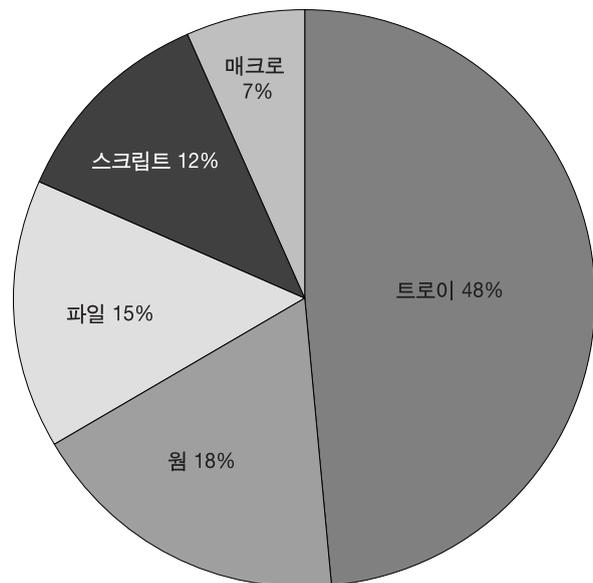
[1]2002, 2003

2002 Win-Trojan/MircPack 가 2002 IRCBot 가 가

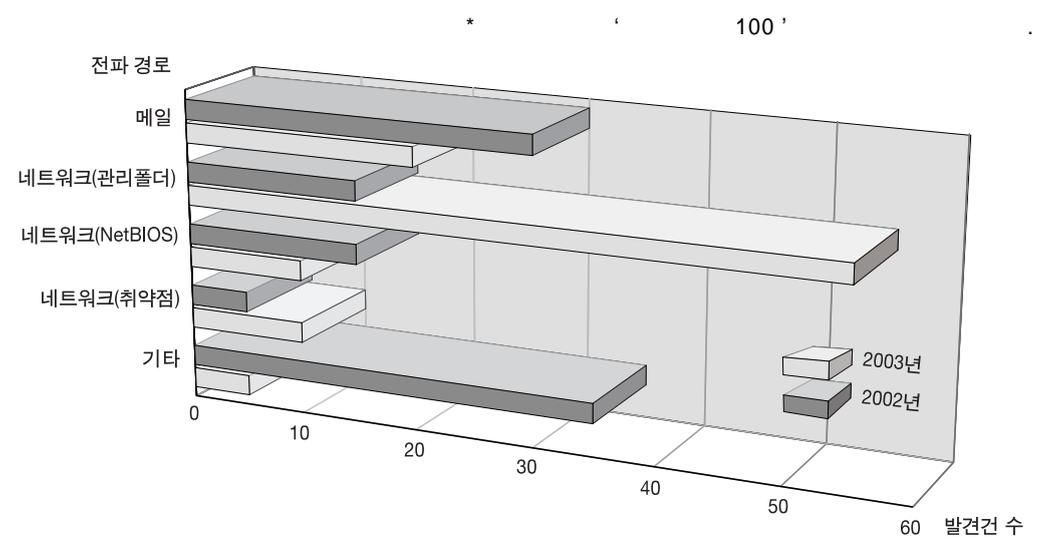
2003 가 . 가 가 8
F .

2002 2003
[2], [3] .

부트/파일 0%
부트 0%
리눅스 0%



[2]2002



[4]2002 , 2003

가 가

가

가

가

가 SQL_Overflow

가

NT

가

가

Win32/AgoBot.worm, Win32/SdBot.worm

가

가

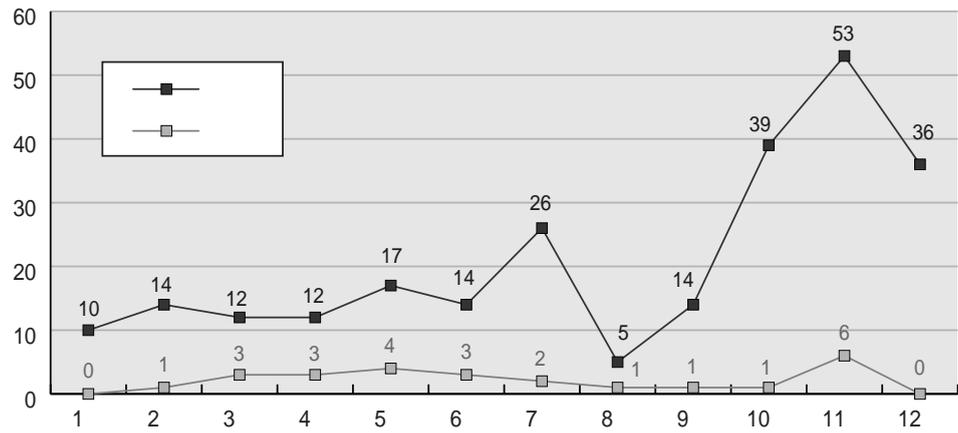
TCP/135, TCP/445

/

/

가

1.5 가 가 ([5], [6]).



[5]2002

/

2002

CD-Key

가

가

2003

IRCBot

IRCBot

가

가

IRC

SYN Flooding

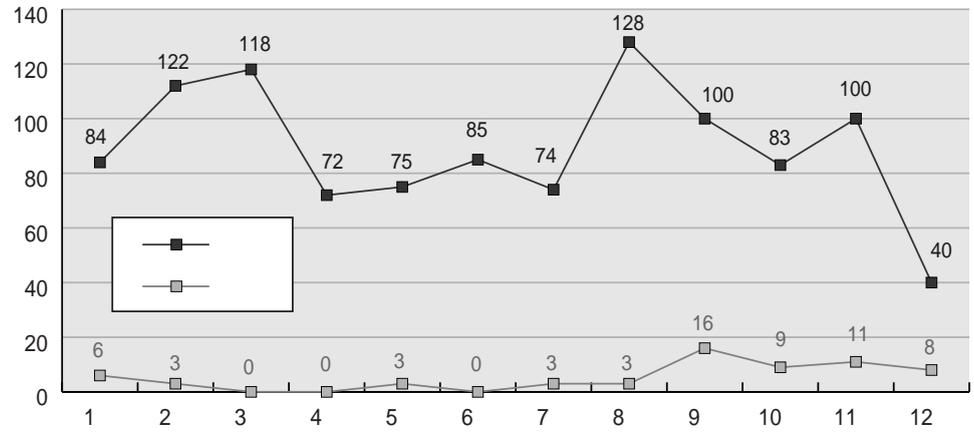
DoS

가

DoS

MSN

가



[6]2003 /

Active X

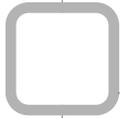
2003

가

가

가

Mass Mailer



2003

: (dubhe@ahnlab.com)

가

. 2000

OS

, ,

MS-DOS

3.x,

9x,

NT

(NT, 2000, XP)

. 9x

가

OS , NT

가

NT

2000 Server ,

2000 Professional

가

OS

OS

()

가

가

PC

가

OS

가

가

가

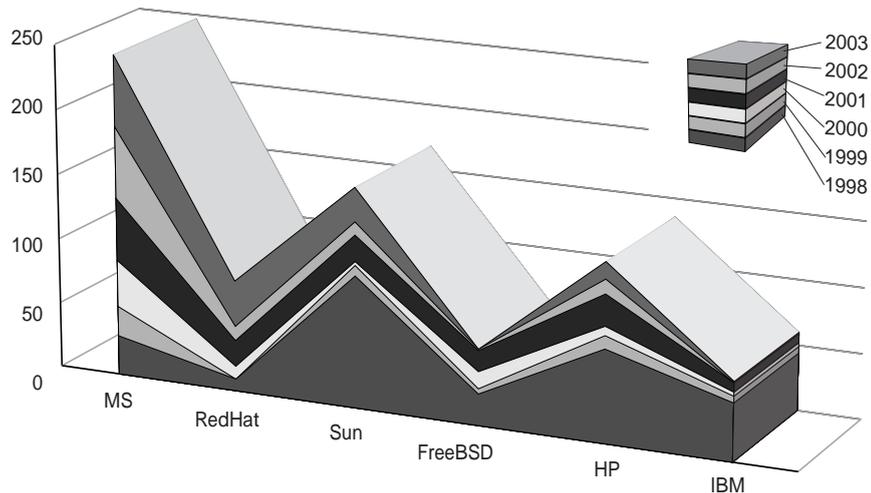
PC가

가

[1] [1] CIAC(<http://www.ciac.org/>)
Vendor

	MS	RedHat	Sun	FreeBSD	HP	IBM
1998	30	9	101	24	71	44
1999	23	0	8	4	10	5
2000	36	10	3	13	7	3
2001	48	20	20	16	24	7
2002	55	11	10	1	11	0
2003	55	35	26	0	13	1
	247	85	168	58	136	60

[1]CIAC OS



[1]CIAC OS

[1] [1] MS OS

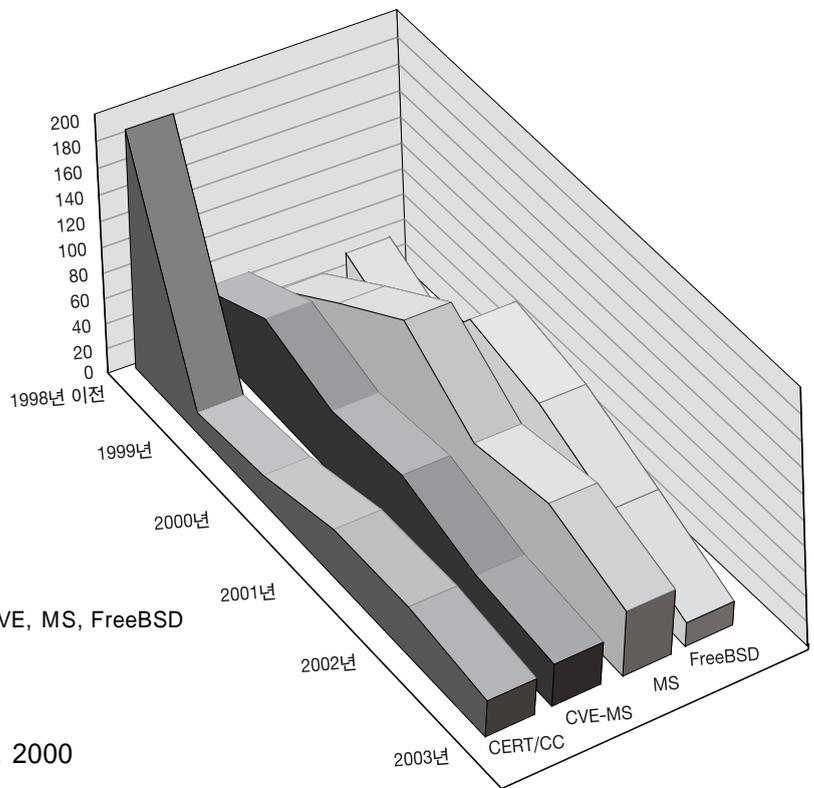
Sun, HP, IBM

1998 MS OS
98 OS가 가 Unix OS . 98
OS

[2] [2] CERT/CC, CVE, MS FreeBSD Advisory
CVE OS Linux, SunOS OS
Advisory가 Patch

	CERT/CC	CVE-MS	MS	FreeBSD
1998	184	43	20	31
1999	17	70	61	6
2000	22	51	100	82
2001	37	57	60	71
2002	37	39	72	46
2003	28	33	51	19
	325	293	364	255

[2]CERT/CC, CVE, MS, FreeBSD Advisory



[2]CERT/CC, CVE, MS, FreeBSD Advisory

1999 , 2000
가

. MS

2000

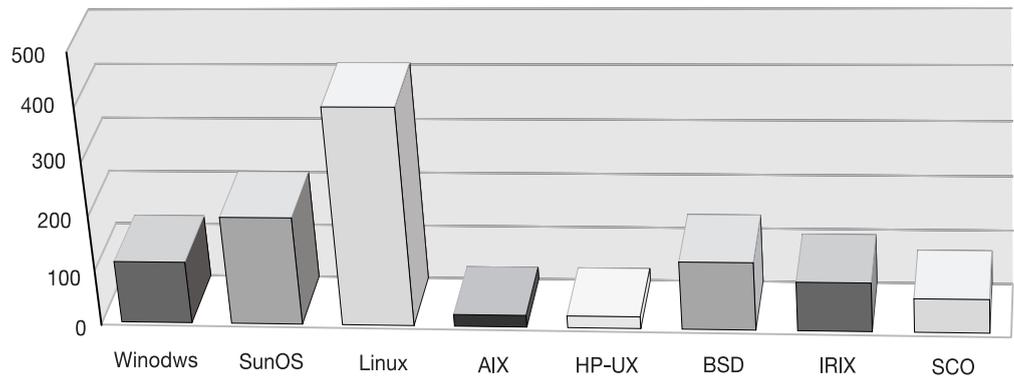
가 OS

. CERT/CC Advisory 88

Advisory 가

OS

[3] 99 8 Exploit
Exploit



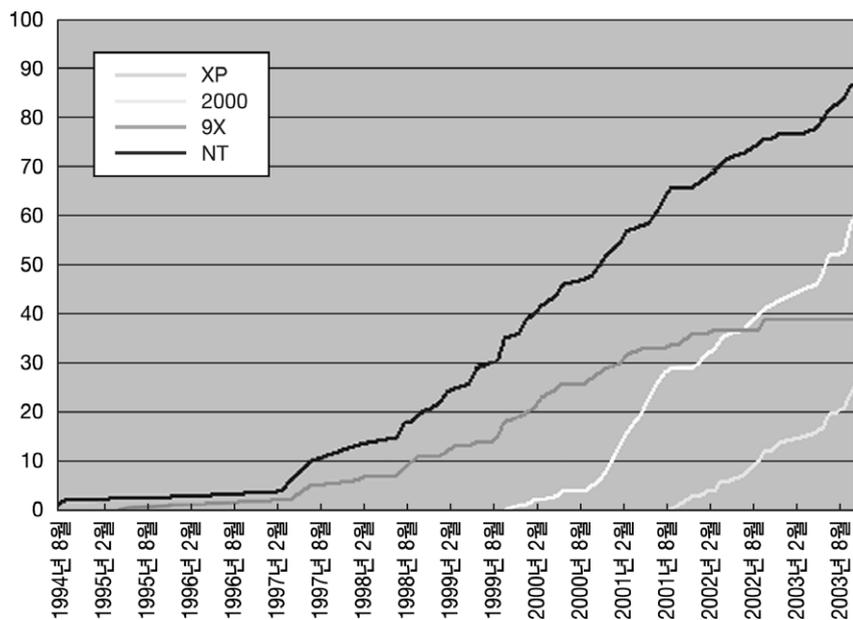
[3] 1999 8 Exploit

NT 9x DoS
 Unix 가 가 x86 Sparc
 Linux, SunOS, BSD, SCO가 . IRIX
 가 HP-UX, AIX
 가 .

2000 가 가
 , 가 .

가

[4] OS CIAC . OS



[4] OS



2003

1.

: (jackycha@ahnlab.com)

2003 1 SQL_Overflow¹⁾ ' 1.25 ' 가

²⁾, ³⁾, ⁴⁾,

⁵⁾, .F⁶⁾

msn⁷⁾, ⁸⁾

Win-Trojan/RtKit.128000⁹⁾, Win-Trojan/HackDef.

50688¹⁰⁾

11

hotdog.exe(Win-Trojan/Hotra.

49152)¹¹⁾가

가

가

가

가

2003

2003

1) SQL_Overflow : , http://info.ahnlab.com/smart2u/virus_detail_1098.html

2) : Win32/Mimail.worm, http://info.ahnlab.com/smart2u/virus_detail_1197.html

3) : Win32/Blaster.worm.6176, http://info.ahnlab.com/smart2u/virus_detail_1202.html

4) : Win32/Welchia.worm.10240, http://info.ahnlab.com/smart2u/virus_detail_1206.html

5) : Win32/Dumaru.worm.9234, http://info.ahnlab.com/smart2u/virus_detail_1207.html

6) F : Win32/Sobig.worm.F, http://info.ahnlab.com/smart2u/virus_detail_1208.html

7) msn : Win32/Sinmsn.worm.20480, http://info.ahnlab.com/smart2u/virus_detail_1193.html

8) : Win32/Smibag.worm.163840, http://info.ahnlab.com/smart2u/virus_detail_1223.html

9) Win-Trojan/RtKt.128000 : http://info.ahnlab.com/smart2u/virus_detail_1222.html

10) Win-Trojan/HackDef.50688 : http://info.ahnlab.com/smart2u/virus_detail_1227.html

11) Win-Trojan/Hotra.49152, http://info.ahnlab.com/smart2u/virus_detail_1240.html

(1) SQL_Overflow

1 25 Win-Trojan/SystEntry.32768.B¹²⁾가
 98 가 . 1
 가 . SQL
 SQL_Overflow
 ' 1.25 ' .

(2) JS/Fortnight

JS/Fortnight¹³⁾
 가
 . JS/Fortnight
 가 가

(3)

(Win32/LovGate.worm.107008)¹⁴⁾ 3
 . (가
 EXE)
 (Code Injection)
 ()가 가
 가 .

(4) Dropper/MircPack

Dropper/MircPack¹⁵⁾
 FTP /
 (Warez)
 Win-Trojan/ServU.212126¹⁶⁾
 가
 가

12) Win-Trojan/SystEntry.32768.B : http://info.ahnlab.com/smart2u/virus_detail_1096.html
 13) JS/Fortnight : http://info.ahnlab.com/smart2u/virus_detail_1182.html
 14) Win32/LovGate.worm.107008 : http://info.ahnlab.com/smart2u/virus_detail_1135.html
 15) Dropper/MircPack.755236 : http://info.ahnlab.com/smart2u/virus_detail_1095.html

(5)

5 Dropper/Delf.74240¹⁷⁾ (Stealth Technique)
 Win-Trojan/RtKit.128000, Win-Trojan/HackDef.50688
 가

(6)

20480 Win32/Smibag.worm, Win-Trojan/Hotra
 Win32/Sinmsn.worm.
 가

(7)

8 2003 Win32/Mimail.worm
 RPC DCOM
 (Code_Red), SQL_Overflow
 XP
 RPC DCOM 2000
 가

*

- <http://www.zdnet.co.kr/ecommerce/biztrend/article.jsp?id=64386&forum=1>
- http://news.naver.com/news_read.php?oldid=2003121100008631081
- http://news.naver.com/news_read.php?oldid=200309240000465999002

(8)

8 Win32/Sobig.worm.F¹⁸⁾ Win32/Dumaru.worm.9234¹⁹⁾
 2003 9 10 가 9 10

16) Win-Trojan/ServU.212126 : http://info.ahnlab.com/smart2u/virus_detail_1151.html
 17) Dropper/Delf.74240 : http://info.ahnlab.com/smart2u/virus_detail_1179.html
 18) Win32/Sobig.worm.F : http://info.ahnlab.com/smart2u/virus_detail_1208.html
 19) Win32/Dumaru.worm.9234 : http://info.ahnlab.com/smart2u/virus_detail_1207.html

가 . 2001 9.11 2
가
가
(9) 가
11 가 hotdog.exe
(Adware)
(Freeware), (Shareware)
가 (Spyware)
가
가
가 hotdog.exe
가 ()
, V3 / (
)
-
-
-
,
가 X 가

2.

(sopara@ahnlab.com)

가 가

가

가

(1)

2003

가

SQL_Overflow
IPA/ISEC

2003

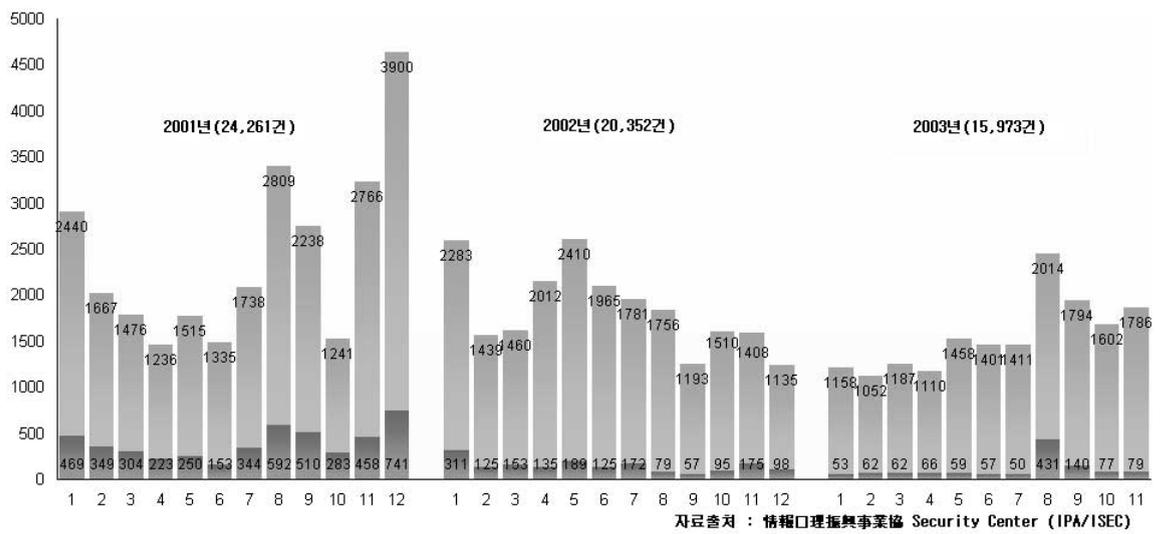
8

RPC

가

가

2002



(2) 2003

Klez

2003

가

(Microsoft)

Outlook

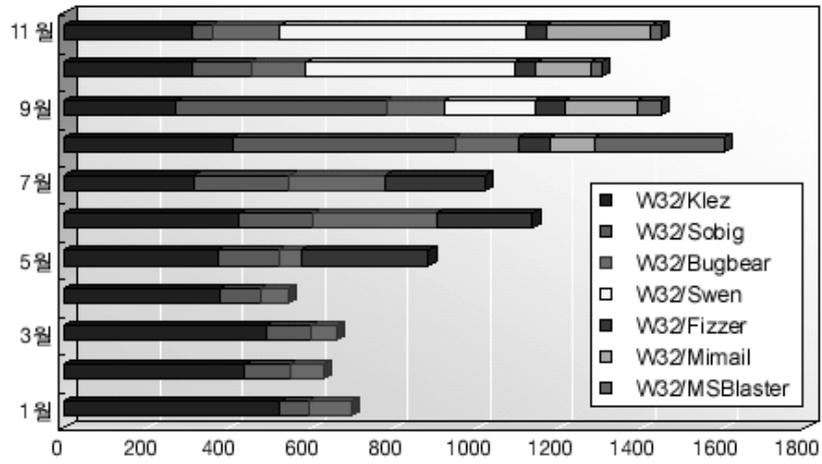
(Win32/Klez.worm)

.F 2003 8 9

10

(Opasoft)

(Nimda)



(3)

1,184 가
 . CGI 가
 가
 東武 가 가 가 가
 . 東武 가 가
 가 가 가
 가 가 가

(4)

가
 가 가
 . 5 331
 786 2
 []
 10 가

(5) Japannet

5 8 Japannet 가 22 가 가

. Japannet 5 4 가
 가 가
 가 5 8
 가 가 .
 20 Unix CPU 가 가 가
 가 가 14 CPU 1 CPU
 가 17 . Japannet 17
 Unix 24
 17 가 .

(6)

Winny
 가 京都

98 가
 (7) 가

가

가

	2000	2001	2002	2002	2003
.	1396	1963	3193	1331	8776
.	2896	3282	2261	1176	2605
Internet · Auction	1301	2099	3978	1495	2309
.	1884	2267	2566	1229	1349
.	1352	2647	2130	1180	1246
· Virus	505	1335	1246	693	506
.	1801	3684	3955	1988	2306

[1] ()

[1]

가

3.

: (zhang95@ahnlab.com)

2003
 가 .
 가 .
 가 .
 2003 , 가 가 .
 가
 2003
 9 2003 .

(1) Win32/Blaster.worm.6176

8 Win32/Blaster.worm.6176
 2003 .
 Win32/Blaster.worm.6176
 2000 RPC .
 가

(2) SQL_Overflow

1 25 SQL_Overflow MS-SQL Database
 ' Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code
 Execution ' 80%
 가 , , , ,
 가 12

(3)

8 8 ,
 IP ' (1) '
 isc.org.cn 8 21 27

(4) (百度)

5 (百度) (百度) (百度)
 가 . 가 38863 .

(5)

1 , 가 .
 가 (家中和)

(6) (工商)

가 , , 가 .

(7) 20

7 , 가 640 2
 가 , , 20
 640 .

(8)

7 , ' 3 ' 3

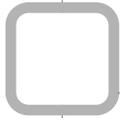
(9)

6 가 가 Cyber
 가 가 10

4.

2003 (jackycha@ahnlab.com)
가 가
가
가 .F , , , .
가 - .
가 가
MSN MSN
가 QQ
가
P2P(Peer-to-Peer) Winny
Win32/Antinny.worm.651264²⁰⁾
가
가

20) Win32/Antinny.worm.651264 : http://info.ahnlab.com/smart2u/virus_detail_1212.html



2003

1.

: (jackycha@ahnlab.com)

(Vulnerability)

(<http://www.terms.co.kr>)

“ . 가 가 . ”

가 가 가 가 , ,

. 2003 8

MS-DOS

가

가

가

1988

Linux/Ramen¹⁾ worm²⁾ 6.2 7.0 OpenSSL Linux/Slapper.

1996 가 가

가 가

가

, 2001 (Code_Red)

1 25 SQL / 2003

가 SQL_Overflow(, SQL)

가

8 12 SQL_Overflow 2003

2000/XP RPC DCOM

가

가

가

가

1) Linux/Ramen : http://info.ahnlab.com/smart2u/virus_detail_784.html

2) Linux/Slapper.worm : http://info.ahnlab.com/smart2u/virus_detail_1030.html

(1) /

1999 11

.

VBS/BubbleBoy³⁾가
HTML

JS/Kak⁴⁾

.

.

.

가

가

X

(2)

040)가

HTML

가

(MS03-

/

가가

[1]

3 가

가

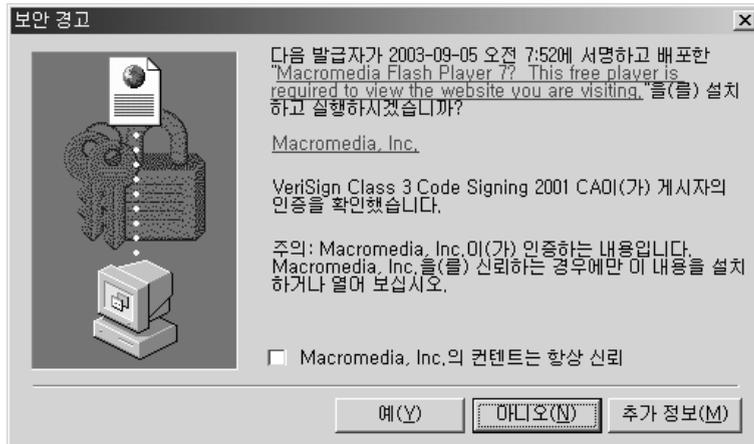
가

가

가

3) VBS/BubbleBoy : http://info.ahnlab.com/smart2u/virus_detail_22.html

4) JS/Kak : http://info.ahnlab.com/smart2u/virus_detail_655.html



[1] ,

가 가 . MS 가 (Microsoft VM
ActiveX Component) 가 JS/Fortnight⁵⁾

(3) IIS

/ , IIS
가 IIS IIS
가
IIS 가 MS01-033⁶⁾ MS01-044⁷⁾

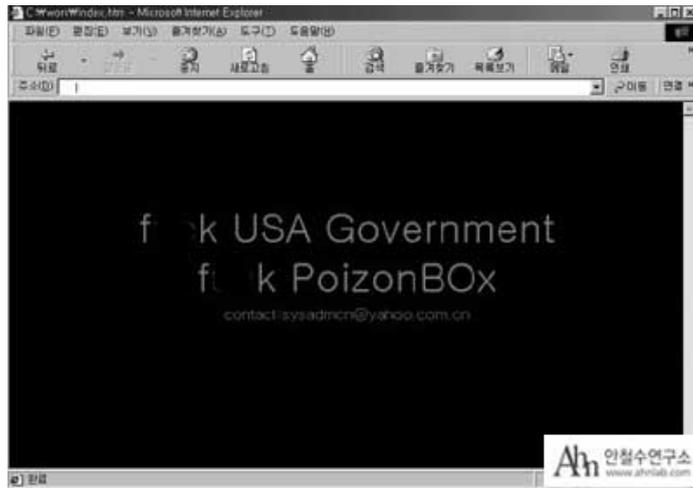
. Solaris/Sadmind.worm IIS
HTML/Sadmind⁸⁾ 가

5) JS/Fortnight : http://info.ahnlab.com/smart2u/virus_detail_1182.html

6) MS01-033 : <http://www.microsoft.com/korea/technet/security/bulletin/MS01-033.asp>

7) MS01-044 : <http://www.microsoft.com/korea/technet/security/bulletin/MS01-044.asp>

8) HTML/Sadmind : http://info.ahnlab.com/smart2u/virus_detail_822.html



[2] HTML/Sadmind

(4) SQL

SQL 가
 SQL_Overflow(SQL) SQL 2000
 (MS02-039)⁹⁾

가
 , SQL 2000
 SQL 2000
 2002 가
 2003 1 25 SQL ‘ 1.25 ’

(5)

(Macromedia) (Flash Player)
 . SWF
 가 가 . 2002
 1 8 SWF/LFM.926¹⁰⁾ 가

. (http://www.macromedia.com/support/flash/ts/documents/swf_clear.htm)

9) MS02-039 : <http://www.microsoft.com/korea/technet/security/bulletin/MS02-039.asp>

10) SWF/LFM.926 : http://info.ahnlab.com/smart2u/virus_detail_909.html

(6) RPC DCOM

NT (2000/XP) , . RPC
 DCOM (MS03-026) 7 17
 7 .

, 8
 RPC DCOM . 가

2003 8 12 () (Win32/Blaster.worm.6176)
 . RPC DCOM
 XP
 가 가 . XP 가

2003 8 18 (Win32/Welchia.worm.10240) RPC DCOM
 .
 가
 가 .

가 .

, /

,

,

/

가 .

가

가

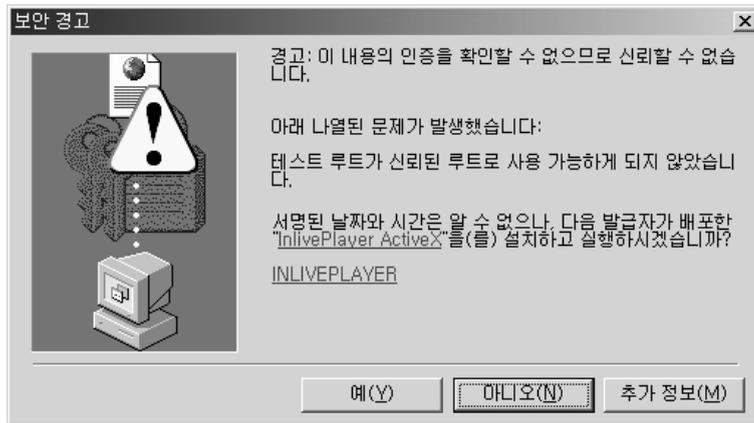
가 .

가 가 . PC 가 ,
 , . ,
 , 가
 가 . 가
 가 가 .
 가 .
 PDA 가 .
 가 가 .
 가
 ,
 가 .

- (http://info.ahnlab.com/securityinfo/virus_search.jsp)
- (http://www.terms.co.kr)

16 5
 0.5 , 9,900
 가 가 가 Aureate/
 Radiate²⁾ . Aureate/Radiate
 가 Dlder³⁾
 가⁴⁾
 가
 가?
 가
 , [1]

1) : <http://messenger.freechal.com/FcVaccine/FcVacFastType.asp>
 2) <http://grc.com/oo/aureate.htm>,
<http://www.kaspersky.com/news.html?id=16>
<http://vmyths.com/hoax.cfm?id=36&page=3>
<http://www.europe.f-secure.com/v-descs/aureate.shtml>
 3) <http://www.europe.f-secure.com/v-descs/dlder.shtml>
<http://www.europe.f-secure.com/v-descs/dlder.shtml>
 4) <http://www.flashtrack.net/policy.html>



[1]

, 가?

/ ()

가 가 가

/ () .

가

가

가 가 () 가 가

(1)

가 가

HTML/NoClose⁵⁾

5) http://info.ahnlab.com/smart2u/virus_detail_987.html

(2)

가

가

가

가

(3)

가

(4)

가

가

(5)

가

가

가“ ”

(1)

VB
가

HTA

가

HTML

가
가

가

(2)

Active X

가

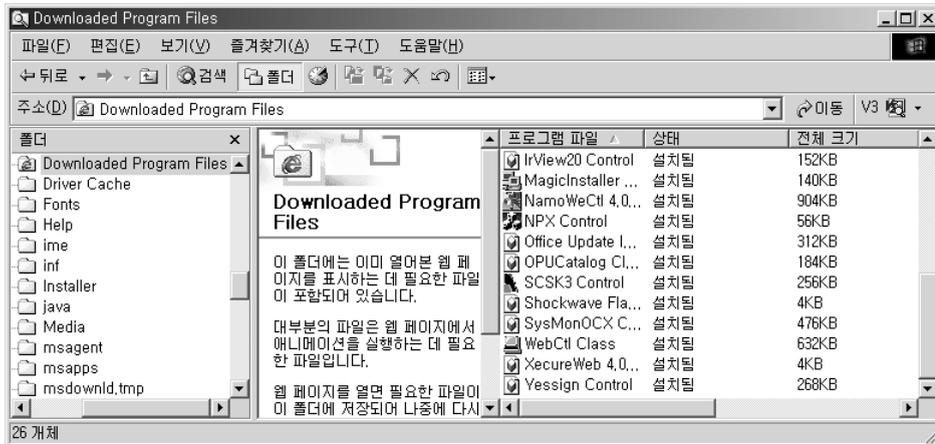
(

C:\Windows

C:\WINNT)

Downloaded Program Files

.[2])



[2] Downloaded Program Files

(3) DLL

ActiveX

가

가 가

EXE

DLL

. DLL

EXE

EXE

DLL

DLL

DLL

DLL

DLL

ActiveX

(1)

가

“ ”

(2)

가

36 50 5 6)

,
가 .
가 .

(3)

가
/ () . , 가

(4)

JS/Fortnight / ()가 가 .
가

6) “ ”

(1)

(2)

(3)

(4)

(5)

Downloaded Program Files
Downloaded Program Files

가

X

X

가

가

가

/ ()

가