

ASEC Report 1월

® ASEC Report

2004. 2

I. 1월 악성코드 Top 10	3
II. 1월 국내 신종 악성 코드 발견 동향	8
III. 1월 신규 보안 취약점	12
IV. 1월 일본 피해 동향	13
V. 1월 중국 피해 동향	15
VI. 테크니컬 컬럼 - 마이둠 웹의 뒷 이야기	18

안철수연구소의 시큐리티대응센터(Ahnlab - Security E-response Center)는 악성 코드 및 보안위협으로부터 고객을 안전하게 지키기 위하여 바이러스와 보안 전문가들로 구성되어 있는 조직이다.

이 리포트는 (주)안철수연구소의 ASEC에서 국내 인터넷 보안과 고객에게 보다 다양한 정보를 제공하기 위하여 바이러스와 시큐리티의 종합된 정보를 매월 요약하여 리포트 형태로 제공하고 있다.

SUMMARY

아고봇 웹 변형 발견과 이메일을 통해 전파되는 웹 발견 증가...

2004년 1월에는 2003년 12월에 비해 두마루 웹에 대한 피해가 감소하였고, 2003년 하반기에 꾸준히 Top 10에 랭크되던 소빅.F 웹에 대한 피해신고도 Top 10에서 자취를 감추었다. 반면 RPC 취약점과 윈도우 2000 계열의 관리목적 공유폴더를 이용한 취약한 로그인계정 암호를 이용하여 전파되는 아고봇 웹 변종에 대한 신고가 증가하는 추세를 보였다. 특히 2004년 1월말에는 이메일을 통해 전파되는 베이글 웹과 마이둠 웹이 발견되어 많은 피해를 입혔다. 특히 마이둠 웹은 지금까지 세계적으로 가장 많이 피해를 입혔던 것으로 알려진 소빅.F 웹의 피해를 능가하는 정도의 피해를 입혔다. 또한 특정 사이트에 DoS 공격을 하는 증상이 추가되어 있어, 앞으로도 공격형태가 가미된 형태의 웹의 출현이 증가될 것으로 예상된다.

1월에는 마이크로소프트에서 3가지 보안취약점을 발표하였으나 악성코드에서 이용될 확률은 그리 높지 않다. 그러나 새로 발견되는 웹들은 2003년에 많은 피해를 입혔던 슬래머 웹이나 블래스터 웹과 같이 보안취약점을 이용하여 전파되는 기능을 포함하고 있는 추세이므로, 앞으로도 계속 발표되는 보안취약점 정보에 주의를 기울이고 패치를 적용해야 하겠다.

I. 1월 악성코드 Top 10

작성자 : 정진성 연구원(jsjung@ahnlab.com)

		%
Win32/Dumaru.worm.9234	2,890	54.2%
Win32/Blaster.worm.6176	501	9.4%
Win32/Parite	171	3.2%
Win32/Yaha.worm.45568.B	96	1.8%
Win32/AgoBot.worm.197120.C	91	1.7%
Win32/Parite.B	83	1.6%
Win32/Agobot.worm.104960	72	1.3%
Win32/Bagle.worm.15872	72	1.3%
Win32/Mimail.worm.13856	67	1.3%
Win32/FunLove.4099	52	1.0%
	1,242	23.3%
	5,337	100

[1] 2004 1 Top 10

* 2003 12 26 ~2004 1 25

2003 12 Win32/Dumaru.worm.9234()
가 Win32/Sobig.worm.F(.F)
가
Win32/Blaster.worm.6176() Win32/Yaha.worm.45568.B,
Win32/AgoBot.worm() Top 10 가
가 Win32/Mimail.worm
가
1 가

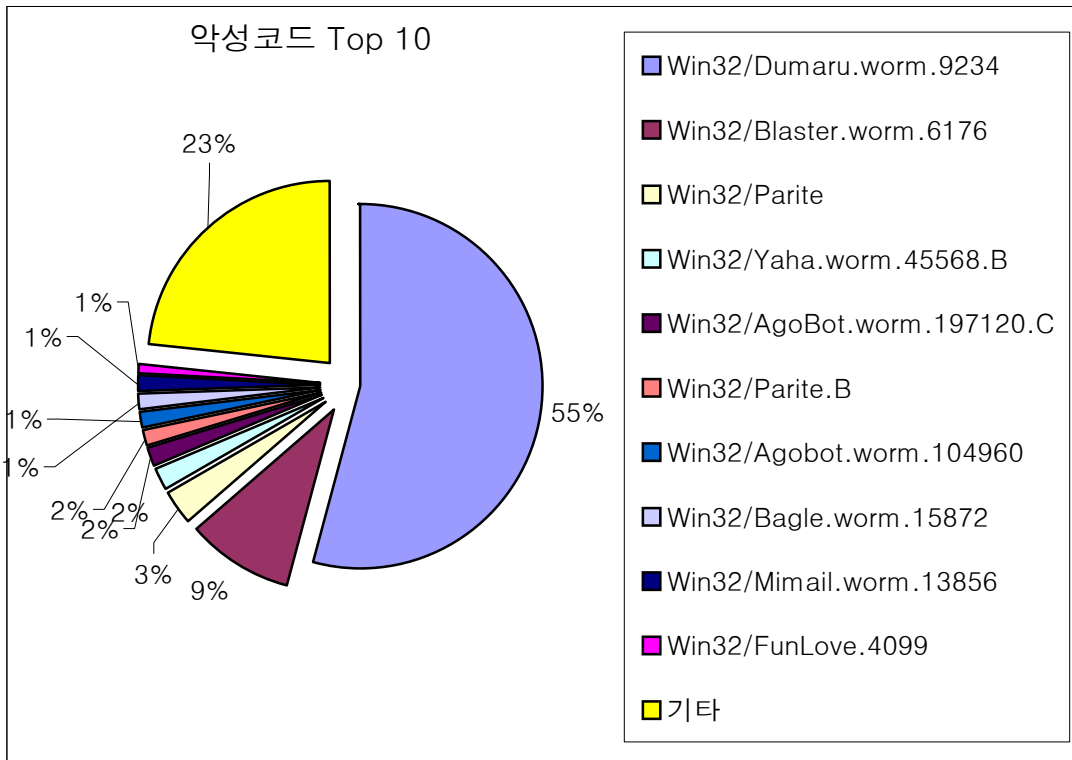
- Win32/Bagle.worm.15872 ()
- Win32/MyDoom.worm.22528 ()

1 19 27
Top 10
1 31 245
VBS(Virus Blocking Service)

1 27
Blocking
Top 10

가

1 Top 10 [1]



[1] 2004 Top 10

가

가
가

()

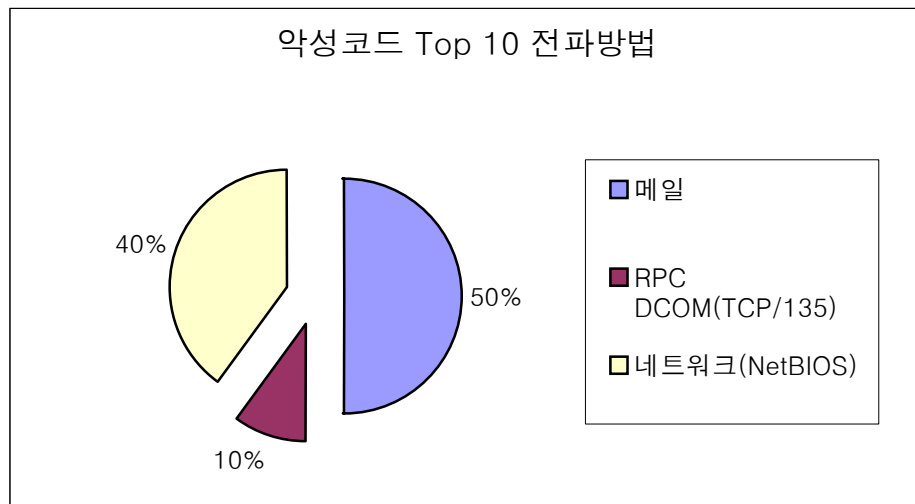
가

[1]

Top 10

가

[2]



[2]

Top 10

Mass Mailer가

가

RPC DCOM

1

가

가

가

1

12

1

가

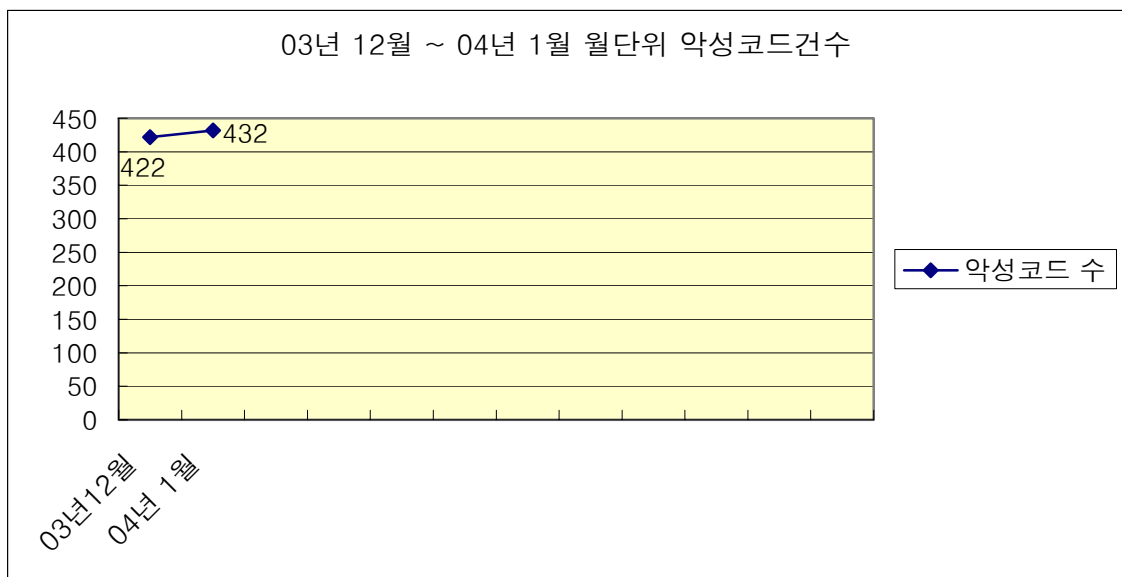
[1], [1]

1

가

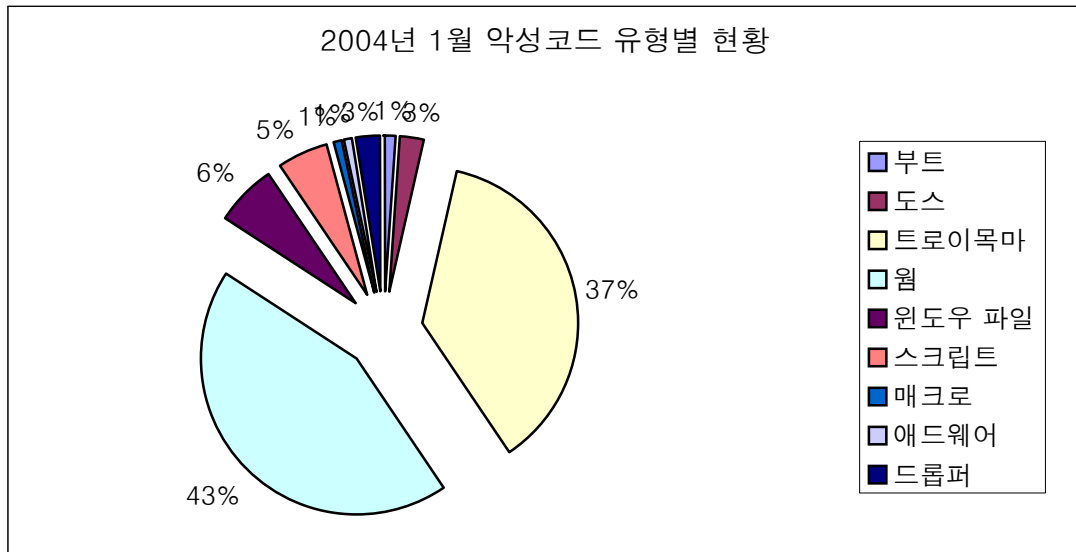
432

가 . (277) 가 64%
) 가 12 가 (422
 , .
 가 가 가
 가 12
 [3] 가 .



[3] 2004

[4] .



[4] 2004 1

12

40%, 42%

가

가

1/4

120

가

II. 1월 국내 신종 악성 코드 발견 동향

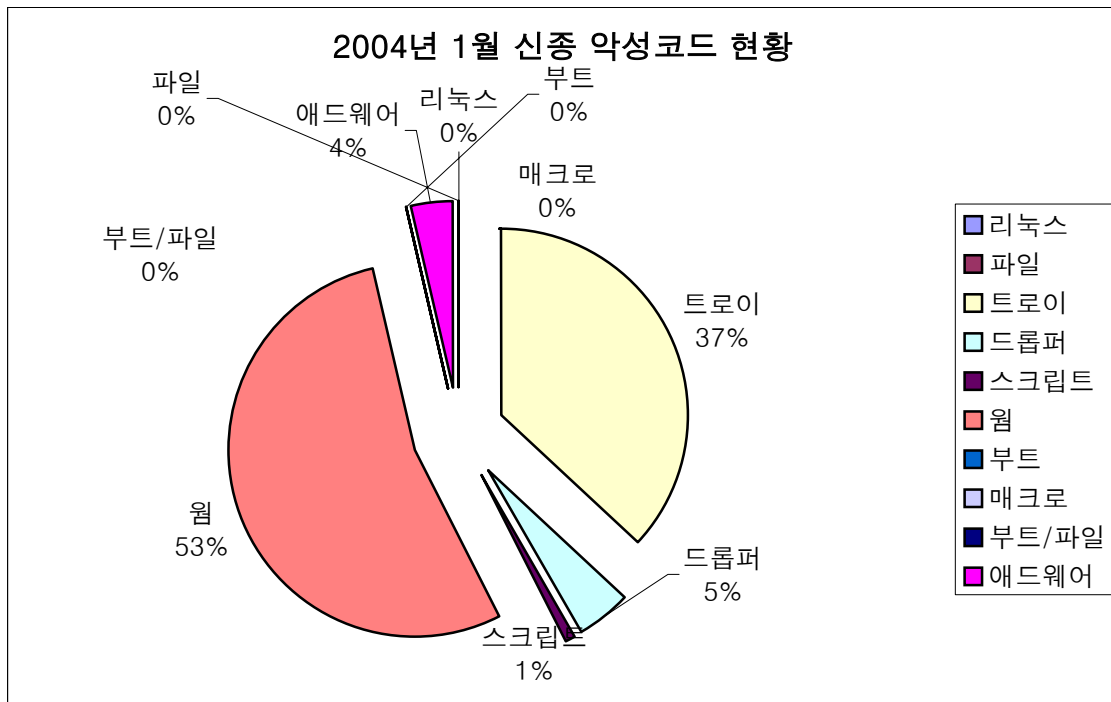
작성자 : 정진성 연구원 (jsjung@ahnlab.com)

1 [1], [1] .

리눅스	파일	트로이	드롭퍼	스크립트	웜	부트	매크로	부트/파일	애드웨어	합계
0	0	40	5	1	58	0	0	0	4	108

[1] 2004 1

* 2003 12 26 2004 1 25



[1] 2004 1

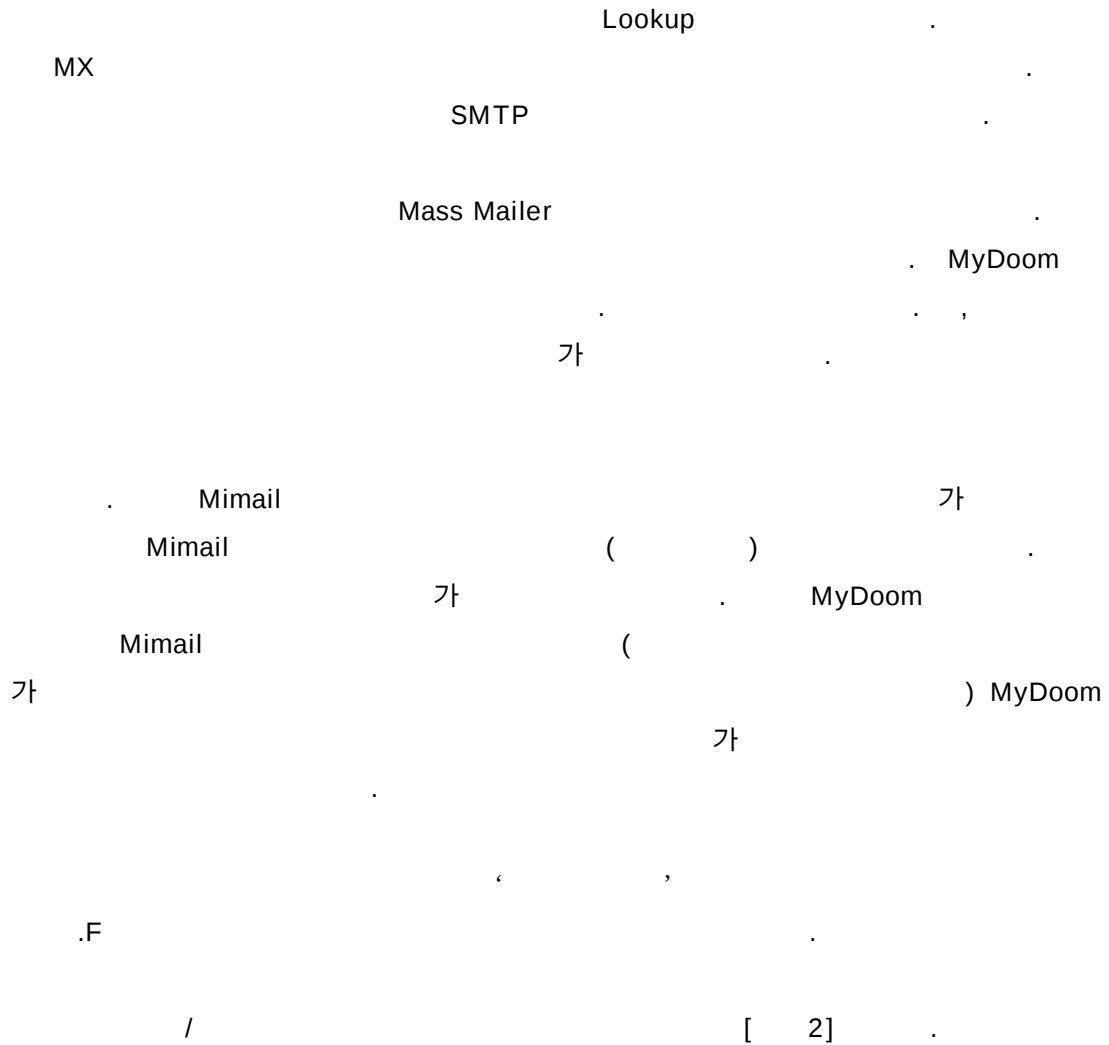
가

가

가 , [1], [1] 2004

가 76%, 10%

가 IRCBot
Win - Trojan/MircPack 가 가 .
.
.
가 IRCBot mIRC IRC
가 IRC
mIRC 가
가 가 가
가 AgoBot
IRCBot
IRCBot
1 IRCBot 74 가 .
가
Win32/MyDoom.worm.22528()
8 Win32/Sobig.worm.F(.F)
?
3가
-
- MX
-
Mass Mailer
MX 가
가
) mx1. / mx.



[3]2003 12 ~ 2004 1

12
 75% 가 . 1 가
 . 1 가 12 가
 .
 ,
 가
 가
 1 ASEC Report
 가
 SPAM
 Mass Mailer
 1
 가 ()
 가 .

III. 1월 신규 보안 취약점

작성자 : 정관진 연구원(intexp@ahnlab.com)

2003 가 . 2003

(SQL Overflow –) . MS SQL

RPC(Remote Procedure Call)

가 . 2004

가

1

1 1 13 () , 3가

ISA(Internet Security and Acceleration)	2000
---	------

H.323

H.323	VoIP(Voice over IP)
-------	---------------------

H.323

. ISA 2000 H.323

가 ISA Firewall

DoS(Denial of Service)

1

가 .

SCO

. SCO 가 SCO

SCO

TCP/80

HTTP

가 . 가 가

가 .

IV. 1월 일본 피해 동향

작성자 : 김소현 연구원(sohkim@ahnlab.com)

1 가 가
W32/Mydoom(Win32/MyDoom.worm.22528,)
1 27
가 Klez Mmail
1 가 [1]
IPA 1 27
3
Klez
1
W32/Bagle(Win32/Bagle.worm.15872) 가

Window/Dos Virus		Macro Virus		Script Virus	
W/Mydoom	245	Xm/Laroux	12	VBS/Redlof	54
W32/Klez	242	W97M/X97M/ P97M/Tristate	3	Wscript/Fortnight	11
W32 Mmail	150	X97M/Divi	2	VBS/Netlog	2
W32/Swen	138	W97M/Ethan	1	VBS/Loveletter	1
W32/Bugbear	103	W97M/Marker	1		
W32/Bagle	95				

[1]

[2]

2004 1

94%

가

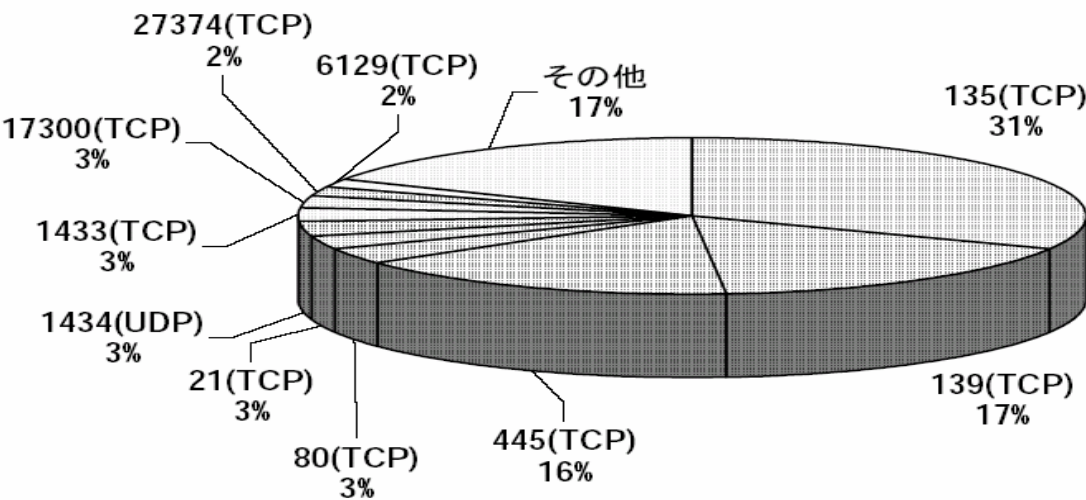
가

. 2003 1 0
가

	2004 1		2003 12		2003 1	
	1,210	91.5%	1,306	89.9%	854	73.7%
	37	2.8%	20	1.4%	232	20.0%
	6	0.5%	15	1.0%	16	1.4%
	1	0.1%	6	0.4%	22	1.9%
	58	4.4%	71	4.9%	0	0%
	11	0.8%	34	2.3%	4	2.9%

[2]

1 135, 139 445
(1). RPC



[1]

V. 1월 중국 피해 동향

작성자 : 장영준 연구원(zhang95@ahnlab.com)

1 1

2003 8 19

Worm.Sobig.F(Win32/Sobig.worm.F)

Worm.Novarg.A(Win32/MyDoom.worm.22528) 1 27

2

	Rising	CNCVERC
1	Worm.Novarg.A	Worm_Mimail.A
2	Worm.Mimail	Worm_lentin
3	Worm.Lentin	Worm.Klez
4	Worm.Klez	Worm_Sobig.F
5	Worm.Sobig.F	Worm_Msblast.A

[1]2004 1

(Rising) 가

(China National Computer Virus Emergency Response Center,

CNCVERC) 2004 1 1

Worm.Novarg.A(Win32/MyDoom.worm.22528) 가

. CNCVERC 1 29

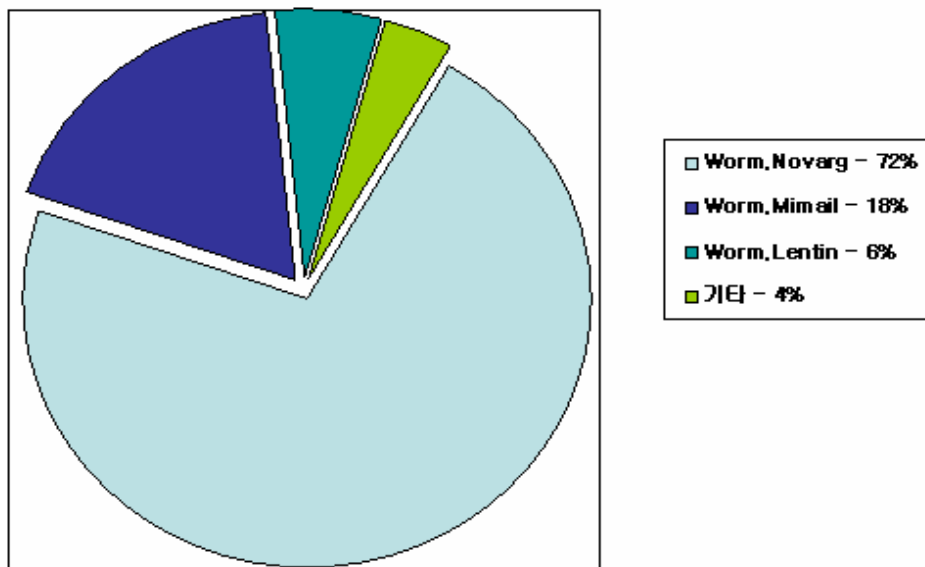
Worm.Novarg.A(Win32/MyDoom.worm.22528) 가

. 1 30 1

(Rising)

Worm.Novarg.A(Win32/MyDoom.worm.22528) 1

가



[1]2004 1

2004 1

Worm.Novarg.A(Win32/MyDoom.worm.22528) 72% 가
 가 . 28% 2003 12 1
 Worm.Mimail(Win32/Mimail.worm, Win32/Mimail.worm.12832)
 18%, Worm.Lentin(Win32/Yaha.worm.20992, Win32/Yaha.worm.27648)
 6% . 4%
 Worm.Klez(Win32/Klez.worm.57345, Win32/Klez.worm.61441) ,
 Worm.Sobig.F(Win32/Sobig.worm.F), Worm.Blaster(Win32/Blaster.worm.6176)
 Script.Redlof(VBS/Redlof) .

Trojan.HuiGeZi Trojan.LMir.Killer 2 1
 . Trojan.LMir.Killer
 Trojan.HuiGeZi
 TCP/5001
 가 .

2 2
 Worm.Novarg.A(Win32/MyDoom.worm.22528) 가 3
 . (Rising),
 Worm.Novarg.A(Win32/MyDoom.worm.22528) 가

가

Worm.BBeagle(Win32/Bagle.worm.15872)

Worm.Novarg.A(Win32/MyDoom.worm.22528)

가

가

ZIP

2004 1 Worm.Novarg.A(Win32/MyDoom.worm.22528)

가

가

2004

VI. 테크니컬 컬럼 - 마이둠 웜의 뒷 이야기

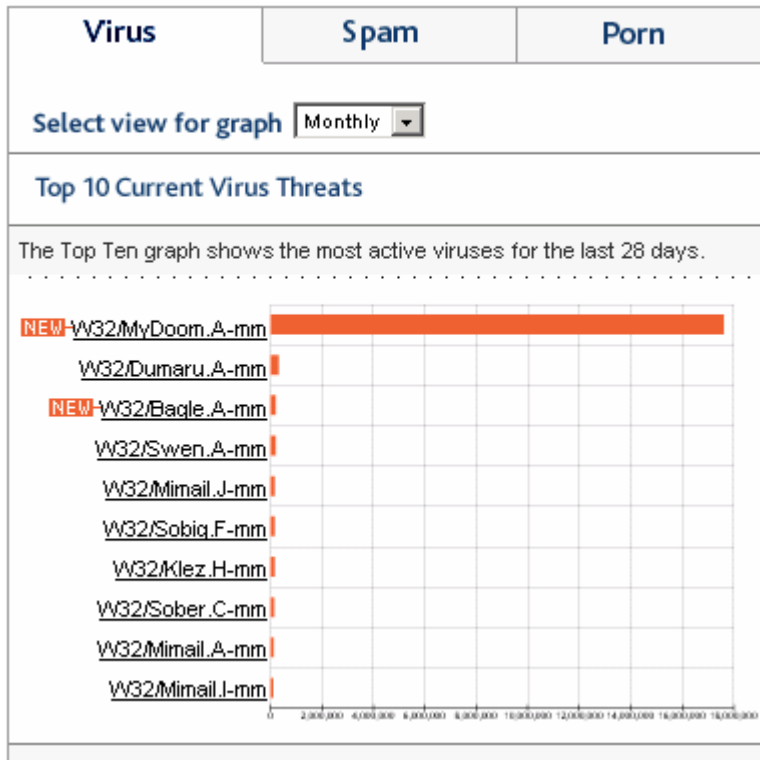
작성자 : 차민석 연구원(jackycha@ahnlab.com)

2004 1 27 가 .
 . “(sync.c,v 0.1
 2004/01/xx xx:xx:xx andy)”
 .
 , , 가
 가 가
 가 . (Mydoom,
http://info.ahnlab.com/smart2u/virus_detail_1298.html)
 ‘Novarg’, ‘Shimg’, ‘Mimail.R’ . , .R
 .R 가
 . , .R .R
 .S .
 가 가
 가 .
 1 29 1 ()
 (http://info.ahnlab.com/smart2u/virus_detail_1299.html) . 2
 7 . sco.com
 가
 2004 2 4 .
 .
 ‘(sync-1.01; andy; I'm just doing my job, nothing personal, sorry)’
 SCO 25
 25

*

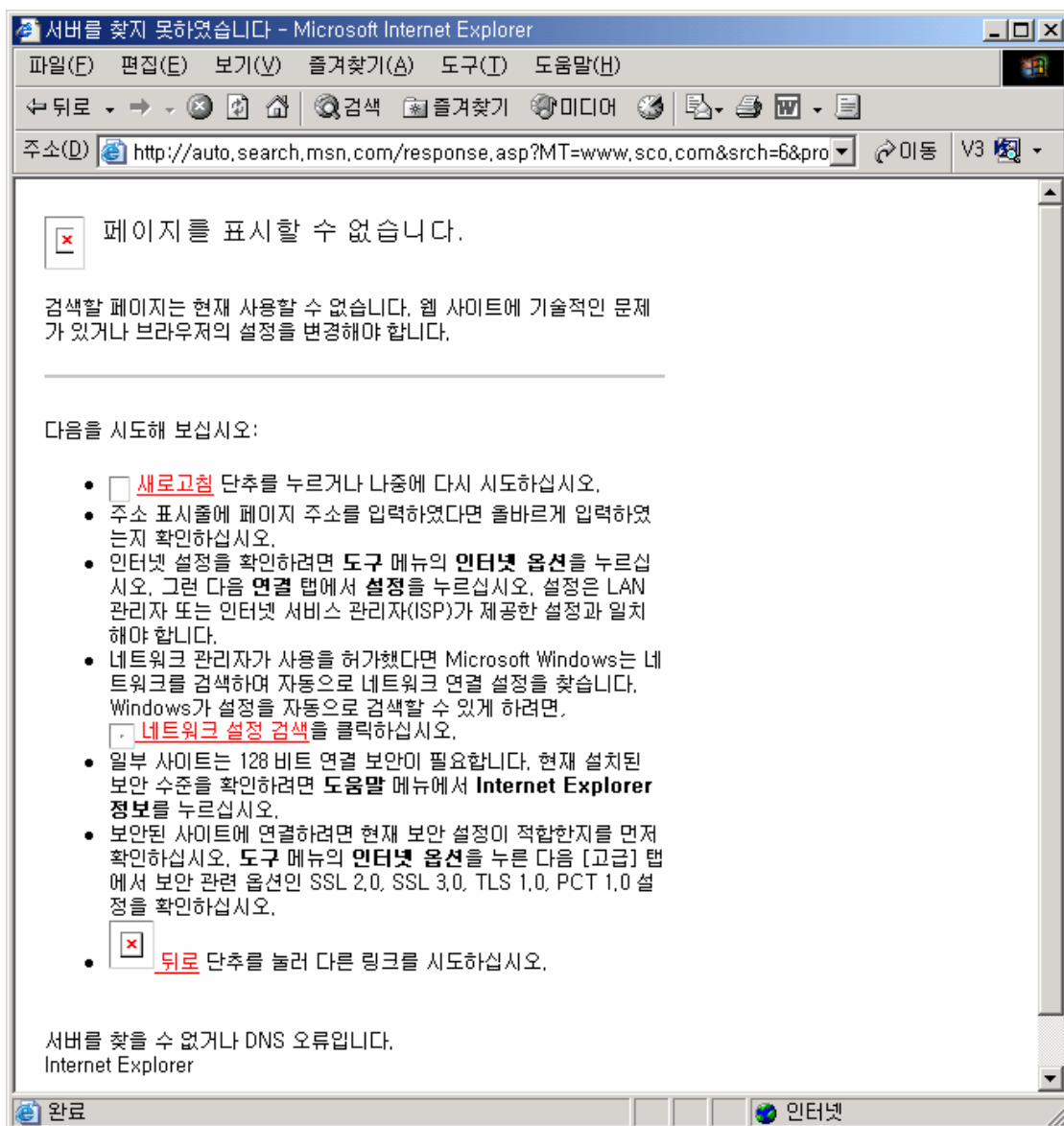
- <http://www.zdnet.co.kr/foreignnews/article.jsp?id=66722&forum=1>
- <http://www.zdnet.co.kr/ecommerce/biztrend/article.jsp?id=66785&forum=1>

10 VBS(Virus Blocking Service) 1,500 ,
 가 50 8 가
 Frisk 13.51%가
 1 28 3 17 62 , 67
 , VBS 19,249 . Frisk 10 8 31.85%,
 3 1
 252 , 114 , 4



[1] / : (http://www.message-labs.com)

sco.com 가 가 . sco.com
sco.com Microsoft.com . Sco.com



[2] sco.com

*

- , SCO

(<http://www.zdnet.co.kr/ecommerce/biztrend/article.jsp?id=66854&forum=1>)

2 4

가 .

.