

통계 · 분석보고서

2003년 9월
해킹바이러스 통계 및 분석 월보

2003년 9월



본보고서 내용의 전부나 일부를 인용시 반드시 [자료:한국정보보호진흥원(KISA)]를 명시하여 주시기 바랍니다.
칼라로 출력하거나 화면으로 보시면 도표를 구분하기가 편합니다.

I . Overview

1. 9월 핫이슈 노트

쟁점사항요약	참조	구분
<ul style="list-style-type: none"> ○ 9월의 CERTCC-KR 신고접수 특징은 전체적으로 사고접수가 감소하였음 <ul style="list-style-type: none"> - MS RPC 취약점을 이용하는 Blaster, Welchia와 그 외 웜들이 많이 발생하였으므로 국내 Windows NT/2000/XP 사용자들은 마이크로소프트사에서 제공하는 패치를 필히 설치를 권고 - Nimda와 CodeRed와 같은 과거에 발생한 웜이 감소한 이유는 개인 사용자들이 백신 이용과 백신엔진 업데이트 이용률이 증가한 것으로 판단됨 ○ Windows NT/2000/XP 계열의 피해가 타 운영체제에 비해 보다 높게 나타남 <ul style="list-style-type: none"> - NT 계열의 MS RPC관련 취약점에 의한 사고 증가가 주요 원인인 것으로 파악 - Windows 사용자들의 취약점 패치 및 Null 패스워드 사용 점검이 필요 ○ MS RPC(135 포트)에 대한 스캔이 상대적으로 많은 증가를 보인 것은 MS Blaster와 Welchia 웜으로 인한 결과 ○ 악성프로그램 및 불법침입은 8월에 비해 감소 	<p style="text-align: center;">본문 3 페이지, 6 페이지 7 페이지 참조</p>	<p style="text-align: center;">해킹</p>
<ul style="list-style-type: none"> ○ 9월의 바이러스로 인한 피해신고 건수는 총 20,681건으로 전월보다 9,462건 증가 <ul style="list-style-type: none"> - 기존에 발견된 메일을 통하여 전파되는 Sobig.F 웜에 의한 피해 급증 ○ 9월 한 달간 신종 바이러스의 총 9종 출현하여 전월보다 6종 감소 <ul style="list-style-type: none"> - 국산 1종, 외산 8종 - 인터넷웜 7건, 트로이 목마 2건 - MSN 메신저를 통하여 전파되는 신종 Sribag 웜 출현 ○ 최근에 주로 윈도우 취약점을 이용한 웜 등이 등장하여 많은 피해를 주고 있어 보안 패치 점검 필요 	<p style="text-align: center;">본문 4 페이지, 8 페이지 참조</p>	<p style="text-align: center;">바이러스</p>
<ul style="list-style-type: none"> ○ 지난 8월보다 전체 스캔탐지 건수가 증가하였음 <ul style="list-style-type: none"> - MS Blaster와 Welchia에 의한 공격으로 인한 결과로 보임 - 135(RPC)포트 스캔 증가 ○ 국외로부터의 스캔탐지는 지난 8월보다 대폭 증가(164-> 1526) 현상을 보임 ○ 주로 MS RPC관련 135번 포트 스캔 비율이 가장 높음 	<p style="text-align: center;">본문 9 페이지 10 페이지 11 페이지 참조</p>	<p style="text-align: center;">스캔탐지</p>

2. 전체 추이

□ 해킹사고 처리 및 대응

- 9월의 CERTCC-KR 신고접수 특징은 전체적으로 사고접수가 감소하였음
- Windows NT/2000/XP 계열의 피해가 타 운영체제에 비해 보다 높게 나타남
 - NT 계열의 MS RPC관련 취약점을 이용한 Blaster 또는 Welchia 웜에 의한 사고 증가가 주요 원인인 것으로 파악
 - Windows 사용자들의 취약점 패치 및 Null 패스워드 사용 점검이 필요
- MS RPC(135 포트)에 대한 스캔이 상대적으로 많은 증기를 보인 것은 MS Blaster와 Welchia 웜으로 인한 결과
- 지난 8월보다 전체 스캔탐지 건수가 증가하였음
 - MS RPC(135) 포트 스캔 대폭 증가

구분	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
일반 해킹	6,684	1,120	912	934	923	1,012	1,076	991	1,311	1,179				9,458
일반 웜	2,971	974	522	1,158	771	221	307	48	423	119				4,543
스팸릴레이	5,537	469	392	1,308	1,616	1,904	436	774	301	122				7,322
합계	15,192	2,563	1,826	3,400	3,310	3,137	1,819	1,813	2,035	1,420				21,323

※ 2002. 6월 스팸릴레이 6,851건 대응현황은 제외되었음.

※ 스팸릴레이는 CERTCC-KR 접수분과 홈페이지를 통한 원격점검시 문제서버로 판명된 서버(59개)들의 합.

※ 2002년 동월 대비 일반해킹(442, 166% 증가), 일반 웜(172, 31% 감소), 스팸릴레이(529, 77% 감소)

□ 바이러스 신고건수 및 신종출현건수

- Sobig.F 등 메일로 전파되는 기존의 웜의 기승으로 인하여 9월 한달 간 총 20,681건 피해 접수됨 (전월보다 9,462건 증가)
- 신종 바이러스 9건 출현 (국산 1, 외산 8)
 - 웜 7종, 트로이목마 2종 출현

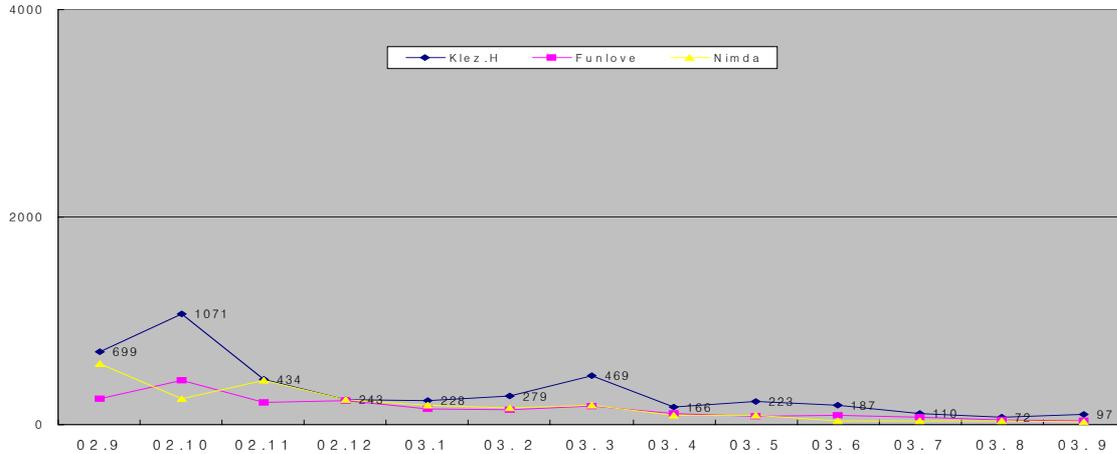
구분	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
신종출현건수	232	33	6	7	2	4	14	8	15	9				98
피해신고접수건수	38,677	3,757	3,238	3,797	3,180	4,612	3,522	2,550	11,039	20,681				56,376

※ KISA, 안철수, 하우리, 시만텍, 트렌드 공동집계

※ 바이러스 신고 건수 : 바이러스로 인하여 국내에서 피해가 발생한 건수

○ 8월보다 클레즈변종, 펀러브 등 악성바이러스의 피해는 다소 감소함.

※ Klez.H(72건->97건), Funlove(41건->38건), Nimda(34건->26건)



○ 9월 바이러스 피해신고 중 인터넷 뭍이 19,682건으로 가장 많음

구분	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
바이러스	9,308	1,096	975	783	467	536	924	925	832	522				7,060
인터넷 뭍	27,021	1,361	1,320	2,537	2,350	3,704	1,854	1,185	9,748	19,682				43,741
트로이목마 (or 백도어)	1,687	1,284	876	419	303	304	491	411	334	387				4,809
가짜(Hoax)	13	0	16	10	5	9	5	6	4	2				57
조크(Joke)	111	5	1	6	3	0	0	3	1	2				21
기타	537	11	50	42	52	59	248	20	120	86				688
합계	38,677	3,757	3,238	3,797	3,180	4,612	3,522	2,550	11,039	20,681				56,376

○ 9월에 국내에서 발견된 신종바이러스는 총 9건으로 인터넷 뭍 7종, 트로이목마 2종임

구분	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
바이러스	57	3	0	0	0	1	0	2	0	0				6
인터넷 뭍	108	26	2	5	2	3	7	1	9	7				62
트로이목마 (or 백도어)	60	4	4	1	0	0	5	5	6	2				27
가짜(Hoax)	0	0	0	0	0	0	0	0	0	0				0
조크(Joke)	0	0	0	1	0	0	0	0	0	0				1
기타	7	0	0	0	0	0	2	0	0	0				2
합계	232	33	6	7	2	4	14	8	15	9				98

※ 악성프로그램의 정의에 의한 분류임.

○ 신종 바이러스 출처별로는 국산 1종, 외산 8종으로 외산이 주종을 이룸

구분	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
국산	23	2	0	0	0	0	0	0	2	1				5
외산	209	31	6	7	2	4	14	8	13	8				93
합계	232	33	6	7	2	4	14	8	15	9				98

□ 해킹시도탐지 건수 및 대응 현황

- 9월보다 전체 스캔탐지 건수가 많이 증가하였음
- MS RPC(135)에 대한 스캔 대폭 증가
 - MS Blaster에 의한 공격으로 인한 결과로 보임

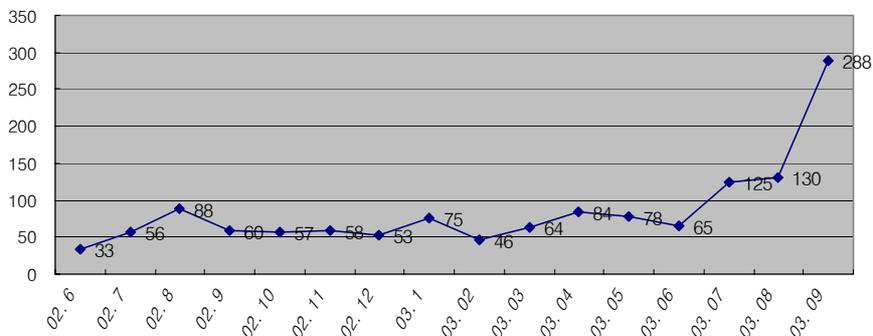
구분	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
탐지건수	22,036	648	593	656	402	345	1,489	469	1,168	3,120				8,890
대응건수	6,200	425	422	519	329	266	1,246	410	451	1,496				5,564

- ※ 2000년 11월부터 국내 30여개 서버에 설치된 에이전트의 스캔탐지결과를 분석.
- ※ 2002년 3월부터 KISA가 국내외 CERT 등에 탐지내 RTSD용을 통지하고 있음.

□ 일반상담 현황

- 9월 일반상담에는 기타 컴퓨터관련 문의가 287건, 타인 명예훼손이 1건 접수
 - 기타 컴퓨터 관련 문의에는 윈도우 업데이트 및 패치방법에 대한 문의 및 인터넷 익스플로러의 초기화면이 특정사이트로 변조되어 수정되지 않거나 성인사이트로 접속유도하는 등의 증상 관련 문의
 - MS RPC 취약점을 이용하는 MS Blaster와 Welchia와 관련된 패치 및 업데이트 방법에 대한 문의가 상당히 많았음
- ※ 일반상담은 컴퓨터관련 문의와 타인명예훼손으로 구분

월	02.09	02.10	02.11	02.12	03.01	03.02	03.03	03.04	03.05	03.06	03.07	03.08	03.09	2003년 총계
건수	60	57	58	53	75	46	64	84	78	65	125	130	288	834



(2003년 일반상담현황)

II. 세부분석

1. 9월 해킹 분석

o 2003년 9월 접수한 총 1,196건 중 분석 가능한 186건을 토대로 하여 작성

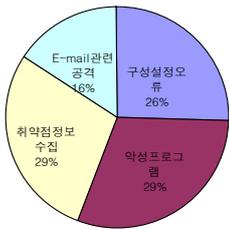
□ OS현황 (분석자료 기준)

- o Windows NT/2000/XP 계열의 피해가 타 운영체제에 비해 보다 높게 나타남
 - NT 계열의 MS RPC관련 취약점에 의한 사고 증가가 주요 원인인 것으로 파악
 - Windows 사용자들의 취약점 패치 및 Null 패스워드 사용 점검이 필요

운영체제	2002	2003												2003년 합계	
		1	2	3	4	5	6	7	8	9	10	11	12		
Win NT/2000/XP	2,279	687	248	1,338	1,082	935	189	227	463	72					5,241
Win 95/98	2,098	458	405	366	564	347	370	129	126	65					2,830
Linux	574	29	74	62	53	33	21	20	11	3					306
Solaris	90	7	1	2	1	3	0	0	0	0					14
AIX	19	0	1	0	2	0	0	0	0	0					3
HP-UX	12	0	1	1	1	0	1	0	0	0					4
Digital Unix	6	0	1	0	0	1	0	0	0	0					2
DEC/IRIX	3	0	0	0	0	0	0	0	0	0					0
CISCO	2	0	0	0	0	0	0	0	0	0					0
N/A	1,361	278	180	476	859	901	165	166	82	46					3,153
합계	6,444	1,459	911	2,245	2,562	2,220	746	542	682	186					11,553

※ OS별 현황자료는 OS별 안전성과는 상관관계가 없으며, 단지 신고에 따른 분석자료임

□ 공격수법별 구분 (분석자료 기준)



o 전체적으로 8월에 비해 감소하였으나 MS Blaster와 Welchia 웜으로 인한 취약점 정보수집과 관련한 사고는 비슷한 수준을 나타내고 있음.

※ 좌측의 그래프는 9월의 Top 4 현황임

공격수법	2002	2003												2003년 총계	
		1	2	3	4	5	6	7	8	9	10	11	12		
사용자도용	147	12	9	7	4	1	3	3	1	1					41
S/W보안오류	602	130	34	893	452	92	14	0	3	1					1,619
버퍼오버플로우	243	445	28	28	43	42	47	42	392	25					1,092
구성설정오류	4,638	733	808	2,059	1,960	2,031	585	399	203	101					8,879
악성 프로그램	4,112	1,148	557	1,232	934	306	450	185	544	119					5,475
프로토콜취약점	1	0	0	0	0	0	0	0	0	0					0
서비스거부	18	29	0	0	0	0	0	1	0	0					30
E-mail관련	1,943	258	346	1,018	1,617	1,905	289	353	137	63					5,986
취약점정보수집	3,971	703	535	1,219	930	303	440	171	175	113					4,589
사회공학	0	0	0	0	0	0	0	0	0	0					0
총계	15,675	3,458	2,317	6,456	5,940	4,680	1,828	1,154	1,455	423					27,711

- ※ 한 사고내에 다수의 공격수법이 사용될 수 있음
- ※ 전체 취약점정보수집은 9쪽 "3. 스캔탐지 현황"을 참조

□ 침해유형에 따른 구분(분석자료 기준)

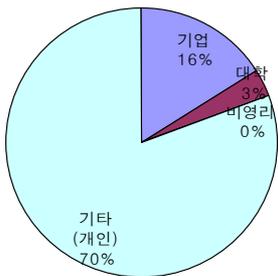


- 타 시스템의 불법자원 사용 감소
- 침입시도 및 불법침입 또한 7월에 비해 감소
- ※ 좌측의 그래프는 9월의 Top 3 현황임

불법행위	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
침입시도	4,044	705	537	1,217	930	303	435	168	174	115				4,584
불법침입	3,364	1,006	530	1,202	827	262	365	97	111	62				4,462
자료유출	1	0	0	0	0	0	0	0	0	0				0
자료변조삭제	61	1	1	1	3	1	5	5	1	1				19
불법자원사용	3,296	601	722	1,997	1,884	1,997	558	386	529	79				8,753
홈페이지변조	5	1	0	0	0	1	1	1	0	1				5
시스템파괴	0	0	0	0	0	0	1	0	0	0				1
시스템오류	2	0	0	0	1	0	0	0	0	0				1
서비스거부	11	29	0	0	0	0	0	1	0	0				30
총계	10,784	2,343	1,790	4,417	3,645	2,564	1,365	658	815	258				17,855

※ 한 사고내에 다수의 불법행위가 사용될 수 있음.

□ 기관별 구분(분석자료 기준)



- 기관별 전체 사고접수는 전월에 비해 상당히 감소하였으며, 특히 기업과 개인에 대한 사고접수가 감소
- 윈도우 계열 공격이 타 운영체제에 비하여 많으므로 개인들의 피해가 상대적으로 높은 편임
- ※ 좌측의 그래프는 9월의 Top 4 현황임

기관	도메인	2002	2003												2003년 총계
			1	2	3	4	5	6	7	8	9	10	11	12	
기업	co	1,812	298	190	900	303	254	101	104	123	20				2,293
대학	ac	716	142	71	108	155	79	44	27	55	4				685
비영리	or	154	31	11	24	22	17	6	5	2	0				118
연구소	re	22	3	2	2	3	3	0	0	1	0				14
네트워크	ne	4	6	2	2	0	10	12	0	0	0				32
기타(개인)		3,736	979	635	1,235	2,042	1,587	572	410	424	100				7,984
총계		6,444	1,459	911	2,271	2,525	1,950	735	546	605	124				##

※ ISP는 기타에 포함.

2. 바이러스(악성프로그램)

□ 9월중 주요 악성프로그램 현황

바이러스명	최초 발생시점	2002	2003												2003년 총계
			03.1	03.2	03.3	03.4	03.5	03.6	03.7	03.8	03.9	03.10	03.11	03.12	
Klez.H	02.4	8,711	228	279	469	116	223	187	110	72	97				1,781
Nimda.A	01.9	6,717	189	157	186	90	86	39	32	34	26				839
Funlove4099		4,413	153	145	174	110	78	87	69	41	38				895
Opaserv	02.10	2,332	365	173	300	172	126	89	86	62	83				1,456
Nimda.D		1,362	63	59	59	43	43	47	276	37	21				648
Winevar	02.11	944	20	35	6	4	2	1	2	7	2				79
Spida		568	5	57	7	0	1	2	1	0	1				74
Bride	02.11	438	4	0	12	0	3	0	0	0	0				19
mIRCpack	02.11	343	683	125	180	71	80	103	60	35	26				1,363
Sircam		270	8	6	4	4	1	5	4	1	2				35
Slammer	03.1	0	67	81	2	4	2	4	2	9	0				171
Blaster	03.8	0								5,792	1,005				6,797
Welchia	03.8	0								195	441				636
Sobig.F	03.8	0								2296	15255				17,551
Smibag	03.9	0									221				221
Swen	03.9	0									62				62

※ KISA, 안철수, 하우리, 시만텍, 트렌드 공동집계

□ 9월중 Top10 악성프로그램 현황

순위	명칭	건수
1	SOBIG.F	15,255
2	YAHA	1,820
3	BLASTER	1,005
4	WELCHIA	441
5	SMIBAG	221
6	PARITE	178
7	DUMARU	159
8	VALLA	117
9	RTKIT	112
10	KLEZ.H	97
	기타	1,276
계		20,681

□ 9월의 신종바이러스 경보 발령 (A급: 0건, B급: 0건 C급 : 3건)

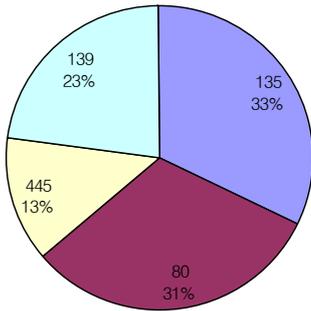
구분	바이러스명	등급	발령일	참고사이트
1 주의	Win32/Smibag.worm	C	09.26	http://www.certoc.or.kr/cvirc/Alert/warning/2003/Wn32_Smibag_worm.html
2 주의	Win32.Swen@mm.worm	C	09.19	http://www.certoc.or.kr/cvirc/Alert/warning/2003/W32_Swen@mm_worm.html
3 주의	Win32.Agobot.worm	C	09.10	http://www.certoc.or.kr/cvirc/Alert/warning/2003/Wn32_Agobot.html

※ A : 비상, B : 경고, C : 주의

3. 스캔탐지 현황

- o CERTCC-KR에서 인지한 스캔 관련 정보를 일괄적으로 취합하여 작성.

□ 국내 공격자가 행한 포트 스캔 현황



- o 지난 9월보다 전체 스캔탐지 건수가 증가하였음
- o MS RPC(135)에 대한 스캔 증가
 - MS Blaster와 Welchia에 의한 스캔 공격으로 인한 결과로 보임

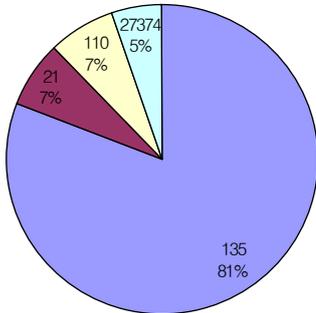
※ 좌측의 그래프는 9월의 Top 4 현황임

포트 번호	2002	2003												2003년 합계
		1	2	3	4	5	6	7	8	9	10	11	12	
21	2,065	114	97	74	51	70	61	131	39	170				807
22	672	18	17	22	9	2	3	5	10	15				101
23	70	9	6	2	3	5	6	11	3	14				59
25	4,228	200	136	105	49	56	54	110	248	358				1,316
53	372	5	7	6	1	9	8	17	4	21				78
80	1,065	262	151	529	712	455	194	649	342	991				4,285
110	241	0	0	1	0	10	13	23	20	43				110
111	744	12	10	10	10	6	6	12	6	18				90
135	53	15	22	8	3	15	6	21	993	1,014				2,097
137	746	254	386	193	117	12	27	39	39	78				1,145
139	441	309	47	21	135	84	550	634	95	729				2,604
443	270	15	43	19	11	29	100	129	29	158				533
445	287	127	180	718	183	165	193	358	66	424				2,414
515	136	1	4	2	2	2	1	3	1	4				20
1433	2,452	150	100	92	78	38	40	78	33	111				720
1434	0	429	7	10	7	5	6	11	15	26				516
8080	36	1	0	0	0	0	2	2	3	5				13
12345	1,717	121	7	6	43	18	61	79	39	118				492
17300	16	0	61	4	44	118	228	346	32	378				1,211
27374	601	116	27	32	4	23	58	81	11	92				444
기타	4,123	53	148	139	17	141	324	465	336	801				2,424
합계	20,335	2,211	1,456	1,993	1,479	1,263	1,941	3,204	2,364	5,568				21,479

※ 본 항목은 CERTCC-KR 접수분과 RTSD 탐지분의 합임.

※ 기타는 3389, 500, 3128, 1080 포트 등

□ 국외 공격자가 국내로 가한 포트 스캔 현황



- 국외로부터의 스캔탐지는 지난 8월보다 대폭 증가(164> 1526) 현상을 보임
- 주로 Blaster 또는 Welchia에 의한 스캔공격으로 인하여 135번 포트 스캔 비율이 가장 높음

※ 좌측의 그래프는 9월의 Top 4 현황임

포트 번호	2002	2003												2003년 합계
		1	2	3	4	5	6	7	8	9	10	11	12	
21	2,528	40	55	63	53	50	71	15	17	90				454
22	696	6	6	12	4	3	9	1	2	5				48
23	109	2	4	2	3	1	0	0	2	0				14
25	514	13	8	6	7	10	14	2	28	14				102
53	179	0	3	4	2	6	2	1	0	15				33
80	6	0	0	684	1	7	3	1	15	14				725
110	44	0	2	0	0	2	0	0	0	92				96
111	764	3	0	1	0	0	1	0	1	2				8
135	6	1	0	1	0	1	12	0	7	1,048				1,070
139	83	0	0	2	1	2	68	2	5	10				90
443	151	8	13	13	2	1	3	2	1	3				46
445	50	4	26	34	13	13	116	1	0	30				237
515	228	0	0	0	0	0	1	0	8	0				9
1433	1,518	23	23	20	2	3	21	0	0	3				95
8080	3	0	0	0	0	0	0	2	0	3				5
12345	47	3	0	0	1	1	3	1	0	5				14
17300	0	0	11	2	7	8	12	0	0	0				40
27374	174	2	0	0	2	3	4	1	1	68				81
기타	1,143	42	28	49	24	57	218	50	77	124				669
합계	8,243	147	179	893	122	168	558	79	164	1,526				3,836

※ 본 항목은 CERT 접수분과 RTSD 탐지분의 합임.

※ 기타는 1080, 3128, 3389 포트 등

□ 최근 해킹(웜 포함)에 이용되는 포트별 특징

포트	주요서비스	참고사항
80	web 서비스	o CodeRed, Nimda 등의 공격에 사용
135	MS RPC	o MS RPC 취약점을 공격하는 악성프로그램 및 인터넷웜들의 공격방법에 사용
445	SMB	o Window 계열 NetBios 공유폴더를 이용하는 각종 바이러스 공격에 사용
1433	MS-SQL	o Spida 웜의 공격에 사용
1434	MS-SQL	o Slammer 웜의 공격에 사용
8080, 3128	Squid	o 릴레이를 허용하는 서버를 찾는 스캔 - http://www.certcc.or.kr/paper/tr2002/tr2002_04/spam.pdf
2222	Apache 웜 백도어	o 상세내용은 아래의 문서참조 - http://www.certcc.or.kr/advisory/ka2002/ka2002-060.txt
6667	mIRC	o mIRC 프로그램을 이용한 트로이목마 공격에 사용
12345	netbus	o Window98용 백도어 netbus에서 사용
17300	Kuang2	o Windows용 트로이 목마로 중국에서 제작된 것으로 추정됨
27374	SubSeven	o Window용 백도어 subseven에서 사용

□ 9월 포트 스캔 출발지·목적지의 특징

- o 인터넷 웜에 의한 포트 스캔이 많아져, 정확한 포트 스캔 방향을 규정짓기 어려워지는 경향이 있음.

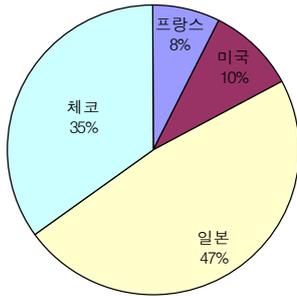


※ 위의 표는 신고접수 기준으로 한 자료임.(RTSD 탐지건수는 포함되지 않았음)

※ 사용자 도용 등 포트 스캔이 사용되지 않는 경우와 SPAM의 경우는 제외하였음.

Ⅲ. 국가/지역별 분석

□ 스캔 Source가 국내, Destination이 국외인 경우 (whois 정보기준)

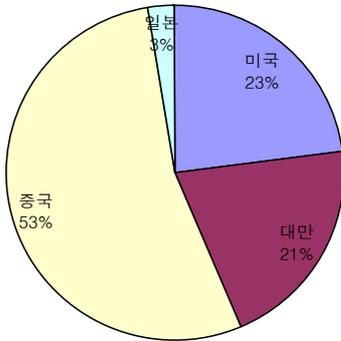


- 국내에 출발한 스캔공격의 대다수는 아시아와 아메리카, 유럽 대륙을 목표로 하고 있음.
 - 체코에 대한 스캔이 특이하게 많이 발생하였음
- ※ 좌측의 그래프는 9월의 Top 4 현황임

대륙	국가	2002	2003												2003년 총계
			1	2	3	4	5	6	7	8	9	10	11	12	
아메리카	미국	2,100	611	639	441	401	247	416	185	215	80				3,235
	브라질	68	46	15	7	5	6	50	21	8	29				187
	캐나다	173	63	73	31	47	31	33	25	29	16				348
	기타	189	0	0	0	10	0	18	4	30	17				79
	소계	2,530	720	727	479	463	284	517	255	290	201				3,936
아시아	대만	0	0	0	0	0	0	8	0	0	0				8
	일본	2,050	595	188	537	345	289	479	457	853	398				4,141
	중국	0	1	0	0	0	0	0	0	0	0				1
	이스라엘	418	102	21	241	578	369	8	51	41	0				1,411
	기타	43	2	1	1	36	2	41	29	32	132				276
	소계	2,511	700	210	779	959	660	536	537	926	530				5,837
아프리카	기타	1	0	0	0	0	0	1	0	0	50				51
	소계	1	0	0	0	0	0	1	0	50					52
오세아니아	뉴질랜드	20	1	2	10	9	1	24	11	0	0				58
	호주	407	21	5	1	9	5	10	8	9	7				75
	소계	427	22	7	11	18	6	34	19	9	7				133
유럽	네덜란드	7	10	3	30	1	0	0	0	1	1				46
	덴마크	7	1	0	0	3	1	0	1	0	0				6
	독일	349	29	12	11	3	1	0	1	0	0				57
	벨기에	5	0	1	0	0	0	0	0	0	5				6
	스웨덴	132	3	0	1	3	0	4	0	0	0				11
	체코	0	0	0	0	0	0	0	0	0	291				291
	스페인	5	3	32	0	0	1	0	0	0	0				36
	영국	34	3	4	10	8	17	11	4	11	25				93
	오스트리아	11	6	2	0	2	2	1	2	2	1				18
	프랑스	358	53	52	56	54	54	48	50	40	63				470
기타	154	111	66	4	90	2	24	46	36	3				382	
	소계	1,062	219	172	112	164	78	92	114	89	210				1,250
총계		6,531	1,661	1,116	1,381	1,604	1,028	1,180	926	1,314	998				11,208

※ 위의 표는 신고접수 기준으로 한 자료임.(RTSD 탐지건수는 포함되지 않았음)

□ 스캔 Source가 국외, Destination이 국내인 경우(whois 정보기준)



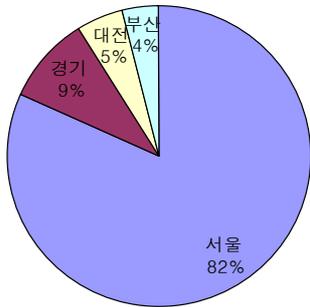
○ 8월 국외 스캔공격은 8월보다 상당히 감소하였으며, 그 가운데 중국, 미국으로부터 스캔시도가 많은 것을 알 수 있음

※ 좌측의 그래프는 9월의 Top 4 현황임

대륙	국가	2002	2003												2003년 총계
			1	2	3	4	5	6	7	8	9	10	11	12	
아메리카	미국	4	43	81	41	22	44	111	9	41	9				43
	브라질	0	0	0	0	0	0	0	0	0	0				0
	캐나다	1	5	11	5	4	2	6	0	0	0				5
	기타	9	0	18	8	3	8	0	2	1	2				0
	소계	14	48	110	54	29	54	117	11	42	11				476
아시아	대만	48	5	53	21	6	7	44	0	4	8				148
	일본	24	3	11	10	2	1	21	1	4	1				54
	중국	98	13	66	40	30	41	163	41	94	21				509
	이스라엘	10	0	5	4	0	1	9	2	0	0				21
	기타	51	5	10	8	7	8	23	6	8	6				81
소계	231	26	145	83	45	58	260	50	110	36				813	
아프리카	기타	2	0	0	0	0	1	1	0	0	0				2
	소계	2	0	0	0	0	1	1	0	0	0				2
오세아니아	뉴질랜드	0	0	0	0	0	0	1	0	0	0				1
	호주	7	46	39	19	1	1	1	0	3	1				111
	소계	7	46	39	19	1	1	2	0	3	1				112
유럽	네덜란드	13	4	12	11	5	12	102	1	4	0				151
	덴마크	2	0	0	0	1	3	0	0	0	0				4
	독일	85	11	31	16	10	9	17	2	0	0				96
	벨기에	13	1	5	2	1	0	3	0	0	0				12
	스웨덴	8	0	1	0	0	2	2	0	0	0				5
	스위스	6	1	0	0	1	0	0	0	0	0				2
	스페인	3	0	2	2	0	2	2	0	0	0				8
	영국	0	0	6	2	3	4	6	1	0	0				22
	오스트리아	5	1	1	0	0	0	0	0	0	0				2
	프랑스	52	5	11	4	10	7	25	3	2	0				67
	기타	27	3	21	12	17	9	15	13	7	2				99
소계	214	26	90	49	48	48	172	20	13	2				468	
총계		468	146	384	205	123	162	552	81	168	50				1,871

※ 위의 표는 국내신고를 기준으로 한 자료임.(RTSD 추출정보는 2002년 10월 이후 추가되었음)

□ 지역별(국내) 스캔 Source 현황(whois 정보 기준)



○ 금월, 지역별 구분에서는 이전의 경향과 같이 서울에서 발생한 스캔이 가장 많음.

※ 좌측의 그래프는 9월의 Top 4 현황임
 ※ (국내->국외) + (국내->국내)

분류	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
서울	5,162	1,026	792	1,118	1,085	758	1,187	703	980	1,683				9,332
부산	384	66	41	44	27	17	25	39	43	82				384
대구	191	21	29	21	23	20	6	10	12	22				164
인천	105	16	16	18	17	14	7	12	13	25				138
광주	108	16	2	11	10	4	10	7	6	13				79
대전	180	70	36	49	53	43	46	30	70	100				497
울산	56	12	5	15	8	2	2	0	2	2				48
경기	825	143	84	126	90	92	133	79	115	194				1,056
강원	140	11	11	24	6	4	11	3	29	32				131
충북	249	10	11	21	5	5	11	3	11	14				91
충남	106	34	14	7	10	5	7	4	12	16				109
전북	116	20	16	139	99	34	58	8	23	31				428
전남	141	79	52	11	6	7	8	3	5	8				179
경북	122	20	12	19	17	20	5	5	7	12				117
경남	143	9	13	14	10	9	21	25	31	56				188
제주	30	2	3	4	4	3	4	0	1	1				22
N/A	1,565	656	317	397	317	226	397	417	389	806				3,922
총계	9,623	2,211	1,454	2,038	1,787	1,263	1,938	1,348	1,748	3,097				16,885

※ RTSD 추출정보는 2002년 10월 이후 추가되었음

□ 기관별(국내) 스캔 Source 현황(whois 정보 기준)



○ 금월, 기관별 구분에서는 이전의 경향과 같이 개인이용자가 발생시킨 스캔이 가장 많음

※ 좌측의 그래프는 9월의 Top 4 현황임
 ※ RTSD 추출정보는 추가되지 않았음.

기관	도메인	2002	2003												2003년 총계
			1	2	3	4	5	6	7	8	9	10	11	12	
기업	co	1,634	289	206	228	236	159	141	125	209	152				1,745
대학	ac	815	171	75	155	127	90	68	61	140	90				977
비영리	or	99	34	27	33	18	15	15	10	24	10				186
연구소	re	20	4	5	3	2	0	0	4	3	1				22
네트워크	ne	9	7	2	2	1	14	27	0	0	0				53
기타(개인)		3,917	1,207	809	1,148	1,237	812	944	765	978	775				8,675
총계		6,494	1,712	1,124	1,569	1,621	1,090	1,195	965	1,354	1,028				11,658