통계 · 분석보고서

2003년 12월
해킹바이러스 통계 및 분석 월보

2003년 12월

한국정보보호진흥원

Ⅰ. Overview

1. 12월 핫이슈 노트

쟁점사항요약	참조	구분
o 12월의 CERTCC-KR 신고접수 중 일반해킹과 스팸릴레이 관련 사고는 증가하였으나 일반 웜에 대한 사고는 감소 - 특히, 개인 사용자들을 대상으로 하는 일반해킹에 의한 피해가 많으므로 주의가 필요함 - 스팸릴레이 관련 사고도 여전히 발생하고 있으므로 이에 서버 관리자들의 스팸릴레이 여부 확인이 필요 o 사고 운영체제는 주로 Windows 계열(9X/NT/2000/XP) 피해가 많음 - 일반 사용자들이 보안이 강화된 유닉스시스템의 서버보다 보안이 취약한 윈도우제품을 많이 사용하므로 해커의 주 공격대상이 되고 있음 - 윈도우 사용자들의 윈도우 보안 업데이트와 취약점 패치가 필요하며, 개인 방화벽을 사용이 필요	본문 3 페이지, 6 페이지 7 페이지 참조	해킹
o 12월의 바이러스로 인한 피해건수, 신종 바이러스 건수 감소함 - 지난달에 이어 Dumaru 웜에 의한 피해가 지속적으로 발생 - PC 사용자들이 실제 메일과 패치관련 바이러스 메일을 구분하지 못하여 피해를 보고 있는 것으로 판단됨 - PC 사용자들의 바이러스 메일에 대한 정확한 구분과 함께 이에 대한 적절한 대응 방법 필요	본문 4 페이지, 8 페이지 참조	바이러스
o 국외(국내)로부터의 스캔탐지는 지난 11월보다 감소함 - 국내 공격자는 주로 네트워크 공유와 NetBIOS 관련 포트, 국외 공격자는 445번 포트에 대한 스캔이 많았음 - 이에 해당포트에 대한 스캔을 주시하고 불필요한 서비스는 사용하지 않는 것이 필요함 - 또한, 개인 PC의 보안을 위하여 개인 방화벽 제품 사용이 필요 됨 - Real Time Stream Protocol(554)에 대한 스캔공격이 증가하고 있음	본문 9 페이지 10 페이지 11 페이지 참조	스캔탐지

2. 전체 추이

□ 해킹사고 처리 및 대응

o **12**월의 CERTCC-KR 신고접수 특징은 일반해킹과 스팸릴레이 관련 사고는 증가하였으나 일반 웜에 대한 사고는 감소하였음
- 특히, 개인 사용자들의 일반해킹관련 사고가 많이 증가하였으며 이에 개인사용자들의 주의가 필요함

o Windows 계열(9X/NT/2000/XP) 피해가 주를 이룸
- 일반 사용자들의 타 운영체제에 비하여 보안 취약점이 많이 내재된 윈도우 운영체제를 많이 사용
- 해커들이 보안이 강화된 유닉스 등의 서버보단 보안이 취약한 윈도우를 주 공격대상으로 삼고 있음
- 윈도우 운영체제에 대한 사용자들의 취약점 패치와 윈도우 보안 업데이트 및 개인 방화벽 설치가 필요

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	946	1,027	1753	13,184
일반 웜	2,971	974	522	1,158	771	221	307	48	423	119	53	75	48	4,719
스팸릴레이	5,537	469	392	1,308	1,616	1,904	436	774	301	122	139	404	411	8,276
합계	15,192	2,563	1,826	3,400	3,310	3,137	1,819	1,813	2,035	1,420	1,138	1,506	2,212	26,179

※ 2002. 6월 스팸릴레이 6,851건 대응현황은 제외되었음.

※ 스팸릴레이는 CERTCC-KR 접수분과 홈페이지를 통한 원격점검시 문제서버로 판명된 서버(72개)들의 합

※ 2002년 동월 대비 일반해킹(618, 63% 증가), 일반 웜(451, 83% 감소), 스팸릴레이(591, 32% 감소)

□ 바이러스 신고건수 및 신종출현건수

o 12월 한달 간 총 10,157건 피해 접수됨
- Dumaru 웜에 의한 피해가 지속적으로 발생

o 신종 바이러스 4건 출현 (국산 0, 외산 2)
- 웜 2종 출현

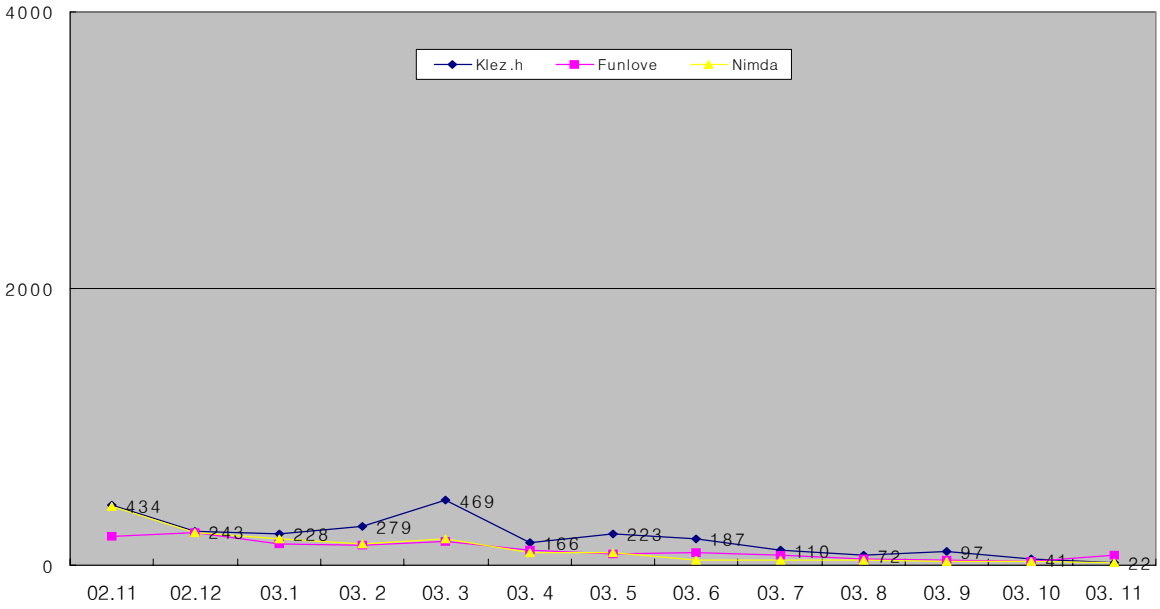
구분	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
신종출현건수	232	33	6	7	2	4	14	8	15	9	4	4	2	108
피해신고접수건수	38,677	3,757	3,238	3,797	3,180	4,612	3,522	2,550	11,039	20,681	5,453	13,037	10,157	85,023

※ KISA, 안철수, 하우리, 시만텍, 트랜드 공동집계

※ 바이러스 신고 건수 : 바이러스로 인하여 국내에서 피해가 발생한 건수

o 11월보다 클레즈변종과 펀러브 바이러스의 피해는 다소 증가하였으나, 님다 웜바이러스의 피해는 감소함

※ Klez.H(22건->25건), Nimda(14건->12건), Funlove(76건->122건)



o 12월 바이러스 피해신고 중 인터넷 웜이 8,949건으로 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	455	882	797	9,194
인터넷 웜	27,021	1,361	1,320	2,537	2,350	3,704	1,854	1,185	9,748	19,682	3,999	11,658	8,949	68,347
트로이목마	1,687	1,284	876	419	303	304	491	411	334	387	475	448	355	6,087
가짜(Hoax)	13	0	16	10	5	9	5	6	4	2	1	0	1	59
조크(Joke)	111	5	1	6	3	0	0	3	1	2	1	0	1	23
기타	537	11	50	42	52	59	248	20	120	86	522	49	54	1,313
합계	38,677	3,757	3,238	3,797	3,180	4,612	3,522	2,550	11,039	20,681	5,453	13,037	10,157	85,023

o 12월에 국내에서 발견된 신종바이러스는 총 2건이며 모두 인터넷웜임

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	0	0	0	6
인터넷 웜	108	26	2	5	2	3	7	1	9	7	2	3	2	69
트로이목마 (or 백도어)	60	4	4	1	0	0	5	5	6	2	2	1	0	30
가짜(Hoax)	0	0	0	0	0	0	0	0	0	0	0	0	0	0
조크(Joke)	0	0	0	1	0	0	0	0	0	0	0	0	0	1
기타	7	0	0	0	0	0	2	0	0	0	0	0	0	2
합계	232	33	6	7	2	4	14	8	15	9	4	4	2	108

※ 악성프로그램의 정의에 의한 분류임.

o 신종 바이러스 출처별로는 국산 0종, 외산 2종으로 외산이 주종을 이룸

구분	2002	2003												2003년
		1	2	3	4	5	6	7	8	9	10	11	12	
국산	23	2	0	0	0	0	0	0	2	1	1	0	0	6
외산	209	31	6	7	2	4	14	8	13	8	3	4	2	102
합계	232	33	6	7	2	4	14	8	15	9	4	4	2	108

□ 해킹시도탐지 건수 및 대응 현황

o 국외(국내)로부터의 스캔탐지는 지난 11월보다 감소함
- 국내 사용자의 경우는 135포트, 국외 사용자의 경우 445번 포트를 대상으로 한 스캔 비율이 가장 높음

o 네트워크 공유와 NetBIOS 관련 포트에 대한 해킹시도가 가장 많이 나타남
- 135/139/445포트에 대한 스캔현황을 주시하고 불필요한 서비스는 사용하지 않는 것이 필요함

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	3,560	2,201	315	14,966
대응건수	6,200	425	422	519	329	266	1,246	410	451	1,496	1,296	1,633	262	8,755

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

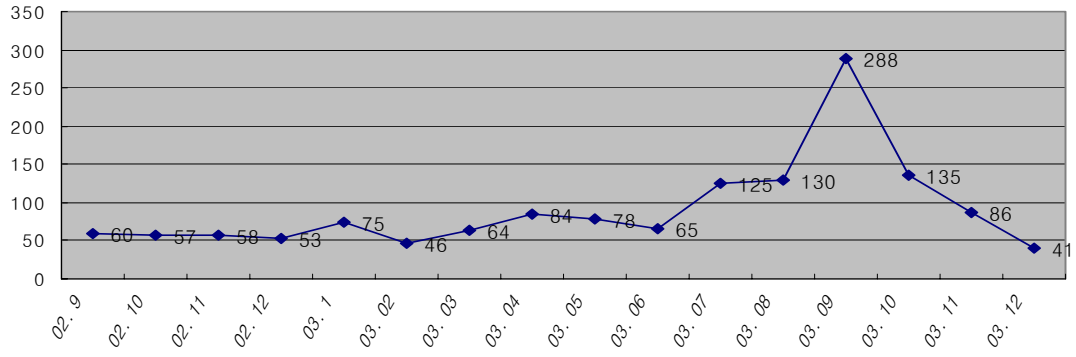
□ 일반상담 현황

o 12월 일반상담에는 기타 컴퓨터관련 문의가 40건, 타인 명예훼손이 1건 접수

- 기타 컴퓨터 관련 문의에는 원치 않는 광고창 문의 및 인터넷 익스플로러의 초기 화면이 특정사이트로 변조되어 수정되지 않는 문의가 대부분이었음
- 이외에 인터넷상의 사기, 게임아이템도난 등 사이버수사대 관련된 문의가 다수 있었음

※ 일반상담은 컴퓨터관련 문의와 타인명예훼손으로 구분

월	03.01	03.02	03.03	03.04	03.05	03.06	03.07	03.08	03.09	03.10	03.11	03.12	2003년 총계
건수	75	46	64	84	78	65	125	130	288	135	86	41	1,217



(2003년 일반상담현황)

Ⅱ. 세부분석

1. 12월 해킹 분석

o **2003년 12월 접수한 총 1,356건 중 분석 가능한 459건을 토대로 하여 작성**

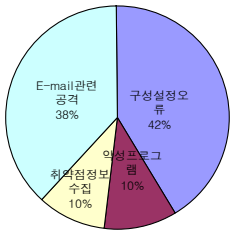
□ OS현황 (분석자료 기준)

o Windows 계열(9X/NT/2000/XP) 피해가 주를 이룸
- 일반 사용자들의 비교적 타 운영체제에 비하여 보안 취약점이 많이 내재된 윈도우 운영체제를 많이 사용
- 보안이 강화된 유닉스등의 서버보단 보안이 취약한 윈도우를 공격대상으로 삼고 있음
- 윈도우 운영체제에 대한 사용자들의 취약점 패치 및 윈도우 보안 업데이트 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	154	158	180	5,733
Win 95/98	2,098	458	405	366	564	347	370	129	126	65	76	91	44	3,041
Linux	574	29	74	62	53	33	21	20	11	3	10	4	3	323
Solaris	90	7	1	2	1	3	0	0	0	0	2	0	0	16
AIX	19	0	1	0	2	0	0	0	0	0	0	0	0	3
HP-UX	12	0	1	1	1	0	1	0	0	0	0	0	0	4
Digital Unix	6	0	1	0	0	1	0	0	0	0	0	0	0	2
DEC/IRIX	3	0	0	0	0	0	0	0	0	0	0	0	0	0
CISCO	2	0	0	0	0	0	0	0	0	0	0	0	0	0
N/A	1,361	278	180	476	859	901	165	166	82	46	78	246	232	3,709
합계	6,444	1,459	911	2,245	2,562	2,220	746	542	682	186	320	499	459	12,831

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

□ 공격수법별 구분 (분석자료 기준)



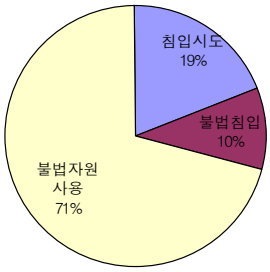
o 11월에 비해 감소하였으며, 스팸릴레이 사고와 관련 있는 E-mail과 구성설정오류를 이용한 공격수법이 가장 많았음

※ 좌측의 그래프는 12월의 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	1	0	4	46
S/W보안오류	602	130	34	893	452	92	14	0	3	1	1	0	0	1,620
버퍼오버플로우	243	445	28	28	43	42	47	42	392	25	19	30	19	1,160
구성설정오류	4,638	733	808	2,059	1,960	2,031	585	399	203	101	218	410	392	9,899
악성프로그램	4,112	1,148	557	1,232	934	306	450	185	544	119	137	129	96	5,837
프로토콜취약점	1	0	0	0	0	0	0	0	0	0	0	0	0	0
서비스거부	18	29	0	0	0	0	0	1	0	0	0	0	0	30
E-mail관련	1,943	258	346	1,018	1,617	1,905	289	353	137	63	181	370	363	6,900
취약점정보수집	3,971	703	535	1,219	930	303	440	171	175	113	129	124	95	4,937
사회공학	0	0	0	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	686	1,063	969	30,429

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

□ 침해유형에 따른 구분(분석자료 기준)



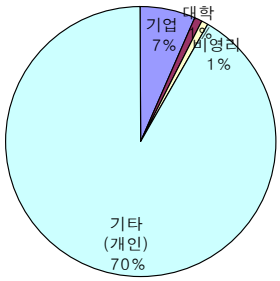
o 타 시스템의 불법자원 사용이 상대적으로 많음
o 11월에 비하여 12월에는 주요 불법행위가 감소

※ 좌측의 그래프는 12월의 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	130	124	98	4,936
불법침입	3,364	1,006	530	1,202	827	262	365	97	111	62	59	71	52	4,644
자료유출	1	0	0	0	0	0	0	0	0	0	0	0	0	0
자료변조삭제	61	1	1	1	3	1	5	5	1	1	3	0	0	22
불법자원사용	3,296	601	722	1,997	1,884	1,997	558	386	529	79	191	373	363	9,680
홈페이지변조	5	1	0	0	0	1	1	1	0	1	0	0	0	5
시스템파괴	0	0	0	0	0	0	1	0	0	0	0	0	0	1
시스템오류	2	0	0	0	1	0	0	0	0	0	0	0	0	1
서비스거부	11	29	0	0	0	0	0	1	0	0	0	0	0	30
총계	10,784	2,343	1,790	4,417	3,645	2,564	1,365	658	815	258	383	568	513	19,319

※ 한 사고내에 다수의 불법행위가 사용될 수 있음.

□ 기관별 구분(분석자료 기준)



o 기관별 전체 사고접수는 전월에 비해 증가하였으며, 특히 개인에 대한 사고접수가 증가

※ 좌측의 그래프는 12월의 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	56	36	31	2,416
대학	ac	716	142	71	108	155	79	44	27	55	4	6	10	4	705
비영리	or	154	31	11	24	22	17	6	5	2	0	4	0	4	126
연구소	re	22	3	2	2	3	3	0	0	1	0	0	0	0	14
네트워크	ne	4	6	2	2	0	10	12	0	0	0	0	0	0	32
기타(개인)		3,736	979	635	1,235	2,042	1,587	572	410	424	100	254	395	425	9,058
총계		6,444	1,459	911	2,271	2,525	1,950	735	546	605	124	320	441	464	12,351

※ ISP는 기타에 포함.

2. 바이러스(악성프로그램)

□ 12월중 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	41	22	25	1,869
Nimda.A	01.9	6,717	189	157	186	90	86	39	32	34	26	26	14	12	891
Funlove	02.9	4,413	153	145	174	110	78	87	69	41	38	30	76	122	1,123
Opaserv	02.10	2,332	365	173	300	172	126	89	86	62	83	66	61	50	1,633
Nimda.D	01.10	1,362	63	59	59	43	43	47	276	37	21	14	12	13	687
Winevar	02.11	944	20	35	6	4	2	1	2	7	2	1	0	0	80
Spida	02.5	568	5	57	7	0	1	2	1	0	1	0	0	2	76
Bride	02.11	438	4	0	12	0	3	0	0	0	0	0	0	0	19
mIRCPack	02.11	343	683	125	180	71	80	103	60	35	26	19	18	26	1,426
Sircam	02.71	270	8	6	4	4	1	5	4	1	2	0	0	1	36
Slammer	03.1	0	67	81	2	4	2	4	2	9	0	0	0	1	172
Blaster	03.8	0								5,792	1,005	738	625	560	8,720
Welchia	03.8	0								195	441	239	161	67	1,103
Sobig.F	03.8	0								2,296	15,255	589	183	1,277	19,600
Smibag	03.9	0									221	122	91	13	447
Swen	03.9	0									62	56	8	3	129
Dumaru	03.9	0									159	1416	9,280	6,211	17,066
Hotra	03.11	0											212	11	223

※ KISA, 안철수, 하우리, 시만텍, 트랜드 공동집계

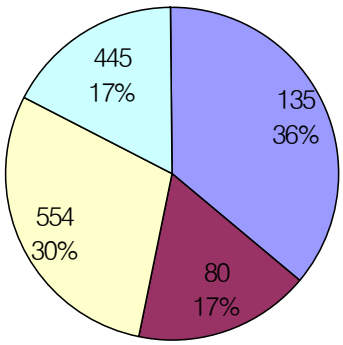
□ 12월중 Top10 악성프로그램 현황

순위	명칭	건수
1	Dumaru	6,211
2	Sobig.F	1,277
3	Blaster	560
4	Parite	439
5	Yaha	251
6	Agobot	180
7	Funlove	122
8	Valla	92
9	Welchia	67
10	Opaserv	50
	기타	908
계		10,157

3. 스캔탐지 현황

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

□ 국내 공격자가 행한 포트 스캔 현황



o 지난 11월보다 전체 스캔탐지 건수가 감소하였음

o 국내 사용자는 주로 네트워크 공유와 NetBIOS 관련 포트에 대한 스캔이 많았음.

o Real Time Stream Protocol(554)에 대한 스캔공격이 증가하고 있음

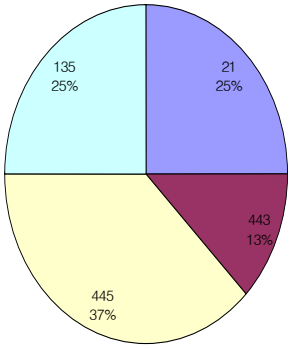
※ 좌측의 그래프는 12월의 Top 4 현황임

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	149	106	54	1,116
22	672	18	17	22	9	2	3	5	10	15	2	2	3	108
23	70	9	6	2	3	5	6	11	3	14	3	9	5	76
25	4,228	200	136	105	49	56	54	110	248	358	269	1	37	1,623
53	372	5	7	6	1	9	8	17	4	21	1	2	4	85
80	1,065	262	151	529	712	455	194	649	342	991	270	61	108	4,724
110	241	0	0	1	0	10	13	23	20	43	148	15	0	273
111	744	12	10	10	10	6	6	12	6	18	4	3	4	101
135	53	15	22	8	3	15	6	21	993	1,014	1,585	1,150	232	5,064
137	746	254	386	193	117	12	27	39	39	78	13	3	3	1,164
139	441	309	47	21	135	84	550	634	95	729	82	226	60	2,972
443	270	15	43	19	11	29	100	129	29	158	37	38	20	628
445	287	127	180	718	183	165	193	358	66	424	129	166	112	2,821
515	136	1	4	2	2	2	1	3	1	4	3	38	1	62
1433	2,452	150	100	92	78	38	40	78	33	111	30	3	29	782
1434	0	429	7	10	7	5	6	11	15	26	4	3	0	523
8080	36	1	0	0	0	0	2	2	3	5	1	6	1	21
12345	1,717	121	7	6	43	18	61	79	39	118	30	8	8	538
17300	16	0	61	4	44	118	228	346	32	378	27	15	24	1,277
554	0	0	0	0	0	0	0	0	0	0	9	176	190	375
901	0	0	0	0	0	0	0	0	0	0	21	16	35	72
27374	601	116	27	32	4	23	58	81	11	92	22	52	38	556
기타	4,123	53	148	139	17	141	324	465	336	801	307	237	184	3,152
합계	20,335	2,211	1,456	1,993	1,479	1,263	1,941	3,204	2,364	5,568	3,146	2,336	1,152	28,113

※ 본 항목은 CERTCC-KR 접수분과 RTSD 탐지분의 합임.

※ 기타는 3389, 500, 3128, 1080 포트 등

□ 국외 공격자가 국내로 가한 포트 스캔 현황



o 국외로부터의 스캔탐지는 지난 11월보다 감소
o 주로 445포트 스캔 비율이 가장 높음
※ 좌측의 그래프는 11월의 Top 3 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	72	71	2	599
22	696	6	6	12	4	3	9	1	2	5	4	0	0	52
23	109	2	4	2	3	1	0	0	2	0	1	0	0	15
25	514	13	8	6	7	10	14	2	28	14	48	0	0	150
53	179	0	3	4	2	6	2	1	0	15	0	1	0	34
80	6	0	0	684	1	7	3	1	15	14	0	0	0	725
110	44	0	2	0	0	2	0	0	0	92	1	0	0	97
111	764	3	0	1	0	0	1	0	1	2	4	3	0	15
135	6	1	0	1	0	1	12	0	7	1,048	3	6	2	1,081
139	83	0	0	2	1	2	68	2	5	10	7	0	0	97
443	151	8	13	13	2	1	3	2	1	3	13	10	1	70
445	50	4	26	34	13	13	116	1	0	30	14	10	3	264
515	228	0	0	0	0	0	1	0	8	0	0	0	0	9
1433	1,518	23	23	20	2	3	21	0	0	3	0	1	0	96
8080	3	0	0	0	0	0	0	2	0	3	1	0	0	6
12345	47	3	0	0	1	1	3	1	0	5	1	0	0	15
17300	0	0	11	2	7	8	12	0	0	0	37	1	0	78
27374	174	2	0	0	2	3	4	1	1	68	2	1	2	86
기타	1,143	42	28	49	24	57	218	50	77	124	61	77	0	807
합계	8,243	147	179	893	122	168	558	79	164	1,526	269	181	10	4,296

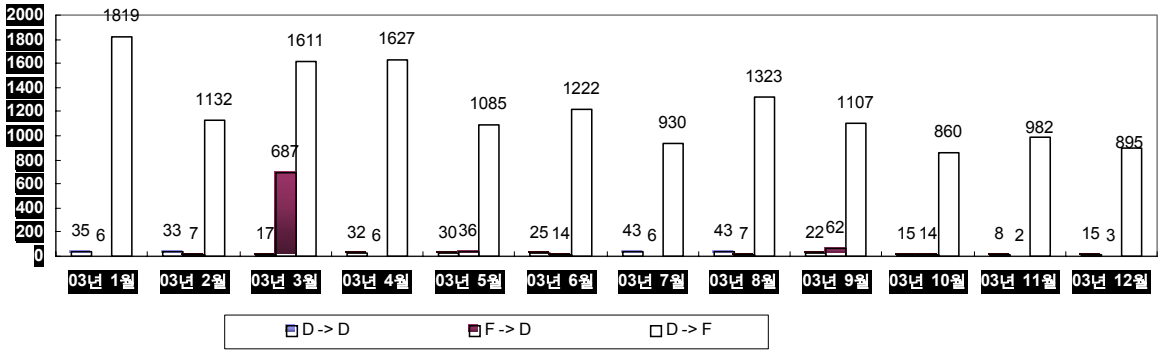
※ 본 항목은 CERT 접수분과 RTSD 탐지분의 합임.
※ 기타는 1080, 3128, 3389 포트 등

□ 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

□ 12월 포트 스캔 출발지·목적지의 특징

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

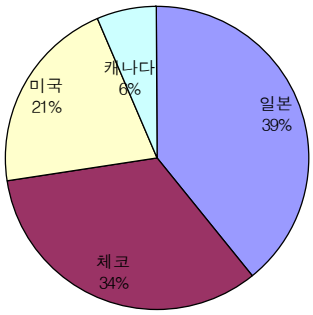


※ 위의 표는 신고접수 기준으로 한 자료임.(RTSD 탐지건수는 포함되지 않았음)

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

Ⅲ. 국가/지역별 분석

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



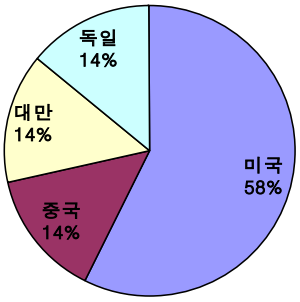
o 국내에 출발한 스캔공격의 대다수는 아시아와 아메리카, 유럽 대륙을 목표로 하고 있음.

※ 좌측의 그래프는 12월의 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	136	113	160	3,644
	브라질	68	46	15	7	5	6	50	21	8	29	21	8	10	226
	캐나다	173	63	73	31	47	31	33	25	29	16	48	30	49	475
	기타	189	0	0	0	10	0	18	4	30	17	47	0	15	141
	소계	2,530	720	727	479	463	284	517	255	290	201	252	151	234	4,573
아시아	대만	0	0	0	0	0	0	8	0	0	0	0	0	0	8
	일본	2,050	595	188	537	345	289	479	457	853	398	365	505	298	5,309
	중국	0	1	0	0	0	0	0	0	0	0	0	0	0	1
	이스라엘	418	102	21	241	578	369	8	51	41	0	0	0	0	1,411
	기타	43	2	1	1	36	2	41	29	32	132	33	21	15	345
	소계	2,511	700	210	779	959	660	536	537	926	530	398	526	313	7,074
아프리카	기타	1	0	0	0	0	0	1	0	0	50	0	33	0	84
	소계	1	0	0	0	0	0	1	1	0	50	0	33	0	85
오세아니아	뉴질랜드	20	1	2	10	9	1	24	11	0	0	0	0	0	58
	호주	407	21	5	1	9	5	10	8	9	7	11	6	4	96
	소계	427	22	7	11	18	6	34	19	9	7	11	6	4	154
유럽	네덜란드	7	10	3	30	1	0	0	0	1	1	9	1	0	56
	덴마크	7	1	0	0	3	1	0	1	0	0	0	0	1	7
	독일	349	29	12	11	3	1	0	1	0	0	0	1	0	58
	벨기에	5	0	1	0	0	0	0	0	0	5	0	0	0	6
	스웨덴	132	3	0	1	3	0	4	0	0	0	0	0	0	11
	체코	0	0	0	0	0	0	0	0	0	291	68	133	256	748
	스페인	5	3	32	0	0	1	0	0	0	0	1	0	0	37
	영국	34	3	4	10	8	17	11	4	11	25	18	12	21	144
	오스트리아	11	6	2	0	2	2	1	2	2	1	4	1	2	25
	프랑스	358	53	52	56	54	54	48	50	40	63	73	85	43	671
	기타	154	111	66	4	90	2	24	46	36	3	80	22	18	502
	소계	1,062	219	172	112	164	78	92	114	89	210	253	255	341	2,099
총계		6,531	1,661	1,116	1,381	1,604	1,028	1,180	926	1,314	998	914	971	892	13,985

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

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



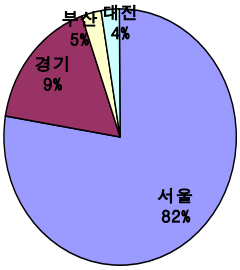
o 12월 국외 스캔공격은 11월보다 감소하였으며,
o 중국과 미국으로부터의 스캔시도가 많았음

※ 좌측의 그래프는 12월의 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	83	43	4	531
	브라질	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	캐나다	1	5	11	5	4	2	6	0	0	0	16	12	1	62
	기타	9	0	18	8	3	8	0	2	1	2	2	0	0	44
	소계	14	48	110	54	29	54	117	11	42	11	101	55	5	637
아시아	대만	48	5	53	21	6	7	44	0	4	8	22	9	1	180
	일본	24	3	11	10	2	1	21	1	4	1	4	3	0	61
	중국	98	13	66	40	30	41	163	41	94	21	63	54	1	627
	이스라엘	10	0	5	4	0	1	9	2	0	0	2	0	0	23
	기타	51	5	10	8	7	8	23	6	8	6	13	14	0	108
	소계	231	26	145	83	45	58	260	50	110	36	104	80	2	999
아프리카	기타	2	0	0	0	0	1	1	0	0	0	0	0	0	2
	소계	2	0	0	0	0	1	1	0	0	0	0	0	0	2
오세아니아	뉴질랜드	0	0	0	0	0	0	1	0	0	0	0	0	0	1
	호주	7	46	39	19	1	1	1	0	3	1	4	1	0	116
	소계	7	46	39	19	1	1	2	0	3	1	4	1	0	117
유럽	네덜란드	13	4	12	11	5	12	102	1	4	0	3	0	0	154
	덴마크	2	0	0	0	1	3	0	0	0	0	1	0	0	5
	독일	85	11	31	16	10	9	17	2	0	0	7	5	1	109
	벨기에	13	1	5	2	1	0	3	0	0	0	0	2	0	14
	스웨덴	8	0	1	0	0	2	2	0	0	0	1	0	0	6
	스위스	6	1	0	0	1	0	0	0	0	0	0	0	0	2
	스페인	3	0	2	2	0	2	2	0	0	0	2	0	0	10
	영국	0	0	6	2	3	4	6	1	0	0	4	2	0	28
	오스트리아	5	1	1	0	0	0	0	0	0	0	1	1	0	4
	프랑스	52	5	11	4	10	7	25	3	2	0	6	5	0	78
	기타	27	3	21	12	17	9	15	13	7	2	24	11	2	136
	소계	214	26	90	49	48	48	172	20	13	2	37	26	3	534
총계		468	146	384	205	123	162	552	81	168	50	246	162	10	2,289

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

□ 지역별(국내) 스캔 Source 현황(whois 정보 기준)



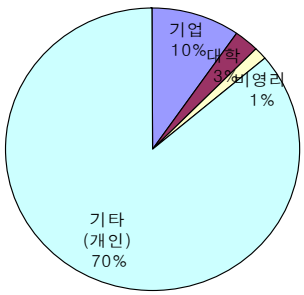
o 금월, 지역별 구분에서는 이전의 경향과 같이 서울에서 발생한 스캔이 가장 많음.

※ 좌측의 그래프는 12월의 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	719	1,075	929	588	10,960
부산	384	66	41	44	27	17	25	39	43	51	58	43	21	475
대구	191	21	29	21	23	20	6	10	12	0	5	16	10	173
인천	105	16	16	18	17	14	7	12	13	9	33	31	2	188
광주	108	16	2	11	10	4	10	7	6	30	1	3	0	100
대전	180	70	36	49	53	43	46	30	70	47	74	56	20	594
울산	56	12	5	15	8	2	2	0	2	0	3	3	0	52
경기	825	143	84	126	90	92	133	79	115	79	675	432	129	2,177
강원	140	11	11	24	6	4	11	3	29	57	7	10	6	179
충북	249	10	11	21	5	5	11	3	11	0	6	6	6	95
충남	106	34	14	7	10	5	7	4	12	14	23	10	1	141
전북	116	20	16	139	99	34	58	8	23	0	15	27	5	444
전남	141	79	52	11	6	7	8	3	5	1	8	5	1	186
경북	122	20	12	19	17	20	5	5	7	0	2	27	6	140
경남	143	9	13	14	10	9	21	25	31	11	24	14	3	184
제주	30	2	3	4	4	3	4	0	1	1	1	2	1	26
N/A	1,565	656	317	397	317	226	397	417	389	432	142	817	249	4,756
총계	9,623	2,211	1,454	2,038	1,787	1,263	1,938	1,348	1,748	1,451	2,152	2,431	1,048	20,870

※ RTSD 추출정보는 2002년 10월 이후 추가되었음

□ 기관별(국내) 스캔 Source 현황(whois 정보 기준)



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

※ 좌측의 그래프는 12월의 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	125	138	88	2,096
대학	ac	815	171	75	155	127	90	68	61	140	90	64	39	25	1,105
비영리	or	99	34	27	33	18	15	15	10	24	10	5	11	11	213
연구소	re	20	4	5	3	2	0	0	4	3	1	0	0	2	24
네트워크	ne	9	7	2	2	1	14	27	0	0	0	0	0	0	53
기타(개인)		3,917	1,207	809	1,148	1,237	812	944	765	978	775	663	789	773	10,900
총계		6,494	1,712	1,124	1,569	1,621	1,090	1,195	965	1,354	1,028	857	977	899	14,391