통계 · 분석보고서

2003년 10월
해킹바이러스 통계 및 분석 월보

2003년 10월

한국정보보호진흥원

Ⅰ. Overview

1. 10월 핫이슈 노트

쟁점사항요약	참조	구분
o 10월의 CERTCC-KR 신고접수 특징은 일반해킹 사고와 웜에 대한 사고접수는 감소한 반면에 스팸릴레이 관련 사고는 증가하였음 - MS RPC 취약점을 이용하는 Welchia와 그 외 웜들이 아직도 국내 이용자들에게서 발생하고 있으므로 국내 Windows NT/2000/XP 사용자들은 마이크로소프트사에서 제공하는 패치를 필히 설치를 권고 o Windows NT/2000/XP 계열의 피해가 타 운영체제에 비해 보다 높게 나타남 - NT 계열의 MS 취약점에 의한 사고가 여전히 발생하고 있는 것이 주요 원인인 것으로 파악 - Windows 사용자들의 취약점 패치 및 Null 패스워드 사용 점검이 필요 o 그 외 Real-Time Streaming Protocol(554)와 smpnameres(901)에 대한 새로운 사고가 접수되고 있음 o 악성프로그램 및 불법침입은 9월에 비해 증가	본문 3 페이지, 6 페이지 7 페이지 참조	해킹
o 10월의 바이러스로 인한 피해건수와 신종바이러스 출현건수 감소함 o 10월의 바이러스 피해의 특징은 Blaster, Welchia, Sobig.F에 의한 피해는 감소한 반면에 Dumaru 웜으로 인한 피해는 증가하였음. - Dumaru의 웜의 피해가 증가한 이유는 최근 주로 윈도우 취약점을 이용한 웜이 많이 등장으로 이에 대한 보안 패치 점검 필요성을 강조 한다는 것을 바이러스 제작자가 이를 악용 - 마치 마이크로소프트에서 보내온 보안 패치 관련 메일처럼 위장하여 웜을 전파함으로써 많은 사용자들이 피해를 본 것으로 판단됨	본문 4 페이지, 8 페이지 참조	바이러스
o 지난 9월보다 전체 스캔탐지 건수가 감소하였으나 상대적으로 135(RPC)포트 스캔 증가 - MS Blaster에 의한 공격이 아직 국내에 많이 유입되고 있음 o 그 외 Real-Time Streaming Protocol(554)와 smpnameres(901)에 대한 스캔공격이 발생하고 있음 o 국외로부터의 스캔탐지는 지난 9월보다 많이 감소(1529->269) 현상을 보임 o 주로 Telnet 25번 포트 스캔 비율이 가장 높음	본문 9 페이지 10 페이지 11 페이지 참조	스캔탐지

2. 전체 추이

□ 해킹사고 처리 및 대응

o **10**월의 CERTCC-KR 신고접수 특징은 일반해킹 사고와 웜에 대한 사고접수는 감소한 반면에 스팸릴레이 관련 사고는 증가하였음

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

o MS RPC(135 포트)에 대한 스캔이 상대적으로 많은 현상을 보이는 것은 Welchia 웜이 아직도 국내 사용자들에게 전파되고 있음을 보여줌

o 지난 9월보다 전체 스캔탐지 건수가 감소하였으나 상대적으로 135(RPC)포트 스캔 증가
- MS Welchia에 의한 공격이 아직 국내에 많이 유입되는 것으로 판단

o 그 외 Real-Time Streaming Protocol(554)와 smpnameres(901)에 대한 새로운 스캔공격이 발생하고 있으므로 주의가 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			10,404
일반 웜	2,971	974	522	1,158	771	221	307	48	423	119	53			4,596
스팸릴레이	5,537	469	392	1,308	1,616	1,904	436	774	301	122	139			7,461
합계	15,192	2,563	1,826	3,400	3,310	3,137	1,819	1,813	2,035	1,420	1,138			22,461

※ 2002. 6월 스팸릴레이 6,851건 대응현황은 제외되었음.

※ 스팸릴레이는 CERTCC-KR 접수분과 홈페이지를 통한 원격점검시 문제서버로 판명된 서버(53개)들의 합.

※ 2002년 동월 대비 일반해킹(606, 56% 증가), 일반 웜(433, 88% 감소), 스팸릴레이(462, 70% 감소)

□ 바이러스 신고건수 및 신종출현건수

o 10월 한달 간 총 5,453건 피해 접수됨
전월보다 많이 감소하였지만 상반기 평균수준피해(월 3684건) 보다 높은 수치임

o 신종 바이러스 4건 출현 (국산 1, 외산 3)
- 웜 2종, 트로이목마 2종 출현

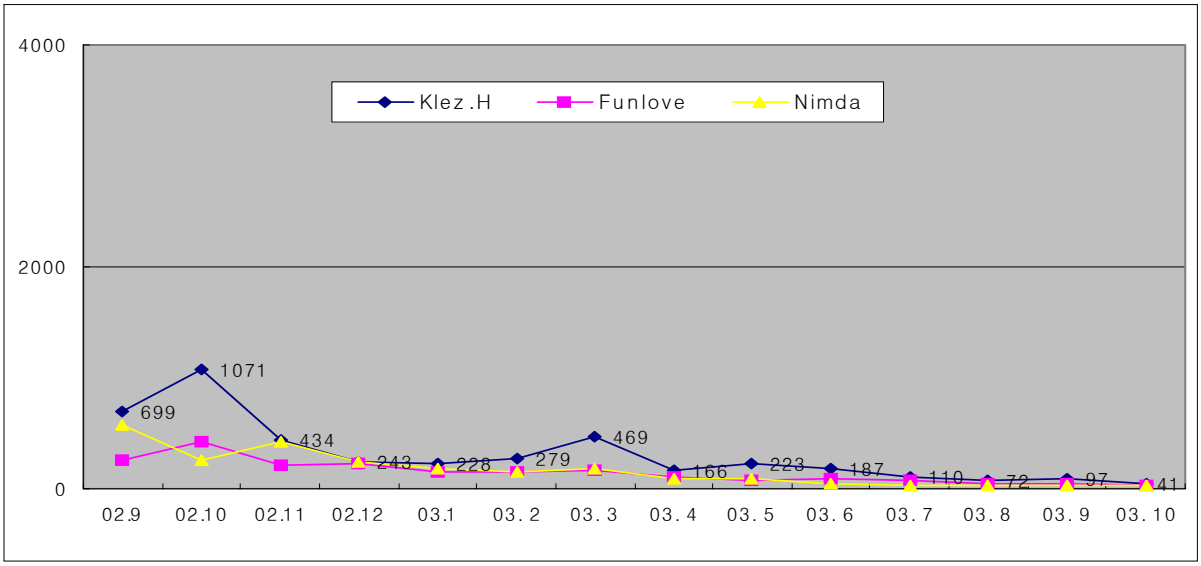
구분	2002	2003												2003년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
신종출현건수	232	33	6	7	2	4	14	8	15	9	4			102
피해신고접수건수	38,677	3,757	3,238	3,797	3,180	4,612	3,522	2,550	11,039	20,681	5,453			61,829

※ KISA, 안철수, 하우리, 시만텍, 트랜드 공동집계

※ 바이러스 신고 건수 : 바이러스로 인하여 국내에서 피해가 발생한 건수

o 9월보다 클레즈변종, 펀러브 등 악성바이러스의 피해는 다소 감소함.

※ Klez.H(97건->41건), Funlove(38건->31건), Nimda(26건->26건)



o 10월 바이러스 피해신고 중 인터넷 웜이 3,999건으로 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			7,515
인터넷 웜	27,021	1,361	1,320	2,537	2,350	3,704	1,854	1,185	9,748	19,682	3,999			47,740
트로이목마 (or 백도어)	1,687	1,284	876	419	303	304	491	411	334	387	475			5,284
가짜(Hoax)	13	0	16	10	5	9	5	6	4	2	1			58
조크(Joke)	111	5	1	6	3	0	0	3	1	2	1			22
기타	537	11	50	42	52	59	248	20	120	86	522			1,210
합계	38,677	3,757	3,238	3,797	3,180	4,612	3,522	2,550	11,039	20,681	5,453			61,829

o 10월에 국내에서 발견된 신종바이러스는 총 4건으로 인터넷 웜 2종, 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	0			6
인터넷 웜	108	26	2	5	2	3	7	1	9	7	2			64
트로이목마 (or 백도어)	60	4	4	1	0	0	5	5	6	2	2			29
가짜(Hoax)	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			1
기타	7	0	0	0	0	0	2	0	0	0	0			2
합계	232	33	6	7	2	4	14	8	15	9	4			102

※ 악성프로그램의 정의에 의한 분류임.

o 신종 바이러스 출처별로는 국산 1종, 외산 3종으로 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	1			6
외산	209	31	6	7	2	4	14	8	13	8	3			96
합계	232	33	6	7	2	4	14	8	15	9	4			102

□ 해킹시도탐지 건수 및 대응 현황

o 10월보다 전체 스캔탐지 건수가 증가하였음

o MS RPC(135)에 대한 스캔이 상대적으로 많음

- 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	3,560			12,450
대응건수	6,200	425	422	519	329	266	1,246	410	451	1,496	1,296			6,860

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

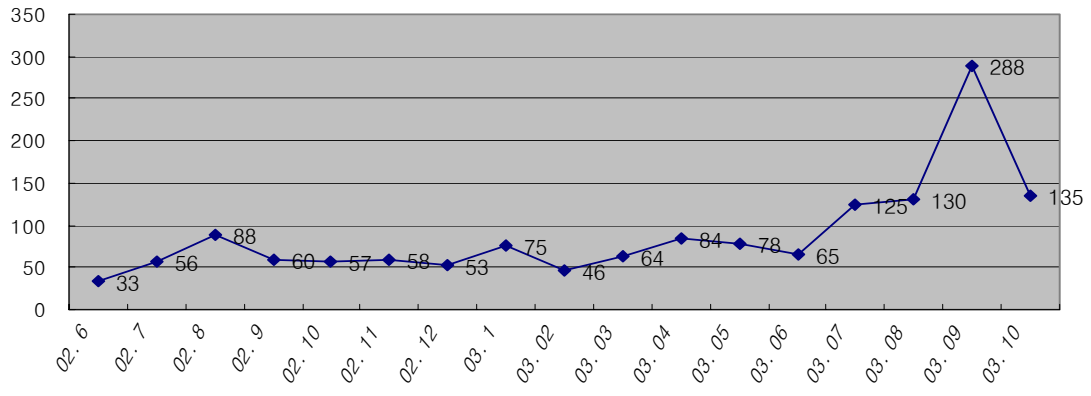
□ 일반상담 현황

o 10월 일반상담에는 기타 컴퓨터관련 문의가 127건, 타인 명예훼손이 8건 접수

- 기타 컴퓨터 관련 문의에는 윈도우 업데이트 및 패치방법에 대한 문의 및 인터넷 익스플로러의 초기화면이 특정사이트로 변조되어 수정되지 않거나 개인정보도용 등의 증상 관련 문의
- 악성 스크립트를 이용한 초기화면 및 특정사이트 접속유도 문의가 상당히 많았음

※ 일반상담은 컴퓨터관련 문의와 타인명예훼손으로 구분

월	02.11	02.12	03.01	03.02	03.03	03.04	03.05	03.06	03.07	03.08	03.09	03.10	2003년 총계
건수	58	53	75	46	64	84	78	65	125	130	288	135	1,090



(2003년 일반상담현황)

Ⅱ. 세부분석

1. 10월 해킹 분석

o **2003년 10월 접수한 총 1,180건 중 분석 가능한 320건을 토대로 하여 작성**

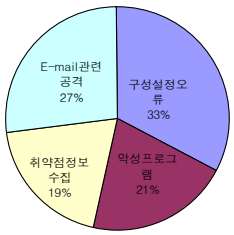
□ OS현황 (분석자료 기준)

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	154			5,395
Win 95/98	2,098	458	405	366	564	347	370	129	126	65	76			2,906
Linux	574	29	74	62	53	33	21	20	11	3	10			316
Solaris	90	7	1	2	1	3	0	0	0	0	2			16
AIX	19	0	1	0	2	0	0	0	0	0	0			3
HP-UX	12	0	1	1	1	0	1	0	0	0	0			4
Digital Unix	6	0	1	0	0	1	0	0	0	0	0			2
DEC/IRIX	3	0	0	0	0	0	0	0	0	0	0			0
CISCO	2	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			3,231
합계	6,444	1,459	911	2,245	2,562	2,220	746	542	682	186	320			11,873

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

□ 공격수법별 구분 (분석자료 기준)



o 전체적으로 9월에 비해 증가하였으며, MS Blaster와 Welchia 웜으로 인한 취약점 정보수집과 관련한 사고는 비슷한 수준을 나타내고 있음.

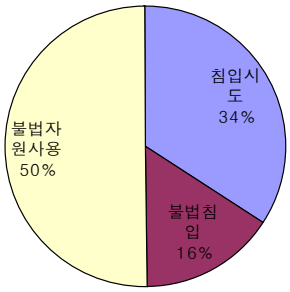
o 9월에 비해 스팸릴레이 사고가 증가하였음

※ 좌측의 그래프는 10월의 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			42
S/W보안오류	602	130	34	893	452	92	14	0	3	1	1			1,620
버퍼오버플로우	243	445	28	28	43	42	47	42	392	25	19			1,111
구성설정오류	4,638	733	808	2,059	1,960	2,031	585	399	203	101	218			9,097
악성프로그램	4,112	1,148	557	1,232	934	306	450	185	544	119	137			5,612
프로토콜취약점	1	0	0	0	0	0	0	0	0	0	0			0
서비스거부	18	29	0	0	0	0	0	1	0	0	0			30
E-mail관련	1,943	258	346	1,018	1,617	1,905	289	353	137	63	181			6,167
취약점정보수집	3,971	703	535	1,219	930	303	440	171	175	113	129			4,718
사회공학	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			28,397

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

□ 침해유형에 따른 구분(분석자료 기준)



o 타 시스템의 불법자원 사용 증가

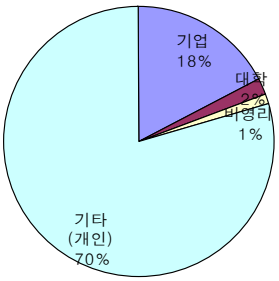
o 침입시도 및 불법침입 또한 9월과 비슷한 현상

※ 좌측의 그래프는 10월의 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			4,714
불법침입	3,364	1,006	530	1,202	827	262	365	97	111	62	59			4,521
자료유출	1	0	0	0	0	0	0	0	0	0	0			0
자료변조삭제	61	1	1	1	3	1	5	5	1	1	3			22
불법자원사용	3,296	601	722	1,997	1,884	1,997	558	386	529	79	191			8,944
홈페이지변조	5	1	0	0	0	1	1	1	0	1	0			5
시스템파괴	0	0	0	0	0	0	1	0	0	0	0			1
시스템오류	2	0	0	0	1	0	0	0	0	0	0			1
서비스거부	11	29	0	0	0	0	0	1	0	0	0			30
총계	10,784	2,343	1,790	4,417	3,645	2,564	1,365	658	815	258	383			18,238

※ 한 사고내에 다수의 불법행위가 사용될 수 있음.

□ 기관별 구분(분석자료 기준)



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

- 윈도우 계열 공격이 타 운영체제에 비하여 많으므로 개인들의 피해가 상대적으로 높은 편임

※ 좌측의 그래프는 10월의 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			2,349
대학	ac	716	142	71	108	155	79	44	27	55	4	6			691
비영리	or	154	31	11	24	22	17	6	5	2	0	4			122
연구소	re	22	3	2	2	3	3	0	0	1	0	0			14
네트워크	ne	4	6	2	2	0	10	12	0	0	0	0			32
기타(개인)		3,736	979	635	1,235	2,042	1,587	572	410	424	100	254			8,238
총계		6,444	1,459	911	2,271	2,525	1,950	735	546	605	124	320			###

※ ISP는 기타에 포함.

2. 바이러스(악성프로그램)

□ 10월중 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			1,822
Nmda.A	01.9	6,717	189	157	186	90	86	39	32	34	26	26			865
Funlove4099		4,413	153	145	174	110	78	87	69	41	38	30			925
Opaserv	02.10	2,332	365	173	300	172	126	89	86	62	83	66			1,522
Nmda.D		1,362	63	59	59	43	43	47	276	37	21	14			662
Winevar	02.11	944	20	35	6	4	2	1	2	7	2	1			80
Spida		568	5	57	7	0	1	2	1	0	1	0			74
Bride	02.11	438	4	0	12	0	3	0	0	0	0	0			19
mIRCPack	02.11	343	663	125	180	71	80	103	60	35	26	19			1,382
Sircam		270	8	6	4	4	1	5	4	1	2	0			35
Slammer	03.1	0	67	81	2	4	2	4	2	9	0	0			171
Blaster	03.8	0								5,792	1,005	738			7,535
Welchia	03.8	0								195	441	239			875
Sobig.F	03.8	0								2,296	15,255	589			18,140
Smibag	03.9	0									221	122			343
Swen	03.9	0									62	56			118
Dumaru	03.9	0									159	1416			1,575

※ KISA, 안철수, 하우리, 시만텍, 트랜드 공동집계

□ 10월중 Top10 악성프로그램 현황

순위	명칭	건수
1	Dumaru	1,416
2	Blaster	738
3	Sobig.F	589
4	Welchia	239
5	Yaha	209
6	Parite	150
7	Smibag	134
8	Rtkit	120
9	Valla	83
10	Opaserv	66
	기타	1,709
계		5,453

□ 10월의 신종바이러스 경보 발령

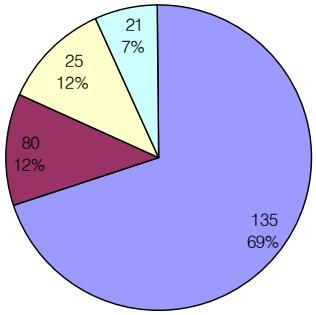
	구분	바이러스명	등급	발령일	참고사이트
1	주의	W32/Sober@mm	C	10.30	http://www.certcc.or.kr/cvirc/Alert/warning/2003/Sober@mm.html

※ 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 10월보다 전체 스캔탐지 건수가 감소하였음

o MS RPC(135)에 대한 스캔은 상대적으로 증가

- MS Blaster에 의한 공격이 지속적으로 발생하는 것으로 보임

o 그 외 Real Time Stream Protocol(554)와 smpnameres(901)에 대한 새로운 스캔공격이 발생하고 있음

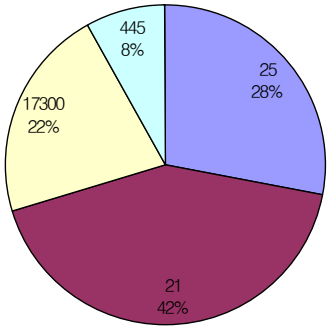
※ 좌측의 그래프는 10월의 Top 4 현황임

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			956
22	672	18	17	22	9	2	3	5	10	15	2			103
23	70	9	6	2	3	5	6	11	3	14	3			62
25	4,228	200	136	105	49	56	54	110	248	358	269			1,585
53	372	5	7	6	1	9	8	17	4	21	1			79
80	1,065	262	151	529	712	455	194	649	342	991	270			4,555
110	241	0	0	1	0	10	13	23	20	43	148			258
111	744	12	10	10	10	6	6	12	6	18	4			94
135	53	15	22	8	3	15	6	21	993	1,014	1,585			3,682
137	746	254	386	193	117	12	27	39	39	78	13			1,158
139	441	309	47	21	135	84	550	634	95	729	82			2,686
443	270	15	43	19	11	29	100	129	29	158	37			570
445	287	127	180	718	183	165	193	358	66	424	129			2,543
515	136	1	4	2	2	2	1	3	1	4	3			23
1433	2,452	150	100	92	78	38	40	78	33	111	30			750
1434	0	429	7	10	7	5	6	11	15	26	4			520
8080	36	1	0	0	0	0	2	2	3	5	1			14
12345	1,717	121	7	6	43	18	61	79	39	118	30			522
17300	16	0	61	4	44	118	228	346	32	378	27			1,238
554	0	0	0	0	0	0	0	0	0	0	9			9
901	0	0	0	0	0	0	0	0	0	0	21			21
27374	601	116	27	32	4	23	58	81	11	92	22			466
기타	4,123	53	148	139	17	141	324	465	336	801	307			2,731
합계	20,335	2,211	1,456	1,993	1,479	1,263	1,941	3,204	2,364	5,568	3,146			24,625

※ 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 9월보다 대폭 감소(1,529 -> 269) 현상을 보임

o 주로 메일서버 25번 포트 스캔 비율이 가장 높음

※ 좌측의 그래프는 10월의 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	72			526
22	696	6	6	12	4	3	9	1	2	5	4			52
23	109	2	4	2	3	1	0	0	2	0	1			15
25	514	13	8	6	7	10	14	2	28	14	48			150
53	179	0	3	4	2	6	2	1	0	15	0			33
80	6	0	0	684	1	7	3	1	15	14	0			725
110	44	0	2	0	0	2	0	0	0	92	1			97
111	764	3	0	1	0	0	1	0	1	2	4			12
135	6	1	0	1	0	1	12	0	7	1,047	3			1,072
139	83	0	0	2	1	2	68	2	5	10	7			97
443	151	8	13	13	2	1	3	2	1	3	13			59
445	50	4	26	34	13	13	116	1	0	30	14			251
515	228	0	0	0	0	0	1	0	8	0	0			9
1433	1,518	23	23	20	2	3	21	0	0	3	0			95
8080	3	0	0	0	0	0	0	2	0	3	1			6
12345	47	3	0	0	1	1	3	1	0	5	1			15
17300	0	0	11	2	7	8	12	0	0	0	37			77
27374	174	2	0	0	2	3	4	1	1	68	2			83
기타	1,143	42	28	49	24	57	218	50	77	120	61			726
합계	8,243	147	179	893	122	168	558	79	164	1,529	269			4,100

※ 본 항목은 CERT 접수분과 RTSD 탐지분의 합임.

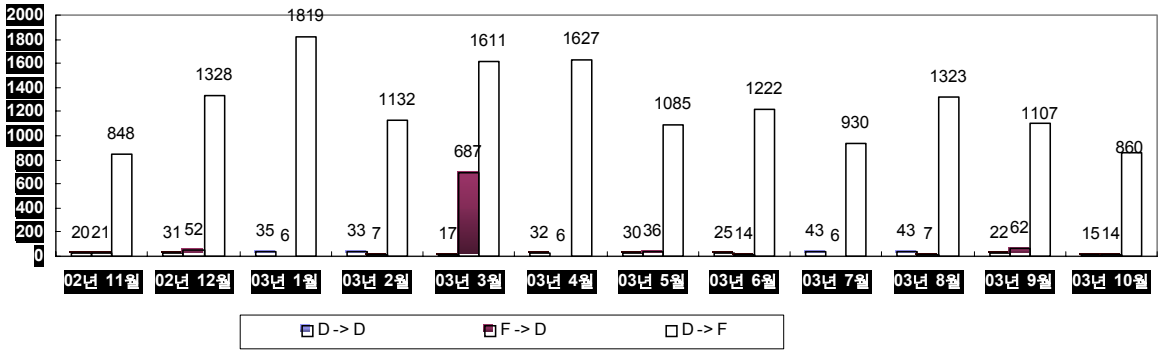
※ 기타는 1080, 3128, 3389 포트 등

□ 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

□ 10월 포트 스캔 출발지·목적지의 특징

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

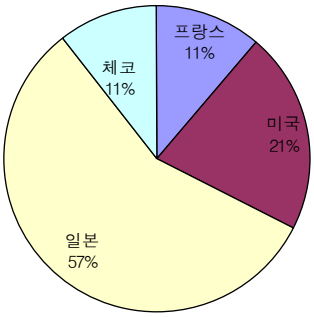


※ 위의 표는 신고접수 기준으로 한 자료임.(RTSD 탐지건수는 포함되지 않았음)

※ 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.

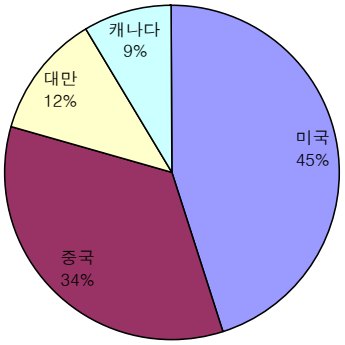
o 체코에 대한 스캔이 9월보다는 감소하였지만 꾸준히 발생하였음

※ 좌측의 그래프는 10월의 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			3,371
	브라질	68	46	15	7	5	6	50	21	8	29	21			208
	캐나다	173	63	73	31	47	31	33	25	29	16	48			396
	기타	189	0	0	0	10	0	18	4	30	17	47			126
	소계	2,530	720	727	479	463	284	517	255	290	201	262			4,198
아시아	대만	0	0	0	0	0	0	8	0	0	0	0			8
	일본	2,050	595	188	537	345	289	479	457	853	398	365			4,506
	중국	0	1	0	0	0	0	0	0	0	0	0			1
	이스라엘	418	102	21	241	578	369	8	51	41	0	0			1,411
	기타	43	2	1	1	36	2	41	29	32	132	33			309
	소계	2,511	700	210	779	959	660	536	537	926	530	398			6,235
아프리카	기타	1	0	0	0	0	0	1	0	0	50	0			51
	소계	1	0	0	0	0	0	1	1	0	50	0			52
오세아니아	뉴질랜드	20	1	2	10	9	1	24	11	0	0	0			58
	호주	407	21	5	1	9	5	10	8	9	7	11			86
	소계	427	22	7	11	18	6	34	19	9	7	11			144
유럽	네덜란드	7	10	3	30	1	0	0	0	1	1	9			55
	덴마크	7	1	0	0	3	1	0	1	0	0	0			6
	독일	349	29	12	11	3	1	0	1	0	0	0			57
	벨기에	5	0	1	0	0	0	0	0	0	5	0			6
	스웨덴	132	3	0	1	3	0	4	0	0	0	0			11
	체코	0	0	0	0	0	0	0	0	0	291	68			359
	스페인	5	3	32	0	0	1	0	0	0	0	1			37
	영국	34	3	4	10	8	17	11	4	11	25	18			111
	오스트리아	11	6	2	0	2	2	1	2	2	1	4			22
	프랑스	358	53	52	56	54	54	48	50	40	63	73			543
	기타	154	111	66	4	90	2	24	46	36	3	80			462
	소계	1,062	219	172	112	164	78	92	114	89	210	176			1,426
총계		6,531	1,661	1,116	1,381	1,604	1,028	1,180	926	1,314	998	847			12,055

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

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



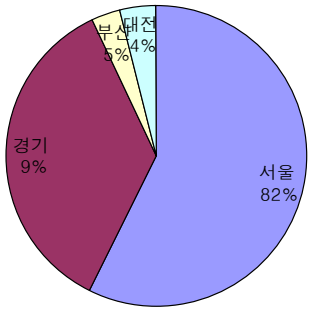
o 10월 국외 스캔공격은 9월보다 5배정도 증가하였으며, 그 가운데 미국, 중국으로부터 스캔시도가 많은 것을 알 수 있음

※ 좌측의 그래프는 10월의 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
	브라질	0	0	0	0	0	0	0	0	0	0	0			0
	캐나다	1	5	11	5	4	2	6	0	0	0	16			5
	기타	9	0	18	8	3	8	0	2	1	2	2			0
	소계	14	48	110	54	29	54	117	11	42	11	101			577
아시아	대만	48	5	53	21	6	7	44	0	4	8	22			170
	일본	24	3	11	10	2	1	21	1	4	1	4			58
	중국	98	13	66	40	30	41	163	41	94	21	63			572
	이스라엘	10	0	5	4	0	1	9	2	0	0	2			23
	기타	51	5	10	8	7	8	23	6	8	6	13			94
	소계	231	26	145	83	45	58	260	50	110	36	104			917
아프리카	기타	2	0	0	0	0	1	1	0	0	0	0			2
	소계	2	0	0	0	0	1	1	0	0	0	0			2
오세아니아	뉴질랜드	0	0	0	0	0	0	1	0	0	0	0			1
	호주	7	46	39	19	1	1	1	0	3	1	4			115
	소계	7	46	39	19	1	1	2	0	3	1	4			116
유럽	네덜란드	13	4	12	11	5	12	102	1	4	0	3			154
	덴마크	2	0	0	0	1	3	0	0	0	0	1			5
	독일	85	11	31	16	10	9	17	2	0	0	7			103
	벨기에	13	1	5	2	1	0	3	0	0	0	0			12
	스웨덴	8	0	1	0	0	2	2	0	0	0	1			6
	스위스	6	1	0	0	1	0	0	0	0	0	0			2
	스페인	3	0	2	2	0	2	2	0	0	0	2			10
	영국	0	0	6	2	3	4	6	1	0	0	4			26
	오스트리아	5	1	1	0	0	0	0	0	0	0	1			3
	프랑스	52	5	11	4	10	7	25	3	2	0	6			73
	기타	27	3	21	12	17	9	15	13	7	2	24			123
	소계	214	26	90	49	48	48	172	20	13	2	37			505
총계		468	146	384	205	123	162	552	81	168	50	246			2,117

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

□ 지역별(국내) 스캔 Source 현황(whois 정보 기준)



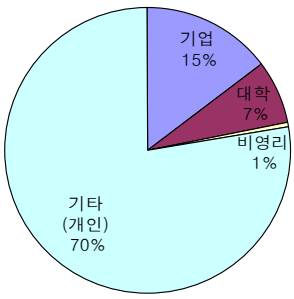
o 금월, 지역별 구분에서는 이전의 경향과 같이 서울에서 발생한 스캔이 가장 많음.

※ 좌측의 그래프는 10월의 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			9,443
부산	384	66	41	44	27	17	25	39	43	51	58			411
대구	191	21	29	21	23	20	6	10	12	0	5			147
인천	105	16	16	18	17	14	7	12	13	9	33			155
광주	108	16	2	11	10	4	10	7	6	30	1			97
대전	180	70	36	49	53	43	46	30	70	47	74			518
울산	56	12	5	15	8	2	2	0	2	0	3			49
경기	825	143	84	126	90	92	133	79	115	79	675			1,616
강원	140	11	11	24	6	4	11	3	29	57	7			163
충북	249	10	11	21	5	5	11	3	11	0	6			83
충남	106	34	14	7	10	5	7	4	12	14	23			130
전북	116	20	16	139	99	34	58	8	23	0	15			412
전남	141	79	52	11	6	7	8	3	5	1	8			180
경북	122	20	12	19	17	20	5	5	7	0	2			107
경남	143	9	13	14	10	9	21	25	31	11	24			167
제주	30	2	3	4	4	3	4	0	1	1	1			23
N/A	1,565	656	317	397	317	226	397	417	389	432	142			3,690
총계	9,623	2,211	1,454	2,038	1,787	1,263	1,938	1,348	1,748	1,451	2,152			17,391

※ 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 10월의 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			1,870
대학	ac	815	171	75	155	127	90	68	61	140	90	64			1,041
비영리	or	99	34	27	33	18	15	15	10	24	10	5			191
연구소	re	20	4	5	3	2	0	0	4	3	1	0			22
네트워크	ne	9	7	2	2	1	14	27	0	0	0	0			53
기타(개인)		3,917	1,207	809	1,148	1,237	812	944	765	978	775	663			9,338
총계		6,494	1,712	1,124	1,569	1,621	1,090	1,195	965	1,354	1,028	857			12,515