정보화 사회에서 살아남기 위한 개인정보보호 방안

2009년 동서대학교 초청강연

동명대학교 정보보호학과

신 원

차 례

다양한 위협

옥션 개인정보 해킹 한국인 범인 추적

- 작년 1월 회원 1081만 명의 개인정보가 유출된 인터넷 경매사이트 옥션의 해킹은 한국인이 중국인 해커를 고용해 저지른 것으로 드러났다고 경찰이 밝힘
- 경찰청 사이버대응센터 관계자는 “옥션 회원정보 해킹 사건을 수사 중인 중국 공안과 함께 해킹을 기획, 주도한 한국인 A씨와 중국인 해커 B씨의 신원을 확인하고 이들을 추적 중”이라고 밝힘
- 거액의 사례금을 받기로 한 중국인 해커 B씨는 1월 옥션 회원 1081만 명의 주민등록번호와 주소·전화번호·계좌번호 등 개인정보를 해킹하는 데 성공. 빼낸 데이터베이스(DB)를 A씨에게 전달한 것으로 조사
- 경찰이 행방을 쫓고 있는 A씨는 한국과 중국을 오가며 개인정보를 판매해 온 전문 암거래상인 것으로 추측

가짜 백신으로 2년간 125만명에 92억 뜯어

- 정상 파일을 악성코드로 분류하는 가짜 바이러스 프로그램을 통해 92억원에 이르는 거액을 챙긴 업체 대표가 불구속 기소
- 서울중앙지검 첨단범죄수사부는 정상적인 파일을 악성코드로 검출하여 부당 이익을 챙긴 혐의(사기)로 미디어포트 전 대표 이모씨를 불구속 기소

〈Dr.Virus 3 실행창〉

금융기관 전산망 해킹 시도 적발

- 서울지방경찰청 외사과는 고객계좌 등에서 불법으로 예금을 인출하기 위해 은행 건물에 설치된 인터넷 무선공유기 해킹을 시도한 혐의(정보통신이용촉진 및 정보보호에 관한 법률 위반)로 총책 이모씨(51)와 해커 김모씨(25) 등 3명을 구속
- 지난 11일 새벽 0시50분께 서울 명동 하나은행 주차장에서 자신들의 노트북컴퓨터에 무선랜카드와 Access Point를 장착, 해킹프로그램을 이용해 은행의 인터넷 무선공유기 MAC 주소를 스니핑한 후 PC관리자 번호를 입력, 12차례에 걸쳐 접속을 시도하는 등 2개 은행의 정보통신망에 접근을 시도한 혐의
- 경찰 조사 결과 총책 이씨는 2006년부터 중국을 오가며 범행을 준비하면서 범행 대상지를 수 차례에 걸쳐 답사, 해커 김씨 등은 기업체 네트워크 시설 유지·보수 용역업체에 근무한 경력이 있는 전문가로 드러남

GS칼텍스 정보유출 용의자는 자회사 직원

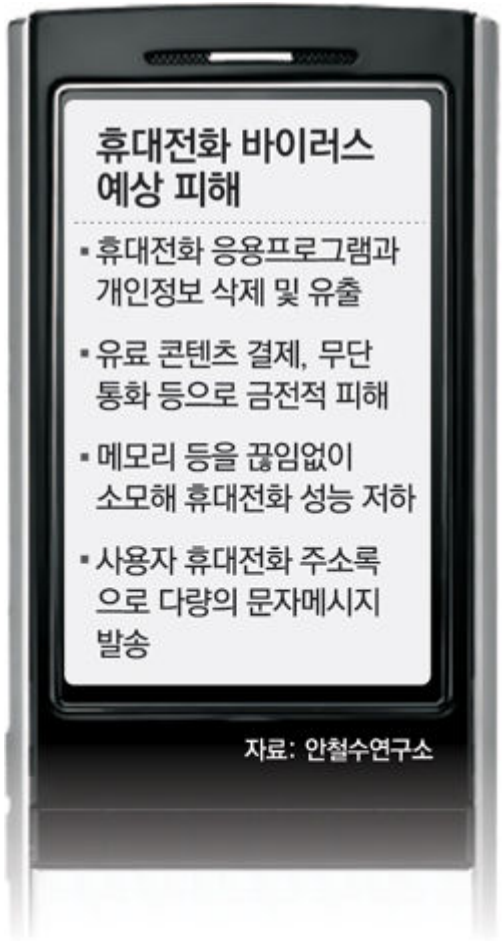
- 경찰에 따르면 정 씨는 GS칼텍스 고객들의 개인정보 데이터베이스(DB)에 접근할 수 있는 권한을 이용해 7월 중순부터 8월 말까지 1119만여 명의 GS칼텍스 보너스카드 고객들의 개인정보를 자신의 업무용 컴퓨터로 빼돌려 DVD로 제작한 혐의

GS칼텍스 고객정보 유출 일지

6월 말	용의자 정모(28) 씨, 고객 정보 및 네트워크 관리 업무 배정
7월 10일	정 씨, 고교 동창 왕모(28) 씨와 범행 공모
7월 13일	정 씨, 고객 정보 빼돌려 샘플 CD 제작. 왕 씨의 후배 김모(24) 씨, 범행 합류
8월 27일	정 씨, 동료 직원인 배모(30·여) 씨에게 고객 정보를 엑셀 파일로 정리 부탁
8월 29일	정 씨, 정리된 파일을 DVD로 제작. 왕 씨, 이 DVD를 "언론에 제보해달라"며 김 씨에게 전달
9월 2일	김 씨, 모 언론사 기자 등에게 제보. DVD 5장 복사해 전달
9월 5일	DVD를 전달받은 기자, 고객 정보 유출 사실 보도. 경찰, GS칼텍스의 의뢰로 수사 착수
9월 6일	경찰, 정 씨 일당 검거

“휴대전화 바이러스 주의보” 한국 더이상 안전지대 안돼

- 보안업계에 따르면 지금까지 휴대전화 바이러스는 핀란드 노키아의 심비안, 미국 마이크로소프트(MS)의 윈도모바일 운영체제(OS)를 탑재한 유럽, 미국 지역의 스마트폰에서 주로 발생
- 휴대전화가 적은 한국에선 아직 바이러스가 발견된 적이 없으나, 국내 거의 모든 휴대전화에 탑재된 휴대전화용 소프트웨어 ‘자바2모바일에디션(J2ME)’ 기반의 바이러스가 최근 외국에서 등장한 뒤 확산되는 것으로 밝혀져 대책 마련이 시급



본인만 가능한 '본인 인증' 주목

- ‘본인이 맞나?’ 인증체계 강화 – 목소리나 지문과 같은 생체 정보를 통해 본인임을 확인하는 시스템을 도입하자는 주장
- 목소리는 인터넷뱅킹 뿐 아니라 텔레뱅킹에도 이용할 수 있는 장점
- 지문의 경우, PC에 이미 활용되는 등 대중화되어 있다는 것이 장점, 인터넷뱅킹뿐 아니라 텔레뱅킹에도 활용될 수 있으며, 감기에 걸리는 등 목소리가 변해도 인증이 가능하고 녹음사실도 분별 가능
- 스마트카드에 본인 정보를 저장해 인증하는 방식, 해킹이 어려운 스마트카드 칩에 본인 정보를 내장하고 PC가 아닌 별도의 단말을 통해 이를 인증
- 해킹이 불가능한 가상공간을 만들어 본인 인증을 하고 데이터를 전송하는 방식도 등장
- 전화확인을 통한 본인 인증 방식, 이미 통신사에 저장된 개인정보를 이용하는 방식

네티즌 10명중 7명 "정보 보호방침 확인 안해"

- 네티즌 10명중 7명은 개인정보의 중요성을 인식하면서도 정작 회원 가입 때 개인정보보호 방침을 제대로 확인하지 않는 것으로 나타남
- '2008년 정보보호 실태조사 결과'에 따르면 인터넷 이용자 중 사이트에 회원으로 가입할 때 개인정보 취급방침을 공개한다는 사실을 아는 이용자는 59%로 절반을 넘었지만, 개인정보 취급방침을 확인하지 않는 가입자는 전체의 68.7%에 달하는 것
- 개인정보 취급 방침을 읽지 않는다는 이유에 대해서는 내용이 너무 많아 번거롭거나(85.7%), 내용이 너무 어려워 이해하기 힘들다(11.8%) 고 대답
- 또 해킹(3.4% 포인트), 웜 • 바이러스(4.1% 포인트), 스파이웨어(2.5% 포인트) 등으로 인한 피해는 증가했지만 피해 경험자의 절반 가량(47.1%)이 '신고기관을 몰라서 피해사실을 알리지 않았다'고 말해 이에 대한 홍보 강화가 필요

방통위, KISA 개인정보보호지원센터에 신속대응팀 신설

- 방송통신위원회는 개인정보침해사고에 신속하고 효과적으로 대응할 수 있도록 한국정보보호진흥원(KISA) 개인정보보호지원센터에 '개인정보침해 신속대응팀'을 구성, 운영
- 개인정보보호 법률 및 기술 전문가 15명으로 구성된 '개인정보침해 신속대응팀'은 앞으로 개인정보 유·노출 사건 발생시 관계 공무원과 현장점검부터 점검 후 개선사항 이행 모니터링 단계까지 세부 점검 절차와 방법 등을 마련해 대응
- 개인정보를 침해당한 경우에는 누구나 KISA 개인정보침해신고센터(국번없이 전화 1336번)에 신고할 수 있으며, 개인정보 유·노출 사고가 발생할 때에도 관계공무원과 개인정보침해 신속대응팀이 함께 현장에 투입

악성코드 유포 “가짜백신” 기승

- 지난해부터 논란이 됐던 가짜백신이 꾸준히 증가하고 있어 사용자들의 주의와 정부의 대책마련이 시급하다는 지적
- 지난해 1월부터 올해 2월까지 조사한 자료에 따르면 지난해 129개의 가짜백신이 확인됐으며 특히 이들 중 상당수는 지난해 하반기에 집중적으로 등장,또 올해 1월, 2월 두 달간 찾아낸 가짜백신만도 지난해의 약 1/4인 31개로 조사돼 지난 하반기부터 올해 초까지 계속 증가 양상
- 가짜 백신은 악성코드를 유포하거나 이상이 없는 파일을 이상이 있다고 진단해 금전적 이득을 취하는 두 가지 종류로 구분
- 첫 번째 경우는 악성코드를 유포하기 때문에 가짜백신을 진단해 막는 것이 쉽지만 두 번째 경우는 오진에 고의성이 있는지를 가릴 수 있는 기준이 명확하지 않아 가짜 백신을 가리는 데 어려움
- 이에 대해 업계는 사용자 개인의 주의와 함께 정부 차원에서 가짜백신 출현을 막을 수 있는 명확한 기준 마련이 시급하다고 지적

다양한 정보

메일을 사용하다

- 어느날, 국제적으로 이미 유명해져 버린 자신을 발견
- 쇼핑, 보험, 대출, 성인물 등 국적 불문의 다양한 스팸
- 익숙한 메일 주소에서 처음 보는 외국인 메일주소까지 자신도 모르는 첨부파일도 다양

리포팅 대상 시간 2008년 10월 25일 00시 00분 ~ 2008년 10월 25일 23시 59분
발송 시간 2008년 10월 26일 01시 00분
사용자 계정 shinweon@tit.ac.kr

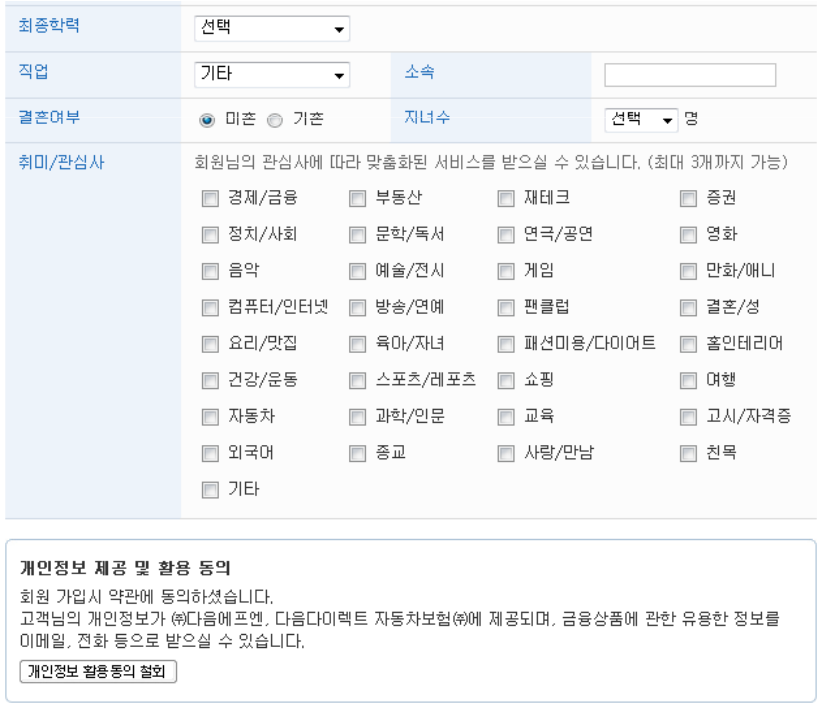
구분	정상	스팸	바이러스	합계
수신메일	1	4	0	5

수신된 스팸/바이러스 메일 목록

번호	시간	구분	제목	발신자	필터링 정보
1	03시 18분	스팸	[복구] [허용] Your 9 inch worm will amaze ..	lolam1962@Ariz..	RPD Engine X-CTCH-..
2	09시 13분	스팸	[복구] [허용] Double your chances of winni..	smccormick@cos..	메일본문, .eurocas..
3	17시 28분	스팸	[복구] [허용] Respective Libidos	syn@synchrodan..	메일본문, shopthou..
4	23시 01분	스팸	[복구] [허용] Fail too fast in bed?	hock1994@CALIF..	RPD Engine X-CTCH-..

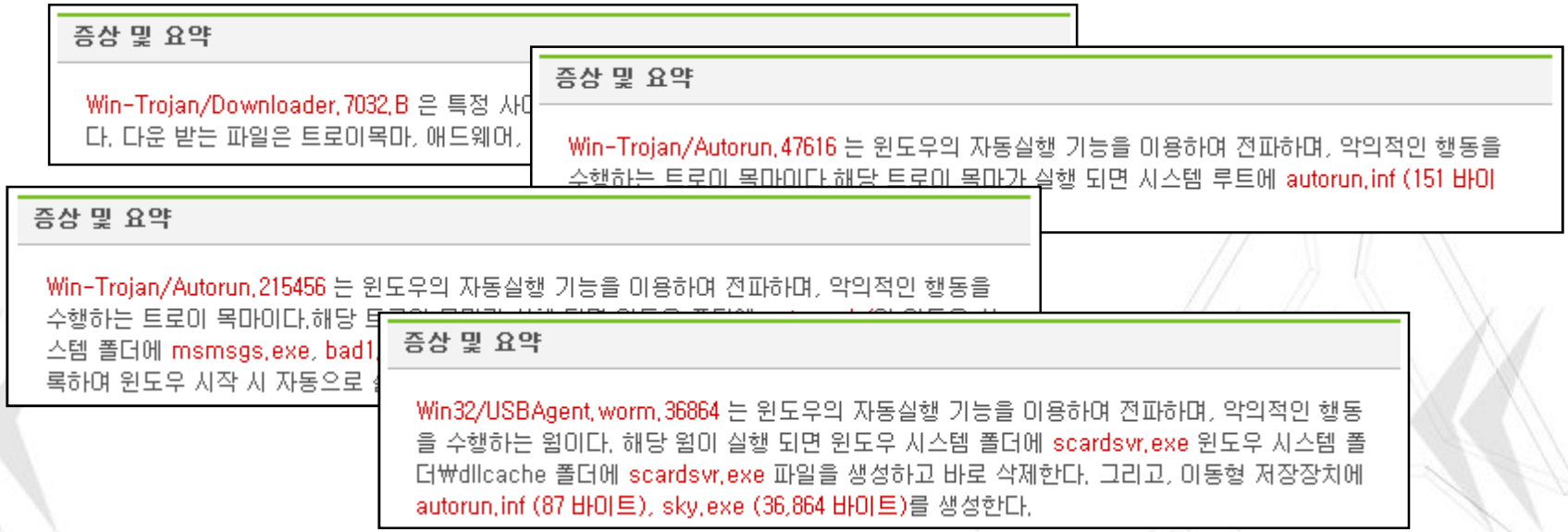
포털 사이트에 가입하다

- 주로 무료 메일, 블로그를 사용하기 위한 수단으로 가입
- 실명인증을 위해 주민등록번호 입력 필수
- 결혼여부, 자녀수, 취미, 개인정보 제공 및 활용 동의



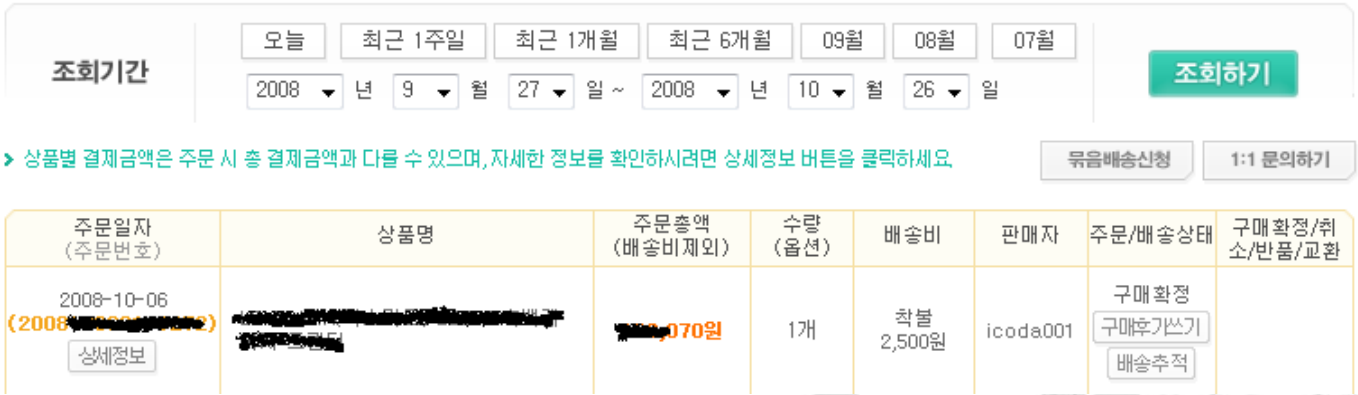
누구나 사용하는 USB 메모리

- 저렴한 가격, 기가급 용량, 편리한 휴대성, 깜찍한 디자인으로 디스켓을 대체하여 사용되는 USB 메모리
- PC방, 다른 사람 컴퓨터에서도 급한 용무로 USB를 꽂아서 즐겨 사용



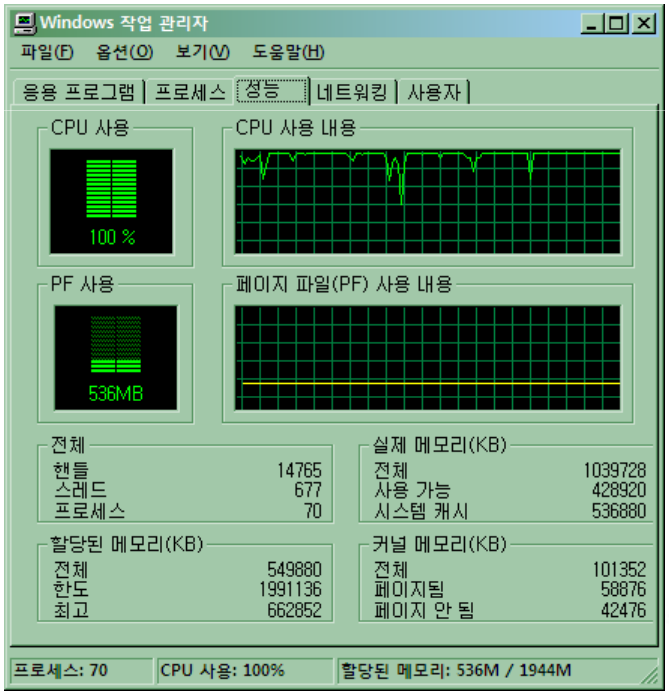
인터넷 쇼핑몰에서 물건을 사다

- 자신이 구매한 성인물(?), 의류, 전자제품 등을 진행 중인 거래, 취소/반품/교환한 내역까지 마음대로 조회
- 신용카드 번호를 입력한 후 인증서를 발급해주고 다음부터는 비밀번호만으로 결제가 되던데… (안심결제)



잘 쓰던 컴퓨터가 어느날 갑자기~

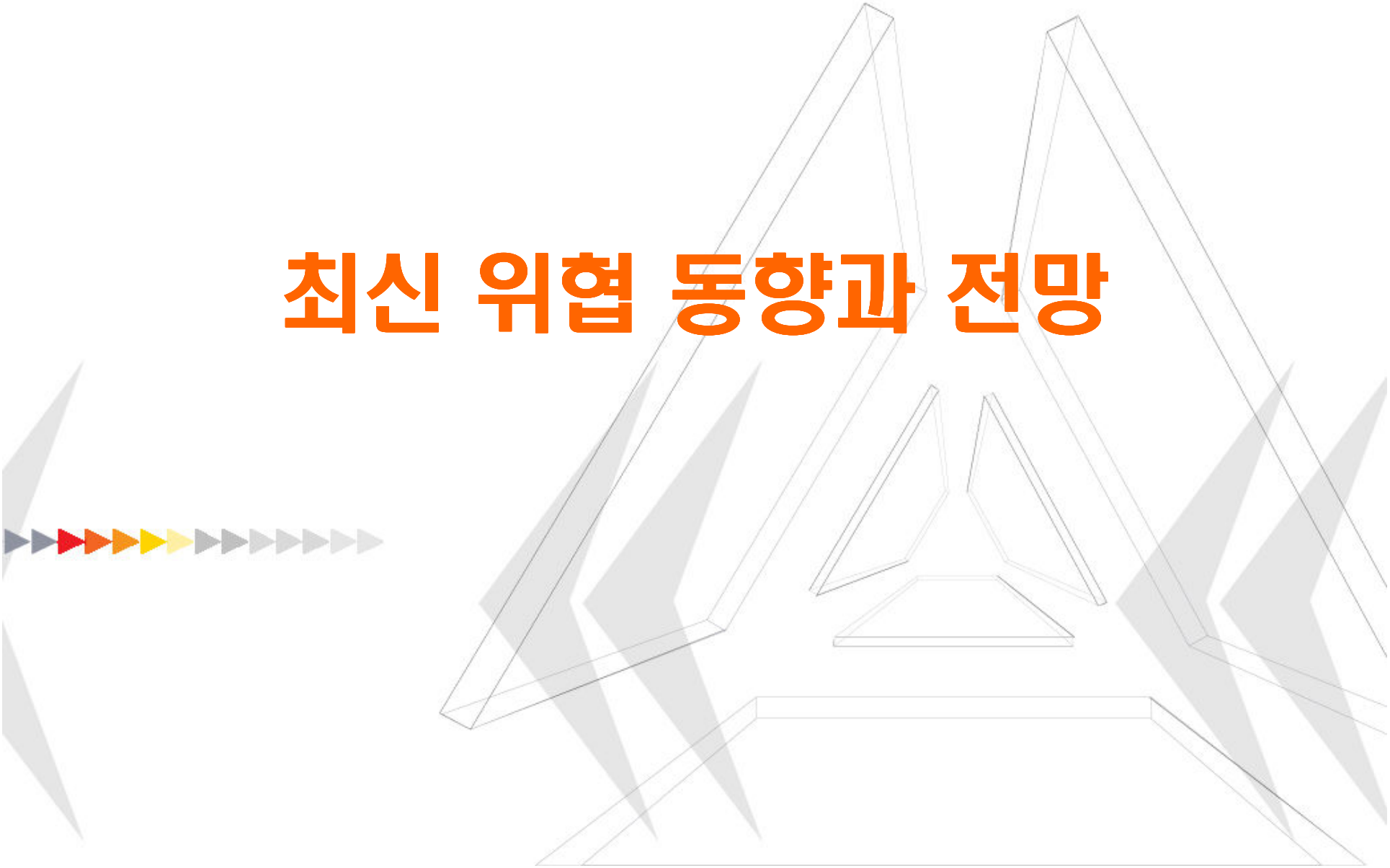
- 오늘따라 왠지 컴퓨터가 느려터진다?
- 어젯밤 성인 사이트에 들어가서 뭔가를 설치한 이후로, Internet Explorer만 띄우면 내 인내심을 자극한다



기타

- 자동차 보험 만료 시점에 걸려오는 보험회사 전화들
  - 보험 만료시기가 되면 줄기차게 걸려오는 전화들…
- 휴대폰으로 오는 대출 메시지
  - 초고속통신망을 집에 설치했더니 초고속 대출 메시지가 휴대폰으로 날아온다?
- 급한 용무로 PC방에서 인터넷을 해야 하는 경우
  - Internet Explorer, 게임은 물론 이상한 프로그램들이 잔뜩 깔려 있다.
  - Internet Explorer 사용 중 닫아도 닫아도 계속 뜨는 광고 창

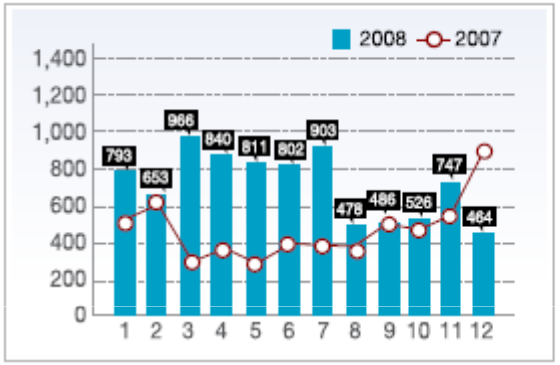
최신 위협 동향과 전망



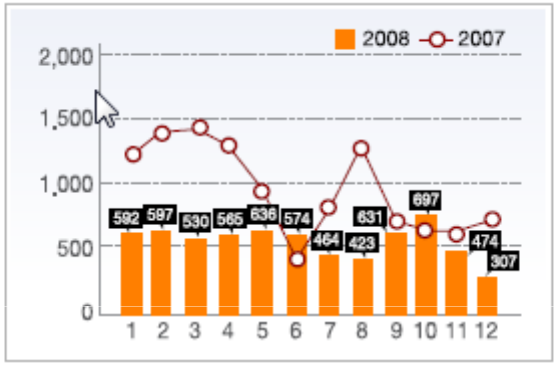
월별침해사고 동향

다양한 방법으로 침해 발생

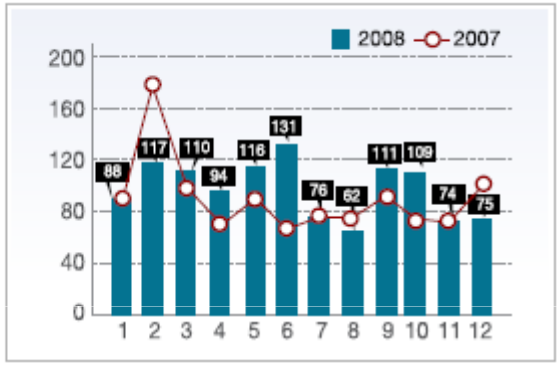
한국정보보호진흥원 인터넷침해사고대응지원센터



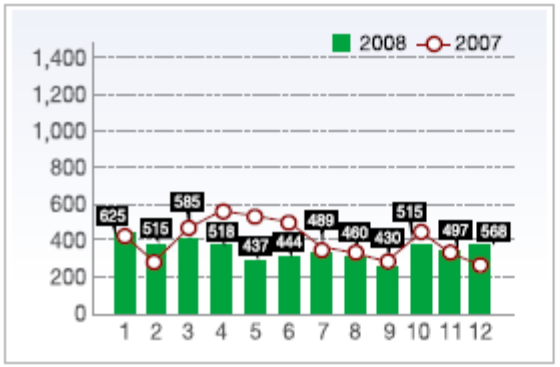
| 웜 바이러스 신고 접수건수 |



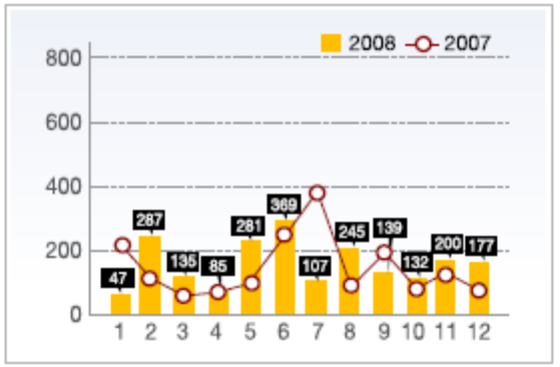
| 스팸릴레이 신고 처리건수 |



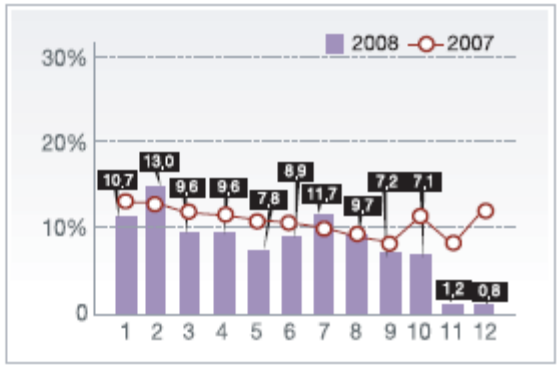
| 피싱 경유지 신고 처리건수 |



| 단순침입시도+기타해킹신고 처리 |



| 홈페이지 변조사고 처리건수 |



| 악성 Bot 감염비율 |

해킹사고 피해기관별 분류

- 전통적인 웜과 바이러스보다 트로이 목마의 증가
- 금전적 이득을 얻기 위한 개인 정보 탈취

한국정보보호진흥원 인터넷침해사고대응지원센터

기관	2007년 총계	2008년												2008년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
기업	3,039	305	291	274	228	249	285	242	259	273	295	285	358	3,344
대학	1,121	55	42	78	84	59	30	47	25	45	66	39	33	603
비영리	273	18	15	20	5	8	17	16	13	18	19	15	9	173
연구소	5	0	0	0	0	0	0	0	0	1	0	0	1	2
네트워크	133	0	0	0	0	0	0	0	0	0	0	0	0	0
기타(개인)	17,161	974	1,168	988	945	1,154	1,186	831	893	974	1,073	906	726	11,818
합계	21,732	1,352	1,516	1,360	1,262	1,470	1,518	1,136	1,190	1,311	1,453	1,245	1,127	15,940

※ 기관 분류기준 : 침해사고 관련 도메인 이나 IP를 기준으로 기업(co,com), 대학(ac), 비영리(or,org), 연구소(re), 네트워크(ne,net), 기타(pe 또는 ISP에서 제공하는 유동 IP 사용자)으로 분류

해킹사고 운영체제별 분류

- 국내에서 가장 많이 사용하는 Windows 운영체제에 대한 공격이 압도적인 가운데 LINUX도 증가 추세
- 기타 플랫폼을 대상으로 한 공격 증가

한국정보보호진흥원 인터넷침해사고대응지원센터

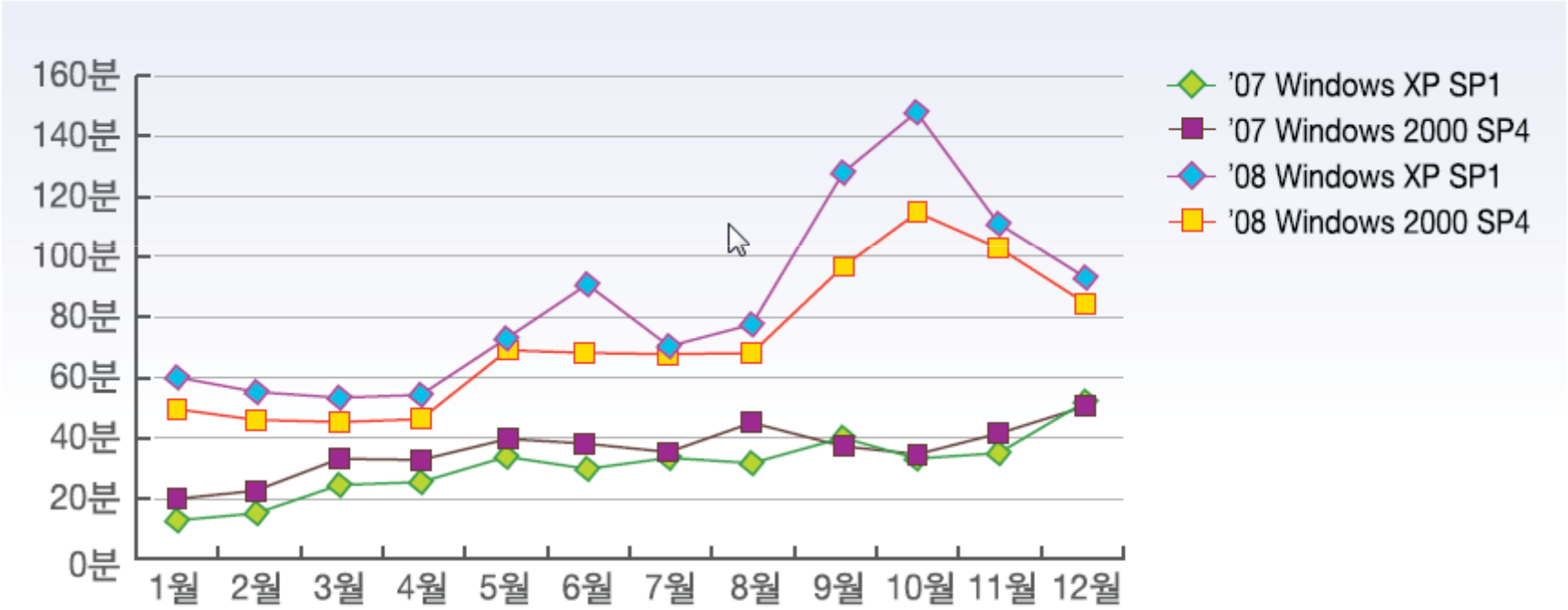
운영체제	2007년 총계	2008년												2008년 총계
		1	2	3	4	5	6	7	8	9	10	11	12	
Windows	19,128	1,039	1,070	996	938	929	982	775	747	908	1,034	777	639	10,834
Linux	2,063	135	274	170	158	402	281	185	230	230	212	240	227	2,744
Unix	27	14	5	3	8	0	58	16	49	15	5	14	5	192
기타	514	164	167	191	158	139	197	160	164	158	202	214	256	2,170
합계	21,732	1,352	1,516	1,360	1,262	1,470	1,518	1,136	1,190	1,311	1,453	1,245	1,127	15,940

※ 운영체제별 분류 자료는 각 운영체제의 안전성과는 상관관계가 없으며, 단지 신고에 따른 분석 자료임

월별 평균 생존 가능시간 변동 추이

작년에 비해 생존 가능 시간이 2배 이상 증가

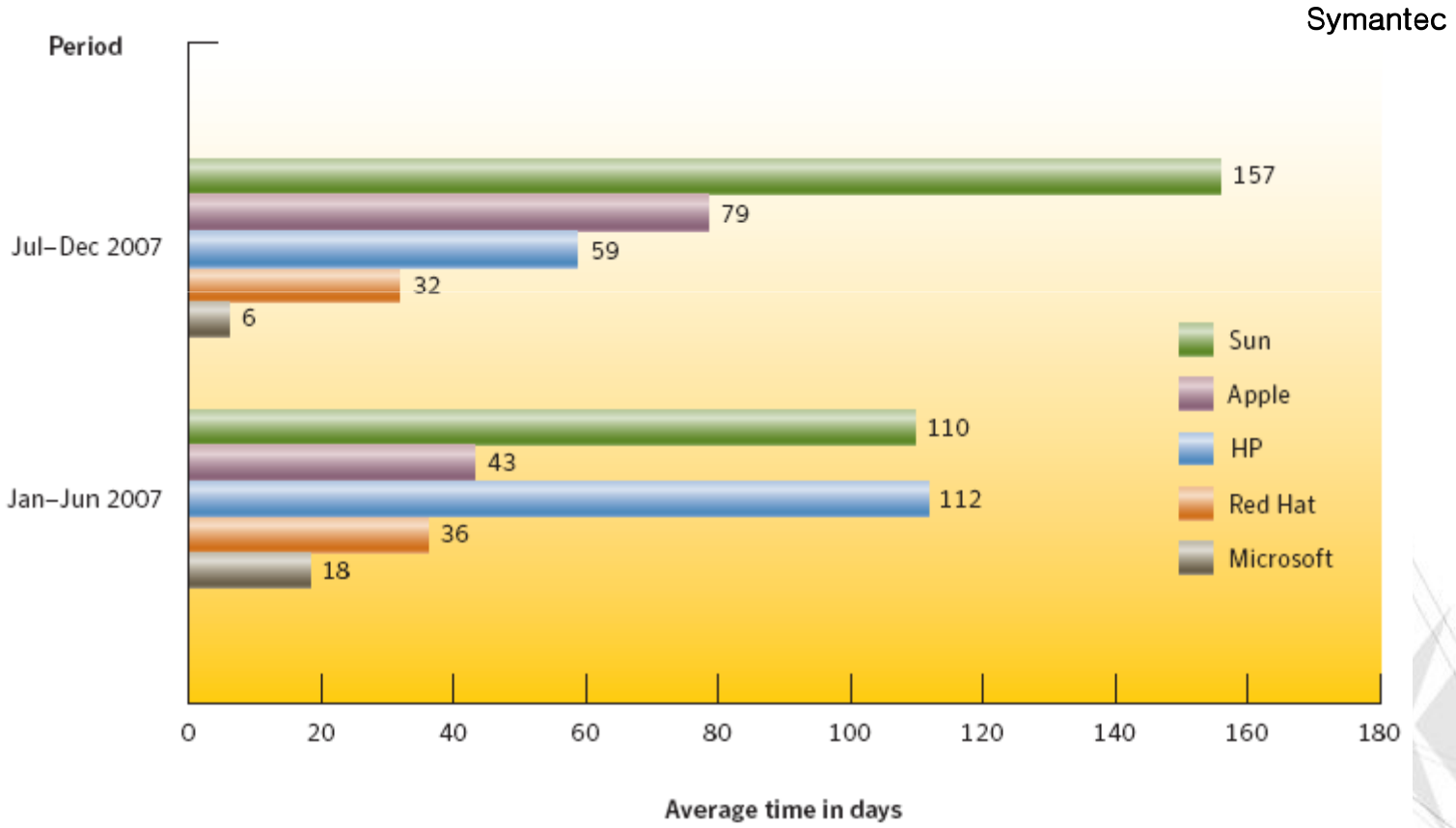
한국정보보호진흥원 인터넷침해사고대응지원센터



※ 생존시간은 "윈도우 네트워크서비스 취약점"을 악용하는 유형의 전파활동 증감 추이만을 반영하므로 이메일 악성코드 등 다른 유형의 전파기법을 이용하는 악성코드 감염활동 추이동향과는 무관함

운영체제 패치 개발 기간

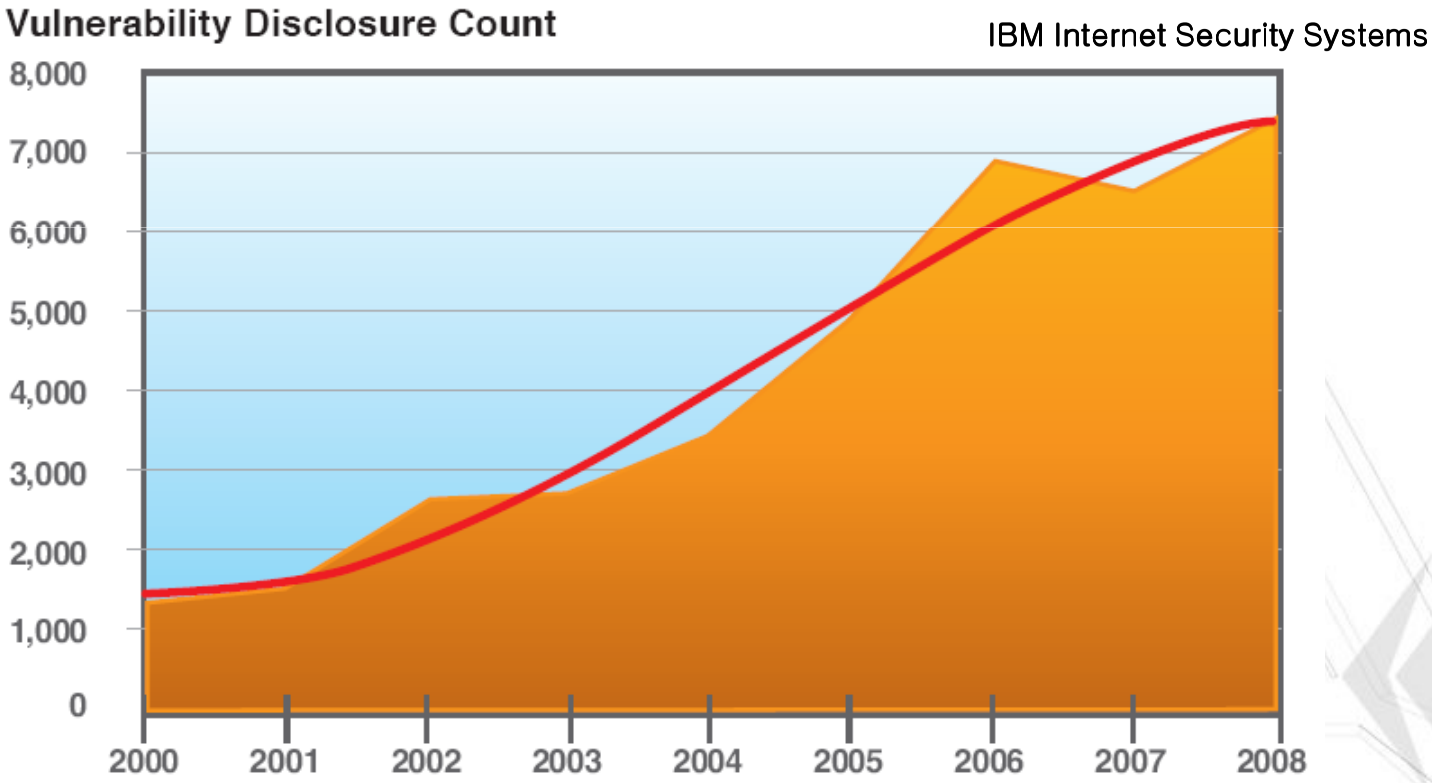
제작 회사별 운영체제 패치 개발 평균 기간 (2007년)



소프트웨어 취약성

해마다 증가하는 소프트웨어 취약성

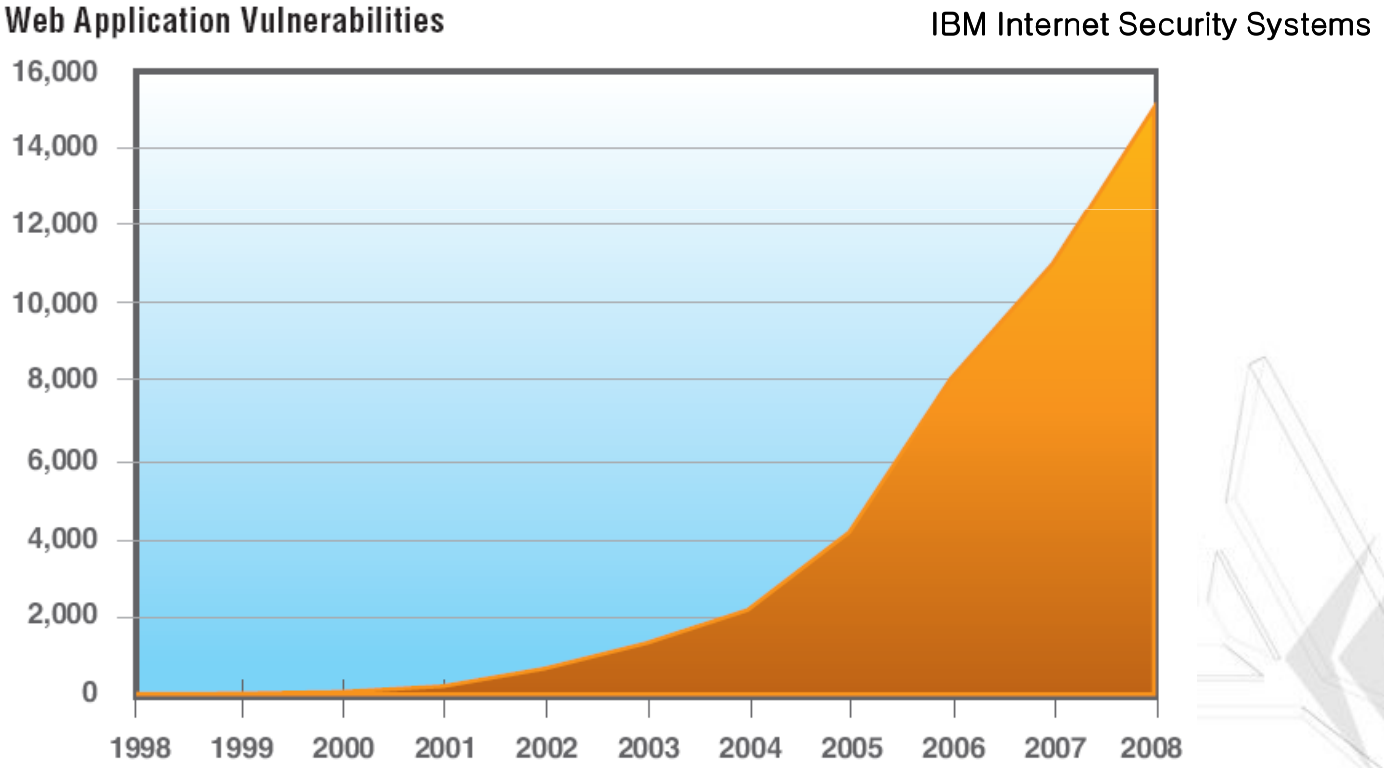
- 단, 알려진 취약성에 한함



웹 어플리케이션 취약성

공격 방식에 따른 웹 어플리케이션 취약성

- 단, 알려진 취약성에 한함

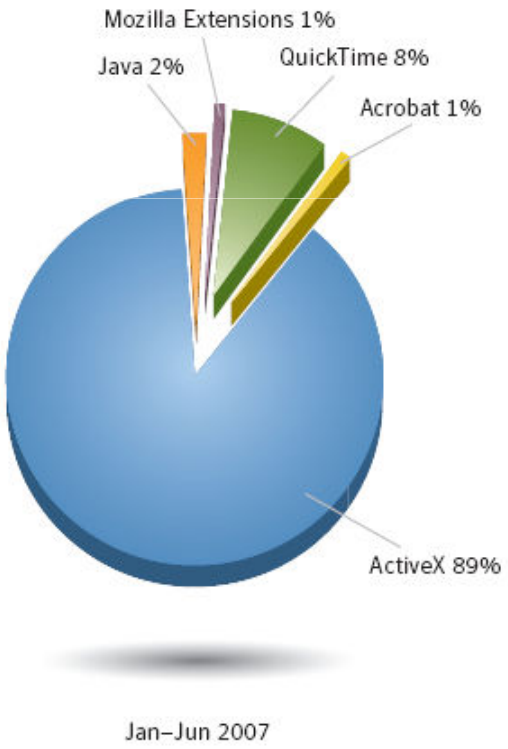


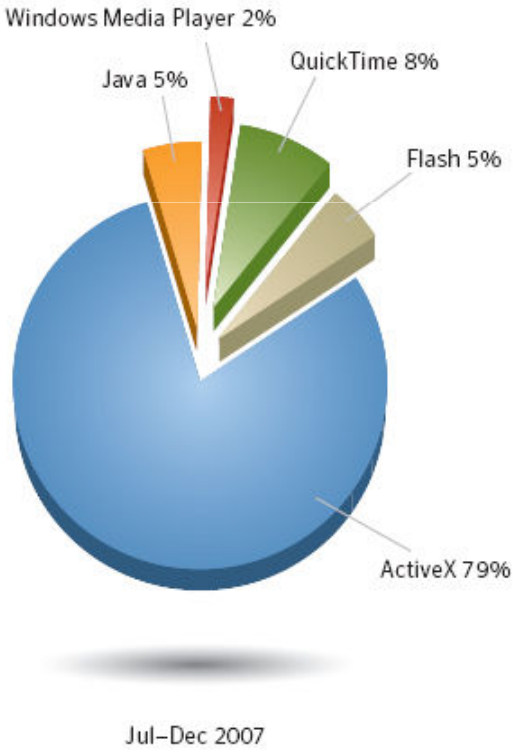
웹 브라우저 취약성

웹 브라우저 플러그인 취약성 (2007년)

- 단, 알려진 취약성에 한함

Symantec

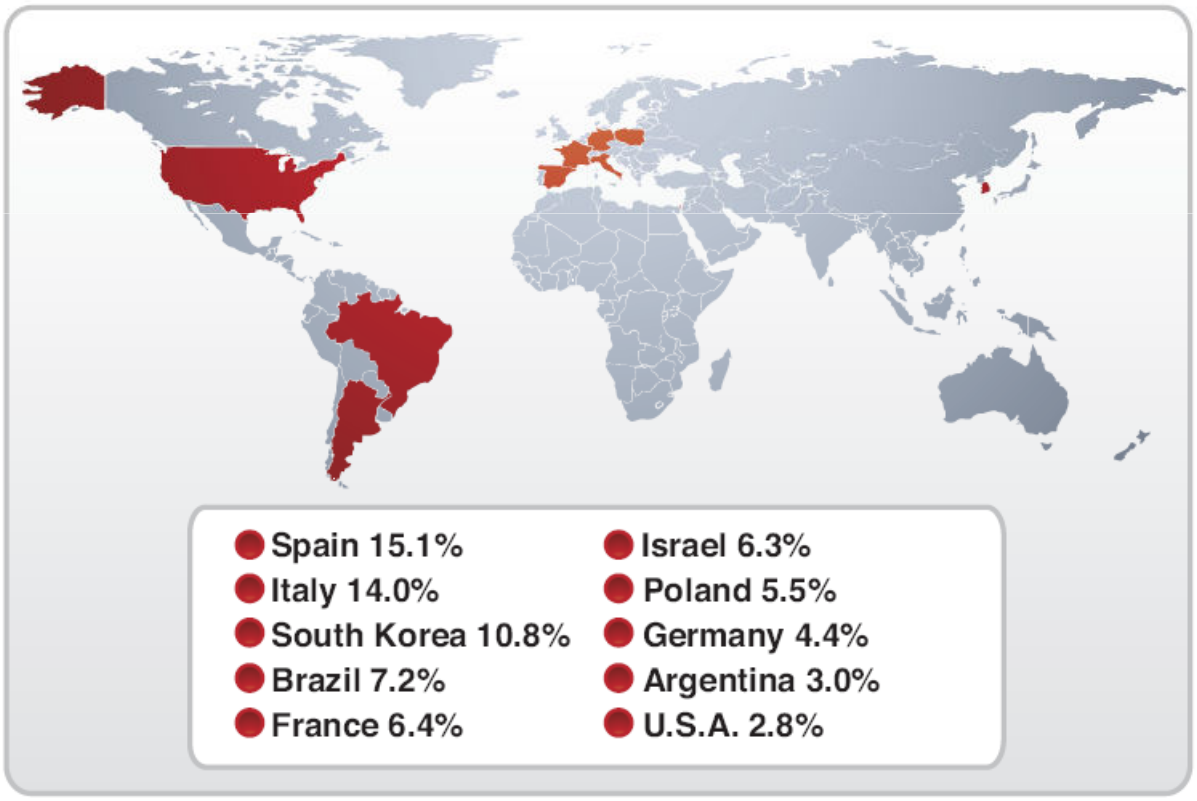




국가별 피싱 주소 분포

- 피싱 주소에 포함된 국가별 웹 사이트 주소 비율 (2008년)

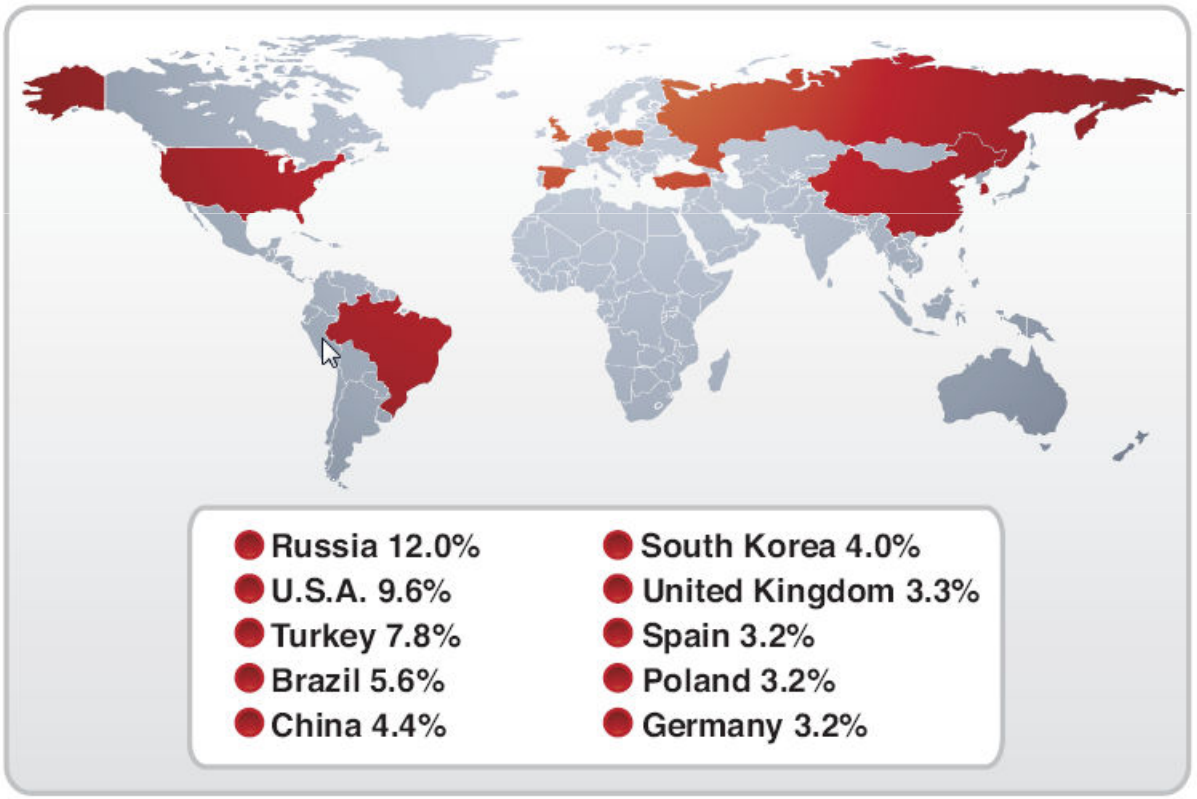
IBM Internet Security Systems



국가별 스팸 주소 분포

- 스팸 메일에 포함된 국가별 웹 사이트 주소 비율 (2008년)

IBM Internet Security Systems



국가별 위협 통계 순위

국가별 위협 통계 순위 (2007년)

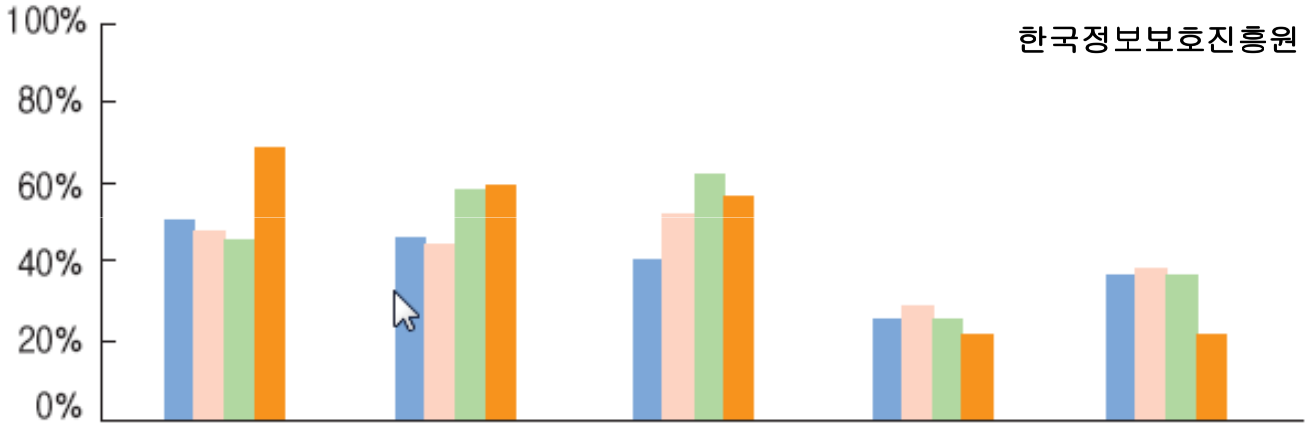
Symantec

Current Rank	Previous Rank	Country	Current Percentage	Previous Percentage	Bot Rank	Command-and-Control Server Rank	Phishing Web Sites Host Rank	Malicious Code Rank	Spam Zombies Rank	Attack Origin Rank
1	1	United States	31%	30%	1	1	1	1	1	1
2	2	China	7%	10%	3	5	2	2	4	2
3	3	Germany	7%	7%	2	2	3	7	2	3
4	4	United Kingdom	4%	4%	9	6	7	3	12	5
5	7	Spain	4%	3%	4	19	15	9	9	4
6	5	France	4%	4%	8	13	6	11	7	6
7	6	Canada	3%	4%	13	3	5	4	35	7
8	8	Italy	3%	3%	5	10	11	10	6	8
9	12	Brazil	3%	2%	6	7	13	21	3	9
10	9	South Korea	2%	3%	15	4	9	14	13	10

개인정보 침해 유형

개인정보/프라이버시 침해 피해를 경험한 이용자

❖ 전국 13~59세 월 1회 이상 인터넷 이용자 목수 응답

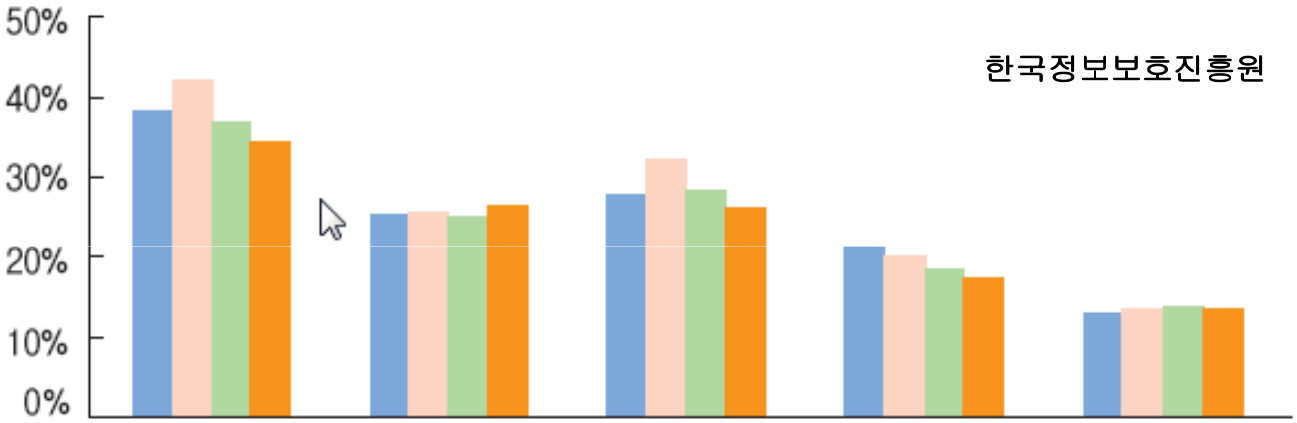


한국정보보호진흥원

	사업자의 관리소품 개인정보유출	동의 없이 개인정보 본목적 이외의 용도이용/제3자제공	텔레마케팅 목적 개인정보를 무단수집/회원가입	ID 및 비밀번호 도용	주민번호 도용
2005년	52.3	45.2	43.2	37.8	38.8
2006년	45.7	44.4	51.0	39.3	39.8
2007년	47.1	58.0	61.9	35.2	36.2
2008년	72.5	58.4	51.7	26.3	22.9

패스워드 설정

패스워드 설정 여부

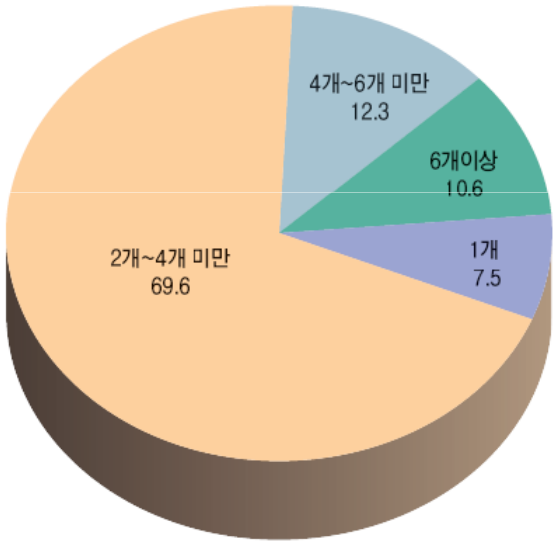


한국정보보호진흥원

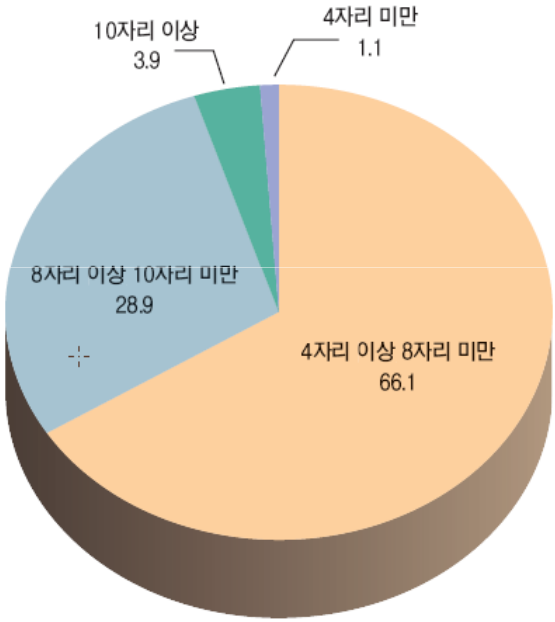
	중요 데이터 저장 파일	윈도우 로그인 시	공유 파일 및 폴더	PC 부팅 시 (CMOS 암호)	화면보호기능 해제시
2005년	38.2	25.1	27.5	21.1	12.8
2006년	41.8	25.6	32.3	20.1	13.4
2007년	36.8	24.7	28.4	18.1	13.7
2008년	34.3	26.4	25.8	17.3	13.6

패스워드 및 데이터 관리

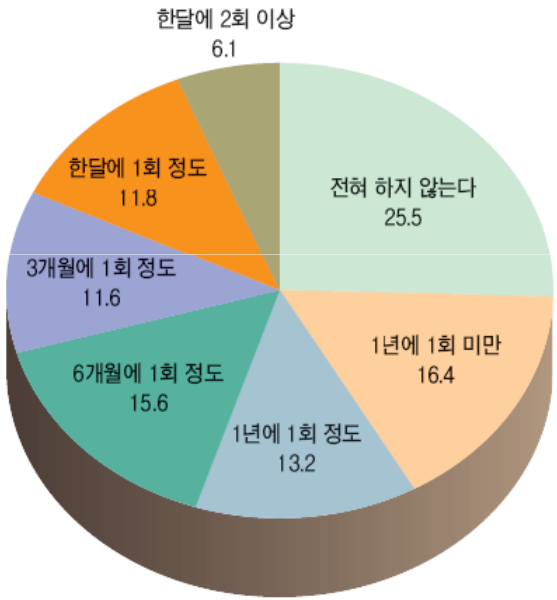
패스워드 종류



패스워드 길이



데이터 백업 빈도



한국정보보호진흥원

최신 위협의 특징

- 다양한 인터넷 기술과 어플리케이션이 등장함에 따른 역기능들도 함께 증가
  - 사회공학적 공격 기승
  - 국산 게임 계정 탈취용 악성코드의 폭발적 증가
  - 무선랜의 취약성을 이용한 공격 증가
  - DDoS 공격의 급증
  - 내부자에 의한 개인정보 유출
  - 이동저장장치로 전파되는 악성코드 기승
- 다양한 해킹 시도, 바이러스 및 웜을 이용한 공격

※ 최근 공격의 대다수가 금전적인 목적을 위한 공격

위협의 전망

- 불특정 다수를 겨냥한 공격보다 특정 그룹, 특정 사용자에 대한 국지적인 공격 증가
- 해킹, 악성코드가 Windows를 벗어나 Vista, Mac OS, 휴대폰 등 다양한 플랫폼으로 이전
- 개인의 금융정보를 노린 홈페이지 해킹 증가
- 국내 기업 홈페이지를 대상으로 한 중국 해커의 서비스 거부 공격 증가
- Internet Explorer, MS Office, Media Player 등 사용빈도가 높은 특정 응용프로그램 취약점을 겨냥한 공격 증가
- UCC, SNS 등 웹2.0 서비스 통한 악성코드 전파 가속화

정 리

정리하면…

- 1인 1PC에서 1인 Multi 기기로
  - 과거의 정보보호는 장비 및 솔루션 도입을 통한 전체적인 네트워크 및 시스템 보안의 범주
  - 이제는 네트워크 및 시스템 보안은 물론 개인 컴퓨터, 모바일 기기에 저장된 개인정보보호 영역으로 확장
- 개별 기능 기기에서 융합 모바일 기기로
  - 카세트, 휴대전화, TV 등의 개별 기능을 갖춘 통신 및 방송 기기들이 다양한 기능을 모바일 기기에서 융합
  - TV 수신 가능한 디지털 카메라, Voice Record 및 MP3 Player 기능을 갖춘 전자사전, 인터넷 접속이 가능한 휴대폰 등장

정리하면…

- 특정 플랫폼에서 다양한 플랫폼으로
  - 과거에는 해킹 및 악성코드가 Windows 플랫폼을 중심으로 제작 및 배포
  - 최근에는 LINUX, Mac OS, 휴대폰 운영체제를 대상으로 하는 공격도 발생
- 단순 공격에서 융합 공격으로 진화
  - 여러 악성 기능의 복합화, 발견과 치료가 어려운 방법 선택
  - Virus + Downloader, Bot + Spyware, Bot + Spam, Downloader + Trojan Horse
  - 개인정보 수집 및 탈취, 인터넷 광고, 파일 감염 및 악성코드 확산, 데이터 훼손 등 공격도 융합으로 진화

정리하면...

- 기술 발전에 따른 다양한 위협의 등장
  - 검색엔진, Blog, UCC, SNS 등을 통한 개인 정보의 유출
  - 금전적인 목적을 위해서 다양한 모든 방법을 동원 – 해킹, 악성 코드, 피싱, 사회공학적 공격
- 정보보호 패러다임의 변화
  - 기술 중심의 정보보호에서 기술, 인력, 정책 중심의 정보보호로 전환
  - 통신 정보보호에서 시스템 및 네트워크 정보보호를 지나 생활 속의 정보보호로 변화
  - IT기반의 정보보호에서 융합 환경의 지식정보보안으로 진화 – IT 정보보호, 물리적 정보보호, 융합 정보보호를 포괄

매마

인터넷 시대 정보보호 생활수칙

- 자동 업데이트가 가능한 백신 소프트웨어 설치 및 실시간 감시기능 사용
- 출처, 첨부파일이 의심스러운 E-Mail은 열람하지 말고 삭제
- 정기, 비정기적인 윈도우즈 보안 패치를 실시하고, PC용 방화벽을 사용
- 패스워드는 영문, 숫자, 특수기호 등을 조합하여 8자리 이상으로 설정하고 주기적으로 변경
- 개인 컴퓨터에 부팅, 로그인, 화면보호기의 패스워드를 설정하고 반드시 사용
- 공유폴더 사용은 최소화하고, 사용시 반드시 최소권한만을 부여하여 사용
- 웹사이트 방문시 설치하는 프로그램은 인증서 및 디지털 서명을 참고하여 신뢰성 확인 후 설치
- P2P, 메신저를 이용한 파일 다운로드시 최신 백신 소프트웨어로 점검 후 사용
- 중요한 자료는 패스워드를 설정하여 저장하고 주기적인 백업 및 인터넷이 연결된 PC에 저장 금지
- 정품 소프트웨어의 사용

정보보호 실천 수칙

- 윈도우즈 보안 패치 자동 업데이트 설정하기
- 바이러스 백신 및 스파이웨어 제거 프로그램 설치하기
- 윈도우 로그인 패스워드 설정하기
- 패스워드는 8자리 이상의 영문과 숫자로 만들고 3개월마다 변경하기
- 신뢰할 수 있는 웹사이트에서 제공하는 프로그램만 설치하기
- 인터넷에서 다운로드 받은 파일은 바이러스 검사하기
- 출처가 불분명한 메일은 바로 삭제하기
- 메신저 사용 중 수신된 파일은 바이러스 검사하기
- 인터넷 상에서 개인 및 금융 정보를 알려주지 않기
- 중요 분서 파일은 암호를 설정하고 백업 생활화하기

전자금융 이용자 정보보호 수칙

- 금융회사에서 제공하는 보안프로그램을 반드시 설치하기
- 전자금융에 필요한 정보는 수첩, 지갑 등 타인에게 쉽게 노출될 수 있는 매체에 기록하지 않고 타인에게(금융회사 직원을 포함) 알려 주지 않기
- 금융 계좌, 공인인증서 등의 각종 비밀번호는 서로 다르게 설정하고 주기적으로 변경하기
- 금융거래 사이트는 주소창에서 직접 입력하거나 즐겨찾기로 사용하기
- 전자금융거래 이용내역을 본인에게 즉시 알려주는 휴대폰 서비스 등을 적극 이용하기
- 공인인증서는 USB, 스마트카드 등 이동식 저장장치에 보관하기
- PC방 등 공용 장소에서는 인터넷 금융거래를 자제하기
- 바이러스백신, 스파이웨어 제거프로그램을 이용하고 최신 윈도우보안패치를 적용하기
- 의심되는 이메일이나 게시판의 글은 열어보지 말고, 첨부파일은 열람 또는 저장하기 전에 백신으로 검사하기
- 선수금 입금 요구, 상식수준 이상의 대출 조건을 제시하는 경우 해당 금융회사에 동 대출 취급여부를 직접 확인하기

10 IE Browser Settings for Safer Surfing

1. Disable XPS documents
2. Disable font download
3. Disable inclusion of local file directory path when uploading fil es to a server
4. Disable prompting if you are prone to just clicking "yes"
5. Always prompt for username and password
6. Disable SSL 2.0 support
7. Enable TLS support
8. Disable searching from the URL bar
9. Disable unnecessary add-ons
10. Uninstall old Java installations