What's Going On?

2007년 침해사고 동향 및 2008년 전망 보고서

지난 2008년 1월초 KISA 인터넷침해사고대응지원센터가 '2007년 침해사고 동향 및 2008년 전망'에 대한 분석보고서를 내놓았다. 침해사고에 대한 축적된 사고사례들을 토대로 분석된 침해사고 동향과 전망이라는 점에서 이번 보고서는 다가올 위협에 대비해야 하는 정보보호 관계자에게는 유용한 참고자료가 될 것이다. 2007년 한해 우리 IT 환경을 괴롭혔던 침해사고 유형은 무엇이었고, 향후 우리가 대비해야 할 문제들은 무엇인지 주요 요소들을 중심으로 살펴보고자 한다.

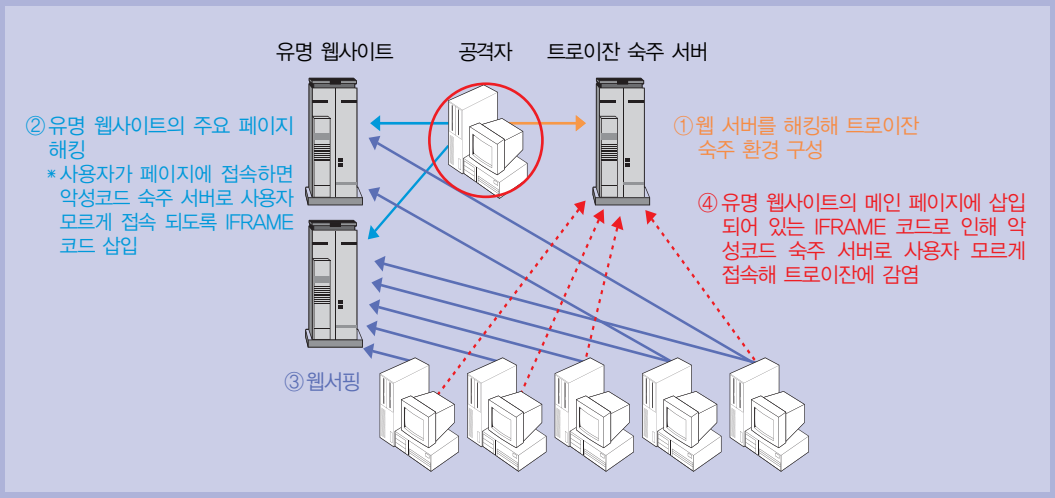
인터넷침해사고대응지원센터 상황관제팀

2007년 웜·바이러스 동향 및 2008년 전망

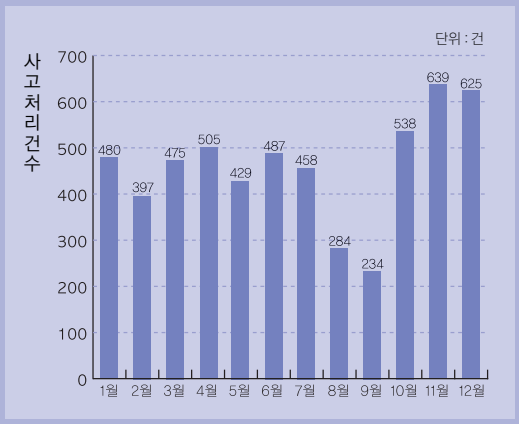
사용자 PC 내 있는 정보를 유출하고, 시스템 자원을 소비하며 악성 네트워크 트래픽을 유발하는 웜·바이러스가 2007년에도 다양하게 출현했다. 특히, 웹 브라우저 취약점 및 ARP 스푸핑을 이용한 악성코드 전파를 비롯해, 실행파일 등을 감염시키는 바이러스 감염피해 등 다양한 형태가 등장했으며, 향후에도 금전적인 목적을 위한 웜·바이러스 유포 및 이를 통한 공격이 증가할 것으로 예상된다.

2007년 웜·바이러스 동향

지난 2006년과 마찬가지로 웹 브라우저가 트로이잔[1] 전파수단으로 악용되는 피해가 많이 발생했다. 대부분의 유명 웹 사이트에 악성코드가 은닉되는 방식으로 피해가 발생했으며, 감염되는 트로이잔은 주로 특정 게임 관련 정보를 유출시키는 유형이 많았다. 이 경우, MDAC, ANI 취약점 등을 이용하는 경우가 많았고, 전파효과를 높이기 위해 ARP 스푸핑을 이용하는 피해가 다수 확인됐다.



▲ 웹사이트를 통한 악성코드 전파의 예



▲ 2007년 악성코드 은닉 사이트 사고처리 건수

특히, Virut 및 Alman 등 바이러스는 PC 내 다수의 실행파일을 감염시켜, 파일 시스템 전체 점검 방식으로 치료하지 않을 경우, 잠복된 감염파일에 의해 재감염될 수 있으며, 분산 서비스 거부 공격에도 악용될 수 있다. 또한, 커널 후킹을 통해 자신을 은폐하는 악성코드들도 다수 발견됐는데, 커널이 후킹되면 악성파일 및 악성코드가 생성한 레지스트리 등이 은폐돼 분석 및 치료는 매우 어려워져 향후에는 커널 후킹을 통한 자기 은폐형 악성코드가 증가할 것으로 예상된다.

반면, 윈도우즈 취약점을 악용한 전파활동은 둔화됐는데, 이는 개인 방화벽 사용효과와 더불어 인터넷침해사고대응지원센터(이하 KISC)가 신규 악성코드에 대한 지속적인 명령전달 채널 제거 및 백신업체와의 악성코드 샘플 공유 등 감염 예방활동이 성과를 거두고 있기 때문으로 풀이된다.

2008년 웜·바이러스 동향

2008년 웜·바이러스의 주요 전파경로 역시 Active X 등 웹사이트를 이용하는 방법이 지속될 것으로 보인다. 그러나 Active X 뿐만 아니라, 최근 등장한 Social Network와 같은 웹 서비스를 악용하거나, P2P 등을 통한 전파가 예상되며, Third-Party 제품군이나 모바일 기기를 겨냥한 악성코드도 등장할 것으로 예상된다.

한편 웜·바이러스 감염을 통한 분산 서비스 거부공격이 많아질 것으로 예상되며, 공격 대상도 성인사이트, 게임 아이템 거래 사이트 등 소형 웹 서비스 업체에 그쳤던 것과 달리, 향후에는 공격대상 범위와 규모, 그리고 피해발생 건수가 지속적으로 늘어날 것으로 예상된다. 또한 ARP 스푸핑을 이용한 악성코드 감염 피해사례가 2008년에도 지속적으로 발생할 것으로 보이며, 특히 악성코드 감염 외에도 피싱 및 파밍 등 악용할 수 있는 범위가 매우 넓어져 이용자의 주의가 필요하다.

2007년 악성 봇 현황 및 2008년 악성 봇 전망

악성 봇(Bot)은 IRC라는 인터넷 채팅에서 사용자 로그아웃 이후에도 대화방을 보전하기 위해 홀로 남아 대화방을 지키던 프로그램(IRC Robot)에서 발전한 것으로, 여기에 여러 기능이 추가되고 해커들이 웜, 바이러스에 접목시키면서 현재의 악성 봇으로 진화돼 왔다. KISC에서는 2004년도부터 악성 봇에 대한 대응을 하고 있지만, 국내에서 발견되는 악성 봇 C&C 서버와 좀비의 수는 여전히 상당수에 이르고 있으며, 최근 악성 봇을 이용해 특정 사이트에 DDoS 공격을 수행하고 금품을 요구하는 등 그 악용 사례들이 다양해지고 있다.

2007년 악성 봇 현황

KISC 허니넷 트래픽을 통해 추정한 2006년 악성 봇 국내 감염률은 평균 12.5%지만, 2007년 평균 감염률은 11.3%로 소폭 감소했다. 다음 표는 KISC 허니넷에서 집계한 전 세계 악성 봇 감염 대비 국내 감염 비율이다.

	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	연평균
국내 감염률	13.7%	13.0%	11.9%	11.6%	10.8%	10.2%	10.1%	9.4%	11.4%	11.7%	9.5%	12.4%	11.3%

▲ 전세계 악성 봇 감염 대비 국내 감염 비율

KISC는 악성 봇 감염 피해를 줄이기 위해 2005년도부터 국내 ISP 및 IDC 사업자, 해외 관련 기관들과 악성 봇 대응을 위한 협조 체계를 구축·운영하고 있다. 일례로 국내 ISP사업자에게는 악성 봇 C&C 서버 정보와 봇 감염 IP 리스트를 일일 단위로 전달해 차단요청을 하고 있으며, 악성 봇 감염 시스템이 봇 C&C 서버로 접속하는 것을 막기 위한 'DNS 싱크홀(Sinkhole)'을 운영하는 등 적극적으로 대응하고 있다. 국내 주요 ISP들 뿐만 아니라 대학 등 DNS 싱크홀 적용기관을 확대하고 있으며, 향후 이를 통해 악성 봇 감염률을 좀 더 낮출 수 있을 것으로 기대된다.

한편, 2007년 악성 봇의 가장 두드러진 특징은 악성 봇을 이용한 랜섬형 DDoS 공격의 증가라고 할 수 있다. 2007년 10월 특정 기업의 홈페이지를 대상으로 DDoS 공격을 감행하는 것이 확인됐는데, 이 공격에 사용된 악성코드는 기존의 게임 아이템 탈취를 위한 트로이잔의 유포 특징과 유사하지만 HTTP에 기반한 악성 봇의 특징을 확연히 보여주고 있다. 이 같은 방식은 기존의 취약점 스캔에 의한 봇 확산과 달리, 네트워크 트래픽을 증가시키지 않아 은밀한 확산이 가능하며 적은 감염 PC 대수로도 공격이 손쉽게 이뤄질 수 있어 향후 DDoS 공격용 악성 봇 등의 확산에 많이 악용될 것으로 예측된다. 또 다른 특징으로 악성 봇에 대한 분석이 어렵도록 분석 회피 기술이 적극적으로 활용되기 시작했다는 점을 꼽을 수 있다.

2008년 악성 봇 전망

2008년 악성 봇은 지난해와 마찬가지로 홈페이지와 같은 악성코드 유포지를 통한 다운로드 사례가 더욱 증가할 것으로 보인다. 특히 구체적인 악성 봇의 확산방법으로는 기존 IRC 기반의 악성 봇보다 웹을 이용한 HTTP 기반의 악성 봇이 더욱 증가하고 DNS 싱크홀과 같은 중앙 서버로의 연결을 차단하는 방법을 우회할 수 있는 P2P 봇의 증가가 예상된다.

특히, 봇의 발견과 분석을 어렵게 하기 위해 변형 및 암호화하거나 백신과 같은 보안제품의 실행을 막고, 가상환경에서 제대로 동작하지 못하게 하는 분석회피 기술이 더욱 발전할 것으로 보인다. 여기에 2007년 발생한 사고들처럼 특정 목적을 위한 수단으로 사용되는 봇넷[2]의 사례가 더욱 증가할 것으로 예상되며, 금전적 이득

을 목적으로 한 DDoS 공격, 게임 아이템 등의 탈취를 위한 개인정보 습득 등의 범죄가 2008년에도 더욱 증가할 것으로 예상된다.

2007년 피싱 사고 동향 및 2008년 전망

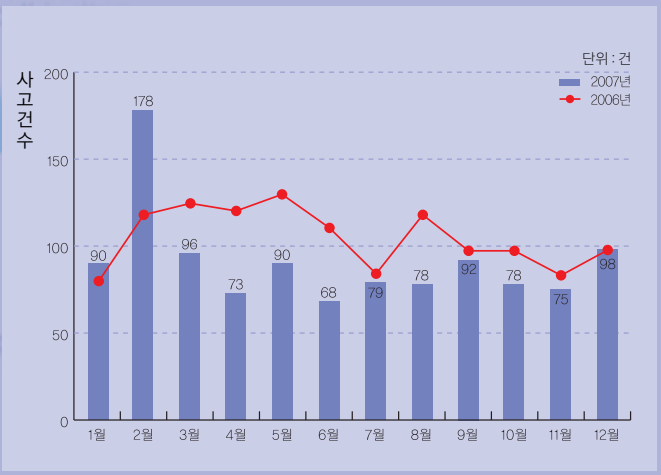
2007년 1월 국내 은행 두 곳을 사칭한 피싱 사이트 개설 및 악성코드 유포를 통해 공인증서, 일부 금융정보가 유출되는 사고가 발생해 지난 2007년 정부와 금융기관 및 보안업계가 이에 대한 대책 마련에 고심했던 한 해이기도 하다.

2007년 피싱사고 동향

국제 피싱대응협의체 APWG(Anti-Phishing Working Group)에 따르면, 2007년 월 평균 피싱 사이트 수는 31,160건으로 2006년 대비 약 2배 증가한 것으로 나타났다. 미국, 영국, 캐나다, 호주, 독일, 이탈리아 등이 주요 사칭 대상 기관이 소속된 국가인 것으로 나타났으며, 그 가운데 미국은 2007년 피싱에 의한 피해규모가 약 30억 달러에 이르는 것으로 나타났다.

이와 달리, 국내에서는 기관 사칭 피싱사고 2건, 피싱경유지 사고 1,095건이 발생, 지난 2006년에 비해 감소한 것으로 나타났다. 피싱사고 유형은 지난 2006년과 유사했지만 악성코드와 결합한 호스트 단위의 파밍 기법이 국내에 등장했다는 점이 가장 큰 특징이었다.

지난 2007년 1월 발생한 은행 사칭 피싱사고는 국내에서 첫번째로 기록된 파밍 기법을 이용한 피싱사고였는데, 당시 사건은 Window XP의 취약점을 가진 PC를 감염시켜 공인인증서를 유출하고 Hosts 파일을 변조시켜 특정 은행 홈페이지 주소가 입력되면 자동으로 피싱 사이트로 접속시키는 형태였다.



▲ 2006년·2007년 피싱경유지 사고 현황

한편, 1,095건이 접수된 피싱 경유지 사고를 분석해 본 결과, 피싱 사이트 개설에 이용된 포트 및 사칭대상 기관이 매우 다양하게 나타났다. 경유지 사이트 개설에 이용된 포트는 TCP/80 포트가 86.2%로 대부분을 차지했으며, TCP/84포트, TCP/8080 등을 포함해 총 21개의 포트가 악용됐다.

2008년 피싱 전망

국제적으로 2008년 피싱사고는 증가추세가 이어질 것으로 예상되며, 국내 피싱경유지 사고도 2007년과 비슷한 수준이 될 것으로 보인다. 그 원인은 피싱이 상업적 이익을 노리는 해커들의 공격성향과 맞아떨어지는 반면, 피싱에 대응하기 위해서는 금융, 전자상거래, 온라인게임 등의 분야에서 기술적 보안대책 뿐만 아니라 사람을 속이는 사회공학적인 요소까지 반영된 대안이 마련되어야 하는 등 단시간 내 해결하기가 쉽지 않기 때문이다.

반면, 국내 기관을 사칭한 피싱사고의 발생 가능성은 낮아질 것으로 생각된다. 국내 은행, 게임, 포털 업체 등에서는 이미 OTP, 안티피싱 기능, PC 등록제, 보안 로그인 등 보안 서비스 도입 및 처리 매커니즘이 강화돼 일부 정보가 유출되더라도 금전적 피해로 이어지기는 더욱 어렵기 때문이다. 다만, 피싱만을 위한 개별적인 대응이 아닌 악성코드, 웜·바이러스, 봇 등을 포함하는 통합적인 대응이 필요할 것으로 생각된다.

2007년 홈페이지 해킹동향 및 2008년 전망

지난 해 국내에서는 많은 홈페이지가 공격을 당하고 악성코드가 삽입되는 사고가 광범위하게 발생된 것처럼, 홈페이지 해킹은 그 자체가 최종 목적이 아닌 악성코드 삽입, 홈페이지에서 보유하는 개인정보 탈취 등을 위한 중간 공격 형태로 발전됐다. 이런 공격은 결국 금전적 이익을 위한 악의적인 해킹으로 이어지고 있는 실정이다.

2007년 홈페이지 해킹사고 동향

2007년 한 해 동안 많은 홈페이지가 공격을 당하고 악성코드가 삽입되는 해킹사고가 광범위하게 발생됐다. 이제 홈페이지 해킹은 악성코드 삽입, 홈페이지가 보유한 개인정보 탈취 등을 위한 중간 공격의 형태로 발전되고 있다. 홈페이지 해킹을 통해 유포되는 악성코드의 종류도 초기 게임 아이템 유출을 위한 트로이잔에서 다른 악성코드를 다운로드하기 위한 다운로더 종류, 특정 사이트에 대한 공격을 위한 DDoS 공격도구 등으로 변화하고 있다. 이와 같이 홈페이지 해킹은 운영체제나 네트워크 취약점의 공격이 어려워진 상황에서 응용 프로그램의 취약점을 악용하는 방식으로 공격 방법이 옮겨지고 있기 때문으로, 이런 공격 형태는 당분간 지속적으로 증가할 것으로 예측된다.

구분	2006년 총계	2007년												2007년 총계
		1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	
피해 홈페이지 수	3,206	289	148	63	89	145	305	485	125	236	116	177	117	2,293
피해 시스템 수	1,047	95	80	37	29	45	35	96	64	130	72	93	52	828

▲ 2007년 홈페이지 변조 사고 현황

구분	2006년 총계	2007년												2007년 총계
		1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	
유포지	993	108	90	126	190	146	113	120	88	102	152	228	156	1,619
경유지	5,624	372	307	349	315	283	374	338	196	132	386	411	469	3,932
합계	6,617	480	397	475	505	429	487	458	284	234	538	639	625	5,551

▲ 2007년 홈페이지 악성코드 은닉사고 현황

2008년 홈페이지 해킹전망

앞서 설명한 것처럼 금전적 이익을 목적으로 한 해킹이 증가하면서 홈페이지 해킹은 하나의 수단으로 변화되고 있다. 현재까지 홈페이지를 해킹하는 가장 큰 목적은 악성코드 삽입으로 판단되며, 분산 서비스거부 공격을 수행하여 금전적 이득을 취득하는 사례도 증가하고 있다. 피해를 차단하기 위해서 홈페이지에 대한 보안성을

강화해야 한다. 특히 게시판의 파일 업로드/다운로드 기능은 악성코드를 서버에 업로드 할 수 있도록 하기 때문에 해당 기능의 보안기능을 강화해야 한다.

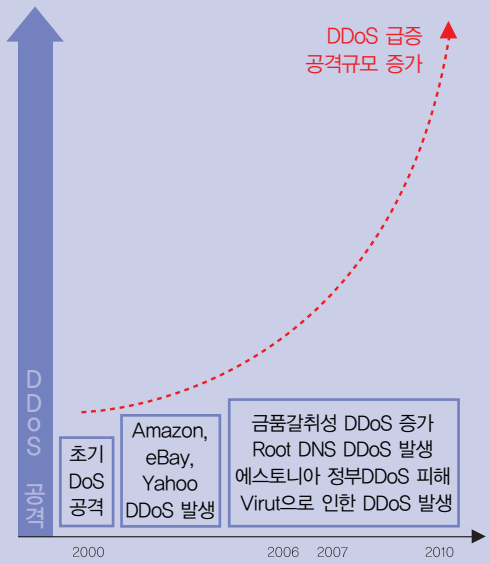
한편, 2007년 하반기에 수집된 ARP 공격도구는 키워드를 기반으로 해 특정 문자열을 수집할 수 있는 기능이 존재하며 이 기능을 악용할 경우, 사용자의 아이디 및 비밀번호의 획득이 매우 손쉽게 진행될 수 있어, 2008년에는 관리자들이 ARP 공격에 대해서 많은 대비를 해야 할 것으로 보인다.

2007년 DDoS 공격 동향 및 2008년 전망

2007년에는 홈페이지 해킹, 웜 바이러스 등 다른 유형의 침해사고 보다 분산 서비스 거부공격이 가장 큰 이슈가 됐던 해였다. 이들 공격자들은 서비스 기업에게 금품을 요구하고 협박해 많은 문제를 일으켰으며 초기와 달리, 공격 대상 웹 사이트이 다양화되고 있고, 공격에 악용되는 좀비 PC 감염 수단도 다양화되고 있다.

2007년 DDoS 공격동향

지난 2007년에는 그 어느 때보다 분산 서비스 거부공격(DDoS)이 이슈가 됐던 해이다. DDoS 공격은 대규모 유해 트래픽을 일시에 유입시켜 서비스를 마비시키는 그 특성 상 사전에 탐지하기 어렵고, 효율적인 방어가 어렵다는 문제가 있다.



- 2007년 9월~10월
  게임아이템거래사이트에 대한 금품요구
  트래픽 규모 : 수 Gbps~15Gbps
- 2007년 9월
  Virut 바이러스에 의한 e-gold.com 공격
- 2007년 6월~8월
  여행업, 팬션예약 사이트 등에 대한 금품요구
- 2007년 5월
  에스토니아 정부 및 국회 등의 사이트가 DDoS 공격에 피해
- 2007년 2월
  루트 DNS 6개가 Virut으로 인한 DDoS 공격 피해
- 2007년 1월
  도메인 등록대행사 사이트에 대한 DDoS 공격
- 2006년 11월
  미국 특정 IP에 대한 공격(일부 IDC 부분장애)
- 2006년 10월~11월
  성인 화상 채팅사이트에 대한 금품요구

▲ 최근 주요 DDoS 공격 사례

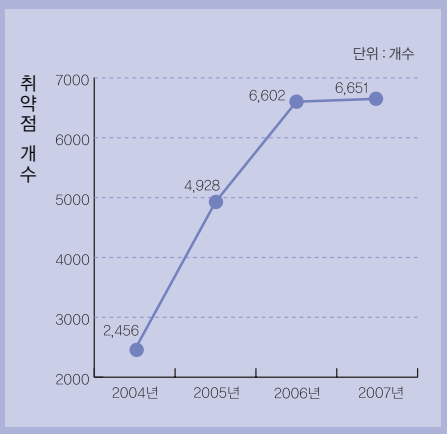
KISC에서는 2007년에 발생했던 주요 DDoS 공격 발생시 공격명령을 전달하는 명령/제어 서버를 찾아 해당 서버 접속을 차단해 왔지만, 현실적으로 악성코드 변종이 너무나 많고 또 악성코드 샘플 채취를 위해 일반가정과 소규모 업체에 협조를 구해야 하기 때문에 신속한 대응에 많은 어려움이 있었다. 이런 어려움을 감안할 때

DDoS 공격에 대한 가장 효과적인 방어는 예방이라고 할 수 있다. 즉, 보안이 취약해 악성코드에 감염된 후 DDoS 공격 근원지로 악용되는 국내 좀비 PC의 수를 최소화하는 것이 DDoS를 포함한 각종 침해사고에 대한 가장 효과적이고, 효율적인 방법이라고 생각된다. 특히 PC 1대가 수십 Mbps까지 트래픽을 유발할 수 있는 국내 인터넷 환경을 감안해 볼 때 국내 좀비 PC의 보안조치는 필수적이라고 판단된다.

2008년 DDoS 공격전망

2008년에도 금품을 요구하는 협박성 DDoS 공격은 지속적으로 증가할 것으로 예상된다. 하지만 소규모 업체를 공격대상으로 삼았던 것과 달리, 그 대상이 일반 유명 웹 사이트로 확대될 것으로 보인다. 한편, DDoS 공격에 이용되는 좀비 PC를 감염시키는 수단으로는 웹 사이트가 가장 보편적이었지만 2008년도에는 이메일, 메신저, P2P 등 웜 · 바이러스 전파수단이 좀비 PC 확보 수단으로 다시 악용될 가능성이 높다. 또한 최근 관심사가 되고 있는 인터넷 TV, 인터넷 전화 서비스를 타깃으로 한 분산 서비스 거부 공격도 출현할 수 있을 것으로 보인다.

2007년 보안 취약점 현황



▲ 2007년 취약점 증가 추이
(출처: http://nvd.nist.gov/statistics.cfm)

2007년 CVE(Common Vulnerabilities and Exposures)에 등록된 보안 취약점의 개수는 전년도와 유사한 수준을 유지했다. 그 가운데 웹 페이지 상에서 공격당할 수 있는 윈도우즈 애니메이션 커서 취약점(ANI 취약점)이 주요 이슈가 됐고, Office 관련 취약점은 지난해와 유사한 비중을 차지했다. 또한, MS 제품에 대한 제로데이 취약점은 2006년과 같은 수치(18건)를 나타났다.2008년도는 2007년과 마찬가지로 사용자 개입이 필요한 공격방식이 주를 이룰 것으로 예상되는 가운데, 이에 따라 Office와 인터넷 익스플로러가 주공격 대상이 될 것으로 예상된다. 또한 MS의 새로운 서버 운영체제인 윈도우즈 2008이 출시됨에 따라 새로운 운영체제를 대상으로 하는 취약점 발생에 주의를 기울일 필요가 있다.

2007년 등장한 취약점 분석 결과, 응용 프로그램 즉, 사용자의 동작이 개입되는 공격형태가 주를 이루고 있어 어느 때보다 개인 PC에 대한 보안이 중요시 되는 한 해였다. 따라서 MS 및 Apple 운영체제 이용자들은 항상 최신 보안 업데이트를 유지하고 백신, 방화벽 등 부가적인 보안장비를 적극적으로 활용할 필요가 있으며, 또한 의심스러운 메일 및 파일을 삭제하고 신뢰할 수 있는 웹사이트만 방문하는 정보보호 실천수칙 준수가 필요하다.

click 보안용어!

1 트로이잔(Trojan) : 자기복제 능력은 없으나 정상기능의 프로그램으로 가장하여 프로그램 내에 숨어 있는 코드조각으로 의도하지 않은 기능을 수행하는 컴퓨터 프로그램 또는 실행 가능한 코드

2 봇 넷(BotNet) : 많은 Bot 감염 시스템들이 명령을 수신할 목적으로 IRC에 연결되어 있는 네트워크