# 2009년에는 어떤 일들이 일어날까

## -2008년 침해사고 동향 및 2009년 전망

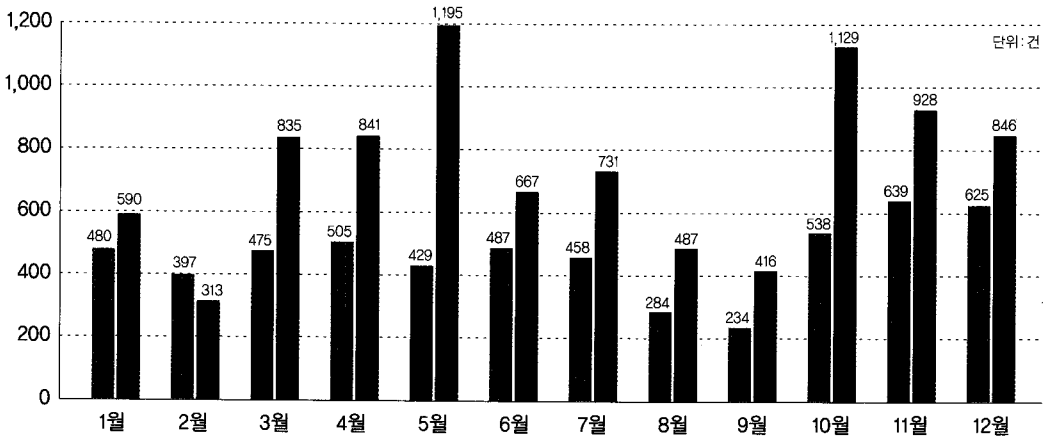
KISA 인터넷침해사고대응지원센터가 지난 1월 '2008년 침해사고 동향 및 2009년 전망'을 발표했다. 침해사고 동향을 분석하고 향후 등장할 위협을 예측하는 이 보고서는 국내외 정보보호 분야의 기술 지형을 한눈에 보여준다는 점에서 큰 의미를 지니고 있다. 웜·바이러스와 악성 봇 분야의 주요내용을 중심으로 2008년 침해사고 동향과 2009년을 전망해 본다.

글 박진완 | 상환관제팀 선임연구원_jwpark@kisa.or.kr

## 2007년 피해유형의 지속, 확대 : 2008년 웜 · 바이러스 동향

2008년 역시 많은 신·변종이 출연한 웜은 분산서비스거부공격(DDoS), 정보유출 등 사이버 침해사고의 주요 공격수단으로 악용됐으며, 대응 및 치료를 점점 더 어렵게 하기 위해 진화·발전하고 있다.

2007년에 이어 2008년에도 ARP 스푸핑(Spoofing) 및 이동식 저장매체를 통한 악성코드 감염 등의 피해가 지속적으로 발생했으며 홈페이지 악성코드 은닉사고의 경우, 2007년 대비 62% 가까이 증가했다. 이런 악성코드는 주로 온라인 게임정보 등 개인정보 유출, 스팸성 메일 발송, DDoS 공격 및 허위백신을 통한 결제 유도 등 궁극적으로 금전 획득을 목적으로 유포되는 것으로 확인됐다.




2008년 악성코드 은닉사고 처리건수 그림 1

자동화된 도구를 통한 대량의 악성코드 및 손쉬운 변종 제작이 가능해짐과 동시에 ARP 스푸핑을 위한 간단한 공격코드를 이용해 해당 클라이언트 서브넷(Subnet) 또는 서버군 서브넷 시스템을 공격하는 한편, 원격명령전달 서버와의 통신방식이 기존 서버/클라이언트 방식에서 P2P 방식으로 변화하는 등 공격기술 또한 지속적으로 진화했다. 여기에 MS Office, Acrobat 등 복합적 전파경로의 확대로 공격 성공 가능성이 높아지고 자기 은폐기술의 진화 등 생존력을 높이기 위한 기술이 적용돼 점차 대응 및 치료를 어렵게 만들고 있다.

## 2009년 웜 · 바이러스는

2008년 동향을 토대로 2009년을 예측해 본다면, 역시 금전적 이득을 위한 악성코드 감염사례가 지속적으로 증가할 것으로 예상된다. 특히, 광케이블, FTTH 환경 등 인터넷 대역폭이 크게 확장됨에 따라 DDoS 공격의 영향력은 더욱 증가할 것이며, 그 대상은 금융, 전자상거래 등 다양한 사이트를 대상으로 더욱 확대될 것으로 보인다. 또한 운영체제보다는 상대적으로 패치에 대한 관심이 적은 문서 파일 애플리케이션 취약점이 악성코드 전파경로로 많이 악용될 것으로 예상되며, 메일첨부 등을 통해 특정인을 대상으로 한 공격이 2009년에도 많이 발생할 것으로 보인다.

한편, 악성코드 제작자들은 감염성공률을 높이기 위해 알려지지 않은 취약점을 악성코드 전파경로로 악용하는 사례가 증가할 것이며, 악성코드의 생존력을 높이기 위한 HTTP와 P2P 통신방식, 그리고 자기은폐기능이 구현된 악성코드는 더욱 많아질 것이다. 이밖에도 위피(WiPi) 의무탑재가 없어짐에 따라, 외산 스마트폰에서 발생한 모바일 악성코드가 국내로 유입될 가능성이 증대되고 있다.

## Netbot에 의한 DDoS 공격 : 2008년 악성 봇 동향

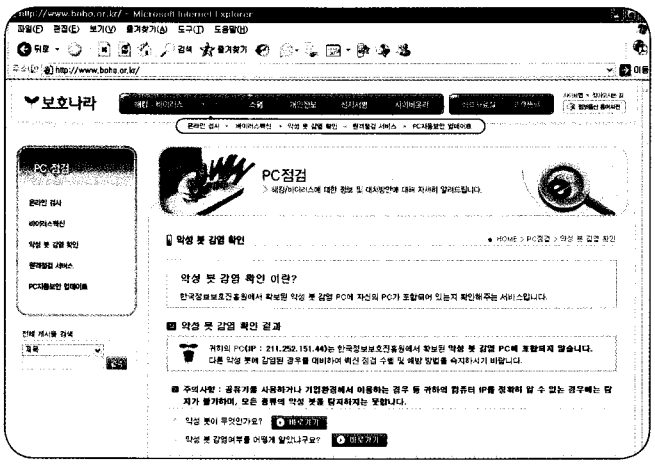
KISA 허니넷 트래픽을 통해 추정한 2008년 전세계 악성 봇 감염 대비 국내 감염률은 평균 8.1%로 2007년 11.3%에 비해 감소했다. 11월부터는 MS Windows 취약점인 MS08-067의 영향으로 TCP/445 트래픽의 유입이 증가했지만, 국내의 많은 ISP에서 TCP/445 트래픽을 차단하고 있어 국외 IP로부터의 트래픽 유입만이 크게 증가했을 뿐 이로 인한 악성 봇 감염율은 감소되는 효과가 나타났다.

최근 국내에서 발생한 DDoS 공격은 Netbot에 의해 주로 이뤄지고 있는 것으로 파악되고 있다. Netbot은 자기전파 기능이 없는 대신, 악성코드 링크가 은닉된 홈페이지 및 국내 포털 카페 등을 통해 전파되고 있는 것으로 추정되며, Netbot 프로그램이 인터넷을 통해 저렴한 금액으로 거래되고 있어 많은 해커들이 손쉽게 사용하고 있는 것으로 보인다.

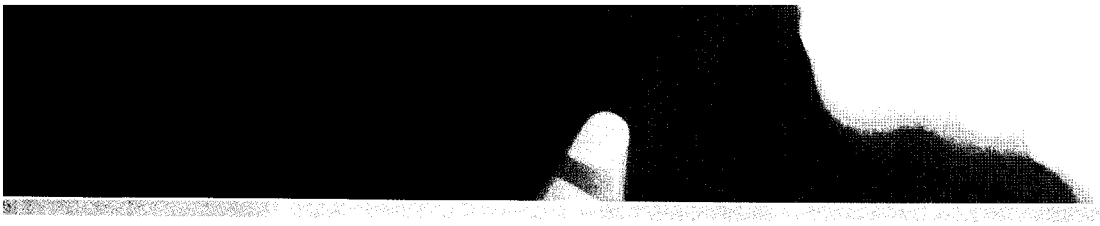
하지만 여전히 IRC 기반의 악성 봇도 활동을 하고 있으며 국내외에서는 지속적으로 악성 봇 명령/제어 서버가 나타나고 있다. 이런 악성 봇 명령/제어 서버는 보안 취약점이 존재하는 상태로 웹쉘 등 다양한 해킹 도구를 통해 해커에 의해 원격제어 당할 수 있으나 해당 서버 자체에 영향을 미치는 악성행위는 거의 없어 서버 관리자라 할지라도 해킹 여부를 확인하기 어려운 실정이다.

## 2009년 악성 봇은

조지아공과대 정보보호센터(GTISC)에서 발표한 자료에 따르면, 2009년 기업 및 일반 사용자가 직면할 주요 사이버 위협으로 '악성프로그램', 'Botnet', '사이버전쟁', 'VoIP 및 무선기기에 대한 위협', '사이버 경제의 진화' 등 5가지를 꼽았다. 기존의 악성 프로그램과 Botnet 뿐만 아니라 사이버전쟁 역시 실제로 발생하였는데, 에스토니아 정부 사이트에 대한 DDoS 공격과 러시아-그루지아 간 사이버 전쟁이 그 예이다. 이처럼 해킹은 단순 실력과시와 금전적 이득을 위한 해킹을 넘어 정치적 목적의 해킹까지도 발생하고 있고, 향후에도 이런 해킹이 지속적으로 발생할 가능성이 있다. 또한 휴대전화가 경량화, 고성능화되면서 DDoS나 Botnet이 휴대전화기기에서 발생하는 날도 머지않아 등장할 것으로 보인다. 국내의 경우 휴대전화를 통해 인터넷 뱅킹을 이용하는 사례가 늘고 있어 모바일 보안에 대한 새로운 접근방법이 요구된다.




악성 봇 감염 확인 홈페이지 그림 2



악성 봇에 대응하기 위해 KISA는 기존에 운영해 온 악성 봇 DNS 싱크홀을 ISP 뿐만 아니라, 대학이나 일반 기업으로 그 적용범위를 2008년부터 확대했으며, 2009년에도 지속적인 홍보활동을 통해 보다 많은 기관에서 DNS 싱크홀을 적용하도록 유도할 계획이다. 하지만 악성 봇에 대응하기 위해서는 일반 PC 사용자의 적극적인 동참이 수반되어야 한다. 이를 위해 KISA는 DNS 싱크홀을 통해 확보된 악성 봇 감염 시스템을 사용자들이 직접 확인할 수 있는 '악성 봇 감염확인 서비스'를 시작했으며, 악성 봇 감염이 확인되지 않은 경우에도 악성 봇 및 악성 봇 감염 PC 확인 시스템의 동작원리/예방방법을 안내함으로써 향후에도 악성 봇 감염에 대해 대비할 수 있도록 지원하고 있다.

## 조직적 사이버 범죄 심화 : 2008년 DDoS 공격 동향

최근 침해사고 경향을 언급함에 있어 누구든지 DDoS 공격을 빼놓지 않을 것이다. 그만큼 DDoS는 빈번히 발생하고 있으며 특히, 금품요구 목적의 협박성 DDoS 공격은 2008년 들어서도 게임, 쇼핑몰, 증권사 등 사회 전반의 모든 분야를 대상으로 확대돼 지속적으로 발생했다.

2008년 DDoS 공격의 두드러진 특징 가운데 하나는 보다 조직화된 사이버 범죄로 발전하고 있다는 것이다. 즉, DDoS 공격용 악성코드 제작자, 악성코드 유포자, 금품요구 및 협박자, DDoS 공격자 등 각기 고유한 역할을 가진 범죄자들이 은밀한 거래를 통해 조직화돼 있고, 일회성이 아닌 피해업체의 경제적 파급효과 및 고객사의 관계까지 감안해 공격대상을 선정하는 등 날로 지능화된 수법을 보이고 있다.

.
.
**만약시 잡힌다구 그래두 내 진공하는 기술자가 아이구**
**내느 돈 받아서 합의해주는 사람이길래 내 혹 잡히더래두 본질상**
**진공을 막을수 있는 방법은 아이라는거만 명심하쇼.**
.
.

협박 메일내용 일부 그림 3

## 2009년 DDoS 공격은

글로벌 경제위기와 더불어 2009년에도 금품 갈취성 DDoS 공격은 더욱 증가할 것으로 예상된다. 이제 'DDoS'라는 용어는 공중파 방송에도 자주 접할 수 있을 만큼 일반적이고 보편화된 용어가 되고 있다. 금품 갈취성 DDoS 공격 외에도 사이버 시위의 한 형태로써 사회적 갈등 표출형 DDoS 공격이 2009년에 나타날 가능성이 있다. S