인터넷 침해사고 동향 변화에 따른 대응 정책

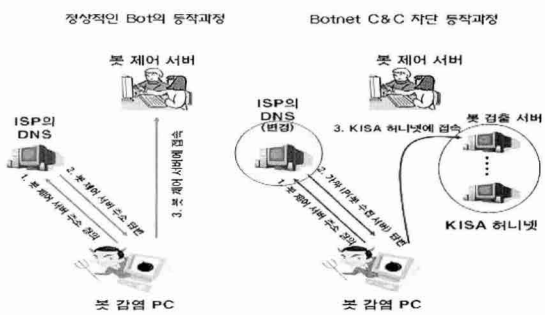
글 | 정보통신기반보호대응팀 연장길

4. 침해사고 대응기반 확대

1) 악성 Bot 차단활동

악성 Bot이란 웜 · 바이러스의 일종으로 인터넷상에서 MS 윈도우 취약점, 비밀번호의 취약성, 웜바이러스의 백도어 이용 등을 통해 유포된다. 기존 웜바이러스와는 달리 유포자의 제어 및 명령을 전달받아 수행한다는 점에서 더욱 위험하며, 유포자는 악성 Bot를 이용하여 여러 가지 악의적인 목적으로 사용하고 있다. 이러한 악성 Bot에 감염된 PC가 국내에 수 십만 여대에 이르는 것으로 추정되고 있으며, 외부 해커에 의해 일시에 특정 공격명령을 수행한다는 점에서 그 위험성은 매우 크다 할 수 있다.

KISA는 작년 7월부터 악성 Bot 명령/제어 서버로 악용되는 주소를 파악하여, ISP/IDC 협조로 Bot 감염 PC와 Bot 명령/제어 서버간 연결을 차단하고 있다. 현재 KT · 데이콤 · 하나로텔레콤 · 두루넷 · 드림라인 · 온세통신 · SK 네트웍스 · EPN · KIDC 등 9개 사업자 협조로 Bot 명령 서버에 대한 차단을 실시하고 있으며, 향후 케이블 인터넷사업자까지 확대 실시할 예정이다.



악성 Bot 동작 및 차단 과정

2) 국내 · 외 공조 모의훈련 실시

인터넷은 범세계적으로 그물망으로 연결되어 있으며, 해가 거듭할수록 고속화되어 가고 있다. 이러한 인터넷 환경에서 발생하는 침해사고는 한 나라만의 문제가 아닌 범세계적인 문제이며, 인터넷 침해사고 피해의 최소화는 대응 능력의 신속 · 정확성에 의해 결정된다.

정보통신부에서는 ISP · IDC · 보안업체 등 국내유관기관과 공동으로 최신 해킹기법을 적용한 모의훈련을 실시함으로써 유사시 대응능력을 제고하고, 국외 유관과의 국제 모의훈련을 통하여 국제공조체제를 강화하고자 한다.

이에 연간 총 5차례에 걸쳐 사이버공격에 대비한 모의훈련을 실시한다.

즉, 자체 훈련 2회(3월, 9월), ISP공동훈련 1회(6월), 을지훈련(8월), 국제 공동 모의훈련(12월)이 실시된다.

특히, 국제 모의 훈련은 주변 국가뿐만 아니라 유럽 국가까지 포함하는 글로벌 침해사고 모의훈련이 될 전망이다.

3) CERT 활동 지원 강화

CERT, 민 · 관합동조사단 및 대학 정보보호 동아리 등 침해사고 관련 유관기관 지원을 위한 세미나를 개최하고, 대학 CERT 및 해킹 동아리에 대한 지원을 강화하여 정보보호 전문인력 저변 확대 및 정보보호 인식 확산을 추진한다.

또한, 최신 해킹기법에 관한 '침해사고 분석 절차 가이드' 등을 제작 · 배포하여 중소기업 해킹 대응능력을 제고할 계획이다.

III. 결 론

바야흐로 우리나라는 초고속 인터넷 보급률 세계 1위를 자랑하는 인터넷 강국으로 그 위상을 돈독히 하였다. 그러나 그 위상이 높으면 높을수록 그 그늘도 짓게 드리우고 있는 것 또한 현실이다. 정보화와 정보보호는 떨어질 수 없는 동전의 앞뒷면과 같은 것이다.

정보보호를 배제한 정보화는 사상누각으로 언제 무너질지 장담 못하며, 오히려 정보화가 우리에게 위해가 될 수 있다는 점에서 정보보호의 중요성은 아무리 강조하여도 지나치지 않다. 특히 정보화 의존도가 높은 우리나라에서는 더욱 그러하다.

최근 들어 해킹 양상이 변화하고 있는 것은 여러 사례에서 밝혀진 바 있다. 단순한 호기심이나 공명심이 아니라 인터넷 침해행위를 통하여 실질적인 금전적 이득을 취하려는 경향이 두드러지게 나타나고 있으며, 더욱이 해킹 도구 습득의 용이성, 해킹 기법의 고도화 양상을 띠게 됨에 따라 대응이 점차 어려워지고 있다.

정통부에서는 이러한 해킹 경향을 면밀히 분석하여 관련기관/업체와의 긴밀한 협조 속에 민간부문의 해킹방지를 위해 노력할 것이다. 또한 가까운 미래에 다가올 차세대 네트워크에서 발생가능한 사이버 침해사고에 적극 대응하고자 한다.K

※알림※
이 원고는 2회에 걸쳐 연재되었으며, 첫 번째 원고는 정보화사회 05~06월호에 게재되었습니다.