한국, 코드레드 주 활동무대로 전락…피해 사상 최대

응급 대응체제 정비 · 철저한 보안 시스템 절실

지난 8월은 국내의 컴퓨터 사용자들을 공포로 몰고 간 날들이었다.

이는 바로 서캠(Sircam) 바이러스 폭풍의 여파가 채 가시기도 전에 강력한 바이러스인 코드레드(Code-Red) 바이러스의 위협에 의한 것이기 때문이다.

최근 들어 신종 바이러스의 종류는 눈에 띄게 줄어들고는 있는 실정이지만, 소수 바이러스에 의한 피해 사례는 급증하고 있어 컴퓨터 사용자들에게는 더더욱 공포의 대상이 된 것이다.

코드레드 바이러스는 지난 7월 19일 처음 배포된 이래 7월 20일 백악관에 분산서비스공격(DDoS)을 시도하면서 그 위험이 알려지기 시작했다. 그 후 7월 28일부터 31일까지 잠복기를 지닌 후 다 시 지난달 1일부터 활동이 시작되면서 3일 후 코드레드Ⅱ가 배포됐다.

국내에는 8월 6일 처음으로 코드레드Ⅱ에 의한 피해사례가 접수되면서 국내에서도 코드레드 바이러스 비상이 걸리기 시작했다. 이후 안철수연구소, 트렌드마이크로 등 많은 보안업체들이 앞 다투어 코드레드와 관련된 안티바이러스 제품을 내 놓기 시작했다.

코드레드의 감염 배경 및 증상

네트웍 전체 느려져…주변 서버까지 영향

코드레드의 감염 배경은 코드레드 및 코드레드Ⅱ가 메모리 상주형 웜으로서 MS IIS의 'Unchecked Buffer in Index Server ISAPI Extension(MS01-033)'의 취약점을 이용해 인터넷에 연결되어 있는 임의의 시스템으로 연결을 시도하여 MS IIS가 구동중인 윈도우 NT/2000에 감염되는 것이다.

코드레드Ⅱ는 코드레드와 동일한 방법으로 전파 · 감염되며 감염시 백도어 프로그램으로 'cmd.exe' 또는 'explorer.exe'를 설치하여 이 웜에 감염된 시스템을 외부에서 웹을 통해 원격제어를 통해 C, D 드라이버의 모든 내용을 복사 · 삭제 · 변조할 수 있도록 한다.

코드레드 및 코드레드Ⅱ 감염시 지속적으로 임의의 주소로 연결시도는 네트웍 패킷을 보내므로 분산 서비스 공격을 시도하는 것과 같은 결과가 나타난다.

코드레드의 일반적 특징은 네트워크 자체의 리소스를 많이 점유하기 때문에 패치가 설치된 서버일지라도 해당 네트워크가 느려지는 경향이 있다. 즉, 이는 서버A와 서버B가 동일 네트워크 세그먼트에 있다면 감염된 서버가 다른 쪽으로 propagation하기 위해서 수백 개의 thread를 만들게 되는 것이다. 그럴 경우 많은 네트워크 리소스를 사용해 네트워크 전체가 느려지기 때문에 감염이 안 된 서버까지도 영향을 받을 수 있는 것이다.

코드레드Ⅱ의 특징은 코드레드 변형으로 지난 8월 4일에 발견됐다. 코드레드와 같은 취약점을 이용하고 같은 방식으로 동작을 하지만, 이는 7월 11일에 발견된 코드레드의 변종이 아니고 새로 제작된 것이다.

원형과는 달리 백도어 트로이목마를 설치하는데, 설치 시점은 2002년 10월쯤이다. 원형은 메모리에만 존재해서 리부팅을 하면 사라졌으나, 코드레드Ⅱ는 리부팅하면 백도어와 레지스트리의 시작 시 가동값이 작동하면서 다시 살아나는 것이 특징이다.

같은 클래스 대역으로 범위를 좁혀서 접근하므로 비교적 은폐가 쉽고 메모리에 상주하여 리부팅 시 사라지나 시작 시 재실행된다, 백도어는 MS 보안패치와는 상관없이 윈도우 부팅할 때 자동 실행되기 때문에 패치해도 백도어로 활용될 수 있다.

즉, 코드레드Ⅱ 바이러스에 의해 생기는 현상은 네트워크 속도 저하와 웹서버 서비스 거부 현상, 시스템 재부팅, 기밀자료 유출, 주요 데이터 손실 등의 문제들이 발생한다.

이러한 코드레드Ⅱ 바이러스의 영향을 받는 시스템들은 감염 시스템으로 Window 2000과 Internet Information Server(IIS) 5.0이고, 피해 시스템으로는 Window NT 4.0, Cisco Router, 3Com CoreBuilder, HP JetDirect, Xylan

Omni Software, Telocity/Direct TV DSL Gateway 등 이다.

코드레드의 피해 현황

인터넷 역사상 최대 피해 액수 예상

코드레드의 피해현황은 지난 8월 14일 현재 안철수연구소 집계에 의하면 전세계 40만대 이상이 감염되었으며, 대만 30,000DSL 서비스 사용자가 감염되었고, 현재 20억불 이상 피해가 예상되었다. 이에 대해 이번 코드레드 피해액수는 향후 인터넷 역사상 최대 피해액수로 집계될 것이라고 예상했다.

국내 피해규모로는 한국이 최대 위험지역으로 분류되면서, 14일 현재 14,000여 기관 4만3천2백여대가 감염됐다고 밝혔다.

또한 한국정보보호진흥원이 발표한 자료에 의하면 윈도 NT와 윈도 2000 시스템을 공격한 코드레드 웜의 대량유포에도 불구하고 7월 한달 동안 침해사고 접수건수는 6월의 432건에 비해 15.7% 감소한 370건으로 나타났다. 이 같은 감소에 대해 이 보고서는 해당 시스템 관리자들이 코드레드 웜의 공격사실을 인지하지 못했거나 인지하고 있어도 시스템 리부팅 후 별다른 보안조치를 강구하지 않았기 때문인 것으로 추정했다.

7월에 접수된 침해사고 분석 결과 해커들의 해킹 수법은 취약점 정보수집이 226건으로 가장 많았고, 다음으로 코드레드 웜 · 백오피스 등 악성코드 이용이 65건, 버퍼오버플 취약점 이용이 29건, 사용자 도용이 23건 등의 순으로 분석됐다.

또한 가장 많은 피해를 본 운용체계는 리눅스가 167건으로 나타났으며, 다음이 윈도 95 · 98이 73건으로 윈도 NT · 2000이 39건으로 나타났다.

그러나 몇몇 관계자에 의하면 현지 실제 피해 현황은 이보다 몇 배가 더 높은 것으로 추정되고 있으며, 현제 IDC업체나 ISP, 민간기업들이 코드레드 피해 신고 건수에 대해 숨긴다는 의문이 제기되고 있다.

예방 및 피해 복구 요령

미온 대응 시 피해 확산…2차 역습 우려

코드래드에 감염되는 것을 지속적으로 방지하기 위해서는 아래와 같은 사이트를 통해 프로그램을 다운받아 보안패치를 해야 한다.

Windows NT 4.0 사용기관은 http://www.microsoft.com/korea/technet/security/bulletin/downloads/MS01-033/korq300972i.exe

Windows 2000 Professional, Server와 Advanced Server는 http://www.microsoft.com/korea/technet/security/bulletin/downloads/MS01-033 /q300972_w2k_sp3_x86_ko.exe 에서 다운 받아 보안패치를 하면 된다.

Windows 2000 Datacenter Server는 OEM 업체로부터 프로그램을 입수하여 보안조치를 취한 후 개발된 백신을 통해 치료하거나 다음과 같은 요령으로 복구해야 한다.

감염된 시스템의 복구 방법은 이전 코드레드 버전에서는 시스템 패치 후 리부팅만 하면 끝났지만, 새로운 버전에서는 시스템에 생성된 트로이목마나 백도어들을 찾아서 제거가 필요하다.

우선 첫 번째로 root.exe 파일을 삭제한다. "\inetpub\scripts"와 "\program files\common files\system\msadc" 디렉토리에 root.exe가 생성되므로 이를 제거해야 한다.

두번째로 C: 나 D: 의 루트 디렉토리에서 트로이목마 버젼의 Explorer.exe를 제거한다. 세 번째로는 아래와 같이 감염된 시스템의 레지스트리 변경시키므로 이를 복구해야 한다.

HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\VirtualRoots에서 키를 추가하고, HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\WinlogonSFCDisable 키가 0xFFFFFF9D으로 수정해야 한다.

정보통신부는 이에 대해 향후 ISP 및 IDC 입주업체나 서비스 이용기관에 대한 예방 및 대응방법을 홍보하고 기술 지원을 할 것이며, IDC에서는 입주업체에 대한 코드레드 웜공격에 이용되는 IIS 웹서버 취약점을 점검하고, 보안패치가 되지 않은 업체에 대한 필요한 조치를 지원하기로 했다.

또한 갑자기 네트워크 부하로 인한 서비스 마비에 대한 사전 대책을 마련할 방침이다.

일반 정보통신망 및 정보시스템 운영기관에는 윈도우 NT/2000 IIS 웹서버가 없는 경우에도 코드레드 웜에 해킹당한 시스템에 의하여 지속적인 공격시도로 인하여 네트워크에 부하가 발생할 가능성이 있으므로 일시적으로 웹서비스를 중단하고, 침입탐지시스템, 침입차단시스템 등에서는 탐지 패턴을 최신버전으로 갱신하여 탐지하고, 기타 라우터 로그, 웹서버 로그 등을 통하여 공격을 탐지하라고 권고하고 있다.