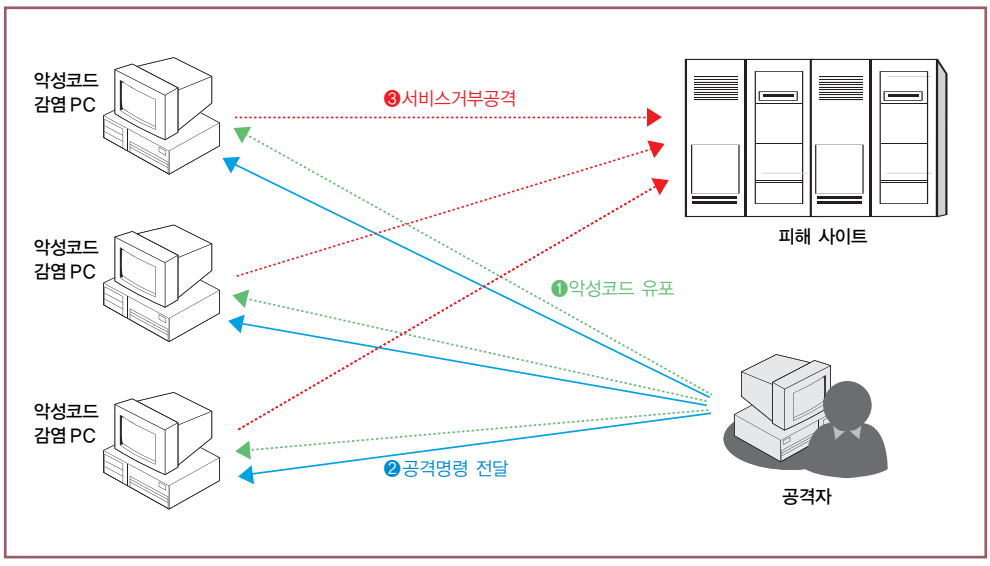
아이템 거래 사이트 대상 DDoS 공격 사례

지난 2007년부터 등장한 공격유형 중 게임 아이템 거래 사이트를 대상으로 이뤄진 분산서비스거부공격은 금품을 요구하는 공격의 한 유형으로 적지 않은 사례가 발견됐다. 흔히 DDoS(Distribute Denial of Service)로 불리는 분산서비스거부공격은 공격의 대상이 되는 서버에 서비스 장애를 발생시킬 뿐만 아니라, 네트워크의 안정성에도 위협이 되고 있으므로 각별한 주의가 필요하다. 본 기고에 소개되는 사례는 악성코드 Anti.exe 및 Down(1).exe를 국내 인터넷 사용 PC에 몰래 설치해 DDoS를 위한 에이전트로 악용, 국내 게임 아이템 거래 사이트에 대량의 트래픽을 발생시켜 서비스 장애를 유발시킨 사고로, DDoS 기능 이외에도 시스템 제어 등의 기능이 구현됐던 것으로 확인됐다.

최중섭 해킹대응팀 팀장(jschoi@kisa.or.kr)

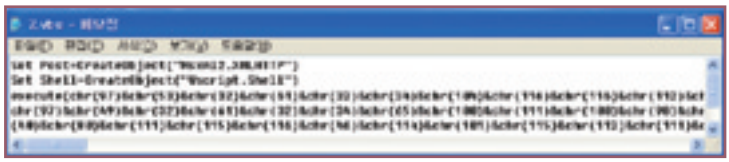
게임 아이템 거래업체에 대한 DDoS 공격기법 분석

우선 DDoS 공격을 위해 공격자는 다수의 사용자 PC를 악성코드에 감염시킨 후, 원격에서 공격명령을 전달하는 등 특정 사이트에 대한 DDoS 공격을 수행하도록 하는 방법을 이용했다. DDoS 트래픽을 발생시켰던 PC를 추적해 확인한 결과, 해당 PC는 Anti.exe에 감염돼 있었으며, 일부 PC에서는 Down(1).exe라는 파일명의 악성코드에도 감염돼 있었다. 이들 악성코드는 DDoS 공격을 위한 기능이 구현돼 있었던 것으로 확인됐다.



▲ 그림 1. 인터넷 사용자 PC를 이용한 DDoS 공격

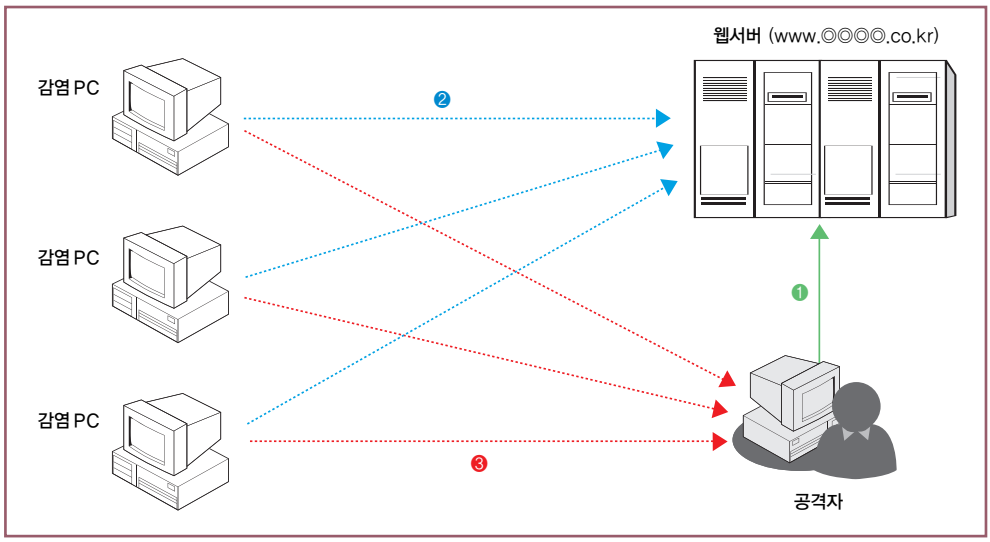
PC를 악성코드에 감염시키기 위해 공격자는 웹 사이트 또는 P2P 등을 이용했을 것으로 추정되며, 그림 2처럼 실제로 악성코드가 설치돼 있는 PC에서 Anti.exe 악성코드 설치를 위한 2.vbs 파일이 발견됐다.



◀ 그림 2. 2.vbs 파일의 예

공격코드 Anti.exe 분석

Anti.exe 악성코드는 원격명령 전달을 통해 DDoS 공격을 수행할 수 있는 기능이 있었으며, 기타 정보 유출 및 원격통제 기능도 확인됐다. 특히 공격자는 추적을 피하기 위해 특정 웹 서버를 이용, 원격명령 전달을 위한 서버 IP 주소를 주기적으로 변경하는 치밀함까지 보였다.



▲ 그림 3. 감염 PC 원격통제 방법

❶ 공격자는 http://www.○○○○.co.kr/ip.txt에 감염 PC를 통제할 공격자 IP 주소를 올려놓는다.

❷ 감염이 되면 Anti.exe는 http://www.○○○○.co.kr/ip.txt에 접속해 원격 공격자의 IP 주소와 포트 정보를 받아온다.

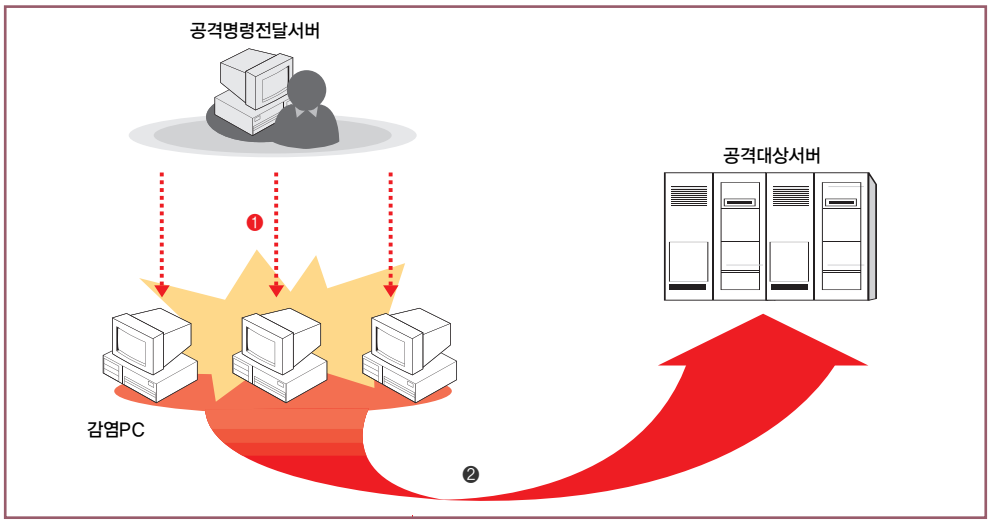
❸ Anti.exe는 수신한 사이트 주소를 확인한 후 해당 주소로 접속해 공격자의 원격통제를 받는다.

※ 피해 접수 당시 인터넷침해사고대응지원센터에서는 피해예방을 위해 해당주소의 ip.txt 파일을 제거하는 조치를 취했다.

사용자의 PC가 감염될 경우, 공격자는 원격통제를 통해 DDoS 공격 등을 수행할 수 있었으며, DDoS 공격 수행 이외에도 'PC의 파일 시스템 통제(파일 열람, 변경, 삭제)', '공격자가 지정하는 특정 사이트로부터의 파일 다운로드 및 실행', 'PC 시스템 정보 확인', 'PC 프로세스 관리', 'PC 레지스트리 생성·변경·삭제', 'PC의 서비스 생성·삭제·수정' 등이 가능했다.

DDoS에 악용된 공격코드 Down(1).exe 분석

한편, DDoS 공격 트래픽을 일으킨 일부 PC에서는 Anti.exe 외에도 Down(1).exe라는 악성파일이 추가로 발견됐으며, 이 코드 역시 DDoS 공격 기능이 구현돼 있는 것으로 확인됐다. 다만, 분석결과, Down(1).exe는 자기전파 기능이 없는 것으로 밝혀짐에 따라, Anti.exe 악성코드에 의해 추가적으로 설치됐거나, 웹 사이트 등을 통해 유포됐을 것으로 추정된다. 이 악성코드는 http 프로토콜을 통해 특정 웹 사이트로부터 공격대상 사이트, 공격방법 등에 대한 정보를 전달받은 후 공격을 시작했다. 특히, Down(1).exe는 http://www.◎◎◎◎.co.kr/config.txt의 config.txt 파일 내에 기입된 주소와 프로토콜을 확인해 공격을 진행하기 때문에, 공격자는 해당 내용을 변경하며, 공격대상 및 프로토콜을 바꿀 수 있었다. 또한 재부팅 시에도 계속적인 활동을 유지하기 위해 시스템에 악성코드 자신을 등록시키도록 프로그래밍이 돼 있었다.



▲ 그림 4. Down(1).exe에 의한 DDoS 공격

❶ 해당 프로그램은 공격자가 구성한 공격명령 전달을 위한 웹사이트 (http://www.◎◎◎◎.co.kr/config.txt)로부터 공격명령이 포함된 설정파일 다운로드

❷ Down(1).exe는 다운로드 받은 공격명령을 확인하여 명령파일에 기록된 주소로 대량의 패킷 발송

DDoS 공격 대응을 위한 필수사항

인터넷 통신망 환경이 데이터 위주에서 음성(VoIP), 인터넷 TV(IPTV) 등 통신과 방송의 융합이 가능한 BcN(Broadband Convergence Network)으로 진화되고, 또한 PC 성능이 크게 향상됨에 따라, 최근 일반 PC를 이용한 DDoS 공격이 인터넷망의 안정성에 커다란 위협이 되고 있다. 이미 국내의 초고속 인터넷 환경은 가입자단의 속도가 100 Mbps를 지원하는 만큼 이들 PC가 DDoS 공격에 악용될 경우, 과거와 달리 많은 양의 공격 트래픽을 발생시킬 수 있다.

특히, 인터넷 침해사고 가운데 DDoS 공격은 그 특성상, 효과적으로 방어하기가 매우 어려우며, 여기에 최근 등장하는 DDoS 공격은 원격조종 기능을 가진 악성코드나 악성 봇을 인터넷 이용자의 PC에 설치해 이들을 좀비 PC로 만들고, 해커가 원격에서 이를 조종하는 형태를 보이고 있다는 점에서 대응이 쉽지 않다.

보안이 취약한 개별 PC에서 발생된 DDoS공격 트래픽은 마치 '개울물→시냇물→강물→바닷물'의 순서처럼 이미 공격이 시작한 후에는 감당하기 어려울 정도로 발전하기 때문에 '바닷물'이 되기 전, 즉 '개울물' 단계 이전에 차단하는 것이 가장 효과적이라고 할 수 있다. 이를 위해서 '개울물'에 해당하는 인터넷 이용자의 PC를 최신 보안 업데이트 상태로 유지하는 것이 무엇보다도 중요하며, 각 주체별로 다음과 같은 예방 및 대응조치가 필요하다.

첫째, 인터넷 사용자는 무엇보다 PC를 최신 보안 업데이트 상태로 유지하고, 백신과 개인방화벽을 설치·운영함으로써, 자신의 PC가 자신도 모르는 상태에서 DDoS 공격을 유발하는 공격용 PC가 되거나 개인정보 유출, 스팸릴레이 발송 등 침해사고에 악용되지 않도록 주의해야 한다. 또한 P2P 사이트 등에서 내려 받은 파일은 PC에 설치된 백신을 사용해 안전성 검사를 반드시 실시해야 한다.

둘째, ISP/IDC 및 기업 네트워크 운영자는 평소 유효하지 않은 IP주소 및 악성 봇 명령 제어/서버 도메인 등에 대한 사전 필터링 조치로 DDoS 공격을 발신지부터 제거하는 노력이 필요하다. 또한 DDoS 공격 발생 시 정보통신부, KISA 등 유관기관에 적극 신고 및 협조하고 DDoS 공격의 근원지 및 원격 조종자 PC를 신속하게 찾아낼 수 있도록 조치하는 것이 필요하다.

셋째, IDC, 웹 호스팅 업체, 기업, 개인 등 웹 서버 운영자는 지금까지 살펴본 아이템 거래 사이트에 대한 DDoS 공격 사례처럼 자신이 운영하는 웹 서버가 해킹돼 악성코드를 유포하거나 DDoS 공격 관련 스크립트 전달 경유지로 악용되지 않도록 웹 방화벽 설치, 웹 서버 및 운영체제에 대한 최신 보안 업데이트 설치와 주기적인 로그 분석 등을 해야 한다.

마지막으로, 피해기업의 네트워크 및 웹 서버 운영자는 자신이 운용하는 서버에서 허용되지 않는 서비스를 차단하기 위한 방화벽을 비롯해 침입시도를 탐지·차단하는 침입방지 시스템 및 DDoS 차단 시스템 등을 설치해 DDoS 공격 및 침입시도에 대한 대응도 필요하다. 또한 금품요구 등 협박이 있을 경우, 범인의 계좌번호, 메신저 아이디 등 수사에 도움이 되는 정보를 반드시 수사기관에 알려 범인검거에 협조하는 것도 잊지 말아야 한다. S