**침해사고**

: 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태

**3.20 및 6.25 사이버 공격(‘13년)**

: 국내 주요 언론사와 금융권의 전산망이 악성코드에 감염되어 다운되는 사태가 발생

방송 및 금융부문 6개사 전산망이 동시에 마비되어 최장 10일간의 복구 기간이 소요

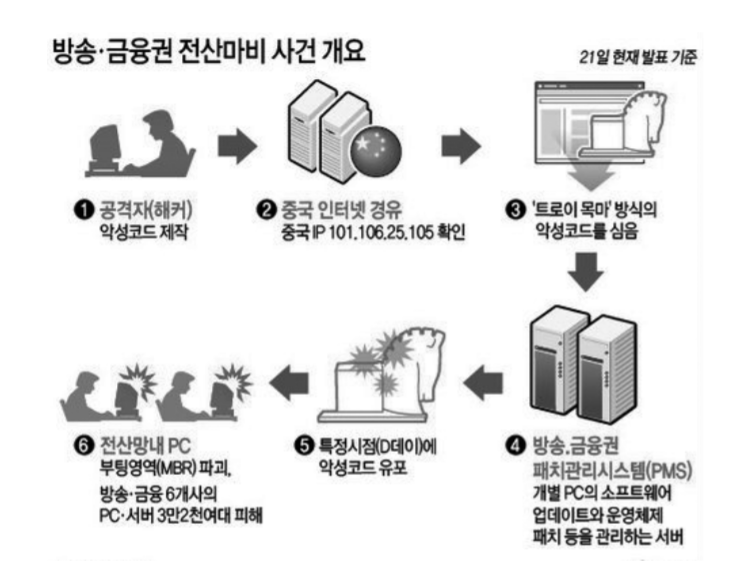
**3·20 전산 대란**

악성코드의 유포로 3만 2천여 대의 시스템이 감염

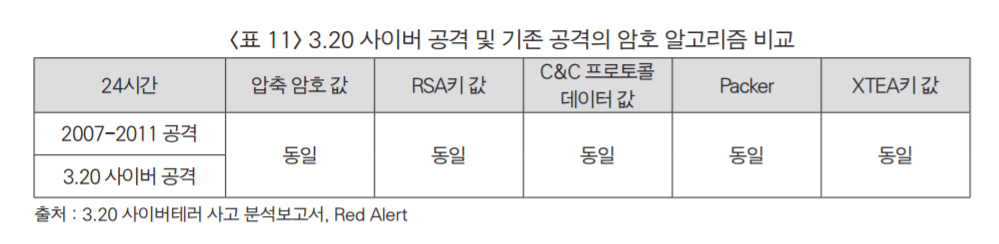
단일 조직에 트로이 목마를 통해 사전에 유입된 악성코드에 공격당한 것으로 추정

보안 업체인 잉카인터넷의 분석 자료에 따르면 ApcRunCmd.exe, Othdown.exe라는 파일명의 악성코드가 확인. 이 악성코드는 2013년 3월 20일 오후 2시가 되면 시스템을 파괴하도록 설계되어 있었다. 악성코드에 포함된 다양한 명령은 난독화되지 않았다. 미국의 보안 업체는 이 악성코드가 PuTTY의 설정 파일을 취득하여 원격에 있는 시스템을 파괴하는 명령도 포함되어 있으며, 다른 파일을 추가로 받거나 윈도 레지스트리를 변경하는 일은 없이 오직 시스템을 사용 불가능한 상태로 파괴하는 목적만 있다고 결론 내렸다. 덧붙여 이 악성코드의 초기 형태가 지난해 발견되었다고 말했다.

3.20 사이버 공격으로 악성코드에 감염된 PC는 마스터 부트 레코드(MBR)와 볼륨 부트 레코드(VBR)가 파괴되어 부팅되지 않았으며, 기존 데이터들이 소실되는 피해를 입었다. 부팅 영역만 공격한 것이 아니라 하드디스크 자체를 손상시켰기 때문에 손상된 데이터의 완전 복구는 어렵다.



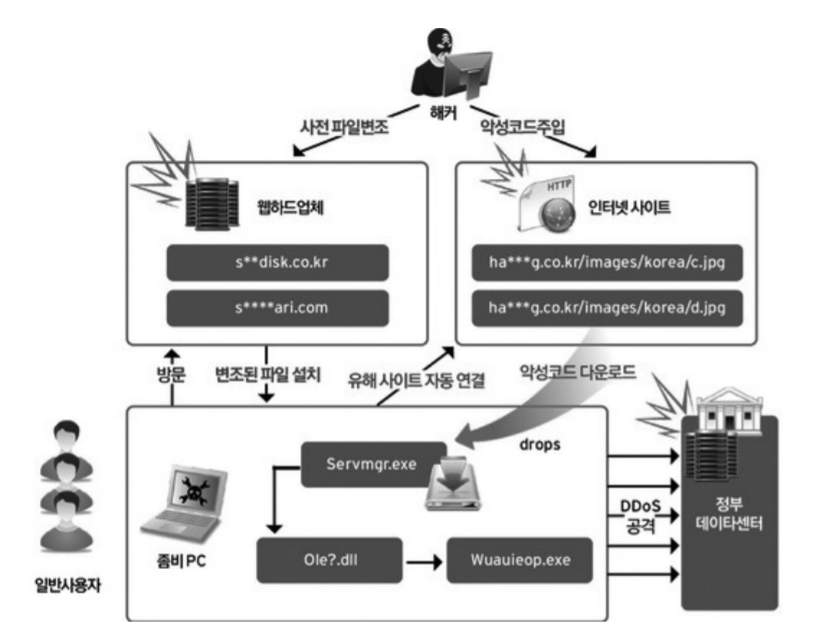
< 3.20 전산대란의 주요 진행과정 >



Red Alert에서 발표한 3.20 사이버테러 사고 분석보고서에 따르면, 3.20 사이버 공격의 암호 알고리즘과 기존의 2007년에서 2011년 사이에 있었던 공격의 암호 알고리즘을 비교 분석한 결과 아래 표 11과 같이 주요 유형별 데이터 값이 동일하게 나타나, 3.20 사이버 공격이 일시적이고 갑작스런 공격이 아닌, 동일한 조직에 의한 치밀하게 준비되고 계획된 공격으로 추측됨

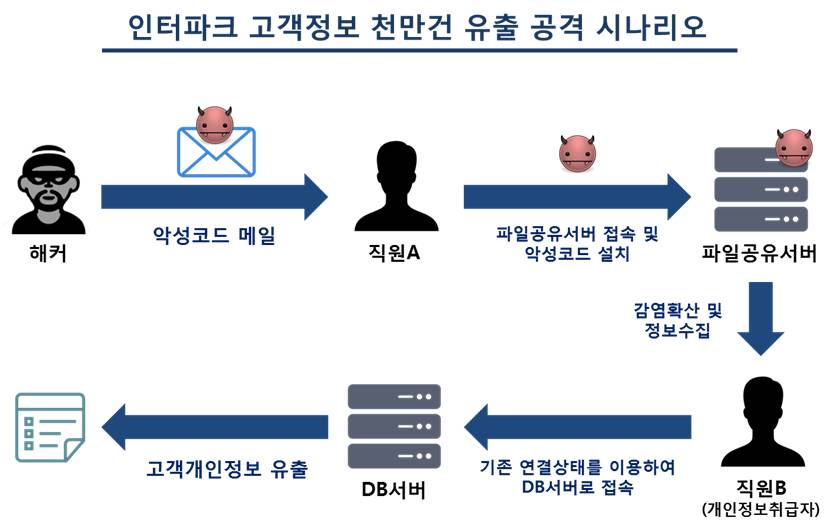
**6·25 사이버 테러**

2013년 6월 25일 오전 9시 10분경 청와대 홈페이지 및 주요 정부기관, 언론사 등에 웹 사이트 변조, 분산서비스거부(DDoS), 신상정보 유출 등의 공격이 수행



<6.25 사이버 공격의 전체적인 흐름>

**인터파크 1000만 고객 정보 유출 사건**



피싱 사이트를 통해 이메일 주소를 알아낸 뒤 악성코드를 첨부한 메일을 통해 악성코드를 감염시킴. 그 후 악성코드를 통해 C&C 서버에 접속하였고, 취약점을 통해 관리자 PC 에 접근하였다. 그 후 DB에 개인정보를 탈취함. 정확한 표적을 대상으로 지속적으로 공격을 수행하는 APT 공격을 수행함.

**야후 계정 30억개 해킹**

야후 해킹은 2014년 초 야후 직원에게 보낸 스피어 피싱 이메일로 시작됐다. 스피어 피싱이란 한 개인이나 조직을 집요하게 노리는 피싱 공격을 말한다. 많은 직원에게 이메일을 보냈고 단 한명의 직원이 이메일을 클릭하여 해킹이 시작되었다.

해커는 사용자 데이터베이스를 편집할 수 있는 계정 관리 툴을 이용해 백도어를 설치하였고, 데이터베이스의 백업본을 자신의 컴퓨터로 전송하였다.

**2009년 7·7 사이버 테러**

|  |  |  |
| --- | --- | --- |
| **구분** | **기존 DDoS** | **7.7 DDos** |
| 명령.제어 서버 존재여부 | 해커로부터 명령을 받는 명령.제어 서버존재 | 악성코드를 업데이트를 하는 서버존재 |
| 공격방법 | 명령.제어 서버의 네트워크를 통한 실시간 공격 제어 | 일정 주기로 악성코드를 업데이트 받아 스케줄링을 통한 공격 |
| 감염경로 | 윈도우, 브라우저 취약점을 악용한 홈페이지 악성코드로 인한 감염 | 공격자가 정상적인 프로그램에 숨겨둔 악성코드가 동작 |
| 방어 방법 | 명령.제어 서버 차단 | 공격PC의 악성코드 제거 |
| 공격 대상 | 홈페이지 1~2개 | 다수 홈페이지에 공격 |
| 악성 행위 | 해커의 명령을 지속적 수행 | 단기공격 수행 후, 하드디스크 삭제 |
| 공격 목적 | 금전적 이득 | 사회혼란 유발 |

·국가정보원에서는 발생의 진원지가 북한의 110호 연구소로 추정된다는 발표

·공격은 1차, 2차, 3차로 나누어 진행

1. **공격 방식**

**Cache-Control** : no-store, must-revalidation **CC attack** 이라고하는 **방법**을 이용했다.

이는 캐쉬를 이용한 공격으로 no-store는 캐쉬를 저장하지 않는다는 것이고, 보통 클라이언트와 서버는 캐쉬에 대하여 유효 값을 정하는데 이 값이 만료 될 경우 revalidation을 합니다. 공격은 revalidation을 하게 끔 하여 서버에 부하를 준다.

1. **피해**
   1. 115,000여개 IP주소에서 공격 트래픽이 발생하였다.
   2. 피해사이트는 국내 22개, 국외 14개
   3. 사이트별로 최소 24시간, 최대 72시간 동안 접속장애
   4. 일부 PC의 하드디스크 손상
2. **악성코드 감염 경로**
   1. 웹하드 이용자는 감염된 국내 웹하드 업체 서버에 접속하여 업데이트를 위장한 악성코드를 다운 받아 감염
   2. 2. 감염된 피해자의 PC는 C&C 서버에 연결된다.
   3. 3. 북한 해커가 C&C 관리 서버를 통하여 공격 명령 전달하여 C&C 서버에 연결된 피해자 는 DDOS 공격
   4. 4. DDoS 공격 후에 감염된 피해자 자신의 PC 하드디스크를 파괴하는 명령어 수행
3. **방어**
   1. 안철수연구소는 1차 공격 직후 전용백신 공급
   2. 공격을 받은 포털들도 대응이 빨랐다.

예를 들어 mail.naver.com 이면 main2.naver.com로 서비스 하는 등