방송통신위원회
KOREA COMMUNICATIONS COMMISSION

2011. 3.5.(토)

해명자료

문의 : 네트워크정책국 네트워크정보보호팀 박철순 팀장(☎750-2750)
네트워크정보보호팀 이상국 사무관(☎750-2757) sklee@kcc.go.kr

방통위 "DDoS 공격 정보 파악 즉시 철저 대응"

- 조선일보 보도(3. 5) 사실과 달라 -

'11. 3. 5.(토) "디도스 공격, 알고도 당했다" 기사(조선일보 1면)과 관련, 사실과 다른 내용이 있어 다음과 같이 알려 드립니다.

□ 보도 내용

"방송통신위원회는 4일 청와대·국가정보원·한국철도공사 등 주요 사이트 40곳을 겨냥한 사이버 테러 공격이 시작되기 13~16시간 전에 공격 계획을 정확하게 알았지만 주무당국으로서 사전 경보조차 발령하지 않은 것으로 확인됐다. (……) 다른 보안업체 임원은 "방통위 측에서 '늘 있는 공격 같으니 괜히 언론에 알리지 말라'고 지시했다"고 말했다" 라고 보도

□ 해명 내용

1. 국정원·방통위 등 정부는 **3일 오전**에 통상적인 소규모 DDoS 공격이 6개 사이트를 대상으로 발생한 것을 탐지한 후, 악성코드 샘플을 채취하여 안철수 연구소 등 업체와 긴밀히 협력하면서 분석을 진행하였습니다.

   그 결과 **40개 사이트가 공격 대상**인 것을 확인하고, 접속 서비스에 영향을 미치는 수준은 아니었지만 **해당 사이트에 통지하여 대처**토록

하였습니다. 또한, 방통위가 지난해 구축한 **사이버 치료 체계**를 가동하고 백신업체와 협력하여 **치료 백신을 개발·배포**하는 등 대응에 만전을 기하였습니다.

또한 **3월 4일 아침**에 추가로 유포된 악성코드가 29개 사이트를 대상으로 10시에 공격이 발생한다는 것을 확인하고 즉시 국정원, 국방부, 행안부 등과 협의하여 **10시 기준으로 '주의 경보'를 발령**하였습니다.

그러나 3일의 DDoS 공격은 일 평균 수백건 씩의 새로운 악성코드가 탐지되고 수십건의 **DDoS 공격이 발생되는 수준 내**에 있었기 때문에 **경보를 발령하지 않는 것으로 관계기관간 협의**를 하였습니다.

따라서 정부는 공격 예상 사이트에 대해 **사전 통보 조치 및 필요한 대응을 충실히 수행하였고 대응수칙에 따라 상황 변화에 신속히 대응**하였음을 알려드립니다.

2. 한 보안업체가 "디도스 공격의 조짐이 포착되어 3일 오후 6~9시 사이에 방통위에 신고했다"는 보도내용과 관련, 앞서 밝힌대로 방통위는 이미 3일 오전부터 악성코드를 채집하여 백신업체와 분석, 오후 6시부터 공격 대상 40개 사이트에 통보하였으며 보안업체 및 ISP와 공조하여 백신 개발·보급에 나서는 등 필요한 조치를 취하였습니다.

   또한 방통위는 보안업체에게 **"늘 있는 공격 같으니 괜히 언론에 알리지 말라"고 지시한 바가 없음을 밝힙니다.** 끝.