4 에스토니아: 최초의 대규모 사이버전쟁(2007.4.27~5.18) <하> 2007년 4월 27일 에스토니아 정부는 수도 탈린 중심부에 위치한 '탈린 해방 기념비(Monument to the Liberators of Tallinn)'를 외곽의 국립묘지로 옮겼다. 에스토니아의 민족주의자이자 친서방 정책을 옹호하는 입장에서, '청동 군인상(Bronze Solider)'이라고도 불린 이 기념비의 이전은 1940년부터 약 50년간 그들을 압제했던 소련의 자취를 지우려는 행위였다. 그런데, 에스토니아의 이러한 행보는 사이버 전쟁의 빌미가 되었다.

좀비PC 100만 대 디도스 공격에 국가 마비 사태

<DDoS: 분산 서비스 거부 공격>

첫 사흘간은 트래픽·스팸 폭증 양상
정부·국회 등 공공부문 서버 '먹통'
주로 반에스토니아 유저 수동적 공격

'봇넷' 이용 자동화 대규모 공격 이어져
민간 회사까지 모든 사이버 공간 표적
3주간 사회 대혼란·수천만 달러 피해
배후 미궁…사이버 위협 경각심 커져

유럽 안보를 맡고 있는 나토는 2007년 에스토니아에 대한 러시아의 사이버공격 이후 NATO 사이버 방어협력센터를 설립하고, 당시 전 세계에서 가장 규모가 크고 최첨단인 사이버 방어 훈련 '락트 실즈(Locked Shields) 2017'을 실시했다. 이 훈련에는 국가 IT 시스템 보호를 책임진 보안전문가를 비롯해 정책 전문가, 나토 회원국과 파트너국의 법적 자문단 등 25개국에서 약 800명이 참가했다. 사진=NATO

사이버 강국 에스토니아

에스토니아는 1991년 소련으로부터 독립한 인구 130만 명의 신생국가였다. 그러나 북유럽에 위치한 작은 국가지만 사이버 분야에서만큼은 세계를 선도하고 있었다. 사이버 공격을 받을 당시인 2007년 기준으로 에스토니아 시민들은 온라인을 통해 언제든 99% 이상의 공공 서비스를 이용할 수 있었다. 인구의 절반 이상이 인터넷 뱅킹을 사용했다. 2005년 에스토니아 정부는 인터넷을 통해 지방선거를 실시했다. 법적으로 유효한 인터넷 기반 총선거를 실시한 최초의 국가였다. 국내 총생산에서 IT 산업이 차지하는 비중 역시도 상당히 높았다. 즉, 에스토니아는 인터넷을 통해 모든 공공 행정 및 민간 서비스 업무를 처리할 수 있도록 시스템이 잘 갖추어져 있었기에 국제적으로 E-에스토니아로 불렸었다. 이렇게 사이버에 대한 의존도가 남달리 매우 높았던 에스토니아에 전면적 사이버 공격은 대재앙으로 다가왔다.

에스토니아는 국제적으로 E-에스토니아로 불릴 만큼 사이버강국이다. 사진=e-estonia

1단계: 사이버 전초전

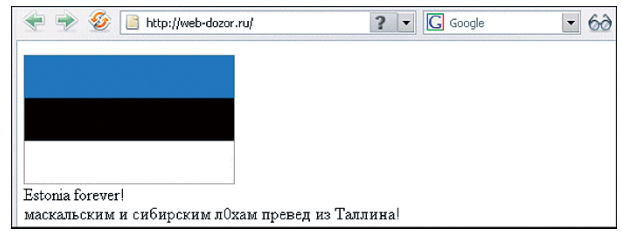
사이버 공격은 4월 27일 22시부터 즉각 개시되었다. 초기 공격의 대상은 공공부문에 집중되었고, 중요 시스템과 서버에 평소와 달리 이상하리만큼 많은 양의 데이터 트래픽이 발생했다. 정부의 주요 웹사이트는 위·변조 공격을 받아 심하게 훼손되었다. 에스토니아 주요 인사들의 이메일 보관함은 스팸과 피싱 이메일로 넘쳐났다. 에스토니아 정부 공식 웹사이트(valitsus.ee)는 4월 28일 오후 약 8시간가량 접속 자체가 완전히 불가능했다. 복구 이후에도 이틀간 접속 실패 사례가 속출되었고, 접속하더라도 오랜 대기 시간을 필요로 했다. 이외에도 총리실, 국회, 경제통신부, 내무부, 외무부 등이 전부 공격을 받았다.

일부지만 에스토니아인들에게 온라인을 통해 각종 소식을 전하는 언론도 공격의 대상이었다. 사이버 공격이 시작되었을 당시 에스토니아의 한 유력 언론사 IT 책임자는 자신의 사무실 벽에 걸린 모니터로 언론사 서버의 용량 대비 방문자 수를 보고 있었다. 그는 평소 20~30% 정도 여유가 있던 서버의 용량이 서서히 20%, 10%, 5%로 줄어들고 결국 0%로 변하더니 순간적으로 웹사이트가 접속 불가 상태가 되어버리는 광경을 목격하고 소스라치게 놀랐다. 사이버 공격으로 만들어진 인위적인 트래픽 증가로 인해 해당 언론사의 서버는 무려 20회에 걸쳐 다운되었다.

그나마 다행인 것은 사이버 전쟁이 시작되고 첫 3일간은 수동적인 공격이 주를 이루어 그 규모가 크지는 않았다는 것이다. 초기 사이버 공격은 공격을 주도하는 세력이 러시아어를 사용하는 온라인 포럼과 커뮤니티에 공격 대상과 방법을 올려놓으면, 에스토니아의 정치적 방향성에 반대하는 온라인 유저들이 이를 따라 사이버 공격에 참여하는 방식으로 진행되었다. 물론, 수동적인 사이버 전초전이었지만, 기습은 대성공이었다. 초기에 에스토니아는 사이버 공격에 속수무책이었다.

2단계: 전선의 확대

본격적인 대규모 사이버 전쟁은 4월 30일부터 시작되었다. 공격자들은 2단계 작전에 돌입하며, 악성코드를 통해 감염되어 자신들의 통제하에 놓여있던 좀비PC들로 구성된 봇넷(Botnet)을 이용하여 자동화된 대규모 공격을 실시했다. 또한, 공격의 목표도 1단계 동안 정부기관과 주요 정치인, 일부 언론사에 국한되었던 것이 2단계에는 은행, ISP(인터넷 서비스를 제공하는 회사), 학교, 전 통신사와 언론기관, 그리고 민간 회사의 웹사이트까지 에스토니아의 전 사이버 공간으로 확대되었다.



에스토니아 해커들이 자국의 홈페이지들이 공격 당하자 그 대응의 일환으로 러시아의 웹사이트(www.web-dozor.ru)에 "에스토니아인이 되어 자랑스럽다!"와 "에스토니아 영원하다!" 등의 문구를 써넣었다. 필자 제공

에스토니아를 공격한 해커들은 제3국에 위치한 자신의 지휘 및 통제 서버를 이용해 인터넷으로 연결된 수천 대의 좀비PC를 원격으로 제어했다. 해커들의 명령에 따라 좀비PC는 지정된 공격 대상인 서버, 시스템, 또는 웹사이트에 동시에 접속하여 이들을 무력화시켰다. 1단계에서 수동 방식의 서비스 거부 공격(DoS)이 있었다면, 2단계에서는 더 위력적인 분산 서비스 거부 공격(DDoS)이 자행되었던 것이다. 또한, 해커들은 봇넷을 이용해 이전과 규모와 용량에서 비교도 되지 않을 만큼 많은 스팸 및 피싱 이메일을 공격 대상에게 발송하여 업무를 마비시켰다. 웹사이트에 대한 위·변조 공격도 사방에서 발생했다.

2단계 사이버 공격은 봇넷에 의한 사회 전반에 대한 조직적인 자동화 공격으로 정의될 수 있다. 에스토니아와 국제사회의 대응은 2단계 공격이 한창인 상황에서야 겨우 시작되었고, 그들은 공격 시작 후 3주가 흐른 5월 18일에서야 모든 사이버 공격을 막아낼 수 있었다.

약 3주간 일어난 다양한 사이버 공격으로 인해 에스토니아는 큰 사회적 혼란과 함께 수천만 달러에 달하는 천문학적인 금전적 피해를 보았다.

사이버 전쟁의 배후와 대응

에스토니아 정부는 청동상 이전과 관련된 정황적 증거를 넘어 과학적인 분석을 통해 사이버 전쟁의 배후로 러시아를 지목했다. 공격에 동원된 약 100만 대의 좀비PC 중 많은 수가 러시아의 것이었다. 그리고 공격에 사용된 대표적 IP주소 중 일부가 러시아 정부 기관 것이기도 했다. 이외에도 러시아를 지목하는 과학적 증거들이 많았다. 그러나, 러시아는 자신들의 관련성을 강하게 부인했다. 또한, 그들은 나토와 함께 공격의 배후를 밝히기 위한 에스토니아의 수사에도 협조하지 않는 행태를 보였다.

러시아의 강력한 부인과 비협조로 에스토니아에 대한 조직적인 사이버 공격에 대한 적절한 처벌과 보복 행위는 이루어지지 않았다. 그럼에도, 이번의 첫 대규모 사이버 전쟁으로 전 세계 모든 국가가 현실화되어 가는 사이버 전쟁의 위협을 인식하게 되었다. 북대서양조약기구(나토·NATO)는 앞으로 러시아의 사이버 공격에 대한 회원국 간의 집단 방위를 천명하기 위해 에스토니아의 수도 탈린에 나토 사이버 방어협력센터라는 상징적 기관을 설립했다.

필자 **박동휘 소령**은 육사 61기로 졸업·임관 후 美 워싱턴대에서 사이버 전쟁과 전략에 관한 연구로 박사 학위를 받았다. 현재 육군3사관학교 군사사학과 학과장으로 근무하고 있다.