27. 국내 랜섬웨어 피해 속출… 피해예방 보안수칙은?

[이데일리 김현아 기자] 국내 랜섬웨어 피해가 속출하고 있어, 사용자의 주의가 요구된다.  
  
이스트소프트(047560)(대표 정상원)는 3일부터 국내 대형 커뮤니티를 중심으로 ‘CryptXXX(크립트XXX)’ 랜섬웨어 변종 유포가 급격히 증가했다고 밝히며, 랜섬웨어 피해 주의보를 발령함과 동시에 개인 및 기업의 데이터 보안 강화를 당부했다.  
  
이번에 유포된 ‘CryptXXX’ 랜섬웨어는 다양한 변종이 꾸준히 제작되고 있으며, 현재 한국어를 포함해 약 25개국의 다국적 언어 서비스를 제공할 정도로 국제적 사이버 범죄 양상을 띠는 게 특징이다.

이 공격 유형은 랜섬웨어 제작자들이 유포지를 쉽게 파악할 수 없도록 함과 동시에 보안이 취약한 광고 플랫폼을 경유해 불특정 다수의 이용자를 대상으로 동시다발적 공격을 수행하는 ‘멀버타이징(Malvertising)’ 공격 기법을 이용하고 있다.   
  
‘멀버타이징’ 기법은 이메일 첨부파일 기법과 함께 2015년 중순 이후 국내에 증가하기 시작한 주요 랜섬웨어 유포 통로 중 하나이다.   
  
특히 이 기법에 의해 피해에 노출되는 경우 보안이 취약한 광고 플랫폼이 존재하는 웹 사이트에 인터넷 익스플로러(IE)를 이용해 단순히 접속만 하여도, 해당 사이트 내 광고를 보여주기 위해 사용되는 ‘플래시 플레이어(FlashPlayer)’의 취약점을 악용해 사용자의 PC를 랜섬웨어에 감염시켜 각별한 주의가 필요하다.  
  
**<랜섬웨어 피해 예방 보안 수칙 3선>**  
  
**1기본적인 보안 수칙을 잘 지켜야 합니다.**  
  
**: 윈도우 운영체제 업데이트,** IE**브라우저,** Adobe Flash Player**,** Office **등 자주 사용하는** SW**를 항상 최신 버전으로 유지해야 합니다.**  
  
**2알약 등 신뢰할 수 있는 백신을 사용하고,** DB**업데이트 상태를 최신으로 유지합니다.**  
  
**: 현재 알약 최신 버전에는 랜섬웨어 행위기반 차단 기능이 포함되어 있습니다. 알려진 랜섬웨어는 패턴 기반으로 차단하고, 새로운 신변종 랜섬웨어는 행위 기반으로 차단할 수 있습니다.**  
  
**3중요 파일에 대한 백업을 습관화합니다.**  
  
**중요한 파일들에 대하여 로컬**PC**가 아닌 외장하드,** USB **등 다른 저장매체에 백업을 습관화합니다. 클라우드 서비스에 저장을 하여도, 최근에는 실시간 동기화 서비스가 제공이 되어 로컬에 있는 문서들이 즉각 동기화 되기 때문에, 자칫하다가는 클라우드에 있는 정보들까지 모두 암호화될 수도 있습니다.**  
  
**특히 상대적으로 기업 환경에서는 중요 문서를 많이 다루고 관리해야 할 임직원들이 많아 랜섬웨어 악성코드에 감염될 경우 피해가 매우 큽니다.**  
  
**이러한 기업환경에서 임직원들의 중요 자료를 실시간으로 자동 백업 시켜줄 수 있는 문서 백업솔루션 및 문서중앙화 솔루션을 도입하는 것도 랜섬웨어 공격의 피해를 막을 수 있는 하나의 방법이 될 수 있습니다.**  
  
지난 주말 기간 집중적으로 감염자 피해가 속출한 대형 커뮤니티의 경우도, 이와 같이 웹 사이트에 탑재된 특정 광고 배너를 통해 ‘CryptXXX 랜섬웨어’가 다량으로 유포되었다.   
  
이스트소프트가 자사의 백신 프로그램 ‘알약(ALYac) 공개용’ 제품을 통해 제공하는 ‘행위 기반 기술 랜섬웨어 차단 통계 현황’에 따르면, 통계를 집계하기 시작한 지난 1월부터 알약을 통해 차단된 랜섬웨어 공격 건수는 약 220만 건 이상이다.  
  
또한 역대 최대 규모의 랜섬웨어 유포가 시작된 지난 3일에는 전일 대비 랜섬웨어 차단 건수가 약 2배로 급격히 증가한 것으로 나타났으며, 7일에는 3배 이상 급증한 약 4만 5천여 건의 차단 통계가 집계되었다.   
  
‘CryptXXX’ 랜섬웨어에 감염되면 각종 이미지 파일, 문서파일 등이 암호화되어 사용하지 못하게 되며, 특히 HWP 문서 파일도 암호화 대상에 포함되어 있어 감염된 PC 사용자의 큰 피해가 예상되고 있다.  
  
아울러 이 랜섬웨어의 공격자는 암호화된 파일을 인질로 삼고, 복호화(암호 해제)를 조건으로 1.2 BTC 비트코인 결제(한화 약 82만원 상당)를 요구하는 안내창을 띄워 현금 갈취도 시도하는 것으로 확인되었다.   
  
이스트소프트 보안사업본부 김준섭 본부장은 “대형 온라인 커뮤니티 등을 통한 랜섬웨어 유포는 불특정 다수를 대상으로 개인과 기업 모두에게 돌이킬 수 없는 큰 피해를 입힐 수 있다”며, “운영체제(OS)를 포함해 플래시 플레이어, 자바 등은 항상 최신 버전으로 유지하고, 랜섬웨어 차단 기능이 탑재된 보안 제품 활용과 중요 자료 백업을 생활화하는 등 보안 수칙 준수에 만전을 기하는 것이 매우 중요한 시기다.”라고 강조했다.  
  
현재 알약에서는 이번 랜섬웨어 악성코드를 ‘Trojan.Ransom.CryptXXX“으로 탐지하고 있다.