[Discussion] Network Security Forensics

Sinflection

genius0han@gmail.com

不飛不鳴(불비불명)

보안

한국트렌드마이크로, 기간 시설에 대한 공격 조사 보고서 발표

2013.04.04 편집부 | ITWorld

한국트렌드마이크로(www.trendmicro.co.kr)는 모의 실험을 통해 3.20 대란에 이어 일상 생활에 필수 불가결한 전력, 가스, 수도 등 국가 기반 시설과 산업시설에 사이버 공격이 우려되고 있다며 기간 산업망 보안에 각별한 주의를 기울일 것을 당부했다.

이번 트렌드마이크로의 모의 실험은 산업설비 제어 시스템과 유사한 환경에 허니팟(비정상적 접근 탐지를 위해 의도적으로 설치한 시스템)을 설치해 급수 펌프 시스템, 생산 시설, 공장 온도 조절 시스템 등으로 가정해 유입되는 타깃 공격을 면밀히 모니터링 한 것이다. 조사결과 허니팟 설치 18시간 만에 첫 번째 공격이 유입됐으며, 총 28일 동안 14개 국가에서 총 39회의 공격이 발생하는 등 산업 설비 제어 시스템에 대한 공격이 실존 위협임을 증명됐다.

허니팟에 유입된 공격 중 12회는 각각 별개의 표적 공격이었고, 13회는 동일 공격자에 의한 반복 공격이었다. 국가별로는 중국이 35%로 가장 많았으며, 미국 19%, 라오스 12% 등 순서로 집계됐다. 눈에 띄는 부분은 북한으로 추정된 공격도 2%를 차지하고 있다는 점으로, 북한의 사이버 공격 그룹이 산업기간 시설 또한 사이버 공격 대상으로 검토하고 있음을 추정할 수 있게 하는 결과다

한국트렌드마이크로 장성민 침해 대응 센터장은 "산업기반 시설 보호를 위해서는 오프라인 상태에서의 악성코드 탐지와 화이트리스트 방식의 응용 프로그램 제어 등 기존 보안제품과는 다른 접근 방식이 요구된다"고 밝혔다. editor@itworld.co.kr

O APT공격을 유인할 허니넷 모델은? Preemptive Network Forensics ?

- 기존 : Passive Honeynet, Active Honeynet 등

- 목표 : 3.20 사이버 공격과 같은 APT 공격을 사전에 인지할 수 있는 허니넷?

Discussion

- 공격자 유인할 정보를 가진 시스템 구축 방법

- 악성행위 격리 및 모니터링 방법

포렌식 조사관 생명단축 원인은 현장(IDC)

- 현장이동, 활성데이터 수집, 이미징, 복귀, 이미지복사, 밤새분석, 보고서작성

- 현장에 답이 있지만, 생명단축을 피할 수 없다.

Discussion

- IDC 작업시간 단축 방안

  (원격 수집, 원격 이미징)

- 이미징 VS 활성 데이터 수집 방안

- 효율적인 네트워크 트래픽 수집 방안

Question and Answer