정부혁신 보다나은 정부	보 도 자 료	KISTI 한국과학기술정보연구원 Korea Institute of Science and Technology Information

배포 즉시 보도 가능합니다.

대전(본원): 대외협력실 이종성 042-869-0976 / 이해준 0676 / 손영주 0997
문의: 과학기술사이버안전센터 송중석 책임연구원 (042-869-0729)

배포번호 : 2020-50 배포일자 : 2020.07.22.(수)	매수 : 보도자료 2매	배포처 : 대외협력실

"KISTI, KINS 등 국가기관 단말기의 '폼북' 악성코드 감염은 사실과 달라"

- 악성코드 전용 보안장비의 정상적인 분석활동으로 확인 -

☐ 최근 언론보도(전자신문, 이데일리)를 통해 한국과학기술정보연구원(이하 KISTI) 및 한국원자력안전기술원(이하 KINS)의 단말기가 정보탈취형 악성코드인 '폼북' 에 감염되어 국가 기반시설에 대한 추가 공격가능성이 우려된다는 기사가 게재되었으나, 이는 사실이 아닌 것으로 밝혀졌다.

☐ KISTI 과학기술사이버안전센터(S&T-CSC)가 국가사이버안전센터(NCSC)의 협조를 통해 해당 IP에 대한 상세분석을 수행한 결과, 해당 IP는 한국항공우주연구원(KARI) 및 KINS에서 자체적으로 구축·운영하고 있는 악성코드 수집·분석 전용 보안장비인 'APT 대응 솔루션'인 것으로 확인됐다. 따라서, **해당 언론보도에서 언급한 KISTI의 내부 시스템이 아닌 것은 물론, 일반 사용자 PC인 단말기가 악성코드에 감염됐다는 기사 내용도 사실과 다른 것으로 판명**됐다.

☐ KISTI 과학기술사이버안전센터는 KARI 및 KINS 보안담당자와 협력을 통해 APT 대응 솔루션의 '폼북' 악성코드 및 동적분석 결과자료를 기관으로부터 직접 제공받아 분석하였으며, 다크웹의 감염리스트에 기록된 악성코드 경유지 주소, 악성코드 설치일, 경유지 접속일시 등이 해당 APT 대응 솔루션의 실제 분석행위와 일치하는 것으로 확인됐다.

☐ 해당 'APT 대응 솔루션' 은 이메일의 첨부파일을 통해 전송되는 악성코드를 실시간으로 수집·분석·차단하는 전용 보안장비이며, ①해당 기관으로 유입된 이메일의 첨부파일에 포함된 "폼북" 악성코드 수집 → ②해당 악성코드 분석을 위해 실행 → ③악성코드 내 C2 서버주소에 대한 접근 시도의 과정을 거쳐 다크웹 악성코드 감염 리스트에 해당 IP주소가 등록된 것으로 분석됐다. 또한, 해당 '폼북' 악성코드가 빈번하게 해당 기관에 유입된 것을 발견하였으며, 이로 인해 다크웹에 기재된 악성코드 최초 설치일과 최종 접근일에 차이가 발생한 사실도 확인했다.

☐ 다크웹 등 외부에서 수집한 악성코드 감염리스트는 실제 악성코드의 감염여부와 상관없이 실행 시 전송된 정보를 토대로 작성되기 때문에, 정보의 정확성 및 신뢰도가 높지 않은 것이 사실이다. 특히 APT 대응 시스템, 허니팟, 샌드박스 등 악성코드 자체를 수집·분석하는 솔루션, 기술 등이 지속적으로 확대됨에 따라, 실제 악성코드 감염이 아닌 분석환경에서 실행된 악성코드 전송정보일 가능성이 높기 때문에 오탐률이 높아질 수밖에 없는 상황이다. **따라서 이러한 외부 감염리스트에 대해서는 해당 시스템의 유형, 감염여부 등에 대해 면밀한 조사·분석·검증 과정이 선행되어야만 감염리스트 정보에 대한 신뢰성을 확보할 수 있다.**