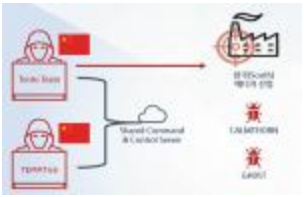
중국 기반 해커, 국내 에너지 기관 공격

datanet.co.kr/news/articleView.html

April 25, 2019



파이어아이 “한국·일본 타깃 중국 기반 해킹조직, 국내 에너지 시설 공격한 증거 발견”

중국 기반 사이버 범죄조직이 국내 에너지 기업을 공격한 사실이 드러났다. 파이어아이가 공개한 보고서에 따르면 최근 국내 에너지 분야 기업 네트워크에서 멀웨어가 발견됐으며, 이는 중국 정부가 후원하는 것으로 의심되는 사이버 범죄 조직과 연관 있는 것으로 분석됐다.

이 공격그룹은 한국과 일본의 주요 기관을 공격해왔으며, 우리나라 에너지 산업 관련 기업을 노린 공격이 발견된 것은 이번이 처음이다. 다만 최초 감염 요소는 무엇인지 알려지지 않았다.

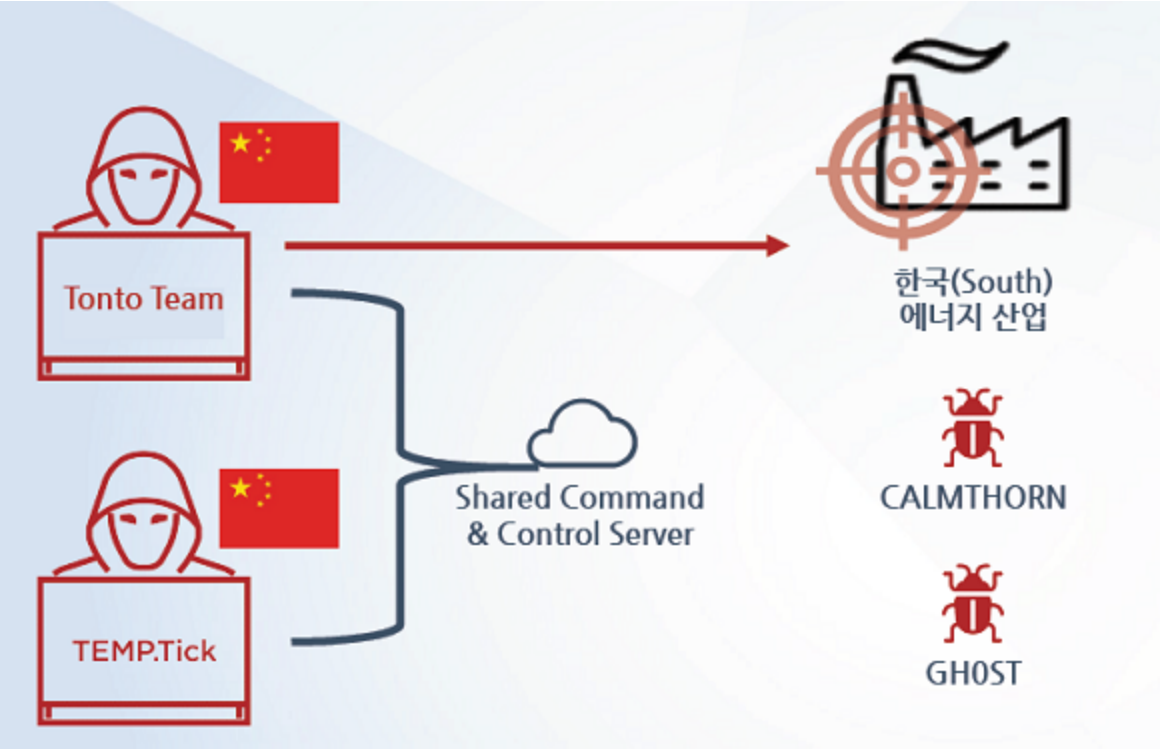
러시아·일본·한국 군사 조직 노리는 공격자

파이어아이가 국내 에너지 관련 기업에서 발견한 멀웨어는 캄손(CALMTHORN)과 고스트(GH0ST)다. 캄손은 TCP로 통신하는 비컨 백도어로, 파일 업로드, 리버스 쉘, 프록시 트래픽, 시스템 정보 수집 등의 명령을 지원한다. 고스트는 인터넷에 공개돼 있는 소스코드에서 유래한 원격 접속 해킹 도구(RAT)로, 공격자가 스크린과 오디오 캡처, 웹캠 작동, 프로세스 리스팅·종료, 명령쉘 열기, 이벤트 로그 삭제, 파일의 생성조작, 삭제, 실행, 전송 등의 기능을 활용할 수 있다.

캄손과 고스트는 중국 연계된 사이버 첩보 활동 단체인 톤토팀(Tonto Team)과 연관 있는 멀웨어다. 톤토팀은 2012년 혹은 이전부터 활동하고 있으며, 러시아, 일본, 한국의 군사·보안 관련 조직을 대상으로 공격을 수행하고 있다.

파이어아이는 톤토팀이 해킹그룹 탬프틱(TEMP.Tick)과 연관있을 것으로 보고 있다. 탬프틱은 중국 반체제 조직에 대한 모니터링 작업을 수행하는 집단으로, 중국 정부가 지원하는 해킹그룹으로 의심된다. 2009년 혹은 그 이전부터 활동한 것으로 알려지며, 중국 반체제 조직 뿐 아니라 한국, 일본의 국방, 중공업, 항공우주, 기술, 은행, 헬스케어, 자동차, 미디어 산업을 주로 공격한다.

캄손, 고스트, 톤토팀, 탬프틱의 연관성을 드러내는 증거로, 파이어아이는 이들의 공격 목표가 동일하다는 것을 든다. 톤토팀과 탬프틱은 우리나라와 일본의 주요시설을 노리고 있다. 또한 이들이 특정 레벨에서 리소스를 공유하고 있는 정황도 발견했다. 톤토팀의 이전 공격 사례에서 캄손과 고스트를 사용했던 것을 보아 이번 국내 에너지 기관 공격도 톤토팀의 소행으로 의심된다.



▲중국 기반 해킹 조직의 한국 에너지 기업 공격 사례

동일한 공격도구 반복 사용하는 공격자

톤토팀과 탬프틱의 연관성은 지난해 9월 발견된 아이앰킹(IAMKING) 멀웨어 샘플을 통해 증명됐다. 아이앰킹은 파일 작성, 쉘 접근 확보, 폴더 및 파일 열기, 프로세스 실행, 피해자 데이터 수집 등이 가능한 백도어 프로그램이다. 파이어아이는 아이앰킹이 톤토팀과 탬프틱 전용 툴이라고 판단하고 있다. 톤토팀과 탬프틱은 둘 다 명령 및 제어를 위해 동일 IP 주소를 사용했다.

아이앰킹은 하드코딩한 사용자 에이전트 문자열이 포함된 HTTP 기반의 드롭퍼 하드시멘트(HARDCEMENT) 다운로더와 동일 서버에 호스팅됐다. 하드시멘트는 탬프틱이 국내 포털사이트 다음의 도메인으로 위장해 공격할 때 사용한 것이다.

하드시멘트는 멀웨어 컴파일 시간이 지나고 몇 달 후 도메인 이름풀이(Domain resolution) 방법이 변경되었는데, 이는 탬프틱이 네트워크 사인을 변형하는 조치를 취하거나 업스트림 서비스 제공 업체가 명령 및 제어 통신을 원활하지 못하게 막는 조치를 취한다는 의미일 수 있다.

도메인 중 두 개에서 동적 DNS를 사용하므로 업스트림 업체가 이를 변경하기는 어렵기 때문에 후자의 경우일 가능성은 상대적으로 낮다. 만약 탬프틱이 변경하고 있는 것이라면, 이는 템프틱과 톤토팀이 연관되어 있다는 추가적인 증거가 될 것이다.

“공격조직 개편으로 우리나라, 더 큰 위협 직면”

파이어아이는 “오바마 미국 전 대통령과 시진핑 중국 국가주석이 체결한 사이버 첩보활동 금지·합의 후 사이버 범죄 시장에서 조직개편이 일어났으며, 톤토팀의 사명과 구조에 변화가 있었을 것”이라며 “그들은 툴과 인프라 등의 자산을 통합하고, 중앙 배포 센터를 구축해 더 능숙하게 공격하고 있다. 이는 해당 지역에 더 큰 위협이 될 수 있다”고 설명했다

-
-
-
-
-

김선애 기자 다른기사 보기