[긴급] 한국에 해킹 선전포고한 中 해커조직...”KISA 해킹하겠다” 예고 - 데일리시큐

dailysecu.com/news/articleView.html

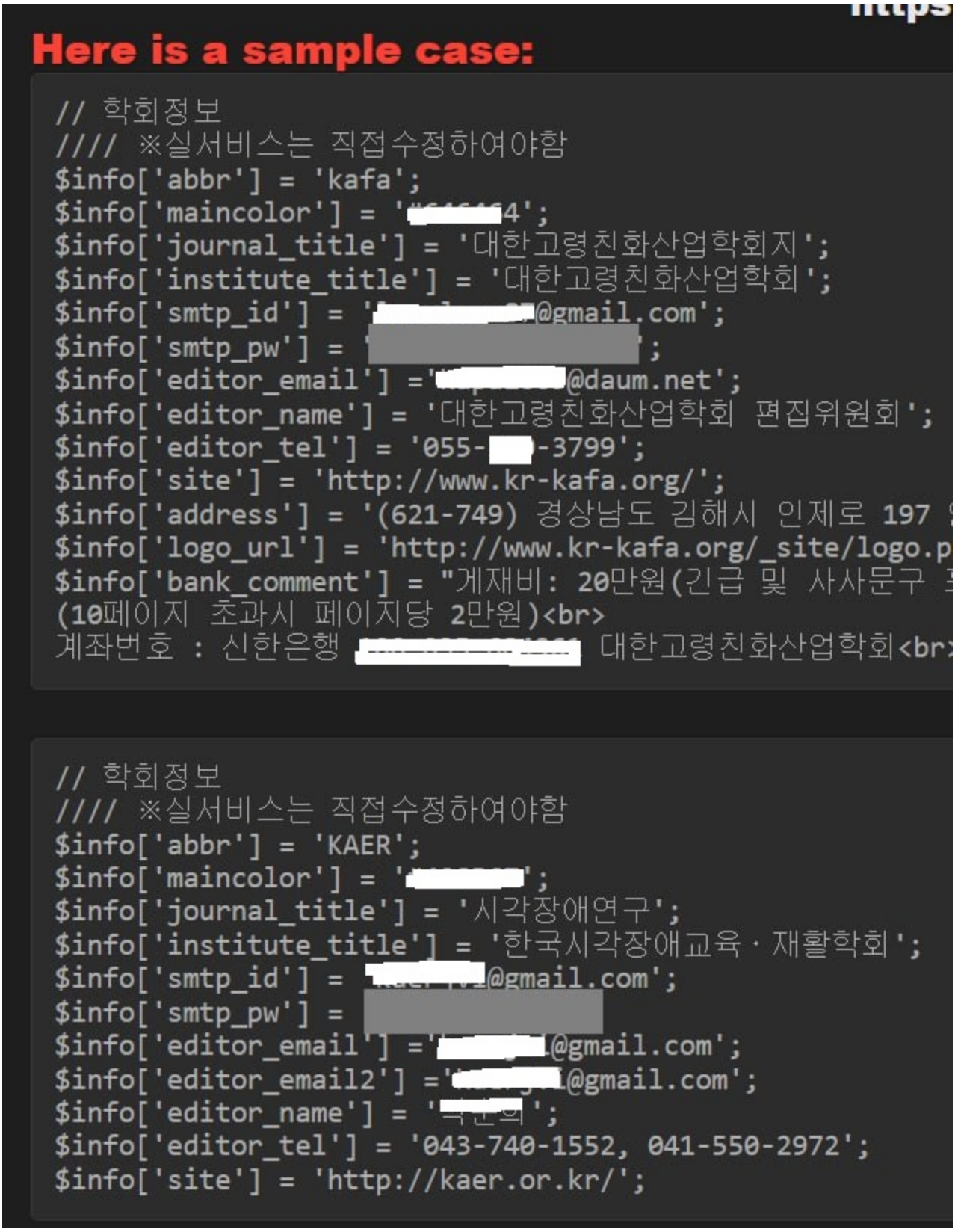
January 24, 2023

중국 샤오치잉’ 조직으로 드러나...각종 학회 등 해킹해 정보 공개 중

KISA를 해킹하겠다고 게시한 글

한국의 2천개 정부, 공공기관 사이트를 해킹하겠다고 선전포고한 중국 해커조직의 정체가 드러났다. 2022년 12월 27일 ‘샤오치잉’(晓骑营. 중국 진나라 시절 군사조직 명칭)이라는 해커 조직이다. 한편 이들은 1월 24일 새벽 3시, 한국인터넷진흥원(KISA)을 타깃으로 사이버공격을 하겠다고 예고까지 한 상황이다. (1차 관련기사: **클릭)**

국내 사이버인텔리전스 전문가에 따르면, ‘샤오치잉’ 조직은 지난해 활동해 왔던 ‘Teng Snake (APT-C-61)’라는 조직으로 확인됐다. 이들은 2021년 경부터 해킹 활동을 시작하며 전세계 각국을 대상으로 사이버 공격을 해 온 조직이다. 이들이 이번에 조직명을 바꿔 ‘샤오치잉’이란 조직명으로 한국을 공격하겠다고 예고한 것”이라고 분석 내용을 전했다.



중국 해커조직들이 이번에 해킹한 학회 사이트 정보를 공개한 이미지

중국 해커들이 내부적으로 공유하고 있는 한국 사이트 해킹 데이터
샤오치잉 조직이 지난해부터 한국을 타깃으로 공격하고 공개한 내용을 살펴보면 다음과 같다.

▲2022.04.30 한국 의료 분야 해킹 주장

▲2022.05.05 한국의료기기산업협회 해킹 및 데이터 유출/판매

▲2022.05.06 한국 국방부 인트라넷 침투 및 기밀문서 탈취 주장

▲2022.12.27 '晓骑营' 샤오치잉이란 조직명으로 활동 시작

▲2023.01.07 한국에 대한 데이터 유출 작전 공표

▲2023.01.17 삼성 내부 해킹 및 데이터 탈취 주장

▲2023.01.20 한국 언론사 30개 공격 예고

▲2023.01.20 한국건설정책연구원 웹사이트 해킹 및 내부 연구원 데이터 유출 공개

▲2023.01.20 한국 공공 및 정부 네트워크 공격 선언, 공격 타겟 한국 정부 도메인 2300여 개 조직내 공유 (우리는 다시 돌아왔다고 언급 / 2022년 5월 한국에 대한 해킹 활동 이후 돌아왔다는 의미로 추정됨)

▲2023.01.20 동아시아연구원 데이터베이스 해킹

▲2023.01.21 한국 교육, 과학, 바이오, 의학 등 연구원 및 협회, 정부, 서울시 해킹 및 데이터 탈취 주장

▲2023.01.23 한국 정부 부처 데이터 54GB 유출 주장

▲2023.01.24 한국 각종 학회 40여곳 해킹 및 데이터 유출 공개

▲2023.01.24 KISA 공격 예고

이번 KISA 사이버공격 예고를 최초 공개한 보안분석가는 “이 조직은 주로 새벽1시까지 일하다가 취침을 했다. 하지만 오늘은 새벽3시에 KISA를 공격하겠다는 글을 올렸다. 아마도 KISA에서 올린 공지글을 확인하고 기분이 상했을 수도 있다”며 “이외에도 국내 41개 학회 리스트를 공개하고 그 중 몇개 서버는 내부망까지 침투해서 서버 소스코드까지 공개한 상태다”라고 전했다.

또 “지난해에도 이들은 한국 사이트들을 해킹해서 회원 정보를 공개한 바 있으며, 최근 삼성을 해킹해 내부데이터라고 주장하며 올린 내용도 있다. 현재 100MB 정도 샘플만 공개했고 추후 2GB 데이터를 추가 공개하겠다고 예고했다. 하지만 실제 삼성을 해킹해서 탈취한 정보인지 협력업체를 해킹한지는 조사해 봐야 한다. 이 조직은 80프로 정도는 신뢰할 수 있고 다소 과장된 내용을 게시하기도 하지만 현재 상황은 심각한 상황이다. 사이버 공격에 대해 정부, 공공, 협회, 기업 모두 각별한 주의를 기울여야 할 상황이다”라고 주의을 당부했다.

★정보보안 대표 미디어 데일리시큐!

-
-
-
-
-

길민권 기자 다른기사 보기