



THE UNITED STATES ATTORNEY'S OFFICE

NORTHERN DISTRICT *of* OKLAHOMA

**FORMER NAVY NUCLEAR SYSTEM ADMINISTRATOR CHARGED WITH  
HACKING THE UNITED STATES NAVY, NATIONAL GEOSPATIAL-  
INTELLIGENCE AGENCY'S COMPUTER SYSTEMS**

**FOR IMMEDIATE RELEASE**

**May 5, 2014**

TULSA, OKLAHOMA—Today, the United States charged two men for their participation in a conspiracy to hack into the computer systems of over 30 public and private organizations, including the United States Navy and National Geospatial-Intelligence Agency, announced Northern District of Oklahoma United States Attorney Danny C. Williams Sr.

The single-count Information alleges that Nicholas Paul Knight, 27, of Chantilly, Virginia, and Daniel Trenton Krueger, 20, of Salem, Illinois, conspired to hack computers and computer systems as part of a plan to steal identities, obstruct justice, and damage a protected computer.

“The Navy quickly identified the breach and tracked down the alleged culprits through their online activity, revealing an extensive computer hacking scheme committed across the country and even abroad,” said U.S. Attorney Danny C. Williams. “We aggressively pursue individuals who steal personal information, especially when they victimize the men and women who bravely defend our country and our Constitution.”

According to the Information, in June 2012, the Naval Criminal Investigative Service (“NCIS”) detected a breach of the U.S. Navy’s Smart Web Move (“SWM”) database. Prior to this breach, the Navy used SWM to manage transfers for service members of all branches of the military. The SWM database stored sensitive personal records, including Social Security numbers, names, and dates of birth, for approximately 220,000 service members. The servers that stored these records were located in Tulsa, giving rise to the venue in the Northern District of Oklahoma.

The SWM hackers were initially known only by their online aliases as members of a hacking group called Team Digi7al (pronounced “Digital”). However, the NCIS investigation, later assisted by investigators of the Defense Criminal Investigative Service (“DCIS”), identified Knight and Krueger as the alleged hackers.

The Information alleges that Knight, Krueger, and other Team Digi7al co-conspirators hacked the computer systems of over thirty public and private organizations to steal sensitive information. The victims included the following organizations:

- U.S. Navy
- U.S. National Geospatial-Intelligence Agency
- U.S. Department of Homeland Security
- AT&T U-verse
- Autotrader.com
- Harvard University
- Johns Hopkins University
- Kawasaki
- Library of Congress
- Los Alamos National Laboratory
- Louisville University
- MeTV Network

- Montgomery Police Department (Alabama)
- Peruvian Ambassador's email (in Bolivia)
- San Jose State University
- Stanford University
- Toronto Police Service (Canada)
- Ultimate Car Page
- University of Alabama
- University of British Columbia (Canada)
- University of Nebraska-Lincoln
- World Health Organization

The Information also charges that Knight served as the criminal organization's self-proclaimed leader and publicist, while Krueger completed the technical hacking work of the SWM database and claimed to do so "out of boredom." One conspirator stated online that the group was "somewhat politically inclined to release the things [they had]," but also because it was "fun, and we can." After hacking these organizations, the defendants and other conspirators posted links to the stolen information on Team Digi7al's Twitter account to make the private information available to the public.

At the time of the hacking attacks, Knight was an active duty enlisted Navy member assigned to the nuclear aircraft carrier USS Harry S. Truman as a systems administrator in the nuclear reactor department. Krueger was a student at an Illinois community college where he studied network administration.

The charges contained in the Information are only allegations. A person is presumed innocent unless and until he or she is proven guilty beyond a reasonable doubt in a court of law.

If convicted, Knight and Krueger face a maximum penalty of five years of imprisonment and a \$250,000 fine, in addition to paying restitution to the victims of the crime. A trial date has not been set.

The case was investigated by the NCIS Atlantic Cyber Operations office in Norfolk, Virginia with the cooperation and assistance of the DCIS Cyber Field Office and other federal, state, and local agencies. The case is being prosecuted by Assistant United States Attorney Ryan Souders, the Computer Hacking and Intellectual Property crimes prosecutor for the United States Attorney's Office.