



Department of Justice

United States Attorney Danny C. Williams, Sr.
Northern District of Oklahoma

FOR IMMEDIATE RELEASE
TUESDAY, MAY 20, 2014
WWW.JUSTICE.GOV/USAO/OKN

CONTACT: Trent Shores
PHONE: (918) 382-2706

FORMER NAVY NUCLEAR SYSTEMS ADMINISTRATOR PLEADS GUILTY TO HACKING INTO U.S. NAVY AND OVER 50 OTHER COMPUTER SYSTEMS

TULSA, OKLAHOMA—Two leaders of a massive computer hacking conspiracy today pleaded guilty in federal court to participating in a plan to hack into the U.S. Navy, the National Geospatial-Intelligence Agency (NGA), and over 50 public and private computer systems to steal thousands of individuals' personal information, obstruct justice, and damage protected computers, announced U.S. Attorney Danny C. Williams Sr.

Nicholas Paul Knight, 27, of Chantilly, Virginia, and Daniel Trenton Krueger, 20, of Dix, Illinois, pleaded guilty to a one-count information containing the allegations, and each face up to five years in prison, a fine of \$250,000, and restitution to the victims. Sentencing is scheduled for August 27, 2014 before U.S. District Judge James H. Payne.

“Cybercriminals think the anonymity of the Internet can obscure their illegal activities and make it impossible to find and apprehend them. That is not true,” said U.S. Attorney Williams. “Criminals cannot hide in cyberspace. We will find you, charge you, and prosecute you to the fullest extent of the law.”

Records indicate that investigators with the Naval Criminal Investigative Service (NCIS), later joined by the Defense Criminal Investigative Service (DCIS), identified Knight and Krueger as the co-founders of a hacking group known as Team Digi7al (pronounced “Digital”), which was responsible for hacking into the U.S. Navy’s Smart Web Move (SWM) database. Prior to this breach, the SWM database stored sensitive personal records, including Social Security numbers, names, and dates of birth, for approximately 220,000 service members. As a result of the breach, over 700 deployed members of the military could not access logistical support for transfers for more than 10 weeks. The servers that stored these records were located in Tulsa, giving rise to the venue in the Northern District of Oklahoma.

The United States advised the court that the defendants, and at least three minors and a citizen of Canada, coordinated their hacking activities over email, IRC chat, and Facebook private messages, including one message in which Knight told Krueger “if anything happens . . . send me a message saying goodbye so we know one of us is caught.” After discovering that Knight regularly accessed the Team Digi7al Twitter account from within the Navy’s network,

NCIS cyber investigators conducted a sting operation in a controlled environment aboard the USS Harry S. Truman, the aircraft carrier on which Knight worked as a systems administrator in the nuclear reactor department. During the sting, Knight hacked into a fake database, which he believed to be real while NCIS monitored his activity.

According to the United States, Knight and Krueger later confessed to leading the Team Digi7al conspiracy. Victims of the Team Digi7al conspiracy include the following organizations:

- U.S. Navy
- U.S. National Geospatial-Intelligence Agency
- U.S. Department of Homeland Security
- MobiTv
- 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 case was investigated by the NCIS Atlantic Cyber Operations office in Norfolk 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 U.S. Attorney Ryan Souders.

###