U.S. Department of Justice

James T. Jacks
Acting United States Attorney
Northern District of Texas

FOR IMMEDIATE RELEASE
THURSDAY, JULY 23, 2009
www.usdoj.gov/usao/txn

MEDIA INQUIRIES: KATHY COLVIN
PHONE: (214)659-8600
FAX: (214) 767-2898

FEDERAL GRAND JURY INDICTS ARLINGTON SECURITY GUARD FOR HACKING INTO HOSPITAL'S COMPUTER SYSTEM

Defendant Allegedly Posted Video of Himself Compromising a Hospital's Computer System on YouTube

DALLAS — A federal grand jury in Dallas has returned an indictment charging an Arlington, Texas, man, who worked as a contract security guard at the Carrell Clinic on North Central Expressway in Dallas, with felony offenses related to his compromising and damaging the hospital's computer system, announced Acting U.S. Attorney James T. Jacks of the Northern District of Texas. Jesse William McGraw, a/k/a "Ghost Exodus," 25, is charged with two counts of transmitting a malicious code. McGraw has been in custody since his arrest late last month on related charges outlined in a criminal complaint.

The indictment alleges that from April 2009 through June 2009, McGraw transmitted malicious code that caused damage to a computer at the Carrell Clinic that maintained patient medical records, giving him the potential to modify and impair medical exams, diagnoses, treatments or care of individuals. The indictment further alleges that during the same time frame, McGraw transmitted malicious code that caused damage to the HVAC computer that controlled the heating, ventilation and air conditioning at Carrell Clinic, giving him the potential to modify the building's HVAC system, resulting in the impairment of patient medical exams, diagnoses, or the care of one or more individuals, and threatened public health and safety. Upon McGraw's arrest, the Carrell Clinic Information Technology staff identified and remedied the numerous compromised computers in the building.

According to the affidavit filed in support of the criminal complaint, McGraw is the leader of the hacker group, "Electronik Tribulation Army." He was employed as a security guard for United Protection Services, in Dallas, and worked the night shift, from 11:00 p.m. to 7:00 a.m. at the Carrell Clinic hospital. McGraw, who used the online nickname "Ghost Exodus," posted pictures on the Internet of the compromised HVAC system and videos of himself compromising a computer system in a hospital.

The affidavit further stated that the investigation revealed that McGraw was planning to use his compromised systems to commit additional crimes on or before July 4, 2009, a date that McGraw, according to the affidavit, called "Devil's Day." He posted videos on the Internet which included admonitions to other hackers to assist him in conducting unauthorized computer intrusions in support of a "massive DDOS" on July 4, 2009. DDOS is an acronym for Distributed Denial of Service, a type of computer attack in which an unauthorized individual assumes control of other computers and uses the massed ability of those computers, over which they have unauthorized access and control, to attack targeted computers. The investigation also revealed that McGraw recently provided United Protection Services his one week notice and his last day of

work was to be July 3, 2009, the day before the scheduled DDOS attack.

An indictment is an accusation by a federal grand jury and a defendant is entitled to the presumption of innocence unless proven guilty. However, if convicted, each count carries a maximum statutory sentence of 10 years in prison, a $250,000 fine and restitution.

Acting U.S. Attorney Jacks praised the investigative efforts of the FBI and Texas Attorney General's Criminal Investigation Division. Assistant U.S. Attorney C. S. Heath is prosecuting the case.

###