U.S. Department of Justice

United States Attorney James T. Jacks
Northern District of Texas

FOR IMMEDIATE RELEASE
FRIDAY, MAY 14, 2010
http://www.usdoj.gov/usao/txn/

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

ARLINGTON SECURITY GUARD, WHO HACKED INTO HOSPITAL'S COMPUTER SYSTEM, PLEADS GUILTY TO FEDERAL CHARGES

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

DALLAS — Jesse William McGraw, who worked as a contract security guard at the North Central Medical Plaza on North Central Expressway in Dallas, pleaded guilty today, before U.S. District Judge Jane J. Boyle, to felony offenses related to his compromising and damaging the hospital's computer system, announced U.S. Attorney James T. Jacks of the Northern District of Texas.

McGraw, a/k/a "Ghost Exodus," 25, of Arlington, Texas pleaded guilty to an indictment charging two counts of transmitting a malicious code. Each count carries a maximum statutory sentence of ten years in prison and a $250,000 fine. McGraw, who has been in custody since his arrest in June 2009 on related charges filed in a criminal complaint, will be sentenced by Judge Boyle on September 16, 2010.

The North Central Medical Plaza houses medical offices and surgery centers, to include the W.B. Carrell Memorial Clinic and the North Central Surgery Center. McGraw, a contract security guard for United Protection Services, generally worked the night shift, from 11:00 p.m. to 7:00 a.m.

McGraw gained physical access to more than 14 computers located in the North Central Medical Plaza, including a nurses' station computer on the fifth floor and a heating, ventilation and air conditioning (HVAC) computer located in a locked room. The nurses' station computer was used to track a patient's progress through the Carrell Memorial Clinic and medical staff also used it to reference patients' personal identifiers, billing records and medical history. The HVAC computer was used to control the heating, ventilation and air conditioning for the first and second floors used by the North Central Surgery Center.

McGraw installed, or transmitted, a program to the computers that he accessed that allowed him, or anyone with his account name and password, to remotely access the computers. He also impaired the integrity of some of the computer systems by removing security features, e.g., uninstalling anti-virus programs, which made the computer systems and related network more vulnerable to attack. He also installed malicious code (sometimes called a "bot") on some of the computers. Bots are usually associated with theft of data from the compromised computer, using the compromised computer in denial of service attacks, and using the computer to send spam. In this case, McGraw admitted that he intended to use the bot to launch a denial of service attack on the website of a rival "hacker" group.

McGraw knew his actions would damage the security and integrity of these stems. He advocated taking these

kinds of actions to adversely affect the integrity of systems in instructions that he posted online for members of his "Electronik Tribulation Army" (ETA) and other individuals interesting in committing crimes against computers.

On February 12, 2009, McGraw abused the trust placed in him and bypassed the physical security to the locked room containing the HVAC computer. At approximately 11:35 p.m., he began downloading a password recovery tool from a website, which he used to re-recover passwords. By February 13, 2009, at approximately 1:19 a.m., McGraw, again without authorization, physically accessed the HVAC computer and inserted a removable storage device and executed a program which allowed him to emulate a CD/DVD device. He remotely accessed the HVAC computer five times on April 13-14, 2009.

On April 28, 2009, at about 1:45 a.m., McGraw abused the trust placed in him as a security guard and accessed without authorization a nurses' station computer. McGraw made a video and audio recording of what he called his "botnet infiltration." While the theme of "Mission Impossible" played, McGraw described step by step his conduct, accessing without authorization an office and a computer, inserting a CD containing the OphCrack program into the computer to bypass any passwords or security, and inserting a removable storage device into the computer which he claimed contained a malicious code or program. The FBI found the CD containing the OphCrack program in McGraw's house and found the source code for the bot on his laptop.

McGraw was aware that modifying the HVAC computer controls could affect the facility's temperature. By affecting the environmental controls of the facility, he could have affected the treatment and recovery of patients who were vulnerable to changes in the environment. In addition, he could have affected treatment regimes, including the efficacy of all temperature-sensitive drugs and supplies.

He was also aware that the nurses' station computer was used to access and review medical records. While he claims that he did not review or modify patient records, and the government is not aware of any evidence to the contrary, by gaining administrator access to these computers he would have had the ability to modify these records if he had taken additional steps to circumvent additional security measures.

The case is being investigated by the FBI and the Texas Attorney General's Criminal Investigation Division. Assistant U.S. Attorney C. S. Heath is prosecuting the case.

###