U.S. Department of Justice

United States Attorney James T. Jacks
Northern District of Texas

FOR IMMEDIATE RELEASE
FRIDAY, MARCH 18, 2011
http://www.usdoj.gov/usao/txn/

MEDIA INQUIRIES: KATHY COLVIN

FORMER SECURITY GUARD, WHO HACKED INTO HOSPITAL'S COMPUTER SYSTEM, IS SENTENCED TO 110 MONTHS IN FEDERAL PRISON

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

DALLAS — Jesse William McGraw, a former contract security guard at the North Central Medical Plaza on North Central Expressway in Dallas, who admitted hacking into that hospital's computer systems, was sentenced late yesterday afternoon by U.S. District Judge Jane J. Boyle to 110 months on each of two counts, to be served concurrently, announced U.S. Attorney James T. Jacks of the Northern District of Texas. In reaching this sentence, Judge Boyle cited the need for those who commit computer crimes to understand the potentially devastating consequences of their actions, to promote respect for the law, and to deter others involved in or contemplating hacking. Judge Boyle ordered McGraw to make restitution to the occupants in the building affected by his criminal conduct, specifically the W.B. Carrell Memorial Clinic, the North Central Surgery Center, and the Cirrus Group.

In May 2010, McGraw, a/k/a "Ghost Exodus," 26, of Arlington, Texas pleaded guilty without a plea agreement to an indictment charging two counts of transmitting a malicious code. He has been in custody since his arrest in June 2009.

During his 11:00 p.m. to 7:00 a.m. shift at the North Central Medical Plaza, McGraw gained physical access to more than 14 computers, 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 codes (sometimes called"bots") on most of the computers. Bots are usually associated with theft of data from the compromised computer, using the compromised computer in denial of service attacks (DDoS), and

using the computer to send spam. McGraw knew his actions would damage the security and integrity of the computers and computer systems. McGraw was the self-proclaimed leader of a hacking organization called the "Electronik Tribulation Army" (ETA). He advocated compromising computers and computer systems in instructions that he posted online for members of the ETA and other individuals interested in engaging in computer frauds and participating in DDoS attacks.

In this case, McGraw admitted that he intended to use the bots and the compromised computers to launch DDoS attacks on the websites of rival hacker groups. ETA's rival hacker groups included "Anonymous," the hacker group currently claiming responsibility for attacks against PayPal and others in support of Wikileaks.

On Feb.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 Feb. 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.

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