MONSTER.COM DATA BREACH

By: Jair Gonzalez
WHO WAS ATTACKED?

- **Monster.com in August 2007**
  - **One of the most visited employment websites in the United States and one of the largest in the world.**
  - **It was established in 1999 by the merger of The Monster Board (TMB) and Online Career Center (OCC) and is now owned and operated by Monster Worldwide, Inc.**
  - **Monster is primarily used to help those seeking work to find job openings that match their skills and location.**
WHAT WAS STOLEN?

- Monster.com’s database breach lead to the lose contact and account data, including user IDs, passwords, e-mail addresses, names, phone numbers, and demographic data. The demographic data that was stolen includes date of birth, gender, ethnicity, and in some cases, the state where the person resides.
WHO WAS AFFECTED?

- **Monster.com’s credibility took a hard hit with a poor demonstration of data protection.**
- **Monster.com’s customers were all affected, which tallies up to a total of 1.3 million customers.**
WHO WAS RESPONSIBLE?

- After the Monster breach was disclosed by researchers at Symantec Corp., Monster defended its policies by pointing out that its network security had not been broken. No one hacked in, after all.

- Rather, the criminals obtained legitimate keys to the system — most likely by phishing or guessing passwords belonging to recruiters with access to Monster’s tens of millions of resumes.
WHO WAS RESPONSIBLE?

- E-mails were sent out to encouraged users to download a Monster Job Seeker Tool, which was in fact a program that encrypted files in their computer and left a ransom note demanding money for their decryption.

- Till now its unknown who were responsible for the robbery of Monster.com’s customer data via Trojan horse emails. The only certain thing known is its source, Servers in the Ukraine.
WHAT HAPPENS NOW?

- Monster.com made the situation look worse for themselves when they waited 5 full days to announce to their customers a warning on its Web site of the data theft and advised that its job seekers should beware of suspicious E-mails asking for personal and financial information.

- To respond, Monster has said it would spend at least $80 million on upgrades to its site, which now include security changes.

Attention USAJOBS® Users

As is the case with many companies that maintain large databases of information, our technology provider (Monster), often is the target of illegal attempts to access and extract information from its database. We recently learned that the Monster database was illegally accessed and certain contact and account data were taken, including user IDs and passwords, email addresses, names, phone numbers, and some basic demographic data. The information accessed does not include resumes. The accessed information does not include - sensitive data such as social security numbers or personal financial data.
WORK CITED

- HTTP://WWW.FUDZILLA.COM/NEWS/986-HUGE-DATA-SECURITY-BREACH-AT-MONSTERCOM