**CWA**

**Crackas With Attitude // DotGovs**

**Criminal History:**

* **Social engineering several high ranking government officials**
* **Doxing ~30K government and military employees**
* **Social engineering and doxing high ranking government officials’ family members**

**CWA, or Crackas With Attitude, is a now defunct hacking group that specialized in social engineering. CWA is best known for their high profile targets, which included close to 30,000 government and military employees, a DNI Director, an FBI Deputy Director, and the Director of the CIA. These hacks, while publically embarrassing, had very little technical background. The majority of the attacks were carried out via social engineering, convincing the victims to give up their information of their own volition.**

**The group was comprised of a surprisingly young group of high school students, many of them 15 and 16, with one of the oldest members being 24. The group was based in the US and UK and carried out their attacks in the name of the Free Palestine movement, expressing extreme anger towards the US’s perceived human rights violations against Palestine and their continued funding of Israel. Their hacking campaign lasted a surprisingly long period of time, considering the high-profile nature of the case against them, and it is believed that the members of CWA, while largely non-technical, did a pretty good job of covering their trail.**

**CWA also carried out certain measures to try to shift blame to other groups. Several members of CWA tried to shift blame for their largest dump, a collection of ~30K military and government employees’ information, to a group called DotGovs. This group was actually a CWA front, a possible attempt at confusing investigators or shifting blame to someone else. They changed Twitter names, possibly to make it appear that the group is larger than it was. By the end, there was a core 4 members and several others who were affiliated.**

**CWA highlighted the need for protection against social engineering. The CIA director used an AOL email address to pass sensitive personal information, long after two-factor authentication became common in every other mailbox except AOL. Several other high profile targets had not protected themselves against social engineering. Much of the fault should fall on ISPs and cell carriers like Comcast and Verizon, who didn’t have policies in place to protect customer’s data from social engineering attacks.**

**Of course, the victims should be blamed for not protecting themselves. Weak passwords and ignorance of the threat were both likely causes of the success of the CWA. At least one of the attacks, was a direct result of the hackers targeting the victim’s family members, with a spearphishing attack against the wife of a high-ranking intelligence official. This parallels very well with what we’re seeing in jihadist hackers, who have been reported as targeting the friends and loved ones of military personnel to gain access to sensitive information.**

**Eventually, all core members of CWA were arrested, in the UK and the US. The personality behind Default is looking at a maximum sentence of 5 years in federal prison after pleading guilty to his charges.**