2-Computerworld-Hackers

By Darlene Storm , Computerworld |

About |

Most security news is about insecurity, hacking and cyber threats, bordering on scary. But when security is done right, it’s a beautiful thing…sexy even. Security IS sexy.

News

Hackers breach DOJ, dump details of 9,000 DHS employees, plan to leak 20,000 from FBI

Hackers social engineered access to a DOJ portal, allegedly downloaded 200GB of data, dumped a DHS staff directory with over 9,000 employee listings and claimed a leak of 20,000 FBI employees are next.

Thinkstock

While some people were enjoying Super Bowl 50, hackers brought the pain to the Department of Home Security by dumping a directory of over 9,000 DHS employee names, email addresses, locations, telephone numbers and titles such as “DHS PRISM Support.” The same Twitter account announced plans to leak data of 20,000 FBI employees – including those who work outside of the US.

The hacker claimed to have downloaded “hundreds of gigbytes of data from a Department of Justice computer.” The unnamed hacker also told Motherboard that the data was obtained after compromising a DOJ employee’s email account, which is what the he used to contact the reporter. The email account wasn’t enough to access a DOJ web portal, but the hacker called the relevant department, social engineered his way in, and gained access to databases via a DOJ intranet.

“So I called up, told them I was new and I didn’t understand how to get past [the portal],” the hacker told Motherboard’s Joseph Cox. “They asked if I had a token code, I said no, they said that’s fine—just use our one.”

The hacker says he then logged in, clicked on a link to a personal computer which took him to an online virtual machine, and entered in the credentials of the already hacked email account. After this, the hacker was presented with the option of three different computers to access, he claimed, and one was the work machine of the person behind the originally hacked email account.

“I clicked on it and I had full access to the computer,” the hacker said. Here the hacker could access the user’s documents, as well as other documents on the local network.

The hacker claimed to have downloaded 200GB of data, although he allegedly had access to 1TB of data. Regarding the DHS employee directory, it contains all manner of directors, managers, specialists, analysts, intelligence staff members and more. Among the over 9,000 titles, some were a surprise such as DHS PRISM Support mentioned previously.

When Motherboard was trying to vet the data, Cox spoke with Homeland Security’s National Operations Center; the reporter’s call was the first NOC had heard about the leak. *[Deny]* The hackers claim it took DOJ a week before the agency realized it had been breached. *[Disappointment]*

The Homeland Security staff directory posted on CryptoBin begins with a message that states, “This is for Palestine, Ramallah, West Bank, Gaza, This is for the child that is searching for an answer.”

If tweets from @DotGovs are accurate, then the hackers plan to dump a directory of 20,000 FBI employees today.

Related: