security affairs

Hackers leaked DHS staff records, 200GB of files are in their hands□

February 8, 2016 By Pierluigi Paganini

A hacker accessed an employee’s email account at the Department of Justice and stole 200GB of files□ including records of 9,000 DHS staffers and 20,000 FBI employees.

Yesterday, the data related a Department of Homeland Security (DHS) staff directory were leaked online, a Twitter account shared the link to an archive containing 9,355 names.

The responsible for the data leakage first contacted□ Motherboard to share the precious archive.

Each record of the DHS Staff Directory includes name, title, email address, and phone number.

Going deep in the archive it is possible to note that it

The same Twitter account has announced later the imminent release of an additional data dump containing 20,000 FBI employees.

Are the records authentic?

Motherboard that obtained the archive reached the operations center of the FBI, and in one case the individual who pick up the phone presented himself with the same name associated with that number in the archive. A similar circumstance occurred with a DHS employee, Motherboard so confirmed that the information is legit.

Which is the source of data?

According to Motherboard, a hacker accessed an employee's email account at the Department of Justice. As proof, the hacker sent the email message to Motherboard's contributor Joseph Cox directly from the compromised account.

"A hacker, who wishes to remain anonymous, plans to dump the apparent names, job titles, email addresses and phone numbers of over 20,000 supposed Federal Bureau of Investigation (FBI) employees, as well as over 9,000 alleged Department of Homeland Security (DHS) employees, Motherboard has learned." wrote Cox in a blog post.

"The hacker also claims to have downloaded hundreds of gigabytes of data from a Department of Justice (DOJ) computer, although that data has not been published."

The hacker first tried to use the compromised credentials to access a DOJ staff portal, but without success, then he called the department directly and obtained the access through social engineering techniques.

The hacker accessed the DoJ intranet where the database is hosted, then he downloaded around the, out of 1TB that he had access to.

"I HAD access to it, I couldn't take all of the 1TB," the hacker told to MotherBoard.

The hackers confirmed his intention to release the□ rest of the data in the near future.Which is the motivation behind the attack?

It is not clear at the moment why the hacker released the archive, surely it's not financially□ motivated. The hacker only left the following message when has leaked the data-

"This is for Palestine, Ramallah, West Bank, Gaza, This is for the child that is searching for an answer…" which are the verses of "Long Live Palestine"

The only certainty right now is that similar incidents are becoming too frequent, apparently the government staff is not properly trained on the main cyber threats or the hacking technique. Similar incidents show the lack of knowledge on the most basic security measures.
Whenever a hacker leaks so sensitive data, I think the number of his peers who had access to the same information with the intent to use them in other attacks or resell them, perhaps to a foreign government.

Pierluigi Paganini

(Security Affairs – DHS, hacking)

Share it please ...

data breach | data leakage | DHS | DoJ | FBI | Hacking

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

Reuse of login credentials put more than 20M Alibaba accounts at risk

NEXT ARTICLE

T9000 backdoor, a sophisticated malware that spies on Skype users

YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6 Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

The IPT ruled that GCHQ spies can legally hack any electronic devices

February 13, 2016 By Pierluigi Paganini

[redacted]

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in□ identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top ^