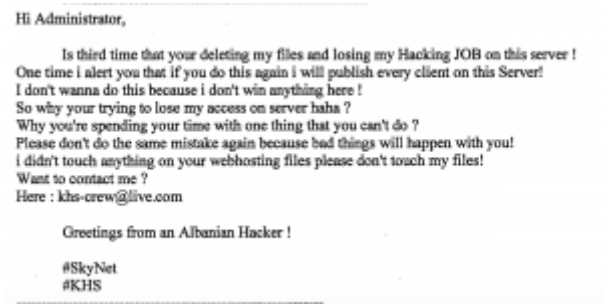
# FBI CAUGHT THEIR ISIS HACKER BY TRACKING HIS SIGNED EMAIL TO HIS SIGNED FACEBOOK AND TWITTER ACCOUNTS


Hi Administrator,

Is third time that your deleting my files and losing my Hacking JOB on this server !
One time i alert you that if you do this again i will publish every client on this Server!
I don't wanna do this because i don't win anything here !
So why your trying to lose my access on server haha ?
Why you're spending your time with one thing that you can't do ?
Please don't do the same mistake again because bad things will happen with you!
i didn't touch anything on your webhosting files please don't touch my files!
Want to contact me ?
Here : khs-crew@live.com

Greetings from an Albanian Hacker !

#SkyNet
#KHS

The FBI just charged an Albanian hacker living in Malaysia, Ardit Ferizi, aka Th3Dir3ctorY, with stealing the Personally Identifiable Information of over 1,000 service members and subsequently posting that PII online to encourage people to target them (he provided the data to, among others, Junaid Hussain, who was subsequently killed in a drone strike).

Given Jim Comey's repeated warnings of how the FBI is going dark on ISIS organizing, I thought I'd look at how FBI found this guy.

- Ardit Ferizi, the suspect's real name, was connected to the @Th3Dir3ctorY account on Twitter. On that account Ferizi linked to an article about the Kosova Hacker's Security group (KHS) for which he had been interviewed. He also identified himself as the owner of KHS.
- Ferizi registered the

Twitter identity to a hotmail account tied to an IP address in Kosovo.

- @Th3Dir3ctorY subsequently logged into Twitter from various ISPs in Malaysia, including 210.186.111.14.
- The hacker who first broke into "Victim Company" on June 13, 2015 and ultimately stole the data of 100,000 people created an account with the identity KHS. On August 19, 2015 – after the company had removed the malware used to exfiltrate the data – someone identifying himself as "Albanian Hacker" and using the email "khs-crew@live.com" contacted the company and asked them to stop taking down their files (which the FBI interpreted to mean the malware left on the server). The IP address tied to the SQL injection used by the hacker was 210.186.111.14.
- A Facebook account tied to the name "ardit.ferizi01" also used that IP address. Ferizi sent himself a spreadsheet via that facebook account with the stolen PII.

In other words, Ferizi apparently did nothing to hide the association between his public Twitter boasting about stealing PII and association with KHS and the hack, down to his repeated email nudges to the victim company (and his attempt to get 2 Bitcoins to stop hacking them). His Twitter account, Facebook account, and email account could all be easily correlated both through IP and name, and activity on all three inculpated him in the hack.

The only mention of any security in the complaint is that Bitcoin account.

Sure, Ferizi was not playing the role of formal recruiter here, but instead agent provocateur and hacker. Still! The FBI is billing this guy *as a hacker*. And he did less to protect his identity then I sometimes use.

At least in this case, FBI isn't going dark on ISIS' attempts to incite attacks on Americans.