Bank of Italy	**BL1001** – Corporate Items	
EL0202 – System Security External - Wilful Damage	EUR – **Not Identifiable LOSS**	**EUR** – Euro
IT – ITALY	**Western Europe**	

Email accounts of Bank of Italy's former executives allegedly hacked using malware

On 10 January 2017, the Italian police arrested two siblings for allegedly hacking about 20,000 email accounts, including those of two former executives of the Bank of Italy.

The two siblings, Giulio and Francesca Maria Occhionero, resident in London but legally domiciled in Rome, are charged with procurement of information about state security, unlawful access to IT systems and illicit interception of communications and telecommunications.

The investigation, which was launched in March 2016 further to a security expert receiving a suspicious email, was carried out with the help of the Federal Bureau of Investigation (FBI). It underlined that the Advanced Persistent Threat (APT) hacking attack was managed through a malware called EyePyramid. The malware sent out an email with an attachment that infected the receiver's email account upon opening. The malware then stole information contained in the emails as well as the user's password via a keylogger, which records all keystrokes made on an infected computer.

Most of the data was stored by the hackers in computer systems in the United States. The emails accounts and relevant passwords were in folders labelled with different nicknames according to the category of the stored data.

According to Roberto di Legami, head of the specialised cyber-crime unit that conducted the investigation, there is no evidence that the information had been sold to a third party or used for blackmail. However, formiche.net suggests that the gathered information was used to carry out favourable investments by Giulio Occhionero.

Il Sole 24 Ore and La Repubblica underlined that from 2011 to August 2016, the hackers accessed over 18,327 usernames, but only obtained the password of 1,793 accounts. Amongst them are addresses of people related to the Italian financial and political world.

The accounts the hackers attempted to access include the accounts of Fabrizio Saccomanni, former governor of the Bank of Italy, as well as the former president of the Bank of Italy, Mario Draghi, who is now the president of the European Central Bank (ECB). Only Draghi's Bank of Italy email account is believed to have been hacked. The two men were targeted through their Bank of Italy email addresses.

Notably, Giulio Occhionero is an engineer related to the financial world as the owner of Westlands Securities. He was also a quantitative analyst and used to be a financial advisor for Monte dei Paschi di Siena (MPS). In 2002 MPS used his system for daily trading operations. He is thought to have been a high-ranking member of a Masonic lodge in Rome. The name of the malware, EyePyramid, is thought to refer to the Eye of Providence, a symbol of an eye inside a triangle, which is associated with Freemasonry.

As of 12 January 2017, the two siblings are under preventive incarceration under request of the Procurement Office. The investigation is still ongoing to clarify the number and extent of hacked accounts. Ibtimes.it confirmed on 12 January 2017 that although the hackers had attempted to obtain Draghi's and Saccomanni's passwords, they were unsuccessful. It is unknown whether they accessed confidential information. Also, as reported by ilfattoquotidiano.it, the two siblings destroyed some of the hacked information. ORX News has reported this story as a story of interest relating to cyber-crime.

Author: Caterina Ciccone
Last Update: 11:06 - 13/Jan/2017

Source(s):

http://www.wsj.com/articles/italy-accuses-two-of-hacking-email-accounts-of-mario-draghi-politicians-1484077973
http://it.ibtimes.com/6-risposte-sullhack-con-eye-pyramid-cose-e-come-funziona-il-malware-spia-dei-politici-e-istituzioni
http://www.repubblica.it/cronaca/2017/01/10/news/cyberspionaggio_polizia_arresti-155733437/?rss
http://www.ilsole24ore.com/art/notizie/2017-01-10/cyberspionaggio-spiati-politici-e-istituzioni-due-

Related Articles

There are no linked loss events

Event	Published in Media	Date of Occurrence – From	Date of Occurrence – To	Discovery Date	Date of Recognition / Settlement
	10/Jan/2017	01/Jan/2011	31/Aug/2016	N/A	N/A

Loss Amount USD **USD Not Identifiable**	Loss Amount EURO **EUR Not Identifiable**	Provision **No**	Boundary Risk **Other Risk**
Industry Event **N/A**	Scenario **ITSEC - IT Security**	Product **PD9900 - Not Product Related**	Process **PC1004 - IT Security**
Parent Company **N/A**	ORX Member **No**	Role of Firm **LS0308 - Not Identifiable**	AMA Status **N/A**
Cause 1 **CS0102 - Assault by Criminals / Terrorists**	Cause 2 **N/A**	Cause 3 **N/A**	
Counterparty **LS0212 - Not Identifiable**	Jurisdiction / Choice of Law **LS0105 - Western Europe (excluding United Kingdom)**	Environmental Volatility **LS0401 - Cultural / Social**	