L-Atti tal-Inkjesta datata 19 ta' Novembru 2019, rigward skont it-Termini ta' Referenza ta' l-Inkjesta Pubblika dwar l-Assassinju ta' Daphne Caruana Galizia.

Seduta miżmuma llum il-Gimgha 19 ta' Gunju 2020, fid-9:30 a.m. fit-Tieni Sular, Awla 20, il-Qorti.

Xhud **Ian Castillo** iben Mark u Angela nee` Dedomenico, imwieled San Giljan u residenti Ta' Sliema bil-Malti u bil-gurament tieghu jghid :

Dr Therese Comodini Cachia :
Sur Castillo, intom kontu hejjejtu rapport fuq istruzzjonijiet jew fuq talba ta' Daphne Caruana Galizia. Jiena r-rapport rajt il-kopja tieghu u ovvjament ftit li xejn nista' nifhem il-konsegwenzi li wiehed - an ordinary person jista' juza jew jista' jahseb fuq dak ir-rapport; allura nitolbok tispjegalna xi jfisser il-komunikazzjoni li jidher f' dak ir-rapport, u x' ifisser per ezempju ghalija li ghandi blog jew ghal qarrej tieghi li jrid li jkollu access.
Ghax dak li hu illegible ghalija ghalih huwa very legible.

Ix-Xhud :
Jekk hu possibbli nixtieq nitkellem bl-Ingliz?

Imhallef A Lofaro :
Mhix problema.

Ix-Xhud :
So the report is rather complex because it contains technical information ....

Imhallef A Lofaro :
Can you speak in the microphone?

Ix-Xhud :
Sorry about that. The report is very technical because it contains information which is needed, if, you know, there is an investigation and there is a lot of technical details that would be required in order to chase the origins of the emails. So essentially background is around 2014 my company started handling some work for Daphne's blog, this included fixing different errors, adding new features and given Daphne some advice on how to improve the

readership on her blog. In February 2017 on Saturday the 11th we received an email requesting some information on how to access blog. The email was not from Daphne although the email looked like it was from her. The email was spoofed essentially.
The person who was sending this email falsifying Daphne continued to send emails to different addresses within our organisation until obviously we realized what was happening and we stopped communicating with this person. The essentially what they were asked....

Imhallef A Lofaro :
Had you have given information though?

Ix-Xhud :
No we had given no information.

Imhallef A Lofaro :
No.

Ix-Xhud :
We did reply to the person before we realized this was a social engineering attempt asking them for more information, but they ignored that request and continue trying different email addresses.

Imhallef A Lofaro :
Ok.

Ix-Xhud :
So if I could just move on to what is significant about this; firstly it is not a standard hacking attempt. Typically hacking attempts stand to be anonymous high volume and automated. There is simply robots which scan servers for weaknesses and then try and explode those weaknesses. Once they find the weakness they automatically try and penetrated. This was an example of social engineering, so this a person who actually knew the names of people within our organization. They knew that obviously we were servicing Daphne Caruana Galizia's blog. They also knew email addresses and they try to explode different avenues to get the information they needed.

Also what is significant is what they were asking for. So they were asking for email servers and DNS records. And what that means is they weren't actually looking to.. although I'm sure they would have used it, but they weren't actually looking for the username and password of the blog itself, to for example take over the blog; they were looking for the details to change

information related to the URL, that is the website address daphnecaruanagalizia.com.
Essentially if they had been given that information they could have used it to send emails on behalf of Daphne which would have originated with her full email address; receive incoming emails which were intended to be send to her and they could have also created a duplicate website daphnecaruanagalizia.com made it an error image of her origin website

Imhallef A Lofaro :
Like a clone then?

Ix-Xhud :
A clone, correct. And publish the information they wanted to and most people wouldn't have noticed until sometime afterwards.

Dr Therese Comodini Cachia :
So if I understand well, if this person would have obtained such information this person would have been able to identify who her sources were?

Ix-Xhud :
Potentially yes. If the sources were sending her emails, which I believe they were..

Imhallef A Lofaro :
Ehe.

Ix-Xhud :
Until .., you know, it was discovered that this person was doing what they were doing, any email sent would have been received by these people.

Dr Therese Comodini Cachia :
And you said something, you said this was social engineering

Ix-Xhud :
Correct.

Dr Therese Comodini Cachia :
And if I understood you well, you differentiating between let say the ordinary hacking were it's a robotic an AI working to find weaknesses and exploiting them, and this was someone specifically intending to do so?

Ix-Xhud :
Correct. Yes, I think that's ..

Dr Therese Comodini Cachia :
This was a targeted specific attack?

Ix-Xhud :
Correct; in fact I've been in this industry for 20 years and the automated hacking attempts were extremely common. We have very strong defences against them, and you know, they …for course there are things you take for granted, and you protect yourself well against them.

Imhallef A Lofaro :
By spyware?

Ix-Xhud :
Sorry?

Imhallef A Lofaro :
Would spyware help?

Ix-Xhud :
Anti-spyware.

Imhallef A Lofaro :
Yes.

Ix-Xhud :
So yes. Its anti viruses

Imhallef A Lofaro :
But then this anti spyware would not help in this case.

Ix-Xhud :
In this case no.

Imhallef A Lofaro :
No.

Ix-Xhud :
And that's what's so unique about this attack

Imhallef A Lofaro :
Ok;

Ix-Xhud :
In 20 years of running a web development company we've handled many you know hacking attempts; there..very ordinary run of the mill. Most of them go unnoticed we have staff to which handles …for us; but this was probably the only case I ever remember where we actually had social engineering that is somebody who carried out the research to try and find out information to exploit that information, and I give the analogy of somebody pretending to be a meter reader to try and get your alarm code for your house

Imhallef A Lofaro :
Yes

Ix-Xhud :
And that's the analogy …

Dr Therese Comodini Cachia :
And are you aware of other similar attacks that were carried out on her blog?

Ix-Xhud :
Yes. So, our services related simply to providing Ms Caruana Galizia with consultancy and minor changes on the blog. The actual blog was hosted by different company; so it wasn't our responsibility to hosted. One attack that I know of was called the DDOS attack

Imhallef A Lofaro :
DDOS?

Ix-Xhud :
DDOS attack yes. They are not very common, but when they do happen essentially they have one aim and that is to drop the website and make it inaccessible for her visitors. Essentially it is flooding the web servers with high volumes of traffic, bogus traffic to the point where the web servers can't cope and exactly they are no longer available ....

Imhallef A Lofaro :
And it clashes…

Ix-Xhud :
Yes. And the attacks are distributed, so its not one source, it's from all over the world and are very very difficult to stop ...

Imhallef A Lofaro :
And for someone to carry out a DDOS attack would it have to be a professional; no?

Ix-Xhud :
Well yes a professional in criminal.

Imhallef A Lofaro :
Not an amateur

Ix-Xhud :
No no. It's under… they can be quite expensive as well ..

Imhallef A Lofaro :
Of course.

Ix-Xhud :
..a resource intensive. And I believe it wasn't just once, if I am not mistaken I remember ..

Imhallef A Lofaro :
How much would this cost such an attempt?

Ix-Xhud :
I'm sorry it's not my of expertise so I wouldn't able to ....

Imhallef A Lofaro :
But it's expensive.

Ix-Xhud :
But yes it's a resource intensive attack.

Imhallef A Lofaro :
Ehe.

Imhallef J Said Pullicino :
When this happens it is indicative of a criminal action basically; do you agree?

Ix-Xhud :
Yes, the..when the time speaking about I believe it is yes.

Imhallef J Said Pullicino :
Correct. And would it ..

Dr Therese Comodini Cachia :
Can I just ask something?, actually comment. It was never in the public domain that this company was servicing Daphne, and I don't know if the witness realizes that what you've just said may well have been reported, so if you don't want to report you need to ask the Board.

Ix-Xhud :
I have no issues

Imhallef J Said Pullicino :
…problem?

Imhallef A Lofaro :
He has no problem, ok.

Ix-Xhud :
I'm sorry I have no main issues.

Imhallef J Said Pullicino :
I was asking, if it was,… I mean to your knowledge that it was a criminal attempt which could involved a number of experts, to your knowledge ..

Imhallef A Lofaro :
It's a crime it's a crime.

Imhallef J Said Pullicino :
Would it you have… your responsibility to report this .. to the police?

Ix-Xhud :
I reported the issue obviously immediately to Daphne Caruana Galizia. She engaged a lawyer and she was giving an advice; but we left it up to her to carry it forward and carry up the police report ..

Imhallef J Said Pullicino :
You are not aware whether there was actually a complaint with the police?

Ix-Xhud :
I believe there was, but I am not one hundred percent sure, because we know that she took it forward.

Imhallef J Said Pullicino :
And you had no means to try and … the source of hacking?

Ix-Xhud :
No. In fact our technical advice although we dropped this report, it contains a lot of technical information, is that essentially when somebody impersonates somebody else via email using a … email address, if they know what they are doing and they don't have to be very very sophisticated, but even if.., you know, they know the basics they can make it impossible to trace and to find out of the..

Imhallef A Lofaro :
And how many times they carry out such an attack?

Ix-Xhud :
So this particular incident of social engineering happened once

Imhallef A Lofaro :
Once.

Ix-Xhud :
And across all our customers, Daphne Caruana Galizia was the only customer of ours in 20 years who had this type of ..

Imhallef A Lofaro :
Can you tell us when this happened?

Ix-Xhud :
Yes; it happened on the 11th of February 2017. The email exchange lasted 2 days – 3 days maximum.

Imhallef A Lofaro :
Ok,

Dr Jason Azzopardi :
11th February 2017.

Imhallef A Lofaro :
February. No more questions?

Dr Jason Azzopardi :
11th February 2017…; wara l-burdell.

Dr Therese Comodini Cachia :
Exactly. The date is important because it is significantly close to the incident on which the previous witness was testifying.

Imhallef A Lofaro :
The Chris Cardona case; ok thank you.

Dr Jason Azzopardi :
Ghaxart ijiem wara biss.

Imhallef A Lofaro :
That's why I asked the date; you know?

Din hija s-sustanza tax-xhieda ta' **Ian Castillo** kif giet dettata minnu stess fil-prezenza ta' l-istess xhud.

Niddikjara li traskrivejt bl-ahjar hila tieghi x-xhieda ta' l-istess xhud.

Saviour Scicluna
Traskrittur