

## **Operation Cabin Q&As**

*The following questions and answers are an abridged version of Norfolk Constabulary's Operation Cabin media briefing held on Thursday 19 July 2012.*

### **How do you know it was an external hack?**

In outline terms, we know it came via the internet from a number of different IP addresses, in various countries, which may have been proxy servers.

The attack was, first of all, into the web server (CRUweb8) in the Climate Research Unit (CRU) at the UEA. From there, a link was established to a CRU back-up server (CRUback3).

It's fair to say, the university has to draw the right balance between giving access to information – it's an academic establishment and, as such, has a proportionate level of security which enables people to work remotely and access information to operate in that academic environment. As a consequence of the attack, the UEA has taken a number of measures and its ICT infrastructure now looks very different.

We identified that the attackers breached several password layers to get through and they got to a position where they employed different methodologies to return the data. We identified a significant quantity of data that was taken in this way, certainly in excess of that which was subsequently published in the two files in 2009 and 2011.

We've used the expression 'sophisticated' and that's because that's the view of our experts who conducted that side of the investigation for us. They identified that, as well as achieving the breach, they also took significant steps to conceal their tracks and lay false trails and change information available to us in order to frustrate the investigation. The conclusion was the person /s were highly competent in what they were doing.

That technical investigation was the primary line of investigation although we did cater for other possibilities, these were later ruled out.

### **Which specific countries were involved in the trail of proxy servers and which countries were either helpful or uncooperative in your investigations?**

While we will not be confirming the names of the countries specifically, we can confirm there were a number across the majority of the continents.

We would underline that the use of a proxy server in any country is not necessarily evidence that the hack originated in that domain.

We worked with partners in these countries and the level of response and support we got varied from being excellent to being quite time consuming.

The logistics involved meant it was a complex picture with different legal jurisdictions and sovereignties. Sometimes it's a procedural issue and sometimes it's a political issue with a small or a big P.

### **Can you confirm that the US was helpful?**

We will not confirm the identity of individual countries but we can say, in general terms, there is a healthy and productive relationship between law enforcement in the US and the UK.

### **Did you detect that any national government could be behind this?**

No. The hypothesis was, and remains, that the person or persons responsible for this could be anyone on a spectrum from an individual right through to the other end of the spectrum, including commercial organisations and governments. It is obvious that some commercial organisations would have an interest in maintaining their commercial position; similarly there will be economies and governments which have an interest in protecting their position. To be clear, we did not get any indication as to who was responsible.

**It is clear the person responsible has knowledge of this subject; did you interview all the bloggers that showed an interest?**

We interviewed a number of people and the logistical issues involved meant that much of this work was carried out remotely because, physically travelling to countries, and the logistics involved in achieving that – for the anticipated outcome – would have not be proportionate.

Of course, the climate sceptic community would, in the main, give the appearance of welcoming the published data because it supports their view. Therefore, we were realistic about the prospect of them being helpful to our investigation.

**Can you describe what investigations you undertook at the UEA and who you interviewed there?**

The focus internally was on the IT infrastructure and working out from there. We also looked at people working at or with connections to the Climate Research Unit and, in simple terms, we were looking for anything obvious. All members of staff were interviewed. If someone had some obvious links or had an axe to grind, then that might have been a line of enquiry.

Generally speaking, it was a screening exercise which did not provide any positive lines of enquiry.

Whilst - because we have not found the perpetrators - we cannot say categorically that no one at the UEA is involved, there is no evidence to suggest that there was. The nature and sophistication of the attack does not suggest that it was anyone at the UEA.

**You say that the hacker had to go through a series of passwords; do you know that someone at the UEA would not have had access to these passwords?**

Anyone with access to these passwords has been excluded as a suspect. Additionally, there was some evidence of work undertaken to break passwords.

**It has been reported that the hacker accessed the server on three separate occasions, can you confirm if that's true and if there were any further attempts to access the server after 'climategate' broke and have there been any recently?**

The report is inaccurate. The attack was conducted over a period of time and access would have occurred on a number of occasions and certainly more than three. Of course, we only know what we know. I have already described it was a sophisticated attack; we have established a substantial amount of what happened. What I can't say is whether we have established everything that happened.

There were no further data breaches once the story had broken in November 2009, not least because we had taken possession of Cruback3 and it wasn't available to be accessed.

**Do you know when the attacks began?**

There's a timeline of events and there has been speculation, in the media and the blogs, that there may have been an orchestrated campaign of Freedom of Information requests to the University in the summer of 2009. It appears the attacks were undertaken late in that summer, early autumn, through to November. The first tactic that we were aware of was in September 2009.

**There was news that some other institutions, including in Canada, that may have come under a similar attack at that time. Are there any other institutions that you have found that were attacked at this time?**

We did have some dialogue and there were one or two that had been attacked and we did have a preliminary examination but they did not give us any indication or cause to suspect that it was in any way linked to the UEA.

**What happens to Cruback3 now?**

It has been returned to the University of East Anglia, having been retained as an exhibit through the course of the investigation. It was necessary to retain the actual server for this time. It contained a massive amount of data, something in the region of five terabytes.

**When the second batch of e-mails was released, there was the note that came with them. Did you or your colleagues contemplate doing structural linguistics or analysis to try and trace it to a particular location in the world?**

It was speculated on and it was something we did consider. Our conclusion was that it would be unlikely to take the investigation anywhere and, in fact, if you are trying to conceal your tracks it could have been constructed to mislead.

**You have been restricted by the statute of limitations, would you have continued with this investigation otherwise?**

The decision to close the case was a combination of the time limit and an acknowledgement that we had pursued this as far as we reasonably can.

**Did you consider prosecuting people dealing in the information that was clearly stolen?**

In terms of offences committed, it becomes a much greyer area. The same challenges exist in terms of identifying those individuals. An operational decision was made not to pursue this.

<Ends>