HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON INFRASTRACTURE AND COMMUNICATIONS

AUSTRALIAN FEDERAL POLICE

Question No. 1

The Committee asked the below question at the hearing on 29 October 2014:

Mr Zuccato: We have to also appreciate that the telco's do not just cooperate in relation to this one area; we are knocking on their door every day and, in the main, the major providers are very, very helpful within the parameters that they have. One thing I heard you ask about earlier was an example of when something goes wrong and when we have to block. I do not need to bore you at the moment, but we do have one example: Gameover ZeuS, which was a botnet that delivered malicious payload and encouraged consumers to divulge their details. We would be more than happy to provide you with a snapshot, a summary, of what that looks like so that you get an idea of when something like this hits that we need—and, again, that is why I think the legislation is really useful. We need to move really fast because the whole judicial process takes times—if we have got to type documents and so forth—to do something that simply makes something stop, right. We are not asking for information—we're just saying, 'Look, this needs to stop.'
The example would be the ability for me to go outside and identify that there is a threat coming up the road and ask my people to erect bollards so that folks cannot get into this building. That is what this is about, right? It is simply staying: 'Stop. You can't come. You can't enter.' And it allows us to do what we need to do at the back. This is a really useful little couple of pages that deal with a botnet that did exactly—Gameover ZeuS was a really famous episode—and it just shows you what happens and the reasons why we take those immediate actions and the reasons why we utilise 313(3), in particular, to do what we do for very limited instances.
CHAIR: That would be great.

The answer to the Committee's question is as follows:

In April 2014, the AFP's Cyber Crime Operations was approached by the Federal Bureau of Investigations (FBI) with information concerning a disruption operation being planned against the botnet known as "GameOver Zeus".

GameOver Zeus (GOZ) is a peer-to-peer banking malicious software (malware) which is designed to steal personal banking/financial information, such as login credentials, from the platforms of computer users. GOZ is suspected of infecting anywhere from 500,000 to 2 million computers worldwide at any one time.

It is suspected that GOZ activity has led to the loss of millions of dollars through electronic funds transfers. Infected systems can also be used to engage in other malicious activities, such as ransomware infections, sending spam or participating in distributed denial-of-service (DDoS) attacks.

The FBI publicly noted that GOZ was responsible for the theft of more than $US100million, obtained by criminals using the stolen banking credentials to access the victims' bank accounts and diverting the money to themselves or other criminals.

A Russian national, Evgeniy Michailovich Bogachev, the alleged administrator of the network was charged in the United States with 14 counts which included conspiracy, computer hacking, wire fraud, bank fraud and money laundering in the GOZ and other malware schemes.

Bogachev is not in custody and is believed to be residing in Russia.

The AFP assisted the FBI in the global take down of GOZ by liaising with and requesting Australian based ISP's, using section 313 (3) to block suspect domains, as provided by the FBI.

The AFP worked with two Australian ISP's to block their customers from connecting outbound and inbound to several thousand .ru domain names which were supporting the command and control infrastructure for GOZ. (Note: .ru is the internet country code top-level domain for the Russian Federation).

These domain names were automatically produced with a unique algorithm and were of such randomness, length and complexity that is was highly unlikely they were going to match other domain names in existence.

As a result the AFP were confident that the section 313 (3) request was unlikely to inadvertently resulting in the blocking of a website conducting lawful activity.

As the .ru domains were blocked to the vast majority of Australian internet users through the AFP section 313 requests, the malware was rendered impotent. The malware didn't disappear from the infected computers, but it was rendered useless as it had no 'mothership/s' to connect to in order to perform functions such as updating itself and exfiltrating stolen data.

Malware such as GOZ receives control and update data to remain connected to the botnet and to be potent/viable. Banks, security researchers, anti-virus companies and the like release updates and secure defences against malware, so malware itself needs to be constantly re-engineered and updated to defeat these defences.

In the GOZ example, the AFP's actions effectively rendered the malware useless in Australia, whilst the AFP worked collaboratively with the FBI to identify suspects.