Cyber threats at the G20 (and why they don't pose much of a risk)

November 11 2014, by Robbie Fordyce And Thomas Apperley

The G20 might seem like a tasty target for hackers, but any real threats will come from elsewhere. Credit: Imaginary Museum Projects: News Tableaus/Flickr, CC BY-ND

You might have seen reports that the Australian Signals Directorate (ASD) has issued cyber security advice ahead of the G20 Leaders Summit in Brisbane this weekend. So under the watchful eye of the media and countless security agencies, will the meeting be hacked?

The answer depends on what people think might be involved in "hacking" the G20. Popular wisdom suggests "hacking" involves a large amount of information centrally held by 20 national governments being moved from a secure site into the hands of nefarious criminals.

Or perhaps ideologically blinkered anarchists or radical theocrats will use technical measures to disrupt the proceedings of the Summit, resulting in a colossal and fundamental shift in the international balance of power.

If this is what hacking the G20 is, then the short answer is simply "no" – the G20 will not be hacked in the way that people imagine. But that's not to say there definitely won't be some kind of digital disruption on the weekend.

Press pressure

The main reason that there will be no significant hacking of the Leader's Summit is that the G20 is most important as a media event. This is plainly obvious when one looks at the conference details: there are 7,000 registered attendees for the G20 Leader's Summit, of which 3,000 are media representatives.

The event is mainly held in order to retain a semblance of a democratic component in the bargaining between nation states. Perhaps this is why there has been such a focus on Tony Abbott threatening to "shirtfront" Vladimir Putin in recent weeks – it's a good way to sell newspapers.

It's a particularly important place for Abbott and co as a space to flex political muscle to the public, as Australia does not happen to have much authority at more influential economic forums, such as the World Bank, the IMF and Davos.

There are ways in which cyber security may well shape some parts of the G20 conference. The question of hacking is being raised more readily given that digital networks are, in recent years, more frequently becoming a component of political dissent (used by Anonymous, Lulzsec, the Honker Union, Wikileaks and others).

The G20 is a political exercise for many of its member states, where significant figures gather together in board rooms and eat shrimp cocktails. The G20 has websites, staff, infrastructure and other resources that are used to hold the event and give it publicity, but the events that take place are generally public speeches that the media are already present for, and which aren't particularly technical in nature.

The G20 Leader's Summit is in many ways a company retreat, and is about as hackable as a dinner party. Because of this, the G20 holds no particular special resources or secrets that people might steal or disrupt. What is at stake, and what hacking may contribute to, is the war of political credibility which will play out at the end of this week.

Gone phishing

It's worth reading closely into the briefing from the ASD; specifically the passages where they refer to the risks of "phishing" attacks as being the main means by which the G20 conference will infiltrated.

Phishing attacks are almost completely non-technical attacks, and are much better described as a type of "social hacking", which relies simply on a user clicking on a link to download malware to their computer.

This is a fairly trivial thing to avoid, and is a commonplace part of online security to anyone even remotely familiar with the use of email. As a colleague noted, this suggests that the ASD does not have a high opinion of the digital literacy of the G20 attendees.

Cyber war … or PR exercise?

What may happen is that people or delegates associated with the G20 may well end up being the targets of cybernetic attacks.

First, we may see a PR war between G20 and activists. Activist hackers (awkwardly known in some circles as "hacktivists") tend to focus on publicly visible displays of success, such as defacing websites or releasing personal information.

This is general done in order to prove the weakness of large institutions in the face of small but talented computer users, such as the occurrences around the MasterCard blog defacement in 2010, and the periodic attacks by nationalistic hackers who target government websites in other nations (such as Pakistani hackers defacing Indian government websites, Indonesians defacing Australian websites and a host of anti-Israeli defacements).

The result is supposedly that large and powerful nation states end up with a bit of pie on their face for being unable to prevent such an occurrence, but the long-term damage is fairly minimal.

We can see a bit of a history here with the Paris G20 Leader's Summit in February 2011, where the French Ministry of Finances had a number of infections perpetrated by "Asian countries", or the fact that the ASD's G20 cyber security briefing is informative insofar as it is warning people about the threat to Australian businesses, rather than the G20 itself.

International espionage

The second type of hacking that might occur at the G20 would be the various nations spying on each other. This, though, is something that we are less likely to find out about. Thanks to leaks from those such as Edward Snowden and Chelsea Manning, we are well aware of the extent to which nations continue to spy on each other.

While the ill-fated feline spies of Project Acoustic Kitty are behind us, digital espionage is still alive and well.

In fact, historical evidence would suggest that host nations tend to be the biggest spies, with the British intelligence organisation Government Communications Headquarters (GCHQ) closely monitoring the cellular and terrestrial internet use of other nations during the 2013 G20 Summit in London.

Given Australia's relationship to spying on other nations, and Abbott's reluctance to proffer apologies, we should consider what threats Australia may hold for other nations.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Cyber threats at the G20 (and why they don't pose much of a risk) (2014, November 11) retrieved 14 May 2024 from https://phys.org/news/2014-11-cyber-threats-g20-dont-pose.html