A state actor has targeted Australian political parties – but that shouldn't surprise us

Tom Sear

February 18, 2019 10.44pm AEDT

The Australian political digital infrastructure is a target in an ongoing nation state cyber competition which falls just below the threshold of open conflict.

Today Prime Minister Scott Morrison made a statement to parliament, saying:

The Australian Cyber Security Centre recently identified a malicious intrusion into the Australian Parliament House computer network.

During the course of this work, we also became aware that the networks of some political parties - Liberal, Labor and the Nationals - have also been affected.

But cyber measures targeting Australian government infrastructure are the "new normal". It's the government response which is the most unique thing about this recent attack.

The new normal

The Australian Signals Directorate (ASD) – which incorporates the Australian Cyber Security Centre (ACSC) – analyses and responds to cyber security threats.

In January ASD identified in a report that across the three financial years (2015-16 to 2017-18) there were 1,097 cyber incidents affecting unclassified and classified government networks which were "considered serious enough to warrant an operational response."

These figures include all identified intrusions. The prime minister fingered a "sophisticated state actor" for the activity discussed today.

Cyber power states capable of adopting "sophisticated" measures might include the United States, Israel, Russia, perhaps Iran and North Korea. Suspicion currently falls on China.

Advanced persistent threats

Cyber threat actors with such abilities are often identified by a set of handles called Advanced Persistent Threat or APTs.

An APT is a group with a style. They are identifiable by the type of malware (malicious software) they like to deploy, their methods and even their working hours.

For example APT28 is associated with Russian measures to interfere with the 2016 US election

Some APTs have even been publicly traced by cyber security companies to specific buildings in China.

APT1 or Unit 61398 may be linked to the intrusions against the Australian Bureau of Meteorology and possibly the Melbourne International Arts Festival. Unit 61398 has been traced to a non-descript office building in Shanghai.

The advance in APT refers to the "sophistication" mentioned by the PM.

New scanning tool released

The ACSC today publicly released a "scanning tool, configured to search for known malicious web shells that we have encountered in this investigation."

The release supports this being called a state sponsored intrusion. A web shell is an exploitation vector often used by APTs which enables an intruder to execute wider network compromise. A web shell is uploaded to a web server remotely, and then an adversary can leverage other techniques like privileges and issue commands. A webshell is a form of a malware.

One well-known shell called "China Chopper" is delivered by a small web application, and then is able to "brute force" password guessing against the authentication portal.

If such malware was used in this incident, this explains why politicians and those working at Australian Parliament House were asked to change their passwords following the latest incident.

Journalism and social media surrounding incidents such as these pivot on speculation of how it could be an adversary state, and who that might be.

Malware and its deployment is close to a signature of an APT and requires teams to deliver and subsequently monitor. That the ACSC has released such a

specific scanning tool is a clue why they and the prime minister can make such claims.

An intrusion of Australian Parliament House is symbolically powerful, but whether any actual data was taken at an unclassified level might not be of great intelligence import.

The prime minister's announcement today suggests Australian political parties have been exposed.

How elections are hacked

In 2018 I detailed how there are a few options for an adversary seeking to "hack" an election.

The first is to "go loud" and undermine the public's belief in the players, the process, or the outcome itself. This might involve stealing information from a major party, for example, and then anonymously leaking it.

Or it might mean attacking and changing the data held by the Australian Electoral Commission or the electoral rolls each party holds. This would force the agency to publicly admit a concern, which in turn would undermine confidence in the system.

This is likely why today the prime minister said in his statement:

I have instructed the Australian Cyber Security Centre to be ready to provide any political party or electoral body in Australia with immediate support, including making their technical experts available.

They have already briefed the Electoral Commissions and those responsible for cyber security for all states and territories.

They have also worked with global anti-virus companies to ensure Australia's friends and allies have the capacity to detect this malicious activity.

Vulnerability of political parties

Opposition Leader Bill Shorten's response alluded to what might be another concern of our security and electoral agencies. He said:

… our party political structures perhaps are more vulnerable. Political parties are small organisations with only a few full-time staff, they collect, store and use large amounts of information about voters and communities.

I have previously suggested the real risk to any election is the manipulation of social media, and a more successful and secretive campaign to alter the outcome of the Australian election might focus on a minor party.

An adversary could steal the membership and donor database and electoral roll of a party with poor security, locate the social media accounts of those people, and then slowly use social media manipulations to influence an active, vocal group of voters.

Shades of grey

This is unlikely to have been the first attempt by a "sophisticated state actor" to target networks of Australian political parties. It's best not to consider such intrusions as if they "did or didn't work."

There are shades of grey.

Adversaries clearly penetrated a key network and then leveraged access into others. But the duration of such a presence or whether they are even still in a network is challenging to ascertain. Equally, the government has not suggested data has been removed.

Recognition but no data theft may be a result of improved security awareness at parliament house and in party networks. The government and its administration have been taking action.

The Department of Parliamentary Services – that supplies ICT to parliament house – has improved security in "network design changes to harden the internal ICT network against cyber attack".

This month a Joint Committee opened a new inquiry into government resilience following a report from the National Audit Office last year which found "relatively low levels of effectiveness of Commonwealth entities in managing cyber risks".

Government response is what's new

As the ASD and my own observation has noted, this is likely not the first intrusion of this kind – it may be an APT with more "sophisticated" malware than previous attempts. But the response and fall out from the government is certainly new.

What is increasingly clear is that attribution has become more possible, and especially within alliance structures in the Five Eyes intelligence network –

Australia, Britain, Canada, New Zealand and the United States – more common.

Sometimes in cyber security it's challenging to tell the difference between the noise and signal. The persistent presence of Russian sponsored trolls in Australian online politics, the blurring of digital borders with China and cyber enabled threats to our democratic infrastructure: these are not new.

Australia is not immune to the new immersive information war. Digital border protection might yet become an issue in the 2019 election. In addition to raising concerns our politicians and cyber security agencies will need to develop a strong and clear strategic communication approach to both the Australian public and our adversaries as these incidents escalate.