briefing note 390 March 2019

Cyber Attack on the Australian Parliament and the Lessons Learned

The following article was published by the Australian Outlook on March 4th, 2019. It highlights some of the most important technical and political points regarding the recent cyber attack against the Australian Parliament Network and other political parties.

Risk Frontiers are a partner in the Optus Macquarie University Cyber Security Hub focusing on quantitative risk modelling of cyber risks.

Synopsis:

In the lead up to the federal election, the Australian Parliament and multiple political parties have been hit by a sophisticated cyber attack. Experts are divided on who is to blame but the attackers had clear motives and there are some key lessons to learn from this incident.

By *Associate Professor Christophe Doche, Dr Stephen McCombie and Dr Tahiry Rabehaja*

On February 8, reports emerged regarding an attempt to infiltrate the Australian Parliament network, which is primarily used to exchange emails and store data. On February 18, Prime Minister Scott Morrison and Opposition Leader Bill Shorten addressed the Parliament to acknowledge the attack. The next day, the Australian Cyber Security Centre (ACSC), which is now part of the Australian Signals Directorate (ASD), confirmed that a cyber actor gained illegal access to the networks of the Liberal, Nationals and Labor parties.

Since then, investigations have revealed that the attack was sophisticated and most likely state-sponsored. It is understood the initial breach was the result of a phishing campaign, where a staff member opened an infected document attached to an email. Once the criminals got a foothold on a computer attached to the network, they scanned and infected other targets, including intranet servers. They were then able to redirect network traffic in order to exfiltrate data. They also erased logs to cover their tracks and placed additional malware to maintain control of the infected systems for later use.

A digital forensics analysis has shown that the attack relied on a series of malware and exploits, which happened to be in several cases slight modifications of existing open source tools. That is what fooled primary anti-virus software. Many of these open source tools are ironically used by the ethical hacking community to find vulnerabilities in computers and systems with the aim to report and, ultimately, fix them. They are written in the popular language C# for the .NET framework. All these factors indicate there was a clear desire from the attackers to remain undetected for as long as possible and to make attribution – the identification of the perpetrators of the attack – a difficult task.

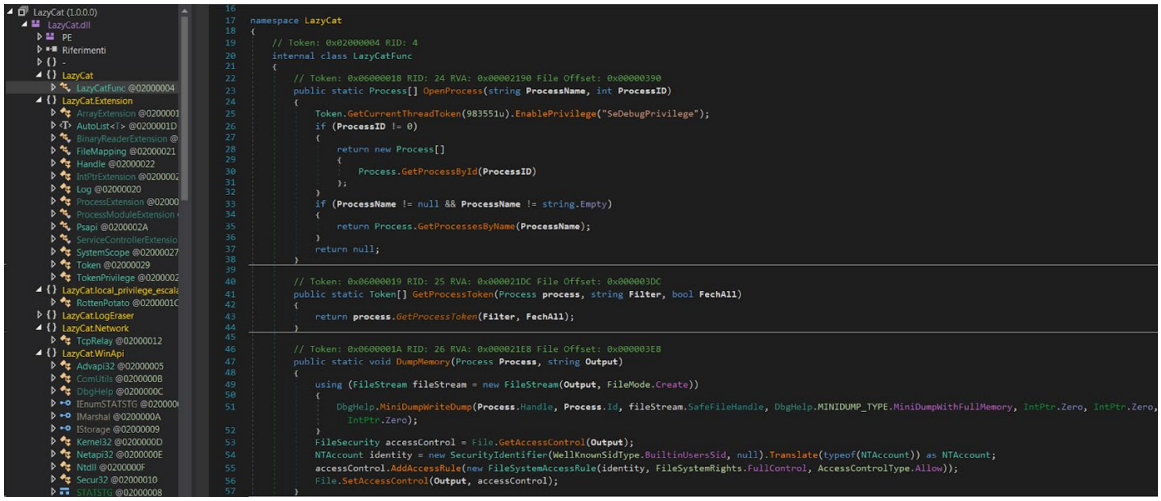

Figure 1: Reverse engineering some parts of the malware used by the hackers shows that they leverage on well-known penetration testing tools (source: Yoroi).

Although there is no clear evidence – at least none that has been released – the media speculation is that China is most likely behind this attack. China has a long history of cyber espionage operations globally and also locally against the Australian Government, our defence sector, mining industries and even universities. This incident happened on the back of the banning of Huawei from Australia's 5G network, recent tensions in regard to trade and multiple claims of improper Chinese influence on Australian political parties. There have also been reports that Iran may have been the perpetrator but it is difficult to see what they would gain in Australia from such an action. They have been active in recent times against US targets and perhaps may see Australia as a way into the Five Eyes intelligence alliance or alternately our close relationship with Israel (their bitter enemy) and plans to formally recognise West Jerusalem as the capital of Israel may have made us a target.

Perhaps most surprising is that this attack was actually successful at getting into the Parliament and Australia's major parties, despite the amount of warning of the potential for such attacks to occur. Attacks on the Democratic National Committee in the United States in 2016, which accessed multiple email accounts including that of Hillary Clinton's campaign director, by Russian Military Intelligence (GRU) are well known and documented. In the aftermath, members of the Democratic Party visited a number of European countries and spoke to political parties to specifically warn of the risk of such cyber breaches. Similarly, the ASD briefed political parties on threats to our elections in 2017. In July 2018, the Australian Government also offered $300,000 to help political parties shore up their cyber security. In addition, the Government has significantly grown the scope and size of the ACSC and other cyber capabilities. Despite this, these attacks have penetrated our Parliament and major political parties just months before a highly contested election where matters of relations with China are likely to be debated.

One key observation here is that the Government has a very large cyber risk footprint. It employs tens of thousands of employees and human beings have always been part of cyber security issues and solutions. This incident is no exception. Governmental networks are

complex, shared and scaled infrastructures, which greatly increases the chance of overlooking security lapses and facilitates the propagation and replication of attacks to other agencies cheaply and quickly. Government agencies are also very attractive targets. They hold a large volume of confidential and personally identifiable information, they are the top target for politically motivated attackers and cyber warfare, and they are amongst the main victims of cyber espionage. This means that they are attracting multiple categories of threat actors ranging from organised cyber criminals looking for financial gains to advanced persistent threats backed by state actors. The Australian Parliament network incident emphasises these three points, but also highlights the Government's large cyber attack surface area, since such an attack could have occurred in any one of the many interlinked agencies' digital information and infrastructure.

Although the response to this incident has been swift and there is no evidence that any data has been leaked, the ACSC has warned that the actor, whoever it may be, will probably further target other Australian Government departments. The Government needs to understand, build and protect its digital infrastructure, and associated exposure, with the appropriate controls and responses. The NSW Government and the Government Chief Information Security Officer have taken a leading role in this area by releasing in February 2019 the NSW Cyber Security Policy. Among other measures, this policy mandates every agency to identify its crown jewels – its most valuable or operationally vital systems or information – and implement regular cyber security education for all employees, contractors and outsourced ICT service providers. These two measures alone will go a long way to improve the cyber resilience of NSW Government agencies.

Associate Professor Christophe Doche is executive director of the Optus Macquarie University Cyber Security Hub, the first initiative of this kind in Australia, linking academics in information security, business, criminology, intelligence, law and psychology together with cyber security experts from industry. As part of his role, he oversees research, education and thought leadership activities in cyber security.

Dr Stephen McCombie is a senior lecturer in Cyber Security at Macquarie University. His current research interests are in digital forensics, cyber threat intelligence and information warfare. His research draws on a diverse background in policing, security and information technology over the last 30 years. He has also held senior positions in information security with IBM, RSA, National Australia Bank and most recently SecureWorks.

Dr Tahiry Rabehaja is a Software Engineer at Risk Frontiers and research fellow at the Optus Macquarie University Cyber Security Hub specialising in quantitative risk modelling. He has a background in information security and formal program verification and, in particular, the development of mathematical models for quantifying confidentiality in programs. His current research is on the quantification of cyber security risk.