TriskeleLabs
DEMYSTIFYING CYBERSECURITY

☎ 130024CYBER 🌐 www.triskelelabs.com
info@triskelelabs.com
⚑ Level 14, 60 Albert Rd
South Melbourne VIC 3205

Nick Morgan
CEO
Triskele Labs Global Pty Ltd

Date: 19 June 2020

Subject: Cyber-attack on the Australian Federal Government – June 2020

Triskele Labs are aware that, this morning the Prime Minister of Australia, Hon Scott Morrison, has made an announcement that the Federal Government have identified a large-scale cyber-attack on Government agencies and Critical Infrastructure by an un-named Nation State. The first signs point to this being related to Telerik , IIS deserialization, 2019 Sharepoint and 2019 Citrix vulnerabilities identified by the Australian Cyber Security Centre (ACSC) across early 2020. The Triskele Labs Security Operations Centre (SOC) have assisted several clients who have been hit by these attacks and suffered compromises. Our immediate advice and guidance includes the following cybersecurity hygiene:

- Ensure all externally facing systems are patched 100% up to current levels
- Implement Multifactor Authentication (MFA) on all login systems
- Conduct ongoing Vulnerability Scanning of all external and internal systems
- Undertake at least annual Penetration Testing (or following a major release)
- Deploy a 24x7x365 monitoring service that includes User Behaviour Analytics
- Ensure endpoint security tools are deployed holistically, up to date and working as expected

Furthermore, it has been advised that if these attacks failed, the Nation State launched attacks leveraging techniques utilised heavily by the Triskele Labs Offensive Security team following a sophisticated attack pattern:

- Utilising credential harvesting and dark web resources to gather usernames and possible passwords
- Launching phishing attacks (spear and mass) to gain legitimate credentials
- Utilising these credentials to login to Office365 and other resources such as VPNs
- Launching password spraying utilising compromised passwords
- Targeting accounts without MFA, or with unregistered MFA
- Moving laterally through Office365 searching for stored credentials (such as insecure password files)
- Leveraging open source, custom and known tools to quietly move through the network
- Creating a new Domain Admin account using a compromised privileged account for persistent access

It is imperative that a Defence in Depth approach is taken and a systematic approach to testing these controls is followed. The world is moving at an extreme pace with more and more systems being interconnected, increasing our attack surfaces. We also highly recommend engaging a specialist firm to undertake Attack Simulation (Red Teaming) to mimic the behaviour of a sophisticated actor in a campaign such as that affecting Australia right now. In the short to medium term, we recommend reviewing your approach to mail filtering and endpoint protection to leverage tools that will provide a safety net should other controls fail. In addition, we also highly recommend running a password cracking exercise on your Active Directory to identify weak or generic passwords. We are expecting more details to come to light and will update on our blog (please see the website) as more details are released.

If you require assistance with any of these controls, please reach out on 130024CYBER. We provide one of the only ISO27001 certified 24x7x365 Security Operations Centres running 100% from Australia to Australian businesses. In addition, our highly skilled CREST Red Team is ready to challenge your best defences.

Regards,

Nick Moran

CEO