CyberGuard Technologies

Proactive Cyber Defence Report

September 2017

The Scottish Parliament, this week, alerted the 129 Members of the Scottish Parliament and staff that their email accounts were being targeted in unauthorised login attempts. Whilst there is currently no evidence to suggest that the access attempts succeeded, the attack appears to be a standard scanning attack on accounts, where a tool continually tries different passwords for given logins. The system will normally lock-out after a number of incorrect logins, but could lock-out the user until there is a reset on the account. The email accounts targeted in the attacks, which use the "parliament.scot" domain, are Office 365 accounts. The attack against the Scottish Parliament email accounts follow a similar effort, in June, against members of the House of Commons and the House of Lords, as well as their staff. Parliament officials said about 90 accounts were compromised in those attacks. It's unclear if the attack against the Scottish Parliament was launched by the same individual or group.

CyberGuard is seeing a sharp rise in attacks on Office 365 users. We have talked a lot about the need to protect cloud-based users with strong passwords and multi-factor authentication, but gaining visibility into potential breaches early enough in the attack cycle is critical.

Microsoft has revealed that the frequency of attacks against users of its cloud services, including Microsoft Azure and Office 365, has increased by 300% over the last year.

“A large majority of these compromises are the result of weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services,” said Microsoft in its ‘Security and Intelligence’ report.

According to the post, over two-thirds of Azure attacks came from IP addresses in China and the US, with 32.5% from the US, and 35.1% from China. The remainder came from 116 countries and regions, with Korea the lowest at just 3.1% of attacks.

How do you know when potentially suspicious activity has occurred in your Office 365 subscription, so that you can take the appropriate action?

Microsoft has launched a new product called Office 365 Advanced Security Management that gives you an insight into suspicious activity in Office 365, so you can investigate situations that are potentially problematic, and if needed take action to address security issues.

With Advanced Security Management, you can:

- See how your organisation's data in Office 365 is accessed and used
- Control access to Office 365 data on mobile devices/apps
- Define policies that trigger alerts for atypical or suspicious activities
- Suspend user accounts exhibiting suspicious activity
- Require users to log back in to Office 365 apps after an alert has been triggered

If you are using Office 365 it would be worth looking into advanced security management.

In other news, ‘Locky’ ransomware makes a comeback. There has been widespread media and finance sector reporting of ‘Locky’ ransomware incidents following large spam runs in August. New variants have been seen in the wild, with campaigns directed at the UK. ‘Locky’ ransomware uses various forms of social engineering to entice the unsuspecting victim to enable macros on their computer which in turn downloads and executes the ransomware. The victim is then sent payment instructions. There is no free decryption tool and currently the ransom is 0.5 Bitcoin (approx. 1,800GBP).