CyberGuard Technologies

Proactive Cyber Defence Report

June 2019

Sometimes I feel with these threat reports that I am in danger of repeating myself over and over again. Unfortunately, this report will highlight two areas that we have persistently covered over the last 12 months:

- Patching
- Two Factor Authentication

Some of you may have read about a newly discovered vulnerability in the following Microsoft products:

- Windows XP
- Windows Vista
- Windows 7
- Windows server 2003
- Windows server 2008 / 2008R2

The vulnerability in Microsoft Remote Desktop protocol can be abused remotely, and Microsoft have likened this to the EternalBlue exploit that fuelled the WannaCry, NotPetya and Bad Rabbit ransomware outbreaks in 2017.

In recent days we have seen a number of proof-of-concept codes for exploiting this vulnerability appearing online, and Microsoft have deemed this vulnerability so serious that they have issued fixes for Windows XP, which is officially not supported.

It is estimated that there are over 1 million computers with this vulnerability, directly connected to the internet.

Microsoft first warned about this vulnerability on 14 May. At the time, it was said that the flaw was dangerous because it not only allowed remote execution, but the bug was also wormable (having the ability to self-replicate).

Microsoft also warns companies about the dangers of thinking that workstations not connected to the internet are safe. It only takes one vulnerable computer connected to the internet to provide a potential gateway into the networks, where advanced malware could spread, infecting computers across the enterprise, even if they are patched.

If you wish to read the official guidance from Microsoft please use the following link: https://support.microsoft.com/en-gb/help/4500705/customer-guidance-for-cve-2019-0708

If you are running any of the above operating systems, I urge you to apply the patch as soon as possible.

Our Incident Response team have again seen a large increase in customers who are running cloud-based email, notably Microsoft Office 365, having email accounts compromised.
We are currently investigating one new email breach per day. The number of users currently on Office 365 and the relatively low technical skill required to conduct this attack make it popular with cyber criminals.

CyberGuard's advice is to turn on two-factor authentications to all cloud-based apps and monitor suspicious user activity. Microsoft have an application for this called Cloud App Security, and further information can be found here:

https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

In other CyberGuard news, on the back of signing with Kaspersky Lab for Threat Intelligence, we have added an exciting new partner to our portfolio of products, Darktrace.

Darktrace Enterprise is an artificial intelligent cyber defence solution. It combines real-time threat detection, network visualisation and advanced investigation capabilities in a single, unified system that is fast and easy to install.

Using proprietary machine learning and AI algorithms, Darktrace Enterprise works by passively analysing raw network traffic to form an evolving understanding of 'normal' for every user, device and subnet in an organisation.

Without presuming to know in advance whether or not an activity is 'malicious', Darktrace Enterprise independently learns to detect significant deviations, and immediately alerts the organisation to emerging threats. These can range from subtle insiders and low-and-slow attacks by unknown threats, to automated viruses like ransomware.

In early proof of concepts this has worked really well with our other products, such as Carbon Black and AlienVault, to provide excellent coverage across the network, and is extremely promising.

Thank you to NCSC, Kaspersky Labs, Carbon Black and Anomali labs for content.

Stay safe

Paul