CyberGuard Technologies

Proactive Cyber Defence Report

October 2018

Just when we thought ransomware was slowing down, we have started to see a rise in infections again. The traditional attack method of email is still there, but a recent change of tactics has seen an increase of attacks on companies' Terminal servers. Internet facing servers not fully patched, with weak user passwords offer an enticing target for cyber-criminals. Once a cyber-criminal is in your network, escalating privileges to domain admin is simple in most cases. Once this is achieved the cyber-criminal has full access to your network infrastructure, including any backups that might also be available. The last couple of incidents that we have responded to have seen the attacker targeting the backup, damaging the customer's ability to recover, and therefore the customer is more likely to pay the ransom. I urge all customers to make sure they have at least one recent backup stored offline using tape, disk or cloud that is NOT accessible with your network domain credentials.

Cyber-criminals continue to utilise weaponised macros in Microsoft Office documents to deliver malware. In a recent report from Cofense, it was noted that the exploitation of Microsoft Office macros comprised of 45% of all deliveries. A separate report showed that a further 37% exploited the Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882).

Macros can be easily developed and distributed. Despite Microsoft having disabled macros by default, it only takes minimal user interaction to start the infection chain.

The default installation of recent versions of Microsoft Office on Windows have macros enabled but rely on the user to click a button before any macros can run. You should change this default behaviour to only allow macros where they are needed.

As a minimum, CyberGuard recommends you should disable macros where they are not needed. For example, never create or receive office-based documents, so there is no need to access them, also blocking any macros that are received from the internet, which can now be implemented in Office 2013 and above. Make sure that you apply patch updates to these machines whenever you need to.

High profile attacks on British Airways, Bristol Airport and Superdrug show there is no slowing down in cyber-attacks. The Information Commissioner's Office (ICO) recently provided the first update on the impact of the General Data Protection Regulation (GDPR) since it went live three months ago.

Over this period, the ICO, who is the regulator under GDPR, received an average of 500 calls a week, to their breach reporting line.

Of the cyber incidents that were reported, nearly half were the result of phishing. Malware (10%) and ransomware (6%) were also other notable causes of breaches reported.

One of the most important items businesses should be focusing on at the moment is making sure that you have a working, tested Cyber Incident Response plan. Should the worst happen, being able to respond quickly and make sure the right people and teams are involved is critical. Dealing with an ongoing cyber incident is complex and will involve a number of teams, not only technical but operational. Departments including Marketing, PR, and Legal, as well as directors, will want to know what's going on. Having a plan that is tested will remove these obstacles and let you focus on getting back to normal as quickly as possible.

CyberGuard continues to invest in building our capabilities to support you better, and we completed the first advanced cyber training on hunting advanced threats delivered by global leaders Kaspersky Lab. We are looking to put these skills to good use in the next couple of months.

Stay safe

Paul Colwell
Chief Technical Officer