CyberGuard Technologies

Proactive Cyber Defence Report

March 2019

As CyberGuard looks to expand its detection rate and offer customers more protection, I am delighted to confirm that we have signed an agreement with Kaspersky Lab to provide their Threat Intelligence service.

Cyber-attacks happen every day. Cyber-threats are constantly growing in frequency, complexity and obfuscation, as they try to compromise your defences. Adversaries currently use complicated intrusion kill chains, campaigns and customised Tactics, Techniques and Procedures (TTPs) to disrupt your business or damage your clients.

Kaspersky Lab offers continuously updated Threat Data Feeds to inform CyberGuard's Security Operations Team about risks and implications associated with cyber-threats, helping us to mitigate threats more effectively and defend against attacks, even before they are launched.

There is no doubt in our minds that we have access to the best threat intelligence, and the following two points will help you:

1) This data will power our Security Operations Centre and analysts to provide your company with faster, more complete information about alerts that are created.
2) If you are an AlienVault customer this data will be added to your solution, providing you with even greater visibility of the threats you face.

When we created CyberGuard, our goal was to offer UK small to medium businesses access to security, that is only normally in reach for large enterprises. This is a significant step towards achieving this goal.

I am led to believe that we are the first UK company to provide this service to our customers and puts CyberGuard at the front of fighting cyber-crime.

I will provide more information about this over the next couple of months but within the next couple of days we should be live and reap the benefits from this service.

A joint report by Recorded Future and Rapid7 has accused APT10 of infiltrating the network of Norwegian cloud computing company Visma.

According to Visma, its IT security staff detected the intrusion promptly. Although the incident did not affect any systems belonging to Visma's clients, it "could have been catastrophic" had it not been identified early.

Visma is one of the largest cloud service providers in Europe. The firm offers online HR, accounting, and other software to over 900,000 customers across Scandinavia and other regions of Europe.

The attacks are believed to be a part of a global hacking campaign, codenamed Operation Cloudhopper, that started in 2017 and mainly targets cloud service providers. Although Visma might not be familiar to you, it does highlight the risk of supply chain attacks and it is important that you are asking your IT and communications suppliers what they are doing to protect themselves from these type of attacks.

A new phishing campaign to steal login credentials from businesses is specifically targeting senior executives.

A fake email claiming to be from a company CEO discusses the rescheduling of a board meeting, but the email's link leads users to a page resembling a Doodle poll which can steal Office 365 credentials. Researchers at GreatHorn first discovered the campaign.

According to findings, the campaign is hitting organisations of different sizes and industries with the email's content always remaining the same. If successful, the attackers could have the opportunity to steal important credentials which could create an entry point for further attacks.

It is not unusual for us to see this type of attack. In fact, it is currently our number one incident response call out, but what is interesting with this email is you do not have to enter your credentials to be compromised, just clicking on the link within the email is enough to steal your credentials. The NCSC has issued an alert regarding this type of attack. CyberGuard customers considered at high risk of this type of attack have been notified and AlienVault and Carbon Black have been updated to protect you against this threat.

Stay safe

Paul