6 Burning Questions about the cyber security latest threats for the CEO and Founder of SafeComs

October 13, 2016

These days, companies getting hacked and their data being leaked, stolen or encrypted seems to happen more often than not.

In 2014, it happened to the Japanese conglomerate otherwise known as Sony. A year prior to that, it happened to Target, the US' second largest retailer, when they had 40 million credit cards stolen. To complete the hattrick, Yahoo had more than 500 *million* account hacked in 2014, only that it was made known to the public a few weeks ago, in September, 2016. And these cases are *far* from the only ones.

These are crazy days – but there's hope.

It turns out, there are ways of staying secure, avoiding financial and image-harming damage in the process. We have turned to our very own IT Security expert, Bernard Collin, CEO and Founder of SafeComs, for the latest trends and threats in the world of cybersecurity.

Our CEO, Bernard Collin, greeting a guest at a talk we hosted last week with AustCham Thailand. All image rights belong to AustCham Thailand.

1. Bernard, you've been in this industry for 39 years. What are the hottest cyber security latest threats right now?

Well, we've seen two main challenges recently – one being ransomware, and the other one being ID theft.

- Ransomware is especially dangerous to suffer from for a company, as it totally damages your hard drives and servers, leaving you paralysed without any data until you pay the demanded ransom and get the decryption key – which, by the way, only happens in 30% of the times.
- The scary thing about ID Theft is that you can be on the damaging end of an incident without actually being compromised or hacked yourself.

Today, these types of crimes are so well done and the methods incredibly sophisticated that it's very easy to be fooled. Their goal is to trick you to pay money to a fake bank account, making it look like it's to your own bank account, a friend's bank account, your employer's bank account, and so on – only that it isn't. It's someone else's – and before you know it, your money is gone.

We at SafeComs always use to say that "people are the first line of defence", and it's certainly true. By being completely aware of the risks, the common methods, and how to spot them, you can rest assured that the chances of you suffering from any of these threats is minimal.

2. What challenges have you helped customers overcome recently?

Recently, we saw an increase in companies who had lost data due to a hard drive crash without proper backup. We helped them recover their data from the damaged drive – and they were very lucky that the drive plates were not damaged. Thanks to that, we could successfully restore their data.

Also, we are extremely happy to have been able to help a charity organisation that builds bridges to help remote populations in the mountains of Myanmar. These bridges are their only chance of communicating with other people and tribes without spending days hiking in the mountains. The charity organisation had lost data from one of their operations, containing crucial information to these projects. This was a data retrieval we were very happy with.

The other challenge is to make sure our customers understand that technology should never be their first line of defence – awareness is. You can deploy just about any sophisticated technology, if a person replies to an email asking them for their password, or rework a money transfer to another bank account, you will lose money, and you will be compromised.

CEO Bernard and Sales Manager Isak talking shop with a guest. All image rights belong to AustCham Thailand.

3. How has the big Yahoo hack affected the industry?

We have not yet seen the effect of it on hacking statistics, and it will take a little while before anything is known, if ever. The most damaging element is a blow to the credibility of these large data-handling organisations. They are constant targets of hackers; they try hard to protect their data silo, and in the end, someone gets in through a small undiscovered vulnerability. I am eagerly awaiting the results of the forensics to see whether people got in through a technical vulnerability, or as before with LinkedIn or Dropbox, they got in through a staff error.

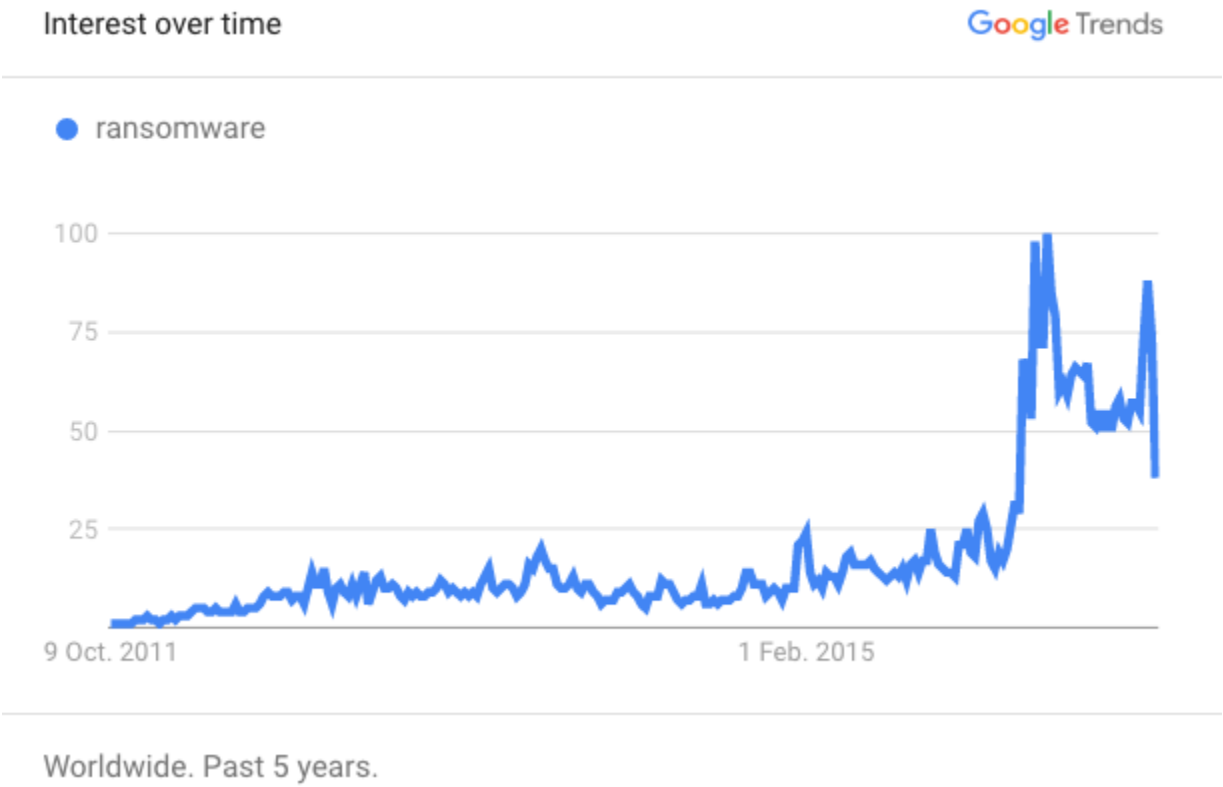
4. What could've been done to prevent hacks like those from happening? Is there anything at all?

Like I said, it is too early to make a comment, as we still don't know how they got in. But you need to understand that the game is very unfair. Companies are under pressure to reach their business goals and requirements, there are needs to be cost-effective, all employees need fast access to data wherever

they are, and the security team needs to secure every single entry point in the organisation. On the other end, the hacker has plenty of time and automated resources to try every possibility relentlessly. The worst thing is, he (or she) only needs *one* little entry point to gain access to your systems.

Security is a real challenge.

5. According to Google Trends, ransomware is a very popular search word these days. What are your thoughts about it?



I believe it is the most profitable criminal activity around with the least amount of risk. Which is why it's not going anywhere – it'll continue to do harm.

On the internet today, you can actually purchase all the tools you need to start a ransomware campaign of your own. There are cloud tools to perform ransomware attacks and exploit existing technology. The bright programmers who have developed the tools are too scared to use them and perform the crime themselves, so they have made their tools available online for others to use.

Although, if you look on the bright side, it's pretty easy to protect yourself from it, because all that's required is:

- Awareness of phishing baits (education, know what signs to look for)
- Technical protection (regular backups stored remotely with history, and good Antivirus/Anti-SPAM technology

If you have those two, you've come a long way in protecting yourself.

Bernard spreading the word. All image rights belong to AustCham Thailand.

6. What is on the plate right now for SafeComs?

We are continuing our mission to help all our customers be as secure and safe as possible by bringing the best technology available to them, and by educating them on risk avoidance and mitigation.

These coming months, we are going to host a series of presentations in cooperation with various Chambers of Commerce in Thailand. For instance, last week, we had a really insightful – tooting my own horn here – talk in cooperation with AustCham Thailand at the Banyan Tree.

It was a really good turnout and a lot of people had a lot of questions and testified that it's indeed a dangerous, risky time in the cybersecurity world. It's certainly not only large corporations that's being hacked.

Make sure you never miss a post! Sign up for our non-commercial newsletter, and also don't forget to follow us on Facebook and LinkedIn.