Ransomware… did you get caught?

May 24th, 2016

My enduring advice on computer security:

Do not solely rely on technology or systems to resist hackers, your first and best line of defense should always be your employee awareness and education program! Technology will assist and can also help in the recovery after a case of damage but first make sure your employees are trained to react appropriately.

Ransomware is the act of using malware to penetrate a computer and encrypts its hard drive, and then, requesting a payment (ransom) from the owner to decrypt his data.

But in fact, how bad is it and what are the Ransomware risks?

This past year has seen some of the most devastating cyber-attacks and highly profitable ransomware for the perpetrators. They added up to astronomical costs for the companies that got caught. Despite the resistance to give in to the threat, some had no choice but to pay extremely high value ransoms.

The health care business was particularly targeted with ransoms in the thousands of US Dollars, paid in bitcoins to recover access to their patient data, which in some cases were vital as their life could have been at risk.

Despite the increase in monitoring software and serious deployment of sophisticated automated technology with the latest generation of firewalls, anti-virus, intrusion detection, web traffic filtering and so on, specially crafted spear phishing attacks ultimately reached their high value target.

But low value targets were also in the line of fire. Automated phishing targets anyone and the ransom is proportional to the size of the business. Some small companies got away with paying 0.99 bitcoin, some with a couple more, but it is always costly, a serious waste of time and energy, lots of frustration and stress, and
you never know if you will get your data back, even if you pay. Moreover, even if you think you are clean there is no guarantee they haven't left a backdoor and won't be coming back for more…

In many cases, we have to admit the failure of the legacy perimeter defenses to identify and stop the most basic phishing attacks, and there is a serious risk that sooner or later one unprepared employee will click on a tempting email link that will bypass the lines of defense. Hackers are now adapting their email subject lines making it impossible to preemptively block them.

Is Ransomware slowing down?

Not really and we are trying to predict what's cooking for this year. Analysts are observing the skyline as the demise of Dyre malware in 2015 seems to indicate a preparation of something far more dangerous. The next wave will probably propagate through worms crawling from site to site and disk to disk, and stay dormant for a long time before emerging. Which indicates that the last line of defense, the backup needs to seriously increase to keep data history unaffected. History of Backup allows you to go back in time to a version of the data without malware… but how much recent development will you have lost?

A serious preparation for all companies is paramount, and it is not really clear how the next attack will develop.

It is certain that mobile technology is the prime target as it is so pervasive in everyone's life. Some employees don't even have a PC any more and manage their e-life on their phone with a bigger screen. As a result, most IT managers have lost total control and are desperate in their attempt to protect the company’s network and assets (see our article on EMM –Enterprise Mobility Management to see the difficulty)

New tools are being developed, new defenses are being crafted and it is a race with time to get a response as quickly as possible when the next threat emerges. Companies must deploy the latest technology for their peripheral protection and sharpen their intrusion detection tools, with a strong emphasis on behavioral analysis. However, is it available to all? And at what cost?

Your chances of surviving an attack will increase with the amount of sophistication you can afford for your periphery but the first line of defense remains the education of your staff.

The most disturbing trends are now:

- Phishing emails are smarter with adaptive subject lines
- Phishing emails use fake company names targeting those close to you
- Worms will stay dormant for longer limiting the capacity to recover

What you need to do:

Train your staff, show them what phishing is, explain Trojans and worms, and consult with a competent security company to reduce the risks. Be prepared if you get hit, so the damage is limited and you can recover without paying up.

Always be aware of the threat and expect the worse so you are prepared to survive any incident. The government is not close to catching the bad guys, they are potentially far away and extremely well organised, so you need to take your security very seriously.

The Author:

Bernard Collin is the CEO of SafeComs, a security firm based in Bangkok Thailand, with offices in Myanmar. Bernard started his IT career with Apple in 1997 in Paris, then moved to Digital Equipment in Geneva and specialised in IT security in 1987 with the evolution of DECnet network and later on the Internet. Bernard Started SafeComs in 1999 in Australia and throughout his life consulted with large businesses in Europe and in Australia. His expertise includes office automation and network security, and he is a regular speaker at Security events and at Chambers of Commerce. His company SafeComs has been awarded numerous prizes including SIPA (Software Industry Promotion Agency) in Thailand for creative software development.