When espionage meets globalization

Published on Published on May 17, 2017; Written by Doron Sivan, CEO of Cronus Cyber Technologies and Itay Sagie, CMO & Business Development at Cronus Cyber Technologies.

The NSA among other things deals with cyber activities. As part of this field, the NSA identifies weaknesses in the network and writes exploits for them. Meaning a small piece of software that can exploit this vulnerability to hack or penetrate into a computer. After this penetration, a small piece of software is injected into the operating system that allows various malicious activities to take place, such as file encryption and a complete remote takeover of the computer.

The problem, in this case, is that malicious hackers, in this case, shadowbrokers, were able to steal this tool and the code that the NSA developed for their own uses.

The weakness that was identified was the SMB protocol which enables shared access to files, printers, and communication between computers in the network.

The use of this protocol involved credentials and is being used in windows operating system, although Linux can also support SMB.

How does the exploit reach the target computer?

The exploit can be transferred either via attached file in an email or in some cases there is a direct connection to the SMB to the outside world. This is very risky and ill-advised.

In March Microsoft published a patch numbered MS17-010, however, many organizations did not install this patch.

The reason is that old patch management methods and the tedious work involved means that organizations are sluggish and too slow to perform the necessary updates on time.

Organizations are swamped with thousands of vulnerabilities that demand their attention and lack of proper prioritization makes them inefficient against attackers which are much quicker to act.

This vacuum is what allows hackers to exploit these vulnerabilities, often 6 months or older, by sending files that exploit the vulnerability, encrypt the computers and ask for ransom, this is called ransomware. In this case, the name is WannaCry.

What should you do now regarding WannaCry?

Organizations must immediately patch their operating system, they must make sure there is no outside access to the SMB, it is also advised to update all the information security systems such as antivirus and IDS systems and utilize

automated and continuous penetration testing to detect potentials attack path scenarios that threaten the critical business processes and assets.

On a state level, cyber management is critical to healthcare systems, banks, critical infrastructure and more. Countries have better tools to monitor cross-border traffic.

There is no doubt that continuous 24/7 monitoring of all the networks infrastructure is mandatory in order to prevent the next cyber attack. Hospitals are a weak link due to their complex structure, multiple branches, clinics and multiple stakeholders that have access to the network from doctors, nurses, patients, and vendors

This is the reason the healthcare system was targeted, their sensitive information has great value and needs to be protected and heavily regulated.

Cronus's CyBot will prevent the next attack from reaching your critical business process

The only thing more efficient than a human hacker is a cyber bot capable of testing a million potential attack scenarios at the same time it takes a human hacker to attack a single target.

Cronus Cyber Technologies has developed CyBot - an automated and autonomous ethical hacker or Cyber-Bot - "CyBot" that will continuously scan your network for potential attack path scenarios, even your global branches,

and show you a visual map of how hackers could threaten your business processes and critical assets on a global scale, 24/7. All you have to do is install CyBot in various locations in your network or on your cloud and let it run. No need for a cyber expert on your team to manage CyBot.

CyBot will autonomously detect and assign the proper significance to your critical targets and how to reach them. You can choose to customize your list of critical assets and business processes using an easy drag and drop interface to help focus the system. Once such a critical "Attack Path Scenario" is found, you and your SIEM are alerted and a response can take place with a click of a button.

Cronus is changing the way companies protect themselves from the next attack. No more peripheral systems which will be breached one way or another, no more annual pen testing that is invalid the next day due to your dynamic (and often cloud-based) environment and new vulnerabilities, no more sleepless nights not knowing if your millions of dollars spent on cyber protection will actually work. Now you will finally know and see exactly why and how you will be hacked and how to stop it in time.

For more information visit https://cronus-cyber.com/