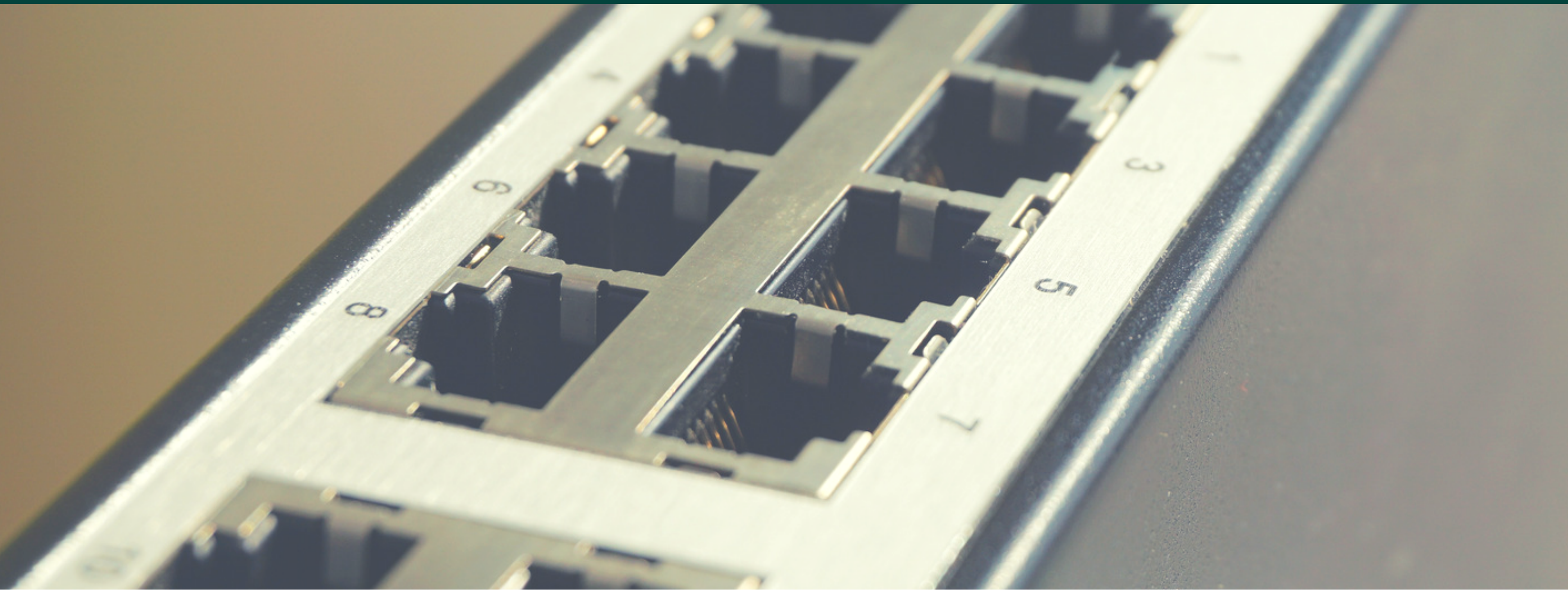
MAY 17TH 2017

RANSOMWARE ATTACK

InterRisk Asia (Thailand) Co., Ltd.



WannaCry Malware Outbreak

On May 12th 2017, a malware threat called WannaCry emerged worldwide, affecting businesses and institutions including a shipping and logistics company in the US, train systems in Germany, a Spanish telecommunications company, universities in Asia, Russia's interior ministry, French and British carmakers and hospitals in the UK. This type of malware locks files and asks for payment to unlock them, hence the word ransomware.

> *The crisis isn't over...patch your systems as they will try again.*
>
> - @MALWARETECHBLOG

This malware can easily infect other computers in the same network. WannaCry ransomware uses the vulnerability of "SMB (Server Message Block)" Remote Execution Vulnerability, a security flaw in Microsoft's Window Operating System. Users without Window updates are at risk of getting this malware.

During the month of April, the vulnerability was released to the public but Microsoft has released an update to fix this vulnerability since the 14th of March. However, computers which have not updated the patch were attacked, with more than 230,000 computers in 150 countries.

One example case in Thailand is the Royal Thai Police system breach, which caused a road sign error to be displayed on Witthayu Road on the 14th of May, 2017. A total of $55,165, or less than 2 million Baht, from 209 payments via Bitcoin were paid to the hackers according to Reuters as of 9 pm Monday Thailand time.

Windows XP, Windows Server 2003 until Windows 10 and Windows Server 2016 systems were affected from the malware attacks. Since the support period of Windows XP and Windows Server 2003 is no longer available, there is no update to fix this vulnerability for the two systems. Despite this, there are still computers running on the two operating systems and have Internet connection. Therefore, Microsoft has issued an emergency update to resolve this issue. Users may download the update from the Microsoft website.

To Prevent Infection:

1. Update antivirus and other security software.
2. Have a separate backup of your important data not connected to a network.
3. Update your software frequently to block the vulnerabilities.
4. Close the Server Message Block (SMB).
5. Do not open links or attachments from suspicious e-mail.
6. Turn on your smart screen (in Internet Explorer), which helps identify reported phishing and malware websites and helps you make informed decisions about downloads.
7. Have a pop-up blocker running on your web browser.

Newer strains of the ransomware are possible. The Ministry of Information and Communication Technology has already issued ThaiCERT and the ETDA (Electronic Transactions Development Agency) to create guidelines on preventative measures for the general public. It is advised to keep yourself updated (patched) as the authorities are certain that there will be further cyber attack attempts in the near future.

REFERENCES

https://www.thaicert.or.th/alerts/user/2017/al2017us001.html
http://www.sciencealert.com/experts-are-warning-the-global-wannacry-ransomware-hack-isn-t-over
http://www.npr.org/sections/thetwo-way/2017/05/14/528355526/repercussions-continue-from-global-ransomware-attack
https://www.it24hrs.com/2017/wannacry-ransomware-malware-effect/
https://www.blognone.com/node/92410
http://www.bangkokpost.com/news/general/1250106/cyber-worm-slows-hobbles-chinese-police-schools
http://fingfx.thomsonreuters.com/gfx/rngs/CYBER-ATTACK/010041552FY/index.html
http://www.reuters.com/article/us-cyber-attack-idUSKCN18B0AC
http://www.aljazeera.com/news/2017/05/ransomware-avoid-170513041345145.html