Cybint
BARBRI Cyber Solutions

ON MAY 12, 2017, THE WORLD EXPERIENCED ONE OF THE LARGEST "RANSOMWARE" ATTACKS IN HISTORY.

The Ransomware hit dozens of countries around the world, causing damage to critical infrastructures within hospitals and public transportation, and to businesses including law firms and financial institutions. The countries in blue were affected:

Since then, cyberattacks through Ransomware have grown exponentially, and now surpass all other forms of malware as the number one menace to cyber assets and the technology infrastructure. The rise of Bitcoins (digital untraceable payments) has contributed greatly to the increasing popularity of Ransomware among hackers. Protecting yourself and your clients from Ransomware means understanding how it works, then taking appropriate security actions. The information contained in this piece is meant to arm you with the knowledge you need to minimize your risk from Ransomware.

WHAT IS A "RANSOMWARE"?

Ransomware is a type of Malware (Malicious Software) that prevents or limits users from accessing their systems, either by locking the system's screen or by locking the users' files until a ransom is paid. Modern Ransomware families are collectively categorized as crypto-ransomware. They encrypt certain file types on infected systems and force users to pay the ransom online to get the decrypt key.

It's important to emphasize that while ransomware may harm you personally, it is a much bigger threat to your firm, company or clients. Some Ransomwares work as "Worms," which means that when they get into one computer, they look for other devices and spread across the network, thus compromising the entire company and its clients. The attack of the "WannaCry" Ransomware worked that way, causing tremendous damage on its way.

When attacking firms or companies, the hackers behind Ransomware can demand a massive amount of money (professional extortion) to restore the company files. In addition, although the main motivation for a crime like this is quite obviously money, there are other motivations that can trigger someone to activate this kind of malware. These include a desire to disrupt legal procedures, harm your reputation, or force you to give away sensitive information (different types of Cyber Extortion).

Cybint
BARBRI Cyber Solutions

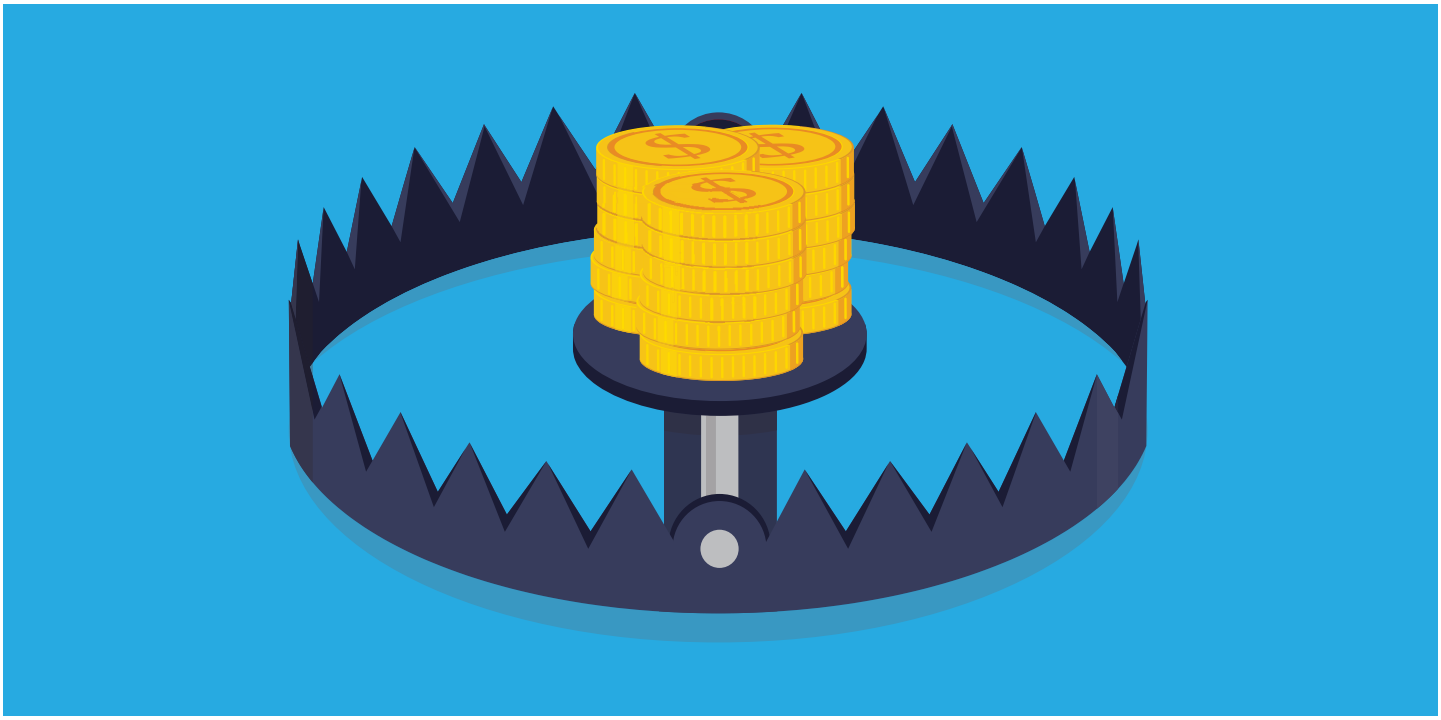
HOW DOES THE RANSOMWARE GET INTO MY SYSTEM?

Ransomware usually penetrates the system when unsuspecting and unaware users (like you) make a mistake. These are two of the most common mistakes: a. Visiting unfamiliar websites, without checking if they are trustworthy. Some websites are malicious or compromised

THESE ARE TWO OF THE MOST COMMON MISTAKES:

1. Visiting unfamiliar websites, without checking if they are trustworthy. Some websites are malicious or compromised websites, and cause an immediate infection once you access them. In this case, you don't need to download anything, the website will do it automatically. b. Downloading attachments or clicking on links: Ransomware can also arrive as a payload either dropped or downloaded by other malware. Some
2. Downloading attachments or clicking on links: Ransomware can also arrive as a payload either dropped or downloaded by other malware. Some Ransomwares are known to be delivered as attachments from spammed email, downloaded from malicious pages, or dropped by exploit kits into vulnerable systems.

WHAT SHOULD I DO TO PROTECT MY COMPANY, MY CLIENTS AND MYSELF?



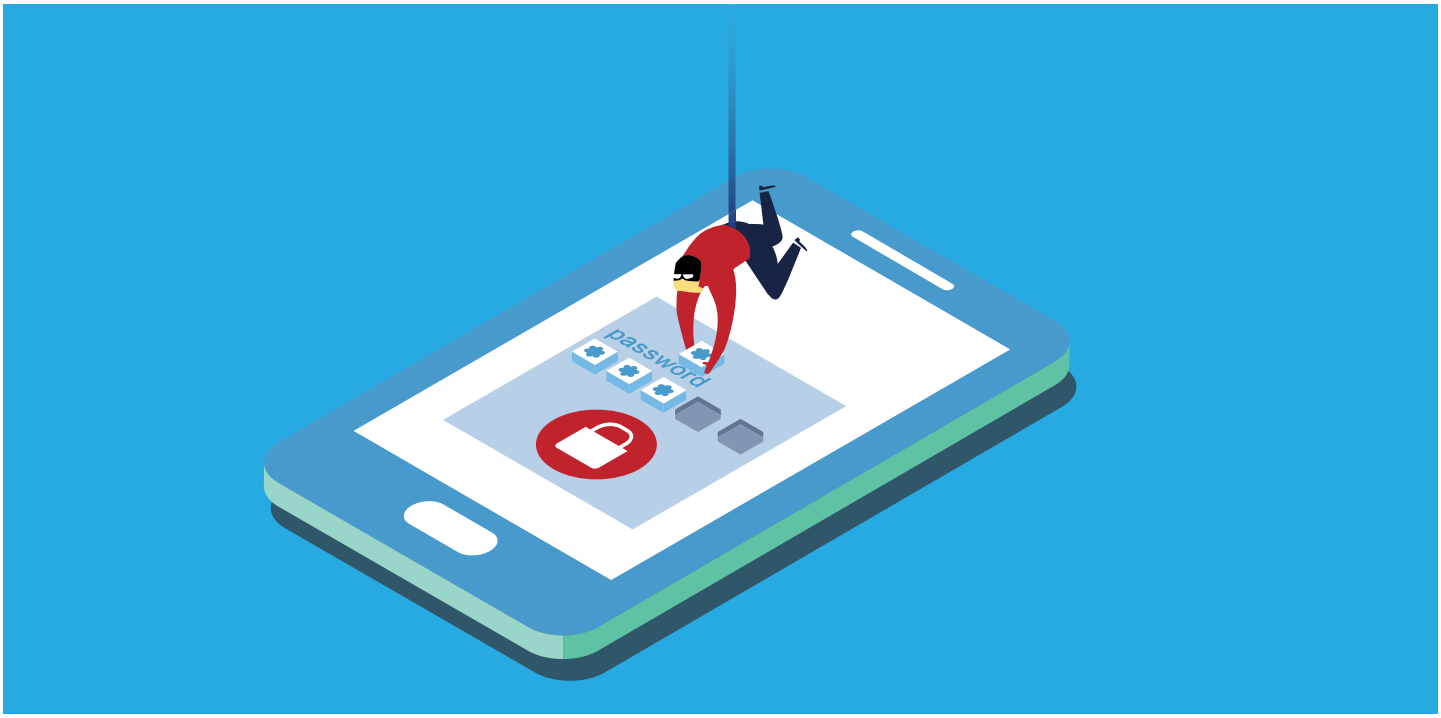
1. Know your "Cyber Rating" and improve cyber awareness. 95 percent of all security incidents involve human error, so the first stage is to identify the main human factor gaps in the organization. At Cybint, we offer a free assessment for you and your firm to gain the insights you need here.

2. Update your system regularly. Many of the updates you get to your computer or smartphone are security updates. It means that the company (for example Microsoft® for Windows) identified a security breach, and asked you to update your system to avoid this breach. The same update was released to hackers, who will be looking for the "weakest links." Most of those weakest links are people, perhaps like you, who didn't have the time to update their system until it was too late.

3. Avoid unfamiliar websites. Before entering an unfamiliar website, you should check its trustworthiness. There are available online tools to help you do it like MyWot and lists of dangerous websites like MalwareDomain List.

4. Backup. Hackers know that the secret of effective Ransomware is penetrating your backup systems. Your approach should be to use several types of backup, with a cloud-based file syncing backup (to allow recovery of the previous version), and long-term "offline" (or logically isolated) backups of data stored in locations inaccessible to the infected computer. Backing up to locations such as external storage drives can prevent them from being accessed by the Ransomware, thus making data restoration faster and easier.

I WAS ATTACKED BY RANSOMWARE, WHAT SHOULD I DO OR KNOW?



THERE ARE SEVERAL STEPS YOU CAN TAKE:

- If you took the right measures in advance, the best thing is to use your "Offline" backup.
- If you don't have a safe backup to your critical files, you can try to use available decryption tools. There are a number of tools that are specifically designed to decrypt files locked by Ransomware. For example, try to upload your files to this website.
- Microsoft officially ended its support for most Windows XP, and today it's delivering one more public patch for the 16-year-old OS. Download and install the patch for Windows XP to fight the 'WannaCrypt' attacks
- Unfortunately, successful recovery may not always be possible, however, paying the money is never a good option. It does not guarantee that your files will be restored, it supports the ransomware industry, and it might mark you as a target for future attacks.

TAKE-AWAY

Ransomware is a popular product in the malware market. It locks your computer or files and demands a payment in order the restore them.

We also learned that the best way to protect our networks and data is to avoid being infected. However, it is possible to mitigate its effects after being infected.