RANSOMWARE IS HITTING US...
BE CAREFUL!

What is Ransomware?
It is a type of malware (virus) that restricts access to the infected system in some way depending on its complexity and tactics. The goal of a malware operator is to demand ransom to be paid in order to remove restriction. However, even if the ransom was paid, there are no guarantees that a user’s access gets restored.

Ransomware infects systems through several approaches, most commonly are downloads from untrusted sites, email attachments from suspicious sources, and in a more targeted manner, exploiting a vulnerability of a system or a network service.

History
Early versions of ransomware would disguise as an anti-virus solution ambushing a user by fabricating the detection of critical malwares on his system and requesting purchase of full license in order to remove detected malwares. Another version of ransomware would lock a user out of system until a specific payment is done.

More recently, the complexity of ransomware elevated its technique to include “Encryption”, the hardest of types to break. Encrypting ransomwares are the most difficult to recover. They target files and systems and lock them by using an encryption algorithm. Ransomware operators at this stage used the new Bitcoin digital currency platform to collect ransom payments. It was estimated, for example, that one type of encrypting ransomware has contributed to a total of US $27 million from infected users.

Industry-oriented Attacks
In light of an observed worldwide collaboration among malicious hackers and hacker groups, the latest trending ransomware attacks are targeting industries, such as education and healthcare sectors.

Why target individuals when you can target an organization, and not just any organization?
It is because the type and nature of data that circulates within the healthcare industry is of utmost criticality to patients’ health and safety, which brings hackers greater interest in profitability. One of the recent headlines that flashed all over social media was “HOLLYWOOD HOSPITAL PAYS $17,000 to RANSOMWARE HACKERS”.

Redemption
Despite the collective and collaborative efforts among cybersecurity leaders, the ransomware attacks still pose serious threat to all individuals, organizations, and industries alike. Organizations worldwide implement several layers of security to protect their data. However, practice has shown that 100% security is impossible and that security is everyone’s responsibility. Up to this date, one of the best ways to recover from such attacks is by trying to maintain continuous and regular data backups.

For more information, please contact IT Helpdesk ext 2260 or e-mail: it.helpdesk@aub.edu.lb