Ransomware and the threat to the public and private sector

Authors: **Leonardo Palhares** lpalhares@almeidalaw.com.br **Caio Faria Lima** cilima@almeidalaw.com.br

Abstract:

It is extremely important that companies and public authorities take a series of precautions to avoid the Ransomware cases, malware known as a “system kidnapper”, due to the increase of victims of this global threat that prevents or restrains the access of the user to its own system.

A recent report analyzed which are the cyber crimes that will affect companies and consumers in the year of 2016. Among them, the Ransomware menace stands out. This “practice” consists in the contamination of a system with a malware that, when installed in the device, prevents or restrains the access of the user and the person in control of the system charges an amount in order to supposedly reestablish such access. It is the equivalent of a kidnap of a system by criminals: they will only release it against payment of a ransom.

This is a wide threat to companies and public authorities of all over the world. An attack of such magnitude may hinder and damage a companies’ activities, as well as cause a permanent loss of archives.

In this sense, we present below a series of orientations to guarantee prevention against this kind of attack:

- **Backup:** One of the most important guidance appointed by specialists in cyber security consists in the creation and constant update of a backup. If your system is victim of the malware, the company can restore the device and transfer all archives saved with a complete backup, getting rid of the threat without much trouble.

- **Orientation of employees:** In a company, the action of an uninformed employee can affect the whole system. In this sense, the guidance of the employees is essential to improve the security. It is important to establish rules against the opening of suspect emails, the visitation of questionable sites, among other simple measures that are fundamental to the good functioning of any system.

- **Keep all programs and anti-virus updated:** Taking advantage of failures of the own system as the lack of a good anti-virus and vulnerabilities of programs and applications outdated is one of the easiest ways that the criminal uses to enter in a system.

It is highly recommended to proceed with the following steps in case of a Ransomware attack:

1) Disconnect your system: With a simple measure as shutting down the system hacked, you can prevent the transferring of your personal data to the criminal;

2) <u>Seek legal assistance</u>: Once the attack is identified, it is extremely important that the company seeks professional advice from a specialized legal team in order to protect its rights and to proceed with the complaint to the local authority. Such authority should become aware of the number of attacks and the *modus operandi* of the criminals, allowing the leading of a good investigation.

The payment of the ransom is not recommended in any circumstance considering that, besides indirectly financing and encouraging this kind of activity, the criminals often do not release the system.

Once these preventive measures are duly followed, in case the company is still a target of such attack, it is possible to seek compensation directly with the Judiciary branch with a thorough investigation in order to determine the source of the attack and, then, request civil compensation for the damage inflicted, as well as the criminal conviction of all participants.

Almeida Advogados has a team specialized in Technology, that is following all news regarding the matter. The team is available to clarify any questions on this threat and assist the companies with a possible attack.