HOW CAN RANSOMWARE ATTACK ME?

Once the threat to us as users, as well as the possible impact of being infected by a Ransomware virus, is understood, we must ask, how can we be infected?

Although there are many methods, and variants thereof, of infecting us, the main one is Trojans on malicious web pages or on legitimate web pages that have been compromised by criminals for the sole purpose of infecting their users. Anomalous behavior is often not detected nor does it affect our browsing experience; the virus simply installs itself in the background, going unnoticed by the user.

The second most widespread method of propagation is to send **links in massive mails to compromised websites** (spam), and even **instant messaging, social networks**, or s**haring files on P2P networks** (torrent, etc.).

Attacks targeting companies, although they are less common for users, include attacks aimed at servers exploiting **known vulnerabilities in the remote desktop protocol (RDP)** used by the systems administrators to access organizations' servers.

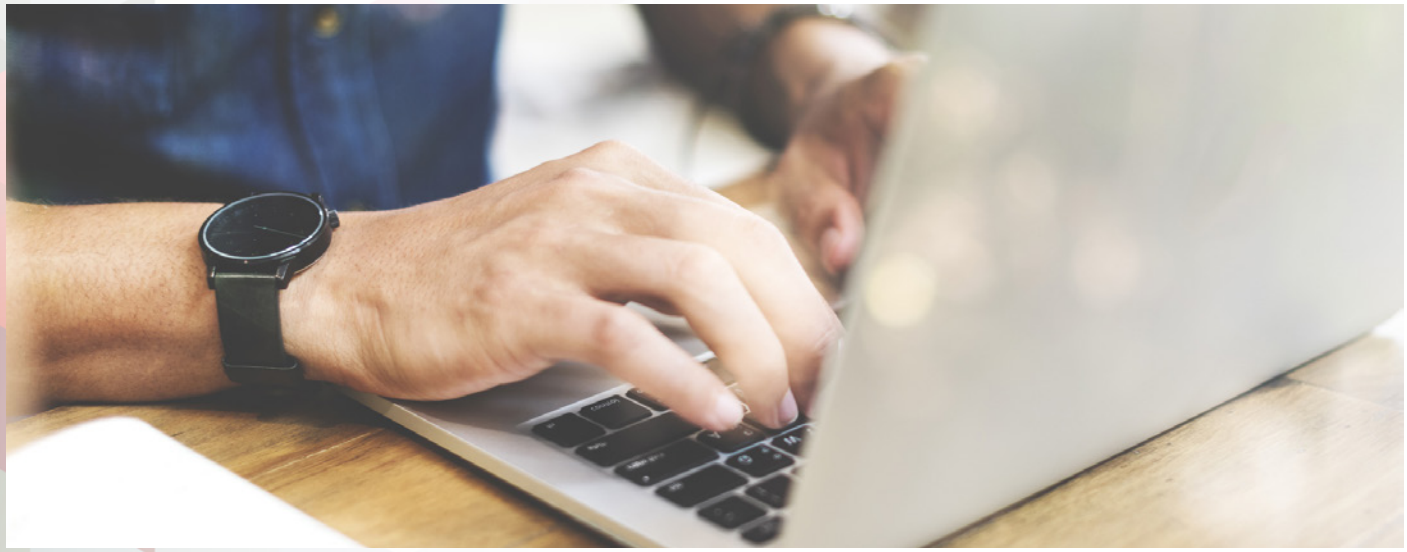
Since we have talked about the growth of attacks detected on mobile devices, it is important to know how a virus can be introduced into our devices. The form is similar, based on deceptions published on malicious web pages causing the user to access c**opies of the Google Play Store with malicious content**, where the user ends up installing a malicious application that executes the "hijack" of the device. Interestingly, many of these deceptions are based on making users believe they have a virus on their device and to access and download a supposed antivirus.

WHAT CAN I DO TO AVOID BECOMING INFECTED AND/OR MINIMIZE THE IMPACT?

Having understood how these types of programs work and the most common ways of being attacked, what should be done to prevent an attack?

- Making ***backups*** of our files regularly is definitely the most effective way of combating them. Unfortunately, in most cases affected files or computers cannot be recovered, so recovering through backups is almost always the only way possible.
- Use of **antivirus** systems in devices. As we have seen, one of the most common ways is to execute certain files on our computers. With a recognized, updated antivirus it will be easier to repel attacks.
- In order to reduce the chances of being attacked, both our equipment's applications and operating system must be updated to the **latest available version and have all the security patches installed**. Web browsers (Chrome, Firefox, Internet Explorer, Safari, etc.) are especially important, because infections sometimes occur when browsing certain web pages (either because they have been created for this purpose or because they have been compromised previously).
- Use common sense and, as a general rule, **do not trust** strange or unknown websites, files or links. If for example, a link is sent to your email address regarding an order you do not expect, ignore it, or, in case of doubt, inform us before accessing it. Often, a simple Google search on the subject or body of the email message will be sufficient for us to find that what we thought to be legitimate is actually a threat.
- Having **file extensions enabled** can help us to identify better an attempted attack. If for example, we expect to receive an image in an email but we receive a compressed file (a "*.zip*" for example) this may indicate that something is wrong.
- If we suspect that a recently received file may be some kind of virus, the first thing we should do is **disconnect the computer from the network**. This will mitigate the risk, especially in business environments, of it extending to other computers in the network.

WHAT TO DO IN CASE OF INFECTION?



If, unfortunately, we have not been able to implement the controls mentioned, and infection occurs, what should we do? First, **it is recommended not to pay the ransom** asked for by the cybercriminals, since doing so does not guarantee that the files will be recovered and it foments this criminal practice. According to recent studies by the anti-virus company Kaspersky, one in three users pay the ransom for their files and approximately 20 percent fail to recover them. Instead, depending on the scale of the incident, it is recommended first to assess the possibility of informing the State Security Forces, especially if certain fundamental rights are considered to be violated or people's safety is in any way jeopardized. In the particular case of public bodies and companies of strategic interest to the country, this communication should be channeled through the National Cryptologic Center – CERT, a public body reporting to the National Intelligence Center with a mission to ensure the security of information systems in public administration.

En este caso, la estrategia de recuperación debe de ser, primero la eliminación del archivo que produce el cifrado de los archivos en nuestro dispositivo y segundo la obtención de la clave, la llave, con la que han sido cifrados. Por suerte para nosotros, existen organismos y entidades privadas que trabajan activamente en esta tarea ofreciendo aplicaciones y recursos gratuitos que pueden servirnos para tal fin. Especialmente conocido en el mundo de la ciberseguridad es el proyecto "No More Ransom", liderado por Europol y la unidad de crimen tecnológico de la policía holandesa junto con alguna de las empresas privadas más importantes del sector. A través de esta organización, se ofrecen un conjunto de herramientas gratuitas que permiten descifrar los archivos atacados por una gran mayoría de Ransomware, así como consejos o guías para abordar un incidente de esta naturaleza.

IS THERE ANY WAY TO INSURE AGAINST POSSIBLE COMPUTER INCIDENTS?

The increased incidence of new cyber threats has led to a proliferation of **insurance products** in our markets to provide cover to companies. A recent report from the PwC consultancy says that about 30 percent of American organizations currently have some form of coverage to protect themselves against the consequences of cyberattacks (mostly in the health, technology and *retail* sectors). In Spain the figure is lower, and currently it is only Ibex 35 companies that seem to be aware of the problem, about half of them already having, or being in the process of taking out, some kind of policy. It should be noted that policies of this kind are often not standardized, but individually adapted to allow the companies to customize the coverage to be applied, so they can choose the coverage most appropriate to the specific needs of their business.

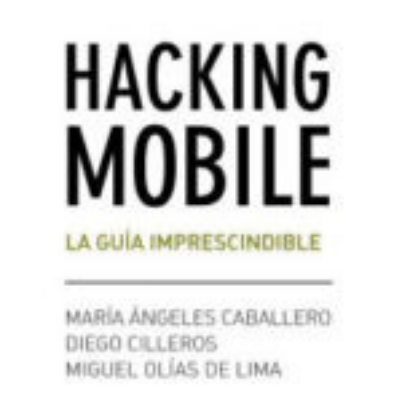
Since cyber attacks often have a direct impact on company operations, cyber risk insurance should be prepared to cover potential financial losses, along with expenses related to forensic investigation or the process of communication to clients (it should be noted that the future European Union regulation 2016/679 will oblige companies to report security breaches and notify third parties of breaches of their data). Particularly in the case of Ransomware attacks, the main aspect distinguishing the type of policy to be applied from others is coverage related to extortion costs.

MAPFRE now offers a Cyber Risk Insurance to protect its clients, SMEs and self-employed, against this new type of threat:

- Image restoration costs.
- Fines and penalties as a result of the attack.
- Legal defense expenses.
- Theft of confidential information.
- Damage to IT systems.
- Financial losses due to business interruption.

You can get more information via the following link https://www.mapfre.es/seguros/empresas/seguros-de-responsabilidad-civil/seguro-ciberriesgos/

RELATED BIBLIOGRAPHY



Since Ransomware on mobile devices is one of the vectors in which growth is predicted to be exponential, if you are interested in learning about and exploring the world of cybersecurity on mobile devices, we recommend, as a basic bibliography, the book "*Mobile Hacking*" published by ANAYA, which looks at questions of this type. http://www.anayamultimedia.es/libro.php?id=4312499