ADWARE AND WATERING HOLE:
Cyberattacks on the rise
If you are sick and tired of watching advertisements everywhere from the moment you turn on your computer or when using your cellphone, then you may be a victim of this cyberattack modality.

This is a malicious software that is installed in the devices with the purpose of showing advertisements on any device screen.

Depending on user´s likes, it creates a profile to show advertisements that may be of your interest, however, the way it does it can become invasive and irritating, even hindering the correct use of the equipment.

Those advertisements get revenues when someone clicks on them, then eventually they become more and more persistent, because they need the user to access to them so they can produce profits.

Also, they might seize vulnerable data that allow them to cause reputational and economical damages. That is to say, adware also searches for stealing information such as personal data, credit card numbers and access codes or passwords, data that can be sold to a third person.
This is how you can identify if you have been a victim of Adware

- Your browser homepage has changed and now shows a different search engine.
- Occasionally, strange apps or icons appear in your device.
- Sometimes it is impossible to properly use your devices because of the invasive advertisement.
- Some links take you to different web sites.
- Your device and browser begin to work slower.

How to avoid being an Adware victim?

1. Do not download unofficial software or apps, especially free tools.
2. Always use antimalware solutions that will help you to constantly scan your devices.
3. Avoid clicking on attached links present in your received emails in your mailbox.
4. Frequently erase cookies and temporary files from your browser.
5. Keep your official apps and devices updated, this is to prevent that you be an easy target for a malware cyberattack.
6. Pay attention to program or apps installing processes because they may install additional tools containing Adware.
What is Watering Hole?

It gets this name because this cybernetic attack modality is quite similar to the moment when a predator hunts its prey in apparently still waters. It is one of the most difficult cyberattacks to detect and its success rate is incredibly high.

Criminals chose companies with a low level of cybersecurity, where its users constantly access web sites with corporative information. This way, they take advantage of the user’s confidence to install malicious software that enables spying on vulnerable data inside a company.

It is considered a very sophisticated technique because attackers take a lot of time to study user’s habits, chose a victim and create a profile so they can be led directly to a third party site, this is why it is very difficult to detect signs of a possible hacking on the site.

How to avoid being a Watering Hole victim?

1. Perform constantly audits to your company corporative sites.
2. Always keep your site´s content management and each device operating system updated.
3. Block the script automatic execution on the browsers.
4. Make your collaborators awake about the risks immersed in this kind of cyberattacks.

InterNexa is your best ally on cybersecurity

Together with us, you can keep your company’s cybersecurity level at its high. Explore our portfolio and discover our managed Safety solutions.

Would you like to know more?

I want an advisory!