21. May 2019.

COLLECTING DIGITAL EVIDENCE

Introduction

Cyberspace attacks are a daily scenario, in the Republic of Serbia but worldwide as well. There are numerous attempts of intrusion into information systems, PCs or mobile devices. Nowadays, more and more targeted attacks are pointed into gaming consoles, digital cameras, navigation systems or IoT devices and wireless Internet access (*Wi-Fi*). The goals of these attacks can differ, from the theft of personal data, abuse of social networks accounts, an accomplishment of terrorist goals, all the way to espionage. The ultimate goal of an attacker in all these attacks is gaining profit against the law.

Collecting digital evidence

When users take precautionary measures, recommended by the National CERT, in order to protect themselves against cyber attacks, most of these types of attacks can be prevented. However, a certain number of attacks are still being successfully executed and causing damage to information systems or personal devices and computers. The question is, what users can do in such situations, so that the caused damage is minimized, and the computer is ready for work again.

Users, who become victims of a successful attack, the National CERT of the Republic of Serbia recommends taking the following steps:

- disconnect the Internet connection of the computer, whether it's a direct connection through a cable or a Wi-Fi device,

- If the computer is part of an information system, it is necessary for users to remove the network cable from the computer in order not to infect other computers on the network.

It is of crucial importance that computer/s remains plugged in, without restarting the Operating System/s. This way users preserve digital evidence for forensic analysis that should be conducted by the Department of High-Tech Crime at the Ministry of Interior of the Republic of Serbia (vtk@mup.gov.rs), as well as the Special Prosecution Office for Combating High-Tech Crimes of the Republic of Serbia (http://www.beograd.vtk.jt.rs/).

For the purpose of preserving digital evidence, it is necessary to create an identical hard drive copy (Clone) that contains the entire structure of the disk itself, as well as all the data, programs, files and folders that were on the computer at the time of the attack. There are several software solutions for creating a copy (e.g., Symantec Ghost, EaseUS Todo Backup) that users can download. In addition to this, users can also store other data that can be more than useful when carrying out investigative actions by the competent authorities, such as:

- Keeping log files - a recorded data set of activity for a particular device,
- e-mail Header - is a set of metadata that can contain details of the sender of a malicious message,
- Cyberbullying can be recorded by users. A specific text message or a video posted on Social Networks, that represent a form of harassment of users via the Internet.

Upon completion of cloning and data collection, users can start recovering their computers by following steps:

- re-install the OS (e.g. Windows, Linux, MacOS) that contains all patches,
- re-install the latest available version of the application solutions that were used on the infected computer or mobile device,
- re-install and run the latest version of AV software released by the manufacturer.

If there are multiple infected devices online, it is necessary for each of them to carry out all of the above steps. After recovery, it is necessary to monitor the infected computer/s, in order to determine that there is any type of irregularities in their functioning.

Conclusion

Every day, there are approximately 3000 new malicious content on the Internet and it is hard to expect users to defend themselves against each one of it, but using a preventive approach can significantly reduce the likelihood of hacking attacks on computers and other electronic devices and thus enable the smooth operation of information systems and our presence on the Internet.