## **What is malware**

Malware is a software designed specially to do harm to a computer, server or network. It causes damage after the succesful implantation in its target system. It can have many form from executable code, scrip to active content and other software. Malware exploits security defects, vulnerabilities and other problems in the design of the operating system.

Malicious computer programs are constantly growing as the “vendors” apply patches to their systems and the malware evolves once the targeted system becomes more complex. Malware attacks consist as stated in [1] in 2011 from 17 different categories, which only continued to grow until the present days, which will only continue to evolve until they won’t look anything like the malware types we currently battle.

Aici grafic din [1]

Only in 2015 where reportet, stated in [2], that 884,774 new mobile malwares were introduced in 2015, triple the number they fought in 2014. From these new malwares only 6% where new mobile malware categories, where more than 40% are variants of old existing malwares, this is also explained in [2]. Presented in the same documentation [2] presents, briefly, the first malware dataset created in android malicious software, which contained in 2011 1,260 Andoid malware from 49 different categories collected in over a year, from August 2010 to October 2011. This only emphasisez the problem the world is facing, that malware is one today’s greatest threats.

Malware isnt only found in the problems of big companies or important personalities. Malware is a breaking point in computer forensics. As stated in [3], criminal uses malware defence to ty and get away with their criminal activities while claiming they did nothing wrong. Computer security focuses on keeping the cyberspace protected, computer forensics is fighting to bring the digital footprint to the court.

As seen for now malwares are found everywhere and people fighting against it, have a non-stop job and many barriers. For the computer forensics as [3] describes, the struggle is to bring a clear, simple and direct way to present the behaviour of malwares without all the technical jargon. They even categoriezed the malware types as simple as possible, so that everyone can understand the implications of each category. Presented below we see the categories from perspective of [3].

Aici categoriile din [3]

## **Why?**

## **How to stop it**

## **Who fights against it?**