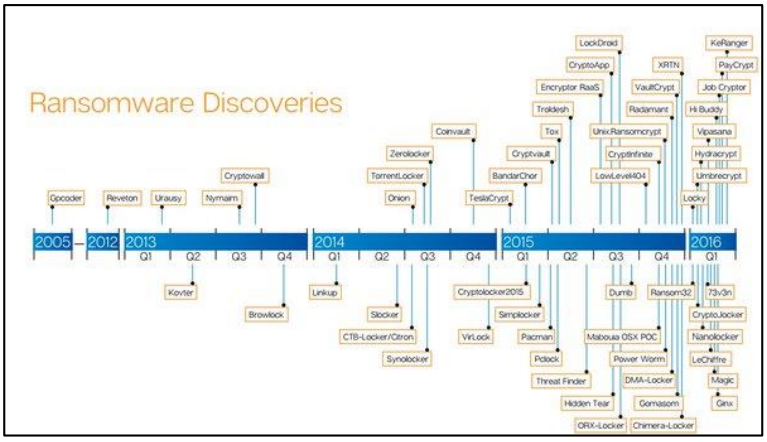
Editorial

Cyber-Attacks Trends in 2016

Cybercrime is becoming more hostile and confrontational. The number of cyber-attacks is growing and the cyber criminals are becoming increasingly aggressive, especially in case of extortion.

Cybercrime nowadays represents a grown industry; the Cybercrime-as-a-Service (CaaS) model offers easy access to illegal products and services. Unexperienced cybercriminals can use these services and launch cyber-attacks anywhere in the world with less knowledge and resources and sizeable profits for them. That's why malware attacks, particularly information stealing and banking trojans, represent the major threat encountered in the cyberspace, as reported by police enforcement.

Ransomware attacks, that can encrypt all the victim's files, have grown in terms of scale and impact and represent one of the primary threats. With free tools and documentation from the Dark Net, many hackers can built and spread their own forms of ransomware. That is one of the reasons why the number of ransomware variants exploded in the last months.



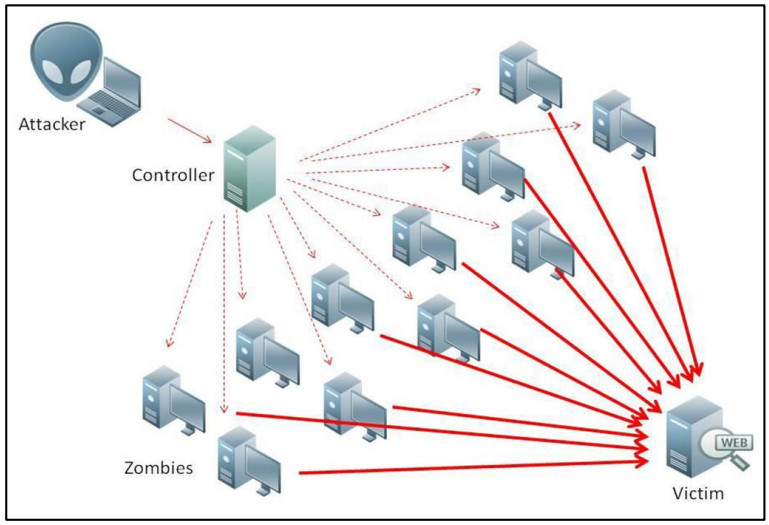
Source: Internet Security Threat Report - Symantec

Banking malware still represent a common threat for citizens and the financial sector, generating huge profits for cybercriminals. Cybercrime groups can use the source code from famous banking trojans such as Zeus, Citadel or Spyeye, and make their own variants of trojans, like Game-over-Zeus or Peer-to-Peer Zeus. More than this, a new generation of malware such as Dyre or Dridex, started to affect the financial sector.

The number and frequency of publicly disclosed data breaches is dramatically increasing. Such breaches, especially when sensitive personal data is disclosed, lead to secondary offences as the data is used for fraud and extortion.

Child sexual exploitation in on-line environment represents also a major concern for police enforcement. There are hidden services, websites and forums that are used for the distribution of child abuse pictures and videos. These services can be easily accessed by users with Tor (The Onion Router) browsers for sharing materials and opinions on specialized forums. Files of this nature can be posted with innocent intent on social networks and collected by offenders in order to exploit the victims. The big volume of indecent materials and the rate of its evolution represents an important challenge for law enforcement.

Most of cyber-attacks are possible because of the grown number of vulnerabilities. The industry focuses for the moment on productivity and profit and not on cybersecurity or privacy. Many smart devices are not secured and have a lot of vulnerabilities that can be easily exploited by hackers. All the compromised devices can be parts of botnets and can be used in major cyber-attacks, like DDoS (Distributed Denial of Service) attacks.



Source: Massive DDoS Attacks - RealNets

Social engineering is a common and effective tool used for anything from complex multi-stage cyber-attacks to fraud. Cybercriminals use the Social Networks like Instagram, Twitter or Facebook to corroborate the information and to build targeted and successful attacks.

Services like Darknet, technologies like Internet of Things (IoT) or artificial intelligence, the existence of zero-day vulnerabilities, tools for anonymisation and encryption, and the lack of cybersecurity awareness offer new opportunities for cybercriminals.

In order of fighting and combating the cybercrime phenomenon, law enforcement have to expand initiatives to share knowledge, expertise and best practice in cyber investigations. In this process, the priority is given by the international cooperation among cybercrime divisions, cybersecurity industry, academia and private sectors.

Assist. Prof. Dr. ***Ioan-Cosmin MIHAI***
Vice President of Romanian Association for Information Security Assurance