Analysis of Computer Malware and Common Attacks

Andreea-Ioana FRĂȚILĂ
ETTI, University "Politehnica" of Bucharest, Romania
andreea.fratila@yahoo.com

Abstract

Technological evolution comes the progress of cybercrime, which continually develops new attack types, tools and techniques that allow attackers to penetrate more complex or well-controlled environments and produce increased damage and even remain untraceable. This paper provides in two different chapters an overview of techniques for analyzing, classifying the malware and different attack types and presents measures that each company must implement in order to ensure security. Organizations need to understand and protect themselves from many different types of threat actors, so it is valuable to know a little about them, their attributes, and the types of attacks they are likely to launch.

Index terms: cyber-attack, malware, protection, cybersecurity

References:

[1]. Norton, Keep your digital life safer, https://us.norton.com, Accessed: December 2019.
[2]. D. Gibson, CompTIA Security+, 2017, ISBN 978-1939136053, pp. 431-520.
[3]. Technology Dictionary, https://www.techopedia.com/definition, Accessed: December 2019.
[4]. R. Nastase, Securitate Cibernetica: Ghid complet de initiere in Securitate si Hacking, https://ramonnastase.ro/blog/, Accessed: December 2019.
[5]. SQL injection, https://portswigger.net/web-security/sql-injection, Accessed: December 2019.
[6]. Think like a hacker: How to protect your business from cyber attacks, https://www.bytestart.co.uk/think-like-hacker-protect-cyber-attack.html, Accessed: December 2019.
[7]. Beaming, UK businesses are attacked online once every 2.5 minutes, https://www.beaming.co.uk/cyber-reports/uk-businesses-attacked-online-every-two-half-minutes/, Accessed: December 2019.