Cybersecurity. An Analysis on Cyber-Attacks Structure

Ioan-Cosmin MIHAI[1], Ioan C. BACIVAROV[2]

[1] Police Academy "Alexandru Ioan Cuza" University, Bucharest, Romania;
[2] EUROQUALROM - ETTI - University POLITEHNICA of Bucharest, Romania
cosmin.mihai@academiadepolitie.ro

Abstract
The recent cyber-attacks (May 2017) have increased the importance of the issue of cybersecurity at both national and global level. It is important to mention that the cyber-attacks experienced during the last period a great diversification and some of them can be classified as a global epidemics. There are many kind of cyber-attacks like malware: computer viruses, worms, trojans, adware, spyware, ransomware, rogueware, Distributed Denial of Service, e-mail and web based attacks. This paper examines and classifies all these cyber-attacks using the intrusion model Kill Chain, defined by researchers from Lockheed Martin.

Keywords: Computer, Security, Cybersecurity, Cyber-attack, Virus, Analyses, Intrusion model, Model Kill Chain

References:

[1] Gorman, S. and Barnes, J., "Cyber Combat: Act of War", 2011.
[2] Tidwell, T., Larson, R., Fitch, K. and Hale, J., "Modeling Internet Attacks", 2001.
[3] Cowan, C., Wagle, P., Pu, C., Beattie, S. and Walpole, J., "Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade", DARPA Information Survivability Conference and Expo (DISCEX), 2000.
[4] Hutchins, M. Eric., Clopperty, Michael J., and Amin, Rohan M., "Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", 2011.
[5] Majority Staff Report, "A Kill Chain Analysis of the 2013 Target Data Breach", 2014.
[6] ENISA Threat Landscape 2014, "Overview of Current and Emerging Cyber-Threats", 2014.
[7] Tulloch, M., Koch, J., and Haynes, Sandra, "Microsoft Encyclopedia of Security", Microsoft Press. 2003, p. 16.
[8] Preimesberger, C., "DDoS Attack Volume Escalates as New Methods Emerge", eWeek, 2014.
[9] Ramzan, Z., "Phishing attacks and countermeasures", Handbook of Information and Communication Security, Springer, 2010.
[10] Gragido, W., "Lions at the Watering Hole – The "VOHO" Affair", RSA Blog. EMC Corporation, 2012.