Cyber Kill Chain Analysis

Ioan-Cosmin MIHAI[1], Ștefan PRUNĂ[1], Ionuț-Daniel BARBU[2]
[1] "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
cosmin.mihai@academiadepolitie.ro, stefan.pruna@academiadepolitie.ro
[2] EUROQUALROM, University POLITEHNICA of Bucharest, Romania
barbu.ionutdaniel@gmail.com

Abstract
The purpose of this paper is to present a structured approach of Advance Persistent Threats attacks and to analyze the intrusion kill chain in order to determine intrusions indicators. The analysis divides the phases of a cyber-attack and map them to response procedures.

Index terms: cyber kill chain, cyber-attacks, APT, incident response

References:

[1]. E.M. Hutchins, M.J. Cloppert, and R.M. Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., 2010, pp. 113-125.
[2]. F. Duran, S. H. Conrad, G. N. Conrad, D. P. Duggan, and E. B. Held, Building a System for Insider Security. IEEE Security & Privacy, 7(6), 2009, pp. 30-38.
[3]. K. Epstein and B. Elgin, Network Security Breaches Plague NASA, 2008.
[4]. B. Krekel, Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation, October 2009.
[5]. J.A. Lewis, Holistic Approaches to Cybersecurity to Enable Network Centric Operations, April 2008.
[6]. Mandiant, M-Trends: The Advanced Persistent Threat, January 2010.
[7]. Microsoft Security Bulletin MS09-017: Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (967340), May 2009.