Critical Analysis on Advanced Persistent Threats

Volume 141 - Number 13

Year of Publication: 2016

Authors:
Murtaza A. Siddiqi, Naveed Ghani

Abstract

Since the birth of Internet, cyber securities have always been an area full of unsolved problems for researchers. Particularly in the age of information, every corporate and government site needs to keep their sensitive data secure from hackers or intruders. With rapid advancement in improved security measures, there always comes along a threat which forces researchers to be on alert. In recent times “Advanced Persistent Threat” (APT) has been among the most highlighted threat for security experts. At early stages such attacks were dedicated to government or financial organizations, but recent studies based on security breaches indicate that such attacks are now carried out on a much wider domain. In this paper crucial attack stages with the most common methods and tools use by intruders to initiate APTs are discussed, along with recommendation on how a model can be defined to perceive an APT attack being conducted on a network.

References
1. Revealed: Operation Shady RAT By Dmitri Alperovitch, Vice President, and Threat Research McAfee, 2011.
3. Mandiant. APT1: Exposing One of China’s Cyber Espionage Unit.
8. Getting Owned By Malicious PDF – Analysis. GIAC (GPEN) Gold Certification Author: Mahmud Ab Rahman, mahmud@cybersecurity.my. SANS Institute

Index Terms

Computer Science

Biomedical

Keywords

APT, Malware, Security, Cyber, Hacking, Internet.