{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 141
-
Number 13

Year of Publication: 2016

Authors:

Murtaza A. Siddiqi, Naveed Ghani

10.5120/ijca2016909784
{bibtex}2016909784.bib{/bibtex}

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.
2. Protecting Your Critical Assets Lessons Learned from “Operation Aurora” By McAfee Labs and McAfee Found stone Professional Services,2010.
3. Mandiant. APT1: Exposing One of China's Cyber Espionage Unit.
4. OPERATION “KE3CHANG”: Targeted Attacks Against Ministries of Foreign Affairs Authors: Nart Villeneuve, James T. Bennett, Ned Moran, Thoufique Haq, Mike Scott, and Kenneth Geers. FireEye, White Paper.
5. National Institute of Standards and Technology (NIST), Special Publication 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, USA, 2011
6. Advanced Persistent Threats: A Symantec Perspective Preparing the Right Defense for the New Threat Landscape. WHITE PAPER: Cutting Through The Hype(www.symantec.com)
7. FireEye Labs. Fireeye advanced threat report 2013 (Special Report).
8. Getting Owned By Malicious PDF – Analysis. GIAC (GPEN) Gold Certification Author: Mahmud Ab Rahman, mahmud@cybersecurity.my. SANS Institute
9. ADVANCED PERSISTENT THREATS AND OTHER ADVANCED ATTACKS Websense® White Paper.
10. Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game? Authors: Nikos Virvilis, Dimitris Gritzalis, Theodoros Apostolopoulos Information Security and Critical Infrastructure Protection Research Laboratory Dept. of Informatics, Athens University of Economics & Business (AUEB) 76 Patission Ave., Athens, GR-10434 Greece {nvir, dgrit, tca}@aueb.gr.
11. In-Depth Look: APT Attack Tools of the Trade. Author: Kyle Wilhoit (Senior Threat Researcher) Trend Micro-TrendLabs Security Intelligence Blog.

Index Terms

Computer Science Biomedical

Keywords

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