Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 123 (2018) 278–284

Procedia Computer Science

www.elsevier.com/locate/procedia

8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017

Remote Attacks Taxonomy and their Verbal Indicators

Natalia Miloslavskaya

National Research Nuclear University MEPhI
(Moscow Engineering Physics Institute), Moscow, Russia
ngmiloslavskaya@mephi.ru

Abstract

To detect and to timely interrupt increasingly sophisticated attacks against modern networks, their systems, services and resources, it is especially important to understand the scenarios and phases of various possible attacks, specific for these networks. Based on the analysis of tremendous number of sources and generalizing various descriptions, remote attacks taxonomy (classification) and their key verbal indicators are proposed.

Peer-review under responsibility of the scientific committee of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures

Keywords: Attack Kill Chain Model, Verbal Attack Indicator, Remote Attack, Attacks Taxonomy (Classification)

1 Introduction

According to ISO/IEC 27000, an attack is referred to an attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (ISO/IEC 27000, 2016). 2016 Cyber security Skills Gap report by ISACA indicates that more than one in four organizations have already experienced an advanced persistent threats (APTs) and predicts $150 mln average cost of data breach by 2020. Thus, the paper's goal is to present the results of analysis of different attack scenarios description and their phases as they are defined in different sources, using them for working out taxonomy (classification) and key verbal indicators of remote network attacks.

2 "Attack Kill Chain" Model Evolution

The "Kill Chain" term was originally used as a military F2T2EA concept. As an integrated, end-to-end process described as a "chain" because an interruption at any stage can interrupt the entire process, it includes the following phases (Hutchins, 2010): Find/locate the target; Fix it location or make it difficult for it to move; Track it movement; Target: select an appropriate weapon to use on the target to create desired effects; Engage/ apply the weapon to the target; Assess/evaluate effects of the attack. Outside of military context, phase-based models have been used in the information security (IS) field. The first typical intrusion scenario was presented by Robert Graham in (Graham, 2000):

Peer-review under responsibility of the scientific committee of the 8th Annual International Conference on Biologically Inspired Cognitive Architectures
10.1016/j.procs.2018.01.043

1. *Outside reconnaissance*, during which an intruder tries to find out as much as possible without actually giving him(her-)self away by finding public information or appearing as a normal user. In this stage, he/she cannot be detected. The intruder does a "whois" lookup to find information about the target network as registered along with its Domain Name, walks through DNS tables to find the names of computers in the target network, browses other public information, such as public websites, anonymous FTP sites, etc.
2. *Inside reconnaissance*, where the intruder uses more invasive techniques to scan for information, but still doesn't do anything harmful, for example, walking through the web pages and looking for vulnerable CGI scripts, doing "ping sweeps" to find alive computers and UDP/TCP scans/strobes on target computers in order to see what services are available. At this point, the intruder has done "normal" activity on the network that can be classified as an intrusion.
3. *Exploit usage*, during which the intruder starts exploiting possible vulnerabilities on the target computers, for example, attempting to compromise a CGI script by sending shell commands in input fields, to exploit well-known buffer-overrun holes by sending large amounts of data, starting to check for login accounts with easily guessable or empty passwords, etc.
4. *Foot hold*, aimed at hiding the attack evidence (modifying the audit trails and log files) and making sure he/she can get back in again by installing toolkits for further access, replacing existing services with trojans that have backdoor passwords, creating new user accounts, etc. The intruder then uses the system as a stepping stone to other systems, since most networks have fewer defenses from inside attacks.
5. *Profit*, where the intruder takes advantage of his/her status to steal confidential data, misuse system resources, etc.

Slightly different, but very similar view on the same process is given in (Olzak, 2008):

1. Reconnaissance to collect as much information as possible about the target;
2. Scanning perimeter and internal network devices looking for vulnerabilities;
3. Gaining access to resources to extract information of value to the intruder or to use the network as a launch site for attacks against other targets;
4. Maintaining access long enough to accomplish his/her objectives;
5. Covering tracks to hide the intrusion and possible controls left for future visits.

The later appeared "Attack Kill Chain" modifies these models for actionable intelligence when defenders align network defensive capabilities to the specific processes an intruder undertakes to target that network. Computer scientists at the Lockheed-Martin Corp. articulated a new "Intrusion Kill Chain" framework or model to defend computer networks in 2011 (Graham, 2000), containing the following stages:

1. *Reconnaissance*: the intruder selects target, researches it (via passive search, port scans and so on) and attempts to identify vulnerabilities in the target network;
2. *Weaponization*: the intruder creates remote access malware weapon with exploit (such as a virus or worm) into a deliverable payload (e.g. Adobe PDF or Microsoft Office files), tailored to one or more vulnerabilities;
3. *Delivery*: the intruder transmits weapon to target (e.g. via e-mail attachments using spear phishing, infected websites or USB drives);
4. *Exploitation*: the malware weapon's program code triggers, which takes action on target network to exploit vulnerability of systems, applications and so on;
5. *Installation*: the malware weapon installs access point (e.g. "backdoor", trojan) usable by intruder and allowing him/her persistent access and escalate privileges;
6. *Command and control*: the malware enables intruder to have "hands on the keyboard" persistent access inside the target network;