Modeling and analysis of Advanced Persistent Threats

Giulia De Santis, Abdelkader Lahmadi, Olivier Festor
INRIA - Nancy Grand Est
{giulia.de-santis, abdeklader.lahmadi, olivier.festor}@inria.fr

1. Motivation

- Advanced Persistent Threats (APTs) are one of the information threats faced today by enterprises and government agencies.
- An APT involves several attack steps, dispersed spatially and temporally. Even if they seem to be unrelated, as a whole they constitute a single powerful attack.
- Assessing if the system is facing such a threat requires to collect, analyze and correlate various sources of data to create summarized views.

Is it possible to detect running APTs by correlating individual attack steps?

2. Related work

Most of the existing work focuses on modeling already known attacks [1, 2]:

- **Attack trees** [3]: leaves or branches are linked by AND or OR gates.
- **Attack graphs** [4]: they capture changes over time of the total security of the network by capturing interrelations of vulnerabilities.
- **Attack pyramid** [5]: an attack path may go across different environments of the organization.
- **Hidden Markov Models** [2]: used to estimate patterns followed by attacks and the stage they are in.

3. Motivation scenario: the Carbanak APT

The cyberattack can be described through:

- the **context** where it takes place,
- **events** which happen in the system,
- already known **attack patterns**.

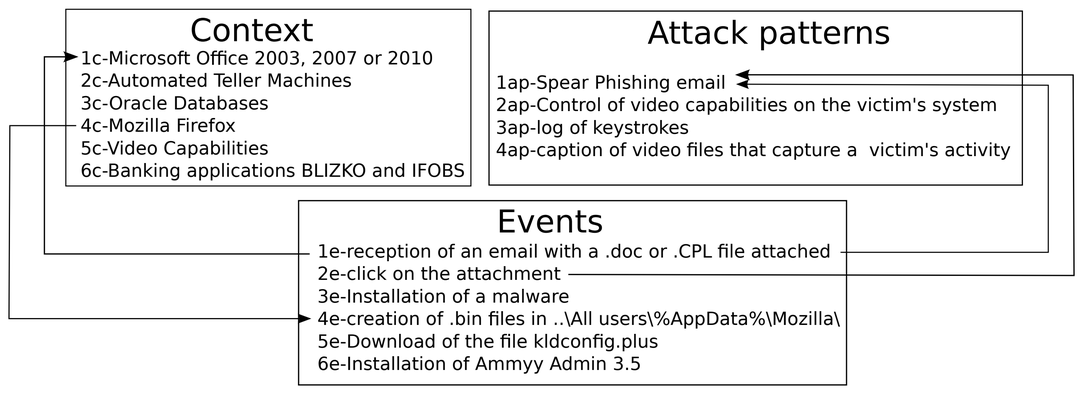

Figure 1: Modeling elements and their relations for Carbanak attack

Required environment and previous knowledge for Carbanak to be operating:

- presence of Microsoft Office 2003, 2007 or 2010 (context);
- reception via e-mail of a .doc file (event);
- opening of the .doc file (event): this action installs a malware;
- presence of Mozilla Firefox (context);
- creation of a .bin file by the malware (event) in a folder created by Mozilla Firefox;
- spear phishing model (attack pattern).

4. Modeling of APTs

The proposed approach:

- aims to characterize relations (if they exist) between attacks faced by the system, since some of them may be related and part of the same complex attack;
- relies on a multi-layer modeling technique to integrate low and high level patterns of APTs;

in order to create a suitable assessment model before knowing the attack faced by the system.

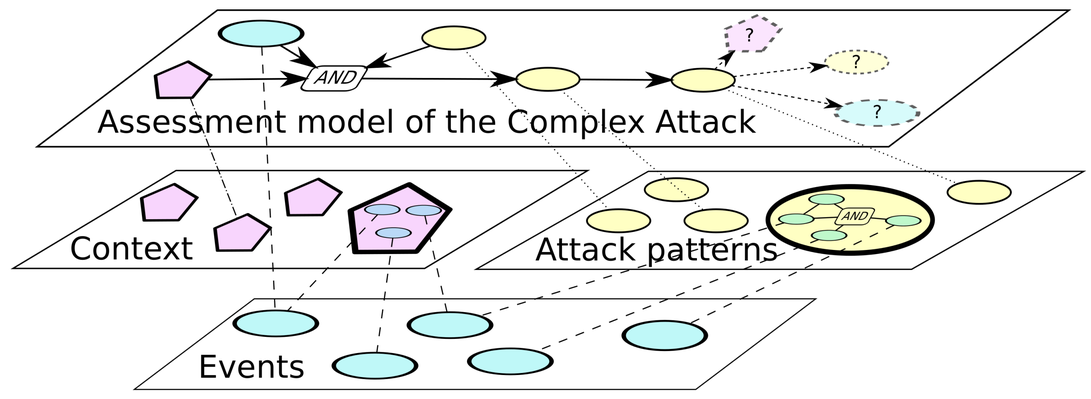

Figure 2: Proposed approach

- **First layer, Events**: normal actions and alarms generated by security systems;
- **Second layer, Context and previously known Attack patterns**: the context representing the configuration of the system;
- **Third layer, Assessment model**: the model for the possible running APT, created through relations between elements of the other layers.

5. Future Work

- Evaluation of possible models of APTs and their attack steps.
- Correlation of events, attack patterns and context in an assessment model using machine learning and AI techniques.
- Application of this methodology to real datasets and systems which are facing unknown attacks.

6. Bibliography

[1] B. Kordy, L. Piètre-Cambacèdés, and P. Schweitzer, “Dag-based attack and defense modeling: Don’t miss the forest for the attack trees,” *Computer science review*, vol. 13-14, pp. 1–38, 2014.

[2] Z. Cui, I. Herwono, and P. Kearney, “Multi-stage attack modelling,” in *Proceedings of Cyberpatterns 2013*, pp. 78–89, 2013.

[3] B. Schneider, “Attack trees,” *Dr. Dobb’s Journal*, December 1999.

[4] S. Abraham and S. Nair, “A predictive framework for cyber security analytics using attack graphs,” *International Journal of Computer Networks & Communications*, January 2015.

[5] P. Giura and W. Wang, “Using large scale distributed computing to unveil advanced persistent threats,” *SCIENCE*, vol. 1, no. 3, p. 93, 2013.

Acknowledgement

This work is partially funded by the HUMA project under the FUI-19 and the Region of Lorraine.