A USER/EVENT BEHAVIOR ANALYTICS (UEBA) APPROACH TO CYBERSECURITY THREAT PREDICTION AND EARLY ALERT

Lam Kwok Yan*, Zhao Yunwei* and Chi Chi-Hung+

*School of Computer Science and Engineering, NTU +Commonwealth Scientific and Industrial Research Organisation, Australia

CYBERSPACE AND CYBERSECURITY

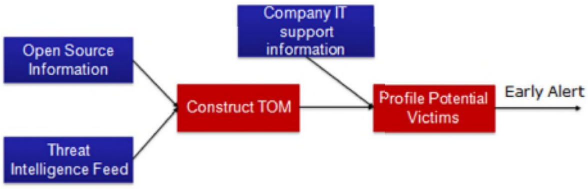
Increasing complexity of Cyberspace

- Increasing number of parties involved
- Loosely regulated infrastructure
- (Non-IT) human users deeply engaged

User/Event behavior driven approach

- A new dimension over system/data security
- Big data approach to Cybersecurity
- Holistic view on lifecycle of cyber attacks
- Patterns as well as correlations
- Prediction and early alerts/intervention of "Cyber Kill Chain"

SOLUTION DEVELOPMENT



We defined the notion of Threat Operating Model (TOM). Cybersecurity analyst studies and investigates the behavior and target system characteristics of cyber attacks. Results of the analysis can be represented by a TOM, which describes how does an attack work and what environments does it target and operate in, as well as what impact/damages will it cause to the victim.

Key Steps:

- Construct TOM based on open source information
- Establish the connection between behavior in the log file and potential threat via TOM
- Similarity analysis between the user/system behavior profile and TOM constructed

PROBLEM DEFINITION

Open source threat information

Environment of Interest:

Given an environment of interest,

- user behavior
- system installation and configuration

How do we describe their behavior w.r.t Cyber security based on open source threat information widely available today?

How likely will this environment be attacked?

THREAT OPERATING MODEL

Threat Operating Model (TOM) is a model for describing cyber threats. It describes the behavior of the attack actor, the system environment that the attack is applicable to, the observed behavior of the target systems and the impacts/damages to the victims, etc.

Threat Operating Model

- Operation system
- Security protection
- Browser characteristics
- Software installation
- Software configuration
- Connection to real world, e.g. BYOD (Bring your own device)

……

TOM (example)

- Distribution Channel: IRC, P2P networks, newsgroup postings, email spam, etc
- Type: Trojan
- Systems Affected: Win10,..
- Attack Process: SONAR.MSWord!g5 is a heuristic detection for threats distributed as Microsoft Word documents.
- Damages: Unexpected Connection to a remote website displaying adverts.