Research Paper

Volume : 2 | Issue : 8 | August 2013 • ISSN No 2277 - 8179

Analysis of a cyber attacker's behavior characteristics under economical changes

Computer Science

KEYWORDS : agent based simulation model, cyber security, vulnerability, economic dynamics

Diana Neghina Institute of Doctoral Studies, ASE, Bucharest, Romania

Emil Scarlat Faculty of Cybernetics, ASE, Bucharest, Romania

ABSTRACT

Our research aim is to present certain cyber attacker behavioral characteristics studied using agent based simulation modeling, highlighting their trends in the context of economic changes. There is to be determined that the overall behavior progression of such cyber threats is greatly influenced by economical shifts.

While a constant improvement of technology and security controls is a characteristic of matured IT environments, in the case of upper middle developing countries that are still growing, organizations are managing security controls at lower levels and cooperation between business entities and regulatory institutions. By implying different reputational and operational risks exposures, the development process of the cyber security framework is developing slowly within these organizations with the negative effect of being an open market for vulnerabilities exploitation.

1. Introduction

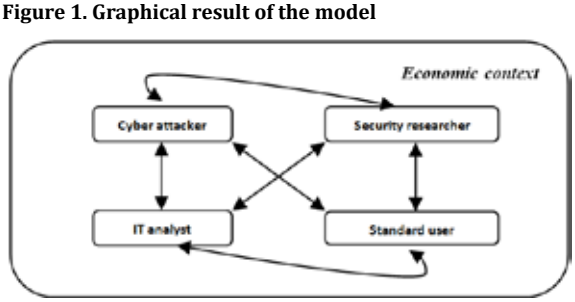
Agent based systems are a significant exploration domain, especially in the field of information technology and cyber security, with an extensive number of research starting from the fundamental roles, basics and its effects on private and public organizations (Amoroso, 2007), to comprehensive approaches of information assurance from both a national and global perspective covering risks, threats and emergency response planning (Knapp, 2009) and going through deep cyber warfare technical information sustained by real world examples and guidance on network defensive strategies (Andress and Winterfeld, 2011) up to the present by providing policies issues on a global scale as well as objectives and guidance for decision makers (Bayuk et al., 2012); on a more technical approach, research studies detailing encryption techniques, networking protocols, security standards and management systems are also provided (Zubairi and Mahboob, 2012).

2. Research Objectives

Though our research, we are attempting to determine the changes that occur in the behavior of a cyber-attacker in the context of macro-economic changes, with the purpose of raising awareness of required security controls and decision making strategies in response to the accelerated growth in complexity and intensity of malware threats. Defined parameters to monitor the characteristics of the agents permit the performance review and impact over the security elements. Economic changes considered as events motivate behavior to occur, and consequences such as a high probability of not being caught sustain it (Jackson, 2012).

The general cyber security model proposed in prior work (Neghina and Scarlat, 2013) is defined with a focus on forecasting methods and risk analysis of cyber threats. An overview of the components of the model is presented below:

Figure 1. Graphical result of the model



Based on the model design presented in fig. no. 1, it is highlighted a significant degree of symmetry and interactions between actors, the optimization being applied based on its immediate scientific benefits as an effective approach to investigating cyber-defense mechanisms against network threats (Kotenko, 2010). The characteristics of the cyber attacker's behavioral model are designed to interconnect with each actor in a manor corresponding to the interactions and operational environment of a real IT security system. A graphical diagram of the cyber attacker's model input elements, expected output parameters as well as other impacting elements is presented below.

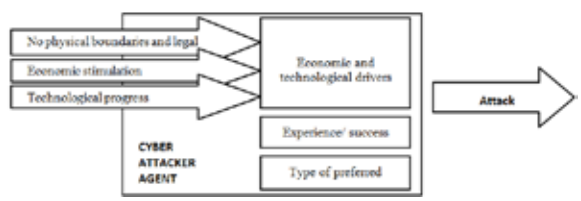


Figure 2. Proposed cyber attacker agent architecture

For the current study, the economic factors (dynamics and availability of information to be obtained, investment rate in technology and security of assets, etc.) are seen as a class of risk factors of a cyber-threat such as social or political activism, classified governmental data theft, foreign economic interest, leakage of business intelligence to be further traded on underground markets.

Based on the existing Lewin's equation in psychology, the mathematical statement of behavior as a function of the person P in their environment E (Sansone, Morf & Panter, 2004) B = ƒ(P, E), our aim is to express through a linear expression the profile of the cyber attacker based on the defined input characteristics, as follows:

(1) Profile = f (TRL, CP, DE, APP, ST)

Table 1. Influencing variables of the cyber attacker's behavioral function

Var.	Definition	Explanation
TRL	Technology Readiness Assessment	The technological and security maturity level of the targeted entity, expressed by a qualitative variable ranging from 1 to 9 (TRA Guidance, 2011).
CP	Cooperation Percentage	Level of cooperation between entities (either private or public) to notify uncertain activity within private networks.
DE	Motivation	Dynamics of the entity's economy, representing a general measure of the winnings expected by the cyber attacker.
APP	Approach	Variable influenced by parameters such as attack approach – either structured or not, type of attack, etc.

ST	Skills and Tools	Variable influenced by the attacker's experience and skills, available tools – more advanced that the available technology of the entity in scope, teamwork or not, etc.

In order to sustain our research, based on the National Institute of Statistics data, the trend of the investments indices within Romania for the previous year is a slightly increasing one, having a positive percentage rate of 2%, encouraging a more dynamic behavior of the cyber attacker. However, as per the previous year e-Threat Landscape Report (BitDefender, 2012), an increasing activity in cyber threats and behavior was forecasted for the following period, with a rate of approximately 6% from previous year, in 2011, presenting a more dynamic environment of the cyber threats. As highlighted in previous work (Neghina & Scarlat, 2013) the cyber attacker's activity has a tendency to develop more rapidly than decision makers may assess problems and determine appropriate countermeasures. Moreover, based on the study into cyber security (Security and Defense Agenda report, 2012), Romania ranked in the top most vulnerable countries to cyber-attacks and cybercrime, having a relative low level of resilience to cyber threats. It is considered a developing, upper middle income country (World Bank Institute, 2013) and is characterized by growing technological infrastructures with a middle maturity level that clearly represent new opportunities for cyber attackers in the context of economic changes.

By increasing and decreasing the economic stimulation, however with a direct impact over the technological progress, we have obtained different modifications in the output of the cyber agent behavior model. The effects were identified in certain schemes of events in which the cyber attacker agent was first monitored for a period of time after which the input parameters for economical characteristics are altered multiple times, determining lower values and increased ones:

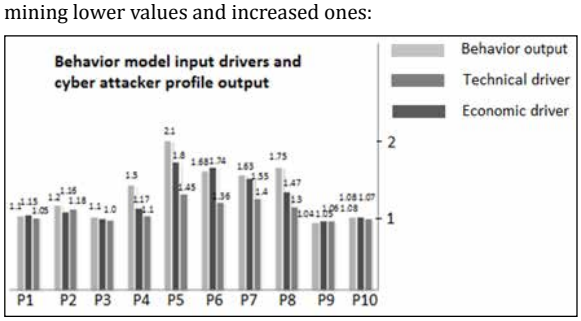


Figure 4. Behavior agent parameters variation results

3. Discussions over Obtained Results

We have set the first cluster of columns with an average level of 1 of all input and output elements of the model, generating a starting reference point. For the second one, we have slightly increased the economical parameter, with an influence over the technological parameter and an increase in the cyber attacker's behavior. Such a situation is plausible for the malicious behavior of an individual hacker with the profile of a hacktivist.

For the second and third simulation exercises, we have modified the technological input, slightly decreasing it, obtaining also a decrease for the economic aspects and for the behavior of the attacker. Interestingly enough is the fact that for the fourth cluster, the economical aspect was raised with the technical aspect kept constant and a significant increase in the dynamism of the behavior can be easily observed. This is explained as a real situation since the attacker will be provoked and would take advantage of the fact that the targeted gains may be higher, thus intensifying his activity and aggressiveness in actions. For the fifth simulation test we have increased the economic parameter, observing an approximately doubled activity for the cyber attacker's profile. We have considered this as a theoretical case, where the economy is developing over a very short period of time, attracting malicious behavior.

The rest of the simulation trials are based on variations of the same principal situations described above, simulated for assessment purposes in order to test a wide functional profile of malicious behavior, directly impacted by economic and technological drivers. To change this basic agent model into a significant decision making data analysis tool, mainly for forecasting use and validation, additional work is required to correct and catalogue the characteristics of the involved actors in order to reflect to the best extent the capabilities the human behavior and actual situations.

4. Conclusions and Future Work

It is important to see the cyber attacker in the context of the global model, being impacted by other actors and additional parameters. The model may support IT security analysts in verifying different hypotheses without any impact and time and resource consuming activities.

Open research areas are achieved by validating further the group cyber attacker's characteristics, as they increase significantly the impact they have as a formation on the same parameters and actors of the model. If the behavior of a cyber-attacker can be modeled, the anticipated impact on the security environment of an entity can be efficiently predicted, allowing for better planning and resources allocation.

REFERENCE

1. World Bank Institute: Country Classification, http://data.worldbank.org/about/country-classifications/country-and-lending-groups#Upper_middle_income (2013) | 2. Neghina, D.E., Scarlat, E.: Managing information technology security in the context of cyber-crime trends, International Journal of Computers, Communications and Control, | vol. 8 - 1 (2013) | 3. Amoroso, E.: Cyber Security, Silicon Press (2007) | 4. Knapp, K.J. (Ed.): Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions, IGI Global (2009) | 5. Andress, J., Winterfeld, S.: Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, Syngress Publishing (2011) | 6. Bayuk et al., Jennifer L.: Cyber Security Policy Guidebook. John Wiley & Sons (2012) | 7. Zubairi, J. A., Mahboob, A. (Eds.): Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies, IGI Global (2012) | 8. Kotenko, I., Goti A., (Ed.): Agent-Based Modeling and Simulation of Network Infrastructure Cyber-Attacks and Cooperative Defense Mechanisms, Discrete Event Simulations, http://www.intechopen.com/books/discrete-event-simulations/agent-based-modelingand-simulation-of-network-infrastructure-cyber-attacks-and-cooperative-defense- (2010) | 9. Jackson, G.M.: Chapter 1 - Analyzing the Malicious Individual, Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security, John Wiley & Sons (2012) | 10. Security and Defence Agenda Report: Cyber-security: the vexed question of global rules, | http://www.securitydefenceagenda.org/Contentnavigation/Library/Libraryoverview/tabid/1299/articleType/ArticleView/articleId/3063/categoryId/63/SDA-report-Cybersecurity-The-vexed-question-of-global-rules.aspx (2012) | 11. Sansone, C., Morf C., Panter A.T.: The SAGE Handbook of Methods in Social Psychology, SAGE Publications (2003) | 12. Technology Readiness Assessment (TRA) Guidance: US Department of Defense | http://www.acq.osd.mil/chieftechnologist/publications/docs/TRA2011.pdf (2011) | 13. Botezatu B.: Bitdefender H2 e-Threat Landscape Report | http://www.bitdefender.com/media/materials/ethreats/en/H2_2012_EThreat_Landscape_Report-final-edited.pdf (2012)