Distributed Cybersecurity Strategy, applying Intelligence Operation concept through data collection and analysis

Ignacio Martín Gallardo Urbini[1][0000-0002-1983-895X] ,
Patricia Bazán[2][0000-0001-6720-345X] ,
Paula Venosa[3] and Nicolás Del Río[4][0000-0002-0889-0752]

[1] National University of La Plata, Buenos Aires, La Plata, Argentina
ignacio.gallardou@info.unlp.edu.ar,
[2] LINTI. National University of La Plata, Buenos Aires, La Plata, Argentina
pbaz@info.unlp.edu.ar,
[3] LINTI. National University of La Plata, Buenos Aires, La Plata, Argentina
pvenosa@info.unlp.edu.ar,
[4] National University of La Plata, Buenos Aires, La Plata, Argentina
ndelrio@info.unlp.edu.ar,

Abstract. This document presents a line of doctoral research that proposes a cybersecurity strategy that has not been formally standardized up to now, based on knowledge of defense intelligence operations, and applying a dynamic approach, in a context of threat risk, anticipating its effectiveness . In this way, change the current approach, leaving aside the old concept of "walled" defense, for a more innovative one, where information collectors or "spies" infiltrate "unknown terrain" or external networks to extract data and information, learn from context, analyze and detect patterns, be willing to share the knowledge, and then be able to make defensive, deterrent, or offensive decisions in real time.

Keywords: Cybersecurity, Big Data, Data Intelligence, Multivendor.

1 Introduction

Many people in the world have studied computer science, specializing in information security, cybersecurity and cyber defense; however, many of them are currently responsible for related sectors to these areas of knowledge in different parts of the world, including Government Agencies, the Army or big private organizations directly linked to society and the State. However, just few of this large population have actually devoted their time to practicing and studying intelligence strategies and tactics; perhaps it is due to this reason the rarity of bringing the security of information systems to the field of intelligence and making use of these ancient techniques. This line of research and development has the general objective of addressing a reflection on static defensive schemes and then proposing new techniques that are born in the intelligence doctrine and address the inequality between the millions of internet threats and specific objectives specially defined to combat them, applying new methods of operations. Any leader of an intelligence strategy, known to the unequal defense forces, must not be static but it should be dynamic; observing and analyzing the enemy by means of data collectors distributed in the observation field, gathering techniques, information analysis, exchanging other resources for “time”, sharing the learned knowledge with other allies (interoperating with external vendors [12] for cooperation and information enrichment), and only when there is a high degree of certainty, then respond. In the specific case of an intelligence operation[1], there will be a threshold below which no further progress can be made, this line is called the "diffusion stage", and it reaches it by applying a strategy to guarantee security called "intelligence operation" and it is what gives rise to this thesis proposal.

2 Objectives

Among the specific objectives of this research are the following:

- Plan and organize the defensive security strategy applying intelligence operations tactics and strategies[10] in order to transform the current "static" defensive attitude[2] into an innovative and "dynamic" one.
- Investigate, develop and implement computer components distributed in the network for the gathering of information, in order to efficiently maintain the picture of the threat situation both in the observation stage for learning and knowledge of the hostile context.
- Develop and implement an intelligent system applying data mining concepts and machine learning techniques that are nourished by the information obtained by the computer components named in the previous objective.
- Study and evaluate different machine learning models to check and select the most optimal and efficient one.
- Provide an Application Programming Interface and Communication Protocol for sharing the intelligence knowledge with external solutions.
- Converge in the implementation of an early and real-time detection system of anomalous patterns in the network, in order to make decisions in advance of the materialization of a possible threat.

The original contribution of this line of research is practically based on the proposal of a cybersecurity strategy not yet formally or standardized, supported by knowledge of intelligence operations for defense, and applied to a dynamic approach, in the face of the existence of a risk of threat, anticipating that it becomes effective. In this way, change the current approach, leaving aside the old concept of "walled" defense for a more innovative one, where information collectors or "spies" infiltrate "unknown terrain" or external network to extract data and information , learn from the context, analyze and detect patterns, and then early and in real time, be able to make defensive, dissuasive or offensive decisions.

3 Motivation and State of the Art

Traditional security solutions[2] focus primarily on protecting the perimeter of interest, thus focusing primarily on external threats. Yet these are constantly evolving, requiring those who wish to remain resilient in their operations to stay informed and one step ahead of attackers. For the definition of a defensive cybersecurity strategy, the same variables that are taken into account in the intelligence doctrine applied to national security can be used, where elements of aggression similar to those analyzed in a cyber attack are presented: sabotage, harassment the victim in his own land, use of irregular detachments with rapid and surprise attacks, secrecy, great mobility, temporary blockages of the basic channels of communication and supplies, and kidnapping / theft of assets. Faced with this new context of advanced cyber threats, in which criminal and hacktivist groups with political and economic interests are involved, the motivation arises to start this line of investigation in order to carry out the development of an intelligence or cyber intelligence strategy as an element key to reinforcing the information security strategy.

Currently projects that address similar objectives:

- Splunk Behavioral Analytics is a software product designed to face internal risks in organizations. It aims to cover the problem from the analysis of user behavior [3].
- FireEye Threat Analytics, a software solution that applies threat intelligence, firewall rules, and advanced security data analytics to optimize detection and response to alerts that matter [4].
- Munin, is an initiative that wants to build a low interaction honeynet, where vulnerable services that are considered critical in an organization are simulated, and that are typically published on the Internet. This project aims to collect information on botnet attacks and then study them [5].
- C1fApp is a threat feed application, which provides a single feed, both Open Source and private. Provides statistics dashboards, API open for search, useful and running for a few years. Searches are historical data [6].
- Cymon is a multi-source indicator aggregator with threats history that provides an API for searching a database along with a nice web interface [7].
- Palo Alto Artificial Intelligence and Machine Learning in the Security Operation Center - Cortex Module, provides components spread out across the enterprise and cloud, providing data to AI services that within minutes can detect new malware and identify malicious domains. The components also provide the point at which policy enforcement, based on the results of the AI services, prevent successful cyber-attacks [12].

The framework proposed in this thesis includes tactics and strategies, and procedures applied in intelligence operations included in the national intelligence doctrine itself [7], in Spanish and for public use, with a open communication protocol for sharing the learned knowledge with external vendors to be used or consuming data from them, integrating data collectors, adaptable anomaly detection modules and a frame of reference to get ahead of the enemy and thus be able to take a dissuasive, offensive or defensive action. Of these similar projects described above, none provide a comprehensive joint framework like the one proposed in this thesis.

4 Experimental Proposed Work

To validate the proposal, put the strategy into practice and test the operation, the development and implementation of a systems architecture that will be made up of different software components will be addressed. On the one hand, the network of sensors (baits) "spies" in charge of collecting information on the activity of the network will be developed. These will have the property of simulating conventional communications with each other and at the same time being able to report in real time to the expert knowledge system. On the other hand, the development of a prototype tool should be addressed to contribute to the detection of behaviors compatible with cyberattacks or cyber threats. Information processing and analysis comes into play here, invoking the different machine learning algorithms, thus converging on a system of expert knowledge and its implementation in real time. The following requirements should also be addressed:

- Observe the behavior of the tool under different cyber attack situations. To achieve this, the development of an alert system must be carried out.
- Have operational and upgradeable ease of the tool: With learning and training mechanisms as its use increases.
- Observe metric graphs, comparing the values obtained from the network flows where the monitoring system is installed.
- Identify behavior patterns: according to the observed graphs, associated with different stages of cyber attacks and classify the threats.

- Build an Application Programming Interface with a Communication Protocol to be able to share the intelligence knowledge with external similar solutions.

5 Research Methodology

As previously stated, any security solution will be tied to the strategic decision to use. However, opting for tactics and strategies applied to intelligence doctrine[9] provides dynamism and great added value at the time of defense. This research work adopts a qualitative methodology[10] for the development of the security architecture from scratch together with its component components, in order to achieve this strategy. Current security measures fall short of polymorphic threats, therefore a new line of thinking must be considered. It is reiterated that what is really critical is the total ignorance of the adversary regarding its location, magnitude, resources, behavior and capabilities, from which the first imbalance of forces arises. On the other hand, when studying defense and security activities throughout history, there are no records of any invulnerable fortress. Given these two aspects, it is proposed to analyze cybersecurity from the point of view of dynamism and intelligence, that is, leaving aside the current conception of static and centralized defense materialized in Instruction Detection Systems, Intrusion Protection Systems, or Firewalls. The intelligence doctrine[9] with its millenary experience in collecting, analyzing information and making decisions, raises a particular scenario of operations, where the reason for this research called "Cybersecurity Strategy applying the concept of intelligence operation" takes center stage. This procedure is precisely designed for contexts in which the threat is greater than the victim, there is little information about the victim, and by virtue of this imbalance is why it is planned to "Exchange resources by *time*, to be able to know the threats, anticipate to the facts and have a clear and defined overview of the context".

References

1. Andrew C.: The Secret World, a history of intelligence. (2019).
2. Endorf C., Schultz G., Mellander J.: Intrusion Detection and Prevention. 1st Edition. ISBN-10 0072229534. (2003)
3. Splunk Integrated Behavior Analytics Homepage, https://www.splunk.com/, last accessed 2021/03/20.
4. FireEye Overview page, https://www.fireeye.com, last accessed 2021/03/20.
5. Munin Homepage, http://munin-monitoring.org/, last accessed 2021/03/20.
6. C1fApp Homepage, https://blog.thehive-project.org/tag/c1fapp/, last accessed 2021/03/20.
7. Cymon Api Homepage, https://cymon.docs.apiary.io/#, last accessed 2021/03/20.
8. National Argentine Intelligence Law Homepage, http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm, last accessed 2021/03/20.
9. Handel M.: Intelligence and Military Operations. (1990).
10. Sampieri R, Fenández, Collado C. and Baptista L.: Metodología de la Investigación, 5ft Edition, McGraw-Hill Interamericana. (2010).
11. Washington P.: Producción de Inteligencia Estratégica. Buenos Aires. Struhart Cia. (1983).
12. Palo Alto Artificial Intelligence Module Overview Page, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/artificial-intelligence-and-machine-learning-in-the-security-operations-center, last accessed 2021/04/05.