Proceedings of the International Conference on
Information Technologies (InfoTech-2018)
20-21 September 2018, Bulgaria

NEW APPROACHES IN THE EXAMINATION OF THE CYBER THREATS[1];

Roumen Trifonov[1], Slavcho Manolov[2], Radoslav Yoshinov[3], Georgi Tsochev[1], Georgi Popov[1], Galya Pavlova[1]

[1]Technical University of Sofia, 8 Kl. Ohridski bul.,Sofia 1000,
[2]Association EDIBUL, Sofia 1220
[3]Bulgarian Academy of Sciences, Sofia 1000
r_trifonov@tu-sofia.bg, slav1943@gmail.com, yoshinov@cc.bas.bg, gtsochev@tu-sofia.bg, popovg@tu-sofia.bg, raicheva@tu-sofia.bg
Bulgaria

Abstract: The present paper describes some of the results obtained in the Faculty of Computer Systems and Technology at Technical University of Sofia in the implementation of project related to the application of intelligent methods for increasing the security in computer networks. In order to build a rational and consistent approach to the choice of artificial intelligence methods best suited to counteract certain classes of threats, it is necessary to achieve systematization, unification and classification of the cyber-security threats and the sources of these threats. This can be realized using the new concepts and classifications in the field of cyber threats examination.
Key words: cyber threats, taxonomy, threat agents, threat vector, threat matrix, kill chain

1. INTRODUCTION

This report aims to outline the main points of a study "Analysis of the latest trends in threats in various cyber-attacks" carried out within the framework of the project "Increasing the level of the Network and Information Security using Artificial Intelligence methods", funded by the Science Fund of the Ministry of Science and Education. The above mentioned study is a part of the work package 1 of the project

[1] This research is conducted and funded by a scientific-research project № H07/56 "Increasing the level of network and information security using intelligent methods" under the contract D07-4 with National Science Fund in Bulgaria.

named "Analysis of the application of Artificial Intelligence methods in the Network and Information Security".

The main purpose of the study is to analyze, above all, the existing practices in the worldwide investigations for a unified description and comprehensive classification of Cyber-Security threats and the sources of these threats so as to build a rational and consistent approach to the choice of methods of Artificial Intelligence, best suited to counteract certain classes of threats. Moreover, having into account not only the use of these methods for predicting certain types of attack, for repulsion of attacks, but also for automation of the process of incident handling (i.e. dealing with the consequences of the attacks).

The motivation of the research is based on the belief that the new approaches to identification, classification and analysis of the threats will be useful in choosing the appropriate application method for counteraction. Such comprehensive research into new approaches has not been found in the reference sources, which shows its novelty. The research at this stage has been completed and their outcome has served as a basis for selecting Artificial Intelligence methods for various cyber-protection cases.

2. A NEW STAGE IN THE EVOLUTION OF CYBER-SECURITY THREATS

Among the leading experts, there is a consensus that the last five or six years have been celebrated by the fifth generation of cyber-crime, where threats are becoming more complex and automated. The major cyber-crime schemes realize integration within a few sets of tools that perform different functions. One of the peculiarities of the fifth generation is so called "Advanced Persistent Threats" (APT), as a definition for targeted attacks against concrete organizations by certain well-coordinated cybercriminals [1].

In recent years, like popular cloud computing services as SaaS (Software as a Service), IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and so on in the cyber-crime world has been developed so called Crimeware as a Service (CaaS) - a modern model that provides easy access to the tools and services needed to commit cyber attacks [2]. This allows even novice cyber-criminals to perform attacks on a scale that is disproportionate to their technical capacity. The next picture (Fig. 1) shows organization of Ransomware attack using the CaaS.

The radical changes in the field of Cyber-Security during the last two or three years have been formulated and adequately described in the remarkable ENISA report "Threat Landscape Report 2016" [3]. ENISA and other leading Cyber-Security players have identified a transition from the phase of Cyber-Criminality to the phase of Cyber-Ware, where the most serious destructive effects are those of a hybrid nature - a combination of cyber-attack and physical attack, the cyber-attack focused

to critical kinetic process, cyber-attack in the time of natural disaster, or critical system failure.

The expert community has very quickly adopted military approaches, technologies and tools. The "Kill chain" is a military concept related to the structure of the attack and aimed to create an effective counter-attack against the opponent in the various phases of the attack or preventive action. The IT specialists of the Lockheed-Martin Corporation have adapted this concept to information security [4], and it is already accepted in the security information community as cyber-defense instrument defining the stages of cyber attacks and corresponding countermeasures at each stage.

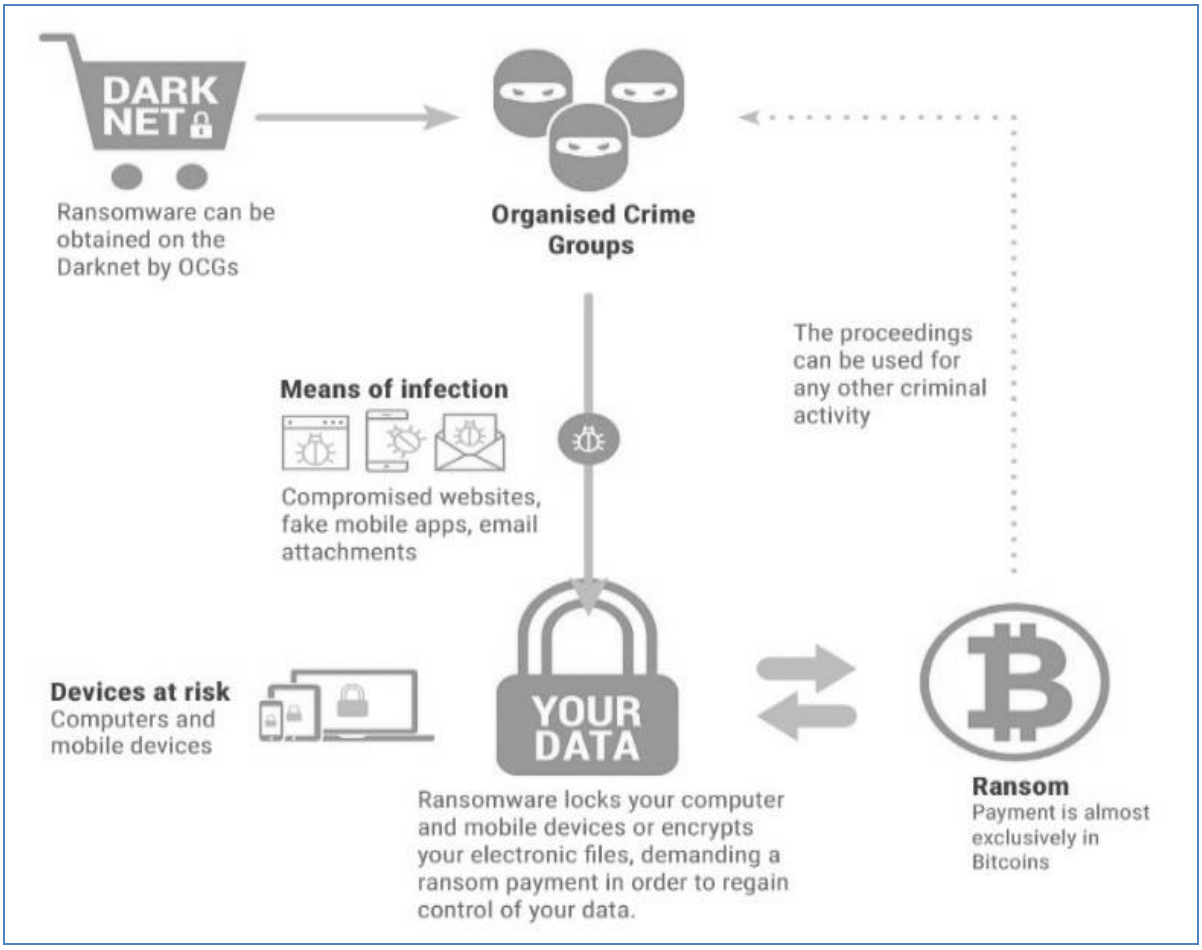

Fig. 1. Organization of Ransomware attack using the CaaS

The "Lockheed-Martin" model includes the following seven steps: a) Intelligence: the attacker selects a target, examines it, and tries to identify vulnerabilities in the target network; b) Creation of the weapon: the attacker creates weapons for remote access, such as a virus or worm, adapted to one or more vulnerabilities; (c) Delivery: the attacker sends the weapon to the victim (for example, via e-mail attachments, websites or USB devices); (d) Exploitation: the activation of the malicious weapon program code that takes action on the target network to exploit the vulnerability; (e) Installation: the malicious software installs

an access point (eg, a "back door") usable by the offender; f) Command and control: the malicious software allows the intruder to get so called "keyboard hands" - constant access to the target network; g) Action on the target: the attacker takes action to achieve his goals, such as data mining, data destruction, or ransom encryption.

3. NEW CLASSIFICATIONS AND CONCEPTS IN THREAT ANALYSIS

To enable systematization, unification and classification of cyber-security threats and the sources of these threats so that will be possible to build a rational and consistent approach to the choice of artificial intelligence methods best suited to counteract certain classes of threats, it is necessary to identify and analyze the new concepts and classifications in the field of Cyber Threats.

Above all, this is so called "Cyber Threats Taxonomy" [5] published by ENISA on the basis of an analysis of about 40 taxonomies developed by world-leading organizations (including NIST and the US Department of Defense (USA), BSI (BRD), TERENA (Netherlands), etc.).

The Threat Taxonomy is structured in three fields:

• the threat category primarily used to differentiate families of threats;

• different threats in a given category;

• details of threats - based on a specific type / method of attack or direction to a specific IT asset.

The aAdditional fields include help information such as: affected assets, threat agents, related sources / URLs, etc.

An important element of the systematic analysis of cyber threats is the systematization of the sources of threats. This is achieved through the formation of groups of sources with similar characteristics (motivations, level of capabilities, focus, level of preparedness, striking power, etc.) and called "threat agents". In [3] has been defined the following threat agents:

- cyber-criminals are the most active threat agent group in cyber-space, being responsible for at least two third of the registered incidents. This group has undergone some further maturity and progress, merely regarding its capabilities and used techniques to maximize monetization;
- insiders have been one of the main actors to threaten their organisations, both intentionally and unintentionally. Intention, negligence and error are the three sources of threats attributed to this group, intention is source of the fewer incidents. Most typical are violations of existing security policies through negligence and user errors;
- hacktivists usually protest against themes such as environmental policy, discrimination, corruption, pacifism, public health issues, support of minorities, media (incl. large events, commercial developments and international conflicts).

Experience shows that hacktivists cooperate on a group basis without any leadership schemes;

- state (or large corporation)-sponsored actors, the cyber-spies have been approximately the fourth most active threat agent group. Formally speaking, this threat group would include intelligence agencies and military organisations. Due to the early maturity of military cyber-capabilities it is not perfectly clear where the differentiation between cyber-spying and cyber-combating might be. This raises important questions in the cyber-security community, namely if the loss of high-end state-sponsored cyber-tools are equivalent to loss of heavy weapons;
- others - less important as their role in the landscape – are: cyber-fighters, cyber-terrorists and script-kiddies.

The involvement of the above mentioned threat agents in the deployment of the identified top cyber-threats is presented in the Table 1. Its purpose is to visualize which threat agent groups are involved in which threats. This information is targeted towards stakeholders who are interested in assessing possible threat agent involvement in the deployment of threats. This information might be useful in identifying the capability level can be assumed behind the top threats and thus support in decisions concerning the strength of the security controls that are implemented to protect valuable assets.

Table 1.

	Treat agents							
	Cyber criminals	Insiders	Nation states	Corpo-rations	Hacktivists	Cyber-fighters	Cyber-terrorists	Script kiddies
Malware	●	♦	●	●	♦	♦	♦	♦
Web-based attacks	●		●	●	●	●	●	●
Web application attacks	●		●	●	●	●	♦	♦
Denial of service	●		♦	♦	●	●	●	●
Botnets	●		●	●	♦	●	●	●
Phishing	♦	●	●	●	●	●	♦	
Spam	♦	●	♦	♦				
Ransomware	●	♦	●	●		♦		♦
Insider treats	●					♦	♦	
Physical manipulation/damage/ theft/loss	●	●	●	●	♦		♦	♦
Exploit kits	●		●	●		●		
Data breaches	●	●	●	●	●	●	●	♦
Identity theft	●	●	●	●	●	●	♦	♦
Information leakage	●		●	●	♦	♦	●	♦
Cyber espionage		♦	●	●		♦		

Attack methods and tools applied by the concrete threat agent form the so-called “attack vector”. This is a means by which a threat agent can abuse of weaknesses or vulnerabilities on assets (including human) to achieve a specific outcome. In the correct context, the study of the different steps performed on an

attack vectors can provide valuable information about how cyber threats can be materialized.

The description of the workflow of the attacks are important pieces of information in order to have a better understanding of cyber threats and the tactics, techniques and procedures (TTP) followed by threat agent, and gives to defenders the opportunity to implement appropriate defences to eliminate vulnerabilities.

Since kill-chains provide a generic classification scheme which is helpful for a better understanding of the method of an attack, references to the kill chain nomenclature may be found during the descriptions of the attack vector and the behavior of involved threat agents.

The identification of the adversary's abilities, the current situation, patterns of past and current behavior, and specific tasks, techniques and procedures are supported by the historical review of past campaigns, reflected in the so-called "threat matrix" [6]. This matrix (Fig. 2) gives priority to the potential scope of the threat sources by focusing on those who have already shown intent and ability to attack. It is used for priority allocation of resources to most likely opponents and contains qualitative and quantitative evaluation criteria.

THREAT PROFILE							
THREAT LEVEL	COMMITMENT			RESOURCES			
	Intensity	Stealth	Time	Technical Personnel	Knowledge		Access
					Cyber	Kinetic	
1	H	H	Years to Decades	Hundreds	H	H	H
2	H	H	Years to Decades	Tens of Tens	M	H	M
3	H	H	Months to Years	Tens of Tens	H	M	M
4	M	H	Weeks to Months	Tens	H	M	M
5	H	M	Weeks to Months	Tens	M	M	M
6	M	M	Weeks to Months	Ones	M	M	L
7	M	M	Months to Years	Tens	L	L	L
8	L	L	Days to Weeks	Ones	L	L	L

Fig. 2. Threat matrix

The threat modelling [7] is another useful tool for the systematic analysis of threats. This is an iterative process consisting of five major steps (Fig. 3):

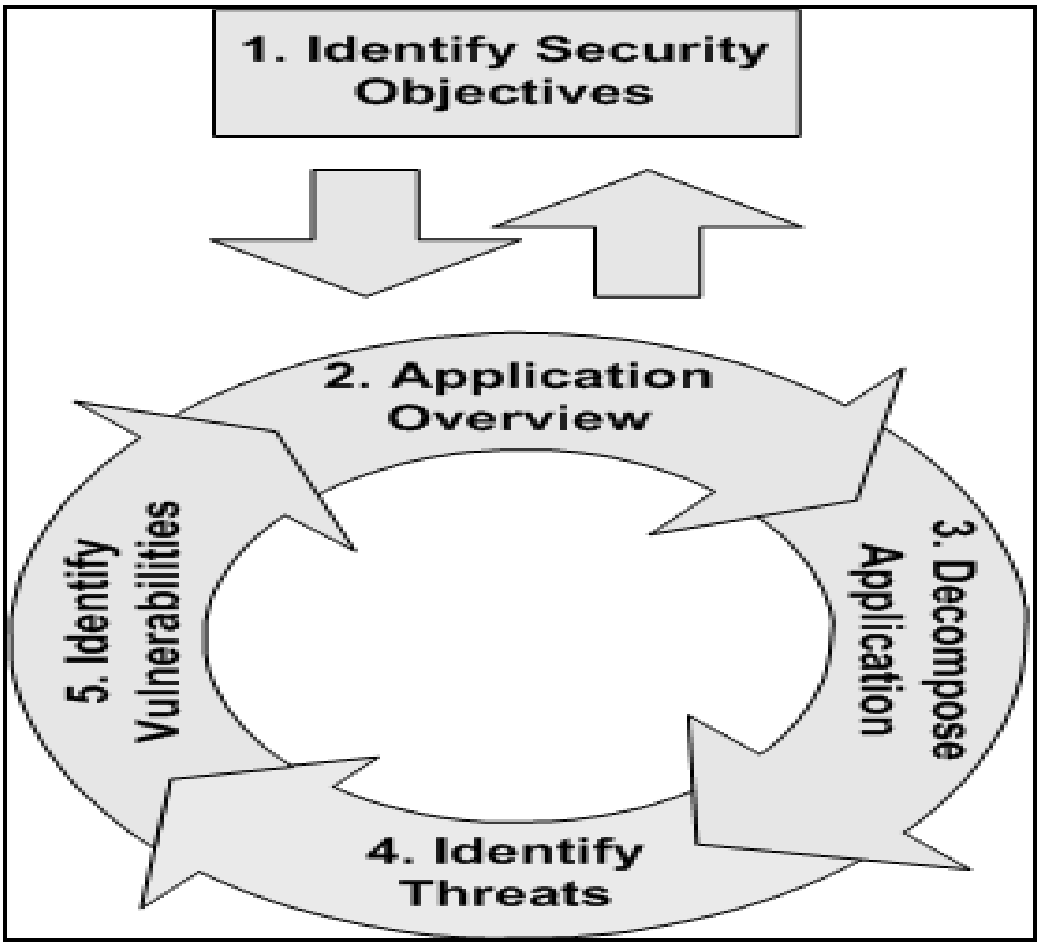

Fig. 3. Threat modelling

a) identification / verification of security objectives – it helps to focus the threat modelling activity and to determine how much effort to spend on subsequent steps;

b) creation of application overview - itemizing application's important characteristics and actors it helps to identify relevant threats during next steps;

c) decomposition of application - a detailed understanding of the mechanics of application makes it easier to uncover more relevant and more detailed threats;

d) threats identification - using threat analysis such as so called "STRIDE" [7], attack trees and a generic risk model;

e) vulnerabilities identification – reviewing the layers of application for searching weaknesses related to these threats and using vulnerability categories to focus on those areas where mistakes are most often made.

Because the key resources identified in threat modelling are also likely to be key resources from a performance and functionality perspective, the model can be adjusted for the concrete needs.

4. CONCLUSIONS

Using part of the above-mentioned new classification and concepts for threat analysis, over 40 types of threats (some with several subspecies) were examined in the Work package 1 of the project - in terms of their evolution, level of impact and complexity, sophistication, availability, attribution, etc.

The analysis of the most important of these threats gives opportunity to evaluate possibility for potential attack pattern recognition and to develop models for active cyber defence.

Ultimately, this predetermined the choice of Artificial Intelligence methods for experiment in the subsequent phases of the project (Multi-agent system - for the case of Tactical Cyber Intelligence and Recurrent Neural Networks - for the case of Operational Cyber Intelligence.

REFERENCES

[1] State of Cybersecurity, *An ISACA and RSA Conference Survey ISACA*, 2016

[2] TrustWave Global Security, *Report TrustWave*, 2016

[3] Threat Landscape Report 2016 ENISA, 2017

[4] www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/ LM-White-Paper-Intel-Driven-Defense.pdf

[5] *ENISA Threat Taxonomy A tool for structuring threat information*, Version1.0, January 2016

[6] Duggan, D. P., Thomas, S. R., Veitch, C. K., & Woodard, L. *Categorizing Threat: Building and Using Generic Threat Matrix Retrieved from* http://www.idart.sandia.gov/methodology/materials/Adversary_Modeling/SAND2007-5791.pdf

[7] Shostack, A. *Threat Modelling desined for securi*ty, John Wiley & Sons, Inc, 2014.