Adversary Profiling and Activity Emulation in the Process of Development and Evaluation of Information Security Threat Countermeasures

Anna Golushko [1] *and* Vadim Zhukov [1]

[1] *Reshetnev Siberian State University of Science and Technology, 31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation*

Abstract

The article describes the problem of insufficient methodical practice in the field of effective countermeasures development against cyber-threats. The knowledge about potentially dangerous adversaries` activity and their methods of action can be applied to find appropriate solution of the issue. Adversary profiling and activity emulation are considered as possible methods for further effective evaluation of the potential information security threats landscape for defended information systems in practice.

Keywords

Information security threat model, adversary profiling, adversary activity emulation, FSTEC, MITRE ATT&CK, TEACH Tripwire, STIX 2.x

1. Introduction

Information security measures effectiveness depends on the overall level of information security maturity in the organization. The international practices, developed by state regulators with the support of experts and research laboratories, are aimed at minimizing information security risks and neutralizing the greatest number of cyber-threats that can be implemented in the conditions of applied technologies. This approach makes it possible to select basic security measures and tools to reduce the likelihood of mistakes that can be made by information security specialists during the process of determining cyber-threats landscape to information security.

For example, the SANS Institute presents the top 18 CIS Controls (Critical Security Controls) which are a recommended group of measures with additional prioritization between them [1]. The Australian Cyber Security Centre presents several lists of Top-4, Top-8, Top-35 information protection strategies [2]. The NIST group of standards in the USA defines an integrated approach to the definition of information protection measures [3].

Methods for assessing risks and cyber security threats are also applied by specialists in order to determine supplementary defensive measures in addition to existing requirements, which must be implemented firstly. However, these methods of assessing risks and cyber security threats are intended for independent expert analysis of the most harmful vulnerabilities, potentially dangerous adversaries, their tactics and techniques of action and used tools.

At the same time, there is a question of insufficient methodical practice to assessing adversaries` skills and capabilities for further definition of potential threats landscape to the protected information infrastructure. Besides, the formed list of cyber security threats affects the approaches for configuration of applied software, hardware devices, security tools and the overall countermeasures structure against computer attacks and any other malicious activity.

AISMA-2021: International Workshop on Advanced in Information Security Management and Applications, October 1, 2021, Stavropol, Krasnoyarsk, Russia
EMAIL: glushko.ap@yandex.ru (Anna Golushko), vadimzhukov@mail.ru (Vadim Zhukov)
ORCID: 0000-0003-0933-3269 (Anna Golushko), 0000-0002-7933-6820 (Vadim Zhukov)

At this moment, potential threats landscape for many types of information systems in Russia is evaluated according to new methodic, developed by Russian government regulator [4], which takes into account knowledge about adversaries, their tactics and techniques of action and potential risks. However, there is not enough practice in the application of new approach that explains the relevance of the problem considered in this paper.

2. Adversary profiling

Information security threat modeling includes the identification of possible adversaries (attackers, malicious users) and their potential. Adversaries are divided into external and internal. External adversaries usually include state intelligence services, competing organizations, unscrupulous partners, criminal groups (criminal structures) and external entities (individuals). Internal adversaries include users, system administrators, service personnel, persons providing maintenance and repair of technical devices, etc. [4]. Possible potential and motive of action are determined for each category of adversaries.

Taking into account the knowledge about attacker actions during cyber-attacks, the existing approach can be improved. This will provide comprehensive approach to the problem described in this paper and helps to develop an information security threat model that is valuable in practice.

As an example, there is considered the category "criminal structures". It can be divided into several groups that have a certain set of characteristic features. In practice, there are the following names of groups that are widely used in publications, annual and quarterly reports in the field of information security: hackers, hacktivists (groups with political motives), cyber terrorists, script kiddies [5]. These categories of external adversaries differ from each other in terms of the level of technical skills, financial resources, goals of activity and other parameters.

It is proposed to build an adversary profiles (threat profiles), which will make the description of each adversary more complete and meaningful for further evaluation of threat landscape to protected information infrastructure. Recommendations for adversary profiling are based on the best practices of SANS [6], recommendations for describing threat metrics of the Sandia National Laboratory under the US Department of Energy [5] and the international information exchange standard on information security threats STIX 2.x [7].

2.1. Attributes of adversary profile

An attacker's profile can contain the following attributes [6]:

- Name.
- Description (category: external/internal, organization level (attack resource level): individual, club, contest, team, organization, government) [8].
- Type of action (targeted/deliberate, mass attacks/accidental reasons).
- Involvement in top security threats (for example, malicious software, web-oriented attacks, denial of service, botnets, phishing, spam, extortion, insider threats, physical damage, exploits, data integrity violation, theft, information leakage, espionage). Examples are given in accordance with the annual reports of ENISA [9] and [10].
- The sphere of target organizations activity (banks, healthcare, education, transport, etc.) [8], [20].
- Region of adversary activity (Europe, Asia, North America, etc.).
- Motive / intention (accidental, coherence, dominance, ideology, notoriety, organizational-gain, personal-gain, personal satisfaction, revenge, unpredictable, financial gain) [8].
- Object of attack (one of the protected objects in the information system / asset).
- Examples of criminal groups (for example, known APT groups representing this category of adversaries).
- Skill level/potential (classification is proposed in accordance with the STIX 2.x standard: none, minimal, intermediate, advanced, expert, innovator, strategic) [8].

- Opportunities. They can include various sub-attributes, for example, technical strength, the availability of financial support, the availability of political support, the number of participants (size), the danger of the threat in terms of consequences (intensity), the time of activity before the attack is detected or the end of the attack (persistence, stealth (ability to hide)).

Table 1 illustrates an example of adversary profile.

Table 1

Adversary profile example

№	Attributes	Profile 1	Profile 2
1	Name	Cyber Criminal	Individuals
2	Description	External, team/organization	Internal, individual
3	Type of action	Targeted	Accidental reasons
4	Involvement in top security threats	Data integrity violation, theft, web-oriented attacks	Insider threats, information leakage
5	The sphere of target organizations activity	Banks	-
6	Region of adversary activity	Europe, Asia, Russia	-
7	Motive / intention	Financial gain, notoriety, organizational-gain	Personal-gain, revenge
8	Object of attack	Databases, servers, software	Databases
9	Examples of criminal groups	APT38, Carbanak, Cobalt Group, RTM, Silence	-
10	Skill level/potential	Intermediate, advanced, expert	None, minimal
11	Opportunities	In Table 2	In Table 2

2.2. Parameters of adversaries` opportunity level

The Sandia National Laboratory in the document [5] defines sub-attributes of adversary opportunities and offers a more formal approach to the categorization of adversaries.

In this approach, eight categories of adversaries (eight levels) are distinguished without differentiation into internal and external. For implementing this approach, known categories of adversaries (hackers, APT-groups, external entities, etc.) can be associated with the values of special parameters and put in accordance with eight levels.

In total, there are seven parameters, which determine the level of adversary:

- Threat danger from the possible consequences point of view (intensity).
- Ability to remain undetected (persistence, stealth (ability to hide)).
- Time of activity until the attack is detected or ended (time).
- Number of group members (technical personnel).
- Level of knowledge and skills in the field of information technologies and information security, which allows implementing attacks (cyber knowledge).
- Level of knowledge in the field of activity of the organization under consideration (kinetic knowledge, in document [5] this name is given in connection with the field of Sandia National Laboratory activity: development, creation and testing of non-nuclear components of nuclear weapons).
- Ability to provide access to the target resources of the attacked organization (access).
- Table 2 illustrates an example of adversarial parameters for attackers from possible defined profiles.

Table 2
Adversarial parameters example for profile

№	Parameters	Cyber Criminal	Competing organizations	Individuals
1	Intensity	High	Medium	Low
2	Ability to hide	High	Medium	Low
3	Time	Months - Year	Few months	1-4 Weeks
4	Technical personnel	10-100	5-25	1-5
5	Cyber knowledge	High	Medium	Low
6	Kinetic knowledge	Medium	High	Low
7	Access	High	Low	Low

In addition, in document [5] authors describe how information security incidents can be evaluated with defined sub-attributes of adversary opportunities.

2.3. An example of profile impact to defensive measures

The importance of objectivity and completeness of the adversaries' assessment can be illustrated by the following example.

One of the protected objects in the organization is a website that operates on the basis of a Content Management System (CMS). Type of action in attack (targeted attacks or mass attacks), capability for writing exploits and other attributes influence the methods of defense [11].

If mass attacks are considered as potentially dangerous, then target organization needs to implement timely security updates of the CMS and installed plugins and control the unavailability of the configuration file containing passwords from databases. Meanwhile, as a method of analyzing the initial security of the website, it will be enough to use a security scanner to search for and eliminate vulnerabilities.

If there is high probability of implementing targeted attacks to information system, then the company's website should be checked with usage of automation tools:

- for collecting information about the CMS from the internet: CMS version, open directories, configuration files, installed plugins, vulnerabilities;
- for availability of ready-made exploits for the identified vulnerabilities.

It is recommended to make an attempt to crack the administrator's password, to exploit the identified vulnerabilities, in other words, to conduct a penetration test for this entry point into the company's infrastructure [12].

3. Adversary activity emulation for further threat countermeasures development

The dependence between methods of attacks used by adversaries and goals of their activity, as well as with possible effective countermeasures, exists for a large number of information security threats. Such dependencies are identified by research laboratories during the process of information security incidents analysis and can be presented in a systematic form.

The most complete and detailed classification was presented by MITRE Corporation in the form of ATT&CK (Adversarial tactics, techniques & common knowledge) matrices [13] and the CAR (Cyber analytics repository) activity detection analytics repository [14].

The ATT&CK matrices contain hundreds of methods (techniques) of malicious actions that can be used in attack scenarios for realization of information security threats. This concept provides opportunity to form a list of information security threats, which definitely may be implemented by adversaries.

The main task for the first stage of working with the adversary techniques taxonomy is to analyze initial list of techniques from ATT&CK and determine those that are probably executable in protected

system. The author has previously considered this issue; the results are presented in articles [15] and [16].

Then, the list of information security threats is studied thoroughly in order to determine the necessary defensive measures. At the same time, defensive measures may depend on adversary profile.

3.1. Adversary activity emulation

In order to ensure the practical significance of the process of determining information security threats landscape, it is reasonable to analyze the initial security level of information system by emulating selected tactics and techniques of adversary actions.

To emulate in this context means to imitate exact tactics and techniques, that attackers use against protected information infrastructure. Emulation provides opportunity to ensure that information security system can detect and defend against the exact type of attacks, which may be expected from real-world attackers.

Emulation of adversary activity can be carried out by building respective plans/chains of techniques for implementation. This approach is the most appropriate, since it allows evaluate possibility of implementing previously successfully carried out attacks in the world that have become known and information about which has been entered in ATT&CK.

In addition, selective emulation of techniques for any tactic can be carried out in order to check individual defense subsystems for resistance to possible actions of attackers.

The tactics in ATT&CK are related to each other. To emulate one tactic, specialist may need the results obtained when emulating another. Figure 1 shows an example of sequential emulation of techniques for the Credential Access [13] and Lateral Movement [13] tactics with Atomic Red Team tests [21].

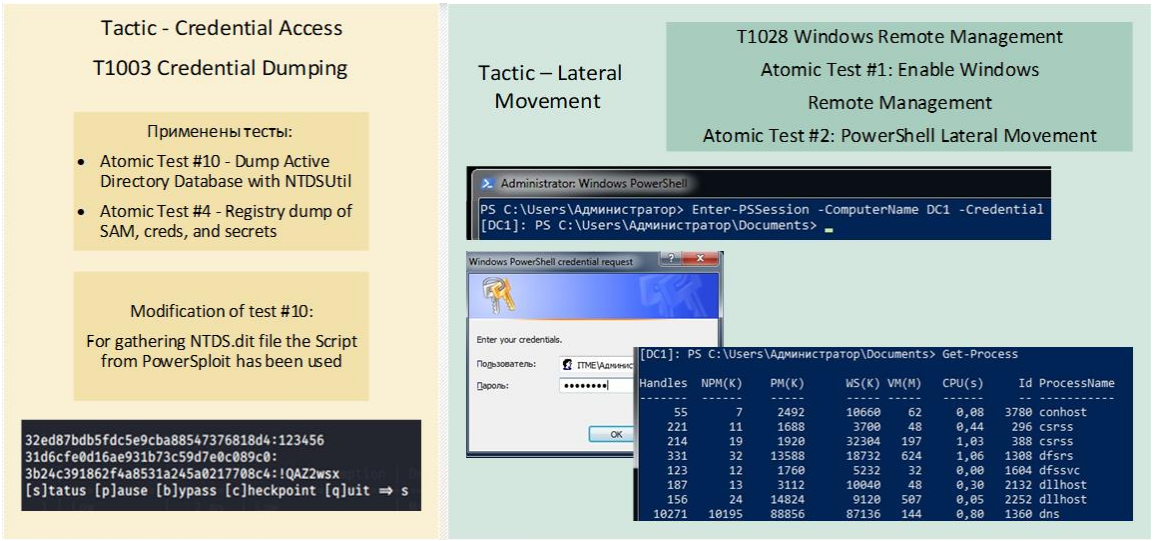

Figure 1: Example of adversary activity emulation

3.2. TEACH approach

It is recommended to take into account results of the Tripwire expert analysis of exploiting techniques complexity from the ATT&CK Enterprise matrix [17]. It is more difficult to emulate some techniques than others are. The Tripwire experts proposed the TEACH classification and laid out a table with a color gradation of techniques in accordance with this classification.

The TEACH approach presents the following complexity levels of adversary activity emulation:

- Techniques Only (those techniques that are not represented by an independent exploit and in general don`t need special actions to achieve tactic);

- Exploitable to Anyone (easily implemented techniques that do not require specialized tools and scripts, can be implemented with built-in services);
- Additional Steps Required (easy-to-use techniques using PowerShell/cmd/bash scripts, Metasploit and other emulation tools);
- Cost Prohibitive (more complex ways of performing actions, it may be necessary to model the real information infrastructure (Active Directory, network and switching equipment, DNS server, DHCP server) [18];
- Hard (the most difficult to implement technologies that require customized libraries and executable files).

Considering these recommendations, emulation of techniques scenarios can be performed starting with the most easily implemented chains of adversary tactics and techniques. It is useful to implement multi-stage threats based on the analysis of criminal group activities that used emulated techniques [19]. Such actually used techniques by adversaries with examples are called procedures in terms of ATT&CK matrices.

4. Conclusion and future work

To sum it up, at the current stage of work, recommendations have been formed for building adversary profile reflecting valuable attributes of criminal group activity. Implementation of adversary activity emulation provides opportunity to evaluate whether possible adversary may actually conduct computer attack using different techniques.

In future work author plans to conduct a research on the questions of mitigation measures implementation against techniques and existing practical issues in application of new threat evaluation methodic [4], where construction of computer attack scenarios from adversary techniques is required.

5. References

[1] CIS Controls, 2021. URL: https://www.cisecurity.org/controls/.
[2] Australian Cyber Security Centre, 2021. URL: https://www.cyber.gov.au/.
[3] NIST SP 800-53, 2020. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.
[4] Methodology for assessing information security threats, the FSTEC of Russia, 2021. URL: https://fstec.ru/component/attachments/download/2919.
[5] Cyber Threat Metrics, 2012. URL: https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2012/122427.pdf.
[6] Creating a Threat Profile for Your Organization, 2014. URL: https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492.
[7] STIX A structured language for cyber threat intelligence, 2021. URL: https://oasis-open.github.io/cti-documentation/.
[8] STIX™ Version 2.1, 2020. URL: https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html.
[9] «ENISA Threat Landscape Report 2017. Top Cyber-Threats and Trends. FINAL VERSION 1.0 ETL 2017», 2017. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017.
[10] «ENISA Threat Landscape Report 2018. Top Cyber-Threats and Trends. FINAL VERSION 1.0 ETL 2018», 2018. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.
[11] Hack-the-web, 2020. URL: https://xakep.ru/2020/02/27/hack-the-web/.
[12] Types of attacks on sites and site protection, 2018. URL: https://o-es.ru/blog/aktualnye-tipy-ugroz-i-dinamika-ih-razvitiya/.
[13] Adversarial Tactics, Techniques & Common Knowledge 2021. URL: https://attack.mitre.org/wiki/Main_Page.
[14] Full Analytic List, 2021. URL: https://car.mitre.org/wiki/Full_Analytic_List.

[15] ATT&CK knowledge base application in the building process of information security threats models. Materials of the XXII International Scientific and Practical Conference "Reshetnev Readings" (November 12-16. 2018, Krasnoyarsk): Krasnoyarsk, 2018, part 2, pp. 322-323. A. P. Golushko, M. N. Zhukova.
[16] Systematized adversary techniques knowledge implementation in the process of assessing information security system effectiveness. Materials of the XXIII International Scientific and Practical Conference, dedicated to in memory of the general designer of rocket and space systems, Academician M. F. Reshetnev (November 11-15, 2019, Krasnoyarsk): Krasnoyarsk, 2019. - part 2, pp. 418-419. A. P. Golushko, V. G. Zhukov.
[17] Tips on how to implement and use the MITRE ATT&CK framework, 2019. URL: https://ethhack.com/2019/05/how-to-implement-and-use-the-mitre-attck-framework/.
[18] Setting up a Threat Hunting Lab, 2017. URL: https://cyberwardog.blogspot.com/2017/02/setting-up-pentesting-i-mean-threat.html.
[19] MITRE ATT&CK groups, 2021. URL: https://attack.mitre.org/groups/.
[20] Five Clear Steps to Enhance SecOps with MITRE ATT&CK, 2021. URL: https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.
[21] Atomic Red Team, 2021. URL: https://github.com/redcanaryco/atomic-red-team.