




# Preventing APT attacks on LAN networks with connected IoT devices using a zero trust based security model

Bruno Carneiro da Rocha <sup>\*</sup>, Laerte Peotta de Melo <sup>\*</sup>, Rafael Timóteo de Sousa Jr. <sup>\*</sup>  
National Science and Technology Institute on Cyber Security, Electrical Engineering Department,  
University of Brasília (UnB), P.O. Box 4466, Brasília-DF, Brazil, CEP 70910-900\*  
Email: rocha.carneiro@aluno.unb.br, peotta@gmail.com , desousa@unb.br

**Abstract**—Many organizations are being targeted by different types of attacks. One of the most dangerous attacks is called Advanced Persistent Threats (APT) as it is silent and focused on espionage and information theft, unlike a denial of service (DoS) attack. The proposed solution addresses the implementation of a security model based on zero trust in order to prevent APT attacks on LAN networks. The proposal is to use the concepts of micro-segmentation and Next-Generation Firewalls (NGFWs). Many IoT devices are present in most networks and most of them have several vulnerabilities that can facilitate the theft of information and compromise the local network.

**Keywords**—APT, IoT, zero trust, micro-segmentation, NGFW

## I. Introduction

With the advancement of internet technologies, information security has become one of the main concerns of organizations. Ghafir found that the volume, complexity and variety of cyber attacks is growing exponentially and many organizations have been targeted by a new type of attack called Advanced Persistent Threat (APT) [1]. This growing trend is being driven by the rise of cyber warfare and also by the rise of the Internet of Things (IoT).

So, a problem arises: how to avoid APT attacks having several IoT devices connected in the network with different architectures, different software and different types of vulnerabilities? To solve this problem, a research was carried out using the Design Science Research (DSR) methodology, consisting of several phases, namely: phase 1 - awareness of the problem, phase 2 - preparing a proposed solution, phase 3 - developing the solution with the application of the proposed solution and making small adjustments, phase 4 - the validation phase of the tests and analysis of the results and finally phase 5 - the conclusion.

978-1-6654-1078-6/21/\$31.00 ©2021 IEEE

In this article, a study of a security model based on zero trust will be presented, in an attempt to prevent APT attacks that can exploit vulnerabilities in LAN networks, mainly coming from IoT devices. In chapter II, important information about the technologies used in this study will be described. Chapter III will describe work already carried out by other researchers in an attempt to stop advanced attacks and in the implementation of zero trust. Chapter IV will describe the proposed defense model and in chapter V an analysis of this model will be made. Chapter VI will describe the conclusions the authors reached as well as possible future work.

## II. Background

### A. Traditional security in LAN networks

Security on LAN networks is usually done at the perimeter of the network, where a Firewall and/or an intrusion detection system (IDS) are usually installed. [2] (Figure 1). However, an external adversary can initiate an attack from a command and control center through an internal user who has previously been infected with malware.

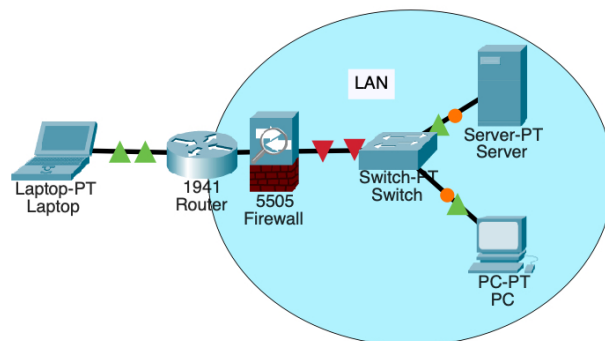


Figure 1: Traditional security in LAN networks

### B. Advanced Persistent Treats (APT)

Zhang found that the term APT Attack was first proposed by the USAF (United States Air Forces) in 2006 [3]. According to the US National Institute of Standards and Technology (NIST), the definition of APT is: Technologically proficient adversaries use a variety of intrusion programs (networking, physical and fraud) with valuable resources to achieve the objective of the attack. According to Ghafir, APT is a cyber threat based on "one-day exploits" where the opponent can still have other attack objectives even with the critical system violated [4]. In [5], the authors show a generic APT attack in four steps, namely: Preparation, Infiltration, Lateral Movement and Data Exfiltration. (Figure 2). Preparation consists of researching which organization will be targeted and which organization has digital assets that are of some importance. Then an employee analysis is done and a generic email is created for the malware submission. Infiltration consists of sending the malware email to selected employees who would be potential targets to run the backdoor. When executed, the adversary has command and control with the target server. Lateral movement consists of installing other backdoors on other nodes of the network to propagate access throughout the company. And finally, data exfiltration from the organization's network nodes is done by the adversary, leaving no logs, so that the attacker continues to infiltrate the network and constantly collect data.

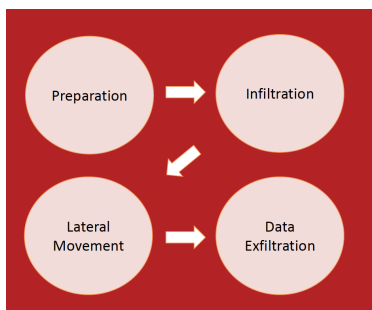


Figure 2: Generic APT Attack

### C. Internet of Things (IoT)

With recent technological advances made in the Internet of Things (IoT), there is an exponential growth of smart devices that help to build ever more interactive scenarios that help people in their daily lives. The authors in [6] found that many popular IoT devices on the market have weak security. This allowed several attacks to these devices using known techniques, such as DDoS (Distributed Denial of Service) attacks or identity theft. Attacks like this compromised the local network and man-in-the-middle attacks were effective

in stealing information. Even with the due concern to protect IoTs from these attacks by companies specialized in security, many devices have a relatively weak firmware (with low power and energy) and the adoption of more efficient security measures is not yet possible.

There are several techniques for exploiting IoT vulnerabilities. The authors in [7] describe in their article some attacks on IoT devices, namely: Distributed Denial of Service DDoS Attacks, Sybil Attacks, Wormhole, Sinkhole or Black Hole, Hello Flood, Traffic Analysis and espionage.

### D. Attack trees

Bruce Schneier, in 1999, described the concept of attack trees as a way to create a threat model against computer systems [8]. This model allows visualizing the threats of a system, from a top-down structure, and encompassing different methods the adversary can attack the system. The adversary's main objective is at the top, at the root node. Leaf nodes represent several ways to achieve the goal. Defense models against cyber attacks can be elaborated from the visualization of the tree structure, observing the possibilities that each node can develop and the information of who the main adversaries and their threats may be.

### E. Zero Trust

According to NIST [9], zero trust is the cybersecurity term to group a series of paradigms that transform "static" defense, which is focused on the network perimeter, into defense focused on users, assets and resources. A Zero Trust Architecture (ZTA) uses zero trust principles to plan workflows and infrastructures for organizations. The basic principle of zero trust is that there is no trust in user assets or accounts based solely on their network location. Whether on the local network or on the internet, user authentication and authorization is required to use resources or perform certain functions. zero trust solves common network problems such as remote users using the local network, use of personal equipment on the network and assets that are in the cloud and that are not available unless the user is physically within the network perimeter. Zero trust's protection focus is on resources (assets, services, workflows, network accounts, etc.) and not on network segments as the location of the network is no longer the main security issue when this posture is adopted.

The main purpose of zero trust is to prevent unauthorized access to data and services so that access is as granular and specific as possible. That is, authorized and approved subjects (combination of users, applications and devices) can have access to specific

resources (printers, computers, IoTs, data, etc). In an abstract access model, a subject needs access to an organization's resource. Access is obtained through a policy decision point (PDP) and corresponding policy enforcement point (PEP) (Figure 3).

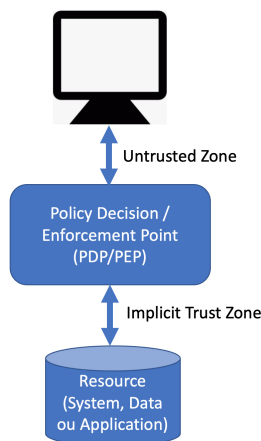


Figure 3: Zero Trust Access

The implicit trust zone represents an area of trust since the last PDP/PEP gateway. PDP/PEP applies a variety of controls so that all traffic after PEP has a common level of trust. PDP/PEP cannot include new security policies after this location in traffic. For the PDP/PEP to be as specific as possible, the implicit trust zone should be as small as possible. And so, for this, a new concept of micro-segmentation of the network is needed.

1) *Network micro-segmentation*: According to NIST [9], there are several approaches that ZTA can be used in workflows. There are three approaches: Enhanced Identity Governance, Logical Micro-segmentation and Software-based Physical Micro-segmentation on the network. These approaches vary depending on the components used and the rules and policies used by the organization. Each approach uses one or more zero trust principles, depending on the security proposal adopted. A complete zero trust solution includes elements of all three approaches. In this work, the focus will be on logical micro-segmentation.

Also according to NIST, an organization can implement a zero trust architecture based on the principle of separating resources individually or in groups on a network segment protected by a gateway security component. In this approach, the organization designs its security devices as smart switches (or routers), Next-Generation Firewalls (NGFWs), or gateways to act as Policy Enforcement Point (PEP), protecting each resource or a small group of related resources.

2) *Next-Generation Firewalls (NGFWs)* : According to Gartner [10], Next-Generation Firewalls (NGFWs)

are firewalls that can do a deep inspection of the transmitted packets. They are not limited to layers 3 and 4 of the OSI model (network and transport), but can also analyze packets at the application level (layer 7). Therefore, they also have a built-in intrusion prevention system. The benefits of using NGFWs over a traditional firewall are many. NGFWs are able to block malware from entering the network, that is, they respond very well in detecting and preventing advanced attacks (APTs).

### III. Related Works

When conducting the research, first, several articles dealing with detection and possible defenses of APT attacks were analyzed. Subsequently, several articles that used the zero trust solution as a defense were also researched. No articles were found that use zero trust as a defense against APT attacks.

In the work on [11], several tests of APT attacks based on the MITER ATT&CK framework [12] were elaborated. The attacks were carried out by injecting a backdoor into the system under study. An analysis of human actions, intentions and severities of APT attacks was done in [13].

The authors in [14], created an architecture based on the zero trust framework to protect IoT devices on the network. In this study, an analysis of a unified identity for IoT devices was performed by determining the security level and the trust level.

A study of the main APT attacks and the main defense mechanisms in IoT was carried out in [15]. In this study, a network defense middleware protecting IoT devices against APT attacks was proposed.

A zero trust model based on Elastic Stack was created in an attempt to protect data transmission over LAN networks [16].

### IV. Development of a Zero Trust APT Attack Security Model

To develop the security model, a case study was prepared. The purpose of this case study is to prevent the adversary from reaching its target, which is to have access to images from a security camera that is connected to the LAN. To create the models, the Cisco Packet Tracer [17] software was used.

For this, a LAN network was modeled containing a camera (representing an IoT device), a gateway for wireless access of the camera on the network, a computer (representing a network user), a switch (to interconnect the computer and the gateway in the network. same network) and this switch connected to a firewall at the edge of the network, representing a typical LAN network with its security focused on the network perimeter (figure 4).

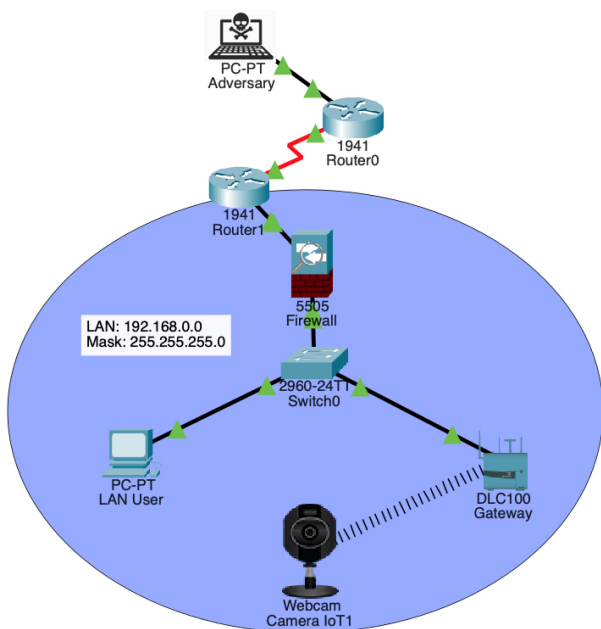


Figure 4: Original LAN Network

Then, the generic APT attack model consisting of four phases (Preparation, Infiltration, Lateral Movement and Data Exfiltration) was used in an attempt to identify the possible attacks of an opponent on the LAN. And before that, an attack tree was created for better analysis and understanding of possible attacks (figure 6). To create the trees, the software SecurITree ([18]) was used.

Some zero trust principles were applied in this LAN. First, the netmask was changed from 255.255.255.0 to 255.255.0.0 to make it easier to configure VLANs. Then the network was micro-segmented, in order to separate a VLAN for IoT devices and a VLAN for users. And then, NGFW was applied to each micro-segmentation. Each segment of this has its own security policy. Unless a user needs to have access to the camera, the firewall has been configured to not have access by default. The network edge firewall has also been replaced by an NGFW. In addition to being able to control which users can connect to the network through its interconnection with Active Directory, it can also identify some possible malware that may be traveling on the network and prevent the initial attacks (Figure 5).

In the first network micro-segmentation, VLAN 1 192.168.1.0 was created. In this VLAN, there is a "LAN User", which corresponds to a network user who received the static ip 192.168.1.1. The NGFW made the VLAN boundary and all connections were closed, so the "Lan User" can only access authorized resources in

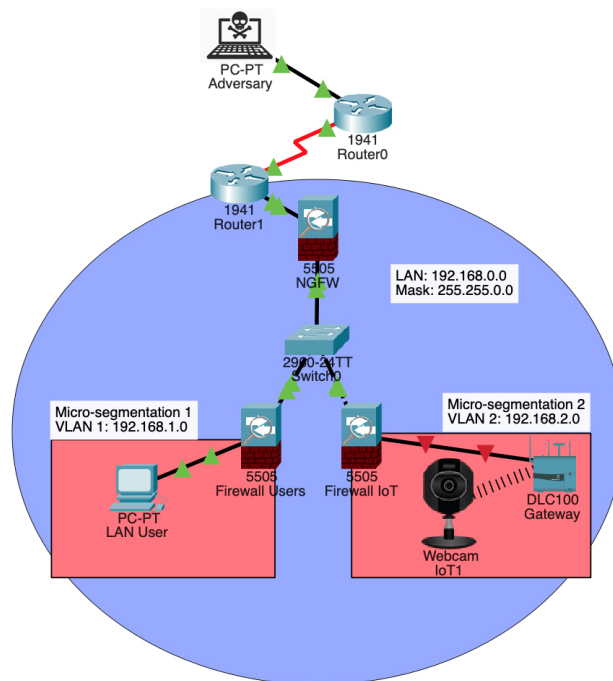


Figure 5: LAN Network with micro-segmentation and NGFWs

addition to being authenticated. Within this VLAN the concept of Implicit Trust Zone was applied, and the NGFW played the role of PEP.

In the second network micro-segmentation, VLAN 2 of ip 192.168.2.0 was created. This segmentation corresponds to the IoTs, separated from the rest of the network by an NGFW, in order to protect any and all unauthorized access attempts, attacks or espionage. The IoT camera, used as an example, received the ip 192.168.2.1 and is also in an Implicit Trust Zone context, performed by NGFW.

## V. Discussions

After the network was micro-segmented and after the installation of NGFWs in the respective perimeters, the attack tree was analyzed again and it was verified which attacks would no longer be possible with these security implementations based on zero trust (Table I):

Table I: Attack tree Analysis

ID	Commentary
1.1	The NGFW blocked direct access to the camera and now only authorized users can access the device. In addition, a specific authorization in the NGFW would be required.

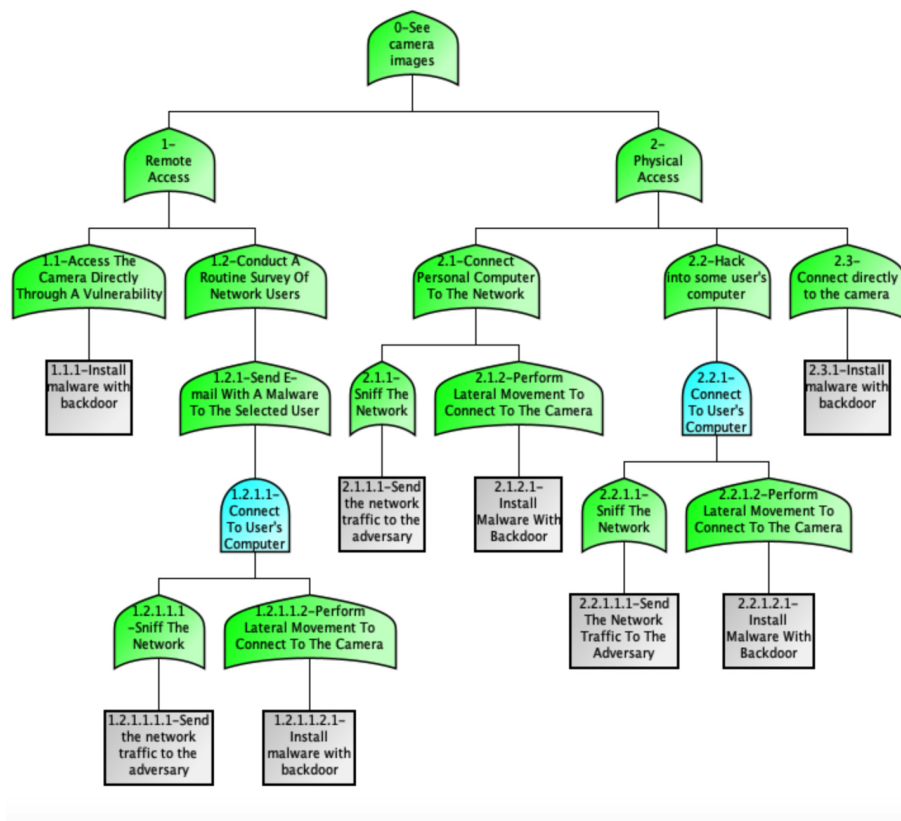


Figure 6: Attack tree

ID	Commentary	ID	Commentary
1.2.1	The Network edge NGFW was configured in an attempt to identify the signature of known malware being sent.	2.2.1.1	The micro-segmentation of the network did not allow access to the entire network.
1.2.1.1.1	The micro-segmentation of the network did not allow access to the entire network.	2.2.1.2	The NGFW no longer allowed lateral movement as the user lacked access to other micro-segments of the network.
1.2.1.1.2	The NGFW no longer allowed lateral movement as the user lacked access to the other segment of the network (Figure 7).	2.3	It was still possible to connect directly to the camera and install a malware.
2.1	It was still possible to connect a personal computer to the network, but it was left without access to perform the lateral movement and to sniff to the network.	VI. Conclusions and Future Work	
2.1.1	The micro-segmentation of the network did not allow access to the entire network.	The advantages of using the zero trust philosophy are noticeable. Creating separate network policies for each micro-segmentation prevents unauthorized users from using network resources. However, it was possible to observe that the implementation of micro-segmentation requires a great operational complexity and there is little automation. The requirement for great human involvement is still necessary in this type of approach. The communication mapping for each specific software (layer 7 of the OSI model) is complex as it requires that the information security professional know different software and how they communicate between them. If the micro-segmentation work is not done well, communication may become inaccessible at	
2.1.2	The NGFW no longer allowed lateral movement as the user lacked access to other micro-segments of the network.		
2.2	It was still possible to hack into a user's computer, but it was not possible to perform lateral movement or sniff to the network.		

```

Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection: (default port)

Connection-specific DNS Suffix...:
Link-local IPv6 Address...: FE80::2D0:FFFF:FE85:A6ED
IPv6 Address...: ::
IPv4 Address...: 192.168.1.2
Subnet Mask...: 255.255.0.0
Default Gateway...: 192.168.0.1

Bluetooth Connection:

Connection-specific DNS Suffix...:
Link-local IPv6 Address...: ::
IPv6 Address...: ::
IPv4 Address...: 0.0.0.0
Subnet Mask...: 0.0.0.0
Default Gateway...: 0.0.0.0

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Figure 7: Lateral movement made impossible by network restrictions

some point in the network and depend on human action to correct possible problems.

For future work, a database is being provided with several logs containing different types of attacks that we can consider as APT. An artificial intelligence system will be important and useful in analyzing these attack patterns. Another work to be developed is to apply zero trust practices in other networks such as SDN, ad-hoc and even in IoT sensor networks.

#### Acknowledgement

This work was supported in part by CNPq - Brazilian National Research Council (Grants 312180/2019-5 PQ-2 and 465741/2014-2 INCT on Cybersecurity), in part by the Brazilian Ministry of the Economy (Grant DIPLA 005/2016 and Grant ENAP 083/2016), in part by the Administrative Council for Economic Defense (Grant CADE 08700.000047/2019-14), in part by the General Attorney of the Union (Grant AGU 697.935/2019), in part by the National Auditing Department of the Brazilian Health System SUS (Grant DENASUS 23106.118410/2020-85), and in part by the General Attorney's Office for the National Treasure (Grant PGFN 23106.148934/2019-67).

#### References

- [1] I. Ghafir, M. Hammoudehc, V. Prenosilb, LiangxiuHanc, R. Hegartyc, K. Rabiec, and F. J. Aparicio-Navarro, "Detection of advanced persistent threat using machine-learning correlation analysis," *Future Generation Computer Systems*, 2018.
- [2] J. Kurose and K. Ross, *Redes de Computadores e a Internet: Uma Abordagem Top-Down*, W. L. Zucchi, Ed. Pearson Universidades, 2015.

- [3] Q. Zhang, H. Li, and J. Hu, "A study on security framework against advanced persistent threat," *7th IEEE International Conference on Electronics Information and Emergency Communication*, 2018.
- [4] I. Ghafir and V. Prenosil, "Advanced persistent threat attack detection: An overview," *International Journal of Advancements in Computer Networks and Its Security- IJCNS*, 2014.
- [5] L.-X. Yang, K. Huang, X. Yang, Y. Zhang, Y. Xiang, and Y. Y. Tang, "Defense against advanced persistent threat through data backup and recovery," *IEEE Transactions on Network Science and Engineering*, 2020.
- [6] D. Kumar, K. Shen, B. Case, D. Garg, G. Alperovich, D. Kuznetsov, R. Gupta, and Z. Durumeric, "All things considered: an analysis of iot devices on home networks," *28th USENIX Security Symposium*, 2019.
- [7] H. K. Kalita and A. Kar, "Wireless sensor network security analysis," *International journal of computer science & information Technology (IJCSIT)*, 2009.
- [8] B. Schneier, "Attack trees," *Dr. Dobb's Journal of Software Tools*, 1999.
- [9] NIST, "Zero trust architecture," URL: <https://doi.org/10.6028/NIST.SP800-207> . Accessed on August 20, 2021.
- [10] GARTNER, "Next-generation firewalls (ngfw)," URL: <https://www.gartner.com/en/information-technology/glossary/next-generation-firewalls-ngfw> . Accessed on August 25, 2021.
- [11] K. Park, B. Ahn, J. Kim, D. Won, Y. Noh, J. Choi, and T. Kim, "An advanced persistent threat (apt)-style cyberattack testbed for distributed energy resources (der)," *IEEE Design Methodologies Conference (DMC)*, 2021.
- [12] MITRE, "Mitre att&ck," URL: <https://attack.mitre.org> . Accessed on August 25, 2021.
- [13] J. Chacon, S. McKeown, and R. Macfarlane, "Towards identifying human actions, intent, and severity of apt attacks applying deception techniques - an experiment," *International Conference on Cyber Security and Protection of Digital*, 2020.
- [14] Z. Xiaojian, C. Liandong, F. Jie, W. Xiangqun, and W. Qi, "Power iot security protection architecture based on zero trust framework," *IEEE 5th International Conference on Cryptography, Security and Privacy*, 2021.
- [15] B. C. Rocha, L. P. Melo, and R. T. de Sousa Jr., "A study on apt in iot networks," *18th Internacional Conference on E-Business (ICE-B)*, 2021.
- [16] C. Kong, J. Liu, M. Xian, and H. Wang, "A small lan zero trust network model based on elastic stack," *5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE)*, 2020.
- [17] CISCO, "Cisco packet tracer," URL: <https://www.netacad.com/courses/packet-tracer> . Accessed on August 20, 2021.
- [18] AMENAZA, "Securitree," URL: <https://www.amenaza.com/> . Accessed on September 7, 2021.
- [19] H.-M. Sun, C.-E. Shen, and C.-Y. Weng, "A flexible framework for malicious open xml document detection based on apt attacks," *IEEE INFOCOM Poster*, 2019.