Intelligent Detection and Recovery from Cyberattacks for Small and Medium-Sized Enterprises

Miguel Ángel López, Juan Manuel Lombardo*, Mabel López, Carmen María Alba, Susana Velasco, Manuel Alonso Braojos, Marta Fuentes-García

Fundación I+D del Software Libre (FIDESOL), Granada (Spain)

Received 16 May 2020 | Accepted 29 July 2020 | Published 7 August 2020

unir
LA UNIVERSIDAD
EN INTERNET

Abstract

Cyberattacks threaten continuously computer security in companies. These attacks evolve everyday, being more and more sophisticated and robust. In addition, they take advantage of security breaches in organizations and companies, both public and private. Small and Medium-sized Enterprises (SME), due to their structure and economic characteristics, are particularly damaged when a cyberattack takes place. Although organizations and companies put lots of efforts in implementing security solutions, they are not always effective. This is specially relevant for SMEs, which do not have enough economic resources to introduce such solutions. Thus, there is a need of providing SMEs with affordable, intelligent security systems with the ability of detecting and recovering from the most detrimental attacks. In this paper, we propose an intelligent cybersecurity platform, which has been designed with the objective of helping SMEs to make their systems and network more secure. The aim of this platform is to provide a solution optimizing detection and recovery from attacks. To do this, we propose the application of proactive security techniques in combination with both Machine Learning (ML) and blockchain. Our proposal is enclosed in the IASEC project, which allows providing security in each of the phases of an attack. Like this, we help SMEs in prevention, avoiding systems and network from being attacked; detection, identifying when there is something potentially harmful for the systems; containment, trying to stop the effects of an attack; and response, helping to recover the systems to a normal state.

Keywords

Attack Detection, Attack Recovery, Blockchain, Cybersecurity, Machine Learning, SME.

DOI: 10.9781/ijimai.2020.08.003

I. Introduction

Cybercrime is being increased to alarming levels nowadays, thus being already included in the national security and defense agenda. These crimes are a global epidemic that affect every computer system in the world [1]. The cybercriminal profile is not related to the expert and enthusiastic hacker that aims breaking security to test systems anymore [2]. Technically advanced countries and nations are now more involved in security incidents with different impact (due to either political or economical reasons) [3]. At the same time, criminal organizations tend to change their activity area in order to make their criminal practices more sophisticated. Cybercrime has become more professional, smart and stealthy [4]. This has lead to a change in the attacks, which are even more frequent in the last years.

Attacks aimed at exploiting vulnerabilities existing in information systems from critical infrastructures have been increased [5], [6], as well as from strategic areas such as energy or water supply, health, transports or finances [3]. In addition, Small and Medium-sized Enterprises (SMEs), due to their weakness and relevance in the activities and economy of a country, are also relevant targets. SMEs attacks aims to disturb or interrupt their basic structures, having a huge impact both in the entity [7] and the continuity of its services [8] that, sometimes, are essential. These attacks are well studied actions that imply a significant benefit with low risk for the criminals, due to its international nature, adaptability, mobility, and opacity [9].

Some of the most common attacks in 2018 were phishing, social engineering and data hijacking [10]. These attacks were performed achieving a 78% of effectiveness. Due to its fast propagation and effects in computer systems, which has even a more impact in SMEs, ransomware is one of the most important data hijacking attacks [11], [12]. This malicious software is really harmful [13], since it is diversified and it attempts to hide its actions and to maximize the benefits using advanced techniques [14]. When ransomware are activated, it is needed to switch off the systems and to activate all the security protocols for severe risks. The worst ransomware attack until the date was *WannaCry*, which took place in 2017. This attack affected many organizations and companies in 150 countries, having about 200,000 hosts affected [15]. The *Ryuk* attack, which was planned in a better way than *WannaCry*, took place more recently. *Ryuk* was designed to block as much number of systems as possible in a corporate environment [16]. On the other hand, the Covid-19 crisis has made the cybercriminals to be focused in health systems [17] and laboratories in order to worsen the consequences of the attacks [18].

Another dangerous example of stealing data is a bank Trojan that pursues the misappropriation of electronic bank accounts by means of collecting user credentials [19]. This attack has become more sophisticated since it appeared by 2004 for the first time. Checking the authenticity of a web page is not enough anymore: this malware fetches

* Corresponding author.
E-mail address: jmlombardo@fidesol.org

the introduced data, as well as the screen or data in the web page that is visited, making measures like virtual keyboards to be inefficient [20]. Distribution mechanisms in financial malware are better and better, which has serious effects in those entities that show a low defense against this type of attacks [21]. Financial malware increased 58% in 2019 in relation to the previous year, having more presence among threats, which is alarming [22].

Different malware families, such as ransomware, bank Trojans, and other attacks aiming to steal information, use the Domain Generation Algorithm (DGA) to generate many malicious domain names pseudo-randomly [23]. These domains can be used to compromise hosts, which makes it more difficult for the investigators to find the origin of the attack. Another attack that allows data stealing is SQL injection (SQLi), which introduces malicious code in a database by means of a web application, taking advantage of existing vulnerabilities in such database. Like this, the attacker can, for example, steal credentials for phishing the administrator identity and access, modify or delete information in the compromised database [24], even making it to be inaccessible. SQLi had high relevance during 2018 y 2019, being related to more than 72 % of attacks vectors to the web. From such vectors, 36% affected financial services directly [25]. Deny of Service (DoS) is also a dangerous attack against the availability of systems, which makes their legitimate users not being able to use compromised systems [26]. Distributed DoS (DDoS) evolved from the original DoS attack, having similar effects but applying different strategies. In a DDoS attack, the attacker usually builds an army (computers network, which is normally named botnet) by means of infecting hosts with malware (called zombies or bots). Bots can address the attack against a specific server, which ends suffering a heavy network traffic due to the overload [27]. The most advanced versions of DDoS are performed using Internet of Things (IoT) devices. This is the case of *Mirai*, *Brickerbot* or *Hajime* [28], which carry out DDoS attacks against low cost IoT devices that do not implement security measures. Like this, it is easier to control the infected devices, transforming them in an army that serves the hackers.

A. Mechanisms of Detection and Defense Against Attacks: the SME Problem

Both infrastructure and reputation turn damaged as a consequence of the aforementioned attacks. These damages can be even more severe for SMEs, having negative effects such as: reducing sells, losing clients [29], investors and number of employees, decreasing incomes, or even closing the company [30]. The number of cyberattacks increases everyday, which makes no organization to be free from suffering damages due to cybercrime. Furthermore, suffering a cyberattack in essential services provided by SMEs can produce a highly negative impact, yielding catastrophic effects if this happens in systems involved in critical infrastructures [31].

Although organizations invest in security mechanisms, most of these mechanisms are not effective due to attacks are more and more complex and evolve daily [32]. There is no doubt about sophistication and adaptability of cybercriminals to both environment and circumstances, since they study the most weak systems that are potential targets for the attacks [33]. This evolution is so fast that security teams can not predict the moment and target of an attack. Thus, it is essential to have a proactive security system allowing to detect threats and attacks timely in order to minimize damages. Companies are aware of this evolution and, for this reason, they invest in advanced security systems, such as Intrusion Detection Systems (IDSs), Security Information Event Management (SIEM) systems, Security Operations Centers (SOCs) or Managed Security Service Providers (MSSPs). These tools, by means of artificial intelligence, provide advanced threat and attack detection techniques and allow the automation of security processes [34]. Furthermore, companies create response plans according to systems and profiles in order to determine guidelines that need to be applied when a security incident is detected [35]. Yet, companies usually have a reduced economic capability to implement the aforementioned systems. Indeed, about 87% of companies do not have resources enough to acquire security systems [36]. This is the case of SMEs, which usually do not introduce the protection mechanisms needed. This makes them to be the main target for cybercriminals [37]. Furthermore, protecting new gadgets that are essential for working, such as smartphones or IoT devices is even more complicated [38]. For all these reasons, it is needed to develop a system with advanced features (similar to IDSs or SIEM systems), providing security against the most relevant attacks and being affordable for SMEs. This system should allow any organization to decrease both economic and social impact of suffering a cyberattack.

This paper shows the work carried out as a part of the IASEC project, which aims creating a researchers unit (*Unity of Innovation*) composed by workers both from Vector SF and Fidesol. The goal of IASEC is to perform research and development activities to build and optimize algorithms and tools, allowing to reach solutions that improve cybersecurity both in companies and other institutions. Initially, this project is being developed in a restricted environment for, later, being transferred to Andalusian SMEs for its evaluation under real conditions. The main objectives of IASEC are: *i)* providing resources to optimize detection and self-recovery of systems and services after suffering an attack, *ii)* creating a solution to allow detecting and dealing fake publications on the Internet, *iii)* protecting IoT devices and Industry 4.0 from the most relevant attacks for SMEs, and *iv)* detecting and avoiding fake news and hoaxes spreading. These objectives are tackled by combining both smart systems and blockchain. Like that, blockchain help us to improve the security systems by protecting data integrity in a secure and transparent way. Thus, the *Unity of Innovation* aims to be a reference point in relation to cybersecurity technology transference to Andalusian SMEs and institutions. In this work, we introduce an architecture for smart detection of the most important attacks for SMEs, addressing the first of the objectives in the IASEC project.

The rest of the paper is organized as follows. In Section II we review the literature related to cybersecurity incidents in SMEs. In addition, we explain some of the algorithms for detecting the most affecting attacks for such companies. In Section III, we introduce our proposal in the IASEC framework for solving the detection and recovery problems against the previously identified attacks. The platform developed for detecting these attacks, as well as the corresponding architecture, are also described in this section. Finally, in Section IV we present the main conclusions derived from this work.

II. Related Work

A. Cybersecurity Solutions for SMEs

Companies utilize different security tools with the aim of detecting and, sometimes, responding to security incidents. SIEM systems are one of the most extended tools. SIEM systems allow compliance of security regulations and managing events. These systems also allow event correlation as well as perform analysis of records and events from different data sources [39]. However, including a SIEM solution is really expensive and complex for SMEs [40]. IDSs are another security tool widely used. IDSs can be network-based (NIDS) and host-based (HIDS) [41]. NIDS monitor and analyze network traffic in real time, while HIDS analyze records, databases and other elements in a host to detect possible intrusions. Recently, researchers are focused in IDS development to achieve effective solutions against intrusions and attacks [42]. IDSs can also be grouped according to the type of detection technique. Thus, they can be signature-based [43] and model-based [44].

Different factors can be considered to choose a cybersecurity solution for an SME. For example, one can select indicators for the implementation of IDSs. Authors in [45] compare the main existing IDSs (*e.g. OSSEC*[1], *Snort*[2] or *Suricata*[3]), and then they normalize the obtained data, assigning quantitative values to each indicator (*e.g.* license type, type of IDS, operating system, and interface). Weighting values are fixed by each SME according to its needs. The results of this study show that the most accurate IDS for SMEs is Suricata [45]. Furthermore, authors in [46] analyze different solutions for protecting sensitive information in SMEs. As a result, they obtain a ten tools comparative, where IDSs are highlighted. Authors in [47] propose using model-based IDSs for SMEs. They use Machine Learning (ML) techniques for data collecting, testing and evaluation the proposal. Their main goal is to determine which is the most efficient algorithm for intrusion detection. To do this, they compare the following algorithms for supervised detection: C4.5 (Decision Tree), Bayesian Network, Random Forest, Support Vector Machines (SVM), and Artificial Neural Network (ANN). The study is performed by taking measures from different sampling data. Results show that C4.5 is the most precise among the studied algorithms [47].

Finally, another proposal is to build a solution focused in cybersecurity for Smart-Home or Smart-Office [48]. This work deals two research topics: data collecting from commercial or industrial IoT networks, and datasets exploitation for intrusion detection applying ML methods. For the last one, authors apply two variants of Long Short-Term Memory (LSTM), which is a type of neural network [48].

B. Detection and Response Algorithms for the Main SMEs Attacks

As we explained before, DoS (and DDoS), malware, or web-based attacks are some of the most extended security incidents [24]-[27]. Below we review some detection techniques for DDoS, SQLi and DGA, due to its impact for SMEs [26].

1. DDoS

Authors in [49] propose detecting DDoS attacks using Random Forests. The algorithm is validated using the *KDD´99 cup* dataset [50], which is labeled indicating whether exists an attack or not. The results of the study show that precision for attack detection is 94%, while 100% is reached for those that are attack-free [49]. Similarly, and using the same dataset, authors in [51] introduce a script to optimize the learning process. They start by selecting those features in the dataset that are more accurate for model building, thus reducing the training time. Then, they implement a Random Forest (motivated by results from a previous comparison) reaching 99,92% precision.

There exist solutions for recovery once a DDoS has taken place. For example, authors in [52] show that blockchain can be used to mitigate DoS attacks. To do this, they propose to create a smart contract and a blockchain infrastructure in *Ethereum*. When a server suffers a DoS attack, the system records in the smart contract those IP addresses that are involved in the attack, creating new blocks every 14 seconds. Thus, each user in this network has an updated list with malicious addresses in the interval, allowing the security people to take actions for attacks mitigation. This solution can be extended to DDoS attacks.

2. SQLi

Authors in [53] obtain a model for SQLi attacks detection by feature extraction from web traffic. These authors use a free dataset provided by the European Conference on Machine Learning and Principles and Practice of knowledge Discovery in Databases (ECML-PKDD) [54]. Expert knowledge allows selecting those features that help to detect patterns in web traffic related to SQLi attacks. Authors analyze and compare different detection algorithms using those features that have been selected. These algorithms are: Decision Stump, Naïves Bayes, Bayesian Network and Radial Basis Function (RBF) network, which is an ANN. The most efficient algorithm is Decision Stump [53]. Authors in [55] apply Naïve Bayes to classify SQL queries in malicious and legitimate. To do this, they take into account both grammar and SQL syntax, extracting features from language and defining rules. Another work that also apply feature extraction from SQL queries is [56]. Authors in this work train several classifiers, such as SVM, Ensemble Bagged Trees or Ensemble Boosted Trees. In this case, the best results are obtained for Decision Tree.

There exist solutions for SQLi attacks prevention and for system integrity preservation. For example, it is possible developing a blockchain system to avoid attacks against database management systems [57]. Authors in this work propose restricting access from nodes to the web server and the database. Access is filtered by using the blockchain, where the IP address used for accessing is recorded. Thus, only non-malicious IP addresses can access the server. Another work propose a framework that uses smart contracts from blockchain [58]. This framework has two components: the first one stores type of users and SQL queries, while the second one stores hash chains from queries that are allowed for each user. These chains are tokenized using the cryptographic function SHA256.

3. DGA

Authors in [23] propose classifying DGAs using LSTM. This proposal can be applied under real-time conditions, it is not based in features and allows classifying in families of DGA attacks [23], [59]. This type of neural networks are efficient for problems with sequential relationships, where previous states have effect in the current one [23]. LSTM is also applied in [60] for DGA classification. In this case, authors add a neuron with memory and the ability of discarding previous values that are far in time. DGA can be detected analyzing DNS traffic in pseudo-real time [61]. This work introduces an algorithm that is implemented using Aizoon Research for Advanced Malware Identification System (ARAMIS). The proposal filters non-resolved DNS requests (*UNRES*) and identifies those hosts showing the highest peaks for this value. When *UNRES* is increased suddenly, an analysis is performed, since it can be related to non-trusted domains trying a connection.

III. Detection and Response for Attacks Against SMEs. The IASEC Proposal

The IASEC project is composed of three main milestones. The first of them aims studying main threats for a company, as well as the stages of an attack from the point of view of defending the company. The goal is developing methods and tools for detection and self-recovery of systems and services after a cyberattack takes place. The second milestone aims tackling user identity management in the Internet by means of blockchain for digital identity certification. Finally, the last one aims obtaining the knowledge needed for detecting and managing fake information publication in the Internet. This should be performed by combining both ML and blockchain.

A. Steps for Defending an Attack

As explained during the Introduction, this paper is focused in detection and self-recovery of systems after an SME has suffered an attack. As a part of this first milestone, we have proposed a security platform for detection and self-recovery against cyberattacks. During the first stage of the project, we have designed and implemented the general architecture for the platform, as well as the detection (but not

[1] https://www.ossec.net/

[2] https://www.snort.org/

[3] https://suricata-ids.org/

the recovery) micro-services. Prior to this design and development, we have studied the steps for defending an attack, which are described in the next paragraphs from the perspective of the IASEC project.

1. Prevention

The goal of prevention is to avoid systems from being attacked and/or compromised, *i.e.* adopting required measures to make it more difficult carrying out a successful attack [62]. Prevention is essential, given that no company wants to deal with information stealing or denial of its services. These situations could involve serious economic consequences, as well as losing the reputation of the company [63]. Taking into account the relevance of preventing an attack, from IASEC we recommend that the implemented security system should include: access control, self-backup for critical files, self-update for security features, and black / white access lists. In addition, we believe that it is needed to install firewalls and anti-malware solutions to complement the aforementioned measures.

2. Detection

The goal of detection is to identify irregularities in systems [64]. This step is related to systems such as IDSs or SIEMs, which sometimes use ML to detect intrusions. In IASEC, we have studied some ML algorithms to detect the most affecting attacks for SMEs [23], [49], [51], [53], [55], [56], [60]. Then, we have selected the most accurate for each of the attacks, implementing an individual micro-service to detect each of them. These micro-services and the architecture proposed to implement our security platform are explained later in this section.

3. Containment

The goal of containment is to minimize the impact of having a cybersecurity incident in a company, avoiding its propagation and gaining time to build a recovery strategy [65]. Related actions can be disabling those accounts that have been compromised or isolating those hosts that have been infected [66], as well as making backups from hard-disks [67]. Another possibility is implementing fake systems that are similar to the real ones. These systems are used as traps, showing vulnerabilities that catch the attention from attackers, which makes the fake system to be attacked instead of the real one. Examples of this technique are honeypots or sandboxes [68]. From IASEC, we propose creating a virtual environment that should be designed to cheat the cybercriminals, emulating that it is possible to perform privilege escalation and steal user credentials. This solution is based in Deception Technology [69].

4. Recovery

The goal of recovery is to restore systems to a normal state after a security incident has taken place. To do this, it is needed to perform some actions after removing the threat [62]. Recovery, similarly to detection, is one of the most important stages in defense. Like this, recovery allows performing a fast restoration to the normal state of the organization, thus minimizing costs. From IASEC, we propose two solutions: *i)* creating a Security Incident Response Plan (SIRP) [35], and *ii)* implementing self-recovery measures. The former should include countermeasures in case of detecting any security breach. The latter is based in creating lists of malicious and legitimate IP addresses [52], [56]. Thus, we propose designing and developing a recovery system after attacks. This system should include a list containing malicious IP addresses that belong to the attacks previously detected using the micro-services. These IP addresses should be recorded in a blockchain network. Like this, it is possible to obtain a database updated with the malicious addresses for the server, allowing a faster recovery of the systems.

B. Architecture of the Platform

The proposed security platform is designed to be a system with an architecture organized in micro-services, which are deployed individually in dockers. Micro-services can communicate with the user using an API, as well as with other micro-services. The platform is implemented using different programming languages, depending on the needs, with higher priority for Python versus Java or .Net.

Fig. 1 shows the scheme for the architecture, the components and their relationships in the micro-services platform. This platform is composed of a front-end and a back-end. The front-end, which is represented in green color in the left part of Fig. 1, corresponds to a client application that allows users interacting with the security micro-services. The back-end is composed of micro-services and a relational database. Users can provide data, and those data that are generated by the platform are stored using a static storage. A non-relational database is also available for the algorithms, to support the big data processing. User-platform interaction is performed by the exposition of an *API REST*, a hub and a request balancer based in *Netflix OSS* (API Gateway, Service Mesh)[4]. Micro-services are run in a docker ecosystem (represented in the bottom of Fig. 1), which ensures running independence, high availability and scalability. Docker container receive load balancing, routing, and orchestration (docker swarm). The CORE module, which is represented in the right bottom corner in Fig. 1, includes multi-language services to provide the following functionalities: database connection, notification (*e.g.* e-mail), security, log recording, generation of files, managing the generated files or those that have been sent to the platform, and other transversal utilities to cybersecurity services.

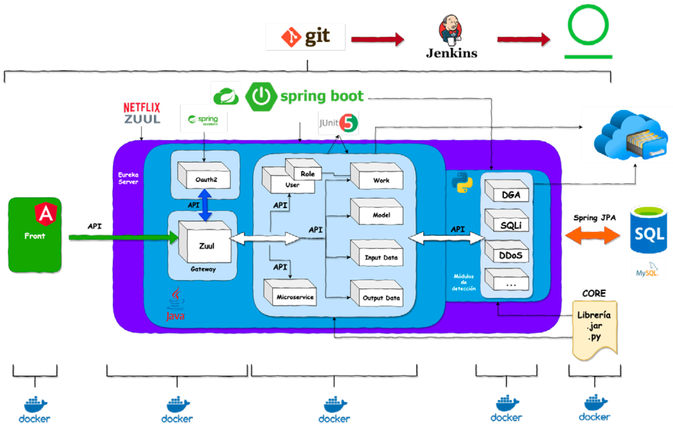


Fig. 1. Architecture for the IASEC micro-service platform.

Like this, our platform can be divided into two main parts:

1. **Part I**. This part manages user-related aspects of the platform: the database is created containing the tables that are needed for managing, like those related to users, micro-services and jobs (service requests). It is in charge of providing services to the user such as cybersecurity, data loading and downloading, authentication or job visualization, among others. Management is divided in *i)* web client (front-end), *ii)* back-end, and *iii)* load balancing (*Netflix* tools). The former ensures an agile interaction between user and platform. The second is composed by the management micro-services. Finally, the latter routes and balances algorithm requests for training and prediction, activating one instance of the docker where the requested algorithm is included.
2. **Part II**. This part involves the algorithms and the CORE module. The algorithms are run in instances of the docker, which will be stopped after each running due to the first phase of the project does

[4] https://netflix.github.io/

not allow real-time monitoring yet. Thus, intermediate information that is generated by the algorithm (*e.g.* support tables) is only available during the living time of the instance. In this first stage, micro-services allow loading a labeled dataset for the evaluation of the detection algorithms. The micro-service returns quantitative information related to the obtained prediction about detection. The micro-service output is saved into the static storage system.

C. Micro-services for Detection of Known Attacks

Attack detection micro-services are implemented using the python Micro-Framework, *Flask*[5]. Micro-services are scalable, and it is possible to connect them to a database or any other component. Each of them trains a model according to some features that has been previously defined and using a supervised ML algorithm. We have implemented an individual micro-service for each selected attack (recall DDoS, SQLi and DGA) under the hypothesis that it is more efficient to perform an independent detection (in terms of precision) than having a single algorithm to detect all the attacks. It is possible adding other modules in the future, like the self-recovery component.

Micro-services can access the storage system of the platform, where they can obtain files that have been uploaded by the user and write output files or saving models. Thus, micro-services input is the path for those files that are needed to process data, while output corresponds to a state indicating the result of the process (successful or not) and paths for the generated files. The attack detection micro-services need to perform the training using the input data. Training is composed of different steps: *1)* data pre-processing, *2)* model building (using the selected algorithm), and *3)* saving the model in a *pkl*[6] file, which is stored in the static storage system. Then, the generated model is used to carry out the prediction. This model is applied to new monitored data to detect whether there exist an attack or not. Please, recall that in this first stage of the project it is not possible to perform real-time monitoring, instead a labeled dataset can be loaded and the micro-service returns the detection rate and other relevant information about the dataset for positive detection. This output is also saved in the static storage system.

1. DDoS Detection

We have studied two different algorithms to implement the DDoS detection micro-service: Random Forest [49] and Decision Trees [51]. We have selected Decision Trees [49], since this algorithm obtain better results using the same dataset (*KDD´99 cup* [50]). For our testing, we have also used the *KDD´99 cup*, although it is possible to use any other dataset containing labels related to TCP connection, domain, and network traffic features [49].

2. SQLi Detection

We have selected Decision Stump [53] to develop the SQLi detection micro-service, since it obtain the best results among the studied algorithms (Naïve Bayes [55] and Decision Trees [56]). In this first stage, we have used the same dataset as in Reference [53] for our testing. Like for the DDoS micro-service, it is possible using any other dataset containing those features that are needed for model building.

3. DGA Detection

We have studied different proposals to implement DGA detection [23],[59]-[61]. We think that the best alternative is not only detecting DGA attacks, but also performing the classification among different families of DGA [23],[59]. Thus, we have decided implementing an LSTM neural network like in Reference [23], given its high precision both detecting DGA domains and classifying them. Our testing has been carried out using the domains database from Alexa[7] and a database that has been created in the IASEC framework, where the latest malicious domains detected by OSINT [59] are collected. Thus, we have trained the algorithm with two datasets: one containing legitimate domains and another with malicious domains. However, our micro-service accepts any dataset containing urls from domains.

D. Self-recovery

At the beginning of the section, we described the first milestone of the IASEC project, where one of the main goals is recovery for SMEs after suffering an attack. More precisely, one of these goals is self-recovery to protect the system integrity. Automation is usually related to design a tool being able of efficient self-recovery of the services in the compromised system. From IASEC, we propose implementing a module composed of micro-services being able to act in recovery tasks. Below we describe the proposed mechanisms for recovery after suffering any of the attacks that can be detected in our platform.

1. DDoS Recovery

We consider different mechanisms for resilience and recovery after suffering a DDoS attack. First, we propose creating a micro-service for recovery that uses blockchain to record IP addresses related to the attacks. The micro-service should discard those network packets containing malicious IP addresses by means of network traffic analysis, similar to the proposal in Reference [57]. This mechanisms can be improved creating black-lists and white-lists, also using blockchain [52]. Like this, the micro-service should prevent and recover services after the attack takes place. Additionally, if the server is being overloaded, we propose redirecting network traffic to alternative or backup servers if the origin IP addresses are not in the black-list. Thus, if the main server is suffering an attack but the IP addresses have not been identified as malicious, the server will maintain its services available.

2. SQLi Recovery

A possible solution to deal with an SQLi attack is locating those IP addresses that are injecting code and block them. To achieve this goal, we propose developing a micro-service for recovery. This micro-service should filter users requesting services taking into account their IP addresses. Queries that have been previously identified as malicious should be also denied. These IP addresses could be recorded using a smart contract in a blockchain. Like this, if a user is trying to access the system, a request should be performed to the blockchain network to allow or deny the access depending on the IP address in the origin [57]. Furthermore, this micro-service proposes a recovery mechanism for those tables that have been affected. This mechanism should check the writing history and restore to the last version before suffering the attack [70]. Like this, we propose a micro-service to avoid damages and allow recovering from an SQLi attack if finally it has been successful.

3. DGA Recovery

To deal with DGA attacks, we propose creating a black-list including those domains that have been identified as malicious using the detection micro-service. This black-list should be used to update the detection system. In the same way as for the rest of the attacks, the proposal is to develop a micro-service that should record the malicious domains in a blockchain network to provide integrity to the system. Additionally, the micro-service should be able of creating backups from critical files before the attack is completed. Like this, after suffering attacks such as ransomware (which is related to DGA), the micro-service should be able of recovering the system to a normal state, ensuring that no relevant information is damaged or corrupted.

Furthermore, we propose alerting the person in charge of security

[5] https://palletsprojects.com/p/flask/

[6] https://docs.python.org/3/library/pickle.html

[7] https://www.alexa.com/topsites

about each detected attack and the actions that have been carried out. Like this, he or she will be aware of the incident and will take needed actions. Finally, SME employees should be trained to avoid social engineering attacks and data hijacking, and should be also informed about the SIRP.

IV. Conclusion

In this work, the main cybersecurity problems for companies are analyzed, paying special attention to SMEs. In this sense, main available solutions to protect their infrastructures and systems are also studied. One of the main conclusions derived from this work is that, sometimes, early detection is even more important than prevention. Thus, detecting an attack in an early manner, allows the security team troubleshooting the incident properly.

The main cybersecurity problem affecting SMEs is that they do not have resources enough to set up efficient security systems, such as SIEMs. In this paper, we have proposed a solution considering each of the attack steps from the point of view of the protection of the company (prevention, detection, containment, and recovery). Our solution aims improving SME security, reducing both economical and social problems derived from suffering an attack. The proposal is part of the IASEC project. More precisely, we implement a security platform that provides different micro-services to detect DDoS, SQLi and DGA attacks. The proposed architecture is scalable, allowing to add new micro-services according to the needs of the SME. These micro-services can be both for detection and recovery. The results have been satisfactory for the first release of the platform, yielding a good basis for the next stages where it is expected that the attacks can be detected in real time.

As a future work, we propose developing a second release that provides micro-services for automatic recovery after suffering an attack. These micro-services will be blockchain-based in order to enhance the integrity of the system. In addition, new experiments will be performed using real network traffic, allowing to validate our current models with data from an SME. Finally, the IASEC project will continue, working in the certification of digital identities using blockchain and providing solutions to deal with fake information in the Internet.

Acknowledgment

The IASEC project has been funded by the IDEA Agency (Junta de Andalucía). Project code: 402C1800002.

References

[1] Kapersky, "Cyberthreat real-time map.Statistics", 2020. [Online]. Available: https://cybermap.kaspersky.com/stats/

[2] J. Salom, "El ciberespacio y el crimen organizado", Cuadernos de estrategia, no. 149, pp. 129-164, 2011.

[3] CCN-CERT, "Ciberamenazas y tendencias 2019", 2020. [Online]. Available:https://cutt.ly/JyxichC

[4] D. S. Wall, "Dis-organised Crime: Towards a distributed modelo of the organization of cybercrime", The European Review of Organised Crime, vol. 2, no. 2, pp. 71-90, 2015.

[5] L. Joyanes, "Introducción. Estado del arte de la ciberseguridad", Cuadernos de estrategia, no. 149, pp. 11-46, 2011.

[6] Council of the European Union, Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. 2008.

[7] M. S. Gordon, "Economic and National Security Effects of Cyber Attacks Against Small Business Communities", ProQuest Dissertations Publishing, 2018.

[8] S. Kamiya, J.-K. Kang, K. Jungmin, A. Milidonis and R. M. Stulz,"What is the impact of successful cyberattacks on target firms?", *NBER,* no. 24409, 2018. DOI:10.3386/w24409.

[9] Departamento de Seguridad nacional. Presidencia del gobierno, "Estrategia de seguridad nacional", 2013. [Online]. Available: https://cutt.ly/iyxinvl

[10] C. M. Arce, "Ciberseguridad y crímenes informáticos: el lado oscuro de la red", Revista Académica Arjé, vol. 2, no. 2, pp. 14-19, 2019.

[11] N. K. Popli and A. Girdhar, "Behavioural Analysis of Recent Ransomwares and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware", Computational Intelligence: Theories, Applications and Future Directions - Volume II. Advances in Intelligent Systems and Computing, vol 799, pp. 65–80, 2019. DOI:10.1007/978-981-13-1135-2_6.

[12] S. Bhattacharya and C. R. S. Kumar, "Ransomware: The CryptoVirus subverting cloud security", in 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017, pp. 1-6.

[13] N. Scaife, H. Carter, P. Traynor and K. R. Butler, "Cryptolock (and drop it): stopping ransomware attacks on user data", in IEEE 36th international conference on distributed computing systems (ICDCS), 2016, pp. 303–312.

[14] M. Antonakakis, R. Perdisci, Y. Nadji, N. Vasiloglou, S. Abu-Nimeh, W. Lee and D. Dagon, "From Throw-Away Traffic to Bots: Detecting the Rise of DGA-Based Malware", in 21st USENIX Security Symposium, 2012, pp. 491-506.

[15] A. O'Dowd, "Major global cyber-attack hits NHS and delays treatment", BMJ, 2017. DOI:10.1136/bmj.j2357.

[16] J. Hernandez-Castro, A. Cartwright and E. Cartwright, "An economic analysis of ransomware and its welfare consequences", Royal Society Open Science, vol 7, 2020. DOI:10.1098/rsos.190023.

[17] M. V. Fontanilla, "Cybercrime pandemic", Eubios Journal of Asian and International Bioethics, vol. 30, no. 4, pp. 161-165, 2020.

[18] Dr. Rajib Subba, "Collective intelligence and international coordination: antidote for the novel biological zero-day exploit #COVID-19", Security Nexus Perspectives, 2020. [Online]. Available: https://apcss.org/wp-content/uploads/2020/04/Security-nexus-subba.pdf

[19] D. Kiwia, A. Dehghantanha, K.-K. R.Choo and J. Slaughter, "A cyber kill chain based taxonomy of banking Trojans for evolutionary computational intelligence", Journal of Computational Science, vol. 27, pp.394–409, 2018.

[20] P. Peris-Lopez and H. Martín, "Hardware Trojans against virtual keyboards on e-banking platforms – A proof of concept", AEU - International Journal of Electronics and Communications, vol. 76, pp.146–151,2 017.

[21] N. Tariq, "Impact of cyber-attacks on financial Institutions", Journal of Internet Banking and Commerce, vol. 23, no. 2, pp 1-11, 2018.

[22] V. Chebyshev, F. Sinitsyn, D. Parinov, B. Larin, O. Kupreev, E. Lopatin, "IT threat evolution Q1 2019. Statistics",2014. [Online]. Available: https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

[23] J. Woodbridge, H. S. Anderson, A. Ahuja and D. Grant, "Predicting Domain Generation Algorithms with Long Short-Term Memory Networks", Applied Sciences, vol.9 no. 20, 2019. DOI:10.3390/app9204205.

[24] W. G. J. Halfond, J. Viegas and A. Orso, "A Classification of SQL Injection Attacks and Countermeasures", in Symposium on Secure Software Engineering (ISSSE 2006), 2006.

[25] Akamai Research, "Financial Services - Hostile Takeover Attempts", State of the internet security, vol 6, no. 1, 2020.

[26] M. Jensen, N. Gruschka and N. Luttenberger, "The Impact of Flooding Attacks on Network-based Services" in Third International Conference on Availability, Reliability and Security, Barcelona, 2008, pp. 509-513.

[27] B. B. Gupta and O. P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment", Neural Computing and Applications, vol. 28, no.12, pp. 3655–3682, 2016.

[28] McAfee Labs, "Mirai, BrickerBot, Hajime Attack a Common IoT Weakness | McAfee Blogs," 2017. [Online]. Available: https://cutt.ly/UyxiQ9F [Accessed: Apr 17, 2020].

[29] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis and R. M. Stulz, "Risk management, firm reputation, and the impact of successful cyberattacks on target firms". Journal of Financial Economics, 2020. DOI:10.1016/j.jfineco.2019.05.019 2020.

[30] M.S. Gordon, "Economic and National Security Effects of Cyber Attacks Against Small Business Communities", ProQuest Dissertations Publishing, 2018. [Online]. Available: https://cutt.ly/WyxiRFu

[31] B. Genge, I. Kiss, and P. Haller, "A system dynamics approach for

assessing the impact of cyber attacks on critical infrastructures", International Journal of Critical Infrastructure Protection, vol 10, pp. 3–17. 2015. DOI:10.1016/j.ijcip.2015.04.001.

[32] M. A. Salitin and A. H. Zolait, "The role of User Entity Behavior Analytics to detect network attacks in real time" in 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2018, pp. 1-5.

[33] A. Saravanan and S. S. Bama, "A Review on Cyber Security and the Fifth Generation Cyberattacks," Orient. J. Comput. Sci. Technol., vol. 12, no. 2, pp. 50–56, 2019.

[34] IBM, "Inteligencia artificial para una ciberseguridad más inteligente - España", 2020. [Online]. Available: https://www.ibm.com/es-es/security/artificial-intelligence. [Accessed: May 5, 2020].

[35] INCIBE, "¿Ya tienes tu Plan de Recuperación ante Desastres?," 2019. [Online]. Available: https://www.incibe.es/protege-tu-empresa/blog/tienes-tu-plan-recuperacion-desastres. [Accessed: May 5, 2020].

[36] Centro de estudios EY, "Global Information Security Survey, 9 de cada 10 empresas no cuentan con el presupuesto necesario para protegerse contra los ciberataques," 2019. [Online]. Available:https://cutt.ly/YyxoqEY [Accessed: Apr 17, 2020].

[37] Eleven Paths, "La importancia de la ciberseguridad en las Pymes" 2019. [Online]. Available: https://empresas.blogthinkbig.com/importancia-ciberseguridad-pymes/. [Accessed: Apr 29, 2020].

[38] J. Mesa, "IoT Dispositivos IoT dentro de la empresa : escenarios de ataque y protección", Red Seguridad, no.84, pp. 18–19, 2019.

[39] Gartner, "Security Information and Event Management (SIEM)",2020. [Online]. Available: https://cutt.ly/yyxotmu [Accessed: Apr 22, 2020].

[40] Gartner, "Magic Quadrant for Security Information and Event Management," 2020. [Online]. Available: https://cutt.ly/Zyxoiy8 [Accessed: Apr 22, 2020].

[41] J. Burton, I. Dubrawsky, V. Osipov, C. T. Baumrucker and M. Sweeney, "Introduction to Intrusion Detection Systems" in Guide to secure intrusion detection systems, Elsevier, 2003, pp. 1-38. [Online]. Available: https://cutt.ly/ayxooFL [Accessed: Apr 22, 2020].

[42] A. Boukhamla and J. Coronel, "Cicids2017 dataset: Performance improvements and validation as a robust intrusion detection system testbed", International Journal of Information and Computer Security, 2018.

[43] H. Holm, "Signature based intrusion detection for zero-day attacks: (not) a closed chapter?" in 2014 47th Hawaii International Conference on System Sciences, HICSS, IEEE Computer Society, 2014, pp. 4895-4904, 2014.

[44] V. Jyothsna, "A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, no.28 , pp.26-35, 2011.

[45] N. D. Pantoja, S. A. Donado and K. M. Villalba, "Selección de indicadores para la implementación de un IDS en pymes", RISTI, no. E27, pp. 777–786, 2019.

[46] J. Waite, "Security Tools for the SMB and SME Segments", SANS Institute Information Security Reading Room, 2017.

[47] O. Elezaj, S. Y. Yayilgan, M. Abomhara, P. Yeng, and J. Ahmed, "Data-driven intrusion detection system for small and medium enterprises," in IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD, pp. 1–7, 2019.

[48] N. Vakakis, O. Nikolis, D. Ioannidis, K. Votis, and D. Tzovaras, "Cybersecurity in SMEs: The smart-home/office use case", 2019 IEEE 24th Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD, pp. 1–7, 2019.

[49] I. Moles, "Ancert: aplicación de técnicas de machine learning a la seguridad", Repositorio institucional (O2), 2018. [Online]. Available:http://hdl.handle.net/10609/88925

[50] Irvine, "KDD Cup 1999 Data," 1999. [Online]. Available:http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. [Accessed: Apr 17, 2020].

[51] J. M. Rodriguez, "Aplicación de técnicas de Machine Learning a la detección de ataques", Repositorio institucional (O2), 2018.[Online]. Available: http://hdl.handle.net/10609/81126 [Accessed: Apr 17, 2020].

[52] J. Dheeraj and S. Gurubharan, "DDoS Mitigation Using Blockchain", Int. J. Res. Eng. Sci. Manag., vol. 1, no. 10, pp. 622–626, 2018.

[53] P. Aaby, "Evaluating Web App Datasets towards Detection of SQL Injection Attacks with Machine Learning Techniques", 2016. [Online]. Available: https://cutt.ly/fyxosIm [Accessed: Apr 17, 2020].

[54] C. R. Raïssi, J. Brissaud, G. Dray, P. Poncelet, M. Roche and M. Teisseire, "Web Analyzing Traffic Challenge: Description and Results", in The 18th european conference on machine learning and The 11th european conference on principles and practice of knowledge discovery in databases, 2007, pp.47-52.

[55] A. Joshi and V. Geetha, "SQL Injection detection using machine learning" in 2014 Int. Conf. Control. Instrumentation, Commun. Comput. Technol. ICCICCT, 2014, pp. 1111-1115.

[56] M. Hasan, Z. Balbahaith and M. Tarique, "Detection of SQL Injection Attacks: A Machine Learning Approach" in 2019 Int. Conf. Electr. Comput. Technol. Appl. ICECTA, 2019, pp.1-6.

[57] M. A. Mohd Yunus, M. Zainulariff Brohan, N. M. Nawi, E. S. Mat Surin, N. Azwani Md Najib and C. W. Liang, "Review of SQL Injection : Problems and Prevention", JOIV Int. J. Informatics Vis., vol. 2, no. 3–2, p. 215, 2018.

[58] M. Tmiezh, "A Framework for securing web applications against injection attacks using Blockchain technology", 2018, [Online]. Available: http://scholar.ppu.edu/handle/123456789/935. [Accessed: Apr 17, 2020].

[59] OSINT, "Feeds from Bambenek Consulting," 2019. [Online]. Available:https://osint.bambenekconsulting.com/feeds/.[Accessed: Apr 17, 2020].

[60] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory", Neural Comput., vol. 9, no. 8, pp. 1735–1780, 1997.

[61] F. Bisio, S. Saeli, P. Lombardo, D. Bernardi, A. Perotti and D. Massa, "Real-time behavioral DGA detection through machine learning" in Proc. - Int. Carnahan Conf. Secur. Technol., 2017, pp. 1–6.

[62] Deloitte, "Pasos a seguir ante un ataque informático", 2020. [Online]. Available: https://www2.deloitte.com/es/es/pages/legal/articles/Pasos-a-seguir-ante-un-ataque-informatico.html. [Accessed: Apr 24,2020].

[63] Deloitte, "Los riesgos ocultos de un ciberataque," 2020. [Online]. Available: https://www2.deloitte.com/es/es/pages/governance-risk-and-compliance/articles/los-riesgos-ocultos-de-un-ciberataque.html. [Accessed: Apr 30,2020].

[64] Red Hat, "Manual de seguridad: Detección de intrusos," 2005. [Online]. Available: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html. [Accessed: Apr 24, 2020].

[65] P. Cichonski, "Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology", NIST Spec. Publ., vol. 800–61, p. 79, 2012.

[66] Bluegrass Group, "Containment," 2020. [Online]. Available: http://cybersecurityawareness.uk/recover/containment/. [Accessed: May 4,2020].

[67] Kaspersky, "Incident Response Guide Contents," 2017. [Online]. Available:https://cutt.ly/5yxojnV [Accessed: May 4,2020].

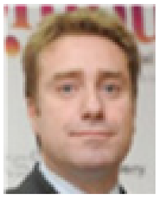
[68] Inforges, "CiberSOC: Gestión y monitorización de la seguridad informática en las empresas - Inforges", 2019. [Online]. Available: https://cutt.ly/ByxovlC[Accessed: Apr 30, 2020].

[69] Forcepoint, "What is Deception Technology? Deception Technology Defined and Explored" 2019. [Online]. Available: https://www.forcepoint.com/cyber-edu/deception-technology. [Accessed: Apr 24, 2020].

[70] K. Kurra, B. Panda, W. N. Li, and Y. Hu, "An agent based approach to perform damage assessment and recovery efficiently after a cyberattack to ensure E-government database security" in Proc. Annu. 2015 48th Hawaii Int. Conf. Syst. Sci., pp. 2272–2279, 2015.

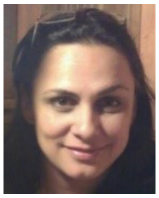
Miguel Ángel López

Has a degree in Engineering in Technical Engineering in Computer Systems from the University of Almería, graduates in Computer Engineering and Master in Softcomputing and Intelligent Systems from the University of Granada. Currently he is CTO. at Fidesol where performs diferent roles on the projects. His research focuses on distributed systems, management, integration and analysis of data, robotics, fuzzy logic systems, and the development of virtual reality environments for diferent purposes.



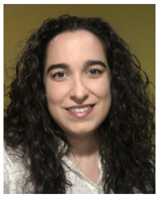
Juan Manuel Lombardo

PhD in Computer Science from the Pontifical University of Salamanca, was graduated in Economics and Business Administration in the University of Granada, Spain, Diploma of Advanced Studies (DEA) in Economics from UNED, Research Sufficiency in Business Science from the Complutense University of Madrid and Diploma of Advanced Studies (DEA) in Sociology from the Pontifical University of Salamanca. He is CEO at Fidesol and Professor at Andalusia Business School. Dr. Lombardo is the author of numerous articles and research papers published in journals and books of national and international conferences. Visiting Professor at the Private Technical University of Loja (UTPL Ecuador), The National University of the Northeast (Argentina), University Francisco José de Caldas (Colombia), Catholic University of Colombia, Catholic University of Ibarra (Ecuador), University of Lisbon (Portugal) and National Engineering University (Peru). Member of the Knowledge Management committee of AEC (Spanish Association for Quality) and the Institute CICTES (Ibero-American Centre on Science, Technology and Society).



Mabel López

Has a degree of Computer Science Engineering. She is Knowledge Manager at Fidesol. Participates in the research and development strategy of this entity, technology transfer and analysis of technological trends, such as big data, internet of things, virtual reality, cognitive engines, machine learning, etc. Currently, she is involved in several R & D projects related to the mentioned technologies.



Carmen María Alba

Degree in Information and Documentation at the University of Granada and web development technician specialized on Python. Currently, I am a document management in IASEC project and researcher in technologies as Big Data, Machine Learning and Blockchain.

Susana Velasco

Has a Technical Engineer in Computer from the University of Granada. In the past, she worked in manufacturing, financial and service sector enterprises as software engineer and analyst programmer. Her research interests include quality assurance, software quality management systems, Ambient Intelligence (AmI) systems and devices, and new generation of ICT technologies.

Manuel Alonso Braojos

Degree in Computer Science Engineering at the University of Granada. Currently he is a researcher at Fidesol where performs the role of fullstack software developer. He has participated in the development of various internet applications with different languages and technologies. His final degree work was an application for the representation of bibliometric data.

Marta Fuentes García

Holds a PhD in Information and Communication Technologies by University of Granada. She studied Computer Science and has a Master Degree in Software Development from the University of Granada. Her research has been mainly related to anomaly detection and diagnosis both in industrial processes and network traffic. Her PhD is focused in anomaly detection for network security using multivariate data analysis. She also has work experience in different companies as a programmer and, nowadays, she is part of the research team at Fidesol.