

Prevention of Cyber-Attacks and Privacy Breaches in Healthcare Sector

Antonio Scarfò[1(✉)], Carmine Piccolo[2], Francesco Palmieri[1], and Michele Mastroianni[1]

[1] Department of Information of Computer Science, University of Salerno, Salerno University of Salerno, 84084 Salerno, Italy
ascarfo@unisa.it

[2] Center for Computer Services, University of Naples Federico II, 80138 Napoli, Italy
carmine.piccolo@unina.it

Abstract. Periodically, analysts in the cybersecurity sector, collect and share relevant data about recent cybercrime trends. These insights cover many aspects of the current cyber-threat scenario, including actors involved, motivations of the attacks, attack vectors, consequences, targets, and so on. Many organizations leverage such data to prepare their risk management plans and cyber defense strategies. This paper illustrates a case study involving two sample structures, a university and its hospital that want to compare the data available in last cyber security reports with the one collected from their actual operating environment, with the aim of being aware of how the mentioned reports could be helpful in reducing cybersecurity risks.

Keywords: Cybersecurity · healthcare · risk · vulnerability · CVE · EPSS

1 Introduction

Nowadays, cybersecurity and risk management scenarios are getting more and more complex and hard to manage. Indeed, attackers can leverage both an always wider attack surface and increasingly powerful attack tools. According to the last IBM report [1] about cyber security trends, from 2020 to 2022 the average cost of data breaches has grown from 3.86 M$ to 4.35 M$. The report also says that the healthcare sector resulted in the highest cost per stolen record in data breaches.

Another key insight from IBM is that the average time needed to identify a data breach is 207 days, and the average time necessary to contain an attack is 77 days from its detection. Reducing these times means significantly decreasing the cost of data breaches.

[1] shows the key factors that affect the costs of data breaches. It appears that there are several prevention actions that can reduce considerably its overall cost. The adoption of Artificial Intelligence-driven platforms for the automation of defense tasks, and the arrangement of a more reactive cybersecurity governance model, may be significantly helpful in containing the cost of successful attacks.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14109, pp. 162–178, 2023.
https://doi.org/10.1007/978-3-031-37120-2_11

On the other side, the complexity, and lack of compliance with common security recommendations exacerbate the cost of a data breach. Finally, to better highlight the relevance of the problem, we consider that the healthcare services industry will be one of the most important drivers for the growth of IoT technologies, fostering the Internet of Medical Things (IoMT) ecosystem, which is already one of best potential targets for data breaches. Due to the aforementioned evolution dynamics, the attack surface will expand dramatically in the years coming. Fortune Business Insight forecasts a CAGR of 29.8% for the period 2021–2028, ending in 187 billion dollars.

In EU countries, due to the adoption since 2016 of the General Data Protection Regulation (GDPR), companies and public agencies are forced to comply with such regulation, implementing both technical and organizational security measures [17].

Moreover, the recent COVID-19 pandemic caused a sharp increase in the use of ICT technologies in all fields of real life, mainly within the healthcare sector. Unluckily, the pervasive use of such technologies led to an exponential growth of cybercriminal activities, and the new threats are directed primarily to smartphone apps and healthcare related IoT devices, often affected by severe vulnerabilities [18]. Also, energy-related attacks could play a key role, causing power failures and untimely battery faults on IoT devices [19].

Therefore, the need for network monitoring and breach prevention is increasingly critical to ensure an adequate perimeter defense. In order to help network and security managers to focus on the most frequent and threatening attacks, a number of reports have been periodically redacted by various stakeholders and organizations. This paper aims to investigate about some of the most popular report in the field of cyber-attacks. The reports have also been compared with each other, and then compared with a real-world analysis with two different datasets generated by perimetral firewall of two big organizations: a University and his University hospital in order to verify the coherence of the reports with attacks detected by the university firewalls.

2 The Methodology

The methodology used is structured in three steps, the first one aims to identify the most relevant and common threats, by seeking them in the literature and in recently published reports. The second step is focused on collecting real operational data from the field that are comparable with the one selected in the previous step. The last step consists in comparing the data of step one and step two, with the aim of evaluating the usefulness of the data published against the threats collected from the field. To better introduce the topic, this chapter will present the key concepts and organizations that are useful for our specific purposes.

To compare the data coming from the reports and from the field, a process of standardization is required. The basic element that helps to compare the data collected is the CVE concept.

2.1 CVE Program

The CVE stands for Common Vulnerabilities and Exposures. The CVE has the purpose of "Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities" [7]. The

vulnerabilities discovered and verified, are assigned and published by organizations from around the world that have partnered with the CVE Program. These organizations publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure uniqueness in managing the same issues and to coordinate efforts for prioritizing and addressing the vulnerabilities. The Program counts 275 partners, covering several different roles.

The original concept was introduced by the MITRE [5] Corporation's David E. Mann and Steven M. Christey in 1999. Later, the CVE program was recommended by the National Institute of Standards and Technology (NIST) in "NIST Special Publication (SP) 800–51" [6]. In June 2004, the U.S. Defense Information Systems Agency (DISA) issued a task order for information assurance applications that requires the use of products that use CVE IDs.

CVE has also been used as the basis for totally new services. The NIST's U.S. National Vulnerability Database (NVD), a "comprehensive cybersecurity vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources" is synchronized with, and based upon, the CVE. A CVE must be numbered and clearly described, as well as maintained, according to the form and the rules that govern the Program. A classification of the risk related to the vulnerability is provided by the National Vulnerability Database (NVD) which provides the CVSS (Common Vulnerability Scoring System), which is a method used to provide a qualitative measure of severity and score for almost all known vulnerabilities. CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. It should be clear that CVSS is not a measure of risk. CVSS consists of three metric groups: Base, Temporal, and Environmental, and the NVD provides just CVSS 'base scores', which represent the innate characteristics of each vulnerability. The metric group Temporal and Environmental can be used to customize the risk analysis providing a score of a CVE for a specific environment where the product operates. The Base Score metric is both quantitative and qualitative, like Fig. 3 shows. The base score of CVSS, is composed of a set of metrics. These metrics are chosen to take into account both the exploitability of the vulnerability and its impact when it is exploited. These metrics and their granularity have evolved through the different versions of CVSS. Figure 1 shows the qualitative and the quantitative score for CVEs through the releases,

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Fig. 1. Score and severity model of CVSS.

2.2 EPSS Program

The FIRST organization "aspires to bring together incident response and security teams from every country across the world to ensure a safe internet for all" [8]. So, FIRST wants to create a global language about cybersecurity, make available tools and means for incident responders, and work together with key stakeholders according to clear policy and governance rules.

With the aim of improving, in some ways, the CVSS systems, the organization called FIRST has created the Exploit Prediction Scoring System (EPSS) model, which is an open, data-driven effort for estimating the likelihood that a software vulnerability will be exploited in the wild. The purpose is to help the network defenders to optimize and prioritize the remediation of the vulnerability. The difference with the CVSS standards is clear, since it has been useful for capturing innate characteristics of a vulnerability and providing measures of severity, but it is limited in its ability to assess threats. EPSS was born to fill that gap because it composes current threat information from CVEs and real-world exploit data. The EPSS model produces a probability score between 0 and 1 (0 and 100%). The higher the score, the greater the probability that a vulnerability will be exploited.

3 Analysis of the Reports

In this chapter, we analyze the reports selected to extrapolate and compare data. There are four different reports.

3.1 ENISA Threat Landscape Report 2022

ENISA is the European Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act. As an observatory about cyber security dynamics, ENISA issues an annual report on the status of the cybersecurity threats landscape. The report identifies the prime threats, the major trends observed with respect to threats, the threat actors, and the attack techniques, and describes the relevant mitigation measures. Looking at the ENISA's report of 2022 [2], which provide a wide view about cyber threats from June 2021 to June 2022, it is possible extrapolate the following main threats, limiting the scope to healthcare and education fields.

- Ransomware, the period records an increasing activity of the attackers The most active groups, that produce more than half of the attacks are Lockbit, Conti, and ALPHV, followed by Black Basta and Hive. RDP (Remote Desktop Protocol) and Phishing are the most used vectors of attack. Brute force without multi-factor Authentication is the most common method used.
- Malware, after the Covid crisis, malware is on the rise again, likely because the alert to IT department is re-started since people are back in offices and the increasing precision of the attackers. The increase of malware is related mainly to crypto-jacking and IoT malware. Botnets, crypto miners, and info stealers have been the most common threats. IoT malware are doubled in 2022, and the main actors have been Mirai

and Mozi botnets. Relevant malicious activities are focused on supply-chain attacks, especially related to open-source packages (typo squatting). Also, from the blocking of macros from internet files by Microsoft, the attack is shifted away from VBA and has gone towards container files (ISO, ZIP, RAR, LNK)

- Attacks against availability, DDoSes remain one of the most critical threats. The Pandemic and Ukraine-Russian war influenced the shape of DDoSes like never in the past. An increasing fuel for DDoSes comes from mobile and sensor devices. These devices, whose number is on rapid rise, can be attacked both for exhausting their energy resources and also used as individual bots within a botnet to attack external targets. Multi-vector attacks are preferred as well as applications/protocols-based attacks. A relevant dynamic is that IoT devices are easy to attack since patching and updating are often done too late. A new kind of attack is a combination of DDoS and Ransomware, referred as RDoS attack.

The threat listed by ENISA and mentioned above, are linkable to some kye CVEs, which are summarized below, Table 1.

Table 1. ENISA Top Threats and CVEs

Threats	**CVE**
Lokbit [9]	CVE-2021-34523, CVE-2021-31207, CVE-2021-34473, CVE-2021-22986, CVE-2018-13379, CVE-2021-36942, CVE-2021-20028, CVE-2020-0787, CVE-2022-36537
BlackCat (ALPHV) [10]	CVE-2016-0099, CVE-2019-7481, CVE-2021-31207, CVE-2021-34473, CVE-2021-34523
Conti [11]	CVE-2018-13379, CVE-2018-13374, CVE-2020-0796, CVE-2020-0609, CVE-2020-0688, CVE-2021-21972, CVE-2021-21985, CVE-2021-22005, CVE-2021-26855, CVE-2015-2546, CVE-2016-3309, CVE-2017-0101, CVE-2018-8120, CVE-2019-0543, CVE-2019-0841, CVE-2019-1064, CVE-2019-1069, CVE-2019-1129, CVE-2019-1130, CVE-2019-1215, CVE-2019-1253, CVE-2019-1315, CVE-2019-1322, CVE-2019-1385, CVE-2019-1388, CVE-2019-1405, CVE-2019-1458, CVE-2020-0638, CVE-2020-0787, CVE-2020-1472, CVE-2021-1675, CVE-2021-1732, CVE-2021-34527
MIRAI [12]	CVE-2012-4869, CVE-2014-9727, CVE-2017-5173, CVE-2019-15107, CVE-2020-8515, CVE-2020-15415, CVE-2022-36267, CVE-2022-26134, CVE-2022-4257
MOZI [16]	CVE-2016-6277, CVE-2014-8361, CVE-2015- 2051, CVE-2008-4873, CVE-2017-17215, CVE-2018-10561, CVE-2018-10562

From the perspective of CVEs, ENISA leverages two reports, [13, 14], by IBM and RedCanary. These reports mention ProxyLogon, ProxyShell, PrintNightmare, whose CVE are included in the following reports and in Conti Botnet. Also mentioned are:

- Kaseya VSA, CVE-2021-30116
- ManageEngine CVE-2021-40539, CVE2021-44077, CVE-2021-44515
- Accellion FTA vulnerability susceptible to SQL injection, CVE-2021-27101
- Liferay Portal deserialization of untrusted data allows for remote code execution via JSON web services, CVE-2020-7961
- MobileIron vulnerability allowing for remote code execution, CVE-2020-15505
- ForgeRock AM server Java deserialization vulnerability allows for remote code execution, CVE-2021-35464
- Citrix Server path traversal flaw, CVE-2019-19781

3.2 CISA Reports 2021

The Cybersecurity and Infrastructure Security Agency (CISA) is an agency of the United States Department of Homeland Security (DHS), which that is responsible for strengthening cybersecurity and infrastructure protection across all levels of government, coordinating cybersecurity programs with U.S. states, and improving the government's cybersecurity protections against private and nation-state hackers (February 19, 2019). The agency covers two key roles: "CISA acts as the quarterback for the federal cybersecurity team, protecting and defending the home front—our federal civilian government networks", also CISA "coordinates the execution of our national cyber defense, leading asset response for significant cyber incidents and ensures that timely and actionable information is shared across federal and non-federal and private sector partners". The mission of the agency requires an intensive collection and analysis of insights from the field, working across the private and public sectors. Periodically, the agency issues reports that light on the threats on the field. One of the most interesting is "2021 Top Routinely Exploited Vulnerabilities" [3], which reports the vulnerabilities most used by attackers, observed by U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities during the 2021. These CVEs are:

- CVE-2021-44228 (Log4Shell). This vulnerability affects Apache's Open Source Log4j library. It is exploitable to submit a specially crafted request to a vulnerable system, which is open to the execution of an arbitrary code. Log4j is incorporated into thousands of products worldwide. This CVE is critical and scores 10.0.
- CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065 (ProxyLogon). These vulnerabilities, affect Microsoft Exchange email servers. Exploiting them in combination, is possible that an unauthenticated actor executes arbitrary code, allowing to gain persistent access to files and mailboxes on the servers, as well as to credentials stored on the servers.
- CVE-2021-34523, CVE-2021-34473, CVE-2021-31207 (ProxyShell), affect Microsoft Exchange email servers. Like in the previous case, the exploitation of the vulnerabilities in combination allows a remote actor to execute arbitrary code. These vulnerabilities reside within the Microsoft Client Access Service (CAS), CAS is commonly exposed to the internet to enable users to access their email via mobile devices and web browsers.

- CVE-2021-26084. This vulnerability affects Atlassian Confluence Server and Data Center, it allows an unauthenticated attacker to execute arbitrary code on vulnerable systems. This vulnerability quickly became one of the most exploited, mass exploitation attempts of this vulnerability was observed in September 2021, after its disclosure.
- CVE-2021-40539 is a high-rated (9.8) and highly exploited vulnerability, that allows to bypass authentication with remote execution code.
- CVE-2021-21972 is the vulnerability of VMware vCenter plugin that contains remote code execution, also critical with 9.8 score by NIST.
- CVE-2020-0688 is another critical vulnerability for Microsoft Exchange that allows remote code execution. Score 8.8.
- CVE-2019-11510 is a 10.0-scored vulnerability in Pulse Secure Pulse Connect Secure (PCS), which allows an unauthenticated remote attacker to perform an arbitrary file reading vulnerability.
- CVE-2018-13379 is a 9.8-scored vulnerability in Fortinet FortiOS and FortiProxy under SSL VPN web portal that allows an unauthenticated attacker to download system files via specially crafted HTTP resource requests.

2021 Top Malware Strains is another report by CISA, it discloses the top Malware in 2021. These malwares are Agent Tesla (RAT), AZORult (Trojan), Formbook (Trojan), Ursnif (Trojan), LokiBot, (Trojan) MOUSEISLAND (Macro downloader), NanoCore (RAT), Qakbot (Trojan), Remcos (RAT), TrickBot (RAT) and GootLoader (Loader). An interesting insight is that Cyber-criminals have used these malwares in the last five and, in some cases, ten years. The awareness of the methods of attacks may really help to defend infrastructures and data.

3.3 FORTINET'S Report 2022

Fortinet is an American multinational corporation headquartered in Sunnyvale, California. The company develops and sells cybersecurity solutions, such as physical firewalls, antivirus software, intrusion prevention systems, and endpoint security components. The business is the most important at the worldwide level in terms of appliances delivered, it records 37% of the market by IDC.

Based on its threat intelligence activity, Fortinet publishes a biannual report about threats and vulnerabilities observed. The report is called "Global Threat Landscape Report" by Fortiguard labs in the first half of 2022 [4], the company has observed 10.666 ransomware variants. The alarming trend of Wipers malware is increasing at a worldwide level. Finally, OT devices as a target are increasing dramatically, due to the high number of vulnerabilities exposed. From these first three macro-finding appear the main threat of zero-day, which are in significative rising compared to the past, 72 discovered.

Figure 2 shows the top 20 detections by IPS, Intrusion Detection System, which helps to discover exploitation attempts and can log the CVE that is tried to be exploited.

Following the top attacks together with their CVEs:

- Log4j2: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105), that is the Remote Code Execution. The CVE-2021-44228 is already mentioned and scored 10.0, and

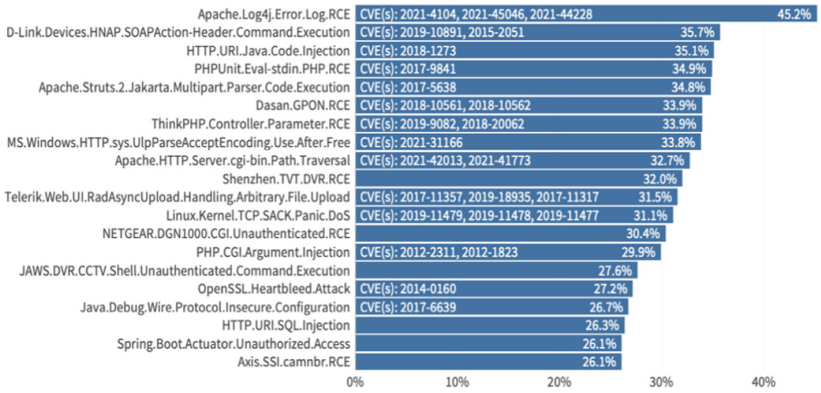

Fig. 2. Top IPS detection H12022

also, the report mentions CVE-2021-45046, a vulnerability that affects the patch of the CVE-2021-44228 and is critical due to its score of 9.0. Also, the 2021-45105 is another but medium base score CVE for Log4j2. The report links the Fortiguard services pages, where some insights are shown.

- D-Link.Devices, CVE-2019-10891, CVE-2015-2051. These are CVEs affecting D-Link Routers. The first allows RCE on the router and score 9.8, the second CVE in under review currently.
- HTTP.URI.Java.Code.Injection CVE 2018-1273, is another RCE by a remote malicious user that affects Java. The CVE scores 9.8 and is critical.
- PHPUnit.Eval-stdin.PHP.RCE, CVE 2017-9841, this is critical, scoring 9.8, vulnerability that allows a RCE in PHPUnit, and the remote attacker can gain control of vulnerable systems.
- Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution, CVE 2017-5638, this is a critical 10.0 scoring vulnerability, that can exploit a remote Code Execution vulnerability in Apache Struts.
- Dasan.GPON.RCE, CVE(s) 2018-10561, 2018-10562. It is another RCE where a remote attacker can take the control of the device. Both CVEs score 9.8.
- MS.Windows.HTTP.sys.UlpParseAcceptEncoding.Use.After.Free, CVE-2021-31166 scores 9.8. This indicates an attack attempt to exploit a Use After Free Vulnerability in Microsoft Windows HTTP.sys. A remote, authenticated attacker can exploit this vulnerability by sending a crafted HTTP request to the target server.
- ThinkPHP.Controller.Parameter.Remote.Code.Exec utionhis, CVEs 2019-9082, 2018-20062. This is an attack attempt to exploit a Remote Code Execution Vulnerability in ThinkPHP.

3.4 Data from EPSS

As mentioned in paragraph II.B, EPSS is a program that has the mission to predict the most dangerous CVEs in the days coming. Looking at these data is another interesting analysis that can tell us if the ESSP's predictions are observed in the field. With this purpose, hereafter is presented some insights from EPSS data.

There are two main pieces of information that are useful to be analyzed. The first is the relationships between ESPP data and CVE, which is shown in Fig. 3. The CVEs are scored by CVSS v3.0 included in NVD. It comes clear that CVSS and ESPP are totally different approaches, but both useful.

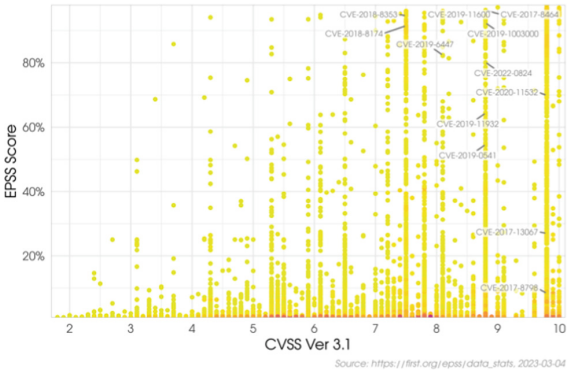

Fig. 3. EPSS compared to CVSS 3.0 (NVD)

The EPSS score is calculated by a Machine Learning system, that collects data from several sources. ML collects data continuously, and, unlike CVSS, also from the field. These data include information coming also from Fortinet Fortiguard labs. Collecting data from the field, EPSS, by its nature, is more dynamic than CVSS,

Both EPSS and CVSS cannot estimate the risks related to the environment where the affected devices are installed. In some way, EPSS is more specific than CVSS, it, analyzing data from the field can include temporal elements.

So, it is interesting to compare the EPSS predictive score with data from the field. With that aim, in the following are reported the most critical CVE, scored by EPSS.

Table 2 shows the riskiest CVEs based on the evaluation of EPSS, all above 96% of score. The list is related to the EPSS report of 15 February 2023, and reports the CVEs that most likely will be exploited in the following 90 days.

3.5 Data from the Field

In this chapter is disclosed the data collected from the field. The architecture of analysis consists in a double pair of Firewalls that act as perimeter protection in a university network infrastructure and its hospital. A couple of Firewall Fortigate 3400E work as perimetral defense internal- internet segmentation, whereas the second couple of firewalls, Fortigate 1800F, act as a perimetral defense for the datacenter of the hospital. These couples of firewalls are equipped with a Fortiguard UTM license of software, which include features like Intrusion Protection System (IPS) and Antivirus. The IPS are system of protection that can detect the attempts to exploit a CVE. The Fig. 4 shows the architecture of the analysis, it highlights the firewall form which are taken the dataset. These firewalls manage two typologies of traffic, the traffic to and from Internet, which

Table 2. Most risky CVE by ESPP march compared to CVSS 3.0 (NVD)

CVE	EPSS Likelihood	CVE	EPSS Likelihood
CVE-2021-26084	97,72%	CVE-2014-6271	96,24%
CVE-2021-40438	97,22%	CVE-2019-0708	96,11%
CVE-2017-12635	97,11%	CVE-2018-0296	96,09%
CVE-2021-44228	97,10%	CVE-2019-17558	96,09%
CVE-2022-47966	96,96%	CVE-2017-0144	96,09%
CVE-2020-5902	96,82%	CVE-2019-3396	96,09%
CVE-2019-16759	96,82%	CVE-2017-0037	96,08%
CVE-2021-26855	96,74%	CVE-2021-21972	96,08%
CVE-2020-1938	96,55%	CVE-2014-0160	96,06%
CVE-2019-11510	96,51%	CVE-2021-26295	96,05%
CVE-2017-8464	96,39%	CVE-2018-7600	96,02%
CVE-2022-28219	96,35%	CVE-2021-44077	96,02%
CVE-2019-2725	96,29%	CVE-2019-11043	96,00%
CVE-2016-10033	96,29%	CVE-2018-15961	96,00%
		CVE-2021-26084	97,72%
		Model Version v2022.01.01 – Score_Date:2023-03-04T00:00:00+0000	

is prefiltered by the second cluster of firewalls 3400E, and the traffic to and from the internal network.

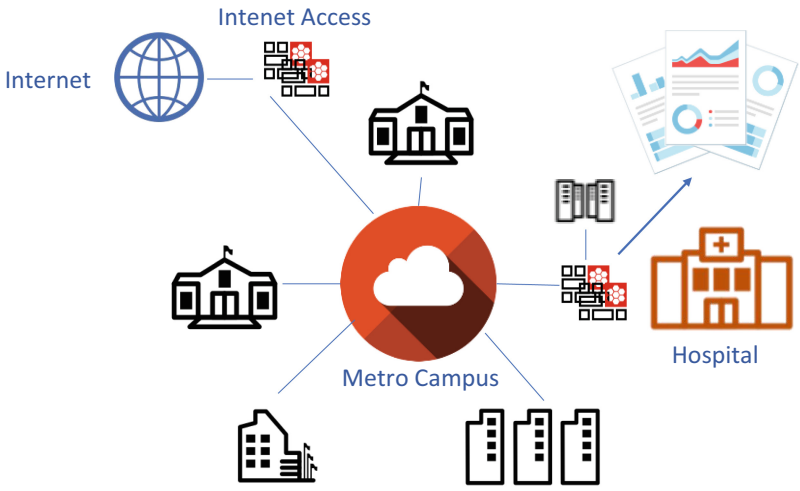

Fig. 4. Field Architecture – Dataset 1

The Dataset 1 is taken for the cluster of Fortigate 1800F in the period from 19 Feb 2023 and 24 Feb 2023, which defend the perimeter of the hospital and its datacenter. The most important intrusions detected by IPS are the of DDoS, mostly, and Malware. Mostly, attacks are related to an old botnet called Andromeda. This botnet was born in 2011 and is quite disappeared since years. The second attack detected is DoublePulsar Backdoor, it allows the connection of remote hosts, thought SMB and RDP (port 3389), for malicious actions. Then, as high-scored threats, there is Robot.PKCS.RSA.Information..Disclosure, this attack exploits some vulnerabilities in TLS protocol cryptographic, vulnerability in TLS protocol in RSA key exchange, to recover private keys. The attack is linked to some CVE. Also, there are Adobe.Acrobat.CVE-2018-16042.Security.Bypass, MS.IE.CTreePos.Objects.Memory.Corruption, Mirai and DCRat.botnet.

Given the not so numerous attempts of threats detected from the IPS protecting the hospital datacenter, another dataset (dataset 2) was carried out from the IPS of the Firewall exposed to the internet, Fig. 5.

Figure 6 shows these intrusions detected and some of the main important: 1.7M critical severity threats, 1.1M high severity threats, 2.4M medium severity threats. The threats detected by the first dataset are related to internal networks, whereas the threats detected by the second dataset from the field are related to the internet. The internet perimetral firewall acts efficiently as a first filter towards the hospital datacenter, analyzing all traffic but the internal one. Looking at the dataset 2, the list of threats detected it is possible identify some relevant attacks already mentioned in the previous analysis.

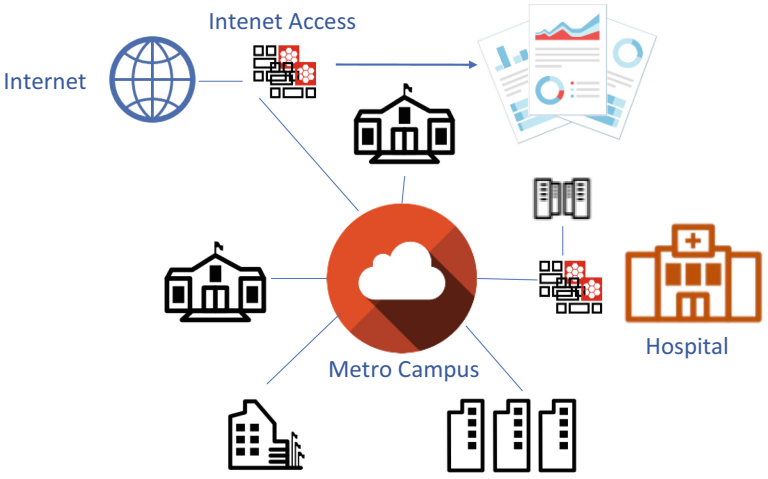

Fig. 5. Field Architecture – Dataset 2

Among the critical attacks there are Log4j2, line 10, with its CVEs (CVE-2021-4104, CVE-2021-44228, CVE-2021-45046), and Open SSL (CVE-2014-0160), line 14. Among the high severity attacks we can identity two critical Botnet: Mirai, line 4, and Mozi, line 9.

Criticity	ID	Attack Name	CVE-ID	Counts
###Critical Severity Intrusions###	1	Realtek.SDK.UDPServer.Command.Execution	CVE-2021-35394	1.501.221,00
	2	MikroTik.RouterOS.Arbitrary.File.Read	CVE-2018-14847	87.799,00
	3	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	CVE-2017-9841	50.133,00
	4	H-worm.Botnet		47.642,00
	5	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	CVE-2015-2051,CVE-2019-10891	18.635,00
	6	Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection	CVE-2021-36260	14.364,00
	7	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution		12.663,00
	8	Dasan.GPON.Remote.Code.Execution	CVE-2018-10561,CVE-2018-10562	12.224,00
	9	ThinkPHP.Controller.Parameter.Remote.Code.Execution	CVE-2019-9082,CVE-2018-20062	5,127,00
	10	Apache.Log4j.Error.Log.Remote.Code.Execution	CVE-2021-4104,CVE-2021-44228,CVE-2021-45046	3.756,00
	11	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	2.753,00
	12	WordPress.HTTP.Path.Traversal	CVE-2019-9618,CVE-2018-16283,CVE-2018-16299,CVE-2020-11738	2.589,00
	13	Bladabindi.Botnet		2.439,00
	14	OpenSSL.Heartbleed.Attack	CVE-2014-0160	242,00
	15	Eir.D1000.Modem.CWMP.Command.Injection	CVE-2016-10372	2.341,00
	16	GitLab.Community.and.Enterprise.Edition.Command.Injection	CVE-2021-22205	1.794,00
	17	Gh0st.Rat.Botnet		1.356,00
	18	Zeroshell.Kerbynet.Type.Parameter.Remote.Command.Execution	CVE-2009-0545,CVE-2019-12725	1.333,00
	19	Java.Debug.Wire.Protocol.Insecure.Configuration	CVE-2017-6639	1.263,00
	20	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	CVE-2017-5638	1.106,00
###High Severity Intrusions###	1	Linux.Kernel.TCP.SACK.Panic.DoS	CVE-2019-11477,CVE-2019-11478,CVE-2019-11479	550.495,00
	2	malicious-url		236.099,00
	3	HTTP.URI.SQL.Injection		107.502,00
	4	Mirai.Botnet		103.816,00
	5	Multiple.Routers.GPON.formLogin.Remote.Command.Injection		50.453,00
	6	AndroxGh0st.Malware		40.248,00
	7	RedLine.Stealer.Botnet		24.765,00
	8	Web.Server.Password.File.Access		11.936,00
	9	Mozi.Botnet		10.788,00
	10	RotaJakiro.botnet		10.739,00
	11	HTTP.Unix.Shell.FS.Remote.Code.Execution		4.198,00
	12	MS.Office.EQNEDT32.EXE.Equation.Parsing.Memory.Corruption	CVE-2018-0798,CVE-2018-0802,CVE-2017-11882	376,00
	13	Joomla!.CMS.Webservice.API.index.php.Unauthorized.Access	CVE-2023-23752	1.622,00
	14	JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution	CVE-2016-20016	1.525,00
	15	NetSupport.Rat.Botnet		1.277,00
	16	Alcatel-Lucent.OmniPCX.Office.MasterCGI.User.Command.Execution	CVE-2007-3010	1.003,00
	17	PHP.URI.Code.Injection		949,00
	18	MS.IIS.Command.Shell.SQL.Injection	CVE-2005-4149	842,00
	19	VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution		806,00
	20	PHP.CGI.Argument.Injection	CVE-2012-1823,CVE-2012-2311,CVE-2012-2688	688,00
###Medium Severity Intrusions###	1	SSLv3.POODLE.Information.Disclosure	CVE-2014-3566	2.298.422,00
	2	HTTP.Referer.Header.SQL.Injection	CVE-2007-1061	99.372,00
	3	WordPress.xmlrpc.php.system.multicall.Amplification.Attack		16.639,00
	4	WordPress.xmlrpc.Pingback.DoS		12.571,00
	5	Android.ADB.Debug.Port.Remote.Access		9.123,00
	6	TCP.Split.Handshake		8.377,00
	7	WordPress.REST.API.Username.Enumeration.Information.Disclosure	CVE-2017-5487	5.972,00
	8	NTP.Monlist.Command.DoS	CVE-2013-5211	3.564,00
	9	PHP.Diescan		1.031,00
	10	MS.IIS.DLL.Request.DoS	CVE-2005-4360	756,00
	11	HTTP.URI.Script.XSS	CVE-2002-1315,CVE-2017-0068	325,00
	12	Sophos.Anti-Virus.Reserved.Device.Name.Handling.SMTP	CVE-2004-0552	192,00
	13	NetworkActiv.Web.Server.XSS		158,00
	14	Atlassian.Server.S.Endpoint.Information.Disclosure	CVE-2021-26085,CVE-2021-26086	140,00
	15	Novell.NetBasic.Scripting.Server.Directory.Traversal	CVE-2002-1417	132,00
	16	Apache.Axis2.Default.Password.Access	CVE-2010-0219	127,00
	17	HTTP.Malformed.Request.Directory.Traversal	CVE-2005-2020,CVE-2008-2938	110,00
	18	PHP.mosConfig_absolute_path.Remote.File.Inclusion	CVE-2004-1693,CVE-2006-3396,CVE-2006-3736,CVE-2006-3773,CVE-2006-377	103,00
	19	VBulletin.Vote.PHP.Nodeid.Parameter.SQL.Injection	CVE-2013-3522	100,00
	20	FCKeditor.CurrentFolder.Arbitrary.File.Upload	CVE-2009-2265	93,00

Fig. 6. Dataset 2, data from the internet perimeter

4 Comparison Between the Reports and the Datasets

In this chapter, the CVEs extrapolated from the four reports taken into consideration are compared. The methodology followed consists of the calculation of the intersections among the four sets of CVEs. The first evaluation is between the set of CVEs form ENISA, CISA and Fortiguard with the CVEs of EPSS. This step is useful to highlight which CVE, part of these reports, are forecasted by EPSS to be exploited. FortiGuard shares with EPSS just the CVE-2021-44228 (10%) related to Log4j2 and, specifically Log4Shell, vulnerability. The set of CVEs by ENISA shares with EPSS two vulnerabilities (3%): CVE-2021-21972, CVE-2021-26855; both related to Conti Botnet. CISA shares with EPSS 5 CVEs: CVE-2021-44228, CVE-2021-26855, CVE-2021-26084, CVE-2021-21972, CVE-2019-11510 (30%). These CVEs are related to Log4j2, ProxyLogon, Atlassian Confluence, VMware vCenter, Pulse Secure Pulse Connect Secure. The CVE reported by CISA will be mostly likely exploited in the next future.

Looking at the correlation between the set of CVEs of the report, there are the following outcomes:

- CISA and ENISA share 8 CVEs. These CVEs are related to the attack techniques of Lokbit, Conti and Mozi. Among these CVEs, EPSS forecasts CVE-2021-21972, CVE-2021-26855 as most likely to be exploited, and both related to Conti.
- ENISA and Fortiguard share 2, that are related to MOZI Botnet for remote control execution. None of these are forecasted to be exploited in the next future by EPSS.
- ForiGuard and CISA shares one CVE, which is related to Log4j2,

If we look at CVEs included in all of three reports by ENIA, CISA and Fortiguard, there are not any CVEs included in all these three reports. Finally, CISA is the report that has in common the majority of CVE with EPSS, and CISA (53%) and ENISA (11%) share the most CVEs among the three reports.

The Venn's Diagram in the Fig. 7 shown the intersection among the set of CVEs of the report analyzed. Then, looking at four reports, ENISA, CISA, FortiGuard and EPSS, the critical CVEs are being extrapolated and correlated. These reports have in common some CVEs, mostly related to recent and widespread threats like Conti, Mozi and Log4j2. The first analysis has been comparing the reports from ENISA, CISA and ForiGuard against EPSS in order to highlights the CVEs belonging to these three reports that will be, most likely, exploited in the next future. CISA lists the most CVEs that EPSS predicted to be exploited, 5 out 15; ENISA share with EPSS 2 CVEs out of 72, and, finally, FortiGuard just 1 CVE out of 20. The CVEs shared by CISA and EPSS are the riskiest because there include all CVEs shared by ENISA and FortiGuard with EPSS.

Then, looking at the intersection among the reports by ENISA, CISA and Forti-Guards, we have seen the all the three reports together do not share any CVEs. ENISA and CISA share 8 CVEs out of the 72 selected from ENISA, 2 are the CVEs shared by ENISA and FortiGuard, only 1 CVE is shared between CISA and FortiGuard.

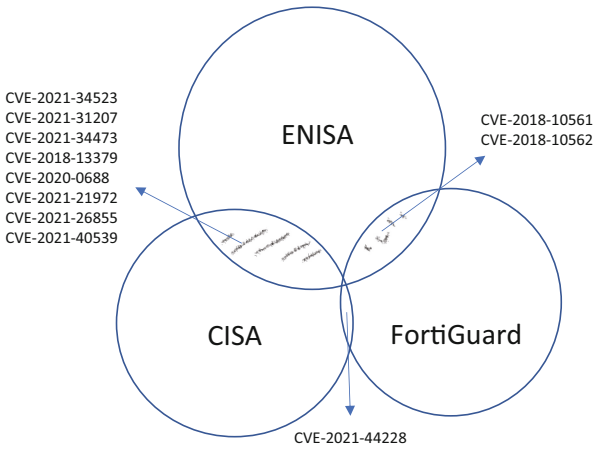

Fig. 7. CVEs shared by ENISA, CISA, FortiGuard, Venn Diagram

CISA is the report that is more aligned with ENISA and EPSS, whereas FortiGuards is the less aligned with the others reports.

Trying to extrapolate the riskiest CVE, the CVEs belonging at least to two reports are 11, and are related to Conti, Mozi, Lokbit and Log4j2. Out these 11, the CVEs also listed by EPPS are 3, that are related to Conti and Log4j2.

Table 3. Riskiest CVEs

CVEs Sets	**CVE**
$(ENISA \cap CISA) \cup (ENISA \cap Foriguard) \cup (CISA \cap Foriguard)$	CVE-2021-34523 CVE-2021-31207 CVE-2021-34473 CVE-2018-13379 CVE-2020-0688 CVE-2021-21972 CVE-2021-26855 CVE-2021-40539 CVE-2018-10561 CVE-2018-10562 CVE-2021-44228
$[(ENISA \cap CISA) \cup (ENISA \cap Foriguard) \cup (CISA \cap Foriguard)] \cap ESPP$	CVE-2021-44228 CVE-2021-21972 CVE-2021-26855

Looking at the data collected from the field, specifically from the report 1, surprisingly, there are not threats and CVE shared with any of the reports analyzed. Except for CVE-2018-1388, that is a high scored CVE related to GSKit V7 of Tivoli IBM platform. The intrusion detected by the IPS and AV system in place, in the report 1, are related to old CVE and even the attacks that are not listed by no one of the report analyzed in the most critical CVEs.

In we extend the analysis to the report, report 2, from the internet perimeter IPS the scenario completely changes. First, the intersection between the sets of CVEs coming from the report 1 and the report 2 consists in just a CVE: CVE-2005-4360, RCE for Microsoft Internet Information Services (IIS) 5.1. Then, we record the following situation about the internet perimeter IPS:

- the intersection with ENISA's consist in two CVEs, which are about Mozi. ENISA predicts the 2.7% of all the detected exploitations and 10% among the critical attempts of exploitation.
- the intersection with CISA's is one CVE, which is relate to Apache Log4j 2. CISA predicts the 1.35% of all the detected exploitations and 5% among the critical attempts of exploitation.
- the intersection with Fortiguard are ten CVEs. As to be expectable, the CVE shared are the most numerous. The threats are related to Mozi, Log4j2, and ThinkPHP. FortiGuard predicts 13.9% of all the detected exploitations and 50% among the critical CVEs.

- the intersection with EPSS are two CVEs. These are related to Log4j2 and Heartbleed in OpenSSL. EPSS predicts 2.7% of all the detected exploitations and 10% among the critical CVEs. This is a bad data because of EPSS should works as predictive engines for the defenders.

The scenario is summarized in the Table 4, the data form the filed says that FortiGuard report is the most helpful report to arrange an action of defense. Even if it helps to predict just the 50% of the critical threats. Out of the 11 riskiest CVEs of the Table 3 the report 2 lists only 3: Log4j2 CVE-2021-44228 is shared by all reports but the ENISA one, CVE-2018-10561, and CVE-2018-10562. We can deem it as the threat most dangerous and, fortunately, filtered by the perimetral cluster in our scenario.

Table 4. Intersection among CVEs of Report 2 and CVEs of Report 2

CVEs Sets	CVE	Impact
ENISA ∩ *Report*2	CVE-2018-10561, CVE-2018-10562	2.7% Total CVEs 10% Critical CVEs
CISA ∩ *Report*2	CVE-2021-44228	1.35% Total CVEs 5% Critical CVEs
Fortiguard ∩ *Report*2	CVE-2017-9841 CVE-2015-2051 CVE-2019-10891 CVE-2018-10561 CVE-2018-10562 CVE-2019-9082 CVE-2018-20062 CVE-2021-44228 CVE-2021-45046 CVE-2017-5638	13.9% Total CVEs 50% Critical CVEs
EPSS ∩ *Report*2	CVE-2012-4869 CVE-2014-9727 CVE-2017-5173 CVE-2014-0160 CVE-2021-44228	2.7% Total CVEs 10% Critical CVEs

5 Conclusions and Future Works

The paper has the aim of evaluating the usefulness of data coming from some of the most relevant reports in the cyberspace sector for the operative defense against cyber-attacks. As a matter of fact, models like MITRE allow to prepare infrastructures, organizations, and people against well know attacks, and in [15] is shown how it is possible linking MITRE ATT&CK TTP (Tactics, Techniques and Procedures of attacks) and CVEs, this allows to predict the behaviors of the attackers and, consequently, helps to prepare the defense.

In conclusion, the reports analyzed are not particularly useful with the purpose to prepare the defense, even EPSS does not find confirmation by the data from the field, at least, in this specific case. Even if all reports identify some critical threats observed on the field. And, even putting together ENISA, CISA and EPSS is possible predict just the 5.5% of the attacks overall, and 20% of critical attacks detected from the field. The exception is the FortiGuard Threats Landscape report, which usefulness of the is certainly more interesting. Indeed, following the insights of that report, it is possible to be prepared for the 50% of the critical attacks. Somehow it is something we could imaging.

The works presents a limitation, the miss of the SSL inspection configuration on the firewalls. In this way, the firewall must detect a CVE exploitation through the analysis of encrypted traffic. In that case, the firewall can access just clear text information, limiting its ability to detect CVE exploitation activities. In that constrain, the IPS limiting the analysis just to some features, like IP addresses, time of packets inter-arrival, packets length, number of ACK packets, number of retransmissions, and all statistics linkable with this information. So, the IPS could, mainly, carries out some behavioral analysis that is not its purpose, since it works on signature base.

Future works can be developed on the analysis improvement. Extending, for example, the IPS configuration the mean of SSL inspection, or implementing IPS at host level, with the purpose to detect a most wide set of attempts of CVE exploitations.

References

1. Ponemon Institute LLC, September 16, 2022: Cost of a Data Breach Report 2022. https://www.ibm.com/downloads/cas/3R8N1DZJ. Accessed 25 Mar 2023
2. Ifigeneia Lella, Eleni Tsekmezoglou, Rossen Svetozarov Naydenov, Cosmin Ciobanu, Apostolos Malatras, Marianthi Theocharidou – European Union Agency for Cybersecurit, October 2022, ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. Accessed 25 Mar 2023
3. Cybersecurity Advisory (CSA), Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security, (CCCS), New Zealand National Cyber Security Centre (NZ NCSC), United Kingdom's National, Cyber Security Centre (NCSC-UK), 27 April 2022, 2021 Top Routinely Exploited Vulnerabilities. https://www.cisa.gov/sites/default/files/publications/AA22-117A_Joint_CSA_2021_Top_Routinely_Exploited_Vulnerabilities_Final.pdf. Accessed 25 Mar 2023
4. Foriguard Labs, 16 Agust 2022, "Global Threat Landscape Report, 1H 2022. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2022.pdf. Accessed 25 Mar 2023
5. Ahmed, M., Panda, S., Xenakis, C., Panaousis, E.: MITRE ATT&CK-driven Cyber Risk Assessment. In: Proceedings of the 17th International Conference on Availability, Reliability and Security, ARES 2022. Association for Computing Machinery, New York, NY, USA, Article 107, pp. 1–10 (2022). https://doi.org/10.1145/3538969.3544420
6. Waltermire (NIST), D., Scarfone (G2), K.: Guide to Using Vulnerability Naming Schemes, February 2011. https://csrc.nist.gov/publications/detail/sp/800-51/rev-1/final
7. U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), The MITRE Corporation, About the CVE Program. https://www.cve.org/. Accessed 25 Mar 2023

8. Forum of Incident Response and Security Teams, FIRST Vision and Mission Statement. www.first.org/about/mission. Accessed 25 Mar 2023
9. Aluri, S.: Posted on Sep 28, 2022 and Updated on September 29, 2022, All about LockBit Ransomware. https://cybersecurityworks.com/blog/ransomware/all-about-lockbit-ransomware.html. Accessed 25 Mar 2023
10. By Ravindran, P.: posted on Jul 14, 2022 and Updated on 06 Sep 2022, All about BlackCat (ALPHV). https://cybersecurityworks.com/blog/ransomware/all-about-blackcat-alphav.html. Accessed 25 Mar 2023
11. Narang, S.: ContiLeaks: Chats Reveal Over 30 Vulnerabilities Used by Conti Ransomware, 24 March 2022. https://www.tenable.com/blog/contileaks-chats-reveal-over-30-vulnerabilities-used-by-conti-ransomware-affiliates. Accessed 25 Mar 2023
12. Lei, C., Zhang, Z., Hu, C., Das, A.: Mirai Variant V3G4 Targets IoT Devices, 15 February 2023. https://unit42.paloaltonetworks.com/mirai-variant-v3g4/. Accessed 25 Mar 2023
13. Astle, J., et al.: 2022 Threat Detection Report, Mar 25 2023. https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf
14. Singleton, C., et al.: X-Force Threat Intelligence Index 2022, February 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ. Accessed 25 Mar 2023
15. Kuppa, A., Aouad, L., Le-Khac, N.-A.: Linking CVE's to MITRE ATT&CK Techniques. In: Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 21). Association for Computing Machinery, New York, NY, USA, Article 21, pp. 1–12 (2021). https://doi.org/10.1145/3465481.3465758
16. Tu, T.-F., Qin, J.-W., Zhang, H., Chen, M., Xu, T., Huang, Y.: A comprehensive study of Mozi botnet. Int. J. Intell. Syst. **37**, 6877–6908 (2022). https://doi.org/10.1002/int.22866
17. Di Martino, B., Mastroianni, M., Campaiola, M., Morelli, G., Sparaco, E.: Semantic techniques for validation of GDPR compliance of business processes. In: Barolli, L., Hussain, F.K., Ikeda, M. (eds.) Complex, Intelligent, and Software Intensive Systems. AISC, vol. 993, pp. 847–855. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-22354-0_78
18. Bobbio, A., Campanile, L., Gribaudo, M., Iacono M., Marulli F., Mastroianni M.: A cyber warfare perspective on risks related to health IoT devices and contact tracing Neural Comput. Appl. 1–15 (2021).https://doi.org/10.1007/s00521-021-06720-1
19. Palmieri, F., Ricciardi, S., Fiore, U., Ficco, M., Castiglione, A.: Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures. J. Supercomput. **71**(5), 1620–1641 (2014). https://doi.org/10.1007/s11227-014-1242-6