Journal of Digital Science

ISSN 2686-8296

Volume 4 Issue 2 December 2022

CONTENTS

Cyber-Security Attacks, Prevention and Malware Detection Application

Darius Moldovan [1[0000-0003-2262-3746]], Simona Riurean [2[0000-0002-5283-6374]]

[1] Bit Sentinel, București, Romania
[2] University of Petroșani, Petroșani, Romania

https://doi.org/10.33847/2686-8296.4.2_1

Received 20.10.2022/Revised 20.11.2022/Accepted 23.12.2022/Published 28.12.2022

Abstract. The internet has become more or less, for most of us a dangerous place to live, work and relax when no proper measures are taken, and the response to incidents is not very clear and well implemented, both for organizations and individuals. This paper makes a short overview of current types and incidents of cyber-attacks, as well as the current state of threats, and the grade of awareness worldwide. Some methods to prevent cyber-attacks, malware analysis, and threat hunting, are presented, too. The paper also contains an application developed with a series of APIs that link the application to open-source tools and activate them, hence analyzing the content of the possible malicious files.

Keywords: malware, ransomware, social engineering, phishing, crypto-jacking.

1. A Short Overview of Cyber-Attacks

The Internet network improves the efficiency of our daily activities, however, it also brings a lot of drawbacks, one of them being the lack of security, such as the possibility of being attacked or hacked while operating online.

Some of the major threats, that lately bring a great deal of loss (financial, image, time, and so on), both upon persons and companies under attack, are: ransomware, malware, social engineering threats, threats against data, threats against availability (denial of service), crypto-jacking, threats against availability (internet threats), disinformation/misinformation, fake news, and supply-chain attacks [1].

Ransomware cyber-attacks can take a variety of forms, infiltrate victim systems in various ways, but they are all based on the same fundamental principle. After the attack, the victims are not able to access their own data (that are encrypted by the attacker) until they pay the required fee to the attacker. Usually, the attackers do not return data after the payment is made. After the first payment, there is a very high chance that the next time the attackers ask for an even higher amount. Even though a number of security mechanisms, such as firewalls, anti-virus programs, and automated analysis programs, have been developed to fight against this threat, in most of cases the current mechanisms are not able to guard data stored in local or cloud storage resources [2].

Phishing, as part of the social engineering cyberattack, has evolved (since 1995 when the first instance of this technique was reported, when attackers convinced victims to share their AOL account details [3]) into one of the most widespread and malicious forms of cybercrime in the world. The attack occurs when an attacker poses as an official entity to trick their targeted victim to divulging personal information (in an attempt to obtain sensitive information such as usernames, passwords, and credit card details, and money), often for malicious reasons, installing malware, or visiting a website that hosts malware [4].

A DDoS (distributed denial-of-service) attack is an attempt to interrupt the normal traffic of a server, service or network, by overwhelming it or the computing infrastructure, with a flow of traffic. Denial-of-Service (DoS) and DDoS attacks are serious threats both on local and cloud services' availability, due to numerous novel vulnerabilities (especially in cloud, where multi-tenancy and resource sharing are available) [5]. Attackers changed their attack format over the years, damaging operating systems and protocols in an attempt to deny or reduce the quality of the service provided to valid users. Today, attacks are sneakier and impersonate legitimate user in such a way that detection mechanisms of traffic against high – rate DoS attacks are no more appropriate. The LDoS (Low-rate Denial of Service) attack, has the potential to produce more damage than its predecessor due to its advanced nature and the lack of appropriate recognition and protection means. A most recent taxonomy divides DoS attacks in QoS attacks, Slow rate attacks, and Service queue attacks [6].

Crypto-jacking is a hazardous attack because it is silent and well-hidden. The victim has no clue that the malware is installed on his/her own device. Nothing happens and the victim still has access to their own device and data. The malware don't mine personal data, compromise files, ask for rewards, or crash computers. The purpose of crypto-jacking is to use the victim's computer's resources to create virtual currency. The only thing that gives evidence to victims about being under attack is the higher power consumption of the device. There are two main types of cryptojacking attacks; one requires a malicious payload to be installed on the user's computer and the other runs inside the user's browser upon visiting dubious web sites. More advanced methods exploit unpatched vulnerabilities, often zero-days to bypass the user entirely and install the payload. [7].

Powerful organizations spread fake news and a very large volume of disinformation through social networks and organizations-run media outlets, especially since current defenses must keep up with an increasing volume of Zero-Day types attacks [8].

The supply-chain attacks (targeting software or hardware) aim to damage an organization by pointing to less secure elements in the supply chain [9,10]. It can be launched towards any organization from the financial sector, oil industry, to the government sector. The attackers usually interfere within the manufacturing or distribution division of a product by compromising software (build tools or updated infrastructure), by steeling code-sign certificates or signed malicious apps using the identity of dev company, by compromising specialized code shipped into hardware or firmware components, or by pre-installing malware on devices (cameras, USB, phones, etc) [11, 12].

A software supply chain attack occurs when a third-party software dependency used in multiple 'downstream' applications is compromised. By compromising a single open-source package or library, attackers steal confidential data, cause a denial of service, or breach networks at thousands of organizations. This attack vector has become increasingly common, once the "Sunburst" attack in 2020 became widespread [13]. SUNBURST is a massive, fifth-generation cyber-attack, waged against US government agencies and technology companies. The attack compromised systems in over 40 government agencies, including the National Nuclear Security Administration (NNSA - the US agency responsible for nuclear weapons) and additional targets in other countries, including Canada, Belgium, Britain, and Israel, were also hit. The attacker hides a Trojan in a software update of the SolarWinds Orion software, and pushed this update to 18,000 customers, including almost all Fortune 500 companies, government agencies, and contractors including Lockheed Martin. They only discovered the attack in December, 2020, eight months after the original breach [14].

The most frequent attacks in Romania during 2022, have been ransomware, phishing, DDoS and others, as seen in Fig. 1.

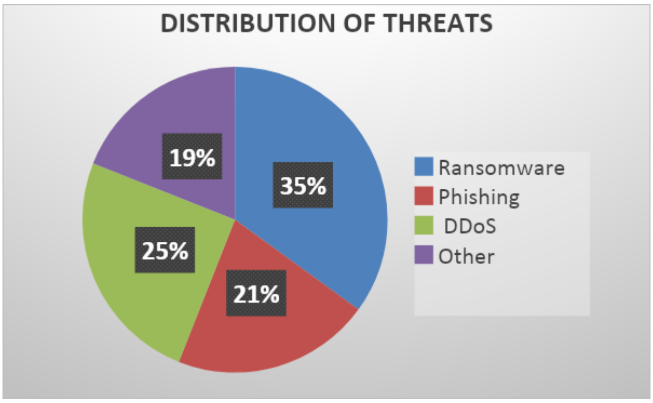


Fig. 1. Distribution of threats in Romania during 2022, by type [15]

1.1. Current Status Regarding Threats and Awareness Worldwide

One of the most distressing personal events that can result from being online is identity theft. According to Norton Cyber Safety Insights Report [16], conducted approximately 12 months (until February 2021), 55 million people have had their identity stolen. The Report that follows a survey conducted by The Harris Poll among 10,030 adults (aged 18 +) in 10 countries, shows that over 55% of internet users do not know what to do if their identity was stolen. Additionally, 60% of those surveyed admit to being "very worried" their identity will be stolen. According to the same report, people in India and the US are more likely to be taking more precautions online, while those in Japan are most likely to struggle with deciphering if the information is from a credible source.

What is more intriguing, the report shows that more than half of adults are more worried than ever about being the victim of cybercrime, but a similar proportion doesn't know how to protect themselves from it. More than 475 million consumers have ever been the victim of a cybercrime, nearly 330 million in 2021 alone [17].

As a response to those alarming results of the report presented above, the Norton Identity Advisor (as well as Norton™ Identity Advisor Plus [18] addresses this concern, by helping consumers each step of the way when they discover they're a victim of identity theft. It has an easy-to-use dashboard to register personal information for monitoring, including Social Media Monitoring that aim to monitor and also notify the account holder if there are signs the account is compromised or if potentially risky links are found. In case that the customer suspects an identity theft, a dedicated Identity Restoration specialist is available [19].

Any of the internet users can be a potential victim of malicious attacks, but recent research shows that small businesses are one of the most popular targets. In fact, small businesses are the target of approximately 43% of all cyber-attacks.

According to the public reports from Orange Business Services [20], the National Security Agency/Central Security Service [21] and the Cyber Security Agency of the European Union (ENISA) [22] there is published a relevant statistic for the year 2022 with the most common cyber-attacks in the online environment, concluding that "The year 2022 we all came under attack".

Hence, ransomware attacks represent approximately 31% of the total and target critical infrastructures in the HIPAA (Health Insurance Portability and Accountability Act) environment, i.e., the medical environment, also the private and public environment where personal data is encrypted or sold in "Black Market" [23].

Identifying cyber-attacks in most cases takes days, if not weeks or even months. As a result, small and medium-sized businesses must overcome these problems, therefore being aware of the most important cyber security dangers and knowing preventive measures that must be followed to reduce the risk of an incident, are compulsory for these companies.

1.2. Some Examples of Recent Cyber-Attacks Worldwide

A well-known case of ransomware attack was the attack on Colonial Pipeline, on May 7, 2021 where a ransom of around $5 million was paid [24] to regain access to files and data that have been encrypted. This company was the target of a group called DarkSide [25] They used this type of attack to steal 100 GB of data in less than 2 hours. This data includes payment data and confidential information held by the company [26].

In January, 2022 Crypto.com was hacked with some 500 wallets targeted. The malicious actors used a 2FA authentication attack to gain access. The hackers stole 33$ Million in cryptocurrency. The total value of the unauthorized withdrawals was 4,836.26 ETH and 443.93 BTC — equivalent to roughly $15.2 million and $18.6 million respectively, at current exchange rates — as well as $66,200 worth of other currencies [27].

In order to exploit the vulnerability regarding a breach (a Multiple Authentication - MFA fatigue), one of the biggest attacks was over the Uber company, in September, 2022. Although the attack on Uber was disruptive to their internal systems, no user data was compromised as part of the hack. The hackers initially gained access to Uber’s Slack messaging service and from there moved to the internal databases and then attackers gained access to the Uber Google Cloud account of Uber and the Uber Amazon Web Services (AWS) account. Although Uber got off easy from the attack, it should serve as a stern reminder that the human element is often the weakest link in security defenses. In the Uber attack, the victim was part of the incident response team and likely had some administrative privileges. Through these privileges, the attacker gained access to a file with other credentials giving them essentially the keys to the kingdom [28].

This attack takes advantage of users whose login credentials have been compromised, bombarding them with authorization requests until they give in and approve one. An MFA attack is based on the fact that people have trust in this procedure as being a protective one. When users try to connect to MFA-protected resources, they usually receive a push notification or a code to confirm their credentials. Users respond to these alerts believing that they are being granted permission to access resources. Since this procedure exploits users’ trust, they do not expect their own organization's MFA platform to betray them. This caused one of the biggest data leaks and mass layoffs.

One of the major breaches in Thailand’s history, records of 39 million patient from Bangkok’s Siriraj Hospital have been offered for sale on a dark web forum. The attacker followed up by posting on raidforums.com that goes under the name of “WraithMax” offered to sell the data and supply a sample file via Telegram. The poster claims the data includes names, addresses, Thai IDs, phone numbers, gender details, dates of birth and other information [29].

A „very elaborated” attack compromised The International Committee of the Red Cross servers, attackers compromised data of more than 515.000 “highly vulnerable persons" including those separated from their families due to conflict, migration and disaster, missing persons and their families, and people in detention [30].

The war in Ukraine (that started on 24th of February, 2022) significantly changed the threat scenery in 2022. There have been noticed important changes in hacktivist activity, cyber actors conducting operations along with kinetic military action, the mobilization of hacktivists, cyber-crime, and aid by nation-state groups during this conflict [31].

The Orange Business Internet Security Report [15] publishes a very interesting report regarding various cyber-attacks worldwide, during 2022, that seriously affected organizations in several regions worldwide and a number of professional areas.

All these attacks brought into focus the importance of insider threats monitoring and security.

At the beginning of the year, in Germany, two oil supply companies said they were victims of the cyberattack since Saturday January 29. Both companies declared force majeure. At the beginning of February, Belgian prosecutors launched an investigation into the hacking of oil facilities in the country's maritime entryways, including Antwerp, Europe's second biggest port after Rotterdam.

In Germany, prosecutors said they were investigating a cyberattack targeting oil facilities in what was described as a possible ransomware strike, in which hackers demand money to reopen hijacked networks [32].

In February 2022, (the 7th), Swissport, an important aviation operations company (that provides services to many airports across Europe) was a victim of ransomware in an attack that caused flight disruptions for at least 22 scheduled flights [32].

In February (the 8th) this year, Vodafone Portugal was the victim of a deliberate and malicious cyberattack intended to cause damage and disruption. The company's 4G and 5G mobile networks, along with fixed voice, television, SMS, and voice/digital answering services were all offline following the attack [33].

One of the world's biggest private banks, Credit Suisse was the victim of a data leak, with confidential information on more than 18.000 bank accounts, gathering some 100$ Billion in wealth, was leaked to a German Newspaper by a whistle-blower [34].

Hackers leaked a large collection of data exfiltrated from Samsung Group's Systems, including source code of applets and system components in use in sensitive environments. On 7th of March, 2022, Samsung today confirmed a breach of its systems, reportedly the work of hacking gang Lapsus$, which saw 190GB of the South Korean electronics company's data, including source code for its Galaxy devices, leaked online. The attack came days after Lapsus$ breached another Big Tech business, chipmaker Nvidia. While both incidents appear to have been mercenary in nature, security researchers believe the gang could be pursuing another agenda too [35].

France's Caisse Nationale D'assurance Maladie (CNAM) health insurance body, made a formal complaint, explained that, in March 17th, 2022, "unauthorized people" had connected to the "Amelipro accounts" of the healthcare workers whose "email addresses had been compromised". It shows that the accounts of 19 healthcare staff had been hacked, causing the details (names, surnames, date of birth, social security numbers, GP details) of at least 510.000 people to be stolen [36].

A brute-force DDoS attack over Finland's Ministry of Defense's website was launched during April 2022. The attack caused minor availability issues for the web portals, and the operators managed to restore their websites in short time [37].

A dataset containing user data for more than 21 million users of several VPN services, was leaked on Telegram. The data contains names, usernames, hashed passwords and e-mail addresses of GeckoVPN, SuperVPN and ChatVPN clients [38].

In May, 2022, a German library was crippled by ransomware. Customers were unable to rent audio books, digital copies of magazines, e-books, nor were able to make requests online or by phone. The attack severely affected Onleihe, a popular app that connects users via EKZ's service to local libraries German Library Service crippled by ransomware, in an attack orchestrated by the Lockbit ransomware group, who then published the data they exfiltrated during the attack, claiming their ransom requests have not been met [39].

The NFT marketplace OpenSea, had a data breach after an employee of the company’s e-mail delivery vendor, misused their employee access to download and share email addresses provided by OpenSea users with an unauthorized external party” [40].

The Pegasus Airline company used an unsecured AWS Bucket (bucket is a container for objects stored), and exposed 6.5 TB of data consisting of personal information of flight crews. The EFB bucket was misconfigured to allow open access from the internet [41].

In May 2022, exploiting a misconfiguration, a triple ransomware attacked an automotive supplier, exposing RDP through a border firewall. LockBit, Hive and BlackCat – the three culprits – have encrypted files (some files were encrypted at least 3 times each), the attack lasted for more than 2 weeks [42].

In June, the 1st, 2022, Costa Rica’s Public Health services went offline after ransomware attack. The Hive Ransomware was the culprit, with the initial breach happening some 3 days before the report was published. The employees of the Public Health agencies targeted by the ransomware were instructed to “unplug their computers” in order to prevent the malware from spreading through their networks. [43]

Using a Zero-Day Vulnerability in the software stack, Twitter was also breached in July, 2022. That breach allowed the attackers to associate usernames with e-mail addresses and registered phone numbers. The hackers generated a dataset of more than 5.4 million affected user profiles [44].

The virtual pet website Neopets has suffered multiple data breaches since its inception and transfer from Viacom to JumpStart Games in 2014, 2016, and 2020. On 27th of July, 2002, suffered a data breach exposing a database containing personal information (players’ names, gender, dates of birth, usernames, email addresses, IPs, countries, and zip codes) of 69 million users. The website reported that the attackers exfiltrated source code of its software products [45].

In August, the 12th, 2022, a hacker obtained the personal information of 48.5 million users of a COVID health mobile app run by the city of Shanghai. This was the second claim of a breach of the Chinese financial hub's data in just over a month. The hacker with the username as "XJP" also posted an offer to sell the data for $4,000 on Breach Forums [46].

According to Romanian National Directorate of Cyber Security and Response to Incidents (DNSC) that released a report regarding cybersecurity attacks in Romania, a series of DDoS attacks targeting the following Romanian government websites [47] have been developed this year:

- gov.ro (the official website of the Government of Romania);
- mapn.ro (the official website of the Ministry of National Defense of Romania);
- politiadefrontiera.ro (the official website of the Border Police);
- cfrcalatori.ro (the official website of the Romanian railways);
- otpbank.ro (the official website of OTP Bank).

Although the examples above are far from being close to the real number of different cyberattacks during 2022 only, it shows that no organization is safe enough online these days and can become the victim of any kind of malicious cyber-attack. So, as many cyber-security measures and personalized procedures are implemented in organizations, the safer their data are.

Hence, no matter the model of business we are involved in, or technology we use [48-50] is essential to be aware of treats and follow the experts' advice and the advanced tools available against cyber- attacks.

1.3. Methods to Prevent Cyber-Attacks

Cyber-attacks are now the fastest growing crime on a global scale. Since the volume and effects of cyber threats continue to accelerate, it has never been more important for individuals and organizations to address emerging threats and to mitigate possible troubles. With a great certainty of the cyber-attacks to come, the need to take a more forward-thinking attitude is compulsory. The Future of Cyber Security aims to help businesses to stay one step ahead of cyber attackers through a number of insightful sessions [51].

Protecting critical assets or networks from disruption or attack is one of the primary concerns in both cyber-security and risk analysis. When these two fields intersect the concept of cyber resilience is born, which can simply be defined as an entity's ability to plan for, absorb, recover from, and successfully adapt in the face of adverse cyber events [52].

According to the standards imposed by NIST (National Institute of Standards and Technology) and ISO/IEC 207001 (International Organization for Standardization and the International Electrotechnical Commission), there are some good practices useful both to people who use an IT system and to organizations to prevent potential cyber-attacks:

- The use of a password manager to create and retain unique and complex passwords for each account;
- To implement two-step authentication for the online accounts whenever possible. This option is offered now by banks, social media platforms, e-commerce platforms and so on. Two-step authentication involves two steps, (as the name suggests) entering the password and then, a unique access code that is received on a different device (the phone, for example;
- To protect the internet browsing activity as every internet action is tracked by businesses and websites. The location, browsing history, and other data are collected by every ad, social button, and website. The data collected reveals more about personal identity than might be expected. Is possible that the websites visited are regularly providing all the data advertisers need to identify the type of person/customer/audience the client is. This is part of how targeted advertising remains one of the Internet's most disturbing innovations;
- To use antivirus software on the computer and keep it up to date. As an organization, it is recommended to perform regular security audits (vulnerability assessment and penetration testing, etc.);
- To use protection technologies such as firewalls, cloud WAF services, periodic backups, and monitoring agents connected to a Security Operation Center (SOC);
- It is recommended for organizations to have well-established procedures regarding "Risk Management" [53].

There are some important procedures and steps to be followed by security responsible in organizations to avoid such disturbing situations (ransomware attacks) that the organizations or individuals can face.

Therefore, a specific procedure for a regular backup of all personal data and data related to the company's activities, is compulsory to be defined and followed, especially to avoid any loss in case of a ransomware event. A periodic audit to prevent attack vectors has to be performed in companies. A cyber risk awareness program has to be developed and employees must be trained accordingly.

The Internal Security Rule Planning of the organization must restrict (and even forbid in some special situations) the use of peripheral devices (or external storage supports) as much as possible. An organization’s cyber-security responsible must stay up to date with the latest news in the field and in the event of a cyber-attack report the situation to official entities that can assist and help, before making any payment to the attackers or implementing a protection system.

To protect the organization from phishing attacks, the following actions is compulsory to be implemented:

- One of the most important steps that can be taken to defend an organization against this type of attack, is to train employees and establish certain standards, and develop periodic simulations;
- Employees should be given proper and periodic training so they recognize various phishing patterns and strategies;
- The awareness of the employees/future possible victims, to identify what is malicious in the online environment and what is not, is the greatest resource of prevention to avoid such attacks becoming efficient for attackers. It all depends on how well-prepared and informed are the targeted victims in the online environment and the dangers that exist in this environment.

Mitigating a multi-vector DDoS attack requires a variety of strategies to counter the different trajectories. In order to protect organization against Distributed Denial of Service attacks, the following actions are compulsory:

- The first step, as a compulsory act, is to check that the service provider is prepared for an overload of allocation resources;
- To monitor the DoS and DDoS attacks and test equipment against such an attack (Stress Testing);
- To reduce the attack surface, including the exposure of the ports and protocols used in the Internet, as little as possible;
- To use a cloud service that allows quick access to resources and back-up restoration in record time.

2. Malware Analysis and Threat Hunting

2.1. Malware Analysis Procedure

In order to analyze or identify malware, a study on the infected system is required first. The best method against these attacks is based on "The Cyber Kill Chain" [54] when the Security Engineer needs to think like a bad intruder.

The Cyber Kill Chain contains few steps to be followed:

- Reconnaissance is the first step of investigation as part of a malicious attack when data about the target is gathered, such as what type of technology is used, the e-mail addresses, user IDs, physical locations, software applications, and operating system details, and any other kind of information that might be useful in phishing or spoofing attack;
- Weaponization is the second step that an attacker would follow to create the malware, virus, or worm that can exploit a known vulnerability;
- Delivery is the third step of the process when the intruder launches the attack;

- Exploitation is the phase when the malicious code is executed within the victim’s system;
- Installation procedure follow when malware or other attack vectors will be installed on the victim’s system like rootkit or backdoor;
- Command and Control is the phase when the attacker is able to use the malware to assume remote control of a device or identity within the target network;
- Actions based on Objective is the final phase when the attacker reaches the objective, naming data theft, destruction, encryption or exfiltration.

Although difficult to accept, every cyber-attack leaves a trace. These traces in technical terms are called "Indicators of Compromise (IOC)" [55]. Based on the procedures mentioned above, an analyst starts from the initial problem and looks for similarities such as: where the malware connects, what files are modified in the system, what new processes have been developed in the system, what applications the malware tries to install, etc.

For a better prevention procedure, a Security Operations Center has well-defined plans to be aware of how to act according to each individual attack's particularities. Under the given conditions, the analyst follows the analysis phases described in PICERL (Prepare, Identify, Contain, Eradicate, Recover, and Lessons Learned) [56].

PICERL (Fig. 2) is a plan recommended by all security training institutions regarding the management of activities in the event of an incident:

- Preparation - refers to the capability of the cyber-security team to respond quickly in case of an incident by knowing all the procedures in case of a cyber security attack and having all the tools for action. They have full access (all the rights) in the network to complete the investigation and ensure that no law interferes with the activity of the analyst to hinder or stop him. Also, the continuous education that analyst takes in case of exceptional events is important and must be provided by the company or by an up-to-date, specialized organization;
- Identification - follows the analysis of the incident, the analyst must find out what happened, when it happened, if the user was compromised, what changes were created on the system, what internet connections were made, what he download-ed, where he made the persistence and what subsequent behavior it may have if it tried to connect to other stations in the network with the aim of compromising them. From this perspective, being only a phishing analysis, the focus is strictly on the analysis of metadata from the mail as well as attachments or added URLs;
- Containment is the phase when steps are taken with the aim to stop the spread of the infection. Domains used in case of infection will be blocked, and hashes of malware samples used to infect systems are also blocked;
- Eradication follows when the analysis has already been completed, and attempts are made to eliminate all systems that have been compromised. In the case of phishing e-mails, the victims are asked to delete them from the mail servers;
- Recovery phase is considered when the incident is over and attempts are made to bring all the stations that were isolated upstate;
- Lessons learned is maybe the most important step of the PICERL procedure. In this state, the incident is resolved and the conclusions drawn must prevent future infections. The discussion here can vary from applied patches, redone configurations, or extra rights for analysts.

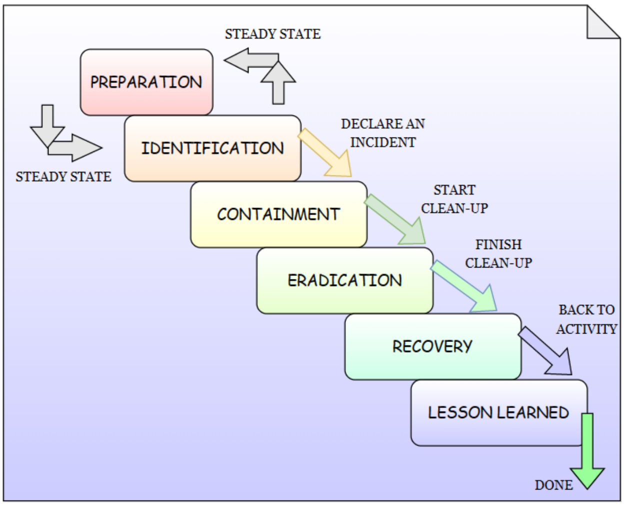


Fig. 2. PICERL Phases of incident response [57]

Malware analysis is extremely important as it helps individuals as well as organizations to identify if a specific file is malicious or not. It provides all information regarding the origin of the file, the processes behind it, and its capabilities and can help identify if the file is legit.

Based on the incident management model, we refer here to all the above-mentioned phases, less the identification step involving e-mail analysis. Regardless of the tools used, the process is the same, following certain steps in extracting information and making a decision if the file or URLs are malicious or not:

- The first step, a look at the body of the e-mail is necessary to analyze the message, to see if the one who sent the e-mail is trying to convince the recipient to take a certain action for his own benefit. Most of the time attackers use social engineering techniques, taking advantage of human weaknesses such as curiosity, listening spirit, etc. The URLs and attachments sent with the e-mail in question will also be extracted, and will later be analyzed.
- The second step is to analyze the email header since it is necessary to look for the following artifacts: Message-ID and Hops. The Message ID is a field that provides a unique identifier of the message that refers to a certain particular version of a message. Hops–represents the route followed by the mail until it reaches the destination mail server.

Thus, it is represented by the 'Received' field. Forefront Antispam Report Header – after an antispam solution has scanned the mail that was sent, inserts the 'Forefront Antispam' field containing additional information about the mail and how it was processed such as country of origin of the message, language in who wrote the message, and other reports on security measures plus scores that allowed the mail to pass. Authentication results–Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC) [58].

SPF is an authentication protocol that lists IP addresses in a DNS TXT record that are authorized to send e-mails on behalf of domains.

DKIM is an ID or passport that can verify identity. When it is sent from an e-mail server, the server attaches DKIM so the receiving server can verify. Therefore, DKIM authentication provides a method for validating a domain's identity that is associated with a message through cryptographic authentication. It does this by using an encrypted key pair (one public in DNS and one private) to add a digital signature to every email message. Receiving email servers use this DKIM signature to both validate the authenticity of the sender, and detect if the message was altered/changed during transit. DKIM-signed messages provide Mailbox Providers (MBPs) with trust that the message is authentic and is not being spoofed. MBPs' internal filtering algorithms use SPF and DKIM along with other factors to determine if an email should be placed in the inbox, or spam folder, or be rejected. However, both SPF and DKIM don't allow domain owners to instruct MBPs how to treat a message if the authentication checks can't be validated. To help tell MBPs to know what to do if DKIM and/or SPF fail, senders can implement DMARC. DMARC leverages both SPF and DKIM and provides instructions from the domain owner about what to do with unauthenticated email [59].

DMARC is an email authentication, policy, and reporting protocol. It helps domains address domain spoofing and phishing attacks by preventing unauthorized use of the domain in the Friendly-From address of email messages.

DMARC allows the domain owner to specify how unauthenticated messages should be treated by MBPs. This is accomplished by what is known as a "policy" that is set in the DMARC DNS record. The policy can be set to one of three options: NONE, QUARANTINE, and REJECT.

- Policy = (p=none): no action and message delivered as normal;
- Policy = (p=quarantine): places the message to spam/junk/quarantine folder;
- Policy = (p=reject): the message rejected/bounced.

The R in DMARC is for the Reporting component of the protocol. These reports allow the domain owner to see where all email using their domain in the form address is being sent from [59].

The recipient, the sender, and the subject of the mail are also identified. At this point, a conclusion can be drawn in case there is an inconsistency between the servers the mail originated from and what the message is, the sender, and what the attacker is trying to trick the victim into doing.

This is the step of the procedure when the analysis must be focused on attachments. The analysis can be statically or dynamically according to certain well-defined malware analysis rules. Her free attachment or URL analysis tools can be used. The necessary step to be made is the analysis of the URLs in question, looking for indicators of compromise: HTML 'href' tags or javascript 'iframes'.

At the same time, what the page displays is also important to draw a conclusion in case an URL is in the mail or a malicious attachment.

2.2 Customize Personal Application for Threat Hunting

A "Thread Hunting" application must be dedicated mainly for the purpose of identifying potentially malicious content. The application must be easy to use for those who analyze bad threads. Another requirement that an application must meet is scalability. This is most important to keep the product on the market and to be able to be upgraded with the latest detection methods.

The application presented in our demo example has the possibility to implement open-source tools and execute their detection rules. Each function has been containerized with docker in order to provide both the flexibility to be used on any type of platform and to be easily modified by adding new functions or removing existing detection functions.

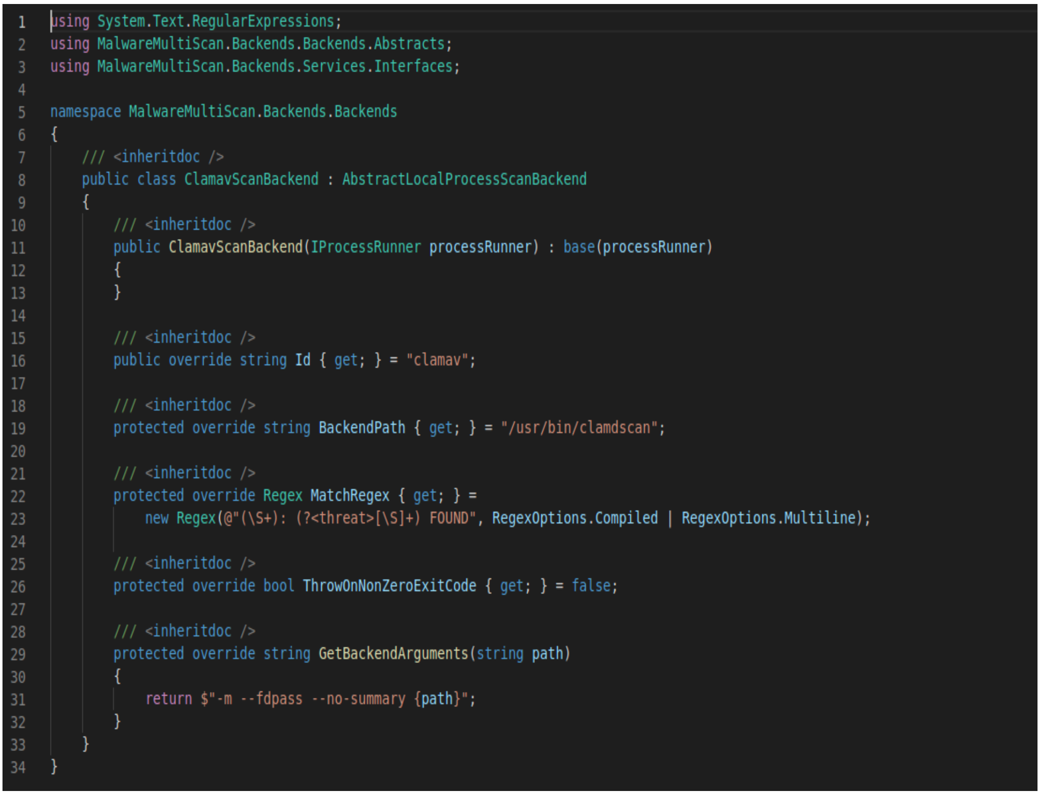
Based on a containerization model, the application can be easily changed (scalability) so that it can be used either as a file filter or as a plugin for customers.

The application, regardless of the model chosen for use, receives as input a file with the extension of word *.doc, or *.exe, or *.elf, etc.

The application analyzes the content of the malicious file using the ClamAV Scan [60] utility to get as many suspicious indicators about the nature of the file, from the analysis of the headers to the analysis of Windows_API.

This will give the analyst an overview of what is being analyzed in case there are specific indicators.

In Fig. 3 is presented a part of the code that is incorporated in the software and uses an open-source tool like clamav.

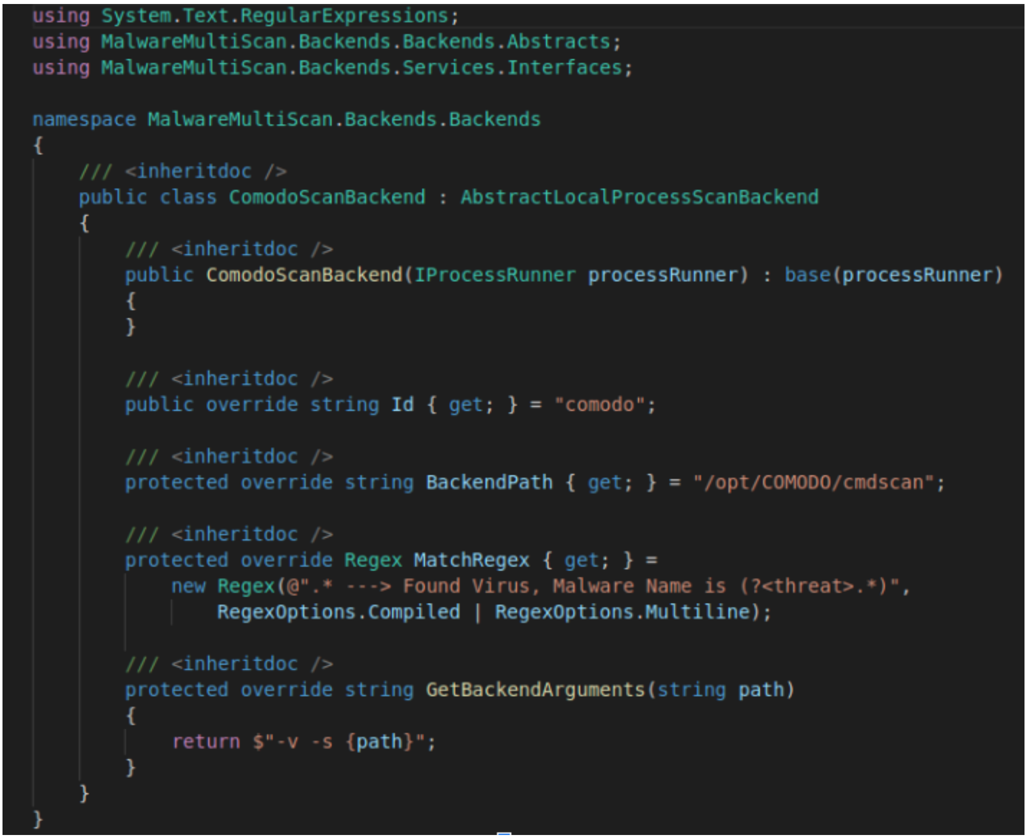


```
using System.Text.RegularExpressions;
using MalwareMultiScan.Backends.Backends.Abstracts;
using MalwareMultiScan.Backends.Services.Interfaces;

namespace MalwareMultiScan.Backends.Backends
{
    /// <inheritdoc />
    public class ClamavScanBackend : AbstractLocalProcessScanBackend
    {
        /// <inheritdoc />
        public ClamavScanBackend(IProcessRunner processRunner) : base(processRunner)
        {
        }

        /// <inheritdoc />
        public override string Id { get; } = "clamav";

        /// <inheritdoc />
        protected override string BackendPath { get; } = "/usr/bin/clamdscan";

        /// <inheritdoc />
        protected override Regex MatchRegex { get; } =
            new Regex(@"(\S+): (?<threat>[\S]+) FOUND", RegexOptions.Compiled | RegexOptions.Multiline);

        /// <inheritdoc />
        protected override bool ThrowOnNonZeroExitCode { get; } = false;

        /// <inheritdoc />
        protected override string GetBackendArguments(string path)
        {
            return $"-m --fdpass --no-summary {path}";
        }
    }
}
```

Fig. 3. Example of code

The application has implemented several scanners such as: Comodo (comodo is a tool based on Endpoint Detection and Response) [61], DrWebScan (similar website like virustotal), DummyScan (based on Yara rules scanner), KesScan (tool by Kaspersky), McAfeeScan (Antivirus) SophosScan and WindowsDefender (solution for detection by Microsoft).

In Fig. 4 is open-source Comodo (EDR) integration.



```
using System.Text.RegularExpressions;
using MalwareMultiScan.Backends.Backends.Abstracts;
using MalwareMultiScan.Backends.Services.Interfaces;

namespace MalwareMultiScan.Backends.Backends
{
    /// <inheritdoc />
    public class ComodoScanBackend : AbstractLocalProcessScanBackend
    {
        /// <inheritdoc />
        public ComodoScanBackend(IProcessRunner processRunner) : base(processRunner)
        {
        }

        /// <inheritdoc />
        public override string Id { get; } = "comodo";

        /// <inheritdoc />
        protected override string BackendPath { get; } = "/opt/COMODO/cmdscan";

        /// <inheritdoc />
        protected override Regex MatchRegex { get; } =
            new Regex(@".* ---> Found Virus, Malware Name is (?<threat>.*)",
                RegexOptions.Compiled | RegexOptions.Multiline);

        /// <inheritdoc />
        protected override string GetBackendArguments(string path)
        {
            return $"-v -s {path}";
        }
    }
}
```

Fig. 4. An open-source Comodo (EDR) integration

Using open-source tools as well as open threat intelligence feeds, we can categorize the file as malicious or not based on the results after the analysis.[62-67]

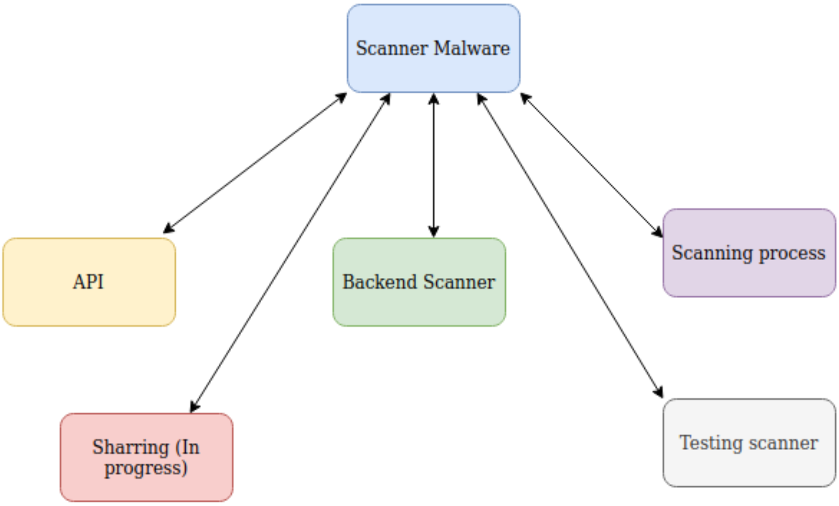


Fig. 5. The diagram of software

To create this application, we used what the mentioned above methodology, “The Cyber Kill Chain” [68]:

1. Reconnaissance: In this stage, the attacker/intruder chooses their target. Then they conduct in-depth research on the target to see specifics and to identify available vulnerabilities that can be exploited.
2. Weaponization: In this step, the intruder creates a malware weapon like a virus, worm or such in order to exploit the vulnerabilities of the target. Depending on the target and the goal of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or it can focus on a combination of different vulnerabilities.
3. Delivery: This step involves sending the weapon to the target. The intruder/attacker can use different methods like USB drives, e-mail attachments and websites for reaching his purpose.
4. Exploitation: In this step, the malware activity starts. The program code of the malware is triggered to exploit the target’s vulnerability/vulnerabilities.
5. Installation: In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.
6. Command and Control: The malware gives the intruder/attacker access in the network/system.
7. Actions on Objective: Once the attacker/intruder gains persistent access, they finally take action to fulfill their purpose, such as encryption for ransom, data exfiltration or even data destruction.

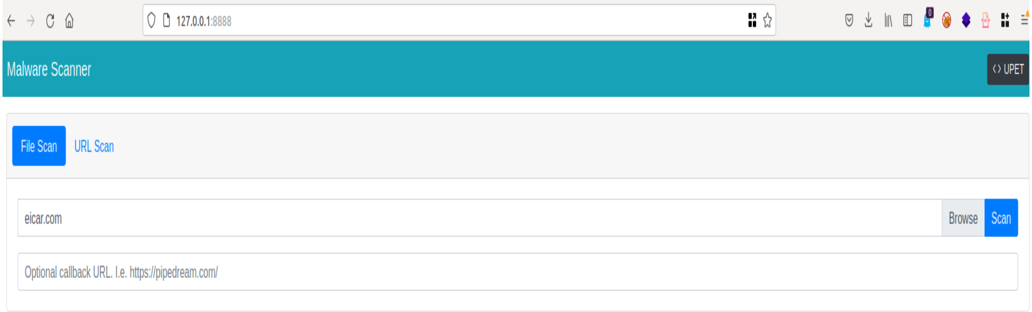
For better detection/evasion techniques it is important to examine the components of the operating system and how different tools interact with those components.

In case that a detection is too sensitive, then the monitoring procedure takes too much because the team is flooded with false positives and the analysts waste time or the potential burn out.

On the other hand, if the detection rule is too specific, then evasion becomes trivial to achieve for the attacker.

Therefore, an evasion engineer's goal is to conduct their operation while avoiding preventative and potentially detective controls. In order to do this, it is important to understand what aspects of the attack the attacker has control of.

In the following demo. we are uploading a malicious file like malware but keep in mind examples presented here are not to harm any informatic system.



127.0.0.1:8888

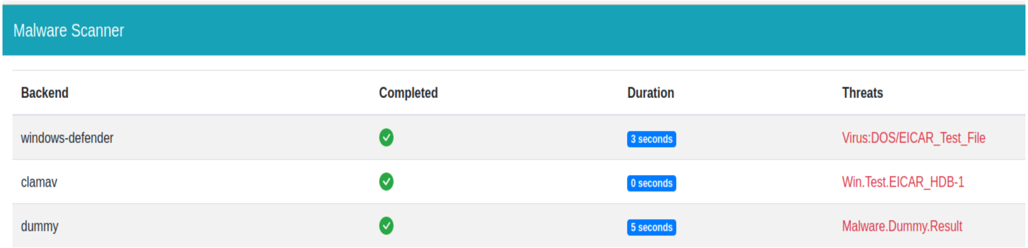
eicar.com

Optional callback URL. I.e. https://pipedream.com/

Fig. 6. Upload malicious file

The application works with a series of APIs that link the application to open-source tools and activate them. Therefore, the executable uploaded to the platform is analyzed based on a public database. Once the application hash is verified, it shows if the application is malicious or not.

But that's not all, there's also a sandbox behind it that tries to detonate the executable to see how it responds. In Fig. 7, the result can be seen [60-68].



Malware Scanner

Backend	Completed	Duration	Threats
windows-defender	✓	3 seconds	Virus:DOS/EICAR_Test_File
clamav	✓	0 seconds	Win.Test.EICAR_HDB-1
dummy	✓	5 seconds	Malware.Dummy.Result

Fig. 7. Result based on the custom scanner

3. Conclusions

In this paper, we took a broad overview of malicious attacks during this year, the results of these attacks, and the preventive measures to avoid unwanted situations and their results following cyber-attacks. We present an application that should assist enthusiasts in malware analysis to reach a quick and efficient conclusion on attachments or on the malware spread vector, or to protect companies that use certain services both locally and remotely. We designed the application to be used from the command line as a stand-alone tool where an executable file of *.exe or *.elf types are given as input. The application developed here solves the compatibility problem of operating systems based on Linux or Windows with the help of the Docker engine. The main purpose of this application is to facilitate the analysis of executable files. The application is also extremely useful because both it and the technologies used are open sources, which allows further improvements in time.

References

1. European Union Agency for Cybersecurity, ENISA Threat Landscape NOVEMBER 2022, ISBN: 978-92-9204-588-3, DOI: 10.2824/764318.
2. Ilker Kara, Murat Aydos., The rise of ransomware: Forensic analysis for windows-based ransomware attacks, Expert Systems with Applications, Volume 190, 2022, ISSN 0957-4174, https://doi.org/10.1016/j.eswa.2021.116198.
3. Jakobsson, M.; Myers, S. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft; Wiley: Hoboken, NJ, USA, 2006. 3. Rekouche, K. Early Phishing. arXiv 2011, arXiv:1106.4692
4. Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. Future Internet, 12(10), 168. doi:10.3390/fi12100168
5. Bonguet, A., & Bellaiche, M. (2017). A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. Future Internet, 9(3), 43. doi:10.3390/fi9030043
6. V. D. M. Rios, P. R. M. Inácio, D. Magoni and M. M. Freire, "Detection and Mitigation of Low-Rate Denial-of-Service Attacks: A Survey," in IEEE Access, vol. 10, pp. 76648-76668, 2022, doi: 10.1109/ACCESS.2022.3191430.
7. Askarov, A., Hansen, R. R., & Rafnsson, W. (Eds.). (2019). Secure IT Systems. Lecture Notes in Computer Science. doi:10.1007/978-3-030-35055-0
8. W. Shahid et al., "Detecting and Mitigating the Dissemination of Fake News: Challenges and Future Research Opportunities," in IEEE Transactions on Computational Social Systems, doi: 10.1109/TCSS.2022.3177359
9. Maria Kotolov (4 Feb 2021) Supply chain attacks show why you should be wary of third-party providers, https://www.csoonline.com/,
10. [Online] https://learn.microsoft.com/

11. [Online] https://learn.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide,
12. Urciuoli, L., Cyber-Resilience: A Strategic Approach for Supply Chain Management, Technology Innovation Management Review; Ottawa Vol. 5, Iss. 4, (Apr 2015): 13-18.
13. [Online] https://portswigger.net/daily-swig/supply-chain-attacks
14. [Online] https://www.cynet.com/attack-techniques-hands-on/sunburst-backdoor-c2-communication-protocol/
15. Orange Business Internet Security Report 5th edition, 2022, https://newsroom.orange.ro/orange-business-services-lanseaza-raportul-business-internet-security-2022/
16. [Online] https://us.norton.com/blog/id-theft
17. [Online] https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf
18. [Online] https://uk.norton.com/products/identity-advisor-plus.
19. [Online] https://www.prnewswire.com/news-releases/norton-launches-robust-identity-monitoring-in-the-uk-to-help-consumers-resolve-their-identity-theft-issues-301502907.html
20. [Online] https://www.orange.ro/docs/business/pdf/Business-Internet-Security-Report-5th-edition-2022.pdf
21. [Online] https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/
22. [Online] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
23. [Online] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html
24. Perlroth, Nicole (May 13, 2021). "Colonial Pipeline paid 75 Bitcoin, or roughly $5 million, to hackers". The New York Times. Retrieved May 13, 2021.
25. Helmore, E. (May 10, 2021). "FBI confirms DarkSide hacking group behind US pipeline shutdown". The Guardian. Archived from the original on May 12, 2021. Retrieved May 10, 2021
26. Walsh, Joe. "Ransomware Attack Shuts Down Massive East Coast Gasoline Pipeline". Forbes. Retrieved February 6, 2022.
27. [Online] https://www.theverge.com/2022/1/20/22892958/crypto-com-exchange-hack-bitcoin-ethereum-security
28. [Online] https://veruscorp.com/mfa-fatigue-leads-to-breach-of-ubers-corporate-systems/
29. [Online] https://informationsecuritybuzz.com/38-9m-health-records-stolen-from-bangkok-hospital/
30. [Online] https://www.orange.ro/docs/business/pdf/Business-Internet-Security-Report-5th-edition-2022.pdf
31. European Union Agency for Cybersecurity, ENISA Threat Landscape NOVEMBER 2022, ISBN: 978-92-9204-588-3, DOI: 10.2824/764318
32. [Online] https://www.securityweek.com
33. https://therecord.media/cyberattack-brings-down-vodafone-portugal-mobile-voice-and-tv-services/
34. [Online] https://www.theguardian.com/news/2022/feb/20/
35. [Online] https://techmonitor.ai/technology/cybersecurity/lapsus-big-tech-samsung-nvidia
36. [Online] https://www.connexionfrance.com/article/French-news/French-health-insurance-data-leak-what-to-do-if-you-are-affected
37. [Online] https://www.infosecurity-magazine.com/news/finland-government-sites-offline/
38. [Online] https://www.spiceworks.com/it-security/data-security/news/data-of-millions-of-vpn-users-leaked/
39. [Online] https://www.itgovernance.eu/blog/en/cyber-attacks-and-data-breaches-in-review-may-2022
40. Hardman C., Important Update on Email Vendor Security Incident, https://opensea.io/blog/articles/important-update-on-email-vendor-security-incident
41. Glover C., Pegasus Airline breach sees 6.5TB of data left in unsecured AWS bucket, https://techmonitor.ai/technology/cybersecurity/pegasus-airline-data-breach-aws-bucket
42. Smith L., Wason R., Zaidi S., Lockbit, Hive, and BlackCat attack automotive supplier in triple ransomware attack, https://news.sophos.com/en-us/2022/08/10/lockbit-hive-and-blackcat-attack-automotive-supplier-in-triple-ransomware-attack/
43. Page C., Costa Rica’s public health system hit by Hive ransomware following Conti attacks, https://techcrunch.com/2022/06/01/costa-ricas-public-health-system-hit-by-hive-ransomware-following-conti-attacks

44. Abrahams, L., Twitter confirms zero-day used to expose data of 5.4 million accounts, https://www.bleepingcomputer.com/news/security/twitter-confirms-zero-day-used-to-expose-data-of-54-million-accounts/
45. Hope, A. Data Breach on Virtual Pet Website Neopets Affected 69 million Users and Leaked Source Code, https://www.cpomagazine.com/cyber-security/data-breach-on-virtual-pet-website-neopets-affected-69-million-users-and-leaked-source-code/
46. Baptista, E. Hacker offers to sell data of 48.5 million users of Shanghai's COVID app, https://www.reuters.com/world/china/hacker-offers-sell-data-485-mln-users-shanghais-covid-app-2022-08-12/
47. [Online] https://dnsc.ro/citeste/comunicat-site-uri-ro-afectate-de-un-atact-de-tip-ddos
48. S. Riurean, M. Leba and L. Crivoi, "Enhanced Security Level for Sensitive Medical Data Transmitted through Visible Light," 2021 International Symposium on Networks, Computers and Communications (ISNCC), 2021, pp. 1-6, doi: 10.1109/ISNCC52172.2021.9615732
49. Riurean, S. A study on the VLC security at the physical layer for two indoor scenarios, MATEC Web of Conferences; Les Ulis, Vol. 342, (2021). DOI:10.1051/matecconf/202134205009
50. Riurean Simona, Robert Alexandru Dobre, Alina-Elena Marcu, Security and propagation issues and challenges in VLC and OCC systems, Proceedings Volume 11718, Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X; 117182B (2020) https://doi.org/10.1117/12.2572029
51. [Online] https://www.cshub.com/
52. Hausken, K. Cyber resilience in firms, organizations and societies. Internet Things 2020, 11, 100204, doi: 10.1016/j.iot.2020.100204
53. [Online] [https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
54. [Online] https://www.sentinelone.com/cybersecurity-101/cyber-kill-chain/
55. [Online] https://abnormalsecurity.com/glossary/indicators-of-compromise
56. https://www.sans.org/media/score/504-incident-response-cycle.pdf
57. https://playbooks.flexibleir.com/incident-response-phases-best-practices/
58. [Online] https://www.techtarget.com/searchsecurity/answer/Email-authentication-How-SPF-DKIM-and-DMARC-work-together
59. [Online] https://www.higherlogic.com/blog/spf-dkim-dmarc-email-authentication/
60. [Online] https://www.clamav.net/
61. [Online] https://github.com/ComodoSecurity/openedr
62. [Online] https://vms.drweb.com/online/?lng=en
63. [Online] https://dto.to/group/11539
64. [Online] https://support.kaspersky.com/KES4Linux/11/en-US/177138.htm
65. [Online] https://www.mcafee.com/en-us/antivirus/mcafee-security-scan-plus.html
66. [Online] https://www.sophos.com/en-us/free-tools/virus-removal-tool
67. [Online] https://www.microsoft.com
68. [Online] https://www.lockheedmartin.com/

Aims and Objectives

Published online by ICS two times a year, Journal of Digital Science (JDS) is an international peer-reviewed journal which aims at the latest ideas, innovations, trends, experiences and concerns in the field of digital science covering all areas of the scholarly literature of the sciences, social sciences and arts & humanities. The main topics currently covered include: Artificial Intelligence Research; Digital Economics, Education, Engineering, Finance, Health Care.

The main goal of the journal is the effective dissemination of original incites/results generated by the human brain and presented/reflected in articles using modern information/digital technology.

Editorial Board

Contact information

Website: https://ics.events

Email: conf@ics.events