electronics

MDPI

Systematic Review

Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges

José Antonio Gómez Hernández*,†,‡, Pedro García Teodoro †,‡, Roberto Magán Carrión † and Rafael Rodríguez Gómez †

Network Engineering & Security Group, University of Granada, 18071 Granada, Spain; pgteodor@ugr.es (P.G.T.); rmagan@ugr.es (R.M.C.); rodgom@ugr.es (R.R.G.)

* Correspondence: jagomez@ugr.es; Tel.: +34-958-240-572

† Current address: Network Engineering & Security Group (NESG), ETSIIT, C/Periodista Daniel Saucedo Aranda s/n, 18071 Granada, Spain.

‡ These authors contributed equally to this work.

Abstract: According to the premise that the first step to try to solve a problem is to deepen our knowledge of it as much as possible, this work is mainly aimed at diving into and understanding crypto-ransomware, a very present and true-world digital pandemic, from several perspectives. With this aim, this work contributes the following: (a) a review of the fundamentals of this security threat, typologies and families, attack model and involved actors, as well as lifecycle stages; (b) an analysis of the evolution of ransomware in the past years, and the main milestones regarding the development of new variants and real cases that have occurred; (c) a study of the most relevant and current proposals that have appeared to fight against this scourge, as organized in the usual defence lines (prevention, detection, response and recovery); and (d) a discussion of the current trends in ransomware infection and development as well as the main challenges that necessarily need to be dealt with to reduce the impact of crypto-ransomware. All of this will help to better understand the situation and, based on this, will help to develop more adequate defence procedures and effective solutions and tools to defeat attacks.

Keywords: ransomware; prevention; detection; response

Citation: Gómez-Hernández, J.A.; García-Teodoro, P.; Magán-Carrión, R.; Rodríguez-Gómez, R. Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges. *Electronics* **2023**, *12*, 4494. https://doi.org/10.3390/electronics12214494

Academic Editors: Chunying Zhang and Andrei Kelarev

Received: 21 September 2023
Revised: 11 October 2023
Accepted: 24 October 2023
Published: 1 November 2023

1. Introduction

Ransomware has become a digital pandemic in recent years, and it is expected to remain so in the coming ones [1,2]. Although there are a number of typologies and, thus, the associated tactics, techniques and procedures (TTPs) can differ, all of them (as the name indicates) are aimed at kidnapping the target's device resources and then extorting the victim to recover them. Although the very origin of the term 'ransomware' is not clear [3], it is mainly used for marketing purposes since the term crypto-virus would have been more accurate.

Ransomware causes not only extortion but also data breaches, intellectual and industrial property theft, loss of reputation and other harmful effects [4]. Cheating, spying and disrupting operations are examples of motivations in the current geopolitical game. In such a case, no ransom payment mechanisms are considered. Recently, before and during Russia's war against Ukraine, some ransomware attacks have been triggered by both sides. In particular, NotPetya disrupted the operation of several Ukrainian companies, as did the recent WhisperGate attack [5]. Among the most relevant cybersecurity threats at present [6], ransomware appears as the second cause for concern in relation to the possible types of attacks [7]. In fact, it has evolved in the last few years to select organizations and enterprises as its main objectives, since the balance between benefits and attack cost is higher than in other cases. The report by Deloitte [8] indicates that around 4000 ransomware attacks occur

daily; on average, 191 days pass until an attack breach is identified, and the average number of exfiltrating and dropping ransomware cases has increased 8.7% from the first quarter of 2021. From an economic perspective, ransom payments reached 350 million dollars in 2020 with an increase of about 109% compared to 2019. In fact, around 42% of companies with cyber-insurance against ransomware have not recovered the losses suffered. To present some more figures, on average, system shutdown lasts 19 days; 92% of companies that paid the ransom did not recover the data; 53% of them claim that the attacks damaged the trademark; and 26% of companies had to temporarily close.

In the above general context, this work is aimed at knowing more in detail about this damaging cyber-attack typology, the procedures and countermeasures developed to fight against it (based on the Cyber Kill Chain and MITRE ATT&CK frameworks), as well as the defence methods deployed according to the specific attack stage: prevention (prior to the attack), detection (when the attack is triggered) and response/recovery (after the attack). Moreover, current trends and new challenges in the field are discussed. All of this is clearly exposed and organized for the reader's understanding. This way, a better comprehension of the problem can result in the development of more effective defence schemes.

To perform the present study, an exhaustive search for works related to ransomware or crypto-ransomware was carried out, from which a total of almost 600 bibliographic references were obtained. The sources included articles from magazines and conferences, as well as technical reports and publications in specialized newspapers that provide characteristics of the way crypto-ransomware samples usually operate. In order to reduce that number and focus on the study, a filtering process was carried out based on three main criteria: (a) the introduction of a specific defence proposal (prevention, detection and recovery) or approach (technical or regulatory) to the problem; (b) the quality of the proposal determined by a proper description of it and some associated experimentation; and (c) the appearance date of the proposal after 2017. Around 250 out of the 315 works finally included in the 'References' section correspond to magazines or conferences and the rest to technical reports, specialized journals or data sources that allow for understanding the characteristics of recent crypto-ransomware samples or specific aspects of their development.

There are very good reviews of the state of the art and taxonomies of ransomware included in the present work. Aimed at unifying all of them, we introduce here a new taxonomy that covers all the phases to tackle the ransomware problem (prevention, detection and recovery), unlike similar previous works that usually focus on some specific stages, generally detection, or techniques, such as Machine Learning. In this regard, the present review covers all known/documented techniques in each of the problem stages, while the topic is addressed not only from a technical point of view but also from a regulatory and legal perspective.

With all of that in mind, the rest of the document is organized as follows. Section 2 is devoted to describing ransom concepts, the RaaS model (Ransomware-as-a-Service). The implemented attack model is described in Section 3. In Section 4, the families appeared over time and their associated attack methodologies are presented. Afterwards, Section 5 introduces the primary defence proposals in the literature to combat this attack, from the perspectives of preventing, detecting, responding and recovering. For extension purposes, the bibliography review is mainly focused on works developed in the last five years. In Section 6, current trends in ransomware attacks and new challenges in preventing this pandemic are presented. Finally, the main conclusions of the work are highlighted in Section 7.

2. Ransomware-as-a-Service Ecosystems, Crypto-Coins and Extortion

There are a variety of ransomware typologies. In terms of attack severity, we can discern among the following ones [9–11]:

- *Device locker*. It is aimed at locking the victim's device functions, such as the screen or keyboard. W32.Rasith or Android.LockDroid.H are some examples of this typology.

- *Crypto-ransomware*. Contrary to the previous type, this focuses on encrypting the victim's data. The victim should pay a ransom to obtain the key for deciphering the affected files and recovering them.
- *Victim intimidation (scareware)*. This kind of ransomware just scares the victim through specific messages indicating that their files are blocked or ciphered, although that is not true.
- *Data exfiltration (leakware or doxware)*. Sensitive information is exfiltrated from the victim's device. Different from crypto-ransomware, the victim can still access the files.

Among the previous types, the most prevalent one at present is that of crypto-ransomware. In this work we focus on crypto-ransomware, but we will use the terms ransomware or crypto-ransomware indistinctly from now on for the sake of simplicity. Crypto-ransomware is mainly motivated by its inherent properties of persistence and reversibility. In other words, the attacker keeps the control over the hijacked files even if the malware is removed, while she is also able to reverse the ciphering process if required.

Traditionally, people who developed the ransomware samples and people who performed the attack were the same. Instead, the RaaS exploitation model has recently appeared, which inherits the SaaS (Software-as-a-Service) approach but with its own features.

It proposes a specialization of the work performed by attackers [12,13]. Thus, there are *operators* who include an organized group of people to build the malware, create a panel of command and control to manage the attack, enable a data leak site, recruit affiliates, negotiate with the victims or carry out money laundering.

Affiliates are people who pay for tools to carry out the attacks without having special technical skills for that because they can receive guidelines and support from the operator to attack by just using ransomware samples. They can participate in the business by paying a tax or a percentage of the benefits to the operators. They are responsible for running the ransomware and requesting the ransom. In recent attacks, when the victim refuses to pay, the so-called *negotiator* role appears, which consists of convincing the victim to pay for the extortion by making an economic balance of the losses derived from the affected systems in respect to the ransom amount demanded.

Figure 1 shows a functional diagram of the RaaS model, where the stages inside the dashed red line are the steps followed by non-specific RaaS-based attacks. The diagram is simplified for a more general vision, while we can find more specific models in works like reference [14], for Evil Corp. The overall process is as follows: *(1)* the ransomware developer creates a specific exploit to be afterwards licensed/shared with an affiliate; *(2)* the affiliate updates the exploit code to the hosting site and *(3)* selects the target victim as well as the attack vector to deliver the exploitation (email, web, etc.); *(4)* the victim bites the trap so that *(5)* the ransomware is downloaded and installed; *(6)* the ransomware will communicate with the command and control (C&C) server to get the ciphering key and, apart from ciphering the victim's files, *(7)* it can perform lateral movements to identify other potential targets, make itself persistent, delete file backups and hide its presence; *(8)* the extortion message is shown to the victim, as is the way to pay; *(9)* another malicious agent is potentially in charge of money laundering such that it would be difficult to identify both the ransomware developer and affiliate; *(10)* the affiliate can decide to send the ciphering key to the victim or not in order to get additional payments.

Beyond the economic profit itself, the RaaS approach makes the identification of the developer even more difficult. Together with the existence of ransomware, generation toolkits, like Thanos [15] or Chaos Ransomware Builder [16], boost the creation, use and promotion of RaaS not only by their own developers but also by other actors like individuals, companies or governments. An example of the business model could be found in reference [17] for the case of the Conti group.

An increasing trend in benefits can be observed for ransomware, with profits raising up to USD 602 million in crypto-coins in 2021, a 2500% increase in comparison with 2016. In particular, Conti has been the most profitable RaaS model until now, with a total of USD 180 million raised [18].

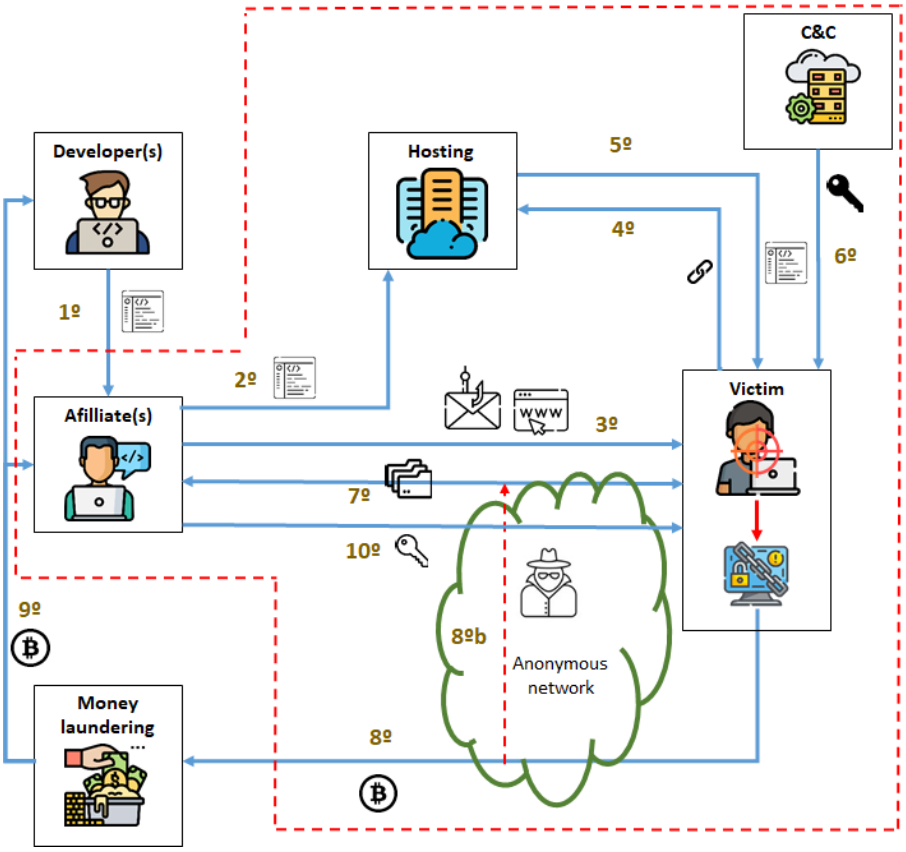

Figure 1. Stages involved in the RaaS model.

3. Crypto-Ransomware Attack Model

With the aim of understanding how crypto-ransomware attacks work, we introduce here a taxonomy based on the CKC (Cyber Kill Chain) defence model [10,19,20] where all the life cycle attack steps and phases are described. A different approach is proposed in reference [21], where a ransomware process model is used to identify the chain processes associated with ransom-related behaviors.

The CKC model extends a previous one named IKC (Intrusion Kill Chain) [22] to provide fine-grain information for each attack phase. This model has been successfully tested before to characterize intrusion attacks in industrial environments and, in general terms, to obtain the tactics, techniques and procedures attackers can carry out.

The CKC model defines seven steps that an attacker must follow to effectively execute the attack. They are as follows:

1. *Reconnaissance*. In this phase, the attacker gathers as much data as possible about potential targets from, e.g., email lists, social networks, system and service vulnerabilities, among other sources of information. Such information will help the attacker to perform a targeted, more robust attack [23].
2. *Weaponization*. The malicious payload is prepared to be delivered to the target in this stage.
3. *Delivery*. In this phase, the attacker searches for a valid way to deliver the malicious payload to the targets. For instance, by sending a compromised email to them.
4. *Exploitation*. This comprises methods and techniques for exploiting vulnerabilities on the target computer and allowing attackers to execute the malicious payload.

5. *Installation*. The methods through which attackers are able to access and compromise nearby nodes and install administrative tools like *Remote Access Trojans* (RAT) or backdoors [24] are involved in this phase.
6. *Command & Control*. The attacker builds dedicated communication channels to manage the compromised system.
7. *Actions*. In this phase, the attacker carries out actions on the compromised system according to the main attack objective. For instance, file ciphering, data exfiltration or data erasing.

Figure 2 graphically summarizes and extends the CKC taxonomy proposed in reference [19] and shows the relation with the MITRE ATT&CK framework [25]. In the following, each of the previous attack stages is described a bit more in detail.

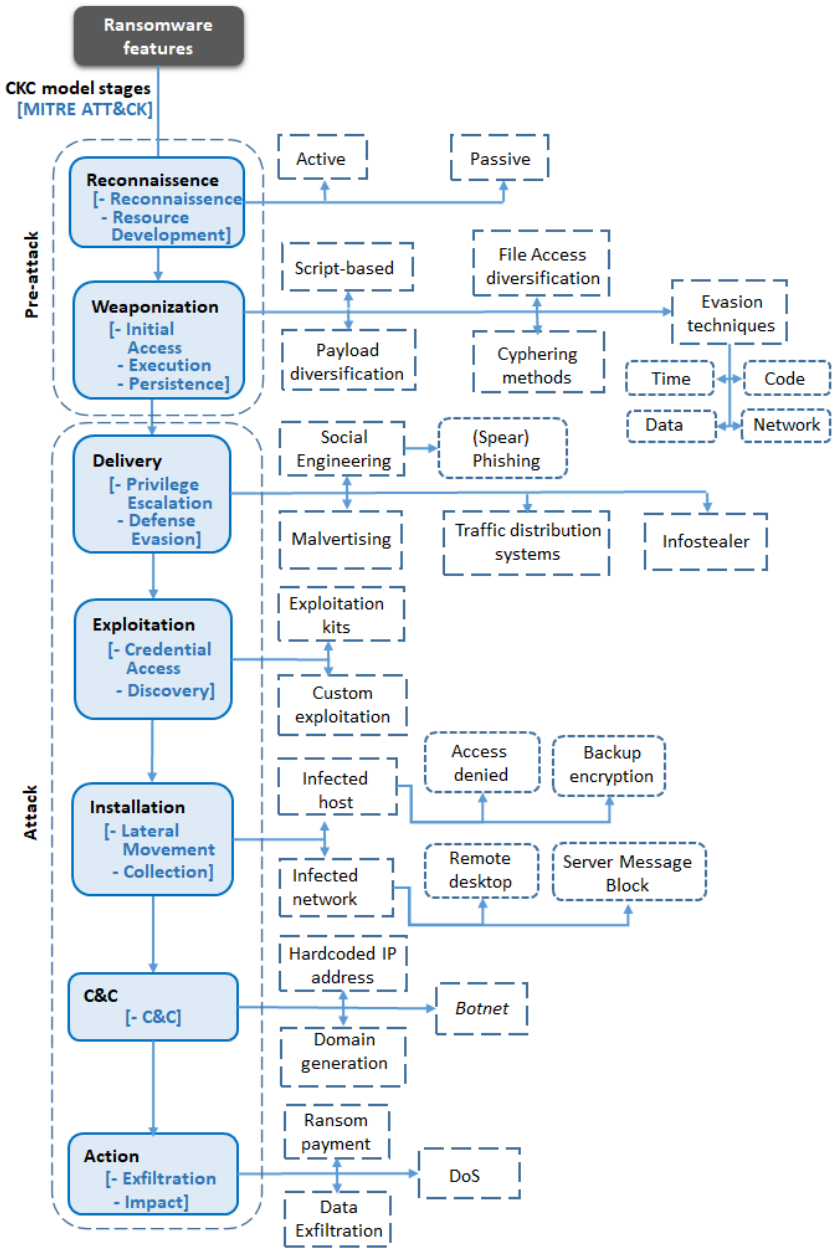

Figure 2. CKC-based crypto-ransomware taxonomy (extended from reference [19]).

3.1. Reconnaissance Stage

In fact, this phase is seen generally in attacks and is not specific to ransomware. In this stage, information about the target is gathered (in an active or passive way) in order to decide the attack method and tools to be used.

In previous decades, attackers usually sought easy targets for ransomware attacks. In order to do this, publicly available tools like Shodan were used. Instead, targeted attacks against specific or preselected organizations are more common at present, with the objective of minimizing effort while maximizing benefits.

In the MITRE TTP&CK framework, this stage corresponds with the Reconnaissance and Resources Development phases, where Discovery (named TA007), Priority Definition Planning (TA0012), Priority Definition Direction (TA0013), Target Selection (TA0014), Technical Information Gathering (TA0015), People Information Gathering (TA0016), Organization Information Gathering (TA0017), Technical Weakness Identification (TA0018), People Weakness Identification (TA0020), and Organization Weakness Identification (TA0020) are included.

In the Weaponization Stage, there are different techniques for a ransomware attack to carry out: script-based, diversification or evasion techniques.

Script-based ransomware encrypts files by following commands in a script. Such scripts are removed after the malware operation. This way, the malware code is only found in memory, thus making it a fileless sample that is more robust against security defences.

Diversification techniques are intended to evade security mechanisms. For instance, a payload diversified into different apparently benign files is commonly used in this kind of attack to hide them. Another example of diversification is the typology of malware access to the target files. Moreover, attackers can also diversify the ciphering methods to be used. In this case, the two main categories are as follows: standard and customized. The first ones are well-known ciphering algorithms (e.g., symmetric, asymmetric or hybrid) that make use of system native encryption APIs (*Application Programming Interfaces*). They usually require administration permissions and the API access can be easily blocked. Conversely, the customized techniques make use of their own ciphering suite, making them more robust against crypto-API defence techniques [26].

Regarding evasion mechanisms, we can discern four categories [27–29]:

- *Time-based* evasion techniques schedule the attack execution or measure how long the attack execution was. They, in turn, can be split into two: delayed and event-based execution. The first ones delay the ciphering procedure, while the second ones wait for a specific system event to start the ciphering process (e.g., a system reboot).
- *Data-based* evasion schemes are focused on removing all the attack evidence, making them difficult to detect and identify. As an example, anti-memory-dumping techniques make reverse engineering difficult in the case of applying digital forensic analysis. To do that, removing executable file headers or moving them to different memory locations can be implemented. One more example is ADS (*Alternate Data Streams*) [30], which consists of adding extra attributes to the file containing the malware.
- *Code-based* evasion techniques have four variants. The first typology is called the *debugger evasion technique* and it tries to detect if the code is being debugged. In that case, the malware stops its execution or tries to kill the debugger. Some other techniques add useless pieces of code/data to obfuscate it; the reverse engineering process thus becomes more difficult and the antivirus detection performance is reduced [31]. They are also known as *anti-disassembling evasion techniques*. *Anti-sandboxing code evasion* techniques are devised to detect and avoid running a malware sample in a virtualized environment or sandbox, which is usually employed by security analysts to safely characterize the malware behavior. Finally, *polymorphism and metamorphism techniques* add little modifications to malware samples so that they can evade signature-based detection techniques.

- *Network-based evasion techniques* are applied to network communications with the main aim of fooling IDS/IPS (*Intrusion Detection Systems/Intrusion Prevention Systems*). Network traffic ciphering or anonymizing, domain shadowing and fast flux are some examples of such kind of techniques. Thus, *ciphering C&C communications* prevent external analysis. *Network traffic anonymization*, using darknets, for instance, does not only cipher but also prevents the disclosing of the source of the communication. Attackers also use *domain shadowing*, which consists of first stealing a legitimate domain to be subsequently used for building sub-domains. Then, such sub-domains are periodically rotated to point to malicious servers. Finally, *fast flux techniques* prevent the attacker's IP from belonging to black lists. For that, the associated IP is periodically changed according to a predefined list.

In the MITRE ATT&CK framework this stage corresponds with the Initial access, Execution and Persistence phases, where Adversary OPSEC (OPerational SECurity, TA0021), Establish & Main Infrastructure (TA0022), Build Capability (TA0023), Test Capability (TA0024) and Stage Capability (TA0025) are included.

Delivery Stage Delivering the malicious payload to the target victim requires specific techniques that usually include people as one of the weakest links in the security chain. Thus, this kind of technique is mainly based on social engineering and misleading advertising techniques [32,33]. For that, phishing [34] and social engineering [35] are widely utilized. In general, phishing techniques are aimed at gathering sensitive victim data like credentials or credit card information. For instance, attackers send malicious emails (spam) that mimic legitimate ones from well-known companies, send an SMS (Short Message Service) or just make a phone call. Sometimes, they encourage the victim to visit a compromised website or to download an infected file.

Through misleading advertising, attackers promote advertising campaigns where legitimate websites are in charge of redirecting the victim to malicious websites from where the malware is finally downloaded. Instead of malware being delivered by directly accessing malicious sites, attackers can pay for a traffic distribution service that redirects users to malicious websites [33].

Table 1 summarizes the most predominant delivery methods [36] and protocols [37] at present. As shown, they are not exclusive, since, for instance, an SMS or a spam email may also contain a link to a downloader. As could be expected, spam campaigns are still the most relevant and useful way to effectively deliver malware. However, they are closely followed by remote access procedures that may be motivated by the COVID-19 pandemic, when companies and workers operated remotely.

Table 1. Percentage of non-exclusive delivery methods (two left columns) and protocols (two right columns) used by crypto-ransomware.

Delivery Method	Usage %	Protocol	Usage %
Spam email	60	SMTP	45
Remote Desktop	21	IMAP	26.5
Trojan	20	Web-browsing	22.3
Vulnerability exploitation	15	POP3	3.8
Botnet/Downloader	11	FTP	2.3
Malicious advertising	8	Other	3.3
Endpoint	7		
External server	7		
Removable media	6		
Social media	5		
Insider	3		
Unfair administration	2		
SMS	1		
Affiliate scheme	1		

Apart from the previously mentioned mechanisms to deliver ransomware, the following five are the most important delivery artifacts in the last two years: Emotet, Zbot, Dridex, Gozi and Danabot [38]. Recently, ransomware actors have been using infostealer to get credentials and evade defense mechanisms. Another aspect that we will have to observe the evolution of is the use of AI to improve the methods used in phishing.

In the MITRE ATT&CK framework, this stage corresponds with the Privilege escalation and Defense evasion phases, where Initial Access (TA001), Defense Evasion (TA005) and Discovery (TA007) are included.

3.2. Exploitation Stage

After delivering the malware, the attacker will need to effectively execute it. For that, two main methods can be distinguished: EK-based (*Exploitation Kits*) or targeted exploitation. An EK comprises a hacking toolkit to, firstly, perform a vulnerability scan and, secondly, to exploit one or more of the vulnerabilities found by executing the malicious program [39,40]. To do that, attackers will redirect users to malicious domains where they are able to scan and exploit vulnerabilities. Nowadays, malicious agents offer that as an *exploit-as-a-service*.

Among others, the following EK can be remarked: Fallout used by Gandcrab and Maze [41]; Ring used by Sodinokibi, CrySys and Cerber ransomware; Spelenko also used by Maze [42]; and GrandSoft Exploit Kit to deliver GandCrab 3.0 [43].

According to the 2021 CyberSecurityWorks report [44], 35 new vulnerabilities have become associated with ransomware (13 in the last quarter), making a total of 323 vulnerabilities related to ransomware. That means an increase of 466% since 2019. Moreover, 11 vulnerabilities were labeled as critical, even though scanners like Nessus, Nexpose or Qualys could not detect them. The S21sec company summarizes in reference [45] the most exploited vulnerabilities by ransomware creators up to 2021.

While EKs are devised to be massively applied, the targeted exploitation methods are oriented to specific hosts or network devices. In this case, attackers are searching for the senior management people staff of a company (e.g., CEOs (Chief Executive Officers)) that control and have access to sensitive information and systems.

The last ransomware report, released by VirusTotal in 2021 [38], shows that just 5% of the found ransomware samples include or are associated with exploits. This fact is supported by the CKC model, where the exploitation stage is needed before the ransomware can take place.

In the MITRE ATT&CK framework, this stage corresponds with the Credential Access and Discovery phases, where Initial Access (TA001), Execution (TA002) and Defense Evasion (TA005) are included.

3.3. Installation Stage

During the installation stage, the malicious payload is installed on the target system. Then, it is spread over the network the system belongs to. Indeed, the installation stage can be split into two steps: host and network installation.

During host installation, the deployed executable tries to encrypt all the possible local files and backups (local or cloud-based). After that, network installation takes place to infect other nodes by performing lateral movements. Some tools used by the attacker to perform network installation are, among others, Mimikatz or Cobalstrike [38]. In terms of services and protocols, three of these are the most exploited ones in this phase: RDP (*Remote Desktop Protocol*) [46], SMB (*Server Message Block*) [47] and VPN (*Virtual Private Network*) [48].

In the MITRE ATT&CK framework, this stage corresponds with the Lateral Movement and Collection phases, where Persistence (TA003) and Defense Evasion (TA005) are included.

3.4. C&C Stage

Once the ransomware has been successfully installed on the target, communications to/from the C&C server are crucial for both asking and receiving the ciphering keys and for managing the ransom payment. In the MITRE ATT&CK framework, this stage corresponds with the same phase that corresponds with Command&Control (TA001).

How the ransomware knows the C&C server's IP (Internet Protocol) address is commonly faced using three methods: a code-embedded IP address, domain generation algorithms or botnets. The two first techniques will be described in detail in Section 5.2, while the last one consists of the use of botnets to perform different malicious activities: data ex-filtration, phishing campaigns or malware spreading [49], among others.

3.5. Action Stage

After ciphering files, ransomware will show a message on the victim's computer informing its user of the type of attack and the form to recover the affected files, usually through some kind of payment method. In this line, several levels of extortion can be used: from simple data ex-filtration to publicly publishing them if the user declines the payment.

In the beginning, attackers considered classical payment methods (e.g., Paypal), but the use of crypto-currencies is the most widely accepted method at present. To push the victim for the payment, some ransomware families like *Jigsaw* both increment exponentially the cost of the ransom and delete files over time. For instance, *FrenchLocker* deletes a file every few minutes.

In the MITRE ATT&CK framework, this stage corresponds with the Exfiltration and Impact phases, where Privilege Escalation (TA004), Credential Access (TA006), Lateral Movement (TA008), Collection (TA009), Exfiltration (TA0010) and Impact (TA0040) are included.

Figure 3 graphically depicts the typical life cycle of a ransomware incident according to the previous CKC stages. Moreover, Table 2 shows, for different ransomware families, the stages and techniques involved to provide a complete overview of how ransomware attacks work to devise novel security solutions against this type of malware.

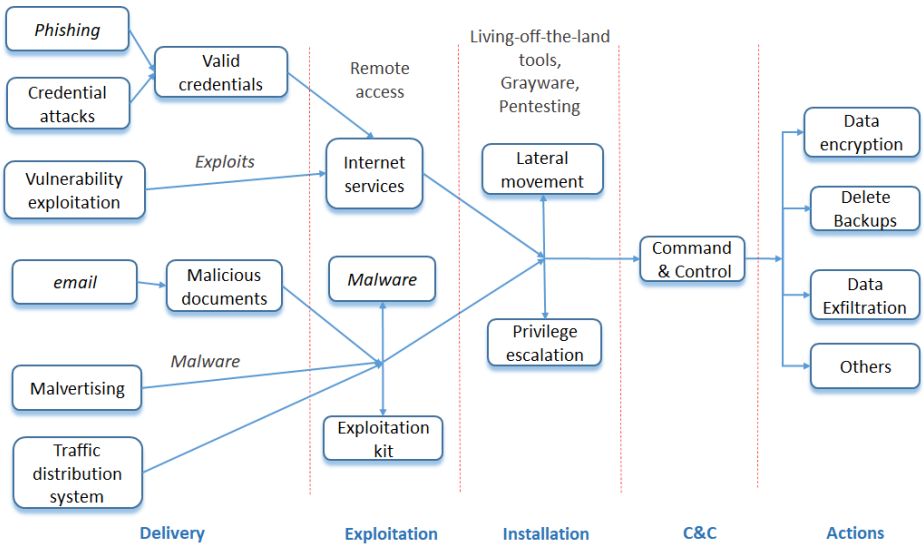

Figure 3. Ransomware incident life cycle.

Table 2. Ransomware families and their attack techniques.

Family	Cyber Kill Chain Stage																					
	Weaponization									Delivery			Exploit		Installation					C&C		Action
	Scripting	Payload	FAP	Encryption	Evasion				Social	Engineering	Malvertising	TDS	Exploit Kit	Custom Exploit	Host		Net	Hardcoded IP	DG	Botnet		
					T	D	C	N	P	S					AD	BE	RD	BMS				
Avaddon [50,51]			✓	3 9		✓	✓			✓				✓		✓						I
BlackByte [52,53]			✓	1		✓	✓			✓				✓		✓						I
BlackCat [54,55]		✓	✓	1		✓	✓	✓	✓			✓		✓				✓				o
Cerber [56–58]	✓	✓		7 8	✓	✓	✓		✓	✓	✓		✓		✓						✓	
Diavol [59,60]		✓	✓	8				✓		✓			✓			✓	✓		✓			E
Ekans [61,62]	✓			3 9			✓	✓		✓	✓					✓	✓					I
Entropy [63,64]		✓	✓	7		✓	✓	✓	✓				✓				✓				✓	
Hive [65]	✓		✓	8		✓			✓			✓		✓	✓							
Khonsari [66]		✓	✓	2 4										✓			✓			✓		
Locky [27] [67–69]	✓	✓	✓	21 5		✓	✓	✓	✓			✓	✓			✓			✓	✓	✓	
Megacortex [70]	✓		✓	23 10 11			✓	✓		✓			✓			✓			✓			
REvil [71]		✓		7		✓	✓	✓					✓	✓								E
Ruyk [72,73]				1			✓		✓				✓			✓	✓			✓		E
Sabbath [74]		✓	✓	1			✓	✓			✓		✓			✓					✓	E
Sodinokibi [75]	✓	✓		1 6 11	✓	✓		✓	✓			✓		✓		✓	✓					Z
TFLower [76,77]		✓		8		✓	✓			✓					✓			✓		✓	✓	
WannaCry [78,79]			✓	1 8		✓	✓									✓		✓				I

Abbreviations: AD: Access denial; BE: Backup encryption; BMS: Block Message Server; C: Code; D: Data; DG: Domain Generation; E: Data Ex-filtration; FAP: File Access Pattern; I: Inhibit system recovery; N: Network; o: Denial of Service; RD: Remote Desktop; P: Phishing; S: Spear phishing; T: Time-based; TDS: Traffic distribution system; Z: Inhibit system recovery and data ex-filtration. 1: AES; 2: AES-128; 3: AES-256; 4: CBC; 5: CTR-EBC; 6: ECDB; 7: RC4; 8: RSA; 9: RSA-2048; 10: RSA-4096; 11: Salsa20.

4. Crypto-Ransomware Evolution

This section presents the ransomware's historical evolution, from the appearance of the first sample until the present day. This historical description is focused on attacks directed to generic targets, individuals or business teams of all types of organizations.

There are numerous works where the evolution of ransomware is studied [80–82]. An overview of the abovementioned evolution is shown in Figure 4, showing in blue text the most relevant milestones that have given ransomware its current damaging power. The most notable moments are as follows: 1989, considered the origins; 2005, when modern ransomware incorporating asymmetric encryption appeared; 2013, where crypto-currencies payment was incorporated; 2015, considered the explosion year of this threat; 2016, ran-

somware's focus on organizations; 2017, with government-sponsored ransomware (e.g., the work [83] documents the relationship between ransomware groups and states); 2019, with the addition of new extortion tactics (in the double extortion case, the operator threatens the victim by publishing the data if the ransom is not payed; in the triple extortion case, the target's customer and partners are notified about sensitive data related to them that would also be disclosed if the victim does not pay the ransom; and in the quadruple extortion case, ransom note includes a threat to bring down the target's public-facing servers with a distributed denial-of-service (DDoS) attack if it refuses to pay the ransom); 2021, beginning of the attacks on critical infrastructures and supply chains. The figure also includes (in blue boxes) examples of the most relevant families by appearance date. It is worth highlighting the growing number, complexity and impact of new ransomware samples, as discussed in the following. In addition, it should be noted that the problem is far from disappearing in the short-medium term.

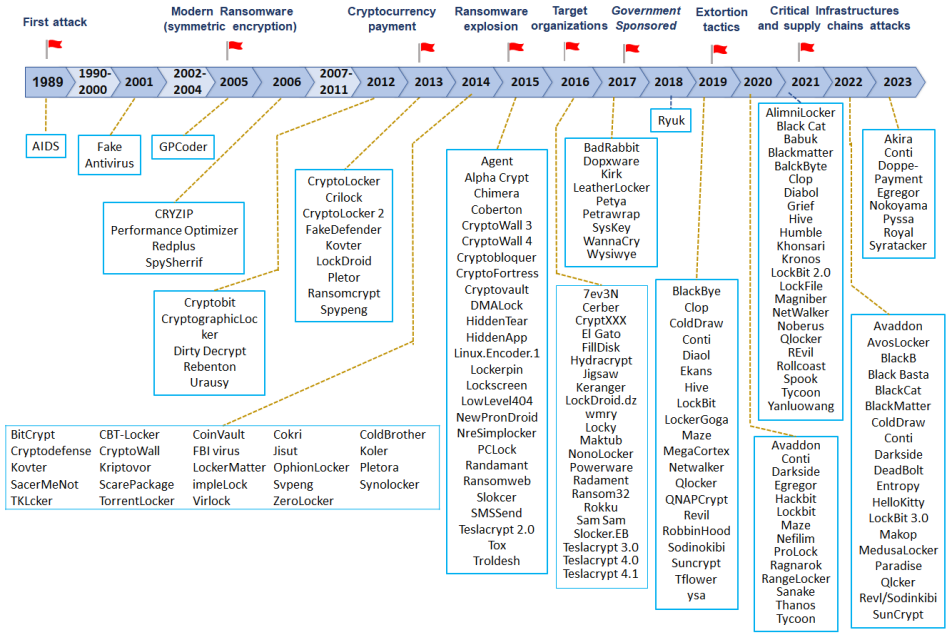

Figure 4. Evolution and families of ransomware.

4.1. The Origins

With the development of the Internet, in late 2004 and earlier 2005, *GP-Coder* infected different systems by using a personalized encryption algorithm. It requested a ransom payment of USD 200 through Western Union or premium SMS. Fortunately, the encryption key was weak and easy to break. With *Archiveus* in 2006, ransomware's authors realized the importance of using strong encryption by only encrypting the 'My Documents' folder. Although it was the first time that a 2014-bit RSA encryption code was used, the authors' failure was not to use different keys to lock down the target systems. Once this error was discovered, the malware fell into disuse.

Until now, one of the major limitations of ransomware attacks was the traceability of payments. Therefore, the following families started to use gift cards to pay the ransom. This medium allowed the victims to pay the ransom simply by going to a store, video game vendor, or credit card company. This is what *Locker* did, since 2009 in Russia and since 2010 in the rest of the countries, and *WinLock* as well. In particular, *Locker* was installed by visiting a malicious or compromised website and was usually written in JavaScript. Its objective was to block access to device functionality with a popup that indicated how to pay the ransom through a gift card or wallet. This variant also spread to mobile phones

by downloading applications outside official sources. This has been seen again in the COVID-19 pandemic, where cybercriminals used an infection tracker that turned into a device blocking a sample [84]. These attacks pretended to look like some state security body and indicated to the victim that they had committed an illegality for which they had to pay a penalty. This technique had little success as the victim's files were not affected and, thus, it was possible to bypass the lock screen.

4.2. Use of Cryptocurrencies

Combining device blocking and crypto-currencies gave rise to *Reveton* in 2012, which was the first to use the RaaS business model and Bitcoin payment. With it, the ability to massively infect victims began. *Reveton* also showed a fraudulent message posing as some state security body and force depending on the country and accusing the victims of committing a criminal act for which they could be imprisoned if they did not pay the extortion. In this regard, the emergence of crypto-currencies in 2009 revolutionized the ransomware business by enabling easy and anonymous payments

Up until the mid-2010s, ransomware was more focused on PCs, given the popularity of the Microsoft market that offered a high number of victims. Despite that, an expansion of the target platforms began: mobile, Linux and Mac. Specifically, in 2012, *SimpleLocker* became the first ransomware to encrypt files on Android device's SD cards, thus opening a new niche of victims and attacks.

Another important milestone was in 2013, with the appearance of *CryptoLocker*. This had the double form of payment through Bitcoin or wallet cards. Also, it used a 2048-bit RSA key. It spread as an apparently normal email with an attachment. One of the variants managed to raise a significant amount of money (USD 27 million in two months) and it is estimated that it affected around 234,000 victims. The fight against this attack was an example of collaboration between security forces and private security companies that culminated in the identification of the responsible person, who was never arrested.

In 2015, *LockerPin*, which also targeted Android devices, aimed to completely block user access by changing the device PIN (Personal Identification Number), instead of encrypting files. This year, *Linux.Encoder.1*, the first ransomware for Linux, was released.

From the defence point of view against this threat, in 2015 the source code of *Hidden Tear* was published by a group of Turkish researchers, with the intention that security teams knew how it worked [85]. Unfortunately, this also allowed attackers to make improvements and launch new attacks. In 2020, some new ransomware variants contained traces of this code, such as *Chaos Ransomware Builders* [86], a software with a graphical interface to create ransomware according to certain options. For example, these similarities appear in its V3 version, both in the code to generate the keys and in the AES encryption, which are practically identical. Something similar happens with *Bagli*.

The change in evolution culminated with variants capable of attacking Windows, Linux and Mac systems without differentiated codes for each platform. *Ransom32*, which appeared in 2016, is a variant of the RaaS model developed in JavaScript, and allows it to operate on most platforms.

4.3. Crypto-Ransomware Explosion

In the next stage, the sophistication of attack techniques increased, in addition to expanding globally. In 2016, *Petya* was the first variant to overwrite the MBR (*Master Boot Record*) instead of encrypting individual files, blocking disk access faster than other techniques. This same year, *Locky* appeared, sending up to 500,000 phishing emails per day for its propagation [3]. Other families that also appeared that year were *TeslaCrypt*, *Jigsaw* and *Cerber*. All of them have in common that they were used for automated attacks, delivered via phishing emails, exploit kits or malicious advertisements located on websites, against a single machine. There were so many variants that 2016 was designated as the 'year of ransomware', even though it was only the beginning of its rise.

Another of these families was *SamSam* (named after a village in northwestern Iran) which, instead of using exploit kits or phishing, exploited vulnerabilities in JBoss (*Open Java Application Server*) and looked for exposed RDP (*Remote Desktop Protocol*) servers to launch password brute force attacks to obtain access to them. Instead of installing itself on one machine, as today's families do, it spreads through the target network with different tools and exploits by installing itself on as many machines as possible. It was operational until 2018 when the United States Department of Justice charged its perpetrators and the attacks stopped.

A few months later, *Zcryptor*, which combines features of a worm, created an attack called a crypto-worm or ransom-worm, which is particularly damaging as it can stop an entire system by replicating itself across the network.

WannaCry, in 2017, was cataloged as one of the largest attacks in terms of the machines and business sectors affected. It used the *EternalBlue* exploit [87] that exploited the vulnerabilities of Microsoft's SMB (*Server Message Block*) protocol. It demanded the ransom in Bitcoin, equivalent to USD 300, but as the encryption key was not available, thousands of paying victims found they could not get their files back. At the end of 2017, the United States of America and the United Kingdom attributed the ransomware to North Korea. Two months after *WannaCry*, the *NotPetya* attack (successor to *Petya*) took place. It encrypted files and did the same with the MBR, which meant that, even with the decryption key, the victim could not recover the files. It was distributed using a trojanized version of the *M.E.Doc* software for updates, necessary for companies doing business in Ukraine. The attackers compromised the update server to insert the malicious software. A few months later, the attack was attributed to Russia according to the United States, Canada and Australia.

This period of time was also characterized by the development of new variants of existing ransomware instead of developing new families. For example, *Goldeneye* appeared in 2017, which is a variant of *Petya*, and is pretty similar to *WannaCry*. However, this new variant is more dangerous because it solves the encryption problems of its predecessors.

Since 2016, there has been ransomware using the RaaS model, such as *Stampado*, *Goliath* and *Locky*. However, the operators initially only provided the executable file, so the attacker who bought it was responsible for the entire operation. This aspect changed with *GandCrab* (2018), which offered a portal for affiliates, allowing them to follow the attack and manage the payment. This same year, *Ryuk* appeared, setting a new standard by being the first to operate as a targeted attack. It used *Tribot* and *PowerShell Empire* to spread and install itself. Additionally, it used *PowerShell* and *Windows Management Instrumentation* (WMI) to perform lateral movements.

4.4. New Extortion Techniques

In 2019 and 2020, new ransomware attacks appeared with two dangerous and destructive aspects: double extortion and oriented to organizations instead of individuals. Double extortion encrypts and steals the victim's files so that, if victims do not pay, they are threatened with publishing data or selling it on the black market. An example of this is *Maze* (2019), which provides a leak site and, therefore, uses ransomware as a data theft attack (double extortion). Its successor, *Egregor* (2020), incorporates a support service for victims to protect their systems if they paid. On the other hand, to maximize profit, attackers select victims in large, well-known organizations where the ransom amount can be higher. This does not mean that individualized attacks will disappear.

The COVID-19 pandemic has triggered the explosion of double extortion and RaaS. During this period, the number of attacks on hospitals, government organizations and universities increased, with 72% of new samples and 77 new campaigns during the first months [88]. Attackers took advantage of the event to carry out the following: *(i)* execute more and faster attacks (shortening the time between infection and activation), *(ii)* recruit collaborators to maximize impact, and *(iii)* offer RaaS on the Dark Web [89]. This increase was generalized to all types of malware. We must highlight campaigns that took advantage

of the coronavirus issue, such as *Ransomware-GVZ* [90], *NetWalker* and *CoViper*. One of the reasons for this proliferation is the increase in remote work, which allowed the vulnerabilities of remote desktop protocols to be exploited at a higher level. Also, we should indicate that the amount requested in ransoms with these attacks increased by 60% on average [91].

Also, in 2019, *QLocker* attacked NAS (*Network Attached Storage*) systems, the CVE-2021-28799 vulnerability being exploited. This ransomware was active again in early 2022 [92]. In this same year, *Conti* appeared, one of the most common ransomware families, with more than 450 known victims and considered a relative of *Ryuk* (2018–2021), since both are operated by the same Wizard Spider subgroup, and reuses code from it. *Conti* is especially hard since it persecuted health organizations during the pandemic. After the attack on Ireland's Health Service Executive, the group was forced to give the decryption key to stop the possible response from the government. In 2020, the *Trickbot Trojan* began to be used together with *Emotet* and *Ryuk*, and *Trickbot* was eventually included inside *Conti* [18].

Lockbit appeared in 2019 and continued throughout 2020, reporting more than 9000 incidents. Given the large number of affiliates, it is difficult to establish how it proceeds. Some gain access using phishing campaigns while others take advantage of exposed RDP servers or even exploit VPN vulnerabilities or cloud infrastructures such as *SonicWall* or *Microsoft SharePoint*. *REvil* reappeared as *LockBit 2.0*, hoping to capture *REvil*'s affiliates. One of its features is the automation of the deployment process for affiliates, who only have to take control of Active Directory and run a script. The rest is done by the program.

In May 2021, the RaaS variant of *REvil* was used to carry out one of the largest attacks in history, where the attackers demanded Kaseya USD 70 million for unlocking more than one million devices. In December of this same year, *Konsari* appeared, the first to exploit the *Log4Shell* vulnerability (CVE-2021-4428).

Grief (2021) was the successor of *DoppelPaymer*. It was deployed in an environment already compromised by *Dridex* and the post-exploitation was performed using *Cobal Strike*. This family is obfuscated and uses anti-analysis techniques that include API hashing, VEH (*Vector Exception Handling*), the Heaven's Gate technique [93] and the encryption of relevant data carried out with RC4. *Grief* runs with specific parameters calculated based on the victim's environment and fails if these are missing or incorrect. Moreover, it disables *Windows Defender* and deletes shadow copies with *vssadmin* and *diskshadow* [94].

4.5. Critical Infrastructure Attacks

Another important milestone in the evolution of ransomware is the appearance in 2021 of attacks against critical infrastructures (CI). The Sabbath group, which operates various ransomware including *Rollcoast*, exposed data and extorted several US school districts using social networks like *Reddit* and *Twitter*. Since July, it started using *Themida* to package ransomware samples and prevent detection. It is designed to run in memory and check the system language (it has an exclusion list of 40 languages). Similarities to *Tycoon* ransomware were detected.

In a recent work on attacks on CIs [95], a change in this type of incident is shown mainly due to the pandemic of COVID-19. A change is shown in the type of organizations affected, where attacks on government organizations are less frequent (going from 35.9% to 16.6%) while increasing the attacks to other sectors. The study also reflects how the ransom payment, given the pressure and tracking of Bitcoin, has shifted to the use of conventional means.

Another important aspect in 2021 was the publication in a hacker forum of the complete source code of *Babuk* (or *Babyk*) ransomware [96]. This was made by one of the developers, a 17-year-old suffering from advanced cancer. The group that operated this family also announced a change in the way they operated according to which they were not going to encrypt the data but just steal them. If the victim does not contact attackers after being notified of the theft, the data will be published [97].

In 2022, the attackers of *UNC2596* (known as *Cuba*) operated the *ColdDraw Cuba* ransomware, which targeted public service providers, government agencies and organizations that support non-profit and healthcare entities. They used a re-branding approach, as is the case with *Entropy*, which has many similarities with the general-purpose malware *Dridex*, or like *Sabbath* with *Arcane*. From the second half of 2022 until today, some changes can be observed. First, ransomware groups are centered on more directed attacks and especially on critical infrastructures [98]. Second, because more organizations are refusing to pay, ransomware is more centered on data ex-filtration so they can extort the victims with their publication. Some recent incidents are the attack on the Costa Rican government by Conti, or the NFC team by the BlackByte group. Third, phishing emails are the preferred way to obtain valid access credentials for the target [99].

Another interesting aspect is that of collaboration between ransomware actors like Ex-Conti and FIN7, also known as ITG14, which work together with the new Domino backdoor, used to distribute the payload of the Nemesis infostealer project [100].

During the Russia–Ukraine conflict, the ransomware with more activity affecting strategic sectors is especially related to defence, like LockBit 3.0, BlackCat (ALPHV) or Black Basta [45].

Recently, a ransomware evolution from Windows to Linux systems in large companies has been observed. Here, a double extortion is carried out, with different persistence mechanisms and evasion mechanisms by erasing log files [101]. Also, MacOS-related [102] and even cloud-based [103] samples appeared.

In summary, it should be noted that, since the appearance of the first sample of ransomware, the growth of attacks has been enormous. We can highlight the following factors in this evolution: pseudo-anonymous payment mechanisms [104], anonymous networks [105], RaaS [106,107] and botnets [108]. All of them make it easier for ransomware operators to work with higher impunity.

In the first half of 2021, we can find 130 active families grouped into 30,000 clusters. The most active ones were *GandCrab* with 6000 clusters, followed by *Babuk, Cerber, Matsnu, Congur, Locky, TeslaCrypt, Rkor* and *Reveton* [38].

An interesting fact regarding evolution is to see how fresh the samples used in the attacks are. VirusTotal shows, in the same report [38], the existence of a correlation between the specimens already examined on the platform and those that appeared in the first instance. This could indicate that the attackers prepare new samples for most of their attacks, except for the peak observed in the first quarter of 2021, where the activity seems to show that previous samples are being reused. These experimental data agree with the analysis carried out in reference [109], which establishes a formula to predict the probability of new attacks. The data analyzed between 2016 and 2020 indicates that a previously observed ransomware attack is more likely than a new one.

Although ransomware attack vectors tend to be similar to those for general malware [110,111], a recent prominent trend can be observed [112]:

- An attack on the supply chain. This attack tries to extend the radius of affection of ransomware to the entire software supply chain by inserting malicious code into a trusted component [113].
- The use of the RaaS model to launch and maintain an attack campaign [10].
- An attack on unpatched systems. While new ransomware to exploit zero-day vulnerabilities appears, known vulnerabilities continue to be exploited on unpatched systems.
- Phishing. Although they are not the main cause, phishing emails are frequent in ransomware attacks.
- Multiple extortion. New extortion models include multiple levels of extortion, personalization and evolution towards new protected goods such as IoT (Internet of Things) [114]. It should be noted that, according to a report by the consulting firm Unit 42 [115], some families of ransomware have evolved from double to quadruple extortion [116]. The Suncrypt group even called the victim to pressure her into making the payment [117].

As a summary of the current situation, the cyber-intelligence report by S21Sec [45], covering the second half of 2022, shows that the most active groups were *Lockbit*, *BlackCat* and *Black Basta*. Among the countries mainly affected, we find the United States of America (619), the United Kingdom (79), France (58), Germany (62) and Spain (48).

5. Defence against Crypto-Ransomware

As is usual for any other kind of security threats, the defence lines against crypto-ransomware can be organized at three different levels: *prevention*, *detection* and *response* (including *recovery* in this last phase). First, mechanisms to avoid the occurrence of crypto-ransomware events should be deployed on the target environment. Since we cannot guarantee the complete avoidance of such a kind of situation, the environment should be monitored over time in order to detect potential incidents. In case they occur, countermeasures should be deployed to solve the incidents and, if so, to recover the affected system and restore it to its original operation state.

In the rest of the section, a revision of the proposals in the literature for each of the above defence lines is presented.

5.1. Crypto-Ransomware Mitigation

Several recommendations are provided in the literature to mitigate this harmful threat and, thus, to try to avoid its occurrence [118–123]:

- Periodically patching software and firmware, since ransomware usually attacks known vulnerabilities [124].
- Segmenting networks to reduce the number of reachable systems [125]. In a more general way, the *Zero Trust Model* can be adopted to avoid the existence of any reliable perimeter [126].
- Blocking access to web resources that are potentially dangerous such as name servers and malicious or suspicious IP addresses, ports and protocols.
- Use of whitelists for authorized applications.
- Use of standard accounts instead of privileged ones.
- Establishing BYOD (*Bring Your Own Device*) policies for personal devices on corporate environments [127].
- Avoiding the use of personal applications on the equipment such as email clients or social networks.
- Training staff and users about security risks, in particular regarding social engineering. Associated behaviors should be supervised.
- Managing authorization credentials to every asset in the organization. In particular, regarding the file system.
- Making periodic off-site backups [128].
- Protecting against data ex-filtration events, which are identified in the MITRE ATT&CK report [129].

In addition to the previous most adopted ones, a variety of other prevention schemes can be found in the literature. For instance, a multi-layered prevention system is proposed in references [130,131], where, among other possible techniques, anti-malware software deployment, firewall configuration, DNS/Web filtering and email security can be considered. In this way, in case of a ransomware incident, the multi-layer defence will allow us to recover data. Furthermore, reference [132] implements a module of traffic analysis to detect potential communications between victims and C&C servers to get cipher keys. This way, in case of a ransomware incident, the data could be deciphered. Similarly, the authors of reference [133] rely on the DFR (*Digital Forensics Readiness*) framework to collect, in a pro-active way, system artifacts over time so that, in the case of a ransomware incident, we are able to perform a forensics analysis to recover ciphering keys and, from them, to recover the data affected by the attack.

A different approach addresses attack simulation where data breaches occur based on Cyber Threat Intelligence (CTI) and the MITRE ATT&CK framework to mitigate the

threat [134]. Sensitive system points for surveillance can be identified with *Rantology* [135], an ontology that allows the evaluation of the program's maliciousness based on different factors, including API function calls and the running behaviors. Moreover, it is possible to learn from the different attack types through multistage game theory in order to derive measures to mitigate their negative impact and improve the decision-making process of defenders [136].

A complementary prevention scheme is the convenience of designing a recovery plan. That is, the elaboration of a procedure aimed to restore the system in case of an incident or disaster is definitive to guarantee its continuity. Recovery, however, is usually described in conjunction with the response schemes, as we shall describe below in Section 5.3.

Some recent papers in the literature are specifically intended to create a survey of prevention and mitigation schemes [137,138]. In what follows, some of the previously itemized prevention mechanisms are detailed.

5.1.1. Access Control

Access control and permission policies are principal in avoiding privilege escalation by ransomware in case of incidents through user credentials [139]. It is recommended to implement the lowest privilege and separate functions basis through a role-based access control scheme.

AntiBotics [140] makes use of a periodic biometric and challenge-based manual authentication procedure to prevent data loss or modification. Likewise, whitelist-based solutions seem to be promising [141], like that in reference [142] where only specific programs are allowed to access files while the rest of the programs are blocked. Similarly, the authors of reference [143] propose limiting the access to the pseudo-random numbers generator API, since it is considered a critical resource.

Another different approach is provided by *MTD* (*Moving Target Defense*) [144], where file extensions are continuously and randomly modified with the aim of reducing the impact of attacks. Instead, other works propose differing the control access decisions to analyze the access consequences and, if necessary, to undo changes [145].

Sophos developed *Intercept X Endpoint*, a tool that makes use of behavioral analysis to prevent ransomware from writing on the system's registry [146]. Intercept X is capable of blocking zero-day APTs (*Advanced Persistent Threats*) and relies on *Crypto Guard* to recover files.

In a similar line, Microsoft released two products to fight against ransomware: *Defender for Endpoint* and *Defender for Identity*. The first one allows access to folders only for reliable applications [147], while the second tool is aimed at identifying advanced threats, especially those regarding lateral movements [148].

Some other proposals rely on firmware. This is the case for reference [149], where a mechanism is proposed to prevent unauthorized applications from accessing file data if they do not know the key registered in the disk. To avoid *Petya*-like attacks against the MBR (Master Boot Record), the authors of reference [150] introduce a hardware-based architecture to protect and control access to the boot process and the associated data.

There are also proposals based on SDN (*Software Defined Networks*) to prevent ransom propagation over the network. For instance, the authors of reference [151] perform anomaly detection on traffic SMB-related ports 139 and 445.

The *Staged Event-Driven Access Control* (SEDAC) approach incorporates both program-centric and user-centric access control measures to intercept a greater number of ransomware attack vector types than other proposals. For that, only delegate access control decisions regarding file operations that users either need or are capable of making and where the security is not affected, while non-negotiable access control decisions made by OS and software developers are enforced [152].

5.1.2. Data Backups

The use of backups is a generic mechanism aimed at recovering information due to a number of threats, either random or deliberate. In the case of a ransomware incident, only new data generated after the last backup will be affected. For that, the backups should not be accessible to attackers. This way, it is necessary to balance data protection and the resources needed to achieve it. This way, the authors of reference [153] introduce improvements to the evaluation of security risks and develop a tool to analyze backups.

Amoeba [154] is a Solid-State Drive (SSD) backup and restoration system that detects infected pages through a hardware accelerator and minimizes the backup overhead. According to the evaluation provided by the authors, the tool gives a high detection accuracy due to the small total ratio of False Positives (FP) and False Negatives (FN), only 2.58%.

Safe Zone [155] maintains all the user's (compressed) files into a unique file (safe zone), which is always open for writing to prevent access by other resources. The application has a File Watcher register to collect the events of the safe zone. This way, the last version of the files is recovered from the safe zone in the case of a ransomware incident.

More recently, reference [156] considered a backup scheme called *RAP* (*RAnsomware Protection*) focused on confidentiality and DoS attacks. RAP adjusts the backup overhead and the recovery through a secure channel based on blockchain by using an AONT (*All-Or-NoThing*) optimization.

Another solution by Dell is PowerProtect Cyber Recovery [157], which duplicates every writing and adding operation. One of them is local (production system), while the second is remote over the network, in the recovery site. To measure the de-duplication rate, a time window is used so that a ransomware attack is concluded in case a given threshold on the rate is reached. In such a case, the remote I/O operations are inhibited to protect the data.

Some more daring proposals consider a specific filesystem, like *Model Core* [158]. It is decentralized and analyzes in real-time the client petitions to check data integrity (by monitoring the metadata structure of files) and conclude the potential infection. A private cloud is the proposed alternative for data backup in reference [159]. Furthermore, the proposal found in reference [160] affords file immunization by storing a backup of files at the end of them.

5.1.3. Deception Techniques

The relevance of deception techniques in computer security [161] is well known, since they constitute a pro-active defence approach. A formal study and test of such techniques can be found in reference [162]. For example, *RansomTracer* [163] is a *honeypot* designed to collect traces from an attack by using a monitored bait. The environment is configured to monitor remote access, clipboard, mounted disks and executable files. Likewise, a *honeyfile* is a trap file aimed at generating a notification if it is accessed. In this line, the authors of reference [164] propose to create a big central file to be monitored. In case a ransomware sample accesses the file, the time involved in ciphering it will be enough to allow the detection of this circumstance and to protect the rest of the archives.

Decoy files are a variety of trap files, where archives are deployed around the folders on the filesystem to compute the number of times a thread traverses the filesystem and generates a score to measure its potential malicious behavior [165].

Other specific practical deception systems are as follows. *RWGuard* [166] also uses decoy files to detect and trace the behavior of input/output processes and changes in files. To do this, a machine learning (ML)-related model is considered. *RansomWall* [167] uses the decoy file approach in a multi-layered defence. Thus, when a process is suspected to be malicious in the trap layer, the files are copied until determining if it is really malicious or benign on other layers. Furthermore, *SentryFS* [168] is a specialized filesystem that deploys trap files around the environment. Traps are generated using NLP (*Natural Language Processing*) and both content and metadata are constantly updated to be attractive for ransomware. Moreover, the proposal clones files to avoid the actual data being ciphered.

After that, an AI agent assigns the activity a suspicion value to allow users to approve or discard changes.

Focused on Android IoT devices, decoy files are used by *KRProtector* [169] to prevent ransomware in the ciphering phase without root privileges. *R-Sentry* deploys decoy files across the filesystem by analyzing the filesystem traversal patterns of existing ransomware samples. When the decoy file detects the access, the process is killed [170].

A more elaborated and current decoy-file-based approach is *R-Locker* [171,172], where authors deploy a set of trap files around the filesystem with the particularity that they are FIFO-based files. This way, once a ransomware sample accesses the file it is blocked by the OS. Thanks to that, a countermeasure is automatically launched to solve the problem with no affection to the rest of the filesystem.

In a different way, the proposed approach in reference [173] detects attacks when a decoy file disappears, it responds in such a case by making a system shutdown. *RTrap* [174] also creates deceptive files through machine learning to attract access to them by attackers (or ransomware). When detecting any access to deceptive files, RTrap autonomously contains the incident disconnecting the victim from the network and killing all the malicious processes. The proposed decoy-watcher can catch, contain and control the running of the ransomware in less than 5.35 s.

5.1.4. User Training and Awareness

As previously indicated, the attack vectors of ransomware are the same as those for malware in general. Considering that users are the weakest links in the security chain, social engineering and phishing are very relevant techniques. As a consequence, it is principal user training and awareness to effectively fight against ransomware.

In reference [175], the most relevant attack vectors for ransomware as well as the principal training and awareness aspects to be applied to mitigate social engineering are identified and analyzed. Software-based solutions like gamification and simulation are adequate to reach that goal. A similar study is performed in reference [176] to prevent spear phishing.

The authors of reference [177] apply PMT (*Protection Motivation Theory*) to investigate the motivation of users to adopt protection measures against ransomware. Experimentation establishes that the main motivation is derived from fear due to the severity and vulnerability of threats. The principal recommendations to users to fight against ransomware are as follows [178]: antivirus/anti-malware installation on computers and mobile devices, the use of strong and different passwords for personal and work computers, periodic security backups, not opening enclosed files in mail and the use of mirror shielding technologies. In addition, reference [179] proposes carrying out training exercises to help identify potential security breaches and guarantee the correctness of mitigation and recovery processes.

After analyzing the TTPs associated with different ransomware families, a predictive model regarding the characteristics of this threat is created. The model, *RANDEP* (*RANsomware and DEPloyment*) [180], allows for knowing when users are aware of the appearance of ransomware in the environment.

5.2. Detection of Crypto-Ransomware

The aim of deploying detection solutions relies on environment supervision to determine the potential occurrence of ransomware incidents [181]. If so, the necessary actions to thwart its effect as soon as possible will be launched [182].

Figure 5 shows a taxonomy of detection mechanisms for ransomware which is based on the previous ones in references [183,184]. This new taxonomy includes more detection schemes while unifying and organizing them better. Two main categories of detection approaches are defined: based on the data source considered and based on the processing performed.

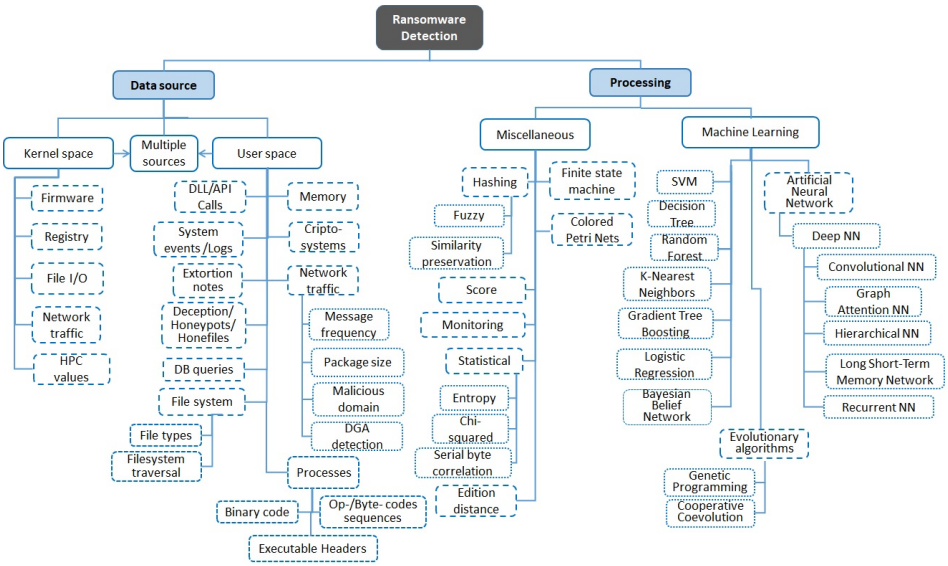

Figure 5. Taxonomy of detection schemes for ransomware.

5.2.1. Data Source

Detection solutions usually rely on dynamically monitoring diverse activities to obtain data from which to be able to conclude the occurrence of certain events. As indicated through Figure 5, such monitoring may involve kernel or user space. In the first case, detailed information about the inner state of the system can be obtained. For that, however, root privileges are required. In addition, developing a kernel module or controller is a complex and critical task, as a little error can give way to a generalized system error (i.e., kernel panic). It is also important to mention that installing a kernel controller is feasible for Windows or Linux platforms but that task is only allowed in mobile devices after jailbreaking/rooting them, which implies removing the security mechanisms in the system and, thus, exposing the device. On the other hand, monitoring the user space is easier but less complete than the kernel one from the perspective of knowing the real state of the device.

The most common activities to be monitored concern filesystem and storage devices. Works like that in reference [183] rely on the correlation between the number of bytes written into a file (usually low for ciphered files) and the edition distance of file names.

Ransomware uses the same I/O operations as regular users (e.g., read(), write()). In this way, the authors of reference [185] propose a system to learn the behavior of ransomware from header information in Input/Output (I/O) operations (block address, operation typology, data size) to detect ransomware. Also, reference [186] introduces a system to obtain the probability of ransomware based on the comparison of the current I/O activity with a historical one. These proposals, like the one in reference [187], rely on an unrestricted access to I/O request packets (IRP).

Gathering information from the user space is the approach used by *PayBreak* and *UShallNotPass* [143], which make use of hooks to intercept cryptographic library calls.

In reference [188], the authors introduce *Sentinel* to detect and recover data based on access patterns by using system mechanisms like audit logs, filter controllers (Windows), file system stack (Unix) or light events (Linux and IBM Spectrum Scale). In addition, reference [189] considers process creation patterns as well. Furthermore, the tool *ARW* in reference [190] combines the analysis of the life cycle of files with their content to detect cryptographic attacks.

As mentioned, system and service logs are also recurrent data sources for ransomware detection [191,192]. This is also the case of the system *DeepRan*, where *BiLSTM* (*Attention-based Bidirectional Long Short Term Memory*) is considered for detection [193]. Similarly,

reference [194] makes use of a number of features obtained through a forensic analysis of artifacts, like process descriptors or DLL (Dynamic-link Library), to feed a *XGBoost* (*eXtreme Gradient Boosting*) classifier.

The file typology or the extension can be modified when files are ciphered by ransomware. Such changes can be monitored to determine the presence of this kind of attack [166]. This work also uses the similarity of different file versions to detect ransomware actions.

API calls are recurrently monitored to determine the occurrence of a number of activities: C&C communications, privilege escalation, file access, ciphering and many other functions associated with ransomware action [195]. Some works, like references [196,197], analyze and filter API calls to obtain the most relevant ones. API calls can be also combined with DLL-related features like in reference [198].

Also, opcodes or bytecodes contain rich information about context and semantics, which provides information about the behavior of a given program. Some works that make use of these kinds of features are references [199–204], where ML models like SVM (Support Vector Classifier), HMM (Hidden Markov Model), CNN (Convolutional Neural Network) or RF (Random Forest) are used.

References [205,206] focus on variables related to executable programs in Windows like code size, image, DLL features or initialized data. Over them, ML detection methods like PCA (Principal Component Analysis), SVM, KNN (K-Nearest Neighbors) and RF are applied.

The authors of reference [207] make use of a number of features (entropy changes, apps retention state, lateral movement, system resources) to define an eight-final-states FSM (*Finite State Machine*). When one of these states is reached by the system, a ransomware event is concluded. Also, using a number of different features, the proposal in reference [208] relies on an ACO (*Ant Colony Optimization*) procedure for ransomware detection. More, Refs. [209,210] also makes use of a number of features among which are file ciphering rate, writing operations, registry changes, CPU usage or DLLs used.

Traffic monitoring is also relevant for ransomware detection, where features like packet size, message frequency and malicious domains, among others, support C&C communications occurrence. In this vein, the authors of reference [211] make use of *Domain Generation Algorithms* (DGA). Also, reference [212] considers message size in HTTP headers to detect *CryptoLocker* and *Locky* samples. In such a case, an SDN is used to stop the communication with the malicious domain. Also based on SDN and auto-organizative networks, reference [213] introduces a defence scheme against ransomware. The authors of reference [214] introduce *REDFISH*, a system to detect ransomware actions through monitoring network traffic for shared network data volumes. Further works in a similar vein can be found in references [215–217], where either generic traffic features (communication duration, protocol, IP addresses, etc.) or specific TCP-related features are considered by using ML algorithms like RF, SVM, DT (Decision Tree) and LR (Logistic Regression).

Since phishing is a recurrent attack vector, some researchers analyze URLs based on ML techniques to detect if they are malicious or benign by considering features like protocol, domain, path and other traffic features [218]. To detect ransomware samples against database servers, the proposal *DIMASQ* (*Dynamic Identification of Malicious Query Sequences*) is introduced in reference [219], where colored Petri networks are used to classify malicious requests.

In some cases, the detection proposal is focused on analyzing the extortion notice provided to the user once the data are ciphered. In reference [220], the ransomware embedded in Android apps is detected by comparing the similarity of a set of images of the analyzed program with a set of extortion images corresponding to ransomware variants. Reference [221] introduces a forensics tool to analyze the extortion pop-up message of the ransomware. Based on an OCR (*Optical Character Recognition*) process, the message and the payment instructions are recovered. More recently, the authors of reference [222] propose studying files related to ransomware to identify it. For that, LSA (*Latent Semantic Analysis*),

used to seek similarities among files, and ML, used to classify files as benign or malicious, are implemented.

A recent work is reference [223], where a ransomware SSD (State Solid Disk) (RSSD) controller is constructed based on an assisted hardware registry. This keeps old data copies in a conservative way and performs storage requests with a small overhead. Moreover, the subsequent analysis of the attack is allowed, from which we can obtain storage evidence for attack investigation purposes. Also based on hardware, the authors of reference [224] propose *RAPPER* to determine static and dynamic programs' integrity by using a model with a time series of HPC (*Hardware Performance Counter*). Furthermore, reference [225] introduces *RanStop*, where hardware events feed a neural network using the model LSTM (Long Short Term Memory). Similarly, reference [226] makes use of hardware profiles for Windows-related ransomware detection. A more recent work determines, for early detection, the most effective time frame and also the appropriate HPC registers [227].

A different approach is proposed in reference [228], where the cryptocoin rate and blockchain congestion are monitored over time. If an increase is detected, the system is blocked to avoid malware infection [229].

5.2.2. Processing

Whichever the data source considered, some kind of processing of the information collected is needed to conclude the occurrence of a ransomware event. As in the case of malware in general, detection schemes can be classified as signature-based or anomaly-based. That is, a set of well-known (ransomware-related) pre-defined patterns or behaviors are either detected, or a certain deviation with respect to the expected normal operation of the target system occurs.

An example of signature-based processing is the case of hashing, used, for example, in VirusTotal (https://www.virustotal.com/gui/home/search (accessed on 25 October 2023)), to identify and classify malicious samples. Hashing can also be used in combination with other techniques like diffuse signature and entropy to detect samples for which no signatures are known [230].

Other proposals consist of assigning values to quantify the malicious behavior of a process. This is the case of *Redemption* or *CryptoDrop*. This is also the case of reference [231], where YARA rules [232] are used to characterize the behavior of a sample based on API functions, extortion-related words, cryptographic signatures and file names. If the rule reaches a given threshold, the sample is classified as malicious. In comparison with signature-related detection, the anomaly-based paradigm is able to detect unknown malware samples.

There are a number of detection proposals based on entropy [166,233,234]. Also, the authors of reference [235] make use of entropy for file headers, the accuracy obtained being 99.96%. This feature feeds an SVM model to discriminate between malicious and benign files [236]. However, because entropy by itself cannot detect the differences between ciphered files and compressed files [237], or it can be even evaded [238,239], the analysis should be complemented. This is the case of reference [240], where a decoy file is additionally considered.

EntropySA and *DistSA* are ML-based schemes too but they make use of byte frequency and frequency variation, respectively, to reduce the cost of entropy [241]. Another possibility to reduce such a cost is to consider visualization, like in reference [242]. In this case, ransomware is described in terms of images which are analyzed by using neural networks.

Whatever the data gathered, ML algorithms are generally applied over them for detection purposes [243–246]. In reference [247], a comparison of ML-based ransomware detectors is performed. Table 3 shows the main ML-based detection techniques used in the literature and the features collected in each [248]. Let us remark on some works in the field. In reference [249], a natural language processing scheme is used over API calls. A Random Forest detection algorithm over DLL features combined with resource consumption (communications, RAM, CPU, disk, among other resources) and opened files is implemented in reference [250].

More novel, the proposal of *ZSL* (*ZeroShot Learning framework*) introduced in reference [251] is inspired by brain mechanisms to identify new concepts. The approach is based on API calls and is divided into two stages: the first one to learn basic features for ransomware, and the second to infer the final malicious or benign behavior.

API calls are monitored in reference [252], but, in this case, a previous binary static analysis is performed in a hybrid detector named *PEDA* (from *Pre-Encryption Detection Algorithm*). The authors of reference [253] propose a behavioral anomaly detector based on the combination of Random Forest, Decision Trees and K-Nearest Neighbor schemes. Furthermore, the authors of reference [254] introduce the system *DRTHIS* (*Deep Ransomware Threat Hunting and Intelligence System*) based on the combination of two ML techniques: LSTM and CNN.

Table 3. ML-based ransomware detection approaches.

Name	Classification Algorithm(s)	Feature(s)	Ref.
-	Random Forest (RF)	Raw bytes	[255]
DNAact-Ran	LiR	K-mer frequency	[256]
RansomWall	ANN, GTB, LR, RF, SVM	System calls/API	[167]
-	DT, LR, NB, RF	Logfiles	[166]
-	ANN, DT, KNN, LiR, LR, SVM	File I/O	[257]
PEDA	RF	System Calls/API	[252]
-	SVM	System calls/API	[258]
-	SVM	System calls/API	[259]
DPBD-FE	ANN, Boosting, CART, DT, KNN, LDA, LR, NB, RF	System calls/API	[260]
DRDT	CNN	System calls/API	[261]
-	ANN	Log files	[262]
-	KNN, LR, NB, RF, SGD, SVM	System calls/API	[263]
-	DT, LiR	System calls/API	[264]
-	AdaBoost, Bagging, BN, DT, LogiBoost, LR, NB, RF	System calls/API, RAM memory dump	[265]
iBagging/ESRS	Linear regression	System calls/API	[247]
RAPPER	ANN (LSTM)	HPC	[224]
-	BN, RF, SVM, RT	Network traffic	[266]
-	ANN, KNN, RF, SVM	CPU consumption	[267]
-	RF	Network traffic	[268]
-	CNN	Operation codes	[201]
-	SVM	Operation code sequences/*byte*	[269]
-	CNN	PE executable headers	[270]
-	DT, LR, NB, RF, SVM	DLL calls, Operation/bytes codes	[271]
-	DT, LR, RF, SVM	DLL calls, operation code/byte sequences	[272]
DRTHIS	CNN, LSTM	Event sequences	[254]
-	NB, SVM	Network traffic	[273]
DRDT	TextCNN	System calls	[261]
-	RF	DDL calls, OS resources	[250]
-	RF, OoW	DDL calls	[249]
-	KNN, LR, NB, RF, SGD, SVM	System calls	[195]
AIRaD	AI	DLL calls	[198]
DeepRan	BiLSTM, FC	Logs	[193]
RanStop	LSTM	Hardware events	[225]
MUSTARD	RF	Folders, file operations and types	[274]
DIMAQS	CPN, DNN	DB SQL queries	[275]
BGPGuard	CNNs, GBDT, GRU, LSTM, RNNs	Features selection	[276]
-	RF	Network traffic (PSO)	[277]
SwiftR	HNN, LSTM	Binary code, word-embedded)	[278]
RANDES	GAT	lists of assembly mnemonic	[279]
-	NN	API calls	[280]
-	GP, CC	API calls, extension of dropped files, Registry key operations, embedded strings	[281]

Abbreviations: ANN: Artificial Neural Network; BN: Bayesian Networks; CC: Cooperative Coevolution; DT: Decision Tree; GAT: Graph Attention Network; GP: Genetic Programming; GTB: Gradient Tree Boosting; HNN: Hierarchical Neural Network; KNN: K-Nearest Neighbors; LDA: Linear Discriminant Analysis; LiR: Linear Regression; LR: Logistic Regression; LSTM: Long Short-Term Memory; NB: Naïve Bayes; PSO: Particle Swarm Optimization; RF: Random Forest; SVM: Support Vector Machine.

5.3. Response to Crypto-Ransomware

Once ransomware is detected, it is necessary to launch the required actions to solve the event. Such a response is part of the so-called disaster recovery, contingency plan or business continuity [282,283].

Maybe the most evident reaction scheme is that of killing the malicious process when we are sure about its harmful nature. Another possibility is to put it under inspection to

obtain more indicators about its dangerous condition, although that can imply consuming more system resources. Additionally, it is also possible to notify users of the event so that they take corresponding corrective actions, which mainly rely on prevention mechanisms (e.g., data backups).

Depending on the affectation level of the target system, the first aspect involved in data recovery is that of ransom payment. Should we pay or not? The short answer is "No!". On the one hand, it should be noticed that the payment is considered an illegal action in some countries, which is mainly intended to reduce the success and impact of this kind of attack on society [284–286]. Moreover, payment is not the end of the story! First, it does not guarantee that the attacker will return the victim's data. Second, the data or the tools provided by the attacker to recover the information can be infected with malware. Finally, data can be stolen again later to demand additional ransom payments (provided the fact that the victim is demonstrated to be prone to pay!) [287].

As a consequence of all of the above, it is usually recommended to restore the complete system from scratch and restore the information from backups. A clarifying recovery experience from a crypto-ransomware attack can be found in reference [288].

To conclude pragmatically with defence techniques against ransomware, Table 4 shows the various anti-ransomware tools developed in the recent literature. As a general comment, detection solutions are prevalent, in particular those focused on filesystem monitoring.

Table 4. Anti-ransomware tools (modified from reference [183]).

	Detection													Recovery				
	Source		ML			Processing				Actions				Sources			Processing	Actions
Name	Kernel	User	DT	RF	ANN	Scoring	Monitoring	Statistical	Distance	Kill	Block	Isolation	Notify	I/O	Cache	API	Deletion	Restoration
KRProtector		H					✓						✓					
RAPPER	AC			✓		✓			✓			✓						
R-Killer	FS	N			✓		✓			✓			✓					
R-Locker		H					✓			✓	✓		✓					
SSD-Insider	S		✓									✓	✓	✓	✓		✓	✓
UShallNotPass		PR					✓			✓		✓	✓					

Abbreviations: AC: Access Control; CS: Crypto-system; FS: File system; H: Honeyfile; N: Network; PR: Pseudo random number generator API; S: Storage.

Regarding a comparison among tools, the framework *FARFEL* [71] analyzes the behavior of detectors from the perspective of accuracy, false positive rate and capacity to detect polymorphic samples and new attack patterns. Moreover, a comparison of them from the perspective of computation and system overhead can be done by using tools of thirds like *CrystalDiskMark* [289], *Geekbench 5* [290] or PCMark 10 [291].

A fundamental issue in developing detection tools is the disposal of working samples for the necessary experimentation purposes. First, with learning and model estimation objectives and second, to allow valid comparisons between alternative solutions based on the same test corpora (reproducibility). Table 5 shows a number of repositories from which researchers usually get real samples. Despite the utility of such repositories, it is important to mention that, in some cases, a number of potential samples are not really operative (in the range of 12–67%, depending on the work). It is also convenient to pay attention to the necessity of adequately labeling the samples, not only from the perspective of the family they belong to but also from the perspective of their real ransomware nature. All of this would introduce a notable bias, if not directly a malfunction, in the developed systems.

Another interesting question is the dataset age and how it affects the detection accuracy of supervised machine learning models. A recent paper proves that supervised machine learning models trained using datasets with new ransomware samples are inefficient in detecting old types of ransomware and vice versa [292].

Table 5. Ransomware samples repositories (modified from reference [293]).

Work	No. Samples	No. Active samples	TP Rate	Ratio Active Samples/Family	Source of the Collection or Method
Ahmed [196]	1254	673	98.8	48.1	virusshare.com, virustotal.com (accessed on 25 October 2023), spider to repositories, forums
Berrueta [294]	70	NA	NA	NA	PCAP repository http://dataset.tlm.unavarra.es/ransomware/ (accessed on 25 October 2023)
Cabaj [212]	NA	787	98	395.5	malwr.com, ransomtracker.abuse.ch (accessed on 25 October 2023)
ISOT [295]	669	NA	NA	NA	www.uvic.ca/ecs/ece/isot/datasets/botnet-ransomware/ (accessed on 25 October 2023)
Morato [214]	NA	54	100	2.8	NA
RISSP [296]	540	NA	NA	NA	github.com/rissgrouphub/ransomwaredataset2016 (accessed on 23 October 2023)
Temple [297]	1156	NA	NA	NA	Critical Infrastructures incidents (2013–2021) https://sites.temple.edu/care/ci-rw-attacks/ (accessed on 25 October 2023)
CIRW [298]	NA	NA	NA	NA	Critical Infrastructure RansomWare. Available by request
Zscaler ThreatLabz	NA	NA	NA	NA	Repository of ransom notes https://github.com/threatlabz/ransomware_notes/ (accessed on 25 October 2023)

NA: Not Available

6. Trends and Challenges

After studying the overall current context of crypto-ransomware, this section is devoted to briefly pointing out the main trends and challenges regarding this threat, which continues to be a principal security threat worldwide [112,299]. In fact, ransomware is not only dangerous but an ever-changing and dynamic form of crime. Some of the keys to this dynamism and the associated risks are as follows.

Crypto-ransomware is usually assumed to consume a number of resources mainly due to cryptographic procedures. In addition, a lot of detection and recovery solutions are based on the local disposal of ciphered files and/or ciphering keys. Regretfully, this situation has evolved over the years, so that new ransomware samples *(i)* can apply only a partial ciphering (around 3–5%) to quick affectation and detection evasion [300,301], and *(ii)* can steal information from the target system instead of, or as well as, ciphering (and locally storing) it [302]. All of this compels us to develop new, more varied and faster detection schemes to minimize system damage. In other words, early detection is a mandatory requirement since the so-called *Time-To-Ransom* (i.e., the time between the initial compromise of the system and the execution of ransomware) is decreasing with new samples. Otherwise, the effective detection can be useless as the system will be already seriously affected. For that, lightweight detection and fast recovery procedures are needed, especially for mobile and IoT-related devices which are characterized by low resources and computation capacities.

Also, related to the above question, one more relevant issue in ransomware fighting is that of detection in Big Data environments, as the computational cost and the detection response involved can make the mechanisms deployed useless. In this regard, authors usually propose performing the feature selection process in order to reduce the problem dimension. For that, schemes like *FeSA* [248], *PCA*, *FA* (*Factor Analysis*), *TSVD* (*Truncated Singular Value Decomposition*) [303] or *VIF* (*Variance of Inflation Factor*) [304] are analyzed. Despite the existence of all those proposals, the increasing speed of current computation and transmission technologies, together with the complexity of new ransomware samples, make it necessary to continue researching and innovating fast and early detection solutions.

As previously explained, ML algorithms are commonly considered in the detection of ransomware solutions. Despite the results usually being satisfactory, ML schemes present some limitations and potential improvements [305,306]:

- Estimating the adequate model is a complex task, since the occurrence of over/under-training, and thus bias, is feasible [307].
- The cost involved in ML classification and detection techniques can be high. To avoid that, dimensional reduction techniques are useful, like PCA in reference [308].

- Despite current detection schemes being efficient, new ransomware samples can implement novel tactics to evade detection procedures in what is called *Adversarial ML* [309]. To solve this problem, hybrid classifiers are developed, which combine both static and dynamic features [310] or different classification algorithms (ensemble malware detection) [243].
- Also related to detection evasion, papers like reference [204] analyze the resilience of ML algorithms against security incidents.

One more relevant aspect of current ransomware is that of life expectation [311]. A decreasing trend is observed in this line, with ∼500 days in 2017 to 60 days in 2021. This fact can be explained by the brand-changing strategy followed by the RaaS operators to hide criminal organizations. For instance, Evil Corp has performed several attacks with different brands: Hades, Phoenix Crypotolocker and Doppelpaymer, among others. Despite the changes that could be unveiled, for instance, by discovering code similarities or following crypto-payments and flow movements searching for similar behaviors and patterns [312], it is evident that the methodology makes its prosecution more difficult.

As pointed out by the authors of reference [313], the growth of ransomware is a consequence of its high degree of economic efficiency and impunity. Current studies are focused on issues such as the juridical implications of ransomware when it is to be considered a law breach under data privacy or data protection laws, but legality should be strengthened and adapted to new technical methodologies to fight against this criminal practice. In the end, without a proper legal sanction and without a proper punishment, the crime will be repeated and extended because of the lack of harmful consequences for the aggressor. For that, several changes should be carried out: *(i)* typifying ransomware as an autonomous and specific crime, due to its technical uniqueness; *(ii)* penalizing incitement, complicity and attempts to commit this offence to limit or reduce its impunity; *(iii)* prohibiting and penalizing insurance contracts for the payment of ransoms to prevent legal instruments from becoming an additional incentive for criminals in a regrettable perversion of the system; *(iv)* the international cooperation is a main instrument for dealing with the impunity arising from the fact that it is a generally transnational crime (as a relevant example in this direction, it should be remarked that a number of countries have recently discussed fighting together against ransomware (https://therecord.media/u-s-convenes-30-countries-on-ransomware-threat-without-russia-or-china/ - accessed on 25 October 2023), and also the private sector should be involved in this common objective (https://www.europol.europa.eu/media-press/newsroom/news/13-countries-join-global-fight-against-ransomware-0 - accessed on 25 October 2023-)); *(v)* promoting crypto-currency exchange and payment regulations as they largely support ransomware proliferation [314].

In summary, ransomware is continuously evolving and thus the efforts to defeat it must be redoubled. In this vein, and according to the recent work in reference [315], it is likely that the behavior of ransomware will gradually evolve and refine its operation mode to achieve the following: *(i)* steal crypto-currencies; *(ii)* guide targets toward cloud and IoT; *(iii)* migrate from ransomware payload to business email compromise (BEC); *(iv)* use the kill chain for stock market manipulation; and *(v)* use the supply chain compromise as a service. As a direct consequence of that continuous evolution, we are aware that the current work is limited in drawing lasting conclusions and, thus, new overviews on the topic should be conducted in the future to shed light on the possible new variants and families of crypto-ransomware that appear.

7. Conclusions

The impact of crypto-ransomware attacks in recent years is indubitable, with heavy losses in terms of both economic and reputation to individuals, companies and organizations all around the world. Regretfully, and despite the efforts in fighting against the threat, that trend will prevail in the coming years. In this way, the main aim of this work is to go into depth about the current fundamentals of this typology of attack regarding infection and attack models, the actors involved and the lifecycle stages to deploy its

malicious load to better understand the inherent operation of such malware and, from it, to develop more effective defence schemes. Also, the principal milestones of the evolution of crypto-ransomware over time are presented and the most famous families and extortion cases are discussed.

In order to complete the study of crypto-ransomware attacks at present, the most relevant works in the last recent years are also presented in this paper. For that, they are organized according to the main defence line for which they are intended: prevention, detection, response or recovery. Such an overview allows us to know the variety and capability of the existing proposals, as well as their restrictions and limitations. Moreover, the main trends in ransomware infection are presented with the aim of forecasting new attack procedures and defence requirements, in particular the convenience of strengthening public and private legal-related collaborations to successfully defeat this scourge.

In summary, the main goal of this work is to update the knowledge and efforts to date against crypto-ransomware, with the aim of fighting against it and minimizing its impact and damage to society.

Author Contributions: Conceptualization, J.A.G.H. and P.G.T.; Investigation/Resources, J.A.G.H. and P.G.T.; Supervision/Validation/Visualization, J.A.G.H., P.G.T., R.M.C. and R.R.G.; Writing original draft, J.A.G.H., P.G.T., R.M.C. and R.R.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by MCIN/AEI 10.13039/501100011033 grant, by project PID2020-114495RB-I00.

Data Availability Statement: No datasets were generated during the current study. The cited datasets are described in the corresponding publication of the bibliography.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. TrendLabs: Ransomware: Past, Present and Future. Report. 2022. Available online: https://documents.trendmicro.com/assets/wp/wp-ransomware-past-present-and-future.pdf (accessed on 25 October 2023) .
2. ENISA: ENISA Threat Landscape (July 2021 to July 2022). European Union Agency for Cybersecurity. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 (accessed on 25 October 2023).
3. Liska, A. *Ransomware: Understand, Prevent, Recover*; ActualTech Media, North Charleston, SC, USA, 2021.
4. Corbet, S.; Goodell, J.W. The reputational contagion effects of ransomware attacks. *Financ. Res. Lett.* **2022**, *47*, 102715. [CrossRef]
5. Microsoft. Destructive Malware Targeting Ukranian Organizations. Available online: https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (accessed on 25 October 2023).
6. Embroker. Top 10 Cybersecurity Threats in 2022. Available online: https://www.embroker.com/blog/top-10-cybersecurity-threats-2022/ (accessed on 25 October 2023).
7. Imperva. 2021 Cyberthreat Defense Report. Cyberedge Group. 2021. Available online: https://www.imperva.com/resources/resource-library/reports/2021-cyberthreat-defense-report/ (accessed on 25 October 2023).
8. Morrison, A. Cyber Security Landscape 2022. Deloitte. 2022. Available online: https://docplayer.net/228758092-Cyber-security-landscape-2022.html (accessed on 25 October 2023).
9. Al-rimy, B.A.S.; Maarof, M.A.; Shaid, S.Z.M. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Comput. Secur.* **2018**, *74*, 144–166. [CrossRef]
10. Kumar, P.R.; Ramlie, H.R.E.B.H. Anatomy of Ransomware: Attack Stages, Patterns and Handling Techniques. In *Computational Intelligence in Information Systems (CIIS)*; Advances in Intelligent Systems and Computing; Suhaili, W.S.H., Siau, N.Z., Omar, S., Phon-Amuaisuk, S., Eds.; Springer: Cham, Switzerland, 2021; Volume 1321. [CrossRef]
11. Beaman, C.; Barkworth, A.; Akande, T.D.; Hakak, S.; Khan, M.K. Ransomware: Recent advances, analysis, challenges and future research directions. *Comput. Secur.* **2021**, *111*, 102490. [CrossRef] [PubMed]
12. Buker, K. Ransomware as a Service (RaaS) Explained. Crowstrike. February 2022. Available online: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (accessed on 25 October 2023).
13. Barr-Smith, F.; Ugarte-Pedrero, X.; Graziano, M.; Spolaor, R.; Martinovic, I. Survivalism: Systematic Analysis of Windows Malware Living-Off-The-Land. In Proceedings of the IEEE Symposium on Security and Privacy (SP), Francisco, CA, USA, 24–27 May 2021; pp. 1557–1574. [CrossRef]
14. Lakshmanan, R. Dridex Malware Deploying Entropy Ransomware on Hacked Computers. The Hacker News. February 2022. Available online: https://thehackernews.com/2022/02/dridex-malware-deploying-entropy.html (accessed on 25 October 2023).
15. Insikt Group. New Ransomware-as-a-Service Tool 'Thanos' Shows Connections to 'Hakbit'. Recorded Future. June 2020. Available online: https://www.recordedfuture.com/thanos-ransomware-builder/ (accessed on 25 October 2023).

16. de Jesús, M.; Ladores, D.O. Chaos Ransomware: A Proof of Concept With Potentially Dangerous Applications. Trend Micro. August 2021. Available online: https://www.trendmicro.com/en_us/research/21/h/chaos-ransomware-a-dangerous-proof-of-concept.html (accessed on 25 October 2023).
17. Gray, I.W.; Cable, J.; Cuiujuclu, V.; Brown, B.; McCoy, D. Money Over Morals: A Business Analysis of Conti Ransomware. In Proceedings of the IEEE Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 30 November–2 December 2022. Available online: https://damonmccoy.com/papers/Ransomware_eCrime22.pdf (accessed on 25 October 2023).
18. Schwartz, M.J. Cybercrime Moves: Conti Ransomware Absorbs TrickBot Malware, Baank Info Security. February 2022. Available online: https://www.bankinfosecurity.com/cybercrime-moves-conti-ransomware-absorbs-trickbot-malware-a-18573 (accessed on 25 October 2023).
19. Dargahi, T.; Dehghantanha, A.; Bahrami, P.N.; Conti, M.; Bianchi, G. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *J. Comput. Virol. Hack Tech.* **2019**, *15*, 277–305. [CrossRef]
20. Mirza, Q.K.A.; Brown, M.; Halling, O.; Shand, L.; Alam, A. Ransomware Analysis using Cyber Kill Chain. In Proceedings of the 8th International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy, 23–25 August 2021; pp. 58–65. [CrossRef]
21. Mahdipour, E.; Aghamohammadpour, A.; Attarzadeh, I. Ransomware Modeling Based on a Process Mining Approach. *Int. J. Inf. Commun. Technol.* **2022**, *14*, 27–36. [CrossRef]
22. Martin, L. The Cyber Kill Chain. Available online: http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html (accessed on 25 October 2023).
23. Mayukha, S.; Vadivel, R. Reconnaissance for Penetration Testing Using Active Scanning of MITRE ATT&CK. In *Information and Communication Technology for Competitive Strategies (ICTCS 2021)*; Lecture Notes in Networks and Systems; Kaiser, M.S., Xie, J., Rathore, V.S., Eds.; Springer: Singapore, 2023; Volume 401. [CrossRef]
24. Zimba, A.; Wang, Z. Malware-Free Intrusions: Exploitation of Built-in Pre-Authentication Services for APT Attack Vectors. *Int. J. Comput. Netw. Inf. Secur. (IJCNIS)* **2017**, *9*, 1–10. [CrossRef]
25. Xiong, W.; Legrand, E.; Åberg, O.; Lagerström, R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Softw. Syst. Model* **2022**, *21*, 157–177. [CrossRef]
26. Genç, Z.A.; Lenzini, G.; Ryan, P.Y.A. Next Generation Cryptographic Ransomware. In *Secure IT Systems. NordSec 2018*; Lecture Notes in Computer Science; Gruschka, N., Ed.; Springer: Cham, Switzerland, 2018; Volume 11252. [CrossRef]
27. Olaimat, M.N.; Maarof, M.A.; Al-rimy, B.A.S. Ransomware Anti-Analysis and Evasion Techniques: A Survey and Research Directions. In Proceedings of the 3rd International Cyber Resilience Conference (CRC), Virtual, 29–31 January 2021; pp. 1–6. [CrossRef]
28. Afianian, A.; Niksefat, S.; Sadeghiyan, B.; Baptiste, D. Malware Dynamic Analysis Evasion Techniques: A Survey. *ACM Comput. Surv.* **2020**, *52*, 1–28. [CrossRef]
29. Veerappan, C.S.; Keong, P.L.K.; Tang, Z.; Tan, F. Taxonomy on malware evasion countermeasures techniques. In Proceedings of the IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 5–8 February 2018; pp. 558–563. [CrossRef]
30. Wilson, C. Forensic Analysis of the Zone. Identifier Stream, Digital Forensic. Blog, 2021. Available online: https://www.digital-detective.net/forensic-analysis-of-zone-identifier-stream/ (accessed on 25 October 2023).
31. Ghafarian, A.; Keskin, D.; Helton, G. An Assessment of Obfuscated Ransomware Detection and Prevention Methods. In *Advances in Information and Communication. FICC 2021*; Advances in Intelligent Systems and Computing; Arai, K., Ed., Springer: Cham, Switzerland, 2021; Volume 1363. [CrossRef]
32. Hassan, N.A. Ransomware Distribution Methods. In *Ransomware Revealed*; Apress: Berkeley, CA, USA, 2019. [CrossRef]
33. Gangwar, K.; Mohanty, S.; Mohapatra, A.K. Analysis and Detection of Ransomware Through Its Delivery Methods. In *Data Science and Analytics. REDSET 2017*; Communications in Computer and Information Science; Panda, B., Sharma, S., Roy, N., Eds.; Springer: Singapore, 2018; Volume 799. [CrossRef]
34. Alkhalil, Z.; Hewage, C.; Nawaf, L.; Khan, I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Front. Comput. Sci.* **2021**, *3*, 563060. [CrossRef]
35. Salahdine, F.; Kaabouch, N. Social Engineering Attacks: A Survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
36. Veeam. 2021 Ransomware Retrospective. Veeam Software. 2021. Available online: https://www.veeam.com/2021-ransomware-retrospective.html (accessed on 30 October 2022).
37. He, G.Q.; Liu, C.; Huang, A. Ransomware Families: 2021 Data to Supplement the Unit42 Ransomware Threat Report. Unit42. July 2021. Available online: https://unit42.paloaltonetworks.com/ransomware-families/ (accessed on 25 October 2023).
38. VirusTotal. Ransomware in a Global Context. 2021. Available online: https://www.virustotal.com/go/ransomware-in-a-global-context-2021 (accessed on 30 October 2022).
39. Trend Micro. Exploit kit. Available online: https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit (accessed on 25 October 2023).
40. Suren, E.; Angin, P. Know Your EK: A Content and Workflow Analysis Approach for Exploit Kits. *J. Internet Serv. Inf. Secur. (JISIS)* **2019**, *9*, 24–47. Available online: http://isyou.info/jisis/vol9/no1/jisis-2019-vol9-no1-02.pdf (accessed on 25 October 2023).
41. Trend Micro. New Exploit Kit Fallout Delivering Gandcrab Ransomware. 2018. Available online: https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/new-exploit-kit-fallout-delivering-gandcrab-ransomware (accessed on 25 October 2023).

42. Gatlan, S. Maze Ransomware Now Delivered by Spelevo Exploit Kit. Blee Ping Computer. October 2019. Available online: https://www.bleepingcomputer.com/news/security/maze-ransomware-now-delivered-by-spelevo-exploit-kit/ (accessed on 25 October 2023).
43. Malware Bytes. GandCrab Ransomware Distributed by RIG and GrandSoft Exploit Kits. Malware Bytes. January 2018. Available online: https://www.malwarebytes.com/blog/news/2018/01/gandcrab-ransomware-distributed-by-rig-and-grandsoft-exploit-kits (accessed on 25 October 2023).
44. CSW. Ransomware—Through the Lens of Threat and Vulnerability Management. CSW SecurityWorks, Spotlight Report, Index Update Q2–Q3. 2022. Available online: https://cybersecurityworks.com/ransomware/ (accessed on 25 October 2023).
45. S21Sec. Threat Landscape Report. S21Sec Cyber Solutions, Second semester of 2022. Available online: https://www.s21sec.com/es/descargar-threat-landscape-report/ (accessed on 25 October 2023).
46. Van Impe, K. How Attackers Exploit the Remote Desktop Protocol. Security Intelligence. 15 November 2021. Available online: https://securityintelligence.com/articles/exploiting-remote-desktop-protocol/ (accessed on 25 October 2023).
47. Stocchetti, V. (Ed.) Exploited Protocols: Server Message Block (SMB). Center for Internet Security (CSI). 2021. Available online: https://learn.cisecurity.org/CIS_Controls_v8_Exploited_Protocols_Server_Message_Block_SMB (accessed on 30 October 2022).
48. Cimpanu, C. Top Exploits Used by Ransomware Gangs are VPN Bugs, but RDP Still Reigns Supreme. ZDNet. August 2020. Available online: https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/ (accessed on 25 October 2023).
49. Ogu, E.C.; Ojesanmi, O.A.; Awodele, O.; Kuyoro, S. A Botnets Circumspection: The Current Threat Landscape, and What We Know So Far. *Information* **2019**, *10*, 337. [CrossRef]
50. Fortinet. The Ins and Outs of the Ransomware: How to Mitigate Email-based Attacks. Fortinet White Paper. 2019, Available online: https://www.insightsforprofessionals.com/it/security/the-ins-and-outs-of-ransomware (accessed on 25 October 2023).
51. Yuste, J.; Pastrana, S. Avaddon ransomware: An in-depth analysis and decryption of infected systems. *Comput. Secur.* **2021**, *109*, 102388. [CrossRef]
52. Yüceel, H.C. TTPs used by BlackByte Ransomware Targeting Critical Infrastructure. Pycus Security. February 2022. Available online: https://www.picussecurity.com/resource/ttps-used-by-blackbyte-ransomware-targeting-critical-infrastructure (accessed on 25 October 2023).
53. Mendrez, R. BlackByte Ransomware—Pt. 1 In-Depth Analysis. Trustwave. October 2021. Available online: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/blackbyte-ransomware-pt-1-in-depth-analysis/ (accessed on 25 October 2023).
54. Hill, J. ALPHV (BlackCat) Ransomware, Inside Out Security. January 2022. Available online: https://www.varonis.com/blog/alphv-blackcat-ransomware (accessed on 25 October 2023).
55. Tanner, A.; Hinchliffe. Threat Assessment: BlackCat Ransomware. Palo Alto Network. January 2022. Available online: https://unit42.paloaltonetworks.com/blackcat-ransomware/ (accessed on 25 October 2023).
56. Kara, I.; Aydos, M. Static and Dynamic Analysis of Third Generation Cerber Ransomware. In Proceedings of the International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 3–4 December 2018; pp. 12–17. [CrossRef]
57. Pletinckx, S.; Trap, C.; Doerr, C. Malware Coordination using the Blockchain: An Analysis of the Cerber Ransomware. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–9. [CrossRef]
58. Kurniawan, A.; Riadi, I. Detection and Analysis Cerber Ransomware Based on Network Forensics Behavior. *Int. J. Netw. Secur.* **2018**, *20*, 836–843. [CrossRef]
59. DFIR. Diavol Ransomware. The DFIR Report. December 2021. Available online: https://thedfirreport.com/2021/12/13/diavol-ransomware/ (accessed on 25 October 2023).
60. Neemani, D.; Rubinfeld, A. Diavol—A New Ransomware Used By Wizard Spider? Forninet. July 2021. Available online: https://www.fortinet.com/blog/threat-research/diavol-new-ransomware-used-by-wizard-spider (accessed on 25 October 2023).
61. Masson, D. What the EKANS Ransomware Attack Reveals about the Future of OT Cyber-Attacks. Darktrace Blog. June 2020. Available online: https://www.darktrace.com/en/blog/what-the-ekans-ransomware-attack-reveals-about-the-future-of-ot-cyber-attacks/ (accessed on 25 October 2023).
62. Dragos. EKANS Ransomware and ICS Operations. Dragos. March 2020. Available online: https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/ (accessed on 25 October 2023).
63. Bradt, A. Dridex Bots Deliver Entropy Ransomware in Recent Attacks. Sophos News. February 2022. Available online: https://news.sophos.com/en-us/2022/02/23/dridex-bots-deliver-entropy-ransomware-in-recent-attacks/ (accessed on 25 October 2023).
64. Palazolo, G.; Duarte, F. Reverse Engineering Dridex and Automating IOC Extraction. Appgate. September 2020. Available online: https://www.appgate.com/blog/reverse-engineering-dridex-and-automating-ioc-extraction (accessed on 25 October 2023).
65. CCN-CERT. Hive ransomware. CCN-CERT ID-15/21. December 2021. Available online: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6326-ccn-cert-id-15-21-hive-ransomware-1/file.html (accessed on 25 October 2023).

66. Muir, M. Analysis of Novel Khonsari Ransomware Deployed by the Log4Shell Vulnerability. Cado Security. December 2021. Available online: https://www.cadosecurity.com/analysis-of-novel-khonsari-ransomware-deployed-by-the-log4shell-vulnerability/ (accessed on 25 October 2023).
67. MacRae, J.; Franqueira, V.N.L. On Locky Ransomware, Al Capone and Brexit. In *Digital Forensics and Cyber Crime. ICDF2C 2017*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Matoušek, P., Schmiedecker, M., Eds.; Springer: Cham, Switzerland, 2018; Volume 216. [CrossRef]
68. Broadhurst, R.; Trivedi, H. Malware in spam email: Risks and trends in the Australian spam intelligence database. Trends and Issues in Crime and Criminal Justice. *Electron. Resour.* **2020**, *603*, 1–18. [CrossRef]
69. Avast. A Closer Look at the Locky Ransomware. Avast. March 2016. Available online: https://blog.avast.com/a-closer-look-at-the-locky-ransomware (accessed on 25 October 2023).
70. Bison, D. MegaCortex Ransomware v2 Released With Anti-Analysis Features, Security Intelligence. 2019. Available online: https://securityintelligence.com/news/megacortex-ransomware-v2-released-with-anti-analysis-features/ (accessed on 25 October 2023).
71. Gupta, S. Kaseya VSA Downed by REvil in Monumental Supply-Chain Attack. CSOnline. July 2021. Available online: https://cybersecurityworks.com/blog/ransomware/kaseya-vsa-downed-by-revil-in-monumental-supply-chain-attack.html (accessed on 25 October 2023).
72. Elshinbary, A. Deep Analysis of Ryuk Ransomware. GitHub. May 2020. Available online: https://n1ght-w0lf.github.io/malwareanalysis/ryuk-ransomware/ (accessed on 25 October 2023).
73. Mason, B. Ryuk Malware - Analysis and Reverse Engineering. Ben's ideas and projects Blog. April 2020. Available online: https://ben.the-collective.net/posts/2020-04-08-ryuk-malware-analysis-and-reverse-engineering/ (accessed on 25 October 2023).
74. Avertium. An In-Depth Look at Ransomware Gang. Sabbath. January 2022. Available online: https://www.avertium.com/resources/threat-reports/in-depth-look-at-sabbath-ransomware-gang (accessed on 25 October 2023).
75. McAfee. McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service—What The Code Tells Us. McAfee. October 2019. Available online: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-analyzes-sodinokibi-aka-revil-ransomware-as-a-service-what-the-code-tells-us/ (accessed on 25 October 2023).
76. Shushan, A.B.; Lifshitz, N.; Kushnir, A.; Korman, M.; Wasserman, B. Lazarus Group's Mata Framework Leveraged To Deploy TFlower Ransomware. Sygnia. August 2021. Available online: https://blog.sygnia.co/lazarus-groups-mata-framework-leveraged-to-deploy-tflower-ransomware (accessed on 25 October 2023).
77. Hybrid Analysis. tflower.exe. October 2019. Available online: https://hybrid-analysis.com/sample/7ca3494c165647424222f80b8b61a9fb80ff695c2be77a9fb6a0a352f5df3140?environmentId=120 (accessed on 25 October 2023).
78. Kao, D.; Hsiao, S. The dynamic analysis of WannaCry ransomware. In Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Republic of Korea, 11–14 February 2018; pp. 159–166. [CrossRef]
79. Hsiao, S.; Kao, D. The static analysis of WannaCry ransomware. In Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT), Chuncheon, Republic of Korea, 1–14 February 2018; pp. 153–158. [CrossRef]
80. Chesti, I.A.; Humayun, M.; Sama, N.U.; Zaman, N. Evolution, Mitigation, and Prevention of Ransomware. In Proceedings of the 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 13–15 October 2020; pp. 1–6. [CrossRef]
81. Zimba, A.; Chishimba, M. Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures. *Int. J. Comput. Netw. Inf. Secur. (IJCNIS)* **2019**, *11*, 26–39. [CrossRef]
82. Ramsdell, K.A.W.; Esbeck, K.E. Evolution of Ransomware. The Mitre Corporation. July 2021. Available online: https://healthcyber.mitre.org/wp-content/uploads/2021/08/Ransomware-Paper-V2.pdf (accessed on 25 October 2023).
83. Martin, J.; Whelan, C. Ransomware through the lens of state crime. *State Crime J.* **2023**, *12*, 1–25. [CrossRef]
84. Zscaler. CovidLock: Android Ransomware Walkthrough and Unlocking Routine. 2020. Available online: https://www.zscaler.com/blogs/security-research/covidlock-android-ransomware-walkthrough-and-unlocking-routine (accessed on 25 October 2023).
85. Goliate. Hidden-Tear. Available online: https://github.com/goliate/hidden-tear (accessed on 25 October 2023).
86. Ryu, S. Anatomy of Chaos Ransomware Builder and Its Origin (feat. Open-source Hidden Tear Ransomware). S2W Blog. August 2021. Available online: https://medium.com/s2wblog/anatomy-of-chaos-ransomware-builder-and-its-origin-feat-open-source-hidden-tear-ransomware-ffd5937d005f (accessed on 25 October 2023).
87. Zhang, X.; Xiao, X. Thoughts on Vulnerability Security by Ransomware Virus. *Int. J. Soc. Sci. Educ. Res.* **2022**, *5*, 120–124. [CrossRef]
88. Security. COVID-19 Pandemic Sparks 72% Ransomware Growth, Mobile Vulnerabilities Grow 50%. Security Magazine. July 2020. Available online: https://www.securitymagazine.com/articles/92886-covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50 (accessed on 25 October 2023).
89. Europol. COVID-19: Ransomware. December 2021. Available online: https://www.europol.europa.eu/covid-19/covid-19-ransomware (accessed on 25 October 2023).
90. McAfee. McAfee Labs COVID-19 Threats Report. July 2020. Available online: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-covid-19-report-reveals-pandemic-threat-evolution/ (accessed on 25 October 2023).

91. Lallie, H.S.; Shepherd, L.A.; Erola, J.C.N.A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [CrossRef]
92. Gatlan, S. Qlocker Ransomware Returns to Target QNAP NAS Devices Worldwide. BleepingComputer. January 2022. Available online: https://www.bleepingcomputer.com/news/security/qlocker-ransomware-returns-to-target-qnap-nas-devices-worldwide/ (accessed on 25 October 2023).
93. Sachiel. Analysis of 'Heaven's Gate' Part 1. January 2021. Available online: https://sachiel-archangel.medium.com/analysis-of-heavens-gate-part-1-62cca0ace6f0 (accessed on 25 October 2023).
94. Lifars. A Deep Dive into The Grief Ransomware's Capabilities. Lifars. 2021. Available online: https://www.lifars.com/wp-content/uploads/2020/11/Whitepaper-Cybersecurity-Exercises-1.0.pdf (accessed on 25 October 2023).
95. Varma, G.; Chauhan, R. Cybercriminals Strike Where It Hurts Most: SARS-Cov-2 Pandemic and its Influence on Critical Infrastructure Ransomware Attacks. In Proceedings of the 16th International Conference on Ubiquitous Information Management and Communication (IMCOM), Seoul, Republic of Korea, 3–5 January 2022; pp. 1–7. [CrossRef]
96. Din, A. The Full Source Code for the Babuk Ransomware Published on a Russian Hacker Forum. Heimdal Security. September 2021. Available online: https://heimdalsecurity.com/blog/the-full-source-code-for-the-babuk-ransomware-published-on-a-russian-hacker-forum/ (accessed on 25 October 2023).
97. Tudor, D. Babuk Focuses On Data-Theft Extortion. Heimdal Security. May 2020. Available online: https://heimdalsecurity.com/blog/babuk-focuses-on-data-theft-extortion/ (accessed on 25 October 2023).
98. Sadeen, A. Ransomware's Favorite Target: Critical Infrastructure and Its Industrial Control Systems. Dark Reading. March 2023. Available online: https://www.darkreading.com/ics-ot/ransomware-s-favorite-target-critical-infrastructure-and-its-industrial-control-systems (accessed on 25 October 2023).
99. CyberEdge. 2023 Cyberthreat Defense Report. CyberEdge Group, 2023. Available online: https://betanews.com/2023/04/11/multiple-threat-ransomware-attacks-become-more-common/ (accessed on 25 October 2023).
100. Hammond, C.; Villadsen, O. Ex-Conti and FIN7 Actors Collaborate with New Domino Backdoor. Security Intelligence. April 2023. Available online: https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-domino-backdoor/ (accessed on 25 October 2023).
101. Nelson, N. IceFire Ransomware Portends a Broader Shift From Windows to Linux. Dark Reading. March 2023. Available online: https://www.darkreading.com/endpoint/icefire-ransomware-portends-broader-shift-windows-linux (accessed on 25 October 2023).
102. Kovacs, E. LockBit Ransomware Group Developing Malware to Encrypt Files on macOS. Security Weeks. April 2023. Available online: https://www.securityweek.com/lockbit-ransomware-group-developing-malware-to-encrypt-files-on-macos/ (accessed on 25 October 2023).
103. Invictus. Ransomware in the Cloud. Invictus Incident Response. April 2023. Available online: https://invictus-ir.medium.com/ransomware-in-the-cloud-7f14805bbe82 (accessed on 25 October 2023).
104. Raheem, A.; Raheem, R.; Chen, T.M.; Alkhayyat, A. Estimation of Ransomware Payments in Bitcoin Ecosystem. In Proceedings of the IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), New York, NY, USA, 30 September–3 October 2021; pp. 1667–1674. [CrossRef]
105. Bin Mohamed Yunus, Y.K.; Bin Ngah, S. Ransomware: Stages, detection and evasion. In Proceedings of the International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM), Pekan, Malaysia, 24–26 August 2021; pp. 227–231. [CrossRef]
106. Meland, P.H.; Bayoumy, Y.F.F.; Sindre, G. The Ransomware-as-a-Service economy within the darknet. *Comput. Secur.* **2020**, *1017*, 92. [CrossRef]
107. Karapapas, C.; Pittaras, I.; Fotiou, N.; Polyzos, G.C. Ransomware as a Service using Smart Contracts and IPFS. In Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–5. [CrossRef]
108. Kapoor, A.; Gupta, A.; Gupta, R.; Tanwar, S.; Sharma, G.; Davidson, I.E. Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. *Sustainability* **2022**, *14*, 8. [CrossRef]
109. Farhat, D.; Awan, M.S. A Brief Survey on Ransomware with the Perspective of Internet Security Threat Reports. In Proceedings of the 9th International Symposium on Digital Forensics and Security (ISDFS), Elazig, Turkey, 28–29 June 2021; pp. 1–6. [CrossRef]
110. Mehra, C.; Sharma, A.K.; Sharma, A. Elucidating Ransomware Attacks In Cyber-Security. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *9*, 3536–3541. [CrossRef]
111. Haber, M.J. *Privileged Attack Vectors*; Apress: Berkeley, CA, USA, 2020. [CrossRef]
112. Kerner, M. Ransomware Trends, Statistics and Facts in 2021. TechTarger. November 2021. Available online: https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts (accessed on 25 October 2023).
113. Blessman, D. Protecting Your Software Supply Chain. *Risk Manag.* **2019**, *66*, 10–11.
114. Haber, M.J.; Hills, C.; Chappell, B.; Maude, J. Beyond Trust Cybersecurity Trend Predictions for 2022 & Beyond. BeyondTrust. October 2021. Available online: https://www.beyondtrust.com/blog/entry/beyondtrust-cybersecurity-trend-predictions-for-2022 (accessed on 25 October 2023).

115. Vaas, L. Ransomware Payments Explode Amid 'Quadruple Extortion'. ThreatPost. 2021. Available online: https://threatpost.com/ransomware-payments-quadruple-extortion/168622/ (accessed on 25 October 2023).
116. Radware. 2021–2022 Global Threat Analysis Report. Radware Ltd. 2022. Available online: https://www.radware.com/2021-2022-global-threat-analysis-report/ (accessed on 25 October 2023).
117. Collier, K. Ransomware Hackers' New Tactic: Calling You Directly. NBC News. January 2022. Available online: https://www.nbcnews.com/tech/security/ransomware-hackers-new-tactic-calling-directly-rcna6466 (accessed on 25 October 2023).
118. Barker, W.C.; Fisher, W.; Scarfone, K.; Souppaya, M. *NIST 8374*; Ransomware Risk Management: A Cybersecurity Framework Profile. National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2022. [CrossRef]
119. Bradley, S. Ransomware. SANS Whitepapers. 2021. Available online: https://www.sans.org/white-papers/37317/ (accessed on 25 October 2023).
120. Ekta; Bansal, U. A Review on Ransomware Attack. In Proceedings of the 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), Jalandhar, India, 21–23 May 2021; pp. 221–226. [CrossRef]
121. CIS. Ransomware Impacts and Defense Controls. Available online: https://www.cisecurity.org/insights/blog/ransomware-impacts-and-defense-controls (accessed on 25 October 2023).
122. CCCS. Ransomware playbook (ITSM.00.099). Canadian Centre for Cyber Security. 2021. Available online: https://cyber.gc.ca/sites/default/files/cyber/2021-12/itsm00099-ransomware-playbook-2021-final3-en.pdf (accessed on 25 October 2023).
123. Sharma, N.; Shanker, R. Analysis of Ransomware Attack and Their Countermeasures: A Review. In Proceedings of the International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 16–18 March 2022; pp. 1877–1883. [CrossRef]
124. Midtrapanon, S.; Wills, G. Linux patch management: With security assessment features. In Proceedings of the 4th International Conference on Internet of Things, Big Data and Security, Heraklion, Crete, Greece, 2–4 May 2019; pp. 270–277.
125. Liu, W. Modeling Ransomware Spreading by a Dynamic Node-Level Method. *IEEE Access* **2019**, *7*, 142224–142232. [CrossRef]
126. Nair, A. The Why and How of adopting Zero Trust Model in Organizations. *TechRxiv* **2021**, techrxiv.14184671.v1. Available online: https://www.techrxiv.org/articles/preprint/The_Why_and_How_of_adopting_Zero_Trust_Model_in_Organizations/14184671/1 (accessed on 25 October 2023). [CrossRef]
127. Atanassov, N.; Chowdhury, M.M. Mobile Device Threat: Malware. In Proceedings of the IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, 14–15 May 2021; pp. 007–013. [CrossRef]
128. Galinkin, E. Winning the Ransomware Lottery. In *Decision and Game Theory for Security. GameSec 2021*; Lecture Notes in Computer Science; Bošanský, B., González, C., Rass, S., Sinha, A., Eds.; Springer: Cham, Switzerland, 2021; Volume 13061. [CrossRef]
129. CIS. Ransomware: The Data Exfiltration and Double Extortion Trends. Center for Internet Security. Available online: https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trend (accessed on 25 October 2023).
130. Pagán, A.; Elleithy, K. A Multi-Layered Defense Approach to Safeguard Against Ransomware. In Proceedings of the 11th IEEE Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 27–30 January 2021; pp. 0942–0947. [CrossRef]
131. Margarov, G.; Mitrofanova, E. Management of Ransomware Detection and Prevention in Multilevel Environmental Monitoring Information System. In *Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security*; NATO Science for Peace and Security Series C: Environmental Security; Sidorenko, A., Hahn, H., Eds.; Springer: Dordrecht, The Netherlands, 2020; pp. 125–131. [CrossRef]
132. Salunke, M.D.; Kumbharkar, P.B.; Pramod, K. A Proposed Methodology to Mitigate the Ransomware Attack. In *Recent Trends in Intensive Computing*; Rajesh, M., Vengatesan, K., Gnanasekar, M., Sitharthan, R., Pawar, A.B., Kalvadekar, P.N., Saiprasad, P.M., Eds.; IOS Press: Amsterdam, The Netherlands 2021; Volume 39, pp. 16–21. [CrossRef]
133. Singh, A.; Ikuesan, A.R.; Venter, H.S. Digital Forensic Readiness Framework for Ransomware Investigation. In *Digital Forensics and Cyber Crime. ICDF2C 2018*; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Breitinger, F., Baggili, I., Eds.; Springer: Cham, Switzerland, 2019; Volume 259, pp. 91–105. [CrossRef]
134. Mundt, M.; Baier, H. Threat-based Simulation of Data Exfiltration Towards Mitigating Multiple Ransomware Extortions. *Digit. Threat. Res. Pract.* **2022**, *4*, 54. [CrossRef]
135. Keshavarzi, M.; Ghaffary, H.R. An ontology-driven framework for knowledge representation of digital extortion attacks. *Comput. Hum. Behav.* **2023**, *139*, 107520. [CrossRef] [PubMed]
136. Zhang, C.; Luo, F.; Ranzi, G. Multistage Game Theoretical Approach for Ransomware Attack and Defense. *IEEE Trans. Serv. Comput.* **2023**, *16*, 2800–2811. [CrossRef]
137. Tiu, Y.L.; Zolkipli, M.F. Study on Prevention and Solution of Ransomware Attack. *J. IT Asia* **2021**, *9*, 133–139. [CrossRef]
138. Manjezi, Z.; Botha, R.A. Preventing and Mitigating Ransomware. In *Information Security. ISSA 2018*; Communications in Computer and Information Science; Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., Eds.; Springer: Cham, Switzerland, 2019; Volume 973, pp. 149–162. [CrossRef]
139. McIntosh, T.; Kayes, A.S.M.; Chen, Y.P.; Ng, A.; Watters, P. Dynamic user-centric access control for detection of ransomware attacks. *Comput. Secur.* **2021**, *111*, 102461. [CrossRef]
140. Ami, O.; Elovici, Y.; Hendler, D. Ransomware prevention using application authentication-based file access control. In Proceedings of the 33rd Annual ACM Symposium on Applied Computing, New York, NY, USA, 9–13 April 2018; pp. 1610–1619. [CrossRef]

141. Turaev, H.; Zavarsky, P.; Swar, B. Prevention of Ransomware Execution in Enterprise Environment on Windows OS: Assessment of Application Whitelisting Solutions. In Proceedings of the 1st International Conference on Data Intelligence and Security (ICDIS), South Padre Island, TX, USA, 8–10 April 2018; pp. 110–118. [CrossRef]
142. Kim, D.; Lee, J. Blacklist vs. Whitelist-Based Ransomware Solutions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 22–28. [CrossRef]
143. Genç, Z. A.; Lenzini, G.; Ryan, P. No random, no ransom: A key to stop cryptographic ransomware. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science*; Springer: Cham, Switzerland, 2018; Volume 10885, pp. 234–255. [CrossRef]
144. Lee, S.; Kim, H.K.; Kim, K. Ransomware protection using the moving target defense perspective. *Comput. Electr. Eng.* **2019**, *78*, 288–299. [CrossRef]
145. McIntosh, T.; Watters, P.; Kayes, A.; Ng, A.; Chen, Y. Enforcing situation-aware access control to build malware-resilient file systems. *Future Gener. Comput. Syst.* **2021**, *115*, 568–582. [CrossRef]
146. VLCM, Sophos Intercept X: The World's Best Endpoint Protection. 2023. Available online: https://www.vlcm.com/intercept-x (accessed on 25 October 2023).
147. Microsoft. Protect Important Folders with Controlled Folder Access. 2022. Available online: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/controlled-folders?view=o365-worldwide (accessed on 25 October 2023).
148. Microsoft. What's new in Microsoft Defender for Identity. 2023. Available online: https://learn.microsoft.com/en-us/defender-for-identity/whats-new (accessed on 25 October 2023).
149. Ahn, J.; Park, D.; Lee, C.; Min, D.; Lee, J.; Park, S.; Chen, Q.; Kim, Y. KEY-SSD: Access-Control Drive to Protect Files from Ransomware Attacks. *arXiv* **2019**. [CrossRef]
150. Siddiqui, A.S.; Lee, C.-C.; Saqib, F. Hardware based protection against malwares by PUF based access control mechanism. In Proceedings of the 60th IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, USA, 6–9 August 2017; pp. 1312–1315. [CrossRef]
151. Akbanov, M.; Vassilakis, V.G.; Logothetis, M.D. Ransomware detection and mitigation using software-defined networking: The case of WannaCry. *Comput. Electr. Eng.* **2019**, *76*, 111–121. [CrossRef]
152. McIntosh, T.; Kayes, A.S.M.; Chen, Y.P.P.; Ng, A.; Watters, P. Applying staged event-driven access control to combat ransomware. *Comput. Secur.* **2023**, *128*, 103160. [CrossRef]
153. Thomas, J.; Galligher, G. Improving backup system evaluations in information security risk assessments to combat ransomware. *Comput. Inf. Sci.* **2018**, *11*, 14–25. [CrossRef]
154. Min, D.; Park, D.; Ahn, J.; Walker, R.; Lee, J.; Park, S.; Kim, Y. Amoeba: An autonomous backup and recovery ssd for ransomware attack defense. *IEEE Comput. Archit. Lett.* **2017**, *17*, 245–248. [CrossRef]
155. Baykara, M.; Sekin, B. A novel approach to ransomware: Designing a safe zone system. In Proceedings of the 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–5. [CrossRef]
156. Lao, W.; Chen, Z.; Gao, B.; Wang, J.; Ta, Y.; Zhang, R. RAP: RAnsomware Protection Scheme Based on Blockchain. In Proceedings of the 2nd International Conference on Consumer Electronics and Computer Engineering (ICCECE), Guangzhou, China, 14–16 January 2022; pp. 13–20. [CrossRef]
157. Dell. Dell PowerProtect Cyber Recovery. 2022. Available online: https://www.delltechnologies.com/asset/zh-hk/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf (accessed on 25 October 2023).
158. Tafkov, S.; Minchev, Z. Decentralized File Storage and Ransomware Protection. In Proceedings of the 12th International Conference on Business Information Security (BISEC-2021), Belgrade, Serbia, 3 December 2021; pp. 1–4. [CrossRef]
159. Golev, A.; Hristev, R.; Veselinova, M.; Kolev, K. Crypto-ransomware attacks on Linux servers: A data recovery method. *Int. J. Differ. Equ. Appl.* **2022**, *21*, 19–29. [CrossRef]
160. Hutton, W. Immunizing Files Against Ransomware with Koalafied Immunity. In *Intelligent Computing, Proceedings of the 2022 Computing Conference*; Lecture Notes in Networks and Systems; Arai, K., Eds.; Springer: Cham, Switzerland, 2022; Volume 508, pp. 735–741. [CrossRef]
161. Han, X.; Kheir, N.; Balzarotti, D. Deception Techniques in Computer Security: A Research Perspective. *ACM Comput. Surv.* **2019**, *51*, 80. [CrossRef]
162. Genç, Z.A.; Lenzini, G.; Sgandurra, D. On Deception-Based Protection Against Cryptographic Ransomware. In *Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2019*; Lecture Notes in Computer Science; Perdisci, R., Maurice, R., Giacinto, G., Almgren, M., Eds.; Springer: Cham, Switzerland, 2019; Volume 11543. [CrossRef]
163. Wang, Z.; Wu, X.; Liu, C.; Liu, Q.; Zhang, J. RansomTracer: Exploiting Cyber Deception for Ransomware Tracing. In Proceedings of the IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 21 June 2018; pp. 227–234. [CrossRef]
164. Patel, A.; Tailor, J.P. A malicious activity monitoring mechanism to detect and prevent ransomware. *Comput. Fraud. Secur.* **2020**, *2020*, 14–19. [CrossRef]
165. Moussaileb, R.; Bouget, B.; Palisse, A.; Le Bouder, H.; Cuppens-Boulahia, N.; Lanet, J.L. Ransomware's Early Mitigation Mechanisms. In Proceedings of the 13th International Conference on Availability, Reliability and Security, New York, NY, USA, 27–30 August 2018; pp. 1–10. [CrossRef]

166. Mehnaz, S.; Mudgerikar, A.; Bertino, E. RWGuard: A Real-Time Detection System Against Cryptographic Ransomware. In *Research in Attacks, Intrusions, and Defenses*; Lecture Notes in Computer Science; Bailey, M., Holz, T., Stamatogiannakis, M., Ioannidis, S., Eds.; Springer: Cham, Switzerland, 2018; Volume 11050, pp. 114–136. [CrossRef]
167. Shaukat, S.K.; Ribeiro, V.J. RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. In Proceedings of the 10th International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 3–7 January 2018; pp. 356–363. [CrossRef]
168. Al-Nemera, G.; Al-Otaibi, S.; Tahir, R.; Alkhatib, M. Making Honey Files Sweeter: SentryFS—A Service-Oriented Smart Ransomware Solution. *arXiv* **2021**. [CrossRef]
169. Wang, S.; Zhang, H.; Qin, S.; Li, W.; Tu, T.; Shen, A.; Liu, W. KRProtector: Detection and Files Protection for IoT Devices on Android Without ROOT Against Ransomware Based on Decoys. *IEEE Internet Things J.* **2022**, *9*, 18251–18266. [CrossRef]
170. Sheen, S.; Asmitha, K.A.; Venkatesan, S. R-Sentry: Deception based ransomware detection using file access patterns. *Comput. Electr. Eng.* **2022**, *103*, 108346. [CrossRef]
171. Gómez-Hernández, J.A.; Álvarez-González, L.; García-Teodoro, P. R-Locker: Thwarting Ransomware Action through a Honeyfile-based Approach. *Comput. Secur.* **2018**, *73*, 389–398. [CrossRef]
172. Gómez-Hernández, J.A.; Sánchez-Fernández, R.; García-Teodoro, P. Inhibiting crypto-ransomware on Windows platforms through a honeyfile-based approach with R-Locker. *IET Inf. Secur.* **2021**, *16*, 64–74. [CrossRef]
173. Lin, Y.S.; Lee, C.F. Ransomware Detection and Prevention through Strategically Hidden Decoy File. *Int. J. Netw. Secur.* **2023**, *25*, 212–220. [CrossRef]
174. Ganfure, G.O.; Wu, C.F.; Chang, Y.H.; Shih, W.K. RTrap: Trapping and Containing Ransomware With Machine Learning. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 1433–1448. [CrossRef]
175. Bello, A.; Maurushat, A. Technical and Behavioural Training and Awareness Solutions for Mitigating Ransomware Attacks. In *Applied Informatics and Cybernetics in Intelligent Systems. CSOC 2020*; Advances in Intelligent Systems and Computing; Silhavy, R., Eds.; Springer: Cham, Switzerland, 2020; Volume 1226. [CrossRef]
176. Thomas, J. Individual Cyber Security: Empowering Employees to Resist Spear Phishing to Prevent Identity Theft and Ransomware Attacks. *Int. J. Bus. Manag.* **2018**, *13*, 1–14 . [CrossRef]
177. Ophoff, J.; Lakay, M. Mitigating the Ransomware Threat: A Protection Motivation Theory Approach. In *Information Security. ISSA 2018*; Communications in Computer and Information Science; Venter, H., Loock, M., Coetzee, M., Eloff, M., Eloff, J., Eds.; Springer: Cham, Switzerland, 2019; Volume 973, pp. 163–175. [CrossRef]
178. Chung, M. Why employees matter in the fight against ransomware. *Comput. Fraud. Secur.* **2019**, *8*, 8–11. [CrossRef]
179. Angafor, G.N.; Yevseyeva, I.; He, Y. Bridging the Cyber Security Skills Gap: Using Tabletop Exercises to Solve the CSSG Crisis. In *Serious Games. JCSG 2020*; Lecture Notes in Computer Science; Ma, M., Fletcher, B., Göbel, S., Baalsrud Hauge, J., Marsh, T., Eds.; Springer: Cham, Switzerland, 2020; Volume 12434, pp. 117–131. [CrossRef]
180. Hull, G.; John, H.; Arief, B. Ransomware deployment methods and analysis: Views from a predictive model and human responses. *Crime Sci.* **2019**, *8*, 2. [CrossRef]
181. Maigida, A.M.; Abdulhamid, S.M.; Olalere; Ismaila. An Intelligent Crypto-Locker Ransomware Detection Technique using Support Vector Machine Classification and Grey Wolf Optimization Algorithms. *i-manager's J. Softw. Eng.* **2019**, *13*, 15–23. [CrossRef]
182. Nadir, I.; Bakhshi, T. Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In Proceedings of the International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 3–4 March 2018; pp. 1–7. [CrossRef]
183. Pont, J.; Abu Oun, O.; Brierley, C.; Arief, B.; Hernández-Castro, J. A Roadmap for Improving the Impact of Anti-ransomware Research. In *Secure IT Systems, NordSec*; Lecture Notes in Computer Science; Askarov, A., Hansen, R., Rafnsson, W., Eds.; Springer: Cham, Switzerland, 2019; Volume 11875. [CrossRef]
184. Herrera Silva, J.A.; Barona López, L.I.; Valdivieso Caraguay, A.L.; Hernández-Álvarez, M.A. A Survey on Situational Awareness of Ransomware Attacks, Detection and Prevention Parameters. *Remote Sens.* **2019**, *10*, 1168. [CrossRef]
185. Baek, S.; Jung, Y.; Mohaisen, A.; Lee, S.; Nyang, D. SSD-insider: Internal defense of solid-state drive against ransomware with perfect data recovery. In Proceedings of the IEEE 38th International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria, 2–5 July 2018; pp. 875–884. [CrossRef]
186. Natanzon, A.; Derbeko, P.; Stern, U.; Bakshi, M.; Manusov, Y. Ransomware detection using I/O patterns. US Patent 10,078,459, 2018.
187. Bottazzi, G.; Italiano, G.; Spera, D. Preventing Ransomware Attacks Through File System Filter Drivers. In Proceedings of the Second Italian Conference on Cyber Security, Milan, Italy, 6–9 February 2018; pp. 1–10.
188. Constantinescu, C.; Seshadri, S. Sentinel: Ransomware detection in file storage. In Proceedings of the 14th ACM International Conference on Systems and Storage (SYSTOR), New York, NY, USA, 14–16 June 2021; Volume 1, p. 28. [CrossRef]
189. Ahmed, M.E.; Kim, H.; Camtepe, S.; Nepa, S. Peeler: Profiling Kernel-Level Events to Detect Ransomware. In *Computer Security—ESORICS 2021*; Lecture Notes in Computer Science; Bertino, E., Shulman, H., Waidner, M., Eds.; Springer: Cham, Switzerland, 2021; Volume 12972, pp. 240–260. [CrossRef]

190. May, M.J.; Laron, E. Combating Ransomware using Content Analysis and Complex File Events. In Proceedings of the 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 24–26 June 2019; pp. 1–5. [CrossRef]
191. Herrera Silva, J.A.; Hernández-Alvarez, M. Large scale ransomware detection by cognitive security. In Proceedings of the IEEE Second Ecuador Technical Chapters Meeting (ETCM), Salinas, Ecuador, 16–20 October 2017; pp. 1–4. [CrossRef]
192. Bahrani, A.; Bidgly, A.J. Ransomware detection using process mining and classification algorithm. In Proceedings of the 16th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Mashhad, Iran, 28–29 August 2019; pp. 73–77. [CrossRef]
193. Roy, K.C.; Chen, Q. DeepRan: Attention-based BiLSTM and CRF for Ransomware Early Detection and Classification. *Inf. Syst. Front.* **2021**, *23*, 299–315. [CrossRef]
194. Arfeen, A.; Khan, M.A.; Zafar, O.; Ahsan, U. Process based volatile memory forensics for ransomware detection. *Concurr. Comput. Pr. Exper.* **2022**, *34*, e6672. [CrossRef]
195. Moreira, C.; Sales, C., Jr.; Moreira, D. Understanding Ransomware Actions Through Behavioral Feature Analysis. *JCIS* **2022**, *37*, 61–76. [CrossRef]
196. Ahmed, Y.A.; Koçer, B.; Al-rimy, B.A.S. Automated Analysis Approach for the Detection of High Survivable Ransomware. KSII Trans. *Internet Inf. Syst.* **2020**, *14*, 2236–2257. [CrossRef]
197. Ahmed, Y.A.; Koçer, B.; Huda, S.; Al-rimy, B.A.S.; Hassan, M.M. System call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. *J. Netw. Comput. Appl.* **2020**, *167*, 102753. [CrossRef]
198. Poudyal, S.; Dasgupta, D. Analysis of Crypto-Ransomware Using ML-Based Multi-Level Profiling. *IEEE Access* **2021**, *9*, 122532–122547. [CrossRef]
199. Sharma, S.; Kumar, R.; Krishna, C.R. A survey on analysis and detection of Android ransomware. *Concurr. Comput. Pr. Exper.* **2021**, *33*, e6272. [CrossRef]
200. Saleh, M.A. A Proactive Approach for Detecting Ransomware based on Hidden Markov Model (HMM). *Int. J. Intell. Comput. Res. (IJICR)* **2019**, *10*, 1004–1013. [CrossRef]
201. Zhang, B.; Xiao, W.; Xiao, X.; Sangaiah, A.K.; Zhang, W.; Zhang, J. Ransomware classification using patch-based CNN and self-attention network on embedded N-grams of opcodes. *Future Gener. Comput. Syst.* **2020**, *110*, 708–720. [CrossRef]
202. Zhang, H.; Xiao, X.; Mercaldo, F.; Ni, S.; Martinelli, F.; Sangaiah, A.K. Classification of ransomware families with machine learning based on N-gram of opcodes. *Future Gener. Comput. Syst.* **2019**, *90*, 211–221. [CrossRef]
203. Sharma, S.; Singh, S. Texture-Based Automated Classification of Ransomware. *J. Inst. Eng. India Ser. B* **2021**, *102*, 131–142. [CrossRef]
204. Chen, Q.; Islam, S.R.; Haswell, H.; Bridges, R.A. Automated Ransomware Behavior Analysis: Pattern Extraction and Early Detection. In *Science of Cyber Security. SciSec 2019*; Lecture Notes in Computer Science; Liu, F., Xu, J., Xu, S., Yung, M., Eds.; Springer: Cham, Switzerland, 2019; Volume 11933, pp. 1–16. [CrossRef]
205. Ayub, M.A.; Sira, A. Similarity Analysis of Ransomware based on Portable Executable (PE) File Metadata. In Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 5–7 December 2021; pp. 1–6. [CrossRef]
206. Ganta, V.G.; Harish, G.; Kumar, V.; Rao, G.R. Ransomware Detection in Executable Files Using Machine Learning. In Proceedings of the International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 12–13 November 2020; pp. 282–286. [CrossRef]
207. Ramesh, G.; Menen, A. Automated dynamic approach for detecting ransomware using finite-state machine. *Decis. Support Syst.* **2020**, *138*, 113400. [CrossRef]
208. Xia, T.; Sun, Y.; Zhu, S.; Rasheed, Z.; Hassan-Shafique, K. A Network-Assisted Approach for Ransomware Detection. *arXiv* **2020**, arXiv:2008.12428.
209. Goyal, P.S.; Kakkar, A.; Vinod, G.; Joseph, G. Crypto-Ransomware Detection Using Behavioural Analysis. In *Reliability, Safety and Hazard Assessment for Risk-Based Technologies*; Lecture Notes in Mechanical Engineering; Varde, P., Prakash, R., Vinod, G., Eds.; Springer: Singapore, 2020; pp. 239–251. [CrossRef]
210. Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R. Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence. *IEEE Trans. Emerg. Top. Comput.* **2018**, *8*, 341–351. [CrossRef]
211. Salehi, S.; Shahriari, H.; Ahmadian, M.M.; Tazik, L. A Novel Approach for Detecting DGA-based Ransomwares. In Proceedings of the 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC), Tehran, Iran, 28–29 August 2018; pp. 1–7. [CrossRef]
212. Cabaj, K.; Gregorczyk, M.; Mazurczyk, W. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. *Comput. Electr. Eng.* **2018**, *66*, 353–368. [CrossRef]
213. Monge, M.A.S.; Vidal, J.M.; García Villalba, L.J. A novel Self-Organizing Network solution towards Crypto-ransomware Mitigation. In Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES), New York, NY, USA, 27–30 August 2018; pp. 1–10. [CrossRef]
214. Morato, D.; Berrueta, E.; Magaña, E.; Izal, M. Ransomware early detection by the analysis of file sharing traffic. *J. Netw. Comput. Appl.* **2018**, *124*, 14–32. [CrossRef]

215. Almousa, M.; Osawere, J.; Anwar, M. Identification of Ransomware families by Analyzing Network Traffic Using Machine Learning Techniques. In Proceedings of the Third International Conference on Transdisciplinary AI (TransAI), Laguna Hills, CA, USA, 20–22 September 2021; pp. 19–24. [CrossRef]
216. Alhawi, O.M.K.; Baldwin, J.; Dehghantanha, A. Leveraging Machine Learning Techniques for Windows Ransomware Network Traffic Detection. In *Cyber Threat Intelligence*; Advances in Information Security; Dehghantanha, A., Conti, M., Dargahi, T., Eds.; Springer: Cham, Switzerland, 2018; Volume 70. [CrossRef]
217. Modi, J.; Traore, I.; Ghaleb, A.; Ganame, K.; Ahmed, S. Detecting Ransomware in Encrypted Web Traffic. In *Foundations and Practice of Security FPS 2019*; Lecture Notes in Computer Science; Benzekri, A., Barbeau, M., Gong, G., Laborde, R., Garcia-Alfaro, J.; Eds.; Springer: Cham, Switzerland, 2020; Volume 12056 [CrossRef]
218. Chaithanya, B.N.; Brahmananda, S.H. Detecting Ransomware Attacks Distribution Through Phishing URLs Using Machine Learning. In *Computer Networks and Inventive Communication Technologies*; Lecture Notes on Data Engineering and Communications Technologies; Smys, S., Bestak, R., Palanisamy, R., Kotuliak, I., Eds.; Springer: Singapore, 2022; Volume 75, pp. 821–832. [CrossRef]
219. Iffländer, L.; Dmitrienko, A.; Hagen, C.; Jobst, M.; Kounev, S. Hands Off my Database: Ransomware Detection in Databases through Dynamic Analysis of Query Sequences. *arXiv* **2019**, arXiv:1907.06775.
220. Alzahrani, A.; Alshehri, A.; Alshahrani, H.; Alharthi, R.; Fu, H.; Liu, A.; Zhu, Y., . RanDroid: Structural Similarity Approach for Detecting Ransomware Applications in Android Platform. In Proceedings of the IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 0892–0897. [CrossRef]
221. García Villalba, L.J.; Orozco, A.L.S.; López Vivar, A; Vega, E.A.A.; Kim, T.H. Ransomware Automatic Data Acquisition Tool. *IEEE Access* **2018**, *6*, 55043–55052. [CrossRef]
222. Lemmou, Y.; Lanet, J.L.; Souidi, E.M. In-Depth Analysis of Ransom Note Files. *Computers* **2021**, *10*, 145. [CrossRef]
223. Reidys, B.; Liu, P.; Huang, J. RSSD: Defend against ransomware with hardware-isolated network-storage codesign and post-attack analysis. In Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), New York, NY, USA, 27 April–1 May 2022; pp. 726–739. [CrossRef]
224. Ala, M.; Sinh, S.; Bhattachary, S.; Dutta, S.; Mukhopadhyay, D.; Chattopadhyay, A. RAPPER: Ransomware prevention via performance counters. *arXiv* **2018**. [CrossRef]
225. Pundir, N.; Tehranipoor, M.; Fahim, F. RanStop: A Hardware-assisted Runtime Crypto-Ransomware Detection Technique. *arXiv* **2020**. [CrossRef]
226. Aurangzeb, S.; Rais, R.N.B.; Aleem, M.; Islam, M.A.; Iqbal, M.A. On the classification of Microsoft-Windows ransomware using hardware profile. *PeerJ Comput. Sci.* **2021**, *7*, e361. [CrossRef]
227. Anand, P.M.; Charan, P.V.S.; Shukla, S.K. Early Detection of Ransomware Activity based on Hardware Performance Counters. In Proceedings of the 2023 Australasian Computer Science Week January, New York, NY, USA, 30 January–3 February 2023; pp. 10–17. [CrossRef]
228. Sokolov, K. Ransomware Activity and Blockchain Congestion. *J. Financ. Econ.* **2018**, *141*, 771–782. [CrossRef]
229. Balachandar, A.; Alsowdh, A.; Arumugam, K. Design and Development of Future Estimate in Confronting Ransomware. *J. Phys. Conf. Ser.* **2021**, *1717*, 012063. [CrossRef]
230. Joshi, Y.S.; Mahajan, H.; Joshi, S.N.; Gupta, K.P.; Agarkar, A.A. Signature-less ransomware detection and mitigation. *J. Comput. Virol. Hack Tech.* **2021**, *17*, 299–306. [CrossRef]
231. Medhat, M.; Gaber, S.; Abdelbaki, N. A New Static-Based Framework for Ransomware Detection. In Proceedings of the IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Athens, Greece, 25–28 October 2018; pp. 710–715. [CrossRef]
232. Yara. Yara's Documentation. Available online: https://yara.readthedocs.io/en/stable/ (accessed on 25 October 2023).
233. Keyes, D.S.; Li, B.; Kaur, G.; Lashkari, A.H.; Gagnon, F.; Massicotte, F. EntropLyzer: Android Malware Classification and Characterization Using Entropy Analysis of Dynamic Characteristics. In Proceedings of the Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS), Hamilton, ON, Canada, 17–19 May 2021; pp. 1–12. [CrossRef]
234. Zhu, J.; Jang-Jaccard, J.; Singh, A.; Welch, I.; AI-Sahaf, H.; Camtepe, S. A Few-Shot Meta-Learning based Siamese Neural Network using Entropy Features for Ransomware Classification. *arXiv* **2021**, arXiv:2112.00668.
235. Simon, R.D.; Macfarlane, R.; Buchanan, W.J. Differential area analysis for ransomware attack detection within mixed file datasets. *Comput. Secur.* **2021**, *108*, 1–14. [CrossRef]
236. Hsu, C.M.; Yang, C.C.; Cheng, H.H.; Setiasabda, P.E.; Leu, J.S. Enhancing File Entropy Analysis to Improve Machine Learning Detection Rate of Ransomware. *IEEE Access* **2021**, *9*, 138345–138351. [CrossRef]
237. McIntosh, T.; Jang-Jaccard, J.; Watters, P.; Susnjak, T. The Inadequacy of Entropy-Based Ransomware Detection. In *Neural Information Processing. ICONIP 2019*; Communications in Computer and Information Science; Gedeon, T., Wong, K., Lee, M., Eds.; Springer: Cham, Switzerland, 2019; Volume 1143. [CrossRef]
238. Boutsikas, J.; Eren, M.E.; Varga, C.; Raff, E.; Matuszek, C.; Nicholas, C. Evading malware classifiers via monte carlo mutant feature discovery. *arXiv* **2021**, arXiv:2106.07860.
239. Lee, J.; Lee, K. A Method for Neutralizing Entropy Measurement-Based Ransomware Detection Technologies Using Encoding Algorithms. *Entropy* **2022**, *24*, 239. [CrossRef] [PubMed]

240. Jiao, J.; Zhao, H.; Liu, Y. Analysis and Detection of Android Ransomware for Custom Encryption. In Proceedings of the IEEE 4th International Conference on Computer and Communication Engineering Technology (CCET), Beijing, China, 13–15 August 2021; pp. 220–225. [CrossRef]
241. Kim, G.Y.; Paik, J.Y.; Kim, Y.; Cho, E.S. Byte Frequency Based Indicators for Crypto-ransomware Detection from Empirical Analysis. *J. Comput. Sci. Technol.* **2022**, *37*, 423–442. [CrossRef]
242. Kakavand, M.; Arulsamy, L.; Mustapha, A.; Dabbagh, M. A Novel Crypto-Ransomware Family Classification Based on Horizontal Feature Simplification. In *Advances in Computer, Communication and Computational Sciences*; Advances in Intelligent Systems and Computing; Bhatia, S.K., Tiwari, S., Ruidan, S., Trivedi, M.C., Mishra, K.K., Eds.; 2021; Volume 1158, pp. 3–14. [CrossRef]
243. Rani, N.; Dhavale, S.V.; Singh, A.; Mehra, A. A Survey on Machine Learning-Based Ransomware Detection. In *Seventh International Conference on Mathematics and Computing*; Advances in Intelligent Systems and Computing; Giri, D., Raymond Choo, K.K., Ponnusamy, S., Meng, W., Akleylek, S., Prasad Maity, S., Eds.; Springer: Singapore, 2022; Volume 1412, pp. 171–186. [CrossRef]
244. Fernando, D.W.; Komninos, N.; Chen, T. A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques. *IoT* **2020**, *1*, 551–604. [CrossRef]
245. Hwang, J.; Kim, J.; Lee, S.; Kim, K. Two-Stage Ransomware Detection Using Dynamic Analysis and Machine Learning Techniques. *Wireless Pers. Commun.* **2020**, *112*, 2597–2609. [CrossRef]
246. Egunjobi, S.; Parkinson, S.; Crampton, A. Classifying Ransomware Using Machine Learning Algorithms. In *Intelligent Data Engineering and Automated Learning—IDEAL 2019*; Yin, H., Camacho, D., Tino, P., Tallón-Ballesteros, A., Menezes, R., Allmendinger, R., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2019; Volume 11872. [CrossRef]
247. Al-rimy, B.; Maarof, M.; Shaid, S. Crypto-ransomware early detection model using movel incremental bagging with enhanced semi-random subspace selection. *Future Gener. Comput. Syst.* **2019**, *101*, 476–491. [CrossRef]
248. Fernando, D.W.; Komninos, N. FeSA: Feature selection architecture for ransomware detection under concept drift. *Comput. Secur.* **2022**, *116*, 102659. [CrossRef]
249. Molina, R.M.A.; Torabi, S.; Sarieddine, K.; Bou-Harb, E.; Bouguila, N.; Assi, C. On Ransomware Family Attribution Using Pre-Attack Paranoia Activities. *IEEE Trans. Netw. Serv. Manag.* **2021**, *19*, 19–36. [CrossRef]
250. Arabo, A.; Dijoux, R.; Poulain, T.; Chevalier, G. Detecting Ransomware Using Process Behavior Analysis. *Procedia Comput. Sci.* **2020**, *168*, 289–296. [CrossRef]
251. Zahoora, U.; Rajarajan, M.; Pan, Z.; Khan, A. Zero-day Ransomware Attack Detection using Deep Contractive Autoencoder and Voting based Ensemble Classifier. *Appl. Intell.* **2022**, *52*, 13941–13960. [CrossRef]
252. Kok, S.; Abdullah, A.; Jhanjhi, N. Early detection of crypto-ransomware using pre-encryption detection algorithm. *J. King Saud Univ. -Comput. Inf. Sci.* **2020**, *34*, 1984–1999. [CrossRef]
253. Tasnim, N.; Sarker, I.H. Ransomware Family Classification With Ensemble Model Based On Behavior Analysis. In *Machine Intelligence and Data Science Applications. Lecture Notes on Data Engineering and Communications Technologies*; Skala, V., Singh, T.P., Choudhury, T., Tomar, R., Abul Bashar, M., Eds.; Springer: Singapore, 2022; Volume 132. [CrossRef]
254. Homayoun, S.; Dehghantanha, A.; Ahmadzadeh, M.; Hashemi, S.; Khayami, R.; Choo, K.K.R.; Newton, D.E. DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer. *Future Gener. Comput. Syst.* **2019**, *90*, 94–104. [CrossRef]
255. Khammas, B. Ransomware detection using random forest technique. *ICT Express* **2020**, *6*, 325–331. [CrossRef]
256. Khan, F.; Ncube, C.; Ramasamy, L.K.; Kadry, S.; Nam, Y. A digital DNA sequencing engine for ransomware detection using machine learning. *IEEE Access* **2020**, *8*, 119710–119719. [CrossRef]
257. Lee, K.; Lee, S.-Y.; Yim, K. Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems. *IEEE Access* **2019**, *7*, 110205–110215. [CrossRef]
258. Takeuchi, Y.; Sakai, K.; Fukumoto, S. Detecting ransomware using support vector machines. In Proceedings of the 47th International Conference on Parallel Processing Companion, New York, NY, USA, 13–16 August 2018; pp. 1–6. [CrossRef]
259. Walker, A.; Sengupta, S. Insights into malware detection via behavioral frequency analysis using machine learning. In Proceedings of the IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 12–14 November 2019; pp. 1–6. [CrossRef]
260. Al-Rimy, B.A.S.; Maarof, M.A.; Alazab, M.; Alsolami, F.; Shaid, S.Z.M.; Ghaleb, F.A.; Al-Hadhrami, T.; Ali, A.M. A Pseudo Feedback-Based Annotated TF-IDF Technique for Dynamic Crypto-Ransomware Pre-Encryption Boundary Delineation and Features Extraction. *IEEE Access* **2020**, *8*, 140586–140598. [CrossRef]
261. Qin, B.; Wang, Y.; Ma, C. API Call Based Ransomware Dynamic Detection Approach Using TextCNN. In Proceedings of the International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Fuzhou, China, 12–14 June 2020; pp. 162–166. [CrossRef]
262. Ayub, M.A.; Continella, A.; Siraj, A. An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme Using Artificial Neural Network. In Proceedings of the IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI 2020), Las Vegas, NV, USA, 11–13 August 2020; pp. 319–324. [CrossRef]
263. Bae, S.; Lee, G.; Im, E. Ransomware detection using machine learning algorithms. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5422. [CrossRef]
264. Javaheri, D.; Hosseinzadeh, M.; Rahmani, A.M. Detection and Elimination of Spyware and Ransomware by Intercepting Kernel-Level System Routines. *IEEE Access* **2018**, *6*, 78321–78332. [CrossRef]
265. Cohen, A.; Nissim, N. Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. *Expert Syst. Appl.* **2018**, *102*, 158–178. [CrossRef]

266. Almashhadani, A.O.; Kaiiali, M.; Sezer, S.; O'Kane, P. A multi-classifier network-based crypto ransomware detection system: A case study of Locky ransomware. *IEEE Access* **2019**, *7*, 47053–47067. [CrossRef]
267. Azmoodeh, A.; Dehghantanha, A.; Conti, M.; Choo, K.K.R. Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *J. Ambient. Intell. Human Comput.* **2018**, *9*, 1141–1152. [CrossRef]
268. Cusack, G.; Michel, O.; Keller, E. Machine Learning-Based Detection of Ransomware Using SDN. In Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Sec'18), Tempe, AZ, USA, 19–21 March 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–6. [CrossRef]
269. Baldwin, J.; Dehghantanha, A. Leveraging Support Vector Machine for Opcode Density Based Detection of Crypto-Ransomware. In *Cyber Threat Intelligence*; Advances in Information Security; Dehghantanha, A., Conti, M., Dargahi, T., Eds.; Springer: Cham, Switzerland, 2018; Volume 70. [CrossRef]
270. Manavi, F.; Hamzeh, A. A New Method for Ransomware Detection Based on PE Header Using Convolutional Neural Networks. In Proceedings of the 17th International ISC Conference on Information Security and Cryptology (ISCISC), Tehran, Iran, 9–10 September 2020; pp. 82–87. [CrossRef]
271. Poudyal, S.; Subedi, K.P.; Dasgupta, D. A Framework for Analyzing Ransomware using Machine Learning. In Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI), Bangalore, India, 18–21 November 2018; pp. 1692–1699. [CrossRef]
272. Poudyal, S.; Dasgupta, D.; Akhtar, Z.; Gupta, K. A multi-level ransomware detection framework using natural language processing and machine learning. In Proceedings of the 14th International Conference on Malicious and Unwanted Software—MALCON, Nantucket, MA, USA, 11–14 October 2019.
273. Fernández Maimó, L.; Huertas Celdrán, A.; Perales Gómez, A.L.; García Clemente, F.J.; Weimer, J.; Lee, I. Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. *Sensors* **2019**, *19*, 1114. [CrossRef] [PubMed]
274. Sanvito, D.; Siracusano, G.; González, R.; Bifulco, R. MUSTARD - Adaptive Behavioral Analysis for Ransomware Detection. In Proceedings of the ACM SIGSAC Conference on Computer and Communications (CCS), Poster, New York, NY, USA, 7 November 2022. [CrossRef]
275. Sendner, C.; Iffländer, L.; Schindler, S.; Jobst, M.; Dmitrienko, A.; Kounev, S. Ransomware Detection in Databases through Dynamic Analysis of Query Sequences. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Austin, TX, USA, 3–5 October 2022. [CrossRef]
276. Li, Z.; González Ríos, A.L.; Trajkovic, L. Machine Learning for Detecting the WestRock Ransomware Attack using BGP Routing Records. *IEEE Commun. Mag.* **2022**, *61*, 21–26. [CrossRef]
277. Hossain, M.S.; Hasan, N.; Samad, M.A.; Hossain, M.S.; Karmoker, J.; Ahmed, F.; Fuad, K.F.M.N.; Choi, K. Android Ransomware Detection From Traffic Analysis Using Metaheuristic Feature Selection. *IEEE Access* **2022**, *10*, 128754–128763. [CrossRef]
278. Karbab, E.B.; Debbabi, M.; Derhab, A. SwiftR: Cross-Platform Ransomware Fingerprinting using Hierarchical Neural Networks on Hybrid Features. *Expert Syst. Appl.* **2023**, *225*, 120017. [CrossRef]
279. Phuangtong, T.; Jaroonchaipipat, N.; Thanundonsuk, N.; Sakda, P.; Fugkeaw, S. RANDES: A Ransomware Detection System based on Machine Learning. In Proceedings of the 2023 15th International Conference on Knowledge and Smart Technology (KST), Phuket, Thailand, 21–24 February 2023; pp. 1–6. [CrossRef]
280. Coglio, F.; Lekssays, A.; Carminati, B.; Ferrari, E. Early-Stage Ransomware Detection Based on Pre-attack Internal API Calls. In *Advanced Information Networking and Applications. AINA 2023*; Lecture Notes in Networks and Systems; Barolli, L., Ed.; Springer: Cham, Switzerland, 2023; Volume 654. [CrossRef]
281. John, T.C.; Abbasi, M.S.; Al-Sahaf, H.; Welch, I.; Jang-Jaccard, J. Evolving malice scoring models for ransomware detection: An automated approach by utilising genetic programming and cooperative coevolution. *Comput. Secur.* **2023**, *129*, 103215. [CrossRef]
282. NIST. Contingency Planning Guide for Federal Information Systems. Available online: https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final (accessed on 25 October 2023).
283. *ISO 22301:2019*; Security and Resilience—Business Continuity Management Systems—Requirements. ISO: Geneva, Switzeland, 2019. Available online: https://www.iso.org/standard/75106.html (accessed on 25 October 2023).
284. Department of the Treasury. Advisory on Potential Sanction Risk for Facilitating Ransomware Payments. 2020. Available online: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf (accessed on 30 October 2022).
285. Ahnert, T.; Brolley, M.; Cimon, D.A.; Riordan, R. Cyber Security and Ransomware in Financial Markets. *SSRN* **2022**. [CrossRef]
286. Mierzwa, S.J.; Drylie, J.J.; Ho, C.; Bogdan, D.; Watson, K. Ransomware Incident Preparations With Ethical Considerations and Command System Framework Proposal. *J. Leadership, Account. Ethics* **2022**, *19*. [CrossRef]
287. Sophos. Paying Ransom Doubles the Cost of Ransomware Attack, According to Sophos. 2020. Available online: https://www.sophos.com/en-us/press-office/press-releases/2020/05/paying-the-ransom-doubles-cost-of-recovering-from-a-ransomware-attack-according-to-sophos (accessed on 25 October 2023).
288. Chen, P.H.; Bodak, R.; Gandhi, N.S. Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *J. Digit Imaging* **2021**, *34*, 731–740. [CrossRef]
289. Crystaldiskmark. Available online: https://crystalmark.info/en/software/crystaldiskmark (accessed on 25 October 2023).
290. Geekbench5. Available online: https://www.geekbench.com (accessed on 25 October 2023).
291. PCMark10. Available online: https://benchmarks.ul.com/pcmark10 (accessed on 25 October 2023).
292. Yaseen, Q.M. The Effect of the Ransomware Dataset Age on the Detection Accuracy of Machine Learning Models. *Information* **2023**, *14*, 193. [CrossRef]

293. Gupta, A.; Prakash, A.; Scaife, N. Prognosis Negative: Evaluating Real-Time Behavioral Ransomware Detectors. In Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, 6–10 September 2021; pp. 353–368. [CrossRef]
294. Berrueta, E.; Morato, D.; Magaña, E.; Izal, M. Open Repository for the Evaluation of Ransomware Detection Tools. *IEEE Access* **2020**, *8*, 65658–65669. [CrossRef]
295. ISOT Research Lab. Ransomware Dataset. 2020. Available online: https://www.uvic.ca/ecs/ece/isot/datasets/botnet-ransomware/index.php (accessed on 25 October 2023).
296. Resilient Information Systems Security. Ransomware Dataset. Available online: https://rissgroup.org/category/contributions/ (accessed on 25 October 2023).
297. Rege, A. Critical Infrastructure Ransomware Incident Dataset. Version 11.8. Temple University. 2022. Available online: https://sites.temple.edu/care/cira/ (accessed on 30 October 2022).
298. Rege, A.; Bleiman, R. A Free and Community-Driven Critical Infrastructure Ransomware Dataset. In Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Wales, UK, 20–21 June 2022; Springer: Singapore, 2023. [CrossRef]
299. CiberSecurity-Insiders. 2022 Ransomware & Malware Report [BitGlass]. Report. Available online: https://www.cybersecurity-insiders.com/portfolio/2022-ransomeware-malware-report-bitglass/ (accessed on 25 October 2023).
300. Han, J.; Lin, Z.; Porter, D.E. On the Effectiveness of Behavior-Based Ransomware Detection. In *Security and Privacy in Communication Networks. SecureComm*; Park, N., Sun, K., Foresti, S., Butler, K., Saxena, N., Eds.; Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering; Springer: Cham, Switzerland, 2020; Volume 336, pp. 120–140. [CrossRef]
301. Loman, M. LockFile Ransomware's Box of Tricks: Intermittent Encryption and Evasion. Sophos News. August 2021. Available online: https://news.sophos.com/en-us/2021/08/27/lockfile-ransomwares-box-of-tricks-intermittent-encryption-and-evasion/ (accessed on 25 October 2023).
302. Palmer, D. Ransomware Warning: Now Attacks are Stealing Data as Well as Encrypting It. ZDNET Report. Available online: https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/ (accessed on 25 October 2023).
303. Purnama, B.; Stiawan, D.; Hanapi, D.; Idris, M.Y.; Afifah, N.; Sharipuddin, S.; Budiarto, R. Time Efficiency on Computational Performance of PCA, FA and TSVD on Ransomware Detection. Indones. *J. Electr. Eng. Inform. (IJEEI)* **2022**, *10, 102–111*. [CrossRef]
304. Masum, M.; Faruk, M.J.H.; Shahriar, H.; Qian, K.; Lo, D.; Adnan, M.I. Ransomware Classification and Detection With Machine Learning Algorithms. In Proceedings of the IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; pp. 0316–0322. [CrossRef]
305. Urooj, U.; Al-rimy, B.A.S.; Zainal, A.; Ghaleb, F.A.; Rassam, M.A. Ransomware Detection Using the Dynamic Analysis and Machine Learning: A Survey and Research Directions. *Appl. Sci.* **2022**, *12*, 172. [CrossRef]
306. Bello, I.; Chiroma, H.; Abdullahi, U.A.; Gital, A.Y.; Jauro, F.; Khan, A.; Okesola, J.O.; Abdulhamid, S.M. Detecting ransomware attacks using intelligent algorithms: Recent development and next direction from deep learning and big data perspectives. *J. Ambient. Intell. Human Comput.* **2021**, *12*, 8699–8717. [CrossRef]
307. Kok, S.H.; Zbdullah, A.; Jhanjhi, N.Z.; Supramaniam, M. Ransomware, Threat and Detection Techniques: A Review. *Int. J. Comput. Sci. Netw. Secur. (IJCSNS)* **2019**, *19*, 136–146.
308. Camacho, J.; Therón, R.; García-Giménez, J.M.; Maciá-Fernández, G.; García-Teodoro, P. Group-Wise Principal Component Analysis for Exploratory Intrusion Detection. *IEEE Access* **2019**, *7*, 31–37. [CrossRef]
309. De Gaspari, F.; Hitaj, D.; Pagnotta, G.; De Carli, L.; Mancini, L.V. Evading behavioral classifiers: A comprehensive analysis on evading ransomware detection techniques. *Neural Comput. Appl.* **2022**, *34*, 12077–12096. [CrossRef]
310. Malik, S.; Shanmugam, B.; Kannorpatti, K.; Azam, S. Critical Feature Selection for Machine Learning Approaches to Detect Ransomware. *Int. J. Comput. Digit. Syst.* **2022**, *11*, 1167–1176. [CrossRef]
311. Chainalysis. As Ransomware Payments Continue to Grow, So Too Does RAnsomware's Role in Geopolitical Conflict. February 2022. Available online: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/ (accessed on 25 October 2023).
312. Wang, K.; Pang, J.; Chen, D.; Zhao, Y.; Huang, D.; Chen, C.; Han, W. A Large-scale Empirical Analysis of Ransomware Activities in Bitcoin. *ACM Trans. Web* **2022**, *16*, 1–29. [CrossRef]
313. Robles-Carrillo, M.; García-Teodoro, P. Ransomware: An Interdisciplinary Technical and Legal Approach. *Secur. Commun. Netw.* **2022**, *2022*, 2806605. [CrossRef]
314. Blessing, J.; Drean, J.; Radway, S. Survey and analysis of U.S. policies to address ransomware. *MIT Sci. Policy Rev.* **2022**, *3*, 38–46. [CrossRef]
315. Hacquebord, F.; Hilt, S.; Sancho, D. The Near and Far Future of Ransomware Business Models. Trend Micro Research. 2022. Available online: https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/the-future-of-ransomware (accessed on 25 October 2023).