Since the 50s, the world has seen the merits and the wonders of the Internet and

World Wide Web (WWW). Internet users generate about 2.5 quintillion bytes of data each day

Ransomware has attracted great attention from cyber security experts in recent years because of the fast growth of its attacks and the creation of new variants capable of bypassing antiviruses and anti-malwares [1]. It is a relatively new malware but has generated much interest from cybercriminals because of its successful attack and direct financial interest. Ransomware objective is to block its victim from accessing their own resources by locking the OS or encrypting targeted files that seem valuable to the victim, such as images, spreadsheets and presentations. [2]. Basically, there are two types of ransomwares: locky and crypto. Locky ransomware locks the entire system from access by its user, but it is usually easy to resolve. However, crypto ransomware uses encryption technology to lock selected files from user access; this is much more difficult to resolve and the damage caused may be irreversible. Crypto ransomware is also the more popular type employed by cybercriminals. A third type of ransomware called scareware has been mentioned in the literature [3]. This ransomware does not actually damage the victim’s computer but only scares the victim into paying the ransom. This type of ransomware is not discussed in this paper.

Since the 50s, the world has seen the merits and the wonders of the Internet and

World Wide Web (WWW). Every user today is now being connected to it at an

immensely quick pace. The amount of data is now exceeding zettabytes (270 bytes)

since last year, and the Pernicious content and corrupt programs have been attacking and

infecting various devices around the world, and the efforts for their prevention and

eradication have also gained pace simultaneously. The software code written

especially toward causing damage or stealing information becomes what is known

as per-ware (pernicious software) or per-ware in short.

In 2018, ransomware dominated the reports on cybercrime,

and became a malware threat targeting both businesses and

users alike. Some reports describe ransomware not only

as a tool of nancially motivated criminals, but also for

groups suspected of being aligned to the interests of some

nations [1]. Ransomware has affected a broad spectrum of

companies from manufacturing, transport, and telecommunications

industries, nancial companies, public law enforcement,

and health services [2], [3].

Ransomware extorts users by locking access to computer

resources and asking for a monetary payment to recover

access. The rst reports on ransomware that had a large

impact referred to them as lockscreen ransomware. This

type of malware locks access to a computer. In some

cases, it impersonates law enforcement organisations, asking

for the payment of a ne for some illegal activity performed

by the user, such as downloading les or browsing

child pornography websites. These strains are called police

ransomware [4].

The associate editor coordinating the review of this manuscript and

approving it for publication was Zahid Akhtar .

Since 2015, police ransomware and lockscreen ransomware

in general decayed in popularity and were substituted

by a type of ransomware that encrypts user les and

asks for a payment to provide the decryption key. This cryptographic

ransomware is called crypto-ransomware or cryptoware.

Ransomware payments can be carried using social

networks [5]. However, most of them carry the payments

using cryptocurrencies, and 98% of ransomware families use

Bitcoin [6]. Although the reports on their economic impact

are hardly accurate [7], each year single strains of cryptoransomware

reach new records of extended multi-national

impact. WannaCry and NotPetya attacks in 2017 were estimated

to have incurred global costs of more than $8 billion

[8]. During only the rst three weeks of 2018, GandCrab

ransomware infected more than 50,000 systems. The incurred

costs came not only from ransom payments but also from

the cessation of business operations, the impact on the public

image of affected companies, and insurance consequences.

Not only desktop systems were affected, but also mobile

ransomware increased its impact in 2017 [1]. Antivirus companies

reported a three-fold increase in ransomware installation

packages during the rst quarter of 2017 compared to the

previous quarter [9], [10]. Since 2018, malware developers

VOLUME 7, 2019 This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/ 144925

E. Berrueta et al.: Survey on Detection Techniques for Cryptographic Ransomware

began to use droppers - trojan software that looks like a

benign program, but once executed, downloads or extracts the

real malware and installs it in a computer [11].

The detection and blockage of crypto-ransomware has

been a very active area of research in recent years, because of

the massive expansion of this form of malware. Proposals and

developments have come from both the industrial sectors and

academia. Most detection solutions run local to a user host,

working like an antivirus software to detect and block ransomware

activity. However, proposals exist that are based on

detecting ransomware network activity or blocking network

trafc to servers needed by the malware. These detection

algorithms are based on a diversity of ad-hoc heuristics and

articial intelligence techniques. The simplest solutions are

customised for detecting a single ransomware type; however,

more general proposals are capable of the detection

of zero-day attacks. Our survey covers the case of cryptoransomware,

and from this point forward, any reference to

ransomware refers to a ransomware that encrypts user les.

No previous complete surveys on ransomware detection

techniques exist because of the novelty of this type of malware

and the fast-paced changing scenario of malware. Most

surveys limited their scope to a description of the behaviour of

different ransomware families [12][14] or the ransomware

families were included as a category in a broader study

of malware [15]. The description of detection techniques

is usually short and only in the form of suggestions and

ideas [16], [17] and not formal algorithms. The most complete

surveys on the topic are those of Eze et al. [18] and

in particular of Al-rimy et al. [19]. Although Eze et al. [18]

cites several research papers on ransomware detection in a

simple classication, it does not provide a complete review

of the literature, but only a two-page introduction to the

topic. Al-rimy et al. [19] presents an extensive classication

on ransomware behaviour and an up-to-date classication

of detection algorithms in the research literature. However,

he does not provide a description of the input parameters and

classication results provided by these proposals. Further,

he covers the broad topic of ransomware without providing

sufcient detail on the detection algorithms, which is the sole

topic of our review.

In this survey, we reviewed 50 proposals for the detection

of cryptoware activity. Most came from academia, but we also

added the description of existing commercial products based

on the available public information. We present a classication

based on the behavioural characteristics extracted from

a running system and the mathematical tools used in their

analysis: machine learning (ML)-based and threshold based.

The techniques for ransomware detection are based on distinguishing

ransomware action from benign software. In this

study, we classied ransomware action as different detection

techniques. This is a different classication from those presented

in the literature. An in-depth analysis of ransomware

characteristics is vital to create an accurate detection algorithm.

We describe the characteristics of 48 different ransomware

families from the analysis of 64 collected samples.

We extracted these characteristics from running the actual

samples. The survey papers in the literature describing ransomware

action had no access to such a large database and

did not offer rst-hand analysis. We classify these families

and relate them to the proposed detection techniques.

There are no common metrics of accuracy and performance

in ransomware detection. Some studies with a new detection

algorithm compared their proposals with previous ones, but

not all of them, and only to the extent of the ransomware

families they targeted. We describe and compare the results

of all these proposals, and we complete this paper with a

description of unsolved issues.

The remainder of this paper is structured as follows:

Section II details the characteristics of the different ransomware

families from the point of view of the design of

detection algorithms. Section III offers a classication and

description of the input data that the detection algorithms

extracted from ransomware. Section IV groups the detection

algorithms based on the logic of how to use the input

data to obtain a classication decision. We also describe

the main aspects of these algorithms. Section VI presents

the detection and performance results offered in the literature.

Section VII discusses open issues in crypto-ransomware

detection. Section VIII concludes the paper.