Computers and Electrical Engineering 000 (2017) 1–16

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics☆

Krzysztof Cabaj[a], Marcin Gregorczyk[b], Wojciech Mazurczyk[b,*]

[a] Warsaw University of Technology, Institute of Computer Science, Warsaw, Poland
[b] Warsaw University of Technology, Institute of Telecommunications, Warsaw, Poland

ARTICLE INFO

Article history:
Received 23 November 2016
Revised 16 October 2017
Accepted 17 October 2017
Available online xxx

Keywords:
Ransomware
Malware
Software-defined networking
Network security

ABSTRACT

Ransomware is currently one of the key threats facing individuals and corporate Internet users. Especially dangerous is crypto ransomware that encrypts important user data, and it is only possible to recover it once a ransom has been paid. Therefore, devising efficient and effective countermeasures is a pressing necessity. In this paper we present a novel Software-Defined Networking (SDN) based detection approach that utilizes the characteristics of the ransomware communication. Based on an observation of network communication between two crypto ransomware families, namely CryptoWall and Locky, we conclude that an analysis of the HTTP message sequences and their respective content sizes is enough to detect such threats. We show the feasibility of our approach by designing and evaluating a proof-of-concept SDN-based detection system. The experimental results confirm that the proposed approach is feasible and efficient.

1. Introduction

The year 2016 was named "the year of the ransomware" by the mass media, and this type of threat is currently considered by the security community and law enforcement agencies (e.g., Europol's recent "2016 Internet Organized Crime Threat Assessment" report [1]) as a key threat to Internet users. Ransomware is a type of malicious software that is designed for direct revenue generation and which after infection holds the victim's machine or user's critical data "hostage" until a payment is made. Ransomware developers are constantly improving their "products" making it harder to design and develop effective and long-lasting countermeasures. Considering the fact that more and more devices are foreseen to be connected to the Internet due to the Internet of Things (IoT) paradigm, it makes it a perfect environment for ransomware to spread in the foreseeable future [2]. The ransomware plague is so widely spread that there are even crime-as-a-service tools available in the dark web (like TOX ransomware-construction kit [3]) that allow even inexperienced cybercriminals to create their own customized malware, to manage infections, and profits.

There are two main types of modern ransomware, i.e., locker and crypto. The infection for both kinds of malicious software happens in a similar way, i.e., a user machine is infected by means of various attack vectors, e.g., by drive-by-download, malvertisement, phising, spam, or different forms of social engineering, etc. However, what comes after the infection is different for both types. *Locker ransomware* denies the user access to an infected machine but typically the underlying system and files are left untouched. On the other hand, *crypto ransomware* is a kind of data locker that prevents the user from

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Zhihan Lu.

* Corresponding author.
E-mail addresses: kcabaj@ii.pw.edu.pl (K. Cabaj), m.gregorczyk@tele.pw.edu.pl (M. Gregorczyk), w.mazurczyk@tele.pw.edu.pl (W. Mazurczyk).

https://doi.org/10.1016/j.compeleceng.2017.10.012
0045-7906/

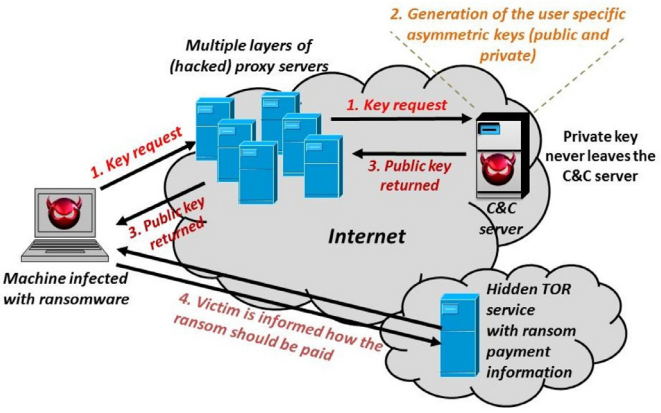

Fig. 1. Typical asymmetric key cryptography-based ransomware scheme.

accessing her/his vital files or data (e.g., documents, pictures, videos, etc.) by using some form of encryption. Therefore, attacked files are useless until a ransom is paid and the decryption key is obtained. Then after the user's machine is locked or data is encrypted the victim is presented with an extortion message. In many cases, paying the ransom to the cybercriminal is the only way to get back access to the machine/data. The value of the requested ransom differs and is typically in the range US$300–$700, and the favored payment currency is bitcoins [2]. It must be emphasized that not only individual users are currently targeted, but also companies and institutions like hospitals and law enforcement agencies, etc. Clearly, effective and efficient solutions to counter ransomware infections are desired.

Although the first cases of crypto ransomware have been known for more than 10 years (e.g., Trojan.Gpcoder), it must be emphasized that the recent plague (Symantec reported an astounding 4000% rise in crypto ransomware incidents in 2014 [4]) of this type of malware is related to the improved design of the cybercriminals' "products". The main difference now is that crypto ransomware has moved from custom or symmetric key to asymmetric key cryptography (Fig. 1). In this case, when the machine is infected, it contacts the C&C (Command & Control) server through multiple proxy servers (which are typically legitimate but hacked machines) to request a public encryption key. At the C&C a pair of matching public-private keys is generated for each infection and the public key is returned to the compromised host (the private key never leaves the C&C server). Then the public key is used to securely transfer the session key to encrypt the chosen files, which are deemed the most important for the user. It is worth noting that if correctly implemented, asymmetric crypto ransomware is (practically) impossible to break. The most prominent ransomware, and one of the first to introduce asymmetric key cryptography, is CryptoWall 3.0, which was discovered at the beginning of 2015, and later followed by others, such as CryptoWall 4.0 and Locky, etc.

Software-defined networking (SDN) is one of the emerging networking paradigms [5]. Its main benefit is that it allows the decoupling of the control and data planes, i.e., the underlying network infrastructure is abstracted from the applications. Therefore, the network can be managed in a logically centralized way. Apart from many potential applications [5], recently SDN has become a promising opportunity to provide security for current networks in a more flexible and effective manner [6]. Moreover, currently, SDN serves as the base of cloud computing environments in public, private, and hybrid clouds, and it is envisioned to become a core of future network services. The majority of network device manufactures are supporting SDN with their physical and virtual equipment using the OpenFlow protocol. SDN is standardizing the management of heterogeneous networks. Applications written for the SDN controller will work without additional adjustments to different devices supporting SDN in both physical and virtual environments. These are the main reasons why SDN was chosen as the key technology for our solution.

Taking the above into account, in this paper we present a dedicated SDN-based system for ransomware detection and mitigation. It must be noted that when it is possible to successfully discover ransomware communication, then, obviously, sometimes, it may be too late to prevent encryption for that particular victim. However, it is still possible to utilize this incident to provide feedback for the detection system to "save" other users. This phenomenon is well-known in nature where a single organism often has to make a self-sacrifice for the sake of the group [7]. As more and more analogies between cybersecurity and nature are continuously drawn [8], this may be another opportunity to reuse natural experiences in this regard to improve communication networks' defenses.

The proposed detection system, in this paper, has a focus on the crypto ransomware that utilizes asymmetric cryptography. While designing and developing the system we took into consideration results from the traffic analysis of two modern ransomware families, i.e., CryptoWall and Locky. Based on the performed analyses we concluded that these ransomware families share some similarities, which can be utilized to create an efficient and effective detection system. Thus, the main contributions of the paper are:

Please cite this article as: K. Cabaj et al., Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics, Computers and Electrical Engineering (2017), https://doi.org/10.1016/j.compeleceng.2017.10.012