Detecting of ransomware using software defined networking

Technology, Computer

Abstract –Ransomware is a major weapon for cyber-extortion. The traditional signature-based detection no longer holds good against modern, sophisticated malware that employs encryption techniques and social engineering. This paper investigates the use of Software Defined Networks (SDN) to detect the illicit communication between infected PCs (ransomware) and their controller known as the Command & Control (C&C) server. SDN provides unique opportunities to detect malicious DNS requests (associated with malware) and where possible block ransomware controls requests, and thereby prevent ransomware triggering. In this article we mostly look at detection at commercial or business scenarios, where the data handled are much more sensitive and might lead to monetary loss.

Index Terms – Ransomware, cyber-extortion, Signature-based detection, Software defined Networking.

Cyber-Extortion malware can be trace back to three decades earlier [1]. It all started with the malware named PC CYBORG which was delivered through floppy disk. The reports of modern malware known as ransomware were started in early 2005. Since then ransomware has developed into more sophisticated method of attack to extort money from people as well as the companies. Ransomware can make a huge impact on businesses, especially if it strikes mission-critical systems. The attacker forces the companies to pay-out money in the form of bitcoins which can be anonymous and not so easily traceable. If refuse to pay, they threaten to destroy the data. This is a profitable business model to cyber criminals as the companies and people tend to pay out to retrieve the data [2].

It is estimated that the pay-outs to ransomware is close to $1 billion an year as per IBM for 2016[3]. This is just known pay-outs and it crosses more than $1 bn if all the pay-outs are considered. The anonymity of the attacker and necessity of the victim makes it one of the popular attacks to extort money, especially from major tech companies and targeted businessmen. The ransomware is not specific to a single OS platform. From past few years, the ransomware have been developed for different platforms like linux, Mac OS and popular one emerging now a days is for android.

In general, the working of modern ransomware is as follows. First, a user machine is infected using various attack vectors for example, clicking on malvertisement, downloads from non-trusted sites, phising, spam, etc. Second, the victim’s system or the stored data is encrypted (locked), based on the type of ransomware. The modern versions of the ransomware can encrypt storage drives such as cloud storage, Dropbox, and shared network devices. As a result, multiple systems on the network can get compromised, by a single infection. Figure 1 shows the general working of the symmetric and asymmetric crypto ransomware.

Fig. 1. (left)Symmetric and (right) asymmetric crypto ransomware

As the ransomware evolves, some well know malwares have come into business, such as CryptoLocker, CryptoWall, TeslaCrypt and Locky have been widely used and updated.

Detecting these ransomware before the payload activates and start encrypting is very difficult [4]. Figure 2. Shows that only half of anti-virus scanners provide protection for this new malware, even after several days of a new attack being circulated.

Fig. 2. Time to detect new malware by antivirus vendors.

Recent study shows that the ransomware is becoming successful as the prices are tailored as per company’s or country’s ability to pay [5]. If the ransom isn’t paid within the expiry of the ransom note, the ransom usually doubles. This instils fear of losing the files or pay higher. This let company or the person feel it is easier and less expensive to pay the ransom and get back the files rather than reporting it and trying to find a solution for it. This makes it important to come up with mitigation techniques to stop this from continuing and

The ransomware developers are constantly improving their product which makes it hard for developing long lasting countermeasures. With large number of devices that are getting connected on the internet like the Internet of things, the ransomware is being developed to multiple devices.

Most common method of detection of ransomware, infact any malware, is signature based detection. Hence most of the experts suggest keeping the antivirus scanners up to date [6]. But as we have seen from the earlier that not many vendors give out updates that regular. Also with the use of encryption techniques and social engineering, it easily evades the defence in firewall and email spam filters. Hence the detection of entry of ransomware into the system or the network is becoming much more difficult.

One more commonly used method of detection is by identifying the extensions. For example, many use extensions like . locky, etc. But this can be masked by encryption techniques.

Microsoft advices the best way to tackle ransomware is by having a tested reliable backup to escape the damages of the ransomware [7]. Although this is one of the best methods, creating and maintaining backups for huge organizations can be really expensive and time consuming.

Now let us take a look at few of the current implementations to detect ransomware in commercial or business network as they are the major victims because of the data they hold. Majorly used method is implementing products which use User Behaviour Analytics (like Varonics or DatAdvantage). This works on the baseline of normal activity and if there is any other abnormal activity, an alert would be sent to the administrator. The major disadvantage with this is any other legitimate activity which is not mentioned under normal behaviour was reported which led to receiving of lot of false positives about the activity.

Other method used was to detect malicious activity by monitoring changes in File Server resource manager (FSRM), function built into Windows Servers. By using canaries, writing unauthorised files can be blocked. This helped in developing PowerShell to block unauthorised user access.

Most of the currently used techniques work fairly well with the symmetric crypto ransomware. They tend to be less efficient with the asymmetric crypto ransomware. In this article we look at one of the basic approach that can be taken to mitigate ransomware with the use of Software Defined Networking (SDN). This method is mostly useful in companies or a small network with a system administrator to monitor the network traffic.

Proposed method is based on findings after analysing CryptoWall ransomware [8]. But this can be applied to other types of crypto-ransomware, such as Locky TeslaCrypt, etc, which communicates with the Command & Control (C&C) servers. The primary intension with this proposed method is to cut-off the connection between the victim and the C&C systems. Without connection to C&C the encryption process is not going to be initiated and thus saving the victim’s system.

With the use of Intrusion detection/Prevention systems(IDPS) or firewalls that are commonly used to filter and detect malicious data, it is very hard to give timely response to such threats as there is lot of data that it encounters because of the number of devices that is connected onto the internet now a days.

In this article we take a look at two SDN-based mitigation concepts. We can call them SDN1 and SDN2. Both of them rely on dynamic blacklisting of proxy servers used for connecting to the C&C server. However for this method to be efficient, it is necessary to have up to date list of all the malicious proxy servers that are previously identified.

In this method of mitigation system, it is necessary to develop a SDN application to cooperate with the SDN controller. The controlled provides all the data necessary for analysis. After the detection of threat, the network can be configured to block all the malicious activity and capture suspicious traffic for investigation. This will also help in recovering symmetric key if the ransomware uses symmetric encryption based ransomware.

The functionality of the SDN1 is a simple switch. The switch forces all the DNS traffic to be forwarded to SDN controller for inspection. All the responses are compared and evaluated with the database that contains the list of malicious proxy servers. If the domain name extracted from the DNS is present in the database, the response is discarded or blocked to not let it reach the proxy server. This eliminates the process of encryption on the victim's system. An alert is sent to the system administrator about this issue for further investigation.

The potential drawback of SDN1 is time taken. The DNS traffic from both legitimate and malicious hosts is delayed as each response is checked with the blacked listed domain database. The SDN2 enhances the performance of SDN1 while addressing this issue. As most of the DNS responses received is legitimate, the SDN2 introduces custom flow. This forwards all the DNS response to intended recipient and only the copy of the response is sent to the SDN controller. While the DNS responses are processed, the controller compares the domains with the ones available on the database. If a blacklisted server is found, the victim IP is extracted and all the traffic between the C&C server and the victim IP is dropped and an alert is sent to the system administrator.

The pictorial representation of both SDN1 and SDN2 are shown in Figure 3.

Fig. 3. SDN-based applications, SDN1 and SDN2. Example testbed of the SDN network

Major advantages of using SDN based detection techniques is that it can be used to detect both symmetric as well as asymmetric ransomware. As mentioned earlier without the connection between victim and C&C server, the infected host will be able to retrieve the public key and hence will not be able to start the encryption process.

As we have seen earlier, this method requires a database that contains all the currently known and used malicious proxy servers. This is the major disadvantage of this method. Currently the developers of this method have a database of about 70, 000 malicious domains. But this won’t be sufficient as the attackers will be looking for new domains to evade detection. Also methods have to be checked frequently and loopholes need to be fixed as the attackers would seek to exploit any loopholes if found.

There are researches that are taking place to detect the ransomware using honeypot techniques. The SDN can be included into the honeypots to further enhance the effectiveness of the detection. Alongside with the SDN, the companies will have to develop an Incident Response team [6]. This team should make plans to tackle the issues according to the importance of the systems and also be given training to be equipped with the necessary steps to take in case of an attack which slipped from the SDN controlled.

In case of an attack, steps should be taken to contain the ransomware just to the affected system and it doesn’t spread to any other system on the network.

It is also important to take a backup of the entire necessary and sensitive files in a secure and tested location. This help in restoring the work quickly in case of unseen attack on a critical system.

Also one of the most important developments in ransomware is that now it is not just delivered as a Trojan, it is being developed in a way that it can replicate its code onto the removable devices and network drives.

This makes it important to educate and train the employees and the staff about the dangers of ransomware and methods that it can be brought in to the network like the spam emails and social engineering [9]. Also companies should discourage the policy of bring your own device (BYOD). Staff a being more alert about the malware makes is very difficult to launch any attack.

As we are looking to develop methods to detect and prevent ransomware, new type of ransomware is emerging that threatens to release all the data online, instead of destroying them, if not paid before the ransom note expires. This is makes it more necessary to develop more sophisticated methods of detection to prevent ransomware attacks.

Also as this is an SDN based security application, further research can be undertaken to broaden the spectrum of detection and prevention of other types of malware and attacks like DDoS attacks

To efficiently fight ransomware, it is important to break the business model of the ransomware developers. With the reduced income to the ransomware developers, they will have to shut down the proxy servers which in turn help in faster detection of newer developers.

The best protection is to prevent infection. This may be tough to achieve and hence in this article we have taken a look at 2 types of SDN based security application that can be implemented to improve protection against ransomware. These rely on up to date database of malicious proxy servers which needs to be updated constantly but once detected, the application works efficiently.

We have also discussed that it is achievable to break the connection between the victim and the C&C server, with the help of SDN application, to make the encryption impossible.

Furthermore, we have seen that it is necessary for the companies to actively invest time and money in training people to develop a sense of security at the workplace to reduce the attacks.

We have also discussed that this SDN based application need not be limited to detecting ransomware. This can be further developed to detect and prevent other malware, detect attacks based on the network traffic characteristics or detecting malware based on pattern.

References

N. Hampton and Z. A. Baig, “ Ransomware: Emergence of the cyber-extortion menace,” in Australian Information Security Management, Perth, 2015.

Chris Moore,” Detecting Ransomware with Honeypot techniques”, 2016 Cybersecurity and Cyberforensics Conference.

“ Ransomware becomes most popular form of attack as payouts approach $1bn a year”, Networksecuritynewsletter. com , January 2017.

Cisco, “ Cisco 2015 Midyear Security Report,” Cisco, San Jose, 2015.

Cath Everett,” Ransomware: to pay or not to pay?” Computer Fraud and security, April 2016.

Ross Brewer, LogRhythm, “ Ransomware attacks: detection, prevention and cure”.

D. Mauser and K. Cenerelli, “ Microsoft Protection Center: Security Tips to Protect Against Ransomware,” 6 April 2016.

Krzysztof Cabaj and Wojciech Mazurczyk, “ Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall”, NETWORK FORENSICS AND SURVEILLANCE FOR EMERGING NETWORKS.

Marc Sollars,” Risk-based security: staff can play the defining role in securing assets”, Networksecuritynewsletter. com

i?›iˆ i??