International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Cyber Security: Ransomware Infects the Cloud

Shanthi D.L[1], Rachana B[2]

[1] Assistant Professor, Information Science and Engineering, BMSIT& M, Bangalore, Karnataka, India

[2] Student, Information Science and Engineering, BMSIT& M, Bangalore, Karnataka, India

Abstract: ***Ransomware is a type of malware in which the data on a victim's computer is locked, typically by encryption, and payment is demanded before the ransomed data is decrypted and access returned to the victim. Ransomware attacks have emerged as one of the new threats to cloud computing because they store huge amounts of data. To safeguard the cloud users and cloud service providers against these attacks requires knowledge about ransomware attacks. This paper briefly discuses about types of ransomware attacks, how these attacks work, which are the targets of these attacks. It considers the impact of ransomware attacks on cloud and its users. Several security measures have been analyzed and a model which can be used in organizations has been designed. This model will help organizations to keep ransomware attacks away from their valuable resources.***

Keywords: Malware, Ransomware, Targets of Ransomware

1. Introduction

Ransomware is a subset of malware in which the information on a victims PC is locked, ordinarily by encryption, and installment is requested before the recovered information is unscrambled and returned to the victim. The main idea for ransomware attacks is nearly always monetary, and unlike other types of attacks, the victim are usually notified that an exploit has occurred and is given instructions for how to recover from the attack [1]. Payment is often demanded in a virtual currency, such as bitcoin, so that the cybercriminal's identity isn't known.

Payment is regularly requested in virtual cash, such as bitcoin, so that the cybercriminal's identity isn't known. Ransomware malware is spread through email connections, infected computer program applications. A number of attacks have utilized inaccessible desktop protocol and other approaches that do not depend on any form of user interaction.

There are a few diverse ways that ransomware can contaminate our computer. One of the most common strategies nowadays is through pernicious spam, of malspam, which is spontaneous email that's utilized to convey malware. The email might incorporate booby-trapped connections, such as PDFs or Word Reports. It might moreover just contain links to noxious websites.

Malspam uses social building in order to trap individuals into opening attachments or clicking on links by showing up legitimate- whether that's by seeming to be from a trusted institution or a friend. Cybercriminals utilize social designing in other sorts of ransomware attacks, such as posing as the FBI in order to scare users into paying them a entirety of cash to open their records. Another well-known strategy which reached its crest in 2016, is malvertising.

Malvertising or malevolent publicizing is the use of online publicizing to distribute malware with little to no user interaction required. Whereas browsing the web, even genuine sites, users can be directed to criminal servers catalog details about victim computers and their locations, and the select the malware best suited to deliver. Frequently, that malware is ransomware.

The existing ransomware can be categorized into crypto-ransomware and locker ransomware. The crypto-ransomware asks for ransom cash by encrypting the user's important information, whereas the locker ransomware locks the users system and requests for cash in order to open it. Normal crypto-ransomware incorporates Crypto-Wall, CryptoLocker. Ransomware incorporates Winlocker. In comparison, the crypto-ransomware is much more hurtful than the locker ransomware, since locker ransomware only locks the victim out of the system, and the victim can still have access to his/her information, e.g., by removing the storage medium from the infected computing system, and utilizing it in another non-infected computing system to duplicate out the data

2. Background

Cloud created a revolution in data storage. It's cost-effective, easy to access and typically very well guarded. The convenience is reflected in its widespread use. A report found that 82% of companies were already using multi-cloud storage strategies. According to the report 78% of small businesses will fully rely on cloud services by 2020.

Figure 1: Background for Petya ransomware

This mass migration of business of all sizes to cloud space rendered it an extremely attractive target. The Petya ransomware first emerged in 2016. It was notable for several things. First, Petya can encrypt a PC's entire Master Boot Record (MBR), causing the system to crash to a blue screen. This renders the entire system essentially unusable. On reboot, the Petya ransom note is not displayed instead, showing a skull and demanding payment in Bitcoin. Shown in fig 2. Second, Petya was spread to some systems through an infected file hosted on Dropbox, posing as resume. The link is disguised as the applicant's details, whereas it actually links to a self-extracting executable that installs the ransomware. Sadly, the Petya ransomware made it clear that ransomware has gone beyond local and physical storage, and can hit everywhere. Although being publicized as on one of the safest storage options, the cloud is not an exception to the threat.

There are various levels in the deployment of cloud infrastructure facilitating splitting the security functionality into sets of modules. The first security measure in architecture hierarchy involves identification of authentication measures and key establishment processes. The second level involves provision of support for authorization based access and the next stage may involve any additional security mechanisms as required or decided by the cloud service provider for every individual component of cloud service access. Multiple security mechanisms implemented at different levels including access to data, services, processes and communication channels are all aimed at preventing common security breaches as well as protecting against perceived fatal attacks.

3. Design

Ransomware attacks have succeeded in gaining everybody's attention including cloud users and cloud service providers. Many designs have been proposed by various authors. Here is a model which is designed to address ransomware attacks to clouds[1]. It consists of 3 main components:

1) Firewall and Gateways
2) Application Controller
3) Backup and Monitoring Server

firewall, spam/web gateway filtering, application controller, backup and monitoring server plays vital role as a team against ransomware attacks on data, network and systems.

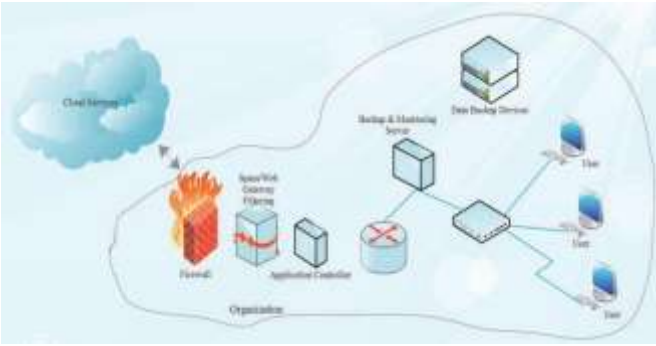

Figure 2: Design to prevent ransomware from entering the organization

Firewalls and Gateways: Basically, a gateway is simply a device that joins together two different networks. In the most common scenario, an internal network with the internet. A firewall is a filter that examines packets against a set of defined rules in order to decide whether to allow the packets through. In this design, these are the points from which the data flows from cloud to organization and vice versa. Malware can be prevented from reaching the end point at this stage by incorporating web and spam filtering technology. The gateway is updated with latest and known ransomware server to block the traffic from that server. If the organization is not using anonymous communications like Tor (The Onion Router), it needs to be blocked.

Application Controller: This contains the whitelist of applications those should be allowed to enter the organization network. A whitelist is a list of items that are granted access to certain system or protocol. When a whitelist is used, all entities are denied access, except those in whitelist. Whitelist of applications have to be formed carefully. Every process goes through this step and if it's not present, that application gets blocked.

Backup and Monitoring Server: The data has to be backed up at periodical time. This is the best solution to fight against ransomware. A proper time interval has to be set to back up the data. The dedicated server will take care of backup and will do monitoring of activities happening in the network. Data backup devices are kept outside the network. Monitoring activities is also one of the best ways to prevent from ransomware attack. This server watches for malfunctioning and blocks immediately. It also watches for any unauthorized process trying to access any system or file in the network and blocks it.

4. Ransomware targets

The most common ransomware targets are:

1. The healthcare sector – Hospitals particularly, are a main target for cyber criminals and according to the Verizon Data Breach Investigations new Report (DBIR) this sector is under greater threat compared to other targets, with 72% of all malware incidents targeted the health care system.

***Why they are vulnerable*:** Because the patients' data is vital for hospitals and could be a life and death situation, so cyber criminals know they could get paid for the ransom. A good example is the case of the Hollywood Presbyterian Medical Center, which paid approximately $17,000 to cyber-criminal for the decryption key to unlock their files.

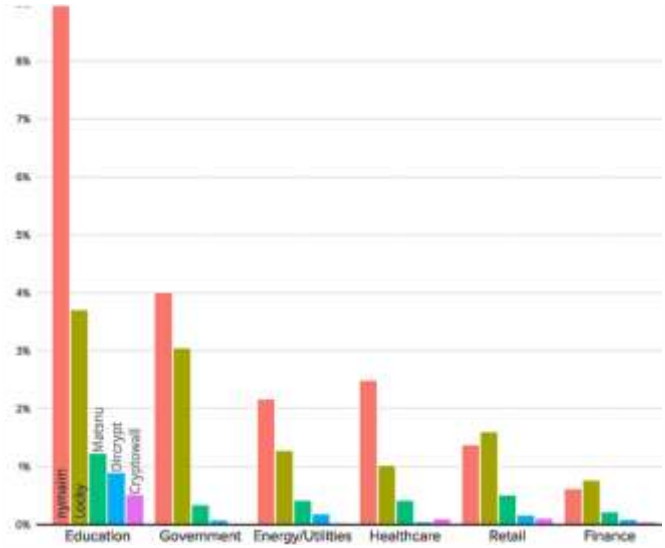

Figure 3: Common Ransomware Targets

2. Government institutions – Another industry that's a vulnerable target for ransomware attacks involves the government agencies and public service organizations that work and hold very important and sensitive personal data.
***Why they are vulnerable*:** Cyber criminals know the Government institutions need to be efficient and operations, so it's more likely to pay the ransom and get their data back. A recent example is the Petya outbreak that impacted important organizations, including Government departments in Ukraine and members who claimed they couldn't access their computers.

3. **Education** – Education, and mostly higher-education institutions, have been a top target for ransomware attacks. Researchers found that education sector had the highest rate of ransomware, "with at least one in ten experiencing this cyber-attack on their network".

***Why they are vulnerable*:** Education becomes an easy target for cyber criminals, mainly for its weak IT hierarchy to which thousands of students connect every day or the ease of launching a spear phishing campaign. Other than that, educational institutions don't have skilled system administrators for this job, and they also don't have financial resources to invest in cyber security. A recent example is the University College London that saw its shared drives and student management system taken down by cyber criminals.

4. **Law firms**: Legal firms are another sector at risk of being a sure target for online criminals, because they are responsible for clients' data, which is sensitive and confidential, and might have the resources to pay for the ransom. Global law firm, DLA Piper, was also a victim of Petya ransomware, as it saw their computers infected with malware.

5. Conclusion

As our daily lives become more and more dependent on Internet-based tools and services, and as those platforms accumulate more of our most sensitive data, the demand grows to secure these data. Security of computer systems and networking has become an issue of extreme importance due to the rapid increase in Internet usage. Also as everybody is migrating to cloud storage, if the service provider does not ensure proper security, thousands of users are going to be affected. Security like proper backup, dedicated monitoring, user training, security policies have to be implemented to ensure ransomware security.

References

[1] Rajani S. Sajjan and Vijay R. Ghorpade," Ransomware Attacks: Radical Menace for Cloud Computing", IEEE WiSPNET 2017 conference.
[2] S Bhattacharya, CRS Kumar," Ransomware: The CryptoVirus Subverting Cloud Security",December 2017.