

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 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.

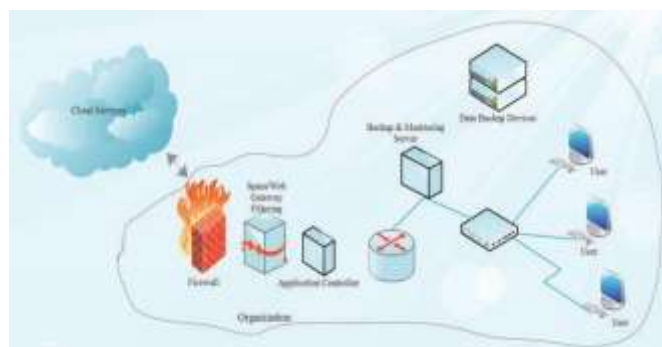


Figure 2: Design to prevent ransomware from entering the organization

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.

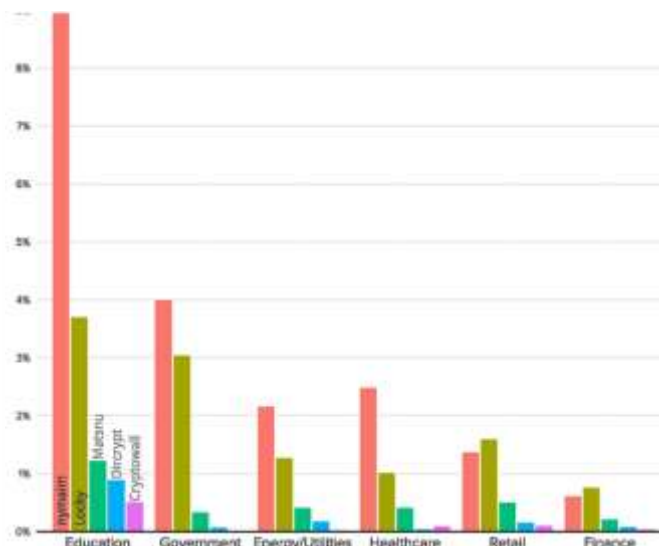


Figure 3: Common Ransomware Targets

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.