KRATIKAL
SECURE FOR SURE

RANSOMWARE WHITE PAPER

WHAT ARE RANSOMWARES?

Ransomware is no new terminology for current IT industry. Ever since its inception as an effective and commercial malware in 2005, it has undergone various upgrades. Essentially, ransomwares are malwares, that use mathematical problems to lock(encrypt) your data. They either lock you out of the operating system or prevent you from accessing your data. With the underground ransomware economy touching almost **$1 Bn** by 2016, ransomware has become one of the biggest revenue sources of several black hat criminals.

The whole idea of ransomware criminals is to use your negligence towards proper IT hygiene and your desperation to access your data into making you pay.

Typically, ransomwares are broadly categorised into two families:

Crypto Ransomware: It encrypts your files, folders and all private non-generic information on the systems of your organanisation. . It can use the symmetric or asymmetric encryption techniques to encrypt the data. You are prompted to pay the ransom to release the key.

Locky Ransomware: This family of ransomware restricts access to your operating system by encrypting critical OS files. The data stored in your PC remains unaffected, but to gain access to your OS, you need to pay the ransom.

RECENT ATTACKS ON BUSINESSES

(September 2015- April 17)

Some of the top ransomware attacks in the past few years are listed below:

1. A new ransomware named “NotPetya.” affected approximately 2,000 organizations around June 27.The digital attack campaign struck banks, airports and power companies in Ukraine, Russia and parts of Europe

2. Hundreds of MySQL databases and tens of thousands of MongoDB databases were held ransom by ransomware criminals.

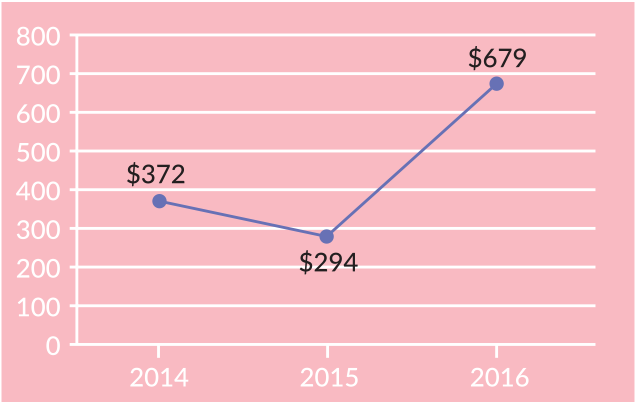
3. Emory Healthcare, an Atlanta healthcare system has been hit with a data breach and a ransomware attack that impacted the electronic health records of nearly **80,000** patients.)

4. Guests at the Romantik See hotel Jaegerwirt in the Austrian village of Turracherhohe, were locked out of their rooms, hotel paid **2 BTC** ransom($2.8k)

5. Texas police in the town of Cockrell Hill have lost eight years’ worth of digital evidence after getting hit by a ransomware attack in December 2016

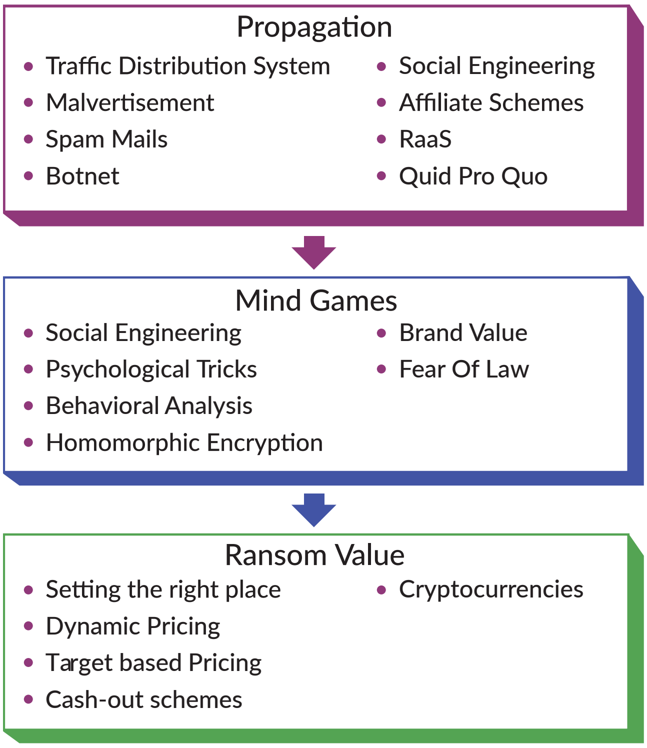
Ransomware are becoming a profitable and unique business proposition for guys black hat hackers. Over the years, the average ransom size has more than doubled.

Average Ransom Amount in US Dollars, by Year



MODUS OPERANDI

The modus operandi of ransomware criminals involves three phases:



Propagation

- Traffic Distribution System
- Malvertisement
- Spam Mails
- Botnet
- Social Engineering
- Affiliate Schemes
- RaaS
- Quid Pro Quo

Mind Games

- Social Engineering
- Psychological Tricks
- Behavioral Analysis
- Homomorphic Encryption
- Brand Value
- Fear Of Law

Ransom Value

- Setting the right place
- Dynamic Pricing
- Target based Pricing
- Cash-out schemes
- Cryptocurrencies

1. **Propagation**: Criminal uses various channels to spread the ransomware into the target network. It may involve infecting the traffic distribution, Malvertisement, sending spam mails, or using botnets. Social engineering is also one of the most preferred ways to spread ransomwares in target computers.

Apart from these, there are various affiliate schemes launched by ransomware terrorists, wherein, you are given a certain revenue share for every victim you infect. Ransomware as a Service (RaaS) is a new domain where you can enlist the services of ransomware criminals to attack a competitor or your adversary. There are also quid-pro-quo schemes where you have the option to pay the ransom or you can agree to infect two other victims in exchange for getting the decryption key.

2. **Mind Games:** Once the target is infected with ransomwares, then starts the mind games. The objective of this phase is to coerce the victim into paying the ransom. This can be achieved using a variety of schemes like appealing to the brand value of the target, displaying fake law enforcement messages, analysing the behaviour of the victims via their data and to craft coercion messages based on it. Something as trivial as displaying a small countdown: depicting when the ransom is due, goes a long way. This can include displaying a countdown timer for when the data will be permanently deleted or when the ransom will be doubled.

3. **Ransom value:** This is the last phase where the ransomware criminal puts a price on the data or the system held ransom. This can be determined by a variety of factors: brand value of the company, urgency of data, importance of the data to the company. As an example, consider the case when all guests of the hotel in Austria were locked out due to a ransomware attack, it became pertinent for the hotel to pay up. However, the hotel denied ever paying the ransom.
The value of data depends from company to company. For an early stage startup, the value of their data repositories is much less, as compared to firms like Facebook and Twitter.

SAFEGUARDING TECHNIQUES

Ransomware is a problem where we have a limited possibility of reactive solutions. The mantra is “Prevention is better than cure”

1. **Updated OS & security software:** Your OS and other applications regularly release patches and updates. Make sure to update all your softwares accordingly. A similar logic is applicable to your security softwares: Antiviruses, Anti-phishing tools and other anti-malware tools. Obsolete antimalware tools are like blunt knives: a good showpiece but useless.

2. **Back up your data**: This technique that has proven to be most effective against ransomware attacks. If you have scheduled regular backups of your data, you can simply format the infected systems and re-establish the entire infrastructure again. This is by far the most effective countermeasure against ransomware attacks.

Apart from these techniques, there are some other common countermeasures which can be taken to prevent ransomware attacks:

a) Use “show hidden file-extensions” so as to prevent accidentally executing malicious scripts on your systems.

b) Never click on unknown links or download attachments from untrusted sources

c) Disable Windows Scripting Host

d) Use Adblocker and Web of Trust(WoT) plugins

e) Using Linux based systems has proven an effective solution in the current scenario. However, using Linux is not a permanent solution of the problem

TAKEAWAYS

To sum up the discussion, ransomwares are a flourishing business model for numerous criminals. This problem will continue to escalate, given the added boost to cryptocurrency, provided by IT professionals around the world. Even governments across the world have started recognising Bitcoins as a means of exchange. Keeping these facts in mind, we need to become proactive in our approach. There is an urgent need for having industry level safeguards and compliances to check the outbreak of ransomwares.