International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 06 | June 2018 www.irjet.net p-ISSN: 2395-0072

Ransomware: A Review

Anusha Chandrasekharan[1], Bhavana Malviya[2]

[1]*PG Student, Department of Masters of Computer Applications, VESIT, Chembur, Mumbai, Maharashtra, India*
[2]*PG Student, Department of Masters of Computer Applications, VESIT, Chembur, Mumbai, Maharashtra, India*

Abstract - *This paper introduces ransomware and discusses its impact on the world and on India. This study will review the history of ransomeware; describe common infection vectors and ransomware types; and propose strategies for detection, remediation and recovery.*

Key Words: **Cyber Attack, Ramsomware, WannaCry, Petya, Locky, Prevention, Solution**

1. INTRODUCTION

A global cyber attack has crippled nearly hundred countries, including India. A cyber gang called Shadow Brokers, which is a mysterious organization, is held responsible for this massive cyber attack. The organization has carried out the attack by stealing a hacking tool called 'Eternal Blue' from the National Security Agency (NSA), America's powerful military intelligence unit. The hacking tool Eternal Blue gives unprecedented access to all computers using Microsoft Windows. It was developed by NSA to gain access to computers used by terrorists and enemy states.
The cyber attack is considered as the biggest ransomware attack of its kind. As per security Software Company Avast, its researchers have observed more than 75,000 attacks worldwide in 99 countries including the UK, Russia, Ukraine, India, China, Italy, and Egypt.

Ransomware is a type of malicious software when infected restricts the user access until a ransom is paid to unlock it.

Hackers have spread ransomware known as WannaCry, WanaCrypt0r 2.0, WannaCry and WCry, often through emails. The files in the infected computers gets locked up in such a way that the user cannot access them anymore. It then demands payment in crypto currency Bit coin to retrieve the locked files. Finance ministers and central bank governors of group of seven nations such as the United States, Canada, Japan, France, Germany, Italy and Britain have agreed to strengthen cooperation to counter cyber threats such as the present global online attack.

1.1 Petya Ransomware

Petya Ransomware is part of a new wave of cyber-attacks and has infected computer servers across the world.

Petya is a ransomware, similar to that of Wannacry attack. The Petya is thought to be a variant of Petya.A, Petya.D, or PetrWrap. Petya was also found to be exploiting EternalBlue exploit that was used by Wannacry attack. WannaCry cyber attack had crippled more than over 300,000 computers globally.

The Petya ransomware, like WannaCry had locked up the computer files and encrypted all data on the computer. It then demanded $300 Bitcoins as ransom to unlock the encrypted data. Once the ransomware infected the system it will wait for an hour and will begin rebooting the system. After the reboot, the files will get encrypted and user will be asked to pay up the ransom.
The Petya ransomware attack is believed to have originated from an update used on third-party Ukrainian software called MeDoc. The software was being used by many government organizations in Ukraine. This explains why Ukraine was the most affected country. The ransomware is labeled as the most comprehensive cyber attack. To fix the 'EternalBlue' exploit in Windows, Microsoft had issued a security patch.

Researchers are yet to identify the persons behind the cyber attack. In Ukraine, Ukrainian Railways, Ukrtelecom, and the Chernobyl power plant were worst affected by the attack. Apart from these companies multinational companies like DLA Piper, shipping giant AP Moller-Maersk, drug maker Merck, as Mondelez International were affected. In the US, hospitals were affected. In India, the Jawaharlal Nehru Port (JNPT) got affected by the cyber attack. JNPT has the capacity to handle over 1.8 million standard container units. Russia, Poland, Italy and Germany are other countries affected by the cyber attack.

1.2 Locky Ransomware

Locky ransomware is being circulated through massive spam campaign in which spam emails with common subject lines target computers by locking them and demanding ransom for restoring access to users. It first had surfaced in 2016.

It encrypts files on victims' PCs and adds a .locky file extension. The attackers then demand ransom in Bitcoin payment to unlock the files. It is demanding ransom of half bitcoin, which at present rate is equivalent to over Rs 1.5 lakh. So far, it has extorted more than $7.8 million in payments, according to a recent study. However, its impact on Indian systems is not clear so far.

The Locky Ransomware cyber attack is third major ransomware attack this year after Wannacry and Petya which had crippled thousands of computers, including those of multinational corporations. According to an Assocham PWC study, India was third worst affected country in list of over 100 countries.

2. CONSEQUENCES

The cyber attack has crippled many hospitals, schools and universities in Europe and Asia. Britain's National Health Service (NHS) is among badly affected. Other affected high profile victims are international shipper FedEx Corp, Spain's telecommunications company Telefonica, Portugal Telecom and Telefonica Argentina, Germany's railway operator Deutsche Bahn etc. According to Avast, the countries such as Russia, Ukraine and Taiwan are the top targets around the world.

In India, Andhra Pradesh's police computers have come under the cyber attack. Computers in 18 police units in Chittoor, Krishna, Guntur, Visakhapatnam and Srikakulam districts have been affected.

2.1 Extent of Attack

India
In India, the ransomware has crippled the operations at one of the terminals of the Jawaharlal Nehru Port Trust. The affected terminal was being operated by AP Moller-Maersk. The company operates the Gateway Terminals India (GTI) which has a capacity to handle 1.8 million standard container units. The attack has impacted the external trade by affecting the systems dealing with the cargo and ships at the country's largest port.

World
The Petya ransomware has hit computer servers all across Europe. Ukraine and Russia are the worst affected countries. The ransomware has also impacted some companies in the US and other Western European countries.In the severely affected Ukraine, government offices, energy companies, banks, cash machines, gas stations, and supermarkets, Ukrainian Railways, Ukrtelecom, and the Chernobyl power plant has been worst affected.

3. PROBLEMS

The problem with ransomware is a specialized form of malware that encrypts files and renders them inaccessible until the victim pays a ransom is an extremely serious Problem and it's quickly getting worse.
The country cyber security agency Computer Emergency Response Team of India has issued a red-colored 'critical alert' in connection with the WannaCry attack, and warned users to not pay the ransom.
The ransomware worm that stopped car factories, hospitals, shops and schools over the weekend worldwide.

4. PREVENTION

What to Do If You're Infected by Ransomware?

First, you'll need to determine whether you've been hit by encrypting ransomware,screen-locking ransomware or something that's just pretending to be ransomware. See whether you can access files or folders, such as the items on the desktop or in the My Documents folder.
If you can't get past the ransom note you see on your screen, you're likely infected by screen-locking ransomware, which is not so bad. If you see a notice claiming to be from the police, the FBI or the IRS that says you've been caught looking at pornography or filing false taxes and must pay a "fine," that's usually screen-locking ransomware, too.

How to deal with encrypting ransomware?

- Disconnect your machine from any others, and from any external drives.
- Use a smart phone or a camera to take a photograph of the ransom note presented on your screen.

- Use antivirus or anti-malware software to clean the ransomware from the machine.

- See if you can recover deleted files.
  Figure out exactly which strain of encrypting ransomware you're dealing with.

- See if there are decryption tools available.

5. SOLUTIONS

Quantum communication allows the sending of encoded messages that are un-hackable by any computer. This is possible because the messages are carried by tiny particles of light called photons.

If an eavesdropper attempts to read out the message in transit, they will be discovered by the disturbance their measurement causes to the particles as an inevitable consequence of the HUP

1: using of photon qubits(they support binary language like 0 and 1)

2:detecting Hacking through HUP(Heisenberg's Uncertainty Principle)In the regime of quantum experiments, by contrast, we are uncertain about the results of experiments because the particle itself is uncertain. It has no position or speed until we measure it. Or so Heisenberg thought, and most physicists still follow this line.

3: To encode the data we need a key i.e, This simple version of quantum key distribution (QKD) secures the channel – the optical fibre, for example – against intrusions. But how can we be sure that their device vendor is not in league? Cyber criminals are very good at setting up sophisticated networks, so how do you ever know whom to trust?

4: The answer is quantum entanglement. Two entangled photons have quantum-linked states: measuring the information stored in one photon tells us about the information in the other.This effect holds even if the two photons are far apart, even if they are on opposite sides of the Earth.

It turns out that measuring the first photon always gives a random result, specifically, a random bit 0 or 1. Does that sound useful? It should -be each perform the same measurement on separate photons from an entangled pair, they will get a random, but shared, number. By repeating this on many entangled pairs they can generate a secret key.

Another solution is as follows:
A software which snapshots your files to learn what your system looks like prior to a ransomware attack and then uses this information to characterize malicious changes to your files.

When the software detects multiple changes that makes the files unreadable, it should spring into action and suspend the application. Then the user or owner will have the option toput the system into lockdown, killing the process and blocking it from further execution.

6. CONCLUSION

This threat study represents a thorough analysis of ransomware, including some of the well-known variants, evolution, vectors, notable attacks, and how to prevent an organization from becoming the next victim. it is clearly evident that ransomware will grow in sophistication and become more widespread as it continues to plague individual users, as well as the enterprise. The success thus far in the extortion of money from victims is paving the way for more cybercriminals to utilize ransomware as their main tactic. Your organization will be armed with the necessary knowledge and tools to protect your environment.

ACKNOWLEDGEMENT

The authors can acknowledge any person/authorities in this section. This is not mandatory.

REFERENCES

[1] https://www.hindustantimes.com/

[2] https://timesofindia.indiatimes.com/

[3] https://www.google.com/

[4] http://www.avg.com/us-en/ransomware-decryption-tools