Wanna cry ransomware: A case study in Indian perspective

[1]Pushkar Sudhir Baviskar, [2]Manikant Roy

[1]Student, [2]Assistant Professor
[1]IBSAR Institute of Management and Studies (University of Mumbai)
[2]Lovely Professional University Punjab

***Abstract*— We all are living in the digital era! Right from morning wishes to work in office everything is taking place online. Our government is trying to make all the services online and connecting with our identity. But the world seems fancy as it makes our life simpler but at the same time it's full of danger too. The million-dollar question is being we ready for it by all means? Do we have the infrastructure to handle the emergency? Is our system being robust enough? Or are we ready to pay the price? WannaCry ransomware was one of the dangers which shook the world on 12th May 2017 by the worldwide cyber-attack. Every place government office for critical services like the hospital got affected. This paper is an exhaustive study of WannaCry ransomware attack and its affect India, explain the methods how to prevent such attacks in the Indian context and highlighted areas where the loopholes are! This study also indicates some of the government. of India corrective measure taken and what are the cyberinfrastructure is available for in the country.**

***Keywords*: cyber-attack, threats, safeguards**

Introduction

The world has experienced a massive global ransomware cyber-attack known as "WannaCrypt" or "WannaCry" since Friday, May 12, 2017.The WannaCry ransomware attack one of the largest ever cyber-attacks appeared to be slowing around 24-hours after it wreaked havoc and shut down tens of thousands of computer systems across 104-countries. India was the third worst hit nation by ransomware WannaCry as more than 40,000-computers were affected even though no major corporate or bank reported disruption to their activities raising doubts whether these entities are disclosing attack at all. According to multiple sources, a new variant of Petya ransomware, also known as Pet wrap, is spreading rapidly with the help of same Windows SMBv1 vulnerability that the WannaCry ransomware abused to infect 300,000-systems and server worldwide in just 74-hours. Apart from this, many victims have also informed that Petya ransomware has also infected their patch systems.

I. The Rate of ransomware infections

At the rate of ransomware infections, we see suddenly dramatically change is occurring from the year 2016 to 2017 according to Symantec. Ransomware infections increase 36 percent in the years 2015 to 2016. Symantec blocked just over 319,000 ransomware infections. If this infection rates continued for the full year, 2017 is a significant increase over 2016, when a total of 470,000 infections was blocked.

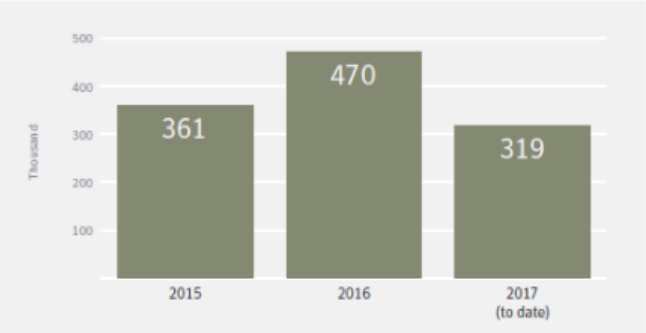

Fig: a

The U.S. has continued to be the region most affected by ransomware during 2017 to date, accounting for 29 percent of all infections. Japan (9 percent), Italy (8 percent), India (4 percent), and Germany (4 percent) were also heavily affected. The top 10 regions were rounded out by the Netherlands (3 percent), UK (3 percent), Australia (3 percent), Russia (3 percent), and Canada (3 percent).

If we see the effect of the ransomware attack in the year 2016 India is a 6th most affected country in the word.

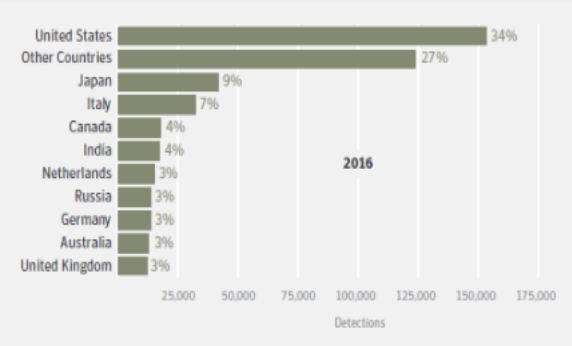

Fig: b

According to initial calculations performed soon after the malware struck around five percent of all computers affected by the attack were in India. If we analyze the date given by Symantec, the cyber security company, India comes in 6th place in the year 2016 but suddenly we see a change in the year 2017. Now India is a 5th most affected country in the world and the 3rd-most attacked in Asia by ransomware.

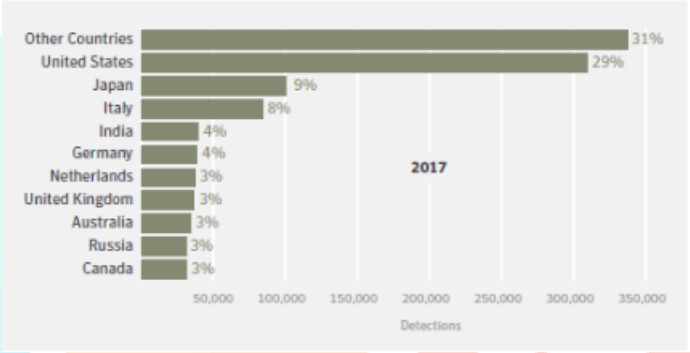

Fig: C

II. TOP RANSOMWARE FAMILY

The ransomware spreading rate is showing no signs of slowing down.These days, not only India are seeing the surfacing of newer families, but the malware creators create continuous updates in previously-released variants prove to be unrelenting. The continuous onslaught of new ransomware families, updated variants, and thriving business and distribution models attest to the fact that ransomware works. In decades , there are 50 new ransomware families have been discovered, which shows an average of 10 new ransomware families a month.

The methodology of ransomware attacking is 4 types.

a) Encrypting ransomware
b) Non-encrypting ransomware
c) Leakware (also called Doxware)
d) Mobile ransomware

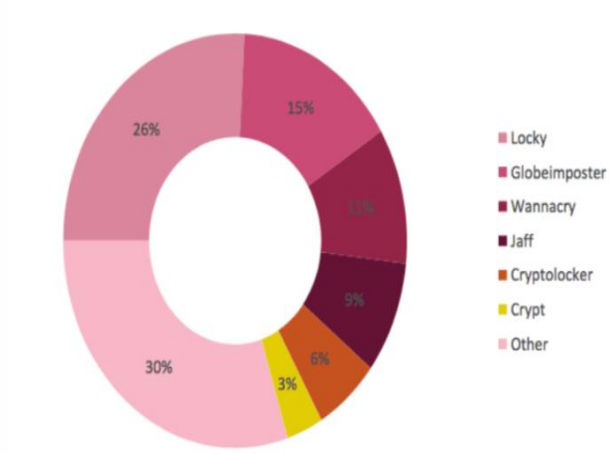

Fig: Family of Ransomware

According to statistical data, we are encounter top-0three families which are spreading through spam emails containing a downloader that's disguised as a Word or Zip attachment.

a) Locky (30%)
b) Globeimposter (26%)
c) WannaCry (15%)

Ransomware attack used Cryptovirology mode. According to Wikipedia Cryptovirology is "A field that studies how to use cryptography to design powerful malicious software." In India, over 11,000-users were attacked by TeslaCrypt ransomware during the period of March-May 2016 and ranked 1st in the list of countries attacked by it in that period. During the same period, around 600 users were attacked by Locky ransomware and ranked 4th in the list of countries attacked by this ransomware during that time. The Android ransomware named Lockdroid is also making its presence felt in the Android OS smartphone segment.

III. LIST OF RANSOMWARE INFECTED STATE IN INDIA

1. Karnataka – 36.58 %
2. Tamil Nadu – 16.72 %
3. Maharashtra – 10.86 %
4. Delhi – 10.00 %
5. West Bengal -6.70 %
6. Uttar Pradesh – 5.33 %
7. Telangana – 4.54 %
8. Kerala – 3.87 %
9. Gujarat – 2.35 %
10. Haryana – 1.96 %

IV. RANSOMWARE ATTACK TARGETS IN INDIA

a) Three Bank & a Pharma company were hit by Lechiffre ransomware.
b) Two Business houses reported having paid $ 5 million.
c) Maharashtra Government hit – Lost data on 150+ computers
d) Banks and Small Businesses
e) Indian Forest Department falls victim to Ransomware attack.

Now let us take a look at the kind of damage Ransomware could inflict government schemes. The Indian Government Announced two Scheme is as follows:

1. E-governance
2. Smart Cities

According to statistics released by Symantec, the main targets other than the India government servers are entities based on Internet of Things and the ones using Android smartphones. We are a little bit familiar with E- governance. In the E- Governance Include more digital oriented modules which are helping people for the life satisfaction. A module like Online complaints, online registrations and even online direct debits for people Cybercriminals won't think twice before encrypting the data of such people.
Smart Cities concepts are based completely on the Internet of Things. All things in a smart city are connected to each other and also to a central point that connects them to other smart cities. As we know we are working hard for to build a smart city concept. Many times, I have seen computers still running the outdated Windows XP in government offices! In such cases, it would be easy for a cybercriminal to take control of an entire city.

V. RANSOMWARE ATTACKS PREVENTION

The number of internet users in India is expected to reach 500 million by June 2018, said a report by the Internet and Mobile Association of India (IAMAI). With such a large user base that does not even take Online Privacy, let alone Ransomware seriously, it is all gold for the cybercriminal.

1. Maintain updated Antivirus software on all systems.
2. Check regularly for the integrity of the information stored in the databases.
3. Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.

4. Keep the operating system third party applications (MS office, browsers, browser Plugins) UpToDate with the latest patches.
5. Don't open attachments in unsolicited emails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited email, even if the link seems benign. In cases of genuine URLs close out the email and go to the organization's website directly through the browser.
6. Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

VI. CONCLUSION

This paper gives us an informative on WannaCry ransomware behavior and its impact on India. It's given a good exposure on how to prevent WannaCry Ransomware Attack in future and also list out the most Dangerous Ransomware family which is high causes of Indian Cyberspace. The study is still going on to prevent this type of attack and give good Exposure.

REFERENCES

[1] https://en.wikipedia.org
[2] https://www.tripwire.com
[3] The WannaCry Ransomware Prepared By CERT-MU May 2017
[4] www.thewindowsclub.com
[5] Internet Security Threat Report ISTR
[6] SentinelOne Ransomware research report data Summary
[7] 48,000 ransomware attack attempts seen in India: Quick heal tech Https://www.liveemint.com