International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7 Issue-2, May 2018

Wanna Cry Ransom Ware: Evaluating Risk & Implementing Security Measures

Eesha Mishra, Archita Bhatnagar

Abstract: ***Incidents of wannacry has been escalated over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan. The software can run in as many as 27 different languages, it is important to understand to what extent cyber attacks can be predicted . There are many related and ongoing research available on cyber security threat, but wannacry ransomware attack has become one of the main security concern now a days. This paper shall evaluate the securitymeasures to secure victim's pc from wannacry ransomware attack and analyze the risk from this threat.***

Keywords: Ransom Ware, Wannacry.

I. INTRODUCTION

Emergence of wannacry malware has significantly changed the cyber threat landscape. This type of ransomware encrypt the valuable data on victim's computer and request a payment to decrypt the data. Victims, with no way to defend themselves, are often advised to simply pay. The payment is in the form of bitcoins i.e. implemented to avoid the traceability of the intruder after or during payment.

Wanna Cry infect the victim's computer if the user -

1. Opens an infected email attachment.
2. Clicks on an infected link.
3. Installs an infected app.
4. Visits a legitimate website that has been infected.

In this paper we evaluate the security measures to overcome security threat & shall provide a system for public to securely use their systems. This paper will not only explain to secure pc from ransomware but also analyze the risk from this security threat.

This paper is divided into 3 sections -

1. Introduction
2. Word cloud approach contained in tweets
3. Incorporating security measures to remove Threat .
4. Conclusion

II. WORD CLOUD APPROACH CONTAINED IN TWEETS

Word cloud is best to visualize most of the terms and words contained in tweets. To use this one should have an active twitter account.

Revised Manuscript Received on 30 May 2018.
***** Correspondence Author
Eesha Mishra, Scholar, Swami Vivekanand Subharti University, Meerut (Uttar Pradesh)-250005, India. E-mail: eeshamishra786@gmail.com
Archita Bhatnagar, Assistant Professor, Swami Vivekanand Subharti University, Meerut (Uttar Pradesh)-250005, India. E-mail: archita.bhatnagar09@gmail.com

Below the word cloud is created by using R Programming language in R Studio. In this code user authenticate from twitter using consumer key, consumer secret, access token and access secret. Then after tweet searching can be done. This code also eliminates numbers, stop words, punctuations,
white spaces and convert the rest into lower case.

```
setup_twitter_oauth(consumer_key,consumer_secret,access
_token,access_secret)
eesha_tweets <- searchTwitter("wannacry", n=200, lang =
"en")
eesha_tweets
eesha_tweets_text <- sapply(eesha_tweets, function(x)
x$getText() )
docs <- Corpus(VectorSource(eesha_tweets_text))
toSpace <- content_transformer(function (x , pattern )
gsub(pattern, " ", x))
docs <- tm_map(docs, toSpace, "/")
docs <- tm_map(docs, toSpace, "@")
docs <- tm_map(docs, toSpace, "\\|")
docs <- tm_map(docs, content_transformer(tolower))
docs <- tm_map(docs, removeNumbers)
docs <- tm_map(docs, removeWords, stopwords("english"))
docs <- tm_map(docs, removeWords,c("tco","https"))
docs <- tm_map(docs, removePunctuation)
docs <- tm_map(docs, stripWhitespace)
docs <- tm_map(docs, stemDocument)
dtm <- TermDocumentMatrix(docs)
m <- as.matrix(dtm)
v <- sort(rowSums(m),decreasing=TRUE)
d <- data.frame(word = names(v),freq=v)
head(d, 10)
wordcloud(words = d$word, freq = d$freq, min.freq =
1,max.words=200, random.order=FALSE,
rot.per=0.35,colors=brewer.pal(8, "Dark2"))
```

Output

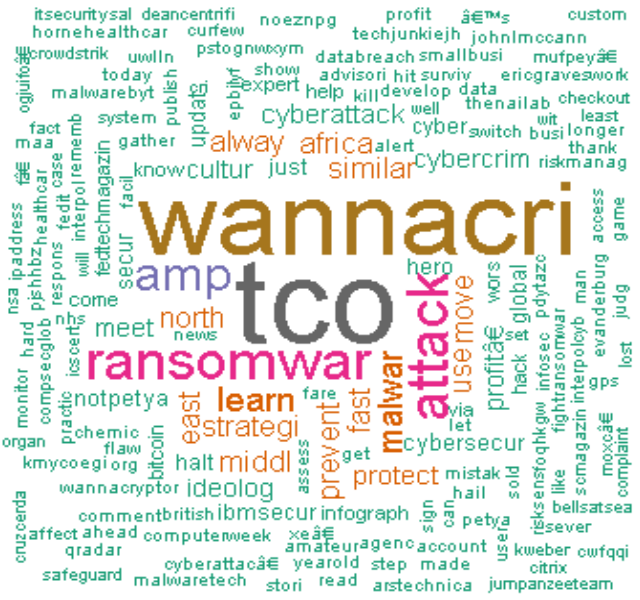

Fig 1: Implementing Word Cloud from Twitter

The resultant word cloud graph from tweets is represented in Figure 1 shows the most frequently used keywords by using text mining method from the twitter. Above Figure shall evaluate the amount of risk from this type of ransom ware.

III. INCORPORATING SECURITY MEASURES TO REMOVE THREAT

Most of the antivirus companies have updated their software to protect against Wanna Cry so that files can be protected for being encrypted. When this type of ransomware activated, immediately Antivirus detected i.e. pc is infected from WannaCry malware.

Pseudo code

A. Install antivirus & virus definition;

```
if(WannaCry Detect) {
  KB4012212 security updates Installed;
  while(Not Resolve)
    Other Security Update Suggest by Antivirus;
}
PC Protected;
```

Pseudo code represents that antivirus should be install in pc and virus definition need to be update regularly in order to remove the threat or to minimize the risk.

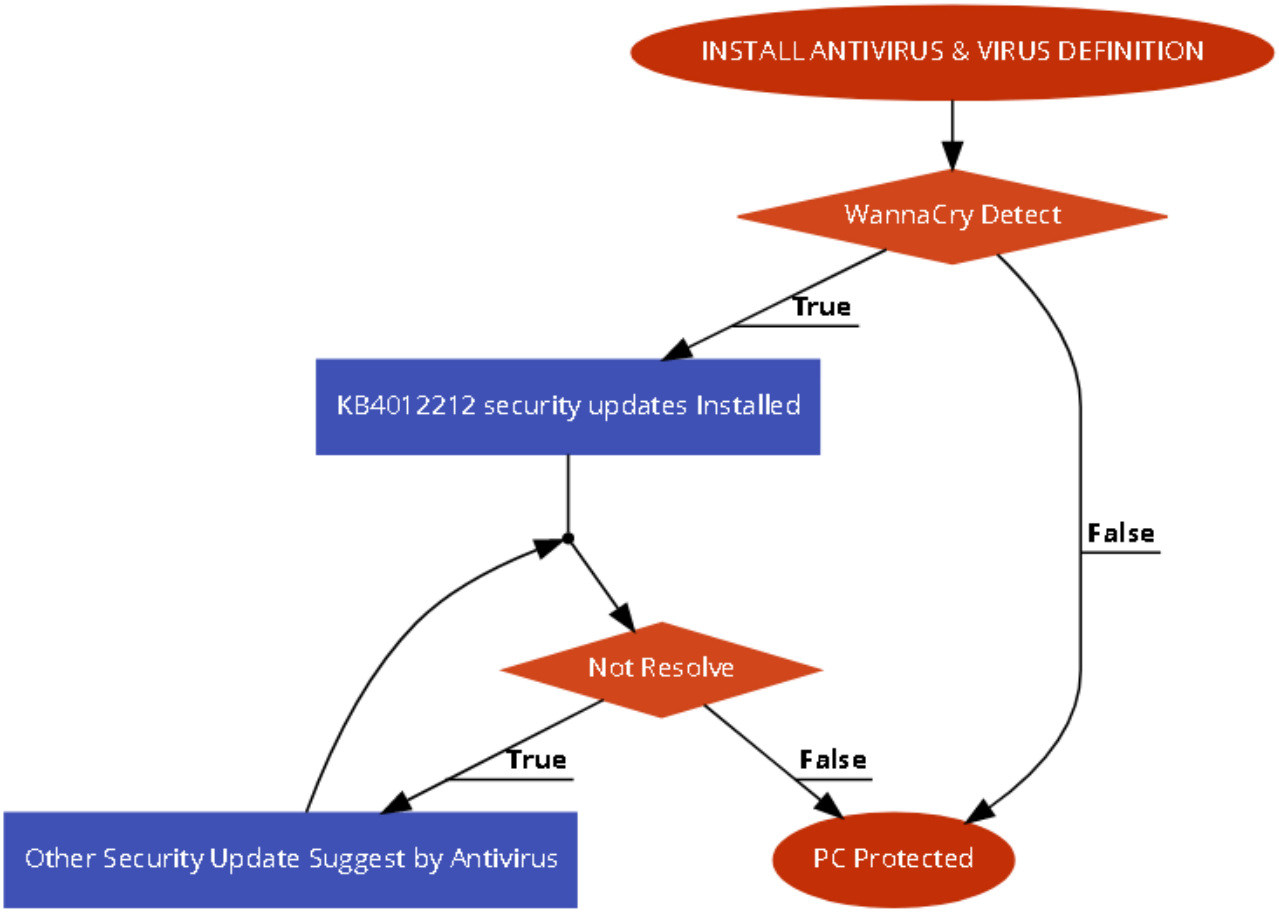

Fig 2: Implement Security Measure to Remove Wanna Cry

The affected pc can be running on older version of Windows file that contains a serious bug .Then link is available to resolve issues. "KB4012212" security updates need to install to remove threat from the pc. Figure 2 shall evaluate the security risk of victim's pc from the intruder. There are also many best practices to prevent from ransomware [1][2][3].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

IV. CONCLUSION

This paper has primarily described how WannaCry can affect victim's pc by encrypting files and asks for bitcoin money to decrypt the files.

Many security patches has been released from antivirus companies that need to be install .Antivirus immediately detect if Wanna Cry malware found and suggest to update security patches for the same.

REFERENCES

1. http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html
2. https://www.avast.com/faq.php?article=AVKB50
3. https://dl.acm.org/citation.cfm?id=3053035

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)