IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 61-68

Ransomware: Upraisal For BITCOIN

NAIRUTI SANGHAVI, RUTVA PATEL
EXTC Department Atharva College of Engineering Mumbai, India
EXTC Department Atharva college of engineering Mumbai, India
SHUBHAM S CHACHAN EXTC Department
Atharva college of Engineering
Mumbai India

Abstract: *On 12 May 2017, a massive ransomware attack occurred across a wide range of sectors, including health care, government, telecommunications and gas. To date, WannaCry has spread to over 300,000 systems in over 150 countries. The countries that appear to be the most affected are Russia and China, probably because of the high percentage of legacy software, with significant impacts elsewhere, notably to the UK National Health Service. The spread of the ransomware reportedly slowed in the two days following the launch of the attack, in part due to the discovery of a "kill switch" in its code. However, there are reports of new variants of the malware (such as) which do not have this kill switch. Data on new variants is unconfirmed and limited at the moment, EY publish updates as more information becomes available*

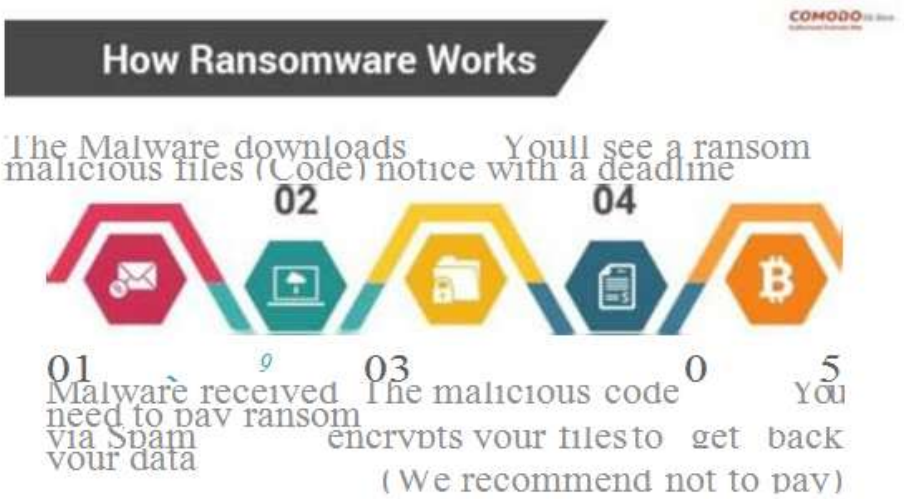
Keywords: kill switch, ransomware and legacy software.

I. Overview Of Wannacry

WannaCry is a Crypto worm which attacks files and local computer of windows. It was developed by national security agency of united states and was separated through eternal blue. It is operated by restricting access of files or folders unless a ransom is paid it majorly targets big companies and organization such as a British national health service, the Spanish telecom company, Telefonica, Russian oil giant Rosneft. They usually demand ransom in form of bitcoins equivalent to few hundred dollars to Un Crypt their files and the ransom increases over a time, until files are permanently damaged.

Both the SMB vulnerability was exploited by double pulsar and eternal blue that was made public by shadow broker hacking set in April.

Fig 1. How it attacks



II. How Wannacry Works

The initial vector of delivery for this malware was originally widely reported to be phishing emails, however data to validate this has not been confirmed and other reports suggest other vectors, such as the use of public-available weak SMB (Server Message Block) to spread the malware in a worm-life fashion. Once a virus takes place, WannaCry beacons out to the kill switch URL in order to determine if the malware is in a sandbox surroundings. If the URL does not respond, then the malware starts to encrypt the victim's files using an AES- 128 cipher. Files encrypted by WannaCry are appended with a file extension of. WannaCry as well as others. Unlike other ransomware families, WannaCry continues to encrypt victim files following any name changes and any new files created following infection. A ransom note is then displayed on the victim's machine, which is completed using text from a library of rich text format (RTF) files, in multiple languages and chosen based on machine location. Observed ransom demands require victims to pay either US$300 or US$600 worth of bitcoin (BTC) for a decryption key. Once infected, the user will see a screen (see Figure 2) with instructions on how to pay the ransomware.

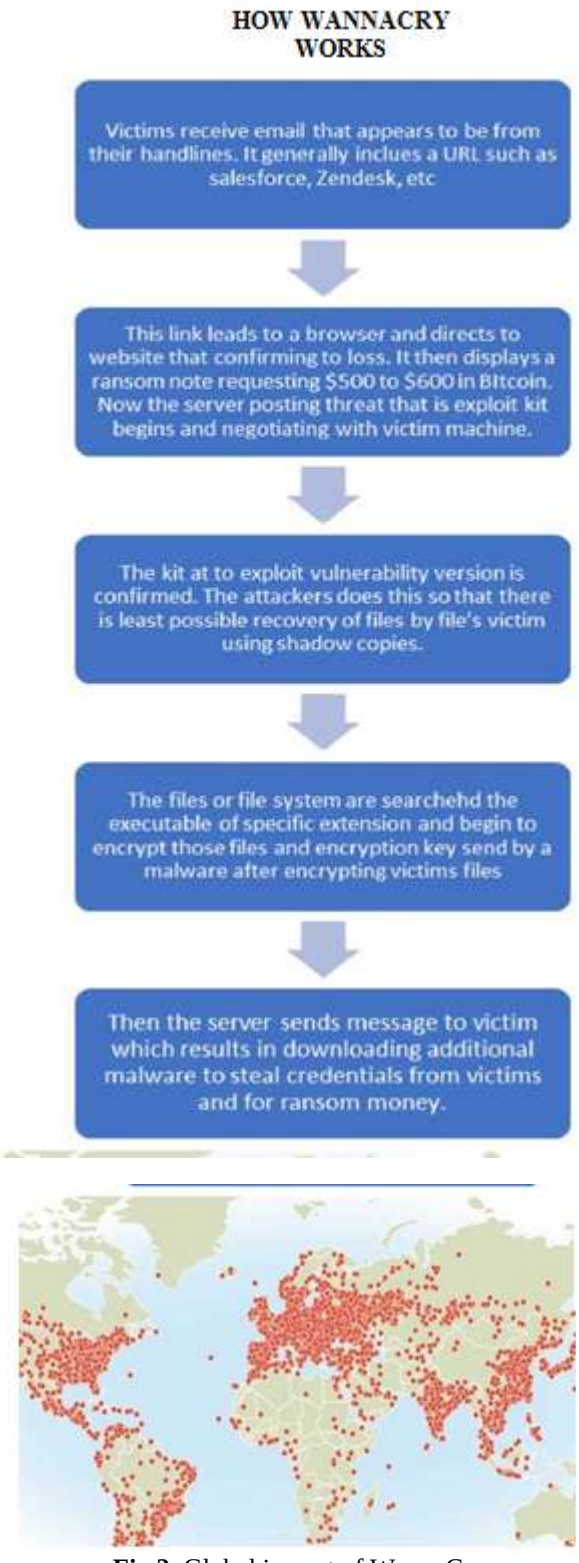


Fig 2. Global impact of WannaCry

On 12 may 2017 (morning) WannaCry entered cyber security.
Within a day more than 2300000 computer were affected in 150 countries leading to loss of approximately 4 billion financial losses.

Fig 3. Ransomware screen

WannaCry utilizes the violence Eternal Blue, created by NSA and released by Shadow Brokers (full details in Appendix IV) on 14 April 2017. Of note, the malware also checks accessible backdoors via Double Pulsar, also out by Shadow Brokers, in order to help through client networks. It should also be stated that the kill switch will not pause the attack if an institute is steering through an alternative for internet access. One of the first questions many fatalities ask is "how did I get infected with ransomware?" While it is not always immediately clear, the infection method for ransomware follows the same modus operandi used by cybercriminals to infect victims with any malware. As seen in Figure 4, there are many paths that can lead to a ransomware virus. However, the skillset and resources required to overcome modern defenses for the distribution of malware is outside of the scale of many amateur cybercriminals.

TRAFFIC DISTRIBUTION SYSTFM MALVERTISEMFINT

Fig4. Routes for ransomware to arrive on a compute

III. Bitcoin Ransomware EXTORTION.

Ransomware is one of the more upsetting types of malware to come into sight in recent years. It works by restricting access to computer files until a money is paid. Victims have included the British National Health Service, the Spanish telecom company Telefonica, the Russian oil giant Rosneft, and many others.

Victims are usually required to pay a Bitcoin ransom correspondent to a few hundred dollars to liberate their files. Typically, the ransom increases over time until a time limit when the files are apparently destroyed. Many companies and individuals have had little choice but to pay up.

And that raises a fascinating question. How much money have Bitcoin ransomware programs generated for their cruel masters?

That's because Bitcoin dealings are openly recorded and free to view. So, in principle, it should be possible to work out exactly how much each account receives. "Our aim was to accurately measure the USD worth of these payments," says Conti and co.

The team began by creating a record of Bitcoin balance sheet associated with this kind of movement since 2013, when the ransomware Crypto locker became the first to ask for payment in Bitcoin. "We found twenty ransomware that fulfilled our selection criteria, i.e., those ransomwares: (i) that used Bitcoin as at least one mode of ransom payment, and (ii) for which at least one Bitcoin address is publicly known," they explain.

For each species of malware, they provide a useful general idea of the way it works and spreads and how it has evolved more time.

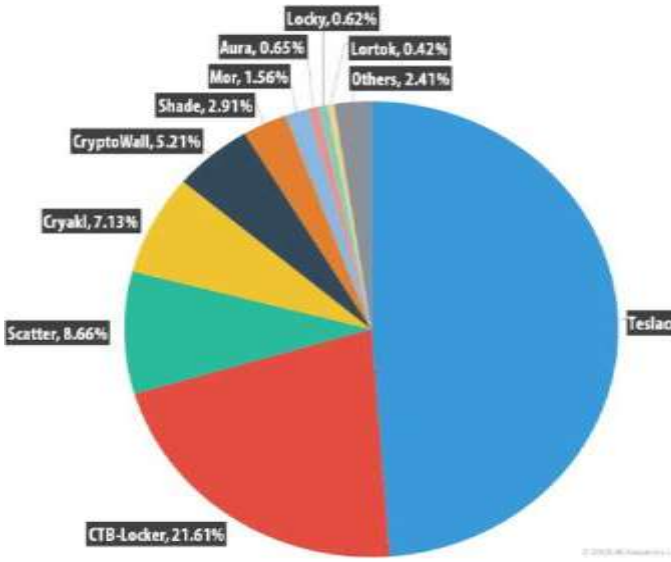
Today we get an rejoin appreciation to the work of Mauro Conti at the University of Padua in Italy and a team of contemporaries. These guys have created a database of Bitcoin accounts used by ransomware criminals and added up the ransoms paid into them. The result is a wide-ranging analysis of the profits made by cybercriminals in this budding area of crime.

Between its release and December 2015, Bitcoin addresses associated with this malware received $2.2 million in Bitcoin payments and a further $2.3 million in higher-value transactions, which Conti and co suspect may

also be ransom payments.
While ransomware can ask for payment in kind of currency, Conti focus only on those that ask for Bitcoin payments.

inquiringly, the total value of payments received by these Bitcoin addresses was over $45 million. Most of these transactions were not directly linked by Conti and co to

ransom amounts. That's a important amount of wealth ar raises the palpable question of what it was expense for. The full ranking of Bitcoin ransomware projects by the L dollar amount they generated is as follows:



Interesting^ , the WannaCiy outbreak received enormous media exposure as the malware spread widely. But the at was blocked b》 , the C3 , bersecurity investigator Marcus Hutchins, who discovered and activated a built-in kill sw that prohibited the malware from being more disparaging "The overall impact (including financial losses) due to WannaCty contagion could have been worse ... thanks tc earty recognition of the kill switch, which prevented the infected computers from spreading WannaCty farther," say Conti and co.

Fig6. Pie-chart

The team also discuss other forms of malware that asked for but do not seem to have received any extensive ransoms. These include TeslaCrypt, and Kill Disk.

Various other groups have passed out similar analysis and come to similar conclusion. However, Conte and co make their data set widely available so others can build on it. "The dataset contains a detailed contract history of all the addresses we accredited for every ransomware," they say.

Cybercriminals use Bitcoin because it provides a rumor has it that unspecified way of assembling and making payments. However, Bitcoin is phony to a certain extent than anonymous. That means users can protect their identify provided that none of their communication can be linked to their real identity. But as soon as a single transaction is associated to their personal identification data, then all of their transactions become linked in the same way.

A useful analogy is to authors who distribute under a pseudonym. As long as the author's identity is never linked to any of the pseudonymous articles, he or she remains unidentified. But if it is linked to just one pseudonymous article, it is linked to all of them, and then ambiguity is lost.
So pseudonymous protection is a fragile obsession. A single transaction that links a Bitcoin account to a personal account can reveal the identity of a cybercriminal. And personal data leaks all the time in web-based transactions. "Last year, we wrote about the imperfections in the anonymity of Bitcoin transactions. That should provide some anticipate tracking these criminals".
Conti and co have set this type of exploration as a future goal. "We will attempt to trace how the received ransoms were used and by whom," they say.

iv. CONCLUSION
Ransomware is not cheap; the average ransom demand hitting individual users now stands at a bulky US$300. In the past 12 months, we saw ransom demands range from US$21 to US$700. The exact amounts may vary depending on the ransomware family and the location of the victim. Striking a balance between volume and pricing is a continuing challenge for cybercriminals and some even offered to return data for free after a set period.
Ransomware attacks have led to vain financially viable victims during the past few years. Given the fact that spam emails represent the most common attack vector, teaching

users and escalating their attentiveness can definitely reduce the number of successful ransomware attacks in the future. Moreover, learning to approve effective backup strategies can reduce the consequences of successful attacks.

• ***References***

(a) https://en.wikipedia.org/wiki/CryptoLocker
(b) http://www.darkreading.com/attacks-breaches/new-zeus-banking-trojantargets-64-bit-s/240164713
(c) http://blog.fortinet.com/Ransomware/
(d) http://threatpost.com/zeus-source-code- leaked-051011
(e) http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-inlaundered-bitcoin-7000024579/
(f) http://threatpost.com/virut-and-waledac-botnets-spamming-sharedmachines-011513/
(g) http://www.fortinet.com/resource center/whitepapers/quarterly-threatlandscape-report-q 213. html
(h) https://www.decryptcryptolocker.com/
(i) http://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-nationalaction-against-gameover-zeus-botnet-and-cryptolocker-ransomware-chargesbotnet-administrator