ARC'18
مؤتمر مؤسسة قطر السنوي للبحوث
QATAR FOUNDATION ANNUAL RESEARCH CONFERENCE
البحث والتطوير: التركيز على الأولويات، وإحداث الأثر
R&D: FOCUSING ON PRIORITIES, DELIVERING IMPACT
19-20 مـــارس
19-20 MARCH

مـؤسـسـة قـطـر
Qatar Foundation
لإطـلاق قـدرات الإنـسـان.
Unlocking human potential.

Computing & Information Technology - Poster Display

http://doi.org/10.5339/qfarc.2018.ICTPD1026

Measurement and Analysis of Bitcoin Transactions of Ransomware

Husam Basil Al Jawaheri*, Mashael Al Sabah, Yazan Boshmaf

Qatar University, QCRI
* haljawaheri@qu.edu.qa

Recently, more than 100,000 cases for ransomware attacks were reported in the Middle East, Turkey and Africa region [2]. Ransomware is a malware category that limits the access of users to their files by encrypting them. This malware requires victims to pay in order to get access to the decryption keys. In order to remain anonymous, ransomware requires victims to pay through the Bitcoin network. However, due to an inherent weakness in Bitcoin's anonymity model, it is possible to link identities hidden behind Bitcoin addresses by analyzing the blockchain, Bitcoin's public ledger where all of the history of transactions is stored. In this work, we investigate the feasibility of linking users, as identities represented by Bitcoin's public addresses, to addresses owned by entities operating ransomware. To demonstrate how such linking is possible, we crawled BitcoinTalk, a famous forum for Bitcoin related discussions, and a subset of Twitter public datasets. Out of nearly 5B tweets and 1M forum pages, we found 4.2K and 41K unique online identities, respectively, along with their public personal information and Bitcoin addresses. Then we expanded these datasets of users by using closure analysis, where a Bitcoin address is used to identify a set of other addresses that are highly likely to be controlled by the same user. This allowed us to collect thousands more Bitcoin addresses for the users. By analyzing transactions in the blockchain, we were able to link 6 unique identities to different ransomware operators including CryptoWall [1] and WannaCry [3]. Moreover, in order to get insights into the economy and activity of these Ransomware addresses, we analyzed the money flow of these addresses along with the timestamps associated with transactions involving them. We observed that ransomware addresses were active from 2014 to 2017, with an average lifetime of nearly 62 days. While some addresses were only active during a certain year, others were operating for more than 3 years. We also observed that the revenue of these malware exceeds

دار جامعة حمد بن خليفة للنشر
HAMAD BIN KHALIFA UNIVERSITY PRESS

Cite this article as: Al Jawaheri H et al. (2018). Measurement and Analysis of Bitcoin Transactions of Ransomware. Qatar Foundation Annual Research Conference Proceedings 2018: ICTPD1026 http://doi.org/10.5339/qfarc.2018.ICTPD1026.

USD 6M for CryptoWall, and ranges from USD 3.8K to USD 700K for ransomware such as WannaCry and CryptoLocker, with an average number of transactions of nearly 52. One address associated with CryptoLocker ransomware also had a large amount of Bitcoins worth more than USD 34M at the time of writing. Finally, we believe that such type of analysis can potentially be used as a forensic tool to investigate ransomware attacks and possibly help authorities trace the roots of such malware.

1- «Ransom Cryptowall.» Symantec. June 14, 2014. Accessed November 01, 2017. https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99.2- Varghese, Joseph. «Ransomware could be deadly, cyber security expert warns.» Gulf Times. May 05, 2017. Accessed November 01, 2017. http://www.gulf times.com/story/546937/Ransomware-could-be-deadly-cyber-security-expert-w.3- Woollaston, Victoria. «WannaCry ransomware: what is it and how to protect yourself.» WIRED. June 28, 2017. Accessed November 01, 2017. http://www.wired.co.uk/article/wannacry-ransomware-virus-patch.