Tracking Ransomware end-to-end by Samuel Idowu

Ransomware attack victims by delivering spam emails into your network, and hiding binaries in your computer. Running the binaries encrypt your data, and you are not aware. Once your file has been encrypted, you get a node on your computer asking you to pay a ransom to an address, to get a decryption information. Once that payment has been made, the ransom family liquidate the payment, that is, they convert it from bitcoin to fiat currency. The utmost goal of the paper was discovering ransom deposit addresses, 25 seed addresses were discovered from forums related to different victims. The article ran binaries on Lockery and Cerber from VirusTotal. It was difficult linking addresses because Locky, Cerber use unique addresses for each ransom, but it ended up being possible as two models were employed, Clustering and Micropayments. Clustering used co-spent heuristics, and Micropayment employed using 0.001 bitcoin to ransom addresses and observing subsequent workflow. Limitations to both models include, Victim reported two ransom address of Sage but never did transaction, Micropayments made to Sage family never moved and Ransomware operator may decide to completely switch to different wallet cluster after receiving payment.

There is always a chance of potentially missing cluster of ransomware family. To determine, study of timing of bitcoin inflow with external indicators, like Google search, and Number of binaries in VirusTool. The article had also explained events overlaps as shown in Table III. The article also explained how it had filtered transactions. With Filter 1, Inflow should be consistent with ransom payment patterns, and any payment received by seed ransom address is potentially victim payment. Filter 2, Inflow sends payment from exchange cluster to ransomware cluster. The article explained Chainalysis is a proprietary online service that links clusters of wallet addresses to the likely real-world identities such as exchanges. Figure 3 presents a visual representation of the results after filtering transactions. The article was able to trace $16,322,006 US Dollars in 19,750 likely victim ransom payments for 5 ransomware families over 22 months.

The article studied time of payments too, Figure 5 presents the chat for the payment dynamics. Overall, both charts suggest that a potential Locky victim probably pays a higher ransom than a potential Cerber victim. With payment timing, It is likely that most of the paying victims of Cerber were located in Asia. Lastly, the article had explained cashing out for ransom families, and it dedicated Fig 8 to show its representation. In the median case, the bitcoins remained in WannaCry's cluster for 79.8 days, while for Cerber and Locky, the median holding durations are 5.3 and 1.6 days respectively.