Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks

Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

The paper presents the results of analysis (and study) of different ransomware attacks. The authors collected 1359 ransomware samples that have observed between 2006 and 2014 and categorized them into 15 different families. To create data set, they gathered the information from multiple sources (both manual and automatic crawling of public malware repositories). They show that, more than 94% samples fail to take all the victims resources as hostage. "Number of families with sophisticated destructive capabilities remain very small"[1]. They also provided, the analysis of how the ransomware samples evolved and changed during that period of time. And authors conclude that stopping these ransomware attacks is simple and not as complex as described previously. They show that, by observing unusual file system activity, it is possible to stop or prevent ransomware attacks (For eg. observing I/O requests and protecting Master File Table (MFT)in the NTFS file system). They also studied the charging methods embraced by different ransomware families. They also tracked down transactions of 1872 bitcoin addresses that were used during cryptolocker attack. From this study they conclude that, attackers are using different evasive techniques to hide the criminal activity.

2 Contribution

The authors analyzed (and categorized them in 15 different families) 1359 ransomware samples, by manual and automatic crawling of public malware repositories. They show that, prevention (defending) of ransomware attacks is not that difficult, even if suggest otherwise by previous research. Their analysis of bitcoin address suggested that the cybercriminals have adopted multiple evasive techniques.

3 Strengths

I like that they tracked down about 1359 ransomware samples and categorized them in 15 different families (which I believe is time consuming work). I also liked that they highlighted an important point - defending against ransomware attacks is not that difficult and achievable (rather than just giving them ransom). Also, I liked that they tracked 1872 bitcoin samples (which I believe is difficult).

4 Limitations

They collected about 3921 samples and removed more than half of them (they used 1359). They also mentioned that they might have missed some important ransomwares. Also, they don't talk much about the performance of the defense mechanisms.

5 Future Work

I think more work needs to be done to add missing ransomwares in the collection and also to develop defense mechanisms (and yes, without affecting the performance).

References

[1] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*, (2015)