Ransomware: Is human error the primary reason for the surge in this increasingly popular malware?

Craig Heptinstall Crh13- 110005643
Institute of Computer Science - Aberystywth University

***Abstract*—As computers and other machines become more and more an integral part of a person's life, the risk of a computer infection increases. The amount of platforms available to the common user today allows malicious attackers a variety of ways to access user's personal data (from contact details to banking details.) A class of malware that has been reported more than others in recent years known as ransomware has been taking advantage of user's fears and errors. Because most ransomware requires users to physically click a link or download a file to instigate this malware, human error can be perceived to one of the biggest causes of the rise of attacks.**

***Index Terms*—Computer Crime, Computing, Human Error, Malicious, Malware, Ransomware, Users, Virus**

I. Introduction

IN the past few years, the amount of news reports on cases of this form of malware has been increasing, showing both the rise of cases, and the sophistication of attacks. The most recent of these includes an article from the BBC [**?**], where a ransomware software known as Maktub emails a user not only a malicious link to the software, but the user's postcode to make it more convincing. With more and more intricate ways of persuading the users to access the malware, it is the up-most importance that user's should know when a link, email or web address is genuine. This paper looks into the opinion that reducing human error could reduce the number of infected machines, and in particular the number of cases of ransomware.

A. Ransomware

In order to look closely at some of the human errors that are causing the rise of ransomware, the malicious software should be examined, and reasons why this form of software is so effective in current times.

In a paper by A. Kharraz (A look under the hoof of ransomware attacks) [**?**], the authors give an insight into how attacks take place, and how a range of different encryption algorithms are used by several of the most common ransomware. Ransomware belongs to a class of malware identified by the author as âĂŸscarewareâĂŹ, which takes advantage of a usersâĂŹ fear of losing their private information or having their data exposed to others.

In addition to the basic introduction of what the author introduces ransomware as, is the startling statistics on this kind of malware. In 2013, the author reported an increase of over 500% (as shown in Figure 1.) on the amount of attacks compared to 2012. Because of this statistic, the author claims that ransomware is one of the most threatening viruses at the time the paper was published. In conducting research about the inner-workings of ransomware the author uses 1359 real-life reported cases of ransomware attacks in order to get consensus of how attacks are generally performed.

[IMAGE OF INCREASE]

They found most prominently:

- There are two main ransomware families (specific pieces of software which have developed over the years). Both with highlighted traits, these are:
  1) TorrentLocker - A ransomware exclusively distributed by email, and uses the infected userâĂŹs email address list to distribute further.
  2) CryptoWall - Communicates back to the attackers using the Tor network, to remain anonymous.
- There are a further 97 variants, most of which are related. Some are direct copies however.
- 35.6% of the attacks were made by ransomware that do not perform encryption, but simply delete users files if they do not pay the ransom.
- CyrptoWall infected 250,000 computers worldwide in the year of publishing (2015).

Both of the described ransomware families above are particularly sophisticated according to the authorâĂŹs findings, stating that they both use AES (Advanced Encryption Standard) to encrypt user data. This happens once a user is infected, and because of the high level of security AES was designed for (this method is used by the U.S. government to encrypt classified information for instance [**?**]), it makes any attempt at decrypting user data without paying extremely difficult.

Although other ransomwares use less sophisticated locking mechanisms such as standard Windows functions as described in the paper, a common user would still not be able to unencrypt the data without the help of good decryption software or with guidance from professionals. The paper noted that it in fact most ransomwares were not concentrating on the strength of the encryption, as long as it took away the ability for users to access files, then they could begin holding such users at ransom. In a whitepaper published by Boromium Security [**?**], file type targeting is something that can increase the efficiency and speed at which more vital files are encrypted. By only encrypting recently modified, new and common file-type files (as shown in Figure 2.), a ransomware can cut its footprint and avoid anti-virus systems detecting major file system changes. [IMAGE OF FILE TYPE TARGETS] Although the paper mentioned earlier (A look under the hood)

goes into great detail of how ransomware functions, and the statistics around them, the means at which users receive the malware is very brief in KharrazâĂŹs paper. In order to understand how ransomware is transported, and how this relates to user responsibilities, other papers gave good insight. The Bromium whitepaper [**?**]listed findings for most common ransomware attacks:

- Spam or social engineering
- Direct or indirect user download
- Malware installation tools and botnets

Where these means of infection relate to the topic of this paper is in the fact that all three contain some user involvement. Without the user clicking on a suspicious link, downloading faulty software, or installing software with unwanted additional add-ons, it could be claimed that malware would not exists or exist in a different manner, as told by K. Wyk [**?**]. Because ransomware realises heavily on user interaction, this is where this form of malware is required to look more professional than traditional viruses or spamming software.

The Bromium report highlights the professionalism that is shown from some of the ransomware seen, and the increase is overall sophistication, making it more believable to be safe software of any kind. As mentioned in the abstract, emails produced to bring users to download the malware has been found to be increasing in sophistication too, with the use of correct user postcodes sent out. Because of this professionalism in the malware produced, software can almost seem to be on the side of the user when trapping them into a ransom.

B. Human errors- the consequences

II. Conclusion

The conclusion goes here.

Appendix A

Appendix two text goes here.

Acknowledgment

The author would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.