# 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 (malicious software) 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.

# Introduction

Over 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 \cite{bbc-ransomware}, 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 upmost 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.

## 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. \par

In a paper by A. Kharraz (A look under the hood of ransomware attacks) \cite{paper4}, 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 ransomwares. Ransomware belongs to a class of malware identified by the author as ‘scareware’, which takes advantage of a users’ fear of losing their private information or having their data exposed to others. \par

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. \par

[IMAGE OF INCREASE]

They found most prominently:

\begin{itemize}

\item There are two main ransomware families (specific pieces of software which have developed over the years). Both with highlighted traits, these are:

\begin{enumerate}

\item TorrentLocker – A ransomware exclusively distributed by email, and uses the infected user’s email address list to distribute further.

\item CryptoWall – Communicates back to the attackers using the Tor network, to remain anonymous.

\item There are a further 97 variants, most of which are related. Some are direct copies however.

\item 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.

\item 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 author’s 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 \cite{aes}), it makes any attempt at decrypting user data without paying extremely difficult. \par

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 \cite{bromium}, 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 Kharraz’s paper. In order to understand how ransomware is transported, and how this relates to user responsibilities, other papers gave good insight. The Bromium whitepaper \citte{bromium}listed findings for most common ransomware attacks:

\begin{itemize}

\item Spam or social engineering

\item Direct or indirect user download

\item Malware installation tools and botnets

\end{itemize}

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 \cite{artical}. 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. \par

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. \par

Physcology of ransomware, giving a free key etc

More physcolodgy stuff

# Human errors- the consequences

# Prevention of ransomware

Research:

2

Ransomware has been increasing in sophistication since it first appeared in September 2013

ransomware immediately makes its presence known by encrypting files and demanding payment for the keys to unlock them. Victims of the attack may experience anxiety or disbelief, so they are likely to pay the ransom to end the incident

After that it notifies the user that their files were encrypted and demands ransom for decryption

Crypto-ransomware is rather different from traditional malware: • It doesn’t steal victim’s information—instead it makes it impossible to access your information • It doesn’t try to remain stealthy after files are encrypted because detection won’t restore the lost data • It’s relatively easy to produce—there are a number of well-documented crypto-libraries

Crypto-ransomware compromises the endpoint through one of the following attack vectors: • Spam / Social engineering [1] • Direct drive-by-download [2] • Drive-by-download through malvertising [3] • Malware installation tools and botnets [4]

Human error stuff:

1

A person can be fool, distracted, persuaded, distracted and blackmailed but the conditions that increase the errors can be individual and based on the humans characteristics for example when a person’s tired, idle, apathetic and uncaring. The study of human errors in the event is relevant to industry accident.

The errors can be caused as a result of lack of knowledge, ignorance, and experience [6].

These days, many organizations spending large portions of their budgets on defending against technical attacks and do nothing to prevent operation of the human factor.

One way is keep people away from making errors or keep the errors from reaching the system.- Prevent emails reaching people?

ISPs to provide protection against phishing, viruses and spyware

Using firewalls and phishing filters are reduced the chances and so reduces the human errors relating to risky computer use. The other way can be keeping a backup of data, it does not any elimination by accidentally delete, disrupt or steals. The backups are reduced recover the data when they accidentally deleted, and also the damage done by cruel effort to destroying data

Using the software that manage the incoming and outgoing emails reduce the general misuse of email and encourage good practice. This software will check sensitive attachment data and reduce the possibility of human errors

Solution stuff:

3

Most infections occur as a result of unsuspecting employees opening infected emails which appear to be legitimate or by following an emailed link or visiting an infected website

This virus can be stopped by utilizing high-quality antivirus software such as Symantec Endpoint Protection, which offers traditional file-based protection, alongside web browser and download protection

There are no tools or Data Recovery Services that can decrypt your data; it is unrecoverable in this state

must be paid in Bitcoin. By using this payment method, these criminals cover their tracks

Educate your staff. One of the most common causes of infection is an employee clicking on a link or opening a file sent from a legitimate source they might have corresponded with in the past

sending you an unknown file, call them and inquire before opening. If it’s a link then evaluate it before clicking on it. This can be done by hovering

All incoming email must be scanned for viruses. This is the primary entry point for Ransomware

Maintain Patch Levels for OS and Applications

Block End Users from Executing Malware

Deploy and Maintain Backups

4

API Call Monitoring

As discussed inSection3.1,asigniﬁcantnumberofransomware samples use Windows API functions to lock the victim’s desktop. Those API calls can be used to model the application behavior and train a classiﬁer to detect suspicious sequenceofWindowsAPIcalls.Thisapproachisnotnecessarilynovel, butitwouldallow us to stop a large number of ransomware attacks that are produced with little technical efforts

MonitoringFileSystemActivity Ouranalysisalsosuggeststhatitispossibletodetect ransomware attacks – even the ones using deletion and encryption capabilities .BycloselymonitortheMFTtable,one can detect the creation, encryption or deletion of ﬁles. For example, when the system is under a ransomware attack, a signiﬁcant number of status changes occur in a very short period of time in MFT entries of the deleted ﬁles

Refs

<http://www.bbc.co.uk/news/technology-35996408>

paper 4

<http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>

article

<http://www.esecurityplanet.com/views/article.php/3377201/Blaming-Users-for-Virus-Chaos.htm>