Ransomware: Studying transfer and mitigation

Conference Paper · December 2016

DOI: 10.1109/CAST.2016.7914946

4 authors, including:

Rhythima Shinde
ETH Zurich
17 PUBLICATIONS **156** CITATIONS

SEE PROFILE

Jan van den Berg
Delft University of Technology
135 PUBLICATIONS **2,766** CITATIONS

SEE PROFILE

2016 International Conference on Computing, Analytics and Security Trends (CAST)
College of Engineering Pune, India. Dec 19-21, 2016

Ransomware: Studying Transfer and Mitigation

Rhythima Shinde
Algorithmics, Faculty of Computer Science
Faculty of Technology, Policy and Management
TU Delft, Netherlands
r.shinde@student.tudelft.nl

Pieter Van der Veeken
Cybersecurity section, Faculty of Electrical Engineering, Mathematics & Computer Science
TU Delft, Netherlands
pietervanderveeken@gmail.com

Stijn Van Schooten
Cybersecurity Section, Faculty of Electrical Engineering, Mathematics & Computer Science
TU Delft, Netherlands
S.vanSchooten@student.tudelft.nl

Jan van den Berg
Information, Communication and Technology, Faculty of Technology, Policy & Management,
Cybersecurity, Electrical Engineering, Mathematics & Computer Science, TU Delft, Netherlands
J.vandenBerg@tudelft.nl

***Abstract*— Cybercrimes today are focused over returns, especially in the form of monetary returns. In this paper - through a literature study and conducting interviews for the people victimized by ransomware and a survey with random set of victimized and non-victimized by ransomware - conclusions about the dependence of ransomware on demographics like age and education areshown. Increasing threats due to ease of transfer of ransomware through internet arealso discussed. Finally, low level awarenessamong company professionals is confirmed and reluctance to payment on being a victim is found as a common trait.**

Keywords—Mitigation, Ransomware, Demographics, Transfer, Internet, Cyber Crime Science

I. INTRODUCTION

Ransomware is a type of malware that makes files on a victim's computer inaccessible and then demands the victim to pay a ransom (usually in the form of bitcoins) in order to regain access to the lost files [1].The research focuses on the delivery of and protection against ransomware. Thus, this paper presents two research objectives: First, an analysis was done on how ransomware is delivered ona victim's computer using literature study and survey distribution and analysis. The most common infection methods, such as popular application vulnerabilities or the wide spread torrent network [2], was studied. It was attempted to gain an insight into the direct means of delivery to form a comprehensive view on how and why ransomware is effective. Second, this study explored the measures and actions which can be taken to defend against these kinds of malware attacks.

Section II explains the methodology of research involving literature study as well as the method of conduct for the surveys and interviews. A literature study was performed on the transfer and mitigation of ransomware, which helps explain the recent developments and criminology trends in ransomware. This is discussed in section III. Section IV elaborates on the survey results and is followed by section V, which analyses the literature and the survey results. Finally, the research paper is concluded with recommendations and conclusions in section VI.

II. METHODOLOGY

The research objectives postulated in section I have been answered by studying literature, the outcomes of a survey and of interviews results. The literature review focused on the development of transfer and mitigation methods of ransomware, and the understanding of the latest trends in criminology mindsets. The survey was validated based on interviews with some subjects who were confirmed victims of ransomware and were willing to disclose information about this event. The methodology has been approved by the ethical committee of the research university.

A. Survey and Interview Conduct

The first round of (structured) interviews provided input and insights, which were used to finalize the survey questions (interview questions can be found on google forms[1]). Then, with the help of social media, which also forms a part of the control group, volunteers were asked to fill in an anonymous survey who belonged to both victim and non-victim groups. Of these volunteers, their perceptions was recorded, with their awareness and (if applicable) initial reactions to ransomware. We used a number of different mediums in attempt to maximize the spread of our survey. The survey was circulated in both Dutch and English language using various mediums like Fraud Help-desk, ICT Help-desk of the Delft University of Technology, Police of Delft, and the affected (victim) acquaintances by means of a snowballing technique.

B. Maintaining the Integrity of the Specifications

The research done on various mitigation strategies was combined with insights gained from relevant literature about ransomware delivery and mitigation methods. The demographics like age, gender, level of education were studied explicitly to understand their dependence (if any) on the type of mitigation strategies, awareness and the losses expected or incurred. The questions were designed in such a manner that confidentiality of the entered information would be maintained

[1]https://docs.google.com/forms/d/e/1FAIpQLSc0geYBXOvJ1egoqwi9OB2JWEU6I-OpucZJaIMPUQ-VlM2Y6A/viewform

at all times. The answers to the interview questions are mentioned in the table. The interviewees evaluated the survey and on the basis of their responses, a modified survey was designed. Analysis of survey results

The survey results were analyzed using statistical analysis (in form of correlation tests, and, if applicable, multivariate analysis) of all the variables affecting 'losses incurred'. Figure 1 shows the assumed dependence of expected losses in cases of non-victims and those incurred in case of victims, on other parameters. The independent variables, for example: the demographics (age, gender, etc.) parameter and 'level of awareness' are considered. The co-dependence of the independent variables (for example, 'type of the delivery method' used on the 'type of company') is used to recommend some measures to control ransomware delivery and losses. These socio-demographics are chosen/assumed based on the literature recommendations [3]. This analysis, explained in detail in section IV aims to help in recommendation for mitigation of ransomware or reducing losses by controlling or affecting the parameter with higher dependence.

III. LITERATURE STUDY

Accompanied by the survey analysis, the literature study on developments in transfer and mitigation of ransomware aims to make the recommendation for prevention of ransomware more practical due to clear understanding of the criminal mindsets.

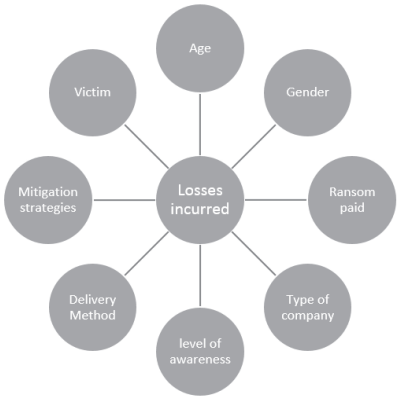

FIGURE 1 DEPENDENCE OF LOSSES ON PARAMETERS

A. Transfer of ransomware

With time, ransomware has evolved now focusing its target on desktop computers and targeting less secured areas like mobiles and M2M(machine-to-machine) communication. The transfer happens via crypto-ransomware, which is defined as a type of malware that injects malicious code and gets installed as an executable in the system location that encrypts a users' data. The access to data is restricted until the user pays a ransom for decryption [4]. Locker-ransomware completely locks the device of user system or input device [5]. The developments with type in transfer methods and its impacts are discussed in the Table 1. The historical developments are relevant to study because ransomware has risen when the opportunity arose. Thus, there is a good chance that the historical methods will be repeated.

Summarizing, the usual recent methods of transfer are as listed below [5]:

- File Encryption Ransomware which involve symmetric (256-bit AES key) for encryption and asymmetric (RSA private key) methods for decryption. Access to Internet and server is usually required for this, but this is not always the case: e.g., CBT lockers do not need access to Internet.
- Screen lock Ransomware: Here a Trojan constantly generates messages using the APIs from the OS to perform continuous loop.
- Windows & Browser Lock: Here the "malware is not executable and the ransom message page contains just images and HTML code running JavaScript controlling the background threads and applications ensuring the message is active[5]".
- POPUP Advertisements are usually built nowadays on Adobe Flash, such that the pop goes undetected. The advertisements are run from the web-page itself. Then, the ransomware scripts are pushed and executed on the fly. In some cases scripts are pushed to understand user browsing patterns and then the malicious applications use these sites for attacks.

This study over the transfer methods reflects that how the complications in implementation of such ransomware have evolved and this suggests that

- The targets have shifted from personal desktops in a physical form (like via a floppy) to more centralized systems like hospitals.
- The transfer is not just based on torrents, mails and such Internet based applications. The latest trends have also made them possible to be activated on an offline system.
- Also, the attacks have occurred at the systems which are not a major IT specific company, like health care centers, and thus security of the IT systems is not one of their major priorities.
- Advertisements have become 'smarter',i.e., they are generated based on learning from the user generated patterns like browsing history. This makes a user more prone to the attacks.

TABLE 1: LITERATURE STUDY OVER TRANSFER AND IMPACT OF RANSOMWARE WITH TIME

Year	*Transfer mode and impacts*	
1989	1) First ransomware ever used - used as "PC CYBORG /AIDS information Trojan" 2) Delivered by floppy disk 3) Replaced autoexec.bat file counting the number of time system reboots, and as number reaches 90"Trojan hides directories and encrypts all file names in the systems root directory." [REF] 4) Finally a message asking ransom is displayed by Trojan	[3]

2005	1) GP coder modified with RSA encryption 2) Enters through email spams, determines and encrypts the files of determined extensions and places ransom notes for getting decoder	[3]
2006	1) CryZip "uses a commercial zip library to store files in password-protected zip files" [REF] and comes in the form of DLL files 2) May Archive with a paradigm shift by provoking the user that they can benefit too	[3]
2007	1) Annoying pop up messages 2) Threats about sensitivity of the downloaded file 3) Blocking user files by saving them with a password in form of compressed archive	[6]
2007	Ransomwares increased its spread, with the study results revealing that the codes are quite basic, stating "ransomwares strength comes from the fear they generate into lambda-user mind, not from their technical skills" [REF]	[7]
2010	1)Evolving social media attacks fooling even sophisticated users 2)Ransomware attacks on mobile platforms	[8]
2013	4.1 million attacks, Health organisations were major targets	[9]
2014	1)Ransomware attacks more than doubled in 2014 (8.8 million) 2)Available toolkits like tox virus which allows crypto-ransomwares to be built in few clicks 3)Crypto-ransomware expanded from 8,274 in 2013 to 373,342in 2014	[10, 4]

B. Mitigation of ransomware

The literature study results show various strategies and social parameters that play a major role in preventing and mitigating ransomware. These methods are consolidated here in the Table 2. This literature study depicts that:

- The socio-demographic parameters of a user like level of education, etc. decides that how prone a system/user is to an attack and how well he/she is going to react to it, if attacked.
- All mitigation strategies mentioned in the literature align towards prevention methods, i.e., user awareness while downloading content from the Internet, etc. Also awareness education and training are discussed in the literature which focus to promote a company culture for prevention of exposure to ransomware.
- The only suggested 'cure' methods emphasize on not paying the ransom and rolling back the machine to earlier versions to clean the malware off (assuming the user has the habit of backing up his/her work).
- The construction of secured platform emphasizes on the need of cloud run platforms, which are open in nature to contribute and make use of for prevention and awareness.

C. Cyber Crime Science

This section of literature study is aimed at understanding that how the criminology is developing in the sector of cybercrime. As it is important to understand users/ potential mindsets (through various social parameters as mentioned in the section B above), it is equally important to understand the evolving criminal minds and theories behind the trends. Some of the relevant studies are mentioned in the Table 3. In section 5, these are discussed in more detail with input from section *A* and *B*. Major conclusions from these literature sources are:

- Attacks in cyber-crimes are more focused on financial gains nowadays.
- The criminal activities happening online have escalated as difference between criminals who operate exclusively online and those who use ICT to enhance their own criminal activities has diminished.
- Online payments, gaming and online auction activities have opened up the 'market'for the criminals and all of these are successful based on principle of disguise.
- Social networking sites gives away personal user information and thus encourage identity theft or context-aware phishing. Alongside blogs,these increases the threat of distributed propaganda by terrorist groups and also dissemination of malicious codes.
- Right legislation needs to follow the same crime tackling steps for cyber-crime as any other crime by asking the right why, what and how questions.

TABLE 2. LITERATURE STUDY OVER MITIGATION OF RANSOMWARE

Strategies		***Sourc***
User Mitigation strategies	**Other strategies:**	
1) Look out for paying through new specific websites which are being "suggested" while browsing web 2) Beware of popups generated as ads and avoid clicking them 3) To prevent malware through botnets, update your antivirus as soon as an update is released 4) Do not submit to the demands of malware 5) Roll back machine to the earlier backed upstate	Parameters for strategies 1. Complexity Level of Malware 2. User Level and type of education 3. Urgency of Recovering the Seized Resource	[3]
1) Avoid clicking on email attachments from unknownusers 2) Reinstalling OS and disconnecting from internet as soon as the malware is detected can help further harm, if affected by the malware	Security Strategies: Implement a cloud based sandboxing which helps other users become aware in any part of the world	[5]
Providing awareness education and training in three ways: 1) Access control and management 2) Exposure analysis and report 3) Policy andregulations		[6]

TABLE 3: LITERATURE STUDYSUMMARY OVER CYBER CRIME

Theory/ Study	*Source*
"Financially-motivated attacks are becoming more	[11]
"Traditional organized criminal groups which make use of ICT to enhance their terrestrial criminal activities; organized cybercriminal groups which operate exclusively online; and organized groups of ideologically and politically motivated individuals who make use of ICT to facilitate their criminal conduct" are no more distinct and their distinction is converging	[11]
The money laundering process takes place in three steps: Placement, Layering and integration which works on the principle of disguise in activities like online auctioning, digital precious metals (offshore banking) and other forms of online payments	[11]
The definition of cybercrime is not just based on deeds such as "deeds as deviance, disorder, antisocial behavior, acts of terrorism, and offenses occurring in cyberspace" but rather includes every "behavior in which computers or networks are a tool, a target, or a place of criminal activity"	[12]
It needs to be understand that "what are the immediate causes and important factors of a particular form of cybercrime by answering why, where, when, by whom, and how a specific offense was committed and determining how to prevent it". This may be solved technically or by using right legislation	[12]
Suitable answers need to be found in understanding "methods for committing a crime, increasing the risk of the crime, reducing the rewards from crime, reducing the provocations that invite criminal behavior, and removing the excuses for criminal behavior".	[12]

IV. SURVEY AND INTERVIEW RESULTS

The results and responses from the interview and the surveys conducted are discussed in this section. The responses are first described from every set of interview and survey. Next, a conclusion of all these results is presented, which is incorporated for the analysis and conclusion of the study. In total, 23 respondents filled the surveys, two interviews were conducted and the details of these respondents are explained in section *B*.

A. Preliminary Interview Responses

Two subjects whom were interviewed are acquainted to one of the researchers. Both of these subjects were male and above the age of 35 (Subject 1: 48 years old and Subject 2: 37 years old). Both subjects were victim of ransomware and Subject 2 came to know about ransomware only after he was a victim. Subject 1 is an employee in a retail firm, which is also where he was targeted. Subject 2 is a freelance designer who was targeted on his personal computer. Both of them were still unaware about possible mitigation steps they could take, even though they both had been victims. When faced with this malware, their first reaction was panic and then they relied on an acquaintance for help. The events happened 2 and 1 years ago for subject 1 and 2 respectively. Both of them were asked money in the form of Bitcoins, for the amounts of 1.2 Bitcoin and 350 dollar respectively.

Subject 1 contacted the IT department of the company where he worked to understand the scenario. When they didn't know what to do, he went to the management. Whereas, Subject 2 waited for a day to get help from his relative studying in an IT field.

Subject 1 left his workstation with the IT department andis to this day still unaware of what was done regarding ransom payment. Subject 2 did not pay because he had already made a backup of his work. Subject 1 assumes the infection was through outlook while subject 2 assumes he was infected through an illegally downloaded torrent.

In summary, both of them lost around 1000 euro worth of time and data (Subject 2 didn't lose any data due to backup). Subject 1 is still unaware of prevention measures, but he has shifted to another workstation, while subject 2 simply reinstalled his MacBook. Subject 1 accepted that he doesn't do anything to prevent ransomware attacks while subject 2 backs up his data more regularly.

B. Survey Descriptive Analysis

1) Sample demographics study

There were total 23 survey respondents and all of them except three had either bachelors or master's degree as the maximum education level (exceptions had maximum high school or trade school education). 64% had master's education while 24% had master's education as the highest education level. The distribution of age has a mean of 32 years and a standard deviation of 15 years (with minimum of 18 years and maximum of 61 years). Having performed a Kolomorgov-Smirnov test [REF] to check whether this distribution is normal or not, the null hypothesis was rejected with test statistic value of 0.357. Outof all the 23 respondents, 24% were female and 76% male. Performing the chi-square test [REF] on age and gender, the data can be said to be non-representative of the population of Netherlands (Netherlands census data - CBS - is used here, and considering the geographical and time constraints, only The Netherlands' population was considered for study purpose here).

2) Descriptives of losses and related parameters

80% of the sample was not a victim and 20% of them were a victim of ransomware. When asked about how they came to know about ransomware, maximum of them, i.e. 36% stated they knew of it from watching the news. 20% of them came to know about this because of articles on Internet, and 16% of them were aware because they were victims. 12% were aware of ransomware due to colleagues or victims and 16% were not aware of ransomware at all. Of those who were victim, except one all of them were victimized in a company/ professional environment. Out of the four who were victimized in professional environment, only one contacted the IT firm, one contacted a security firm and other two chose to rely on family contact or just roll back the operating system. None of them paid, and when asked the reason all of them stated that they were not sure if paying would help them retrieve the data. One of them was able to fix up the malware affects him (her)self, by removing the infected files that caused the popup screen. Some of them lost money, time and data all, and blamed it to be transferred due to downloading infected files.

The preventive measure they take have been updated anti-virus and better backups.

When asked about mitigation strategies to check the level of awareness, 72% of the sample set knew about the mitigation strategies, while 28% were unaware about it. The mitigation strategies were primarily good backups of data, and timely update of antivirus. Some of the suggestions were also about disabling Microsoft remote desktops, and installing ad-blockers. Interestingly, the majority of the victimized people (and also from company/professional environment) were unaware of the mitigation strategies, and considered it as only the responsibility of IT firm. When asked for the mitigation strategies, 60% of them preferred contacting an acquaintance, 20% of them preferred working out on their own (considering some of these were students studying cyber-security), 12% of them preferred an IT department, and just 2 of them preferred either paying or going to an external security firm. None of the non-victim population had taken any precaution against ransomware, but many of them are aware about spam mails and do not download any suspected files, or click on random advertisements on Internet.

3) Correlations of the parameters

It is assumed due to the literatures that some of the parameters specifically affect the level of awareness and the losses incurred by a person when affected by ransomware. The assumptions regarding payments of ransom cannot be checked with the small sample set of only 5 respondents becoming victimized. It should be noted that some tests like gender versus victim or not are not done due to the less number of data points available (no victims were female in the sample). Some of the parameters which are checked for any relation are:

- Education level versus Mitigation strategy known or not? Interestingly, the graphs here as in figure 5 shows that there are only students with bachelor's degree as the highest education level here who are aware of the methodology to mitigate. But it can be because of two reasons; majority of bachelors in the sample set, and students with doing masters in cyber security being a sample set of the research. But this also shows that students/ working people with higher degree are not trained/educated enough to be aware of mitigation strategies at all.
- Age versus mitigation strategy known or not? There is no relation that can be statistically shown for age versus mitigation strategy awareness (null hypothesis of a Mann Whitney test was higher age will make a person more aware of the strategy, but the hypothesis was rejected for significance of 0.000 value) and the relation can be seen in Figure 3.
- Age versus victim or not? It can be seen that though there is not a significant relation (Mann Whitney test - 0.012: significance value), a more aged person is less vulnerable to a ransomware as can be seen in the Figure 2. This can be considered as experience based learnings and thus not a significant but a weak correlation exist between the two. But from the above point, it can be analyzed that though the number of aged victims reduce (reason can also be due to their lack of exposure to internet based applications), but they do not learn the mitigation strategies.
- Gender versus mitigation strategy known or not? It can be seen from Figure 4 that none of the females were aware of the mitigation strategies, but because of the small sample size, no conclusions can be made.
- First reaction versus mitigation strategy known or not Only those who would react to contact their acquaintances, or were ready to solve the issue on their own, or finally were ready to contact a security firm were ready with some mitigation strategies as shown in figure 6. These results cannot be significantly acceptable and applied because the 1st set of group is majority and the 3rd set is a minority and those who claim to work on their own are surely equipped enough with mitigation strategies. The only interesting part here to see is that though the people who were ready to contact their IT department were not at all aware of mitigation strategies. This depicts their complete dependency on IT department for any ransomware attack.

V. ANALYSIS

1) Payment

From the survey results and the literature it can be concluded that only a very small portion of the victims actually pays the attacker. There are most likely multiple reasons for this, such as a deep distrust of the instructions to download the TOR browser [REF] and buy Bitcoins (both technologies with a seedy reputation). Furthermore, it seems likely that a significant portion of the victims do not possess the necessary technical skills to install and manage these technologies, even if they did have the intention to pay.

2) Transfer

Victims which can, from the attacker's point of view, be seen as viable targets are a small subset of the total group of victims. Viable targets are victims who have lost important data, require the technical skills to make a payment and are also willing to do so. It can therefore be assumed that most ransomware distributors use a 'shotgun approach' in the hope of reaching some viable targets and, in process, create a lot of collateral damage. The role of Internet is also a pressing threat for easier spread of ransomware.

3) Mitigation and Awareness

Mitigation of the ransomware can be done in several ways: Off-site backups, capable anti-virus software and user training. From the survey and literature analysis it looks like the former and the latter are the best options for decreasing threat to a user. It has been shown repeatedly that antivirus software are not particularly good at detecting ransomware

software, because they do not perform suspicious actions such elevating access rights or, trying to obtain root access. From the survey the fact has come forward that awareness of basic security best practices is extremely low. As such it seems that a lot of progress can be made by educating computer users of how to create safe backups and how to recognize threats on the internet.

From the survey it too became apparent that in a corporate setting most users will by default assume that any computer problem is the responsibility of the IT department. While this is true to some extent, this attitude also leads to carelessness and irresponsible behavior. Therefore companies could most certainly benefit from training their employees in basic security best practices.

4) Age and Education

The conducted survey shows an inverse correlation between awareness of ransomware and age. This is expected, because older people generally have less knowledge about computers. As such, training efforts should focus on the older segment of the population. Added to the analysis above, one should be aware about the near future threats like, so that there can be enough precautions taken to prevent getting victimized by Ransomware:

- Self-replicating malware (e.g. file infection or mass mailing).
- Ransomware using other malware as its host.
- Ransomware development as a service: "RaaS offers to carry out malware attacks on payment or from the profits running it like a business service on the cloud" [5].
- Threats like lock the access to our own items like car because of easier access through Internet of Things [13].

VI. Conclusions and Recommendations

In this paper we have shown that awareness of ransomware is incredibly low, especially of older persons. The transfer of ransomware has become pretty easy with growing Internet-based services. In company environments, high irresponsibility of the employees and dependence on the IT department for malware attacks is confirmed. Furthermore, existing mitigation strategies generally work well enough, but too few people make use of them. Lastly, we have confirmed the standing notion about ransomware, that nearly all victims are unwilling or unable to pay the ransom.

VII. References

[1] L. Kelion, "Cryptolocker ransomware has 'infected about 250,000 PCs'," BBC News techology, 2013. [Online]. Available: http://www.bbc.com/news/technology-25506020. [Accessed 2016].

[2] G. O'Gorman and G. McDonald, "Ransomware: a growing menace," Symantec Corporation, 2012.

[3] B. N. Giri, N. Jyoti and M. AVERT, "The Emergence of Ransomware," AVAR, Auckland, 2006.

[4] J.-L. Richet, "Extortion on the internet: the rise of crypto-ransomware.," Harvard , 2016.

[5] A. Bhardwaj, G. Subrahmanyam, V. Avasthi and H. Sastry, "Ransomware: A rising threat of new age digital extortion.," in *arXiv preprint arXiv:1512.01980*, 2015.

[6] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention.," *Information Systems Security,* vol. 16, no. 4, pp. 195-202, 2007.

[7] A. Gazet, "Comparative analysis of various ransomware virii," *Journal in computer virology,* vol. 6, no. 1, pp. 77-90, 2010.

[8] M. Fossi, G. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, J. Blackbird, M. Low, D. Mazurek, D. McKinney and P. Wood, "Symantec internet security threat report trends for 2010," Symantec, 2011.

[9] B. Foster and Y. Lejins, "Ehealth security Australia: The solution lies with frameworks and standards.," 2013.

[10] J. C. a. E. A. B. Hernandez-Castro, "UK has little to be proud of as survey reveals sorry state of European cybersecurity," University of Kent, 2015. [Online]. Available: https://kar.kent.ac.uk/51071/1/uk-has-little-to-be-proud-of-as-survey-reveals-sorry-state-of-european-cybersecurity-37505. [Accessed 2016].

[11] K.-K. R. Choo and R. G. Smith, "Criminal exploitation of online systems by organised crime groups," *Asian journal of criminology,* vol. 3, no. 1, pp. 37-59, 2008.

[12] K. Gradon, "Crime science and the internet battlefield: Securing the analog world from digital crime.," *Security & Privacy, IEEE,* vol. 11, no. 5, pp. 93-95, 2013.

[13] T. Zhang, H. Antunes and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework.," *Internet of Things Journal, IEEE,* vol. 1, no. 10, pp. 10-21, 2014.