RAMSES: Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware and Ransomware

Holger Nitsch
University of Applied Sciences for Public Service in Bavaria, Germany

Julio Hernandez-Castro
Edward Cartwright
Anna Stepanova
Darren Hurley-Smith
University of Kent, United Kingdom

Abstract
This paper provides a discussion on the objectives, approach and findings of the European Union's Horizon 2020 research and innovation programme under grant agreement No 700326 funded RAMSES project. As the rise of the use of the Internet is followed by the rise of criminal activity on the Internet, new tools are needed for Law Enforcement Agencies to fight the crime and to collect forensic evidence. The use of ransomware and financially orientated malware is growing very fast and criminals are very innovative in creating new ways to harm citizens and companies. Within this project eleven partners from all over Europe are creating the project jointly and find solutions for the different practitioners involved in the project. This project will provide LEAs with new tools and also covers the dark and deep web. Several tools and functionalities are described such as creating a platform that can e.g. analyse malware payment and hidden files, which can be found and analysed via the platform, to create forensic evidence. The platform will have also a dashboard with different functionalities that will help LEAs in their daily work to fight cybercrime. And also the importance of game theoretic models applying to the determination of the probability and efficacy of malware being used for profit is elaborated. This shows the value of the analysis of malware by different means to help LEAs in the decision making process, which malware might be more distributed and "successful" than others.

Keywords: Ransomware, malware, banking trojans, game theory, cybercrime

Introduction

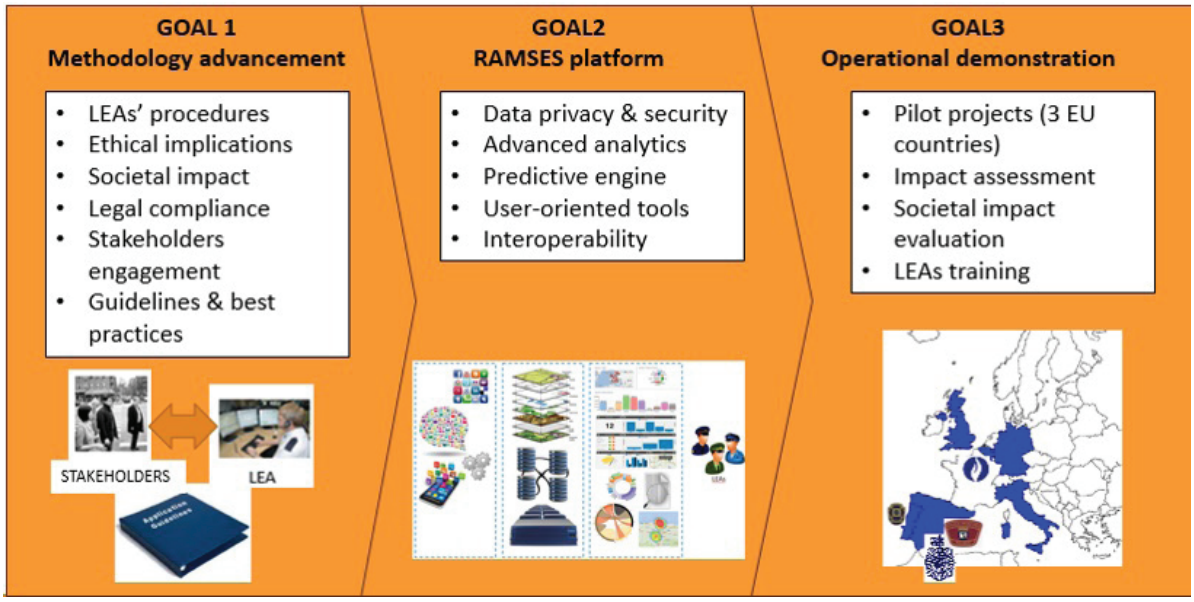
In the recent years the internet has become the key medium of communication and business activities. As business through the internet is growing also criminal activity grows. The exchange of criminal information started in forums like 4chan and has now developed into a wide variety of surface and dark web pages. The 2017 report of NTT Security from Switzerland finds that 77 % of all ransomware concerns four several sectors: administration, retail, business and professional services and health service. Three quarters of there were fish-

ing attacks and 66% of all attacks were coming from the United States. (NTT Services, 2017) The importance of Cybersecurity and information security is constantly rising. The 2016 report of Kaspersky lists a high amount of malware and related incidents. 39% of all internet users were 2016 at least once victims of a cyberattack and 77.26% attacks happened through a malicious URL (Kaspersky, 2018).

The strong rise of internet use has been followed by a stronger use of the internet for criminal activity. For some crimes it is seen by criminals as the perfect tool, because it is easier not to be in direct contact with the victim and to hide their own identity. As the above numbers prove that the numbers are rising, and some see it as a business model to sell their IT knowledge and services to less skilled criminals. So, the investment for criminal activity could be lower than before. According to the Internet Organised Crime Threat Assessment by Europol (iOCTA) (2014) the generated value of the Crime as a Service is around 300 billion dollars.

The Horizon 2020 funded EU project RAMSES to tackle the problem and support Law Enforcement Agencies (LEA) across Europe to resolve problems faster and have court relevant evidence. The RAMSES project (ramses2020.eu) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700326. It aims to design and develop a holistic and intelligent platform for LEAs for facilitate forensic investigations. The system will extract, analyze, link and interpret information extracted from the internet related with financially-motivated malware. That includes the surface web, deep web and the dark web. The RAMSES project focusses on two use cases: ransomware and banking trojans.
Another aim is to demonstrate the impact of the project through several pilots in several stages. At the end, there will be effective guidelines and collaborating methodologies developed. The following diagram shows the main goals of this project:

Diagram 1 – The main goals of RAMES 2017 project



Besides LEAs, other stakeholders like customers, developers and malware victims will be included in the process to get all possible participants throughout Europe involved. This will lead to a better understanding of the problem and the criminal activities and phenomenon. Big Data technologies must be used to extract, store and search for criminal online behaviour to handle the vast amount of structured and unstructured data.

The RAMSES Platform

The platform will include several modules for LEAs to fight malware and to gain court relevant evidence. One of the main problems is to find and extract the relevant data from the internet. The platform will be able to automatically extract this data related to malware from the surface web. This includes also social networks like

Facebook, Twitter and forums. Other challenges are the Deep Web and the Dark net due to the nature of both guaranteeing at least some degree of anonymity and obfuscation of information.The RAMSES platform will also incorporate these elements into the data mining pool and gain relevant information as forensic evidence by doing so.

Further, the platform will be able to analyse malware related payments. This is an important module to judge the importance of the detected malware, as described below in the economic modelling the likeliness of a successful ransomware that might be used more often than others.

Ransomware is often hidden in images, videos and audio files. The platform is able to detect the manipulation of these and perform steganalysis. By doing so LEAs will have the evidence that image, video or audio files were manipulated, and information was hidden, even if the contents of such messages remain unknown. Correlating image manipulation with lines of communication is a potentially powerful way of making items of evidence mutually supporting contributions to prosecution.

In another module malware samples will be extracted and analysed to gain a better understanding of the nature of malware and common trends. This will help also with the prevention of future threats to citizens and to create countermeasures for LEAs and stakeholder against this type of crime.

The results of the different analyses can be visualised in the next module to identify different trends and threats to the citizens or business sectors.

The information feeding the platform comes from a variety of sources. On the one hand, LEAs can input their data to see also their local or nationwide specialities. During the lifetime of the project this will come mainly from the project partners: The University of the Bavarian Police, Belgium Federal Police in Belgium, Policia Judiciara in Portugal and the Spanish National Police. Further information is gained from the common sources of the surface web mentioned above. For the Deep Web and the Dark net sources among others will be TOR, reddit, Pastebin, Zmap and SHODAN, which is a search engine, that is not like Google and others looking for text, but is looking for vulnerable devices (Akhgar; Yates, 2013: 243). Blockchain is another source.

Also, existing knowledge of malware analysis, steganography and multimedia forensics will be fed into the system by the academic partners, specialised on the topic.

There are certain main functionalities. After the processing of a large amount of data the user is able to search for an IP address, a nickname, a certain technology, a name of a Remote Access Trojan (RAT) or any keyword interesting for the investigator. Through to an interactive dashboard the user is able to visualize the different process of malware clustering and forensics. There is also a machine learning process included, so that the more often this functionality is used the more precise the results are according to the needs of the user.

Furthermore, an exploration function will be integrated. Using that will help to explore the relationship between different entities. This can be IP addresses, the name of a malware domains or others. By feeding the platform with information it will show important events concerning malware around the globe. This is useful for LEAs, considering that a successful malware, used in another region, could be easily turn relevant in another region in a very short time. This includes e.g. the de-anonymization of hidden services as well. The alerts are defined by the LEAs.

According to the high amount of malware around the globe, it is of high importance to have a perception of the likeliness of it being used. Therefore, the RAMSES project uses a game theoretical approach to define it.

Ransomware as a business model

Before the RAMSES approach and the findings of Kent University in the next chapter are explained a couple of key elements for the success of certain ransomware. In general ransomware has quite high fixed costs, according to design, programming, development or simply buying it, but very low costs of the use of it, meaning the actual attack. This is in contrary of a "usual" crime or compared to a hijacking, where the costs of the attack / crime are much higher. The developer of a successful ransomware can sell it much more often than an inefficient one. This plays a crucial role for the business model of for-profit ransomware. Other key factors are: if there is a distribution line or if there are certain services included, like offering the victim support in the

way of payment instructions and advice, like hotlines or helpdesks.

Other factors that might influence the success of a certain ransomware are, if there might be a global reach like WannaCry that had a global reach and has hit institutions like the British NHS and companies like Renault and the Deutsch Bahn (Briegleb, 2017). The use against institutions might create a higher ransom than against individuals, even a dual use in which different types of targets receive the same malware with different ransom demands is possible. The sophistication of the ransom demand, be it targeted or random, price discriminatory or fixed, can affect the complexity of the command and control communication required to successfully carry out the attack.

Success is not just related to the quality of the malware used, it is logical that it depends on the situation, emotive and material value of files to individuals or institutions. If the infected computer is part of important infrastructure (such as customer or patient records vital for record keeping and correct allocation of resources) the willingness to pay is much higher.

There is also a relation to the reputation of the ransomware. If the victim does not have the chance to get his data back, this will also be spread around, but if the service was "good" and the data could be restored, the success will be much more likely.

Kent University is providing the RAMSES project with a business model based on game theory to help the project to classify ransomware.

Overview of Game Theory, Economic Modelling and Ransomware

Ransomware is often viewed through the combined lenses of cyber-security and law enforcement, and quite rightly so. However, a purely technical analysis of ransomware doesn't capture the myriad decisions regarding the price of ransom, target selection, and potential negotiating strategy between criminals and victims. Economic modelling is a powerful tool that can identify the costs and revenue streams of ransomware. For the sake of brevity, this discussion focusses on profit-motivated ransomware, disregarding politically motivated or destructive variants.

Research conducted by academics from the University of Kent suggests that current criminals are not very aware of the economics of their activities. Current ransomware demands ransoms that are fixed, and low compared to the optimal price. This optimal price can be found by considering two key attributes of any ransomware victim: their willingness to pay (WTP) and their willingness to accept (WTA). WTP is a simple measure of what a victim states they are willing to pay, whilst WTA is closer to their personal valuation of their files. Horowitz and McConnell (2002) observe that WTA is usually higher than WTP, by up to a factor of 10 in some cases. The true value of files being held to ransom must therefore lie between WTA and WTP. Bateman et al. (2005) argue that the true valuation will be closer to WTA (the higher value).

Hernandez-Castro, Cartwright, and Stepanova (2017) conducted a preliminary survey of 149 adult residents of Canterbury, UK. The results of this survey showed that 9% of respondents expressed a WTA of £990 and WTP of just over £200. 20% of respondents had a WTA of approximately £400, and WTP of £92. Considering that WTA is more reflective of the victim's true valuation of their files, this suggests that charging a ransom which only 9% of victims pay is more profitable than when a larger number of individuals pay. This is because of the assorted reasons victims must refuse payment – they may be unwilling to cooperate with criminals, might place a lower value on their files, are not capable of paying the ransom, or one of any number of reasons that lead to non-payment. Criminals are charging low prices in the hopes of enticing a population who wouldn't pay regardless of how low the ransom is – all the while missing out on the potential profits that a select portion of their victims would yield by paying higher ransoms.

This assumes completely random infection and the perception of victims as individuals, intelligence-led attacks against companies could take this a step further and price-discriminate. Such pricing schemes involve the tailoring of prices to meet the likely WTA of a victim, instead of setting a blanket ransom that attempts to capture the most profitable segment of the paying population. More sophistication is required than is currently common in ransomware attacks, but Remote Access Trojans (RATs) and financial information for publicly traded companies are just two sources criminals may use to determine if they can squeeze a high-value victim for a higher ransom.

Game theory provides a means of playing through hypothetical ransomware attacks. Selten (1988) proposed a simple game of kidnapping. His 6-stage game is applicable to ransomware, if one considers the files encrypted by an attack to be the object being held to ransom. Two actors, the criminal and victim, represent the players of the game. The criminal wishes to extract a sum of money, while the victim wants their files returned, but may not wish to pay. Throughout this game, the criminal is best served by releasing the files if their demand is met or a viable counter-offer is offered. In any one instance of this game, it may appear that the criminal could delete files even after being paid, but one must remember that this game is being played on a massively parallel scale. One must also assume that some victims may communicate. Destruction of files after a ransom has been paid will be communicated, diminishing the trust, and therefore willingness to pay, of victims that are aware of the event. As the cost of infecting each victim is low, but the potential income from each is high, it is in the interests of the criminal to play fairly, but firmly.

Lapan and Sadler (1988) expand on this game by accounting for the possibility of defensive measures. In this game, the victim may spend resources on defence. Such defences reduce the probability of an attack succeeding, but may still fail (due to zero-day exploits or insufficient expenditure). However, additional costs are incurred by criminals who may have to increase the sophistication of their infection method to bypass widely proliferated defensive measures. As the successful defence of one would-be-victim's machine harms the potential profit of the attacker, this generates positive externalities for the entire population of potential victims. This means that if the criminal fails to infect enough victims, they will not be able to generate profit. Even if a portion of victims can defend themselves, profit may fall significantly below the optimal, as high-paying victims may be in the portion of targets the criminal cannot reach.

A game theoretic approach to ransomware can highlight such weaknesses in criminal enterprise and suggest more effective strategies for LEAs and potential victims of cybercrime. Communication is key, increasing the portion of individuals who refuse to play the ransom game (by refusing to pay) is highly effective. This is, however, dependent on the perceived worth of files at risk – encouraging backups can reduce the impact of high-value files being held to ransom by ensuring that the victim can restore them instead of submitting to a criminal's demands.

Economic modelling can provide deep insights into the costs, revenue streams, and weaknesses in the public domain that allow ransomware to be such a profitable enterprise. Though this overview cannot hope to encompass the complexities of current and near future ransomware, it can demonstrate than even cursory analysis of current ransomware highlights a myriad of improvements that criminals are guaranteed to incorporate in the future. Our continuing work with the RAMSES project, will explore optimised forms of ransomware, and identify behavioural and technological countermeasures to them prior to their inception by criminals, where possible.

Conclusion

As it can be expected that the threat from ransomware is not declining, but is instead rising, countermeasures are necessary to help citizens and LEAs to protect critical infrastructure and the privacy of citizens. Especially under the most likely assumption, that the Internet of Things (IoT) will continue to become more critical to daily activity for a great many individuals. The attack of WannaCry in 2017 proved that the connection infrastructure and data in the internet can and will be attacked, also in the future and the criminal activities, like in the past, will become more sophisticated and harder to detect and counter. Cyberattacks against critical infrastructure, like traffic systems, water supply or the energy system would have a very high effect on the population. But also homes and privacy are more at risk, because citizens are more and more depending on the data on the internet and some services can just be used online. The more citizens will use Apps to control their homes including the access will lead to the threat that burglary might change and the innovation for automated driving brings also certain other possibilities for criminals to attack these systems with ransomware. The financial sector is moving with high speed towards business on the internet. This forces citizens to use online banking systems, which includes the risk of infiltration of the financial business sector and the theft of data and money. Other EU funded projects, like Cyberroad (2016), have shown and analysed these risks.

The RAMSES approach will help citizens also according to the future risks to be safer in their privacy and the use of the internet. LEAs will have the possibility to retrieve information faster, respond quicker and it will help them to gain forensic evidence, which is court relevant. They will have the possibility also to create a network by signing up and share their experiences and learn from each other as the phenomenon and the criminal activity is not limited to a single region or country. One of the advantages of the project is that LEAs can use the platform and the developed tools for free, if they sign up. By doing so RAMSES will help to strengthen security for this criminal phenomenon and help LEAs to faster react to threats and speed up the process of findings of forensic evidence.

References

- Akhgar, B. & Yates, S. (2013) *Strategic Intelligence Management*. Butterworth-Heinemann.
- Briegleb, V. (2017) WannaCry: Was wir bisher über die Ransomware Attacke wissen.
  Retrieved from: https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html
- Cyberroad Website (2016)
  Retrieved from: https://www.cyberroad-project.eu/
- Europol, (2014). The Internet Organised Crime Threat Assessment (iOCTA).
- Hernandez-Castro, J., Cartwright, E. & Stepanova, A., (2017) *Economic Analysis of Ransomware*. SSRN Electronic Journal. 10.2139/ssrn.2937641
- Kaspersky Lab and Global Research and Analysis Team (2018) Kaspersky Security Bulletin 2016/17.
  Retrieved from: http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_Security_Bulletin_2016_2017.pdf
- Lapan, H. E., & Sandler, T. (1993) Terrorism and signalling. *European Journal of Political Economy*, 9(3), 383-397.
- Lapan, H. E., & Sandler, T. (1988) To bargain or not to bargain: That is the question. *The American Economic Review*, 78(2), 16-21.
- NTT Security (2017) NTT Security stellt Global Threat Intelligence Report (GTIR) 2017 vor.
  Retrieved from https://www.nttsecurity.com/de-ch/uber-uns/News/detail/ntt-security-stellt-global-threat-intelligence-report-gtir-2017-vor-77-prozent-der-ransomware-in-vier-branchen
- Ramses website (2017) Project.
  Retrieved from https://ramses2020.eu/project/
- Selten, R. (1988) A simple game model of kidnapping. In: *Models of strategic rationality*. 77-93. Springer Netherlands.