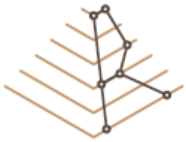

RAMSES

Internet Forensic platform for tracking the money flow of financially-motivated malware

H2020 - 700326

D2.1 Approaches and practices for digital surveillance by Law Enforcement Agencies

Deliverable nature:	Report (R)
Dissemination level: (Confidentiality)	Public (PU)
Contractual delivery date:	28 February 2017
Actual delivery date:	28 February 2017
Version:	1.0
Total number of pages:	52
Keywords:	Cybercrime, Ransomware, Malware, Digital Monitoring, LEAs practices, Forensics, Steganalysis, Multimedia forensic, Payment investigation

Lead Author: Mara Mignone (RiSSC)

With contributions from:

BFP (Federal Police Brussels) - Eli Hoyberghs

BayFHVR – Holger Nitsch, Sarina Ronert

Politecnico of Milan – Stefano Zanero, Andrea Continella

Portugal Cybercrime Unit – Gonçalo Ribeiro, Manuela Cabral, Berta Santos

RiSSC – Valentina Scioneri

Spanish National Police – Alejandro González

Treelogic – Alejandro Prada

UCM – Luis Javier Garcia

UNIKENT – Darren Hurley-Smith, Julio Hernandez-Castro, Edward Cartwright

USAAR - Michael Brengel, Christian Rossow

TRI- Anna Donovan, Rachel Finn

Reviewer: Tatiana Silva (Treelogic)

Abstract

The present Report - D2.1 Approaches and practices for digital surveillance by Law Enforcement Agencies - illustrates the results of the activities implemented within the RAMSES Project WP 2 - Policing Requirements. Scenarios definition, with specific regards to Task 2.1 - Status quo assessment and identification of best practices and guidelines. The Report focuses on the financially motivated malware (specifically on banking Trojans and ransomware) with the intent to contribute at achieving a better understanding of how they work and the sources they derive from; the approaches and practices used for digital monitoring by Law Enforcement Agencies (LEAs); and the role of advanced techniques in the fight against this malicious software. The Study develops a comprehensive and multifaceted analysis, based on an inter-disciplinary approach (e.g. criminological, technological, enforcement, legal, …), and includes contributions from all the partners.

Executive summary

- The Report illustrates the results of the activities implemented within the RAMSES Project WP 2 - Policing Requirements. Scenarios definition, with specific regards to Task 2.1 - Status quo assessment and identification of best practices and guidelines. The Report focuses on the financially motivated malware (specifically on banking Trojans and ransomware)
- The Report is based on an inter-disciplinary approach and on the diverse complementary expertise of the Project partners (e.g. criminological, technological, enforcement…)
- With reference to the *Analysis of the actual scenario (PART 1)*, all the contributions highlight that financially motivated malware are growing at exponential rates, with Trojans being one of the most common and dangerous types of malware, while ransomware are becoming more targeted and sophisticated
- Both banking/financial Trojans and ransomware allow attackers to monetise each infection almost directly and this is the predominant reason for their continuous spread. The optimisation of cybercrime turnover was observed in 2016 and there will not be relevant changes on the short-medium term
- Malware families live in a complex environment with developed kits, web-based administration panels, builders, automated distribution networks, and easy-to-use procedures. Virtually anyone can buy a malware builder from underground marketplaces and create a customised sample
- The emerge of the exploit-as-a-service and of the crime-as-a-service is a serious and sophisticated threat, which is evolving rapidly
- Financially motivated malware is a category of the cybercrime overall phenomenon which is intrinsically dynamic and it has the potential to disrupt the security of both public and private organisations, as well as the functionality and integrity of their IT infrastructures. In some cases (such as the healthcare sector, which is suffering from the increasing number of attacks), also people safety may be at risk
- Regarding financial/banking malware, there are three main emerging factors, which are interdependent: the increasing role of the so called "human factor", the emerging importance of the ransomware based attacks, the mobile dimension, and the geographic location. In particular, the "human factor" includes the use of social engineering techniques combined with malicious software. People are becoming the attackers' preferred entry tactic
- Ransomware are targeting specific victims in some specific sectors, such as healthcare providers, Universities and recently also hotels and other organisations in the hospitality sector
- The approach behind the attacks is generally based on the highest reward to cost ratio or on the desired specific victim
- The hostage-taking models can give clear lessons also about ransomware and cybercrime
- Ransomware can be viewed as a form of kidnapping in which a criminal takes control of a victim's computer in the hope of financial (or other) gain. Any kidnapping incident inevitably gives rise to a conflict between criminal and hostage. Game theory provides a natural tool with which to analyse this conflict and several models of kidnapping have been studied within the literature
- The theoretical model of optimal ransomware strategies can be defined as four key stages: target selection, target infection, negotiation, value extraction. Each of these key stages has a variety of technical, social and economic factors at play
- With reference to the *LEAs experiences and practices (PART 2)*, all the contributions highlight the difficulties and limits which still affect the enforcement activities against cybercrime and in particular against financially motivated malware
- Most cybercrime is committed because of financial motivations, which include individual perpetrators as well as international organised criminal groups. Thereby, perpetrators are reacting flexible and fast to new technological innovations and adjust their behaviour accordingly. This fact makes it

challenging for Law Enforcement Agencies, Security Authorities and economic institutions to counter and prevent financially motivated cyber-attacks

- LEAs current approaches to counter and prevent cybercrime (especially financially driven) can be categorised into three main topics: strategy, forensic expertise and operations:
    - Strategy is mostly linked to continuous efforts to empower human resources, to increase the institutional capacity building to fight back against cybercrime, and to further promote networking and cooperation on a European and international scale
    - Forensic expertise and digital forensic are becoming crucial for the LEAs during all their activities in order to investigate and prosecute cybercrime, but this is a complex area which require high skills and competences
    - Operations mostly relate to cyber intelligence and new intelligence disciplines, with training and education being a fundamental resource for LEAs
- Encryption is resulting to be a serious limit for forensic investigations, along with underreporting, because they both impact on the possibility for LEAs to achieve a better knowledge of the modi operandi and the crime trends.
- The need for knowledge was also strongly reaffirmed by the RAMSES Project end-users
- Another important limit in the fight against financially motivated malware is the feeble cooperation and communication level between LEAs across Europe. Although valuable, the ongoing initiatives are still not sufficient, in some cases there is the need to avoid supplication, while also data protection/privacy laws may become a serious obstacle
- LEAs need to overcome the gap between training and technologies/tools available to them and those used by criminals, which are more advanced and complex
- With reference to the *Monitoring and investigating financially motivated viruses (PART 3)*, all contributions highlight the added value that can have the advanced techniques for police forces
- Among other results, new forensic techniques could contribute to reduce time of investigation and LEAs capacity to handle a greater number of incidents. Accordingly, malware forensic, malware monetisation techniques, steganalysis, multimedia forensic, source camera identification technique and image and video authentication techniques are of relevance
- Open-source intelligence (OSINT) techniques play an important role within the Intelligence community because they can provide general insights and contexts with a relatively low investment. LEAs could improve their capacity to correlate data from their investigations, thus reducing the time and the human resources needed
- Investigating payment information from financially motivated malware could support LEAs in monitoring not only the functioning of the malicious software, but also to track and monitor how it changes over time

Document Information

IST Project Number	700326	**Acronym**	RAMSES
Full Title	Internet Forensic platform for tracking the money flow of financially-motivated malware		
Project URL	http://www.ramses2020.eu		
EU Project Officer	Nada Milisavljevic		

Deliverable	**Number**	D2.1	**Title**	Approaches and practices for digital surveillance by Law Enforcement Agencies
Work Package	**Number**	WP2	**Title**	Policing Requirements, Scenarios Definition

Date of Delivery	**Contractual**	M06	**Actual**	M06
Status	version 1.0		final X	
Nature	prototype □ report X demonstrator □ other □			
Dissemination level	public X restricted □			

Authors (Partner)	RiSSC			
Responsible Author	**Name**	Mara Mignone	**E-mail**	mara.mignone@rissc.it
	Partner	RiSSC	**Phone**	+39 349 45 09 897

Abstract (for dissemination)	The present Report - D2.1 Approaches and practices for digital surveillance by Law Enforcement Agencies - illustrates the results of the activities implemented within the RAMSES Project WP 2 - Policing Requirements. Scenarios definition, with specific regards to Task 2.1 - Status quo assessment and identification of best practices and guidelines. The Report focuses on the financially motivated malware (specifically on banking Trojans and ransomware) with the intent to contribute at achieving a better understanding of how they work and the sources they derive from; the approaches and practices used for digital monitoring by Law Enforcement Agencies (LEAs); and the role of advanced techniques in the fight against this malicious software. The Study develops a comprehensive and multifaceted analysis, based on an inter-disciplinary approach (e.g. criminological, technological, enforcement, legal…), and includes contributions from all the partners
Keywords	Cybercrime, Ransomware, Malware, Digital Monitoring, LEAs practices, Forensics, Steganalysis, Multimedia forensic, Payment investigation

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
15/02/2017	0.1	Mara Mignone	Deliverable structure
19/02/2017	0.2	Mara Mignone	Collection/editing of the contributions from the partners
20/02/2017	0.3	Mara Mignone	Document finalisation
23/02/2017	0.4	Tatiana Silva	Review
28/02/2017	1.0	Mara Mignone	Final version

Table of Contents

List of figures and/or list of tables

Abbreviations

ACH: Automated Clearing House

API: Application programming interface

ATM: Automatic Teller Machine

ATS: Automatic Transfer Systems

CEO: Chief Executive Officer

CERT: Computer Emergency Response Team

CFO: Chief Financial Officer

DDoS: Distributed Denial of Service

DoS: Denial of service

DSCs: Digital Still Cameras

EFT: electronic fund transfers

FBIS: Foreign Broadcast Information Service

HTML: HyperText Markup Language

HTTPS: HyperText Transfer Protocol over Secure Socket Layer

ICT: Information and Communication Technologies

IOC: Indicator of compromise

IoT: Internet of Things

IP: Internet Protocol

LEAs: Law Enforcement Agencies

MitB: Man-in-the-Middle Browser

MitMo: Man in the Mobile

NGO: Non-Governmental Organisation

OSAU: Open Source Analysis Unit

OSINT: Open-Source Intelligence

OCR: Optical Character Recognition

OTPs: One Time Passwords

PCAP: Packet Capture

POS: Point-of-Sale

RaaS: Ransomware-as-a-Service

SSL: Secure Sockets Layer

URL: Uniform Resource Locator

1 Introduction

The present Report illustrates the results of the activities implemented within the RAMSES Project WP 2 - Policing Requirements. Scenarios definition, with specific regards to Task 2.1 - Status quo assessment and identification of best practices and guidelines.

This Deliverable [D2.1] deals with the financially motivated malware (specifically on banking Trojans and ransomware) with the intent to contribute at achieving a better understanding of:

- how they work and the sources they derive from;
- the approaches and practices used for digital monitoring by Law Enforcement Agencies (LEAs);
- the role of advanced techniques in the fight against this Cybercrime.

The Study includes contributions from the partners and is based on an inter-disciplinary approach. In fact, the RAMSES consortium includes valuable complementary expertise (e.g. criminological, legal, technological, enforcement, legal…) and this added value was exploited to develop a comprehensive and multifaceted analysis.

The results highlight the complexity of the phenomenon and how it is of interest at different levels.

The three specific issues addressed are as follows:

- *Analysis of the actual scenario (Part 1 – Status quo assessment)*

  Firstly, this Part gives an overall classification of the financially motivate malware, with particular attention for information stealers (or banking Trojans) and ransomware (author: Politecnico of Milan). A criminological overview of the major threats to individuals and businesses (author: RiSSC) and a prediction of the future evolution of the malware family follow (author: UniKent); Finally, Trilateral gives an overview of the European legal framework governing the identification, detection and prosecution of cybercrimes relevant to financial crime, including malware and ransomware.

- *Analysis of enforcement activities (Part 2 - LEAs experiences and practices)*

  The description of the different approaches, along with the problems and needs, of the enforcement activities performed by Law Enforcement Agencies (LEAs) opens this Part (author: FHVR). The end-users involved in the Project are described as case-studies of reference to detail how the cases of financially motivated malware are managed by the enforcement agencies. Accordingly, the experiences of the Bayerisches Landeskriminalamt (author: FHVR), of the Federal Police Brussels (BFP) – Cybercrime Unit (author: BFP), of the Portugal – Cybercrime Unit (author: MJ) and of the Spanish National Police (author: MI) are included;

- *Analysis of some advanced techniques to foster the fight back against malicious software (PART 3 – Monitoring and investigating financially motivated viruses)*

  This Part focuses initially on the digital forensic models, tools and techniques that could support and enhance the enforcement activities, with a focus on malware forensic, steganalysis and multimedia forensic (author: UCM). The possible contribution from the RAMSES Project is also described. The use of OSINT techniques is also addressed (author: TREELOGIC). Finally, the added value for LEAs of investigating payment information from ransomware and banking Trojans is presented (USAAR).

2 PART 1 – Status quo assessment

This first Part of the Report focuses on the actual scenario of the financially motivated malware with the intent to achieve a better understanding of how and where malware is spread and to get the main characteristics of the threat. The approach is inter-disciplinary and combines the diverse expertise represented in the RAMSES consortium.

The initial classification of the financially motivated malware is then followed by the criminological analysis of the phenomenon based on the victims' perspective. A description of the possible future evolution of this category of malicious software is also included. Finally, the European legal framework against the financially motivated malware is outlined.

What emerge are the intrinsic dynamicity of this segment of the cybercrime phenomenon and the potential to disrupt the security of both public and private organisations, as well as the functionality and integrity of their IT infrastructures. In some cases, such as the healthcare sector, which is suffering from the increasing number of attacks, also people safety may be at risk.

Both banking/financial Trojans and ransomware allow attackers to monetise and this is the predominant reason for their continuous spread; in fact, the optimization of Cybercrime turnover was the main trend observed in 2016 and it can be assumed that there will not be significant changes in the next future.

The fight against this family of malicious software has reached important objectives over the last years. Among the others, there are more coordination, cooperation and synergy between the public/enforcement and the private sectors (in particular, with the vendors); an increased level of maturity in terms of defence; a more effective capacity to mitigate the effects… However, attackers are improving their ability to implement large-scale and multi-layered attacks and extortion-based schemes are on the increase. Like in the physical world, individuals and criminal groups are able to displace their activities, to find out new and more vulnerable targets and to fully concentrate on them in order to maximise the benefits and minimise the risks, thus monetising each single attack.

This stated, the capacity to monitoring and possibly anticipate the new trends is a strategic asset that needs to be further improved.

All these issues are addressed in this first Part.

2.1 Classification of the financially motivated malware[1]

2.1.1 Financially motivated malware: landscape

Malware continues to grow at exponential rates, with Trojans being one of the most common and dangerous types of malware.

Most Trojans are financially-motivated, that is, they are means for the aggressors to monetize each infection almost directly. Their explosive growth is fuelled by the fact that basically anyone, independently from their skill level, can use them, since an active underground economy (sometimes referred to, tongue-in-cheek, as "Crime-as-a-service") provides all the required resources. For example, Goncharov [1] estimated that just the Russian underground economy is a 2.3 billion dollars' market.

Lindorfer et al. [2] measured that Trojans are actively developed and maintained. These and other modern malware families live in a complex environment with development kits, web-based administration panels, builders, automated distribution networks, and easy-to-use customization procedures. The most alarming consequence is that virtually anyone can buy a malware builder from underground marketplaces and create a customized sample.

[1] Contribution from the Politecnico of Milan.

Grier et al. [3] investigated the emergence of the exploit-as-a-service model, showing how attackers pay for exploit kits to infect victims and propagate their own malware through drive-by downloads. Therefore, even with little or no expertise or ability to write a malware, anyone can simply purchase these "kits" and follow detailed guides and video tutorials sold online. The Trojans samples and services available on the underground markets vary, and their price depends on the features (for instance, a new, complete version of a modern banking Trojan can cost about 3,000 US$ [4]).

The two main types of financially-motivated malware deployed nowadays are information stealers and ransomware. Since their characteristics radically differ, we will dedicate a separate section to the analysis of each one.

2.1.2 Information Stealers (or banking Trojans)

A particular type of Trojans, known as Information-stealers or Banking Trojans, allow malware operators to intercept sensitive data such as credentials (e.g., usernames, passwords) and credit card information.

Information-stealing Trojans are a growing, sophisticated threat. The most famous example is ZeuS, from which other descendants were created. This malware is actually a binary generator, which eases the creation of customized variants. For instance, as of February 19, 2017, according to ZeuS Tracker [5], there are 8,151 distinct variants that have yet to be included in the Malware Hash Registry database [6]. This number is very typical and it is also an underestimate, limited to the binaries that are currently tracked. This high number of variants results in a low detection rate overall (40% as of the same date).

Financial Trojans quite often use man-in-the-browser (MitB) techniques to perform attacks. These techniques exploit API (Application programming interface) hooking and, as the name suggests, allow malware to be logically executed inside the web browser and to intercept all data flowing through it. Also, modern banking Trojan families commonly include a module called WebInject [7], which facilitates the manipulation and modification of data transmitted between a web server and the browser. Once the victim is infected, the WebInject module places itself between the browser's rendering engine and the API networking functions used for sending and receiving data. By hooking high-level API communication functions in user-mode code, the Trojans can intercept data more conveniently than traditional keyloggers, as they can intercept data after being decrypted. Therefore, the WebInject module is effective even in case an HTTPS (HyperText Transfer Protocol over Secure Socket Layer) connection is used.

In the following figure (Figure 1), we show an example of a real injection.

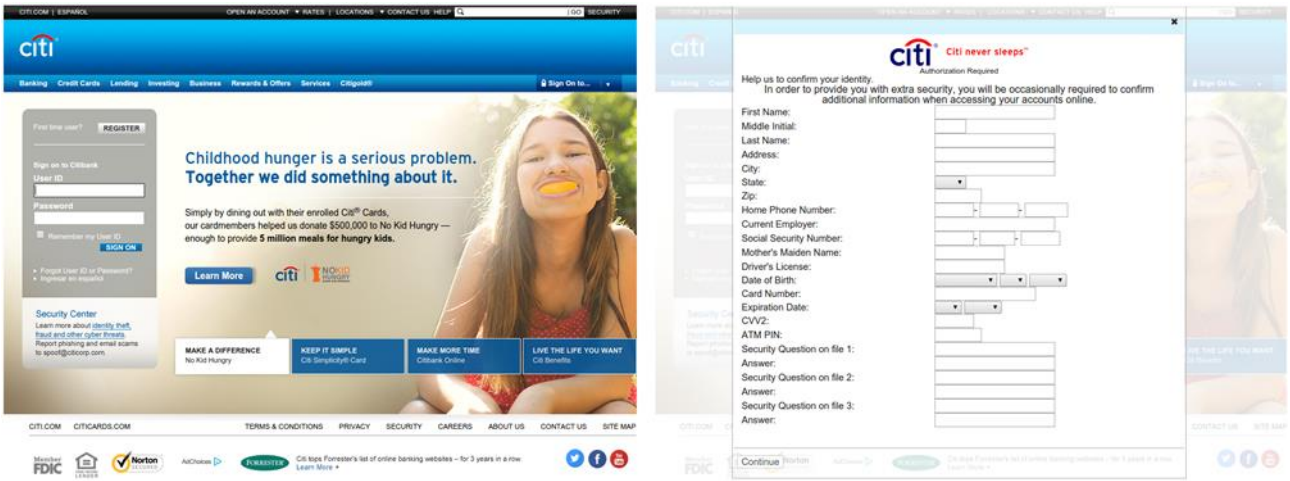

Figure 1 Example of a real injection

Cybercriminals can effectively inject HTML (HyperText Markup Language) code that adds extra fields in forms so as to steal sensitive information. The goal is to make the victim believe that the web page is legitimately asking for a second factor of authentication or other sensitive information (as illustrated above).

In fact, the victim will notice no suspicious signs (e.g., invalid SSL - Secure Sockets Layer certificate or different URL - Uniform Resource Locator) because the page is modified "on the fly" right before being displayed, directly on the local machine.

WebInjects have evolved over time, starting from simple phishing-like key-loggers to offering automatic transfer systems (ATS) and two-factor authentication bypass, together with mobile components and web control panels to manage money and fraudulent transfers [8]. Custom WebInjects can be also purchased for as little as a few tens of US$. Furthermore, cybercriminals offer paid support and customization, or sell advanced configuration files that the end-users can include in their custom builds.

Since banks implemented two-factor authentication using One Time Passwords (OTPs) sent by SMS, in the last years most of the banking Trojans toolkits included a mobile component. This mobile component works in pairs with the PC versions and can access all the information in the user's phone, including SMS, and send it to its C&C server. This attack scheme is also known as "Man in the Mobile" (MitMo). Once the victim's PC is infected, when the victim visits his online banking website the Trojan steals his credentials and inserts a message in the web page that invites the user to download and install a new mobile application to be able to access his account from his mobile phone. This step is usually performed inserting in the web page a QR code that points to the malicious application's download. When the victim downloads and installs the mobile malware, his phone is compromised. The mobile malware can now intercept all the SMS, silently avoid the system notification and remove them after they have been sent to the aggressor. The scheme is illustrated in the following image (Figure 2).

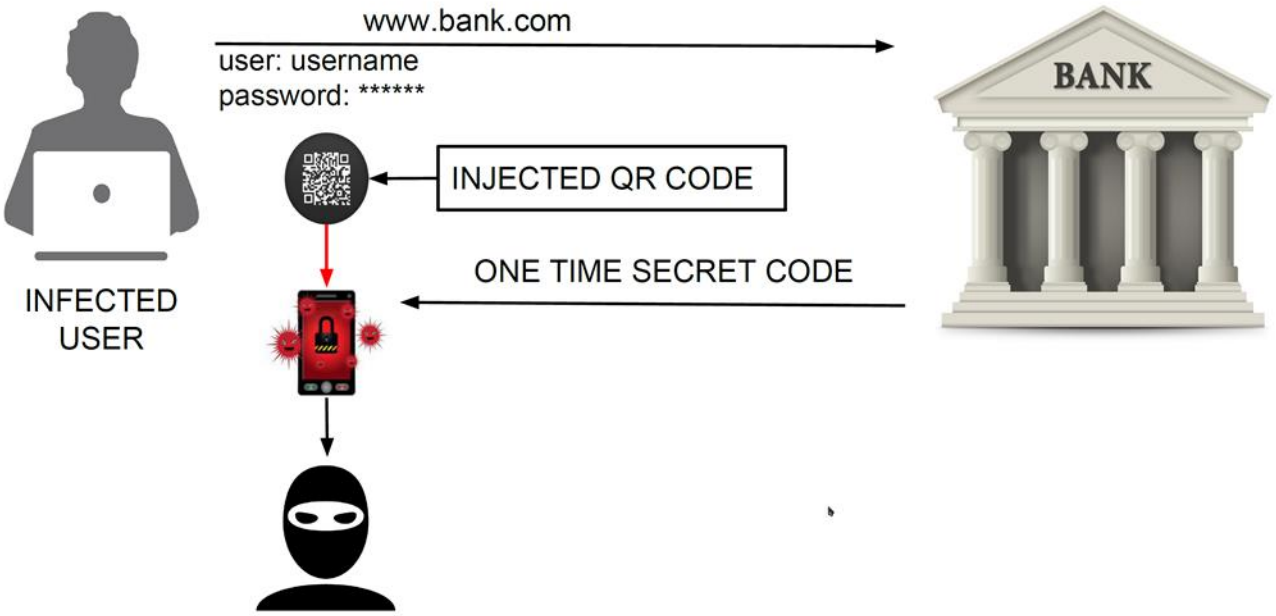

Figure 2 Man in the Mobile: attack scheme

2.1.3 Ransomware

Ransomware is a class of malware that encrypts valuable files found on the victim's machine and asks for a ransom to release the decryption key(s) needed to recover the plaintext files.

Quite interestingly, this class of malware was predicted with uncanny accuracy 20 years ago, in a research paper [9]. The requested ransom payment is typically in the order of a few hundred US dollars [10] (or equivalent in crypto or otherwise untraceable currency) [11]. Clearly, the success of these attacks depends on whether most of the victims agree to pay (e.g., because of the fear of losing their data). Unfortunately, according to a thorough survey dated November 2015 [12], about 50% of ransomware victims surrender to the extortion scheme, resulting in millions of dollars of illicit revenue. In the first three months of 2016, according to a recent analysis [13], more than 209 million US$ in ransomware payments were made in the US alone.

From a technical viewpoint, ransomware families are now quite advanced. While first-generation ransomware was cryptographically weak, the recent families encrypt each file with a unique symmetric key protected by public-key cryptography. Consequently, the chances of a successfully recovery (without paying the ransom) have drastically decreased.

2.1.4 References

[1] Goncharov M., Russian underground 101. Trend Micro Inc. Research Paper, 2012

[2] Lindorfer M., Di Federico A., Milani Comparetti P., Maggi F., Zanero S., Lines of Malicious Code: Insights into the Malicious Software Industry. In Annual Computer Security Applications Conference, 2012.

[3] Grier C., Ballard L., Caballero J., Chachra N., Dietrich C. J., Levchenko K., Mavrommatis P., McCoy D., Nappa A., Pitsillidis A., et al. Manufacturing compromise: the emergence of exploit-as-a-service. In Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012

[4] Doherty S., Krysiuk P., Wueest C., The state of financial Trojans 2013. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_state_of_financial_Trojans_2013.pdf

[5] https://zeustracker.abuse.ch/statistic.php

[6] http://www.team-cymru.org/Services/MHR/

[7] Wueest C., The state of financial Trojans 2014. Symantec, 2014

[8] Boutin J. I., The evolution of webinjects. ESET, https://www.virusbtn.com/pdf/conference/vb2014/VB2014-Boutin.pdf, 2014

[9] Young A., Yung M., Cryptovirology: Extortion-based security threats and countermeasures, 1996 IEEE Symposium on Security and Privacy, pp. 129--140

[10] Savage K., Coogan P., Lau H., The evolution of ransomware. Symantec, 2015

[11] Spagnuolo M., Maggi F., Zanero S., BitIodine: Extracting Intelligence from the Bitcoin Network. 18th International Conference on Financial Cryptography and Data Security, pp. 457-468, Christ Church, Barbados, March 3-7, 2014

[12] Arsene L., Gheorghe A., Ransomware. A Victim's Perspective. Bitdefender, 2016. http://www.bitdefender.com/media/materials/white-papers/en/Bitdefender_Ransomware_A_Victim_Perspective.pdf

[13] Trend Micro. Ransomware Bill Seeks to Curb the Extortion Malware Epidemic. April 2016. http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-bill-curb-the-extortion-malware-epidemic

2.2 The phenomenon and its major threats to individuals and businesses[2]

In this section RiSSC outlines the main characteristics and impact of the financially motivated malware from the victims' perspective. The analysis is mostly based on a sample of relevant cases emerged over the last years. This brief criminological contribution is complementary to the technological ones because together they develop the status quo assessment and they try to better define the potential, the limits and needs of the diverse activities which compose the strategies against Cybercrime developed by the competent actors.

According to the literature and the cases-studies analysed, it emerges clearly that financial malware continues to be a fast-evolving criminal threat for public authorities, private organisations as well as individuals. The need to evolve and adapt the countermeasures is everyday more pervasive at both public and private level. Furthermore, the synergy among investigators and victims is to be considered an essential factor to prevent, limit and mitigate the possible impact and damages of both malware and ransomware.

2.2.1 Financial/banking malware

For the sake of the RAMSES Project, financial/banking malware is intended as a specialized malware, which has been built to scan a computer machine or an entire computer network, to gain information associated with financial transactions. This malware manages to bypass secure information technologies developed specifically to protect the monetary assets of financial institutions and their customers and targets mainly electronic fund transfers (EFT) and Automated Clearing House (ACH) transactions. Doing so, the malware attempts to steal accounting and login information, making it possible to transfer money from the victim's account to the attacker's preferred bank accounts by using EFT (source: Techopedia.com).

According to the literature, the financial malware attacks could be grouped in two main categories:

- General Attacks: the malware used can steal the login information of the user not only for banking sites, but also for any secure socket layer sessions (e.g. social media, web-mails…);
- Targeted Attacks: they exploit the man-in-the-middle browser (MitB) technique, which is a technique in which the configuration file – which is intentionally created by the attacker to target a specific financial organisation - provides a fake Web page to the Internet browser.

The plague of financial Trojans has been targeting the financial sector for over ten years. It could be defined as a sort of "fighting-game" between banks on the one hand, and attackers on the other. Banks have had to enhance their security measures to balance security issues with the new market of online transactions. Attackers adapted to his new approach, thus developing banking Trojans which are becoming more sophisticated and evolved. At present, this malware family allow to commit large scale financial fraud across the globe and to exploit the vulnerabilities of a society that depends heavily on technology.

According to a study conducted by Symantec in 2013 [1], over 600 financial institutions have been targeted by eight of the most popular and sophisticated financial Trojans. 2015 was the culmination of the monetization of vulnerabilities, that was confirmed also in 2016. As a matter of example, 75% out of the top 20 U.S. commercial banks (by revenue) were infected with malware and a number of malware families were discovered within these banks, including Ponyloader, and Vertexnet [2]. Also in Europe, malicious attacks on public and private networks were relentless [3]. European countries were at the bottom of infection rates (Sweden, Norway, Finland, Switzerland and Belgium - infection rates around 20%) [4].

As showed in Figure 3, with reference to both 2015 and 2016, malware continues to be the first of the top threats with no expected change in the ranking. It should be noted that, as regards ransomware, there was a rapid change from position nr. 14 in 2015 to position nr. 8 in 2016, and this situation is likely to change in 2017.

[2] Contribution from RiSSC-Research Centre on Security and Crime.

Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	↑	1. Malware	↑	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Denial of service	↑	↑
5. Denial of service	↑	5. Botnets	↑	↓
6. Physical damage/theft/loss	→	6. Phishing	→	↑
7. Insider threat (malicious, accidental)	↑	7. Spam	↓	↑
8. Phishing	→	8. Ransomware	→	↑
9. Spam	↓	9. Insider threat (malicious, accidental)	→	↓
10. Exploit kits	↑	10. Physical manipulation/damage/ theft/loss	↑	↓
11. Data breaches	→	11. Exploit kits	↑	↓
12. Identity theft	→	12. Data breaches	↑	↓
13. Information leakage	↑	13. Identity theft	↓	↓
14. Ransomware	↑	14. Information leakage	↑	↓
15. Cyber espionage	↑	15. Cyber espionage	↓	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Figure 3 Overview and comparison of the current threat landscape 2016 with the one of 2015 (Source: ENISA [4], p. 7)

In 2017, malware is expected to top cyber-threats for yet another year and surveillance needs to be balanced between the respect of privacy on the one hand, and security related issues on the other. In the middle, there is the need to protect conspicuous financial interests.

There are some key trends that should be highlighted and considered as interdependent among them:

- The increasing role of the human factor;
- The emerging importance of ransomware and information-stealing attacks;
- The mobile dimension;
- The importance of the geographic location.

The emerging issue that could reshape the banking malware criminal phenomenon on the short term is the so-called "human factor", as explained also by ProofPoint [5].
It could be defined as the use of social engineering techniques to trick people into doing things that once depended on malicious code. Accordingly, people – often unintentionally – provide those actions and/or

information that facilitate the Trojans' mission. This could happen in both targeted and large scale attacks. Many diverse campaigns addressed to a plurality of individuals and mostly groups are implemented to convince people for example to disable or bypass security measures, to click on links or open documents, to download files (which are corrupted with malicious software), but also to communicate sensitive information such as accounts, usernames and passwords…

According to ProofPoint, the key elements to be considered as lessons-learned, according to the analysis of the cases occurred in 2015, are as follows:

1. *People are replacing automated exploits as attackers' preferred entry tactic* (Nearly 99.7% of documents used in attachment-based campaigns relied on social engineering and macros, while 98% of URLs in malicious messages link to hosted malware, either as an executable or an executable inside an archive. To work, these files must be opened by the user);
2. *Dridex banking Trojan campaigns were the dominant technique for making people central to the infection chain* (Employees' inboxes were the primary way banking Trojans entered an organization. Mimicking familiar processes - like invoices and statements - to trick a user into clicking on the messages in their email was among the most used modi operandi);
3. *Attackers timed email and social media campaigns to align with the times that people are most engaged* (Attackers optimized campaign delivery times to match the times when people usually click. Email messages are delivered at the start of the business day (9-10 a.m.) in the target regions);
4. *People willingly downloaded more than 2 billion mobile apps that steal their personal data* (Attackers used social media threats and mobile apps, not just email, to trick users into infecting their own systems. Malicious mobile apps should not be seen as corner cases, because they are concrete world threats. In other words, attackers are shifting their efforts to directly attack applications [6]);
5. *URLs linking to credential-phishing pages were almost three times more common than links to pages hosting malware* (The clear majority of URLs used in email-based attacks linked to credential-phishing pages, rather than to sites hosting malware. These pages are designed to induce people to provide their logins and other personal information);
6. *Accounts used to share files and images – such as Google Drive, Adobe, and Dropbox – are the most effective lures for credential theft* (These brand-based lures are effective because these services are familiar, and the user is used to clicking to sign in to view shared content. In these cases, people trust the brand/sender and they believe to be in a secure framework, so their perception/feeling of insecurity is very low);
7. *Phishing is 10 times more common than malware in social media posts* (Fraudulent customer-service account phishing uses social engineering to trick users to divulge logins and personal information);
8. *Dangerous mobile apps from rogue marketplaces affect two in five enterprises* (These marketplaces allow to bypass multiple security warnings in the process and the probability to download an app that is malicious is very high);
9. *Low-volume campaigns of highly targeted phishing emails focused on one or two people within an organization to transfer funds directly to attackers* (Organizations of every size across all business sectors resulted to be highly targeted by phishing messages to people with direct access to wire transfers. These scams are also labelled as "CEO phishing" because the e-mails seem to have CEO, CFO, or another executive as sender. Usually, they don't include links or attachments, but urgent instructions to the recipient to transfer funds to a designated account).

The research activity conducted by ProofPoint highlights the new changing nature of the fraudulent attacks against organisations. However, this should not be considered a recent issue, because the social engineering techniques have been – and still are - largely used in small and large fraud (e.g. Ponzi scheme). The involvement of new technologies in the criminal modi operandi (online social engineering) and their combination with financial/banking malware is likely to increase the complexity and sophistication of the attacks against financial and banking organisations.

In fact, the persons unknowingly involved in the criminal scheme are often deceived, because in many cases they believe they are executing an order, they are talking to/communicating with people having the right to

know the sensitive data they are asked to share. They don't perceive the risk because in many cases they are not aware that financial/banking malware are supposed to need their support to work.

Another element which is resulting to play a significant role in the criminal modi operandi is the geographic location. In fact, the high-volume campaigns implemented during 2015 were much more targeted by region than by organization or individual user, with attackers concentrating on a single country at a time (Figure 4).

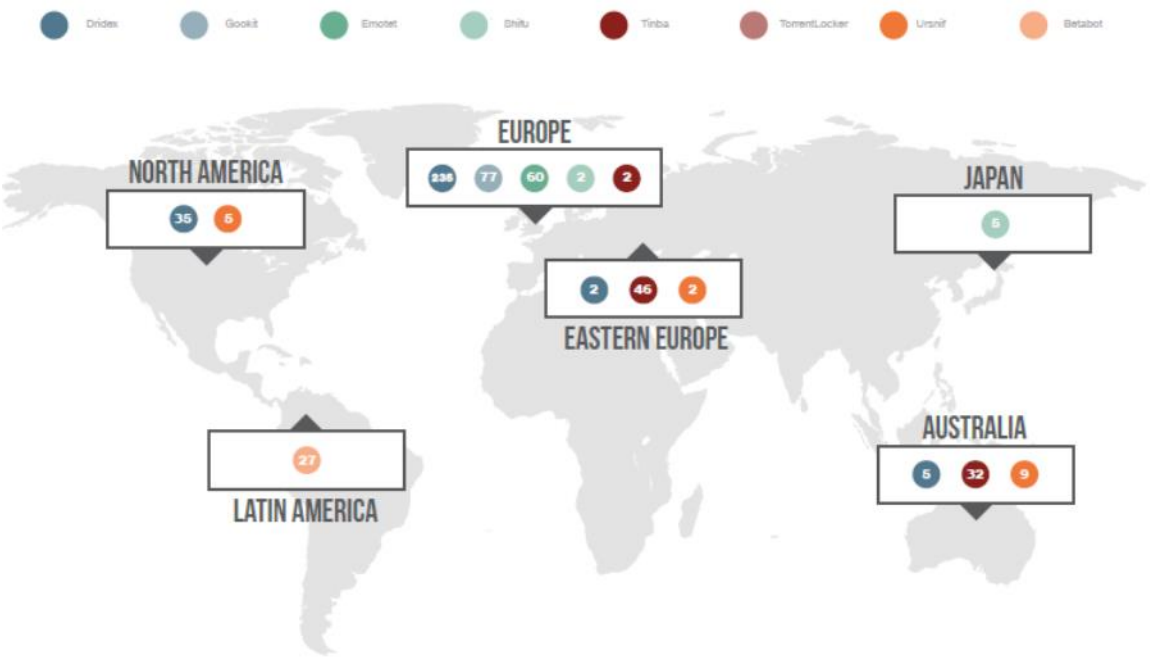

Figure 4 Number of campaigns per malware payload by geographic region, 2015 (Source: ProofPoint, [5], p. 9)

Finally, it is necessary to consider that mobile devices increasingly operate less as simple phones and always more as mobile computers and this is impacting on the nature and complexity of malware attacking mobile devices. The methods used to infect mobile devices are beginning to be more sophisticated and somehow, they mirror those of already known desktop malware.

2.2.2 Ransomware

For the sake of the RAMSES Project, ransomware is intended as a type of malware program that infects, locks or takes control of a system and demands ransom to undo it. Ransomware attacks and infects a computer with the intention of extorting money from its owner. It is typically installed in a system through a malicious e-mail attachment, an infected software download and/or visiting a malicious website or link. When the system is infected with ransomware, it is locked down, the user's files are encrypted, or the user is restricted from accessing the computer's key features.
More in detail, locker ransomware is designed to lock a victim's screen, while crypto-ransomware is developed to encrypt the victim's files.

The ransomware will send pop-up windows asking the user to pay a specific ransom to reclaim or reactivate the computer. Moreover, some ransomware-based applications also impersonate or disguise themselves as police or a government agency, claiming that the user's system is locked down for security reasons, and that a fine or fee is required to reactivate it (source: Techopedia.com).

From the criminological standpoint, ransomware can be depicted as the technological, digital and virtual version of kidnapping, extortion and racketeering. However, the hostage is usually thousand miles away from the abductor. This is a global criminal phenomenon whit no geographical and physical barriers.

Possible examples of the most recurrent modi operandi are numerous and the sectors victimised are heterogeneous, although some are more vulnerable than others.

Recently, in January 2017, hackers took over a four-stars hotel in Austria.
Criminals disabled the electronic key system until a ransom fee was paid, so all guests were locked out their rooms [7]. The ransom was about $1,800 in digital bitcoin currency. Faced with a full house of guests and an inoperable guestroom lock system, the general manager acquiesced and paid the ransom [8].

This event is peculiar, because ransomware attacks are somehow new for the hotel industry, as well as for its guests, while system breaches are more common. In fact, since 2010, more than a dozen breaches at hotel chains or individual properties have been reported [9]. In 2015, most cyber-hacking attacks (74%) have targeted in particular point-of-sale systems, which are particularly vulnerable since many of them are sold or serviced by third-party providers. Denial of service (DoS) attacks were also frequent (21%) [10].

Accordingly, the Austrian case indicates that a concrete threat is emerging for the hospitality sector. The most important vulnerability seems to be represented by the key cards that hotels have embraced as they can be quickly reprogrammed because they are exploited by criminals to infiltrate and disrupt the internal computer system [11].

The ability to choose new targets and displace the activities and efforts needed to commit a crime is considered as one of the key elements of the so called rational choice [12], which is based on the criminals' capacity to maximise risks and benefits. This approach is well suited to most Cybercrime events.

The healthcare sector is representative under this respect, as confirmed by numerous cases. In fact, healthcare providers often depredated by ransomware because, as for the financial and banking sector, they are highly dependent on access to their business-critical information, and they are often weak in terms of protection measures.

In February 2017, the Hollywood Presbyterian Medical Centre in Los Angeles lost access to its computer systems after hackers installed a virus that encrypted their files. The hospital was asked to pay $17,000 worth of bitcoins (average 40 bitcoins) and it decided to finally relent [13].

Considering only the United States, others followed in rapid succession: Los Angeles County Department of Health, Chino Valley Medical Centre and its sister site Desert Valley Medical Centre, Methodist Hospital in Kentucky and MedStar Health in the nation's capital.
In 2016, the Kansas Heart Hospital, in Wichita, was attacked and decided to pay the initial ransom. However, after the payment some of the data appeared to be still locked, and it received a second request for money.

The case-studies collected for the purpose of the present study showed that Universities are among the victims forced to pay out in recent months after being hit by ransomware, too.

Bournemouth University has been hit 21 times in 2015 [14].
According to SentinelOne, 63% of British universities - out of a sample of 58 - have suffered from ransomware events in 2016 [15]. Of the 71 universities contacted, thirteen refused to answer because their response could damage their commercial interests. While only Oxford and Kings College London admitted to not having any antivirus (AV) software, the majority of 'protected' universities suffered ransomware attacks despite investing in AV solutions. No universities confessed to paying a ransom. However, the value of ransoms demanded to decrypt the data ranged between £77 and £2299 (5 bitcoins). Only Brunel university had ever contacted the police in relation to a ransomware attack, most universities preferring instead to deal with the situation internally [16].

Considering the ransomware phenomenon from a more general standpoint, the number of cases has rapidly and incessantly increased in the last two years.
According to a survey conducted by Osterman Research[3] [17], 39 percent of the participants had been impacted by a ransomware attack during the previous 12 months. Across the various industries surveyed, ransomware

[3] The survey was undertaken in the United States, Canada, Germany and the United Kingdom on ransomware and related issues. It was conducted during June 2016 with 165 organizations in the United States, and 125 each in the other nations

attacks resulted to be more common in the healthcare industry and in financial services-related industries, including banking and insurance. Among the nations surveyed, ransomware attacks were most common in the United Kingdom (impacting 54 percent of organizations) and least common in Germany (impacting 18 percent).

The vulnerability of the healthcare sector, where the ransomware threat is growing [18], needs to be analysed with specific attention because it allows to understand important details of the attackers' approach and modi operandi.

In the United States, the Hacking Hospital [19], a two-year study (from 2014 to 2016) by Independent Security Evaluators of 12 healthcare facilities, two healthcare data facilities, two healthcare technology platforms and two medical devices, concluded that security in the healthcare sector is an issue and patient health, patient records and hospital's assets are all at risk (….).

From the hackers' point of view, healthcare providers are the perfect target. They deliver critical care and rely on up-to-date information from patient records, they need prompt and quick access to important data (e.g. drug histories, surgery directives…) and they need to avoid the risk to have patient care delayed or even halted because this can result in deaths (and lawsuits). These are the main reasons why they are more likely to pay a ransom [20]. (Furthermore, in most cases they are somehow obliged to pay because healthcare organizations are generally not prepared, their investments in security and prevention are still minimal[4].

These characteristics of the healthcare providers can be used to explain the two approaches that hackers can adopt when selecting their target and decide the type of attack. In fact, there might be:

1. Untargeted attacks: the hospital to be victimised is chosen based on highest reward to cost ratio;
2. Targeted attacks: the hospital to be victimised is chosen based on desired victims.

Whether an attack is targeted or not depends on the adversary's motivation. Untargeted attacks do not discriminate between assets, while targeted attacks are directed towards specific assets.

The short-medium term scenario is not promising. According to experts, ransomware is now reaching a new level of maturity and this is further proved by the fact that the majority of malware included in phishing emails and exploit kits is currently ransomware [21]. Furthermore, the ransomware-as-a-service (RaaS) model is increasing, so that the need for technological knowledge to use these tools is not mandatory anymore.

2.2.3 References

[1] Symantec (Piotr Krysiuk, Stephen Doherty), The World of Financial Trojans, 2013

[2] SecurityScorecard, 2016 Financial Industry Cybersecurity Report, 2016

[3] EUROPOL, IOCTA 2016 – Internet Organised Crime Threat Assessment, 2016

[4] ENISA, Threat Landscape Report 2016, 2017

[5] ProofPoint, The Human Factor 2016, 2017

[6] HPE Security Research, Cyber Risk Report 2016, 2016

[7] http://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers

[8] http://www.hotelnewsnow.com/Articles/116190/Ransomware-attack-places-hotel-industry-in-new-danger

for a total of 540 surveys completed. The samples were mostly composed by organisations belonging to Financial services/banking/insurance (20%), Manufacturing (12%), Government (9%), Healthcare (9%), Engineering/construction (7%), High-tech (6%), Transportation (6%), Retail/eCommerce (6%) and Education (5%).

[4] According to the study Addressing Healthcare Cybersecurity Strategically developed by HIMSS Analytics and Symantec (available at http://healthcare.report/view-resource.aspx?id=472), more than 80 percent spend less than 6 percent of their IT budgets on security, and more than 50 percent say that figure is less than 3 percent, which is alarming given the significantly higher percentages spent on security in other industries such as government (16 percent) and finance (between 12-15 percent).

[9] http://www.hotelnewsnow.com/Articles/50937/Timeline-The-growing-number-of-hotel-data-breaches

[10] Verizon, 2016 Data Breach Investigations Report, 2016. Available at: http://www.verizonenterprise.com

[11] http://hospitalitytechnology.edgl.com/news/Ransomware--One-of-Hospitality-s-Biggest-Threats-in-2017108863

[12] R. V. G. Clarke, Marcus Felson (edited by), Routine Activity and Rational Choice, Transaction Publishers, 1993

[13] https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center

[14] http://www.bbc.com/news/technology-37166545

[15] https://sentinelone.com/blogs/universities-affected-ransomware-attacks/

[16] https://sentinelone.staging.wpengine.com/item-news/two-thirds-british-universities-hit-ransomware-attacks-research-reveals/

[17] Osterman Research, Understanding the Depth of the Global Ransomware Problem. August 2016. Available at: https://www.malwarebytes.com/surveys/ransomware/?aliId=13242065

[18] http://www.healthcareitnews.com/node/525131

[19] https://www.securityevaluators.com/hospitalhack/. Independent Security Evaluators - ISE, Securing Hospitals. A Research Study and Blueprint, February 2016. Available at: www.securityevaluators.com.

[20] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[21] https://blog.barkly.com/ransomware-statistics-2016

[22] EUROPOL, IOCTA 2015 – Internet Organised Crime Threat Assessment, 2015

[23] NCA Strategic Cyber Industry Group, Cyber Crime Assessment 2016, 2016

[24] RADWARE, Global Application & Network Security Report 2016-17, 2017

[25] MalwareBytes Labs, State of Malware Report, 2017.

2.3 Predicting future evolution of the financially motivated malware[5]

In this section, UNIKENT provides an overview of the state-of-the-art about predicting the future evolution of financially motivated malware. This discussion is literature driven, and represents a review of academic, technical and observational findings.

Two key topics are discussed: predictive modelling considering economic factors and hostage situations, and the role of cryptocurrency and digital marketplaces in sustaining viable ransomware strategies.

2.3.1 Predictive Modelling considering Economics and Hostage-taking

A review of the economic modelling of hijacking and hostage taking has been carried out. Two seminal models – "A simple game model of kidnapping", by R. Selten [1] and "To bargain or not to bargain" by H. Lapan and T. Sandler [2] - have been identified and reviewed. While these models were designed to study hostage taking in conflict situations there are clear lessons that can be drawn with regard to ransomware and cybercrime. For instance, the bargaining power of the criminal is higher if the criminal can credibly commit to returning 'stolen' files and if there is a threat of irrational aggression. In other words, it is in the criminal's interest to build a reputation of being 'nice' to those who pay the ransom and 'nasty' to those who do not. It may be in a policy maker's interest to try and disrupt such a reputation. A paper surveying the literature is nearing completion.

Ransomware can be viewed as a form of kidnapping in which a criminal takes control of a victim's computer in the hope of financial (or other) gain. Any kidnapping incident inevitably gives rise to a conflict between criminal and hostage. Game theory provides a natural tool with which to analyse this conflict and several models of kidnapping have been studied within the literature.

We have identified two seminal contributions to the literature: The first, due to Selten (1988) [1], focuses on the optimal ransom that criminals should charge. The second, due to Lapan and Sadler (1988) [2], focuses on whether potential victims should take action to deter kidnap.

Note that most of the game-theoretic literature on kidnapping has been applied to study terrorist hostage taking in conflict zones. No study, of which we are aware, has explicitly connected ransomware with the game theoretic study of kidnapping. There are, however, clear lessons that can be drawn from the literature on kidnapping with regard to cyber-security. For instance, it gives insight into the willingness of ransomware victims to pay to recover files and the willingness of people to avoid attack through anti-virus protection.

Selten (1988) studies a six-stage game within which the criminal chooses a ransom demand D and the victim can make a counter-offer C. Generically, the game has a unique sub-game perfect Nash equilibrium with an optimal ransom demand of:

$$D^* = \left(\frac{a}{1+a}\right)\left(\frac{W}{1-q}\right),$$

where q is the probability the criminal is caught, W is the value the victim puts on his files being released and a is the probability of irrational aggression from the criminal.

Note that irrational aggression can be interpreted, in this case, as a criminal destroying files because the counter-offer from the victim is too low.

If there is no chance of irrational aggression, meaning a=0, then the optimal ransom demand is 0 and so it is not in the criminal's interest to infect the computer. The intuition behind this result is that, without the threat of irrational aggression, the criminal will accept any positive offer from the victim (because something is better than nothing) and so a high ransom demand is simply non-credible. The threat of irrational aggression is,

[5] Contribution from the University of Kent.

therefore, key to the criminal's bargaining power. The more likely is irrational aggression (or the victim's perception of it) then the higher is the optimal ransom demand.

It may seem counter-intuitive that the criminal benefits from the likelihood he will do something `irrational' but this is a common finding in game theoretic models of bargaining. Essentially, it is in the criminal's interest to `tie his hands' so that he cannot accept a low counter-offer and irrational aggression achieves this end. A specific example would be a criminal who simply does not allow any counter-offers. This would equate to a high a and would mean (if the probability of being caught is low) that the criminal will obtain a ransom near to the victim's willingness to pay to recover her files.

The nature of the ransomed material is a factor that expands this equation. Files are a key target as PCs are a ubiquitous element of home and work life, with financially valuable data on them in most cases. However, J Valdez (2016) [3] identifies a new member of the Locky ransomware family, Odin, which targets IoT (Internet of Things) devices. The ability to brick (or lock), IoT devices gives a new dimension of control and collateral to a ransomware strategy. Being able to hold household functionality, lighting and smart capabilities to ransom lends a sinister edge to what may feel like a distanced ransom experience under file-only conditions.

Ronen et al (2016) [4] explore the issue of extended capability attacks against IoT, a class of attacks into which ransomware falls. The issue of enhanced control over the victims' surroundings is discussed briefly, but the existence of such vulnerabilities is not only confirmed, but described as 'widespread'. Norman et al (2017) [5] advocate a review of IoT security standards and practices in their book, citing the potential for ransomware attacks against IoT devices. Current security standards for IoT products are insufficient to protect many devices, and although firewalls and gateway security measures may prevent them becoming an infection vector for adjacent devices (such as PCs), the IoT devices themselves may be of sufficient value to justify a ransom (or increase its value in a multi-device attack). The bottom-line, when considering models of financially-motivated and hostage-driven ransomware strategies, is that additional perception of control equals more leverage and a likely higher asking price. The cost to the victim may also be higher, reducing their negotiation strength.

Lapan and Sandler (1988) study a four-stage game in which a potential victim can spend money to shield herself from attack. This could, for instance, be equated with anti-virus protection. Generically, if θ is weakly concave, there exists a unique sub-game perfect Nash equilibrium in which the victim will deter attack if and only if:

$$\theta^{-1}\left(\frac{C}{F+C}\right) < (1-\theta(0))W$$

Where θ(E) is the probability an attack would fail given expenditure E on deterrence, C is the ransom and F is the cost to the criminal of launching an attack.

The crucial thing here is the cost of deterring the attack. If that cost is not too high (where high is determined by the previous equation) the victim spends enough to deter the attack. Deterrence works by making it unlikely that the criminal's attempt will succeed. If the cost of deterrence is too high, then the victim accepts the chance of her files being infected and pays the ransom if necessary. What determines whether the cost of deterrence is high or low? This depends on the cost F of a failed attack. If F is small, then deterrence can only work by being highly effective. If F is large, then deterrence is easier.

In a ransomware context, however, the value of F will likely be very small given the low marginal costs of a criminal, say, sending out malware to an email address. Indeed, failed attacks are clearly the norm in common uses of ransomware. A small F means that deterrence has to be highly effective at stopping attack if it is to deter criminals. This puts the focus on θ and the potential effectiveness of anti-virus and anti-malware software. To be effective the software has to be essentially perfect at stopping any attempt to infect the computer.

Various extensions to the two basic games mentioned above have been considered in the literature (e.g. Brandt, George and Sandler 2015) [6]. Particularly important is to allow for imperfect information on W, the willingness of the victim to pay to recover her files. Another issue is the importance of criminal reputation. For instance, it can easily be shown that it is in the criminal's interest to always return access to the victim's

files if a ransom demand was met. In short, the criminal has nothing to gain from taking the money and running because it will only lower the willingness of future victims to pay a ransom.

Table 1 provides a sample of data from four widespread ransomware strains. The demonstrates that there is a variable rate of negotiation between different groups. That is to say, the domain of ransom negotiation is not static, nor is the criminal all powerful, though assertion of dominance through threats of irrational activity remains a key part of their strategy.

Table 1 Sample of data from four widespread ransomware strains

FAMILY	STARTING DEMAND	LOWEST DEMAND	%DISCOUNT
CERBER	530	530	0%
CRYPTOMIX	1900	635	67%
JIGSAW	150	125	17%
SHADE	400	280	30%
			AVERAGE: 29%

These and other relevant works in the literature also point out to the necessity of price discrimination by criminals. It is not in their best interest to request the same ransom regardless of the data present in the computer attacked, as it is common today. Economic models predict that those criminals capable of offering price discrimination features in their malware or ready to engage in some sort of bargaining with their victims will outperform the ones using the fixed-ransom approach and will soon dominate the criminal market. So, we predict that, by trial and error, cyber criminals will in the near future discover the benefits of this approach and will move towards it. In fact, some early evidence seems to confirm this trend is already happening.

2.3.2 The Importance of Cryptocurrencies

A vital element of any financially motivated cybercrime is liquidation, or extraction of financial value from the criminal activity. Cryptocurrencies have become a cornerstone of digital crime, with many newer currencies offering features such as:

- Privacy;
- Claims of anonymity;
- Claims of being untraceable.

These three key points are also addressed in part by services known as tumblers: a term used to describe software that takes batches of cryptocurrency (such as Bitcoin) and randomly reallocates values back to the original contributors, equal to their initial input minus a fee. However, there is a cost associated with the use

of tumblers, and such systems rely on a body of legitimate users, or at least a float of cryptocurrency held by the tumbler service to guarantee that incriminating coins are redistributed in a manner advantageous to the user.

Recent entrants to the cryptocurrency market include a handful of new currencies that claim to provide these three desirable traits as core features. Some examples include:

- XDN;
- Zcash;
- Monero (now accepted on AlphaBay!).

These three currencies represent some of the cutting-edge contributions to the cryptocurrency domain, with elements that by fortune or design favour dark web dealers and cybercriminals. Developed with privacy in mind, all three of these currencies purport to allow anonymity and mostly importantly untraceable transactions.

XDN is an open currency with community tools provided for ongoing work. Zcash is a closed standard, developed around the concept of zero-knowledge proofs, a particularly interesting attribute with effectively allows transactions to be made between two legitimate users with no actionable knowledge of each other ever being communicated. Monero is not based on bitcoins code in any way. It is a common criticism that many cryptocurrencies that claim improved security are built on a potentially flawed premise, as Bitcoin is not engineered for true anonymity, merely privacy at the blockchain level.

A critical consideration is the markets in which these currencies can be used, as commented on by Soska et al [7] at USENIX 2015. Their paper focusses on the longitudinal evolution of the online anonymous marketplace ecosystem, with particular focus on Alphabay. The conversion of cryptocurrencies to fiat currencies is not a simple matter: there is an upper limit on the amount of transactions per day, hard capped by the amount of a given cryptocurrency is available in a given market. This influences the development of predictive models by providing a cost to liquidation once a threshold of activity is reached. This suggests that the optimal currency choice will be situational and fluid, and that prediction must be based on economic and security factors.

Bitcoin has proven popular because it is fungible, it is easily converted into a fiat currency value. However, it is traceable, and this may imply a coming change in how criminals interact with cryptocurrencies. In an increasingly competitive environment, ransomware must compete technologically (infection rate and exploitation of vulnerabilities) and fiscally (extraction of cash value without being caught/denied payment). Currencies that offer increased anonymity and protection from potential tracking by LEAs will be attractive, even more so now that currencies such as Monero are accepted by AlphaBay. If large, criminally-focused enterprises such as AlphaBay back currencies by allow it into their marketplace, this will stimulate use and strategies involving more effective means of avoiding financial paper trails during the critical liquidation process.

Identification of the market activity and capacity of such alternative currencies will give LEAs an idea of how attractive each currency is as an alternative to bitcoin, and their likelihood of being involved in major ransomware crimes. Newer currencies have a smaller pool of currency, and some have a low market footprint by design, limited to hundreds of thousands of dollars of maximum potential currency in circulation (compared to the $15.3 million valuation of Bitcoin [10/02/2017]).

In the predictive economic model, this knowledge will inform the post-ransom phase: how will the criminal extract real cash value form their activity? This is a more economic view on the criminal activity, as by this point the social and economic factors that lead to payment of the ransom merge into the efforts to extract cash value without being caught. This is a critical final phase for our theoretical model, and a contribution that we hope will inform the analysis of liquidation/value extraction behaviours of criminals at the critical post-ransom phase.

2.3.3 Conclusions

The purpose of the previously discussed modelling activities is to devise a theoretical model of optimal ransomware strategies. This can be defined as four key stages (actual labels are placeholders – this is merely to communicate a preliminary idea of our work and further discussion with LEAs for expert input is required):

- Target selection;
- Target infection;
- Negotiation;
- Value extraction.

Each of these key stages has a variety of technical, social and economic factors at play. Selection of a target is achieved by a variety of means, autonomous or human, and the impact of the selection methodology on the subsequent stages must be analysed. Infection is a technical element, in which the attacker must adopt a strategy that bypasses training and security that would prevent the deployment of ransomware. This can be mitigated by appropriate target selection, but a minimum technical element remains, in the form of ransomware type, attacker familiarity with the technology, and experience in launching successful attacks. Both stages require collaboration with LEAs to build a foundation of precedent on which to base our model. Specifically, knowledge of how target selection informs infection vectors (and subsequent phases) must be derived from this work to build an accurate predictive model.

Negotiation is the most socially involved phase, involving communication with the victim that convinces them that paying is the best option. Accounts of ransomware attacks from victims, and a comprehensive analysis of the 'pay/don't pay' decision making process is a more complex element of the proposed model, but one that can be addressed with the research discussed in sub-section 2.3.1.

Value extraction draws on knowledge of cryptocurrencies and dark web market behaviours to define how the ransomer can extract real cash value. This is the final phase of a successful attack. Prudent points that we will seek to address include: how is cash value extracted, on what timescale and does it intersect with additional criminal activity. Subsection 3.2 provides an overview of our understanding of the state-of-the-art in this area.

By incorporating our findings in these areas into a model backed by concrete theoretical work, a comprehensive and predictive model can be created. This model will allow the initial observations of an attack to be used to determine likely paths of progression from the point of initial knowledge (when the LEA in question finds out about the attack). Additionally, it will allow for LEAs to identify potential progression paths from previously unencountered strategies, by plotting the likeliest paths to success form a ransomer's perspective. The creation of such a model will require ongoing and in-depth cooperation with LEAs, and firm adherence to the publication and media guidelines outlined by RAMSES, due to the sensitive nature of the statistical data that we will require.

2.3.4 References

[1] Selten, R. (1988). A simple game model of kidnapping. In Models of strategic rationality (pp. 77-93). Springer Netherlands

[2] Lapan, H. E., and Sandler, T. (1988). To bargain or not to bargain: That is the question. The American Economic Review, 78(2), 16-21

[3] Valdez J., "Meet the latest member of the Locky family: Odin." UPDATE 2016 (2016): 10-25

[4] Ronen E., Shamir A., "Extended functionality attacks on IoT devices: The case of smart lights." Security and Privacy (EuroS&P), 2016 IEEE European Symposium on. IEEE, 2016

[5] Norman J., Joseph P., "Security in Application Layer Protocols of IoT: Threats and Attacks." Security Breaches and Threat Prevention in the Internet of Things. IGI Global, 2017. 76-95

[6] Brandt, P. T., George J., Sandler T. (2015). Why concessions should not be made to terrorist kidnappers. Working paper

[7] Soska K., Christin N., "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem." USENIX Security. Vol. 15. 2015

[8] F-Secure (2017). Cyber-Security Report 2017 . https://www.f-secure.com/documents/996508/1030743/cyber-security-report-2017. Last accessed: 17/02.2017 at 16:40

2.4 The European legal framework governing cybercrimes relevant to financial crime

In this section, Trilateral provides an overview of the European legal framework governing the identification, detection and prosecution of cybercrimes relevant to financial crime, including malware and ransomware. It outlines the key elements of the legal framework and describes their relevance for RAMSES.

2.4.1 Introduction

The legal framework governing cyber-crimes such as Trojan malware and ransomware are fragmented, both at the international and national levels. According to Cannataci, et al., [1] this is because such cyber-crimes touch multiple sectors and involve multiple technologies. Specifically, Internet crimes can touch on multiple areas of law, including:

- Telecommunications
- Wiretapping
- Civil law
- Fundamental Rights
- Criminal law
- Cyber-security acts
- Police investigative acts [1, p. 22].

They may also directly impact sectoral-laws related to finance, child protection or commerce. Furthermore, the borderless nature of cyber-crime makes it difficult to identify jurisdiction and enforcement obligations, as well as parallel issues around evidence gathering and forensics (ibid.). For example, the UN estimates that the majority of cybercrimes include a transnational element [5]. Nevertheless, some European instruments exist that specifically focus on the problem of cyber-crime and suggest avenues for cooperation in relation to identification, evidence gathering and prosecution of offenders. Within the European Union, four major initiatives are relevant for tackling cybercrimes such as Trojan malware and ransomware: The Council of Europe Convention on Cybercrime, the Directive on attacks against information systems, the Cybersecurity Strategy and the NIS Directive.

2.4.2 Convention on Cybercrime (2001)

The Council of Europe's Convention on Cybercrime was signed in Budapest in Nov 2001. It was the first legal instrument to specifically address cybercrime. It is an international treaty that seeks to harmonise European and other States laws on cybercrime to respond directly to novel threats in this space [2]. The instrument argued that an effective defence against cybercrime requires international collaboration, given that cybercrime is itself often a cross-border crime. The main aims of the convention are:

> (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime
> (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form
> (3) setting up a fast and effective regime of international co-operation. [3, p. 4].

As such, the Convention outlines powers to enable European Member States to cooperate to detect, investigate and prosecute cybercrimes. In addition, it recommends legal frameworks that national signatories can put into place to outlaw cybercrime. With respect to the work of RAMSES, the recommended lists of crimes should include offenses against: illegal access (Art. 2), illegal interception (Art. 3), data interference (Art. 4), system interference (Art. 5) and misuse of devices (Art. 6) [1, p. 22], which would cover offenses like botnets, ransomware and malware like Trojans.

The offenses that are intended to be harmonised by the Convention cover those which are intended to mimic non-computer based offenses like forgery and fraud. For example, the Convention covers computer-related forgery, which refers to

> acts involving interference with or illegal accesses to a computer system or data with the intent of deceitfully or dishonestly obtaining money, other economic benefit or evading a liability, as well as to acts involving interference with a computer system or data in way that results in the creation of inauthentic computer data. For example, modifying software used by a bank to redirect money transfer processes [1, p. 29].

This offense may be relevant for malware like Trojans as well as ransomware. Similarly, computer related fraud:

> refers to acts involving interference with or illegal accesses to a computer system or data with the intent of deceitfully or dishonestly obtaining money, other economic benefit or evading a liability, as well as to acts involving interference with a computer system or data in way that results in the creation of inauthentic computer data. [1, p. 29-30].

Cannataci et al, uses the example of phishing (i.e., mimicking an authentic email or communication from an institution to defraud customers) to illustrate this offense.

As well as creating these offenses, the Convention also provides foundational support for electronic evidence gathering, jurisdiction and international cooperation in relation to cybercrimes like malware and ransomware. For example, in relation to **electronic evidence**, the Convention recognises that electronic evidence, by its digital, and easily altered nature, can create questions around integrity, authenticity and continuity that can impact the admissibility of evidence [1]. The Convention recommends setting common standards for evidence gathering, including for acquisition, collection, custody and exchange of such electronic evidence [2]. To assist this, the Council of Europe has developed a specific electronic evidence guide for law enforcement and judicial authorities, and a series of training materials and events for first responders, judges and prosecutors to enable them to gain the most from electronic evidence in the prosecution of offenders [5]. In relation to **jurisdiction**, the Convention outlines two key principles:

> Principle of territoriality: National laws are implicated when the offender, victim or computer is located in a particular country.
> Principle of nationality: Individual states may also be obligated to prosecute their citizens if they break cybercrime laws that are illegal in their state as well as the state in which they are residing, if the activity is illegal in both jurisdictions. [1]

These principles govern the two most common circumstances in which national signatories may be obligated to pursue prosecution. However, the Convention also recommends that national signatories work together to decide jurisdiction of prosecution. Finally, chapter three of the Convention covers **international cooperation**, and covers mutual assistance and extradition rules and provides for a network for information sharing between signatories.

2.4.3 Directive on attacks against information systems (2013)

The Directive on attacks against information systems (2013/40EU) [7] was the first EU wide legislation on cybercrimes such as malware and ransomware that created a set of principles that Member States had to consider and a requirement to create specific national laws that conformed to those principles. However, one of the key shortcomings of such Directive is that Member States are free to transpose the instrument into bespoke national laws, and they do not create a harmonised legal framework. With respect to the Directive, the overall purpose was to provide greater harmonisation of the criminal laws of EU Member States and to create "effective, proportionate and dissuasive criminal penalties and to improve and encourage cooperation between competent authorities (Art. 13 and 14)" [1, p. 37]. Thus, the Directive ensures that acts like illegal access to information systems (Art. 3), illegal system interference (Art. 4), illegal data interference (Art. 5), illegal interception (Art. 6) and making available of tools for committing offences (Art. 7), as well as aiding and abetting and the incitement and attempt to commit an offence (Art. 8) are criminalised across Europe. It also creates a mechanism to punish these offences with criminal penalties via criminal courts (Art. 9).

A secondary objective of the Directive was to improve cooperation between law enforcement authorities. Specifically, it creates linkages between police in Member States and specialised European agencies like Eurojust, Europol, the European Cyber Crime Centre, and the European Network and Information Security

Agency (ENISA). It includes recommendations for data and information sharing between Member States' law enforcement authorities via a swift, 24/7 communication channel. It also includes provisions for sharing "relevant data" with European agencies like ENISA to ensure a complete understanding of technological and procedural developments in cybercrime.

However, once these legal frameworks on cybercrime were established, the EC shifted its focus to prevention rather than prosecution, and further legal developments were focused on cybersecurity rather than cybercrime. As such, the following two initiatives are less relevant for RAMSES and are given comparatively less attention.

2.4.4 Cybersecurity Strategy (2013)

Alongside the Directive on attacks against information systems, the EC was also developing a Cybersecurity Strategy to guide cybersecurity policies for Member States and institutions within them. The Strategy implicates stakeholders at all levels of the cybersecurity chain, including individual citizens, private institutions (e.g., industry), public institutions and governments. The Strategy argues that "information sharing and collaboration while preserving (…) specificities between all actors involved is key to a secure cyberspace" [1, p. 43]. Nevertheless, the Strategy ensures continuity between the cybercrime and cybersecurity strategies of the EU by including the reduction of cybercrime within its security strategy. Specifically, it recommends "coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national [Network and Information Security] NIS competent authorities" [7, p. 6]. However, there is little focus on evidence gathering standards or procedures for prosecution. Yet, the Strategy does specifically discuss supporting the work of the Europol's European Cybercrime Centre (EC3), which is the mechanisms that will:

> support investigations, provide high level forensics, facilitate cooperation, create channels for information sharing between the competent authorities in the Member States, the private sector and other stakeholders, and gradually serve as a voice for the law enforcement community. [7, p. 10].

Similarly, the text also calls on Member States to adopt the Convention on Cybercrime and transpose the Directive on attacks against information systems in a timely manner. Finally, the Strategy proposes a Directive on network and information systems security, which was eventually adopted in 2016.

2.4.5 Directive on network and information systems security (NIS Directive) (2016)

While the Directive on attacks against information systems was the first European legislation on cyber*crime*, the Directive on network and information systems security is the first EU-wide legislation on cyber*security*. The primary aim of this directive is to build cybersecurity capabilities and standards among Member States that would apply to operators of essential services and digital service providers [8]. This could include private sector organisations, public organisations and other essential and digital service stakeholders. As such, it implicates the financial industry as well as other financial service providers relevant to RAMSES. In addition, the legislation seeks to enhance cooperation among EU Member States to ensure that cross-border exchanges of information are efficient and effective. Within this, the NIS Directive also mentions the need to "set up coordinated prevention, detection, mitigation and response mechanisms" [1, p. 44], which maintains a reciprocal relationship between cybercrime detection and prosecution and cybersecurity. While the Directive entered into force in August 2016, Member States have 21 months from that date to transpose it into their national laws. In addition, they will have six additional months to identify operators of essential services. This means that the entities to which the eventual national legislation will apply will be identified more than two years after the entry into force of the legislation.

2.4.6 Conclusion

These legal instruments set out the frameworks that make the activities to be investigated within RAMSES illegal in Europe. However, while these instruments are pan-European, they do not create a firm, harmonised leglislative framework within the EU to govern transnational, cross-border cybercrime. First, as of 2013, not all EU Member States have signed up to the Convention, meaning that some Member States may lack the foundational legislation that governs cybercrime. Second, the nature of the legislation as Directives rather than Regulations, means that each European country will have transposed their obligations into bespoke and varied

frameworks and obligations. This creates a need for RAMSES to remain aware of the potential specificity of the national laws as we apply our system in our pilot countries as well as seek to exploit the system as it is developed through the course of the project. Our work in the remainder of this WP as well as WP8 (pilots and evaluation) and WP9 (exploitation) will be informed by this conclusion and further examination of the relevant legal frameworks will be undertaken as part of this work. Nevertheless, this investigation does demonstrate significant efforts to improve cross-border collaboration and networking to improve detection of cybercrimes, evidence gathering standards, jurisdictional decisions and information sharing between LEAs. The RAMSES tool will specifically investigate how we can positively intervene in these spaces to improve practice and information gathering and sharing for European law enforcement authorities working in these spaces.

2.4.7 References:

[1] Cannataci, J. A., G.P. Mifsud Bonnici, M. Tudorica, *Final report on counter-measure including policy and enforcement responses*, E-Crime Deliverable 3.2, 31 March 2015. http://ecrime-project.eu/wp-content/uploads/2015/02/E-CRIME-Deliverable-3-2-FINAL.pdf

[2] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime, draft February 2013, p. 55.

[3] Council of Europe, Convention on Cybercrime, Budapest, 23/11/2001.

[4] Council of Europe, Explanatory report to the Convention of Cybercrime, (ETS No 185), 2001.

[5] Council of Europe, "Trainings on cybercrime and electronic evidence", 2017. http://www.coe.int/en/web/cybercrime/trainings

[6] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218 14.8.2013, p. 8–14.

[7] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [2013] JOIN(2013) 1 final.

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30

3 PART 2 – LEAs experiences and practices

This second Part of the Report focuses on the enforcement environment with the intent to outline the strengths and weaknesses that characterise the capacity to contrast (and possibly prevent) the attacks.

The results hereby presented combines the findings from a desk research and literature analysis activity with the information directly collected from the RAMSES end-users. This approach has allowed to point out how enforcement activities are still hindered by diverse factors (internal and external), which impact on their efficacy and efficiency.

The experiences of the RAMSES end-users are significant to highlight how LEAs are organising themselves to be more specialised and to have the skills needed to improve their capacities to react against financial motivated malware. Furthermore, these experiences point out the importance of cooperation and the difficulties they face in international investigations.

3.1 Digital monitoring by LEAs: current approaches, limits and needs[6]

Cybercrime include all kinds of offences committed against the Internet, data networks or information technologies or committed with the use of those technologies. The offences in the frame of the Internet range from computer fraud to data espionage to access rights fraud. But according to different statistics [1], most cybercrime are committed because of financial motivations, which include individual perpetrators as well as international organized criminal groups. Thereby, perpetrators are reacting flexible and fast to new technological innovations and adjust their behaviour accordingly. This fact makes it challenging for Law Enforcement Agencies, Security Authorities and economic institutions to counter and prevent financially motivated cyber-attacks.

3.1.1 Current approaches

Cybercrime along with computer-related crime have rendered many time-honoured methods of policing both domestically and in cross-border situations ineffective [2]. At both national and international level, there is an increasing demand of synergy, cooperation, and networking opportunities to support LEAs to respond effectively to the fast-evolving threats. In addition, the harmonisation of the legal framework is becoming mandatory. According to some authors [3], the key cybercrime concern for law enforcement is legal in nature rather than simply technical and technological. Indeed, the key challenge for law enforcement is the lack of an effective legal framework for operational activities that guarantees the fundamental rights principles enshrined in EU primary and secondary law.

The debate on what model(s) should be used in cybercrime investigations has seen many contributions from diverse authors [4] who have tried also to developed extended models stating that they were important for standardising terminology, defining requirements, and supporting the development of new techniques and tools for investigators [5].

The current approaches to counter and prevent cybercrimes, especially financially-motivated cyber-attacks can be categorized into three main topics: Strategy, Forensic Expertise and Operations.

Strategy

Law Enforcement Agencies and Security Authorities across Europe are aware of the threats of cyber-attacks and have started to train its personnel in this field and to create special units dealing with cybercrime. This approach requires the enhancement of human resources and the institutional capacity building to combat the increasing amount of cyber-attacks and the rapidly developing modi operandi. In addition, LEAs and Security

[6] Contribution from FHVR-University of Public Administration and Legal Affairs in Bavaria – Department of Policing

Authorities realized the international character of crimes committed in the Internet and expanded their cooperation with other agencies and authorities within their countries but also within Europe. The majority of European countries has created networks to exchange information and expertise, to develop strategies and to support investigations. Next to outreach activities, LEAs and Security Authorities launched several awareness raising activities to inform the public about current threats in the Internet.

Forensic expertise

Cyber-attacks are representing a new challenge for the security apparatus. This also effects the forensic work of Law Enforcement Agencies and required next to comprehensive researches also the implementation of the digital forensic, a branch of forensic sciences encompassing the recovery and investigation of material found in digital devices. This includes several sub-branches, relating to the type of digital devices involved like computer forensics, network forensic, forensic data analysis and mobile device forensics. But in general, digital forensic encompasses the seizure and analysis of digital media and the production of a report into collected evidence [6].

Operations

Next to forensic expertise, the new threat of cybercrimes required the creation or the realignment of LEA operations. To understand and respond to cyber-attacks, it was essential to implement cyber intelligence as new intelligence discipline. This included unique training, education, skill sets and tradecraft that is required to successfully conduct meaningful collection and analysis in the cyber domain. In addition, Law Enforcement Agencies and Security Authorities started to network with relevant partners in order to carry out joint cybercrime actions.

3.1.2 Limits

One major limitation for forensic investigations is the use of encryption, which complicates or even disrupts initial examinations. Furthermore, laws to compel individuals to disclose encryption are still relatively new and controversial [7].

Next to the issue of encryption, the large number of unreported cases is obstacle in combating and preventing financial motivated cyber-attacks. There are different reasons why individuals may not report cyber-attacks to the Law Enforcement Agencies:

- due to improving technical safety devices, cyber-attacks may remain attempts without having success. The victims may not notice the attempted fraud and therefore do not report it;
- victims may not report cyber-attacks, when they did not suffer any financial damage, but just detected i.e. a virus;
- victims, especially NGO's and organisations, may not report financial motivated cyber-attacks, because they don't want to lose their reputation as "secure and reliable partner";
- in the case of extortion, victims may only report the attack, when the decryption fails to appear.

But Law Enforcement Agencies need the knowledge about cyber-attacks in order to develop the necessary assessment and counteractive measures. In addition, security authorities across Europe often lack personnel with expertise and know-how in order to pursue and prevent financial motivated cyber-attacks in an efficient way.

Another major obstacle in combating and preventing financial motivated cyber-attacks is the too low cooperation and communication between Law Enforcement Agencies across Europe. The modi operandi in the field of financial motivated cyber-attacks goes across borders and is undergoing rapid changes. To effectively counteract and prevent ransomware and Trojans, Law Enforcement Agencies across Europe need to exchange discoveries, experiences and investigations. The core issue in exchanging information between different security authorities nationally and internationally are the strict data protection regulations that often

hamper the cooperation and limit the information and data that can be exchanges. The increasing number of cybercrime and especially financial motivated cyber-attacks has shown that criminals are adapting to the modern environment and its inventions. Therefore, it is essential that legislations and regulations are being modified too, in order to face these new threats.

3.1.3 Needs

As offences committed against the Internet, data networks or information technologies or committed with the use of those technologies is a phenomenon of the 21st century, there is still a need for suitable and effective approaches and tools for LEAs and Security Authorities. The major concern is the gap between training and technologies available to LEAs and the advanced technologies used by individuals and groups committing cybercrimes. The window of opportunity for Law Enforcement Agencies and Security Authorities to keep pace with electronic crime offenders is very short, because of the capacity and the rapid changing of technology used by the offenders. This is why there is a need to maximize investments in new or expanded tools, training, onsite assistance and research with regard to cybercrime.

3.1.4 References

[1] Bundeskriminalamt (2015). Cybercrime – Bundeslagebild 2015

[2] Broadhurst R., Developments in the global law enforcement of Cybercrime, in Policing: An International Journal of Police Strategies and Management 29(2): pp. 408-433

[3] Hayes B., Jeandesboz J., Ragazzi F., Simon S., Mitsilegas V., The Law Enforcement Challenges of Cybercrime: Are We Really Playing Catch-Up?, 2015

[4] Lee H. C., Palmbach T. M., Miller M. T., Henry Lee's Crime Scene Handbook. San Diego: Academic Press. Palmer, G. (ed.) (2001). A Road Map for Digital Forensic Research: Report from the First Digital Forensic Workshop, 7–8 August 2001. DFRWS Technical Report DTR-T001-01, 6 November 2001

[5] Séamus Ó Ciardhuáin, An Extended Model of Cybercrime Investigations, in International Journal of Digital Evidence, Summer 2004, Volume 3, Issue 1

[6] Carrier, B (2001). Defining digital forensic examination and analysis tools. Digital Research Workshop II.

[7] Simson L. Garfinkel (August 2010). Digital forensics research: The next 10 years. Digital Investigation. P. 64-73.

3.2 The handling of cases of financially motivated virus by LEAs. The experiences of the RAMSES end-users[7]

The RAMSES end-users are police forces from Belgium, Germany, Spain and Portugal and most of them are specialised units dealing with cybercrime.

During the first phase of the RAMSES Project implementation, they have shared some inputs about their mission, activities, but also problems and needs, as well as expectations. In particular, they provided information about manual searching, automated searching, databases, examination of electronic evidence and cooperation with other LEAs units.

The synthesis of the most interesting results is hereby enclosed:

Manual searching

- it is currently used mostly to deal with Open-source Intelligence (OSINT), to do cross-check activities, to process metadata …;
- the most relevant problems are related to the lack of skills and capacity, as well as human resources;
- expectations seem to be related mostly to the possibility to automatize the processes and to include also the sources and information available IN the Deep Web and the Dark Nets.

Automated searching

- it is currently used mostly to do the crawling of some specific sources (such as markets, forums and social media …);
- the most relevant problems are related to the lack of human resources as well as to the difficulties determined by the storing and the analysis of the data collected;
- expectations seem to be related mostly to the possibility to analyse the sources and information available in the Deep Web and the Dark Nets.

Databases

- LEAs already have some databases used to store for example "hashes, sources, target sectors, information from crawlers, honeypots and malware analysis results";
- the most relevant problems are related to the manual export, which is not so fast and efficient as they might need;
- expectations seem to be related mostly to the possibility to:
    - have front-end functionalities that allow to perform searches and visualise relations;
    - cross-check technical information with criminal records databases and intelligence databases.

Examination of electronic evidence

- it is used to identify the malware especially from the victims' computers or thanks to contributions from several sectors and CERTs;
- the most relevant problems are related to:
    - the lack of skills and capacity, also because computers and smartphones require different approaches and tools, and determine heterogeneous expected results;

[7] Contribution from RiSSC-Research Centre on Security and Crime

  - the difficult to reach promptly and efficiently the victims, and to identify and extract malware samples and vectors from their devices.

- expectations seem to be related mostly to:
  - the availability of identification tools, intended also as tools to automatize the analysis of the victim's computer remotely;
  - perform Malware Triage (how to identify the various types of security incidents by understanding how attacks unfold, and how to effectively respond before they get out of hand);
  - perform cross-checks with IOCs.

Cooperation with other LEAs units

- there are cooperation initiatives with EU and non-EU LEAs, as well with some economic sectors (bank sector). Platforms are already used to share knowledge on investigation techniques and emerging malware threats;
- the most relevant problems are related to the duplication of the initiatives, which have security problems and don't involve all relevant stakeholders. In many situations, there are no follow-up initiatives after the projects' end
- expectations seem to be related mostly to the enhancement in the mechanisms to exchange information based on both technical and non-technical solutions.

3.2.1 University of Public Administration and Legal Affairs in Bavaria – Department of Policing[8]

3.2.1.1 Organisational model

The national security architecture and apparatus of Germany is very complex. Every Federal State (16 overall) has its own authorities with its own legislations. In addition, there are national authorities, responsible for the whole of Germany and connecting the associated federal authorities.

In the first place, the State Criminal Police Offices (in German: Landeskriminalamt) and the Federal Criminal Police Office of Germany (in German: Bundeskriminalamt) are responsible for the prosecution and the combat of cybercrime. Within the Federal Criminal Police Office of Germany, the Unit "SO 4 – Cybercrime" is responsible for investigation procedures, for the coordination of national and international activities and for the analyzation and situation description of actual cybercrime-phenomenon. Within this unit, there are different working areas:

- Zentrale Ansprechstelle Cybercrime (ZAC): Intermediary and advisor for the economy;
- Operative Auswertung Cybercrime: Evaluation of data and exchange of communication with Interpol, Europol and within the German Law Enforcement Agencies;
- Ermittlungsunterstützung/ Internetrecherche: Research.

3.2.1.2 Consolidated practices in investigating cybercrime

Initial Information Gathering and Undercover Online Investigations

In Germany, the gathering of information takes place on many levels:

- Witness statements of victims;
- Evaluation of IT evidences;
- Analyzation of cyber-attacks;
- Information exchange with national and international authorities responsible for Cybercrime;
- Open Source Intelligence;
- Telecommunications Surveillance.

The Criminal Police Offices are using undercover online investigators in order to collect information and to solve crimes. But it is important to draw a dividing line between undercover investigators and agent provocateurs. Next to Undercover Agents, the Federal Criminal Police Office of Germany is allowed to use so-called BKA-Trojans in order to search and monitor information technologies undercover. Those missions are regulated by §20k Legislation of the Bundeskriminaltamt (BKA-Gesetz) and require the prior consent of a judge.

Tracing and Identifying Criminals

German Law Enforcement Agencies and Intelligence Services are using different databases to collect information of perpetrators or to seek information in the case of crimes.

Digital Forensic Analysis of Evidence

[8] Contribution from FHVR-University of Public Administration and Legal Affairs in Bavaria – Department of Policing

Digital investigation activities are performed by both investigators and forensic experts of the Law Enforcement Agencies and the Intelligence Services. The digital forensic analysis has to be conform with the according legislations in order to ensure the admissibility of such evidence before the courts.

Cross-Border Investigative Abilities

Law Enforcement Agencies and Security Authorities in Germany are able to cooperate and communicate with each other and with authorities abroad. But there are obligatory conditions and legislations that regulate the exchange of information. The major limitation may be the privacy guidelines, that prevent LEAs and Security Authorities to share certain information with other authorities in Germany and especially with other countries.

3.2.1.3 Future scenarios: the challenges for LEAs

Offences committed against the Internet, data networks or information technologies or committed with the use of those technologies will be an important topic in the future. The rapid changing environment of cybercrimes will be challenging for Law Enforcement Agencies and it is important to keep pace with this new form of crimes.

3.2.2 Belgian Federal Police – Cybercrime Unit[9]

3.2.2.1 Organisational model

In the Belgian federal police, there are several Computer Crime Units. These units are divided in in a central unit called FCCU and decentralized per region a RCCU. There are 12 RCCU units in our country. The size of the unit depends on the region it resides in. The size difference from 5 to 40 people per unit. All the agents in the units have a technical background in ICT. 80% of the people have a degree in computer science, some of them are specialized in networking, operating systems and telecommunications.

The year of foundation is somewhere around 1995.

3.2.2.2 Consolidated practices in investigating cybercrime

Initial Information Gathering and Undercover Online Investigations

The initial information gathering happens at the local police offices where there are agents that have followed a course in how to deal with computer crimes. They will gather the initial information from the victims. The course in written by and given by experienced people of the RCCU.
The online undercover investigations are new from this year and the will be done by the people of the RCCU's. But the law is brand new and not yet put down in practice. The main problem is to provide a good undercover profile and the knowledge of using the correct words on the chats … In this field, we are looking for partners that have a lot of experience.

Tracing and Identifying Criminals

Belgian Federal Police has a big database where all the criminal facts are collected and where police officers can search in. So, agents can check if someone is already known for some crimes. The problem is that some facts are not put in the correct category.

Digital Forensic Analysis of Evidence

The forensic analysis is done by the RCCU's. They are trained to do this correctly. All the evidence is numbered and put in a database. There are many tools used to do the analysis like Xway's, Internet evidence finder, caine, deft, wireshark, xplico, ufed, xry...

Cross-Border Investigative Abilities

If police agents need to work with colleagues over the border they need to have a court order to do this and the approval of the other country. Then it is possible to make a joint investigation team. This is not often done because of the cost of all of this.

If they need some information from another country, they need to send an official request to the justice department of that country. And that takes a lot of time.

The problem is that the Internet does not have borders but the laws of a single country is bound by its borders. It is just one mouse-click to go over the border by the Internet and do some crimes but the investigators need a lot of paper to just ask some help from a country.

International Co-operation in Cybercrime Investigations. This is the same as cross border investigation

[9] Contribution from BFP

3.2.3 Policia Judiciária Portugal – Cybercrime Unit[10]

3.2.3.1 Organisational model

Polícia Judiciária (PJ) is a criminal investigation police, under the Ministry of Justice, that operates across the entire internal territory with a total staff of almost 2400 officers. The mission of Polícia Judiciária, under the terms of its organic law and the Organisation of Criminal Investigation Act (LOIC), is to assist the judicial and prosecuting authorities in investigations, to develop and foster preventive, detection and investigative actions, falling within their jurisdiction or the actions which the Polícia Judiciária is entrusted with (serious, organized and/or international crime, with the specific competence for the investigation of those crimes with a higher level of complexity) by the competent judicial and prosecuting authorities

Polícia Judiciária is a highly-specialised police, with reserved competence for criminal investigation (concerning cybercrime matters) of computer offences as well as those committed resorting to information technology. Recently created (November 2016) and, by now, fully operational, Polícia Judiciária has, in its organizational chart, the National Cybercrime Unit (UNC3T) with reserved and exclusive competence to handle national cybercrime investigations and cross border investigations, in following main areas of cyber offences:

- Cyber-attacks [High-Tech Crimes];
- Payment fraud [card, PoS, ATM];
- Online child sexual exploitation.

This new PJ's Unit (UNC3T) is composed of about 50 people assigned to four central criminal investigation sections and one additional central digital investigation technical team. The large majority of these 50 officials have background in law but also, and nowadays most common on a new recruitments processes, background in several areas like Engineering and Sciences. All the UNC3T staff receives a mandatory internal basic digital forensics training.

3.2.3.2 Consolidated practices in investigating cybercrime

Initial Information Gathering and Undercover Online Investigations

Most of the information gathering activities are run by OSINT and cyber threat intelligence tools complemented the sources like the victims and suspect devices. The cooperation between law enforcement and some private sectors, especially the Bank sector, is fundamental to obtain efficient information concerning criminal investigation on this particular area. Regarding undercover online investigations, similar techniques, tools and procedures are also applied in a restricted approach. As weak points, we can address the lack of massive approach and currently no-fusion capabilities with our criminal records that are fully deployed.

Tracing and Identifying Criminals

The use of special tactic and OSINT capabilities, regarding malware and based in an international cooperation approach.

PJ is also taking the opportunity to identify and arrest several criminal actors. As weak points, PJ can address the lack of few tactical solutions per team and attribution capabilities during the earlier stages of investigations.

Digital Forensic Analysis of Evidence

[10] Contribution from Policia Judiciária Portugal – Cybercrime Unit

Digital investigations activities are performed by both investigators and forensic experts. The internal digital forensics framework it´s supported by the most common digital forensics solutions (law enforcement oriented based on a national legal framework), namely focused on computers, mobile, malware and network forensics domains. As weak points are reported lack of human resources and out of date solutions (hardware and software).

Cross-Border Investigative Abilities

The only issues are law related. PJ works formally and on daily basis with several Law Enforcement Agencies (EU and around the world) and it is especially synchronized with Europol and Interpol. Regarding malware, strong abilities and capabilities already exist to exchange malware samples and its metadata.

3.2.3.3 Future scenarios: the challenges for LEAs

Based on a current threats and new complex modus operandi, one should expect:

- increased complexity and density of a ransomware malware family targeting new devices and platforms, which shows more than ever the need to be faster and more efficient with cross-border investigations, namely using more actionable threat intelligence and apply cyber-special techniques, tools and procedures. Now, the challenge is the law catch up the crime reality of the XXI century;
- increase and risk spread concerning mobile malware, targeting smartphones but also several IoT devices. As weak points, PJ mentions the lack of control and an unknown number of IoT vendors, no information and no records to retain. This could result in no digital evidence or intelligence;
- increase of the financially motivated DDoS, namely supported by IoT botnets. Even if they are not purely malware related, they could make use of the same attack vector and opportunity.

Concerning all aspects mentioned above:

A unified solution is the key in order to create more actionable cyber threat intelligence, especially at information gathering stages, but also at the malware analysis stages (cross-check and link analysis: technical data vs. criminal records). A law enforcement botnet tracker should also exist and have the capability to extend those features to the darknet layers with support for virtual currencies mapping.

3.2.4 Spanish National Police[11]

3.2.4.1 Organisational model

The Cybercrime Unit (UIT) is the specialised division in the Spanish National Police in charge of investigating cybercrime at a national level. This unit born in 1995, nowadays have about 80 police officers working in different areas, most of them computer engineers. The different areas in the Unit are

- Online child sexual exploitation;
- OSINT and Social Networks;
- Cyber-attacks and malware;
- Online fraud;
- I+D and Forensic Analysis.

3.2.4.2 Consolidated practices in investigating cybercrime

Initial Information Gathering and Undercover Online Investigations

Most investigations start after the formal complaint from the victim. The information provided by the victim is analysed and all the leads contained are considered. In ransomware cases the complaints are usually limited and the information available is not usually enough to start a proper investigation (mainly Tor domains or bitcoin addresses).

In some other cases, when the victim provides the infected devices, more information can be gathered regarding the vectors of infection and domains and information contained in the malware samples.

Also, other way to initiate an investigation is through the discovery of Command and Control Panels or adverts in underground forums.

Tracing and Identifying Criminals

In ransomware cases the main leads are related to the command and control server (IP addresses, domains, e-mails, jabber accounts, etc.) and also the information from the payment, which are usually made on cryptocurrencies.

Banking malware provides also another lead regarding the money mules.

Nevertheless, those investigations and the identification of the authors are really complex as it is the infrastructure and people involved. As an example, a typical case of ramsomware is explained.

Ransomware is first created by a "coder" who offers it up in criminal underground forums and develops it, either for an individual or for a group of criminal affiliates, for a fix sum or money or for a percentage based on the quantity of infected computers. The coder also provides a daily update service to prevent it from being detected by an antivirus or to hinder its analysis through reversing techniques.

The ransomware coder has access to those numbers through the statistics created by infected computers. The users group called "ransomware exploiters" are the ones who buy the code and exploit it, making available the domain and server infrastructure for its propagation and infection.

In terms of infrastructure, it is characterized by anonymity, both regarding the hiring of the domains and servers, as well as C&C server access and the short lifespan of the servers. The exploiters hire the services through the resellers, which offer low prices and bulletproof hosting services. The service payment is done through Paypal or other e-currency.

[11] Contribution from Spanish National Police

Digital Forensic Analysis of Evidence

The analysis of the malware samples is performed usually using an automatic system like Cuckoo or the Europol EMAS, in order to obtain the initial leads for the investigation. More in deep analysis is done manually.

Also, the forensic analysis of the victim's device to discover the malware sample is done manually.

Cross-Border Investigative Abilities

Most of the cross-Border investigation abilities are based on the Budapest Cybercrime Convention.

International Co-operation in Cybercrime Investigations

Most investigation involve infrastructure located in third countries, and coordination is made through the Police Coordination bodies such as Europol and Interpol.

Based on our experience through our investigations, the biggest obstacles are:

- The judicial systems. The international judicial systems have started to adapt to the requirements of cybercrime, but they still have a long way to go in understanding the seriousness of the problem;
- The bureaucracy of the judicial and international cooperation systems is too slow, and becomes an obstacle to an effective investigation;
- Urgency. We need to obtain the information contained in servers, such as IP connections, software installed, and logs registry, as quickly as possible.

The victim’s computer infection is, in many cases, the most unknown aspect of the investigation. Since the victim is not aware at which point his or her computer has been infected, it’s complicated to trace and analyse the sites.

3.2.4.3 Future scenarios: the challenges for LEAs

Ransomware will keep growing and being most available to new criminals without experience making more difficult to discover the real author for each victim. Baking malware may turn to other Internet financial services that may difficult the investigation even more.

4 PART 3 – Monitoring and investigating financially motivated viruses

This final Part of the Report deals with the solutions to monitoring and investigating financially motivated viruses and how they can represent and added value for LEAs. The contributions try to highlight also how the RAMSES platform's functionalities could contribute to further improve the fight back against malware and ransomware.

In particular, malware analysis, steganalysis, multimedia forensic, OSINT techniques and investigating payment information from ransomware and banking Trojans are discussed because there is an increasing interest from LEAs towards them.

4.1 Digital forensic models, tools and techniques: the added value for LEAs activities[12]

Law Enforcement Agencies, in an effort to fight against new digital crime and collect relevant digital evidence, are incorporating computer forensics techniques into their infrastructure in order to stop the fast growth of this type of crime.

The vertiginous change of technology has converted these tasks into a constant race between the criminals and the LEA's. That is why the use of new forensic techniques will permit LEA's to prevent crime and also, catch all the criminals behind.

Recent cases of child pornography and ransomware extortion, both in Portugal and Spain [1-3], as well as in Europe have increased the interest by the LEA's to improve their current forensic techniques to decreased the presence of these cases in their respective countries.

RAMSES Project presents a set of new forensic techniques engagement to help LEA's, mainly to reduce time of investigation and cybercrime incidents. RAMSES Project will add new techniques for three leading areas, which are show in Figure 5.

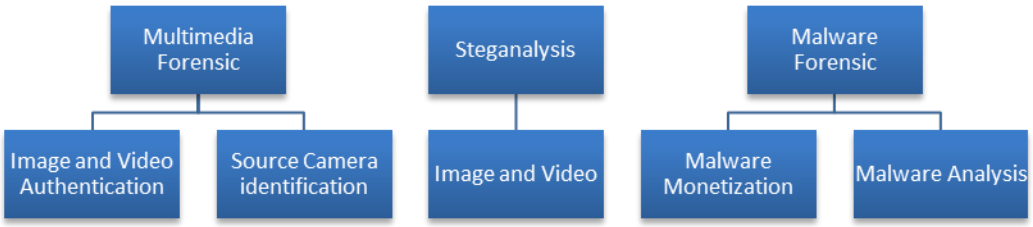

Figure 5 Leading Areas of RAMSES

RAMSES will integrate all these techniques and work along with new technologies like Big Data Analytics which provide a richer cybersecurity context by separating what is normal from what is abnormal.

[12] Contribution from UCM

4.1.1 Malware forensic

The purpose of malware analysis is usually to provide the information you need to respond to a network intrusion [4].

Malware as a whole has been extensively studied but little is known about the specific threats of ransomware and banking Trojans. Technical partners of RAMSES contribute their existing malware analysis environments to the project, in order to assist the dynamic analysis of malware to collect vital information.

In RAMSES, we will propose new unsupervised techniques to cluster ransomware families, which enables us to reveal new attack campaigns on a timely manner. In the other hand, banking Trojans, we are going to explore new introspection techniques to automatically infer attack information from the malware samples.

4.1.1.1 Malware monetization techniques

RAMSES platform will focus on Bitcoin, that is why RAMSES will implement a state-of-the-art deanonymization and transaction graph analysis techniques, connecting and integrating work from several partners and extending it by devising novel methods for aggregating keys into user clusters, annotate them with information crawled from open source intelligence (OSINT) sources, cluster transactions making bitcoin flows more evident and simpler to trace and analyse.

4.1.2 Steganalysis

RAMSES will have a set of tools developed to implement state of the art techniques in steganalysis over images and video. From existing tools, developed by UNIKENT, it will extend to incorporate more techniques and combine them optimally. By first time a steganalysis tool for video will be develop, adding findings made by UCM.

As part of the RAMSES platform, the steganalysis tool will allow detect popular cybercriminal techniques much more reliably than current solutions. In addition to detecting hidden communications and possibly recovering their contents and linking back to the stego software employed, these tools will be of enormous value to detect data exfiltration after a successful data breach. Even thus cybercriminals have recently discovered that by employing steganography to exfiltrate the compromised data, they can easily bypass all security measures put in place to detect and stop this exfiltration vector.

Steganalysis tools will combine the existing multimedia analysis techniques with additional algorithms for assessing the authenticity of multimedia contents, providing important benefits, such as scalability and robustness.

RAMSES will incorporate different technologies into a unique toolbox in order to provide efficient search capabilities and solutions for guaranteeing the integrity and authenticity of digital contents.

4.1.3 Multimedia forensic

The extensive use of smartphone cameras makes enforcing legal restrictions on the capture and sharing of digital photographs very difficult. A consequence of its widespread use, is that digital images can be used as silent witnesses in judicial proceedings (child pornography, industrial espionage, social networks, etc.), and in many cases crucial pieces of evidence in a crime [5]. For these reasons, nowadays, digital image forensic analysis of mobile devices is very important. It is noteworthy that forensics specific images techniques are required for mobile devices, not to be valid in most cases, the techniques used for the Digital Still Cameras (DSCs), because there are significant intrinsic features which differentiate both types of cameras. Also, the quality of the elements that conform them is different, being usually better in the DSCs.

4.1.3.1 Source Camera Identification Techniques

Analogously to ballistic trying to relate a gun with its bullets, digital image forensics tries to identify the link between images and the digital camera which has generated them [6]. RAMSES will have a tool which have novel techniques to identify maker and model of the devices used to generate digital images.

The success of these techniques depends on the assumption that the characteristics are unique to each device. The characteristics used to identify the maker and the models of digital cameras are derived from the differences between image processing techniques and technologies used in camera components [7].

Digital cameras have a powerful source of information which is the embedded metadata in digital images files. These metadata provide relevant information to supplement the main content of a digital document and can also be used as input or aid for other forensic techniques.

RAMSES will have implemented a set of algorithms for source camera identification, that will consider the following aspects: The techniques implemented will allow LEA's to identify multimedia files from any data storage device, where the forensic analyst does not know a priori the camera source which multimedia files are from. Knowing as open sceneries classification. Also, implementation of techniques that allow LEA's to to identify the source on a specific and known beforehand set of cameras. Knowing as closed sceneries classification.

Once that we consider all the possible sceneries, RAMSES will allow LEA's link a digital photo or video to its corresponding origin camera device and used as an evidence in a judicial process.

4.1.3.2 Image and Video Authentication Techniques

In contrast to the prominent role of digital images in our society today, research in the field of image authenticity is still in a very preliminary stage. Attacks on digital image forensic algorithms are aimed at systematically confusing or misleading the procedures for identifying the source of an image or detecting malicious image manipulations. These attacks could have one of the following goals: camouflage malicious post-processing of images or manipulating the image source identification.

With these in mind, RAMSES will have techniques which used algorithms to verify if a multimedia file suffered some local/global edition or manipulation, allowing to LEA's at verify the authenticity of files that could be use in a judicial process.

With the verification algorithm RAMSES will devise a set of anti-anti-forensics measures to detect image/video fingerprint removal or substitution.

4.1.4 References

[1] "El troyano NeverQuest, ¿obra del supuesto hacker detenido en España?." Sputnik Mundo. 01, 2017. consultado el 02, 2017. https://mundo.sputniknews.com/seguridad/201701201066355699-espana-detencion-hackeo-virus/.

[2] "Seis homens detidos por pornografia infantil." Correio da Manha. 02, 2017. consultado el 02, 2017. http://www.cmjornal.pt/portugal/detalhe/seis-homens-detidos-por-pornografia-infantil.

[3] "Dois arguidos em operação de combate à pornografia infantil." Diário de Notícias. 02, 2017. Consultado el 02, 2017. http://www.dn.pt/portugal/interior/buscas-na-regiao-de-lisboa-relacionadas-com-pornografia-infantil-5653021.html.

[4] Sikorski M., Honig A., Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press, 2012.

[5] M. Al-Zarouni: "Mobile Handset Forensic Evidence: a Challenge for Law Enforcement". In Proceedings of the 4th Australian Digital Forensics Conference. School of Computer and Information Science, Edith Cowan University, December 2006.

[6] B. Wang, Y. Guo, X. Kong, and F. Meng: “Source Camera Identification Forensics Based on Wavelet Features”. In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, volume 0, pages 702–705. IEEE Computer Society, September 2009.

[7] T. Van Lanh, K. S. Chong, S. Emmanuel, and M. S. Kankanhalli: “A Survey on Digital Camera Image Forensic Methods”. In Proceedings of the IEEE International Conference on Multimedia and Expo, pages 16–19. IEEE, July 2007.

4.2 The use of OSINT techniques: the added value for LEAs activities[13]

Open-source intelligence (OSINT) [1] refers to a kind of intelligence collected from publicly available sources such as social media, forums, websites, blogs and new sources. The term OSINT means unclassified and available, but it does not imply easy to find, some of this information might be hidden behind networks that protect the identity of their users such as Tor, I2P or Freenet.

Information does not have to be secret to be valuable. OSINT techniques play an important role within the Intelligence community because they can provide general insights and contexts with a relatively low investment. According to the CIA [2], OSINT has always been important in the source analysis tasks, but with the continuing advances in information technology and their impact in the society, the importance of these techniques has shown an impressive growth and they have made possible to address new intelligence questions. One of the main challenges of OSINT is its volume. To separate the valuable from the worthless is not easy and it requires skill, knowledge in the specific field and to take advantage of software tools that help to intelligence analysts to deal with large volumes of data.

The OSINT techniques had also an important role in history. One example is the Foreign Broadcast Information Service (FBIS) [3] created by Roosevelt government in 1941 with the aim to exploit the OSINT content related with the World War II. The classic example of the added value of the OSINT techniques is that this service was able to find as an indicator the price of oranges for confirming that the railroad bridges had been bombed successfully.

However, these techniques do not only belong to the military or law enforcement agencies context. Other sectors such as the business sector have found in the OSINT a good method for acquiring tailor knowledge about their competitors and customers. Craig Fleisher [4] reflects in this report [5] about the experiences of business organizations using OSINT techniques for business/competitive intelligence purposes and the analysis process within the commercial sector.

Law enforcement agencies have been also applying OSINT techniques in order to predict, prevent, investigate and prosecute criminals, including terrorists. In some cases there are specific units within the law enforcement agencies for analysing open sources, like for instance, the Royal Canadian Mounted Police (RCMP) that created his Open Source Analysis Unit (OSAU) [6] [7] by the end of the 80's for gathering criminal intelligence. The process of gathering intelligence from open source follows always 5 steps [8]. The figure below shows the different steps in the OSINT cycle.

Figure 6 The OSINT process [8]

There might be some issues associated with the OSINT process. The main issues are the data volume and the other one is the reliability of the source. The key is a cautious identification of sources as well as a process for

[13] Contribution from Treelogic

filtering the data that is not valuable. The Machine Learning techniques [9] can help to classify the information that are interesting for analysts and to reduce false positives and false negatives.

RAMSES will extract information from the Surface Web, the Deep Web and the Darknet related with malware and ransomware. One of the first goals of the OSINT process in RAMSES is to monitor conversations in common websites of the Surface in order to find people talking about malware, including the sellers offering their services and also people interested in purchase malware or ransomware. Another goal of the OSINT process is to discover what sites in the Darknet are related with the purchase of malware and ransomware and to find all the new ones that have been created.

To avoid the excess of information, the RAMSES platform will have a Machine Learning process for filtering conversations talking about malware and ransomware and to discard the conversations talking about other topics. RAMSES will also analyse the information from posts that are related with malware, the rest, such as the publications related with drug dealing will be dropped.

OSINT techniques will be used in RAMSES with different purposes such as locating new sites on the Internet selling malware, deanonymizing hidden services or discovering more information about the infrastructure of a malware. Besides of these functionalities, RAMSES will also allow to search among large volume of updated data related with malware and to explore the connections between different entities such as emails, IPs, nicknames or domains. This will allow to Law Enforcement Agencies to correlate data from their investigations, helping them to make progress quicker.

4.2.1 References

[1] https://en.wikipedia.org/wiki/Open-source_intelligence

[2] https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

[3] https://en.wikipedia.org/wiki/Foreign_Broadcast_Information_Service

[4] https://en.wikipedia.org/wiki/Craig_Fleisher

[5] http://www.phibetaiota.net/wp-content/uploads/2013/02/2008-Fleisher-on-OSINT-English-and-Spanish.pdf

[6] http://www.academia.edu/7205751/Open_Source_Intelligence_Social_Media_For_Use_In_Investigations_And_Policing

[7] http://www.oss.net/dynamaster/file_archive/040320/b7fad0fa38b940cd0513a3a7ac0ac133/OSS1995-02-17.pdf

[8] http://resources.infosecinstitute.com/the-art-of-searching-for-open-source-intelligence/#gref

[9] https://en.wikipedia.org/wiki/Machine_learning

4.3 Investigating payment information from ransomware and banking Trojans: the added value for LEAs activities[14]

Ransomware and banking Trojans are both subclasses of malware. Therefore, understanding the best practices for malware analysis in general is also important when it comes to the analysis of those two types of malware. When analysing malware, there are two options, namely static and dynamic analysis. Static analysis is done by inspecting the machine code of the malware by looking at it with analysis tools such as disassemblers and hex editors. The analyst is required to have a deep understanding of low-level machine instructions to analyse the binary and extract the information required for LEAs. Besides this required expertise, it should be noted that static analysis also requires manual effort, which makes an automatic and large-scale analysis infeasible. Additionally, malware authors usually deploy techniques to hinder static analysis by obfuscating and encrypting the binary to increase the manual effort to a point where static analysis is rendered impractical. This means that static analysis is not suitable for large-scale automated analysis operations to extract information from ransomware and banking Trojans. Dynamic analysis on the other hand is carried out by executing the binary in a confined environment like a virtual machine for example and observing the behaviour of the binary. In this context, observing means to collect valuable information which can be used to extract important data such as payment information or any information which reveals knowledge about the actors. Such data could include a screenshot of the system, da dump of the memory and PCAP files which include the network activity of the malicious binaries. The memory dump can be analysed with forensic techniques to extract required information.

Ransomware samples share the inherent characteristic that they have a noticeable visual appearance to get the attention of the victim. Additionally, this visual appearance usually includes payment information. This can be used to the advantage of LEAs when it comes to the analysis and extraction of payment information. The samples can be executed in a confined execution environment where a screenshot will be taken after letting the ransomware run for a while. Then a screenshot could be taken of the system. By doing this for many samples, we can gain important information for the LEAs by analysing the screenshots. On the one hand, clustering methodologies can be used to group together ransomware samples with have a similar or an identical visual appearance. This gives important insights on the number and the activity of actors. On the other hand, optical character recognition (OCR) can be used to extract payment information such as Bitcoin wallets. Additionally, this methodology allows to track the payment information over time if the analysis is carried out continuously over a large timespan.

Banking Trojans are different from ransomware in the sense that they usually operate silently. This means that a screenshot of an infected system is unlikely to contain any valuable information for the LEAs. Additionally, banking Trojans usually use a system called "Automatic Transfer Systems" (ATS) [1] to manipulate transactions only at the point in time when the actual transaction is happening. This means that it is not possible to extract payment information from a banking Trojan without doing a transaction. However, the web injects, i.e. the parts which are responsible for manipulating the banking websites in the browser of the victim, can be automatically extract with dynamic and static analysis techniques. This information reveals which banks are attacked by the banking Trojan and can be used to gain knowledge about the actors. Additionally, it can be monitored if the banking Trojans carry out other malicious and financially motivated behaviours such as scanning for a bitcoin wallet for example. Anti-fraud systems on the banking side which try to detect manipulated transactions can also be used as a feedback loop to the LEAs.

[1] http://blog.trendmicro.com/trendlabs-security-intelligence/evolved-banking-fraud-malware-automatic-transfer-systems/

[14] Contribution from USAAR

5 Conclusions

If one adopts the LEAs' point of view, the most important results presented in the present Report could be grouped under three main concepts:

- **financially motivate malware are (and will continue to be) a major concern for European Law Enforcement Agencies**. In the short term, LEAs will face relevant challenges because the criminal modi operandi and the technologies used for the attacks are evolving rapidly. In particular, the spectrum of the possible authors is likely to widen due to the emerge of the exploit-as-a-service and of the crime-as-a-service options. Both are serious and sophisticated threats which are evolving rapidly and are likely to determine a considerable growth in the number of attacks.
- to address these challenges in the best way possible, **LEAs need support. They need to strengthen their knowledge of the phenomenon, their abilities and skills, and to have the right tools** to cope with the evolution of the cyber-attacks. Although they are revising the organisational model (e.g. they are forming specialised units with high-skilled agents), they seem to be still in a sort of "inferior position" compared to cybercriminals. Their efficacy and efficiency is hindered by the lack of adequate procedures, as well as human and technological resources. For example, in many cases, the activities performed during investigations and/or cyber-monitoring are time consuming because they are still managed manually or due to absence of technological solutions to foster the analysis of the data/information retrieved. The need for a closer cooperation with other LEAs, as well as for rapid and agile information exchange procedures, is becoming pervasive. The ongoing initiatives are positive but they need to be improved because they often are discontinuous, insufficient, limited to a restricted number of people or period of time…
- to foster investigations and to support intelligence activities, **LEAs need advanced forensic techniques and analytical skills.** They should be able to handle the single case and to monitor the overall phenomenon and its main trends.

The experiences collected within and outside the RAMSES Project end-users confirm that EU LEAs are strongly motivated, convinced of their role and the importance of the activities they develop. However, it is possible to grasp a sense of frustration and powerlessness as if they had blunt weapons against cyber-attacks and financially motivated malware.