

A mixed-methods approach to provide a better understanding of target selection regarding financial malware attacks within the Single Euro Payments Area

Daan van Moorsel

Faculty of Technology, Policy & Management, Delft University of Technology, Jaffalaan 5, 2628BX, Delft, The Netherlands

Email address: D.P.vanMoorsel@student.tudelft.nl

Student number: 4043197

30 June 2016

Abstract: Financial malware, is one of the attack vectors that is used for the purpose of online financial service fraud. Currently, there is a limited understanding, regarding *why certain financial institutions within the Single Euro Payments Area (SEPA), are more likely to be targeted by financial malware than others*. Experts are consulted, to gather their expectations about target selection including its evolution. These expectations are placed within the theoretical perspective of the Routine Activity Theory (RAT). RAT proposes that crime occurs, when a *suitable target* is in the presence of a *motivated offender* and is without a *capable guardian*. In addition, quantitative analyses are executed, to compare the expectations of experts with the instructions of Zeus botnets, send between 2009 and 2013q1. The experts expect, that in the first years of financial malware, financial institutions were targeted based on their size. Which – for instance - can be expressed by the number of clients. However, according to the experts, the capability of the financial institution's guardian, is assumed to have more influence on target selection over the years. Which can be determined, by the increasing awareness and the adopted sophisticated defense measures. Furthermore, the experts assume, that the context of a country influences target selection. From the quantitative analyses can be concluded, that financial institutions with more clients are targeted more intensively. This is the case regarding targeted domains, from ten selected SEPA countries. Furthermore, this relation also exists for targeted domains, from three of those countries individually. Thereby, the country seems to influences target selection, however further research to the influence of the characteristics of the country is required. Moreover, on a yearly basis, only within 2009 financial institutions with more clients encountered a higher attack intensity. Besides, in the first nine weeks of 2013, financial institutions with fewer clients are targeted more. However, it is unknown, whether this evolution is caused by the improved guardian of the big financial institutions. It should be noticed, that the size of a financial institutions can be expressed by more factors, besides the number of clients.

Keywords: *Cyber risks, experts, financial institutions, financial malware, financial malware schemes, online financial services, Routine Activity Theory, qualitative analysis, quantitative analysis, SEPA, target selection, Zeus.*

1. Introduction

Financial institutions become increasingly dependent on information technology and telecommunications, to deliver services to consumers and business every day. For instance, banks introduced many platforms through which transactions could be done without much effort, in order to enhance their client base (Vrancianu and Popa, 2010). Although, financial institutions are continuously dealing with securing those modern payment services, online financial service fraud is a serious problem. The yearly global losses due to financial fraud are in the billions of Euros (Anderson et al., 2013; Bresiger, 2013; Raghavan et al., 2014). Furthermore, the bank's costs of cyber risks, increase by the security measures in place. According to (Raghavan et al., 2014), the yearly costs to combat cybercrimes, are twice the losses.

Moore et al. (2010) mention, that information security fails regularly, due to non-technical reasons. Furthermore, cyber risks within the financial sector arise not only within the technical context, but also within the socio-technical context (van den Berg et al., 2014). Van den Berg et al. (2014) argue, that nowadays cyber risk management should both have the technical focus on information security, as the focus on the risks that have emerged in the socio-technical context. These concepts can be applied to the environment of online financial services, including its cyber security needs. Hereby, the platform together with the internet and the servers deliver the technology that makes it possible to execute the financial services online (Claessens, 2002; Vrancianu and Popa, 2010). The technical cyber security measures that the financial institutions could adopt to reduce cyber risks, include; sophisticated authentication methods, encrypted layers, firewalls, transactions monitoring, etc.

Besides, the financial services are not only executed on the technical level, but they take place in a broader socio-technical context. This context is constituted, by the organizations and human actors that are involved in the financial services (van den Berg et al., 2014). Hereby, the focus is on the interaction between human actors and the technology, which causes socio-technical cyber risks. Cyber security measures that can be adopted by financial institutions and authorities, to mitigate risks in this socio-technical context, are; researching the socio-technical risks, executing awareness programs about the socio-technical risks and adopting finger print and eye print authentication. Furthermore, the technical systems to enable financial services, including the socio-technical context should be organized. Therefore, both contexts are governed in complex ways, by many different human actors and organizations (Van den Berg et al., 2014). Examples of the actors and organizations involved in the governance of financial transaction are: Financial institutions, Central banks, payment organizations, lobby organizations, policy makers, etc.

Both the measures in the technical context and the socio-technical context including their governance, need to develop constantly, to deal with the evolving sophisticated cybercrimes within the financial sector. The current focus of cyber risk management, within the European financial sector, is on the cyber resilience of financial market infrastructures (CPMI, 2014; DNB, 2015). However, less knowledge exists regarding the level of cyber risks, encountered by different financial market infrastructures and financial institutions. To further develop cyber risk management, it is essential to have a clear understanding of the threat landscape. Therefore, this research intends to address the following **gap**: *The limited understanding of why certain financial institutions are more likely to be selected as target by cybercriminals.*

This article intends to contribute to the understanding of target selection within the Single Euro Payments Area (SEPA). Thereby, empirical insights are provided, into both technical and socio-technical characteristics of financial institutions, which make them more likely to be selected as target by financial malware schemes. Currently, less empirical knowledge exists regarding these characteristics. These insights should support both the financial institutions with their cyber risk management and the authorities with developing cyber security criteria. For example, when according to this research, financial institutions with sophisticated counter measures, like transaction monitoring and anomaly detection, are targeted less intensively. Financial authorities could make those measures accessible for each financial institution, in order to reduce the societal losses of cybercrime.

In this article, **target selection** is defined as: *Attack choices by the financial malware schemes regarding, which financial institution to attack, at which point of time and for how many weeks.* Thereby, the **financial malware scheme** is the synergy of actors and organizations that enables financial malware attacks. Insights regarding target selection in SEPA, are gathered by answering the following research questions:

1. What are the threats of online financial services, what is financial malware, and in what way can target selection be expressed (section 2)?
2. How did target selection evolve, according to the experts from the field (section 4)?
3. What choices regarding target selection are actually made, according to the Zeus dataset (section 5)?
4. Is target selection including its evolution, as assumed by the experts, consistent with the patterns shown by the Zeus dataset (section 6)?

Within section 3, the methods are elaborated, which are used to answer the research questions two, three and four. After answering the research questions, section 7 provides the conclusion. Finally, section 8 contains a discussion of the findings and the limitations of the outcomes.

2. The Background

2.1 Online financial services and their threats

Since the year 1990, financial institutions started providing services online (Claessens, 2002). Moreover, from around 1995 financial institutions adopted many platforms through which financial services become available online (Vrancianu and Popa, 2010). For example, financial transactions are executed via platforms (e.g. mobile application and (mobile) websites), which are connected through the internet with the financial institutions' servers. As a consequence, financial institutions encounter online fraud on a regular basis (Böhme and Moore, 2009; Lagazio, 2014).

Many financial institutions have realized that phishing and financial malware, together with the authentication schemes currently in use, lead to online man-in-the-middle attacks (MitM); which are the most common today (Vrancianu et al., 2010). Moreover, financial malware is on the top of the list of cyber threats (Marinos, 2014; Europol, 2015). The current authentication schemes are of risk, because their robustness is based on the end-client's decisions, which making them entirely vulnerable to social engineering attacks (Vrancianu et al., 2010).

In addition, the cybercriminals typically use MitM, to take over a session once the client has authenticated herself to the bank (Anderson et al., 2008). The man in the middle pretends to be the bank, thereby receives the client's authentication. With that authentication he logs in on the client's bank account (Anderson et al., 2008; Utakrit, 2009). This article focusses on man-in-the-browser (MitB) attacks which have similarities with the described MitM attacks. Specifically, on Zeus financial malware and its variants that enable MitB attacks.

2.2 Zeus malware and MitB attacks

Zeus is a Trojan horse that is able to act as a man-in-the-browser (MitB). A MitB Trojan operates in the internet browser that is displayed on a clients' screen and controls the ingoing and outgoing content of information at the system level (Utakrit, 2009). Zeus malware has been primarily known for its use in financial fraud (Adham et al., 2013). According to Europol (2015), the Zeus malware family can be categorized as a data stealer. Furthermore, it has a high threat level (Europol, 2015). In this subsection is described, how Zeus financial malware works and how it developed itself into more sophisticated versions. The Zeus dataset used for this research, exists of Zeus and the three variants ICE X, Citadel and Power Zeus.

First, the Zeus malware is installed on a client's computer via a phishing mail or a drive-by download, which is an unintended download (Macdonald, 2011; Microsoft, 2014). Subsequently, the configuration files are downloaded by the infected PC. According to Macdonald (2011), the configuration file contains information that the bot will need when it is first executed. Furthermore, Macdonald (2011) mentions that *"the configuration file is downloaded at timed intervals by the bot, and can be used to change the behavior of the botnet."*

Subsequently, the by Zeus infected computer turned into a bot of the botnet and starts communicate with the command and control (C&C) server. The bots are able to gather online financial service information, of all the users of the infected computer. In addition, the criminals are able to insert themselves into an online banking session. The C&C server sends commands to the bot, to execute unnoticed transactions during online banking (Lawrence, 2015).

Furthermore, the stolen money is transferred to a money mule. The key role of money mules, is to convert *"reversible traceable transactions into irreversible untraceable ones"* (Florêncio and Herley, 2010). Transferring the money from the clients to the mules, can be done in multiple ways; 1) all the authentication codes may be available for the mule, and thereby the mule is fully authorized to execute transactions, 2) transactions can be added by the criminals on the background of the transaction lists, which are hidden by web injects, and 3) the transfer of money to the mules is sometimes executed by the clients themselves. Although, unknown amounts are noticed within the transaction list, the client insert the second authentication code.

Finally, the mule transfers the money to the criminal organization, after taking a small percentage. Or the mule withdrawals the money, takes a percentage of it and brings the rest of it to the cyber criminals. Thereby, the criminals remain anonymous.

2.3 Target selection

There is an understanding that not all actors within the financial malware scheme are criminals. Actually, target selection is determined by the criminals within the scheme (Bauer et al., 2008; BITS, 2011). However, the financial malware scheme is a complex ecosystem of multiple actors and

organizations (NVB, 2009; BITS, 2011; Europol, 2014; Lucas, 2015). Therefore, in this article target selection by the financial malware schemes are analyzed.

According to Galien (2014), cybercrime towards financial institutions is particularly aimed at first world countries. Furthermore, the Federal Financial Institutions Examination Council (2014) supports this line of argumentation, by stating that the level of cyber risk exposure varies significantly across financial institutions. However, currently less knowledge exists about target selection by financial malware schemes specifically.

Tajalizadehkhoo et al. (2013), provide some intelligence of target selection with their research; A) the word “bank” within the domain names of financial institutions, doesn’t influence the encountered attack intensity. B) English webpages for online banking, only influence the intensity attack intensity of financial institutions within EU countries. C) Globally, the broadband penetration of a country influences the attack intensity, encountered by the financial institutions established in the country. D) Globally, the GDP of a country influences the attack intensity, encountered by the financial institutions established in the country.

3. Mixed Methods

Mixed methods, of both qualitative and quantitative research are used to get a better understanding of target selection. First, qualitative analyses are executed to gather insights into the ideas of experts, regarding target selection. From these ideas, hypotheses are developed that can be tested with the Zeus dataset. Hereby, the Zeus dataset is used as the most objective available data source that can explain target selection by financial malware schemes. In other words, the Zeus dataset is addressed as the truth regarding target selection. Finally, the ideas of experts are compared with the outcomes of the hypotheses, by placing them in a broader context.

3.1 Qualitative research

3.1.1 Routine Activity Theory

To be able to define target selection by the financial malware schemes, a criminological theory is required that defines why certain financial institutions are more likely to be selected as target than others. The expectations of the experts are placed within the perspective of that theory. The routine activity theory (RAT) by Cohen and Felson (1979) is most suitable for this research. Because RAT clarifies “who are more likely to be victimized” (Cohen and Felson, 1979). Besides, other criminological theories focus on crime prevention, or clarifies why certain persons turn into criminals and execute criminal behavior. However, none of those theories is appropriate to explain target selection.

RAT is developed for the physical world. However, according to Yar (2005) and Choo (2010) this theory can be applied to the cyber domain. RAT proposes that crime occurs, when a *suitable target* is in the presence of a *motivated offender* and is without a *capable guardian* on a certain time and place (Cohen and Felson, 1979). In 2005, Yar described that “*although some of the RAT core concepts can indeed be applied to cybercrime, there remain important differences between ‘virtual’ and ‘terrestrial’ worlds that limit the theory’s usefulness*”. One of the main differences regards the fact that in the terrestrial world, RAT holds that a certain time and space are central for crime. However, Yar (2005), mentions that the spatial and temporal barriers are collapsed in cyberspace. Besides, the cyberspace has many-to-many connections, which makes it possible to select many targets simultaneously, instead of selecting only

one target at the time in the physical world. Finally, the online identity is more anonymous, compared to the non-virtual world (Yar, 2005).

Within this article, the '*Motivated Offender*' is presented by the financial malware schemes. Regarding financial malware, a '*Suitable Target*' is the financial institution's website or other type of webpages that can be included in the malware configuration files (Tajalizadehkhoob et al., 2013). The '*Absence of Capable Guardian*' exists, because it is technically impossible to continuously defend against all the financial malware attacks. In addition, many socio-technical vulnerabilities exist, through which the financial institutions' clients can be exploited (van den Berg et al., 2014).

3.1.2 Consultation of experts

Semi-structured interviews are conducted to gather experts' expectations about target selection. The experts are asked, to provide their perception regarding why certain financial institutions are more likely to be selected by financial malware schemes. Furthermore, they are asked to provide some characteristics based on which cyber criminals could select financial institutions. Thereby, the experts are not limited to Zeus malware. Instead, they are asked to provide their opinion about the evolution of target selection regarding all the financial malware they know.

Before the interview, the experts are informed with the subject and the goal of the research. Furthermore, the meaning of target selection in this research is explained. It is decided, not to provide the outcomes of previous interviews. Thereby, it is intended to prevent the interview from turning into the exact same direction as previous interviews. Finally, the conditions of RAT are used to place the outcomes of the consultations into a theoretical perspective. Hereby, RAT supports in understanding the phenomena of target selection, as assumed by the experts.

3.1.3 Hypotheses

The experts' ideas together with the existing literature, are used to develop hypotheses. Thereby, the hypotheses represent the visions of the experts regarding target selection. Based on the availability of data and time, different hypotheses are selected to test with the Zeus dataset. Before testing, they are processed in order to make them appropriate to test with the Zeus dataset. Subsequently, the hypotheses are tested with the Zeus dataset, after adding more data to it. Thereby, it is tested whether the expectations of experts are justified according to the risks of Zeus malware. Note that multiple hypotheses could hold simultaneously.

3.2 Quantitative research

The quantitative analysis exists of high-level analysis and profound analysis. First, high-level insights are provided into the targeted SEPA institutions, and by how many botnets. Subsequently, the profound analyses are executed, which exist of testing the hypotheses and analyzing the domains that encountered a relatively high attack intensity.

It is possible to gather insight into target selection by Zeus malware schemes, because the malware attacks are botnet based. A botnet is a flexible remote-controlled network containing computers that function together to make a platform available for fraudulent and criminal purposes (Bauer and van Eeten, 2009). A Zeus botnet exists of computers that are infected with Zeus malware (= bots). Those bots need instructions about which financial institutions to attack. These instructions are specified within configuration files, which are set by cyber criminals within the financial malware scheme and among others determine which domains to target. Those configuration files are gathered and stored

in the so called Zeus dataset by Tajalizadehkhoob et al. (2013). Those researchers gathered the data, extracted the targeted domains, analyzed the country of the targeted domains and added a metric for attack intensity.

3.3 The Zeus dataset including additions and adaptations

The Zeus dataset exists of domains that are targeted by Zeus malware between 2009 and 2013q1. The dataset includes the time of the attack, the targeted domains and the unique botnet key that identifies the attacker. For the quantitative analysis, the targeted domains belonging to financial institutions are taken into account, instead of the targeted financial institutions themselves. It is chosen to analyze on domain level, because the domains are really attacked.

The Zeus data consists of globally targeted domains, however for this article only the targeted domains from the SEPA countries are selected. Furthermore, the profound analyses are executed on a selection of the SEPA countries. For the purpose of these profound analyses, new data needs to be added and some of the existing data has to be adapted.

The selected domains

For the profound analysis, only the targeted domains from certain countries are taken into account. Tradeoffs had to be made regarding which countries to select. The targeted domains from the selected countries, are manually checked whether they belong to a financial institution and what the number of clients is of the financial institution. The number of clients is used to indicate the size of the financial institutions.

The countries that are selected for further research are; Austria, Belgium, Bulgaria, Finland, France, Hungary, Ireland, Norway, Romania, and the Netherlands. These are called "the selected SEPA countries", and are selected based on the following criteria:

- 1) **Multiple SEPA countries:** The influence of the country on (the evolution of) target selection is intended to be researched. Therefore, multiple countries have to be selected for this research. Moreover, by selecting the countries, the geographical location has been taken into account. The intention was to select countries spread across whole Europe (provided that they are included in SEPA).
- 2) **Outcomes of the high-level analysis:** The outcomes of the high-level analysis, executed in section 5.1, are used to determine which countries can be interesting to select. Countries that contain domains which are targeted by many botnets per week could be interesting to further analyze. Because the number of botnets targeting a domain, can provide some insights into likely targets.
- 3) **Available time:** The quantitative analyses are executed within three months by one researcher. Researching the number of clients for each targeted financial institutions is a time consuming task. Therefore, time constraints play an exclusive role within the tradeoffs. Which means, that countries with more than 25 targeted financial institutions, are unrealistic for the purpose of this research.
- 4) **Language barriers:** Because the number of clients have to be researched of institutions from different countries, language plays a significant role in the possibility to find a representative number.

- 5) **Countries mentioned by experts:** Because the expectations and assumptions of experts are researched, the countries mentioned by the experts during the consultations are selected first (when they met the other criteria as well).

The number of clients

The number of clients per financial institution are gathered from different data sources invoked through the internet. Hereby the total number of clients is researched, which includes both business clients and private clients of the institution in the specific country. For example: ING in the Netherlands has a different number of clients as ING in Belgium. Unfortunately, it seems impossible to gather data regarding the number of clients of each targeted financial institution. Therefore, the number of clients from a single year is used, it is decided to use the year that is most closely to 2011 (which is the middle year of the dataset).

The preference of the source of the data has the following order: 1) the authority's website is preferred most, 2) subsequently the institution's website, 3) then a third source has been searched and 4) finally Wikipedia has been used. However, for most of the institutions only one data source had been found. For the domains, where no number of clients has been found at all, it is determined whether this financial institution is expected to be small, middle or large. Based on this classification, the domain gets assigned a number of clients. When classified as small, it gets the smallest number of clients found in the country, when classified as medium it gets the average number of clients found within the country and when classified as large it gets the highest number of clients found in the country among the targeted financial institutions.

The dataset used for further analysis

Summarizing, within the selected countries, 106 domains have been targeted between 2009 and 2013q1. For those 106 domains, the attack intensity, in botnet weeks per year, is determined. Because some of the domains are targeted in multiple years, the dataset contains 220 values. Those 220 values are called "**domain years**", which can be calculated by counting the unique targeted domains per year, and then taking the sum of these domains over all the years. Domain years is a new developed unit, based on which the quantitative analyses are executed.

The metric for attack intensity

In the high-level analysis, overviews are provided that show the number of domains attacked per week, and the frequency of the number of botnets attacking these domains per week. With further analysis the intention is to get a better understanding of the choices regarding target selection and the evolution of these choices. To be able to analyze the intensity encountered by different domains, a metric is required that can provide insight into the relative attack intensity.

The metric used for further analysis is a combination of the number of weeks that domains were targeted and the number of botnets attacking the domains per week. This metric can be described as: The average number of botnets attacking a domain per week. Tajalizadehkhoob et al. (2013) mention that, "*to compare over longer periods, one could add up the count for each week ("botnet weeks") or average them*". Within this research **the number of botnet weeks** attacking a domain **per year** is used as **metric**.

3.4 Comparing the outcomes

Finally, the ideas of experts regarding target selection are compared with the outcomes of the quantitative analyses. This comparison is executed, in order to provide meaning to the outcomes of the hypotheses. Thereby, three significant issues are taken into account. First, the scope of the qualitative analyses and the scope of quantitative analyses differ. Hereby, the qualitative analysis focus on target selection regarding financial malware in general. While the data used for the quantitative analyses, provides insight into Zeus malware attacks between 2009-2013q1.

Secondly, the hypotheses that are tested with the Zeus dataset are subject to multiple transformations. In order to create appropriate hypotheses to test with the Zeus dataset. Finally, the Zeus dataset has its own shortcomings. Which means that the outcomes of the quantitative analyses also have their limitations. For those reasons, the expectations of experts that are not consistent with the data, shouldn't be directly discharged. Vice versa, hypotheses that are consistent with the Zeus dataset, do not directly indicate that the experts are perfectly right regarding target selection.

4. Target selection as assumed by experts in the perspective of RAT

In this section, RAT is used to understand why certain financial institutions are more likely to be selected as target than others. Together with RAT, it is determined whether the experts assume that target selection is more focused on **the suitability of a target** or on **the absence of a capable guardian**.

4.1 Target selection and its evolution as assumed by experts from the field in the perspective of RAT

Two main ideas of target selection can be distinguished from the output of the experts' interviews. One of the ideas states, that financial malware schemes target randomly as many financial institutions as possible, and continue attacking the institutions that are valuable and vulnerable (Bras, 2015; Wegberg, 2015; Jak, 2016). In the perspective of RAT, this idea first focusses on selecting many financial institutions as target and subsequently assess both the suitability and the guardian's capability of those institutions. Based on the assessment, the financial malware schemes determine to continue with attacking the financial institution or not.

The other main idea of target selection, discusses that financial malware schemes pre-select targets, based on the characteristics of the financial institutions (Bras, 2015; Kleijmeer, 2015; van Wegberg, 2015; Jak, 2016; Mooiman, 2016). These experts mention many characteristics that could be taken into account, like; authentication methods in place (one/two factor, or innovative ways of authentication), the number of clients, the net income, accepted risk levels, private or public property, the rank in google, availability of web injects, advanced cyber security measures in place, the country where the financial institution operates, whether or not the financial institutions are vulnerable according to reviews on the (dark-)web, etcetera. These characteristics could influence the financial institutions' risk, of being selected for financial malware attacks.

Pre-selecting targets based on characteristics

Three characteristics that are mentioned explicitly by multiple experts, are elaborated and placed within the perspective of RAT. Which are; 1) the size of financial institution, based on the number of clients, 2) the vulnerability of the financial institution, and 3) the country where the financial institution

is established. These last two, relatively high level characteristics, are clarified by the experts through explaining lower-level characteristics.

According to Bras (2015), van Wegberg (2015), Jak (2016) and Mooiman (2016), the size of a financial institution influences target selection. Which can be expressed by the number of clients of a financial institution. Besides, for the purpose of successful Zeus malware attacks, the Zeus malware schemes need an overlap of machines (computers of client's) which are infected with Zeus malware and web injects of the financial institutions of the infected clients. Therefore, from an economic perspective, it makes sense that financial malware schemes focus on developing web injects for either financial institutions with many clients or financial institutions with wealthy clients.

In addition, van Wegberg (2015), de Boer (2015) and Jak (2015) mention that the vulnerability of a financial institutions, can be of influence with target selection. In advance, the cyber criminals can determine vulnerability based on different factors. One factor that is widely mentioned by the experts, is the authentication method in place for online financial services (Bras, 2015; de Boer, 2015; Kleijmeer, 2015; van Wegberg, 2015; Jak, 2016; Mooiman, 2016). More sophisticated counter measures, are mentioned by the experts as well, to indicate vulnerability. However, it seems that sophisticated measures like; SOCs including the SIEMs, Transaction Monitoring, external security partners, and awareness programs in place for their clients and employees, etc., are hard to find out by the cyber criminals. And are therefore hard to take into account as factor to determine vulnerability. Furthermore, the vulnerability of a financial institution can differ per financial malware family as well. Finally, Döttling (2015) mentioned an interesting measure for vulnerability. According to Döttling (2015), financial malware schemes could use a leverage rate per financial institution, as indicator for vulnerability.

Furthermore, according to Bras (2015), Kleijmeer (2015), van Wegberg (2015), Jak (2016) and Mooiman (2016) the context of a country has influence on target selection as well. Regarding financial malware attacks this context can be determined by the degree of cooperation between financial institutions and law enforcement, the degree of cooperation between financial institutions, money transfer policies of the country, the number of financial institutions in the country, and the availability of money mules within the country (Tajalizadehkhoo et al. 2013; Raghavan et al., 2014; Jak, 2015; Mooiman, 2016).

Finally, it is expected that over time, the same characteristics could result into a different selection of targets. In this article, it is called the evolution of target selection. Which is discussed with experts as well.

The evolution of target selection

Due to evolution of target selection, the influence of the three different characteristics changes. In other words, over time pre-selection leads to another selection of targeted financial institutions. This evolution can be clarified with the terms "*static pre-selection*" and "*evolving pre-selection*". Static pre-selection means, that financial institutions with certain characteristics will always be targeted. For instance, experts expect that big financial institutions remain targeted (Wegberg; 2015; Bras, 2015; Mooiman, 2016). More straightforward, it is assumed by the experts, that vulnerable financial institutions will always be targeted (Wegberg; 2015; Bras, 2015; Jak, 2016; Mooiman, 2016). Furthermore, the experts assume that financial institutions in all the SEPA countries will always be

targeted, irrespectively of its less likely context (Wegberg; 2015; Bras, 2015; Kleijmeer, 2015; Mooiman, 2016).

Evolving pre-selection means, that financial institutions which didn't met the certain characteristics in the first time, could be selected over time, even though their characteristics didn't change. For instance, the experts expect that the proportion of targeted financial institutions with fewer clients, increases over time (de Boer, 2015; Jak, 2016; Mooiman, 2016).

Some of the experts assume, that target selection evolves, due to the improvements of the financial institutions' defense measures (Bras, 2015; de Boer, 2015; Jak, 2016). Thereby, it is noticed that the capability of these measures, is both determined by the technical defense measures adopted and by the awareness of the clients. Due to the increasing awareness and the sophisticated defense measures, the presence of opportunities decreased at the valuable financial institutions. Therefore, financial institutions with fewer clients become more targeted, over the years.

It is assumed by the experts, that the three big Dutch financial institutions are targeted less nowadays (Jak, 2016; Mooiman, 2016). Instead, the smaller Dutch financial institutions have become more likely to be selected as target. This expected shift can be called a waterbed effect. Furthermore, experts mention that financial institutions in the Scandinavian countries encounter a relative low attack intensity, because they have sophisticated security measures in place (Jak, 2016).

Besides, the development of more sophisticated malware, made it (economically) interesting to attack smaller financial institutions (Jak, 2016; Mooiman, 2016). For example, the development of hybrid forms of financial malware, created the possibility to attack clients from many different financial institutions. In addition, the suitability of an individual client becomes more important than the suitability of a financial institution (Jak, 2016).

Target selection based on characteristics in the perspective of RAT

Those experts' expectations and assumptions are placed within the perspective of RAT. This results into some propositions of target selection in the perspective of RAT.

First, it is expected that in the early years of financial malware, cybercriminals select targets based on certain characteristics which are focused on the suitability of the target. Especially the value of the financial institutions seems to be used for target selection, which – for instance - can be expressed by the number of clients. Besides, decreasing the accessibility of the financial institution is assumed by the experts, to be a short time solution. Because of the reason, that it is easy for the cybercriminals to find out the new ways of authentication. Subsequently, those are easy to circumvent. Moreover, new ways of access won't distinguish financial institutions for a long period of time, because other financial institutions can easily copy those new ways of authentication.

However, when attacks seem to be less successful, or when even botnets are taken down, due to improvements of the guardian. The experts expect, that cybercriminals start taking the guardian of the financial institutions into account. Therefore, new targets are selected, which in first instance were assessed less suitable. From the experts is extracted, that the capability of the guardian can both be expressed by the financial institutions' technical defense measures, and the awareness of their clients. Which increases when many clients have been targeted.

4.2 The extracted hypotheses

The experts' ideas regarding target selection, are used to develop multiple hypotheses, which can be tested with the Zeus dataset. Based on the criteria, available time and the available data, the following hypotheses are created;

1. *Financial institutions with more clients are targeted more by financial malware schemes, than financial institutions with fewer clients.*
2. *Within different SEPA counties, the financial institutions encounter a different relation between the number clients and the attack intensity.*
3. *Over the years, financial institutions with fewer clients become more likely to be selected as target, by Zeus malware schemes.*

Those hypotheses, all focus on the relation between the number of clients and the encountered attack intensity. First, it is tested over all the years of the dataset, whether financial institutions with more clients also encounter a higher attack intensity. The outcomes provide empirical insight into the influence of one of the characteristics, which according to the experts, is subject to static pre-selection. The experts expect that bigger financial institutions are always targeted (Wegberg; 2015; Bras, 2015; Mooiman, 2016).

Subsequently, the influence of the country, on the relation between the number of clients and the attack intensity, is analyzed. The experts expect that the context of the country influences target selection (Bras, 2015; Kleijmeer, 2015; van Wegberg, 2015; Jak, 2016; Mooiman, 2016). By testing this hypothesis, empirical insights into the influence of the country are provided. When the country seems to have significant influence on target selection. The many mentioned characteristics of the country could be subjects for future research.

Finally, the relation between the number of clients and the encountered attack intensity, is analyzed per year of the dataset. The outcomes of this analysis, provide empirical insight into evolving pre-selection based on the size of a financial institution. The experts expect, that due to the evolution of target selection, smaller financial institutions become targeted more intensively (de Boer, 2015; Jak, 2016; Mooiman, 2016).

5. Targeted domains according to the Zeus dataset

5.1 Selected targets within SEPA

First, high-level insights are provided into the distribution of Zeus malware attacks, among financial institutions within the SEPA. **This distribution** clarifies the number of targeted domains and the number of botnets attacking the domains per week. The botnets represent financial malware schemes. Although one malware scheme can operate multiple botnets, it provides an indication of the popularity of domains within SEPA countries.

Between 2009 and 2013q1, 345 domains belonging to financial institutions, from 26 SEPA countries are targeted. Thereby, 80% of the domains belong to financial institutions from the United Kingdom, Spain, Italy and Germany. It seems, that the number of targeted domains in those countries, roughly decreases and increases accordingly per week. Furthermore, the analyses show, that most of the domains are targeted by one botnet per week. However, certain domains in the United Kingdom, Spain, Bulgaria, France, Germany, Ireland, Italy and Portugal were targeted by more than 10 botnets

in certain weeks. Moreover, domains of financial institutions from the United Kingdom, Spain, Italy and Ireland, are targeted in certain weeks by more than 35 botnets.

Finally, some insights are provided into the targeted Dutch domains, since the research has been executed together with the Dutch Central Bank. Within the Netherlands, the domain Postbank.nl was targeted first. Subsequently, the domains of the big three Dutch financial institutions become targeted. Finally, also smaller Dutch financial institutions become selected as target. The only Dutch domain that hasn't been targeted anymore, after it was target once, is Postbank.nl.

From the consultation with de Boer (2015), it is known that Postbank.nl has been migrated with ing.nl. This migration process is called the TANGO program. The TANGO program realized the technical integration of the systems of ING Bank and Postbank, after they legally merged to ING. Within three waves, the communication to the clients had been integrated (AdVancher, 2016; Brotesse, 2010). Thereby, it can be concluded that between 2009 and 2013q1, Dutch domains that have been targeted once, are only not selected as target anymore when the domain stops to exist.

5.2 A profound understanding of target selection within SEPA

In this subsection, the hypotheses are tested based on the targeted domains from the ten selected SEPA countries (Austria, Belgium, Bulgaria, Finland, France, Hungary, Ireland, Norway, Romania, and the Netherlands). Furthermore, the domains from those countries that are targeted relatively intensive, are analyzed. The data used for these analyses contains 220 domain years. Those domain years are on average targeted by 47.5 botnets.

5.2.1 The relation between the number of clients and the attack intensity

First, hypothesis 1 is tested: *Financial institutions with more clients are targeted more by financial malware schemes, than financial institutions with fewer clients.*

A linear regression model is constructed, to analyze the relation between the number of clients and the attack intensity. The required assumptions to execute a linear regression, are met after a log transformation of the attack intensity. The regression line is shown in figure 1. Furthermore, a summary of this statistical model is presented in table 1. The summary shows, that the number of clients does correlate with the encountered attack intensity. It is noticed that an increase of one million clients, results into an increase of $e^{0.15}$ (≈ 1.16) botnet weeks per year. However, the model is only able to explain 7.8% of the variance within the attack intensity. The other 92.2 % could be explained by other variables, or by a random factor. According to the experts, the context of the country and the year of the attack could explain more of the attack intensity. This is quantitatively researched in the next subsection.

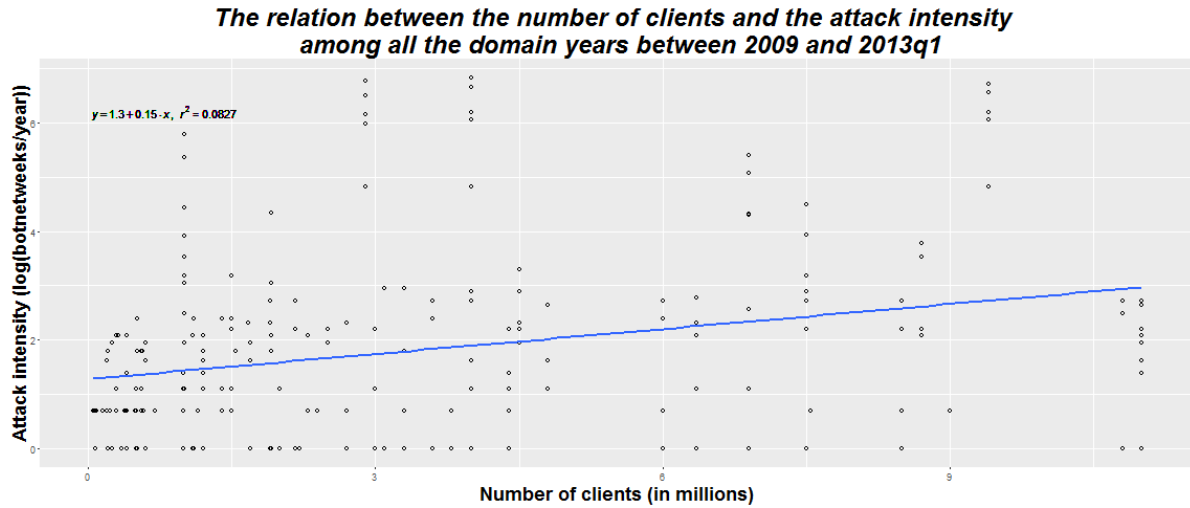


Figure 1: Linear regression model after log transformation over all the domain years

Table 1: Linear regression model information over all the domain years

Coefficients	Regression coefficient	Std. Error	T value	P value
Intercept	1.2815	0.1611	7.954	9.73e-14 ***
Number of clients	0.1534	0.0346	4.434	1.47e-05 ***

Note: *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$; 218 degrees of freedom; R-squared = 0.07851

In addition, the Spearman's Rho is used to analyze the non-linear relation. Hereby, the strength of the monotonic relation between number of clients and attack intensity is measured. According to this test, the relation intensity is significant as well. Thereby, the relation is 0.33, which is a weak monotonic relation. The outcomes of the Spearman's rho test are shown in table 2.

Table 2: The Spearman's rho test on the targeted domains

	Coefficient
P-value	6.123e-07
Rho	0.3287248

Both the Spearman's Rho test and the regression analysis show, that a significant positive relation exists, between the number of clients and the encountered attack intensity. Thereby, the first hypothesis can be accepted. However, the regression line is not able to explain the relation well. Furthermore, the found monotonic relation with the Spearman's rho is weak. Therefore, further analyses are required, to be able to draw stronger conclusion about the relation between the number of clients and the encountered attack intensity. For these further analyses, the domains that encountered a relatively high attack intensity, are taken into account.

5.2.2 The relative intensively targeted domains

According to the regression analysis, three domain years are outliers. Which are aib.ie (2009), procreditbank.bg (2009) and banquepopulaire.fr (2009). Therefore, those domains are analyzed further. First, aib.ie belongs to the Allied Irish Banks, containing 4 million clients and thereby has the most clients of the targeted financial institutions in Ireland. This domain has a relatively high attack intensity in the years 2009 till 2012 (respectively, 920, 769, 427 and 487 botnet weeks). Besides, in the first nine weeks of 2013, the attack intensity was still 123 botnet weeks.

Secondly, procreditbank.bg is a Bulgarian bank belonging to the Procredit group. This financial institution has the most clients among the targeted Bulgarian financial institutions. Within 2009, the domain is attacked for 877 botnet weeks. Furthermore, in 2010 till 2013 by respectively 671, 392, 473 and 123 botnet weeks.

Finally, banquepopulaire.fr belongs to a group of French banks containing 9.4 million clients. Thereby, it is one of the two targeted French institutions that contain the most clients. The domain encountered a relatively high attack intensity in the years 2009 and 2010, by respectively 822 and 705 botnet weeks. In the years 2011 till 2013, the domain was under attack by respectively 423, 490 and 124 botnet weeks. It is noticed, that the three domains that encountered relatively high attack intensities, almost have the most clients among the targeted financial institutions in their own country. The influence the country on attack intensity, is analyzed in the next subsection.

5.2.3 The relation between the number of clients and the attack intensity per selected country

In here, hypothesis 2 is tested: *Within different SEPA counties, the financial institutions encounter a different relation between the number clients and the attack intensity.*

A multiple regression analysis is executed, to test this hypothesis. To remind, the ten countries that are selected for the profound analysis are; Austria, Belgium, Bulgaria, Finland, France, Hungary, Ireland, Norway, Romania, and the Netherlands. However, the data doesn't met the assumptions of homoscedasticity and normality. Therefore the log transformation of the attack intensity is executed. The outcomes of the analysis are provided in table 3.

Table 3: Multiple Linear regression model information based on the number of clients and the country

Coefficients	Regression coefficients	Std. Error	t value	P value
(Intercept)	0.90747	0.26540	3.419	0.000755 ***
NOC (Austria)	0.18328	0.03657	5.012	1.14e-06 ***
Belgium	-0.32384	0.36196	-0.895	0.371990
Bulgaria	3.75729	0.60969	6.163	3.63e-09 ***
Finland	-0.35405	0.42473	-0.834	0.405472
France	-0.11907	0.34070	-0.349	0.727070
Hungary	-0.25665	0.60962	-0.421	0.674188
Ireland	2.29640	0.39085	5.875	1.64e-08 ***
The Netherlands	0.50736	0.37974	1.336	0.182982
Norway	-0.07745	0.42766	-0.181	0.856462
Romania	0.06129	0.54278	0.113	0.910201

Note: ***p<0.001, **p<0.01, *p<0.05; 209 degrees of freedom; R-squared = 0.3581

It is shown, that almost 36% of the variance can be explained by the model based on the number of clients and the country. This is a strong improvement, comparing to the model that is based on only the number of clients. Furthermore, characteristics that could explain the remaining 64% of the variance of attack intensity, could be researched. According to the experts, the sophisticated technical measures in place, the adopted authentication methods and the awareness level of the clients, are variables that could explain attack intensity.

In addition, it can be concluded, that within Austria, Bulgaria and Ireland, a significant linear relation exists between the number of clients and the encountered attack intensity. Which means, that in these countries an increase of the number of clients, results into an increasing attack intensity. However, the

slope of those three regression lines varies. Therefore, among those three countries, an increase with one million clients results into a different increase of the attack intensity.

Besides, in the countries Belgium, Finland, France, Hungary, The Netherlands, Norway and Romania there isn't a significant linear relation between the number of clients and the encountered attack intensity. This indicates, that in only three of the ten selected SEPA countries, the number of clients of the financial institution has influence on the encountered attack intensity. Characteristics that could explain the significant relation, are the number of institutions in the country, or the availability of a money mule network within the country. Moreover, two out three countries that encounter a positive relation, contain a domain that is targeted relatively intensive. This could determine the found significance as well. In that case, it would be interesting to research characteristics of those specific financial institutions. Or characteristics that could explain the context of the country they are located.

Hereby, it can be concluded that hypothesis 2 holds. First, because with the country as an extra variable, the regression analysis is able to explain more of the variance. Furthermore, only in 30% of the countries the number of clients has influence on the attack intensity. In addition, the slope differs among those three countries. In the next subsection, the influence of **the evolution** of target selection, on the relation between the number of clients and the encountered attack intensity, is analyzed.

5.2.4 The evolution of target selection

In this section, hypothesis 3 is tested: *Over the years, financial institutions with fewer clients become more likely to be selected as target, by Zeus malware schemes.*

Hereby, the year of the attack is added as an extra independent variable, besides the number of clients. First, figure 2 provides insight into the targeted domains per category of clients, per year. Hereby, categories are developed of 3 million clients. It is noticed, that the number of targeted domains in the category till 3 million clients, increases every year. Note, that only in the first nine weeks of 2013, that category already contains 24 domains.

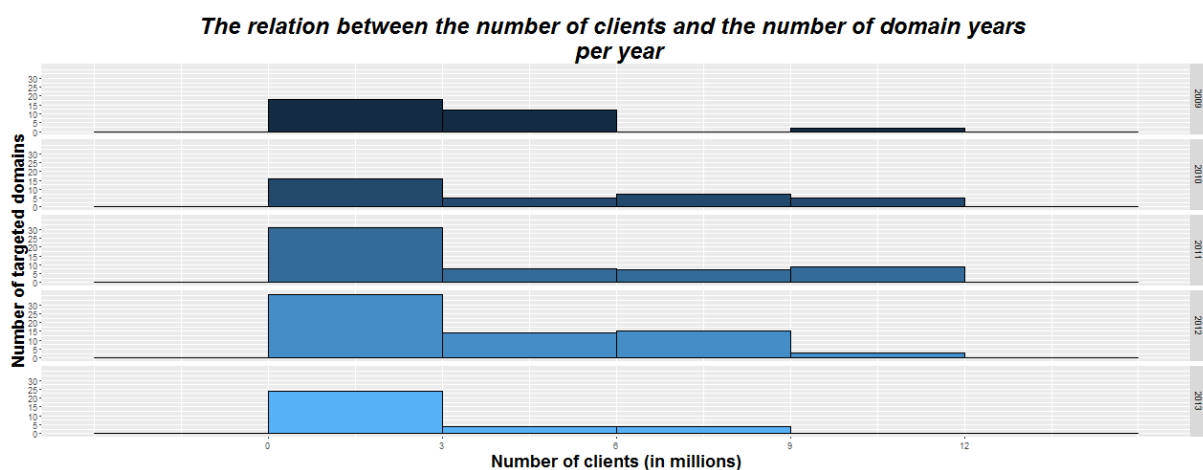


Figure 2: Targeted domains per category of clients per year

Subsequently, a multiple-regression analysis has been executed. The model is able to explain 10% of the variance of the encountered attack intensity. This is an increase, relatively to only using the number of clients. Which means, that the relation between the number of clients and the encountered attack intensity, differs per year. Furthermore, a significant relation exists within the years 2009 and 2013. Which means that in these countries financial institutions seem to be selected based on the number

of clients. Within the year 2009, an increase of one million clients, results into an increasing attack intensity of $e^{0.16}$ (≈ 1.17) botnet weeks per year. However, within 2013, an increase of one million clients results into a decreasing attack intensity of $e^{-1.16}$ (≈ 0.31) botnet weeks per year. In table 4, the outcomes of the multiple-regression analysis are presented.

Table 4: Multiple Linear regression model information based on the number of clients and the year

Coefficients	Regression coefficient	Std. Error	t value	P value
(Intercept)	1.81473	0.31278	5.802	2.34e-08 ***
NOC (2009)	0.15745	0.03469	4.539	9.42e-06 ***
2010	-0.39059	0.39767	-0.982	0.32711
2011	-0.68350	0.35660	-1.917	0.05661
2012	-0.47953	0.34584	-1.387	0.16701
2013	-1.16402	0.40087	-2.904	0.00407 **

Note: *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$; 2014 degrees of freedom; R-squared = 0.1003

It can be concluded that hypothesis 3 holds. Because, in 2009 a positive relation exists between the number of clients and the encountered attack intensity. While four years later, a negative relation exists between the number of clients and the attack intensity.

6. Comparing the outcomes of the qualitative analysis with the quantitative analysis

In this section, the expectations of the experts are compared with the outcomes of the hypotheses. According to tested hypotheses, multiple consistencies and some inconsistencies exist, between the experts and the Zeus dataset. However, these (in-) consistencies exist, between the specific consulted experts and the specific dataset. Besides, the scopes of both analyses differs. Furthermore, the ideas of experts are processed, in order to create hypotheses that could be tested with the dataset. Therefore, the meaning of the (in-) consistencies is placed in a broader context.

According to the tested hypotheses, bigger financial institutions encounter a higher attack intensity. Furthermore, financial institutions from different SEPA countries, encounter a different relation between the number of clients and the encountered attack intensity. Hereby, should be noticed that not in each SEPA country, a significant relation has been found. In addition, smaller financial institutions, become more targeted over the years.

Regarding the hypotheses, the number of clients is used to express size the financial institutions. However, many other factors can determine the size of a financial institution. For instance, the net income of the institution or its total assets. Moreover, nowadays there are many varying financial services. Which all have their own number of clients, in this research the total number of clients has been taken into account. Regarding the attack possibilities of Zeus financial malware, the number of clients holding a payment account, would be most realistic to take into account for target selection.

In addition, according to the experts, smaller financial institutions become targeted more, because the bigger financial institutions improved their counter measures. However, that assumption couldn't be tested with the quantitative analyses.

Furthermore, the experts assume, that the context of the country influences the attack intensity, encountered by the financial institutions. Instead, the hypotheses tested whether the relation between the number of clients and the attack intensity differs per country. For testing whether financial institutions in certain countries are targeted more, different relations should be tested and different metrics are required. For instance, the relation between the number of targeted financial institutions and the total number of institutions per country. Besides, a metric could be developed, which combines the average attack intensity encountered by financial institutions in a certain country, with the online banking penetration of the country.

7. Conclusion

This article provided empirical insights into characteristics of financial institutions, which influence their likelihood of being selected as target for financial malware attacks. Those characteristics are assumed by experts from the field. The expectations of experts regarding target selection, are placed within the perspective of the routine activity theory (RAT). RAT proposes that crime occurs, when a *suitable target* is in the presence of a *motivated offender* and is without a *capable guardian*. Hereby, the financial malware schemes are assumed to be the motivated offender.

Besides, the experts expect that in the first years of financial malware, target selection was particularly focused on the suitability of a financial institution. Especially, the size of the financial institutions is assumed to be taken into account. Which – for instance - can be expressed by the number of clients. Furthermore, the capability of the guardian is assumed to have more influence on target selection, over the years. It is expected, that the capability of the guardian can both be expressed by the financial institutions' technical defense measures, and the awareness of their clients. Due to the increasing awareness and the sophisticated defense measures, the presence of opportunities decreased at the big financial institutions. Therefore, experts expect that smaller financial institutions are targeted more nowadays. In addition, the experts assume that the context of a country, influences target selection.

From the analyses with the Zeus dataset can be concluded, that between 2009 and 2013q1, financial institutions with more clients are targeted more by financial malware schemes. However, on a yearly basis, this relation only holds in 2009. Furthermore, in 2013, financial institutions with fewer clients become more likely to be selected as target. Finally, within different SEPA counties, the financial institutions encounter a different relation between the number clients and the attack intensity.

By comparing the expectations of the experts, with the outcomes of the hypotheses. It is noticed, that the size of a financial institution can be expressed by more factors than the number of clients. Moreover, the financial institutions offer many services. Therefore, the number of clients can be measured in many ways. Furthermore, according to the experts, smaller financial institutions become targeted more, due to the improvements of the big financial institutions their guardian. However, this couldn't be tested, due to the lack of data regarding defense measures. Finally, the experts mention that the context of the country influences the attack intensity. While the quantitative analyses focused, on the relation between the number of clients and the attack intensity.

8. Discussion

The findings of this article, contribute to previous observations with the Zeus dataset, by Tajalizadehkhoob et al. (2013). Furthermore, it provides insight into the differences of the cyber fraud level, between some first world countries. Which is assumed to exist, by the Federal Financial Institutions Examination Council (2014).

First, the value of the qualitative research is discussed. By combining the outcomes of the consulted experts, value is created, by potential characteristics of financial institutions that could influence target selection. The value of those consultations is limited, because only experts are consulted from the Dutch financial sector and from Dutch research institutions. None of the consulted experts, is from another financial sector within SEPA. Furthermore, none of them is from a cyber security company. However, this article contributes to the work of Tajalizadehkhoob et al. (2013), which consulted experts from the security company FOX IT.

In addition, RAT is developed in the physical world. By using it in cyber space, it could simplify this complex artificial space, too much. Which could result in biased and short-sighted research. However, in this article, RAT seems to contribute to the explanation of target selection and its evolution. Although, the two terms “static pre-selection” and “evolving pre-selection”, had to be created to explain the evolution of target selection. Besides, a certain bias could exist, between what the experts intend to articulate, and how the researchers interpreted their assumptions. For instance, the experts could mean that the attacks were not successful anymore. Instead of, financial institutions are not being targeted at all. Furthermore, the experts could also refer to the encountered attack intensity in last two years, which is not part of the dataset.

Secondly, the value of the Zeus dataset is discussed. Which is used, to test the hypotheses that arise from the experts’ ideas regarding target selection. This is valuable data, because it provides ground truth data regarding target selection by Zeus malware schemes. However, the dataset contains only web injects for the purpose of Zeus financial malware. While, many other malware families exist. Besides, it only contains data between 2009 and 2013q1. Furthermore, Zeus malware can be used in multiple ways to target clients of financial institutions, while the web injects only provide insight into the purpose of modifying webpages. In addition, it could be the case that the data still contains web injects, which aren’t effective anymore. Furthermore, only a small subset of the Zeus dataset is used for testing the hypotheses. Moreover, five of the biggest financial sectors in SEPA, haven’t been taken into account. Finally, the data for 2013 only exists of nine weeks.

Notwithstanding these shortcomings, it is assumed that the Zeus dataset is representative for the purpose of target selection by financial malware schemes. Because, Zeus is known as a persistent malware family, which is one of the most dominant malware families that ever existed (Europol, 2014; Tajalizadehkhoob et al., 2013). Besides, Zeus was one of the first developed financial malware families that becomes very popular (Lucas, 2015). In addition, among the four common ways of exploiting clients with Zeus financial malware, inject code can be used to really attack the financial institution. Besides, although the data probably contains ineffective web injects, new web injects are required continuously. For that reason, many web injects within the dataset will be effective. Finally, this article observed the influence of the number of clients on the encountered attack intensity, on country level. Due to this low level, the subsets of the data become small. However, it adds value to the findings of Tajalizadehkhoob et al. (2013), which are on global scale and on EU scale.

References

Adham, M., Azodi, A., Desmedt, Y., Karaolis, I., 2013, *How to Attack Two-Factor*.

AdVanced, 2016, *De rol van AdVanced (medewerkers) bij Tango*, extracted from: <http://www.advanced.nl/referenties/ing>, on February 2016.

Anderson, R., Böhme, R., Clayton, R., Moore, T., 2008, *Security Economics and the internal market*, ENISA.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Levi, M., Moore, T., Savage S., van Eeten, M., J., G., 2013, *Measuring the Cost of Cybercrime*, Springer: The Economics of Information Security and Privacy pp 265-300.

Bauer, J., M., van Eeten, M., J., G., 2009, *Cybersecurity: Stakeholder incentives, externalities, and policy options*, Telecommunications Policy, Volume 33, Issues 10–11, pages 706–719, Elsevier.

BITS, Financial Services Roundtable, 2011, *Malware Risk and Mitigation Report*, Washington DC.

Bresiger, G., 2013, Cost of financial-service cybercrime nearly \$400B, New York Post, Extracted from <http://nypost.com/2013/10/12/cost-of-financial-service-cybercrimenearly-400b/>.

Brottesse, 2010, *ING Tango*, Extracted from: http://www.brottesse.nl/?page_id=61, on February 2016.

Claessens, J., Dem, V., De Cock, D., Preneel, B., Vandewalle, J., 2002, *On the Security of Today's Online Electronic Banking Systems.*, Computers & Security, 21: 253-265.

Committee on Payments and Market Infrastructures (CPMI), 2014, *Cyber resilience in financial market infrastructures*, BANK FOR INTERNATIONAL SETTLEMENTS

Choo, K.-K. R. 2011. The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8): 719-731.

FFIEC, 2014, *FFIEC Cyber security assessment general observations*, Extracted from: [http://www.ncua.gov/Resources/CUs/Documents/FFIEC Cybersecurity Assessment Observations.pdf](http://www.ncua.gov/Resources/CUs/Documents/FFIEC_Cybersecurity_Assessment_Observations.pdf).

Enisa, 2008, <https://www.enisa.europa.eu/activities/cert/support/information-sharing/european-fisac-a-public-private-partnership>

Europol, 2015, *The internet organized crime threat assessment (iOCTA)*, European Cybercrime Centre.

FFIEC, 2014, *FFIEC Cyber security assessment general observations*, Extracted from: [http://www.ncua.gov/Resources/CUs/Documents/FFIEC Cybersecurity Assessment Observations.pdf](http://www.ncua.gov/Resources/CUs/Documents/FFIEC_Cybersecurity_Assessment_Observations.pdf).

Florêncio, D., Herley, C., 2011, *Where Do All The Attacks Go?* Economics of Information Security and Privacy III: 13-33, Springer New York.

Galien, X., 2014, *Behind Point of Sale (PoS) attacks*, Bluelive, Extracted from: <https://www.blueliv.com/research/behind-point-of-sale-pos-attacks/> in 2015.

Grabosky, P., Smith, R., 2001, *Telecommunication fraud in the digital age*, Wall DS (ed) Crime and the Internet, London Routledge.

Hutchings, A., Hayes, H., 2009, *Routine activity theory and phishing victimization: Who got caught in the 'net'?* *Current Issues in Criminal Justice*, 20, 432-451.

Lawrence, 2015, *Financial Industry's Most-Wanted Hacker; The malware known as Zeus and its rogue creator have been at the cutting edge of cyber-crime for nearly a decade*, extracted from: <http://www.bloomberg.com/news/features/2015-06-18/the-hunt-for-the-financial-industry-s-most-wanted-hacker>, on October 2015.

Lucas, M., 2015, *A Short History of Attacks on Finance*, RSA Conference, Extracted from: <https://www.youtube.com/watch?v=3f7v3XtjOqY> on 28-09-2015.

Macdonald, D., 2011, *Zeus: God of DIY Botnets*, FortiGuard Center, Extracted from <http://www.fortiguard.com/legacy/analysis/zeusanalysis.html#3>, on November 2015.

Marinos, L., 2014, *ENISA Threat Landscape 2014, Overview of current and emerging cyber-threats*, Enisa.

Microsoft, 2014, Microsoft Security Intelligence Report, Volume 18.

Raghavan, A., R., Parthiban, L., 2014, *The effect of cybercrime on a Bank's finances*, International Journal of Current Research and Academic Review ISSN: 2347-3215, 2(2): 173-178.

S21sec.com, Advanced cyber security Services 21, 2013, *Zeus timeline (I)*, extracted from: <http://securityblog.s21sec.com/2013/11/zeus-timeline-i.html>, on September 2015.

Symantec, 2016, *Cyber resilience*, extracted from: <https://www.symantec.com/page.jsp?id=cyber-resilience>, on February 2016.

Tajalizadehkhoo, S., Asghari, H., Groenleer, M., Sandee, M., van den Berg, J., van Eeten, M., 2013, *Online banking fraud mitigation; A Quantitative Study for Extracting Intelligence about Target Selection by Cybercriminals from Zeus Financial Malware Files*, Msc Thesis, Delft University Of Technology.

Utakrit, N., 2009, *Review of Browser Extensions, a Man-in-the-Browser Phishing Techniques Targeting Bank Clients*, Edith Cowan University, Australian Information Security Management Conference.

Van den Berg, J., van Zoggel, J., Snels, M., van Leeuwen, M., Boeke, S., Koppen, L., van der Lubbe, J., van den Berg, B., de Bos, T., 2014, *On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education*, Delft University of Technology.

Vrancianu, M., & Popa, L. A., 2010, *Considerations Regarding the Security and Protection of E-Banking Services Consumers Interests*, The Amfiteatru Economic Journal.

Wyke, J., 2011, *What Is Zeus?* Extracted from: <http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/what-is-Zeus.aspx>.

Yar, M., 2005, *The Novelty of 'Cybercrime' an Assessment in Light of Routine Activity Theory*, European Journal of Criminology, 2: 407-427.

Consulted experts:

Arne de Boer (Supervisor at IT oversight at DNB).

Hessel Mooiman (head information risk management and CISO at Binckbank).

Maarten Bras (Member of the Cyber Intelligence Unit at DNB).

Maarten Jak (Intelligence Specialist II at ABN AMRO | Expertise Team Analysis | Security & Intelligence Management).

Raymond Kleijmeer (Member of the Cyber Intelligence Unit at DNB).

Robin Döttling (PhD candidate finance Group University of Amsterdam).

Rolf van Wegberg (PhD candidate Economics of Cybersecurity research group at the Technical University of Delft).