Discerning Novel Value Chains in Financial Malware

On the Economic Incentives and Criminal Business Models in Financial Malware Schemes

van Wegberg, R. S.; Klievink, A. J.; van Eeten, M. J G

DOI
10.1007/s10610-017-9336-3

Publication date
2017

Document Version
Final published version

Published in
European Journal on Criminal Policy and Research

Eur J Crim Policy Res
DOI 10.1007/s10610-017-9336-3

Discerning Novel Value Chains in Financial Malware

On the Economic Incentives and Criminal Business Models in Financial Malware Schemes

R. S. van Wegberg[1,2] · **A. J. Klievink**[1] · **M. J. G. van Eeten**[1]

Abstract Fraud with online payment services is an ongoing problem, with significant financial-economic and societal impact. One of the main modus operandi is financial malware that compromises consumer and corporate devices, thereby potentially undermining the security of critical financial systems. Recent research into the underground economy has shown that cybercriminals are organised around highly specialised tasks, such as pay-per-install markets for infected machines, malware-as-a-service and money mule recruitment. Setting up a successful financial malware scheme requires the aligning of many moving parts. Analysing how cybercrime groups acquire, combine and align these parts into value chains can greatly benefit from existing insights into the economics of online crime. Using transaction cost economics, this paper illustrates the business model behind financial malware and presents three novel value chains therein. For this purpose, we use a conceptual synthesis of the state-of-the-art of the literature on financial malware, underground markets and (cyber)crime economics, as well as today's banking practice.

Keywords Cybercrime · Financial malware · Transaction cost economics · Value chain · Underground markets · Vertical integration

Introduction

Fraud with online payment services has consistently been one of the most damaging forms of cybercrime (Anderson et al. 2012). The European Central Bank (2015) has published fraud

✉ R. S. van Wegberg
r.s.vanwegberg@tudelft.nl

[1] Faculty of Technology, Policy & Management, Delft University of Technology, The Hague, Netherlands

[2] TNO Cyber Security & Resilience, The Hague, Netherlands

Published online: 03 February 2017

statistics for the Single Euro Payments Area (SEPA), which puts the total fraud in 2014 at €1.44 billion. Around 66% of the total is 'card-not-present' (CNP) fraud, which includes online payments. The overall trend is, however, undisputed: online payment fraud imposes substantial cost on the economy and that it is becoming the dominant form of fraud with payment services (Anderson 2008; van Eeten and Bauer 2008; Moore et al. 2009). Next to phishing, malicious software, i.e. malware targeting financial service providers worldwide, is an ongoing and continuous threat to these financial service providers, causing millions in damages in both industrialised and non-industrialised countries (Anderson et al. 2012).

The research covering financial malware has primarily been technical of nature and much of this work focused on only specific parts of the total, overarching malware ecosystem. For example, Grier et al. (2012) inspected the (business) model of exploit-as-a-service,[1] where criminals rent out their infrastructures in order to infect systems, e.g. drive-by downloads.[2] Setting up a successful financial malware scheme however, requires the aligning of many moving parts. Not only having the overview of which parts are needed but also the expertise to actually set up and operate the total scheme requires a serious level of skill. Hence, the underground economy, now seen as a sort of criminal Craigslist where these 'parts', like botnets etc., are sold or rented out, plays an ever more important role in acquiring and aligning all moving parts. This underground economy transforms the necessity of having expertise on specific parts of a financial malware scheme into 'knowing what to buy,' arguably allowing actors with less expertise to operate such a scheme. However, we don't know how these actors choose between setting up the entire scheme themselves or 'outsourcing' parts of the scheme. For instance, leasing a botnet, using crimeware-as-a-service,[3] pay-per-install[4] or money mule recruitment services.[5] And if they do outsource, how does this effect both business models—that of the organiser of the total scheme and that of the seller of 'parts'? Which (economic) incentives influence this 'outsourcing'?

To address these and similar questions, the existing insights on parts of the financial malware ecosystem will need to be combined with insights from research on the 'economics' of crime. By conceptually synthesising the literature on financial malware, we will try to shed light on criminal strategies in financial malware schemes. Next to this specific economic outlook on crime, transaction cost economics can be of beneficiary value to understand outsourcing incentives within these criminal strategies. Specifically, when looking at these economic incentives, the underlying patterns and motivations behind the current modus operandi, i.e. criminal business model, can be unravelled. When combining these insights with the knowledge on the various components of the financial malware ecosystem, the so-called 'value chain' of financial malware can be uncovered.

The field of economics of (cyber)crime has been interdisciplinary from the start. But rather than criminologists or economists, much innovative work has come from computer scientists who were able to extract and capture data around the criminal ICT infrastructure. For example,

[1] Exploit-as-a-service is a service that automates the exploiting of a victim's (internet) browser (Grier et al. 2012).

[2] Any download that takes place without the user's authorisation or prior knowledge; often initiated already active malicious software (Grier et al. 2012).

[3] Crimeware-as-a-service (CaaS) is a business model used in the underground market where illegal services are provided to help underground buyers conduct cybercrimes (such as attacks, infections and money laundering) in an automated manner (Sood and Enbody 2013).

[4] Pay-per-install services play a key role in the modern malware marketplace by providing a means for outsourcing the global dissemination of their malware (Caballero et al. 2011).

[5] An example of CaaS, wherein money mules are offered as a commodity (Sood and Enbody 2013).

Levchenko et al. (2011) have uncovered the spam value chain in an analysis of the full set of resources employed to monetise spam email, including naming, hosting, payment and fulfilment. Other groups have studied the criminal market for fake anti-virus software (Stone-Gross et al. 2013) and the pay-per-install market for compromised machines (Caballero et al. 2011). Similarly, Rossow et al. (2013) inspected the value chain of malware downloaders, i.e. malicious programs that sell the possibility to download and execute malicious modules to end-user devices.

Until now, there has been little to no systematic and comparative empirical research that sheds light on the overall value chains around financial malware. In this paper, we, therefore, aim to unravel novel value chains in financial malware. These value chains can help extricate the interactions between the strategies of attackers on the one side and the properties and policies of the financial service providers on the other. It would enable us to study how the different resources involved in these attacks are being combined and how (new) interventions in one part of the value chain (e.g. interventions aimed at cash-out strategies) affect the other parts (e.g. targeted payment services). Understanding these interactions would help in creating better countermeasures and new security services, ideally making certain fraud models less profitable or even loss-making to begin with.

The goal of this paper is to conceptually synthesise the literature on financial malware, underground markets and (cyber)crime economics, as well as today's banking practice, to make a first attempt at discerning archetypical and novel value chains in financial malware. In the next part of the paper, sections II and III give an overview of the field of economics of crime, respectively on the economics of cybercrime and transaction cost economics. Then, in section IV, we give a state-of-art of the literature on financial malware and identify parts of the whole malware ecosystem which have been studied. In section V, we use both these overviews—(cyber)crime economics and financial malware—to discern three novel value chains in financial malware based on the existing literature, as well as today's banking practice, followed by our conclusions in section VI.

Theoretical Background

Economics and Crime Analysis

Studying crime in an economic fashion is not new. Famous is the work of Becker (1974), wherein he lies to foundation of the economics of crime and punishment. Using a rational choice perspective, he presented the idea that crime and punishment are to be analysed on the basis of individual costs and benefits. Knowing these costs and benefits allows for criminal justice policies to become increasingly effective by raising cost, such as the penal risk, or lowering the benefits; think of bank vaults with time locks in order to lower the immediate reward of robbing a bank.

The work of Becker inspired others to look for an economic approach to study organised crime (Dick 1995; Garoupa 1997, 2007; Kugler et al. 2005; Levitt and Venkatesh 2000). Thereof, the work of Levitt became widely popular when he combined earlier work in the best selling book Freakonomics and its successor SuperFreakonomics (Levitt and Dubner 2005, 2009). Literature on the economics of organised crime, let alone financial cybercrime, is quite scarce when comparing this to the growing amount of economic studies on individual crime and criminal law. Nonetheless, with the attention shifting towards cybercrime more and more, the field of economics of cybercrime, as introduced above, has seen growing amounts of studies with an economical approach to cybercrime from 2006 onwards (Afroz et al. 2013; Anderson 2008; Anderson et al. 2012; Anderson and Moore 2006; Bauer and van Eeten 2009; Kim et al. 2011; Kraemer-Mbula et al. 2013; Lagazio et al. 2014; Li et al. 2009; Moore 2010; Moore et al. 2009; Rao and Reiley 2012; Sood et al. 2013a; Walker 2012).

More, in particular, both Moore et al. (2009) and Thomas et al. (2015) made critical, breakthrough attempts to grasp the market structure of online crime, i.e. underground markets, whereas Afroz et al. (2013) comparatively studied these underground markets, five to be precise, in more depth for one of the first times. Furthermore, Kraemer-Mbula et al. (2013) have shown the ongoing globalisation based on a growing digital ecosystem, in cybercrime and underground markets, using credit card fraud and identity theft as exemplary cases. Moreover, Sood and Enbody (2013) introduced the model of crimeware-as-a-service, describing and analysing multiple forms of criminal services purchasable on underground markets. These underground markets thus have a vast supply of specific parts of the malware ecosystem (Sood and Enbody 2013). Matched with a continuous demand for these parts to set up a financial malware scheme, this creates an extraordinary (criminal) market structure. But how does a criminal (organisation) chose between buying all the parts, buying some parts or even no parts of their (future) financial malware scheme? And how does a criminal (organisation) chose not to buy but to actually sell parts of a financial malware scheme to others, perhaps even potential competitors?

Just like a regular business, the criminal business that aims for the most profit is one that strives towards the most effective business model, with low operational costs and an optimised net gain. In such an effective model, decisions have to be made on whether to organise specific tasks within the criminal organisation itself or to ‘outsource’ these to others. The choice of outsourcing can be seen as an economics-motivated deliberation on, for instance, the frequency of this outsourced task and the specificity of this task (Dick 1995). In other words, how frequent are the outsourced tasks needed, how specific can the task be described and is this sufficient information to deliver this task as a service to the client in question? For example, a botnet needed to spread malware can be argued to be both specific and frequently used, whereas spear phishing a bank employee to infect computers with remote access tooling (RAT)[6] to hack into, until then, unknown internal bank systems is lacking both this frequency and sufficient specificity. In consequence, the latter is less likely to be outsourced, as the costs do not outweigh the potential benefits. These decisions based on the intrinsic transaction costs form the basis of the consonant field of economics (Williamson 1971, 1979). Such perspective is essential, as the total malware ecosystem in terms of value chains consists of numerous (outsourced) parts, where underlying decisions—or, formulated in more economic terms, incentives—form an important part of this generic build-up of parts in an individual financial malware scheme.

Transaction Cost Economics in Offline Crime

Originally aimed at contract law, so-called transaction cost economics sets out economic principles on and identifies incentives for companies (sub)contracting each other for goods

[6] Remote access tooling is software that allows a remote ‘operator’ to control a system, e.g. a computer, as if they have physical access to that system. In that way, the operator can have unlimited access to the computer without being in physical contact with that system.

and services (Williamson 1971, 1979, 2005). This is, in contrast to keeping all activities in-house, so-called vertical integration. The term 'vertical integration' refers to a company who mainly relies on its internal workforce, in contrary to the company who mainly relies on contracted third parties for goods and services needed in the business (Whinston 2003). In his work on transaction cost economics, Williamson (1971, 1979) describes these different organisational structures on the basis of transaction costs that accompany this differentiation in structures, resulting in a series of institutional implications, such as:

> "As uncertainty increases (…) transactions will either be standardized, and shifted to the market, or organized internally." (Williamson 1979, p. 259)
>
> "As generic demand grows and the number of supply sources increases (…) vertical integration may give way to obligational market contracting, which in turn may give way to markets." (Williamson 1979, p. 260)

These propositions imply that, when goods or services involved in a transaction can be described as frequent, standardised and do not require highly specialised know-how or skill, these transactions will take place in the market and will not be vertically integrated.

As described above, most of the literature on the economics of organised crime has been focusing on its market structure. In older but still relevant work by Abadinsky (1987) and Reuter (1983), next to more recent work of Garoupa (1997, 2007) and Turvani (1997), the importance of transaction costs with regard to the (illegal) activities of a criminal organisation have become mainstream in the economics of organised crime. More specifically, Turvani (1997) points out that, as most of the activities of a criminal organisation are generally illegal, the regular structure of a market economy cannot see to a trustworthy system of transaction monitoring. On underground markets, reviews, like trust in other shadow economies, are, therefore, a direct substitute for the absence of this transaction monitoring system (D'Hernoncourt and Méon 2012; Holt et al. 2015). However, a viable business relationship is still hard to establish, factoring in this absence of such a solid transaction monitoring system. This is, for example, the reason why large drug deals often result in rip-offs, because both the drugs and the payment have to be at the same time and place to allow for an immediate exchange of goods.

In a more prominent paper, Dick (1995) developed a comprehensive analytical framework in which he shows that transaction costs and not a form of monopoly power, as argued before, primarily determine the (illegal) activities of crime in an organised structure. The paper predicts that, when there is a production cost advantage in a specific illegal activity, organised crime regarding that illegal activity will be more successful (Dick 1995). When looking at the question Dick asks himself—when does organised crime pay?—he starts with the perspective Williamson laid down. He formulates the hypothesis based on the perspective "that organized crime's activities will be guided primarily by the relative costs of completing illegal transactions within the market versus a downstream firm" (Dick 1995, p. 28). With Williamson as a starting point, he focuses on: (a) is the activity suitable for 'large scale production'?; (b) how specific can the accompanied transaction be described?; and (c) what is the frequency wherein this transaction would take place? Next, he adds a crucial fourth factor: uncertainty. Compared to legal markets, their illegal counterparts do not have a reliable system of enforcement of transactions and lack the accurate estimation of reputation on such a market (Dick 1995). In turn, this creates an incentive to not only assume the production cost advantage of outsourcing, let's say money-mule recruitment, but also incorporating the risk of uncertainty inherent to the specific transaction. In the case of money-mule recruitment, this would be the more general notion of the transaction itself—do I get scammed?—and the more specific notion of the risk of having undercover police informants pose as mules or the scenario wherein the mules have already flagged bank accounts and are, therefore, all but useful.

Economics of Financial Malware

To help discern value chains in financial malware, the transaction cost economic approach is undeniably very useful. We have briefly shown that financial malware schemes exist of different elements and that many of these parts are purchasable on underground markets (Sood et al. 2013a). Using the transaction cost economic perspective, we illustrated how different incentives have an influence on the choice between 'doing-it-yourself' or 'outsourcing,' not only in legitimate but also in illegitimate business. Whereas organised crime has been the main subject of these illustrations, cybercrime, e.g. financial malware, arguably lends itself even more for this perspective. The underground market is blooming, easily accessible, but above all, nearly anonymous. Which poses the obvious risks of scams, but also allows for a relatively low-risk entry to the market. And with the addition of reliable reputation mechanisms, making headway for traditional criminal reputation behaviour, even potentially diminishing the available options of disrupting such a 'dark network' (McBride and Hewitt 2013). Before we can, however, look at financial malware from a transaction cost economic perspective, we have to look in some more detail to our approach of using the state-of-art of existing research on parts of the total malware ecosystem to discern novel value chains in financial malware.

Approach

The following sections of this paper represent the necessary steps towards the actual discernment of the novel value chains in financial malware we present in section IV. To provide insight into the used methodology, we describe our approach in the remaining part of this section. First, we clustered and conceptually synthesised literature on financial malware in specific parts of the total financial malware ecosystem. Herein, we followed the clustering by Sood et al. (2013a). The literature we included in this clustering has been published between 2000 and 2015, is available on Web of Science and has financial or banking malware as keywords. Next, we included literature with keywords related to the concepts per clusters, such as 'infections' or 'botnet,' albeit related to the general keyword of financial/banking malware. Thereafter, we analysed the overview of the literature, identifying gaps and the extent to which a total view of the financial malware ecosystem based on the existing literature can be given. This literature overview thereby served the research goals of discerning the value chains in current-day financial malware schemes and its economic foundation. Next, we used the research into financial malware in relation to the underground market to extrapolate the different underground market alternatives per cluster. In this way, we shed light on the contrast of self-organising, i.e. vertically integrating, and using underground commodities, i.e. outsourcing. To look at the different current-day practices in financial malware schemes, we used prominent security blogs and reports by security firms. A differentiation in financial malware schemes can be constructed based on the distinguished current-day practices. This differentiation then formed the basis of extricating the novel value chains of these financial malware schemes, wherein we described the specific parts that make up every value chain.

Table 1 Example of a value chain from a transaction cost economic perspective

Value chain	Scale	Specificity	Frequency	Certainty
Example	—	−	+	++

Hereafter, we apply the framework proposed by Dick (1995) to analyse (the different elements of) every value chain from a transaction cost economic perspective (see Table 1).

Finally, we therewith can identify the incentives for vertically integrating per value chain. This results in an answer to the question of which elements of a financial malware scheme are most likely to be either vertically integrated or shifted to the underground market. Last, we leverage these answers to conclude on potential chokepoints in financial malware schemes, accompanied by potential intervention strategies and possible future research efforts.

Research on Financial Malware

State-of-the-art

As stated earlier in this paper, the total puzzle of the malware ecosystem has been recently researched by its separate pieces. Looking not only at separate pieces, but at the entire puzzle, will allow us to assess the different elements of the total malware ecosystem in an integral manner. This integral view will enable us to discern, based on the economics of cybercrime discussed in sections II and III, novel value chains in financial malware. Before we can actually connect the pieces to construct such value chains, we have to put the current state-of-the-art in research on these pieces in the right conceptual perspective, namely the perspective where the piece is located within the puzzle or, in this case, within the overarching financial malware ecosystem. By clustering the different pieces of research: (a) the total malware ecosystem, as previously studied in bits, bytes and pieces, will become apparent; (b) research gaps can be identified; and (c) actual value chains in financial malware can be distinguished.

From the mid-2000s onwards, mostly computer scientists, but to some extent also social scientists, have researched elements of the financial malware ecosystem. First, there are studies on the source code and crimeware toolkits.[7] Second, researchers also looked at how malware infections occur and in more detail who is most likely to be infected and how specific online behaviour influences these chances. Third, the infrastructure needed for the operation of financial malware is extensively studied, in particular banking botnets and its command and control (C&C) servers.[8] Fourth, the target-selecting mechanism that is being operated in the financial malware scheme, e.g. which bank to 'hit' and which not, is being researched. Fifth, the cash-out strategies[9] in financial malware are studied, wherein money mules form the most frequent object of study. Last, the underground markets in relation to financial malware are being separately researched, covering a wide array of studies into underground services.

[7] In this case, studies aimed at the understanding of the automation of malware source code and toolkits.

[8] Studies into the automation of the infrastructure supporting cybercrime, such as servers commanding and controlling computers in a botnet used as such an infrastructure.

[9] The term cash-out refers to activities enabling actors to access, remove and drain funds from bank accounts on- and offline (Holt and Smirnova 2014)

These specific parts have been identified before by Sood et al. (2013a) and presented as clusters in their work, aiming at "dissecting the state of the underground enterprise." If we follow their lines of analysis, and stick with the clusters we have described above, we can synthesise the state-of-the-art of research into parts of the financial malware scheme. The studies in each cluster make up a range of divergent concepts as research objects. These concepts are presented in the far right column of Table 2.

In Fig. 1, we see the clusters of the state-of-the-art of research on financial malware mapped on the previously mentioned parts of the financial malware ecosystem. It is noticeable that much research effort was undertaken on the malware source code and the specific set-ups, i.e. crimeware toolkits. Next to the source codes and set-up part, the last couple of years has seen an increase in research interest in the infrastructure used in financial malware schemes, aimed both at the botnet itself as well as at the C&Cs. On the other hand, we can observe that the study of both malware infections and the cash-out strategy have been given little research attention. Moreover, when looking at research into target selection, we also see here that remarkably little study has been carried out.

Make or Buy?

More specifically, if we look at the identified parts of the financial malware ecosystem in Table 2, the literature on underground markets shows the alternatives for the outsourcing of these parts. These parts-for-sale form the underground market counterpart to the option of self-organising—or in the light of the previous sections, vertically integrating—which, as illustrated before, requires a significantly higher skill-set. Next to its function as a platform providing alternatives for vertically integrating, the underground market can be seen a facilitator in the search for co-criminals (Soudijn and Zegers 2012).

Table 3 shows that, for every part of the financial malware scheme, an underground alternative is available, based on the literature clustering on underground markets in relation

Table 2 State-of-the-art of research into parts of the financial malware scheme

Part of a financial malware scheme	Literature	Studied concepts
A. Crimeware (source code and set-up)	Alazab et al. (2012, 2013); Ben-Itzhak (2009); Binsalleeh et al. (2010); Boutin (2014); Criscione et al. (2014); Garcia-Cervigon and Llinas (2012); Riccardi et al. (2013); Sood and Enbody (2013)	Malware source code typologies; crimeware; cybercrime toolkits; web injects
B. Infections (victimisation)	Bossler and Holt (2009); Holt and Bossler (2013)	Victimisation risk; online routine activities
C. Infrastructure	Gañán et al. (2015); Neugschwandtner et al. (2011); Oro et al. (2010); Park et al. (2014); Riccardi et al. (2010); Watkins et al. (2014)	Botnet (detection); command and control servers (lifespan)
D. Target selection	Florêncio and Herley (2013); Ronchi et al. (2011); Tajalizadehkhoob et al. (2014)	Threat model; attack selection; attack vectors
E. Cash-out	Aston et al. (2009); Florêncio and Herley (2010)	Money mules; cash-out strategies
X. Underground markets	Caballero et al. (2011); Christin (2013); Grier et al. (2012); Holz et al. (2009); Miller (2007); Motoyama et al. (2011); Rossow et al. (2013); Sood et al. (2013b); Stevens (2009); Zhuge et al. (2009)	Cybercrime/financial malware-as-a-service

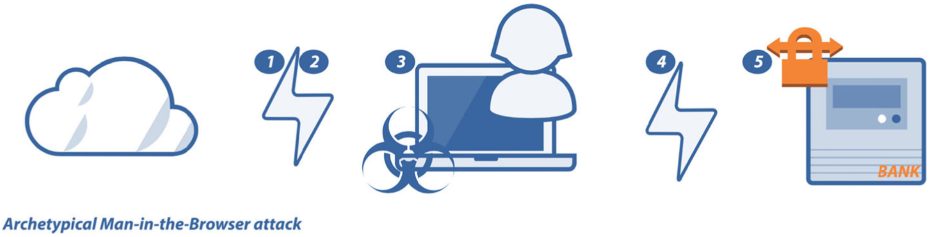

Fig. 1 Archetypical man-in-the-browser attack

to financial malware. In a typical financial malware scheme, the choice exists of, for instance, using in-house malware developers or an existing crimeware toolkit bought via an underground market. The same choice exists in every other cluster, ranging from choosing between setting up your own botnet and spreading malware or renting out an infrastructure and using a pay-per-install service to recruit your own money mules or using an underground cash-out service. But do all these specific underground alternatives get used in the same composition every time? Or form the same scheme in every instance? And which of the parts tend to be most likely serviced by an underground service provider?

Archetypical Value Chain

A first value chain in financial malware we can discern is the chain associated with the established and well-researched man-in-the-browser attack. An average citizen, using online banking like many others, first comes into contact with this financial malware scheme when ordinarily browsing the internet or checking up on email. In hindsight, we know that the criminal has then already set up the first two parts of the scheme, consisting of: (1) the source code and/or crimeware kit of the specific banking malware or Trojan and (2) the infrastructure supportive to the specific malware. These both leverage vulnerabilities in, for example, internet browsers like Internet Explorer or malicious websites, to (3) infect these potential victims with the financial malware in question. However, this malware only becomes operational under two conditions: one, the bank which the infected client is using has to be specifically targeted (4) by the cybercriminals and two, the infected client must use the internet browser in which the malware exploits a vulnerability. When the infected client then uses his or her browser for online banking with the specifically targeted bank, the cybercriminals use their man-in-the-browser attack to near-automatically take over the active banking session to change amounts and bank routing numbers to wire funds to bank accounts under their (in)direct control. Last,

Table 3 Parts of a financial malware scheme and available underground alternatives

Part of a financial malware value chain	Underground alternative
Crimeware (source code and set-up)	Exploit-as-a-service; crimeware-as-a-service; source code for sale/free; exploit kits
Infections	Pay-per-install; drive-by downloads
Infrastructure	Botnet lease; C&C rent
Target selection	Payload, web inject/config files for sale
Cash-out	Money mule recruitment services; bitcoin exchanges; gift cards; prepaid credit cards

the funds stolen will be (5) cashed-out primarily by money mules using ATM withdrawals or the purchasing of high-end or luxury consumer goods. Figure 1 shows this man-in-the-browser attack in some more detail.

Ongoing Developments in Financial Malware Schemes

When we look at publications by known security firms and respected security blogs, we can see that a differentiation in attacks is to observed. First, we still see a continuing momentum of man-in-the-browser attacks with evolving modus operandi and ever more sophisticated set-ups.[10] Next, there is a shift observable to increasingly manual and, thereby, more dynamic, instead of automated, web injects to execute these attacks in the web browser. Furthermore, we see a similar shift to the mobile browser and/or platform as an attack vector.[11] These attacks are both scalable as to some level standardised, allowing on the one hand for a higher frequency of attacks but on the other hand are not, per se, suitable for a more targeted approach. Second, we can distinguish a fairly new trend, wherein criminals use RAT to target small- and medium-sized businesses (SMEs).[12] In this manner, they infect, via spear phishing, business computers, to observe the internal banking or accounting systems. When the criminals have complete insight into the company's financial systems, they hit. For instance, manipulating salary batches that the HR department generates using their financial systems. Then, the salary batch is executed by the bank, like they normally do. The only difference being that not the employees but the criminals get their (monthly) pay. As the pay is high and criminals are moving on to other companies, the eventual detection of the fraud is to be seen as relatively insignificant. Third and last, we note the similar use of RAT not, however, aimed at businesses to get to their bank accounts, but aimed at the banks themselves. Therein, the same modus operandi is used, namely, infecting, in this case, bank employee's computers with RAT via spear phishing in order to gain insight of and control over crucial internal banking systems. Once the compromised systems are that familiar to the criminals, they hit. Most famously, the case of Carbanak or Anunak illustrates this scheme as being highly targeted and professionally executed, with estimations of up to hundreds of millions of dollars in loot.[13]

[10] https://blog.kaspersky.com/the-big-four-banking-trojans/
http://krebsonsecurity.com/2015/02/fbi-3m-bounty-for-zeus-trojan-author/
http://newsroom.kaspersky.eu/en/texts/detail/article/kaspersky-lab-discovers-chthonic-a-new-strain-of-zeus-trojan-targeting-online-banks-worldwide/
http://blog.trendmicro.com/trendlabs-security-intelligence/new-banking-malware-uses-network-sniffing-for-data-theft/

[11] http://blog.trendmicro.com/trendlabs-security-intelligence/german-users-hit-by-dirty-mobile-banking-malware-posing-as-paypal-app/
http://www.americanbanker.com/issues/179_114/first-major-mobile-banking-security-threat-hits-the-us-1068100-1.html
https://securelist.com/blog/research/57301/the-android-trojan-svpeng-now-capable-of-mobile-phishing/
https://securityintelligence.com/svpeng-mobile-malware-expanding-to-new-territories/

[12] https://www.europol.europa.eu/content/users-remote-access-trojans-arrested-eu-cybercrime-operation
http://krebsonsecurity.com/2014/05/blackshades-trojan-users-had-it-coming/
http://www.symantec.com/connect/blogs/blackshades-coordinated-takedown-leads-multiple-arrests
https://www.europol.europa.eu/content/major-cybercrime-ring-dismantled-joint-investigation-team
http://securityintelligence.com/cybercrime-ecosystem-everything-is-for-sale/

[13] http://usa.kaspersky.com/about-us/press-center/press-releases/2015/great-bank-robbery-carbanak-cybergang-steals-1-billion-100-fina
https://www.fox-it.com/en/about-fox-it/corporate/news/anunak-aka-carbanak-update/
http://krebsonsecurity.com/2015/02/the-great-bank-heist-or-death-by-1000-cuts/

Even though the last two trends both use more generic malware type RAT, albeit fine-tuned to their specific use, in contrast to the more specialised financial malware used in the first trend, all three show the overall variation of financial malware schemes, whereas in this case malware targeting financial institutions (in)directly is more suitable. Knowing this variation in schemes takes us back to the original question we asked ourselves. How does a criminal choose between organising the tasks in a financial malware scheme themselves, thus vertically integrating the entire operation, or outsourcing (parts of) their total scheme? Only when we look at attackers, victims and targets in a holistic way can we observe economic mechanisms per type of financial malware scheme. This requires an integral approach through value chains, based on the previously explained economic perspectives on organised (cyber)crime.

Discerning Novel Value Chains

New Financial Malware Value Chains

With the overview of both the state-of-the-art of research in financial malware as well as the three presented differentiations in today's financial malware practices, we can leverage these insights to discern the novel value chains behind those practices. Conforming with previous studies that examined the value chain behind spam, we present the three value chains in today's financial malware practice in the same step-by-step manner (Levchenko et al. 2011; Thomas et al. 2015). Next, using the transaction cost economic model we presented previously in the context of (financial) cybercrime, we can unravel the intrinsic incentives of both outsourcing as well as vertically integrating per value chain. In this instance, we look at the elements of the value chain and apply the framework of Dick (1995). Finally, we can hypothesise how the underground market will be involved as the 'market-of-choice' when not vertically integrating and, thus, using market resources to operate an individual financial malware scheme.

Novel Value Chain 1: Untargeted Consumer-oriented Man-in-the-browser Attack

The first novel value chain in financial malware that we can discern is the chain associated with the already well-known man-in-the-browser attack. With reference to the described developments in this type of attack, we see a slightly different chain compared to the archetypical one. This novel chain uses similar steps as its established counterpart (see Fig. 2).

However, the operated crimeware kit (1) in this case allows the attacker to use dynamic web injects instead of fully automated versions. The infections (2) are identical

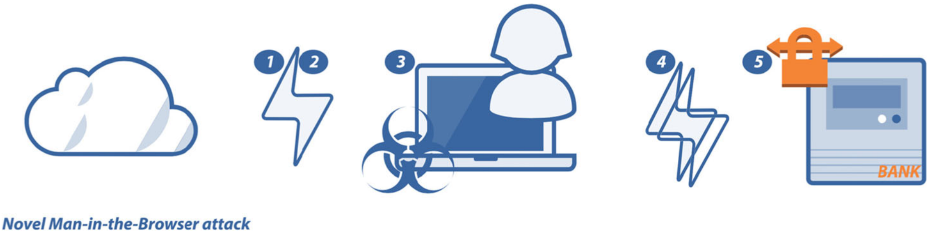

Fig. 2 Novel man-in-the-browser attack

to the other type of man-in-the-browser attacks. Moreover, the infrastructure (3) has to be set up for these dynamic web injects, having human-operated scripts to change the web inject from attack to attack. Again, the malware only becomes operational under two conditions: one, the bank that the infected client is using has to be specifically targeted (4) by the cybercriminals and two, the infected client must use the internet browser in which the malware exploits a vulnerability. When both these conditions are met, the attackers infiltrate the active banking session with a dynamic web inject, varying from pop-up windows for additional login to creating extra fields in a form. This creates the necessity of an actual human operator to execute these dynamic types of attack. Again, the objective is to manipulate the banking session in such a manner that money is transferred to bank accounts controlled by the cybercriminals, without raising suspicion in the active session. Like the more static man-in-the browser attacks, the funds stolen will be (5) cashed out primarily by money mules using ATM withdrawals or the purchasing of high-end or luxury consumer goods. Figure 3 shows these more dynamic man-in-the-browser attacks and their resources from a value chain perspective.

Novel Value Chain 2: Semi-targeted SME-oriented RAT Attack

The second discernable value chain is that of a financial malware scheme using RAT to target SMEs (Fig. 4).

Unlike to the first novel chain, wherein the chances of getting infected are to say fairly random, here the first contact the potential victims have with the financial malware scheme is nearly always a semi-targeted (1) spear phishing attempt. With this method, the criminals single out employees at exploitable positions in the targeted companies, such as the financial administration. Once the often-infected attachment to the spear phishing email has been opened, (2) the RAT source code and/or crimeware kit already in place then has control over the (3) infected client. The criminals, with the RAT having unrestricted access to the infected client, can observe the internal (financial) systems of the targeted SME and spend some time getting familiar with the day-to-day financial practices of the company. By the time they have a full and profound understanding of the systems and know its potential exploitability, they target a (4) specific process in the system. For example, they manipulate salary batches so they get paid instead of the company's employees. Like the other value

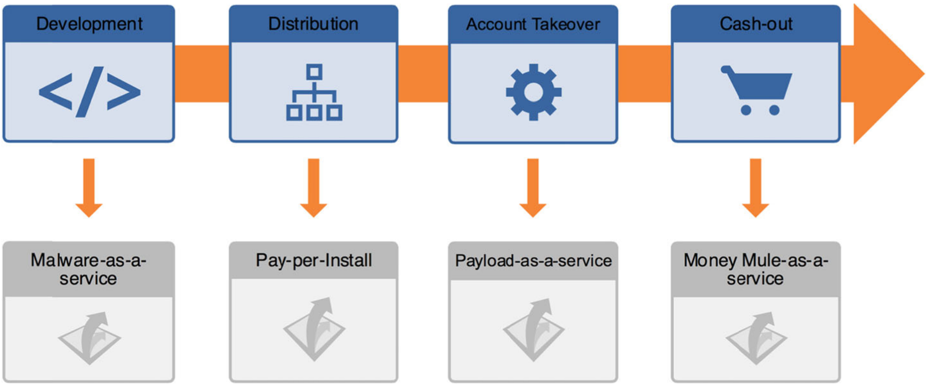

Fig. 3 Value chain of resources of an untargeted consumer-oriented man-in-the-browser attack

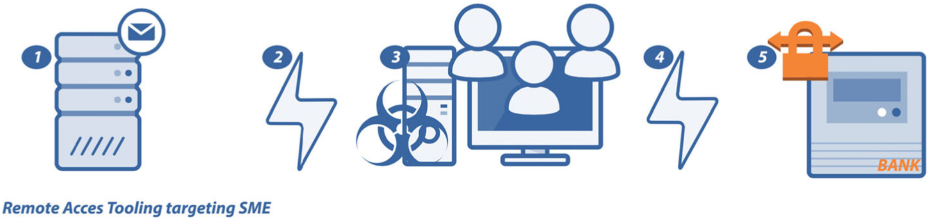

Fig. 4 Remote access tooling (RAT) targeting small- and medium-sized businesses (SMEs)

chains, the last step in the scheme is the (5) cash-out strategy involving money mules to get the stolen money to the criminals. Figure 5 shows the resource value chain of semi-targeted SME-oriented RAT attacks.

Novel Value Chain 3: Targeted (Financial) Business-oriented RAT Attack

The third and last novel value chain that can be discerned is the chain that, like the previous one, uses RAT, but instead of SMEs, this financial malware scheme involves the targeting of banks directly (Fig. 6).

The first three steps of the chain are identical to novel value chain 2, with the difference, of course, that the (1) spear phishing emails are, in this case, sent to singled-out bank employees at exploitable positions within the bank's internal hierarchy and the (2) RAT thereafter is active on the (3) infected clients within the bank. Again, like the second novel value chain, the criminals first observe the complex internal systems and seek exploitabilities. However, in this case, the cybercriminals operating such a scheme are not in it for the quick buck, but for the long run. Having undetected and unrestricted access to internal bank systems is a potential gold mine. Once they have found ways in which they can (4) manipulate the internal banking systems, they shift from observing to acting. The infected clients are used to authorise transactions, create back-to-back loans, hand out mortgages without underlying pledges or trick ATMs in thinking they have a withdrawal. In contrast to the other two value chains, this chain does not primarily rely on money mules as parts of the cash-out strategy. Criminals who have been operating such a scheme relied on the (5) bank systems themselves as their most prominent source of cash-out, ranging from the use of ATMs (the famous example

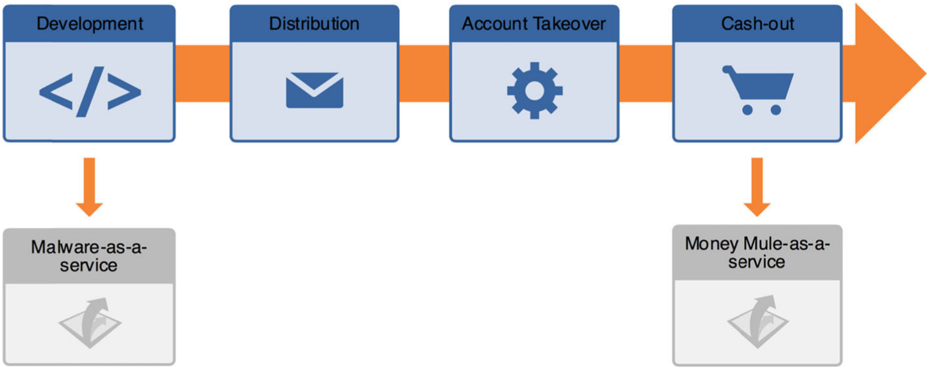

Fig. 5 Value chain of resources of a semi-targeted SME-oriented RAT attack

Fig. 6 RAT targeting banks

of ATMs spitting out money on cue) or setting up accounts whereof the bank thinks they do not exist or simply erasing transactions after they have been executed from the bank systems. Figure 7 shows the resource value chain of a targeted (financial) business-oriented RAT attack.

Incentives for Shifting to the (Underground) Market

Now that we have a view of the three different novel value chains in current-day financial malware schemes, we can apply the framework proposed by Dick (1995) to unravel the underlying incentives per chain. The goal of this application is to analyse how the different components of the value chain are suited to be organised within the criminal organisation. Thus, vertically integrating or to be shifted to the market, making use of the vast amount of the earlier described 'underground market alternatives'. With the last option comes the inevitable financial transaction to be made between the criminal organisation and the underground market salesman. As elaborated upon in section II, the transactions characteristics are, in this case, deal-maker or deal-breaker in shifting a specific activity to the market. The analysis of these characteristics form the basis of the framework contemplated by Dick (1995). His framework consists of the following elements: (a) is the activity suitable for 'large scale production'? (b) how specific can the accompanied transaction be described? (c) what is the frequency wherein this transaction would take place? and (d) what is the uncertainty of the transaction? If we map out the different elements of this framework on the three discerned value chains, we can build the following overview (Table 4).

Novel Value Chain 1: Untargeted Consumer-oriented Man-in-the-browser Attack

Looking at the first novel value chain, the first three elements (source code/crimeware kit, infrastructure and infections) score some positive points on the different components of the framework. Starting with the scale, we have shown that man-in-the-browser attacks rely primarily on infections in bulk, accompanied by, thus, a large infrastructure of infected clients. Next, the activities in the first elements can be described very specifically due to the standardised way of operation and the high availability of the most popular banking malware

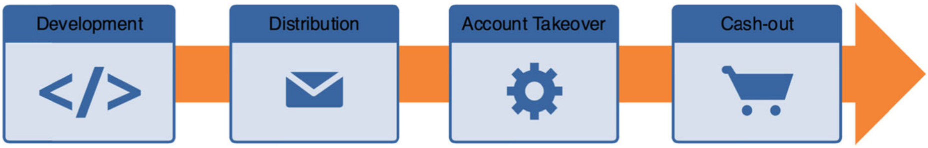

Fig. 7 Value chain of resources of a (financial) business-oriented RAT attack

Table 4 Overview of the discerned value chains from a transaction cost economic perspective

Value chain	Scale	Specificity	Frequency	Certainty
1. Man-in-the-browser	++	+	+	+/−
2. RAT → SME	+/−	−	−	+/−
3. RAT → bank	—	—	—	—

toolkits that almost all man-in-the-browser financial malware schemes use. In turn, the interplay between attackers and defenders, i.e. banks and software developers closing security gaps, creates the necessity of updating the more static parts of the man-in-the-browser financial malware scheme, resulting in more frequent transactions on activities such as crimeware toolkits and infections. Moreover, all these activities are common commodities available on the underground market and, therefore, almost guarantee a continuous supply of these activities. As a consequence of potentially doing business with underground market salesmen, the risk of being scammed—the uncertainty of the transaction—is evident. However, in the case of activities being sold by the dozen, by a wide range of sellers and, in most cases, with an Amazon-like review system in place, the uncertainty is, to a large extent, downplayed or sometimes even neutralised. This results, for these three elements, source code/crimeware kit, infrastructure and infections, in an incentive to shift these specific activities to the (underground) market. However, the development of using more dynamic web injects instead of automated ones, relying on personal interaction and therewith human operators, has the side effect of diminishing part of the specificity and, thereby, scale needed for potential outsourcing. Time will tell whether or not we see an ongoing process of shifting from outsourcing back to vertical integration in these man-in-the-browser attacks.

Yet, the elements of target selection and cash-out are somewhat different in relation to the other elements in the first value chain. For target selection, config files are used that instruct the malware to become active when visiting certain predetermined online banking environments, based on the specific domain name of the bank in question. These config files often come with the crimeware toolkit and are not frequently sold separately. The same goes for money mules in the cash-out strategy, which, in turn, are not being sold by the bulk as frequently as, for instance, in the flourishing pay-per-install market. It can be argued that, maybe, these activities are both too valuable and too scarce and, therefore, not sold as much as other commodities. Acquiring and aligning these parts for your own financial malware schemes seems to be hard enough, let alone selling these on the underground market. In this case, it is not merely the low incentive to shift these activities to the market as it is the lack of a stable underground market alternative preventing in doing so. As a result, both these elements form potential chokepoints in the man-in-the-browser value chain, thereby creating new possibilities for interventions aimed at these elements.

Novel Value Chain 2: Semi-targeted SME-oriented RAT Attack

Moving on to the second novel value chain, we can observe a nearly mirrored mapping on the different components of the framework. As we have demonstrated before, financial malware schemes using RAT coincide with a more targeted approach. The scaling thus depends on the size of the criminal organisation operating such a scheme, as well as the targeted companies in terms of expected return-on-investment. Whereas the man-in-the-browser scheme uses scale to make itself profitable, the schemes using RAT focusing on SMEs start out at least low in scale.

However, to go for the bigger score per attack takes time, thus lowering the scale of the scheme but, on the other hand, increasing the reward per attack to maximise the profitability. Using spear phishing for a RAT infection is, to some extent, a standardised routine, but the activities carried out after the infection—the observation and identification of potential cash cows in unknown internal financial systems—is not to be called 'specific,' therefore, resulting in a lower specificity of the activity to be described on the forehand. Logically, this is also not a high-frequency activity, more a high-intensity activity, albeit that the RAT itself is such a prevailing commodity that it is actually available for free both on the dark as on the clear web. So, in conclusion, next to the RAT itself, there is little incentive to shift the other specific activities in a financial malware scheme using RAT targeting SMEs to the (underground) market.

Novel Value Chain 3: Targeted (Financial) Business-oriented RAT Attack

Last, with regard to the third novel value chain, we can see a similarly mirrored mapping on the different components of the framework compared to the first value chain. Like the second novel value chain, this chain encompasses a financial malware scheme with a (highly) targeted approach. Again, the scaling depends on the size of the criminal organisation operating such a scheme as well as, in this case, the continuous and patient efforts to exploit the targeted bank in the long run. With a scheme targeting banks, the rewards can be dazzling if the scheme operates under the radar of security measures implemented at the targeted bank. This requires being able to alter the modus operandi at least from day to day and perhaps even from hour to hour. That intrinsically creates such an unspecific and infrequent but highly intensive activity that even the possibility of actually considering shifting this activity to the underground market is likely to be absent. With shifting this activity to the underground market also comes the revealing of a maybe very lucrative financial malware scheme to potential competitors. All in all, next to maybe the RAT itself, the conclusion is that there is no incentive to shift the other specific activities in a financial malware scheme using RAT targeting banks to the (underground) market.

Conclusion

The still evolving current-day financial malware schemes can be brought down to three novel value chains. We constructed these value chains based on the conceptual synthesis of the state-of-the-art of the literature on financial malware and the known differentiations in financial malware schemes. A framework of transaction cost economics was used to analyse the incentives that influence decisions within such a value chain to either vertically integrate or outsource specific parts. Combined with the notion of an increase in underground market activity, this illustrates the interweaving of underground commodities in financial malware schemes operated by cybercriminals.

The goal of this paper was to integrate the literature on financial malware, underground markets and (cyber)crime economics, as well as today's banking practice, to discern novel value chains in financial malware. These value chains were constructed in a similar fashion to how other researchers reconstructed the spam value chain. The constructed value chains, aided by the framework of Dick (1995), allowed us to analyse the economical principles within the underlying criminal business models. This resulted in the answering of the question of which elements of a financial malware scheme are most incentivised to be either vertically integrated or shifted to the underground market. We demonstrated that, for financial malware schemes using man-in-the-browser attack vectors, there is a clear incentive to shift (parts) of this scheme to the underground market, in contrary to financial malware schemes that rely on remote access tooling (RAT), although the development of a more dynamic and human operation tends to diminish part of these economical incentives to outsource. Next, we believe that, in our approach, we have shown that a transaction cost economic approach is greatly beneficiary to the series of existing economic perspectives on cybercrime in general and on financial malware schemes in particular. This approach generates new insights as it comes to understanding cybercriminals' operating criminal schemes and doing business with other (cyber)criminals in an underground market. We laid down the deliberative considerations and actions that accompany the shifting of a part of a financial malware scheme to the (underground) market, thereby proving the potential of underground markets in kick-starting the opportunity to operate a financial malware scheme.

Furthermore, by conceptually synthesising the state-of-the-art of the literature in financial malware, we have, next to an overview of the current research efforts, also identified research gaps in financial malware research. Moreover, we have made evident that a value chain approach will be of added value when researching financial malware (schemes) or underlying business models of those who operate it. This creates the opportunity to study the important interactions between the strategies of attackers on the one side and the properties and policies of the financial service providers on the other.

Finally, we came to conclude on the different incentives that are apparent in the different value chains. In turn, these incentives can be used to analyse chokepoints in the value chain. More specifically, if the scarcity of one activity in particular on the underground market influences those incentives, chokepoints derived from these incentives are vital to future interventions. Based on these chokepoints, not only interventions for financial services or security providers but also for, perhaps even more importantly, law enforcement purposes can be developed.

Future Work

Analyse Chokepoints in Financial Malware Value Chains

We briefly touched upon the potential chokepoints that exist within the different novel value chains in financial malware. Concluding that these chokepoints can form the basis of a better understanding of where potential interventions can have the greatest chance of success, more research into validating these chokepoints is a logical first step. New or renewed research efforts should, therefore, focus on further advancing the value chain approach and seek to identify relationships between parts of the value chains and chokepoints.

Based on Chokepoints: Evidence-based Intervention Strategies for Financial Malware Schemes

The next step is to study how the actionable intelligence that these chokepoints create can be used to create evidence-based intervention strategies for financial malware. Identified chokepoints would provide an excellent opportunity to study how (new) interventions in one part of the value chain affect the other parts. Understanding these interactions would enable creating better countermeasures and new security services, idealistically making the underlying business models of financial malware less or unprofitable.

Address Identified Research Gaps in Separate Studies (Target Selection and Cash-out Strategies)

As we have demonstrated in section IV, the state-of-the-art of the literature in financial malware is somewhat confined to a couple of specific clusters. Notable is that research efforts on target selection mechanisms and cash-out strategies were relatively absent. Although there can be a very good reason for this absence, we see the significance of studying these parts of the financial malware ecosystem. In the analysis in section V, we have seen that these parts of the chain strikingly form potential chokepoints and, thus, have our special (future) research interest.

References

Abadinsky, H., (1987). The McDonald's-ization of the Mafia. In T. S. Bynum (Ed.), *Organized crime in America: concepts and controversies* (pp. 43–54). Monsey, NY: Willow Tree Press.

Afroz, S., Garg, V., McCoy, D., & Greenstadt, R., (2013). Honor among thieves: a common's analysis of cybercrime economies. eCrime Researchers Summit (eCRS), pp. 1–11.

Alazab, M., Venkatraman, S., Watters, P., Alazab, M., & Alazab, A. (2012). Cybercrime: the case of obfuscated malware. In R. Bashroush (Ed.), ICGS3/e-Democracy 2011, LNICST 99, pp. 204–211.

Alazab, A., Abawajy, J., Hobbs, M., Layton, R., & Khraisat, A. (2013). Crime toolkits: the productisation of cybercrime. IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1626–1632.

Anderson, R. (2008). Security engineering: a guide to building dependable distributed systems. John Wiley & Sons.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science*, *314*(5799), 610–613.

Anderson, R., Barton, C., Boehme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime. Workshop on the Economics of Information Security.

Aston, M., McCombie, S., Reardon, B., & Watters, P. (2009). A preliminary profiling of internet money mules: an Australian perspective. Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing.

Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*, 706–719.

Becker, G. S., (1974). Crime and punishment: an economic approach. In G. S. Becker, & W. M. Landes (Eds.), Essays in the economics of crime and punishment, pp. 1–54.

Ben-Itzhak, Y. (2009). Organised cybercrime and payment cards. *Card Technology Today*, 21, 10–11.

Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., & Wang, L. (2010). On the analysis of the Zeus botnet crimeware toolkit. International Conference on Privacy, Security and Trust.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: an examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400–420.

Boutin, J.-I. (2014). The evolution of webinjects. Virus Bulletin Conference.

Caballero, J., Grier, C., Kreibich, C., & Paxson, V. (2011). Measuring pay-per-install: the commoditization of malware distribution. Usenix Security Symposium.

Christin, N. (2013). Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace. World Wide Web, pp. 213–224.

Criscione, C., Bosatelli, F., Zanero, S., & Maggi, F. (2014). Zarathustra: extracting webinject signatures from banking trojans. Annual Conference on Privacy, Security and Trust.

D'Hernoncourt, J., & Méon, P.-G. (2012). The not so dark side of trust: does trust increase the size of the shadow economy? *Journal of Economic Behavior & Organization*, *81*(1), 97–121.

Dick, A. R. (1995). When does organized crime pay? a transaction cost analysis. *International Review of Law and Economics*, *15*(1), 25–45.

European Central Bank (2015). Fourth report on card fraud. https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf. Accessed 23 Dec 2016.

Florêncio, D., & Herley, C. (2010). Phishing and money mules. International Workshop on Information Forensics and Security (WIFS).

Florêncio, D., & Herley, C. (2013). Where do all the attacks go? In B. Schneier (Ed.), Economics of information security and privacy III (pp. 13–33). New York: Springer.

Gañán, C., Cetin, O., & van Eeten, M. (2015). An empirical analysis of ZeuS C&C lifetime. ACM Symposium on Information, Computer and Communications Security, pp. 97–108.

Garcia-Cervigon, M., & Llinas, M. M. (2012). Browser function calls modeling for banking malware detection. International Conference on Risk and Security of Internet and Systems (CRiSIS).

Garoupa, N. (1997). The economics of organized crime and optimal law enforcement. Annual Conference of the European Association of Law and Economics.

Garoupa, N. (2007). Optimal law enforcement and criminal organization. *Journal of Economic Behavior & Organization*, *63*, 461–474.

Grier, C., Ballard, L., Caballero, J., Chachra, N., Dietrich, C. J., Levchenko, K., Mavrommatis, P., McCoy, D., Nappa, A., Pitsillidis, A., Provos, N., Rafique, M. Z., Rajab, M. A., Rossow, C., Thomas, K., Paxson, V., Savage, S., & Voelker, G. M. (2012). Manufacturing compromise: the emergence of exploit-as-a-service. ACM Conference on Computer Communications Security.

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420–436.

Holt, T. J., & Smirnova, O. (2014). Examining the structure, organization, and processes of the international market for stolen data. National Institute of Justice: US Department of Justice. https://www.ncjrs.gov/pdffiles1/nij/grants/245375.pdf. Accessed 23 Dec 2016.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81–103.

Holz, T., Engelberth, M., & Freiling, F. (2009). Learning more about the underground economy: a case-study of keyloggers and dropzones. Computer Security—ESORICS.

Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011). The dark side of the internet: attacks, costs and responses. *Information Systems*, *36*, 675–705.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: online innovation in the shadows? *Technological Forecasting and Social Change*, *80*, 541–555.

Kugler, M., Verdier, T., & Zenou, Y. (2005). Organized crime, corruption and punishment. *Journal of Public Economics*, *89*, 1639–1663.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58–74.

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D., Weaver, N., Paxson, V., Voelker, G. M., Savage, S. (2011). Click trajectories: end-to-end analysis of the spam value chain. IEEE Symposium on Security and Privacy. IEEE.

Levitt, S. D., & Dubner, S. J. (2005). Freakonomics: a rogue economist explores the hidden side of everything.

Levitt, S. D., & Dubner, S. J. (2009). SuperFreakonomics: global cooling, patriotic prostitutes, and why suicide bombers should buy life insurance.

Levitt, S. D., & Venkatesh, S. A. (2000). An economic analysis of a drug-selling gang's finances. *The Quarterly Journal of Economics*, *115*(3), 755–789.

Li, Z., Liao, Q., & Striegel, A. (2009). Botnet economics: uncertainty matters. In M. E. Johnson (Ed.), Managing information risk and the economics of security (pp. 245–267). New York: Springer.

McBride, M., & Hewitt, D. (2013). The enemy you can't see: an investigation of the disruption of dark networks. *Journal of Economic Behavior & Organization*, *93*, 32–50.

Miller, C. (2007). The legitimate vulnerability market: inside the secretive world of 0-day exploit sales. Workshop on the Economics of Information Security.

Moore, T. (2010). The economics of cybersecurity: principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*, 103–117.

Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *The Journal of Economic Perspectives*, *23*(3), 3–20.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011). An analysis of underground forums. ICM.

Neugschwandtner, M., Comparetti, P. M., & Platzer, C. (2011). Detecting malware's failover C&C strategies with SQUEEZE. Annual Computer Security Applications Conference, pp. 21–30.

Oro, D., Luna, J., Felguera, T., Vilanova, M., & Serna, J. (2010). Benchmarking IP blacklists for financial botnet detection. International Conference on Information Assurance and Security, pp. 62–67.

Park, C., Park, H., & Kim, K. (2014). Realtime C&C zeus packet detection based on RC4 decryption of packet length field. *Advanced Science and Technology Letters*, *64*, 55–59.

Rao, J. M., & Reiley, D. H. (2012). The economics of spam. *The Journal of Economic Perspectives*, *26*(3), 87–110.

Reuter, P. (1983). Disorganized crime: the economics of the visible hand. Cambridge, MA: MIT Press.

Riccardi, M., Oro, D., Luna, J., Cremonini, M., & Vilanova, M. (2010). A framework for financial botnet analysis. eCrime Researchers Summit (eCrime), pp. 1–7.

Riccardi, M., Di Pietro, R., Palanques, M., & Vila, J. A. (2013). Titans' revenge: detecting Zeus via its own flaws. *Computer Networks*, *57*, 422–435.

Ronchi, C., Khodjanov, A., Mahkamov, M., & Zakhidov, S. (2011). Security, privacy and efficiency of internet banking transactions. World Congress on Internet Security (WorldCIS), pp. 216–222.

Rossow, C., Dietrich, C., & Bos, H. (2013). Large-scale analysis of malware downloaders. International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment. Springer, pp. 42–61.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*, 28–38.

Sood, A. K., Bansal, R., & Enbody, R. J. (2013a). Cybercrime: dissecting the state of underground enterprise. In I.C. Society (Ed.), IEEE Internet Computing.

Sood, A. K., Enbody, R. J., & Bansal, R. (2013b). Dissecting SpyEye—understanding the design of third generation botnets. *Computer Networks*, *57*, 436–450.

Soudijn, M. R. J., & Zegers, B. C. H. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime, 15*(2–3), 111–129. doi:10.1007/s12117-012-9159-z.

Stevens, K. (2009). The underground economy of the Pay-Per-Install (PPI) business.

Stone-Gross, B., Abman, R., Kemmerer, R. A., Kruegel, C., Steigerwald, D. G., & Vigna, G. (2013). The underground economy of fake antivirus software. In B. Schneier (Ed.), Economics of information security and privacy III (pp. 55–78). New York: Springer

Tajalizadehkhoob, S. T., Asghari, H., Gañán, C., & van Eeten, M. (2014). Why them? Extracting intelligence about target selection from Zeus financial malware. Workshop on the Economics of Information Security (WEIS).

Thomas, K., Huang, D. Y., Wang, D., Bursztein, E., Grier, C., Holt, T. J., Kruegel, C., McCoy, D., Savage, S., & Vigna, G. (2015). Framing dependencies introduced by underground commoditization. Workshop on the Economics of Information Security (WEIS).

Turvani, M. (1997). Illegal markets and the new institutional economics.

van Eeten, M. J., & Bauer, J. M. (2008). Economics of malware: security decisions, incentives and externalities. OECD Science, Technology and Industry Working Papers.

Walker, S. (2012). Economics and the cyber challenge. *Information Security Technical Report*, *17*, 9–18.

Watkins, L., Kawka, C., Corbett, C., & Robinson, W. H. (2014). Fighting banking botnets by exploiting inherent command and control vulnerabilities. International Conference on Malicious and Unwanted Software: The Americas (MALWARE), pp. 93–100.

Whinston, M. D. (2003). On the transaction cost determinants of vertical integration. *Journal of Law, Economics, and Organization*, *19*(1), 1–23.

Williamson, O. E. (1971). The vertical integration of production: market failure considerations. *The American Economic Review*, *61*(2), 112–123.

Williamson, O. E. (1979). Transaction-cost economics: the governance of contractual relations. *Journal of Law and Economics*, *22*(2), 233–261.

Williamson, O. E. (2005). Transaction cost economics and business administration. *Scandinavian Journal of Management*, *21*(1), 19–40.

Zhuge, J., Holz, T., Song, C., Guo, J., Han, X., & Zou, W. (2009). Studying malicious websites and the underground economy on the Chinese web. In M. Johnson (Ed.), Managing information risk and the economics of security (pp. 225–244). New York: Springer