

# The Gozi group: A criminal firm in cyberspace?

European Journal of Criminology

2023, Vol. 20(5) 1701–1718

© The Author(s) 2022



Article reuse guidelines:

[sagepub.com/journals-permissions](https://sagepub.com/journals-permissions)

DOI: 10.1177/14773708221077615

[journals.sagepub.com/home/euc](https://journals.sagepub.com/home/euc)

**Jonathan Lusthaus**   
University of Oxford, UK



**Jaap van Oss**  
Independent Researcher, Netherlands

**Philipp Amann**  
Europol, Netherlands

## Abstract

The relative glut of data on cybercriminal forums has led to a growing understanding of the functioning of these virtual marketplaces. But with a focus on illicit online trading, less attention has been paid to the structures of groups that carry out cybercrimes in an operational sense. In economic parlance, some such groups may be known as ‘firms’. This concept has been a significant part of the literature on more traditional forms of organised crime, but is not widely discussed in the cybercrime discourse. The focus of this article is, by way of a case study of the Gozi malware group, to explore the applicability of the concept of firms to the novel environment of cybercrime.

## Keywords

Criminal firms, cybercrime, cybercriminal organisation, Gozi, malware groups

## Introduction

The relative glut of data on cybercrime marketplaces has led to a growing understanding of how these forums function and their role within the illicit digital economy (see, for instance, Décary-Héty and Dupont, 2013; Dupont et al., 2017; Dupont and Lusthaus, 2021; Holt, 2013; Holt and Lampke, 2010; Motoyama et al., 2011). While marketplaces are undoubtedly an important part of the cybercrime economy, less attention has been paid to the structures of

---

## Corresponding author:

Jonathan Lusthaus, Department of Sociology, University of Oxford, 42-43 Park End Street, Oxford OX1 1JD, UK.

Email: [jonathan.lusthaus@sociology.ox.ac.uk](mailto:jonathan.lusthaus@sociology.ox.ac.uk)

groups that carry out cybercrimes in an operational sense (see Broadhurst et al., 2014; Leukfeldt et al., 2017c; Lusthaus, 2018b; Musotto and Wall, 2020; Wall, 2014). That is, those groups which are the source of the products and services that are brought to market. We might regard these as enterprises, businesses or companies. But in traditional economic terms, the concept of *firms* is standard and foundational (on theories of firms see Gibbons, 2005). In short, a *firm* is a profit-making entity supplying a service or good (Sullivan and Sheffrin, 2003).

The concept of firms has been a significant part of the literature on more traditional forms of organised crime (most notably Reuter, 1983; for a review see von Lampe, 2016: 127-157). But its application to cybercrime is less developed. Some comparative research has been done on cybercriminal business models (Broadhurst et al., 2014; Leukfeldt et al., 2016; Leukfeldt et al., 2017a; Lusthaus, 2018b), and the idea of cybercriminal networks has begun to gain greater prominence (see e.g. Leukfeldt et al., 2017b; Leukfeldt et al., 2017c). Yet, only a handful of scholars have directly touched on the concept of a firm or the oft-linked area of transaction cost economics (Herley and Florêncio, 2010; Lusthaus, 2018a; Paquet-Clouston et al., 2018; see also Hardy and Norgaard, 2016). The concept has not been probed in depth, and key questions remain to be answered. Do cybercriminal businesses match our conventional expectations of what a firm is? Do they differ from (non-digital) criminal firms? Does the concept of a firm help us understand the organisational structure of cybercriminal groups?

The focus of this article is, by way of a case study, to explore the applicability of the concept of firms to the novel environment of cybercrime. The first section of this article provides theoretical background on the concept of the firm. The second section addresses the data and methods employed in the study. The third section is the core case study of the Gozi group, one of the leading malware producers and distributors of its time. This section analyses the group's background, structure and operations. A discussion section then follows, linking this case study to broader themes of interest.

## Theory

To explore whether the concept of firms is applicable to cybercrime, we must first outline theoretical background on the nature of both legal and criminal firms. This analysis draws on a range of social science contributions, across not only criminology, but also sociology and economics.

### *The nature of firms*

While definitions, like the one in the introduction, see firms as profit-making entities, this does not tell us much about the nature of firms. The terms *business*, *enterprise* or even *company* might be equally applied. Such a broad approach would incorporate huge swathes of commercial activity, in line with the thinking that 'firms can take many different forms, each with its own sociological profile: partnerships, family firms, joint-stock corporations, and so on' (Swedberg, 2003: 74). Rather than getting caught in the quagmire of exhaustively listing every type of firm that might exist, a more useful analytical

exercise is to engage with the question of why firms emerge instead of other possible structures. In short, what is it that firms offer to those inside them?

The most useful body of theory to assist with this task is known as *transaction cost economics*. In his archetypal paper, Coase famously posits that firms emerge due to costs associated with engaging with markets. These include: costs in purchasing the goods/services, bargaining costs, information costs and concerns regarding trade secrets and enforcement (Coase, 1937). In some cases, bringing certain partners within a firm structure may enhance overall production and economic gains. If the costs of using the market are too high, a firm would be employed.

In perhaps its most influential application, Williamson endorsed and expanded Coase's approach in later decades. He summarises the transaction costs of engaging with markets in two categories: (1) 'ex ante costs of drafting, negotiating and safeguarding an agreement'; (2) 'ex post costs of maladaptation and adjustment that arise when contract execution is misaligned as a result of gaps, errors, omissions, and unanticipated disturbances' (Williamson, 1996: 379). For Williamson there are clear reasons why a firm ('hierarchy' in his terminology) or market will be used in a given case. When transactions are rare and/or straightforward, a market is more appropriate than a firm. Firms are more likely to be used when transactions are frequent, defined by uncertainty and/or asset specificity is high – for example, when a customised product or service might not be of value to other buyers (see Williamson, 1975).

There are some glosses that should be provided to the school of Coase and Williamson. First, it should not be assumed that when either a firm or market approach is chosen that such a choice is a perfect one. This would constitute what Granovetter (1985) regards as a functionalist fallacy: just because certain economic organisations exist does not mean they are inherently efficient. In fact, there are empirical examples of seemingly inefficient business choices and poor organisational decisions (see DiMaggio and Powell, 1991). Second, *networks* have now attained an important theoretical role in the literature, alongside markets and firms. While Coase does not address networks, Williamson adds a third "hybrid" form to account for long contractual relations (Williamson, 1996: 104-105). This alteration suggests that certain examples may fall between either markets or firms. This view is championed more pointedly in the work of others, such as Powell (1990), who posit that networks are of great significance.

The other complicating factor is defining the limits of firms. Firms do not exist in isolation, but interact with other firms and individuals (Davis and Powell, 1992; Swedberg, 2003: 99). Firms may partner in various ways, from a temporary basis up to when multiple firms are consolidated into a single legal entity. Between these two extremes, Granovetter (2005) suggests some firms may formally or informally connect themselves in a persistent way to form a 'business group'. Whether defined as a business group, or a partnership more broadly, there are a range of relationships between firms, such as joint ventures and franchising.

Finally, the internal structure of firms should be delineated briefly. Weber provides the classical analysis of this topic. One of his main contributions is the idea that a firm's property is distinct from its individual members (Weber, [1923] 1981: 228). Beyond that, he establishes three main categories of those inside a firm: entrepreneurs, bureaucrats, and workers. The entrepreneur is "the leading spirit", the bureaucrat is trained for a clearly defined responsibility, while the worker is dependent on the employment the firm

provides (Weber, [1922] 1978: 1403). In more modern firms, this roughly appears to equate with the categories of leaders, middle management and then lower tier employees.

### *Criminal firms*

Discussions of criminal firms have been largely in line with the broader social sciences literature on firms. In his review of illegal enterprises, (von Lampe, 2016: 127) suggests that criminal firms are 'delineable organisational entities that are roughly similar in function to organisations in the legal economy, commonly referred to as businesses, business enterprises, enterprises, corporations, or firms'. He also carries over a similar tripartite division to Powell and others, in that he sees these *firms* sitting alongside both illegal *markets* and illegal *networks* (127).

Despite this broad similarity, analyses of criminal firms often allow for a much more informal conceptualisation. This is likely because criminal enterprises operate under the threat from law enforcement, and without the state apparatus regulating their dealings (Campana and Varese, 2013; Morselli et al., 2007; Reuter, 1983). An obvious point, which sometimes goes unstated, is that many criminal firms will not be legally registered, abide by corporate law, or pay tax (except in cases of front companies or legitimate businesses that 'turn bad'). While legal companies are at least partly defined by possessing their own independent capital, this does not appear to be as great a concern for scholars of illicit firms, who focus on intangible assets like reputations for violence (see Gambetta, 1993; Reuter, 1983; and for a critique Sugden, 1995).

Criminal firms are also likely to be relatively small. Responding to the previously held view that criminal groups were large, shadowy and monolithic enterprises exerting considerable control over illicit markets, Reuter's pathbreaking empirical research suggests that gambling and loan-sharking in New York were instead principally carried out by small, competing and short-lived firms (Reuter, 1983). This was due to a number of factors: the need for secrecy, the risks associated with expansion, and the difficulties in monitoring employees (Reuter, 1983). In studying the so-called 'Capone Gang', Haller (1990: 218) argues that this group should not be viewed as one large, tight hierarchy, but rather as 'a complex set of partnerships'. There were four 'senior partners' of Capone and his closest associates, which one might reasonably conceive of as a firm. But this central group affiliated with a network of other entrepreneurs who were engaged in a range of activities: 'the coordination was exerted through a series of deals with relatively independent businessmen to operate separate, small-scale enterprises' (222).

Many criminal firms appear to lie close to the boundary of the firm, and perhaps not that far from falling into a network or market structure. But where is this boundary drawn for those inside a group? Largely in line with Weber, scholars conceptualise illegal enterprises as having four layers: entrepreneurs, managers, permanent employees who often work on salary/commission, and temporary workers (see for instance Caulkins et al., 2009). Reuter (1985) argues that if an individual works exclusively for, and is largely controlled by, a leader of an illicit firm, then this person is an employee. But if they work for multiple firms and are paid based on results, then they are often an "independent supplier" (Reuter, 1983: 49). One related challenge of delineating the boundary of a criminal firm is that there is often a high degree of fluctuation of those who are involved within particular firms and the roles they play (Bright and Delaney, 2013; Kleemans and Van de Bunt, 1999).

## Data and methods

When evaluating the applicability of the concept of firms to cybercrime, it is most sensible to carry out this analysis by way of case study. Successful case studies of conventional criminal groups have been carried out in the past (see, e.g. Hornsby and Hobbs, 2006; Levitt and Venkatesh, 2000). This approach provides a strong degree of specificity and detail. We have chosen to focus on a malware group, as their products are vital to the broader cybercrime economy and are a damage multiplier, by allowing far less skilled cybercriminals to operate successful enterprises. Our case study is of the criminal group behind the Gozi malware, which was initially detected at the turn of 2007 and operated in its original form until late 2010 (for background on Gozi see Krebs, 2013; USDOJ, 2013). There are a number of reasons for this choice. First, during its time of operation, the Gozi Trojan was one of the most significant pieces of malware available and was widely exploited across the world. Second, the case has largely passed through the justice system with several key players convicted. This reduced certain complexities around ethics and risk. Practically, it also meant that more information could be accessed, both from investigators and public sources, than in active cases.

Another key consideration is that we believed the Gozi case might be of analytical interest in understanding the nature and evolution of malware business models. As discussed below, the case appears to bridge between the early forms of financial malware, where all aspects of the enterprise were controlled internally, and the situation that is faced today, which is less centralised and more service based (see EC3, 2020; van Oss, 2011). Gozi presents an archetypal case that we might expect is typical of groups that followed, and one that also helps us understand the broader dynamics of the evolution of banking Trojans and the organisational structures behind them. The generalisability of this choice will be explored in further detail in the discussion section, when we compare the case of Gozi to other examples to determine external validity.<sup>1</sup>

This paper makes use of a qualitative approach. It draws together data from a range of different sources, to paint a more complete picture of the Gozi group. The key data includes US indictments, complaints and other legal documents concerning the case that are publicly available. We gathered seven of these documents, which ranged from 2 to 26 pages. We were also given access to a confidential investigatory report that contained rich information on the group, including some of their communications. To gain more detailed information on certain points, we carried out interviews with individuals involved in investigating the group. This included both those from the public and private sectors, and in more than one country. In total there were five participants, identified only as P1-5 herein, to preserve their anonymity. Some were interviewed in person, others over the phone. Finally, in a time intensive process, we made use of law enforcement records to verify some important findings coming out of the above data sources. Due to security/sensitivity reasons, these records were not opened to us as a primary source that could be scoured at will. Rather one co-author was able to engage with law enforcement agents to check specific points of interest in this paper against records to ensure they were accurate.

This approach provides a strong degree of triangulation in order to enhance the validity of this research (on validity see, for instance, Hoyle et al., 2002). Triangulation

involves combining multiple methods/data to reduce potential biases in the research design (Denzin, 1978; Patton, 2002: 555-563). Our approach draws on both the analysis of written sources, as well as conducting interviews. The written and interview data have been derived from multiple jurisdictions. The interview participants also come from different perspectives, in that they span law enforcement, related parts of the public sector, and the private sector. Additionally, they have different investigation expertise, ranging from the human, to the technical and the financial. Despite these efforts, the main challenge to validity is that the cybercriminal perspective is not directly represented. As such, the findings in this paper are likely to reflect the investigation perspective, and be missing certain details and richness that could only be garnered by direct contact with the offenders in this case. There are consistent questions around access and accuracy when interviewing cybercriminal offenders, but it is possible to do so (Hutchings and Holt, 2018; Lusthaus, 2018a, 2018b). Nonetheless, for the scope of this article, the decision was made to focus our limited resources on the investigation data, especially as it would have been very difficult to protect the identities of the small number of offenders centrally involved in Gozi.

### **Case study: The Gozi group**

Gozi was a piece of banking malware known as a Trojan horse. Along with Zeus, other well-known examples have included Spyeye, Carberp and Emotet. Simply put, the goal of these Trojans is to capture user credentials for online bank accounts, allowing the cybercriminals to extract the funds from those accounts. Gozi used what's known as the 'man-in-the-browser' technique, which allows the offenders to collect data that has been entered into Internet browsers.<sup>2</sup> In order to get the malware onto the victim computers, the Gozi group had to exploit vulnerabilities in the browser or plugins (e.g. a PDF reader). Gozi was first detected at the turn of 2007 (Jackson, 2007), and originated in the first phase of banking malware.

In this first phase, several groups developed themselves into well run malware crews. Their success initially was based on keeping the malicious code proprietary and the infrastructure under their own control. Zeus, which also came to notice in 2007, was a good example of this (on Zeus see Hutchings and Clayton, 2017). Until the source code was leaked in May 2011, the Zeus malware was coded, developed and maintained by the same group (Goodin, 2011). There were a number of core functions within this business model, as made clear by van Oss (2011). While the developer provided the malware, another part of the group had to distribute it and infect machines. These machines became part of a 'botnet' and had to be managed by a 'botherder'. Online banking credentials needed to be harvested from the botnet and stored in so-called 'drop zones'. Once harvested, one or more group members were required to perform the fraudulent transactions that would transfer the money out of victim accounts. Last, was the 'cashout' process, where individuals had to extract the money from the accounts that received the stolen funds.

The second phase of the banking malware evolution would soon follow. It became far more common for developers to sell or rent their malware to other parties, rather than exclusively exploit it themselves. This is often referred to as 'malware-as-a-service' or,

more broadly, ‘cybercrime-as-a-service’ (EC3, 2020; The PhishLabs Team, 2014). The Gozi group’s contribution was in this second phase, when they developed a partnership model that would become commonly used by a range of other groups.

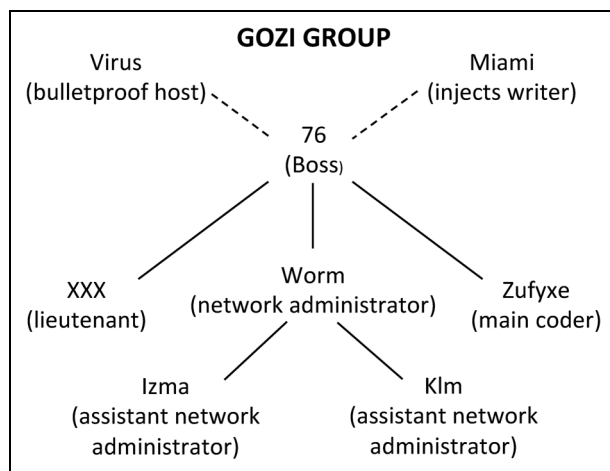
### *Gozi organisational structure*

In order to run a malware development group, it remains essential that some kind of coder or programmer be centrally involved. But the case of Gozi suggests that the leader of the group may instead be an effective manager who has some technical interests and organises the efforts of others. It is not necessary for this person to be a leading coder in their own right. For Gozi, this entrepreneur was Nikita Kuzmin, known online as 76 (and sometimes as Ya), who coordinated the group’s activities from Russia and was widely believed to be the ‘brain’ and the ‘ideas man’ (P5).<sup>3</sup> Although some investigators were hesitant to label him the ‘boss’, they nonetheless saw him as the central node within the organisational network and believed that it was Kuzmin’s vision to create the most powerful banking Trojan in the world (P3; P4). In order to do that, he needed to bring in the right talent and expertise: a developer, a botnet manager (‘botherder’), an expert in injecting malicious code, spammers and money mules (P3; P4). One participant summarised matters like this:

There were different skill sets for each person. 76 was a ‘project coordinator’. He oversaw everything as the business manager. Under him you had people doing different aspects of the business. You had server people, people writing and updating the code, people dealing with the injects. Then you had other people coming in and out of the group that would be contracted to spread the malware, different people writing spam templates, selling email lists, down to different cashout groups. There were different roles involved (P5).

Nonetheless, the core group was small. The majority of the coding of the Gozi Trojan was carried out by a person with the nickname Zufyx, who was based in Russia. There was also the chief lieutenant xxx, who was kept on salary and, according to interviews, paid between US \$50,000-60,000 a year (P1; P2; P3; P4). The complete core group is represented in Figure 1, with the dotted lines indicating ‘freelance contractors’ (independent suppliers) who provided regular and important services from the outside. The central team was Russian-speaking, though may have been from more than one country (P5).

None of the data provided clear evidence of how the group met. Regardless of origin, it appeared that the group primarily communicated through the Jabber (XMPP) messaging service. Some interview participants believed that the Gozi group only sparingly made use of forums, even to promote their product, often preferring to engage with partners who were already known contacts. Compared to forums, Jabber can be a much more private (and encrypted) way for small groups to engage with each other and coordinate their business. Some suggested that Gozi acted almost like a ‘ghost group’ (P1; P2). As argued by Lusthaus and Varese (2021), the offline and local dimension of cybercrime also should not be ignored (see also Leukfeldt et al., 2017a; Lusthaus, 2018b). But in the Gozi case, there was limited data available on this point, other than that some of the



**Figure 1.** Structure of the Gozi group.

members likely met in person (P1; P2), and that 76, aka Nikita Kuzmin, lived in Moscow and was socially active and known within his environment.<sup>4</sup>

Connected to the core group, there were a number of others who played a role within the Gozi enterprise. But, as per Reuter's delineation, it is most accurate to view some of these functions as the work of independent suppliers. For instance, a Latvian known online as Miami was brought in as a specialist in 'injections' (P1; P2; P3; P4). This involves finding ways of exploiting software bugs so that the malware can be placed on victim computers. Miami appears to have been picked by 76 (P1; P2). It is likely that he was paid per inject, at least initially, rather than on salary as the core group members were.<sup>5</sup> Significantly, Miami didn't just work for Gozi as the core group did, but was also known to provide similar services to a number of competitor malware groups such as Zeus and Spyeye.<sup>6</sup> Virus, a Romanian national who provided bulletproof hosting services for Gozi, also served a number of different customers.<sup>7</sup>

There was also the possibility of external organisational elements responsible for supporting and/or protecting the Gozi group. While one investigator had seen organised crime involvement in other similar cases (P5), based on what is known in the Gozi case, there was not strong evidence for the involvement of organised crime groups (P1; P2; P3; P4). Two participants believed that Kuzmin was previously linked to the infamous cybercriminal group, the Russian Business Network (P3; P4), which some argue had connections to the Russian mafia (see Graham, 2009: 173; Krebs, 2014: 22–23). This is a somewhat tenuous connection.

In terms of local protection, a more fruitful line of inquiry might relate to the political system instead. Gozi employed a similar tactic to some other Eastern European groups: they did not target 'home' victims within their own country or region, in order to avoid potential threats of prosecution (P1; P2). But beyond this, some interview subjects suggested that the group may have enjoyed some form of political protection through nepotism or corruption. One investigator noted that 'corruption is rampant over there. I don't



think that's a secret' (P5). Kuzmin is not a hardened criminal, but rather comes from an ostensibly well-off family. It is noteworthy that he is the son of a famous Russian singer called Vladimir Kuzmin. Two participants hypothesised that this status within Russian society, and his father's influential connections, may have helped the younger Kuzmin avoid arrest within his home country (P1; P2). Although their investigation did not lead them into hard evidence that Kuzmin and the Gozi group were directly connected to elements of the Russian government, these participants argued that some level of protection remains a possibility (on corruption and cybercrime more broadly see Lusthaus, 2018b: ch 7).<sup>8</sup>

### *The partnership model*

If the sole function of the Gozi group were malware production, the structure of the enterprise would be relatively simple. The core group would sell their product to various customers and those cybercriminals would make use of it themselves to steal banking credentials and then extract funds from the victim accounts. In reality, the business model was more complicated, and changed over time. In the early days of Gozi, 76 employed a service model, where he sold credit card data and bank account access through his platform. But this created concerns that it exposed him to prosecution.

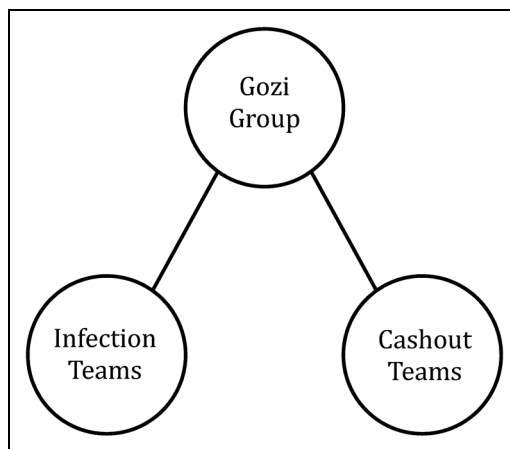
76 later developed a different model that removed him from the coalface of criminality, and saw him act more as a coordinator, rather than the lead actor (P1; P2). The malware group held the source code and infrastructure, but provided access to their botnet for others to harvest credentials and carry out the banking frauds (P5). Key to this approach was bringing on partners who were respectively responsible for driving traffic (for infections) and cashing out. Unlike Miami's injection involvement, which looked more like a freelance relationship, these partners operated in a coordinated way with the central team as part of sustained campaigns. The software, traffic and cashout elements of the business were all 'interdependent' (P2). Each of these teams received roughly a third of the overall profits from each effort. Often these teams were responsible for particular geographical regions. Figure 2 outlines the broader structure of the Gozi network.

This approach seemed to be a departure from both the original model of using malware only within the group, and the simple model of selling/renting the malware to others. As one participant put it: 'Normally you buy Zeus and you use it, and you run your business alone.' But the Gozi case was different because 76 was maintaining greater control over those teams exploiting the malware (P1). This made the group somewhat unusual when compared to other contemporaneous operations. It was essentially a core group that connected with partners who performed other functions for them. The core group neither carried out all the functions, nor did it wash its hands of many of them by purely selling/renting the product. It is also not accurate to view this structure as an outsourcing model because 76 didn't simply pay a fee to specialists to provide their services. It appears more apt to suggest that this was akin to a *partnership* model of one kind or another, where the Gozi group brought on new associates in a range of jurisdictions and provided them with a cut of the profits, in return for their involvement. While allowing 76 to step back from heavy operational involvement, this model also appears to have allowed him to maintain a level of control (P3; P4).

### *The Gozi firm*

In applying the concept of the firm to Gozi, the core structure that produced the malware is well suited to this label in a number of respects. The team had a defined hierarchy and operated together for some time with a clear profit motivation. The entrepreneur and project manager, 76, oversaw the finances with earnings estimated to be about US \$700,000 per year. 76 ensured that his team members were regularly paid.<sup>9</sup> There was value in internalising the different specialisations into the firm, rather than relying only on market relationships. There was a high degree of asset specificity, as the core roles were highly specialised and tailored to the Gozi malware. The transactions between these individuals were very regular, and would otherwise have been characterised by a high degree of uncertainty on the cybercriminal market. Nonetheless, there were limits to the firm. For instance, some functions were provided by freelance contractors like Miami, who also worked for other competitor groups.<sup>10</sup>

This Gozi firm was very business-like and professional in how it operated. To provide but one example, two investigators described how, before the start of a campaign, the group tested the functionality of a bank account they controlled. They would log into the account multiple times and then make small legitimate payments of about US \$50 to recipients like charities. After that, they might begin to make larger payments, perhaps even beyond the level of funds in the account, and thereby would receive an error message. They would never do anything illicit with this account. In short, they were gaining an idea of how the bank account functioned, so they could fit the malware to it, as the illicit transfers that would follow as part of the scam would be automated by the malware rather than being carried out by a human. They even kept control of this account once the campaign had begun against victims, and used it to troubleshoot any problems that emerged (P3; P4).



**Figure 2.** Gozi partnership structure.

We must also apply the firm concept to the broader structure of the Gozi network, which is perhaps a poorer fit. The transfer and cashout teams that the core group engaged with in each jurisdiction were not members of the central hierarchy. In reality, they were more like partners than firm members, not dissimilar to Haller's analysis of the Capone group. Law enforcement sources suggest that some cashout partners may even have worked with other malware operations, as well. While one might argue over whether this partnership arrangement technically should be classified as a business group, franchise or other structure, it is essentially a compromise between insourcing and outsourcing. Rather than contracting with transient external partners, it involves bringing longer-term affiliates into the brand and broadly within the firm's umbrella. The advantages of such an approach are that it transfers many of the costs and risks to the affiliates, while allowing the core firm to retain a degree of control. It allows the firm an expanded pool of profits beyond what the core group could achieve on its own, combined with a more sheltered role within the criminal activity.

### *New Gozi firms?*

The leader of the original Gozi crew was arrested in 2010 while travelling through San Francisco.<sup>11</sup> But that is not the end of the Gozi story. As if emphasising the distinction between the technical and human components of cybercrime, the Gozi malware itself continues to play a role. In short, new players have taken over the business. It is not yet clear exactly who's behind these operations, but it appears that components of the Gozi source code continued to be used past 76's time in control. This might have been the result of leaks or sales of the code (Brumaghin and Unterbrink, 2018). It would be valuable for further research to track exactly how the Gozi code was appropriated over the years and found its way into different operations. This is a similar process with what followed the release of the Zeus source code, with the developments of new variants emerging over time (see for instance EC3, 2014).

Analysis of the current status of the Gozi malware is more speculative as the cases are open so it is more difficult to gather reliable data, beyond public reports. While researchers have used a range of different names to describe the malware (e.g. Rovnix, ISFB, Papras and Ursnif), it also appears credible that the Gozi malware did not continue on just one track after the demise of the original firm, but was possibly adopted by more than one group (Exploits Team, 2014). One clear suggestion of this, is the Goznm Trojan, which appears to have been created as a hybrid between Gozi and another piece of malware called Nymaim (Brewster, 2016). Some of the crew behind that operation were recently arrested in a widely publicised operation (Greenberg, 2019).

## **Discussion and conclusion**

The case study of the Gozi group exhibits core elements that one would associate with firms. In broad terms, it is a group of multiple individuals who operate for profit over a number of years. This firm structure increases efficiency and profits by internalising core components of the malware business. Following Williamson, this matches theoretical expectations in that the transactions within the Gozi group were very frequent,

otherwise characterised by uncertainty if sought through a criminal market, and defined by high asset specificity, in that the malware is highly sophisticated and peculiar, requiring significant expert and tailored functions from members of the group.

But if one takes a more restrictive definitional approach, the firm in this example shares much more in common with the looser conception of criminal firms, than it does with more rigid conceptions that often apply to legal enterprises. We did not find evidence that the Gozi group was legally incorporated, or that it possessed its own independent capital. Leaving aside freelancers and partners, the core Gozi firm was likely made up of perhaps only six individuals, ranging from an entrepreneur down to employees. It only survived for a few years. As such, this example supports the views of those like Reuter who see criminal firms as being primarily small and short-lived. The larger criminal network, which may have included many tens of individuals from across the globe, more accurately reflects a partnership model or business group, than one single hierarchical organisation. In short, there was likely a range of other small distinct firms, along with individuals, who engaged with the Gozi enterprise interdependently.

One might expect cybercrime to offer innovative and new organisational structures. But facing familiar challenges around secrecy, monitoring and expansion – perhaps exacerbated by a digital setting – the firm structure in this case was largely in keeping with the structure of conventional criminal groups. As one participant put it:

‘People continue to look at cybercrime as this highly technical wizzbang thing – oh it’s on a computer and I can’t understand it and try to ignore it... But when you strip away the technical aspects of it, it’s really just business. It’s no different running a malware group than somebody running a numbers scheme. It’s just one’s technical and one isn’t... it’s just an avenue for making money’ (P5).

This view is supported by other analyses that suggest that cybercrime shares much in common with traditional business, and is even ‘boring’ in some respects (Lusthaus, 2018b: ch 3; Collier et al., 2021).

Of course, there are limitations involved with our findings, most notably that the paper contains a sole case study. The reasons for this choice were strong. We believed that the type of richness and nuance provided by such an unusually deep investigation would make an important contribution to the literature. But gathering such detailed, non-public, confidential, and triangulated data around this one case was extremely time-consuming, taking a number of years. Additional cases, with the same level of detail, were not feasible to include.

But this does raise the question of external validity. As we cannot address this through the case study itself, we briefly survey some broader elements within our data, the existing literature and public source information. Some of our main findings can be supported in this way. For instance, a major comparative study suggests that malware groups are usually quite small, with a rough maximum of eight core members (Lusthaus, 2018b: 56). Additionally, there is support for the idea that groups like Gozi can dissolve after a relatively short period, or realign their composition and business models. One of the indicators of the churn and fragility of this business is that enterprises are often termed as ‘projects’ (P5).

We can also use public information that is available to generalise our findings to more recent malware groups. In these cases, the basic firm structure and operations, along with the nature of their freelance relationships and partnerships appear to be similar to Gozi.<sup>12</sup> These examples also support the argument that there has been an evolution of the malware business model from something kept completely ‘in house’, to newer approaches which are far more service based, first in the form of rent-out schemes and eventually as partnership or affiliate models. This can be seen with significant malware operations like Bredolab and Emotet. Bredolab came to prominence in 2009, towards the end of Gozi’s period of operation. While it was also a Trojan like Gozi, it was used as a platform for a wider set of purposes: to deliver spam, fake anti-virus or other pieces of malware, including banking Trojans. As such, the Bredolab botnet was rented out to affiliates, who in turn used the botnet to generate malicious traffic, pay-per-click installs or deploy malware (on Bredolab see Graaf et al., 2013; Kirk, 2010; Sancho, 2009). Emotet shows the continued expansion of this service-based approach. The malware first appeared in 2014 as a banking Trojan that spread by phishing emails, but over time it matured into a malware-as-a-service firm that acted as a door opener for a range of other malware groups such as Ryuk, a ransomware group, or Trickbot, a data-stealing Trojan enterprise. It appears that the group behind Emotet started to sell access to its infrastructure around 2017. It has been a top threat globally (on Emotet see Johnson, 2021; SophosLabs Research Team, 2019).

While it is plausible that a number of our findings may apply to malware groups more broadly, it is possible that other types of cybercriminal groupings take different forms, and further research on these variations is required. As part of this, certain complexities may emerge. For instance, there are some known counter-examples where cybercriminal firms appear to be much larger and more structured than the Gozi group, even operating out of physical office spaces, being legally incorporated and/or having independent capital. These include examples like the Russian Business Network and Liberty Reserve (Graham, 2009; Halpern, 2015). These cases involve activity that looks legitimate, such as acting as an Internet Service Provider or a virtual currency company, but where the customer base is largely criminal. Such shades of legitimacy may play a role in how corporatized these groups become and how closely they begin to resemble legitimate firms. One could develop a hypothesis for further testing: the more obviously illegal an activity is, and the harder it is to hide or shield, the more likely that a cybercriminal firm will be smaller and shorter-lived.

The second main limitation of this article moves in the opposite direction of the first: we were unable to obtain a complete picture of the Gozi group due to data constraints. This relates to the secretive nature of both the group and investigations into it. There are likely investigation documents that exist, but are not publicly available and which were not made available to us. There are also limits to any police investigation, both in terms of the evidence that can be gathered, but also that information gathered for the purpose of prosecution does not always match scholarly needs. Additionally, not having access to the cybercriminal perspective means that more detail on the inner workings of the group cannot be included. As a result, there are a number of facets that remain murky, including accounting for all those involved in the criminal network and the full

scope of any offline dimension, along with whether the firm had its own independent capital.

In sum, what does the application of the concept of the firm to cybercrime, and the Gozi case in particular, teach us? First, and most importantly, the concept appears to have strong relevance, despite any novel aspects of cybercrime. While academic work has made detailed contributions on the 'Dark Web' and the general trade of illicit goods and services online, and law enforcement policy circles have also adopted a market-focussed approach characterised by a crime-as-a-service model (see, for instance, EC3, 2018), it is also important to clearly situate the individuals and groups that produce or exploit the products and services that are traded. But rather than reinventing the wheel, conceptualising cybercrime should draw on existing theory. This tells us that not only are markets important, but so too are networks and firms.

Second, the firm demarcation can provide added clarity when discussing cybercriminal groups and organisations. It helps us understand those tighter hierarchies, when contrasted to looser networks and markets. Some groups will not meet the definition of a firm, and are networks instead. Some cybercrime will involve individuals, who also are not part of firms. Cybercriminal enterprises may involve constellations of different firms and individuals working together, but not within one tight hierarchical structure. In short, the firm is a very useful concept to understand groups, their boundaries, and how they interact with other structural aspects of this criminal industry.

Finally, this analysis is valuable because in order to develop appropriate responses to cybercrime, we need a more complete understanding of what the underground looks like, incorporating all its component parts. We also need to better understand how these concepts interrelate. For instance, it is likely that some firms operate within certain marketplaces, and these are not mutually exclusive concepts. By comprehending how cybercriminal markets, networks and firms interrelate and cause harm, one can develop more focussed ideas around limiting this damage, where best to target interventions, and, ultimately, how to disrupt these structures.

### **Acknowledgements**

We are very grateful to our interview participants, who were very generous with their time and expertise. This article could not have been written without their input. We thank the editors and the anonymous reviewers, who provided extremely clear and constructive critiques, which greatly strengthened this work. Federico Varese also provided very valuable comments and advice on this paper.

### **Declaration of conflicting interests**

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.


### **Funding**

The author(s) received no financial support for the research, authorship and/or publication of this article.

## Notes

1. Another implicit reason for the choice of Gozi as the case study is that it has not been explored in detail by the academic literature. For those who wish to read more widely for foundational background on Gozi, there have been some reports produced by the cybersecurity industry, including: Jackson (2007), The PhishLabs Team (2014) and Check Point Research (2020).
2. Drawn from a confidential investigatory report.
3. See USA v. Nikita Kuzmin, 11Cr.387(LBS) (Southern District of New York) [Information].
4. Drawn from a confidential investigatory report.
5. For public information on Miami see USA v. Deniss Čalovskis, S412Cr.487 (Southern District of New York) [Indictment].
6. USA v. Deniss Čalovskis, S412Cr.487 (Southern District of New York) [Indictment].
7. USA v. Mihai Ionut Paunesco, 13Crim041 (Southern District of New York) [Indictment].
8. It should be noted that there is some conflicting public information on this point. Russian language sources indicate that Nikita is the adopted son of Vladimir Kuzmin, and the elder Kuzmin has distanced himself from Nikita. Meanwhile other reports see Vladimir claiming that the real offender was another man who just happened to have the same name as his son.
9. Drawn from a confidential investigatory report.
10. In certain cases, it is not always easy for observers to distinguish between repeated and regular freelance relationships and inner group membership (P1; P2).
11. USA v. Nikita Kuzmin, 11Cr.387(LBS) (Southern District of New York) [Information].
12. See, for instance, USA v. Maksim V. Yakubets, Criminal No. 19:342 (Western District of Pennsylvania) [Indictment].

## ORCID iD

Jonathan Lusthaus  <https://orcid.org/0000-0002-9386-7708>

## References

- Brewster T (2016) Eastern European Cyber Crooks raid US Banks for \$4 Million in just 3 days. Available at: <https://www.forbes.com/sites/thomasbrewster/2016/04/14/gozonym-bank-malware-steals-4-million-american-banks/#6eeab54d5e98> (accessed 4 July).
- Bright D and Delaney J (2013) Evolution of a drug trafficking network: Mapping changes in network structure and function across time. *Global Crime* 14(2–3): 238–260.
- Broadhurst R, Grabosky P, Alazab M, et al. (2014) Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. *International Journal of Cyber Criminology* 8(1): 1–20.
- Brumaghin E and Unterbrink H (2018) Gozi ISFB remains active in 2018, leverages “Dark Cloud” botnet for distribution. Available at: <https://blog.talosintelligence.com/2018/03/gozi-isfb-remains-active-in-2018.html> (accessed 4 July).
- Campana P and Varese F (2013) Cooperation in criminal organizations: Kinship and violence as credible commitments. *Rationality and Society* 25(3): 263–289.
- Caulkins J, Burnett H and Leslie E (2009) How illegal drugs enter an island country: Insights from interviews with incarcerated smugglers. *Global Crime* 10(1–2): 66–93.
- Check Point Research (2020) Gozi: The malware with a thousand faces. Available at: <https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/> (accessed 16 August).
- Coase R (1937) The nature of the firm. *Economica* 4(16): 386–405.

- Collier B, Clayton R, Hutchings A, et al. (2021) Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture. *British Journal of Criminology* 61(5): 1.
- Davis G and Powell W (1992) Organization-environment relations. In: Dunnette M and Hough L (eds) *Handbook of Industrial and Organizational Psychology*. Palo Alto: Consulting Psychologists Press, pp. 315–375.
- Décary-Héту D and Dupont B (2013) Reputation in a dark network of online criminals. *Global Crime* 14(2–3): 175–196.
- Denzin N (1978) *The Research Act: A Theoretical Introduction to Sociological Methods*. New York: McGraw-Hill.
- DiMaggio P and Powell W (1991) The iron cage revisited: Institutional isomorphism and collective rationality. In: Powell W and DiMaggio P (eds) *The New Institutionalism in Organizational Analysis*. Chicago: University of Chicago Press, pp. 63–82.
- Dupont B, Côté A-M, Boutin J-I, et al. (2017) Darkode: recruitment patterns and transactional features of “the most dangerous cybercrime forum in the world”. *American Behavioral Scientist* 61(11): 1219–1243.
- Dupont B and Lusthaus J (2021) Countering distrust in illicit online networks: The dispute resolution strategies of cybercriminals. *Social Science Computer Review*: 1–22. Online First.
- EC3 (2014) International action against ‘Gameover Zeus’ botnet and ‘Cryptolocker’ ransomware. Available at: <https://www.europol.europa.eu/newsroom/news/international-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware> (accessed 4 July).
- EC3 (2018) *Internet Organised Crime Threat Assessment*. The Hague: Europol.
- EC3 (2020) *Internet Organised Crime Threat Assessment*. The Hague: Europol.
- Exploits Team (2014) Tracking Rovnix. Available at: <https://labs.bitdefender.com/2014/11/tracking-rovnix-2/> (accessed 4 July).
- Gambetta D (1993) *The Sicilian Mafia: The Business of Private Protection*. Cambridge and London: Harvard University Press.
- Gibbons R (2005) Four formal(izable) theories of the firm? *Journal of Economic Behavior & Organization* 58(2): 200–245.
- Goodin D (2011) Source code leaked for pricey ZeuS crimeware kit. Available at: [https://www.theregister.co.uk/2011/05/10/zeus\\_crimeware\\_kit\\_leaked/](https://www.theregister.co.uk/2011/05/10/zeus_crimeware_kit_leaked/) (accessed 28 June).
- Graaf D, Shosha AF and Gladyshev P (2013) BREDOLAB: Shopping in the cybercrime underworld. In: Rogers M and Seigfried-Spellar KC (eds) *Digital Forensics and Cyber Crime*. Berlin: Springer, pp. 302–313.
- Graham J (2009) *Cyber Fraud: Tactics, Techniques, and Procedures*. Boca Raton: CRC Press.
- Granovetter M (1985) Economic action and social structure: The problem of embeddedness. *American Journal of Sociology* 91(3): 481–510.
- Granovetter M (2005) Business groups and social organization. In: Smelser N and Swedberg R (eds) *The Handbook of Economic Sociology*. Princeton: Princeton University Press, pp. 429–450.
- Greenberg A (2019) Global takedown shows the anatomy of a modern cybercriminal supply chain. Available at: <https://www.wired.com/story/goznm-takedown-cybercrime-supply-chain/> (accessed 4 July).
- Haller M (1990) Illegal enterprise: A theoretical and historical interpretation. *Criminology* 28(2): 207–235.
- Halpern J (2015) Bank of the Underworld. Available at: <http://www.theatlantic.com/magazine/archive/2015/05/bank-of-the-underworld/389555/> (accessed 13 September 2016).
- Hardy R and Norgaard J (2016) Reputation in the internet black market: An empirical and theoretical analysis of the deep Web. *Journal of Institutional Economics* 12(3): 515–539.



- Herley C and Florêncio D (2010) Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In: Moore T, Pym D and Ioannidis C (eds) *Economics of Information Security and Privacy*. Boston: Springer, pp. 33–53.
- Holt T (2013) Exploring the social organisation and structure of stolen data markets. *Global Crime* 14(2–3): 155–174.
- Holt T and Lampke E (2010) Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies* 23(1): 33–50.
- Hornsby R and Hobbs D (2006) A zone of ambiguity: The political economy of cigarette bootlegging. *British Journal of Criminology* 47(4): 551–571.
- Hoyle R, Harris M and Judd C (2002) *Research Methods in Social Relations*. Fort Worth: Wadsworth.
- Hutchings A and Clayton R (2017) Configuring Zeus: A case study of online crime target selection and knowledge transmission. In: APWG Symposium on Electronic Crime Research (eCrime), Scottsdale, AZ: IEEE.
- Hutchings A and Holt T (2018) Interviewing cybercrime offenders. *Journal of Qualitative Criminal Justice & Criminology* 7(1): 75–94.
- Jackson D (2007) Gozi Trojan. Available at: <https://www.secureworks.com/research/gozi> (accessed 28 June).
- Johnson E (2021) Emotet one month after the takedown. Available at: [https://www.trendmicro.com/en\\_us/research/21/c/emotet-one-month-after-the-takedown.html](https://www.trendmicro.com/en_us/research/21/c/emotet-one-month-after-the-takedown.html) (accessed 16 August).
- Kirk J (2010) Dutch team up with Armenia for Bredolab botnet take down. Available at: <https://www.computerworld.com/article/2513676/dutch-team-up-with-armenia-for-bredolab-botnet-take-down.html> (accessed 16 August).
- Kleemans E and Van de Bunt H (1999) The social embeddedness of organized crime. *Transnational Organized Crime* 5(1): 19–36.
- Krebs B (2013) Three charged in connection with ‘Gozi’ Trojan. Available at: <https://krebsonsecurity.com/2013/01/three-men-charged-in-connection-with-gozi-trojan/> (accessed 16 August).
- Krebs B (2014) *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*. Naperville: Sourcebooks.
- Leukfeldt R, Kleemans E and Stol W (2017a) Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *British Journal of Criminology* 57(3): 704–722.
- Leukfeldt R, Kleemans E and Stol W (2017b) A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change* 67(1): 21–37.
- Leukfeldt R, Kleemans E and Stol W (2017c) The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist* 61(11): 1387–1402.
- Leukfeldt R, Lavorgna A and Kleemans E (2016) Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research* 23: 1–14.
- Levitt S and Venkatesh S (2000) An economic analysis of a drug-selling gang’s finances. *The Quarterly Journal of Economics* 115(3): 755–789.
- Lusthaus J (2018a) Honour among (cyber)thieves? *European Journal of Sociology* 59(2): 191–223.
- Lusthaus J (2018b) *Industry of Anonymity: Inside the Business of Cybercrime*. Cambridge: Harvard University Press.
- Lusthaus J and Varese F (2021) Offline and local: The hidden face of cybercrime. *Policing* 15(1): 4–14.
- Morselli C, Giguère C and Petit K (2007) The efficiency/security trade-off in criminal networks. *Social Networks* 29(1): 143–153.

- Motoyama M, McCoy D, Levchenko K, et al. (2011) An analysis of underground forums. *Internet Measurement Conference 2011*: 71-80. <https://eg2.novatechset.com//home/Land/114390%7C3>
- Musotto R and Wall D (2020) More Amazon than mafia: Analysing a DDoS stresser service as organised cybercrime. *Trends in Organized Crime*: 1-19. Online First.
- Paquet-Clouston M, Decary-Hetu D and Morselli C (2018) Assessing market competition and vendors' size and scope on AlphaBay. *International Journal of Drug Policy* 54: 87-98.
- Patton M (2002) *Qualitative Research and Evaluation Methods*. Thousand Oaks: Sage.
- Powell W (1990) Neither market nor hierarchy: Network forms of organization. *Research in Organizational Behaviour* 12: 295-336.
- Reuter P (1983) *Disorganized Crime: The Economics of the Visible Hand*. Cambridge, Mass; London: MIT Press.
- Reuter P (1985) Racketeers as cartel organizers. In: Alexander H and Caiden G (eds) *The Politics and Economics of Organized Crime*. Lexington: Lexington Books, 49-65.
- Sancho D (2009) You scratch my back...: BREDOLAB's sudden rise in prominence. Available at: [https://www.trendmicro.co.kr/cloud-content/us/pdfs/security-intelligence/white-papers/wp\\_bredolab\\_final.pdf](https://www.trendmicro.co.kr/cloud-content/us/pdfs/security-intelligence/white-papers/wp_bredolab_final.pdf) (accessed 16 August).
- SophosLabs Research Team (2019) Emotet exposed: Looking inside highly destructive malware. *Network Security* 2019(6): 6-11.
- Sugden R (1995) The sicilian mafia: The business of private protection [book review]. *Journal of Economic Literature* 33(2): 863-865.
- Sullivan A and Sheffrin S (2003) *Economics: Principles in Action*. Upper Saddle River: Pearson Prentice Hall.
- Swedberg R (2003) *Principles of Economic Sociology*. Princeton: Princeton University Press.
- The PhishLabs Team (2014) The unrelenting evolution of Vawtrak. Available at: <https://www.phishlabs.com/blog/the-unrelenting-evolution-of-vawtrak/> (accessed 16 August).
- USDOJ (2013) Three alleged international cyber criminals responsible for creating and distributing virus that infected over one million computers and caused tens of millions of dollars in losses charged in Manhattan Federal Court. Available at: <https://www.justice.gov/usao-sdny/pr/three-alleged-international-cyber-criminals-responsible-creating-and-distributing-virus> (accessed 16 August).
- van Oss J (2011) *Cybercriminal Organisation: An Exploration of ZeuS Malware Deployment*. Dublin: University College Dublin.
- von Lampe K (2016) *Organized Crime*. Thousand Oaks: Sage.
- Wall D (2014) Internet mafias? The dis-organisation of crime on the internet. In: Caneppele S and Calderoni F (eds) *Organized Crime, Corruption and Crime Prevention*. Cham: Springer, 227-238.
- Weber M ([1922] 1978) *Economy and Society: An Outline of Interpretive Sociology*. Berkeley: University of California Press.
- Weber M ([1923] 1981) *General Economic History*. New Brunswick: Transaction.
- Williamson O (1975) *Markets and Hierarchies: Analysis and Antitrust Implications*. New York: Free Press.
- Williamson O (1996) *The Mechanisms of Governance*. Oxford: Oxford University Press.