Dropgangs, or the future of darknet markets

Jonathan “smuggler” Logan

2018-12-26T19:18:17Z

Contents

Dropgangs, or the future of dark markets

The Internet is full of commercial activity and it should come at no surprise that even illegal commercial activity is widespread as well. In this article we would like to describe the current developments - from where we came, where we are now, and where it might be going - when it comes to technologies used for digital black market activity.

We will refrain from any legal, moral or ethical judgment on these activities but focus on the technical and operational security aspects. What is illegal and unethical trade for one is perfectly legal for another. Judge for yourself.

Clearnet black market use, pre 2011

With the spread of the Internet, black market merchants soon started taking advantage of it for communicating with their customers, advertisement and payment facilitation. Early products were mostly centered around pornography, call girl rings, stolen data and intellectual property crimes - mostly stolen software and entertainment media - and thus either focused on digital delivery of goods and services, or facilitating “personal” services.

Use of the Internet to facilitate the marketing and sales of physical goods - drugs, weapons, false identification papers - began latest in the late 1990s, but usually focused on local geographic markets in major cities. This was due to the fact that payment and delivery still required in person meetings. Credit cards were the

only viable online-capable payment system and they proved to be too dangerous for a lot of merchants of illegal goods, therefor physical cash dominated.

This changed fundamentally when in the 2003-2007 period the first widely used pseudonymous centralized digital currencies came to the attention of merchants. Mail-order type businesses for physical goods that did not adhere to local law, tax or otherwise, developed. Most of these businesses however refrained from publicly marketing and instead were only available through word of mouth and to tightly knit online communities.

With the introduction of Bitcoin, the first decentralized cryptocurrency, a paradigm shift took place. It was likely "The Silk Road" that first fused the availability of this new kind of online payment system with anonymous access and publication of web content.

Darknet Markets. 2011-2017

"The Silk Road" was the first of a phenomenon that became widely known: Darknet Markets.

The shallow description of a darknet market consists of a website hosted on an anonymous overlay network like Tor or I2P where merchants can present offers, buyers accept those offers, and the payment between both is conducted through cryptocurrencies. Additional functionality like merchant-to-buyer private communication, reputation tracking, payment escrow services and forums in which both merchants and buyers can have public discussions is often provided.

The shipment of products for these markets typically was conducted by the merchant via the official postal system or parcel services (UPS, FedEx, DHL).

Darknet Markets as such were *centralized* marketing, communication, processing, reputation and escrow platforms which attracted primarily small merchant organizations that featured flat hierarchies - if they had any hierarchy at all. Customer binding and market share was primarily through the market itself, and not to the merchant.

A limiting factor for darknet markets was that customers had to use anonymous overlay networks such as Tor or I2P to be able to access these platforms. This was a barrier of entry for large segments of the potential consumer group and also limited the (secure) access of the markets to non-mobile customer devices like personal computers and laptops. Clearly not the convenience that is required by most modern consumers - especially in the drug user segment.

The centralized nature of these markets, the binding of customers to market, use of the postal service and the flat hierarchies of merchants had significant negative operational security implications.

While fraud by merchants was effectively tamed by the central reputation system of each market, fraud by the markets became a commonplace. Darknet markets would start offering escrow services which then allowed the market operators to

run with the money. This was only curbed by the introduction of multiparty transactions that would require any two of either the buyer, merchant and market to agree for funds to move (a feature that can be implemented with some cryptocurrencies by employing multi-signature transactions).

More severe were infiltrations and take-downs of darknet markets by law enforcement. Since the majority of offers, and most reputation data, was publicly available attacks using open source intelligence methods like web harvesting and analysis, as well as account take- overs became a common threat. Several cases in which law enforcement infiltrated the accounts of moderators and operators as well as merchants undermined trust in the darknet markets. Furthermore several markets were taken offline by law enforcement, often locking up funds and leading to insecurity in the economy.

Furthermore merchants were more and more often targeted by sting operations, tracking of shipments through the postal system, and tracing of cryptocurrency transactions. Merchants that were successfully identified and raided often had access to a long history of payment details and shipping addresses of buyers which further eroded the trust in the darknet markets. The flat hierarchies also lead to the deep penetration and complete identification of the members of market operator teams and merchant organizations.

Lastly, the loss of darknet markets lead to severe disruption of client-merchant relationships - identities and reputation being lost, previous marketing efforts being negated - often leading to temporary or even permanent collapse of merchant business.

Dropgangs. 2017/2018-?

The problems of darknet markets have triggered an evolution in online black markets.

To prevent the problems of customer binding, and losing business when darknet markets go down, merchants have begun to leave the specialized and centralized platforms and instead ventured to use widely accessible technology to build their own communications and operational back-ends.

Instead of using websites on the darknet, merchants are now operating invite-only channels on widely available mobile messaging systems like Telegram. This allows the merchant to control the reach of their communication better and be less vulnerable to system take-downs. To further stabilize the connection between merchant and customer, repeat customers are given unique messaging contacts that are independent of shared channels and thus even less likely to be found and taken down. Channels are often operated by automated bots that allow customers to inquire about offers and initiate the purchase, often even allowing a fully bot-driven experience without human intervention on the merchant's side.

The use of messaging platforms provides a much better user experience to the customers, who can now reach their suppliers with mobile applications they are

used to already. It also means that a larger part of the communication isn't routed through the Tor or I2P networks anymore but each side - merchant and customer - employ their own protection technology, often using widely spread VPNs.

The other major change is the use of "dead drops" instead of the postal system which has proven vulnerable to tracking and interception. Now, goods are hidden in publicly accessible places like parks and the location is given to the customer on purchase. The customer then goes to the location and picks up the goods. This means that delivery becomes asynchronous for the merchant, he can hide a lot of product in different locations for future, not yet known, purchases. For the client the time to delivery is significantly shorter than waiting for a letter or parcel shipped by traditional means - he has the product in his hands in a matter of hours instead of days. Furthermore this method does not require for the customer to give any personally identifiable information to the merchant, which in turn doesn't have to safeguard it anymore. Less data means less risk for everyone.

The use of dead drops also significantly reduces the risk of the merchant to be discovered by tracking within the postal system. He does not have to visit any easily to surveil post office or letter box, instead the whole public space becomes his hiding territory.

Cryptocurrencies are still the main means of payment, but due to the higher customer-binding, and vetting process by the merchant, escrows are seldom employed. Usually only multi-party transactions between customer and merchant are established, and often not even that.

Marketing and initial vetting of both merchant and customer now happens in darknet forums and chat channels that themselves aren't involved in any deal anymore. In these places merchants and customers take part in the discussion of best procedures, methods and prices. The market connects and develops best practices by sharing experience. Furthermore these places also serve as record of reputation, though in a still very primitive way.

Other than allowing much more secure and efficient business for both sides of the transaction, this has also lead to changes in the organizational structure of merchants:

Instead of the flat hierarchies witnessed with darknet markets, merchants today employ hierarchical structures again. These consist of procurement layer, sales layer, and distribution layer. The people constituting each layer usually do not know the identity of the higher layers nor are ever in personal contact with them. All interaction is digital - messaging systems and cryptocurrencies again, product moves only through dead drops.

The procurement layer purchases product wholesale and smuggles it into the region. It is then sold for cryptocurrency to select people that operate the sales layer. After that transaction the risks of both procurement and sales layer are

isolated.

The sales layer divides the product into smaller units and gives the location of those dead drops to the distribution layer. The distribution layer then divides the product again and places typical sales quantities into new dead drops. The location of these dead drops is communicated to the sales layer which then sells these locations to the customers through messaging systems.

To prevent theft by the distribution layer, the sales layer randomly tests dead drops by tasking different members of the distribution layer with picking up product from a dead drop and hiding it somewhere else, after verification of the contents. Usually each unit of product is tagged with a piece of paper containing a unique secret word which is used to prove to the sales layer that a dead drop was found. Members of the distribution layer have to post security - in the form of cryptocurrency - to the sales layer, and they lose part of that security with every dead drop that fails the testing, and with every dead drop they failed to test. So far, no reports of using violence to ensure performance of members of these structures has become known.

This concept of using messaging, cryptocurrency and dead drops even within the merchant structure allows for the members within each layer being completely isolated from each other, and not knowing anything about higher layers at all. There is no trace to follow if a distribution layer member is captured while servicing a dead drop. He will often not even be distinguishable from a regular customer. This makes these structures extremely secure against infiltration, takeover and capture. They are inherently resilient.

Furthermore the members of the sales layer often employ advanced physical tradecraft to prevent surveillance by the procurement layer when they pick up product. This makes it very hard to dismantle such a structure from the top.

If members of such a structure are captured they usually have no critical information to share, no information about persons, places, times of meeting. No interaction that would make this information necessary ever takes place.

It is because of the use of dead drops and hierarchical structures that we call this kind of organization a *Dropgang*.

The result of this evolution is a highly decentralized, specialized and resilient method of running black market commerce. Less information is acquired, shipments are faster, isolation between participants is high, and multiple independent sales channels are established.

Open questions to Dropgangs

Risks

Three main risks present themselves for Dropgangs:

- Cryptocurrency tracing: Since all payments are conducted with cryptocurrency, the use of "Privacy Coins" has established itself within the Dropgangs. However, customers usually only have less private currencies available. This requires a functional exchange infrastructure between less and more private cryptocurrencies. This vector of attack is currently exploited by law enforcement.
- Communication tracing: Dropgangs necessarily operate infrastructure to keep in contact with their customers. Law enforcement can potentially identify and track this infrastructure to find the operators. However, operators usually have access to sufficient anonymization technology and are well trained in using it.
- Surveillance of potential dead drop locations: Potential dead drop locations can be identified and surveilled by law enforcement to find those serving them. This poses a number of problems for law enforcement. First, the number of potential dead drop locations is very high which requires a lot of resources to surveil to even catch anybody by pure luck. Second, it is hard to distinguish customer and supplier at this moment if the dead drop operator uses basic protective tradecraft.

It is likely that the black market will solve the cryptocurrency tracing risk soon. Technology in this field is developing quickly. It is likely that either new exchange methods are found, like peer-to-peer decentralized on-chain swaps, or that additional privacy layers are added to less private cryptocurrencies. Cryptocurrencies like Beam and Grin both provide a reasonable amount of privacy while also supporting atomic on-chain swaps between them and widely accepted cryptocurrencies like Bitcoin and Ethereum.

The other two risks are already handled well by professional operators in the field.

Reputation

Compared to centralized darknet markets, Dropgangs face the issue that reputation is even more important to find customers and to vet customers, while at the same time having less suitable tools available. The current method of reporting sales experience on forums is open to spamming and manipulation since it is hard to show that a deal even took place.

It is likely that forums and merchants develop best practices to solve this problem. There is the potential that merchants will start to issue "proofs of sale" in a cryptographic form, that customers then use to make statements about the performance of the merchant in public forums.

This would allow for distributed and secure calculation of both merchant and customer reputation without the risk of spamming and manipulation. However, it also opens up a small risk in that law enforcement then has access to more data about the activities of a merchant. This risk however will likely be both mitigated by technology, as well as accepted by merchants and customers for

smoother and more efficient market operation. We expect development in this field very soon.

Localization of dead drops

Dead drops have to satisfy four functions:

- They must be plentiful. The more potential locations for dead drops, the more secure their operation in face of law enforcement surveillance.
- They must be easy to locate for the customer who has received the necessary information from the merchant.
- They must be unlikely to be found by accident.

These three functions together form the problem of localizing: There must be a high asymmetry of information required to find the location over the accidental find.

Classically, when used by intelligence agencies, dead drops relied on being concealed. This lead to dead drops being hard to find even by the intended recipients without costly preparation and training. One of the results of this was that dead drops were often used repeatedly, which increased the probability of both sender and recipient being identified by surveillance.

An ideal dead drop is however used exactly once. Only then can the risks of using it be reduced to pure bad luck.

This challenge is met by Dropgangs in various ways. The primary one is that the documentation of each dead drop is conducted in minute detail, covering GPS coordinates, photos of the surrounding and the location, as well as photos of the concealment device in which the product is hidden (such as an empty coke can). The documentation however increases the risk for the Dropgang since whoever creates it would be more easy to identify by surveillance. In addition, even great documentation still requires the customer to understand it and follow it precisely, which can lead to suspicious behavior around the dead drop location (staring at photos, visually comparing them to the surrounding, etc).

A first development to mitigate the problem of localizing is the use of Bluetooth beacons. In addition to the product, the dead drop contains a little electronic device that sends a signal that can be received by a smartphone, which in turn can display the direction and approximate distance to the device. In addition to the GPS coordinates, the customer requires only a smartphone with the correct App. Beacon devices like these are available on the open market for under ten dollars.

They do however pose the risk of a non-authorized party to discover the dead drop, simply by searching an area suitable for hiding dead drops with their own smartphone.

There are first reports of using beacon devices that are not constantly sending a signal, but have to be activated first. The activation usually happens by

establishing a WiFi hotspot on the customer's phone (by using the WiFi tethering feature). Only if the beacon sees a WiFi hotspot with a specific, merchant provided, unique name will it start to send a homing signal itself. Devices like these are very cheap (<15 USD) and have gained traction in the field, but they pose risks to the customer: His smartphone becomes identifiable by observers, even over considerable distance. This can lead to tracking the customer.

An alternative solution found is the use of WiFi activated beacons that instead of sending a Bluetooth signal use audible sounds that are loud and distinct enough to be heard by the customer for localization.

The lifetime of these beacons is surprisingly high. They usually lay dormant for a predefined time before they begin to listen for activation. During the listening phase, they usually only become active for a few seconds every minute. This method allows these beacons to lay passive for days or even weeks using only very cheap chemical batteries (instead of rechargeable batteries that are more expensive).

We expect the next development step to be related to beacons that listen for ultrasound signals before they activate. The customers smartphone would play these signals through its speakers, transmitting a unique code that activates the beacon. The beacon then would send out a homing signal that the customer can follow with his phone. This is likely going to be made available as an App that will make the complete process of localizing very user friendly and fast.

Future development

It is likely that future developments in this area will focus on customer convenience. Better homing beacons will be developed, and mass produced in Shenzhen factories to drive down the price.

Another expectation is that messaging services will appear that combine better anonymity for both merchant and customer with integrated payment systems and potentially even dead drop localizing functionality. Reputation tracking is a further feature that is likely to be integrated.

These messaging services will be dual use. They will be used both by the black market as well as by legitimate vendors, integrating automated, bot-controlled customer interaction with peer-to-peer payment is certainly a major technology to become commonplace in business. First steps in this direction have been taken by Chinese messaging companies, Telegram and even Facebook.

Given the developments in technology and methods, it is very likely that black markets will spread in both availability and demand. All kinds of goods will be widely available, anonymously, securely, in our cities and urban environments. More people will find their livelihoods in taking part in these distribution networks, since required skills and risks are low, while a steady income for the industrious can be expected. Instead of delivering papers, teenagers will service dead drops.

This will lead to further developments that serve the convenience and security of black market merchants and customers. A plausible next step would be the development of markets for dead drop operators that make their living by picking up product from one dead drop and placing it in another, working as a proxy for the customer to increase his safety and to reduce his efforts. This would also make this distribution model wider spread and available to more products, which will blur the lines between the black and the legal market. On this blurred line new services and technologies will establish themselves, inherently dual use services like lock boxes that can be paid by peer-to-peer cryptocurrencies.

Looking even further into the future, it seems plausible that the whole urban environment might find itself integrated into a dynamic landscape of very short-lived dead drops that are serviced by humans and cheap drones (unmanned aerial vehicles), which are already cheaply available and likely only require one market actor to develop and spread a mechanism to pick up and drop goods. Both merchant and customer could use drones, that are available for rent through dedicated Apps, to deliver product to a meeting point on a roof, where another drone would pick it up. Chaining multiple exchanges like this will make the tracing of the delivery extremely hard, essentially leading to mixing techniques so far used only in anonymizing digital communication.

Given the additional plausible development that long distance, high payload drones become available more widely, and for much less cost, the procurement layer of Dropgangs will also become more secure and efficient.

It is far from unlikely that these developments will lead to a breakdown of control and regulation over low weight, low volume goods. The black markets are upon us.

Continue thinking, what is possible if we combine: 4G/5G mobile internet, anonymous messaging, messaging bots, anonymous and untraceable digital currencies, strong end-to-end encryption, GPS, cheap electronics, 3D printed mechanics, cheap drones - both short distance multicopters and long distance fixed wing, visual processing for navigation, and lots of code.

What is possible if others combine these as well?

We have no idea what that will mean for our societies, good or bad. But we better start thinking how to deal with the effects. And we should ask the right people about it, not those still captured in the 20th century and the lobbying by industry.