Examining the Modes Malware Suppliers Use to Provide Goods and Services

Tony Bailetti and Mahmoud Gad

> *"Remove the predators, and the whole ecosystem begins to crash like a house of cards."*
>
> Brian Skerry
> Underwater photojournalist

Malware suppliers use various modes to provide goods and services to customers. By mode, we mean "the way" the malware supplier chooses to function. These modes increase monetization opportunities and enable many security breaches worldwide. A theoretically sound framework that can be used to examine the various modes that malware suppliers use to produce and sell malware is needed. We apply a general model specified recently by Hagiu and Wright to study five modes that malware suppliers use to deliver goods and services to their customers. The framework presented in this article can be used to predict the mode in which a malware supplier will function; to study which types of malware suppliers, agents, and customers are attracted to each mode; to discover new modes; and to better understand the threat a malware supplier presents.

Introduction

Malware suppliers, agents, and customers play important roles in the cybercrime economy. Malware suppliers include technically skilled individuals who produce and distribute malicious code; agents who act on behalf of malware suppliers or directly interact with customers; and customers who purchase goods and services to gain unauthorized access to compromised computers' data and resources, steal e-currency, exfiltrate victims' personal information, and so on (Kamluk, 2009).

The modes that malware suppliers use to provide goods and services to customers increase illicit monetization opportunities and enable many of the recent security breaches that have targeted some of the largest financial, government, military, and retail institutions in the world (Ablon et al., 2014; Armin, 2013; Gu, 2013; Samani, 2013). However, it is difficult to understand what these modes have in common, what makes them different, and what their potential combinations may be.

Consider the following examples of malware supplier modes:

1. *Dark0de:* a multisided platform that served as a venue for the sale and trade of hacking services, botnets, malware, and other illicit goods and services from 2007 until July 2015 when it was shut down by the Federal Bureau of Investigations (Europol, 2015). It took only two weeks for this marketplace to start operating again (Clark, 2015; Kovacs, 2015).

2. *Power Locker:* a reseller that allows customers to customize ransomware (Goodin, 2014; Mathews, 2014).

3. *Hacking Team* (hackingteam.it): a Milan-based firm that focuses on all aspects of offensive cybersecurity. On July 8, 2015, WikiLeaks released more than one million searchable emails from this Italian surveillance malware vendor (WikiLeaks, 2015). Moreover, the source code for Hacking Team's flagship software, Remote Control System, was breached and used to attack websites in South Korea (Peters, 2015; The Chosunilbo, 2015).

4. *The Styx Exploit Pack:* a kit vendor that sells a high-end software package developed for "the underground" but is marketed and serviced online. A 24-hour virtual help desk is available to paying customers (Krebs, 2013).

These examples illustrate that the lack of a theoretically-grounded framework to examine the nuances of the modes in which malware suppliers function hinders understanding of how the cybercrime economy works and weakens mitigation strategies.

The choice a firm makes about the mode it uses to deliver goods and services to customers is relevant in many product markets because of the increase in the number and size of online marketplaces that have emerged recently (Edelman, 2015; Hagiu, 2007; Hagiu & Wright, 2013, 2015b). Moreover, the choice of mode a malware supplier uses to deliver goods and services is prominent in a market where advances in obfuscation and detection-avoidance techniques, software reuse, machine learning, and Internet and mobile technologies have made it possible to use various approaches that offer an increasing variety of malware goods and services to customers.

The literature on the different modes in which a firm can function can be organized based on the methods used to examine them: specification of formal general models (Boudreau & Hagiu, 2009; Hagiu, 2007; Hagiu, 2009; Hagiu & Wright, 2015a; 2015b, 2015c); empirical studies (Boudreau, 2010); and informal descriptions (Choudary, 2015; Edelman, 2015; Eisenmann et al., 2006; Hagiu, 2014; Hagiu & Wright, 2013). This study focuses on five modes in which a firm can operate that have been specified using formal general models: “employment”, “multisided platform”, “reseller”, “vertically integrated”, and “input-supplier” (Hagiu, 2007; Hagiu, 2009; Hagiu & Wright, 2015a, 2015b, 2015c).

In the remainder of this article, we summarize the general model developed by Hagiu and Wright (2015c) to examine the choice a firm with a single agent makes among alternate modes to deliver goods and services and then apply the general model to examine five approaches that we believe malware suppliers use to provide products and services to their customers. We then discuss the contribution of this research and provide conclusions.

General Model with One Firm and One Agent

The general model for a firm and a single agent developed by Hagiu and Wright (2015c) assumes that the revenue generated jointly by the firm and the agent depends on three types of actions, all of which are influenced by asset ownership. These actions are referred to as being non-contractible. The non-contractible actions can be organized into three types: i) actions that can solely be carried out by the firm, ii) actions that can solely be carried out by the agent, and iii) transferable actions that can be carried out by either the firm or the agent.

The firm and the agent incur costs carrying out their actions. These costly actions are expected to increase the revenue generated jointly by the firm and the agent. Any contract offered by the firm to the agent can only depend on the revenue generated by the three types of actions, not just one or two types. The firm can offer the agent a contract that consists of a fixed fee and a variable fee equal to a percentage of the revenue generated jointly by the firm and the agent. The firm or the agent can collect revenues and pay the other party their share.

Hagiu and Wright (2015c) examine the case where a firm can select to operate in one of two modes: “employment” and “multisided platform”. The difference between the two modes is that the firm controls the transferable actions in the “employment” mode and the agent controls the transferable actions in the “multisided platform” mode. A side refers to an actor type. For example, a two-sided platform may enable individuals seeking employment and employers to interact directly. Similarly, a multisided platform may enable service providers, customers, and customers’ customers to interact directly.

According to Hagiu and Wright (2015b), two features make the multisided platform mode special. First, the multisided platform enables direct interactions between agents and customers. The phrase “direct interactions” is used to mean that the agent and the customers, not the firm, retain control over the key terms of the interaction. These terms can include price, bundling, delivery, quality, and so on.

The second feature that makes the multisided platform special is that both the agent and the customers are affiliated to the multisided platform. Agents make cash and in-kind investments in the multisided platform to interact with customers and form expectations of future returns from these investments. Similarly, anticipating returns, customers make cash and in-kind investments in the multisided platform to interact directly with the agent.

Examining the Modes Malware Suppliers Use to Provide Goods and Services

Tony Bailetti and Mahmoud Gad

Examining Modes Used by a Malware Supplier with One Agent

Consider the case where there is one malware supplier, one agent, one or more customers, and one or more customers' customers. Assume that the malware supplier is a technical organization with malware goods and services as its output. To produce and sell malware to customers, the malware supplier needs to choose one of the five modes illustrated in Figure 1:

1. *Employment mode:* employ and incentivize an agent to provide goods and service to customers
2. *Multisided platform mode:* enable the affiliated agent to provide goods and services directly to affiliated customers
3. *Reseller mode:* buy from a seller and resell to customers
4. *Vertically integrated mode:* work for a vertically integrated organization
5. *Input supplier mode:* sell inputs to a kit vendor who in turn incorporates those inputs in goods and services they sell to their customers

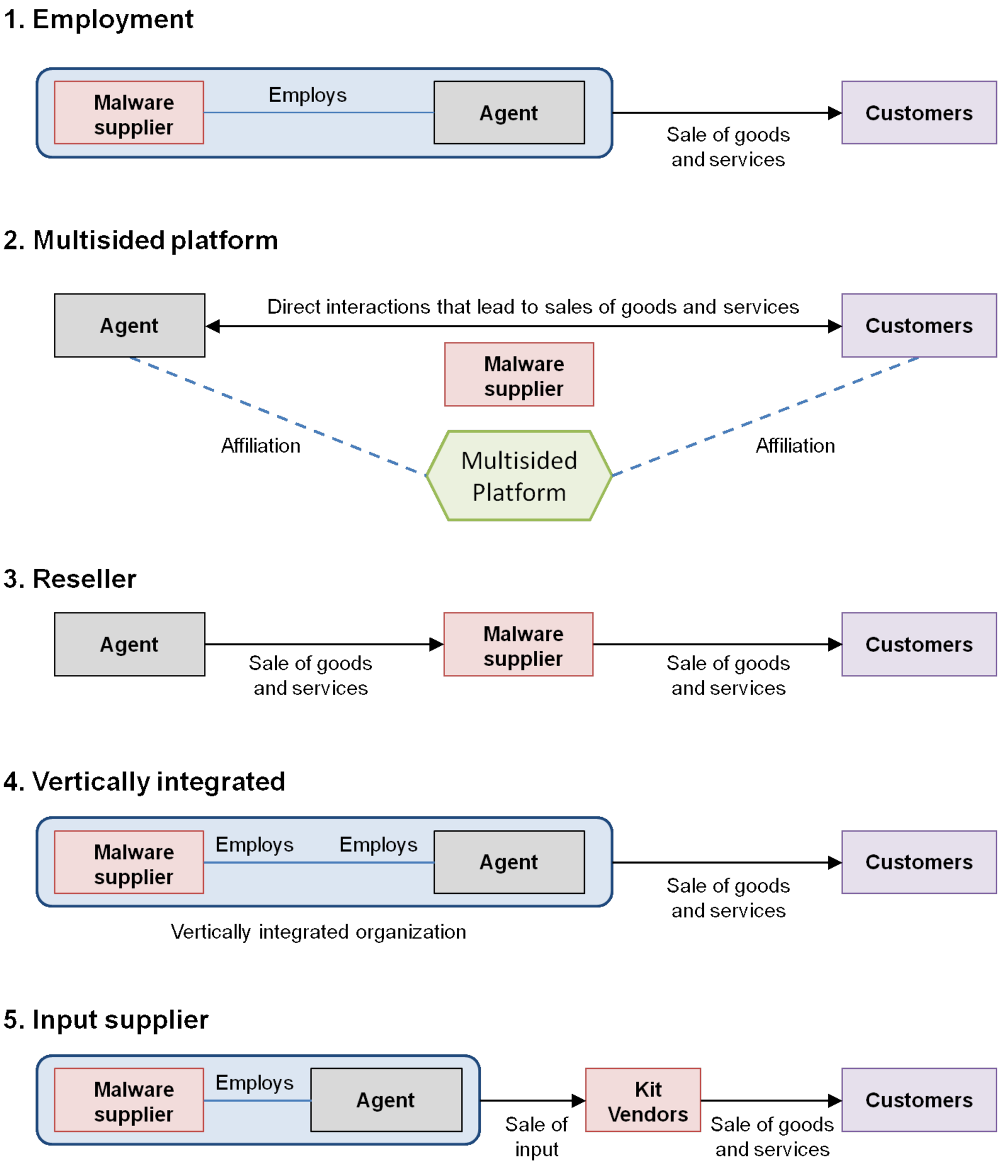

Figure 1. Modes to supply malware goods and services to customers

Further assume that the role of the agent is the same in all five modes: help monetize the output of the malware supplier. In the “employment” mode, the agent is an employee of the malware supplier. In the “multisided platform” mode, the agent is an affiliated independent professional who is enabled by the malware supplier’s multisided platform to provide goods and services directly to customers. In the “reseller” mode, the agent (shown as Seller in Figure 1) sells those goods and services to the malware supplier that their customers wish to purchase. In the “vertically integrated” mode, both the agent and the malware supplier are employees of the same organization. In the “input supplier” mode, the agent is either an employee of the malware supplier or has no role. The malware supplier sells inputs to kit vendors, and these inputs become part of the goods and services kit vendors sell to customers located downstream in the value chain.

Table 1 provides an example of non-contractible actions organized into the three action types identified in the previous section. Note that the information on Table 1 depends on the role of the agent. Recall that, in our example, the agent’s role is to help monetize the outputs of the malware supplier. If the role of the agent was a technical one, the information in rows denoted 2 and 3 in Table 1 would be different.

The non-contractible actions that can solely be carried out by the malware supplier are those which are part of an ongoing investment in the firm. These actions are non-transferable. The non-contractible actions that can solely be carried out by the agent are those that are part of an ongoing effort made by the agent in the provision of its service. These actions are also non-transferable.

Table 1. Non-contractible actions by type

Action Type	Possible Non-Contractible Actions
1. Actions that can be carried out solely by the malware supplier	• Design and maintain the system to avoid detection • Maintain and upgrade code and techniques to reuse in attack approach • Operate specialized equipment to write and test new code as well as integrate new and reused code • Control code versions and modules • Design information and communications infrastructure • Automate the exploitation of client-side vulnerabilities (e.g., target browsers and programs that a website can invoke through the browser)
2. Actions that can be carried out solely by the agent	• Market and sell • Manage service quality • Develop new distribution and sales channels
3. Transferable actions that can be carried out by the malware supplier or the agent	• Assemble and update information about product–market fit • Support customers • Target vulnerabilities to exploit • Train customers and intermediaries • Promote in the underworld • Avoid detection of off-line operations • Arrange for escrow payments • Leverage others’ communications infrastructures (e.g., botnets) and people networks

Non-contractible actions that can be carried out by the malware supplier or the agent are referred to as transferable actions. In the general model with one agent developed by Hagiu and Wright (2015c), the mode in which the malware supplier operates depends on whether the firm or the agent controls the transferable actions. In our example, if the malware supplier chooses to operate in the “employment” mode or the “vertically integrated mode,” it must control the transferable actions shown in row 3 of Table 1.

The main difference between the “employment” and “vertically integrated” modes is that, in the “employment” mode, the malware supplier employs the agent; whereas, in the “vertically integrated” mode, the malware supplier and the agent both work for a vertically integrated organization. If the malware supplier chooses to operate in the "platform” mode, it must enable the agent to control transferable actions.

What is less clear is how to best apply the general model with one agent developed by Hagiu and Wright (2015c) to the “reseller” and “input supplier” modes. Hagiu (2007) formally compared the “reseller” and “two-sided platform” modes using four fundamental economic factors: indirect network effects between buyers and sellers; asymmetric information between sellers and the intermediary; investment incentives; and product complementarities/substitutability. Hagiu concluded that the “reseller” mode is more profitable when the degree of complementarity among sellers’ products is higher and it is very difficult to bring the two-sides to the platform together and spark interactions. The “two-sided platform” mode is preferred when seller investment incentives are important or when there is asymmetric information regarding seller product quality (Hagiu, 2007). This type of guideline focuses on constructs that are difficult to observe and would be difficult to apply in practice, particularly when studying the malware market.

Hagiu and Wright (2015a) compared the “multisided platform” mode with the “reseller” mode and concluded that the decision of which mode to select depends on whether suppliers affiliated to the platform or the reseller have more important information relevant to the optimal tailoring of marketing activities for each specific product. When applied to our example, we interpret the conclusion in Hagiu and Wright (2015a) to mean that the “reseller” mode requires the malware supplier to have control rights over important information that is relevant to assemble and update the product–market fit of the goods and services provided to customers.

The supplier input mode has not been formally studied as much as the other four modes have been. Hagiu and Wright (2015b) made two observations when informally comparing the “input supplier” and the “multisided platform” modes. The first observation was that, when a firm operates in the “input supplier” mode, not all relevant customer types are on board. However, when the firm operates in the “multisided platform” mode, all relevant customer types are affiliated to the platform. The second observation was that, when the firm operates in the “input supplier” mode, it does not benefit from indirect network effects between users and application developers.

For the purpose of our example, we interpret the observations by Hagiu and Wright (2015b) to mean that, when operating in the “input supplier” mode, the malware supplier derives benefits from bringing on board kit vendors as customers, but does not find significant benefits by bringing onboard the kit vendors’ customers. We conclude that the malware supplier and the agent will invest in non-contractible actions related to supporting kit vendors but not downstream customers.

Contribution

The framework presented in this article can be used to anticipate the mode in which a malware supplier with one agent will function. If a malware supplier controls the un-contractible actions that could be carried out by the agent, it will function in the “employment” mode. If the malware supplier enables the affiliated agent to interact directly with affiliated customers, the malware supplier will function in the “multisided platform” mode. If the malware supplier has control rights over important information that is relevant to assemble and update product–market fit of the goods and services provided to customers, the malware supplier will operate in the “reseller” mode. If the malware supplier and the agent are both employed by the same organization, the malware supplier will function in the “vertically integrated” mode. If the malware supplier invests in non-contractible actions to support kit vendors but not downstream customers, it will operate in the “input supplier” mode.

The ability to anticipate the modes in which malware suppliers will function improves the classification of malware suppliers, agents, and customers; it enables defences to be tailored to address attacks of a particular type; it increases the number and quality of operational insights; it enables targeted operations; and it increases the productivity of experimenting with new ways of protecting organizations and individuals against cyberattacks.

The proposed framework can also be used to study which types of malware suppliers, agents, and customers are attracted to each mode, discover new modes, and specify the threat space a malware supplier poses. A better understanding of the actors that each mode attracts, an improved ability to discover new modes, and an improved specification of the threat space offers to lower the impact of improbable events such as those referred to as "black swan" events (Taleb, 2007).

Conclusions

We build on recent advances in the theory of multisided platforms to develop a framework that can be used to examine the various approaches that malware suppliers can take to deliver goods and services to customers. We provide an elemental model distilled from the general model with one agent developed by Hagiu and Wright (2015c). By elemental model, we mean that the model has been reduced to stark simplicity for the purpose of increasing its adoption as an integrative framework to formally examine the modes in which malware suppliers operate. This approach involves judgement, and it is consistent with research that attempts to formalize different theories (Gibbons, 2005). This elemental model is then used to identify five modes we believe that malware suppliers use to provide goods and services to their customers.

This study discusses the application of a theoretical model, essentially ignoring empirical testing and the formal mathematical proofs provided by the researchers to specify the various models. The next steps for this work are: i) to examine existing known marketplaces for the purpose of detailing the framework described in this article and ii) to develop a model with multiple agents and spillovers that is specific to the modes used by malware suppliers.

This article is the first step to develop a theoretically sound framework that can be used to examine the various modes that malware suppliers use to produce and sell malware.

We expect a more formal approach to characterizing the modes in which malware suppliers function will decrease the number and impact of cyberattacks.

About the Authors

Tony Bailetti is an Associate Professor in the Sprott School of Business and the Department of Systems and Computer Engineering at Carleton University, Ottawa, Canada. Professor Bailetti is the Director of Carleton University's Technology Innovation Management (TIM) program. His research, teaching, and community contributions support technology entrepreneurship, regional economic development, and international co-innovation.

Mahmoud M. Gad is a Research Associate at VENUS Cybersecurity. He holds a PhD in Electrical and Computer Engineering from the University of Ottawa in Canada and an MSc in Electrical and Computer Engineering from the University of Maryland in College Park, United States. His research interests include cybercrime markets, machine learning for intrusion detection, analysis of large-scale networks, and cognitive radio networks.

References

Ablon, L., Libicki, M. C. & Golay, A. A. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Santa Monica, CA: Rand Corporation.
http://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf

Armin, J. & Komarov, A. 2013. *Mobile Fraud: Mobile Threats and the Underground Marketplace.* Lexington, MA: APWG.
http://docs.apwg.org/reports/mobile/apwg_mobile_fraud_report_april_2013.pdf

Boudreau, K. 2010. Open Multisided Platform Strategies and Innovation: Granting Access vs. Devolving Control. *Management Science,* 56(10): 1849–1872.
http://dx.doi.org/10.1287/mnsc.1100.1215

Boudreau, K. J., & Hagiu, A. 2009. Multisided Platform Rules: Multisided Platforms as Regulators. In A. Gawer (Ed.), *Multisided Platforms, Markets, and Innovation:* 163–191. Northampton, MA: Edward Elgar.

Choudary, S. P. 2015. *Platform Scale: How an Emerging Business Model Helps Startups Build Large Empires with Minimum Investment.* Platform Thinking Labs.

Clark, L. 2015. Hacker Forum Darkode Is Back and More Secure than Ever. *Wired,* July 28, 2015. Accessed February 1, 2016:
http://www.wired.co.uk/news/archive/2015-07/28/darkode-back-and-more-secure

Edelman, E. 2015. How to Launch Your Digital Multisided Platform. *Harvard Business Review,* 93(4): 91–97.

Eisenmann, T., Parker, G., & Alstyne, M. V. 2006. Strategies for Two-Sided Markets. *Harvard Business Review,* 84(10): 92–101.

Europol. 2015. Cybercriminal Darkode Forum Taken Down through Global Action. *Europol,* July 15, 2015. Accessed February 1, 2016: https://www.europol.europa.eu/content/cybercriminal-darkode-forum-taken-down-through-global-action

Gibbons, R. 2005. Four Formal(izable) Theories of the Firm? *Journal of Economic Behavior & Organization,* 58(2): 200–245. http://dx.doi.org/10.1016/j.jebo.2004.09.010

Goodin, D. 2014. Researchers Warn of New, Meaner Ransomware with Unbreakable Crypto. *Arstechnica,* January 6, 2014. Accessed February 1, 2016: http://arstechnica.com/security/2014/01/researchers-warn-of-new-meaner-ransomware-with-unbreakable-crypto/

Gu, L. 2013. *The Chinese Underground in 2013.* Irving, TX: Trend Micro. http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-chinese-underground-in-2013.pdf

Hagiu, A. 2007. Merchant or Two-Sided Platform? *Review of Network Economics,* 6(2): 115–133. http://dx.doi.org/10.2202/1446-9022.1113

Hagiu, A. 2009. Two-Sided Platforms: Product Variety and Pricing Structures. *Journal of Economics & Management Strategy,* 18(4): 1011–1043. http://dx.doi.org/10.1111/j.1530-9134.2009.00236.x

Hagiu, A. 2014. Strategic Decisions for Multisided Platforms. *MIT Sloan Management Review,* 55(2): 71–82.

Hagiu, A. & Wright, J. 2013. Do You Really Want to Be an eBay? *Harvard Business Review,* 91(3): 102–108.

Hagiu, A., & Wright, J. 2015a. Marketplace or Reseller? *Management Science,* 61(1): 184–203. http://dx.doi.org/10.1287/mnsc.2014.2042

Hagiu, A., & Wright, J. 2015b. Multi-Sided Platforms. *International Journal of Industrial Organization,* 43: 162–174. http://dx.doi.org/10.1016/j.ijindorg.2015.03.003

Hagiu, A., & Wright, J. 2015c. *Enabling Versus Controlling.* Harvard Business School: Working Paper, 16-002. Boston, MA: Harvard Business School.

Kamluk, V. 2009. *The Botnet Ecosystem.* Woburn, MA: Kaspersky Lab. http://latam.kaspersky.com/sites/default/files/knowledge-center/kl_botnet%20ecosystem.pdf

Kovacs, E. 2015. Hacking Forum Darkode Resurfaces. *Security Week,* July 28, 2015. Accessed February 1, 2016: http://www.securityweek.com/hacking-forum-darkode-resurfaces

Krebs, B. 2013. Styx Exploit Pack: Domo Arigato, PC Roboto. *Krebs on Security,* July 13, 2013. Accessed February 1, 2016: http://krebsonsecurity.com/2013/07/styx-exploit-pack-domo-arigato-pc-roboto/

Mathews, L. 2014. $100 Malware Kit Lets Anyone Build Their Own CryptoLocker. *Geek.com,* January 7, 2014. Accessed February 1, 2016: http://www.geek.com/apps/100-malware-kit-lets-anyone-build-their-own-cryptolocker-1581505/

Peters, S. 2015. Hacking Team 0-Day Shows Widespread Dangers of All Offense, No Defense. *DarkReading,* July 8, 2015. Accessed February 1, 2016: http://www.darkreading.com/attacks-breaches/hacking-team-0-day-shows-widespreaddangers-of-all-offense-no-defense/d/d-id/1321224

Samani, R. 2013. *Cybercrime Exposed: Cybercrime-as-a-Service.* Santa Clara, CA: McAfee. http://www.mcafee.com/ca/resources/white-papers/wp-cybercrime-exposed.pdf

Taleb, N. N. 2007. *The Black Swan: The Impact of the Highly Improbable.* New York: Random House.

The Chosunilbo. 2015. N. Korean Hackers Get Access to 'Unbeatable' Tools. *The Chosunilbo,* July 22, 2015. Accessed February 1, 2016: http://english.chosun.com/site/data/html_dir/2015/07/22/2015072201500.html

WikiLeaks. 2015. Hacking Team. *WikiLeaks,* July 8, 2015. Accessed February 1, 2016: https://wikileaks.org/hackingteam/emails/

Citation: Bailetti, T., & Gad, M. 2016. Examining the Modes Malware Suppliers Use to Provide Goods and Services. *Technology Innovation Management Review,* 6(2): 21–27. http://timreview.ca/article/965

Keywords: cybersecurity, cybercrime, malware, suppliers, modes, agents, customers, multisided platform