Online Cybercrime Markets and Cybercrime as a Service

Jin R. Lee, Michigan State University
Leejin26@msu.edu

ABSTRACT: With digital technology becoming more widespread, traditional crimes have steadily shifted into online spaces – most notably, the emergence of online illicit markets and the buying and selling of cybercrime services. However, there is a lack of knowledge around how online criminal markets operate, price services, negotiate deals, and distribute products and/or services. As a result, this Backgrounder presents an overview of online cybercrime markets, with a focus on the illegal online markets for cybercrime services, stolen data, and cybercrime tools.

With digital technology becoming increasingly widespread, traditional offline crimes have steadily shifted into online spaces. In fact, while crime rates in most Western societies have seen declines in recent years, cybercrime rates have witnessed towering growths[1]. However, despite this trend, there is a lack of knowledge around how online criminal markets operate, price services, negotiate deals, and distribute products and/or services.

The purpose of this Backgrounder is to provide an overview of how online criminal markets operate, price services, negotiate deals, and distribute products and/or services. In particular, this Backgrounder will focus on the illegal online markets for cybercrime services, stolen data, and cybercrime tools.

Online Cybercrime Markets

Cybercriminals, which include both buyers and sellers, gather together in online settings to perform business transactions where a wide selection of products and services are exchanged. Products sold through illicit online markets generally fall into three broad categories[2]: (1) *stolen data* from credit cards, bank accounts, online payment accounts, and other personal credentials and/or information (e.g., login IDs and passwords); (2) *cybercriminal tools* such as malware (i.e., malicious software), hacking tools/packages, botnets, and phishing kits; and (3) *cybercriminal services* such as cash out and consulting services.

Online cybercrime markets are made up of buyers and sellers who have various technological skills and expertise[3]. Low-tech savvy buyers are able to acquire stolen data, credentials, and pre-made tools to execute their attacks. Vendors, such as those offering money mule services or stolen data, may also be inexperienced individuals who make profits over the online market[4]. It is worth noting that the majority of buyers seem to be in this low-tech group. Finally, a small group of vendors are highly skilled and perform additional roles within the market as moderators and content experts[5].

Online Market Operations

Research has shown that sellers tend to use web forums and Internet Chat Relay (ICR) to advertise products, while buyers post "wanted" ads for various services[6]. Some online markets use moderators, which can

[1] Aebi & Linde, 2010; Farrell, Tseloni, Mailley, & Tilley, 2011; Ouimet, 2002; Tcherni, Davies, Lopes, & Lizotte, 2015
[2] Ablon, 2018; Leukfeldt, Kleemans, & Stol, 2017
[3] Ablon, 2018
[4] Ablon, 2018
[5] Ablon, 2018
[6] Hutchings & Holt, 2015

increase trust among buyers and sellers[7]. For example, moderators may remove members that scam others out of money or verify sellers and their products.

In some advertisements, sellers will offer multiple points of contact on how to negotiate prices and deals[8]. To complete transactions, buyers and sellers may use additional communication methods that provide them with more privacy, such as private messaging apps or direct messaging features found on forums. Money is also exchanged using multiple methods. Sometimes an escrow or a "go-between" individual ensures that both product and money are properly exchanged between the involved parties. This establishes trust in buyers who have to manage the risk of being scammed and/or ripped off[9].

After a transaction takes place, buyers are often allowed to leave positive or negative feedback[10]. This allows the behavior of market participants to be influenced by social forces that try to maximize rewards and reduce risk for buyers and sellers[11].

Product Pricing and Cybercrime Revenue

Pricing for cybercrime as service varies depending on the product and/or service, but often resemble pricing strategies used in legal service industries. For instance, stolen data may be priced differently based on desirability and quality, with higher limit credit cards selling for greater fees[12].

In terms of cybercrime services sold on illicit online markets, a seller may create malware and advertise its capabilities in the underground market either directly or indirectly through an advertiser[13]. This allows less tech-savvy buyers to purchase preassembled malware. Similar to how stolen data is priced, hacking-as-a-service is valued based on the amount of time and expertise it takes to complete the task.

Buyers are also given the ability to purchase "bulletproof services" from various providers in the cybercrime market to enhance their privacy from law enforcement detection – that is, bulletproof services weaken the detectability of offenders so that even if the attack is spotted, the attacker's identification is hidden.

Pricing significantly influences cybercrime market behavior. Services, tools, and data that are disproportionately priced can come under scrutiny, triggering a vetting process of both the vendor and the product[14]. Since buyers and sellers could be working with different currencies, the involved parties may hire an individual who is able to convert e-currency into usable currency.

Conclusion/Implications

With online technology becoming more commonplace in society, cybercrime attacks that generate data loss, data manipulation, and unauthorized access to devices will increasingly require a reliable solution. Interestingly, a great proportion of cybercrime and cybersecurity discussions have focused on national security threats that pose problems to critical infrastructure and/or on cyber-spying campaigns that target valuable intellectual property rather than on the more mundane cybercrime acts that affect a greater number of people[15].

[7] Holt, Smirnova, & Hutchings, 2016
[8] Hutchings & Holt, 2015
[9] Holt et al., 2016
[10] Holt, Smirnova, Chua, & Copes, 2015
[11] Holt & Lampke, 2010
[12] Holt & Lampke, 2010
[13] Sood & Enbody, 2013
[14] Holt, 2013
[15] Brito & Watkins, 2011; Dupont, 2013

Many police agencies and government departments are under-resourced to effectively deal with these cybercrime issues; allowing sellers to continuously advertise equipment, applications, and services to potential buyers[16].

In order to prevent the dangers posed by online cybercrime markets, political and legal institutions need to be better equipped to keep up with the changes in digital technology[17] – including law enforcement agencies. Another possible solution is to anticipate future attacks and structure our legal system in such a way that reduces legal loopholes and manages offenders in both an efficient and effective manner[18].

References

Ablon, L. (2018). The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.

Aebi, M., & Linde, A. (2010). Is there a crime drop in Western Europe? European Journal on Criminal Policy and Research, 16(4), 251–277.

Farrell, G., Tseloni, A., Mailley, J., & Tilley, N. (2011). The crime drop and the security hypothesis. Journal of Research in Crime and Delinquency, 48(2), 147–175.

Ouimet, M. (2002). Explaining the American and Canadian crime drop in the 1990's. Canadian Journal of Criminology, 44(1), 33–50.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2015). The dark figure of online property crime: is cyberspace hiding a crime wave? Justice Quarterly, 33(5), 890–911.

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The Use of Online Crime Markets by Cybercriminal Networks: A View From Within. *American Behavioral Scientist*, *61*(11), 1387–1402.

Hutchings, A., & Holt, T. J. (2015). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology*, *55*(3), 596–614.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(May), tyw007.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behanvior*, *37*(4), 353–367.

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

Holt, T. J. (2013). Examining the Forces Shaping Cybercrime Markets Online.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: products and market forces. *Criminal Justice Studies Klockars*, *23*(1), 33–50.

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

Brito, J., & Watkins, T. (2011). Loving the cyber bomb-the dangers of threat inflation in cybersecurity Policy. *Harv. Nat'l Sec. J.*, *3*, 39.

Dupont, B. (2013). Cybersecurity Futures: How Can We Regulate Emergent Risks?. *Technology Innovation Management Review*, *3*(7), 6-11.

Dupont, B. (2017). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, law and social change*, *67*(1), 97-116

[16] Dupont, 2013; 2017
[17] Dupont, 2013
[18] Dupont, 2013