Crimeware Marketplaces and Their Facilitating Technologies

Mahmoud Gad

> “*The cause is hidden. The effect is visible to all.*”
>
> Publius Ovidius Naso (43 BC – AD 17/18)
> Poet

The cybercrime community has evolved from one in which criminals develop their own tools into one in which crimeware – tools and services to carry out or facilitate illegal online activity – can be readily bought, sold, traded, hired, or licensed in online marketplaces. Crimeware marketplaces are expected to grow significantly in the near term, and they will offer an increasing number of services and tools that target mobile computing devices. This article examines the actors, value chains, and modes of operation in underground crimeware marketplaces, and it identifies three facilitating technologies that are likely to significantly expand the reach of cybercriminals. Anonymous e-currency (e.g., Bitcoin) enables anonymous financial transactions; anonymity networks (e.g., Tor) enable anonymous Internet access; and mobile computing provides access to a very large number of potential target devices.

Introduction

Over the past 20 years, the degree of sophistication of cybercrimes has increased while the knowledge of the typical intruder has decreased (Ablon et al., 2014). How is it that more sophisticated crimes are being committed by less sophisticated criminals? These seemingly paradoxical trends may be a direct result of value chains anchored on crimeware marketplaces.

Today, online marketplaces exist where participants use web-based platforms to meet, discuss, exchange, and buy and sell goods and services to enable cybercrime activities (Goncharov, 2012, 2014; Holt, 2013; Kraemer-Mbulaa et al., 2013; Lusthaus, 2013). These crimeware marketplaces provide an easy way to find co-offenders, keep up to date on current cybercrime practices, and coordinate actions to gain competitive advantages in specific market niches (Lusthaus, 2013).

Cybercrime refers to a criminal offence involving a computer as the object of the crime (e.g., computer hacking and unauthorized use of computer systems) or as the tool used to commit a material component of the offence (e.g., credit card fraud and identity theft perpetrated over the Internet) (Kowalski, 2002). The global annual cost of cybercrime is estimated to be between $0.3 and $1 trillion USD, which represents 0.4% to 1.4% of the global gross domestic product (McAfee, 2013, 2014).

Cybercrime supports underground economies in both developed and developing countries worldwide. The United States is considered the major generator of malware and the source of most cybercriminal attacks (Kraemer-Mbulaa et al., 2013), and several studies have examined crimeware marketplaces in the United States. For example, Thomas and Martin (2006) studied a marketplace specialized in financial fraud that leveraged the Internet Relay Chat (IRC) protocol. Franklin, Paxson, Perrig, and Savage (2007) were the first to empirically monitor and analyze the underground economy. China is also considered a major cybercrime hub, while Russia is considered to be the birthplace of cybercrime (Symantec, 2008; Goncharov, 2012). Recently, Brazil has emerged as a new player on the global cybercrime stage and its hackers have become known for financial frauds (Kshetri, 2010).

In this article, the actors, value chains, modes of operation, and mediums of exchange related to crimeware marketplaces are discussed. Then, three facilitating technologies that enable the growth of cybercrime marketplaces in the near future are identified. Finally, the last section provides the conclusions.

Crimeware Marketplaces

Cybercriminals rely on marketplaces much in the same way as legitimate businesses (Kraemer-Mbulaa et al., 2013). Cybercriminals have different computer skills as well as different motivations. Crimeware marketplaces enable specialization: a computer programmer can code a malware and sell it without becoming involved in the cybercrime operations and details. Crimeware marketplaces also lower the amount of technical skills required to enter the cybercrime world by providing low-skilled cybercriminals with all the necessary tools and support to commit their crimes. These marketplaces enable criminals to develop new hacking tools, recruit and retain talented individuals, develop required skills, and distribute the proceeds of crime among organizations (McAfee, 2013; Sood & Enbody, 2013). Examples of crimeware marketplaces places are listed below; further example can be found at DeepDot Web (tinyurl.com/lnlyzam):

1. *Evolution:* a marketplace for malware, credit card data, distributed denial-of-service (DDoS) attacks, and hacked accounts with a full-functioning automatic escrow system

2. *HPC:* a forum for Russian-speaking hackers with a marketplace section for buying and selling hacking tools and services

3. *Rescator:* an online market for buying and selling stolen credit cards

A number of high profile underground marketplaces were targeted by law enforcement agencies in United States and Europe in the past two years. The Silk Road marketplace, an underground marketplace for drugs, stolen credit cards, and other crimeware, was shut down by the Federal Bureau of Investigation in the United States in late 2013 (Zetter, 2013). Silk Road 2.0, along with 413 other underground marketplaces, were shut down in a joint operation between law enforcement agencies from 17 countries in late 2014 (Fox-Brewster, 2014). It is expected that the future of these markets is not centralized sites like Silk Road, but sites where listings, messaging, payment and feedback are all separated, controlled by no central party and thus very hard for law enforcement agencies to shut down (The Economist, 2014).

Key Elements

In this section, three key elements of underground marketplaces are discussed: i) actors, ii) value chains, and iii) modes of operation.

Actors

Ablon, Libicki and Golay (2014) studied different crimeware marketplaces and they identified three main actors that operate in typical crimeware marketplaces:

1. *Subject-matter experts and administrators:* elite security researchers, exploit developers, malware coders, identity collectors, programmers, and technology experts who research, develop, and support innovative ideas and products in cybercrime marketplaces. They possess sophisticated technical skills and they operate as wholesale sellers to other vendors.

2. *Vendors:* crimeware operators such as crime-as-a-service providers, spammers, botnet owners, drop-service providers, distributors, and ID/financial data providers. They can be technically sophisticated or not, depending on the type of the product or the service they are selling.

3. *General members:* generally buyers and sometimes observers who visit those marketplaces for research, learning, or out of curiosity. They are typically the least technically skilled of the three actors.

Value chains

A value chain refers to the activities carried out to deliver a valuable product or service for a market (Porter, 1985). The value chain is a key concept in legitimate businesses as well as criminal communities.

Kramer-Mbulaa, Tangb, and Rusha (2013) identified three core activities in the value chains designed to carry out credit card fraud: i) the detection of vulnerabilities in a digital system, ii) the distribution of malware, and iii) the exploitation of network vulnerabilities. Each of these activities is typically carried out by a specialized group. The first activity is carried out by professional hackers and it is considered as the most technically complex. The second activity is carried out by sellers of malicious software in online marketplaces. The third activity is carried out by criminal gangs, and it is considered to be the least complex.

Modes of operation

This section reviews five cybercrime modes of operation facilitated by crimeware marketplaces.

1. *Crimeware-as-a-Service (CaaS):* the rental of malware, computing resources, and hosting services to commit cybercrimes (Sood & Enbody, 2013). CaaS customers do not require technical knowledge to launch an attack. Instead, a CaaS provider will attack a website on behalf of the customer, who need only identify a target, specify the type of service, and provide payment. The wide range of available services includes highly specialized password cracking, distributed denial-of-service (DDoS) attacks, and email spam.

2. *Pay-per-install:* cybercriminals may choose to outsource the distribution process of their malware applications to a third party. They provide this third party with the malware and how many targets they need to infect and pay them based on the final number of infected targets (Caballero et al., 2011).

3. *Crimeware toolkits:* "how-to" software packages that instruct users on how to infect a system and then retrieve data, such as corporate documents, personal photos, or credit card information, for financial gain. These off-the-shelf tools minimize the user's need for programming skills (Ben-Itzhak, 2009).

4. *Brokerage:* brokers act as a trusted intermediary between a seller and buyer of malware, stolen credit cards, or other illegal services (Holt, 2013). Trust between buyers and sellers is an issue in crimeware marketplaces, where there is no easy way to check the quality of the “product” or the “service” before completing the transaction. The brokerage operation mode emerged to partially fill this gap. As an example, in marketplaces for stolen credit cards, the broker will be one of the marketplace founders or operators who will hold the money from the buyer in a trust until the stolen credit card information, such as the card number, name on the card, etc., are verified by the broker and delivered to the buyer. The broker will then release the money to the seller in exchange for a brokerage fee.

5. *Data supplier:* data types include password lists, large spam email databases, medical records, driving license numbers, and corporate information are typical data that can be found in underground markets. Cybercriminals operate servers that are used as "drop sites" for private information harvested using malware.

Facilitating Technologies in Crimeware Marketplaces

In this section, we identify three facilitating technologies in crimeware marketplaces: anonymous e-currency (e.g., Bitcoin), anonymity networks (e.g., Tor), and mobile computing technology. The first two technologies enable anonymous financial transactions and anonymous Internet access, which are highly valued features for cybercriminals. The more these technologies become adopted in crimeware marketplaces, the harder it will be for law enforcement agencies to fight back against cybercrime. The third technology opened a large pool of cybercrime targets compared to the classical personal computing platforms.

Anonymous e-currency

Underground businesses typically use e-currency as a medium to instantaneously exchange money and avoid being tracked by law enforcement agencies. There are many e-currencies available in the market, such as Liberty Reserve, e-gold, WM Transfer, virtual gift cards, and prepaid phone cards. For an e-currency to be a successful option in underground marketplaces, its transactions should be internationally accepted, anonymous, irreversible, and unregulated (Lovet, 2006). However, at some point, cybercriminals must convert their profits into real currency, and there are service providers available to solve this problem. E-currency exchange providers charge fees to cash-out e-currencies based on the amount of a transaction and whether or not it involves the purchase of goods (Ablon et al., 2014).

Anonymous e-currency is a class of e-currency that provides anonymity to both buyers and sellers. Currently, the anonymous currencies market is dominated by Bitcoin, a software-based payment system introduced first as a concept in 2008 (Nakamoto, 2008) and then as open source software in 2009. Since then, the use of Bitcoin in online crimeware marketplaces has grown rapidly to the point that it now dominates all other payment methods in terms of adoption and volumes of transactions in most crimeware marketplaces (Ablon et al., 2014). Payments are processed and recorded on peer-to-peer basis without the need for a central repository or a single administrator. Although its status as a currency is disputed – the Internal Revenue Service in the United States considers it a commodity rather than a currency (Internal Revenue Service, 2014) – media reports often refer to Bitcoin as digital currency (Van Name, 2014).

Bitcoin offers all the four properties of an e-currency (internationally accepted, anonymous, irreversible, and unregulated) in addition to being independent from an issuing entity. Bitcoin is not issued by a central bank and it is not being operated by a company. With these unique properties, Bitcoin is the only anonymous and widely accepted e-currency in crimeware marketplaces. Currently, a growing number of legitimate businesses have started to accept Bitcoin as a method of payment. Bitcoin is also used in different illegal online marketplaces outside of cybercriminal marketplaces. For example, Bitcoin was the preferred method of payment for the original Silk Road marketplace and Silk Road 2.0.

The anonymity and the growing adoption of Bitcoin make it very challenging for law enforcement agencies to track (Ablon et al., 2014). A request for vendors to conduct research on how BitCoin can pose threats to national security has recently been issued by the United States (United States, Department of the Navy, 2014).

Due to the anonymity feature of Bitcoin, it is technically very hard for law-enforcement agencies to prevent their misuse. However, at some point, a Bitcoin holder will need to cash their Bitcoins into real money or services. New regulations can be implemented at these “exit points”. It may be possible to impose the same federal electronic-fund reporting limits imposed on cash and bank transfers, on e-currencies exchanges especially at the cash out point, such as Bitcoin to cash ATMs.

Anonymity networks
Anonymity networks enable anonymous and untraceable access to the Internet. Tor, which stands for "The Onion Router", is the most widely adopted such technology. Tor is an open source project to enable online anonymity and resist censorship. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays for the purpose of concealing a user's location or usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user, including visits to websites, online posts, instant messages, and other communication forms.

Tor networks enable the operation of anonymous website hosting and file sharing, and when combined with Bitcoin, they enable anonymous marketplaces for different criminal activities, including crimeware marketplaces. These un-indexed webpages exist in the Deep Web and operate as the previously discussed crimeware marketplaces but with an added layer of anonymity protection.

Mobile computing devices
The sales of personal computers have declined while the sales of mobile devices for both work and personal use have increased (Sher & Ovide, 2013; Gartner, 2013). This change in consumer preferences is reflected in the cybercriminal underground economy. This sharp increase in mobile devices sales increases the number of targets available to cybercriminals. According to a Gartner’s report on the mobile phone market (Atwal et al., 2013), the Android operating system was installed on 78.4% of the one billion mobile phones sold worldwide in 2013. Because of Android’s quick and wide-scale adoption, it has become the target of malicious applications, which continue to increase in number (Jianwei et al., 2012). This shift towards mobile computing devices is alarming to the cybersecurity community. Yu (2013) expects an increase in the number of available malware applications in online underground marketplaces that are specifically designed for mobile devices.

Prevalence of facilitating technologies
The SERT Quarterly Threat Intelligence Report (2013) shows an increase of 350% in Tor traffic in the third quarter of 2013. This increase is believed to be in part due to privacy concerns after Edward Snowden’s revelations and in part due to cybercriminals using Tor networks to protect their identities in online marketplaces as well as to control their bot network command centers. Also, the report notes that the majority of the new crimeware marketplaces opened in 2013 and later were hosted on "Deep Web" (wikipedia.org/wiki/Deep_Web) hosting servers accessible only by Tor browsers. Also, the report states that Bitcoin is now the de facto payment method in the majority of crimeware marketplaces. There are no statistics about the market share of the Deep Web hosted crimeware marketplaces with respect to all crimeware marketplaces, but these technologies are the preferred choice for new marketplaces as well as for any upgrades in the old crimeware marketplaces.

The anonymity of these technologies lowers the risk of conducting business in crimeware marketplaces, which possibly will increase the overall number of participants in cybercrime activities. In addition, the effect of these technologies goes beyond the cybercrime domain into other domain such as money laundering and cyberterrorism. Although e-currency money-laundering activities are still in their infancy, compared to regular-currency money laundering, Bryans (2014) predicts an increase in e-currency money-laundering activities due to the lack of foresight by regulation writers, which creates a legal grey area. Thus, criminals can continue to capitalize on the unique features of e-currencies to grow their "businesses". Although Jarvis and colleagues (2014) concluded that cyberterrorism is still in an early stage, crimeware marketplaces coupled with anonymity technologies can lower the technical barrier required to launch such attacks, which may increase the risk of cyberterrorism in the near future.

Conclusion

Cybercrime activities are expected to continue to grow and their impact on the global economy will increase. In this article, we have identified three facilitating technologies in crimeware marketplaces that simultaneously offer anonymity and enable cybercriminals to reach an increasing number of targets. These technologies present new challenges to law enforcement agencies, governments, financial institutions, and corporations. More regulations are needed for e-currency exchanges to try to minimize their illegal use. Periodic monitoring and content analysis of crimeware marketplaces can enable the prediction of near-future small to mid-size security threats.

About the Author

Mahmoud M. Gad is a PhD candidate in Electrical and Computer Engineering with a focus on wireless network communications at the University of Ottawa in Canada. Additionally, he holds an MSc in Electrical and Computer Engineering from the University of Maryland in College Park, United States. His research interests include chaos-theory-based security algorithms for wireless networks, analysis of large-scale networks, Internet of Things (IoT), cognitive radio networks, and data mining algorithms.

References

Ablon, L., Libicki, M. C., & Golay, A. A. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar. Report number: RR-610-JNI.* Santa Monica, CA: RAND Publications.
http://www.rand.org/pubs/research_reports/RR610.html

Atwal, R., Tay, L., Cozza, R., Nguyen, T. H., Tsai, T., Zimmermann, A., & Lu, C. K. 2013. *Forecast: PCs, Ultramobiles, and Mobile Phones, Worldwide, 2010-2017, 4Q13 Update.* Stamford, CT: Gartner.
http://www.gartner.com/doc/2639615

Ben-Itzhak, Y. 2009. Organised Cybercrime and Payment Cards. *Card Technology Today*, 21(2): 10–11.
http://dx.doi.org/10.1016/S0965-2590(09)70057-X

Bryans, D. 2014. Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal,* 89(1): 441-472.
http://www.repository.law.indiana.edu/ilj/vol89/iss1/13

Caballero , J., Grier, C., Kreibich , C., & Paxson, V. 2011. Measuring Pay-Per-Install: The Commoditization of Malware Distribution. *Proceedings of the 20th USENIX conference on Security:* 13. San Francisco, CA: USENIX.

The Economist. 2014. The Amazons of the Dark Net. *The Economist,* November 1, 2014.

Franklin, J., Paxson, V., Perrig, A., & Savage, S. 2007. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS) 2007.* Alexandria, VA: Association for Computing Machinery.
http://dx.doi.org/10.1145/1315245.1315292

Fox-Brewster, T. 2014. Silk Road 2.0 Targeted in 'Operation Onymous' Dark-Web Takedown. *The Guardian,* November 7, 2014.

Goncharov, M. 2012. *Russian Underground 101.* Cupertino, CA: Trend Micro Incorporated.

Goncharov, M. 2014. *Russian Underground Revisited.* Cupertino, CA: Trend Micro Incorporated.

Gu, L. 2014. *The Mobile Cybercriminal Underground Market in China.* Cupertino, CA: Trend Micro Incorporated.

Holt, T. J. 2013. Examining the Forces Shaping Cybercrime Markets Online. *Journal Social Science Computer Review,* 31(2): 165-177.
http://dx.doi.org/10.1177/0894439312452998

Internal Revenue Service. 2014. *IRS Notice 2014-21.* United States Internal Revenue Service.
http://www.irs.gov/pub/irs-drop/n-14-21.pdf

Jarvis, L., Macdonald, S., & Nouri, L. 2014. The Cyberterrorism Threat: Findings from a Survey of Researchers. *Studies in Conflict & Terrorism,* 37(1): 68-90.
http://dx.doi.org/10.1080/1057610X.2014.853603

Jianwei, Z., Liang, G., & Haixin, D. 2012. *Investigating China's Online Underground Economy.* San Diego, CA: University of California Institute on Global Conflict and Cooperation.

Kshetri, N. 2010. *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives.* London: Springer.
http://dx.doi.org/10.1007/978-3-642-11522-6

Kowalski, M. 2002. *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.* Statistics Canada Catalogue No. 85-558-X. Statistics Canada, Canadian Centre for Justice Statistics.

Kraemer-Mbulaa, E., Tangb, P., & Rusha, H. 2013. The Cybercrime Ecosystem: Online Innovation in the Shadows? *Technological Forecasting and Social Change,* 80(3): 541–555. http://dx.doi.org/10.1016/j.techfore.2012.07.002

Lovet, G. 2006. Dirty Money on the Wires: The Business Models of Cybercriminal. Montreal: Virus Bulletin Conference 2006.

Lusthaus, J. 2013. How Organised is Organised Cybercrime? *Global Crime,* 14(1): 52–60. http://dx.doi.org/10.1080/17440572.2012.759508

McAfee. 2013. *The Economic Impact of Cybercrime and Cyber Espionage.* Center of Strategic and International Studies Report. Santa Clara, CA: McAfee.

McAfee. 2014. *Net Losses: Estimating the GlobalCost of Cybercrime.* Center for Strategic and International Studies. Santa Clara, CA: McAfee.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.org.* November 1, 2014: http://bitcoin.org/bitcoin.pdf

Porter, M. E. 1985. Competitive Advantage: Creating and Sustaining Superior Performance. New York: The Free Press.

SERT. 2013. *Quarterly Threat Intelligence Report - Q3, 2013.* Omaha, NE: Solutionary Security Engineering Research Team (SERT).

Sherr, I., & Ovide, S. 2013. Computer Sales in Free Fall. *Wall Street Journal,* April 11, 2013.

Sod, A. K., & R. J. Enbody. 2013. Crimeware-as-a-Service: A Survey of Commoditized Crimeware in the Underground Market. *International Journal of Critical Infrastructure Protection,* 6(1): 28-38. http://dx.doi.org/10.1016/j.ijcip.2013.01.002

Symantec. 2008. *Symantec Report on the Underground Economy: July 07–June 08.* Mountain View, CA: Symantec Corporation.

Thomas, R., & Martin, J. 2006. The Underground Economy: Priceless. *Login,* 31(6): 7-16.

United States, Department of the Navy. 2014. BAA for CTTSO/TSWG Support. Solicitation Number: N41756-14-Q-3272.

Van Name, T. 2014. BitCoin Now on Bloomberg. Press release: April 30, 2014.

Yu, R. 2013. GinMaster: A Case Study in Android Malware. Berlin: Virus Bulletin Conference 2013.

Zetter, K. 2013. How the Feds Took Down the Silk Road Drug Wonderland. *Wired,* November 19, 2013.

Citation: Gad, M. 2014. Crimeware Marketplaces and Their Facilitating Technologies. *Technology Innovation Management Review*, 4(11): 28–33. http://timreview.ca/article/847

Keywords: cybercrime, dark web, underground economy, Bitcoin, anonymity, crimeware marketplaces