Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law

Ting Zhang *

Faculty of Law, University of Hamburg, Hamburg, Germany

Keywords:
Cybercrime
Crime-as-a-service industry
Incrimination of individual aiding acts
Comparison of sanction patterns

ABSTRACT

In the context of the global information age, cases concerning the provision of technical assistance to commit cybercrimes are growing in leaps and bounds and a brand-new crime-as-a-service industry is beginning to take shape. German criminal law addresses this issue in the context of joint commission theory and individual incrimination as complementary, whereas the Chinese model, by contrast, has made marked progress in the fight against cyber aiding by introducing new criminal provisions. The change of cyber-aiding indeed represents a significant challenge to current criminal legislation and consideration of its criminal countermeasures is indispensably significant.

1. The emergence of crime-as-a-service industry

As the cybercriminal economy evolves and matures, a business of a particular kind has developed within hacking industry networks that undertakes to monetize technical skills and tools and make them accessible to cyber criminals. It has become known as the 'crime-as-a-service' industry. Up to now, the key classic elements of services that we can see in this underground market can be categorized as follows:

- Criminal infrastructure maintenance[1]: servers are a must in the commission of cybercrime, particularly for career cybercriminals. Instead of risking the undertaking of illicit activities on their own machines, law-breakers prefer to either connect to a dedicated server or a proxy server or appeal to hosting services, so as to evade law enforcement detection. Hosting providers play a critical role in the online criminal economy and bulletproof-hosting services are one of their most sought-after commodities.
- **Malware-related Services**: in a functional sense, malicious software appears in many forms, from those used for stealing, intercepting and altering user data, to hijacking a user's session or providing backdoors, etc.[2] In the first quarter of 2013 alone, there were reportedly over 6.5 million newly created malware samples[3]. Services falling under this category include design, development and distribution of

* University of Hamburg, Rothenbaumchaussee 33, 20148 Hamburg, Germany.
E-mail address: zhangting4766@hotmail.com.
http://dx.doi.org/10.1016/j.clsr.2016.11.017

[1] See Max Goncharov, *Russian Underground 101* (Trend Micro Incorporated, 2012), pp. 3–4.

[2] See e.g. Heli Tiirmaa-Klaar et al., *Botnets* (London: Springer-Verlag, 2013), pp. 46 et seq.; Michael Bailey et al., "Automated Classification and Analysis of Internet Malware," in Christopher Kruegel, Richard Lippmann, and Andrew Clark (eds.), *Recent Advances in Intrusion Detection: 10th International Symposium, RAID 2007, Gold Coast, Australia, September 5–7, 2007. Proceedings* (Berlin et al.: Springer, 2007), pp. 178 et seq.

[3] See Panda Security, "PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record," accessed August 6, 2016 at <http://www.pandasecurity.com/mediacenter/press-releases/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/>.

malware. In practice, as soon as cybercriminals detect any security flaw in software, hardware or an application, they attempt to exploit the vulnerability for their own gain or outsource the design of an 'exploitation kit' before it is patched. By mirroring themselves as a legitimate software development company, a malware-as-a-service business model not only offers a variety of malicious tools, customized malware included, but also provides full-time customer support and frequent patches and updates. In the current underground market, customizable malware kits with multiple exploits are most in demand[4] – epitomized by the 'Blackhole Exploit' Kit[5]. While there is a growing desire to dabble in cybercrime, criminals enlist malware dissemination into their range of services using distribution methods that vary depending on the type of target to be attacked[6]. A popular example is known as the 'pay-per-install' service, namely a service whereby the provider distributes malicious files for a customer and gets paid according to the number of downloads.[7]

- **Hacking Services**: the sphere of such services begins at a basic level like the hacking of email or social networking accounts undertaken by brute force[8]. There also exist more sophisticated forms, including launching distributed-denial-of-service attacks,[9] usually presupposing that the hacker has at least one botnet at his disposal. In addition, along with the constant commercialization of the Internet and increasing significance presented by traffic volume[10], website hacking also starts to flourish.
- **Unauthorized-information-related Services**: the online world is a digital space where many specific cyber offences could not be attainable without required information. Large volumes of compromised data are retailed in the digital underground economy, including not only personal and financial data such as bank account details and email addresses, but also scanned document copies necessary for identity verification, along with diverse timely information concerning website, program or application vulnerabilities. 'DarkMarket' was one of the most infamous online carding forums on which demand and supply of illicit materials such as compromised personal and financial data could meet.[11]
- **Money Laundering Services**: similar to that in the real world, where most traditional culprits need a channel to legitimize their criminal profits, cybercriminals as well require an outlet to cash out from the digital financial system. Typical providers, such as money 'mules', have a prominent role in connecting the online and off-line worlds.[12]

2. German and Chinese *de lege lata* against cyber-aiding

2.1. *German legislative status quo*

As far back as 2006, the German Bundesrat submitted a draft resolution to combat acts of aiding cybercrime, after it was revealed that misuse of devices had broken through territorial limits and had deteriorated into a worldwide problem. The German criminal code would be amended accordingly by referring to *The Council of Europe's Convention on Cybercrime* and *The Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks against Information Systems*, aiming at intensifying international criminal justice cooperation against computer crime.[13] At present German criminal law identifies four categories of such acts, including the crime of aiding data espionage or phishing, the crime of aiding another to tamper data as well as acts that support computer sabotage. Given that the last two kinds of offensive behaviour will be sanctioned pursuant to § 202c StGB, the focus of the following interprets this provision as introduced through *The Amendment (41) to the German Criminal Code*. The basic content is laid out as follows:

> *§ 202c Acts preparatory to data espionage and phishing*
> (1) *Whosoever prepares the commission of an offence under* section 202*a or* section 202*b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible*
> 1. *passwords or other security codes enabling access to data* (section 202*a (2)), or*
> 2. *software for the purpose of the commission of such an offence, shall be liable to imprisonment not exceeding two years or a fine.*
>
> (2) Section 149 *(2) and (3) shall apply mutatis mutandis.*

This provision aligns itself with Article 6 under the Convention on Cybercrime and is meant to prevent certain potentially dangerous aiding behaviours facilitating the commission of cybercrime and to protect the confidentiality of computer systems and data.[14] To be more precise, the object of this offence could be the release of security codes, in any

[4] See Steven R. Chabinsky, "The Cyber Threat: Who's Doing What to Whom?," US Federal Bureau of Investigation, accessed August 6, 2016 at <https://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom>.

[5] See European Police Office, *Internet Organised Crime Threat Assessment* (2014), p. 24.

[6] For more information see ibid.

[7] See Max Goncharov, *Russian Underground 101* (Trend Micro Incorporated, 2012), p. 6.

[8] See ibid., p. 16.

[9] See ibid., pp. 8–9.

[10] Traffic volume denotes the number of visitors (i.e., unique or otherwise) to a website over a certain period of time. For further explanation, see ibid., p. 23.

[11] See e.g. Misha Glenny, *Darkmarket: Cyberthieves, Cybercops and You* (Canada: Random House, 2011), pp. 107 et seq.; Caroline Davies, "Welcome to DarkMarket – Global One-stop Shop for Cybercrime and Banking Fraud," *The Guardian*, accessed August 10, 2016 at <https://www.theguardian.com/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley>; John Leyden, "DarkMarket Carder Forum Revealed as FBI Sting," accessed August 10, 2016 at <http://www.theregister.co.uk/2008/10/14/darkmarket_sting/>.

[12] See European Police Office, *Internet Organised Crime Threat Assessment*, p. 41; Steven R. Chabinsky, "The Cyber Threat: Who's Doing What to Whom ?," US Federal Bureau of Investigation, accessed June 25, 2015 at < https://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom>.

[13] *BT-Drs* 676/06, pp. 1–2.

[14] *BT-Drs* 16/3656, p. 8.