Money flow model in shadow information economics

Grigorii Borta

Abstract. This paper aims to research the money flows in shadow information economics from a botnet owner's point of view: main expenses and profit routs are analyzed.

Introduction. The negative impact of shadow information economic cannot be questioned. Estimates show that damage done to economy is tremendous and tends to rise every year. Shadow information economics is defined as all the criminal and illegal activity related to information technologies.

The main components of the model are as follows:

- Counteraction (law enforcement) – this category includes all the expenses related to avoiding detection and potential losses in case the botnet was detected, or the malefactor was caught. Legislation and law enforcement are usually the main sources of botnet counteraction, although software and hardware protection like anti-viruses, firewalls are an option as well.
- Research and analysis (the market for ideas) – this category includes all the research related to the vulnerabilities in the most wide-spread software and hardware, research related to law shortcomings, and market research. Malefactors usually buy the results of such researches, spending considerable amounts of money, or research by themselves, spending considerable amounts of time.
- Development – this stage usually encompasses the transformation of the vulnerabilities acquired earlier into malicious software that will be deployed to victim devices in order to gain profit later. Profit may be gained from victims' personal data, their devices' computing power, etc.
- Money laundering – a service targeted at legalizing of the profit acquired in the shadow domain of information economics. It is important to note that money can be laundered both in the information domain as well as outside of it. Usually this service is provided in exchange for a part of acquired profit.
- Pay-per-install – is a service that consists of malware installation on a victim's device. This method is extremely effective due to its versatility: there is no need to incorporate infection mechanisms into every piece of malware, thus greatly reducing research, development and testing costs.
- Command and control – this group of expenses includes hardware costs, command channels upkeep costs, internet service costs, electricity, search, creation and upkeep of proxy servers.
- Victims – this category includes both legal and natural persons, and government structures whose devices were infected, personal or confidential data stolen, or who have otherwise fallen a victim to shadow information economics.

Thus, the main source of malefactor's profit are the infected computers, while all the other elements are expenses and potential losses. To sum it up as a model:

$$\max_{(\text{profit})} = (\text{V} - \text{PPI} - \text{C} - \text{R}) \times \text{Ls} \times \text{L}$$

Where

- V – total payments received from the victims;
- PPI – device infection costs;
- C – command and control channels upkeep costs;

- R – research and analysis costs;
- Ls – money laundering service;
- L – expenses coefficient in the case of botnet being found.

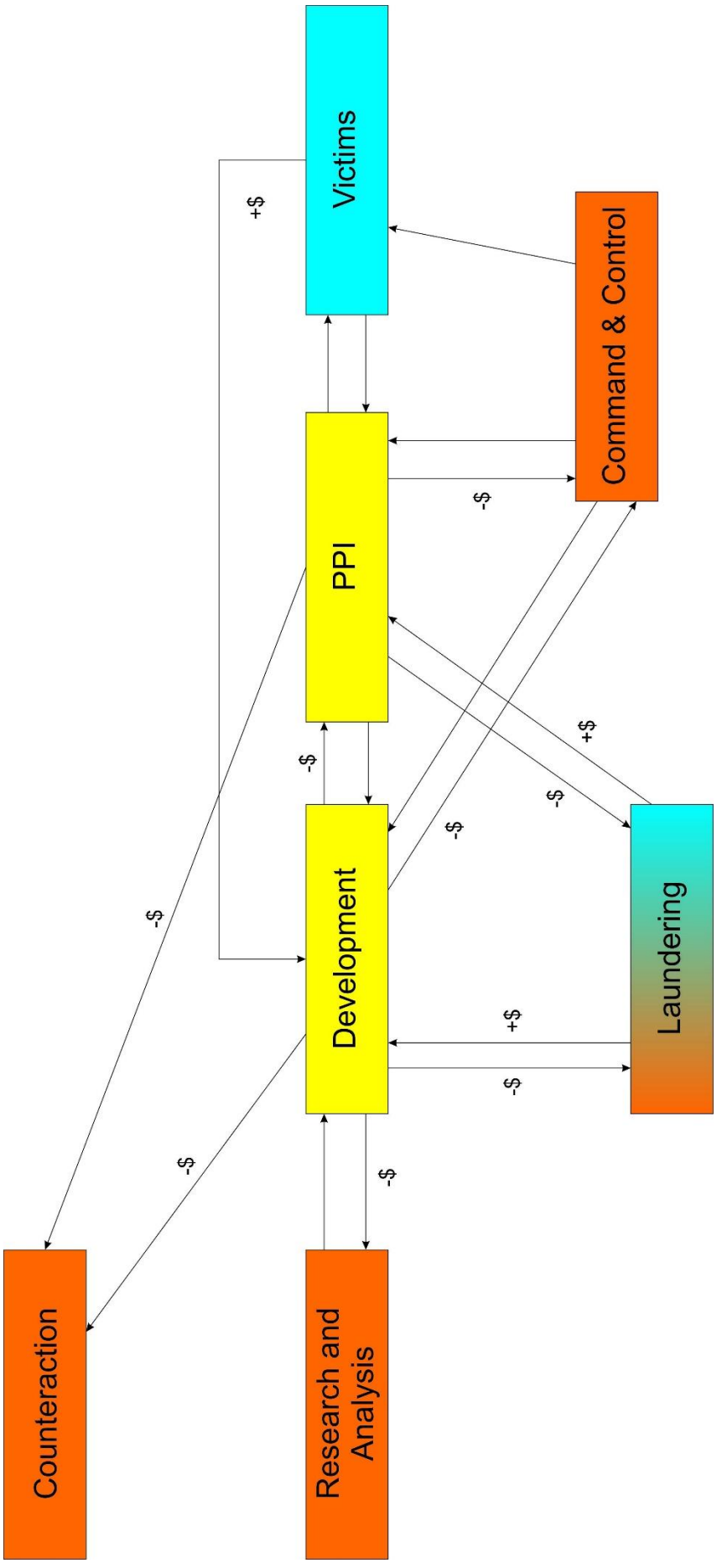

Figure 1. Money flow model

The proposed model by no means encompasses all the monetary flows involved in a botnet owner's profit model, a lot more research is further required in order to be able to develop efficient methods of struggle against shadow part of information economics.

Bibliography

CyberSource. (2013, 04). *2013 Online Fraud Report.* Retrieved 09 27, 2015, from www.cybersource.com: http://www.cybersource.com/content/dam/cybersource/CyberSource_2013_Online_Fraud_Report.pdf

Kaspersky Lab. (2000, 06 12). *TIMOFONICA Virus: Questions and Answers.* Retrieved 03 27, 2014, from Kaspersky Lab: http://www.kaspersky.com/news?id=68

Ponemon. (2012). *2012 Cost of Cyber Crime Study: United States.* Retrieved 09 27, 2015, from www.ponemon.org: http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf

Ponemon. (2012, 07). *2012 Payment Security Practices Survey: United States.* Retrieved 09 27, 2015, from www.ponemon.org: http://www.ponemon.org/local/upload/file/US_Cybersource_WPFinal.pdf

Ponemon. (2014). *2014 Cost of Cyber Crime Study: United States.* Retrieved 09 27, 2015, from idgenterprise.com: http://resources.idgenterprise.com/original/AST-0130677_2014_US_Cost_of_Cyber_Crime_Study_FINAL_2.pdf

Websense . (2014, 04 03). *Websense 2014 Threat Report.* Retrieved 09 27, 2015, from www.websense.com: http://www.websense.com/assets/reports/report-2014-threat-report-en.pdf

Websense. (2015, 04 08). *Websense 2015 Threat Report.* Retrieved 09 27, 2015, from www.websense.com: https://www.websense.com/assets/reports/report-2015-threat-report-en.pdf