Laundering Money Online: an Overview

Jean-Loup Richet

Abstract:
This chapter introduces my research on cybercriminals' money-laundering methods (Richet, 2013). It is the first of a series of chapters dedicated to current trends in online money laundering. We all know the oldest 'physical' placement methods of money launderers: cash smuggling, casinos and other gambling venues, insurance policies, hawalas / fe chi'en or the black market peso exchange, shell corporations, and so on and so forth. But there is also a number of online money laundering schemes currently being used by criminal enterprises to pass illegally received funds through legitimate accounts, and new ones are popping up all the time. Some of the most widespread schemes will be detailed in this series of chapters.

Keywords:

Cybercrime, online gaming, money laundering, micro laundering, black markets.

Introduction

Money laundering is a critical step in the cyber crime process which is experiencing some changes as hackers and their criminal colleagues continually alter and optimize payment mechanisms (Richet, 2012). Conducting quantitative research on underground laundering activity poses an inherent challenge: Bad guys and their banks don't share information on criminal pursuits. However, by analyzing forums, we have identified two growth areas in money laundering:

• Online gaming—Online role playing games provide an easy way for criminals to launder money. This frequently involves the opening of numerous different accounts on various online games to move money.

• Micro laundering—Cyber criminals are increasingly looking at micro laundering via sites like PayPal or, interestingly, using job advertising sites, to avoid detection. Moreover, as online and mobile micro-payment are interconnected with traditional payment services, funds can now be moved to or from a variety of payment methods, increasing the difficulty to apprehend money launderers. Micro laundering makes it possible to launder a large amount of money in small amounts through thousands of electronic transactions. One growing scenario: using virtual credit cards as an alternative to prepaid mobile cards; they could be funded with a scammed bank account – with instant transaction – and used as a foundation of a PayPal account that would be laundered through a micro-laundering scheme.

Laundering Money Online: a review of cybercriminals' methods

Millions of transactions take place over the internet each day, and criminal organizations are taking advantage of this fact to launder illegally acquired funds through covert, anonymous online transactions. The more robust and complex the various online marketplaces become the more untraceable methods criminals are finding to pass 'dirty' money into online accounts and pull 'clean' money out of others. The anonymous nature of the internet and the ever evolving technologies available allow numerous opportunities for online money laundering operations to take place. Many of these methods involve using a ruse to pull unsuspecting participants into their money laundering schemes, often with serious financial and legal consequences for victims. The best way for law abiding citizens to avoid becoming complicit in such illegal activities is to stay informed as to the methods criminals are using to pull them in.

We all know the oldest 'physical' placement methods of money launderers: cash smuggling, casinos and other gambling venues, insurance policies (launderers purchase them and then redeem them at a discount, paying fees and penalties but receiving a clean check from the insurance company), hawalas / fe chi'en or the black market peso exchange (informal value transfer system), shell corporations, and so on and so forth. But there is also a number of online money laundering schemes currently being used by criminal enterprises to pass illegally received funds through legitimate accounts, and new ones are popping up all the time. Some of the most widespread schemes are detailed in this article.

Methodology

Ostensibly, conducting quantitative research on underground laundering activity poses an inherent challenge: Bad guys and their banks don't share information on criminal pursuits. Our approach utilizes an online ethnography, observing large online hacker forums and communities and researching topics related to money laundering on their databases. We used a large variety of keywords, from those linked with payment solutions to those associated with black markets. After a first review, we filtered our data, and discarded irrelevant forum threads. We then analyzed the content of these threads and synthesize our findings into categories that will be explained in following blog posts.

Reference:

Richet, J.L. (2012). "How to Become a Black Hat Hacker? An Exploratory Study of Barriers to Entry Into Cybercrime." *17th AIM Symposium*.

Richet, J. L. (2013). Laundering Money Online: a review of cybercriminals methods. arXiv preprint arXiv:1310.2368.

***

Blog post from https://blogs.law.harvard.edu/jeanlouprichet/