iDEFENSE

VeriSign

// THE POWER OF INTELLIGENCE

Money Mules: Sophisticated Global Cyber Criminal Operations

An iDefense Security Report
Date

TABLE OF CONTENTS

1 Overview

In traditional illegal drug transactions, a "money mule" is simply the person carrying the cash. In the Information Age, the term has an additional meaning. "Money mules" are a lesser known, but very important, aspect of international carding operations and other types of online fraud. Recruited primarily (but by no means solely) in the United States, UK and Australia, money mules serve as money launderers, transferring illegal funds from carding and other fraud operations to criminals located primarily in the former Soviet Union. Many of the websites associated with money mule operations are registered in Panama, which is also the registered location of WebMoney, one of the most popular electronic money services among criminal carders.

This series explores the world of money mule operations and its attendant methodology. The goal is to better understand these techniques in order to assist in spotting potential criminal activities and mitigate them.

2 Background

Many money mules are either very young or naïve, and (at least claim to) believe that the operations in which they are involved are totally legal. Some money mules who suspect they may be involved in illegal activities rationalize their role in any number of ways, seeing it as an easy way to make cash without being held responsible for what is actually happening.

Fraudsters hire money mules through seemingly legitimate businesses (often spamming advertisements for positions via e-mail) and through career websites such as Monster.com. As shown later, one of the most outrageous scams involves an ad for a mule masquerading as a position for a charity representative.

Titles for these positions vary widely, but many have names such as:

- Private Financial Receiver
- Money Transfer Agent
- Country Representative
- Shipping Manager
- Financial Manager
- Sales Manager
- Sales Representative
- Secondary Highly Paid Job
- Client Manager

Money Mule employers typically require the applicant provide them with details of their personal bank accounts, a very unusual practice for legitimate business operations. Many of these job offers contain grammatical errors and other mistakes. While that in itself is not evidence to prove a cyber front operation, it should be seen as a red flag.

Another way to detect a money mule operation is to check the hiring company's WHOIS data; often it is only days old or incongruent with company statements. For example, one cyber front claimed to be in business for more than 100 years; however, WHOIS data shows that the website was only days old when the first mule solicitation was intercepted.

Organized criminal groups use money mules to launder money from one account to another, as various financial crimes are performed using stolen credit cards and other financial accounts. Mules commonly receive direct deposit payments to their personal account within the same country as the victim from whom the money is stolen. The mule then withdraws the cash and makes an overseas wire transfer to an account specified by the company. Mules collect either a certain percentage of the transfer or a base salary.

2.1 Australia: 61 Mules Arrested in Conjunction with World Transfers Inc.

In January 2005, a story broke about a keylogger Trojan, naïve teens and an online phishing scam in Australia. More than 60 people were arrested, many of them teenagers ranging in age from 15 to 17. The money mules were reportedly assisting a global phishing operation; the teens reportedly laundered money from banks to accounts in Russia, collecting a commission based on how much money they moved. Mules reportedly earned $200-500 per day for moving up to $100,000 per day. Mules would normally operate "under the radar," transferring sums of less than $10,000 from different bank branches (Leyden, John, "Aussie Crooks Recruit Teen Phishing Mules," *The Register*, Jan. 6, 2005, http://www.theregister.co.uk/2005/01/06/phisherman_fagins/).

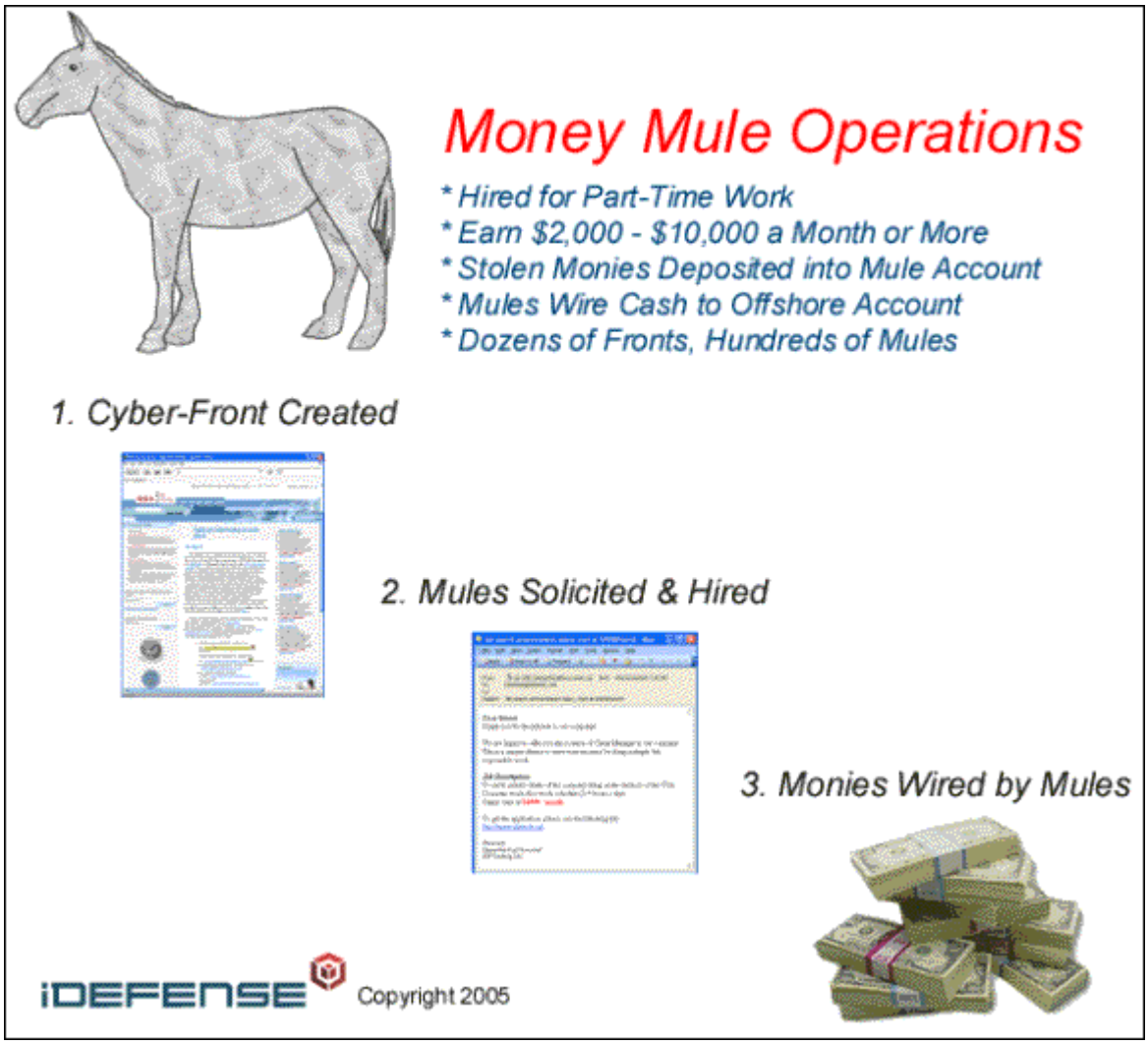
The phishing gang reportedly used fake e-mail alerts to lure victims into visiting a hostile link that installed a keylogging Trojan horse. The gang collected various credentials, banking information and sensitive data required to perform identity theft. Meanwhile, victims were completely unaware of the compromise or the data being collected. The gang emptied bank accounts by moving money into a mule account within the same country as the victim. Mules then made cash withdrawals and performed wire transfers to Russian and other bank accounts.

New South Wales police in Australia reported the arrest of nine members of the gang. A significant number of other arrests were reported as "imminent," indicating that the scope of the operation was quite large. At least one gang ringleader reportedly admitted to charges and was due for sentencing in January 2005. The gang reportedly stole approximately $600,000 in Australian dollars from various bank accounts. However, a police source claimed that the actual losses were more likely in the millions.

3 Cyber Fronts: Where Mule Operations Begin

Once criminals have used phishing attacks, malicious code or other means to steal sensitive data useful for identity theft, they need a way to move the money gained from such identity theft into offshore accounts without being noticed. In the case of the aforementioned Australian operation, the cyber front company was called "World Transfers Inc." During the course of this investigation, affiliated cyber fronts were identified and reviewed in this report. The most significant front in our analysis thus far is called BBA Safe Hosting. The same criminal group appears to be responsible for several cyber fronts, including World Transfers Inc., BBA Safe Hosting, Planett-Design.com, International Trading Company (ITC), P-Pharm.com, Alpenantique.com and others.

Cyber fronts are created to hire mules who often believe they are working for legitimate companies as a manager or shipping agent of sorts. Money is transferred into the mule's account, withdrawn as cash, and then wired to an offshore account. The following image shows how the mule operations typically work:



Graphic Showing Typical Course of Money Mule Operations

3.1 The Case of "World Transfers Inc.:" A Cyber Front for the Russian Mafia or Phishers?

A news report surfaced in April 2005 about Ryan Naumenko, a 22-year-old Australian man who worked as a money mule (\Whinnett, Ellen, "Online Mule Fears Russinan Mafia," April 28, 2005, http://www.heraldsun.news.com.au/common/story_page/0,5478,15110288%255E2862,00.html). After his arrest by Australian authorities, he reportedly feared that his former employers — purportedly the Russian mafia — were out to kill him. Naumenko claimed he thought he was working for a legitimate company, "World Transfers Inc.," as a finance officer, and claimed he did nothing wrong. On the other hand, his claims about the Russian mafia being "out to get him" indicated that he knew what he was doing was wrong but did not feel personally responsible based on how the operation was set up.

Naumenko reportedly laundered about $23,000 for his "employers." He claimed that the scam was active since November 2004 and that his former employers were making close to $1 million each day. Naumenko admitted to using his, his partner's and a friend's account to accept money. He would then go

to the ANZ branch at Narre Warren, withdraw cash and wire it St. Petersburg, Russia, and Latvia. He skimmed several hundred dollars for each transaction completed and claimed that he thought it was a legitimate recruitment and financial operation, that he did not realize the money was stolen by cyber criminals involved in a massive phishing operation.

World Transfers Inc. had a website at one time, but it is now unavailable. New applicants reportedly signed a contract that was e-mailed to them, and the company reportedly required that new hires complete a background check, including tax records. Naumenko claims that there were thousands of employees involved in this operation.

3.2 Job Openings at World Transfers Inc.

Like other cyber fronts, World Transfers Inc. posted various "job openings" online in 2004 and 2005, before part of the crime ring was exposed and arrested in Australia. Example job postings follow:

3.2.1 United Kingdom

Private Financial Receiver
2004-09-10
Payment: 600-900 euros per week
Employer: World Transfers, Inc
Employment term: long term
Position type: part time

World Transfers Inc.
We are quite young company, called World Tranfers Inc. We are increasing our field of work in Western Europe, and particularly in United Kingdom. We are glad to offer you ability of becoming member of our company as PFR - Private Financial Receiver.

You should be older than 18, have bank account in UK, 3-5 hours of free time during the week, and be UK resident.

For that job position we are looking for highly-motivated people. This job isn't very hard, but it requires special attention in every case. It is part time job, and it can become add-on to your main job.

Average salary is 300-500 pounds per week, and it depends on your will of working.

Do not loose your chance to earn good money with our company.

London, United Kingdom
Private Financial Receiver - Simple part time job World Transfers Inc. 08 Sep 2004

Private Financial Receiver - Simple part time job
We are quite young company, called World Tranfers Inc. We are increasing our field of work in Western Europe, and particularly in United Kingdom. We are glad to offer you ability of becoming member of our company as PFR - Private Financial Receiver. You should be older than 18, have ...

Advertiser: *World Transfers Inc.* ***Type: Salary:*** *3000* ***Location:*** *London* ***Date posted:*** *26 Sep 2004 12:05:51*

3.2.2 Germany

> ***Private Financial Receiver***
> *Организация: World Transfers, Inc Оплата: 600-900 euros per week*
> *We are quite young company, called World Tranfers Inc. We are increasing our field of work in Western Europe, and particularly in Germany. We are glad to offer you ability of becoming member of our company as PFR - Private Financial Receiver.*
> *You should be older than 18, have bank account in Germany, 3-5 hours of free time during the week, and be resident of Germany.*
> *For that job position we are looking for highly-motivated people. This job isn't very hard, but it requires special attention in every case. It is part time job, and it can become add-on to your main job.*
>
> *Average salary is 600-900 euros per week, and it depends on your will of working.*
>
> *Do not loose your chance to earn good money with our company.*
> *Thanks you for your attention, if you are interested in our offer please visit our website at http://www.world-transfers.biz . Here you can get more info about our company, our vacancies, and ask us any questions you have.*

Note the various misspellings and grammatical errors in these job announcements. For example, the opening sentence incorrectly says, "We are quite young company," and the company name is misspelled as "Tranfers" rather than "Transfers." In addition, would-be applicants are warned not to "loose your chance to earn good money." Both circumstances point toward a sloppy, non-English-speaking attacker, as is often seen with "419"-type scams and other online content created by criminals.

WHOIS data for the former World Transfers Inc. domain provides several clues as to the operation's scope. Contact information for http://www.world-transfers.biz follows:

Domain Name: WORLD-TRANSFERS.BIZ
Registrant Name: Joseph Miller
Registrant Organization: World Transfers
Registrant Address1: World Trade Center Building,
Registrant Address2: 36th St., Suite 1863
Registrant City: Commercial Area Marbella
Registrant Country: Panama
Registrant Country Code: PA
Registrant Phone Number: +507.2051923
Registrant Email: shipper9999@yahoo.com

Billing Contact Name: Alex Polyakov
Billing Contact Organization: Pilot Holding LLC
Billing Contact Address1: 1105 Terminal way
Billing Contact Address2: Suite #202
Billing Contact City: Reno
Billing Contact State/Province: NV
Billing Contact Postal Code: 89502
Billing Contact Country: United States
Billing Contact Country Code: US

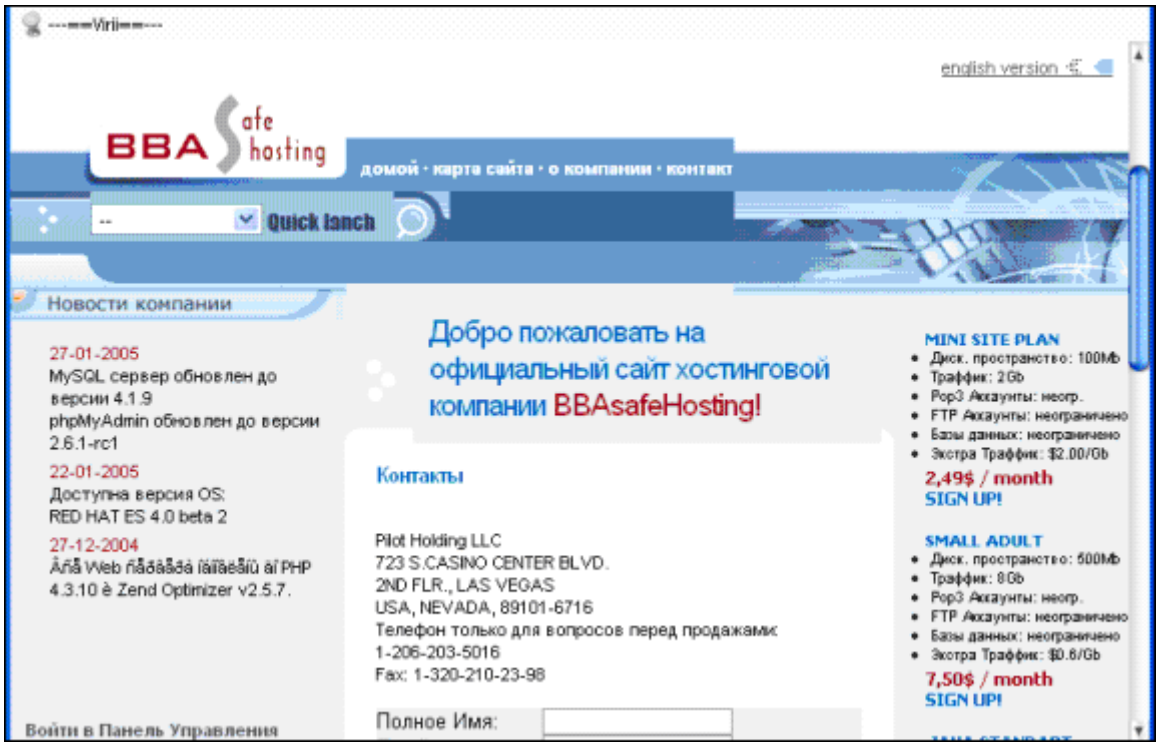
Billing Contact Phone Number: +1.8886164598
Billing Contact Email: sales@bbasafehosting.com
Domain Registration Date: Thu Sep 02 01:59:56 GMT 2004

Of particular interest are the billing contact e-mail and the domain registration date, shown in red above. This reveals that the domain was registered in early September 2004, when the cyber front was likely open for business. The e-mail address led iDefense to another cyber front, BBA Safe Hosting.

3.3 "BBA Safe Hosting"

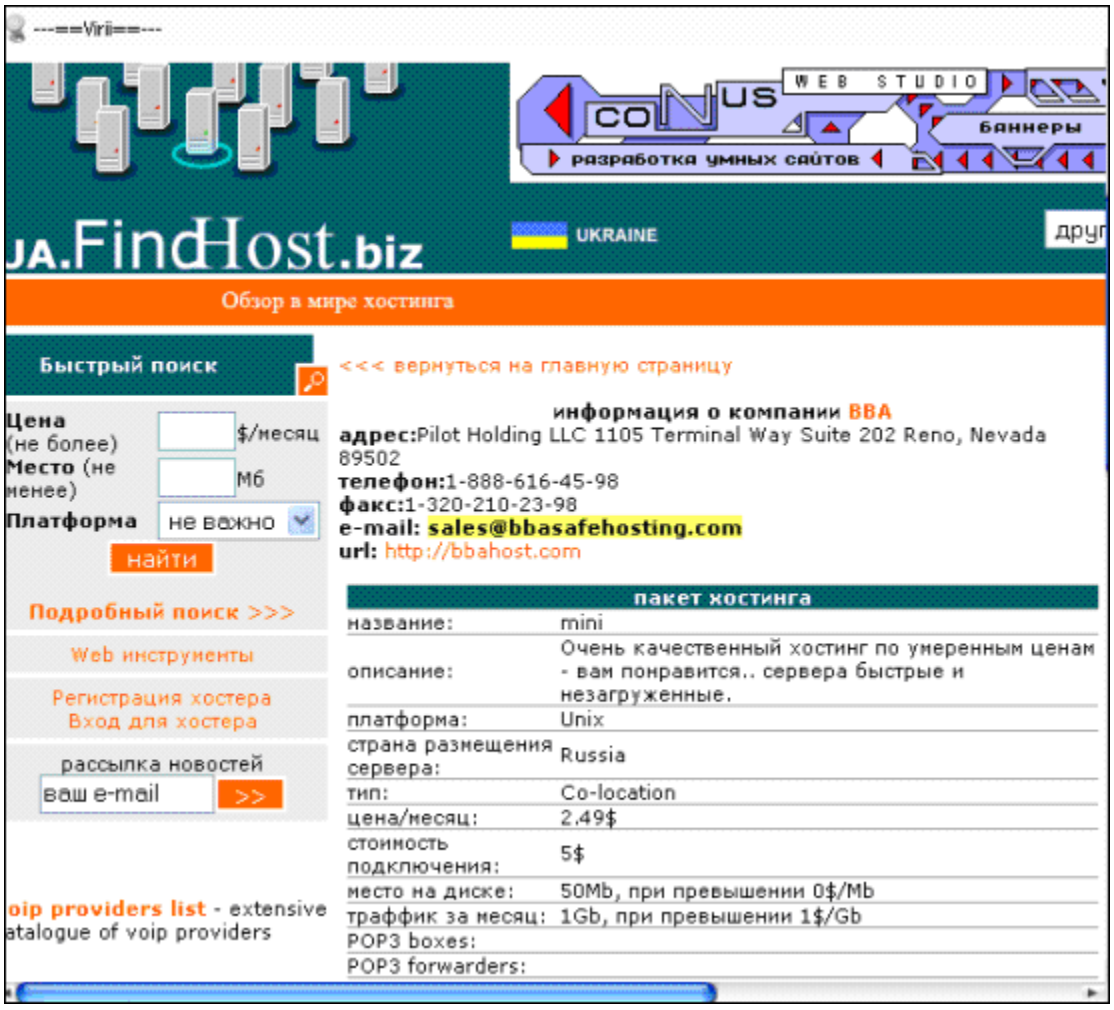
BBA Safe Hosting is a seemingly legitimate hosting organization affiliated with many of the cyber fronts. Queries for the e-mail address of sales@bbasafehosting.com shows all relevant results are directly related to fraud warnings and discussions. As a result, BBA Safe Hosting may also be a front or widely exploited by organized criminals to host cyber fronts.

BBA Safe Hosting had a well-developed, professional-looking website with both English and Russian versions: The cached Russian version of the website (a screenshot of which follows) points to a Las Vegas address:



"BBA Safe Hosting" Russian website showing Las Vegas connection

Another BBA Safe Hosting-related website (a screenshot of which follows) points to a Reno, NV address:



BBA Safe Hosting Website with Reno, Nevada address

WHOIS data for bbasafehosting.com indicates that it was last updated in June 2005, but that the domain was created in January 2003. This indicates that the cyber-front may have been operational for two years or longer. Though WHOIS data states that the country of registration is the Virgin Islands, the web page says that the server is located in Russia.

3.4 International Trading Company (ITC)

Another suspected cyber front, "International Trading Company" (ITC), was also found by looking for additional examples of the sales@bbasafehosting.com e-mail address. An archive of this website was saved by Archive.org before it was shut down Sept. 26, 2004. It is available online at http://web.archive.org/web/20040926021044/ http://www.itradingcompany.com/.

One ITC job posting states:

> *At the end of each month transaction manager's commission comes to 10,7 % of total amount processed. The commission will be sent to the manager's bank account or by money order (if bank account is not available). In case of money order transaction the commission rate comes to 10% of total amount processed.*

Another ITC job posting (shown below) promises a salary of $2,000-3,000 for the first month, followed by a salary of $6,000 a month with bonuses for just 3-4 hours of work a day. If a person works 30 days a month for four hours a day, that works out to $50 an hour:

3.4.1 United States

Work at Home
Financial manager - (US-IL-Chicago)
Min Education: High School
Jobcode: JQ4DB5Y85W61G1Q772
*ITC **(International Trading Company)** is one of the biggest finance companies inEurope.We provide our services for litte over 3 years in different european countries.Now we have opened a new branch of our business in USA.Our company is a door between 2 continents. We help people to make their business succeed, providing our clients with personal agents in countries they need.What you will need to do: Huge part of our clients are traders of different small things (from clothes to car parts). They need to sell things in the USA, but they don't have an opportunity to run their business well with REAL income. You ask why? Because of huge taxes they have to pay. You ask: "But how I can help them? !"You will work like a personal financial manager. In other words you will receive PayPal, money orders/checks and send money to our company's account. What we offer: salary (first month 2000-3000$, then ~6000$/month)+ bonuses If you are ready to spend 3-4 hours a day to receive/manage funds from our clients, please contact our administrator via e-mail **(resume@itcompany.us)**. please, do not call, due to lines are busy. Required Skills: -Legal Age-PC with everyday e-mail access-telephone-verified PayPal with out limits of withdraw-banking account*relocation is not required International Trading Company.*

A college student victimized by the aforementioned scam reveals how the ITC operation worked in the following forum post:

> *Like most college graduates and hard working low income people, part-time jobs are essential to get through the month or week. www.itradingcompany.com(ITC) is a website offering part-time jobs for people as what they call correspondence managers(CM). They claims to be a New York based company originally from London. This company claims to sell goods of all kinds such jewelry, TV's, radio's, furniture, etc.... These jobs are offer at careerbuilder.com and jobcity.com. Once a person is hired he/she is responsible for cashing cashiers/or personal checks and send the money to other ITC representatives. These checks are cashed at check cashiers company's like PAYDAYLOANS, ACED CHECKS CASHED, where you may feel comfortable to do so since they verify that funds are available. ITC rep's are supposed to send items to people who paid for them but they don't. The catch is, all the items are on ebay and people buying these items are not aware they are speaking with an ITC rep. The ITC rep gives the correspondence manager's name and address to the ebay buyer and the CM(correspondence manager) has no idea this is going on. ITC does not send the bought item and they simply ignore emails of the buyer and scam them for they're money. The CM is then contacted by the buyer and is completely unaware that this is going on. When the ITC CM contacts ITC he/she is simply ignored and left to deal with the ebay buyer. If any of the checks cashed by the CM are blocked or bounced after money has been sent, ITC simply ignore the CM(correspondence manager) and makes them take the blame for the money.*
>
> *I have been personally victimized this company as a CM and no one seems to be able to do much about it. if any has any idea on what i should do get in contact with me. Any ebay customer who have been scammed like this please contact me. The FBI will no pay much attention to my case because the dollar amount isn't worth their time. I want to stop these scammers. Their website is*

still up and running and unsuspecting correspondence managers and ebay buyers are being ripped off.

ITC money mules thought they were working for a company that cashed cashier and personal checks, sending funds to other ITC representatives. WHOIS data shows that the domain itradingcompany.com was created in June, 2004, while the domain itcompany.usd was created in October 2004 and registered in Chicago with a registrant e-mail address in Russia: fate13@nm.ru. WHOIS data for a related website, safedns.biz, shows another reference to Pilot Holding LLC (Reno, NV), which continually appears in this particular series of websites and registrations.

It appears the Pilot Holding LLC group, that had addresses listed in Las Vegas and Reno, Nevada, also had an account with the Russian "Passport WebMoney" service, which may have been used to launder monies obtained by the group

3.5 Planett-Design.com

Planett-Design.com is a fraudulent Web design company (now offline) that sought to do illegal funds transfers using mules.

Various victim postings concerning planett-design.com show the same WHOIS contact of sales@bbasafehosting.com, which was covered in last week's report. Selected text from a victim posting follows:

From: <christopheberton11@yahoo.it>
To: <emailaddress>
Sent: Sunday, 19 December, 2004 7:00
Subject: Hello Friends

Hello emailaddress

You can earn from $300 to $2000 per week easily !

You shouldn't invest or purchase anything, it will not cost even $1 for you You should just spend some time, about 1-2 hours per day and even in the first week you will start to receive your earned money.
If you are interested in that, just write us to the following e-mail artur@freelance-biz.info . It is obligatory to indicate in the letter what country are you from and we will send you a detailed description how you can earn those money.

Sincerely yours, Artur Vovan

Your mail is emailaddress
Your fax

A reply from "Artur Vovan" said the following:

Hello firstname,

Sunday, December 19, 2004, 12:24:05 AM, you wrote:

XY> please send me more information.
XY> I live in country.
Thank you for the interest to our proposal.

Our company www.planett-design.com produces different programs, web sites and scripts for the Internet and a lot of other things. We constantly seek more convenient kinds of payment for our clients. A lot of our clients want to pay for the services through payment system www.paypal.com, it is the best and the easiest way for the clients to pay for our services, but unfortunately www.paypal.com company refuses to work with the eastern Europe countries and we seek a representative in one of the countries with which paypal works.
We will offer you 20% from the money turnover on your paypal account, in average the turnover totals about $1500-4000 per week and you can easily earn $300-800 per week. Our company develops very fast and money turnover will constantly raise.
If you are interested we are waiting for your reply and we'll send you more detailed description how all of it will be working.

In the future please use the following e-mail artur@planett-design.com for correspondence.

Best regards, Artur Vovan, artur@planett-design.com

Source: http://www.joewein.de/sw/fraud-planett-design-com.htm

WHOIS information for Planett-Design.com shows Artur Vovan as the official registrant and the location as 6 Okipna Street, Kiev, Ukraine. Vovan also has an alleged German e-mail address of "Vovan, Artur kunihikosim@yahoo.de."

The technical contact information for Planett-Design.com is the same Reno, Nevada contact and address information as that of World-Transfers.biz.

Technical Contact:
Polyakov, Alex sales@bbasafehosting.com
1105 Terminal way
Suite #202
Reno, NV 89502
US
+1.8886164598 Fax: +1.3202102398

Record last updated on 17-Dec-2004.
Record created on 17-Dec-2004.

A cached copy of the Planett-Design.com webpage follows:

Cached version of Planett-Design.com website

Contact information follows:

Contact: support@planett-design.com
artur@planett-design.com
Phone: +38 (044) 239-2490
Address: 04070 Kyiv, Ukraine, Voloska, 20, Suite 76

Interestingly enough, the phone number listed, **+38 (044) 239-2490**, is the same as the fax number for another organization in Kiev, the "Economics Education and Research Consortium" (EERC).

> Economics Education and Research Consortium (EERC)
> vul. Voloska, 10, room 406
> 04070 Kyiv Ukraine
> Tel: 380-44- 239-2494
> **Fax: 380-44-239-2490**
>
> e-mail: eerc@eerc.kiev.ua
> www.eerc.kiev.ua

The EERC is listed as a Higher Education Support Program of the Open Society Institute, which is located in New York. The Open Society Institute says on its website that it is part of the Soros Foundations Network.

Either the EERC has inherited the same phone number that once belonged to Planett-Design.com, or the latter's registration was totally fraudulent. A program in economics education and research was actually involved in the Planett-Design criminal enterprise. It is unknown whether there is any association at all between these entities or whether this is simply a case of a phone number being reassigned.

3.6 ChildrenHelpFoundation.com

ChildrenHelpFoundation.com scam, June 15, 2005 screen shot

iDefense recently obtained an e-mail solicitation from a group calling itself the "ChildrenHelpFoundation.com," billed as a so-called "Internacional [sic] Charitable Fund." The group says that its mailing addresses are in Moscow, Russia and Riga, Latvia. The group is clearly a cyber front playing on people's sympathy for less-fortunate children.

In a section titled "Charitable Programs," the scam artists' English grammar is so terrible that it appears they simply may have cut and pasted a machine translation onto the website:

> *CHARITABLE PROGRAMS*
> *The "Education XXI - Century" Program*
> *The purpose of the program is assistance to growing up generation in education, science, culture, to form aspiration to receive higher or special secondary education and occupation required by modern conditions.*
>
> *The tasks of the program are - Help the Children Foundation renders the social and financial aid to enter institutions and colleges to companies and individuals by concluding contract with them the about rendering of the social and financial aid. This project gives an opportunity to all age children categories studying in various type of schools from the 1-st to the 10-th forms to enter institutions and colleges on a commercial basis after graduating from school at the minimal family expenses.*
>
> *The **basic financial** idea of the project consists that with certain age of the child the relatives determine the sum planned on payment for studying of the child in institution or college. Tariff rates are different in view of age of the child, the earlier payments are carried out, the sum is less. Ten tariff plans differ on size of a total sum of payment: from 30 up to 150 thousand roubles. In the period of payments recieving, and also in process of their accumulation the received money begins to produce a profit as interests. When the sum deposited to the Fund s account no any independent financial operations with accumulation made by the Fund. The accounts are opened in Sberbank of Russian Federation. All the charges of interests are made by bank.*
>
> *At entering institution, according to made contract, student receives the sum of the stipulated social aid with the additional interests charged by Fund for several years (a minimum one Year).*
>
> *Besides, the grants will be paid to the talented students extremely from own Fund's means.*
>
> *All risks for safety of financial assets of Help the Children Foundation are incurred by the well-known insurance companies*

The domain for ChildrenHelpFoundation.com, notably, is registered in Panama:

Domain name: CHILDRENHELPFOUNDATION.COM

Administrative Contact:
Inc, Panama, PanaHOST info@bulok.net
6 , Grouce st.
Zigna, 3471
PA
+507.349471631 Fax: +507.349471631

The domain was created March 31, 2005. The group says that it was established in 1999 and registered as a charity in July 2003. Besides offices in Riga and Moscow, the group says it has also opened two branches in the Republic of Tatarstan.

The June 2005 e-mail solicitation for money mules for ChildrenHelpFoundation.com appears as follows:

> ***International Help the Children Foundation (Latvia)*** *is looking for a proactive and responsible person to fill in the part time Collections Manager. Your essential responsibilities will be to manage the receipt of payments from our US and Canadian benefactors into your bank account and further transfer the monies to our accounts under the supervision of our Collections Executive. This position requires some aptitude with numbers and a great degree of financial discipline. You should also be a good communicator, since most of the business communications is done over phone/fax/email.*
> *Help the Children Foundation was established in 1999 to support and realize programs and actions directed on strengthening of prestige and a role of family in society and state; render financial, technical and humanitarian aid within the framework of own and international charitable programs. At the moment, we are initiating a joint Latvian - USA program to provide financial help to gifted kids from incomplete families.*
> *Since we do not have a full time US representative yet, we are looking for proactive individuals to act as our collections managers in the Americas. This position is commission based, and would require no more than 2-5 hours per week to fulfill your duties. You will be receiving a 5% commission for each benefactor transfer that you forward to us. In example, if $5000 is credited to your account, you will earn a commission of $250.*
> *If you feel that you fit for this position and would like to contribute to the better image of the United States abroad, as well as to better the life of the deprived children, please email us at ICanHelp@childrenhelpfoundation.com with your contact details and a few words about yourself.*

4 Laundering Stolen Money

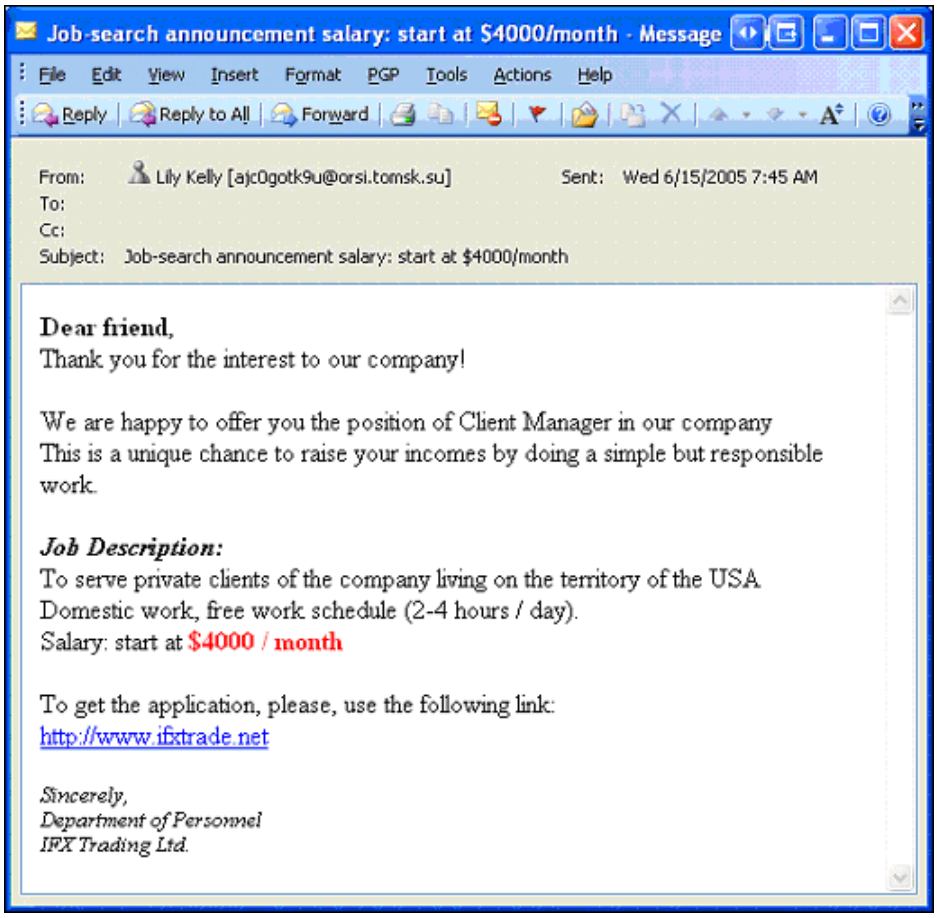
Accompanying the rapid increase in identity theft crimes is the appearance of numerous criminal cyber fronts used to launder stolen money. This section discusses another recent suspected money mules operation and shows some of the methods involved.

4.1 IFX Training Ltd.

One example of money laundering operation is IFX Training Ltd., which purports to be a work-from-home operation but uses a variety of illegal methods to launder money made maliciously.

4.1.1 The IFX Job Search E-Mail

In the IFX job search operation, criminals solicit money mules via job announcement e-mails such as the following. In June 2005, iDefense obtained a suspicious e-mail from IFX Trading Ltd. The message was immediately considered suspicious because it offered a "simple" job with a "free" (presumably flexible) work schedule paying $4,000 a month; a common promise in money mule job offers.



IFX Trading Ltd. Purported Job Announcement, June 15, 2005 (iDefense Intelligence Operations)

An inspection of the message's MIME header shows that the e-mail was actually received from YahooBB219042058037.bbtec.net (YahooBB219042058037.bbtec.net [219.42.58.37]) with a return path of ajc0gotk9u@orsi.tomsk.su.

Normally, a company would have its own e-mail server or something more secure than a Yahoo! account that is used for business communications. Additionally, the orsi.tomsk.su domain associated with the return path is invalid. Nevertheless, the tomsk.su portion of the e-mail indicates a possible Russian connection to this operation (Tomsk is a city in Russia, while the .SU top-level country domain, though nearly obsolete, is still retained by some users). Even at this early stage in the assessment, it already appears that "IFX Trading Ltd." is a cyber front operation promoting the use of money mules.

Cached copies of similar e-mails from the company have been posted to various newsgroups and e-mail addresses, including:

http://66.102.7.104/search?q=cache:tN13ParvZDgJ:www.mail-archive.com/bug-httptunnel%40gnu.org/msg00070.html+%22IFXTRADE.NET%22&hl=en

http://66.102.7.104/search?q=cache:qg7U9VgXhsoJ:lists.gnu.org/archive/html/bug-gplusplus/2005-06/msg00090.html+%22IFXTRADE.NET%22&hl=en

4.1.2 The IFX Trading Ltd. Website Domain

WHOIS data reveals that this address is associated with a London domain belonging to IFX Trading Ltd. (ifxtrade.net). However, as seen with other cyber fronts, this information could easily be a faked or hijacked name and address.

> **Domain name**: IFXTRADE.NET
> 4 Coleman Street
> London, 5JJ EC2R
> GB
>
> **Administrative Contact**:
> Nelson, John ifxtrade@supportwest.com
> 4 Coleman Street
> London, 5JJ EC2R
> GB
> +44.2738224515
>
> **Technical Contact**:
> Nelson, John ifxtrade@supportwest.com
> 4 Coleman Street
> London, 5JJ EC2R
> GB
> +44.2738224515
>
> Record last updated on 10-Jun-2005.
> Record expires on 24-Dec-2005.
> Record created on 24-Dec-2004.
>
> **Domain servers in listed order**:
> NS1.TEENSJCASH.COM 219.234.219.61
> NS2.TEENSJCASH.COM 219.234.219.61

Notably, the this domain was last updated on June 10, 2005, just five days before the job announcement e-mail was received. Former cyber front case studies have shown that e-mail is often received within days of a change to a cyber front website or registration.

The phone number associated with the WHOIS record for IFXTrade.net is no longer valid. The Administrative/Technical contact e-mail address, ifxtrade@supportwest.com, does not work either. Thus, it appears that, as expected, this information is probably forged or hijacked.

The two domain servers (teensjcash.com) are unrelated to the primary domain of ifxtrade.net, which is also suspicious. Registrant data for that domain, which has no website at the time of this writing, is for a registrant located in St. Joseph, Alaska. WHOIS information for Teensjcash.com shows that the domain's record was created on Feb. 24, 2005 and last updated on March 9, 2005.

4.1.3 Scam Alerts for IFXTRADE.NET and Similarity to Phishing

As it turns out, online scam alerts concerning IFX Trading Ltd. are already emerging. Two such postings can be found at http://ideceive.blogspot .com/2005/06/job-scam-ifxtradenet.html and http://www.dynamoo.com/diary/ transfergate-com-scam.htm.

The blogspot.com posting claims that the IFXTRADE.NET website is a "rip-off" of the ifxonline.net website. This, too, is a common practice; often, cyber front operations steal or otherwise abuse another company's name or identity. This is not unlike a phishing scam, where a website may be downloaded, modified and hosted on a hostile server for illicit gain. In this case, the potential victim received an e-mail on June 15, the same date as our sample, just days after the website was updated.

The second posting, on dynamoo.com, is about a company called "TransferGate Group." The author claims that this company is fraudulent, and the lengthy job description distributed by the company has all the earmarks of a money mule operation. As expected, the website (TRANSFERGATE.COM) does not work, and the contact information appears bogus, excluding the original temporary e-mail address used for spamming and soliciting potential money mules. The IFXTRADE.NET domain is listed by the dynamoo.com poster as one of several websites that are "clearly typosquatting or spam-related." The original Transfergate Group domain was reportedly hosted on a server in China at 211.158.6.105. The other websites, including IFXTRADE.NET, are implicated in this posting as possibly related to fraud operations:

- www.1cartoncigarettes.com
- www.Allmysuccess.com
- www.Allukrcharity.com
- www.Annytime.biz
- www.Antiquitaeten-gotthelf.com
- www.Cliport.com
- www.Emailpromo.us
- www.Goodz.biz
- www.Goodz.info
- www.Heathertips.com
- www.Ifxtrade.net
- www.Ivoryvaughan.com
- www.Lannygordon.com
- www.Mysavingtips.com
- www.Prioritet-2005.biz
- www.S-way.biz
- www.S-way.info
- www.Safepayment.biz
- www.Silverise.biz
- www.Broadcastemail.us
- www.Au-uk-usa.com
- www.A-i-k.com
- www.Tgbabez.com

4.1.4 Spyware Installations

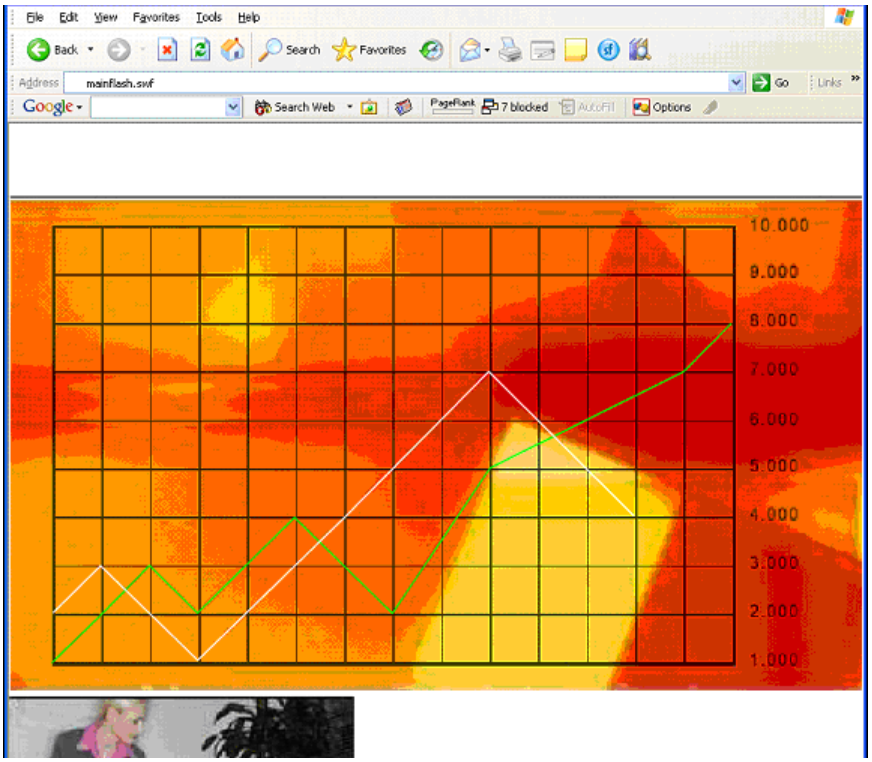
The author of the dynamoo.com post claims that spyware may be installed on computers using vulnerable versions of Internet Explorer to browse TRANSFERGATE.COM. If a user attempted to visit TRANSFERGATE.COM with an alternative browser, the user was reportedly prompted to visit the website with Microsoft Corp.'s Internet Explorer 5.0 or later. The author believes the website contains spyware and keyloggers designed to steal financial information from victimized computers. This claim cannot be validated, however, since TRANSFERGATE.COM is no longer available at the time of this writing.

TRANSFERGATE.NET is also registered, but does not resolve at the time of this writing. It is likely that this website is also related to the suspected fraud operations aforementioned. Both the .com and .net domains for TRANSFERGATE are registered to a person in France with a technical contact in Texas, both pieces of information appear to be fraudulent.

4.1.5 Digging Deeper into IFXTRADE.NET

At first, it appears that the ifxtrade.net domain is inaccessible. However, various files can be leached from the website, including a logo, graphical menu of options for prospective money mules and a Shockwave introduction to the website.

IFX Menu Options



IFX Shockwave Introduction

Text found on the old website is shown here:

> *"IFX offers a professional and competitive Foreign Exchange service. Clients can place their trades with us 24-hours a day by telephone. Our dedicated 24-hour Foreign Exchange Desk was created to serve the requirements of corporate and individual customers.*
> *Our Fx department provides a professional and competitive service tailored to the needs of smaller and larger investors. IFX also welcomes Introducing Brokers from all over the world. Meet our friendly and practical trading department today."*

An image on the website also points to Forex Trading in an apparent attempt to add a measure of legitimacy to the IFX website.

5 Conclusion

This paper is an attempt to describe some of the business operations utilized by cyber-criminals operating around the world. iDefense believes that an important aspect of fighting online fraud is understanding the means, motivations and capabilities of these groups. Following the money, in this case the Money Mules, is the key.

This "ChildrenHelpFoundation.com" operation is just one more example of the depravity of the scam artists behind many money mule operations. If they are not able to recruit money mules through greed or ignorance, they will play on the sympathies of would-be recruits. The scam also provides a ready-made justification for money mules if and when they are caught – that they were supposedly "helping" needy children with these money transfers.

IFX is clearly a cyber front showing all the tell-tale signs of fraudulent operations, using money mules as a key aspect of the group's criminal methods. The IFX example is merely one of many that could be cited. The best advice to consumers for avoiding such scams is to be vigilant and to follow their instincts when a solicitation appears to be too good to be true. A simple investigation can often reveal whether a group is likely part of a cyber front that supports criminal activity.