Worldwide “Money Mule” Operations: The Cyber Dimension

Jim Melnick and Ramses Martinez

Directors, Threat Intelligence and Malcode Operations Teams

iDefense, a VeriSign Company

Where it all comes together.

Agenda

- iDefense Overview
- Goal of Presentation and Definition
- Recruitment, Spotting “Money Mule” Operations, How Do They Work?
- Sample “Money Mule” Ads
- The “Panama Connection”
- A “Money Mule” Charity Scam
- Conclusions
- Q&A

About iDefense: Overview

- iDefense, a VeriSign Company, is a leader in cyber threat intelligence.
- Industry-Leading Service Offerings
  - Intelligence is all that iDefense does
- Marquee Customer and Partner Base
  - Government, financial services, retail, telecom and others
- Experienced Intelligence Teams
  - iDefense Labs
  - Vulnerability Aggregation Team (VAT)
  - Malicious Code Team (Malcode)
  - Threat Intelligence Team
  - Rapid Response Team
- In business since 1998, iDefense became a VeriSign Company in July 2005

iDefense Intelligence Services

Daily / Hourly Research Deliverables

+ Comprehensive Vulnerability Feed
  - Most comprehensive, timely, technical feed in the industry
+ iDefense Exclusive Vulnerabilities
  - More than 250 contributors around the globe
  - Released to vendor and iDefense customers only
  - More than 180 iDefense Exclusive vulnerabilities in 2005
+ Malicious Code Research and Reporting

iDefense Intelligence Services

Weekly / Semi-Monthly Research deliverables

+ Weekly Threat Report
  - Weekly compilation of worldwide threats
  - Critical Infrastructure, State of the Hack, Cyber Crime, Terrorism and Homeland Security, Global Threat
+ Bi-Weekly Malicious Code Review
  - Summary of previous two weeks malcode activity
  - In-depth analysis of specific malcode from the Malcode Lab
+ iDefense Topical Research Papers
  - Examples
    - Security of Enterprise Web-Based E-Mail Interfaces
    - Security Comparisons: Internet Explorer vs. Firefox
    - Phishing and Pharming: A Comparison
    - Mitigating the Threat from Keyloggers
+ Focused Threat Intelligence Reporting
  - Topics specific to individual customers

Goal of This Presentation:

- This presentation and the follow-on paper explore the cyber aspect of worldwide “money mule operations” and their attendant methodologies.
- The goal is to better understand these techniques in order to assist in spotting potential criminal activities and to help mitigate against them.

Definition: “Money Mules”

- 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
  - Cyber “money mules” are a very important aspect of international carding operations and other types of online fraud. Recruited primarily (but by no means solely) in the US, 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.
  - They may or may not know that they are supporting illegal operations.

“Money Mules”: How are they recruited?

- Fraudsters often hire money mules through seemingly legitimate businesses (often spamming advertisements for positions via e-mail) and through career websites. They sometimes even masquerade as online charities!

  Titles vary widely, but many have names or descriptions such as:

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

Potential fraud operation involving “money mules”

- How to spot them?
  - Often there are grammatical errors in the advertisements or e-mails
  - WHOIS registration of the company/organization involved in the fraud operation often is very recent
  - Web queries performed on the company name or contact information for the company reveals multiple posts claiming fraud from a former employee of the company.
  - Explicit request for banking account details so that they can move money into a personal banking account for business operations.

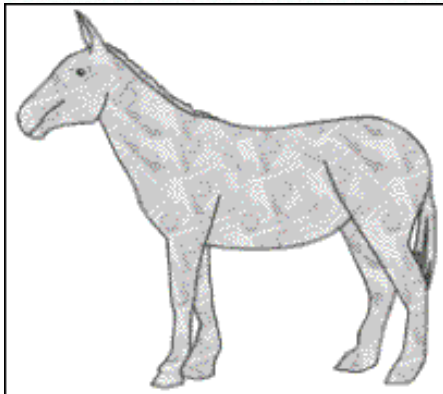
- *NOTE: While neither of these conditions standing alone is conclusive evidence of a “money mule” operation, they may be indicators of one*

How do cyber frauds involving “money mules” work?

+ Often, these are the missing link in international carding [i.e., stolen credit card] operations. Cyber criminals hack or otherwise obtain stolen credit cards; they then need to obtain stolen goods or cash from those accounts but cannot do it directly without triggering standard anti-fraud mechanisms or algorithms

  - *“Money 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.*

How the process works…..



Money Mule Operations

* Hired for Part-Time Work
* Earn $2,000 - $10,000 a Month or More
* Stolen Monies Deposited into Mule Account
* Mules Wire Cash to Offshore Account
* Dozens of Fronts, Hundreds of Mules

1. Cyber-Front Created

2. Mules Solicited & Hired

3. Monies Wired by Mules

iDEFENSE Copyright 2005

Sample “ad” for a “money mule” position:

Private Financial Receiver (Targeted at the UK)

+ *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* (sic) *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.*

Sample “ad” for a “money mule” position:

Private Financial Receiver (Targeted at GERMANY)

+ *Private Financial Receiver*

+ *Организация: World Transfers, Inc* *(NOTE: Russian words)*

+ *Оплата: 600-900 euros per week*

+ *We are quite young company, called World Tranfers Inc.* (sic) *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.

WHOIS registration data points to Panama:

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**

Many such entities seem to have a “Panama connection”:

Registrant City: Commercial Area Marbella

+ Registrant Country: Panama

+ Registrant Country Code: PA

Example of a charity scam using the same “money mule-type” concept:

ChildrenHelpFoundation.com scam, June 15, 2005 screen shot

Connection to Moscow (RUSSIA) and Riga (LATVIA)

+

Recent Example of Suspected Money Mule Ops

Note: trimmed to show important details only:

+ Subject: Fwd: Re: Time saving job with worthly (sic) income.
+ We would like to kindly ask you to send us your bank account information accordingly. All the payments will be transferred to your bank account, therefore please advise us on the following:
+ Now you should research for the closest WesternUnion and MoneyGram locations.
+ 1) send us your bank account information
+ 2) send us the signed contract
+ 4) send us your time schedule
+ 5) find the closest WesternUnion and MoneyGram agencies
+ 6) turn on your cell phone and wait for us to contact you

Conclusions

- *Individual "money mule" operations are usually relatively short-lived, but cyber criminals often just move on to a new location or launch new recruitment efforts when they are discovered*
- *They continue to form a vital part of international criminal carding operations*
  - *Victims include groups of former money mules who did not know what their efforts were actually supporting*
- *Connections often go back to the Former Soviet Union (FSU) and Panamanian registration connections (including Nevada)*
- *The problem will continue until cyber criminals find more expedient methods to transfer stolen funds*
  - *The use of "money mules" is inherently not the most efficient means of cyber crime; thus, these types of operations will probably eventually be superseded by more efficient mechanisms*

Q/A

Jim Melnick and Ramses Martinez

Directors, iDefense and Malcode Operations Teams

iDefense, a VeriSign Company

Where it all comes together.