Australian Government
Australian Institute of Criminology

AUSTRALIAN HIGH TECH CRIME CENTRE

no. 16 ▪ 2007 HIGH TECH CRIME BRIEF

Money mules

The use of people to transfer drugs and/or money, a long standing practice of the criminal fraternity, is being replicated in the high tech crime environment. 'Money mules' (people unrelated to the criminal activity that creates the illicit funds) transfer relatively small amounts of money lodged in their bank accounts to criminals overseas. Money mules are a consequence of the need for criminals to transfer, and disguise the origins of, illicit proceeds of crime.

The recruitment of money mules

Money mules seem to be recruited largely from the US, UK and Australia and transfer illegal funds to criminals located, primarily, in the former Soviet Union (iDefense 2006). The basic process of muling is relatively simple:

- job advertisement offers work as 'financial agent' or similar
- job seeker signs up and opens, or allows access to, domestic bank account
- fraudsters transfer money from scam victims to job seeker's account
- job seeker transfers money to fraudster overseas
- job seeker receives 'commission'
- job seeker is open to prosecution by domestic authorities for money laundering.

Mules are recruited primarily through the use of cyber fronts (fictitious online companies which appear legitimate) or spam advertisements (offering bogus employment opportunities via email). Titles for muling positions vary but have included 'Private Financial Receiver', 'Money Transfer Agent', 'Shipping Manager' and 'Sales Representative' (iDefense 2006). Emails containing such advertisements are similar to phishing scams in that they aim to facilitate control over a bank account (Beardsley 2005). Unlike phishing scams, where the aim is to ensure that the account holder is unaware that their account has been compromised, the aim of muling is to obtain the full consent and cooperation of the account holder.

In September 2005, Clearswift noted that 'work-at-home scams' had accounted for 0.5 percent of spam emails and in October 2005 that had risen to 1.2 percent (Leyden 2005). In 2004, MessageLabs (2004) reported that more than 20,000 copies of a scam phishing mule email were sent purportedly from ICG Commerce (a legitimate company whose name was being used to add credibility to the scam). Further credibility was provided by the fact that a formal application process (including interviews) had to be undertaken, and by a statement provided on the website linked to the email which stipulated that '…we are NOT going to ask you [to] do ANY initial investments or send ANY kind of initial payments'.

In Western Australia, the Department of Consumer and Employment Protection's 'WAScamNet' database recorded 1,709 employment and money mule email offers reported by consumers in October 2006 alone. This was 59 percent of all scam emails reported. This category now represents the largest category of scam emails reported to the Department each month.

Reshipping

Reshipping (or postal forwarding) is a well-used variation of muling in which the mule receives packages at home (containing goods obtained illegally by criminals) and then reships them in exchange for a fixed fee per package.

Arrangements are made so that the mule receives payment directly into their bank account. The mule may then also be used for transferring money to and from that account. Reshipping exploits:

- the ease with which online payments can be made and also the popularity and profitability of online marketplaces
- the natural reticence shown by merchants to ship expensive goods overseas
- the belief that once an online transaction is approved, shipments made to domestic addresses are not subject to any real scrutiny, especially during periods of expected high traffic like Christmas
- the limited oversight of parcels being shipped overseas by domestic citizens.

Project no. 0074a

ISSN 1832-3413

The Australian High Tech Crime Centre funded this research.

CONTACT
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601

T: 02 6260 9200
F: 02 6260 9201
www.aic.gov.au

Reshipping recruiters tend to use well-crafted company websites. A typical reshipping ring in Russia is purported to consist of six operatives in their 20s and 30s, and there are estimated to be 50–100 rings based in Moscow alone, each receiving about $20,000 worth of stolen goods a month (Acohido & Swartz 2005a).

In 2004, it was estimated that reshipping groups had set up approximately 44,000 post office boxes and residential addresses in the USA as package handling points (Acohido & Swartz 2005b). Internet job hosting sites such as Monster.com and CareerBuilder.com claim that they deploy teams to screen advertisements. Reshippers are adept at skirting that rudimentary screening process, however, by changing their names and websites every few months. Indeed, very sophisticated posting patterns have been discerned in particular towns or regions, including the strategic testing of new company names for vulnerability to discovery by website hosts (Dixon 2004).

Prevention

Money muling via online job sites and/or spam email is a key example of a movement from syntactic (targeting the computer) to semantic (targeting the computer user) attacks. Krenn, of the US Postal Service, has noted that muling 'is driven by desperate people looking for jobs…Most of them don't ask questions' (Acohido & Swartz 2005b). In essence, money muling is an advanced form of fraudulent work-at-home schemes. The danger of money muling lies in the fact that, unlike those other schemes, the participants actually receive a form of payment and are liable to prosecution for money laundering activities.

Potential signs of the existence of money muling operations include:

- being informed by the company that payments can only be made by direct deposit, and being asked to provide personal bank account details
- being contacted by a business organisation with a yahoo or hotmail return email address rather than its own and/or its ISP's mail server
- grammatical and other errors: early phishing scams were replete with such errors but have improved dramatically, and it seems likely that money muling scams will follow suit
- checking the hiring company's WHOIS data for warning indicators such as a mismatch between the country of origin code for the email address and the country of residence, particularly when the email address country of origin is a known destination for muled funds. The WHOIS data for the website kflogistics.biz (used in muling scams), for example, lists the registrant as Michael Birman who has a New York mailing address and telephone number. However, the last two letters of Birman's listed email address, tyler052@yandex.ru, indicate a Russian base.

A number of financial institutions globally have imposed a one day delay to payments made by and to their customers in order to detect transfers made by mules through their bank accounts before the scam can be completed.

Examples of money mules

In January 2005, 61 people were arrested in Australia for allegedly wiring money to Russia and other undisclosed locations and collecting a commission based on the amount of money laundered. Mules reportedly earned $200 – $500 per day for moving up to $100,000 per day (AllBusiness 2006).

In November 2005, three people in the UK involved in a phishing operation against eBay customers were arrested during Operation Apple. Thirteen bank accounts were utilised to hide and launder the proceeds. Victims of the eBay operation made transfers to the criminals' money mules who handled multiple transfers ranging from £1,500 to £15,000 (Out-Law 2005).

In February 2006, Russian thieves stole more than €1m from personal bank accounts in France. The thieves then transferred the victims' funds to the accounts of money mules who allowed the money to transit through their accounts (Willsher 2006).

In September 2006, the Spanish National Police detained 23 people in relation to the theft of €2m from online banks and online shops. The funds were siphoned off into intermediary accounts in Spain and then transferred to Russia and the Ukraine via 19 money mules (Kornakov 2006).

FURTHER READING

All URLs were correct at March 2007

Acohido B & Swartz J 2005a. An inside look at a Nigerian reshipping ring. *USA today* 7 November

Acohido B & Swartz J 2005b. Cybercrooks lure citizens into international crime. *USA today* 11 July

AllBusiness 2006. *Money mules: an investigative view*. http://www.allbusiness.com/professional-scientific/management-consulting-services/890852-1.html

Beardsley T 2005. *Phishing detection and prevention*. http://www.planb-security.net/wp/503167-001_PhishingDetectionandPrevention.pdf

Dixon P 2004. *A year in the life of an online job scam*. http://www.worldprivacyforum.org/jobscamreportpt1.html

iDefense 2006. *Money mules: sophisticated global cyber criminal operations*. Sterling VA: iDefense Labs

Kornakov K 2006. Cyberfraudsters detained in Spain. *VirusList.com* 18 September. http://www.viruslist.com/en/news?id=198811138

Leyden J 2005. Email 'get rich quick' scams double in October. *The register* 10 November. http://www.theregister.co.uk/2005/11/10/email_scams_diversify/

MessageLabs 2004. *Job seekers beware: phishing recruiting mules for money laundering*. 23 November. http://www.nl.messagelabs.com/news/pressreleases/detail/default.asp?contentItemId=1237&region

Out-Law 2005. *Follow the evidence*. Winter no. 13: 7–9

Willsher K 2006. Sleeper bugs used to steal 1m in France. *Guardian* 7 February. http://www.guardian.co.uk/print/0,,5393279-110633,00.html