WORLD-CHECK™
REDUCING RISK THROUGH INTELLIGENCE

JANUARY 2010

Expert Talk

Emerging Trends: Money Mules

by BC Tan, Head of Organised Crime Research, World-Check

Understand who you are really doing business with.
www.world-check.com/experttalk

Cybercrime is a particularly fast growing and evolving criminal trade that is unfortunately inadequately understood. In the recent years, there has been a clear proliferation in both the quantity and complexity of cybercrime - rapidly evolving into far more complex and coordinated syndicates; which has enabled a shift away from simply targeting vulnerable consumers to focusing on financial institutions. In a 2008 report, McAfee states that data theft and breaches from cybercrime may have cost businesses as much as $1 trillion globally in lost intellectual property and expenditures for repairing the damage. However the reputational damage from the publicity of cyber attacks could prove far more costly from undermined trust and brand value tirelessly accumulated.

A particularly worrying typology that has emerged in the recent years is the advanced utilisation of money mules in cybercrime operations. While Russian and other Eastern European organised crime groups have been known to use money mules in their cross border movement of illicit finances, cybercrime groups have become far more innovative and successful in the use of money mules for not only laundering criminal proceeds but perpetrating the cybercrime as well.

Money Mules

There have been several cases of money mules utilised by organised crime groups in the laundering of criminal proceeds. In Asia Pacific, there were two major cases in 2005 that caught the attention of the media. In April 2005, a 22 year old Australian Ryan Naumenko was arrested by Australian authorities for alleged involvement in the money laundering operations linked to Russian organised crime. In this case, Naumenko was recruited via online advertising under the false impression of legitimate employment as a finance officer with World Transfers Inc., that turned out to be a fictitious front company operated by a Russian organised crime group. Similarly in 2005, a 41 year old Singaporean Rahmad Ibrahim was found by authorities in Singapore to be laundering criminal proceeds for an Eastern European crime syndicate. Like Naumenko, Rahmad was recruited online and was led to believe that he was legitimately employed by the Financial Investment Advisory Services (FIAS), which in reality operated through a "spoof" website and was not affiliated with the genuine Financial Investment Advisory Services; an organisation associated with the World Bank Group. In 2009 alone, 12 individuals that operated as money mules have been convicted in Singapore.

Recruitment

Money mules are often unwitting members of the criminal conspiracy. The primary method of money mule recruitment is via the internet – often through internet job advertisements for private financial receivers, money transfer agents, shipping managers, financial managers, sales representatives, and secondary highly paid jobs. Money mules operating in money transfer roles are usually paid 3 - 5% fees. However in most cases, money mules will continue to believe their legitimate employment up to the completion of the parent criminal organisation's needs where their "employers" will then completely withdraw the finances from the mule accounts (at times including

the fee paid out) or in worst case scenarios; their arrest by the authorities. In some cases, where the money mule recognises their part in the greater criminal operations; the organised crime group will often coerce them into continued cooperation.

The primary method of money mule recruitment is via the internet

Operation Phish Phry

Today, virtually all known cybercrime groups have been found to operate with the use of money mules. For example, the illusive Russian Business Network (RBN) syndicate where a single division has been estimated to make in excess of $150 million annually, and has been the target of numerous investigations in recent years, has been found to operate extensively with internet recruited money mules.

In October 2009, the Federal Bureau of Investigation in partnership with the Egyptian authorities managed to successfully disrupt a sophisticated cybercrime group – 'Operation Phish Phry' indicted nearly 100 people that included the 80 individuals detained. This particular cybercrime group successful targeted two US based financial institutions and managed to defraud in excess of $1.5 million.

A particular interesting aspect uncovered through the disruption of this cybercrime group is the complexity of the organisational structure and the extensive role of money mules. For instance, there was a clear division of responsibilities within the group such as "recruiters", "drops", "money distributors" and "hackers". This cybercrime group led by three main leaders; Kenneth Joseph Lucas, Nichole Michelle Merzi and Jonathan Preston Clark engaged 18 "recruiters" that sourced at least 36 money mules that acted as "drops" and "money distributors". Essentially the role of the "drops" was to open bank accounts in targeted banks and to accept money transfers from compromised bank accounts; the "drops" would then transfer the stolen funds to "money distributors" they would then distribute the illicit proceeds to other conspirators in the crime group. This complex structure that depended on highly expendable money mules proved far more difficult to uncover and took authorities more than two years to disrupt.

Conclusion

This increasingly popular method poses a significant threat to financial institutions. Taking into consideration that cybercrime syndicates have in the past shared their expertise with other transnational criminal elements for fraud, money laundering and terrorist financing; it should be expected that cybercrime syndicates are now providing this expertise to other traditional criminal networks. It would not be a long wait before complex money mule systems managed by cybercrime groups become a popular method for other criminal organisations.

Professional criminals will always adapt and evolve to address law enforcement and regulatory efforts. Committed criminals will improve traditional methods and occasionally innovate and develop new means to perpetrate their criminal activities. With this clear commitment and motivation to innovate and overcome current protective measures, financial institutions will find that current regulatory benchmarks are simply insufficient. It is critical that the law enforcement community and financial institutions alike keep abreast with emerging trends to keep their risk based approach current.