National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Monthly Fraud Threat Update

March 2017

Key Judgements:

Impact on Individuals:

- Israeli Securities Authority takes action against Binary Options firms
- Evolution of Boiler Room Operations
- Recovery fraud for dating fraud victims

Impact on Enterprise:

- Conveyancing Fraud
- Money Mule Networks – CEO Fraud
- KurDish HaCKer – Website Defacement
- Legion from Heaven ransomware

Introduction

This monthly threat update will provide an overview of the trends affecting individuals and enterprise as reported to Action Fraud. This report incorporates an assessment of information received during the period of 1st February – 28th February 2017. We welcome your feedback so that we can shape future reports to your needs.

Investment Fraud

Israeli Securities Authority takes action against Binary Options firms

The increase in Binary Options reporting seen last month has continued; Binary Options reports represent 50% of all Investment Fraud in February 2017. Negative press surrounding Binary Options firms operating from Israel has resulted in the Israeli Securities Authority taking action. They have proposed a ban on Binary Options firms selling investments to overseas clients if they operate without a trading platform licence issued by the country of its clients. This is a positive step but the Investment Fraud desk believes it will lead to Binary Options firms utilising the European Economic Area (EEA) 'Passporting' mechanism in order to circumvent the new regulations and relocate parts of their businesses to an EEA member country allowing them to operate in all other EEA jurisdictions. The Investment Fraud desk believes that the most likely destination will be Northern Cyprus, however Eastern European countries are also possible destinations due to low costs, ease of travel, similar time zones and poor regulatory oversight and banking controls.

Evolution of Boiler Room Operations

The Investment Fraud desk has observed Boiler Rooms splitting up their functions in order to circumvent Financial Conduct Authority (FCA) and Financial Services Marketing Act (FSMA) regulations around cold calling. Boiler Rooms have separated into a lead generation entity and a brokerage. The lead generation acts as introducer and cold calls victims but does not engage in offering any financial or investment advice. The brokerage receives the leads from the lead generation and then makes the calls offering the financial/investment advice.

Banking & Corporate Fraud

Conveyancing Fraud

Reports of Conveyancing Fraud spiked at this time last year, corresponding with spring being a busy period for the property market. Conveyancing Fraud reporting volumes will therefore be closely monitored. A report in February gives details of a case where the fraudster hacked the solicitor's email account and emailed the victim requesting a payment diverted to another account. However the emails have since been deleted. This could suggest compromise of both sending/receiving accounts. There are various media reports that state that solicitors are still not doing enough to warn their clients about fraudsters.

Money Mule Networks

CEO Fraud networks have been seen regularly where a single suspect email address links to a number of reports. These networks usually show multiple payments to various bank accounts. Given that the payments seen in CEO Fraud are generally high value and credited to multiple accounts, it is likely that work done around these networks is also capturing data around money mules.

Cyber

KurDish HaCKer – Website Defacement

The Cyber desk has identified seven Action Fraud reports recorded in 2017 featuring the same website defacement methodology and suspect entity. The suspect has targeted small and medium sized businesses such as support organisations, schools and training companies which use the software WordPress version 4.7 and 4.7.1. When the victim clicks on the page, a Kurdish flag materialises and no payment is demanded. The message remains on the screen for less than two hours; however, while the message is present the victim is unable to update their company website.

Legion from Heaven – Dharma ransomware

The Cyber desk has identified seven Action Fraud reports recorded from 31st January to 26th February 2017 whereby suspects named 'Legion from Heaven' are using Dharma ransomware to receive Bitcoin funds. The new ransomware works by encrypting files on a server or computer drive through an open firewall port. A 2-3 Bitcoin ransom is demanded via the suspect email address to decrypt files. Victims have emailed the suspect address provided and received a response stating that the ransom demand will increase to 10 Bitcoins if it is not paid by the end of the day. Victims have also been requested to send a decrypted file to the address and in return, the suspect decrypts the file to show the ransom is not a hoax. Once the ransom is paid to a given dot wallet address, the suspect is no longer in contact and no more files were encrypted.

Mass Marketing Fraud

Recovery fraud for dating fraud victims

A case highlighted by the Economic Crime Victim Care Unit (ECVCU) involved a suspect following up a case of dating fraud with the victim by purporting to be an FBI investigator claiming to be looking into the original fraud. Although reporting levels on Action Fraud are currently low, there is a theme of a 'rescue' team at an institution, like Western Union of the FBI, who state they can recover the victim's money. This appears to be a similar MO to the 'recovery fraud' technique usually associated with Boiler Rooms; this involves the suspect contacting the victim and informing them that the money they lost in a previous investment fraud can be recovered. Suspects use genuine investigative organisations as suspect names.

Glossary of Terms

Binary Options	Binary Options are called 'Binary' because there can be only two outcomes – win or lose. To trade, all you need to do is bet on whether the price of something will rise or fall below a certain amount - if it is correct, you win and get paid. If not, you lose all of the money you originally invested. You can choose various commodities to trade in such as gold, oil or stocks etc. The value of a Binary Option is made up from the value of the asset you want to trade.
Ransomware	This is a form of malware that attacks your computer, locking you out and demanding payment in the form of a 'fine' to have it unlocked. The warning page distributed by the fraudsters, typically uses logos from both the Metropolitan Police and the Police Central Crime e-Crime Unit (PCEU) to make it look more like an official warning notice.
Boiler Room	A 'Boiler Room' operation refers to the use of high pressure sales tactics where fraudsters cold-call investors offering them worthless, overpriced or even non-existent shares. While they promise high returns, those who invest usually end up losing their money.
Money Mule	A money mule is someone who is recruited by those needing to launder money obtained illegally. The mule will accept money into their bank account, before following further instructions on what to do with the funds. Instructions could include transferring the money into a separate specified account or withdrawing the cash and forwarding it on via money transfer service companies like Western Union or MoneyGram.

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998.

The cover sheets must not be detached from the report to which they refer.

Protective Marking:	**NOT PROTECTIVELY MARKED**
FOIA Exemption:	NO
Suitable for Publication Scheme:	NO
Version:	FINAL
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Desk_Screening_Reports\Monthly Threat Update\17-03
Purpose:	Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports which have not been verified as true and accurate accounts.
Owner:	NFIB
Author:	Analyst, 105429p
Review By:	Senior Analyst, 88071e