National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Monthly Fraud Threat Update

April 2017

Key Judgements:

Impact on Individuals:

- Binary Options
- Job Internship Fraud – Other Advance Fee Fraud

Impact on Enterprise:

- Cyber Domain Names
- Ransomware Protect Campaign
- Ministry of Justice reports – Other Advance Fee Fraud

Cross Cutting Themes:

- Letting Agents set to clamp down on criminal money launderers

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 March – 30th March 2017. We welcome your feedback so that we can shape future reports to your needs.

Cyber

Cyber Domain Names

In March 2017, there were 367 different domain names recorded under the suspect email address field on Action Fraud, across all Cyber Fraud codes, with the exception of NFIB52D – Computer Hacking – PBX / Dial Through.

French (64) and Canadian (29) registered domain names have been utilised by several suspects in relation to malware / viruses / spyware, Hacking Personal, Hacking Social Media and Email and Hacking Extortion.

Email domains have been exploited by ex-partners or employees of a company seeking revenge or causing harassment; this could involve blackmail, emails received by businesses with changes to invoices (mandate fraud), phishing emails for major internet company platform purchases, and email accounts accessed and messages sent to contacts requesting money stating the victim is stranded abroad or due to other financial difficulties.

Computer Software Service Fraud has been generated from engineers claiming to fix broadband services have been received from organisation email addresses. Two thirds of the phishing suspect emails provided this month have been from foreign domains such as France, Romania, Argentina, Turkey and South Africa.

Domains have been attributed to ransomware from suspects located globally. For example one email domain is associated with Dharma ransomware which has been reported continuously over the last quarter.

Ransomware Protect Campaign

In June 2017 the Cyber Desk will be working to aid a City of London Police campaign exploring different types of ransomware and how they make extort from individuals and businesses for financial gain.

Investment Fraud

Binary Options

Binary Options still represent the biggest threat within the investment fraud arena. The Investment Fraud desk has seen a decline in reporting volumes this month – reporting volume has decreased from 50% of all reporting to just under 40%. However the sum of losses attributable to Binary Options is over £3 million for March, representing 22% of all losses for investment fraud. The total losses for investment fraud for March were £13,690,282.

Mass Marketing Fraud

Ministry of Justice reports – Other Advance Fee Fraud

Twenty five reports were received from the Claims Management Regulation Unit (CMRU), within the Ministry of Justice (MoJ). The Modus Operandi (M.O) is generally the same as Advance Fee Fraud, like PPI claim entitlement, however the theme is that the suspect(s) appear to claim to be different agencies. The MoJ/CMRU are often used along with the Financial Conduct Authority (FCA), Justice Department and Claims Advisory Group – a genuine firm that has been used by fraudsters for some time. A few reports also note that the suspect(s) already appeared to know some details about the victim. Figures that the CMRU provide suggest that although March 2017 is the highest volume in the previous 12 months, it is not historically (since January 2012) exceptional.

Job Internship Fraud – Other Advance Fee Fraud

There have been eight Action Fraud reports received regarding internship fraud involving eight victims, all of whom reside overseas. The victims believed they were being offered an internship to the UK with different companies. Five of the victims paid funds in advance, believing the payments were for insurance and accommodation. A recurring bank account was identified and on two occasions the suspect(s) have used the same employer company name. In two of the reports the original pick up point is identified as a web platform based in Belgium where companies and organisations can publish their internship offers and search for interns, and where prospective internship students can apply for internship vacancies.

Horizon Scanning

Under-35s 'more likely to feel lonely than over-55s'

Young adults are more likely to feel lonely than older people, despite having vastly more "digital friends", a report suggests.

Nearly nine in ten people (89%) aged between 18 and 34 have felt lonely at some point in their lives, compared with seven in ten (70%) over-55s, a survey from Nationwide Building Society found. The survey of 2,000 people also found that generally, people who always feel lonely are much more likely to have fallen victim to a financial fraud, including romance frauds, lottery or prize draw frauds, energy saving frauds and clairvoyance frauds.

Teamviewer

There is a new warning on TeamViewer (Remote Access Tool). It was confirmed by a security representative at TeamViewer that the warning was launched on 23/03/2017, so reporting levels mentioning the tool will be monitored going forward to measure effect/potential displacement.

Money Laundering

Open Source – Letting Agents set to clamp down on criminal money launderers

Letting agents will impose strict anti-money laundering checks on both tenants and landlords from June, raising workloads and pushing up costs.

The checks, on where both renters and their landlords get their cash and their identities, are being brought in under European legislation designed to clamp down on illegal money laundering through property.

http://www.thisismoney.co.uk/money/buytolet/article-4279090/Letting-agents-clamp-criminal-money-launderers.html

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.

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\17-04
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, 74545p