National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Monthly Fraud Threat Update

July 2017

CITY OF LONDON POLICE
Economic Crime Academy

To help prevent your business to counter fraud and/or to obtain details of our available courses, please contact the City of London Police Economic Crime Academy via our website http://academy.cityoflondon.police.uk or you can view our latest prospectus on http://academy.cityoflondon.police.uk/images/prospectus

Key Judgements:

Impact on Individuals:

- Overpayments using cheques
- Phishing emails
- Vehicle insurance and identity crime
- Ticketing Fraud

Impact on Enterprise:

- Email address linked to ransomware
- Virtual/Serviced office providers accepting payments using Bitcoin

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

Banking and Corporate

Overpayments using cheques

A suspect contacted a hotel enquiring about booking a large number of rooms and a pro-forma invoice is sent to the suspect detailing the quote. The suspect arranges for a payment by cheque, which is purposely a higher amount, and contacts the hotel to inform them of the overpayment. The hotel confirms receipt of the suspect's cheque and refunds the overpayment to the suspect. The hotel later realises the cheque sent by the suspect has not only bounced but was a false cheque.

Phishing emails

A victim received a Phishing email purporting to be from an online market place. In response, the victim provided their bank account details to claim a refund. A few days later the victim received a Vishing telephone call whereby the suspect purported to be from a high street bank, claiming there has been fraudulent activity on the victim's account. As part of the 'security process' the victim has provided their online banking details. The suspect carried out transactions and transferred funds to another account which had been set up using recently obtained false identities.

Cyber

Email address linked to ransomware

The email address Black.mirror@qq.com has now been seen as a suspect entity for two different ransomware variants. Originally it was seen in Amnesia ransomware reports, but in early July was seen using the .Aleta file extension (an updated version of BTCWare ransomware). This is the first time NFIB has been able to confirm an email address being used with 2 distinct ransomware strains.

Identity Crime

Vehicle insurance and identity crime

Victims are receiving letters from a car insurance company stating a car insurance policy has been set up using the victims' address details. The victims had not set up the policy and did not recognise the named driver. This is an ongoing trend and is not confined to any particular insurance company.

Investment Fraud

Virtual / Serviced office providers accepting payments using Bitcoin

A virtual office provider is accepting payments for their services using Bitcoin and have being doing so since 2013 and provide virtual / serviced office services to London addresses, including in the City of London. Research to date has not indicated that any UK virtual or serviced offices are currently accepting crypto-currencies as forms of payment. Fraudsters could pay for virtual / serviced offices in Bitcoins, making it harder for the NFIB to determine where the fraudsters are actually based.

Volume

Ticketing Fraud

The NFIB have received 690 Action Fraud reports concerning 'Go Tickets' since 31st May 2017. The victims allege that they have purchased concert and event tickets from the company online, paid by card through the company website, and not received the tickets. The funds have then been dispersed into other bank accounts, as well as being used to pay for VPN services, Google Adverts etc. Enquiries are still ongoing to ascertain which police force this network best sits with. The total loss thus far is £1.2million.

Glossary of Terms

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.
Vishing	Vishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by illegally impersonating a trustworthy entity in verbal communication via phone.

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:	V1.0
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Desk_Screening_Reports\Monthly Threat Update\17-07
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, 74545
Review By:	Senior Analyst, 74545