National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Monthly Fraud Threat Update

May 2017

Key Judgements:

Impact on Individuals:

- Bank Ring Fencing
- Software Exploit Kit
- Boiler Rooms receiving payment via Bitcoins
- Retail Voucher Payments
- Vishing Fraud
- Social media platform advertising rental accommodation
- NHS ransomware attack

Impact on Enterprise:

- Software Exploit Kit
- NHS ransomware attack

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

Banking and Corporate

Bank Ring Fencing

Following the global economic crisis in 2009, the UK Government introduced new rules to protect both the economy and taxpayers, should a similar economic crisis occur again. From 1st January 2019 banks must separate their retail banking operation from any wholesale or investment division, creating a new 'ring-fenced' bank.

To implement ring fencing banks will need to move some customers into a new part of the bank. This will result in some customers experiencing changes to their bank details; for instance, some customers will be issued new bank account numbers and sort codes. Each bank will be communicating with its customers about ring fencing and how it will affect them.

The Banking and Corporate desk is aware that some letters have already been sent out from banks to their customers well before the implantation date of 01/01/19. However a search of relevant keywords has been completed and no relevant reports have yet been identified. The Banking and Corporate desk will monitor in particular an increase in mandate fraud reporting.

Cyber

Software Exploit Kit

Online retailers often use third party payment software to process online payments. The Cyber desk has identified eight reports since January 2017 across various fraud codes where a particular software application has been compromised and as a result victims' credit card details have been stolen. This has either been through an administrator account with a weak password, through an open server vulnerability, or an insecure third party system which is on the company website but is not part of the software. Exploit kits can be purchased on the black market and suspects can scan the configuration of the computer for application security flaws using remote access. If vulnerability is detected, an exploit can be sent to the client often in the form of malware. According to the National Crime Agency this particular software is used by 25% of online retailers.

NHS Ransomware Attack

A global cyber attack crippled the National Health Service (NHS) as well as having a large impact in other European countries. Hospitals and GP surgeries in England and Scotland were among at least 16 health service organisations hit by the ransomware attack, which affected key systems including telephones. Some hospitals and surgeries were forced to turn away patients and cancel appointments as a result. Windows operated systems were attacked and data scrambled with the suspects making ransom demands of $300 to $600 to restore access. The NHS consequently made a decision to shut down their entire IT systems. The suspects allegedly made $60,000 in ransomware payments but the huge disruption to organisations and companies was far more damaging. The NCA are investigating the attack.

Investment Fraud

Boiler Rooms Receiving Payments via Bitcoin

The Investment Fraud desk has been informed by a retail bank that Boiler Rooms are now asking for victims to invest in shares using Bitcoins, by stating that investors would get "more for their money" if they used Bitcoins. Suspects are effectively offering a better exchange rate if payments are made using Bitcoins. The Investment Fraud desk has not yet seen any evidence of suspects taking payments via Bitcoins, however it is concerning as this would allow fraudsters to receive funds with no opportunity for law enforcement to be able to track the payments.

Mass Marketing Fraud

Retail Voucher Payments

In 2017, the Mass Marketing desk has been receiving reports in high volume that consistently reference a popular retail voucher. These vouchers were mentioned in 23% of reports received by Mass Marketing for February, March and April. Such vouchers as a traceless, preferred payment type for fraudsters is not new; however, specifically under Other Advance Fee Fraud, reports mentioning them increased by 23% in April, with 203 reports in total making reference to the vouchers. The most common MO appears to be that suspects contact the victims, often by telephone, and explain that they are owed HMRC tax or PPI repayments. In order to obtain this money the victims are informed that they must make an initial payment in the retail vouchers.

Volume

Vishing Fraud

The Volume Desk has identified eight reports received between November 2016 and April 2017 with variations on a similar MO where the suspects ask the victims to allow them remote access to their personal computer for various reasons, following which they then make transactions away from the account. There is a strong element of social engineering used to execute the frauds. Suspects purport to be from major banks and claim they need to access the victim's account either to pay the victim compensation, for security purposes or to investigate fraudulent activity on the account. Suspects request access to the victim's account via the 'Team Viewer' software tool and then move money between the victim's accounts for 'security testing' purposes. In some reports the suspects had prior knowledge of the victim's personal details which they used to gain the trust of the victim. The MO is very similar to cases of Computer Software Service Fraud where suspects phone the victim purporting to be from Internet Service Providers.

Social Media platform advertising rental accommodation

The Volume Desk has identified four reports which show that suspects are using a popular social media platform to advertise cheap apartments for rent. In three of the four reports the suspect used the same account page on this social media platform. The MO is generally very similar to case of rental fraud; the victims search for cheap rental accommodation on the social media platform and then contact the suspects. The suspect provides the victims with beneficiary accounts to transfer payment, but once payment is received, all communication ceases. It is likely that we will be seeing an increase of similar reports in the future. Research indicates that Action Fraud reporting of fraud offences involving this social media platform has dramatically risen in the last two years and is continuing to rise exponentially. For the calendar year of 2016 there were 1,818 offences involving this social media platform reported and at the beginning of May 2017 – only a third of the way through the year – there were already 913 offences reported involving this social media platform.

Glossary of Terms

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.
Bitcoins	Bitcoin payment is a legitimate, yet unregulated, online currency and its use is becoming more widespread and mainstream.
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:	FINAL
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Desk_Screening_Reports\Monthly Threat Update\17-05
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