National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Monthly Fraud Threat Update

February 2017

Key Judgements:

Impact on Individuals:

- Binary Options Fraud
- Mobile Phone Provider - Lottery Fraud
- .Loan Domain - Lender Loan Fraud
- Boot Sale App

Impact on Enterprise:

- CEO Fraud – Medical Practices Targeted
- Stealth Ravens – DDoS Extortion
- Dharma and Dridex Ransomware

Cross Cutting Themes:

- Online shopping Platform – Phishing Emails

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 January – 31st January 2017. We welcome your feedback so that we can shape future reports to your needs.

Banking & Corporate Fraud

CEO Fraud – Medical Practices Targeted

Medical practices are increasingly being targeted by fraudsters using a strong social engineering approach. The fraudsters send emails purporting to be from senior partners requesting payments under the pretence of a highly sensitive or urgent transaction. Initial contact appears to be primarily made via email from an address similar to the one that the senior partner would use, although the suspect may telephone to complete the fraud if required.

Cyber

Stealth Ravens – DDoS Extortion

Action Fraud reports have identified a DDoS-extortion group named 'Stealth Ravens'. Over the period of a week in late January, six medium to large companies received emails (from two different email accounts) claiming that unless they paid a demand of 10 Bitcoins before a specified date their public facing websites would be subject to full DDoS attacks. A demonstration DDoS was then performed on a company server for a brief period (however these did not impact on the companies' public websites). None of the companies paid the demand and subsequently none of the DDoS threats were followed through with.

Dharma Ransomware

Ransomware continues to be a key threat for cyber crime over the past year. Dharma is a new type of ransomware that has been reported since 2016 but has increased dramatically since the start of the new year

Dharma ransomware encrypts files on the server and adds the extension .wallet to the encrypted files. A text file is then placed on the victim's desktop which instructs victims how to pay a ransom (typically 1-4 Bitcoins) to decrypt their files.

Dridex Banking Trojan

The Dridex banking Trojan has made a return in 2017. So far seen sporadically in phishing emails, the Trojan's aim is to steal financial information off victim's desktops and servers. This financial information is then either sold online or used to commit further fraud.

Investment Fraud

Binary Options Fraud

Binary Options, including Forex and Contract for Difference (CFD) trading, continues to be the largest issue within investment fraud representing 55% of NFIB2E (Other Financial Investment) reports during January which stated a commodity.

Mass Marketing Fraud

Mobile Phone Lottery Fraud – Other Advance Fee Fraud

The Mass Marketing Fraud Desk highlighted the issue of a lottery fraud in January 2016. Victims are contacted by phone (text or call) by suspects purporting to be a mobile phone company and informed that they are a lottery winner. The reason being given that they are a 'winner' may include the victim's phone number or SIM card number being randomly selected in a ballot. The prize is typically £50,000 and an administration fee of approximately £500 is required to obtain the 'winnings'.

The mobile phone company have now advised the NFIB that a new approach of the suspects has been seen, whereby a fraudulent website is setup to compliment the SMS / call received by the victim.

.Loan Domain – Lender Loan Fraud

January recorded the first notable use of a .loan website domain for a lender loan fraud suspect. The .loan domain is classed as a generic top-level domain (gTLD), which is not restricted to specific users. The .loan domain was made generally available in August 2015 and was intended to provide a targeted keyword that connects businesses and people offering loans, credit, and related services with people looking for such services.

The use of the .loan domain may have been used to add credibility to the fraud; however it does not appear to be widely used by the legitimate lenders. Furthermore, options for disruption action by law enforcement are not specifically impeded by the use of a specialist gTLD.

Money Laundering

Online Shopping – Phishing Emails

There has been an increase in reports that state an online shopping platform is a suspect organisation. Victims are reporting that they receive an email that appears to be from this platform, but this is actually a phishing email from an unknown suspect in order to collect the victim's personal information. The email usually states that the victim has purchased a product on this online shopping platform and that to process a refund they need to click a link. There were 56 reports received in December 2016 and 215 reports received in January 2017.

Volume Crime

Boot Sale App

A boot sale app which allows consumers to buy and sell online has been the subject of 85 reports since 2014. 74 of these have been reported between February 2016 and January 2017. Reporting levels doubled between October, November and December. There has been a slight decline in January; however this continues to remain higher than pre-September 2016. The total financial loss is currently £12,338.51 and the most sought after item being a phone. 43 of the victims have paid via bank transfer. Fraudsters can exploit the app from both the perspective of the buyer and the seller.

The Modus Operandi (MO) when the suspect is the buyer is as follows: The victim identifies an item for sale that they wish to purchase and contacts the seller who requests the victim pays via bank transfer prior to the goods being sent via post. The item is not received and the victim is left unable to contact the seller.

The MO when the suspect is the seller is as follows: The suspect contacts the victim agreeing to purchase the item advertised. The suspect agrees to purchase and sends the victim a spoofed PayPal email stating that the funds would be released when a tracking number has been provided. The victim sends the item to the suspect but the suspect does not pay the funds as promised.

Glossary of Terms

DDoS Attack	Distributed Denial of Service (DDoS) attack is where multiple compromised or infected systems flood a targeted system – usually a system of web services. This is often to bring down an organisation's website.
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.
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.
Phishing	Phishing 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 an electronic communication.

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\17-02
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