CITY OF LONDON POLICE

ECONOMIC CRIME ENVIRONMENTAL SCANNING

Economic Crime Directorate

External Issue

May 2016

Purpose and Objective

The content of this document is based upon information gathered from open sources by the City of London Police. The purpose of sharing this information is to increase the awareness of issues identified as potential forthcoming economic crime or fraud threats and emerging issues and trends (some may indeed be current).

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:	
Storage File Location:	Performance
Purpose:	Environmental Scanning Report
Owner:	SDU
Author:	SDU
Review By:	

Contacts

Questions regarding this document can be sent to NFIBOutputs@cityoflondon.pnn.police.uk

Disclaimer

The information contained within this product is for general information purposes only and does not necessarily represent the views of the City of London Police. The City of London Police produces this product to enhance public knowledge of reported potential forthcoming economic crime or fraud threats and emerging issues and trends. This is a product that is continually under development. While the City of London Police strives to make the information on this product as timely and accurate as possible, we make no claims, promises, or guarantees nor do we give any express or implied warranty about the accuracy, adequacy or completeness of the contents of this product, and expressly disclaim liability for errors and omissions in the contents of this product. Any reliance you place on such information is therefore strictly at your own risk. Efforts will be made to correct errors brought to our attention.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not imply its endorsement, recommendation, or favouring by the City of London Police. The views and opinions expressed herein shall not be used for advertising or product endorsement purposes.

In no event will we be liable for any loss or damage howsoever arising including without limitation, direct, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this product or reliance upon any information contained within it.

With respect to articles linked within this document, The City of London Police do not accept any legal liability or responsibility for accuracy, completeness, or usefulness of any of the information disclosed, or represent that its use would not infringe privately owned rights.

Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.

Return to contents

Anti-Corruption Summit 2016

On 12 May, the Prime Minister hosted the Anti-Corruption Summit to step up global action to expose, punish and drive out corruption in all walks of life. The Summit brought together world leaders from countries including Afghanistan, Colombia, Nigeria and Norway.

The UK's Anti-Corruption Summit commitment can be accessed via the link below. It aims to:

- Expose Corruption
- Punish the corrupt and support those who have suffered from corruption
- Drive out the culture of corruption, wherever it exists

Linked articles

Gov.UK
Gov.UK - Summit Commitment

PM Announces New International Effort To Recover Assets of Crime

David Cameron has announced the creation of the first global forum to increase international efforts on asset recovery. The first forum will focus on returning assets to Nigeria, Ukraine, Sri Lanka and Tunisia. It will be held in the US next year, co-hosted with the UK, and will be supported by the UN and the World Bank.

Linked articles

Wired-Gov

New Proposals To Tackle Corporate Fraud

The Ministry of Justice will consult on plans to extend the scope of the criminal offence of corporate bribery and tax evasion to other economic crimes.

Police and other law enforcement agencies can struggle to prosecute corporations for money laundering, false accounting, and fraud under existing common laws. The consultation will seek views and evidence to assess whether changes in the law could allow the courts to more effectively prosecute corporate economic crime.

Linked articles

Wired-Gov

New Corporate Money Laundering Offence To Be Introduced

David Cameron has announced he will be introducing a new corporate offence for executives who fail to prevent fraud or money laundering inside their companies.

The prime minister has also revealed plans that will require all foreign companies buying property in the UK to disclose their true owners in a public register for the first time.

Linked articles

The Guardian

Return to contents

Fake DDoS Blackmailers Posing As Lizard Squad

Unidentified fraudsters are using the reputation of the hacker group Lizard Squad to scare website operators into paying ransoms with empty threats about distributed denial of service (DDoS) attacks.

Reports have been made of individuals being targeted with emails purporting to be from the Lizard Squad demanding users pay five Bitcoin (Approximately $3,000) to avoid a DDoS attack.

Linked articles

IT News

DDoS Researchers Suffer the Most DDoS Attacks

NexusGuard's latest Quarterly DDoS Report notes "Q1 has been incredibly interesting", continuing, "companies have increasingly become targets, and unexpectedly, the Number One target for DDoS attacks was DDoS researchers themselves." NexusGuard explained this finding stating "criminals don't want to be monitored. Furthermore, they do not want to have to work harder to perform their scams so they try to institute fear into the good guys."

Linked articles

SC Magazine UK

Hotels Targeted by Spear Phishing

Hotels have been repeatedly targeted over the previous year with point-of-sale malware attacks.

According to ARS Technica UK, the attacks are reported to have become increasingly targeted, in some cases "spear-phishing" e-mails and malware have been used. This type of spoofing fraud utilises emails that are crafted specifically for the target rather than a generic approach.

Linked articles

ARS Technica UK

72% of Individuals Would Avoid Buying From a Company That's Suffered A Security Breach

The security vendor FireEye interviewed 1,000 UK consumers and found that 72% would probably stop buying from a company in the future if it was revealed that a data breach had been partly caused by the boardroom neglecting to invest in cyber security.

Linked articles

Info Security

Phishing Apps Posing As Popular Payment Services Infiltrate Google Play

PC world has reported that malicious apps are slipping through Google's review process. The malicious apps operate by loading web pages containing false log-in forms that look like the target companies' websites. These web pages are used by the fraudster to collect login credentials and other pieces of personal information.

Linked articles
PC World

Malware Developed that can Hijack a System Without Needing To Infect a Computer First

Security researchers in Germany have created a proof-of-concept malware that can hijack PLC systems that are used to automate crucial processes in critical infrastructure, such as power plants, without needing to first infect a computer to get to those systems.

Linked articles
IB Times

Ransomware Allows Payment With Amazon Gift Cards

A new form of ransomware known as TrueCrypter gives victims the option of paying their ransom with Amazon gift cards. Unlike Bitcoins (which is the other payment method) Amazon Gift Cards are not anonymous and can be tracked by Amazon. That threatens TrueCrypter's author with considerable risk of discovery.

A glitch has also been identified in the malware in which victims can regain their encrypted files by clicking "Pay" without submitting any payment information results in files being automatically recovered without them losing any money.

Linked articles
Graham Cluley

Ransomware Claims to Donate Money to Charity

A new strain of ransomware has been identified which promises to donate the victim's ransom to a children's charity. The malware also offers to provide free technical support for three years to help the victim prevent future attacks.

Linked articles
IB Times

CONSULTATIONS/PUBLICATIONS

Online Transaction Fraud To More Than Double to $25bn By 2020

A study undertaken by Juniper Research has identified that online fraudulent transactions are expected to reach $25.6 billion by 2020; up from $10.7 billion last year. This means that by the end of the decade, $4 in every $1,000 of online payments will be fraudulent.

The new study identified 3 'hot' areas for online fraud:
- eRetail (65% of fraud by value in 2020 – $16.6 billion)
- Banking (27% – $6.9 billion)
- Airline ticketing (6% – $1.5 billion)

Linked articles
Juniper Research

LEGAL

Return to contents

The Pirate Bay Loses Its Main Domain Name

The Swedish Court ruled Thursday that it will take away the domain names 'ThePirateBay.se' and 'PirateBay.se' from The Pirate Bay and hand over them to the state.

The Pirate Bay is one of the most popular file-sharing torrent site predominantly used for downloading pirated or copyrighted media and programs free of charge.

The Pirate Bay's .SE domain was the world's 225th most popular website according to the Alexa ranking. Despite this the website will continue functioning as it also operates under numerous other domain name.

Linked articles
The Hacker News

ORGANISATIONAL

Two Thirds of Large UK Businesses Hit By Cyber Incident in the Past Year

Britain's businesses are being urged to better protect themselves against cyber criminals after government research found that two thirds of large businesses have experienced a cyber breach or attack in the past year. The research also identified:

- Nearly seven out of ten attacks on all firms involved viruses, spyware or malware.

- £1.9bn has been invested by the government to protect the UK, but industry must also act to help protect itself.

Linked articles
Wired-Gov

Swift Report Second Cyber Attack

Swift, the global financial messaging network that banks use to move billions of dollars every day, has acknowledged a second malware attack similar to the one that led to February's $81 million cyber heist at the Bangladesh central bank.

The second case targeted a commercial bank. It was not immediately clear how much money, if any, was stolen in the second attack.

Linked articles
The Guardian