CITY OF LONDON POLICE
Strategic Delivery Unit

Environmental Scanning

22.09.2016

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 current and potential forthcoming economic crime or fraud threats.

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.

CONTENTS

POLITICAL

Return to Contents

Creation of a "Great British Firewall" Mooted

The National Cyber Security Centre (NCSC) is exploring the creation of a national internet firewall with the intention of filtering out malicious websites and software on a national scale.

Some privacy groups have, however, raised issue with the idea of a government-controlled firewall, stating it may inhibit freedom of speech and give the government an unprecedented level of control over what UK citizens can access on the web.

Linked articles

The Next Web
The Guardian

National Cyber Security Centre Outlines New Approach To Combating Cyber Crime

Ciaran Martin, the current Director-General Cyber at GCHQ and the first Chief Executive of the new National Cyber Security Centre, has set out how the new organisation will adopt a more active posture in defending the UK from the range of cyber threats the UK currently faces, as well as the need for government, industry and law enforcement to work in even closer partnership.

The full speech made at the Billington Cyber Security Summit in Washington DC can be accessed via the link below.

Linked articles

Wired-Gov

Brexit: Impact Across Policy Areas – Research Briefing

A government paper has been published looking at the current situation and what impact Brexit might have on a range of policy areas. The policing and justice summary is included below:

"The UK currently has an opt out arrangement with the EU on policing and criminal justice measures, whereby it can chose which measures to opt in to. The UK has chosen, with parliamentary approval, to opt in to a number of measures, the most significant of which is the European Arrest Warrant (EAW). Others relate to information sharing and participation in EU law enforcement agencies.

Predictions about the consequences of Brexit are of course speculative at this stage and depend on the outcome of negotiations. However, it is likely that the UK would wish to recreate at least some of the existing arrangements. Some matters are covered by Council of Europe treaties (e.g. Convention on the Transfer of Sentenced Persons), although in practice these are generally less detailed and may prove to be less effective. In other areas it may be possible to negotiate bilateral treaties with individual Member States, or with the EU as a whole. It is possible that, without the mutual recognition and trust between EU Member States that underpins the EAW and other measures, these arrangements would be more complicated, expensive or time consuming."

Linked articles

Parliament - Research Briefing Summary
Full Briefing Paper

SOCIOLOGICAL/CRIME

Return to Contents

5 Million People Had To Cancel Their Bank Cards Last Year Due To Fraud

According to The Times, approximately five million people had to cancel their bank cards last year because of a cyber attack, identity theft or card cloning. Leaving an average loss of £475.

The paper reported that online fraud is so prevalent that people are starting to avoid the internet to make payments.

Linked articles

The Times

Consumers Avoid Firms That Have Suffered Data Breaches

A study of over 3,000 adults from the UK, France and Germany has identified that 50% of all consumers wouldn't share data with or buy products from firms that have suffered a data breach.

The study undertaken by F5 Network also revealed that 61% of UK respondents thought firms aren't doing enough to protect themselves from attack

Linked articles

Infosecurity Magazine

Data Breach Exposes 6.6million Users Personal Details

It has been revealed that ClixSense, a website that claims to pay users for viewing advertisements and completing online surveys has suffered a data breach.

The breach has exposed plaintext passwords, usernames, email addresses, first and last names, dates of birth, sex, home addresses, IP addresses, payment histories, and other banking details of more than 6.6 Million ClixSense users.

Linked articles

The Hacker News

Amex Customers Targeted With Phishing Prevention Scam *Sourced by NFIB Cyber*

Customers of American Express are being targeted by a phishing campaign under the guise that they are being provided with an identity theft and phishing prevention tool.

The phishing e-mails offer the use of SafeKey, a legitimate program that Amex offers its customers as an additional layer of security to guard against ID theft and phishing.

Linked articles

BetaNews

TECHNOLOGICAL

Return to Contents

PayPal Using Artificial Intelligence to Combat Fraud

PayPal is ahead of many big banks in using Artificial Intelligence (AI) to combat fraud. The company uses a home-grown artificial intelligence engine built with open-source tools to detect suspicious activity and separate false alarms from true fraud.

The system works in conjunction with human detectives who train themselves to think like fraudsters and like law-abiding citizens as they examine real-life cases that have triggered fraud alerts. They develop scenarios for good and bad user behaviour that they then feed into the artificial intelligence program to put this human intelligence into production.

Linked articles

American Banker

CallJam Malware *Sourced by NFIB Cyber*

A newly identified mobile malware named as "CallJam" repeatedly calls premium rate numbers once installed, racking up huge bills for the victim. The malware presents itself as a downloadable game in the official Google Play Store.

The unique threat of this malware is that the downloadable game it hides behind is rated four-stars on the Google Play Store, encouraging people to download it. It is believed that as many as 500,000 people have downloaded the malicious app since it was first uploaded to the Google Play Store back in May 2016.

Linked articles

Graham Cluley

LEGAL

UK Court Has Ruled That Alleged Hacker Lauri Love Can Be Extradited To The US To Face Charges There

Lauri Love, the alleged hacker accused of hacking into FBI systems, the US central bank, and the US missile defence agency, can now be extradited to the US to face charges after a ruling by a UK court.

Love could face up to 99 years in prison if he is convicted of the accusations. This case could set a precedent in future overseas hacking cases.

Linked articles

Infosecurity Magazine

ORGANISATIONAL

Vendor Security Alliance (VSA) Set Up To Improve Cyber Security Standards

The Vendor Security Alliance (VSA) has been set up to help businesses assess how secure third-party providers are. The alliance will undertake a yearly security and compliance questionnaire which will be used to assess vendor risk using a predetermined set of criteria, controls and practices.

The scheme was founded by Uber's head of compliance Ken Baylor. Other founding companies include: Pivotal, Dropbox, Palantir, Twitter, Square, Atlassian, GoDaddy, Docker, and Airbnb.

Linked articles

Infosecurity Magazine