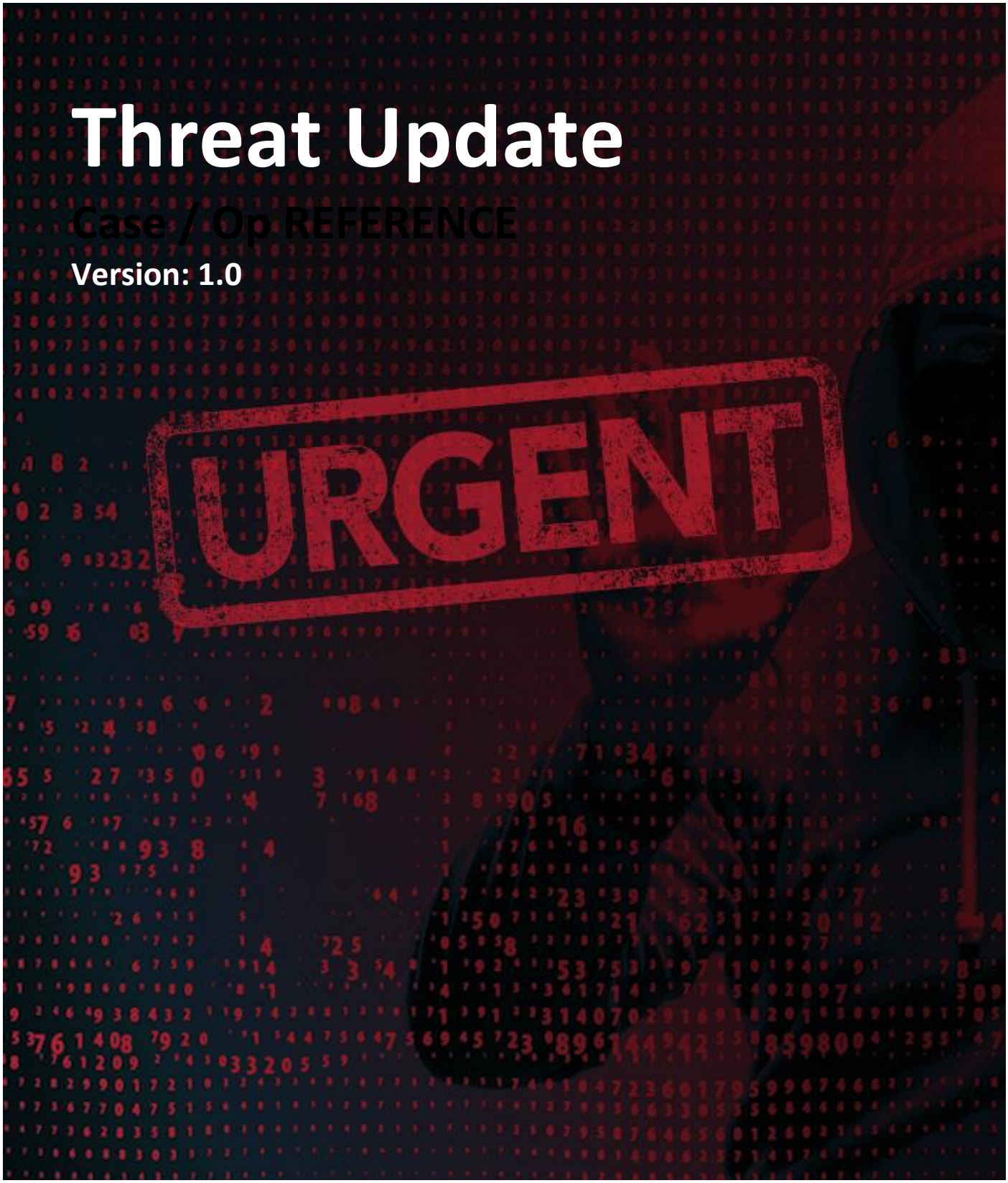
Threat Update

Case / Op REFERENCE

Version: 1.0



CITY OF LONDON POLICE
National Policing Lead For Fraud

Document Owner: National Fraud Intelligence Bureau

Author: Intelligence Analysts

Published: July 2018

Introduction

This 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 June 2018. We welcome your feedback so that we can shape future reports to your needs.

Cyber Crime

Ransomware

Ransomware was the main cyber-crime type reported to Action Fraud during June. 'Dharma' continues to be the most prevalent variant of ransomware reported. There has been an increase in the number of DDoS reports made to Action Fraud as well as more 'hacking servers' being reported.

Action Fraud received over reports relating to a well-publicised 'Wannacry' hoax to the call centre as 'live cyber crimes' but on assessment these were not deemed a threat.

Investment Fraud

Crypto Currency Investments

Cold callers and social media platforms have advertised 'get rich quick' investments in mining and trading crypto currency to members of the public. Victims have signed up to crypto currency investment websites providing personal details such as photocopies of credit cards, driving licence, passports and utility bills to open a trading account. The fraudster then calls the victim after the initial £250 minimum deposit has been made, to persuade the victim to invest again in order to obtain a greater profit. Reports have referred to investments in virtual currencies such as Bitcoin, Neo (Chinese), Ripple and Ethereum. Suspect companies appear to be based abroad but are targeting individuals in the UK. Victims have recognised they have invested in a fraudulent company after the website is deactivated and the suspects can no longer be contacted. Victims have then researched the fraudulent company and found forums stating it is a scam.

Volume Fraud

Use of Social Media for the Fraudulent Sale of Electronic Goods Fraud

A reoccurring observable has surfaced this month concerning an online marketplace. Suspect(s) who appear to reside in the UK have been advertising electronic goods for sale such as iPhones, MacBook-Pros or laptops at overly reasonable prices to entice victims. Suspects then provide the victim with beneficiary account details to transfer the payment to but once payment is made the suspects sever all contact and no goods are received. Victims are across the UK. Further analysis revealed this to be a regular MO employed by suspects each year at intermittent periods. Action Fraud has utilised social media channels to focus on the prevention of offences using alerts which have been well received and subsequently shared by the public across social media.

Author:	Analysts NFIB
Review By:	Senior Analyst 74545

Feedback

The NFIB welcomes feedback from our readers to evaluate the quality of our products through continuous improvement and to inform our priorities. Please would you complete the following NFIB feedback survey through: http://www.surveymonkey.com/s/AnalyticalProductsFeedback

If you have other feedback or additional information that you would prefer to provide by email please send to NFIBOutputs@cityoflondon.pnn.police.uk