National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Metropolitan Police Email Phishing Alert

November 2016

METROPOLITAN POLICE EMAIL PHISHING ALERT

The information contained within this alert is based on information received from various sources. The purpose of this alert is to increase awareness of this campaign currently in circulation. The campaign's primary function appears to be distributing new and powerful malware, through a malicious email attachment.

The alert is aimed at members of the public, local police forces, businesses and governmental agencies.

ALERT CONTENT

Fraudsters are sending out a high number of phishing emails to personal and business email addresses with the message subject heading 'Crime Prevention Advice'. The email sender is potentially spoofing a Metropolitan Police email address, showing the sender as 'crime@content.met.police.uk'.

The email contains the text:

"TO THE GENERAL PUBLIC;

See attached document to read more about crime prevention advice.

Regards,

Metropolitan Police Service."

The email includes an attachment titled '11212527.zip'.

This attachment contains malicious content which downloads the iSPY key logger to the victim's device. This key logger records keystrokes, steals passwords stored in web browsers and Skype conversation records, takes pictures via webcam and stores the license keys of software like Microsoft Office and Adobe Photoshop.

PROTECTION / PREVENTION ADVICE

Having up-to-date virus protection is essential; however it will not always prevent you from becoming infected.

Please consider the following actions:

- Don't click on links or open any attachments you receive in unsolicited emails or SMS messages. Remember that fraudsters can 'spoof' an email address to make it look like one used by someone you trust. If you are unsure, check the email header to identify the true source of communication. Information on how to locate email headers can be found at https://mxtoolbox.com/Public/Content/EmailHeaders/
- Always install software updates as soon as they become available. Whether you are updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
- Most anti-virus software contains an 'anti-spyware' scan which may be able to detect key loggers. If your current software does not offer this function, consider installing software which does - both free and paid for anti-spyware is widely available.
- Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It's important that the device you back up to is not left connected to your computer as any malware infection could spread to that device as well.
- If you think your bank details have been compromised, you should immediately contact your bank**.**
- If you have been affected by this, or any other fraud, report it to Action Fraud by calling **0300 123 2040**, or visiting www.actionfraud.police.uk.

FEEDBACK

The NFIB needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following NFIB feedback survey through: https://www.surveymonkey.com/r/FeedbackSDU. This should take you no more than 2 minutes to complete. If you have other feedback or additional information that you would prefer to provide by email please send to NFIBfeedback@cityoflondon.pnn.police.uk.

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:	V1
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Cyber Crime Desk\Alerts
Purpose:	Alert on malware campaign using Metropolitan police email address
Owner:	NFIB Management
Author:	105098P, Researcher
Review By:	DI Grahame Mace