National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Mass Phishing Campaign
Ransomware and Banking Trojan Alert

September 2016

Mass Phishing Campaign Ransomware and Banking Trojan Alert

The information contained within this alert is based on a high number of recent reports made to Action Fraud. The purpose of this alert is to increase awareness of the mass phishing campaign currently in circulation. The campaign's primary function appears to be distributing well known ransomware and banking Trojan, through an email attachment believed to be malicious.

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

ALERT

Fraudsters are sending out a high number of phishing emails to personal and business email addresses with various message subject headings such as: *'Account report'*, *'Equipment receipts'*, *'Tax invoice'* and *'Your account has been closed'*. The subject headings change daily. The emails include attachments that people are prompted to open for further information.

These attachments contain malicious content which downloads Locky ransomware to lock the victim's device and demand payment to unlock it, or a Dridex banking Trojan which steals banking credentials and other sensitive information in order to obtain an access to victim's financial records.

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.
- 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.
- 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 isn't left connected to your computer as any malware infection could spread to that too.
- Don't pay extortion demands as this only feeds into criminals' hands, and there's no guarantee that access to your files will be restored if you do pay.
- 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 scam, 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 and Date:	V1
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Cyber_Protect_Team\Alerts
Purpose:	Alert on mass phishing campaign distributing ransomware and banking Trojan
Owner:	NFIB Management
Author:	103804X, Analyst
Reviewed By:	103987P, Senior Analyst