National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

'Law Abiding Citizen' Phishing Fraud
Phishing & Banking Trojan Alert

March 2017

'LAW ABIDING CITIZEN' PHISHING CAMPAIGN AND BANKING TROJAN ALERT

The information contained within this alert is based on intelligence from various sources. The purpose of this alert is to increase awareness of a mass phishing campaign currently in circulation. The campaign's primary function appears to be distributing a well known Banking Trojan 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 volume of phishing emails to personal and business email addresses, pretending to come from various email addresses, which have been compromised.

The subject line contains the recipient's name, and the main body of text is as below:

"Hi, [name]!

I am disturbing you for a very serious reason. Although we are not familiar, but I have significant amount of individual info concerning you. The thing is that, most likely mistakenly, the data of your account has been emailed to me.

For instance, your address is:

[real home address]

I am a law-abiding citizen, so I decided to personal data may have been hacked. I attached the file – [surname].dot that I received, that you could explore what info has become obtainable for scammers. File password is – 2811

Best Wishes,"

The emails include an attachment – a '.dot' file usually titled with the recipient's name.

This attachment is thought to contain the Banking Trojan Ursniff/Gozi, hidden within an image in the document. The Ursniff Banking Trojan attempts to obtain sensitive data from victims, such as banking credentials and passwords. The data is subsequently used by criminals for monetary gain.

PROTECTION / PREVENTION ADVICE

Having up-to-date virus protection is essential; however it will not always prevent your device(s) 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 (you can find out how by searching the internet for relevant advice for your email provider).
- Do not enable macros in downloads; enabling macros will allow Trojan/malware to be installed onto your device.
- 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 is important that the device you back up to is not connected to your computer as any malware infection could spread to that as well.
- If you think your bank details have been compromised, you should contact your bank **immediately**.
- If you have been affected by this or any other fraud, report it to Action Fraud by calling **0300 123 2040**, or visit 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 law abiding citizen phishing fraud
Owner:	NFIB Cyber
Author:	105098P
Review By:	12966J