National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Urgent Alert:
"ONLINE EXTORTION DEMAND AFFECTING UK BUSINESSES"

April 2016

ONLINE EXTORTION DEMAND AFFECTING UK BUSINESSES

The information contained within this alert is based on a number of reports made to Action Fraud. The purpose of this alert is to make businesses aware of the problem and to share information with other Law Enforcement Agencies.

ALERT

Within the past 24 hours a number of businesses throughout the UK have received extortion demands from a group calling themselves 'Lizard Squad'.

Method of Attack:
The group have sent emails demanding payment of 5 Bitcoins, to be paid by a certain time and date. The email states that this demand will increase by 5 Bitcoins for each day that it goes unpaid.

If their demand is not met, they have threatened to launch a Denial of Service attack against the businesses' websites and networks, taking them offline until payment is made.

The demand states that once their actions have started, they cannot be undone.

PROTECTION / PREVENTION ADVICE

What to do if you've received one of these demands:

- Report it to Action Fraud by calling 0300 123 2040 or by using the online reporting tool
- Do not pay the demand
- Retain the original emails (with headers)
- Maintain a timeline of the attack, recording all times, type and content of the contact

If you are experiencing a DDoS right now you should:

- Report it to Action Fraud by calling 0300 123 2040 immediately.
- Call your Internet Service Provider (ISP) (or hosting provider if you do not host your own Web server), tell them you are under attack and ask for help.
- Keep a timeline of events and save server logs, web logs, email logs, any packet capture, network graphs, reports etc.

Get Safe Online top tips for protecting your business from a DDoS:

- Consider the likelihood and risks to your organisation of a DDoS attack, and put appropriate threat reduction/mitigation measures in place.
- If you consider that protection is necessary, speak to a DDoS prevention specialist.
- Whether you are at risk of a DDoS attack or not, you should have the hosting facilities in place to handle large, unexpected volumes of website hits.

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.