



NATIONAL SECURITIES CLEARING CORPORATION LIMITED

DEPARTMENT : NSCCL-COMPLIANCE

Download Ref No : NSCCL/CMPT/35725

Date : September 5, 2017

Circular Ref. No : 868/2017

All Members

Sub: Locky ransomware spreading through massive spam campaign

In regards of the recent ICT threat received from regulators, all members are hereby notified and requested to undertake appropriate actions as applicable to their environment. A brief description and immediate steps to be taken are mentioned below.

1) Description of the threat:

- It has been reported that a new wave of spam mails are circulating with common to spread variants of Locky ransomware. Reports indicate that over 23 million messages have been sent in this campaign.
- The messages contain common subjects like “please print”, “documents”, “photo”, “Images”, “scans”, and “pictures”. However the subject texts may change in targeted spear phishing campaigns.
- The messages contain zip attachments with Visual Basic Scripts (VBS) embedded in a secondary zip file. The VBS file contains a downloader which polls to domain “greatesthits[dot]mygoldmusic[dot]com” (please do not visit this malicious website) to download variants of Locky ransomware.

2) Key actions to be taken to mitigate the threat:

- a) Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- b) Update firmware/patches for all network components and network products
- c) Ensure anti-virus signatures are updated on all assets.
- d) Block any suspicious IP addresses on firewall
- e) Block USB usage
- f) Ensure IPS/IDS signatures are updated.
- g) Ensure Email Gateway solutions has all relevant updates for detecting possible mails that may bring Trojans/malicious content in the environment. Also block sensitive file extensions such as “.exe”, “.rtf”, “.vbs”, and “.js” etc. , including macros - at the perimeter level
- h) Make the users aware about this threat and ensure that users do not download any suspicious attachments and/or browse suspicious/malicious links
- i) Maintain a backup of critical data and store it offline and/or at a different location
- j) Please block indicators of compromise as per Annexure A

- k) For additional recommendations, please refer the attachment (Annexure A). Please also refer to the previous advisories issued by CERT-IN – Annexure B and Annexure C

3) Reference Links:

- a) <http://www.cert-in.org.in>
- b) http://www.cyberswachhtakendra.gov.in/alerts/locky_ransomware.html
- c) <http://www.cyberswachhtakendra.gov.in/alerts/ransomware.html>

4) Disclaimer:

- a) The information contained in this notice has been extracted from regulatory sources and has been published only as a guidance to members. As the future course of events with regards to this threat are not known, members are advised to keep a close watch on their systems to identify timely detection and remediation of this threat
- b) Members shall act upon this notice at their own discretion after conducting appropriate impact/risk analysis to their specific environment
- c) Please note that the other exploit kits are also widely in circulation and available for download for free on the Internet and there are possibilities of attack vectors other than this threat which may exist/emanate. It is critical to perform a self-assessment against these zero-days/ exploit kits released in the wild in a controlled environment.
- d) This notice is for informational purpose only

Members are requested to take note of the above.

**For and on behalf of
National Securities Clearing Corporation Limited**

Authorised Signatory

Telephone No	Fax No	Email id
1800 266 0057	022-26598243	nsccl_compliance@nsccl.co.in