

NATIONAL STOCK EXCHANGE OF INDIA LIMITED**DEPARTMENT : MEMBER SERVICE**

Download Ref No : NSE/MSD/34873	Date : May 15, 2017
Circular Ref. No : 13/2017	

All Members,

Wannacry / WannaCrypt Ransomware alert

In regards with the recent ransom-ware threat, members are hereby notified and requested to undertake appropriate actions as applicable to their environment. A brief description and immediate steps to safeguard the systems is given in Annexure-1

Kindly take note of the same.

For and on behalf of
National Stock Exchange of India Limited

Khushal Shah
Chief Manager

Toll Free No	Fax No	Email id
1800 266 00 53	+91-22-26598155	msm@nse.co.in

Annexure-1

1) Description of the threat:

It has been reported that a new ransom-ware named as "Wannacry" is spreading widely. Wannacry encrypts the files on infected Windows systems. This ransom-ware spreads by using a vulnerability in implementations of Server Message Block (SMB) in Windows systems. This exploit is named as ETERNALBLUE. The ransom-ware called WannaCrypt or WannaCry encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN. The ransom-ware also spreads through malicious attachments to emails.

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

- a) Ensure all Workstations and Servers have the latest Microsoft patches, especially the ones related to MS17-010.
- b) Ensure anti-virus signatures are updated on all assets. Block IOCs on anti-virus solution as per the links provided in point 3 below.
- c) Block the IP addresses on Perimeter Firewall as per the links provided in point 3 below.
- d) Ensure IPS/IDS signatures are updated. Verify if the signature that can detect this vulnerability / exploit attempt is enabled and is in blocking mode.
- e) Ensure Email Gateway solutions has all relevant updates for detecting possible mails that may bring the Trojan in the environment. Also block sensitive file extensions as per the links provided in point 3 below.
- f) Ensure Proxy solution has an updated database. Block IOCs for IP Address and Domain names on the Proxy as per the links provided in point 3 below.
- g) Review any traffic towards ports 139, 445 at the perimeter level - Block if not required.
- 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.

3) Additional references:

Detailed advisory can be referred at:

- i. <http://www.cert-in.org.in>
- ii. http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html

4) Disclaimer:

- a) The information contained in this notice has been extracted from public 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 in circulation widely and available for download for free on the Internet and there are possibilities of attack vectors other than ransom-ware 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.