NATIONAL STOCK EXCHANGE OF INDIA LIMITED

DEPARTMENT : MEMBER SERVICE	
Download Ref No : NSE/MSD/35582	Date : August 10, 2017
Circular Ref. No : 19/2017	

All Members,

Malicious Software Script alert

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:

a) A communique from National Cyber Security Coordinator regarding a highly suspicious communication being observed on the internet in the country has been identified.

b) An advanced software script (malware) is associated in such suspicious communication which is specifically targeting critical sectors which predominantly include Energy and Finance. The software infects devices to get foothold in the ICT Networks / systems, steals information, passwords and pass over to the adversaries outside the country. The software script also has the capability to encrypt entire information on the computer system. In some cases, the data hosted or stored on the computer terminals may be lost permanently. The infected files reappear again and again. The software script connects to a malicious domain, the location of which keeps on changing in Germany and Russia.

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

a) In order to prevent infection, users and organizations are advised to apply patches to Windows operating systems and Microsoft Office products.

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) For additional recommendations, please refer the attachment (Annexure A).

3) 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.

For and on behalf of
National Stock Exchange of India Limited

Abhijeet Sontakke
Senior Manager

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