



NATIONAL SECURITIES CLEARING CORPORATION LIMITED

DEPARTMENT : NSCCL-COMPLIANCE

Download Ref No : NSCCL/CMPT/35250

Date : June 30, 2017

Circular Ref. No : 863/2016

All Members

Sub: Petya /Petrwrap Ransomware Alert

In regards of the recent ransomware threat, 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 variants of Petya ransomware with worm-like capabilities is spreading. The ransomware leverages etenalblue exploit, genuine psexec or wmic with appropriate credentials for a quick spread .

These mechanisms are used to attempt installation and execution of the dropped file C:\Windows\perfc.dat” on other devices to spread laterally. The dropped file, if managed to get the Administrator privileges, will encrypt the Master File Tree (MFT) tables for NTFS partitions and overrides the Master Boot Record (MBR) with a custom bootloader making the system unusable.

Further the malware creates a scheduled task via schtasks /at to reboot the system one hour after infection. After the system is reloaded the malware downloads its code from MBR and encrypts data on the hard drive.

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 systems as mentioned in Microsoft Security Bulletin 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 (specifically .rtf) at the perimeter level.
- f) Ensure Proxy solution has 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
- j) For additional recommendations, please refer the attachment (Annexure A) and links provided in point 3 below

3) Additional references:

- a) Detailed advisory can be referred at:
 - i. <http://www.cert-in.org.in>
 - ii. http://www.cyberswachhhtakendra.gov.in/alerts/petya_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 widely in circulation 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

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

Hima Bindu Vakkalanka
Assistant Vice President

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