Government of India
National Critical Information Infrastructure Protection Centre
(A Unit of NTRO)

Date: 23 Dec 2019

Cyber Security Advisory: IPs related to Malware activities

Following IPs/URLs have been found targeting Critical Information Infrastructure and appear to be related to malware activities. The IoCs are:

1. IPs 209[.]99[.]40[.]223 & 209[.]99[.]40[.]222 having Domain: service[-]norton[.]com, belongs to threat actor APT-33(IRAN) responsible for sending spear-phishing emails loaded with malicious HTML Application files.

2. IP 208[.]91[.]197[.]91 Domain: onixcellent[.]com belongs to threat actor 'TrickBot-Anchor' responsible for stealing information.

3. IP 50[.]63[.]202[.]61 belongs to threat actor 'Phoenix Keylogger' responsible for stealing information.

Recommendation:

1. It is requested to monitor the above IP addresses in your IT infrastructure & take appropriate action.

2. It is also advised to update regular patches.

Disclaimer:

The information provided by NCIIPC above is on "as is" basis only. System owners are advised to independently evaluate the contents for its applicability in their specific environment, and take appropriate action as per their own assessment of the implications of the alert/ advisory on their systems. NCIIPC will not be liable for any issues or problems that may arise from application or non-application of the alert/ advisory. System owners are wholly responsible for cyber security updates to their information technology systems.

With Best Regards,
Knowledge Management System
National Critical Information Infrastructure Protection Centre
Block-III, Old JNU Campus, New Delhi - 110067
Website: www.nciipc.gov.in
Toll Free: 1800-11-4430