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

**Date: 28 Nov 2019**

## Cyber Security Advisory: CACTUS PETE APT

This data is to be considered as **TLP:AMBER**

Our trusted partner has reported regarding the surge in malicious activity by threat actor “Cactus Pete”. The initial mode of spreading this infection is via spear phishing mail that carry LNK (Link Configuration File) files as attachments. Once victim opens this LNK file, a backdoor (customized by threat actor) gets installed on victim's machine. Using this backdoor threat actor performs malicious activity on victim's machine like building the connection with Command and Control (C2), data transfer etc.

**IOCs:**

**DOMAINS:**
Vip[.]onedumb[.]com
Babyhome[.]mefound[.]com
wikipedia[.]dnset[.]com
hotandria[.]com

**HASHES(SHA512):**
CF51A0AF59D15CD8BB8AE2E02F411F47
519270876A23309DE5D93BB8023D78C3
5222BCC36D4929E947068978393CED3A
C90D3F841D2C772E5B85D17B304D72C0
044D209CBBE87EED5E04A0AFAB2A480F
418B930934D8402F7B3AFB52424F37CE

**Recommendations:**

- Monitor Connection attempts towards the listed domains. The list may include compromised domains resources as well.
- Deploy web and email filters on the network. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Enforce application whitelisting on all endpoint workstations.
- Both ingress and egress traffic of the listed domains and all hash values should be kept under an active watch-list in the respective endpoints and security solutions.

**Reference:** CERT-In

**Disclaimer:**



**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**