Subject: **SYN ful Knock: A Cisco Router Implant (Technical Advisory No 01 - January 2016)**

1. **Introduction.** Global security experts have identified various worldwide incidents of SYNful Knock which is a stealthy modification of the CISCO router's firmware image that can be used to maintain persistence within a victim's network. This backdoor provides ample capability for the attacker to propagate and compromise other hosts and critical data.

2. **Vulnerability.** The initial infection vector does not appear to leverage a zero-day vulnerability. It is believed that the credentials are either by default or discovered by bruteforce to install the backdoor.

3. **Known Affected Hardware** Devices affected by SYNFul Knock are listed below:-

- **a.** CISCO 1841 router
- **b.** CISCO 2811 router
- **c.** CISCO 3825 router

4. **Method for Detection.** A combination of host and network-based indicators can be used to determine the health of the underlying network.

- **a.** **Host-Based Indicators**
  - **(1)** Hashing the ,image and comparing the result to the hash from CISCO to detect a modified binary
  - **(2)** If command-line access is possible, command attached as Annex 'A' can be used to detect the implant
- **b.** **Network-Based Indicators.** Both active and passive network detection can be deployed to detect and prevent a compromise. Passive detection can be incorporated into network defense sensors while active techniques can be used to hunt for the backdoor.
  - **(1)** **Active Detection.** Following scripts and tools actively scan for the presence of this implant.
    - **(a)** Modified Nmap Scripting Engine (NSE) Script. Attached as Annex **'B'.**
  - **(2)** **Passive Detection.** An IDS monitors the external interface of the router to effectivelydetect this backdoor from the network

5. **Recommendation.** In order to mitigate effect of SYNK nock, following measures should be taken:-

- **a.** Refresh the router with a known authentic firmware from CISCO.
- **b.** Ensure the new image hash values match and then harden the device to prevent future compromise.
- **c.** A compromise assessment (to check the way in which infection have occurred) should be followed.