Subject:- **CYBER WARNING REGARDING REGIN MALWARE (ADVISORY NO.01 DATED 13TH JANUARY, 2015).**

It is to intimate that recently Symantec Discovered Regin, a sophisticated backdoor Trojan used to conduct intelligence-gathering operations. It is a military grade surveillance malware that works in different stages, making it very difficult to understand and analyze.

2. **Intended Targets**. The victims of Regin fall into following categories :-

a. Telecom Operator

b. Government institutions

c. Multinational political bodies

d. Financial Institutions

e. Research institutions

f. Individuals involved in advanced mathematical /cryptographic research

g. Military Organizations

3. **Open Source Analysis**. Regin is a cyber-attack platform, which the attackers deploy in victim networks for total remote control at all levels. The platform is extremely modular in nature and has multiple stages.

a. **Stage 1.** Modules for 64-bit systems are signed with fake digital certificates.

b. **Stage 2.** In second phase, a marker file is created that is used to identify the target machines.

c. **Stage. 3.** The third stage is implemented as a driver module and provides the basic functionality of the malicious framework. It is responsible for operating its own created encrypted Virtual File System (VFS) and loading additional plugins and also provides several built-in plugins for the entire framework.

d. **Stage 4** In fourth stage, code from the Regin platform is stored in encrypted file storages, known as Virtual Files Systems (VFSes).

e. **Stage 5 (Final Executing Phase).** It is implementation phase of Regin Platform which performs all the deadliest tasks including data theft, traffic interception, key logging, taking screen shots etc.

4. **Indications of Infection**. Reportedly, the malware creates following files in various stages:-

a. \system32\wsharp.dll

b. \system32\wshnetc.dll

c. \system32\nsreg1.dat

d. \system32\bssec3.dat

e. \system32\msrdc64.dat

5. **<u>Recommendations</u>**. Due to highly sophisticated method of penetration of this malware, protection from it is a serious concern. Following precautionary measures can be taken to avoid this malware:-

a. Use software firewall such as Comodo Internet Firewall of Zone Alarm or any other firewall and block any unknown files from accessing internet.

b. Install and update reputed antivirus such as Kaspersky, Avira, Avast, Bit defender, Eset etc.

c. Find and delete the files mentioned at para 4 above.

d. Incase system is found to be infected, do following :-

(1) Disconnect from Internet.

(2) Backup the data to external drive or secondary partition.

(3) Reinstall windows to remove malware from partitions, registry, startup, temporary file locations and windows services.

e. Avoid using VPN software such as spot flux, hotspot shield etc.