CYBER SECURITY BULLETIN
Ghost Rat (or Gh0st RAT)

Cyber Security Bulletin Number: 001

Type of Cyber Threat:

Ghost RAT (or Gh0stRAT): is an Advance Persistent Threat (APT), a malware for Windows platform.

Date Monitored: From 11 Nov – 18 December 2013

Description:

GhostRAT is used by the operator of the Ghostnet. It used to hack into some of the most sensitive computer networks. It is a cyber-spying computer program. The "RAT" part of the name refers to the software's ability to operate as a "Remote Administration Tool".

Analysis:

The GhostNet system disseminates malware to selected recipients via a computer code attached to stolen emails and address, thereby expanding the GhostNet bot network by allowing more computers to be infected. According to the Infowar Monitor (IWM), "GhostNet" infection causes computers to download a Trojan known as "Ghost Rat" that allow attackers to gain complete, real-time control. Such a computer can be controlled or inspected by its hackers, and even has the ability to turn on the camera and audio-recording functions of an infected computer that has such capabilities, enabling monitors to see and hear what goes on in a room.

Ghost is spreading infection together with Backdoor.ADDNEW, a novel kind of backdoor Trojan which seizes passwords stored in Firefox while it carries out Distributed Denial-of-Service assaults. Gh0st that is basically used for online spying, targets Windows computers while having phone-home abilities for GhostNet C&C (command-and-control) server. As the malware controllers maneuver Gh0st-contaminated systems remotely, they plant more malware that include surveillance-featured programs especially keyloggers. The attacks are mainly aimed at high-profile persons' computer systems within the government, finance and also the military.

Suggested Action:

a) Use only licensed Windows OS and softwares. Updates or patches fix the problem with your operating system and software programs. If your Windows OS is unlicensed, the probability of infection with GhostRAT is high.

b) Install and run an Anti-Virus program. Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the last updated: date.

c) Check your computer's security settings for a built-in personal firewall. If you have one, turn it on. Firewalls act as protective barriers between computers and the internet.

d) Do not install unnecessary programs on your computer.