16 - 10 - 2012

**Ricardo Gil Montejo**

***Solución del Cibercafé***

**Propuesta: CiberCap**

* **1er Programa**
* **Programa CiberCap (Se instala en los Clientes de los Cibercafé)**
* Se le configura en un .ini la dirección ip del servidor donde va a estar el servidor ftp
* Al iniciar el programa comienza a enviar hacia esa misma dirección ip un comando llamado “EA” que significa “Estoy Aquí” (cada 5 seg.).
* Captura las pantallas (.bmp) cada vez que cambie el nombre de ventana y las envía hacia el ftp
* Contiene un Keylogger y envía las capturas de teclas cada 15 seg hacia el ftp. (.txt)
* Cuando se conecta un dispositivo extraíble obtinene las propiedades del dispositivo (.txt) y lo envía hacia el ftp.
* Cuando se conecta un dispositivo extraíble hace un árbol de directorios desde la raíz del dispositivo(.txt) ) y lo envía hacia el ftp.
* Captura todo el texto que se copie al clipboard incluso nombre de archivos y lo escribe en el txt del Keylogger.
* Puede apagar la PC por un comando que se le envíe.(APC)
* Puede reiniciar la PC por un comando que se le envíe.(RPC)
* Captura todo el texto que se copie al clipboard incluso nombre de archivos.
* Los comandos a usar son:
* “EA” – Estoy aquí.
* “ConUSB” - Conectado el USB.
* “DesUSB” - Desconectado el USB.
* “RPC” - Reiniciar la PC
* “APC” - Apagar la PC
* **2do Programa**
* **Programa CiberDesp**
* Revisa el directorio del FTP y va creando carpetas dentro con nombre del host que los envía.
* Al mismo tiempo va insertando en la base de datos.
* **3er Programa**
* **CiberLig**
* Recibe los comandos de los CiberCap.
* Inactiva los que se pasen 5 min sin reportarse activos
* Le manda comandos a los CiberCap según los parámetros puestos en la bd.
* **4to Programa**
* **CiberGest**
* Tiene un FrontEnd para analizar los contenidos.
* Tiene una pantalla para asignarle nombre de maquinas a los usuarios.
* Tiene un módulo de trabajo con usuarios.
* Tiene un módulo para configurar los Troyanos que se quieran activar así como los que se quieran desactivar o eliminar de la bd.
* Cyber cafe
* Pgina / suplanta la autentificación de Windows
* Steady State / politicas de windows