Attack Modes

An attack mode is the device type that a USB hotplug attack tool, like the USB Rubber Ducky, is functioning as. The original USB Rubber Ducky had only one mode: `HID` — functioning as a keyboard.

With the introduction of the Bash Bunny, a multi-vector attack tool, the `ATTACKMODE` command was introduced to the DuckyScript language to manage multiple device functions.

Modes of Attack

The new USB Rubber Ducky supports three attack modes — `HID`, `STORAGE`, and `OFF`.

HID

The `HID` attack mode functions as a Human Interface Device (a keyboard) for keystroke injection.

STORAGE

The `STORAGE` attack mode functions as USB Mass Storage (a Flash Drive). This may be used for copying files to or from a target — often referred to as infiltration or exfiltration. In the `STORAGE` attack mode, the MicroSD card connected to the USB Rubber Ducky will be exposed to the target.

OFF

The `OFF` attack mode prevents the USB Rubber Ducky from being enumerated (seen) by the target as a connected device all together.

ATTACKMODE

The `ATTACKMODE` command accepts multiple parameters which describe how the device will be enumerated by the target. At a minimum, a mode (`HID`, `STORAGE` or `OFF`) must be specified.

The `ATTACKMODE` command consists of these parts

- The `ATTACKMODE` keyword
- The mode, or modes `HID` or `STORAGE` or `HID STORAGE` or `OFF`

- Optionally a `VID` and `PID`
- Optionally a `MAN`, `PROD` and `SERIAL`

Example

```
ATTACKMODE STORAGE
REM The USB Rubber Ducky will function as a "flash drive"
```

Result

As the comment suggests, the USB Rubber Ducky will be recognized by the target as a benign USB flash drive.

Example

```
ATTACKMODE HID
REM The USB Rubber Ducky will function as a "keyboard"
```

Result

As the comment suggests, the USB Rubber Ducky will be recognized by the target as a USB Human Interface Device (HID) "keyboard".

Example

```
ATTACKMODE OFF
REM The USB Rubber Ducky will not be enumerated by the target
```

Result

As the comment suggests, the USB Rubber Ducky will not be recognized by the target.

Default Behaviors

If no `ATTACKMODE` command is specified as the first command (excluding `REM`), the new USB Rubber Ducky will default to the original standard `HID` mode and function as a keyboard.

Duplicate or redundant `ATTACKMODE` commands will be ignored. For example, if the ATTACKMODE is currently `STORAGE` and a new `ATTACKMODE STORAGE` command is specified, it will be ignored and the USB Rubber Ducky will not be re-enumerated by the target.

If no `BUTTON_DEF` is implemented, pressing the button will execute `ATTACKMODE STORAGE` — switching the USB Rubber Ducky into a flash drive.

If no `inject.bin` file is found on the root of the MicroSD card (the USB Rubber Ducky storage), then the device will show a red LED and execute `ATTACKMODE STORAGE`.

Multiple Attack Modes

Multiple modes may be specified simultaneously. When this is done, the USB Rubber Ducky device is recognized as what's called "composite device", whereby multiple functions may be defined.

For example, the USB Rubber Ducky can act as both a `HID` keyboard, and a "flash drive" `STORAGE` device.

Example

```
ATTACKMODE HID STORAGE
REM The USB Rubber Ducky will function as both a "flash drive" a
```

Result

As the comment suggests, the USB Rubber Ducky will be recognized by the target as a composite device with both the `HID` "keyboard" and `STORAGE` functions.

Changing Attack Modes

The `ATTACKMODE` command may be used multiple times throughout a payload.

Changing the attack mode will cause the target to re-enumerate the device.

Example

```
ATTACKMODE HID
DELAY 2000
STRINGLN The USB Rubber Ducky is functioning as a keyboard.
STRINGLN It will function as a flash drive for the next 30 secon
```

```
ATTACKMODE STORAGE
DELAY 30000
ATTACKMODE HID
DELAY 2000
STRINGLN Now the USB Rubber Ducky is back to functioning as only
STRINGLN For the next 30 seconds it will function as both keyboa
ATTACKMODE HID STORAGE
DELAY 30000
STRINGLN Now the USB Rubber Ducky will disable itself.
ATTACKMODE OFF
```

Result

- This payload will begin by enumerating as a HID keyboard.
- The USB Rubber Ducky will then enumerate as a mass storage "flash drive" for 30 seconds.
- Once more it will be enumerated as only a HID keyboard.
- Next it will enumerate as both a HID keyboard and a mass storage "flash drive".
- Finally, the device will seem to be disconnected.

VID and PID Overview

USB devices identify themselves by combinations of **Vendor ID** and **Product ID**. These 16-bit IDs are specified in hex and are used by the target to find drivers (if necessary) for the specified device.

Identifying Vendor and Product IDs

On a Linux system, the VID and PID for each connected USB device can be shown using the `lsusb` (list USB) command.

```
┌──(kali㉿xps13kali)-[~/Desktop]
└─$ lsusb
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 003: ID 0489:e0a2 Foxconn / Hon Hai
Bus 001 Device 002: ID 0bda:58f4 Realtek Semiconductor Corp. Integrated_Webcam_HD
Bus 001 Device 012: ID 046d:c31c Logitech, Inc. Keyboard K120
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

In the above screenshot, we can see that the device with Vendor ID `046D` and Product ID `c31c` is connected to the computer. In this example, the vendor is Logitech, Inc. and the Product is Keyboard K120.

Spoofing Vendor and Product IDs

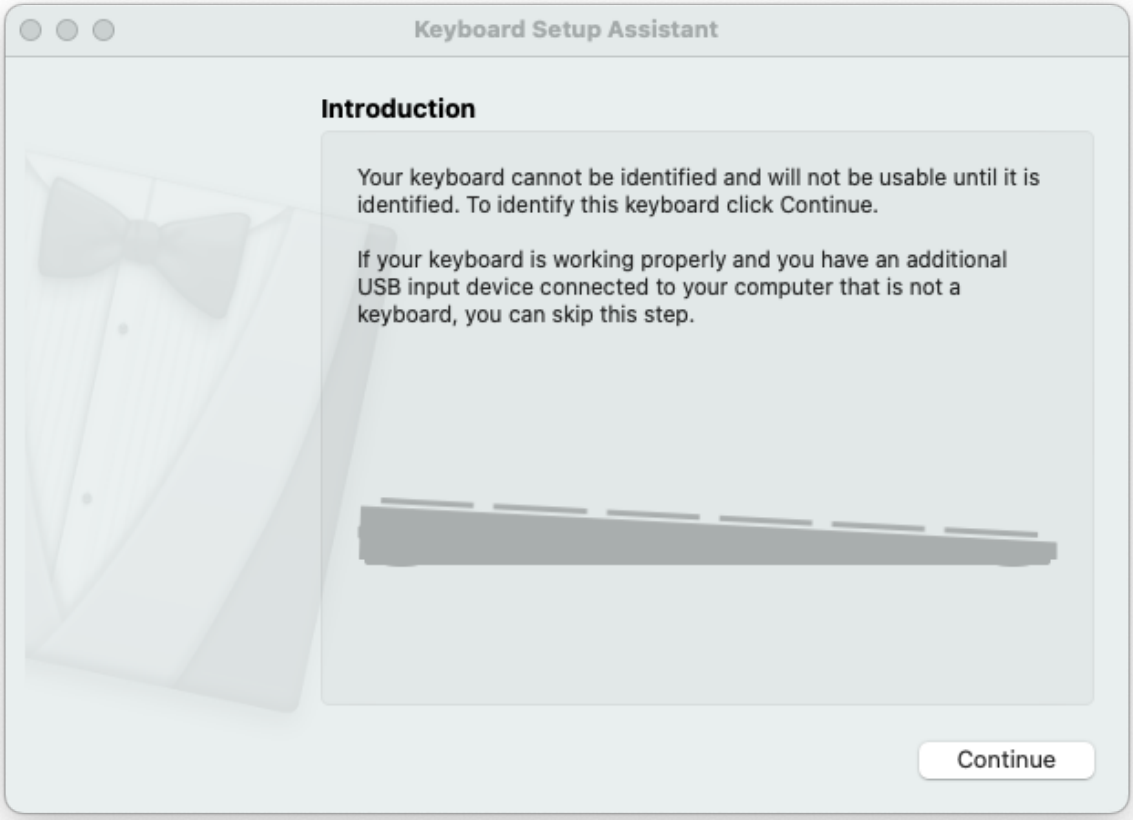
Using the `ATTACKMODE` command, the optional `VID` and `PID` parameters may be specified using the following syntax:

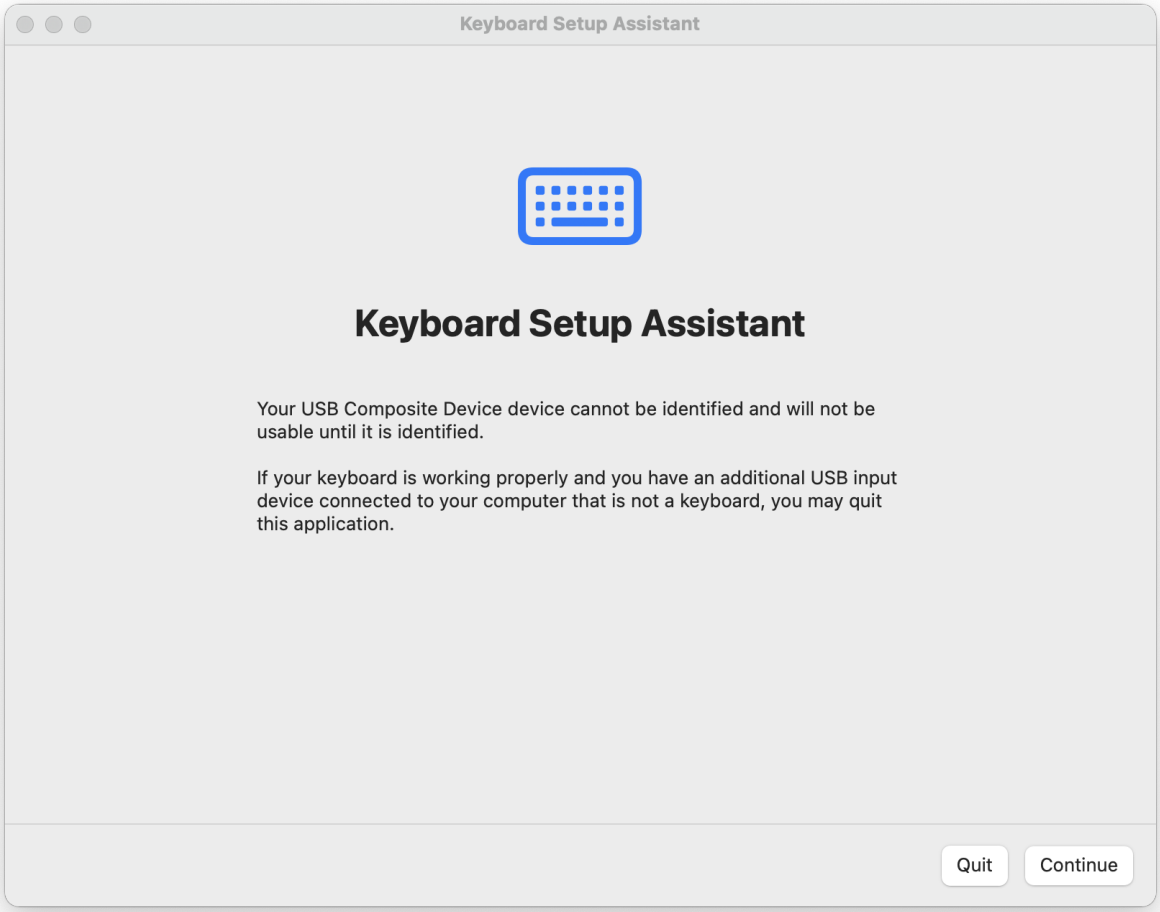
```
ATTACKMODE HID VID_046D PID_C31C
```

This `ATTACKMODE` command will instruct the USB Rubber Ducky to enumerate using the defined values, thus spoofing a real Logitech K120 keyboard. This can be very useful in situations where the target is configured to only allow interaction with specific devices.

A nearly complete list of VID and PID information may be found from Linux USB Project website at http://www.linux-usb.org/usb.ids

Checking this list, we can see that Apple uses the Vendor ID `05AC`. Among others, we find that the Product ID `021E` specifies the Aluminum Mini Keyboard (ISO). This is very useful when deploying payloads against macOS targets as a non-Apple keyboard will result in the Keyboard Setup Assistant opening.


Keyboard Setup Assistant
Introduction
Your keyboard cannot be identified and will not be usable until it is identified. To identify this keyboard click Continue.
If your keyboard is working properly and you have an additional USB input device connected to your computer that is not a keyboard, you can skip this step.
Continue



If the following `ATTACKMODE` is specified, the Keyboard Setup Assistant will be suppressed.

```
ATTACKMODE HID VID_05AC PID_021E
```

MAN, PROD and SERIAL Overview

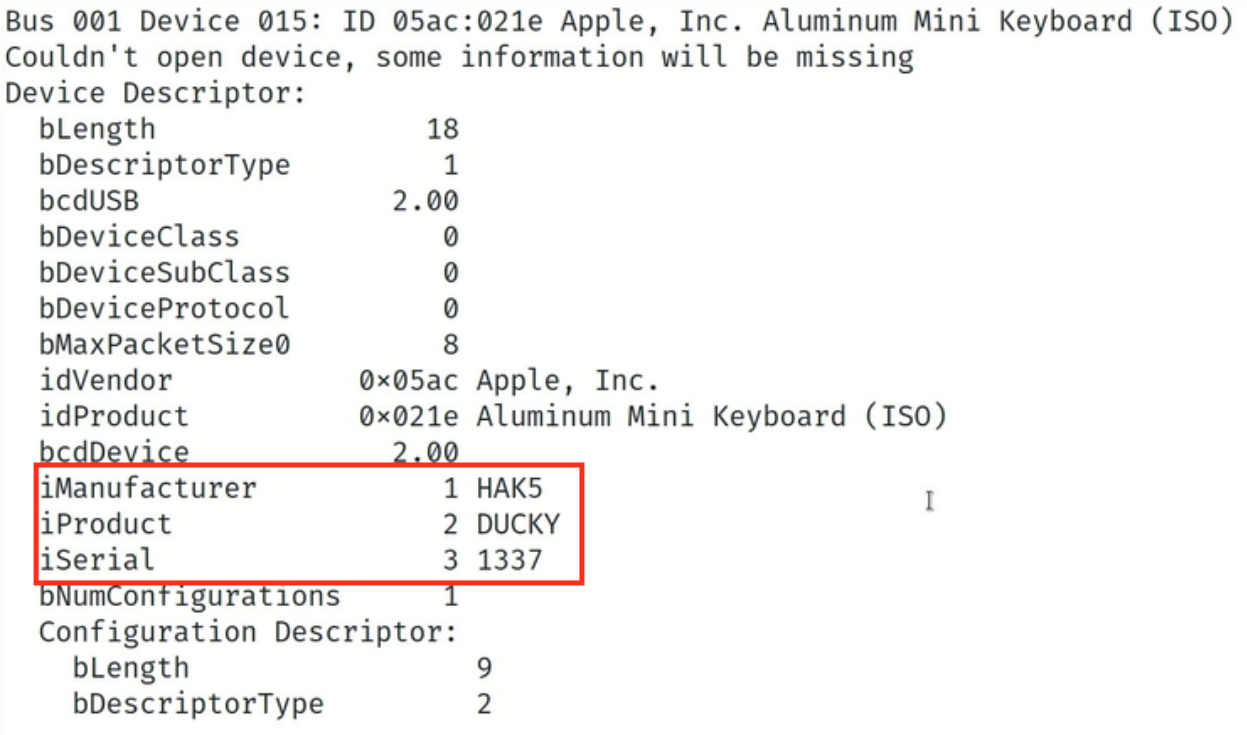
In addition to the Vendor ID and Product ID parameters used to identify a USB device, the device iManufacturer (`MAN`), iProduct (`PROD`) and iSerial (`SERIAL`) may be specified using `ATTACKMODE`.

Example

```
ATTACKMODE HID VID_05AC PID_021E MAN_HAK5 PROD_DUCKY SERIAL_1337
```

Result

Checking `lsusb` (List USB) with the `-v` (verbose) option, we can see that the specified device includes the `VID` and `PID` values of the `Apple, Inc. Aluminum Mini Keyboard (ISO)`, however the `MAN`, `PROD` and `SERIAL` values are defined as specified using the `ATTACKMODE` command.



Default Behaviors

If no `MAN`, `PROD` and `SERIAL` parameters are specified, the USB Rubber Ducky will enumerate with the defaults "`USB Input Device`" (for both `MAN` and `PROD`) and a `SERIAL` of `111111111111`.

Advanced Usage

Keeping in mind that the `ATTACKMODE` command may be executed multiple times within a payload, and that device enumeration is dependant on the identifiers specified within the `ATTACKMODE` command (`VID`, `PID`, `MAN`, `PROD` and `SERIAL`), re-enumerating the device

may only require changing one value — depending on the target OS. This may be useful when re-enumeration is desired.

SERIAL_RANDOM

If specified, the SERIAL_RANDOM parameter will use the pseudorandom number generator to select a unique 12 digit serial number. This is covered in greater detail in the section on randomization.

Example

```
ATTACKMODE HID STORAGE MAN_HAK5 PROD_DUCKY SERIAL_RANDOM
```

SAVE and RESTORE Overview

Within a payload the `ATTACKMODE` command may be executed multiple times.

In some situations it can be useful to "remember" an `ATTACKMODE` state, for later recall.

SAVE_ATTACKMODE

The `SAVE_ATTACKMODE` command will save the currently running `ATTACKMODE` state (including any specified `VID`, `PID`, `MAN`, `PROD` and `SERIAL` parameters) such that it may be later restored.

Syntax

```
SAVE_ATTACKMODE
```

Example

```
ATTACKMODE HID
SAVE_ATTACKMODE
```

Result

The parameters `HID` of the command `ATTACKMODE` will be saved for later recall.

RESTORE_ATTACKMODE

The `RESTORE_ATTACKMODE` command will restore a previously saved `ATTACKMODE` state.

Example

```
ATTACKMODE HID STORAGE VID_05AC PID_021E MAN_HAK5 PROD_DUCKY SEI

BUTTON_DEF
    RESTORE_ATTACKMODE
    STRINGLN The ATTACKMODE has been restored.
END_BUTTON


STRINGLN The USB Rubber Ducky is now in a ATTACKMODE HID STORAGE
SAVE_ATTACKMODE

STRINGLN This state has been saved. Now entering ATTACKMODE OFF
STRINGLN Press the button to restore the ATTACKMODE.
ATTACKMODE OFF
```

Result

The USB Rubber Ducky will be recognized as a composite USB device with both `HID` and `STORAGE` features.

Strings will be typed informing the user of the save state, the button functionality, and entering `ATTACKMODE OFF`.

Pressing the button will restore the previously initialized `ATTACKMODE`.

Internal Variables

The following internal variables relate to `ATTACKMODE` and may be used in your payload for advanced functions.

$_CURRENT_VID

Returns the currently operating Vendor ID with endian swapped.

May only be retrieved. Cannot be set.

$_CURRENT_PID

Returns the currently operating Product ID with endian swapped.

May only be retrieved. Cannot be set.

$_CURRENT_ATTACKMODE

Returns the currently operating ATTACKMODE represented as:

Value	ATTACKMODE
0	`OFF`
1	`HID`
2	`STORAGE`
3	`COMPOSITE` (Both `HID` and `STORAGE`)

May only be retrieved. Cannot be set.