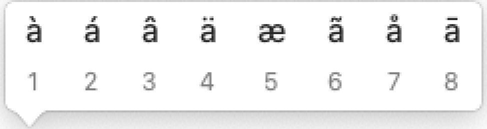
Holding Keys

OverviewWhat happens when you hold down a key on a computer keyboard? To answer that, we must ask ourselves — what does it mean to hold a key? How does holding a key differ from pressing a key? In both cases, the key is both pressed and then subsequently released. The difference between pressing a key and holding a key is the time that goes by between pressing and releasing the key.If you're typing at 80 words per minute you're making 400 keystrokes per minute, or nearly 7 keys per second. This equates to about 0.15 seconds, or 150 milliseconds, per key. Considering the key press, release and travel time between each key — one may approximate that roughly half, or about 75 ms, of that time to be the duration of a key press.Obviously this will change dramatically depending on the human operating the keyboard — but suffice it to say that anything below 200 milliseconds may be considered a key press. When processing the keystroke injection command `STRING Hello, World!` the USB Rubber Ducky interprets each key individually — communicating with the attached computer each respective key press HID code and key release HID code. In the case of the first character of the `Hello, World!` string — the uppercase `H` — the process involves holding down the `SHIFT` modifier key, pressing the `h` key, releasing `h` key, then finally releasing `SHIFT`. Each of these are represented by a Human Interface Device (HID) code which is interpreted by the attached computer. All of this is being processed 60,000 times per second — which is what allows the USB Rubber Ducky to "type" at superhuman speeds. What happens when a key, for example the letter `a` key, is held for a second? The answer is quite dependant on the operating system of the computer to which the USB Rubber Ducky is attached. On a modern Windows computer, a payload holding the letter `a` key for 1 seconds may result in `aaaaaaaaaaaaaaaaaaaaa` while the same payload may result in only `aaaaaaaaaa` on a similar computer running Linux. This can vary from computer to computer, as determined by each systems configured repeat delay and repeat rate.This is to illustrate that the result of holding a key is very much dependent on the way the target computer is configured.



Further, the same payload holding the letter `a` key on a macOS target may result in the accent menu appearing rather than a sequence of `a` characters.

HOLD and RELEASE

The `HOLD` command will hold the specified key, while the `RELEASE` command will release it. Both commands require a key parameter.

Example

```
REM Example HOLD and RELEASE
REM Target: Windows

ATTACKMODE HID STORAGE
DELAY 2000

REM Open Powershell
GUI r
DELAY 1000
STRING powershell
ENTER

REM Hide Powershell Window
DELAY 2000
ALT SPACE
DELAY 100
m
DELAY 100
HOLD DOWNARROW
DELAY 3000
RELEASE DOWNARROW
ENTER

REM Run desired commands in obfuscated powershell window
```

```
STRING tree c:\
ENTER
```

Result

- This example payload targets Windows systems.
- Using the `GUI r` key combo to open the Run dialog, a powershell window will be opened.
- The `ALT SPACE` key combo opens the window menu of the currently active window (in this case, the powershell window), followed by the `m` key to select the Move command.
- The `DOWNARROW` is held for 3 seconds, as specified by the `DELAY 3000` command, before being released — thus hiding the contents of the powershell window below the screen.
- The benign `tree c:\` command is run, producing a graphical directory structure of the disk.

Holding Modifier Keys

Similar to how pressing a modifier key (`GUI`, `SHIFT`, `CONTROL` or `ALT`) requires the `INJECT_MOD` prefix, so too does holding a modifier key.

Example

```
REM Example modifier key hold

ATTACKMODE HID STORAGE
DELAY 2000

INJECT_MOD
HOLD CONTROL
DELAY 4000
RELEASE CONTROL
```

Result

The `CONTROL` key will be held for 4 seconds.

Holding Multiple Keys

Multiple HOLD commands may be combined to hold more than one key simultaneously.

Example

```
REM Example holding multiple keys

ATTACKMODE HID STORAGE
DELAY 2000

STRING iddqd
DELAY 500

WHILE TRUE
    STRING idkfa
    DELAY 500
    HOLD LEFTARROW
    HOLD UPARROW
    INJECT_MOD
    HOLD CONTROL
    DELAY 5000
    INJECT_MOD
    RELEASE CONTROL
    RELEASE UPARROW
    RELEASE LEFTARROW
    DELAY 500
END_WHILEiddqd
```

Result

Answering the age old question, "will it run doom?", this payload proves the 1993 classic first-person shooter no match for the USB Rubber Ducky.

More specifically, this payload will cause Doom Guy to walk in circles firing his weapon.

50
AMMO
100%
HEALTH
ARMS
0%
ARMOR