Automating On-Site USB-Attacks

Presentation by: Sebastian Haas
What is the Bashbunny?
Similarities and differences to a Rubberducky
Speed comparison with different keyboard emulators
When to use?
How to extend / high-level architecture
Make it run more than two payloads
Github repository etc.
~/bashbunny/what

- **USB Device Emulator**
  - Keyboard/HID Emulation
  - Network Emulation (RNDIS + ECM)
  - Storage Emulation (RW and RO)
  - Serial Connector
- **Computer**
~/bashbunny/diff

- **Rubberducky**
  - 60 MHz 32-bit processor
  - Several KB RAM
  - Some KB Flash
  - Scriptlang: Duckyscript

- **Bashbunny**
  - 1.6 GHz Quadcore ARM
  - 512 MB DDR3 RAM
  - 8 GB Flash
  - Scriptlang: Extended Bash
  - RGB Indication LED (!)

$44.99  $99.99
~/bashbunny/speed

Time in seconds needed for 1000 characters (less is better)
• On-Site attacks during security assessments
• Not-So-Legal™ attacks
• Task automation on offline systems
~/bashbunny/original

+-----------------+
|:   |    Boot Modes   |
+----+               *
+--|||------------+
|||
+-|||-- (sw1) Switch Position 1: Customizeable Payload.
|+- (sw2) Switch Position 2: Customizeable Payload.
+- (sw3) Switch Position 3: Arming Mode + Serial + Mass Storage.
How to extend a three position switch virtually?

- LED Pushbutton Sequencer

https://github.com/H8to/HoppEye
Boot Modes

- (sw1) Switch Position 1: Confirm Payload / Run Chosen Payload.
- (sw2) Switch Position 2: Selection ColorWheel.
- (sw3) Switch Position 3: Arming Mode + Serial + Mass Storage.
Folder structure on the device:

```
payloads/
  switch1/
    payload.txt
  switch2/
    payload.txt
```
~/bashbunny/modified

Folder structure on the device:

payloads/
  payload_B_BluePayload/
  payload_G_Green/
  payload_OFF_empty/
  payload_W_network/
  payload_C_empty/
  payload_M_PoisonBunnyTap/
  payload_R_ReverseShellEmpire/
  payload_Y_empty/
  switch1/
  switch2/
  payload.txt <-- This is where magic happens
DEMO TIME!
~/bashbunny/halt

kkthxb
~/bashbunny/man

- https://github.com/H8to/HoppEye
- https://twitter.com/H8_sec
- http://h8.to/

Questions?