HARDWARE HACKING · EL USB QUE PARECE INOCENTE

# Rubber Ducky: el USB que hackea en 30s

Cómo un dispositivo del tamaño de un USB ejecuta un ataque completo en segundos — sin que el antivirus lo detecte, sin instalar drivers, sin dejar rastro visible.

## 01 — ¿QUÉ ES UN USB RUBBER DUCKY?

### Un teclado disfrazado de USB

El USB Rubber Ducky de Hak5 es un dispositivo que se ve exactamente como un USB de almacenamiento normal. Pero cuando se conecta a una computadora, el sistema operativo lo reconoce como un teclado HID (Human Interface Device) — no como almacenamiento. Eso le permite ejecutar secuencias de teclas preprogramadas (payloads) a velocidades imposibles para un humano: hasta 1,000 pulsaciones por minuto.

Fuente: Hak5 · hak5.org/products/usb-rubber-ducky · Primer lanzamiento: 2010 · Versión actual: 2022

**30s**
tiempo promedio de un ataque BadUSB completo

**0**
alertas de antivirus — el SO lo ve como "teclado"

**1K**
pulsaciones por minuto — imposible para un humano

## 02 — VARIANTES DEL ATAQUE BADUSB

### USB Rubber Ducky (Hak5)

**$80 USD**

La herramienta profesional original. Usa DuckyScript — lenguaje simple para scripting de payloads. Almacenamiento en MicroSD para múltiples payloads. Reconocida como estándar de la industria en pentesting.

`DuckyScript · MicroSD · Profesional`

### DigiSpark / Arduino

**$3–8 USD**

Microcontrolador ATTiny85 programable como HID. Más lento y limitado que el Ducky, pero funcional para payloads simples. Disponible en MercadoLibre México.

`ATTiny85 · Arduino IDE · DIY`

### O.MG Cable

**$180 USD**

Un cable USB-C que se ve y funciona como cable normal — pero tiene un chip WiFi interno que puede recibir payloads de forma remota e inyectarlos en la computadora conectada.

`WiFi · Cable normal · Remoto`

### ESP32 como BadUSB

**$9 USD**

Con la librería USB HID de ESP32 puedes programarlo para emular teclado. Menos sofisticado que el Ducky pero funcional como herramienta de aprendizaje y pruebas en entornos controlados.

`ESP32 · USB HID · DIY · MIT License`

## 03 — CÓMO FUNCIONA UN ATAQUE BADUSB PASO A PASO

**0s** — SEGUNDO 0 · CONEXIÓN

### El USB se conecta al puerto

El sistema operativo detecta un nuevo dispositivo HID (teclado). La instalación del "driver" es automática — es el driver estándar de teclado de Windows, macOS o Linux. No hay alerta, no hay pop-up de seguridad.

**1s** — SEGUNDO 1 · PREPARACIÓN

### Espera un segundo para que el driver cargue

El payload incluye un delay de 1 segundo para asegurar que el dispositivo esté completamente inicializado antes de comenzar a "escribir". Este delay es configurable en DuckyScript con el comando DELAY.

**2s** — SEGUNDO 2 · EJECUCIÓN

### Abre terminal y ejecuta comandos a 1,000 pulsaciones/min

En Windows: GUI+R (ejecutar), escribe "powershell", Enter. En macOS: CMD+Space, escribe "terminal", Enter. En segundos tiene acceso a la terminal del sistema. Lo que viene después depende del payload programado.

`⚠ PowerShell / bash / zsh — todos accesibles`

**5s** — SEGUNDO 5–25 · PAYLOAD

### Ejecuta el payload específico del ataque

Descarga un script desde internet, crea un usuario administrador oculto, extrae contraseñas del navegador, instala un RAT (acceso remoto), exfiltra archivos, captura screenshots, activa el micrófono — lo que el payload defina.

**30s** — SEGUNDO 30 · FINALIZACIÓN

### Cierra terminal. Se desconecta. Sin rastro visible.

El payload cierra la terminal, limpia el historial de comandos y el USB se desconecta. Para el usuario, parece que nada pasó. El atacante ya tiene acceso, credenciales o datos exfiltrados.

## 04 — PAYLOADS DOCUMENTADOS EN INVESTIGACIONES DE SEGURIDAD

### Extracción de contraseñas del navegador

Herramientas como LaZagne extraen contraseñas guardadas en Chrome, Firefox, Edge en texto plano desde la base de datos local. El payload las exporta a un archivo y lo sube a un servidor externo.

⏱ Tiempo de ejecución: 5–15 segundos

### Creación de usuario administrador oculto

En Windows: net user hacker P@ss123! /add → net localgroup administrators hacker /add. El usuario aparece en el sistema pero no en la pantalla de login. Acceso persistente remoto establecido.

⏱ Tiempo de ejecución: 3–5 segundos

### Instalación de reverse shell (acceso remoto)

Descarga y ejecuta un agente de acceso remoto que se conecta al servidor del atacante. Desde ese momento, el atacante tiene control completo de la computadora sin necesidad de estar físicamente presente.

⏱ Tiempo de ejecución: 10–25 segundos

### Exfiltración de archivos sensibles

Copia documentos de carpetas específicas (Documentos, Desktop, Downloads) a un servidor externo vía PowerShell o curl. Archivos de contabilidad, contratos, datos de clientes — exfiltrados en segundos.

⏱ Tiempo de ejecución: variable según tamaño

## 05 — CÓMO PROTEGERTE CONTRA ATAQUES BADUSB

### Regla absoluta: ningún USB desconocido en tu computadora

El 48% de los USBs encontrados en estacionamientos de empresas son conectados por empleados curiosos. Un USB encontrado en el piso, recibido como "regalo" o dejado en sala de reuniones es una amenaza real. Sin excepciones: si no sabes de dónde viene, no lo conectas.

### Activa USB Guard o restricción de dispositivos HID

En Linux: USBGuard bloquea dispositivos USB no autorizados. En Windows Enterprise: Device Guard y políticas de grupo permiten whitelist de dispositivos USB aprobados. En macOS: Jamf y MDMs corporativos gestionan acceso por dispositivo.

### Bloquea tu computadora siempre que te alejes

El ataque BadUSB requiere acceso físico a tu computadora desbloqueada. Windows: Win+L, macOS: Ctrl+CMD+Q. Linux: Super+L. 3 segundos de descuido bastan para que el ataque comience y termine.

### Desactiva puertos USB no usados en BIOS

En entornos corporativos de alta seguridad, los puertos USB que no se necesitan pueden desactivarse desde BIOS/UEFI con contraseña. También existen bloqueadores físicos de puerto USB — tapones que requieren herramienta para removerse.

### Usa USB Data Blocker para cargar dispositivos

Los "USB Condoms" o Data Blockers bloquean los pines de datos (D+ y D-) del cable USB, permitiendo solo el paso de energía. Ideales para usar en puertos USB públicos de aeropuertos, cafés u hoteles.

// REALIDAD 2026

**Tu antivirus no puede detectar a un teclado escribiendo comandos. La defensa es física — no digital.**

Bloquea tu pantalla. No conectes USBs desconocidos. Siempre.