EVIL TOOL BadUSB

Un accesorio del lado del mal

Erick Olórtegui

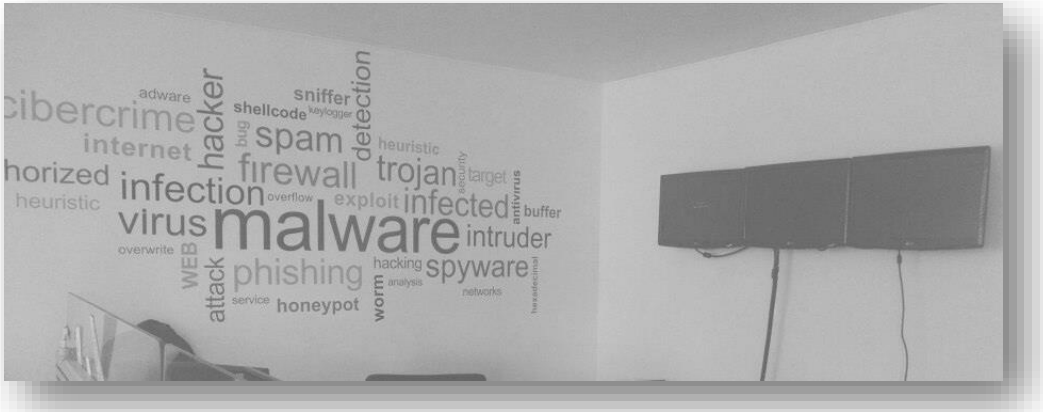
Analista de Malware

[erick.olortegui@securitylabs.pe]

#PERUHACK2017

#PERUHACK2017

- Especialista Ciberseguridad
- Implementación de Seguridad Perimetral
- Analista de malware en STARTLABS I Encargado de Laboratorio de Análisis de Malware en SECURITY LABS PERU
- Buscador de malware
- Speaker OWASP Latam Tour 2016
- Apasionado de la seguridad ofensiva
- Autodidacta.



#PERUHACK2017

./VIDEOS

¿Rubber Ducky?

USB RUBBER DUCKY DELUXE

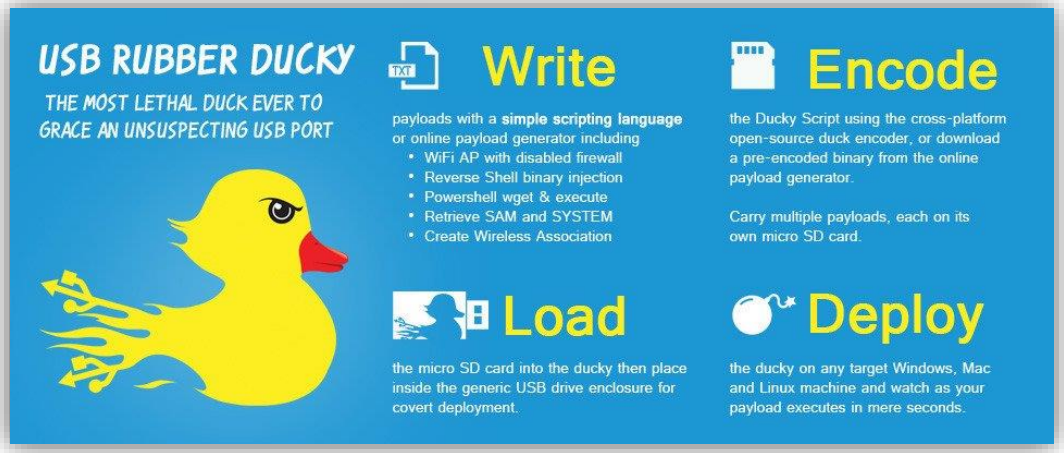
$44.99

Quantity

1 ADD TO CART

Tweet Share Pin It Add Email

Email



HAK5

PERUHACK2017

#PERUHACK2017

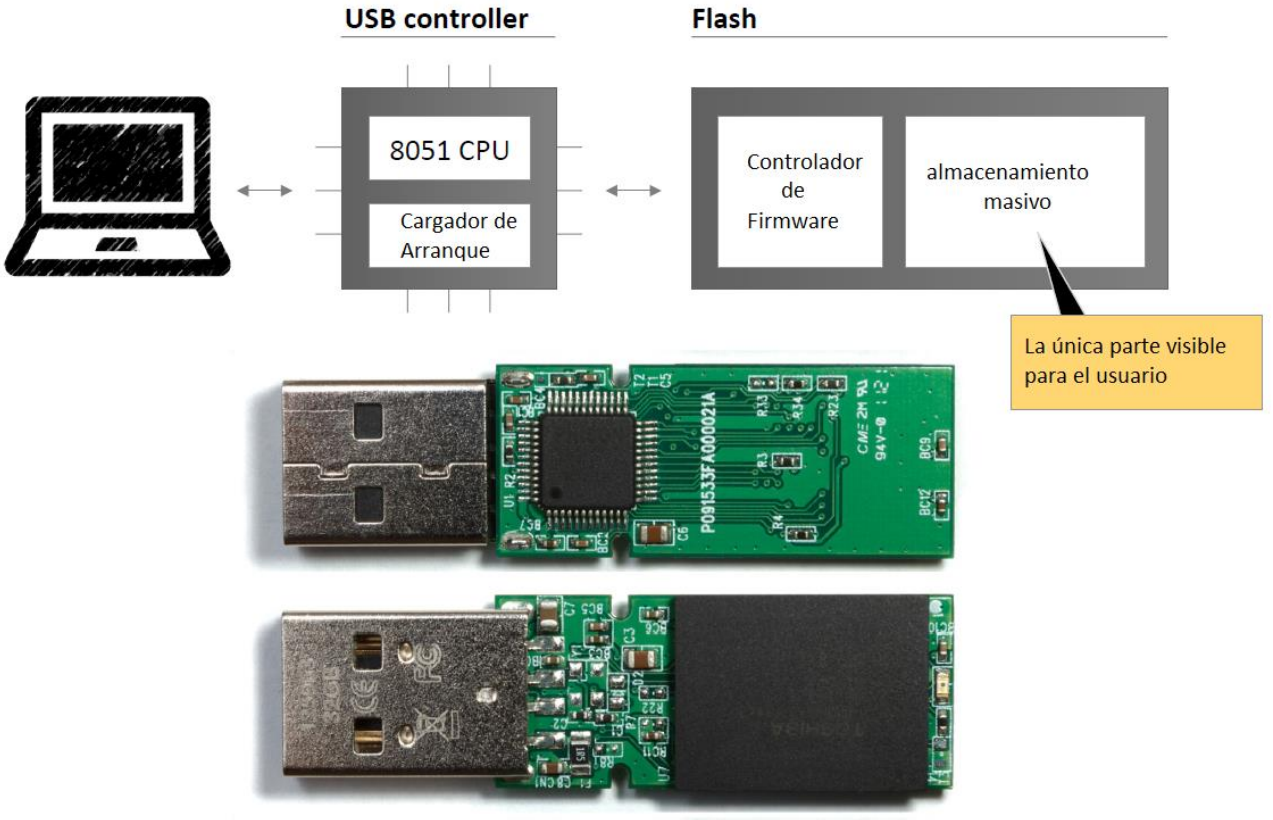
./DEMO1

AGENDA

- ¿Cómo Funciona el USB?
  - ✓ Funcionamiento
  - ✓ Proceso de Inicio
- BadUSB
  - ✓ Inicio
  - ✓ Escenario de ataques
  - ✓ ¿Una amenaza real?
- Conclusiones

¿Cómo Funciona el USB?

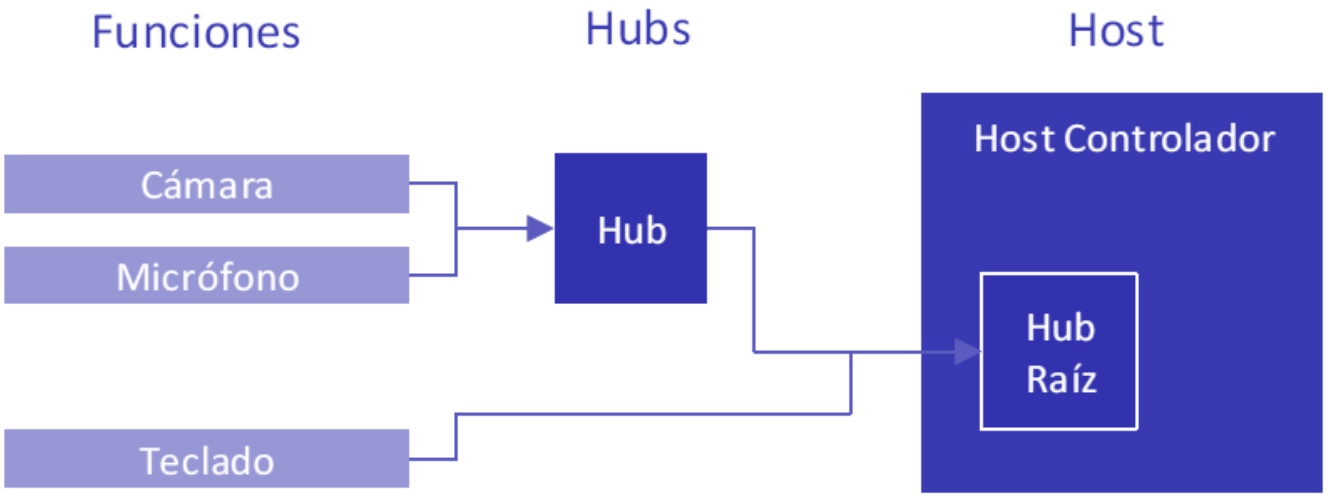
Funcionamiento



PERUHACK2017

#PERUHACK2017

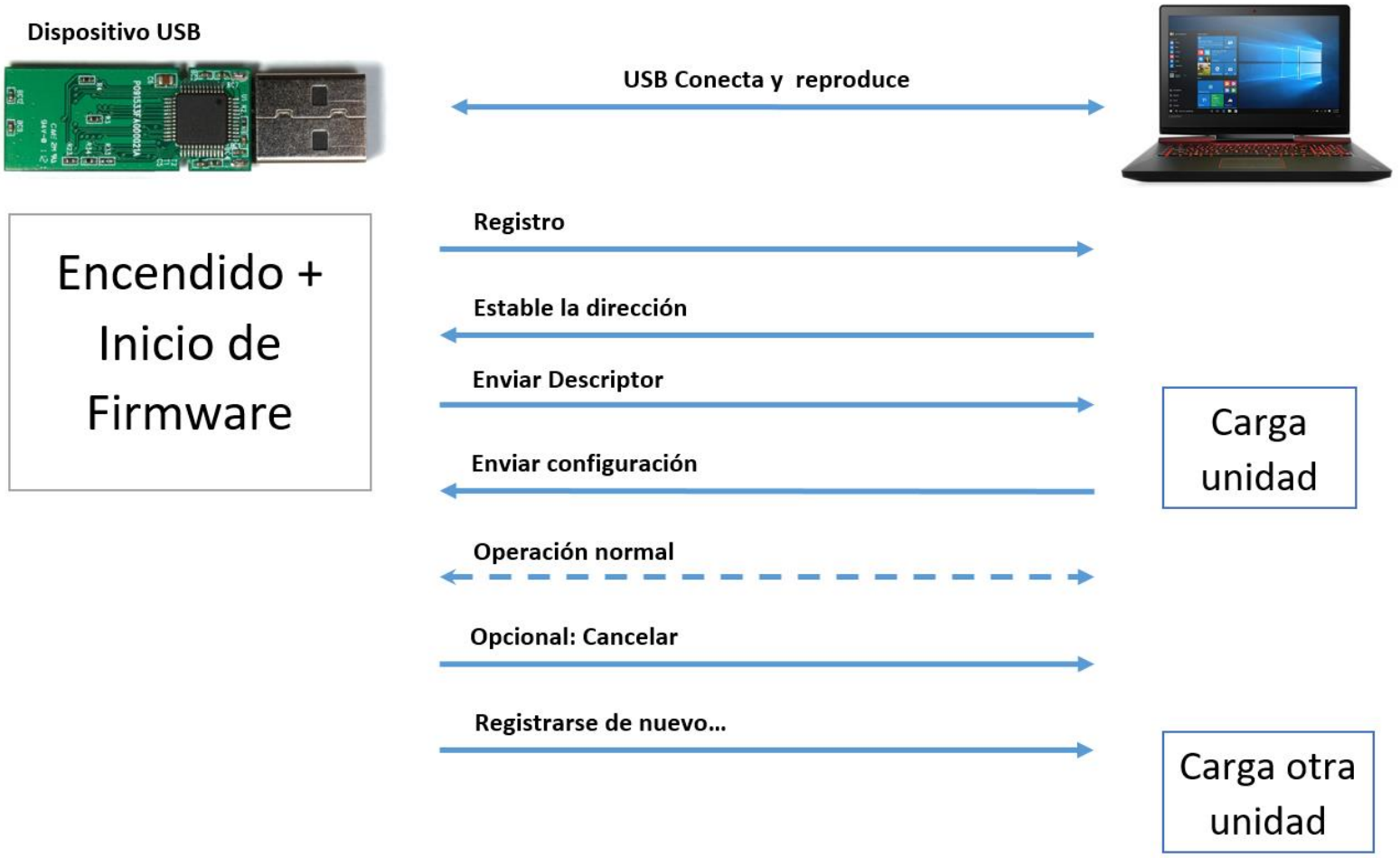
¿Cómo Funciona el USB?



Identificador	Webcam	Teclado
Descriptor de clase	0x01 - Audio Class 0x0E - Video Class	0x03 - HID Class / Human Interface Device Class
Endpoints	0 - Control 1 - Video 2 - Audio	0 - Control 1 - Transferencia de datos

¿Cómo Funciona el USB?

Proceso de inicio



BadUSB

Patriot 8GB Supersonic Xpress (with PS2251-03 (2303) controller)

Patriot 8GB Supersonic Xpress* (Almost all now are 2307 on Amazon [bought 9 from all 9 sellers])

Kingston DataTraveler 3.0 T111 8GB

Silicon power marvel M60 64GB

Patriot Stellar 64 Gb Phison

Toshiba TransMemory-MX USB 3.0 16GB (May ship with 2307)

Toshiba TransMemory-MX USB 3.0 8GB (May ship with 2307)

Kingston DataTraveler G4 64 GB

Patriot PSF16GXPUSB Supersonic Xpress 16GB

Silicon Power 32GB Blaze B30 (SP032GBUF3B30V1K) (May ship with 2307)

Kingston Digital 8GB USB 3.0 DataTraveler (DT100G3/8GB)* - Using PS2251-03 (By the way, the DriveCom.exe does not work for it, you need use Phison MPALL Tools to burn the firmware.)

Verbatim STORE N GO 32GB USB 3.0

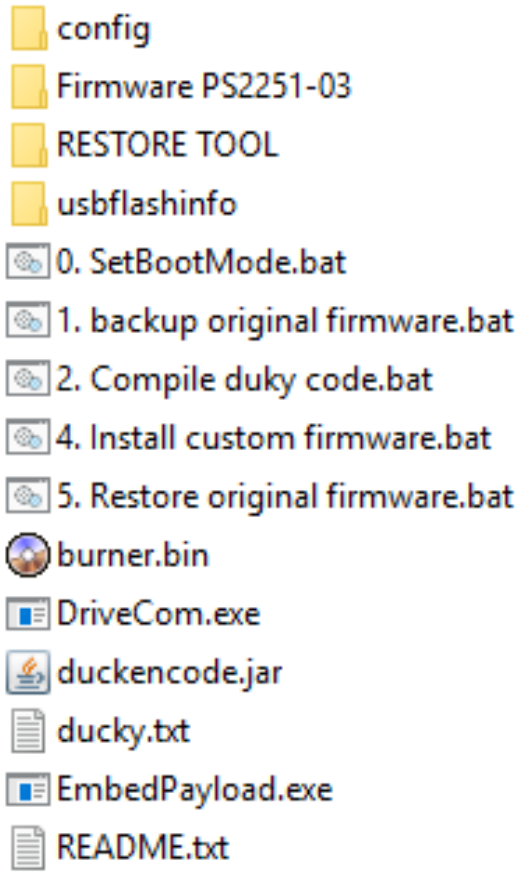
Verbatim STORE N GO V3 8GB USB 3.0 (May ship with 2307)

Phison 2251-03 (2303)
Custom Firmware

DriveCom	Add chip ID & num LBA retrieval commands
EmbedPayload	Adding all the stuffs
Injector	Adding all the stuffs
docs	Adding all the stuffs
firmware	Add chip ID & num LBA retrieval commands
patch	Add no-boot-mode patch
templates	Adding all the stuffs
tools	Force these tools added
.gitignore	Adding all the stuffs
LICENSE	Update LICENSE
README.md	Update README.md

https://github.com/brandonlw/Psychson

BadUSB




```
@echo off
set /p id="Enter your drive letter: "
DriveCom.exe /drive=%id% /action=SetBootMode
PAUSE
```

```
@echo off
set /p id="Enter your drive letter: "
DriveCom.exe /drive=%id% /action=SendExecutable
/burner=burner.bin
DriveCom.exe /drive=%id% /action=DumpFirmware
/burner=burner.bin /firmware=config/backup.bin
PAUSE
```

```
@echo off
java -jar duckencode.jar -i ducky.txt -o config/ducky.bin
DEL config\compiled.bin
COPY "config\original\cfw.bin" "config\compiled.bin"
EmbedPayload.exe config/ducky.bin config/compiled.bin
PAUSE
```

https://github.com/brandonlw/Psychson

#PERUHACK2017

DEMO

¿existe defensa efectiva de los ataques USB?

- Lista blanca de dispositivo USB
  - Los dispositivos USB no siempre tienen un número de serie único.
  - Los sistemas operativos no tienen (aún) mecanismos de listas blancas
- Bloquear dispositivos críticos / bloquear completamente USB
  - Obvio impacto en la usabilidad.
  - Conocer las clases de dispositivos que se utiliza para este tipo de ataque, No queda mucho de USB cuando estos están bloqueados
- Deshabilitar actualizaciones de firmware en hardware
  - Simple y efectivo

DATO ADICIONAL

- Los periféricos USB proporcionan un camino de infección versátil
- Una vez infectado - a través de USB o de otra manera - el malware puede utilizar periféricos como un escondite, dificultando la desinfección del sistema.
- Mientras los controladores USB sean re-programables, los periféricos USB no deben ser compartidos con otros


PERUHACK2017
HACKERS
FORMANDO
HACKERS
0x31322e3035 #