

/Rooted®



# Roapt evil mass storage & Tu-ya aqui?

David Reguera Garcia aka Dreg & Abel Valero Lozano aka SkUaTeR

2020



# David Reguera Garcia aka Dreg

- Senior malware researcher, C, C++, ASM, x86\_64, ARM Cortex & AVR-8-bit
- Contributing to rootkit unhooker, unhide, x64dbg, enyelkm, anticuckoo, dbgchild....
- <https://github.com/David-Reguera-Garcia-Dreg>
- <https://twitter.com/fr33project>
- <http://www.fr33project.org/>
- [dreg@fr33project.org](mailto:dreg@fr33project.org)

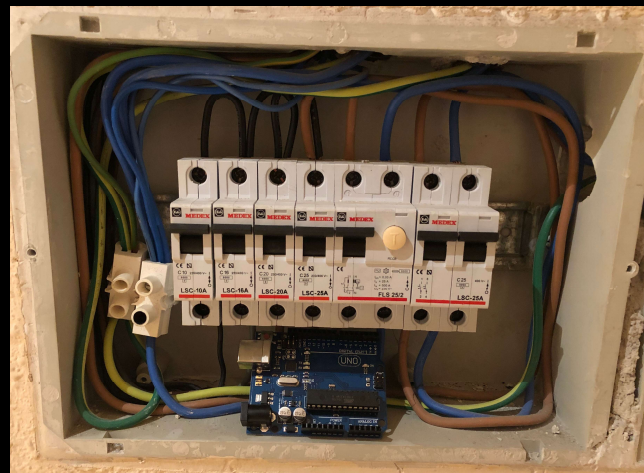


## evil mass storage – POC just for fun

- infect a target machine without NET & exfiltrate info
- hardware: at90usb1287 + atmega328p + ts3usb221 + mosfet + sd card reader (SPI) + rf 433MHz ASK ...
- multi-stage malware: only visible when connected to target
- exfiltrate info via two ways:
  - mass storage: crypt & hidden sectors
  - radio: rf 433MHz ASK
- firmware: keyboard + mass storage (USB composite device). LUFA + FatFs + Dreg adaptation “USB Mass storage SD card for Teensy2/ATMEGA32U4 by Mathieu Sonet”
- dynamic: serial, VID, PID, USB Descriptor, decrypt/delete sectors...

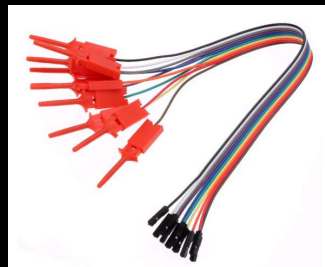
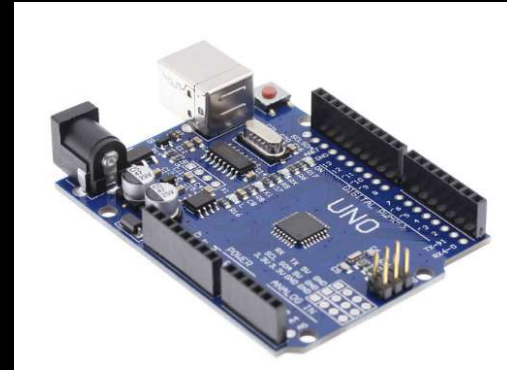
# external hardware - receiving data

- rf 433mhz receiver
- WIFI AP/STA
- SMS
- GSM/GPRS
- MICRO SD CARD



demo prototype

evil mass storage

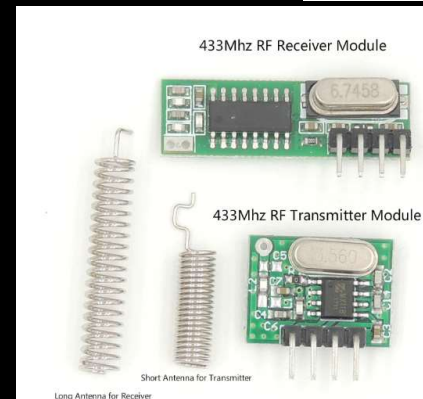
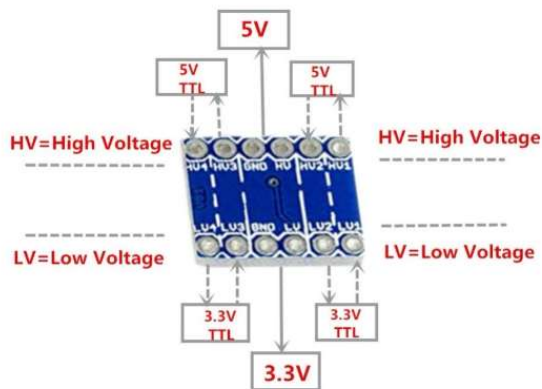
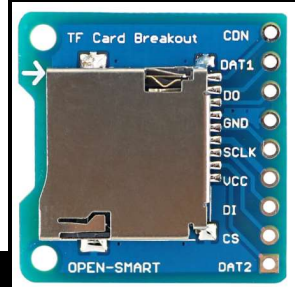


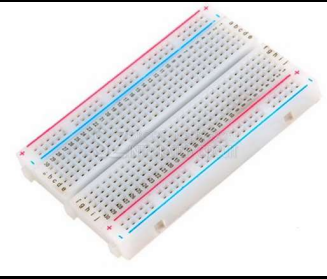
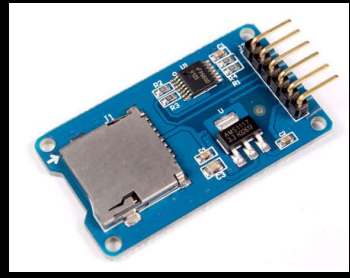
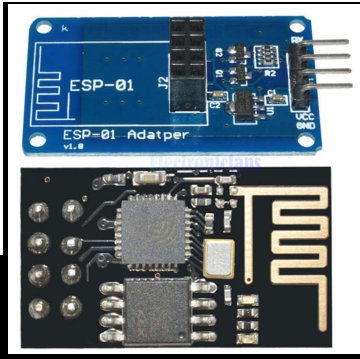
# AT90USBKEY

Part Number: AT90USBKEY2

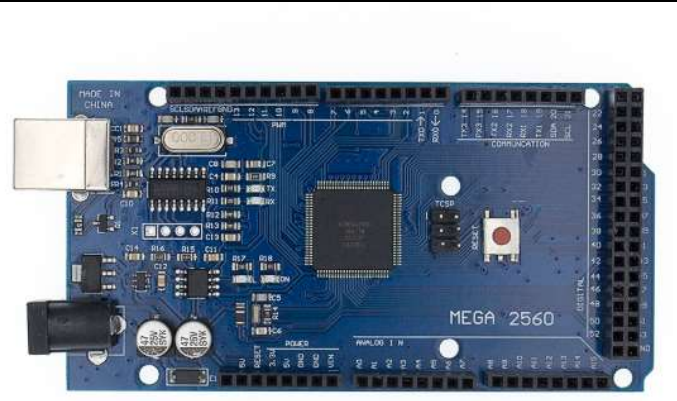
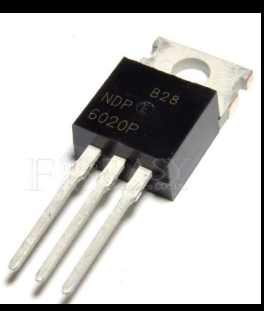


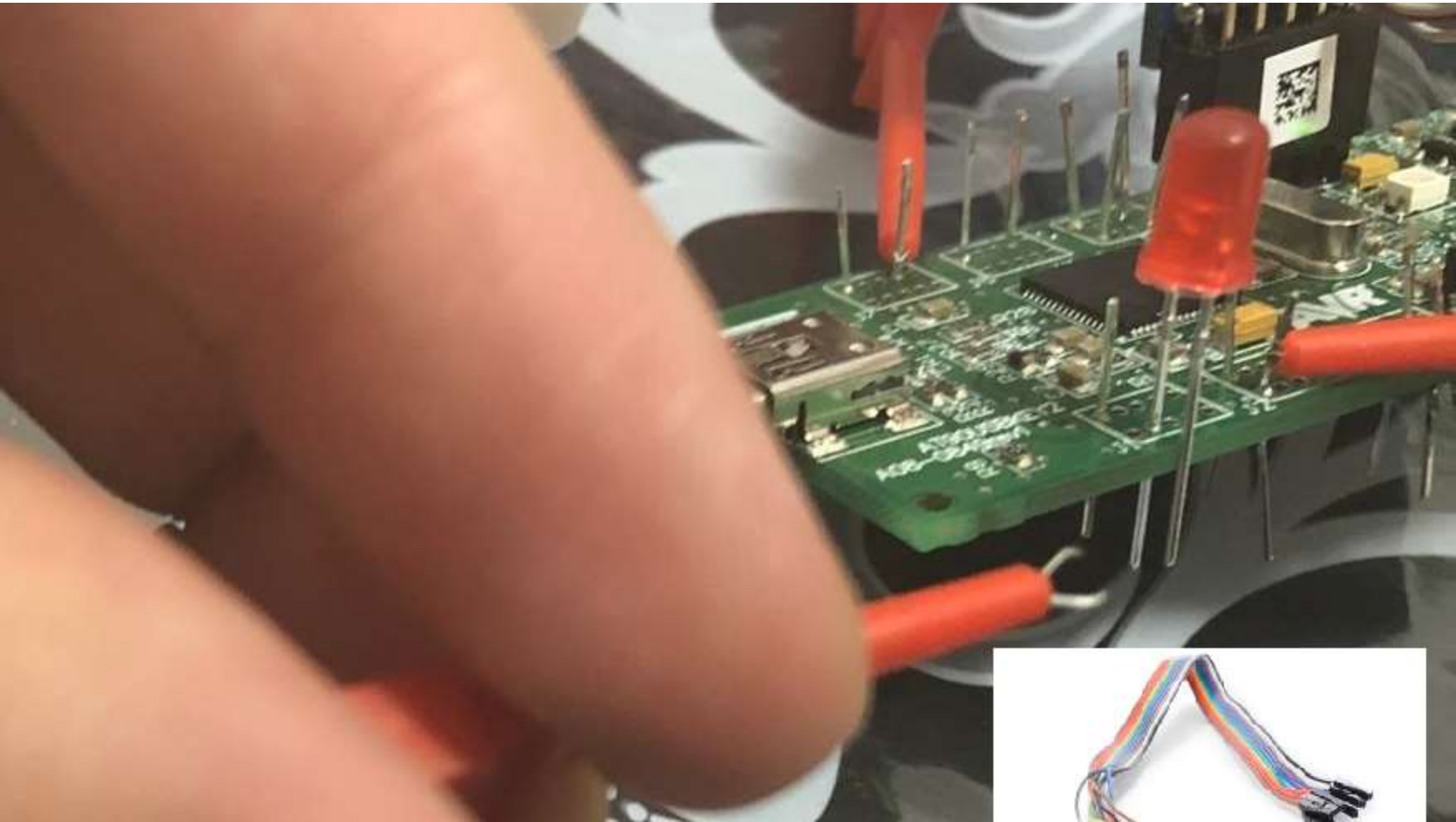
TS3USB221 DIY





Solder Iron Tip Cleaning Sponge Pad





# prototype shopping list 1

- mini soldering iron + iron tip
- arduino uno + cable
- arduino mega 2560 + cable
- USB 2.0 Type A 1-Male 1-Female to 5P Screw with/ Shield Terminal Plug Adapter Connector
- USB to DIP Type A 2-Female 1-Male USB Adapter Converter for 2.54mm PCB Board DIY
- ESP-01S ESP8266 Serial Wi-Fi Wireless Module + ESP-01 Adapter for Arduino (5v)
- 400 Tie Points Solderless PCB Breadboard Mini Universal Test Protoboard DIY Bread Board Bus (x2)

## prototype shopping list 2

- 4 Channel 5V 3.3V IIC UART SPI TTL Logic Level Converter level conversion module
- 10pcs High Efficiency Test Hook Clip Logic Analyzer Cable Gripper Probe Test Clamp Kit
- kit LEDs 5mm Red Blue Green Yellow White
- mosfet NDP6020P TO-220 NDP6020 TO220 6020P P-channel
- 433 Mhz RF Receiver and Transmitter Module. RX470-4, WL102-341, Short antenna for Transmitter. Long antenna for Receiver
- common values resistor Kit
- DIY TS3USB221 High-Speed USB 2.0 (480Mbps) 1:2 Multiplexer To Demultiplexer Switch With Single Enable Board Module

## prototype shopping list 3

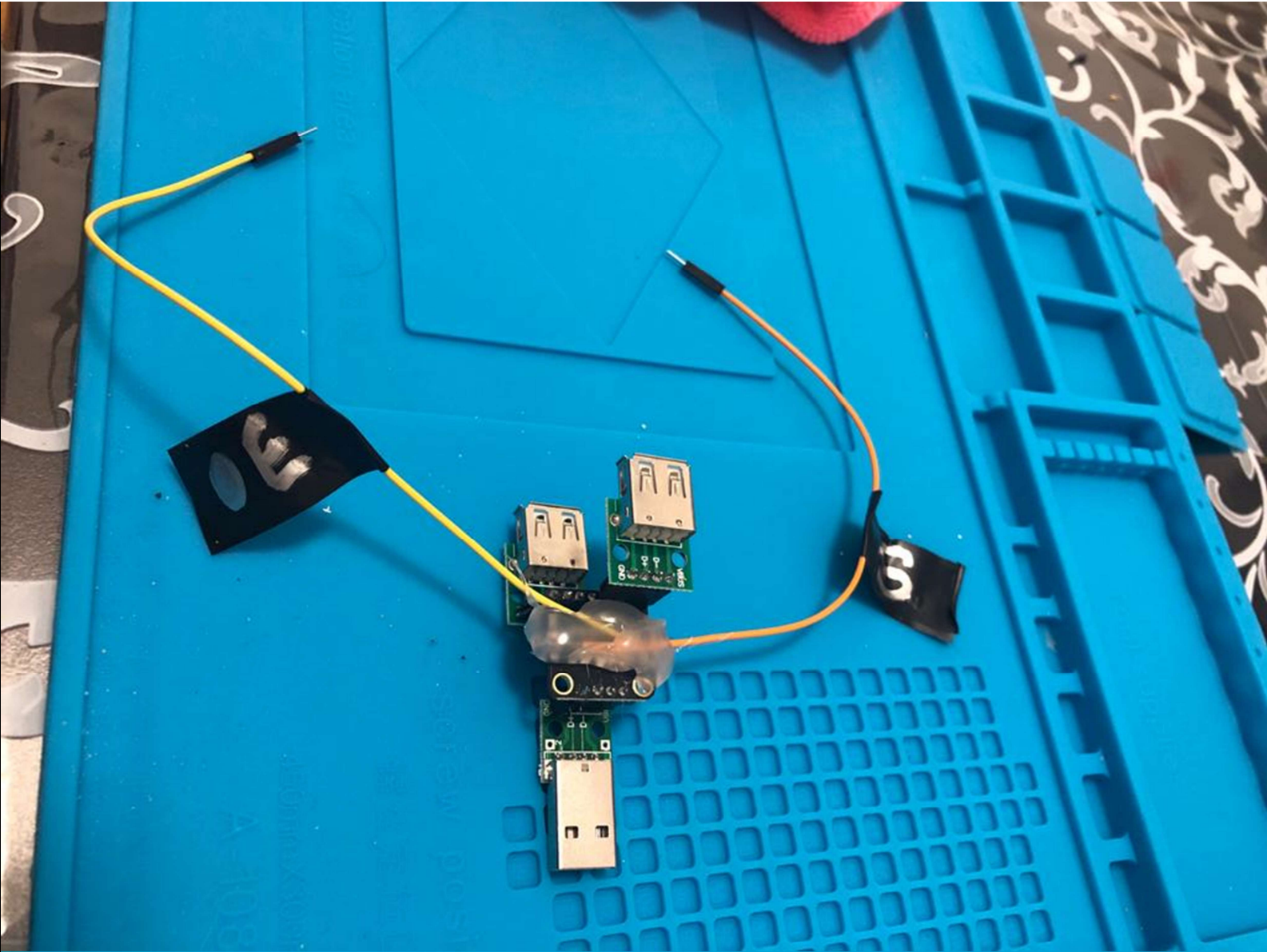
- Reader Adapter for Micro SD USB 2.0 TF M2 MMC MS PRO DUO Card Reader
- 2PCS 9V rechargeable battery large capacity 1000mAh lithium ion rechargeable battery + 1PCS smart 9 V charger
- 9V PP3 Battery Holder Box Case Wire Lead ON/OFF Switch Cover with DC 2.1mm Plug
- SanDisk micro SD card 16GB SDHC + adapter
- DC 9V1A 9V 1A Power Supply AC 100V-240V Converter Adapter Plug Charger 5.5mm x 2.1mm 1000mA
- SIM808 module GSM GPRS GPS Development Board IPX SMA with GPS Antenna

# prototype shopping list 4

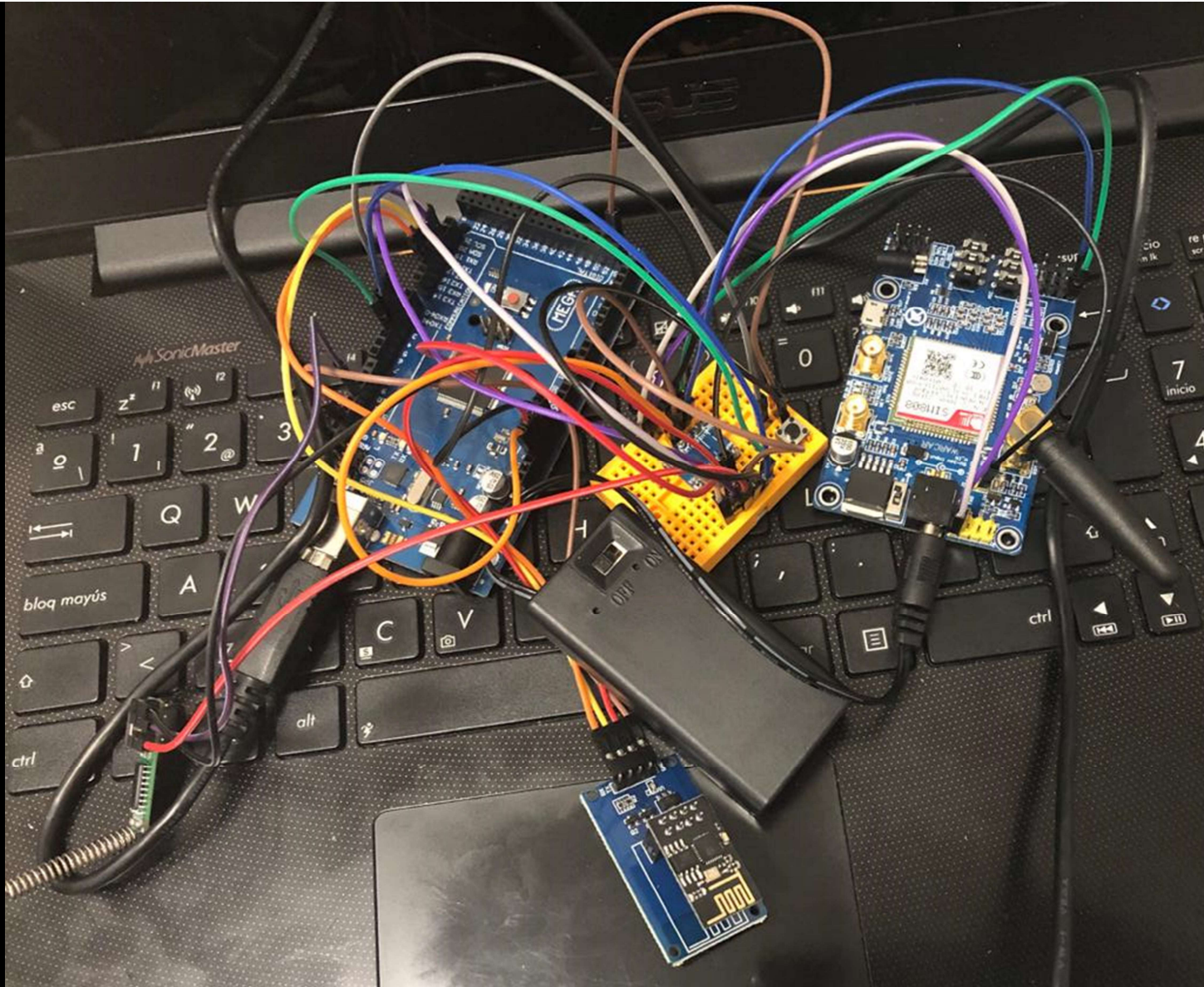
- Screw Kit Screw Driver
- Micro SD / TF Card Breakout to DIP Board Module (3.3v)
- Micro SD Module TF Micro SD Storage Board TF Card Memory Shield (5v)
- 120pcs 40PIN 20CM Dupont Line Male to Male, Female to Male, Female to Female Jumper Dupont Wire Cable
- AT90USBKEY2
- ATMEL ICE (ATATMEL-ICE)
- solder iron tip cleaning sponge pad
- Tin Lead Rosin Core Solder Wire

# prototype shopping list 5

- Hot Air Glue Gun Thermo Electric Heat Temperature
- Test hook clip, Grabber SMD IC Test Probe Hook for Multimeter, Logic analyzer...
- 20pcs 10 pairs 40 Pin 1x40 Single Row Male and Female 2.54 Breakable Pin Header PCB







## Roapt – my own pcb for attack



- soon available at [www.rootkit.es](http://www.rootkit.es)
- JTAG, ICSP, UART...
- current beta prototype 1.0

# SD card SDHC 16GB

- FAT16, Only 1 FAT TABLE. SPI is slow
- f.exe: malware crypted – multi-stage
- exfiltrate blocks crypted from .exe
- g: file for communication with firmware. firmware can encrypt/decrypt sectors, relocate writes & reads, reset USB connection (OS cache), change stages, delete all f.exe entries..
- special area is “protected”
- Its possible switch between special-normal
- normal area can be formatted

special mass storage  
2GB FAT16

- f.exe
- g

normal mass storage  
2GB FAT16

- f.exe
- g

f.exe  
stage1

f.exe  
stage2

...

exfiltrate area

# demo create & burn SD card image

# demo firmware: dev, debug & flash. Atmel studio 7

The screenshot displays the Atmel Studio 7 IDE interface. On the left, a C program is shown with the following code:

```
fr = f_open(&file1, "dreg_test.t\n\n\nif (fr == FR_OK)\n{\n    uart_puts("file open success\n\n\n    uart_puts("disk mounted and\n    f_write(&file1, line, strlen\n\n\n    if (fr == FR_OK)\n    {\n        uart_puts("file write su\n        f_close(&file1);\n    }\n    else\n    {\n
```

The central pane shows the hardware I/O registers:

Name	Address	Value	Bits
I/O Port (PORTA)	0x20	0x00	00000000
I/O Port (PORTB)	0x21	0x00	00000000
I/O Port (PORTC)	0x22	0x00	00000000
I/O Port (PORTD)	0x23	0x00	00000000
I/O Port (PORTE)	0x24	0x00	00000000
I/O Port (PORTF)	0x25	0x00	00000000
PINB	0x23	0xFD	11111000
DDRB	0x24	0x07	00000111
PORTB	0x25	0x07	00000111

The right pane shows the disassembly of the main function:

```
00002BA8 3d.4f          SBCI R19,0xFD      Sut\n00002BA9 ce.01          MOVW R24,R28      Cop\n00002BAA 84.54          SUBI R24,0x44      Sut\n00002BAB 9d.4f          SBCI R25,0xFD      Sut\n                                uart_puts("file write success\n\n\n00002BAC 04.da          RCALL PC-0x05FB   Loa\n00002BAD 80.ec          LDI R24,0xC0      Loa\n00002BAE 92.e0          LDI R25,0x02      Loa\n                                f_close(&file1);\n\n00002BAF 77.df          RCALL PC-0x0088   Coe\n00002BB0 ce.01          MOVW R24,R28      Cop\n00002BB1 84.54          SUBI R24,0x44      Sut\n00002BB2 9d.4f          SBCI R25,0xFD      Sut\n00002BB3 e6.dd          RCALL PC-0x0219   Loa\n                                uart_puts("file open error\n\n\n00002BB4 0b.c0          RJMP PC+0x000C   Loc\n00002BB5 86.ed          LDI R24,0xD6      Loa\n00002BB6 92.e0          LDI R25,0x02      Loa\n00002BB7 6f.df          RCALL PC-0x0090   Coe\n                                uart_puts("mount open\n\n\n
```

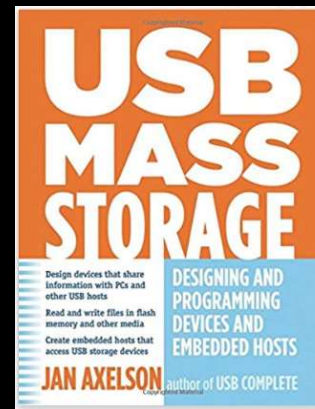
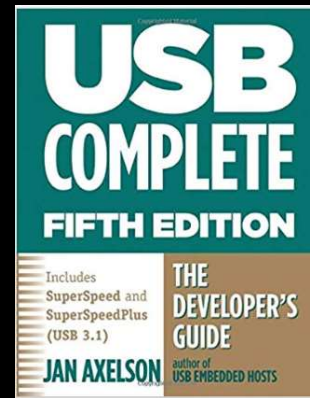
The terminal window shows the output of the program:

```
FatFs Module Test Monitor:\nsuccess\nfile open success\ndisk mounted and file opened\nFatFs Module Test Monitor:\nsuccess\nfile open success\ndisk mounted and file opened\nFatFs Module Test Monitor:\nsuccess\nfile open error\nFatFs Module Test Monitor:\nsuccess\nfile open error
```

The bottom pane shows the Locals window with the following variables:

Name	Value	Type
file1	{FIL[data]@0x20bc ([R28]+700)}	FIL[data]
obj	{FFOBJID[data]@0x20bc}	FFOBJID[...]
flag	0x4a	BYTE[dat]
err	0x00	BYTE[dat]
fptr	0x0000000000000011	FSIZE_t[c]
clust	0x0000000d	DWORD[...]
sect	0x000080b0	DWORD[...]
dir_sect	0x00008000	DWORD[...]

- USB Mass Storage: Designing and Programming Devices and Embedded Hosts
- USB Complete: The Developer's Guide (Complete Guides series)
- <https://www.microchip.com/DevelopmentTools/ProductDetails/PartNO/AT90USBKEY2>
- <https://www.microchip.com/wwwproducts/en/AT90USB1287>
- <https://www.avrfreaks.net/>
- [http://elm-chan.org/fsw/ff/ooindex\\_e.html](http://elm-chan.org/fsw/ff/ooindex_e.html)
- <http://www.fourwalledcubicle.com/LUFA.php>



# TO-DO

- improve source code: leaks, overflows, crap code...
- improve performance: fatfs, ISRs...
- more firmware & examples: SharpLocker/LockScream...
- more doc
- OS X & Linux examples
- more keyboard langs (current English)
- support multi-file (current POC is limited)
- exf mode selection: 433MHz(slow) or mass storage(faster)

# Future (maybe)

- ARM Cortex-M4 180MHz 32 bit + rf transceiver
- NXP Kinetis MK66FN2MoVMD18 or MK66FX1MoVMD18
- native 4bit-SDIO micro sd card port (SPI is very slow)
- cryptographic acceleration unit (AES) & CRC
- random number generator
- <https://www.pjrc.com/store/teensy36.html>
- NXP Kinetis FRDM-K66F board
- <https://www.utasker.com/kinetis/FRDM-K66F.html>

## Greetz & credits

- janio IRC-HISPANO
- Sergio Lara & Luis Fernando Regel – Panda
- Jose Vicente Martínez – electronic engineering
- Paul Stoffregen - pjrc, teensy, altsoftserial...
- Mathieu Sonet: mass storage SD for Teensy2/ATMEGA32U4
- Dean Camera: lufa
- ChaN: fatfs
- Yassin Said Esteller

**avrfreaks.net**

Thx!

/Rooted<sup>®</sup>



Questions?

evil mass storage in my github

- <https://www.rootkit.es>
- <https://github.com/David-Reguera-Garcia-Dreg>
- <https://twitter.com/fr33project>
- <http://www.fr33project.org/>
- [dreg@fr33project.org](mailto:dreg@fr33project.org)

