Bad USB

written by Mert SARICA | 3 November 2014 Every year, in August, at the end of the traditional Black Hat Cybersecurity Conference held in Las Vegas, USA, two researchers, Karsten NOHL and Jakob LELL, signed a striking presentation called BadUSB.

In this presentation, in short, it was provided that the hardware software (firmware) used by the microcontroller in USB can work in a different way than expected by patching it. For this, the researchers first obtained the hardware software used by the microcontroller, then using Wireshark, they detected the commands used during the hardware software update. Then, within a period of less than 2 months, they analyzed the hardware software using reverse engineering, loaded their own commands into the unused areas of the original hardware software, and thus created a new hardware software, and loaded it onto the USB memory, and completed the process. After this, the USB memory connected to the target system could interact with the system by running the commands that the user had loaded into the memory with the hardware software.

What is the difference between BadUSB and other tools like Teensy or USB Rubber Ducky that also allow command execution when connected to the target system via USB? In practice, there is not much difference. In social engineering tests carried out with BadUSB, it may be possible that the chance of being caught/detected is somewhat lower both system-wise and visually compared to others. In terms of cost, you can see that it is possible to make BadUSB for cheaper than a 20\$ Teensy or a 40\$ Rubber Ducky.

If you visit the website of the researchers who work on BadUSB, you can see that they have not published the POC (proof-of-concept) codes for this study. There is no need for those who, like me, want to create a BadUSB to be disappointed because two security researchers, Adam Caudill and Brandon Wilson, also made a similar study and presented it at the DerbyCon Information Security Conference at the end of September, and also uploaded the tools they developed during the research to GitHub along with the source codes.

After looking at the presentation file and codes, I also got to work creating a BadUSB. I ordered a Patriot Xpress model USB memory with a Phison microcontroller, which researchers use, from Amazon because it was not available in Turkey.

If you look at the presentation file, you will see that researchers are working on the Phison PS2251-03 model, so the USB memory that will be used for the tool they developed must have this model microcontroller in order for it to function.

After the USB memory arrived, I checked the model using the GetInfo tool (or you can use Chip Easy tool as well), and I was disappointed to find that the model was different. So this time, I set out to hunt for a Phison brand PS2251-03 model USB memory.

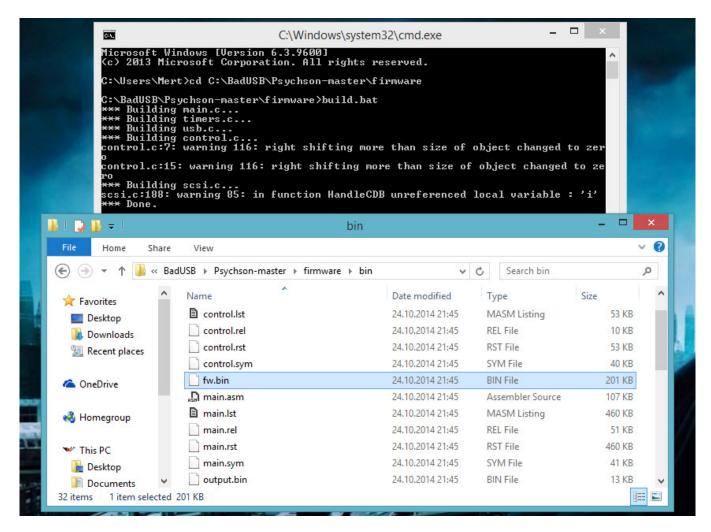


GetInfo V3.10.4.2	Load I Other	File			Read		
Customize Info.).			
VID 13FE	PID	5000	ICVersion	2251-01	Mode	3	
HID VID N/A	HID PID	N/A	FwVerion	01.09.10	FW Date	2012-02-13	
String Manufacture Name			AES	N/A	MAX_NOA		
String Product Name	Patriot Memo	ry	IEEE 1667	Disable 🗸 🗸	DVD+RW	Disable	V
Inquiry Manufacture Name			FC1 - FC2	FF - 01	Sample Lock	No	~
Inquiry Product Name	Patriot Memo	ry	USB Port	2.0]		
Inquiry Revision	PMAP		7				
Smart Card Info.			Flash Info. – Flash Vendor	T 1.1		LUL O	_
CCID VID N/A	CCID PID	N/A			Flash Type	MLC	
CCID Interface String			Flash ID	98 c7 94 32 76	55 Ud UU		
Interface			Production Ir		_		
			MP Ver.	MPALL v3.60.00			
			Production D	ate & Time 20	12-3-24	8:54	
			Serial Numbe	r 07072388B6D	76E35		

Like me, many users around the world set out to hunt for USB memories and provide feedback to researchers, so the researchers decided to compile a list of USB memories that have the potential to be BadUSBs. While checking this list from time to time, I decided to buy Sandisk Ultra 16 GB USB memory (SDCZ48-016G-U46) that I saw by chance while browsing at Teknosa (24 TL) and check its model. With great enthusiasm, I opened the package and, after checking it with the GetInfo tool, I saw that it was Phison's model, the supported model PS2251-03, so I proceed with the BadUSB creation steps on the GitHub page.

Č.		USB 30 Flash Drive S 20 mines faster than Sance f	Up to x tim USB 2.0 dr	Flash Drive Thes faster than			
GetInfo V3.10.1.2 C:\D					Disk.enc)(=
formation Partition setting	Other		nware Info.				
		581 ICV	ersion	2251-03	Mode	3	
Customize Info. VID 0781 HID VID N/A	PID 5	581 ICV	ersion (Verion (2251-03 01.08.53	FW Date	3 2013-07-16	
Customize Info. VID 0781	PID 5	581 ICV I/A FW AES	ersion [Verion [6 [2251-03	FW Date	2013-07-16	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name	PID 5 HID PID N	581 ICV 1/A PW AES	ersion (Verion (6 [E 1667 [2251-03 01.08.53 N/A Disable	FW Date MAX_NOA VD+RW	2013-07-16 Disable	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Manufacture Name	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk	581 ICV I/A Fw AES IEE IEE FC1	ersion (Verion (6 1 E 1667 (- FC2 (2251-03 01.08.53 N/A Disable FF - 01	FW Date	2013-07-16 Disable	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Product Name	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk SanDisk Ultra	581 ICV I/A Fw AES IEE IEE FC1	ersion (Verion (6 1 E 1667 (- FC2 (2251-03 01.08.53 N/A Disable	FW Date MAX_NOA VD+RW	2013-07-16 Disable	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Manufacture Name Inquiry Product Name Inquiry Revision	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk	581 ICV I/A FW AES IEE FC1 USI	ersion (Verion (6 1 E 1667 (- FC2 (2251-03 01.08.53 N/A Disable FF - 01	FW Date MAX_NOA VD+RW	2013-07-16 Disable	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Manufacture Name Inquiry Product Name Inquiry Revision Smart Card Info.	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk Ultra PMAP	581 ICV 1/A PW AES IEE FC1 USI	ersion (Verion (E 1667 [- FC2] B Port [2251-03 01.08.53 N/A Disable FF - 01	FW Date MAX_NOA VD+RW	2013-07-16 Disable	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Manufacture Name Inquiry Product Name Inquiry Revision Smart Card Info. CCID VID N/A	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk Ultra PMAP	581 ICV 1/A FW AES IEE FC1 USI Fla Fla	ersion (Verion (5 1 E 1667 (1 - FC2 (8 Port (5)	2251-03 D1.08.53 N/A Disable FF - 01 2.0	FW Date MAX_NOA DVD+RW Sample Lock	2013-07-16 Disable	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Manufacture Name Inquiry Product Name Inquiry Revision Smart Card Info. CCID VID N/A CCID Interface String	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk Ultra PMAP	581 ICV I/A FW AES IEE FC1 USI Flat I/A Flat Flat Flat	ersion (Verion (E 1667 (- FC2 (B Port (sh Info. sh Info.	2251-03 D1.08.53 V/A Disable FF - 01 2.0 SanDisk 45 4c a8 92 7	FW Date MAX_NOA DVD+RW Sample Lock	2013-07-16 Disable	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Manufacture Name Inquiry Product Name Inquiry Revision Smart Card Info. CCID VID N/A	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk Ultra PMAP	581 ICV 1/A FW 1/A FW AES IEE FC1 USI Fla I/A Fla Pro	ersion (Verion (E 1667 (E 1667 (E 1667 (B Port (Sh Info. Sh Info. Sh Info.	2251-03 D1.08.53 V/A Disable FF - 01 2.0 SanDisk 45 4c a8 92 7 0.	FW Date MAX_NOA DVD+RW Sample Lock	2013-07-16	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Manufacture Name Inquiry Product Name Inquiry Revision Smart Card Info. CCID VID N/A CCID Interface String	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk Ultra PMAP	581 ICV I/A FW AES IEE FC1 USI I/A Flas I/A Flas I/A Pro MP	ersion (Verion (E 1667 (E 1667 (E 1667 (B Port (Sh Info. Sh Info. Sh Info.	2251-03 D1.08.53 V/A Disable FF - 01 2.0 SanDisk 45 4c a8 92 7 0. MPALL v3.70.0	FW Date MAX_NOA DVD+RW Sample Lock	2013-07-16 Disable	
Customize Info. VID 0781 HID VID N/A String Manufacture Name String Product Name Inquiry Manufacture Name Inquiry Product Name Inquiry Revision Smart Card Info. CCID VID N/A CCID Interface String	PID 5 HID PID N SanDisk SanDisk Ultra SanDisk Ultra PMAP	ICV I/A FW AES IEE FC1 USI I/A Flac Flac Flac Flac Flac Flac Flac Flac	ersion (Verion (5 [E 1667 [I - FC2 [B Port (sh Info. sh Vendor sh ID ver. [2251-03 D1.08.53 V/A Disable FF - 01 2.0 SanDisk 45 4c a8 92 7 0. MPALL v3.70.0	FW Date MAX_NOA DVD+RW Sample Lock Flash Type 76 57 0b 00 E 2013-11-13	2013-07-16	

Unfortunately due to a mistake in one of the steps, I had to throw away this disk I bought. Afterwards, I bought two more Sandisk Ultra, and again due to a mistake, I had to throw away one of the disks. I decided to proceed carefully with the BadUSB creation steps. After compiling the hardware software, when it came to creating a set of commands in Ruby Ducky format, I used Duckencoder tool to create a simple command set of run -> notepad -> Mert SARICA. (I followed the instructions in the Running Demo 1 (HID Payload) section in the ReadMe file.)



	key.txt - Notepad	- • ×
File Edit Format View Help DELAY 3000 GUI r DELAY 500 STRING notepad DELAY 500 ENTER DELAY 750 STRING Mert SARICA ENTER		^
	C:\Windows\system32\cmd.exe	- 🗆 🗙
C:\BadUSB\DuckEncoder_2.6.3 o inject.bin Hak5 Duck Encoder 2.6.3	3∖DuckEncoder_2_6_3>java -jar encoder.	jar -i key.txt -
Loading File Loading Keyboard File Loading Language File Loading DuckyScript DuckyScript Complete	E OK J E OK J E OK J E OK J E OK J	
C:\BadUSB\DuckEncoder_2.6.3	NDuckEncoder_2_6_3>_	

Finally, after successfully passing all the steps below, I was able to create a BadUSB :) Unfortunately, with Sandisk's Ultra model, there is only one chance to update the hardware software, so it's a one-shot deal for now, but work is ongoing in this area, so it may be useful to have one of these brand models USB on hand for use in social engineering tests.

C:\Windows\system32\cmd.exe ×
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=SetBootMode Action specified: SetBootMode
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=SendExecutable /bu rner=BN03U104M.BIN Action specified: SendExecutable
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=DumpFirmware /firm ware=dump.bin Action specified: DumpFirmware
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=GetInfo Action specified: GetInfo Gathering information Reported chip type: 2302 Reported chip ID: 45-4C-A8-92-76-57 Reported firmware version: 1.01.10 Mode: Burner
C:\BadUSB\Psychson-master\tools>EmbedPayload.exe inject.bin fw.bin File updated.
C:\BadUSB\Psychson-master\tools>DriveCom.exe /drive=F /action=SendFirmware /burn er=BN03U104M.BIN /firmware=fw.bin Action specified: SendFirmware Gathering information Reported chip type: 2302 Reported chip ID: 45-4C-A8-92-76-57 Reported firmware version: 1.01.10 Mode: Burner Rebooting Sending firmware Executing Mode: Firmware

If you were to ask what measures can be taken against BadUSBs as an organization, you can ban the use of USBs across the organization. If this is not possible, you can choose to use products like IronKey, which have signature control against hardware software updates, across the organization. Additionally, training employees on identifying suspicious USBs and not to use unknown or non-authorized USBs can also help in preventing badUSB attacks.

Hope to see you in the following articles.

Note: You can watch the video I prepared about the USB that has been converted to BadUSB from the link below.