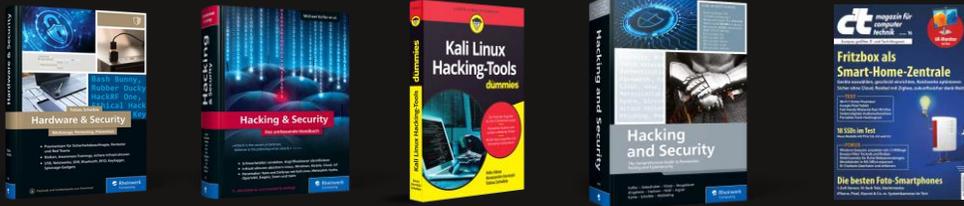


Über mich

- 1999 GeoCities, 2000 Domain, 2001 Kundenprojekte & ab 2010 eigener Blog
- 2009 bis 2012: Softwareingenieur im Bereich Web Development
- 2012 bis 2023: Akademischer Mitarbeiter an der Hochschule Albstadt-Sigmaringen
- Seit 2023: Dozent an der HfPolBW
- Autor, Blogger, Referent & Dozent



Agenda

- 01. Gezielte Angriffe vor Ort
- 02. Bandbreite der Tools
- 04. Gegenmaßnahmen

A blurred background image showing a person sitting at a desk with a computer monitor. The person is in profile, facing left, and appears to be looking at the screen. The image is out of focus, with a soft, greyish-blue color palette. A solid orange horizontal line is positioned below the text.

Gezielte Angriffe vor Ort

Angriffsszenario



ehemaliges oder
frustriertes Personal



Personal von
Drittfirmen



Praktikant*
innen



„falsche“
Kunden

Angreifer
Innentäter



Kamera /
Mikrofon



Keylogger /
BadUSB



Opfer



WLAN /
LAN

Pentest- & Hacking-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.

- Die Geräte wurden für White Hat Hacker, Penetration-Tester, Security-Forscher und Sicherheitsbeauftragte entwickelt, um Schwachstellen aufzuspüren und anschließend schließen zu können.
- Die Tools 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

Gadgets & Logger

Spionage-Gadgets

Keylogger

Screenlogger

BadUSB & Killer

BadUSB

USB-Killer

LAN & WLAN

LAN

WLAN

Bluetooth & RFID

Bluetooth

RFID

SDR & Funk

Software Defined Radio

Funkprotokolle

Multitools

Fertige Lösungen

Flexible Lösungen

Bandbreite der Tools

Spionage-Gadgets

Spionage-Gadgets interagieren nicht mit einem Rechnersystem, sondern werden eingesetzt, um heimlich z.B. sicherheitskritische Informationen zu entwenden. Sie werden zum Beispiel in einer Vorstufe eines Angriffs eingesetzt, um Zugangsdaten auszuspähen.

- Angreifer können ein Opfer gezielt ausspionieren
- Es gibt eine große Bandbreite von verschiedenen Tools
- Tools werden unbemerkt platziert und später wieder abgeholt
- Es können Video- und Audioaufzeichnungen angefertigt werden

Mini-Aufnahmegerät



GSM-Aufnahmegerät



Spionagekamera



GPS-Tracker



Key- & Screen-Logger

Ein Keylogger wird von Angreifern verwendet, um jeden Tastendruck, der auf einer externen Tastatur eines Computers eingegeben wird, aufzuzeichnen. Screenlogger zeichnen heimlich Monitorsignale auf.

- Keylogger zeichnen die Tastatureingaben direkt nach dem Start auf
- Bei Varianten mit WLAN - Verbindung kann der Angreifer diese aus der Entfernung abfragen
- Intelligente Keylogger können auf Eingaben mit Änderungen reagieren
- Screenlogger werden zwischen Rechner und Bildschirm angeschlossen
- Screenlogger zeichnen den Bildschirminhalt als Screenshots oder Video auf

USB-Keylogger



WLAN-Keylogger



Keylogger-Kabel



Key Croc Keylogger



VideoGhost



Screen Grab



PRAXIS Realer Vorfall - Keylogger

Keylogger-Affäre in der taz

Dateiname LOG.TXT

Anfang 2015 kam heraus, dass Computer in der taz mehr als ein Jahr lang ausgespäht wurden. Die Recherche zum Fall führt bis nach Asien.



Der Keylogger wurde inzwischen an die Polizei übergeben

Foto: taz

Ein Editorial der taz zu dieser Recherche [findet sich hier](#).

Es ist wohl reiner Zufall, dass der Keylogger am Ende entdeckt wird. Mindestens ein Jahr lang ist er zuvor im Einsatz. Er wandert von Computer zu Computer, im ersten, dritten und vierten Stock der Rudi-Dutschke-Str. 23 und schneidet dort die Tastaturanschlüsse mit, Passwörter, Mails, Kontodaten. Das geht so lange, bis am Nachmittag des 17. Februar 2015, ein Dienstag, die Computertastatur einer Praktikantin nicht mehr funktioniert.

SCHWERPUNKT ÜBERWACHUNG



Gesellschaft / Medien 4. 6. 2016

MARTIN KAUL

Reporter



SEBASTIAN ERB

Reporter



THEMEN

#Keylogger

Quelle: [taz.de](#) (1)

PRAXIS Realer Vorfall - Keylogger



NETZPOLITIK

Über 90 Noten manipuliert: Student droht jahrzehntelange Haftstrafe

Vorfall an University of Iowa – Hatte sich mit Keylogger die Logindaten von Professoren verschafft

7. November 2017, 10:31

An der University of Iowa ist ein besonders eklatanter Fall von akademischer Manipulation bekannt geworden. Einem Studenten werden gleich mehrere Vergehen zur Last gelegt, die er gemeinsam mit Kommilitonen begangen haben soll, berichtet die [New York Times](#).

Über 90 Mal soll er zwischen März 2015 und Dezember 2016 nachträglich seine eigenen Noten zum Besseren verändert haben, ehe der Betrug aufflog. Dazu soll er auch die Zeugnisse von mindestens fünf anderen Personen manipuliert und sich vorab Zugriff auf Prüfungsfragen verschafft haben, die er auch weitergegeben haben soll.

Logindaten per Keylogger ausgespäht

Ausgangspunkt dafür war ein einfach gestrickter, digitaler Einbruch. Es wurde keine Sicherheitslücke ausgenutzt, sondern es kamen USB-Keylogger zum Einsatz, die an Rechner der Universität angeschlossen wurden. Die Kommilitonen, die mit dem Beschuldigten kooperierten, stellten sicher, dass die Professoren diese PCs auch verwendeten.



Mit den ausgespähten Logindaten wurden Noten manipuliert und Prüfungsinhalte vorab eingesehen.

Foto: [derStandard.at/Pichler](#)

Quelle: [derstandard.at](#) (2)

PRAXIS Realer Vorfall - Keylogger



The image shows a screenshot of a news article from the website 'TAGESSPIEGEL'. The article title is 'Update / IT-Sicherheit Berliner Polizei entdeckt Datenleck'. The main image is a close-up of a police officer's uniform sleeve with a 'POLIZEI' patch. The article text states: 'An einem Dienstcomputer wurde ein Keylogger gefunden. Daten seien aber nicht abgefangen worden, so die Polizei. Dabei soll das Gerät nur Zugangsdaten speichern.' The source is cited as 'Quelle: tagesspiegel.de (3)'.

TAGESSPIEGEL Anmelden ABO

Politik Internationales Berlin Gesellschaft Wirtschaft Kultur Wissen Gesundheit Sport Meinu >

Bezirke Berliner Wirtschaft Polizei & Justiz Stadtleben Fahrrad & Verkehr Schule Nachrufe Checkpoint

Berlin IT-Sicherheit: Berliner Polizei entdeckt Datenleck

Update / IT-Sicherheit Berliner Polizei entdeckt Datenleck

An einem Dienstcomputer wurde ein Keylogger gefunden. Daten seien aber nicht abgefangen worden, so die Polizei. Dabei soll das Gerät nur Zugangsdaten speichern.

Quelle: [tagesspiegel.de](https://www.tagesspiegel.de) (3)

BadUSB-Tools & USB-Killer

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

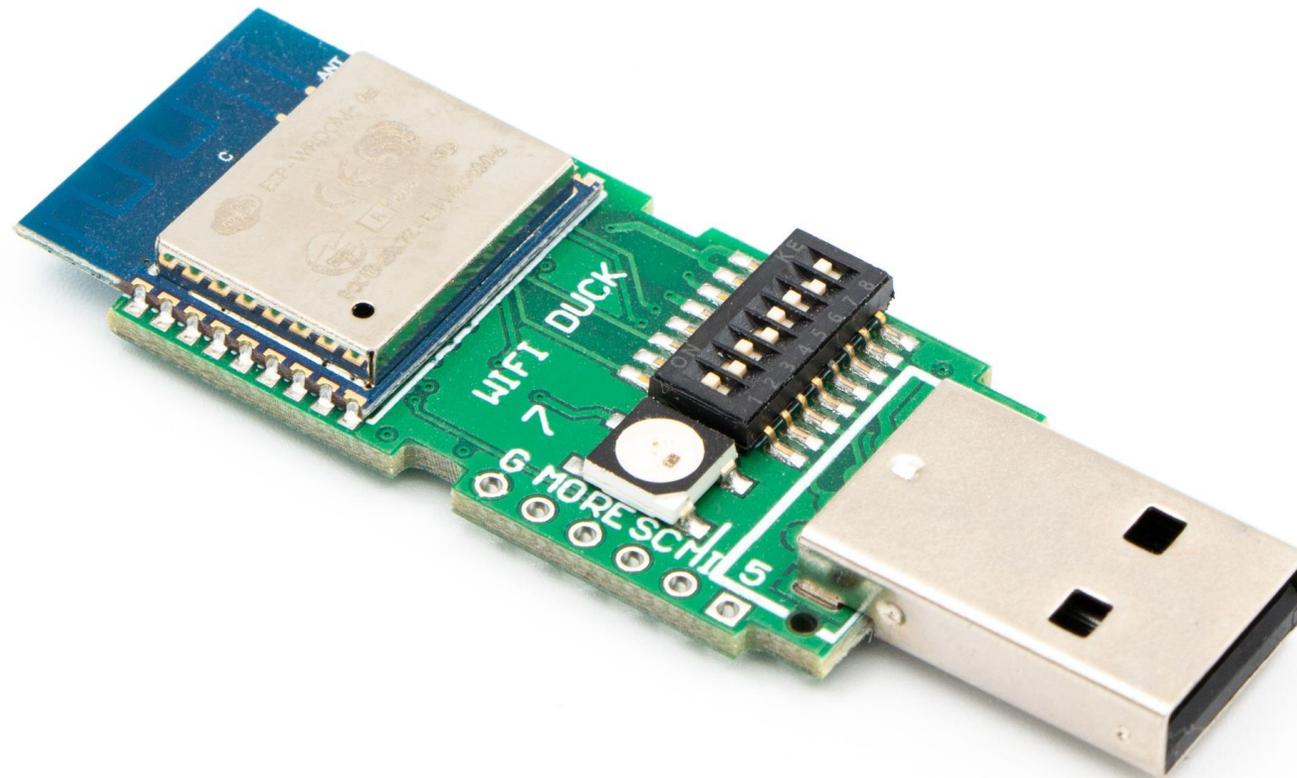
Rubber Ducky



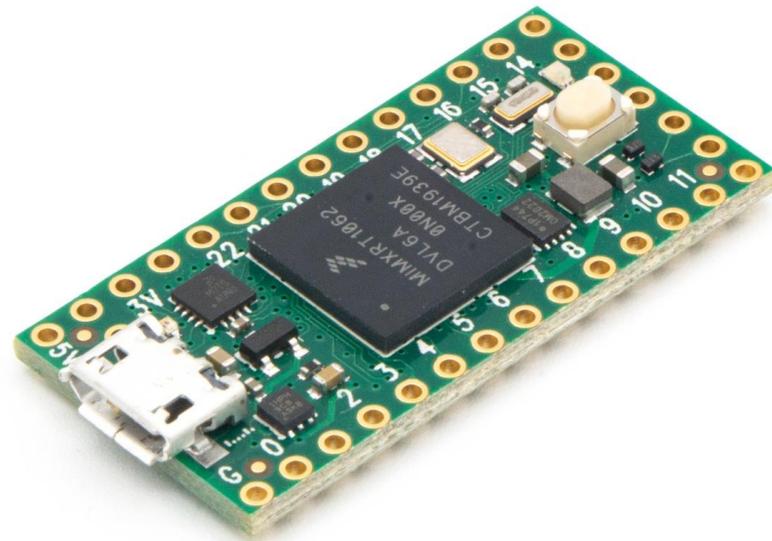
MalDuino



DSTIKE WIFI Duck



Teensy



USBNinja



USB Ninja



BashBunny



PRAXIS Realer Vorfall - BadUSB

The Record
BY RECORDS FUTURE

Leadership Cybercrime Nation-state Government People Technology [Subscribe](#)

IMAGE: THE RECORD, ALEXSPRESS

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

- IS 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 cryptominer 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 219 crypto- and finance-related Malchimp accounts, company said | April 4, 2022

RANSOMWARE TRACKER: THE LATEST FIGURES (MARCH 2022)

RANSOMWARE TRACKER: THE LATEST FIGURES (MARCH 2022)

Quelle: therecord.media (4)

USBKill



USB-Killer



Stromschock



PRAXIS Realer Vorfall – USB-Killer

THE VERGE TECH · REVIEWS · SCIENCE · CREATORS · ENTERTAINMENT · VIDEO · FEATURES · MORE ·  

POLICY / US & WORLD / TECH

Student used 'USB Killer' device to destroy \$58,000 worth of college computers 46

The former College of Saint Rose student faces up to 10 years in prison

By [Chris Welch](#) | [@chrswelch](#) | Apr 17, 2019, 3:07pm EDT



Quelle: [theverge.com](#) (5)

EXKURS Realer Vorfall – Sprengstoff

golem.de IT-NEWS FÜR PROFIS HOME TICKER PODCAST NEWSLETTER GOLEM PLUS FORUM ANMELDEN

Artikel, News, ... Suchen

KARRIEREWELT JOBS IT-FACHTRAININGS COACHINGS SPRACHKURSE GEHALTSCHECK | GOLEM-PC PRODUKTVERGLEICH TOP-ANGEBOTE

MALWARE EXTREM

USB-Sticks mit Sprengstoff-Füllung an Journalisten gesendet

Journalisten in Ecuador haben per Post USB-Sticks erhalten, die so präpariert waren, dass sie beim Einstecken in den Rechner explodieren.

23. März 2023, 8:17 Uhr, Andreas Donath



Einer der nicht explodierten USB-Sticks

Fünf ecuadorianische Rundfunkjournalisten haben per Post mit Sprengstoff und einer Zündvorrichtung bestückte USB-Sticks bekommen, [berichtet CBS News](#). Als ein Journalist den Stick in seinen Rechner steckte, wurde die Explosion ausgelöst.

Dem Bericht nach waren leichte Verletzungen an der Hand und im Gesicht die Folge. Von

(Bild: Fundamedia/f:facebook)

Quelle: [golem.de](#) (6)

LAN & WLAN

LAN-Netzwerke sind das Bindeglied unserer modernen IT-Infrastruktur. Dadurch, dass sie überall verbaut sind, können sie teilweise auch von Angreifern vor Ort angezapft werden. Mit entsprechender Hardware kann der Traffic ausgeleitet und analysiert werden.

WLAN gehört mittlerweile zum Standard und wird für viele Bereiche der IT verwendet. Diese wichtige Infrastruktur kann mit einem Deauther-Angriff gezielt unterbrochen werden oder es werden böartige Zugangspunkte simuliert.

LAN

- Ausleiten von Netzwerk-Verbindungen
- Aufzeichnen von Netzwerk-Übertragungen
- Manipulation von unverschlüsseltem Netzwerkverkehr

WLAN

- Nachahmen von vorhandenen Netzen - Evil-Twin-Accesspoint
- Unterbrechung von vorhandenen WLAN-Verbindungen

Throwing Star LAN Tap Pro



Plunder Bug



Shark Jack



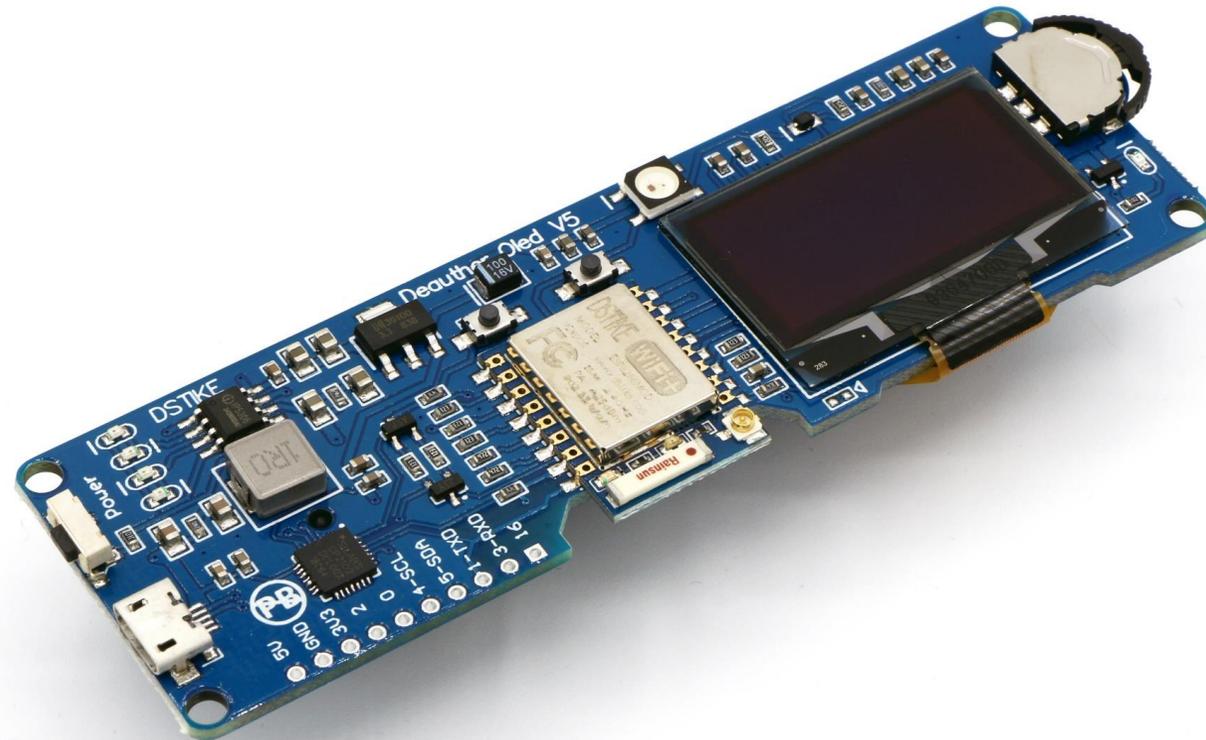
Packet Squirrel



LAN Turtle



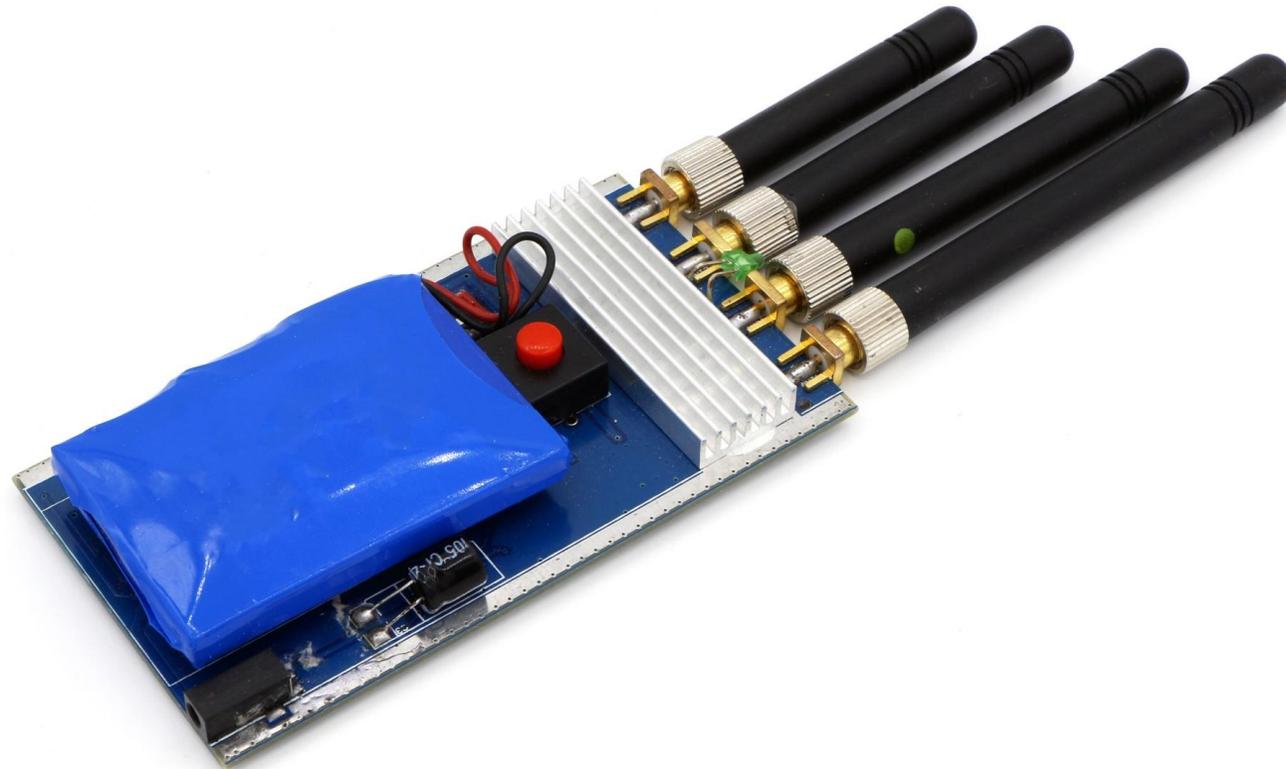
Deauther



WiFi Pineapple



Störsender



Bluetooth & RFID

Bluetooth hat sich zum dominierenden Standard für Funkverbindungen im Nahbereich entwickelt. Das Sicherheitskonzept ist flexibel. Gerade Geräte, die Bluetooth Low Energy verwenden, können mit der passenden Hardware angegriffen bzw. belauscht werden.

RFID-Tags werden in immer mehr Bereichen eingesetzt – von automatisierten Kassen über Türschließanlagen bis hin zur Logistik. Einfache Tags ohne Sicherung können sehr einfach angegriffen werden.

Bluetooth

- Tracking von Bluetooth Geräten
- Manipulation von Bluetooth LE Verbindungen

RFID

- Einfaches Kopieren von unsicheren RFID-Tags
- Duplikate von gesicherten RFID-Chips
- Knacken unsicherer Standards

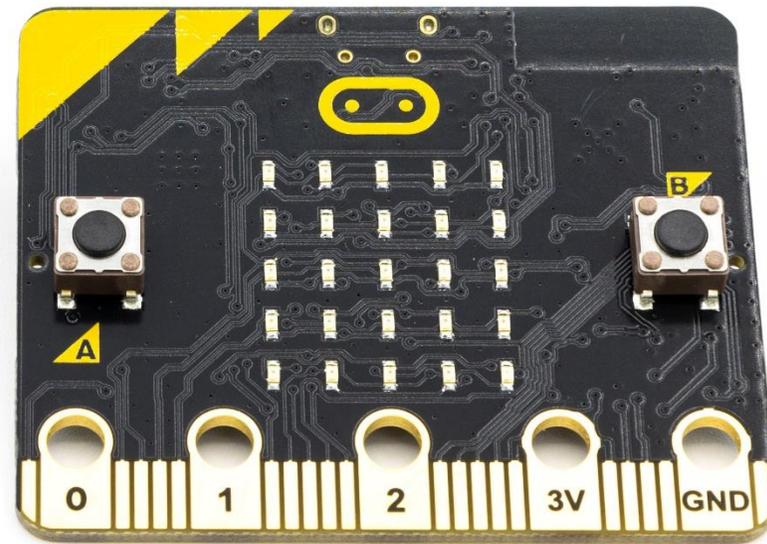
Bluefruit LE-Sniffer



Ubertooth One



BtleJack + BBC micro:bit



RFID Cloner



Keysy



Chameleon Mini



Proxmark



NFCKill



SDR & Funk

Immer mehr Verbindungen werden per Funk realisiert. Per Software Defined Radio (SDR) lassen sich Funksignale in verschiedenen Frequenzbändern aufzeichnen, analysieren und erneut senden. Dadurch können Funkverbindungen angegriffen werden, ohne dass das verwendete Protokoll bekannt sein muss.

- Einfaches „Kopieren“ / Clonen von ungesicherten Funkübertragungen
- Analyse und Aufspüren von Funkverbindungen
- Angriff durch Wiederholung eines Signals (Replay-Angriff)

Cloner



NooElec NESDR SMARt



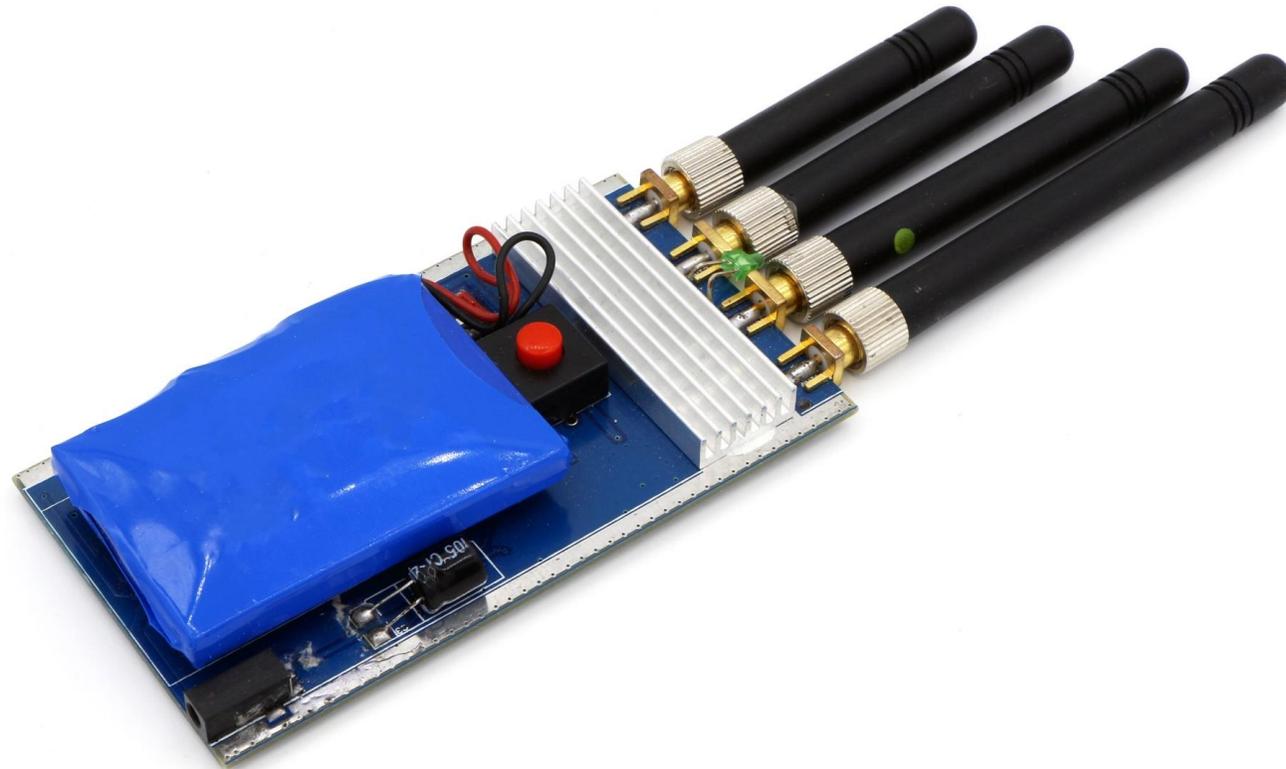
HackRF One



HackRF One + PortaPack



Störsender

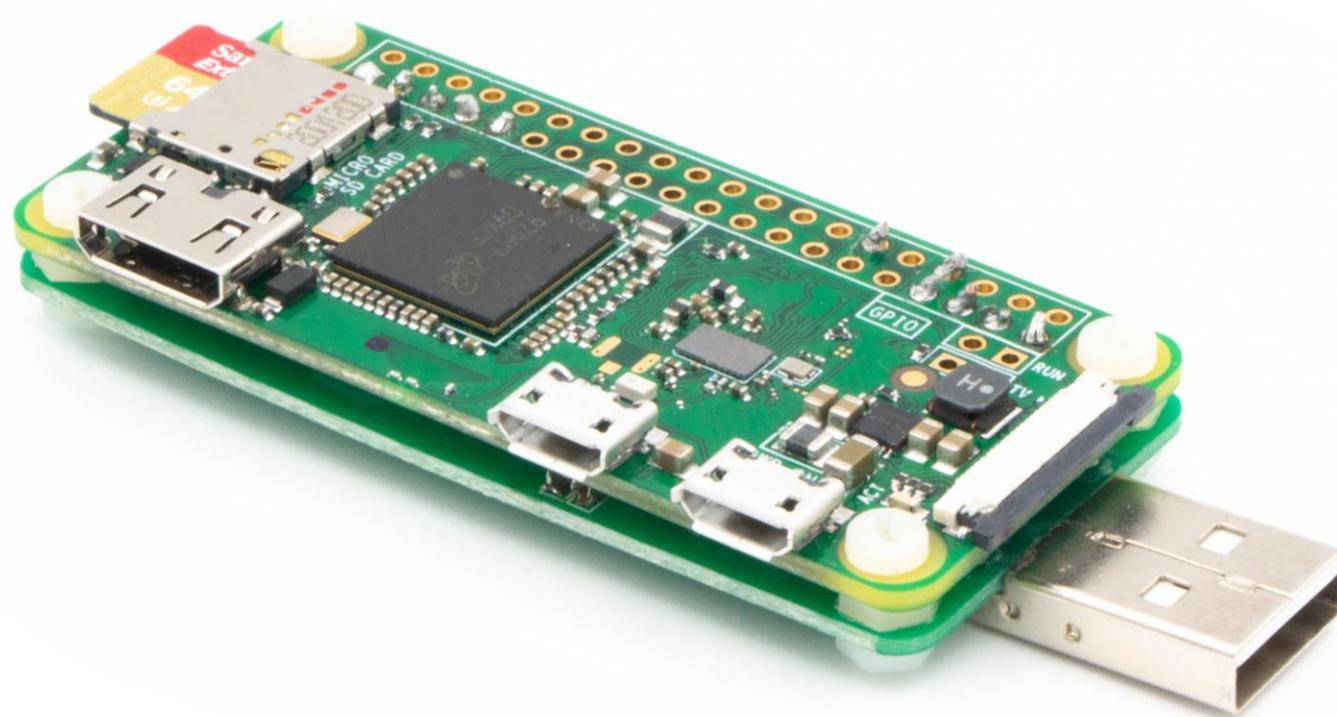


Multitools

Multitools sind eine Generation von Geräten, die mehrere Funktionen in einem Gerät vereinen. Mit dem Raspberry Pi gibt es mehrere Projekte, die ähnliche Funktionen wie spezialisierte Geräte haben. Der Flipper Zero hingegen ist eine spezielle Hardware, die sich durch eine eingängige Steuerung und einfache Handhabung auszeichnet.

- Raspberry Pi
- Flipper Zero

Raspberry Pi



Flipper Zero



Gegenmaßnahmen

Pentest-Hardware Bezugsquellen

The screenshot shows the Amazon.de search results for 'keylogger'. The search bar at the top contains 'keylogger' and the search results show 1-16 of 124 results. The left sidebar contains filters for shipping options, sustainability, category, customer reviews, price, and offers. The main content area displays three products:

- AirDrive Forensic Keylogger Pro**: USB Hardware Keylogger mit WiFi, 16MB Flash, Email und Live-Datenübertragung. Preis: 119,99€. Lieferung bis Samstag, 10. Juni. KOSTENFREIER Versand durch Amazon. Nur noch 6 auf Lager.
- KeyGrabber USB KeyLogger 16MB Schwarz**: Preis: 46,99€. Lieferung Montag, 12. Juni – Donnerstag, 15. Juni. 7,95 € Versand.
- Multipick Profi Dietrich Set**: Made in Germany - Sperrhaken-Set - öffnet nahezu jede Tür - 2 Stück Schlüsseldienst Türöffner Schlüssel für Bunt-Bart-Schloss Öffner. Preis: 13,90€. Lieferung bis Samstag, 10. Juni. GRATIS-Versand durch Amazon.

Below the third product, there is a section for 'Weitere ergebnisse' showing a 'Digitales USB-Aufnahmegerät zum Spionieren von Gesprächen - Mini Spy USB Sound Voice Recorder - mit 8 GB Flash-Drive - Eignet sich am besten für Meetings, Präsentationen, Notizen machen - Mac/Win - Pro...'

Bezugsquellen hak5.org

The screenshot shows the hak5.org website with a dark theme. At the top right, there are links for 'LOGIN' and a shopping cart icon showing '0' items. The main navigation bar includes 'PRODUCTS' (with a dropdown arrow), 'PODCASTS', the 'HAK5' logo, 'COMMUNITY', and 'SUPPORT'. Below this, a grid of product categories is displayed, each with a representative image and a list of items:

- 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

Bezugsquellen **lab401.com**

The screenshot shows the top navigation bar of the lab401.com website. The logo 'LAB|401' is on the left. On the right, there are links for 'Sign in' and 'Create an Account', a search bar with the placeholder 'Search all products...', and a shopping cart icon labeled 'CART'. Below the navigation bar, there is a horizontal menu with links: 'HOME', 'PRODUCTS' (with a dropdown arrow), 'ACADEMY', 'FAQ', 'LEA TOOLS', 'ENTERPRISE TOOLS', and 'MORE' (with a dropdown arrow). To the right of this menu is a 'PRICE PREFERENCE' section with a toggle for 'Ex VAT' (selected) and 'Inc. VAT'. The main content area features a promotional banner for HAK5 products. On the left, there are images of various hardware devices including a wireless router, a small black box, a USB dongle, and a USB drive. On the right, the text reads 'EXCLUSIVE EUROPEAN DISTRIBUTOR' above the 'HAK5' logo. Below the logo, a list of products is shown: 'Wifi Pineapple', 'Rubber Ducky', 'LAN Turtle', 'Plunderbug', 'Signal Owl', 'Bash Bunny', 'Shark Jack', and 'Packet Squirrel'. At the bottom of the banner, it says 'AVAILABLE NOW' and a red button with the text 'VIEW ALL PRODUCTS'.

Bezugsquellen hackmod.de

The screenshot shows the top section of the HackmoD website. At the top left, there are links for 'Mein Konto' and 'Anmelden', followed by the HackmoD logo (a shield with 'H' and 'M'). To the right is a search bar with the text 'Suchen nach' and a magnifying glass icon, and a shopping cart icon with the text 'Ihr Warenkorb ist leer.' and flags for Germany and the UK. Below this is a green navigation bar with the HackmoD logo and the tagline 'IT-Security & Pentest Gadgets'. To the right of the logo are menu items: 'Hak5', 'IT-Security Tools', 'Pentest Tools', 'RFID-Security', 'SDR', and 'Zubehör'. The main banner features the text 'HackmoD IT-Security. Licensed & Official Hak5 Distributor Europe!' in bold black letters. Below this text is a circular logo for 'HACKMOD IT-SECURITY & PENTEST GADGETS' with a stylized 'H' and 'M'. To the right of the logo is the text 'Professional Pentest Tools' and a large 'HAK5' logo where 'HAK' is white and '5' is red. Below the 'HAK5' logo are three circular icons: the German flag, the European Union flag, and the Swiss flag. To the right of these icons is the text 'EU Partner' in red. At the bottom right of the banner is a small shield logo with 'H' and 'M'.

Bezugsquellen firewire-revolution.de

The screenshot shows the homepage of Firewire Revolution. At the top right, there are links for 'MEIN KONTO', 'WARENKORB', and language selection icons for USA, France, and Germany. Next to these are 'ANMELDEN' and 'REGISTRIEREN' buttons. The main header features the Firewire Revolution logo (a fingerprint icon) and the tagline 'We Secure your World'. A search bar with the placeholder 'Suche...' and a magnifying glass icon is positioned to the right of the logo. Further right, the email address 'info@firewire-revolution.de' is displayed, along with a notification icon showing '0'. Below the header is a navigation menu with the following items: 'HOME', 'IT-FORENSIK HARDWARE', 'IT-FORENSIK SOFTWARE', 'FARADAY BAGS', 'DIGITAL CINEMA', 'STORAGE', 'SPEZIAL', and 'ZUBEHÖR'. The main content area features a large red banner with the text 'Willkommen bei FIREWIRE REVOLUTION' in bold red letters, and below it, 'Hotly sought after Pentesting Tools!' in bold white letters. The background of the banner shows silhouettes of server racks.

Grundsätzliche Maßnahmen

Allgemeine Maßnahmen

- Zugangsbeschränkung, so dass nur befugte Personen Zutritt haben.
- Übersichtliche und aufgeräumte Arbeitsplätze und Büroräume.
- Schulungen zur Erkennung von Hacking Hardware.

Spezifische Maßnahmen

- Sicherung von Computersystemen durch bauliche Maßnahmen.

Schnittstellen

Key- & Screenlogger

- Mobile Computer sind unterwegs nicht betroffen, evtl. aber mit Dockingstation.
- Tastaturen, die über Bluetooth (eingebautes Modul) verbunden sind, sind nicht betroffen.
- Überprüfung auf neue oder unbekannte WLANs.

BadUSB

- Computer sperren, damit während der Abwesenheit keine BadUSB-Geräte angeschlossen werden können.
- Softwarelösung zur Erkennung und Sperrung neuer Tastaturen oder USB-Geräte.
- Implementierung über Gruppenrichtlinien möglich.

Physische Gegenmaßnahmen

Stromquelle



USB-Schlösser



Verbindungen

LAN & WLAN

- Detektion von Unterbrechungen
- Aufspüren fremder Geräte
- Zero-Trust (verschlüsselte interne Verbindungen)
- WLAN: Erkennung von Deauther-Angriffen
- LAN: Deaktivierung unbenutzter Ports

RFID & Funk

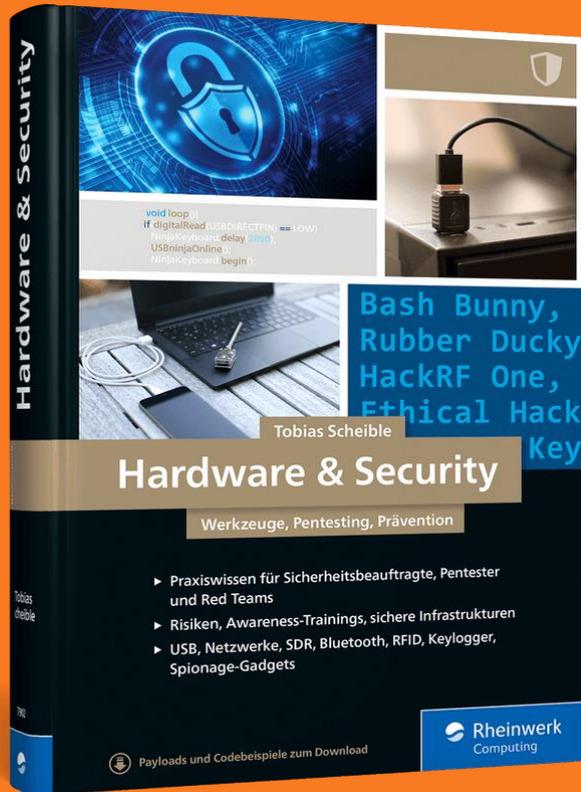
- Detektion von Unterbrechungen
- Erkennung von logischen Fehlern
- Zusätzliche Quellen identifizieren

Physische Gegenmaßnahmen

RJ45-Schlösser



Faszination Hardware



Experimentieren Sie mit verschiedenen Geräten, um die Funktionsweise besser zu verstehen.

Testen Sie Ihre eigene Infrastruktur auf Sicherheitslücken mit Hacking Hardware.

Neugierig?

+ Online-Vorträge & Workshops: www.scheible.it

+ Buch „Hardware & Security“

Quellen

- (1) <https://taz.de/Keylogger-Affaere-in-der-taz/!5307828/>, abgerufen am 29.11.2023
- (2) <https://www.derstandard.at/story/2000067331995/ueber-90-noten-manipuliert-student-droht-jahrzehntelange-haftstrafe>, abgerufen am 29.11.2023
- (3) <https://www.tagesspiegel.de/berlin/berliner-polizei-entdeckt-datenleck-3989428.html>, abgerufen am 29.11.2023
- (4) <https://therecord.media/fbi-fin7-hackers-target-us-companies-with-badusb-devices-to-install-ransomware/>, abgerufen am 29.11.2023
- (5) <https://www.theverge.com/2019/4/17/18412427/college-saint-rose-student-guilty-usb-killer-destroyed-computers>, abgerufen am 29.11.2023
- (6) <https://www.golem.de/news/malware-extrem-usb-sticks-mit-sprengstoff-fuellung-an-journalisten-gesendet-2303-172862.html>, abgerufen am 29.11.2023
- (7) <https://hak5.org>, abgerufen am 29.11.2023
- (8) <https://lab401.com>, abgerufen am 29.11.2023
- (9) <https://hackmod.de>, abgerufen am 29.11.2023
- (10) <https://firewire-revolution.de>, abgerufen am 29.11.2023