

Smashing the Stack for Fun and Non-Profit

Dr. Melanie Rieback



RADICALLY
OPEN
SECURITY

When hackers grow up...



DESFAIR.COM

CONSULTING

IF YOU'RE NOT A PART OF THE SOLUTION,
THERE'S GOOD MONEY TO BE MADE IN PROLONGING THE PROBLEM.



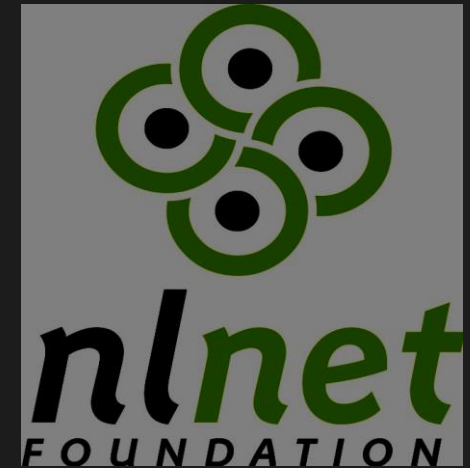
RADICALLY OPEN SECURITY

Jan 27, 2015

Not-for-profit business model

- Fiscal Fundraising Institution (FFI)

We love... 



(With 90% of our profits!)



RADICALLY OPEN SECURITY

Jan 27, 2015

Our Services

[HOME](#)

[NON-PROFIT?](#)

[CORE PRINCIPLES](#)

[SERVICES](#)

[TEAM](#)

[BLOG](#)

[CONTACT US](#)



Services

- [PENETRATION TESTING + ETHICAL HACKS + SOCIAL ENGINEERING](#)
- [MALWARE REVERSING AND ANALYSIS](#)
- [NETWORK MONITORING + THREAT DETECTION](#)
- [FORENSICS](#)
- [CSIRT + INCIDENT RESPONSE](#)
- [CODE AUDITS](#)
- [DDOS TESTING](#)
- [PHYSICAL PENETRATION TESTING + LOCKPICKING](#)
- [CUSTOM R&D PROJECTS](#)
- [WORKSHOPS + TRAININGS + MENTORING](#)
- [MISC: EMBEDDED + ANDROID + RFID SECURITY](#)

[Terms and Conditions](#)



RADICALLY OPEN SECURITY

Jan 27, 2015

Our Team is...

- Founders and Core-Developers:



- Members of:



RADICALLY OPEN SECURITY

ROS Core Principles

- No sketchy sh*t
- Teach to fish
- Open-source
- IOCs for free
- Zero days (responsible disclosure)



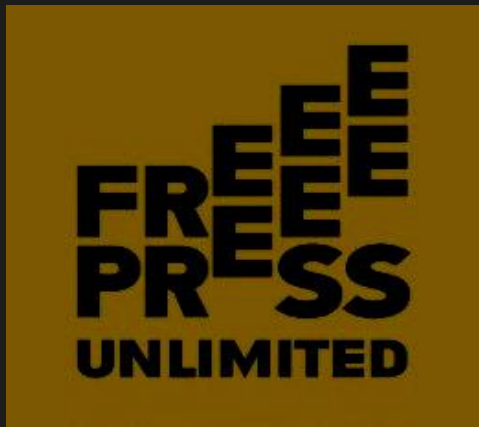
Research is fun!!!

- NetAidKit
- Open-source DDoS analysis (OSAS)
- Cuckoo Malware Sandbox
- We're open to new ideas!!! :-)



NetAidKit

Wi-Fi Tor/OpenVPN Router



<https://netaidkit.net>

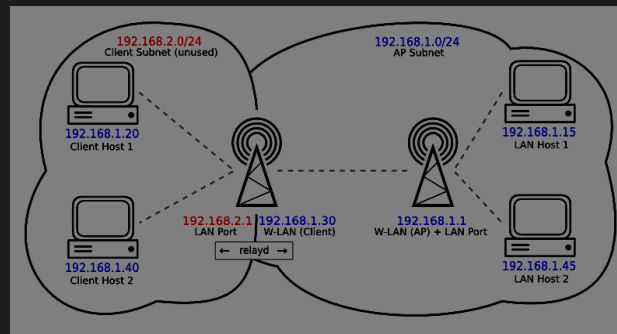


RADICALLY OPEN SECURITY

Jan 27, 2015

NetAidKit

We're not re-inventing the wheel



NetAidKit



Setup

Before you can use the NetAidKit, you've got to make it your own. On this page, we will give your NetAidKit a new wireless network name and password and choose an administrator password you will use to make changes in the future.

Let's get started!

Enter a new network name ∞

Enter a new network password 🔒

To make sure only you and people you trust can connect to your NetAidKit, choose a password to protect your new wireless network.

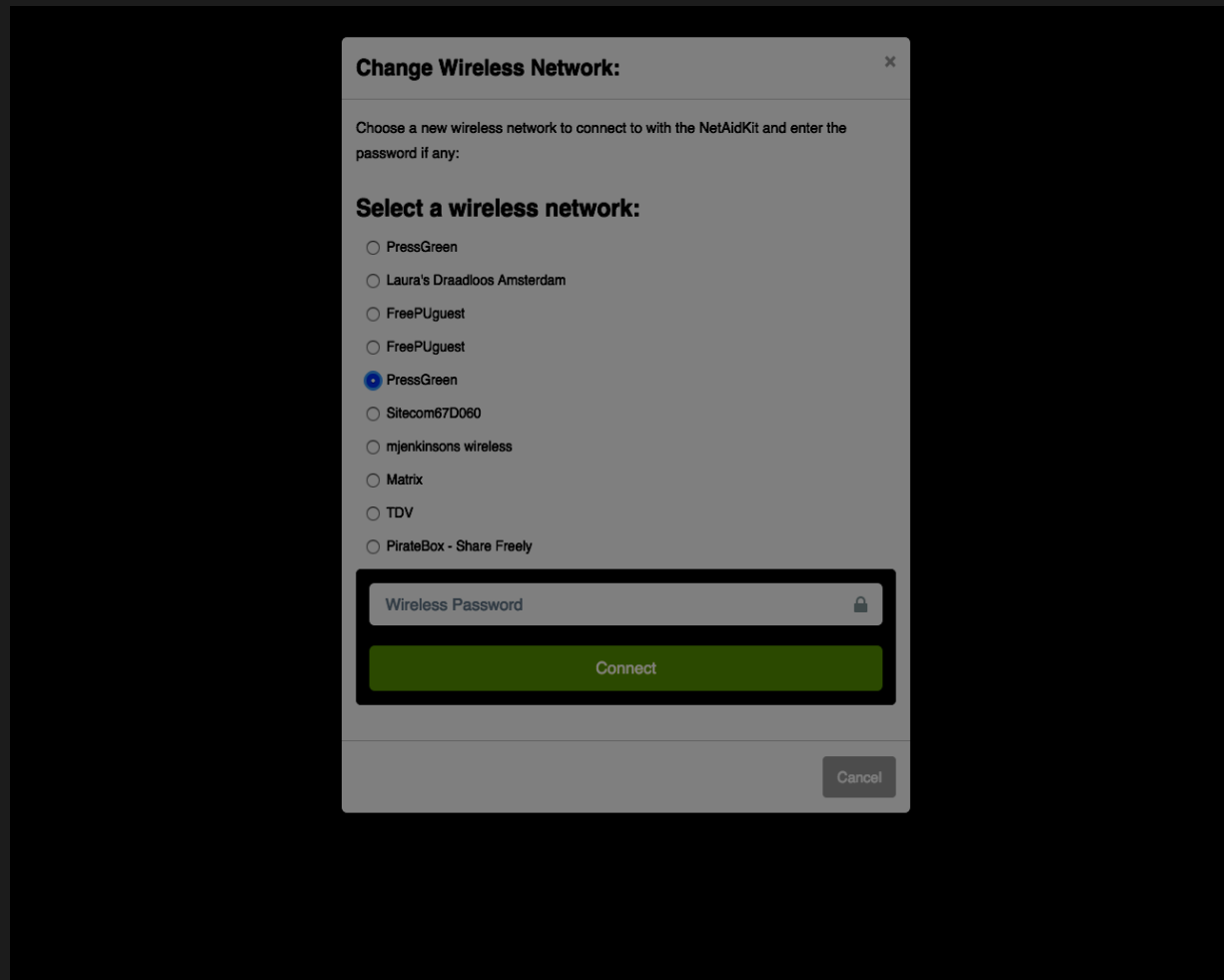
Enter a new administrator password 👤

Enter a distress password 🔒

Finish Setup



NetAidKit



NetAidKit



Welcome!

The NetAidKit is currently connected to the following wireless network:

PressGreen

Change Wireless Network

You are connected to Tor

The Tor network can be used for extra anonymity and to circumvent censorship. Connecting to Tor will send all your traffic over the anonymous Tor network.

Disconnect from Tor

VPN

A Virtual Private Network creates an encrypted tunnel between the NetAidKit and a trusted network over the Internet.

AirVPN_United-Kingdom_UDP-443.ovpn

Connect to VPN



NetAidKit

The screenshot shows the GitHub repository page for `radicallyopensecurity/NetAidKit`. The repository is described as a "Standalone VPN/Tor WiFi router for journalists and activists". It has 12 commits, 1 branch, 0 releases, and 3 contributors. The latest commit is by `sj0rz` a day ago, with the commit hash `2dc73cc975`. The commit message is "Flash messaging added." The file list includes `di`, `doc`, `feeds/packages/netaidkit/nak-web`, `files/etc`, `nak-pkg`, `LICENSE`, `README.md`, and `netaidkit.config`. The right sidebar shows options to clone the repository in Desktop or download as ZIP, and a list of repository features like Issues, Pull Requests, and Wiki.

radicallyopensecurity / **netaidkit** Unwatch 9 Star 8 Fork 0

Standalone VPN/Tor WiFi router for journalists and activists — Edit

12 commits 1 branch 0 releases 3 contributors

branch: master netaidkit / +

Flash messaging added.

sj0rz authored a day ago latest commit 2dc73cc975

di	Removed references to sbbox.	5 days ago
doc	Specification Draft added	3 months ago
feeds/packages/netaidkit/nak-web	Flash messaging added.	a day ago
files/etc	Version 0.1	19 days ago
nak-pkg	Removed references to sbbox.	5 days ago
LICENSE	Initial commit	5 months ago
README.md	Removed references to sbbox.	5 days ago
netaidkit.config	Removed more sbbox files, enable php session.	a day ago

README.md

NetAidKit

Code

- Issues 13
- Pull Requests 0
- Wiki
- Pulse
- Graphs
- Settings

HTTPS clone URL

`https://github.com`

You can clone with HTTPS, SSH, or Subversion.

Clone in Desktop

Download ZIP



RADICALLY OPEN SECURITY

Jan 27, 2015

NetAidKit

ISOC.nl Internet Innovatie Award 2015

Met de ISOC.nl Innovatie Award wil Internet Society Nederland vernieuwende en belangwekkende initiatieven rondom internet de erkenning geven die ze verdienen. Innovaties, die een stimulans betekenen voor de groei van en kennis over het internet. De prijs wordt uitgereikt aan personen, instellingen of initiatieven en is een teken van grote maatschappelijke waardering voor prestaties ter verbetering van het internet en het gebruik ervan.

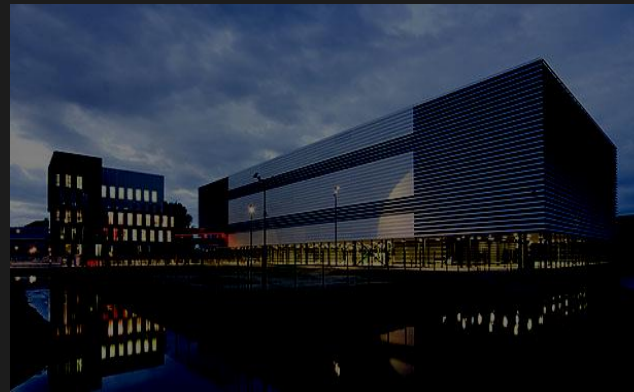
Tijdens de Internetnieuwjaarsbijeenkomst 2015 in Amsterdam werd NetAidKit uitgeroepen tot winnaar van de ISOC.nl Internet Innovatie Award 2015. Bij het gebruik van internet buitenshuis zijn mensen vaak veel kwetsbaarder dan ze denken. Het nemen van tegenmaatregelen (zoals het gebruik van tunnels en dynamische MAC-adressen) is relatief complex, en op veel apparatuur zoals smartphones van Apple of Android-devices bijna onmogelijk. NetAidKit wil een simpel en goedkoop (open source/open hardware) apparaatje bieden dat als buffer functioneert en de complexiteit afvangt - en zo kwetsbare gebruikers zoals journalisten en mensenrechtenactivisten afschermt en beschermt.



Uit handen van juryvoorzitter Jan Andries Wolthuis ontvingen Menso Heus (Internet Protection Lab/Free Press Unlimited) en Melanie Rieback (Radically Open Security) de prijs.



Open-Source DDoS Analysis System (OSAS)



nbip(((((

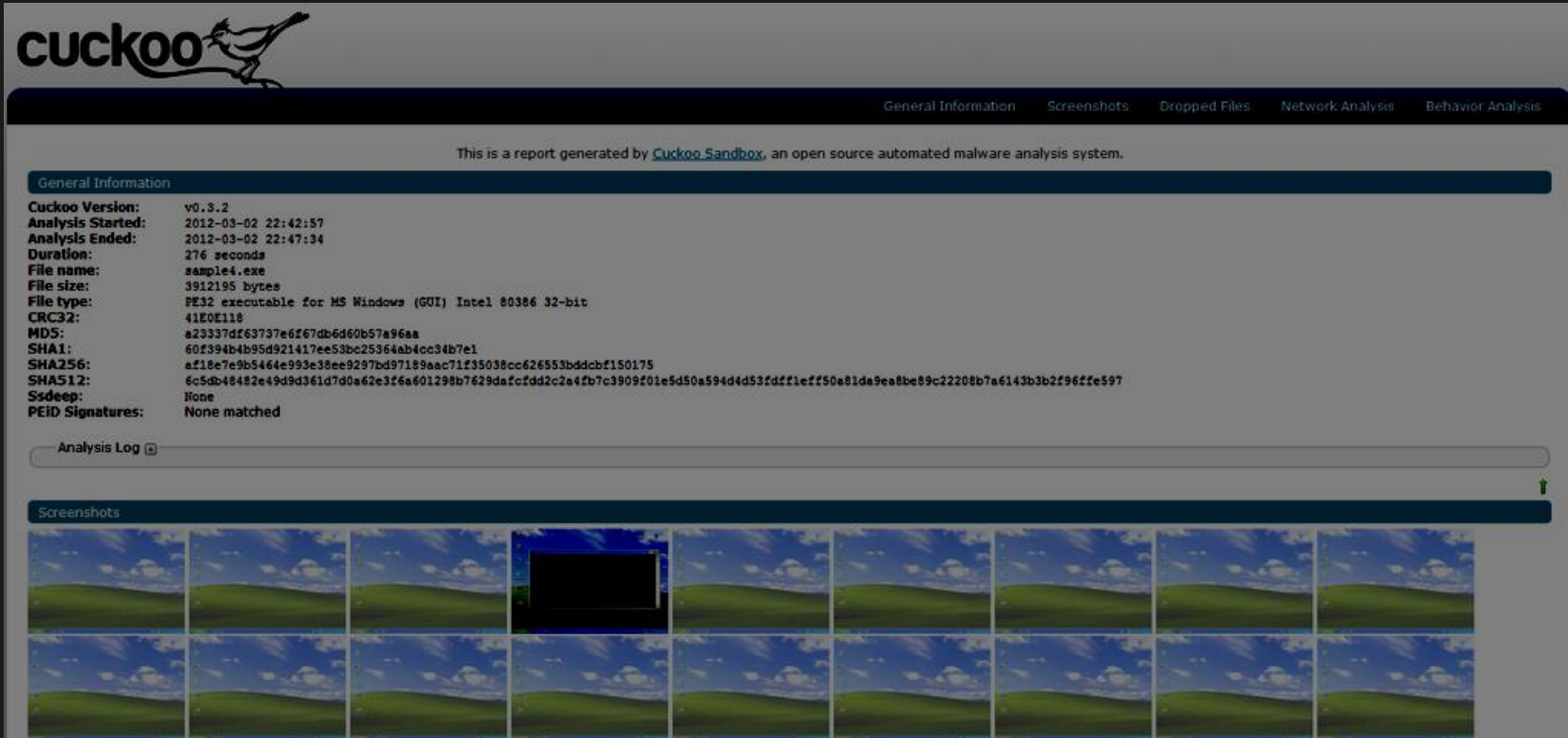
Nationale Beheersorganisatie Internet Providers



RADICALLY OPEN SECURITY

Jan 27, 2015

Cuckoo Malware Sandbox



cuckoo

General Information | Screenshots | Dropped Files | Network Analysis | Behavior Analysis


This is a report generated by [Cuckoo Sandbox](#), an open source automated malware analysis system.

General Information

Cuckoo Version: v0.3.2
Analysis Started: 2012-03-02 22:42:57
Analysis Ended: 2012-03-02 22:47:34
Duration: 276 seconds
File name: sample4.exe
File size: 3912195 bytes
File type: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
CRC32: 41E0E118
MDS: a23337df63737e6f67db6d60b57a96aa
SHA1: 60f394b4b95d921417ee53bc25364ab4cc34b7e1
SHA256: af18e7e9b5464e993e38ee9297bd97189aac71f35038cc626553bddcbf150175
SHA512: 6c5db48482e49d9d361d7d0a62e3f6a601298b7629dafcfd2c2a4fb7c3909f01e5d50a594d4d53fdff1eff50a81da9ea8be89c22208b7a6143b3b2f96ffe597
Ssdeep: None
PEID Signatures: None matched

Analysis Log

Screenshots



How Can We Help?

- Security geeks:
 - Work for us!
- Students
 - Student projects available!!!
- Companies:
 - Buy from us!
- Idealists:
 - Volunteer for us!



Questions?



RADICALLY
OPEN
SECURITY