RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

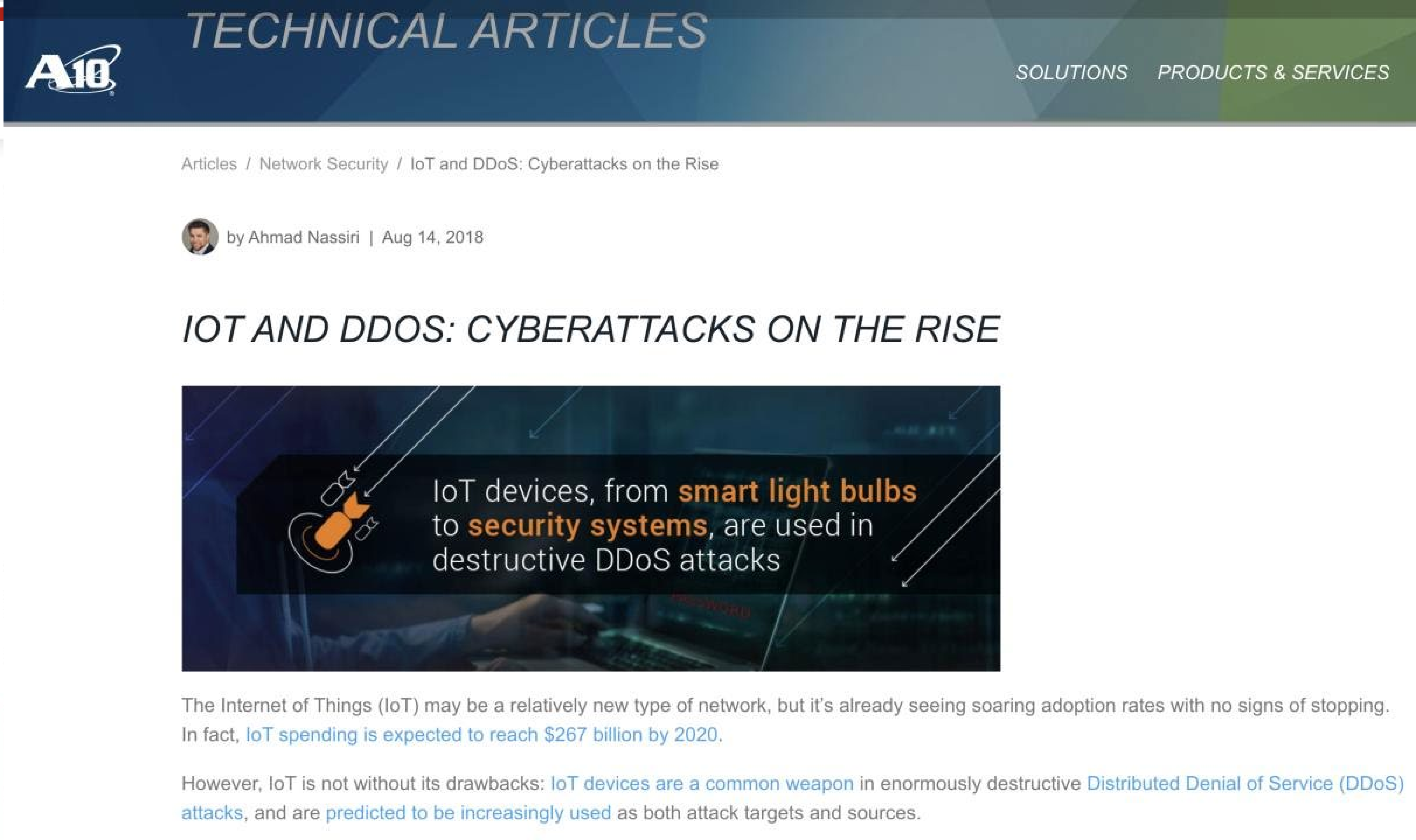
HUMAN ELEMENT

SESSION ID: **SEM-M03E**

# IOT Monetization Schemes from the Cybercrime Underground

**David Sancho**

Senior Threat Researcher
Trend Micro
@dsancho66



Articles / Network Security / IoT and DDoS: Cyberattacks on the Rise

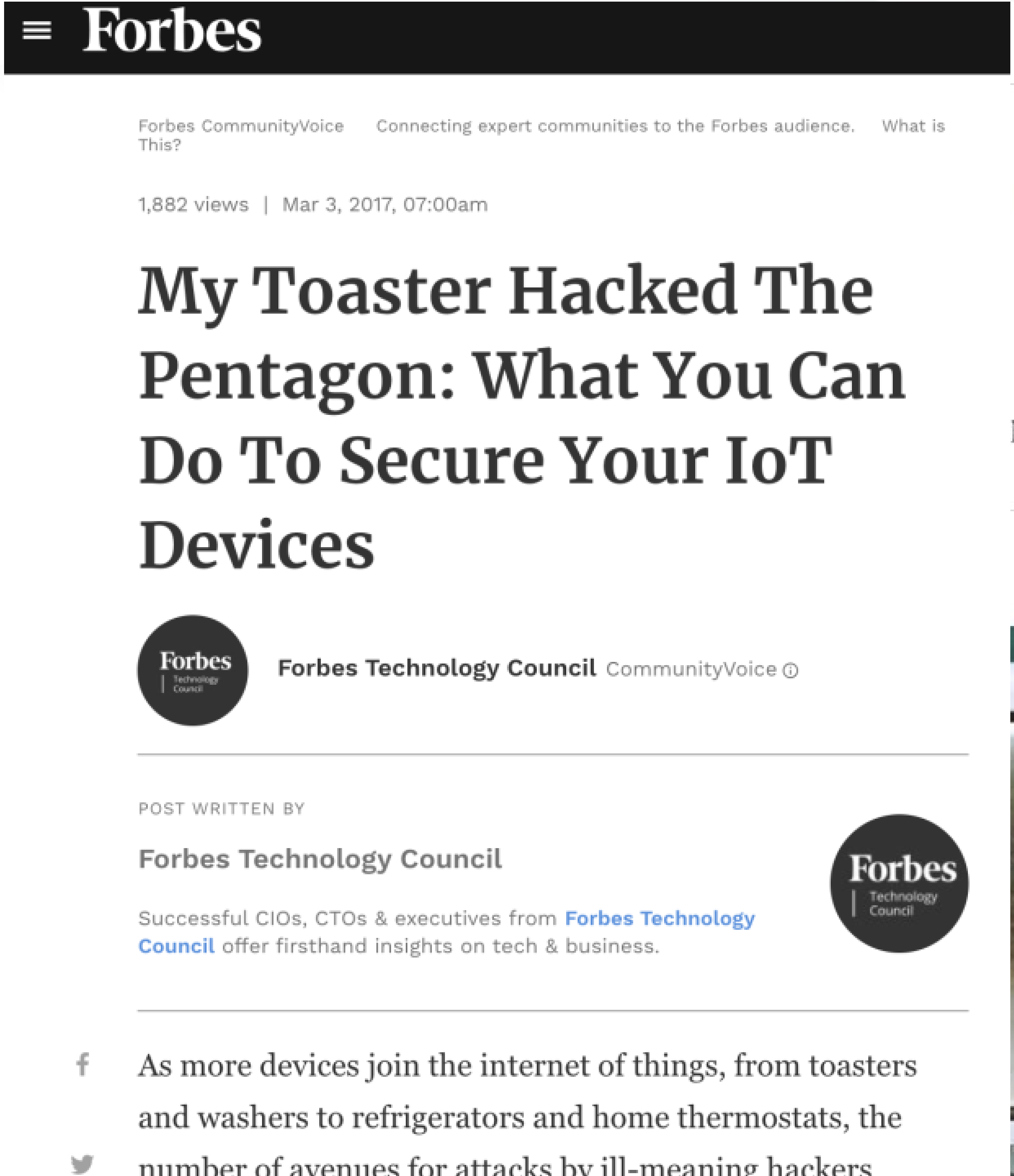
by Ahmad Nassiri | Aug 14, 2018

# IOT AND DDOS: CYBERATTACKS ON THE RISE

IoT devices, from **smart light bulbs** to **security systems**, are used in destructive DDoS attacks

The Internet of Things (IoT) may be a relatively new type of network, but it's already seeing soaring adoption rates with no signs of stopping. In fact, IoT spending is expected to reach $267 billion by 2020.

However, IoT is not without its drawbacks: IoT devices are a common weapon in enormously destructive Distributed Denial of Service (DDoS) attacks, and are predicted to be increasingly used as both attack targets and sources.



Forbes

Forbes CommunityVoice Connecting expert communities to the Forbes audience. What is This?

1,882 views | Mar 3, 2017, 07:00am

# My Toaster Hacked The Pentagon: What You Can Do To Secure Your IoT Devices

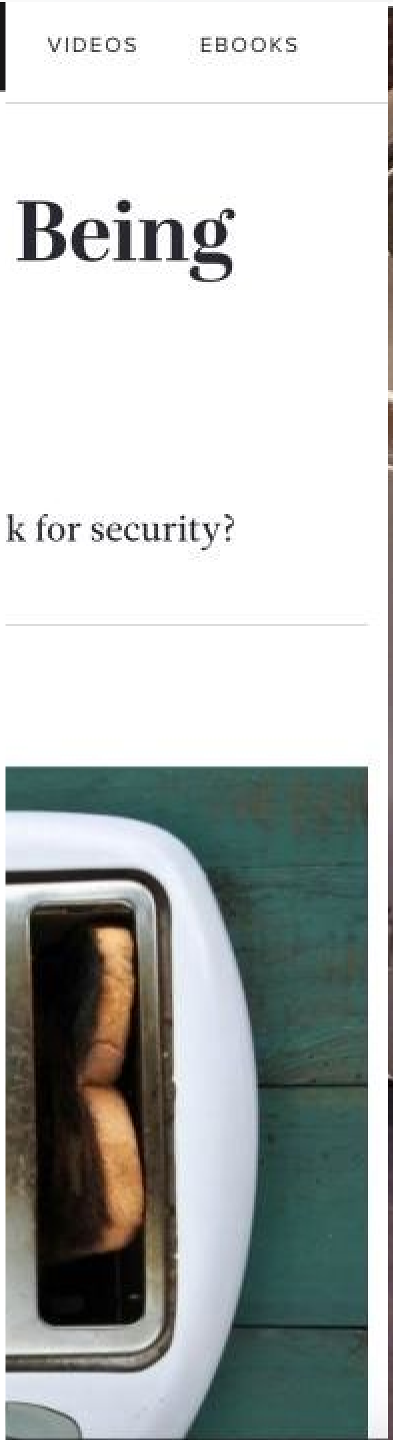
Forbes Technology Council CommunityVoice

POST WRITTEN BY

Forbes Technology Council

Successful CIOs, CTOs & executives from **Forbes Technology Council** offer firsthand insights on tech & business.

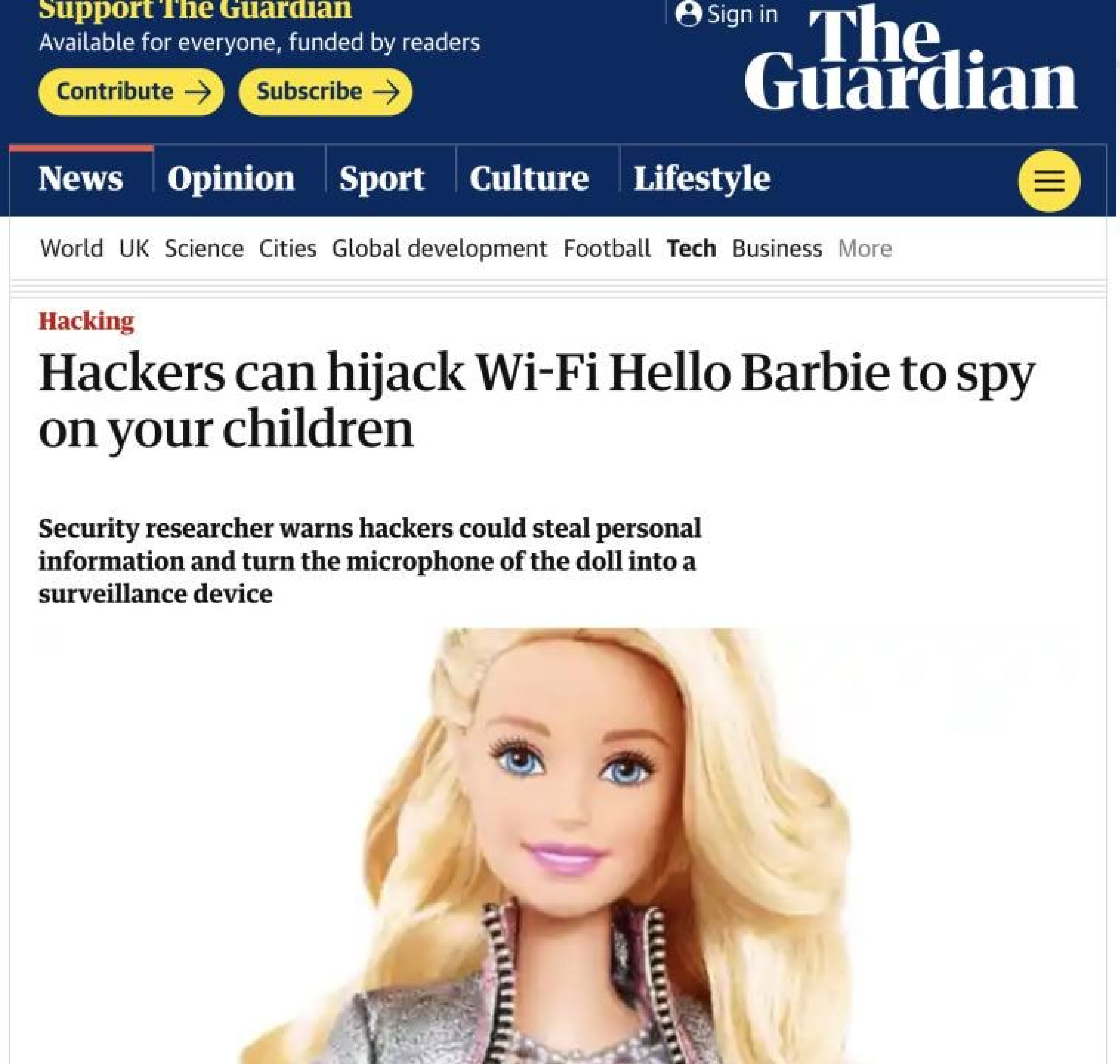
As more devices join the internet of things, from toasters and washers to refrigerators and home thermostats, the number of avenues for attacks by ill-meaning hackers



VIDEOS EBOOKS

Being

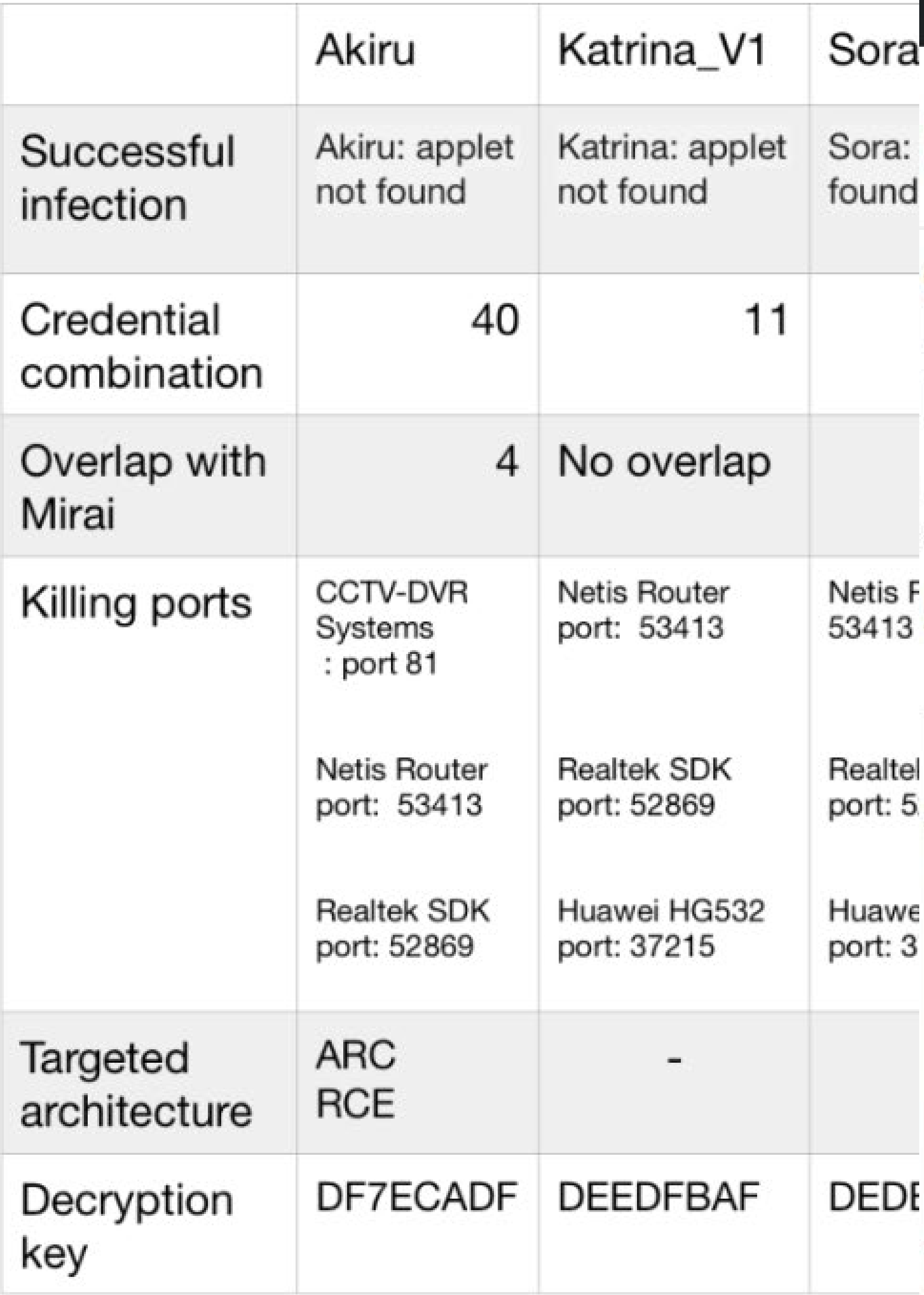
k for security?



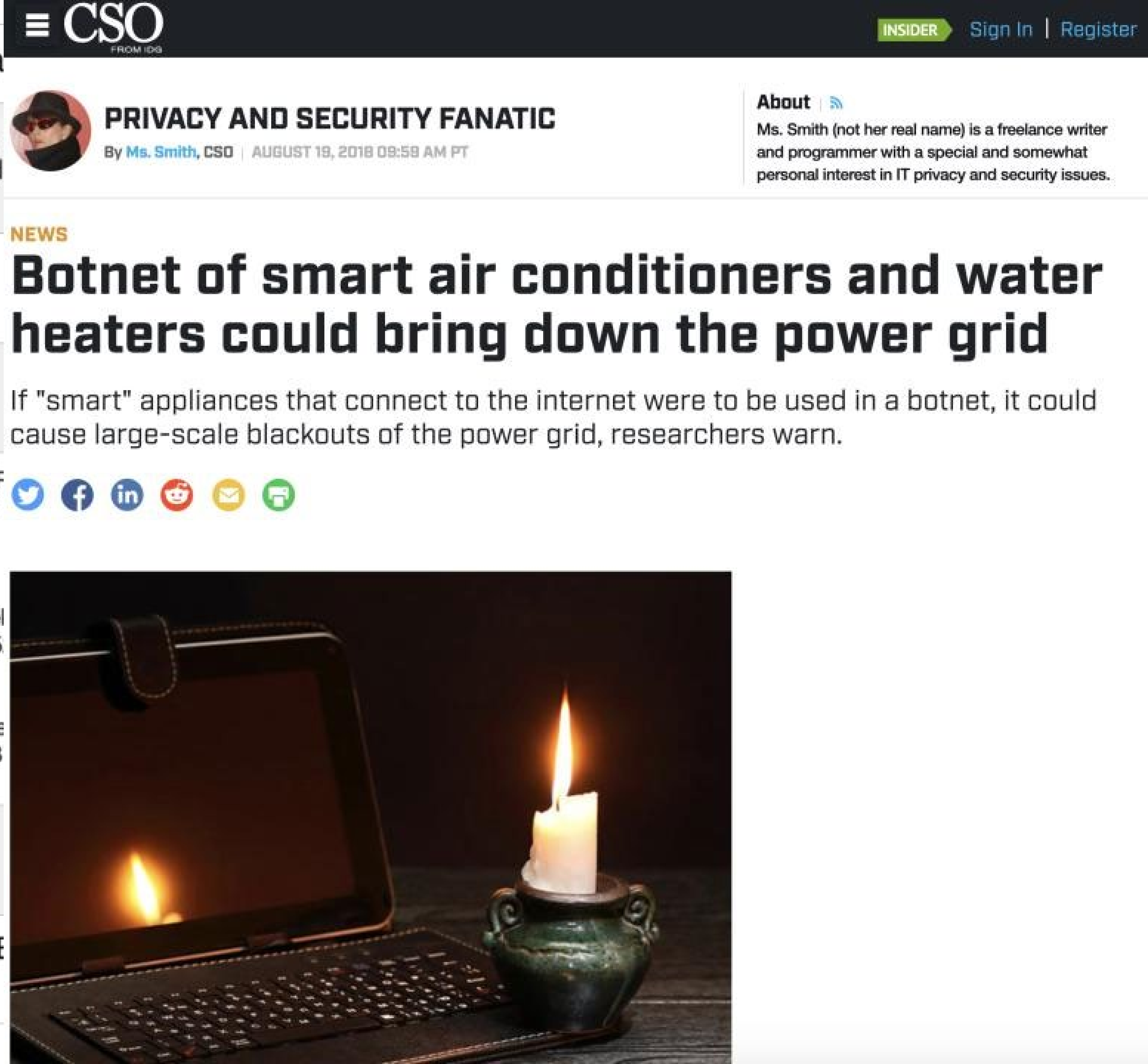
Hacking

# Hackers can hijack Wi-Fi Hello Barbie to spy on your children

**Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device**



| | Akiru | Katrina_V1 | Sora |
|---|---|---|---|
| Successful infection | Akiru: applet not found | Katrina: applet not found | Sora:<br>found |
| Credential combination | 40 | 11 | |
| Overlap with Mirai | 4 | No overlap | |
| Killing ports | CCTV-DVR Systems : port 81<br>Netis Router port: 53413<br>Realtek SDK port: 52869 | Netis Router port: 53413<br>Realtek SDK port: 52869<br>Huawei HG532 port: 37215 | Netis F 53413<br>Realtel port: 5<br>Huawe port: 3 |
| Targeted architecture | ARC<br>RCE | - | |
| Decryption key | DF7ECADF | DEEDFBAF | DEDE |



PRIVACY AND SECURITY FANATIC

By Ms. Smith, CSO | AUGUST 19, 2018 09:59 AM PT

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

# Botnet of smart air conditioners and water heaters could bring down the power grid

If "smart" appliances that connect to the internet were to be used in a botnet, it could cause large-scale blackouts of the power grid, researchers warn.

ORDEM E PROGRESSO
PLVS
VLTRA
جامعة الدول العربية

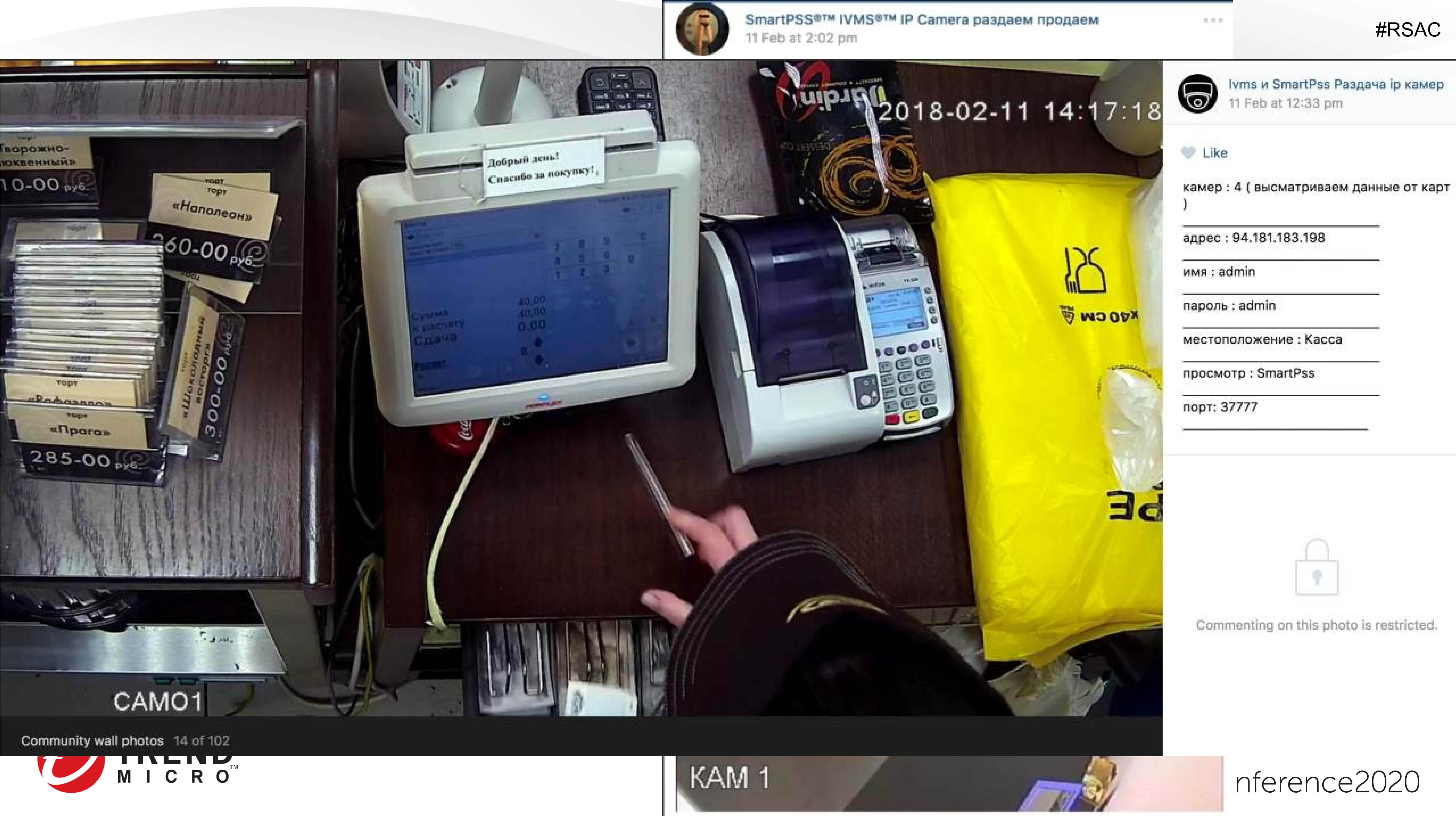
C

Furbo

# What is IOT?

nest
COOLING
75
78

VICTOR
SMART-KILL
Electronic Mouse Trap
WiFi
Receive Kill Alerts On Your Mobile Device
Connect. Control. Defend.



SmartPSS®™ IVMS®™ IP Camera раздаем продаем
11 Feb at 2:02 pm

Community wall photos 14 of 102

Ivms и SmartPss Раздача ip камер
11 Feb at 12:33 pm

Like

камер : 4 ( высматриваем данные от карт )

адрес : 94.181.183.198

имя : admin

пароль : admin

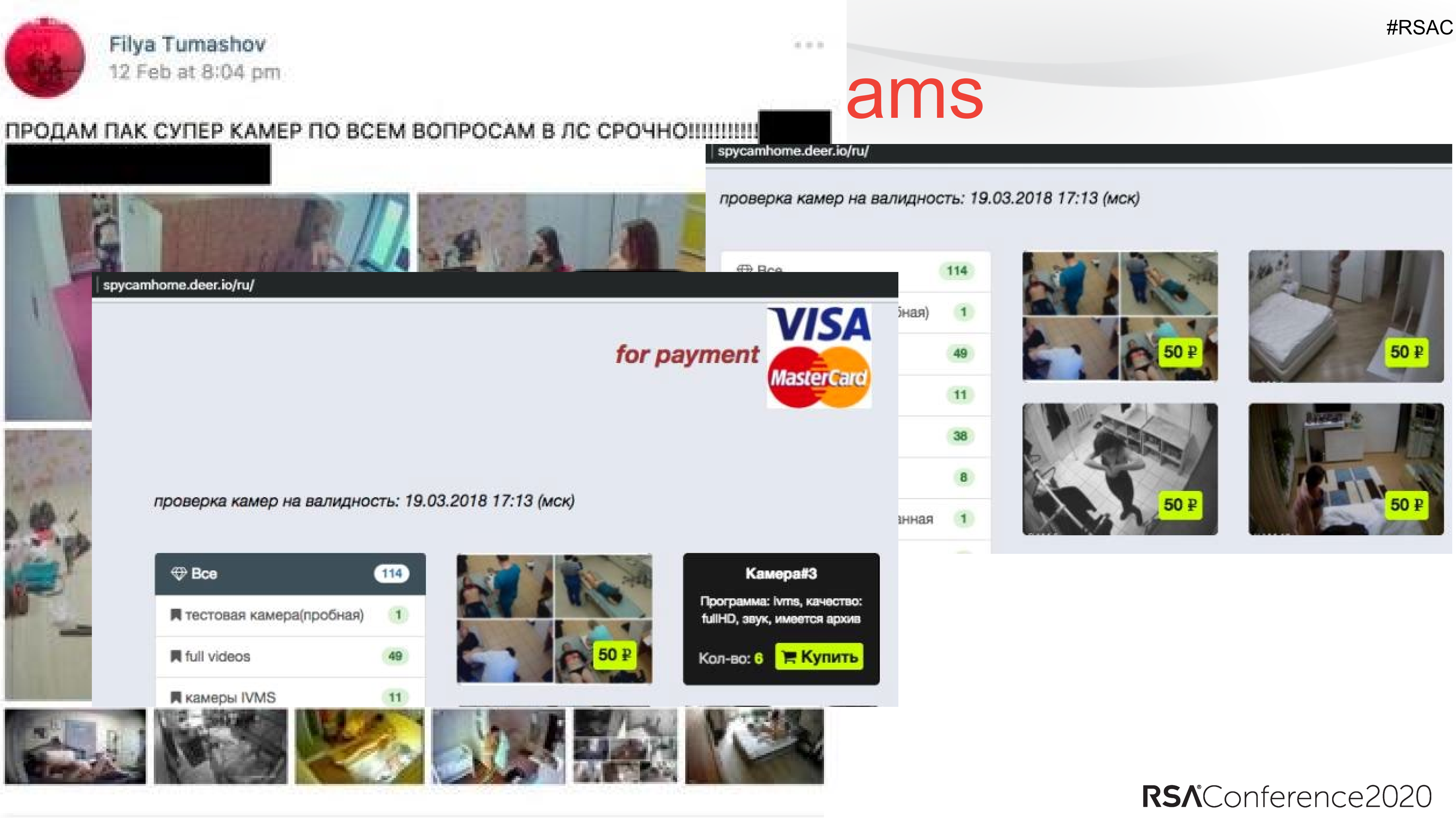
местоположение : Касса

просмотр : SmartPss

порт: 37777

Commenting on this photo is restricted.

# ams



Filya Tumashov
12 Feb at 8:04 pm

ПРОДАМ ПАК СУПЕР КАМЕР ПО ВСЕМ ВОПРОСАМ В ЛС СРОЧНО!!!!!!!!!!! [redacted]

[redacted]

spycamhome.deer.io/ru/

*for payment*

*проверка камер на валидность: 19.03.2018 17:13 (мск)*

| | |
|---|---|
| Все | 114 |
| тестовая камера(пробная) | 1 |
| full videos | 49 |
| камеры IVMS | 11 |

**Камера#3**

Программа: ivms, качество: fullHD, звук, имеется архив

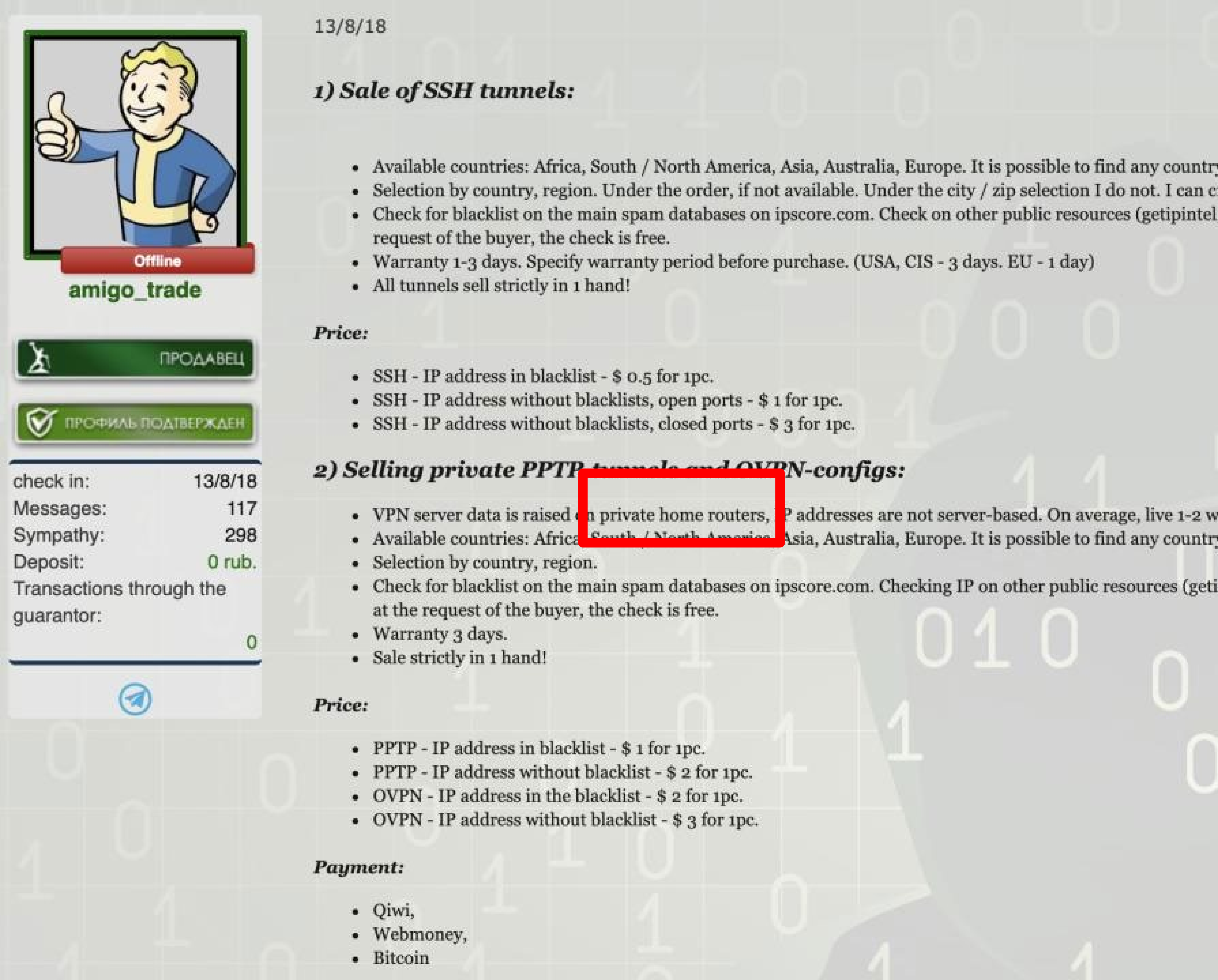
Кол-во: 6 Купить

spycamhome.deer.io/ru/

*проверка камер на валидность: 19.03.2018 17:13 (мск)*

| | |
|---|---|
| Все | 114 |
| бная) | 1 |
| | 49 |
| | 11 |
| | 38 |
| | 8 |
| анная | 1 |

R



amigo_trade

| | |
|---|---|
| check in: | 13/8/18 |
| Messages: | 117 |
| Sympathy: | 298 |
| Deposit: | 0 rub. |
| Transactions through the guarantor: | 0 |

13/8/18

***1) Sale of SSH tunnels:***

- Available countries: Africa, South / North America, Asia, Australia, Europe. It is possible to find any country
- Selection by country, region. Under the order, if not available. Under the city / zip selection I do not. I can c
- Check for blacklist on the main spam databases on ipscore.com. Check on other public resources (getipintel request of the buyer, the check is free.
- Warranty 1-3 days. Specify warranty period before purchase. (USA, CIS - 3 days. EU - 1 day)
- All tunnels sell strictly in 1 hand!

***Price:***

- SSH - IP address in blacklist - $ 0.5 for 1pc.
- SSH - IP address without blacklists, open ports - $ 1 for 1pc.
- SSH - IP address without blacklists, closed ports - $ 3 for 1pc.

***2) Selling private PPTP tunnels and OVPN-configs:***

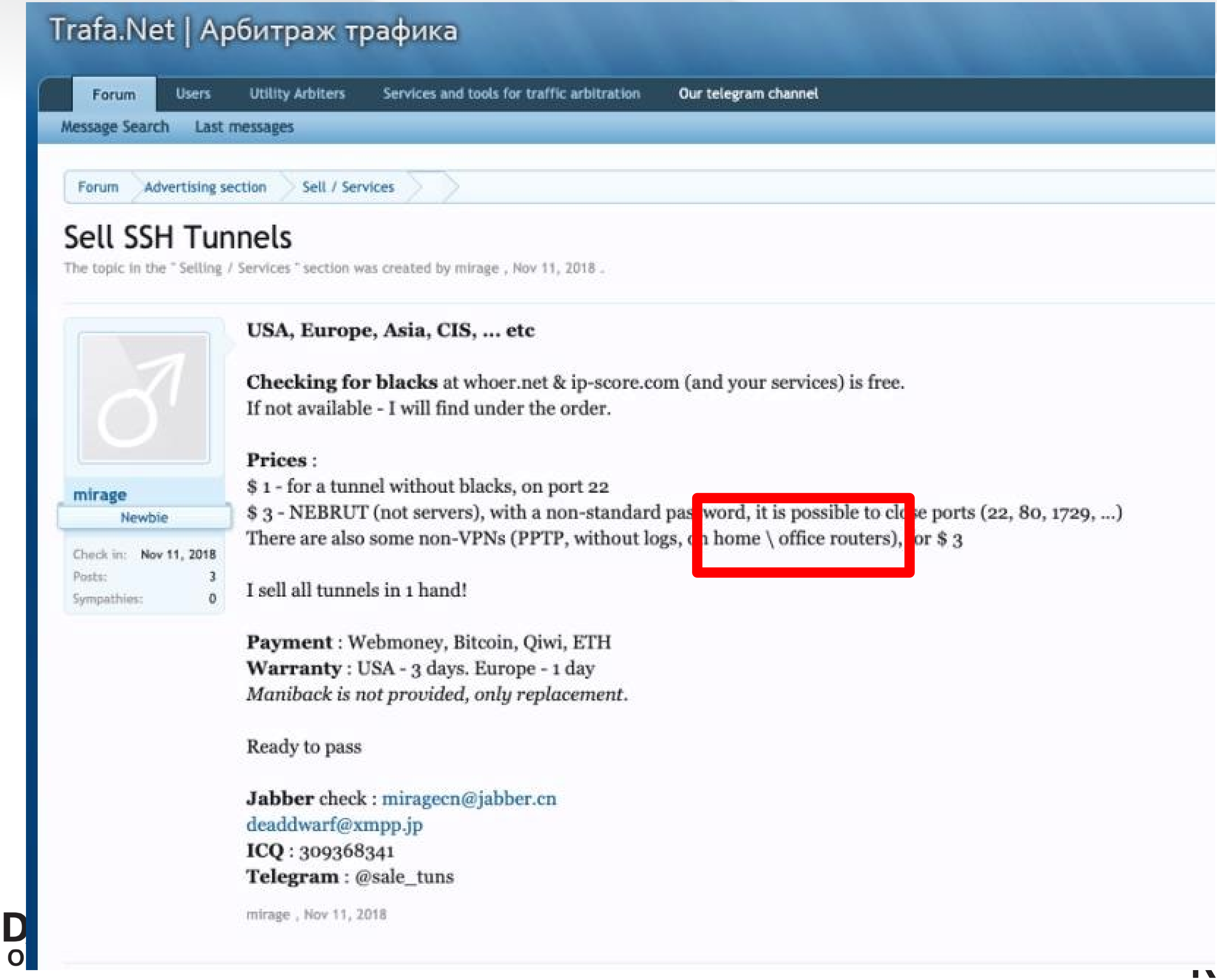
- VPN server data is raised on private home routers, IP addresses are not server-based. On average, live 1-2 w
- Available countries: Africa, South / North America, Asia, Australia, Europe. It is possible to find any country
- Selection by country, region.
- Check for blacklist on the main spam databases on ipscore.com. Checking IP on other public resources (geti at the request of the buyer, the check is free.
- Warranty 3 days.
- Sale strictly in 1 hand!

***Price:***

- PPTP - IP address in blacklist - $ 1 for 1pc.
- PPTP - IP address without blacklist - $ 2 for 1pc.
- OVPN - IP address in the blacklist - $ 2 for 1pc.
- OVPN - IP address without blacklist - $ 3 for 1pc.

***Payment:***

- Qiwi,
- Webmoney,
- Bitcoin



# Sell SSH Tunnels

The topic in the " Selling / Services " section was created by mirage , Nov 11, 2018 .

**USA, Europe, Asia, CIS, ... etc**

**Checking for blacks** at whoer.net & ip-score.com (and your services) is free.
If not available - I will find under the order.

**Prices** :
$ 1 - for a tunnel without blacks, on port 22
$ 3 - NEBRUT (not servers), with a non-standard password, it is possible to close ports (22, 80, 1729, ...)
There are also some non-VPNs (PPTP, without logs, on home \ office routers), for $ 3

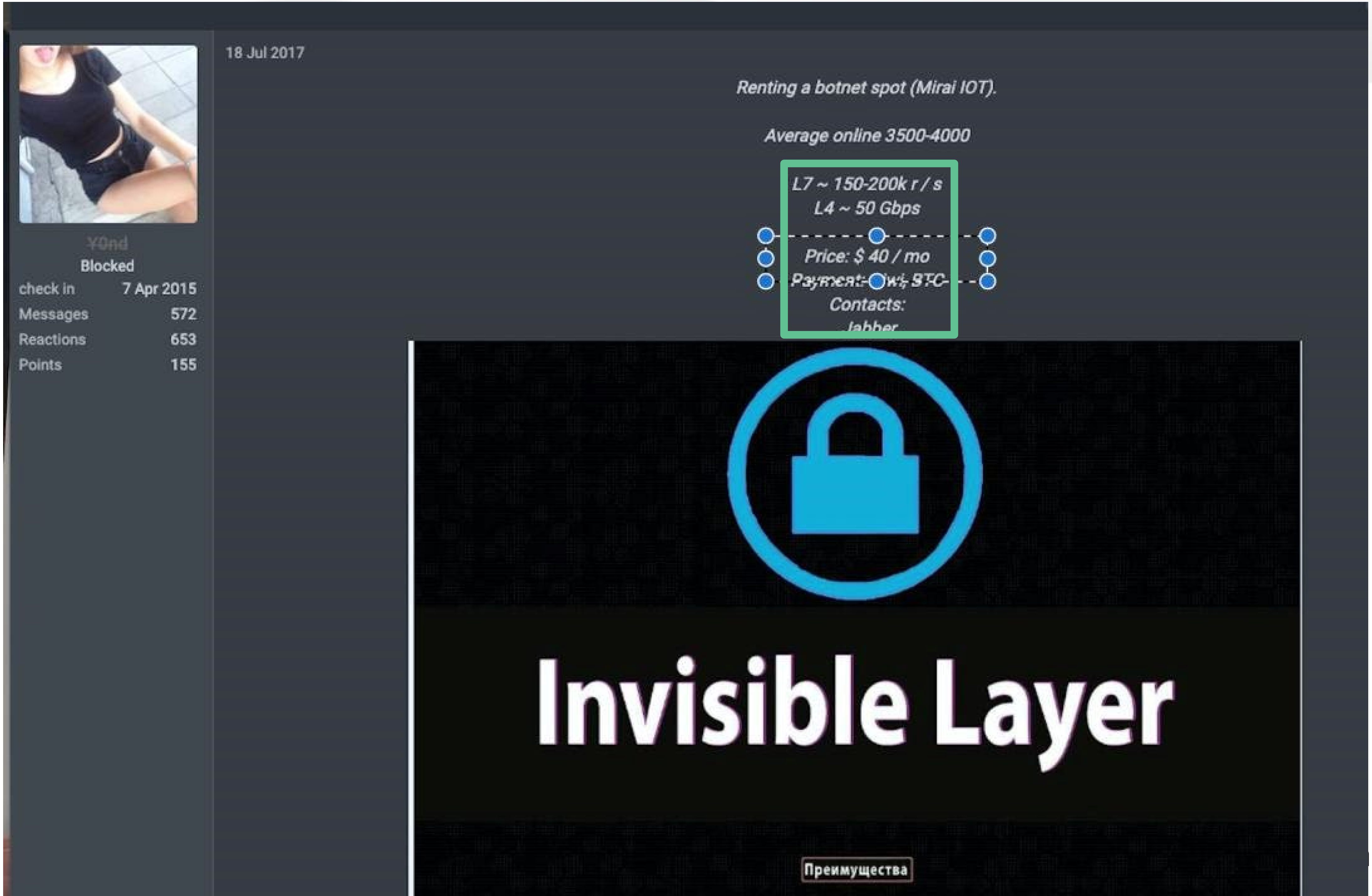
I sell all tunnels in 1 hand!

**Payment** : Webmoney, Bitcoin, Qiwi, ETH
**Warranty** : USA - 3 days. Europe - 1 day
*Maniback is not provided, only replacement.*

Ready to pass

**Jabber** check : miragecn@jabber.cn
deaddwarf@xmpp.jp
**ICQ** : 309368341
**Telegram** : @sale_tuns

mirage , Nov 11, 2018



| | |
|---|---|
| ~~Y0nd~~ | |
| Blocked | |
| check in | 7 Apr 2015 |
| Messages | 572 |
| Reactions | 653 |
| Points | 155 |

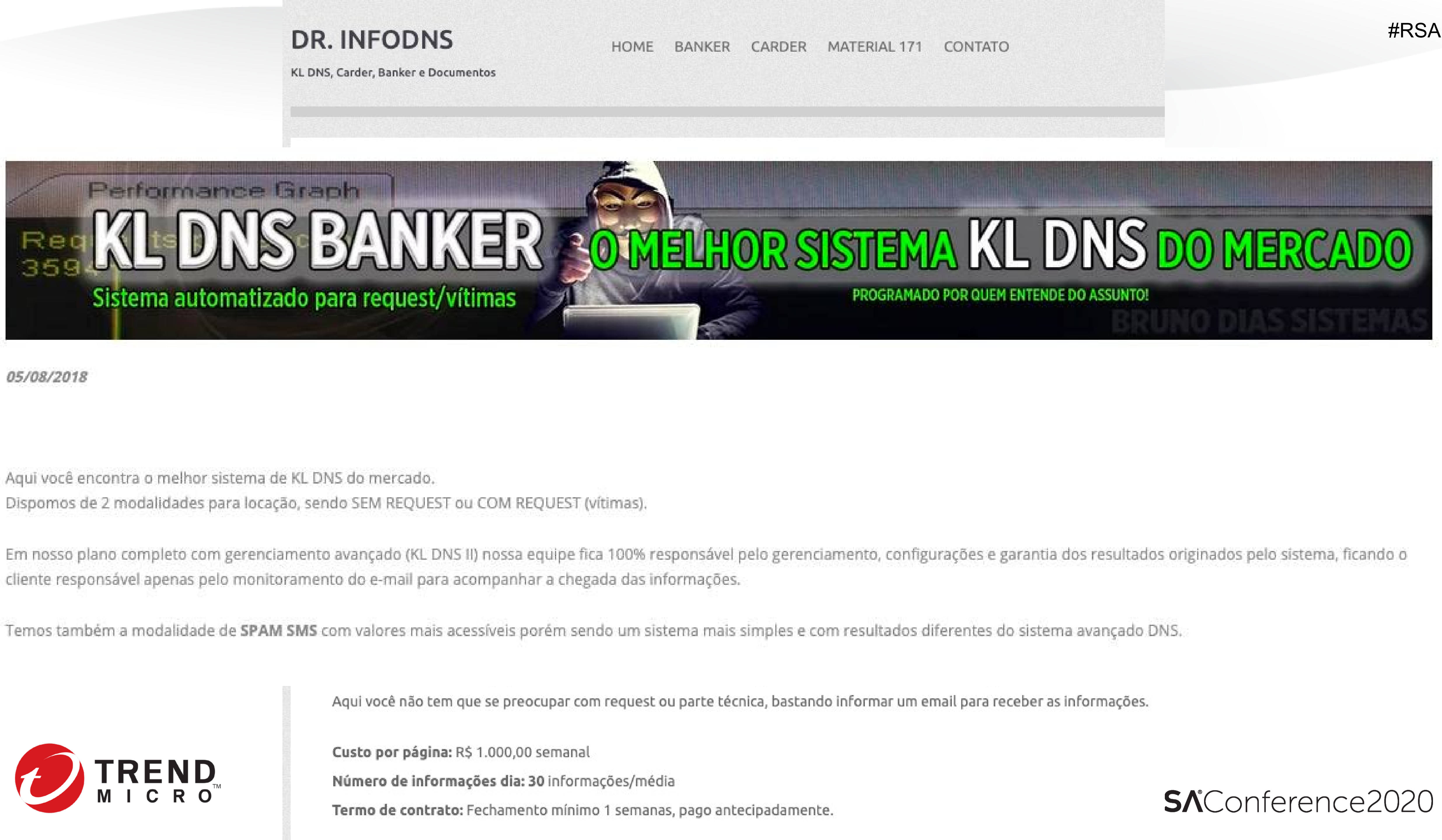
18 Jul 2017

*Renting a botnet spot (Mirai IOT).*

*Average online 3500-4000*

*L7 ~ 150-200k r / s*
*L4 ~ 50 Gbps*

*Price: $ 40 / mo*
*Payment: Qiwi, BTC*
*Contacts:*
*Jabber*



DR. INFODNS

KL DNS, Carder, Banker e Documentos

HOME
BANKER
CARDER
MATERIAL 171
CONTATO
Performance Graph
KL DNS BANKER
Sistema automatizado para request/vítimas
O MELHOR SISTEMA KL DNS DO MERCADO
PROGRAMADO POR QUEM ENTENDE DO ASSUNTO!
BRUNO DIAS SISTEMAS

*05/08/2018*

Aqui você encontra o melhor sistema de KL DNS do mercado.
Dispomos de 2 modalidades para locação, sendo SEM REQUEST ou COM REQUEST (vítimas).

Em nosso plano completo com gerenciamento avançado (KL DNS II) nossa equipe fica 100% responsável pelo gerenciamento, configurações e garantia dos resultados originados pelo sistema, ficando o cliente responsável apenas pelo monitoramento do e-mail para acompanhar a chegada das informações.

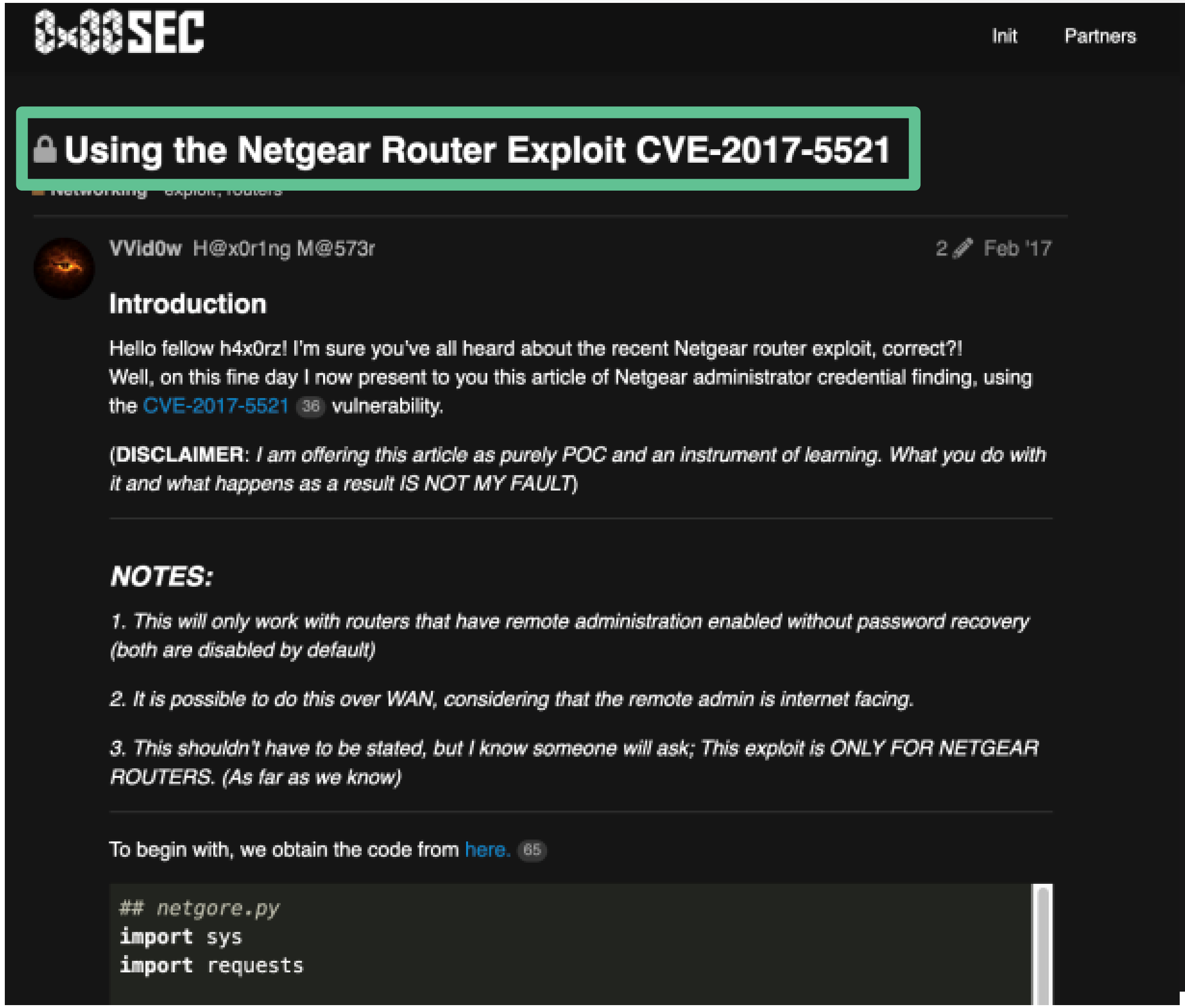
Temos também a modalidade de **SPAM SMS** com valores mais acessíveis porém sendo um sistema mais simples e com resultados diferentes do sistema avançado DNS.

Aqui você não tem que se preocupar com request ou parte técnica, bastando informar um email para receber as informações.

**Custo por página:** R$ 1.000,00 semanal

**Número de informações dia: 30** informações/média

**Termo de contrato:** Fechamento mínimo 1 semanas, pago antecipadamente.



0x00SEC Init Partners

## Using the Netgear Router Exploit CVE-2017-5521

Networking exploit, routers

VVid0w H@x0r1ng M@573r 2 Feb '17

### Introduction

Hello fellow h4x0rz! I'm sure you've all heard about the recent Netgear router exploit, correct?!
Well, on this fine day I now present to you this article of Netgear administrator credential finding, using the CVE-2017-5521 36 vulnerability.

(**DISCLAIMER**: *I am offering this article as purely POC and an instrument of learning. What you do with it and what happens as a result IS NOT MY FAULT*)

### *NOTES:*

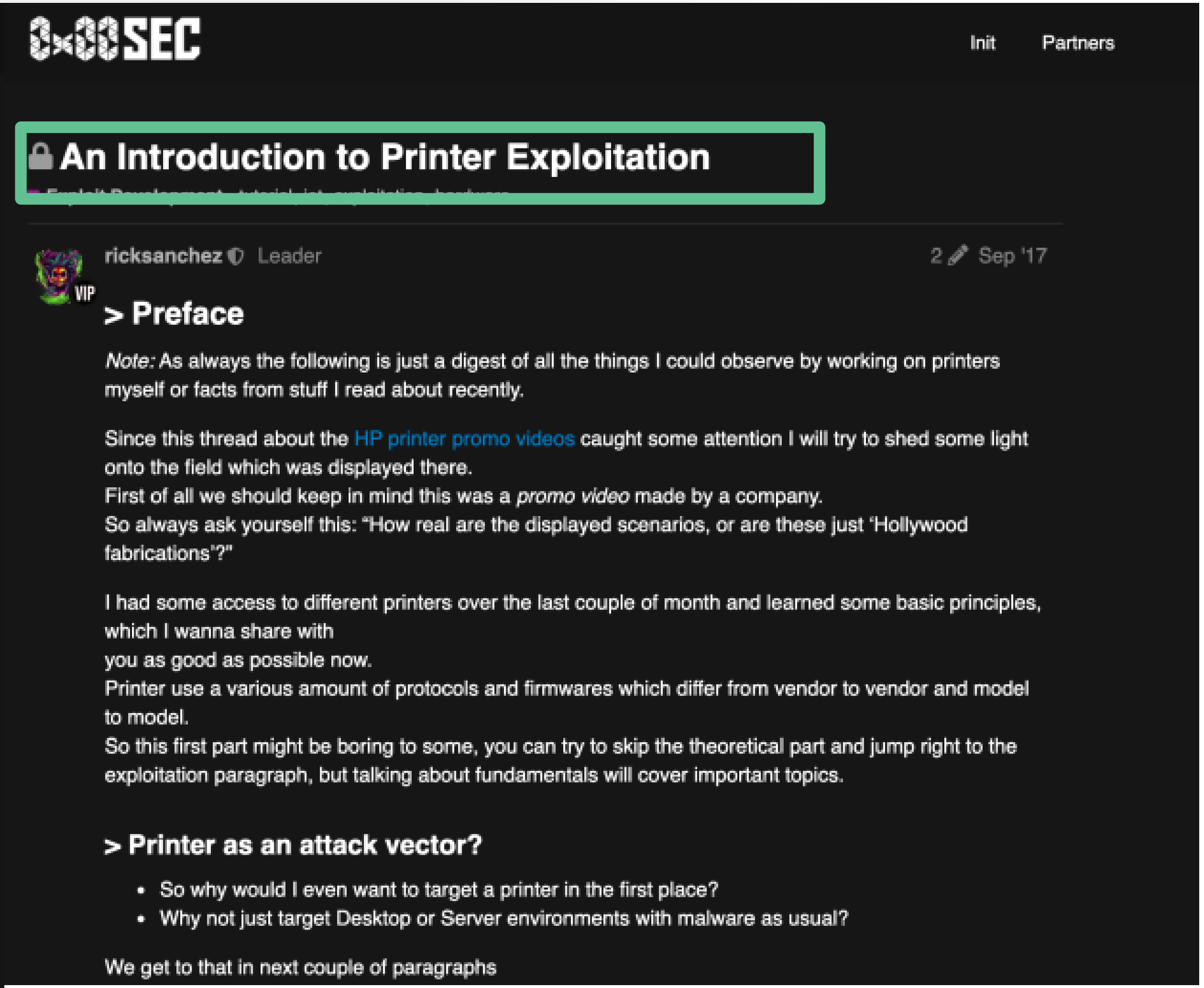
*1. This will only work with routers that have remote administration enabled without password recovery (both are disabled by default)*

*2. It is possible to do this over WAN, considering that the remote admin is internet facing.*

*3. This shouldn't have to be stated, but I know someone will ask; This exploit is ONLY FOR NETGEAR ROUTERS. (As far as we know)*

To begin with, we obtain the code from here. 65

```
## netgore.py
import sys
import requests
```



0x00SEC Init Partners

## An Introduction to Printer Exploitation

Exploit Development tutorial, iot, exploitation, hardware

ricksanchez Leader VIP 2 Sep '17

### > Preface

*Note:* As always the following is just a digest of all the things I could observe by working on printers myself or facts from stuff I read about recently.

Since this thread about the HP printer promo videos caught some attention I will try to shed some light onto the field which was displayed there.
First of all we should keep in mind this was a *promo video* made by a company.
So always ask yourself this: "How real are the displayed scenarios, or are these just 'Hollywood fabrications'?"

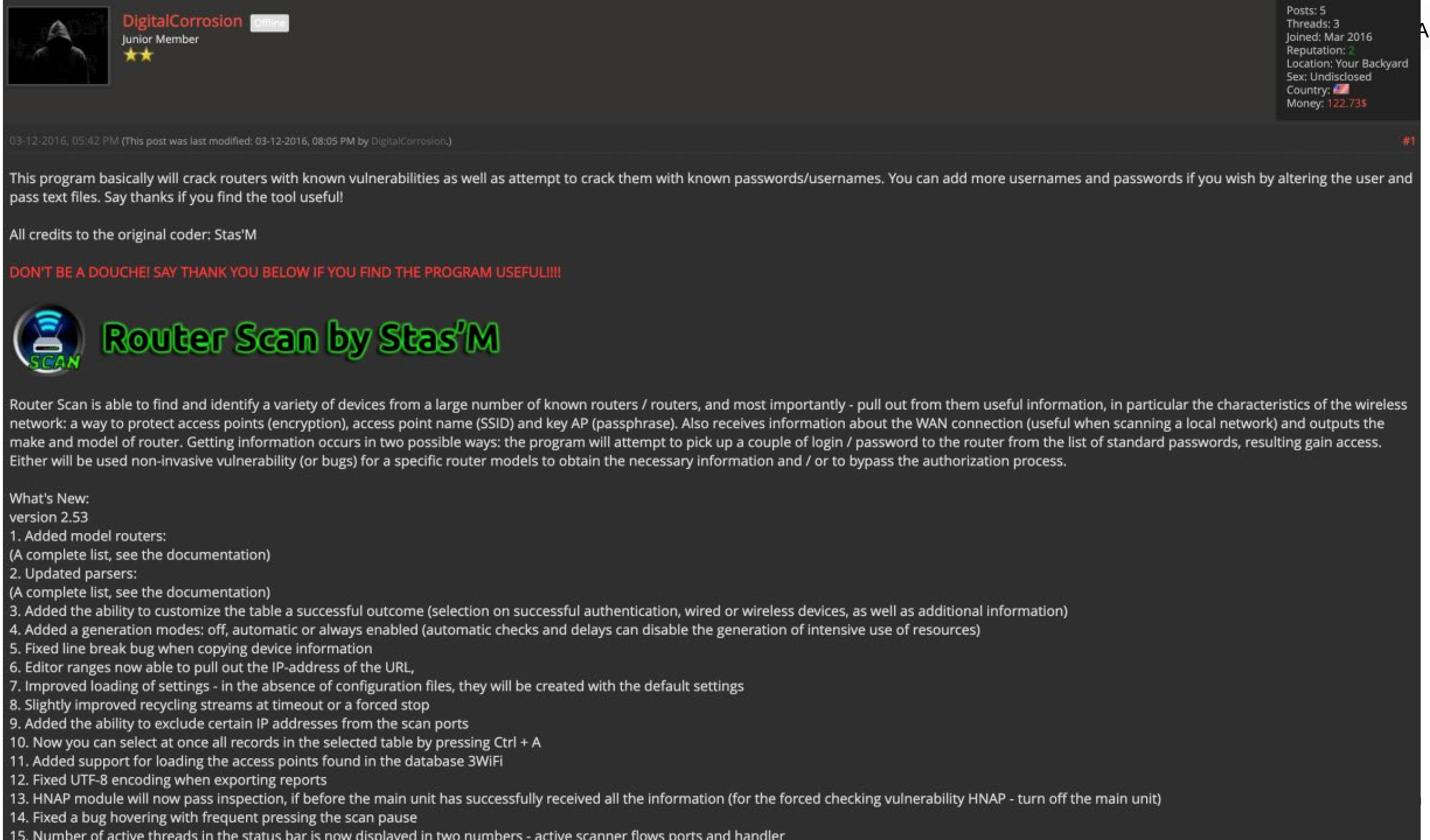
I had some access to different printers over the last couple of month and learned some basic principles, which I wanna share with
you as good as possible now.
Printer use a various amount of protocols and firmwares which differ from vendor to vendor and model to model.
So this first part might be boring to some, you can try to skip the theoretical part and jump right to the exploitation paragraph, but talking about fundamentals will cover important topics.

### > Printer as an attack vector?

- So why would I even want to target a printer in the first place?
- Why not just target Desktop or Server environments with malware as usual?

We get to that in next couple of paragraphs

AC



DigitalCorrosion Offline
Junior Member
★★

Posts: 5
Threads: 3
Joined: Mar 2016
Reputation: 2
Location: Your Backyard
Sex: Undisclosed
Country:
Money: 122.73$

03-12-2016, 05:42 PM (This post was last modified: 03-12-2016, 08:05 PM by DigitalCorrosion.) #1

This program basically will crack routers with known vulnerabilities as well as attempt to crack them with known passwords/usernames. You can add more usernames and passwords if you wish by altering the user and pass text files. Say thanks if you find the tool useful!

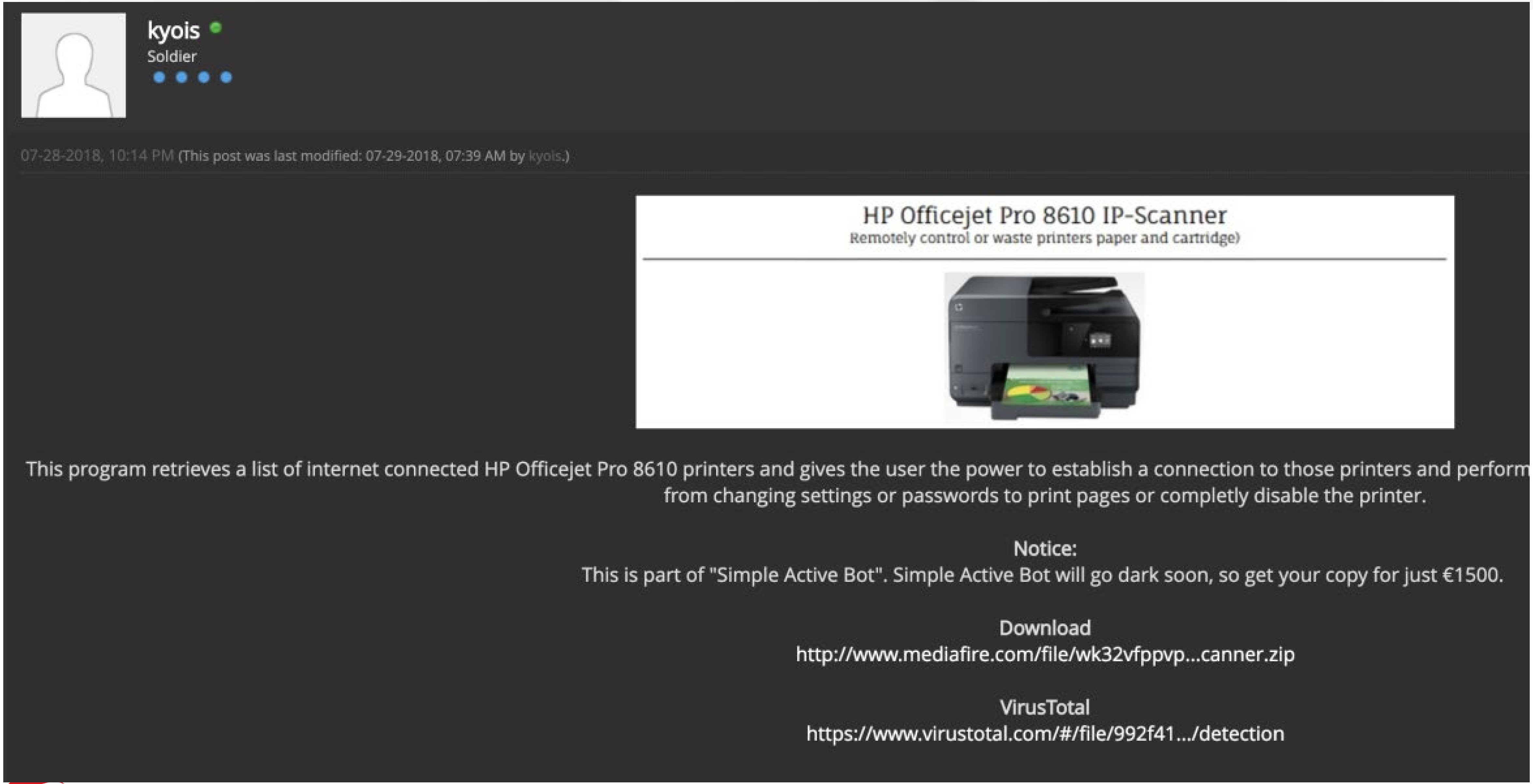
All credits to the original coder: Stas'M

DON'T BE A DOUCHE! SAY THANK YOU BELOW IF YOU FIND THE PROGRAM USEFUL!!!!

SCAN Router Scan by Stas'M

Router Scan is able to find and identify a variety of devices from a large number of known routers / routers, and most importantly - pull out from them useful information, in particular the characteristics of the wireless network: a way to protect access points (encryption), access point name (SSID) and key AP (passphrase). Also receives information about the WAN connection (useful when scanning a local network) and outputs the make and model of router. Getting information occurs in two possible ways: the program will attempt to pick up a couple of login / password to the router from the list of standard passwords, resulting gain access. Either will be used non-invasive vulnerability (or bugs) for a specific router models to obtain the necessary information and / or to bypass the authorization process.

What's New:
version 2.53
1. Added model routers:
(A complete list, see the documentation)
2. Updated parsers:
(A complete list, see the documentation)
3. Added the ability to customize the table a successful outcome (selection on successful authentication, wired or wireless devices, as well as additional information)
4. Added a generation modes: off, automatic or always enabled (automatic checks and delays can disable the generation of intensive use of resources)
5. Fixed line break bug when copying device information
6. Editor ranges now able to pull out the IP-address of the URL,
7. Improved loading of settings - in the absence of configuration files, they will be created with the default settings
8. Slightly improved recycling streams at timeout or a forced stop
9. Added the ability to exclude certain IP addresses from the scan ports
10. Now you can select at once all records in the selected table by pressing Ctrl + A
11. Added support for loading the access points found in the database 3WiFi
12. Fixed UTF-8 encoding when exporting reports
13. HNAP module will now pass inspection, if before the main unit has successfully received all the information (for the forced checking vulnerability HNAP - turn off the main unit)
14. Fixed a bug hovering with frequent pressing the scan pause
15. Number of active threads in the status bar is now displayed in two numbers - active scanner flows ports and handler



kyois
Soldier

07-28-2018, 10:14 PM (This post was last modified: 07-29-2018, 07:39 AM by kyois.)

HP Officejet Pro 8610 IP-Scanner
Remotely control or waste printers paper and cartridge)

This program retrieves a list of internet connected HP Officejet Pro 8610 printers and gives the user the power to establish a connection to those printers and perform
from changing settings or passwords to print pages or completly disable the printer.

Notice:
This is part of "Simple Active Bot". Simple Active Bot will go dark soon, so get your copy for just €1500.

Download
http://www.mediafire.com/file/wk32vfppvp...canner.zip

VirusTotal
https://www.virustotal.com/#/file/992f41.../detection

uestas 👁1813 Vistas

s y 1 Visitante están viendo este tema.

Rootkit_Pentester

Underc0der

Mensajes: 212

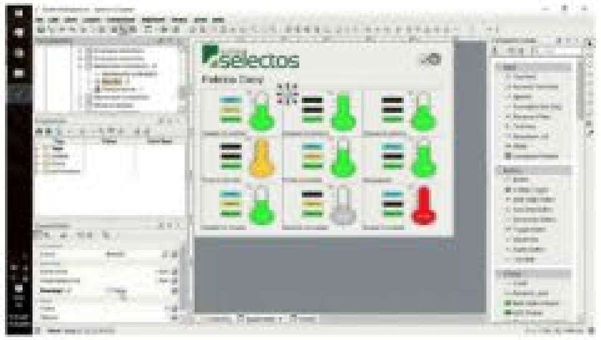
Actividad:
3.33%

Reputación 6

Hacking de Sistemas de

« en: Marzo 23, 2018, 11:05:55 pm »

Hola gente en este post, les comentare como acceder a sistemas scada de refrigeración sin pass }:)



Buscar en google este dork }:)
Dork: inurl:/cgi-bin/cgi.cgi?Cont=
Hay como 3200 sistemas xD.

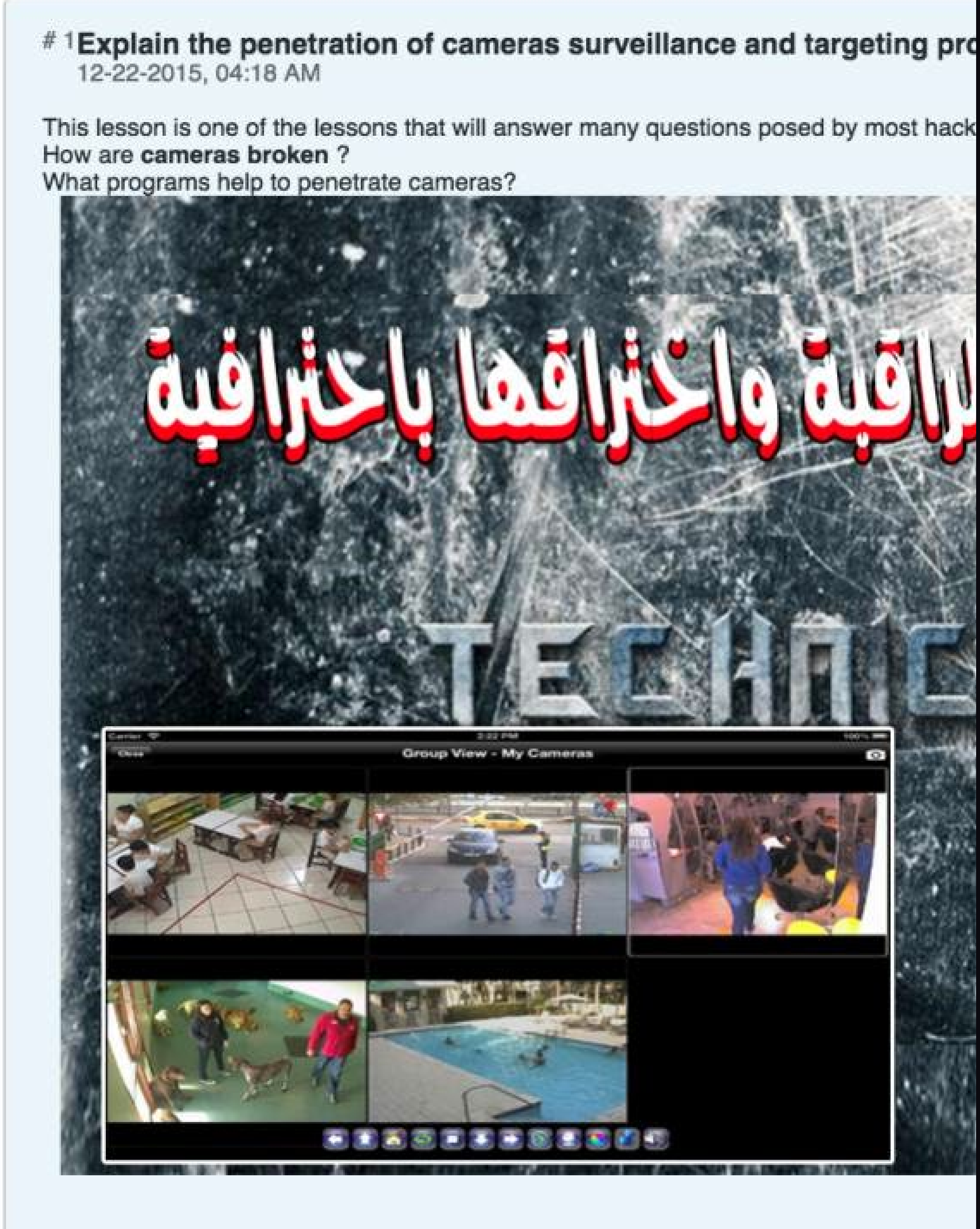
Espero que les haya gustado y sus comentarios.
Saludos Rootkit.

Drok3r

Re:Hacking de Sistemas d

« Respuesta #1 en: Marzo 24, 2018, 11:18:01 pm »

Muy bueno en verdad...



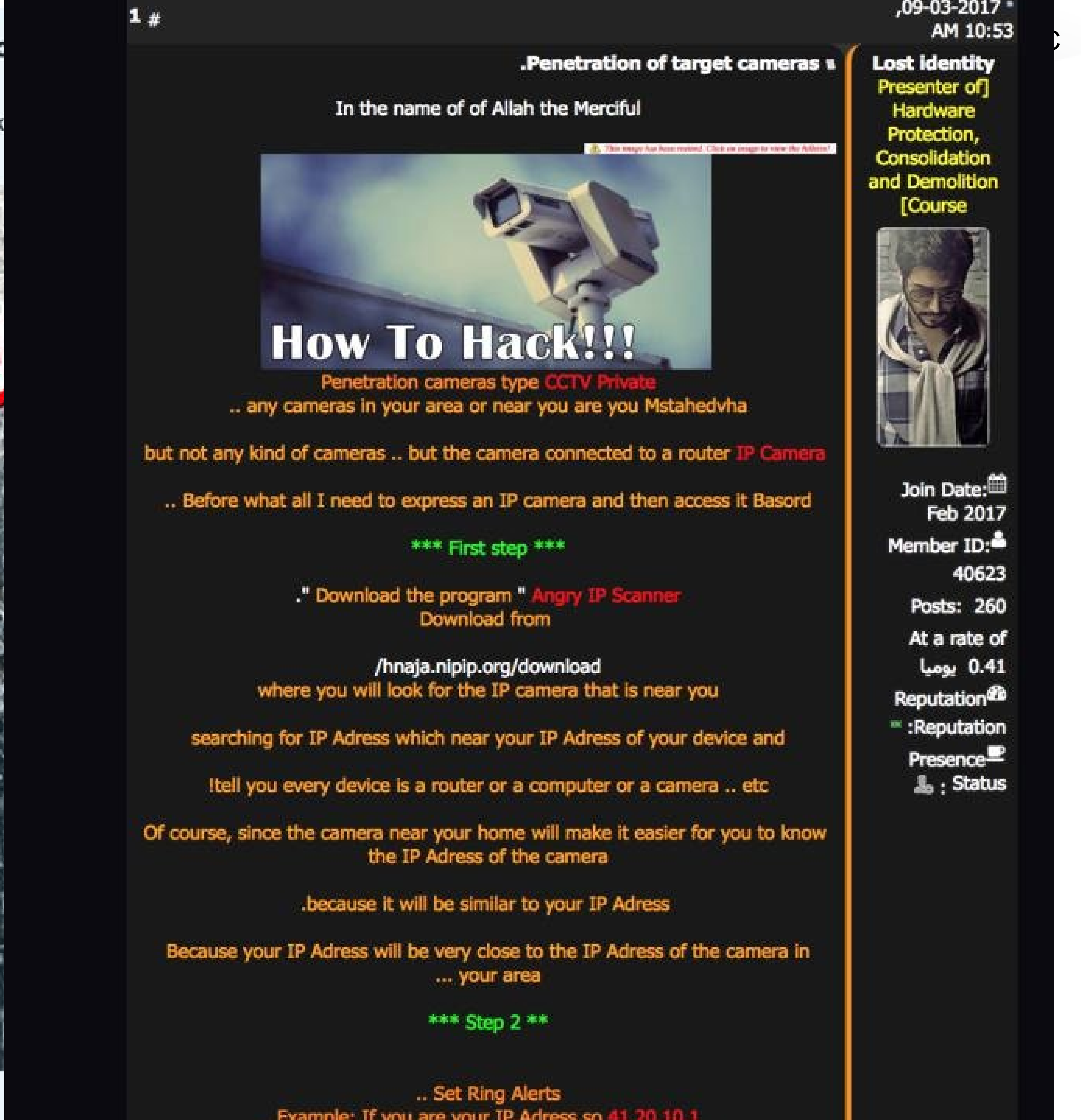
# 1 **Explain the penetration of cameras surveillance and targeting pro**

12-22-2015, 04:18 AM

This lesson is one of the lessons that will answer many questions posed by most hack

How are **cameras broken** ?

What programs help to penetrate cameras?



1 #

,09-03-2017
AM 10:53

**.Penetration of target cameras**

In the name of of Allah the Merciful

This image has been resized. Click on image to view the fullsize!

Penetration cameras type CCTV Private

.. any cameras in your area or near you are you Mstahedvha

but not any kind of cameras .. but the camera connected to a router IP Camera

.. Before what all I need to express an IP camera and then access it Basord

*** First step ***

." Download the program " Angry IP Scanner
Download from

/hnaja.nipip.org/download
where you will look for the IP camera that is near you

searching for IP Adress which near your IP Adress of your device and

!tell you every device is a router or a computer or a camera .. etc

Of course, since the camera near your home will make it easier for you to know the IP Adress of the camera

.because it will be similar to your IP Adress

Because your IP Adress will be very close to the IP Adress of the camera in ... your area

*** Step 2 **

.. Set Ring Alerts
Example: If you are your IP Adress so 41.20.10.1

**Lost identity**
Presenter of]
Hardware
Protection,
Consolidation
and Demolition
[Course

Join Date:
Feb 2017

Member ID:
40623

Posts: 260

At a rate of
0.41 يوميا

Reputation

:Reputation

Presence

: Status

SECURITY

# Apply this knowledge

- Your routers and other devices **can** and **will be** attacked: ACTION ITEM: Start devising a plan to protect them.