

Internet das Coisas IoT

*a inovação e
a segurança.*

GTS 24

São Paulo

28 de novembro de 2014

Leandro Bennaton

 @bennaton

elevenpaths.com



A *Telefónica* COMPANY

Leandro Bennaton



Executivo de Segurança do Grupo Telefónica:

- Chief Security Officer responsável Global por Segurança e Conformidade no **TERRA**
- Chief Security Ambassador na **ELEVEN PATHS**
- Security Mentor na **WAYRA**
- Professor Pós Graduação na **FIAP**



Pós graduado, com MBA em Gerenciamento de Segurança da Informação e certificações internacionais. Participa do *Information Security Forum* e ativamente no Comitê Gestor da Internet.

Premiado pelo 2º ano consecutivo como o melhor executivo de Segurança pela organização Security Leaders.

 @bennaton

Leandro Bennaton

Alguns dos últimos Projetos:



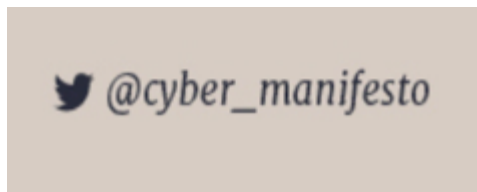
- **SINFONIER**, uma solução *open source* de Apache Storm para cyber security <http://sinfonier-project.net>



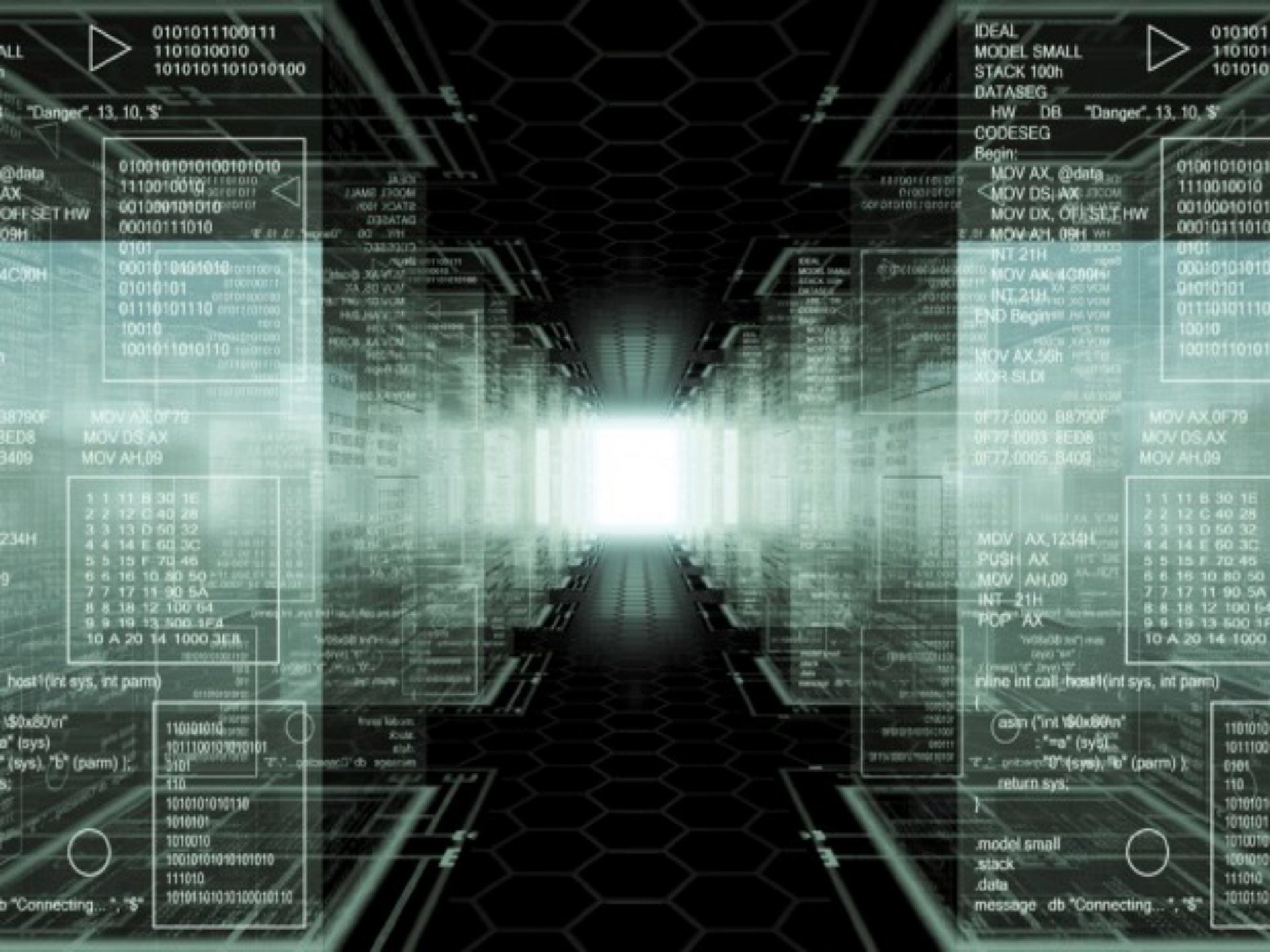
- **THE ANALOGIES PROJECT**, disseminar o conhecimento segurança da informação através de analogias <https://theanalogiesproject.org/>



- **H2HC MAGAZINE**, revista com conteúdo técnico de segurança e hacking <https://www.h2hc.com.br/revista/>



- **CYBER MANIFESTO**, como proteger melhor o Brasil de ataques cibernético <http://www.cyber-manifesto.org>



0101011100111
1101010010
1010101101010100

IDEAL
MODEL SMALL
STACK 100h
DATASEG
HW DB "Danger", 13, 10, '\$'
CODESEG

"Danger", 13, 10, '\$'

"Danger", 13, 10, '\$'

```
0100101010100101010
1110010010
001000101010
00010111010
0101
0001010101010
01010101
01110101110
10010
1001011010110
```

```
0100101010
1110010010
00100010101
00010111010
0101
00010101010
01010101
01110101110
10010
10010110101
```

```
MOV AX,0F7H
MOV DS,AX
MOV AH,09
```

```
MOV AX,0F7H
MOV DS,AX
MOV AH,09
```

```
1 1 11 B 30 1E
2 2 12 C 40 28
3 3 13 D 50 32
4 4 14 E 60 3C
5 5 15 F 70 46
6 6 16 10 80 50
7 7 17 11 90 5A
8 8 18 12 100 64
9 9 19 13 500 124
10 A 20 14 1000 3EB
```

```
1 1 11 B 30 1E
2 2 12 C 40 28
3 3 13 D 50 32
4 4 14 E 60 3C
5 5 15 F 70 46
6 6 16 10 80 50
7 7 17 11 90 5A
8 8 18 12 100 64
9 9 19 13 500 124
10 A 20 14 1000
```

```
MOV AX,1234H
PUSH AX
MOV AH,09
INT 21H
PCP AX
```

```
inline int call_host1(int sys, int parm)
{
    asm ("int %0\n"
        : "=a" (sys)
        : "0" (sys), "b" (parm) );
    return sys;
}
```

```
.model small
.stack
.data
message db "Connecting...", '$'
```

```
110101010
101110010101010101
1101
110
1010101010110
1010101
1010010
10010101010101010
111010
10101101010100010110
```

```
1101010
1011100
0101
110
1010101
1010101
1010010
1001010
111010
1010110
```

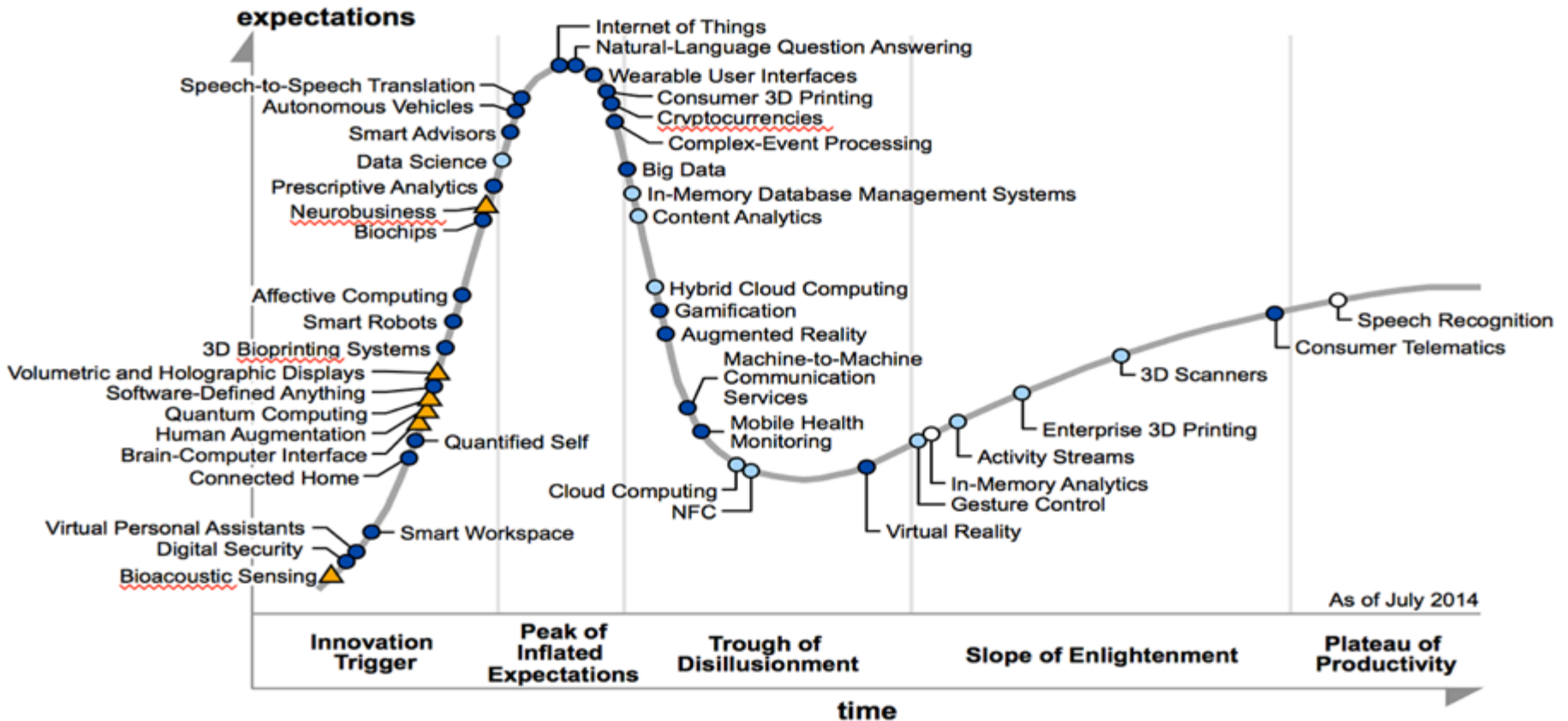
38790F
BED8
B409

234H

host1(int sys, int parm)

"Connecting...", '\$'

IoT no topo do HypeCycle



Plateau will be reached in:

○ less than 2 years

○ 2 to 5 years

● 5 to 10 years

▲ more than 10 years

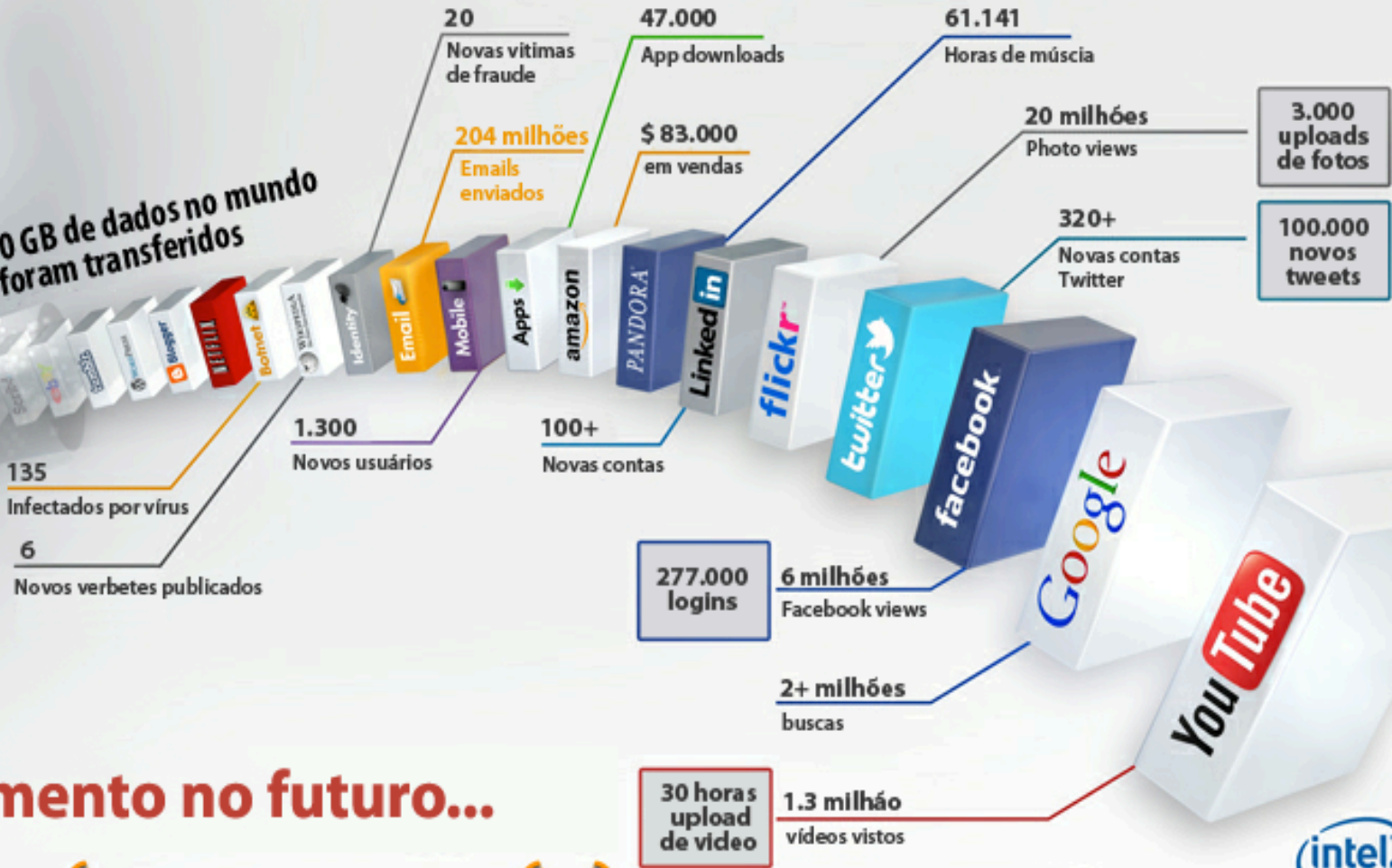
⊗ obsolete before plateau



O que acontece em Um minuto na internet?



639.800 GB de dados no mundo foram transferidos



E o crescimento no futuro...

Hoje, o número de devices conectados

=



Em 2015, o número de devices conectados

= 2x



Em 2015, você levaria 5 anos



para ver todo vídeo produzido no mundo em 1 segundo





Por que tudo é hackeado? ...

The image is a composite. On the left, a portion of the YouTube website is visible, showing the logo, a search bar with the text 'como hackear', and a list of suggestions: 'como hackear una cuenta de facebook', 'como hackear un facebook', 'como hackear wifi', and 'como hackear facebook'. Below the search bar is a 'What to Watch' section with 'BEST OF YOUTUBE' and categories like 'Popular on YouTube', 'Music', and 'Sports'. On the right, a hand holds a piece of paper with the following text written on it: 'IF "Plan A" Didn't Work. The alphabet has 25 more letters! Stay Cool.' The background of the paper is a light greenish-grey.

YouTube^{AR}

Ver YouTube en Español

What to Watch

BEST OF YOUTUBE

- Popular on YouTube
- Music
- Sports

como hackear

- como hackear una cuenta de facebook
- como hackear un facebook
- como hackear wifi
- como hackear facebook

IF "Plan A"
Didn't Work.
The alphabet has
25 more letters!
Stay Cool.

... cambiar la contraseña

... programas

Defacement de sites ...



THE

BUG

IS OUT THERE

Vazamento de informações ...

Daily Report: Hackers' Attack on JPMorgan Affects 76 Million Households

By THE NEW YORK TIMES

The disclosure by the bank dwarfs earlier estimates that attackers had gained access to roughly one million customer accounts.

October 3, 2014, Friday

3 hours ago | The Wall Street Journal

J.P. Morgan Data Breach Draws Scrutiny From States

Big data breach: 360 million newly stolen credentials for sale

NBC News With Reuters

Wednesday, 26 Feb 2014 | 10:47 AM ET

 **NBC NEWS**



The Cybercrime Economy

Russian criminals steal 1.2 billion passwords

By James O'Toole and Jose Pagliery @CNNTech August 6, 2014: 6:56 AM ET

 Recommend 210



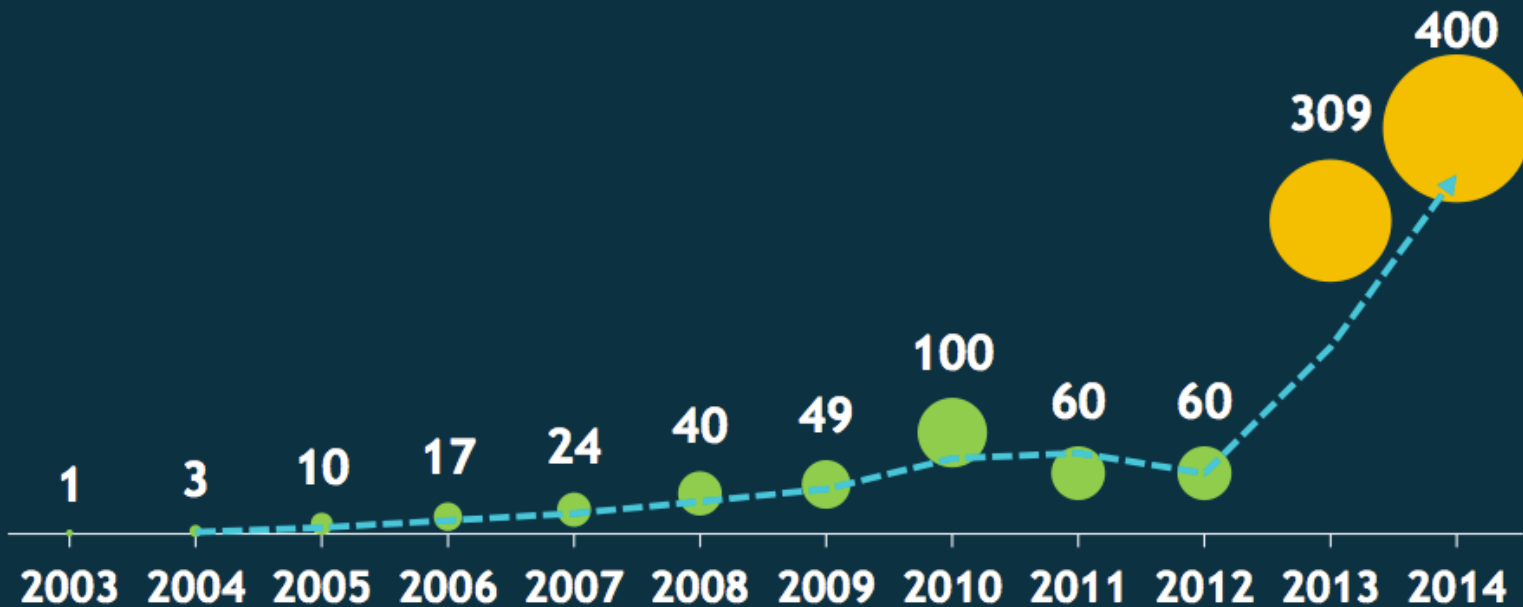
Russian hackers know your password

Target data hack affected 70 million people

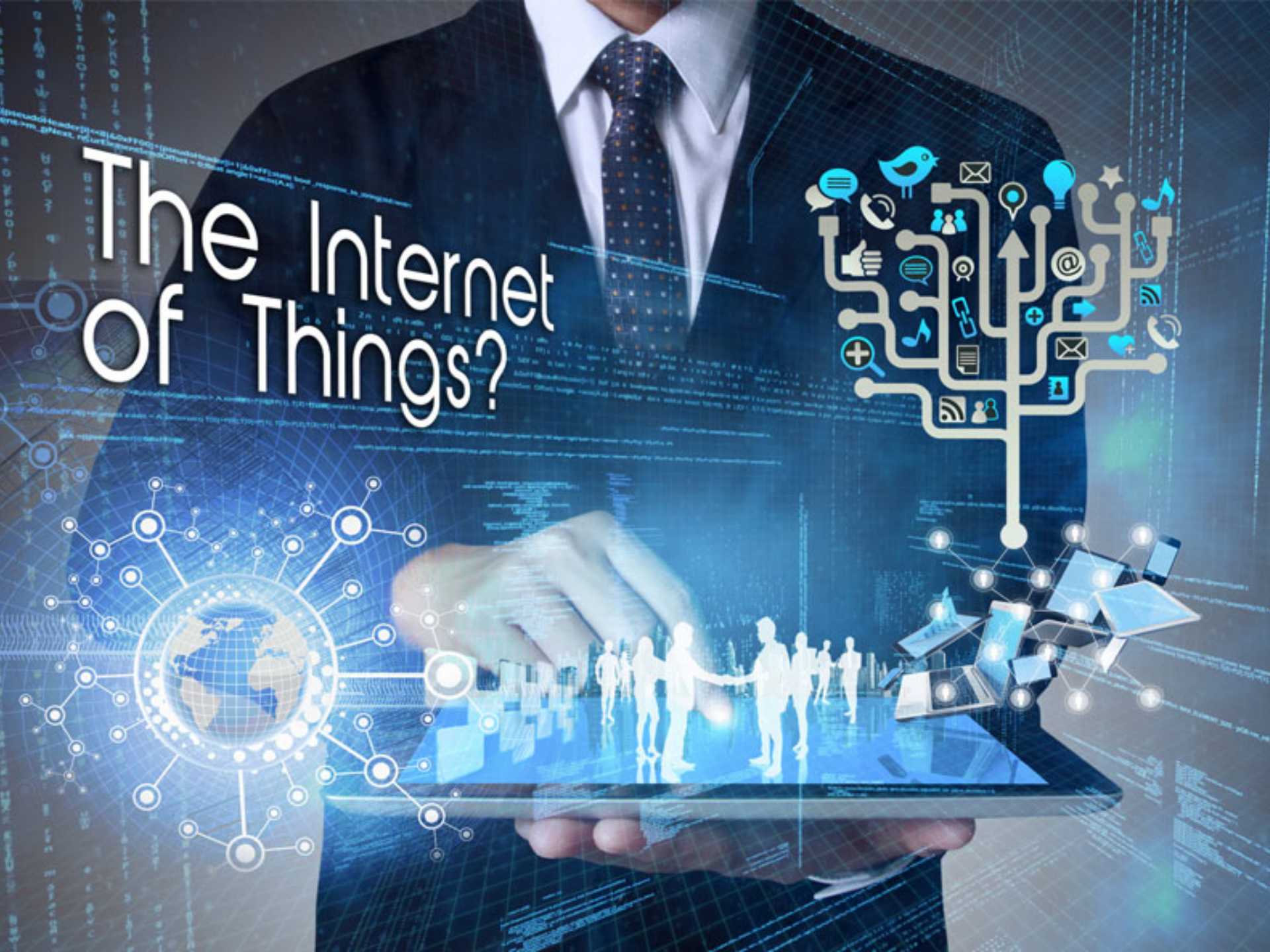
Stock drops as retailer reveals more customers affected and names and addresses leaked

CBC News | Posted: Jan 10, 2014 9:26 AM ET | Last Updated: Jan 10, 2014 8:41 PM ET

Ataques DDoS – Timeline ...



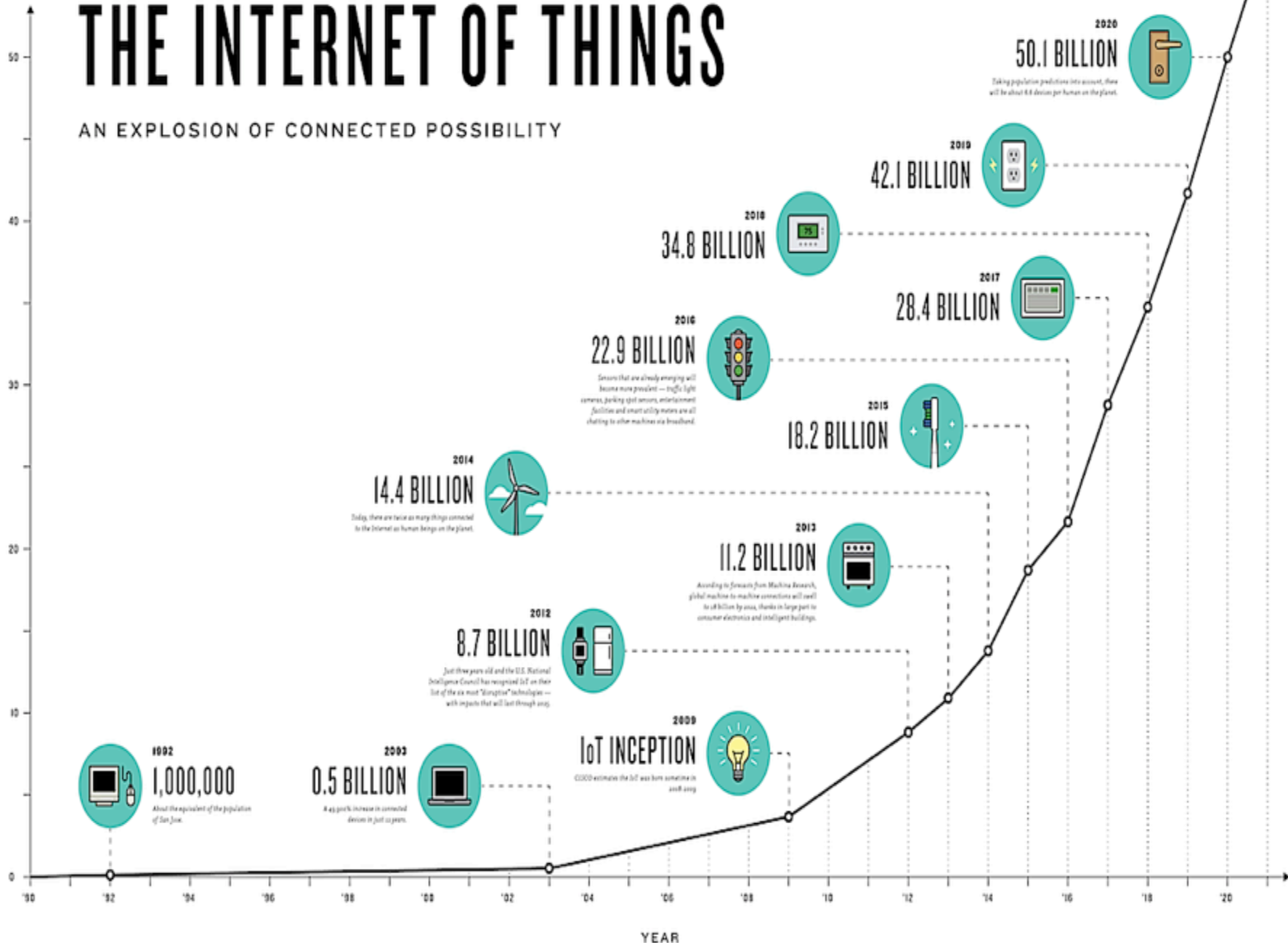
The Internet Of Things?



THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY

BILLIONS OF DEVICES



Blood Pressure Monitor

Simply slip on the cuff, turn on the Wireless Blood Pressure Monitor and the Health Mate app will automatically launch.



<http://www.withings.com/us/blood-pressure-monitor.html>

Smart Weather Station

The Netatmo Weather Station allows you to use indoor temperature, relative humidity and CO2 readings to live in a healthier home.



<http://www.netatmo.com/en-US/product/weather-station/>

Smart Slow Cooker

Enjoy remote access to all your slow cooker's functions, no matter where you are.



<http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/>

MyVessyl Cup

It can hold 13 ounces of liquid. The battery takes 60 minutes to fully charge and will last for 5-7 days. Also has wire-free charging.



<https://www.myvessyl.com/>

INTERNET OF THINGS LANDSCAPE

Platforms & Enablement (Horizontal)

Connectivity FTTT, Symplo, ioBridge, ARRAYENT, haystack, electric imp, ThingWorx, sensinode, N NODE, bugswarm	Open Source Platforms sense, spark, Nimbits, ThingSpeak	Software Platforms sense, SmartThings, Withings, NINJABLOCKS, xively, TWINE, OSITO, zonoff	Sensor Networks MESHSYSTEMS, SAFECAST	Enabling Networks FreedomPop, SocialSign.in, Open Garden, SIGFOX	Corporates IBM, LG, CISCO, Honeywell
---	---	--	---	--	--

Applications (Verticals)

Quantified Self Wearable Computing: GLASS, Pebble Fitness: FUEL, amiigo, Withings, fitbit, JAWBONE Health: BASIS, LUMO, HAPIfork, wahoo, NuMetrex Family: REST, Lively, Good Night Lamp, Withings, EVADO FILIP	Lifestyle Leisure: blossom, ICA kitchen, Thimble, remee, iGrill, HEXBRIGHT, sobi Pets: gibi, FITBARK Toys: sifteo, MakieLab, KAROTZ, greengoose Music: gitar Gardening: BITPONICS, plantlink, Koubachi Home Improv.: Radiator Labs, netatmo	Connected Home Home Automation: SmartThings, NINJABLOCKS, revolv, Ubi, lapka, Wovyn, electric imp, N NODE Energy Efficiency: knut, nest, tado°, ecobee, belkin echo, LIFX, we mo, micasaverde Security: Bosch, Kwikset, ALARM.COM, Lockitron, CANARY, HomeMonitor, iSmartAlarm	Industries Retail: Nomi, euclid, placemeter Healthcare: VISI MOBILE, AdhereTech, AliveCor, TELCARE, intelligentM Automotive: Dashiabs, SYNC, OpenXC, mojiio, ienture Smart Buildings: APOGEE, Johnson Controls, Schneider Electric	Industrial Internet Robotics: KIVA Systems, Double Robotics, Airware, ROBOTEX, 3D Robotics, MOMENTUM Greentech: BigBelly, Axeda, Solar, enlightened, GRIDMOBILITY 3D Printing: BOSYSTEMS, MezzoMill, Stratatsys, formlabs, shapeways, MakerBot INDUSTRIES, RepRap
New Interfaces NeuroSky, gestigon, sphero, PrimeSense, EQUISO, emotivo, Interaxon, LEAP				

Building Blocks

Connection Protocols neul, ZigBee, macheen, RFID, NFC, WiFi, Bluetooth, M-Bus, MQTT, 2G, 3G, 4G	Telecom at&t, verizon, Mobile, boost	M2M Jasper, CROSSBRIDGE, gemalto, Telit, ERICSSON, Numorex					
Software amazon web services, Parse, heroku	Mobile iOS, Android	Hardware apengate, ARDUINO, beagleboard.org, spark	Parts / Kits MARY MARY, Tinkerforge, littleBits, MOSORO, reedymate	Services DRAGON innovation, makexyz, CIRCUIT LAB	Incubators BOLT, LEMNOS Labs, springboard()	Funding KICKSTARTER, indiegogo	Distribution Anvil

Smart Doorlock

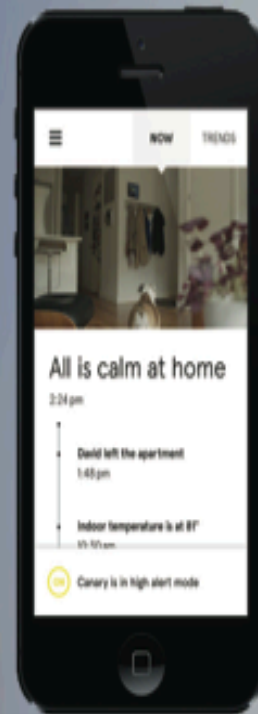
The Genie Smart Lock - A door lock that allows you to lock and unlock your home using your smart phone, bluetooth keyring or computer.



<http://www.geniesmartlock.com/index.php>

Smart Home Security

Canary is a complete security system packed into a single, device. It adapts to your home over time and sends intelligent notifications with HD video directly to your smartphone.



IoT e as pessoas mal intencionadas ...

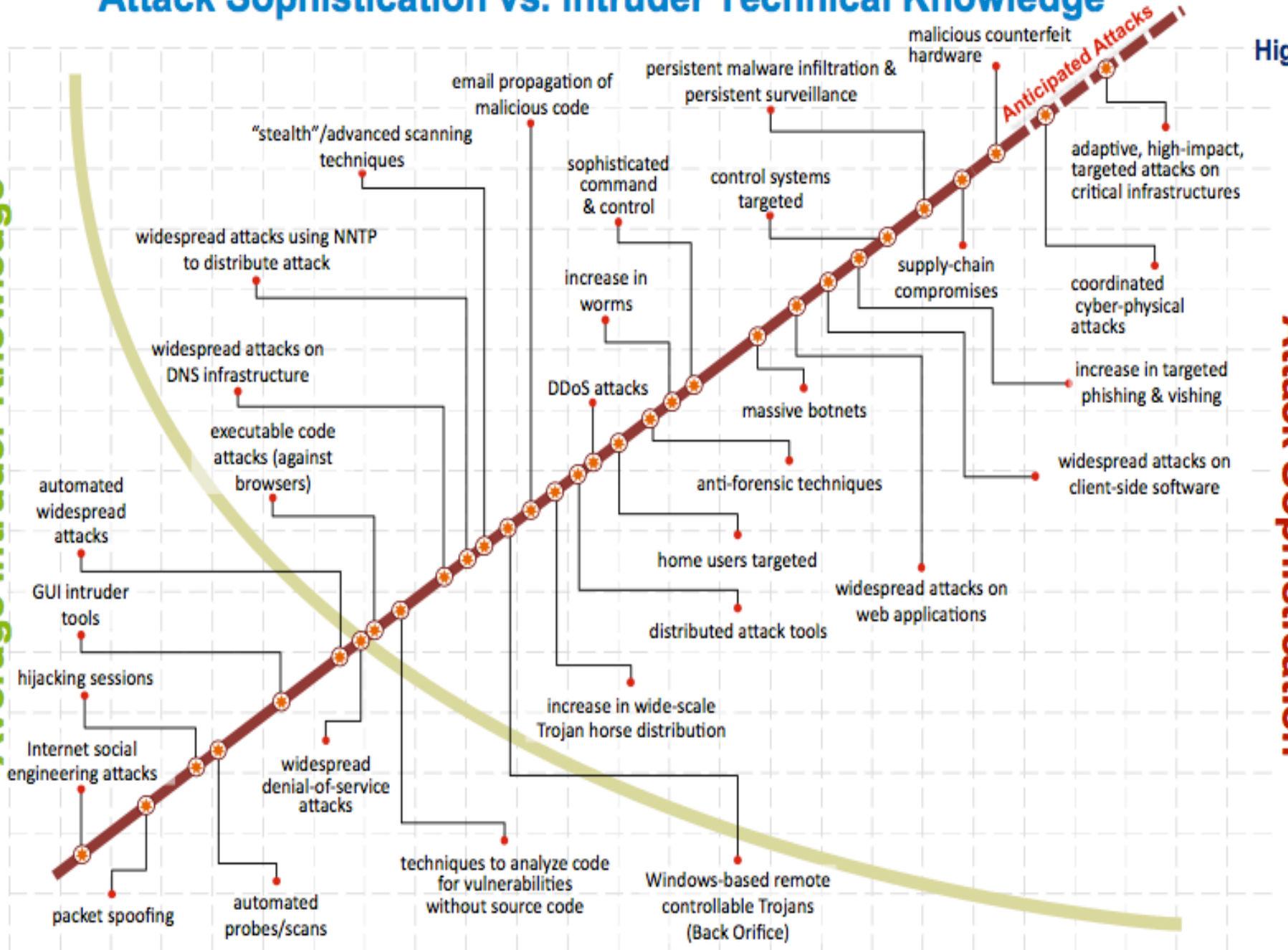


Attack Sophistication vs. Intruder Technical Knowledge

Average Intruder Knowledge

High

Attack Sophistication



1990

2010

Low

Como organizar o caos das cidades

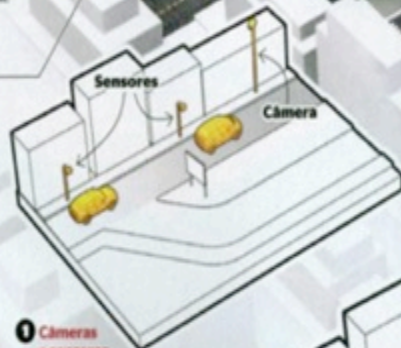
A integração tecnológica pode ajudar a melhorar os problemas de trânsito, violência, falta de energia.

Celso Masson (texto) e Nilson Cardoso (infográfico)

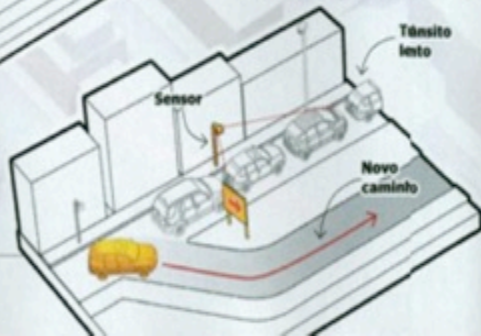
AS CIDADES não precisam ser caóticas. Há cada vez mais pessoas nas grandes áreas urbanas, e elas consomem mais, trafegam mais, usam mais energia - mas estão surgindo várias tecnologias para diminuir o impacto negativo da concentração populacional. É o que mostra um estudo feito pela divisão de consultoria da IBM a partir de demandas apresentadas por seus clientes da administração pública no mundo todo. O estudo é anual, mas pela primeira vez a IBM apresentou um quadro geral de soluções que já existem, mas só são usadas em caráter experimental. "Não estamos afirmando que o mundo será assim em 2015, mas essas ferramentas estarão disponíveis para quem quiser usá-las", diz o executivo Cezar Taurion, responsável pela divulgação do estudo no Brasil.

MOBILIDADE

O trânsito de automóveis é um dos grandes complicadores da vida nos centros urbanos. A tecnologia integrada pode permitir às cidades monitorar o trânsito para evitar congestionamentos e oferecer rotas alternativas em tempo real. Em Cingapura, câmeras e sensores monitoram o fluxo de veículos. Quando há uma redução de velocidade anormal em determinado trecho, painéis eletrônicos informam os caminhos alternativos



1 Câmeras e sensores monitoram a velocidade média das vias e alimentam bancos de dados sobre cada horário e dia da semana



2 Quando há uma redução anormal em determinado trecho, o sistema ativa painéis eletrônicos indicando novas alternativas. Isso evita a formação de engarrafamentos

As cidades crescem seis vezes em relação ao nível atual. Reduzir o desperdício é fundamental: as cidades perdem até 50% da água tratada para consumo apenas com vazamentos e falhas na infraestrutura. Sensores podem identificar vazamentos em tempo real e evitar o desabastecimento

Sensores distribuídos pela tubulação monitoram o fluxo de água e alimentam bancos

Tubulação de água

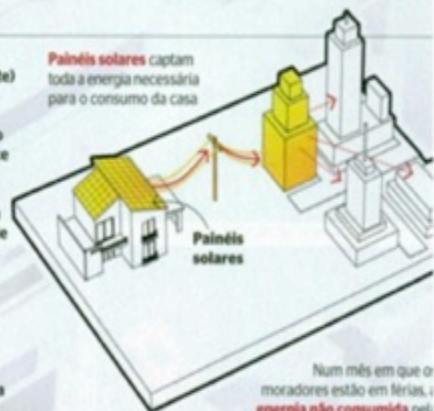
de dados sobre o consumo. Quando há um vazamento, ele é percebido em segundos

O reparo é feito a tempo de minimizar as perdas e manter o fornecimento naquela região

ENERGIA

A smart grid (grade inteligente) transforma a rede elétrica numa via de mão dupla: ela fornece energia para os consumidores e recebe a energia que cada unidade pode produzir. Uma casa que tenha placas de captação de energia solar, por exemplo, pode "vender" o excedente de sua produção para a distribuidora. Essa "sobra" realimenta o sistema

Painéis solares captam toda a energia necessária para o consumo da casa



Num mês em que os moradores estão em férias, a energia não consumida pela casa é enviada para a rede de energia e usada por outros moradores

SAÚDE

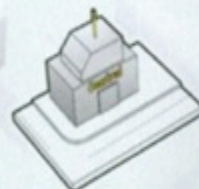
Um sistema inteligente que integre dados de saúde pública coletados em escolas, hospitais, postos de saúde e até em clínicas particulares pode responder a uma crise na saúde antes que ela se instale. Dados sobre internações e suas causas, consultas motivadas por infecções e vírus atípicos podem ajudar a decidir sobre campanhas de vacinação ou mudanças de hábitos

SEGURANÇA

Sistemas de prevenção de crimes por meio de microfones e câmeras colocados em pontos estratégicos ajudam a diminuir a incidência de furtos, assaltos e homicídios. A polícia de Chicago, nos EUA, usa um software que identifica imagens de movimentos suspeitos e emite um alerta para os policiais daquela área, que podem se antecipar à ocorrência



O ShotSpotter é um sistema de captação de som que ouve disparos e informa sua origem por meio de

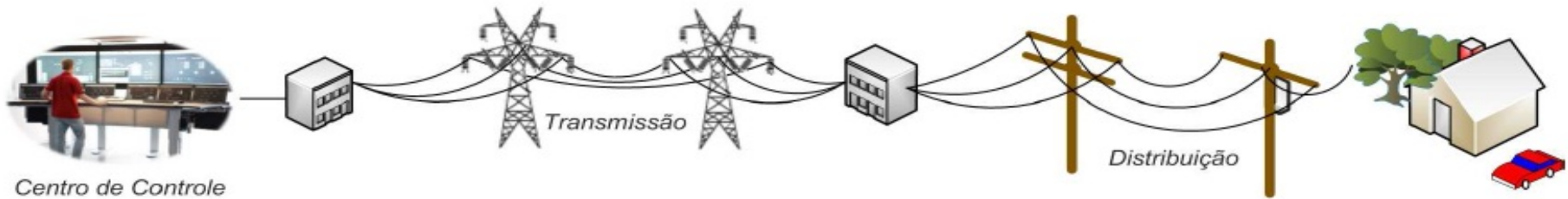


uma "triangulação". Quando um disparo ocorre, uma central recebe as coordenadas do local

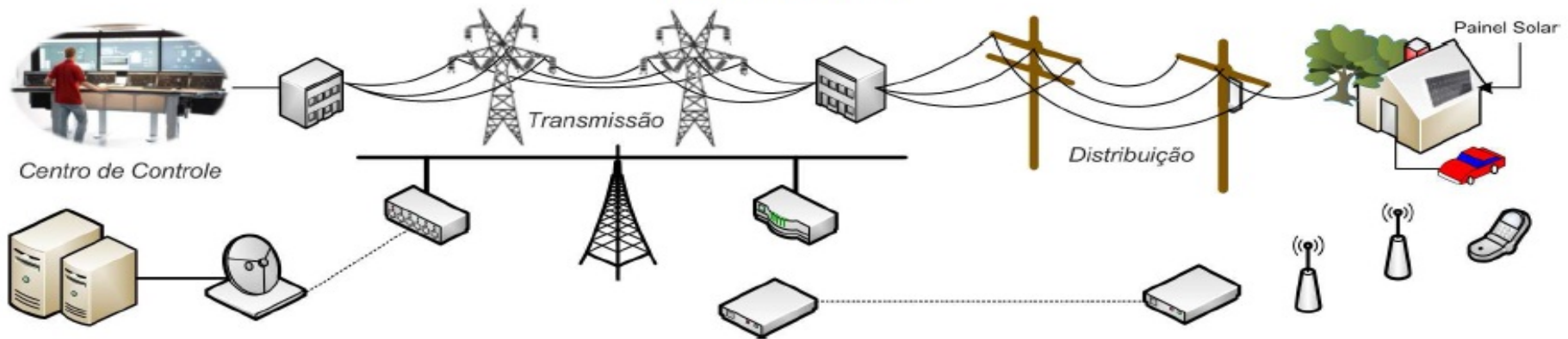


A informação é passada aos policiais próximos, que são enviados para o local

Smart Grid ...



(a) Rede elétrica atual.



Rede elétrica inteligente, com amplo suporte de telecomunicações.

Stuxnet ...

2010

Stuxnet, a virus created for industrial and economic attacks, is discovered. The worm targets systems used to run nuclear power plants and water facilities and is so large and complex, estimates suggest it was developed by the U.S. or Israeli governments and took more than 10 years to develop.



26 September 2010 Last updated at 14:57 GMT



Stuxnet worm hits Iran nuclear plant staff computers

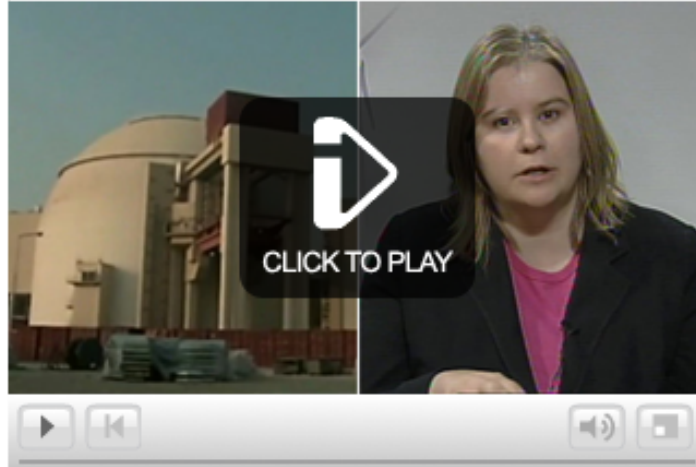
A complex computer worm has infected the personal computers of staff at Iran's first nuclear power station, the official IRNA news agency reported.

However, the operating system at the Bushehr plant - due to go online in a few weeks - has not been harmed, project manager Mahmoud Jafari said.

The Stuxnet worm is capable of seizing control of industrial plants.

Some Western experts say its complexity suggests it could only have been created by a "nation state".

It is the first sign that Stuxnet, which targets systems made by the German company



Sian John, Symantec: "It's very sophisticated"

Los clientes que usan CitectSCADA incluyen gasoductos en Chile, diamante en Australia y Botsuana, un laboratorio farmacéutico en Alemania y plantas de tratamiento de agua en Luisiana y Carolina del Norte.

Para que ocurra un ataque aprovechando la vulnerabilidad citada, el blanco tendría que estar conectado con la Internet. Esto va contra las políticas de la industria, pero puede

Wednesday, April 30, 2014

Hacking US (and UK, Australia, France, etc.) Traffic Control Systems

By Cesar Cerrudo @cesarcer

Hacking like in the movies

Probably many of you have watched scenes from "Live Free or Die Hard" (Die Hard 4) where "terrorist hackers" manipulate traffic signals by just hitting Enter or typing a few keys. I wanted to do that! I started to look around, and while I couldn't exactly do the same thing (too



conference.hitb.org/hitbsecconf2013ams/materials/D1T1N20-K20@Hugob20TesoK20-K20Aircraft...

amsterdam

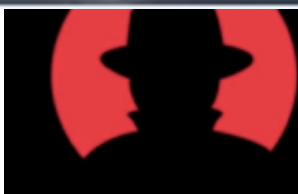
Hacking Series



JACKPOTTING
Automated Teller Machines





CAR HACKING
CHARLIE MILLER
CHRIS VALASEK



Help! My fridge is full of spam and so is my router, set-top box and console


Security company says it discovered spam and phishing campaign run over Christmas, which involved internet fridge

 Share 91


 Tweet 139


 +1 13

 Share 16

 Email

Charles Arthur

 Follow @charlesarthur

 Follow @guardiantech

theguardian.com, Tuesday 21 January 2014 11.40 GMT

 Jump to comments (19)

Technology

Gadgets · Spam · Internet

More news



In the 'internet of things cyberattack', more than 100,000 everyday consumer gadgets were attacked, including an internet fridge. Photograph: Martin Argles for the Guardian

Privacidade ?



Smartphone ...



1ST PLACE


SEE WHY FLEXISPY IS [THE BEST SPYPHONE YOU CAN BUY](#)


This Could Be You!


I Knew It . . .


Thanks to FlexiSPY I finally figured out my wife was cheating on me with my brother. I had a bad feeling about this for over a year. After the divorce, my life is so much better now.


Not Sure?


 ANDROID

 Windows Mobile

 iPhone

 BlackBerry

 NOKIA

 Speak to a live person now

Smart TV...



Wearable devices ...

Google

"sexual activity" site:fitbit.com

About 8 results (0.04 seconds)

Advanced search

Everything

Images

Videos

News

Shopping

More

Larkspur, CA

Change location

All results

Sites with images

Related searches

More search tools

Fitbit Profile

www.fitbit.com/user/22DP9H/activities - Cached

Calories. Automatically calculate calories burned. **Sexual Activity**. General, moderate effort. started at 1:00 am. N/A 45 minutes 70 ...

Fitbit Profile

www.fitbit.com/user/222ZN6 - Cached

May 31, 2011 – **Sexual Activity**. General, moderate effort. started at 10:45 pm. N/A 20 minutes 36. Total N/A 20 minutes 36 ...

Overall - Fitbit Profile

www.fitbit.com/user/22CJ9F - Cached

Aug 23, 2010 – **Sexual Activity**. General, moderate effort. started at 11:00 am. N/A 1 hour 72. Total N/A 1 hour 72. Activity Records Mon Aug 23 20:22:00 UTC ...

Overall - Fitbit Profile

www.fitbit.com/user/227QSS

Feb 13, 2010 – **Sexual Activity**. Passive, light effort, kissing, hugging. N/A 10 minutes 9 ... **Sexual Activity**. Active, vigorous effort. N/A 15 minutes 21 ...

Overall - Fitbit Profile


www.fitbit.com/user/22B6GD - Cached

Calories. Automatically calculate calories burned. **Sexual Activity**. General, moderate effort. started at 12:00 am. N/A 30 minutes 37 ...

Overall - Fitbit Profile

www.fitbit.com/user/228Q4L - Cached

May 12, 2010 – **Sexual Activity**. Active, vigorous effort. started at 10:30 pm. N/A 30 minutes 50. Total N/A 30 minutes 50 ...





Desafios



IoT – Principais desafios

Os principais desafios de IoT são:

- **Segurança**
- **Privacidade**
- **Fraudes**
- **Infraestruturas Críticas**
- **M2M, machine to machine**
- **Padronização**



Segurança é prevenção, não o remédio!

IoT - Desafios de Segurança

É necessário pensar em Segurança do ponto de vista:

- do Dispositivo
- da Arquitetura
- da Informação
- da Comunicação
- da Gestão de Paths
- etc.

É necessário pensar na segurança e proteção dos dispositivos de **Ponta a Ponta**, ou como dizemos em inglês **end-to-end security**.



IoT - Desafios de Segurança

Tenha em mente que os dispositivos podem:

- **Não estarem acessíveis**
um dispositivo não estará conectado na maioria das vezes
- **Serem perdidos ou roubados**
garantir a segurança é difícil quando não há conexão
- **Não gerenciar criptografia**
o processamento dos dispositivos é limitado
- **Ter um tempo de vida finito**
gestão das credenciais, vinculadas ao tempo de vida
- **Ser portáteis**
desta forma podem cruzar fronteiras ...

Uma ferramenta ...



Credenciais de acesso ...





← CREDENCIAIS →



API



App

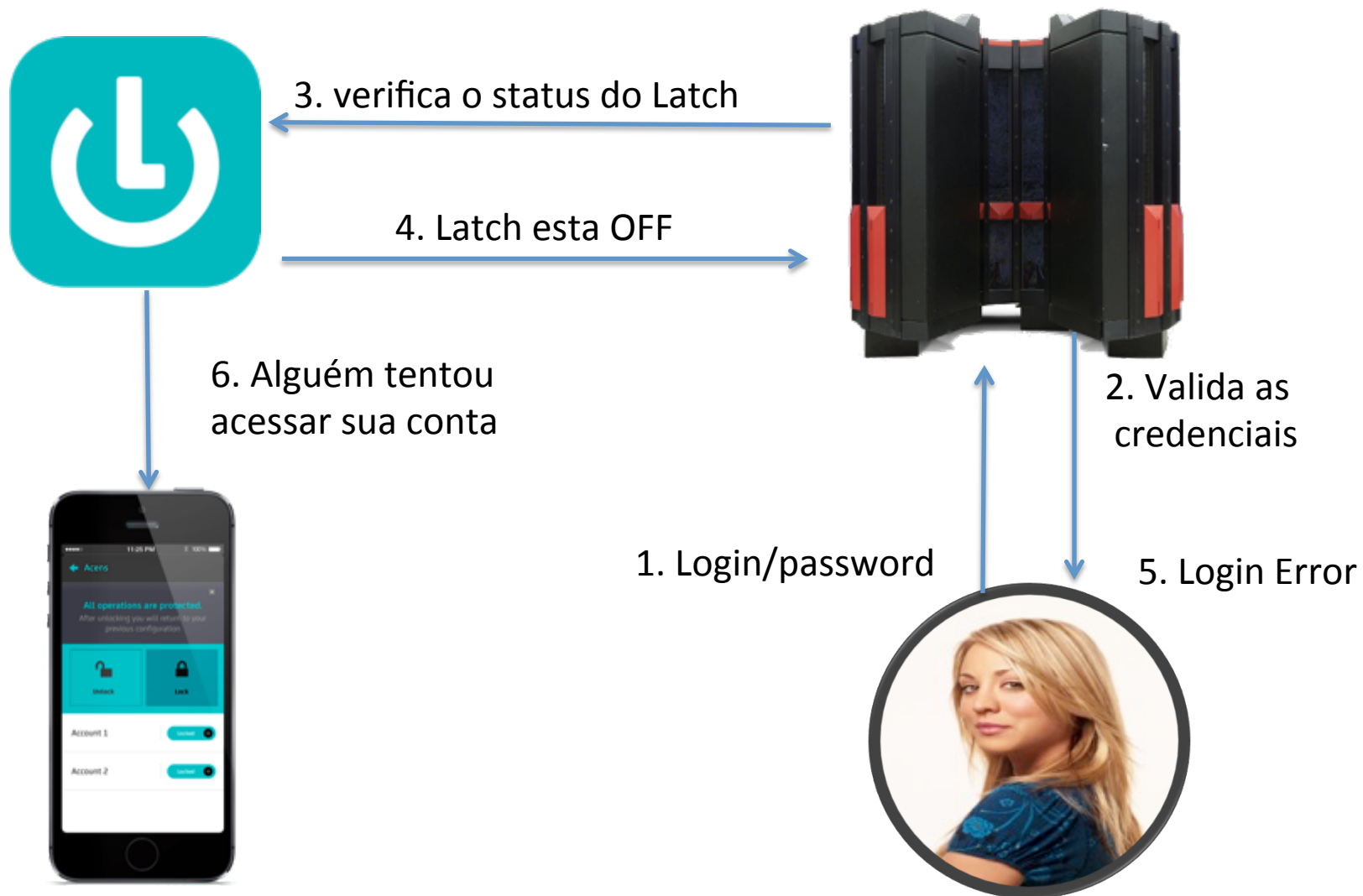


Latch

CRENCIAIS



Autenticação



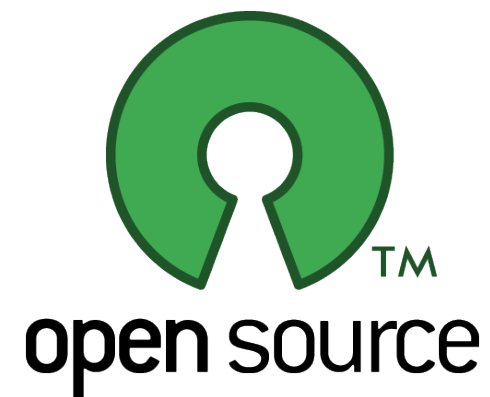


Latch

latch.elevenpaths.com

 Eleven
Paths

A *Telefónica* COMPANY



SDKs



Plugins



Versão gratuita

Community

Teste gratuitamente a segurança adicional do Latch para até 50 contas do usuário

Características do serviço

	Community
Nº máximo de contas pareadas ¹	50
Nº máximo de Aplicativos ²	2
Níveis de granularidade das Operações	4
Plugins Standard e SDKs	Grátis
Dashboard de Aplicativos	✓
Atualizações do serviço gratuitas	✓
Garantia de 'service uptime'	–
Prioridade na participação em Programas Beta	–

O Latch



Assuma o controle da sua identidade digital

Desative suas contas digitais quando não estiverem sendo utilizadas, para evitar o uso não autorizado.



Consiga nível adicional de segurança sobre suas contas

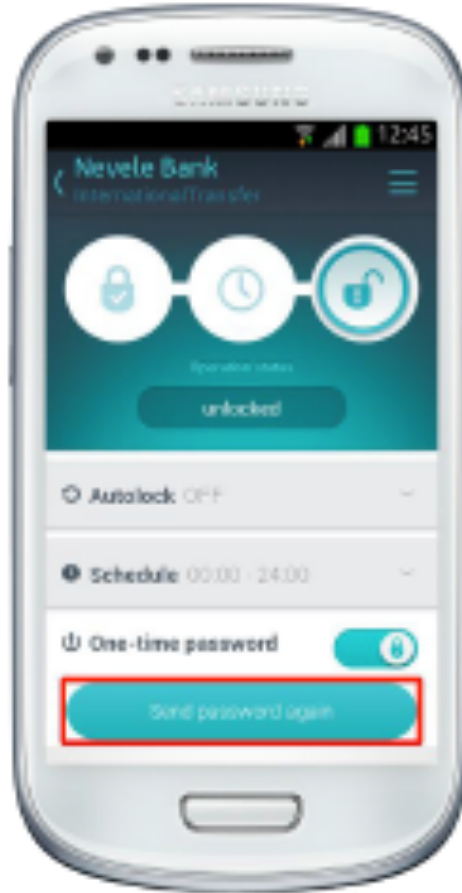
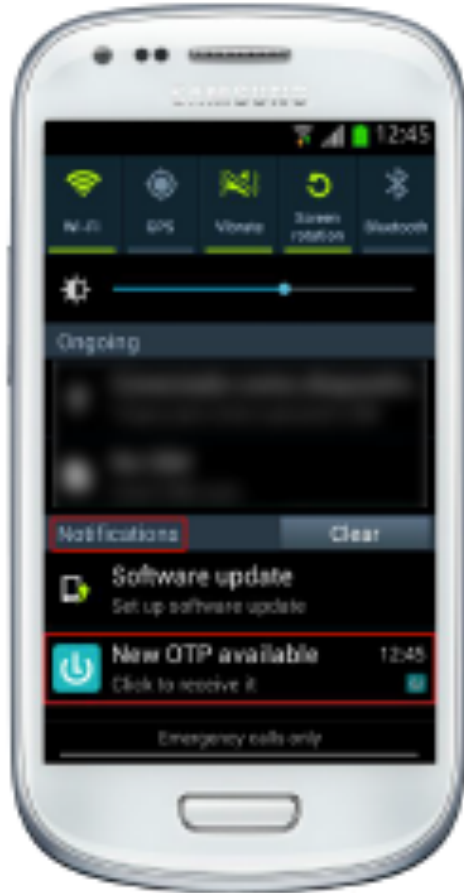
Faça o pareamento de serviços digitais habilitados pelo Latch no site na Web.



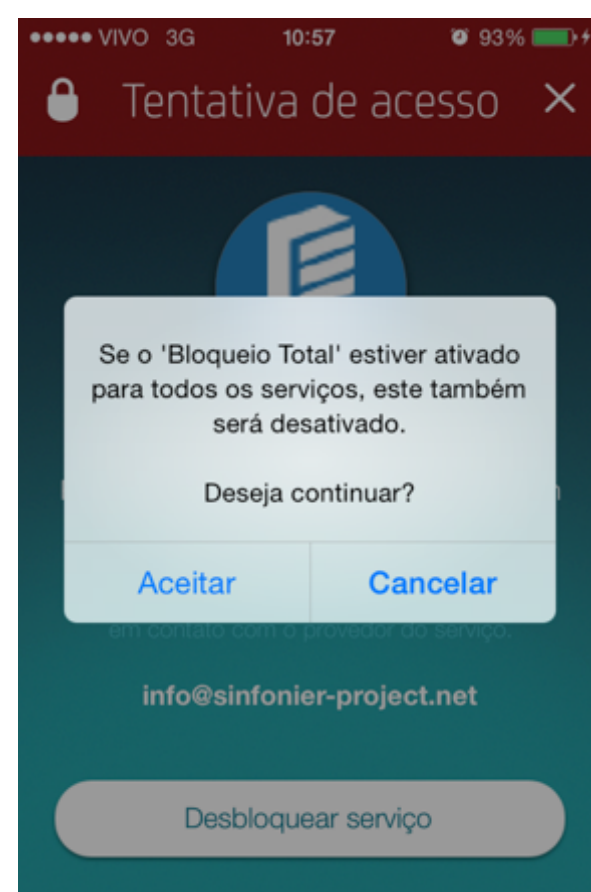
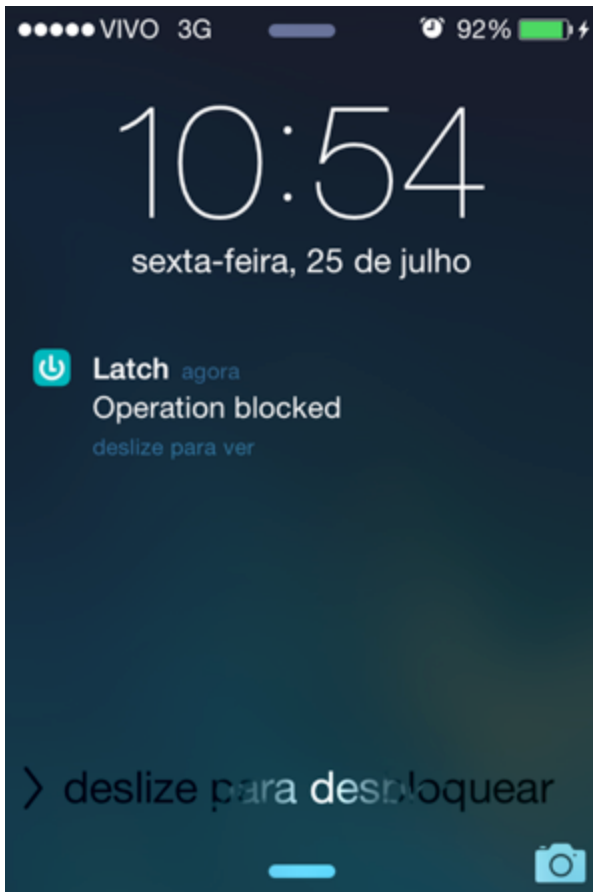
Monitore tentativas de acesso às suas contas

Você pode monitorar tentativas de acesso às suas contas quando elas estiverem bloqueadas e enviar relatórios ao seu provedor.

OTP – 2F Autenticação



Alertas





Seja um usuário

Para usar Latch, você deve registrar sua conta através do site:

latch.elevenpaths.com



Perguntas ???



תודה
Dankie Gracias
Спасибо شکرًا
Merci Takk
Köszönjük Terima kasih
Grazie Dziękujemy Děkojame
Ďakujeme Vielen Dank Paldies
Kiitos Tänname teid 谢谢
Thank You Tak
感謝您 Obrigado Teşekkür Ederiz
Σας ευχαριστούμε 감사합니다
ขอบคุณ
Bedankt Děkujeme vám
ありがとうございます
Tack

 Leandro Bennaton

 @bennaton