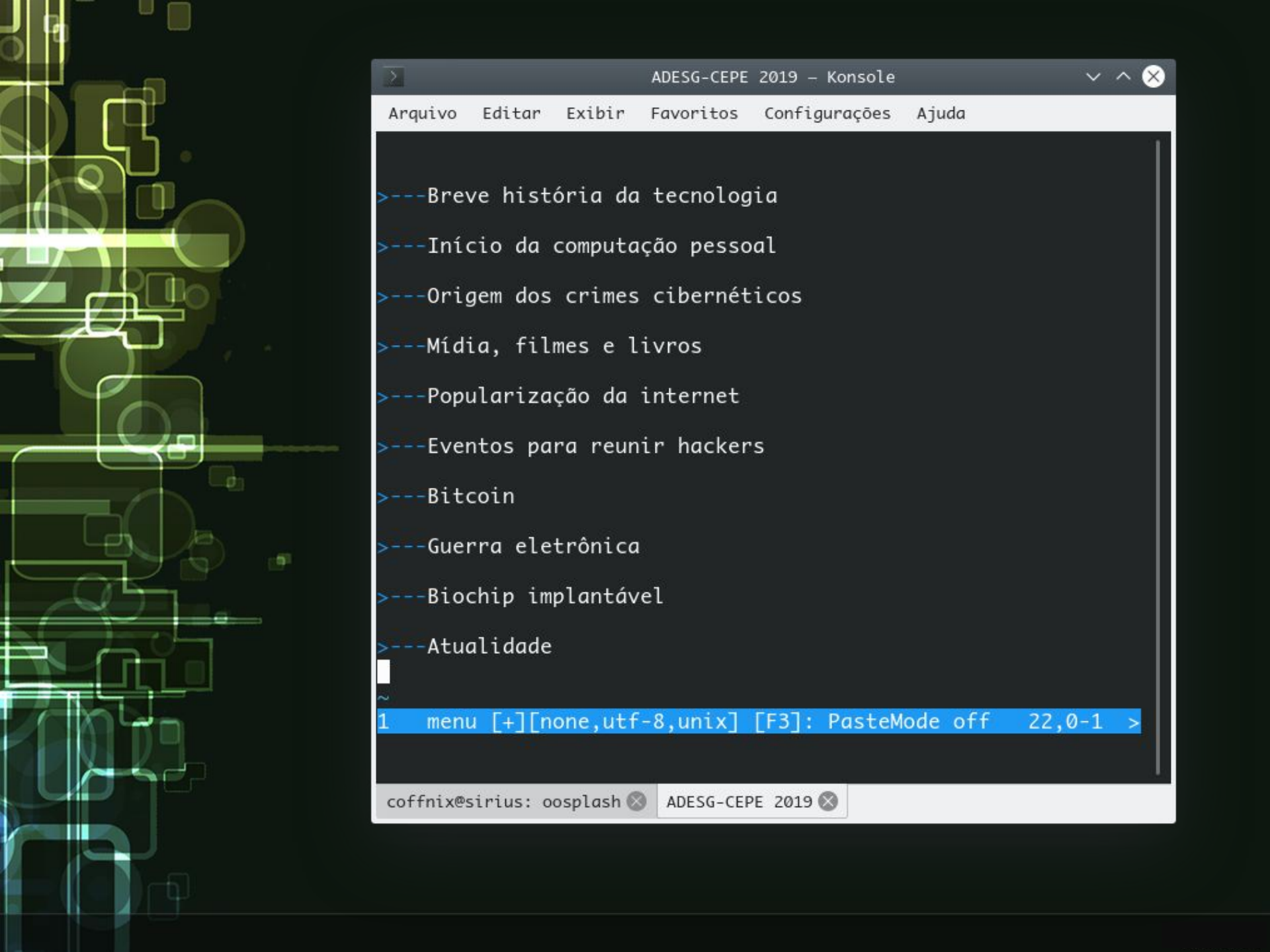
Epítome sobre os inimigos invisíveis nas tecnologias digitalmente transformadoras

Raphael Bastos
ÁREA 31 HACKERSPACE

ADESG/MG - CEPE 2019
Belo Horizonte, 10 de junho de 2019


ADESG-CEPE 2019 – Konsole
Arquivo Editar Exibir Favoritos Configurações Ajuda
>---Breve história da tecnologia
>---Início da computação pessoal
>---Origem dos crimes cibernéticos
>---Mídia, filmes e livros
>---Popularização da internet
>---Eventos para reunir hackers
>---Bitcoin
>---Guerra eletrônica
>---Biochip implantável
>---Atualidade
~
1 menu [+][none,utf-8,unix] [F3]: PasteMode off 22,0-1 >
coffnix@sirius: oosplash
ADESG-CEPE 2019

Antecedentes

* Padre Landell de Moura (1861~1928)
- telefone sem fio
- telegrafo sem fio
- trasmissor de ondas

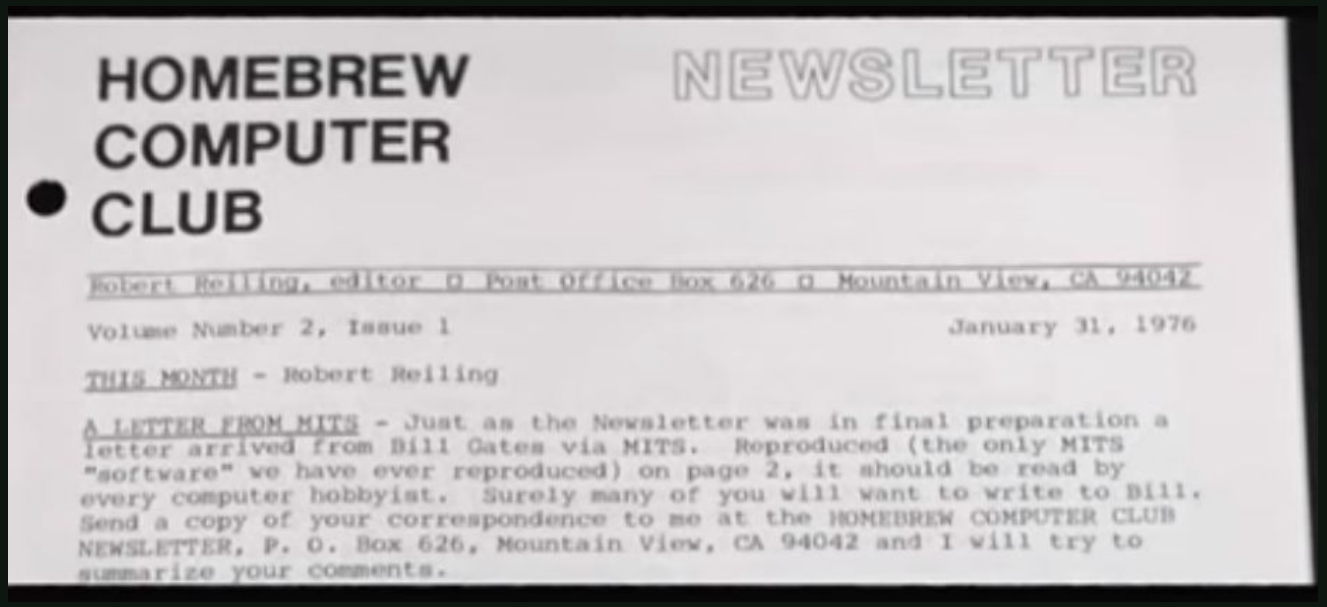
* Isac Asimov
* Steve Jobs

What this is?

- Hacker vs Cracker
- Existe segurança Digital?
- Defesa Cibernética
- Guerra Eletrônica
- Deep web vs WWW
- Internet das coisas
- Blockchain
- Biohacking e biotecnologia

Início da computação pessoal

Início da computação pessoal



HOMEBREW COMPUTER CLUB NEWSLETTER

Robert Reiling, editor □ Post Office Box 626 □ Mountain View, CA 94042

Volume Number 2, Issue 1 January 31, 1976

THIS MONTH - Robert Reiling

A LETTER FROM MITS - Just as the Newsletter was in final preparation a letter arrived from Bill Gates via MITS. Reproduced (the only MITS "software" we have ever reproduced) on page 2, it should be read by every computer hobbyist. Surely many of you will want to write to Bill. Send a copy of your correspondence to me at the HOMEBREW COMPUTER CLUB NEWSLETTER, P. O. Box 626, Mountain View, CA 94042 and I will try to summarize your comments.

(Bill Gates 31/01/1976)

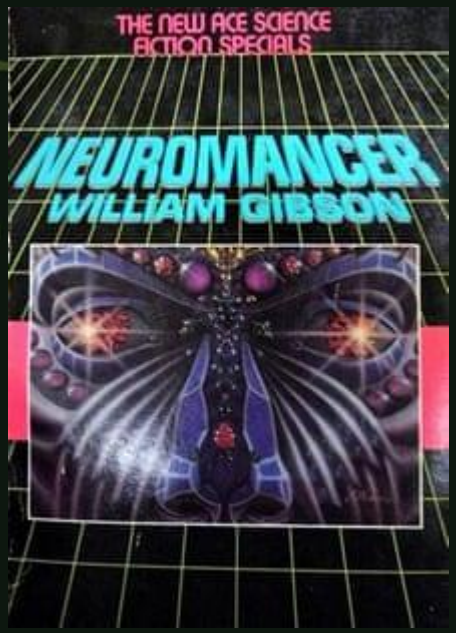
Bluebox (Phreaker)

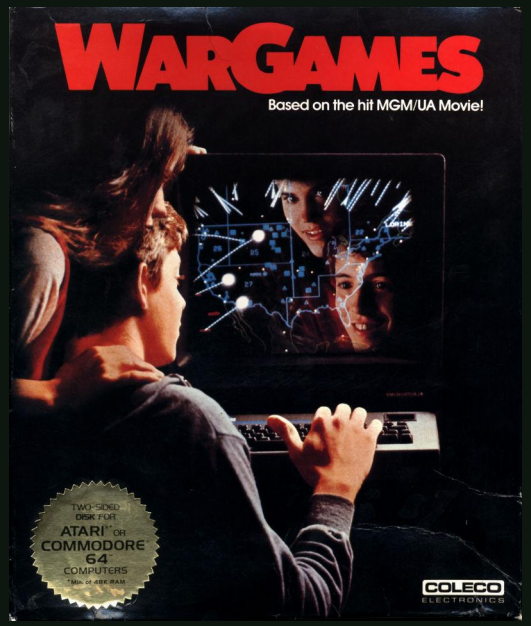
Criado por John Draper, vendido por Steve Wozniak e Steve Jobs

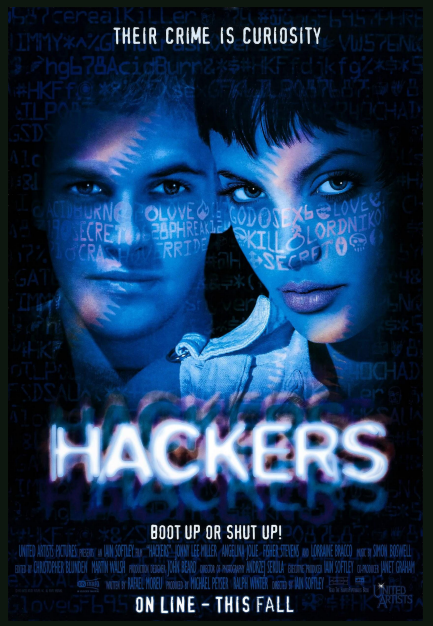
Origem dos crimes cibernéticos (1972)

Mídia, filmes e livros

Anos 80 e 90







Mídia, filmes e livros

Anos 2000

Popularização da internet (Anos 90)

- Software Open Source
- Linux
- A maior criação dos hackers foi a internet

DEFCON

- Primeira edição: 09/05/1993 - Las Vegas

Uma das maiores conferências hacker do mundo

Conferências brasileiras

- H2HC (Hackers to Hackers Conference)

- BHACK Conference

Provedores de BBS e internet

- Comercialização iniciada nos anos 90

Desde 2006 são maioria as Datas wherehouse (nuvem)

Kevin Mitnick

- Preso em 15/02/1995

Wikileaks

Fundado em 04/10/2006

Bitcoin/Blockchain

Criado em 2008 por Satoshi Nakamoto

identidade desconhecida

Guerra Eletrônica

Operação aurora (2009)

- Primeiro ataque sofisticado financiado por um estado (China vs empresas americanas)

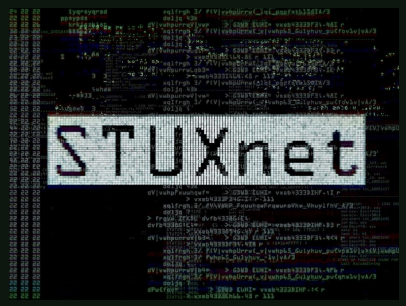
Guerra Eletrônica

Comando cibernético dos EUA (criado em 2009)

Donald Trump decidiu em 2017 elevar o status do comando cibernético à mesma categoria das divisões do Pentágono dedicadas ao combate a ciberataque

Guerra Eletrônica

Stuxnet (2010)



- Vírus desenvolvido em parceria entre EUA e Israel para sabotar uma usina de enriquecimento de urânio no Irã

Guerra Eletrônica

Edward Snowden (2013)

- Tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA americana

Guerra Eletrônica

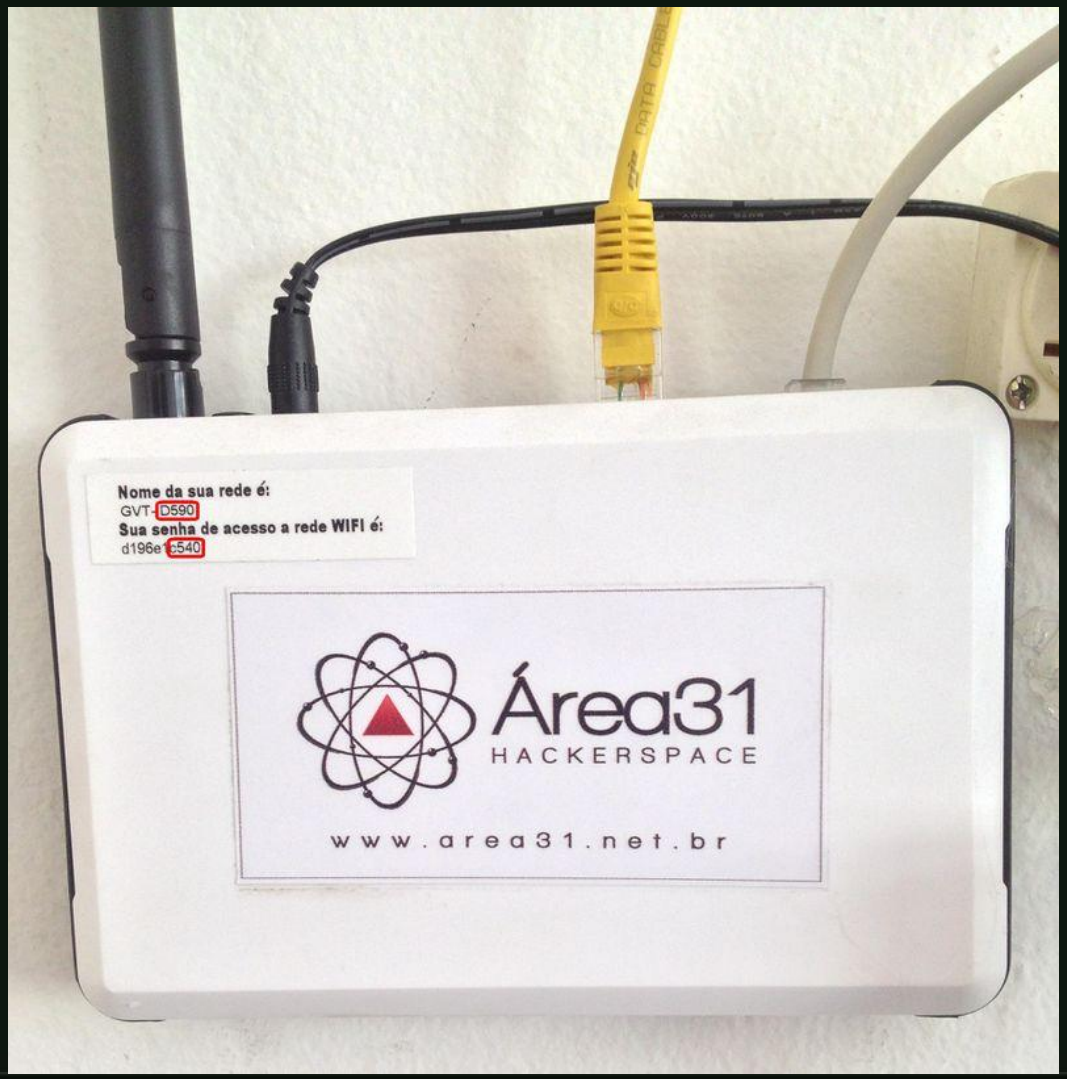
- Huawei
- Israel bombardeia

Deep Web e Dark Web

- The TOR Project foi desenvolvido em 2002

Browser (firefox modificado)

Router Backdoor



Router Backdoor

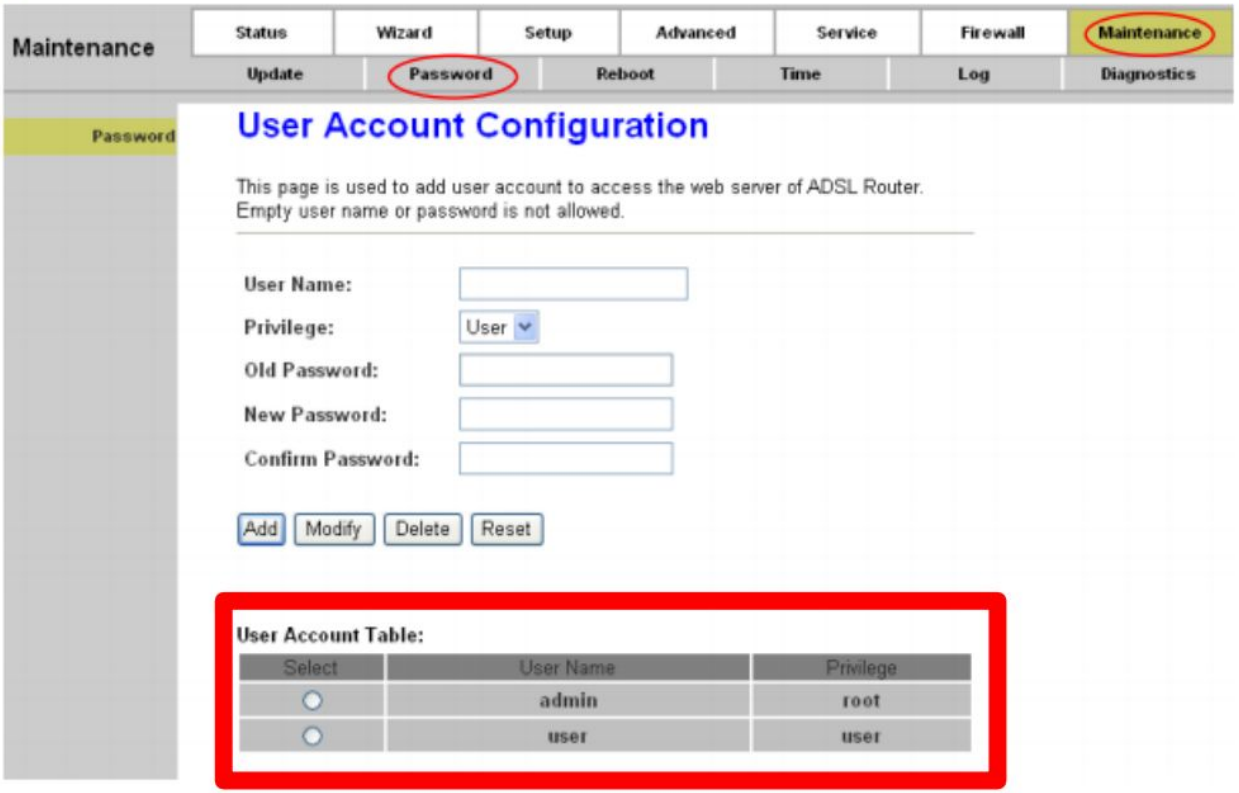
```
18 19  1a 1b  1c 1d  1e 1f
1c 27  b8 05  54 75  65 20   TPLINKOEM ...€.....'.€IŒ.'¸.Tue
74 65  72 2e  69 6d  67 00   Mar 13 14:33:22 2012.router.img.
06 84  00 01  ee f7  70 5a   .....¿A..o..€.u§1..... .„...÷pZ
34 6d  14 4f  5d 6a  72 74   =¬â'.+k>.¡©‡rèÓ$å5'#[ .~p4m.O]jrt
20 9c  96 f4  55 57  6c 31   |R…ŽÓ˜.í. [>›Sa¿E.0ŒY.›. œ-ôUWl1
17 21  e6 c4  0a 9a  f2 7c   ÈOVDV…Î¸ ¼•ëýæ~."t[ ýÝê¨.!æÄ.šò|
```

```
544   <chain N="USERNAME_PASSWORD">
545   <V N="FLAG" V="0x0"/>
546   <V N="USERNAME" V="admin"/>
547   <V N="PASSWORD" V="gvt12345"/>
548   <V N="BACKDOOR" V="0x0"/>
549   <V N="PRIORITY" V="0x2"/>
550   </chain>
551   <chain N="USERNAME_PASSWORD">
552   <V N="FLAG" V="0x0"/>
553   <V N="USERNAME" V="user"/>
554   <V N="PASSWORD" V="uAmqwWhz"/>
555   <V N="BACKDOOR" V="0x0"/>
556   <V N="PRIORITY" V="0x0"/>
557   </chain>
558   <chain N="USERNAME_PASSWORD">
559   <V N="FLAG" V="0x0"/>
560   <V N="USERNAME" V="admin"/>
561   <V N="PASSWORD" V="D590airocon"/>
562   <V N="BACKDOOR" V="0x1"/>
563   <V N="PRIORITY" V="0x1"/>
564   </chain>
```

Router Backdoor

4.6.2. Password

Choose "**Maintenance→Password**", you can configure the user account of the router in the screen (shown in Figure 4-53). Here you can add user account to access the web server, and modify the password of the specified user.



Router Backdoor

```
ADSL-GVT#login show

Username  Password          Priority
admin     gvt12345          2
user      gvt12345          0
admin     D590airocon       1
ADSL-GVT#
```

Router Backdoor

Taking a closer look at the device's memory it was possible to find some interesting information:

```
0x8054a790: c3 10 21 00 0f 4f 62 73 65 72 76 61 20 54 65 6c ..!..Observa Tel
0x8054a7a0: 65 63 6f 6d 10 23 00 06 52 54 41 30 34 4e 10 24 ecom.#..RTA04N.$
0x8054a7b0: 00 0d 45 56 2d 32 30 30 36 2d 30 37 2d 32 37 10 ..EV-2006-07-27.
0x8054a7c0: 42 00 0f 31 32 33 34 35 36 37 38 39 30 31 32 33 B..1234567890123
0x8054a7d0: 34 37 10 54 00 08 00 06 00 50 f2 04 00 01 10 11 47.T.....P......
0x8054a7e0: 00 10 41 44 53 4c 20 53 6f 48 6f 20 52 6f 75 74 ..ADSL SoHo Rout
0x8054a7f0: 65 72 10 08 00 02 00 86 00 00 00 00 00 00 00 00 er..............
```

Redirection link to Chinese company:

```
0x80561470: 56 3d 22 30 78 30 22 2f 3e 0a 3c 56 20 4e 3d 22 V="0x0"/>.<V N="
0x80561480: 55 52 4c 5f 52 45 44 49 52 45 43 54 5f 45 4e 41 URL_REDIRECT_ENA
0x80561490: 42 4c 45 22 20 56 3d 22 30 78 30 22 2f 3e 0a 3c BLE" V="0x0"/>.<
0x805614a0: 56 20 4e 3d 22 55 52 4c 5f 52 45 44 49 52 45 43 V N="URL_REDIREC
0x805614b0: 54 5f 53 54 52 22 20 56 3d 22 77 77 77 2e 63 68 T_STR" V="www.ch
0x805614c0: 69 6e 61 75 6e 69 63 6f 6d 2e 63 6f 6d 2e 63 6e inaunicom.com.cn
```

Even after reset it was possible to retrieve the device's previous user name:

```
0x80571480: 64 00 31 04 00 0e 4d 69 72 74 65 73 20 46 6f 6e d.1...Mirtes Fon
0x80571490: 73 65 63 61 01 08 82 84 8b 96 0c 12 18 24 03 01 seca.........$..
```

The device saves neighbour network names:

```
0x80572de0: 64 00 11 04 00 08 47 56 54 2d 41 35 34 31 01 08 d.....GVT-A541..
0x80572df0: 82 84 8b 96 0c 12 18 24 03 01 0b 05 04 00 01 00 .......$........

0x80578280: 64 00 11 0c 00 0a 41 52 52 49 53 2d 37 31 30 32 d.....ARRIS-7102

0x8057a440: 64 00 31 04 00 0d 50 69 6c 6f 74 20 42 61 7a 7a d.1...Pilot Bazz
0x8057a450: 6f 6e 69 01 08 82 84 8b 96 0c 18 30 48 03 01 0b oni........0H...

0x8057bda0: 64 00 31 04 00 08 47 56 54 2d 32 35 39 35 01 08 d.1...GVT-2595..

0x80581aa0: 64 00 11 04 00 05 41 6c 70 68 61 01 08 82 84 8b d.....Alpha.....
```

Router Backdoor

Sensitive data about GVT credential services:

```
0x805608b0: 02 01 60 56 20 4e 3d 22 43 57 4d 50 5f 53 45 52 ..`V N="CWMP_SER
0x805608c0: 56 45 52 5f 55 53 45 52 22 20 56 3d 22 61 63 73 VER_USER" V="acs
0x805608d0: 63 6c 69 65 6e 74 22 2f 3e 0a 3c 56 20 4e 3d 22 client"/>.<V N="
0x805608e0: 43 57 4d 50 5f 53 45 52 56 45 52 5f 50 57 44 22 CWMP_SERVER_PWD"
0x805608f0: 20 56 3d 22 61 63 73 67 76 74 32 35 73 63 61 22  V="acsgvt25sca"
0x80560900: 2f 3e 0a 3c 56 20 4e 3d 22 43 57 4d 50 5f 49 4e />.<V N="CWMP_IN
0x80560910: 46 4f 52 4d 22 20 56 3d 22 30 78 31 22 2f 3e 0a FORM" V="0x1"/>.
0x80560920: 3c 56 20 4e 3d 22 43 57 4d 50 5f 49 4e 46 4f 52 <V N="CWMP_INFOR
0x80560930: 4d 5f 49 4e 54 45 52 56 41 4c 22 20 56 3d 22 30 M_INTERVAL" V="0
0x80560940: 78 31 32 63 22 2f 3e 0a 3c 56 20 4e 3d 22 43 57 x12c"/>.<V N="CW
0x80560950: 4d 50 5f 49 4e 46 4f 52 4d 5f 54 49 4d 45 22 20 MP_INFORM_TIME"
0x80560960: 56 3d 22 30 78 30 22 2f 3e 0a 3c 56 20 4e 3d 22 V="0x0"/>.<V N="
0x80560970: 43 57 4d 50 5f 43 4f 4e 52 45 51 5f 50 4f 52 54 CWMP_CONREQ_PORT
0x80560980: 22 20 56 3d 22 30 78 31 64 37 62 22 2f 3e 0a 3c " V="0x1d7b"/>.<
0x80560990: 56 20 4e 3d 22 43 57 4d 50 5f 43 4f 4e 52 45 51 V N="CWMP_CONREQ
0x805609a0: 5f 55 53 45 52 22 20 56 3d 22 69 74 6d 73 22 2f _USER" V="itms"/
0x805609b0: 3e 0a 3c 56 20 4e 3d 22 43 57 4d 50 5f 43 4f 4e >.<V N="CWMP_CON
0x805609c0: 52 45 51 5f 50 57 44 22 20 56 3d 22 69 74 6d 73 REQ_PWD" V="itms
0x805609d0: 22 2f 3e 0a 3c 56 20 4e 3d 22 43 57 4d 50 5f 44 "/>.<V N="CWMP_D
0x805609e0: 4c 5f 43 4f 4d 4d 41 4e 44 4b 45 59 22 20 56 3d L_COMMANDKEY" V=
0x805609f0: 22 22 2f 3e 0a 3c 56 20 4e 3d 22 43 80 56 0c dc ""/>.<V N="C.V..
0x80560a00: 80 56 07 1c 54 41 52 54 54 49 4d 45 64 00 11 04 .V..TARTTIMEd...
```

Router Backdoor

ANATEL

REPÚBLICA FEDERATIVA DO BRASIL
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

Certificado de Homologação

(Intransferível)

Nº 2352-12-5751

Validade: Indeterminada

Emissão: 11/09/2012

Solicitante:
BAYTEC TECNOLOGIA LTDA.
RUA ALUISIO AZEVEDO 40 ROCHA
20960050 RIO DE JANEIRO RJ

Fabricante:
OBJETIVOS Y SERVICIOS DE VALOR AÑADIDO
C/ MONTE ESQUINZA, 28 - 28010 2828010
MADRID

S&T TECHNOLOGY (SHEN ZHEN) CO.,LTD
BUILDING 12 THE SECOND INDUSTRIAL DISTRICT HOU REI VILLAGE XI XANG TOWN
SHENZHEN CITY, GUANGDONG PROVINCE - CHINA

Router Backdoor

Outras Unidades Fabris:

S&T TECHNOLOGY (SHEN ZHEN) CO.,LTD
BUILDING 12 THE SECOND INDUSTRIAL DISTRICT HOU REI VILLAGE XI XANG TOWN
SHENZHEN CITY, GUANGDONG PROVINCE - CHINA

Solicitante:

BAYTEC TECNOLOGIA LTDA.
RUA ALUISIO AZEVEDO 40 ROCHA
20960050 RIO DE JANEIRO RJ

BayTech [editar]

Address: Rua Aluisio Azevedo - 40 - Rocha - Rio de Janeiro-RJ / Brazil - CEP: 20960-050

Router Backdoor

https://sistemas.anatel.gov.br/sgch/HistoricoCe...

Apps | Bookmarks | Google Tradutor | Facebook Private... | Plex | Bitcoin Cotação | Outros favoritos

REPÚBLICA FEDERATIVA DO BRASIL
AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES.

ANATEL

Certificado de Homologação
(Intransferível)
Nº **02352-12-05751**
Validade: **Indeterminada**
Emissão: **11/09/2012**

Solicitante:
BAYTEC TECNOLOGIA LTDA.
RUA ALUISIO AZEVEDO 40 ROCHA
20960050 RIO DE JANEIRO RJ

Fabricante:
OBJETIVOS Y SERVICIOS DE VALOR AÑADIDO
C/ MONTE ESQUINZA, 28 - 28010 2828010
MADRID

Outras Unidades Fabris:
S&T TECHNOLOGY (SHEN ZHEN) CO.,LTD
BUILDING 12 THE SECOND INDUSTRIAL DISTRICT HOU REI VILLAGE XI XANG TOWN
SHENZHEN CITY, GUANGDONG PROVINCE - CHINA

Este documento homologa, nos termos do Regulamento para Certificação e Homologação de Produtos para Telecomunicações, aprovado pela Resolução Anatel nº 242, de 30 de novembro de 2000, o Certificado de Conformidade nº 06864/12 , emitido pela **OCD - IBRACE - Instituto Brasileiro de Certificação**. Esta homologação é expedida em nome do solicitante aqui identificado e é válida somente para o produto a seguir discriminado, cuja utilização deve observar as condições estabelecidas na regulamentação do(s) serviço(s) ou aplicação(ões) a que se destina.

SUBSTITUIDO

Tipo:
Modem Digital XDSL - Categoria I

Modelo(s):
RTA-04N 1T1R

Serviço/Aplicação:
Serviço Telefônico Fixo Comutado - STFC

Características técnicas básicas:
Equipamento para transmissão e recepção de dados em tecnologia ADSL, ADSL2 e ADSL2+:
Modos de Operação: G.dmt, G.Lite (espectro não sobreposto) e ANSI T1.413;
Capacidade máxima de Transmissão obtida em laboratório: Upstream: 1 Mbps / Downstream: 24 Mbps;
Interface ADSL para conexão à rede: suporte ao STFC por meio de conector RJ-11.

Transceptor de Radiação Restrita – Modulação Digital:
Faixa de freqüência: 2400 MHz a 2483,5 MHz;
Potência de Máxima de Transmissão: 0,117 W;
Tecnologia: Espalhamento Espectral Sequência Direta (DSSS) e OFDM;
Designação de Emissões: 16M5X9D (DSSS), 16M8X9D (OFDM), 18M2X9D (OFDM) e 38M0X9D (OFDM).
Ensaio de SAR não aplicável.
Observações:
Na instalação do produto devem ser observadas as condições de uso conforme estabelecido no Regulamento sobre Equipamentos de Radiocomunicação de Radiação Restrita.

Constitui obrigação do fabricante do produto no Brasil providenciar a identificação do produto homologado, nos termos do art. 39 do Regulamento anexo à Resolução Anatel nº 242, em todas as unidades comercializadas, antes de sua efetiva distribuição ao mercado, assim como observar e manter as características técnicas que fundamentaram a certificação original.

As informações constantes deste certificado de homologação podem ser confirmadas no SGCH - Sistema de Gestão de Certificação e Homologação, disponível no

Router_anatel.png | Routercmd006....png | Man_router2.png | Exibir todos

Internet das coisas

Vídeo flagra hackers roubando carro Tesla Model S

Criminosos usaram tablet para roubar sinal da chave; ação durou cerca de três minutos

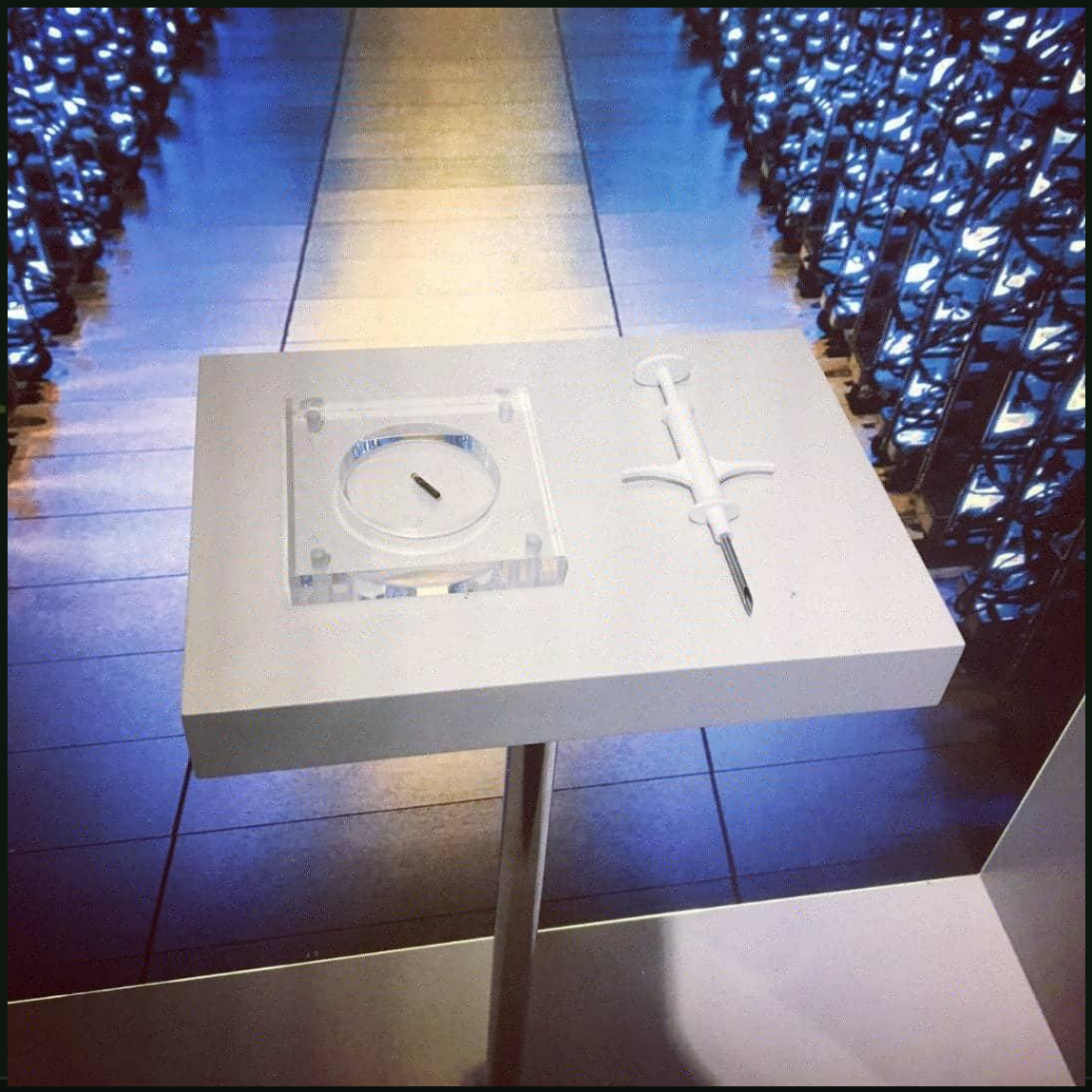
O Globo
23/10/2018 - 14:11 / Atualizado em 23/10/2018 - 15:36

O Tesla Model S foi roubado por volta das 2h de domingo. Ação foi flagrada por câmeras de segurança Foto: Reprodução/YouTube

Biochip implantável

Biohacking

Biochip implantável



Biochip implantável

Especificações:

- Identificador único e imutável
- 888 bytes de memória programável
- Compatível com ISO 14443-A
- Cilindro de 2x12 milímetros
- Frequência de operação RFID: 125 KHz
- Frequência de operação NFC: 13.56 MHz
- NFC compatível com tipo 2

Biochip implantável

Biochip flexível

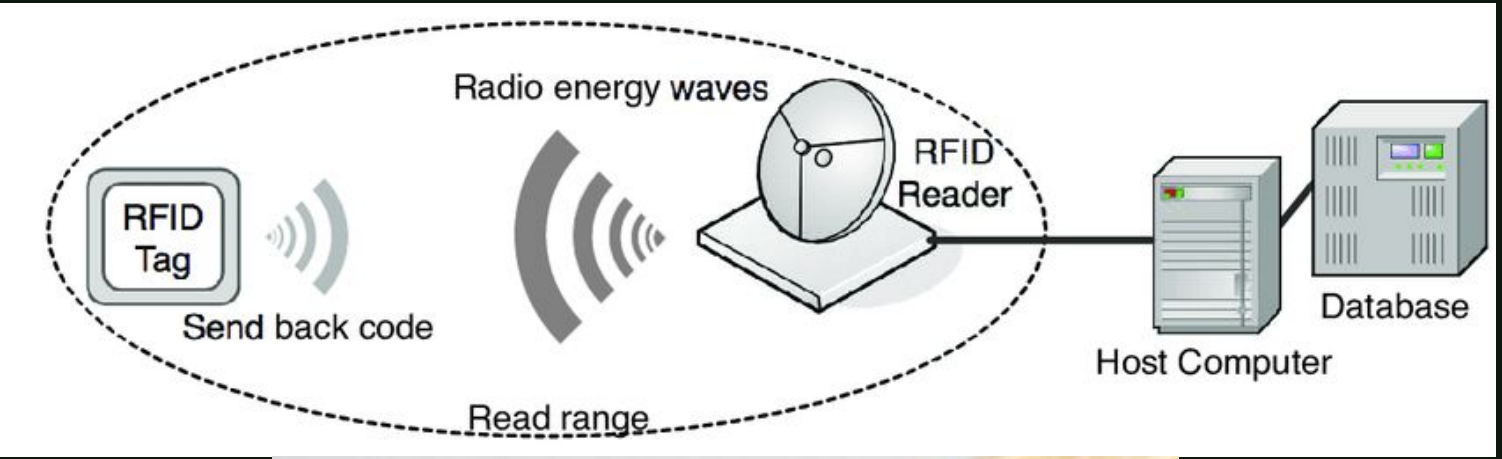
Biochip implantável

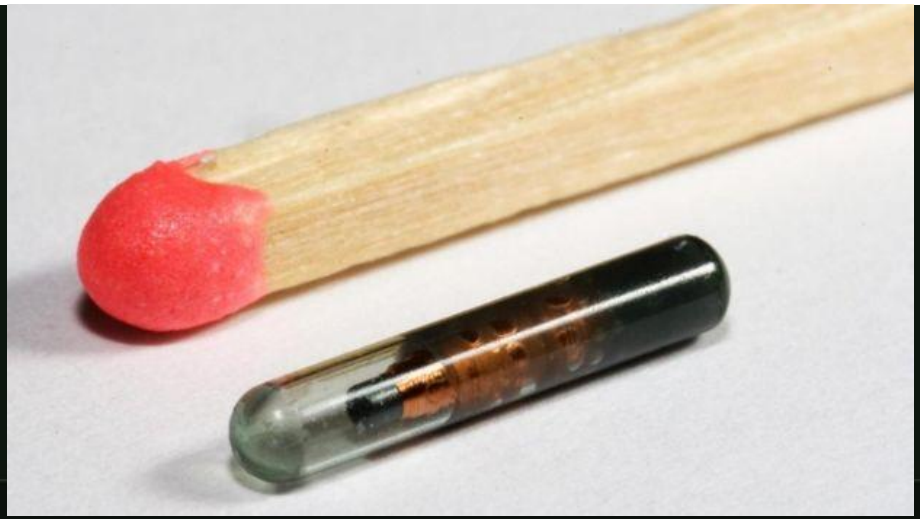
Biochip flexível

Biochip implantável

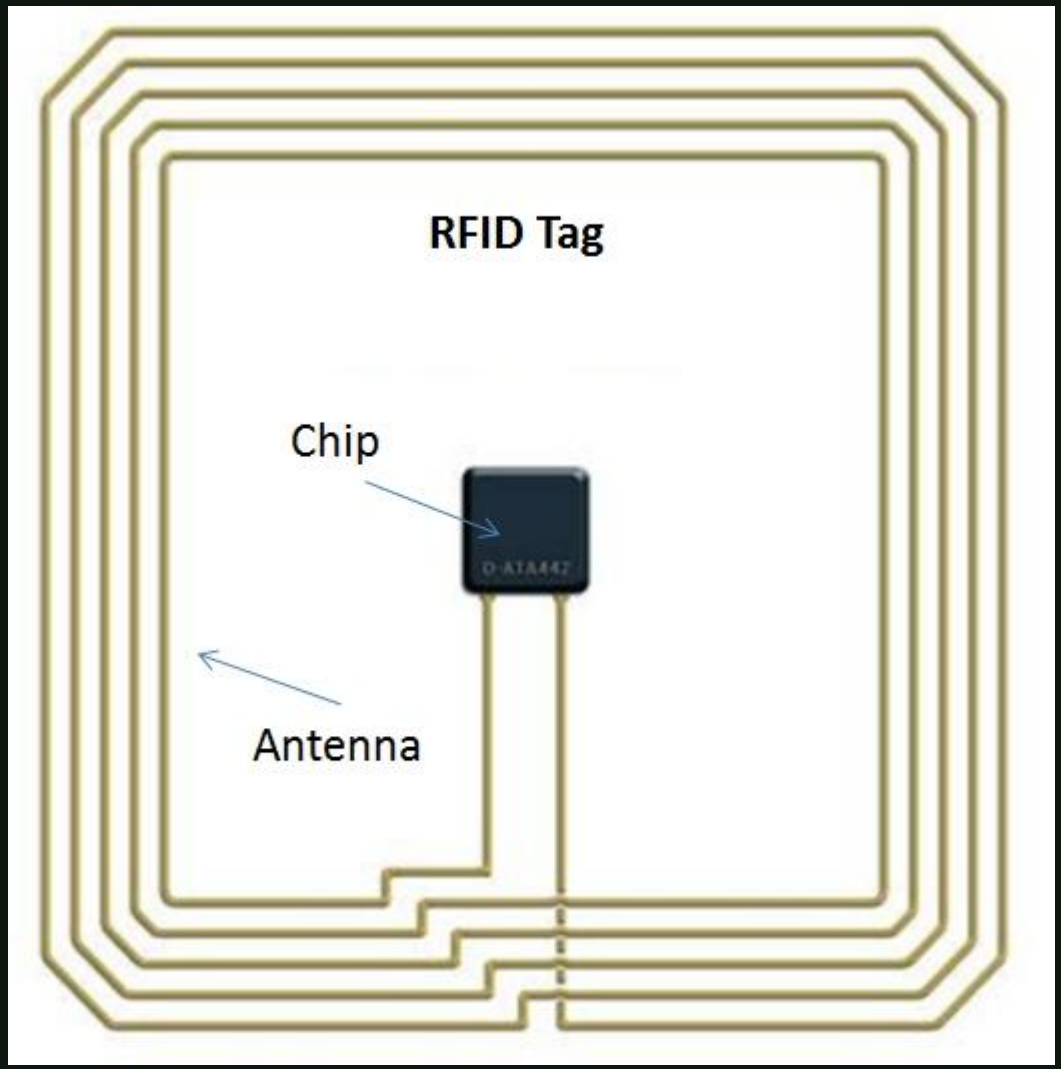
Biochip implantável

Funcionamento

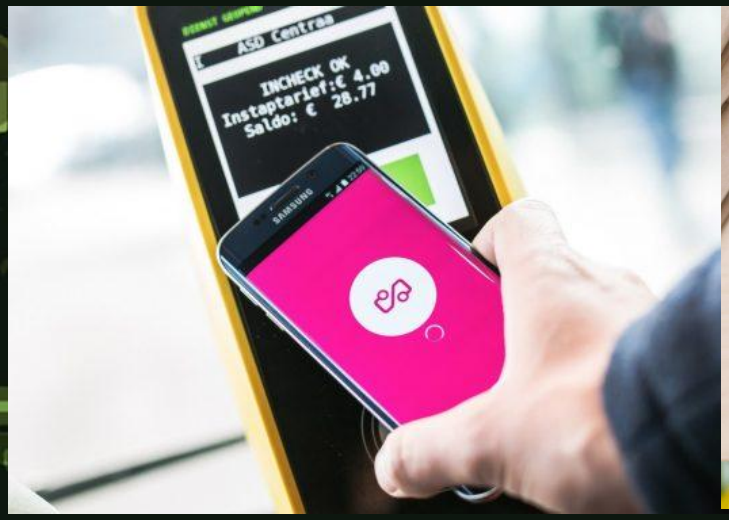


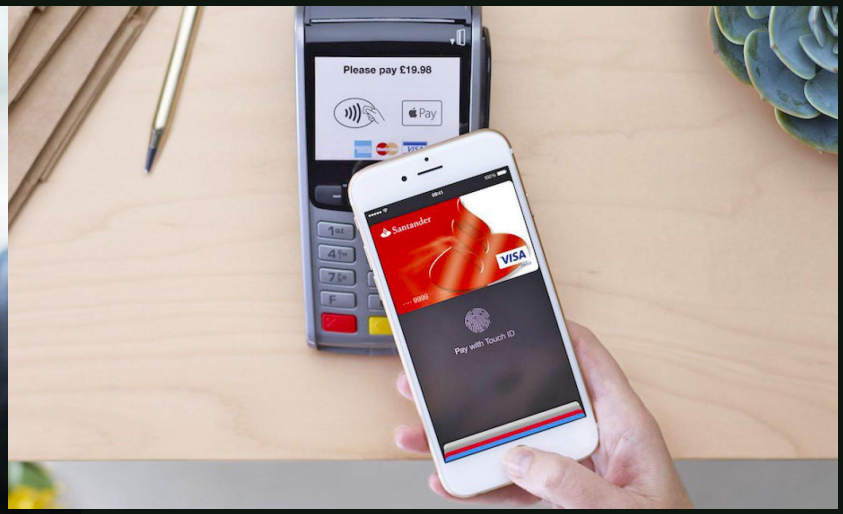


Biochip implantável



Biochip implantável





Biochip implantável

Biochip implantável

Biochip implantável

Smart Gun

Biochip implantável

Smart Gun

Biochip implantável

Hacker implanta chip na mão para invadir aparelhos Android

Com a técnica, criminosos podem roubar dados e assumir o controle de um aparelho

Forbes

117,172 views | Apr 27, 2015, 06:03am

Hacker Implants NFC Chip In His Hand To Bypass Security Scans And Exploit Android Phones

Biochip implantável

Hacker invade celular com chip implantado nas mãos

Rose Eveleth
Da BBC Future

6 julho 2015

Seth Wahle (à esq.) e Rod Soto querem alertar sobre vulnerabilidade de aparelhos

Seth Wahle é um entre um número cada vez maior de pessoas que têm um chip implantado no corpo. O ex-suboficial da Marinha americana e hoje engenheiro da empresa APA Wireless é um "biohacker" – alguém que gosta de brincar com os limites do corpo humano.

Agora, Wahle usa o chip para oferecer uma intrigante janela para o futuro da segurança cibernética.

Com a microestrutura instalada em sua mão, ele e seu parceiro de negócios, Rod Soto, conseguiram provar que ele pode hackear um celular apenas segurando-o nas mãos.

Atualidade

51% das empresas brasileiras foram vítimas de ransomware em 2016

Levantamento ainda mostra que 56% das organizações não possuem tecnologia para detectar comportamento suspeito e setor de Educação é o mais atacado (82%), seguido do Governo

Por: Redação, 13/03/2017 às 16h23 - Atualizado em 15/03/2017 às 17h20

Atualidade

Ransomware

Vítima de vírus, Telefónica usa megafone para pedir desligamento de computadores

De acordo com a agência de inteligência espanhola, Telefónica foi uma das vítimas de um “ataque massivo” lançado esta manhã

Redação com AFP [12/05/2017] [12:08]

Atualidade

Fábrica de processador do iPhone foi atingida pelo vírus WannaCry

Fornecimento de chips para o próximo iPhone pode sofrer atraso

Por Paulo Alves, para o TechTudo

08/08/2018 15h02 · Atualizado há 10 meses

Atualidade

THE NEW YORK TIMES

Medida de Trump tenta barrar Huawei nos EUA e intensifica guerra com a China

Teles americanas serão proibidas de usar equipamentos chineses para instalações de rede 5G

Atualidade

maio 06, 2019

ISRAEL ATACA PRÉDIO QUE ABRIGAVA HACKERS NA FAIXA DE GAZA

—

As Forças de Defesa de Israel (IDF) afirmam que tiveram sucesso ao neutralizar uma tentativa de ciberataque contra o país ao explodir um prédio localizado na Faixa de Gaza. Segundo a IDF, os ataques hacker foram rastreados até o prédio em questão, que recebeu ataques aéreos via drones.

Atualidade

Conversas de Moro com procuradores e ação de hacker serão investigadas

PF vai apurar ataque, enquanto corregedoria abre procedimento sobre atuação de Dellagnol

Gustavo Maia, Jussara Soares, Aguirre Talento, Natália Portinari, Bruno Góes, Daniel Gullino e G1
10/06/2019 - 22:41 / Atualizado em 11/06/2019 - 15:16

O ministro da Justiça e ex-juiz Sergio Moro e o promotor Deltan Dallagnol Foto: Ailton de Freitas / Agência O Globo

Atualidade

STUART MADNICK, DO MIT: "O HACKER TEM MAIS VANTAGENS NUM ATAQUE VIRTUAL"

Um dos maiores especialistas mundiais no combate a crimes virtuais, o professor do Massachusetts Institute of Technology diz que as empresas estão pouco preparadas para combater hackers

Leo Branco
08/06/2019 - 15:00 / Atualizado em 10/06/2019 - 17:29

- https://www.senado.gov.br/noticias/Jornal/emdiscussao/defesa-nacional/razoes-para-a-implementaao-da-estrategia-nacional-de-defesa/inimigos-invisiveis-a-guerra-cibernetica.aspx
- http://www.defesanet.com.br/cyberwar/noticia/29114/O-maior-evento-brasileiro-de-Defesa-Cibernetica--Comunicacoes-e-Guerra-Eletronica/