

Segurança de IoT

João Rocha, MSc, CISSP, CISA
Executivo IBM Security Brasil
joaoplr@br.ibm.com



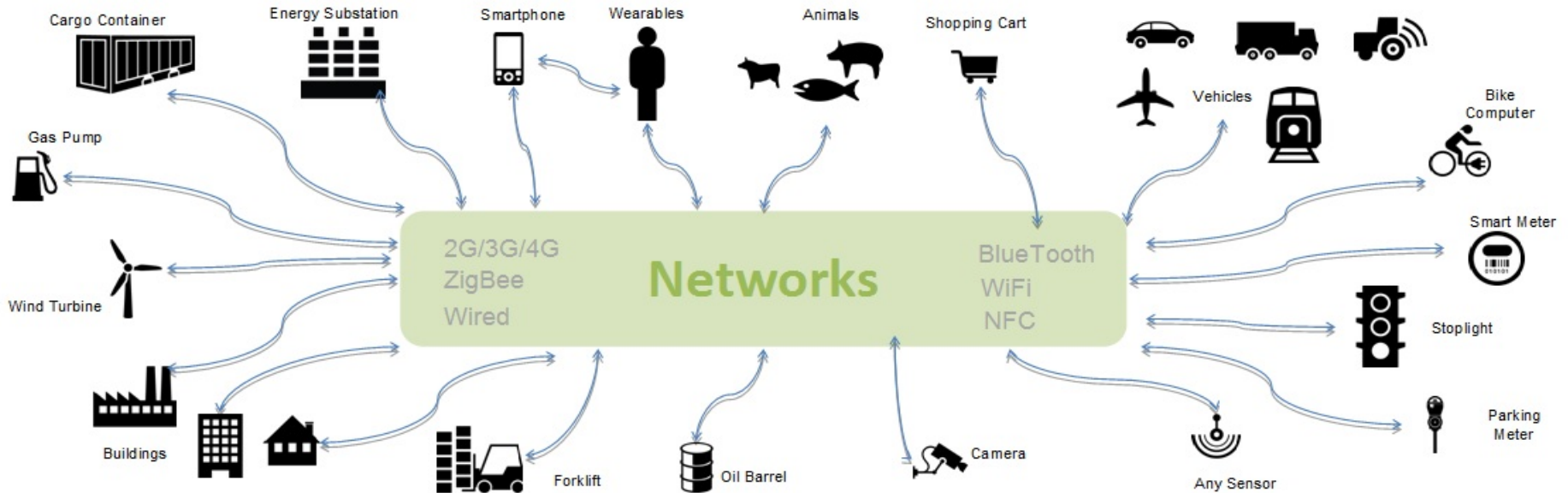


Intuitivo



IoT em Números....uma enorme escala e impacto

“Things” refer to any physical object with a device that has its **own IP address** and can **connect & send/receive** data via a **network**



A Cadeia de Valor do IoT



Processadores

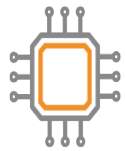
Dispositivos IoT

Gateways

Redes

Nuvem

Soluções e Aplicações



Oil & Gas	Energy & Utilities
Smarter Cities	Consumer Electronics
Connected Vehicle	Transport & Rail
Life Science & Healthcare	Industrial Manufacturing



E a Segurança?

PERIGO DE VÍRUS

Baseado em dica do FBI, MP-DF recomenda que roteadores sejam reiniciados

7 de junho de 2018, 17h21

 [Imprimir](#)  [Enviar](#)   0  

Após o FBI ter identificado um risco de contaminação por vírus em roteadores, o Ministério Público do Distrito Federal agora recomenda medidas de segurança para a população brasileira. Segundo a Comissão de Proteção dos Dados Pessoais do MP-DF, todos os proprietários brasileiros devem reiniciar os aparelhos para interromper temporariamente o vírus, chamado de VPNFilter.

O MP-DF recomenda, ainda, a desativação das configurações de gerenciamento remoto e o uso de senhas fortes. Também é importante atualizar o software (firmware) do roteador.

Os aparelhos infectados podem coletar dados pessoais, bloquear o tráfego de internet e direcionar os usuários para sites falsos de instituições bancárias e de comércio eletrônico.



Invadindo cassino através de um aquário?

- Monitorar PH e temperature da água
- Alimentação automática dos peixes



Hackeando babá eletrônica?

“Wake up, baby!”



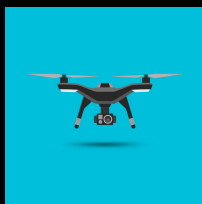
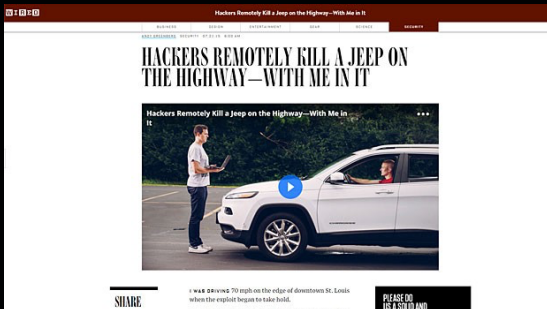
Derrubando uma petroquímica com ajuda de uma cafeteira

- Máquinas atuais são conectadas e exibem propagandas, informações, notícias
- Ataque Ransomware nos desktops
- Isolados e formatados mas ataque continuava
- Máquinas de cafés exibiam a mesma mensagem do Ransomware
- Máquina conectada de forma errada na rede local
- Estações de trabalhos da petroquímica eram de tradicional sistema operacional sem pacote de correção SMB v1

Marcapassos

- Não possuem **criptografia**
- **Alertaram** em 01/2017 – ainda hoje existe
- **Hackear** Através do Carelink 2090 (usado por medicos)
- Alterar **choques** enviados ao marcapasso

E parou por aí?



Existem **várias ameaças potenciais** para todas as indústrias

Quanto mais **dispositivos conectados**

↳ aumenta a quantidade de **vulnerabilidades**

↳ cresce o potencial de **cyber-ataques**

↳ causando enorme **impacto** nos usuários e empresas

Industrial control systems hacked

*Alarm sensors
knocked out*

Vehicle theft

*Remote control on
pacemakers*

Ransomware

*Malware on a fuel
system*

Plant stoppages

Mensagem: Segurança não é necessariamente um obstáculo para IoT, mas um requisito **fundamental** para ser considerado nos processos de desenho, implementação e operação dos ambientes.



5 fatos incontestáveis sobre a Segurança em IoT



Dispositivos vão operar em ambientes hostis

- Visibilidade e controle da implantação e distribuição dos IoT deve ser considerada na arquitetura



Segurança do Software irá degradar com o tempo

- O processo de correções acontecerá em um ambiente muito distribuído e muitas vezes sem controles
- Defesas de Sistema devem ser atualizadas continuamente por toda a vida dos dispositivos



Segredos compartilhados não permanecem secretos

- Dispositivos IoT tem credenciais conhecidas “de fábrica”
- Senhas padrão não secretas, mas sim ameaças potenciais



Problemas de configuração persistirão

- Cabe aos usuários a decisão de habilitar ou não as opções de segurança



Quanto mais dados acumulam, maiores os problemas de exposição

- Dispositivos IoT estão acumulando cada vez mais dados sensíveis e também dados pessoais




OBRIGADO


FOLLOW US ON:

 ibm.com/security

 securityintelligence.com

 ibm.com/security/community

 xforce.ibmcloud.com

 [@ibmsecurity](https://twitter.com/ibmsecurity)

 youtube.com/user/ibmsecuritysolutions

© Copyright IBM Corporation 2018. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.