ABIN

Presidência da República
Gabinete de Segurança Institucional
Agência Brasileira de Inteligência

Proteção de Infraestruturas Críticas contra Ataques Cibernéticos

Alisson Raposo

31 de julho de 2019

ABIN

Roteiro

- ✓ Conceito de Infraestruturas Críticas
- ✓ Incidentes em Infraestruturas Críticas
- ✓ Sistemas SCADA
- ✓ Diferenças para a TI Tradicional
- ✓ Caso Stuxnet
- ✓ Ransomware
- ✓ Boas Práticas

Atribuição Institucional

Lei 9.883, de 7 dez 99

Art. 4º. *- À ABIN, ..., compete:*

I - ...

II - planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade;

*III - **avaliar as ameaças**, internas e externas, à ordem constitucional;*

IV - ...

Infraestruturas críticas

*São os sistemas que compõem a infraestrutura de um Estado, para os quais a **continuidade da operação** é tão importante que a perda, interrupção significativa ou degradação dos serviços poderia ter **graves consequências**, econômicas, políticas e, sobretudo, sociais.*

Incidente na planta nuclear de Davis-Besse

- Em janeiro de 2003, a planta nuclear de Davis-Besse no porto de Oak, no estado do Ohio/EUA, foi infectada com o worm "Slammer".
- A causa do incidente? Uma conexão de rede do laptop de um consultor permitiu que o virus se propagasse na rede de controle, "bypassando" o firewall da planta nuclear.
- Como resultado, os parâmetros de segurança apresentados pelo sistema ficaram *offline por quase* 5 horas e o computador de processos da planta ficou indisponível por 6 horas.
- Felizmente, o reator nuclear estava *offline* no momento em que o incidente ocorreu.

Incidente em plantas da Daimler-Chrysler

• Em agosto de 2005, 13 plantas norte-americanas foram desligadas por um simples worm.

→ Apesar de firewalls profissionais instalados entre a Internet e a rede da empresa, o worm encontrou uma forma de entrar no sistema de controle (provavelmente por meio de um laptop).

→ Uma vez no sistema de controle, ele foi capaz de passar de planta para planta em segundos.

• Aproximadamente 50.000 trabalhadores de campo ficaram parados durante os desligamentos das plantas.

• A causa do incidente? Códigos maliciosos introduzidos através de um caminho secundário na rede.

• O custo estimado do impacto foi de US$ 14,000,000.00.

Incidente de segurança em Browns Ferry

• Em agosto de 2006, operadores da planta nuclear de Browns Ferry, no Tennessee/EUA, tiveram que desligar o reator da usina. Motivos:

- Bombas de recirculação dos reatores 3A e 3B se desligaram após as suas variáveis de frequência de operação terem sido colocadas em estado inoperante.

- O PLC controlador do condensador de desmineralização também falhou, no mesmo momento.

- O tráfego excessivo entre dois produtos de controle de diferentes fabricantes.

• As falhas foram atribuídas aos controladores das conexões Ethernet para as redes ICS ("Integrated Computer System") das plantas, e tráfego excessivo nesta rede.

• A planta ficou off-line por 2 dias, com prejuízo estimado de US$ 600,000.00.

Estônia 2007: cyber war?

- Três semanas de ataques contra a infraestrutura da Estônia, atribuídos à Rússia.

Diversas ocorrências, desde então...

Ataque global de hackers afeta Brasil mais de 70 países

Computadores de diferentes áreas do governo são alvos de vírus. Postos do INSS paralisaram atendimento

POR BRUNO DUTRA
12/06/2017 16:39 / atualizado 12/06/2017 16:23

Países afetados pelos hackers - Reprodução/

02/10/2010 08h00 - Atualizado em 02/10/2010 17h29

Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia

Stuxnet usou brecha grave no Windows para infectar sistemas eletrônicos. De origem desconhecida, praga virtual tem remoção difícil.

Altieres Rohr
Especial para o G1

Imagem de arquivo da agência iraniana Isna mostra a primeira usina atômica do Irã, Bushehr (Foto: AP)

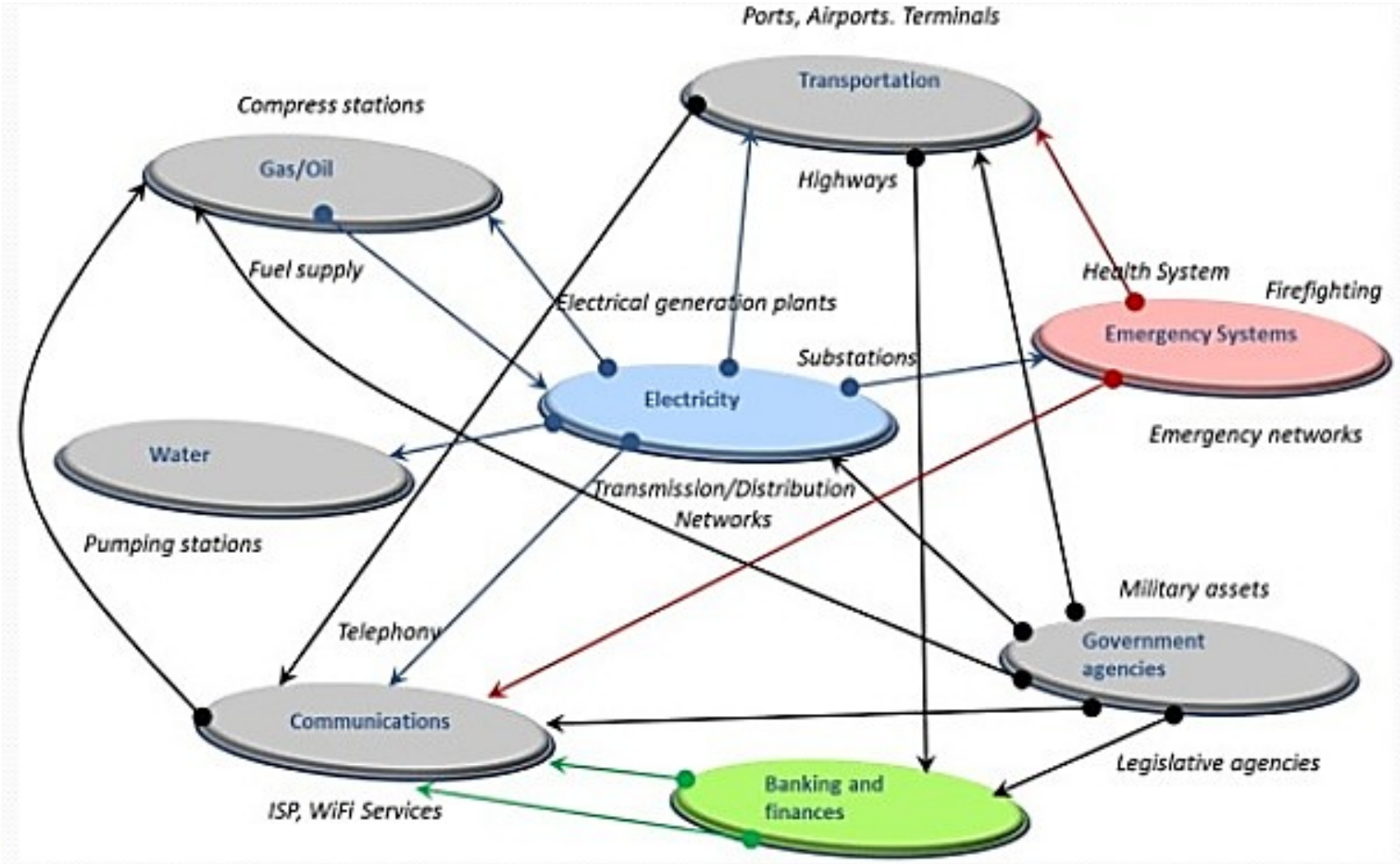
O ataque mais sofisticado já realizado. É dessa forma que pode ser resumido o Stuxnet, um vírus para computadores cujas origens são desconhecidas, mas especula-se que tenha sido obra de um governo. A praga não tem o intuito de roubar dados bancários ou exibir anúncios. Na verdade, ela ataca sistemas usados no controle de equipamentos industriais, e teria chegado a infectar sistemas usados em instalações nucleares do Irã e da Índia.

Para conseguir essa façanha, o vírus utilizou brechas graves e antes desconhecidas no
se capaz de pará-lo. Agora, pesquisadores

Redes do governo sofrem 2.828 ataques cibernéticos em apenas três meses

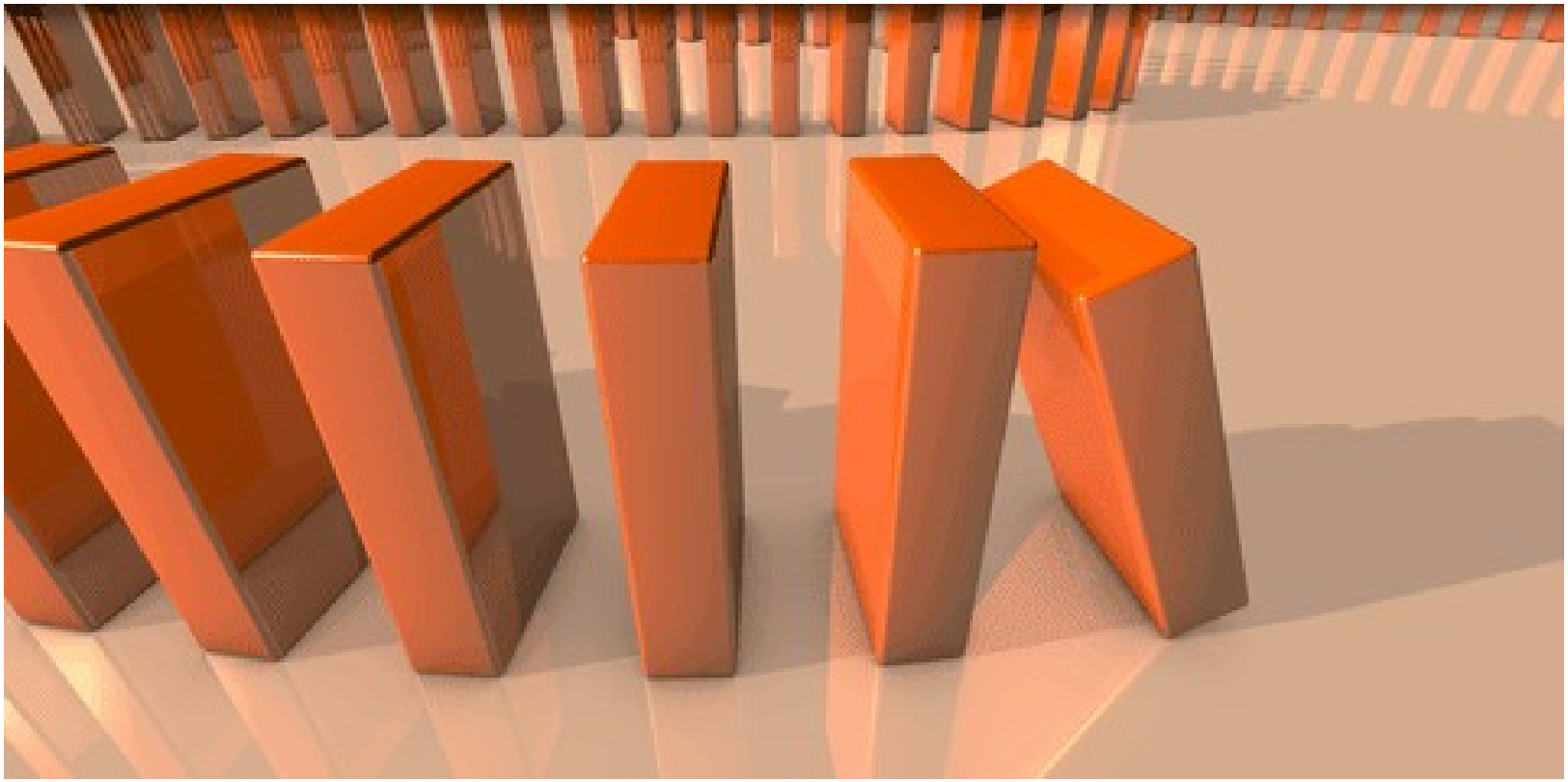
Tentativas de invasão no 1º trimestre buscam acessar e-mails e derrubar portais

Interdependência



Interdependência

Efeito Dominó



O que esses exemplos têm em comum?

- **Alvos fáceis**

- Computadores da maioria das redes de supervisão rodam 24x7 com pouca ou nenhuma oportunidade de instalar atualizações de segurança para seus Sistemas Operacionais e software antivirus.

- Redes de controle são otimizadas para executar operações de I/O em tempo real e não para robustas conexões de rede.

- **Pobre segmentação de rede**

- Muitas redes de supervisão são "abertas", sem isolamento entre diferentes subsistemas.

- Como resultado, os problemas se espalham rapidamente pelas redes.

- **Múltiplos pontos de entrada nas redes**

- A maior parte dos incidentes de segurança são originados a partir de pontos de entrada secundários nas redes.

- Dispositivos USB, conexões de manutenção, laptops, etc.

Sistemas SCADA - Supervisory Control and Data Acquisition Systems

A maior parte das Infraestruturas Críticas é controlada por um conjunto de computadores dedicados chamados SCADA - *Supervisory Control and Data Acquisition Systems*, compostos por:

- *Sistemas de controle de processos*
- *Sistemas de controles distribuídos (DCS)*
- *Programmable Logic Controllers (PLC)*
- *Intelligent Electronic Device (IED)*
- *Human Machine Interface (HMI)*

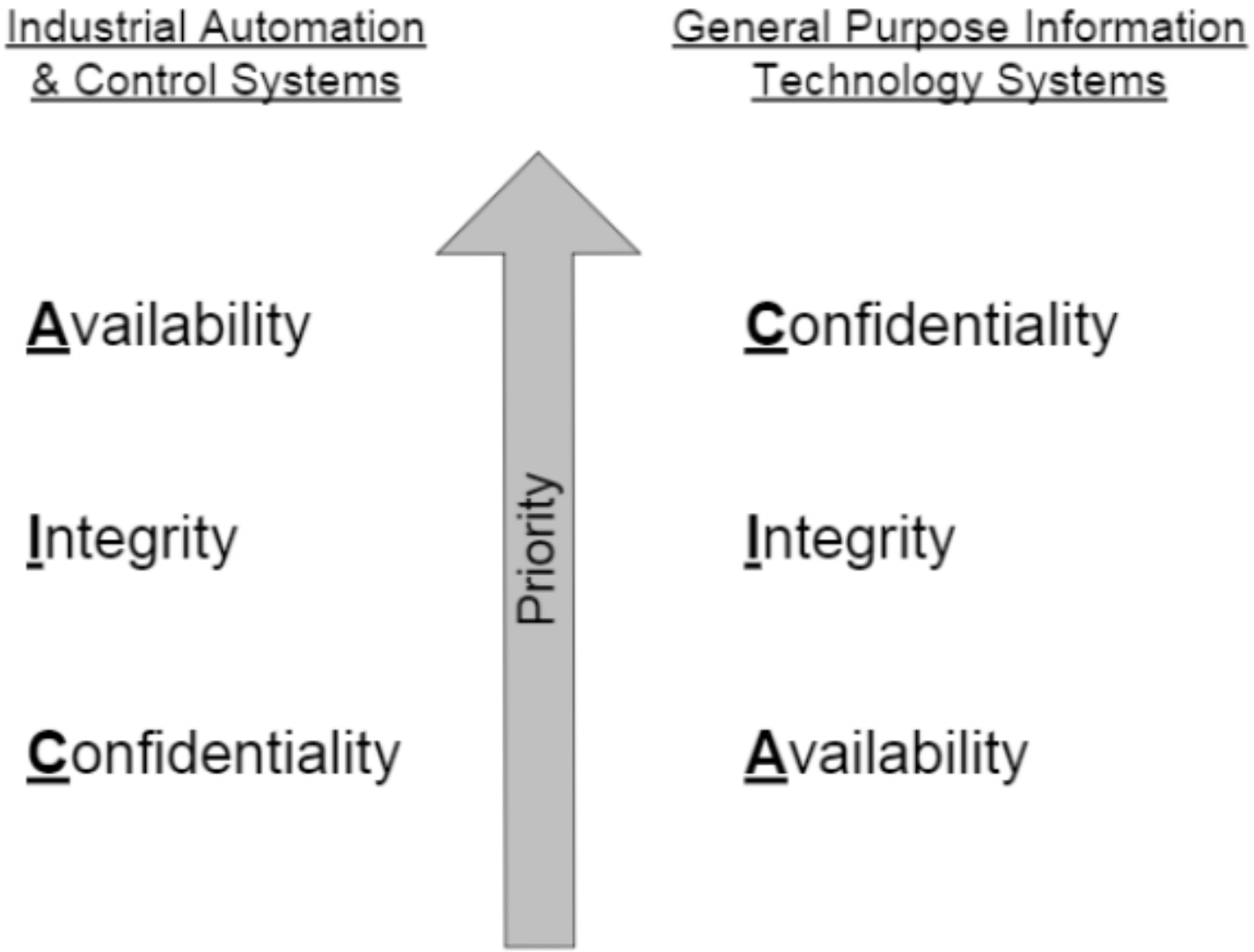
Sistemas SCADA - Supervisory Control and Data Acquisition Systems

*Na **TI**, a integridade dos dados e a proteção de ativos são a prioridade.*

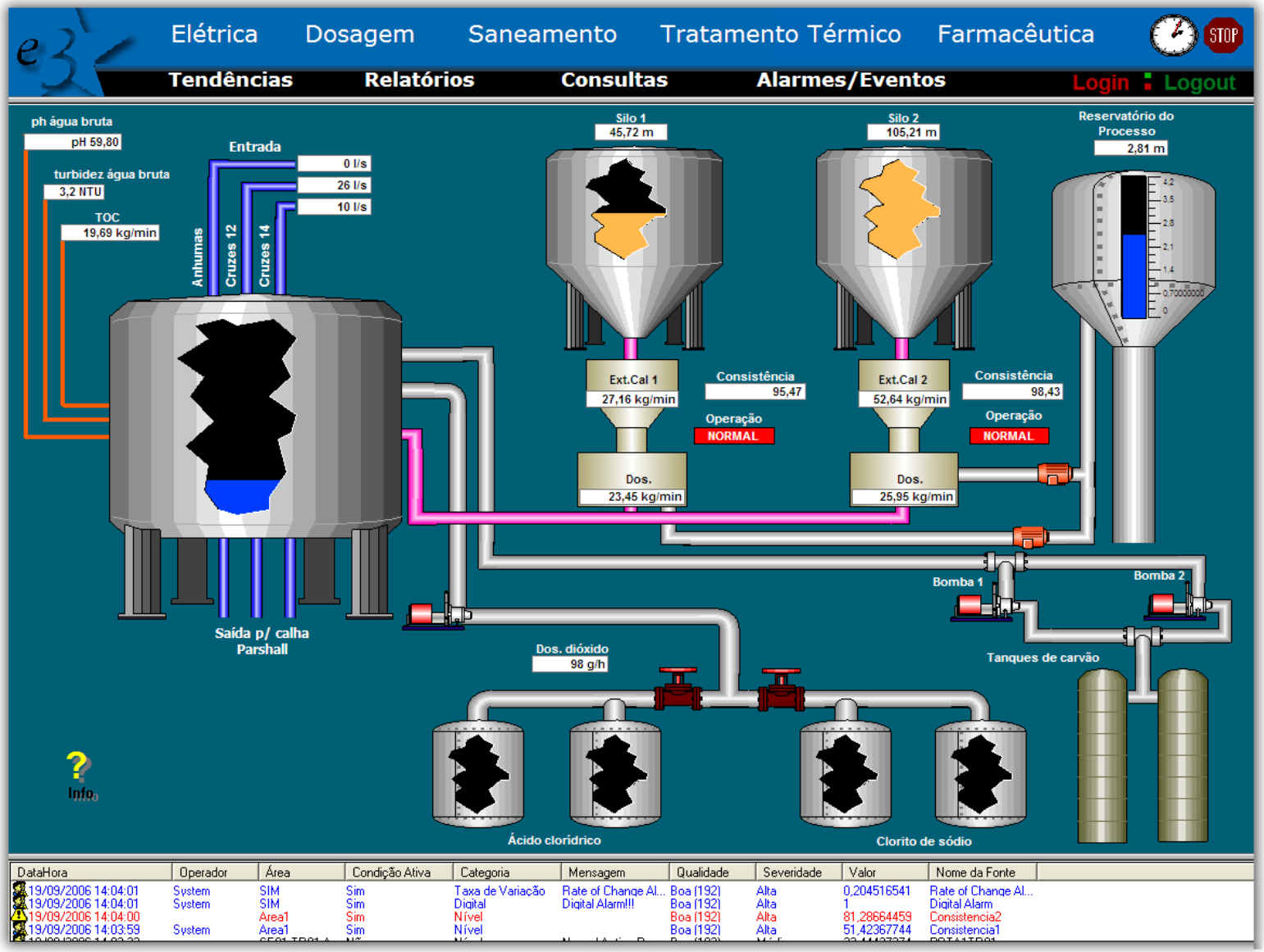
*Em **automação**, a segurança da planta é o mais importante.*

*Os Sistemas de Supervisão são projetados para terem altíssima **disponibilidade**.*

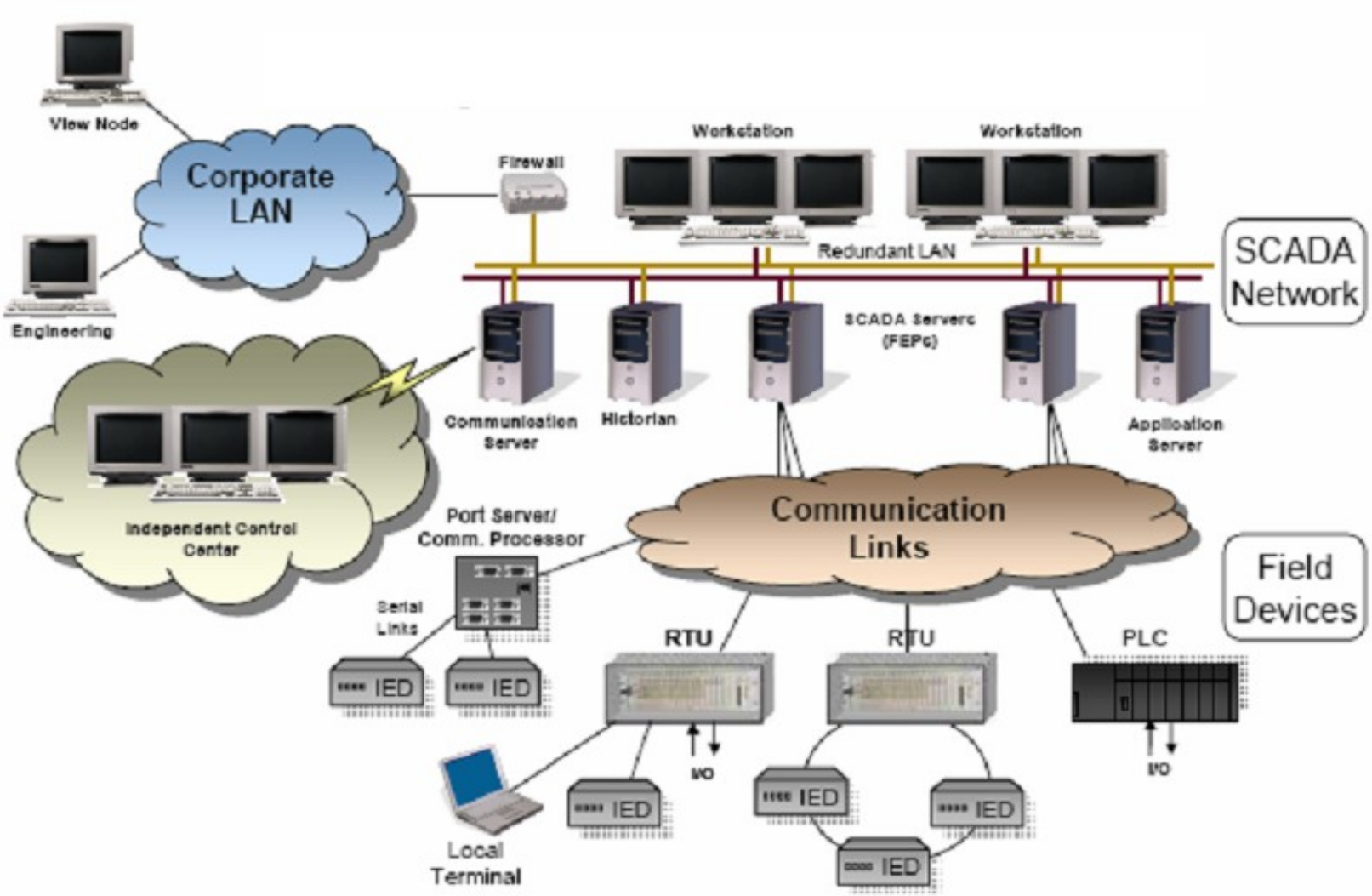
Sistemas SCADA x TI



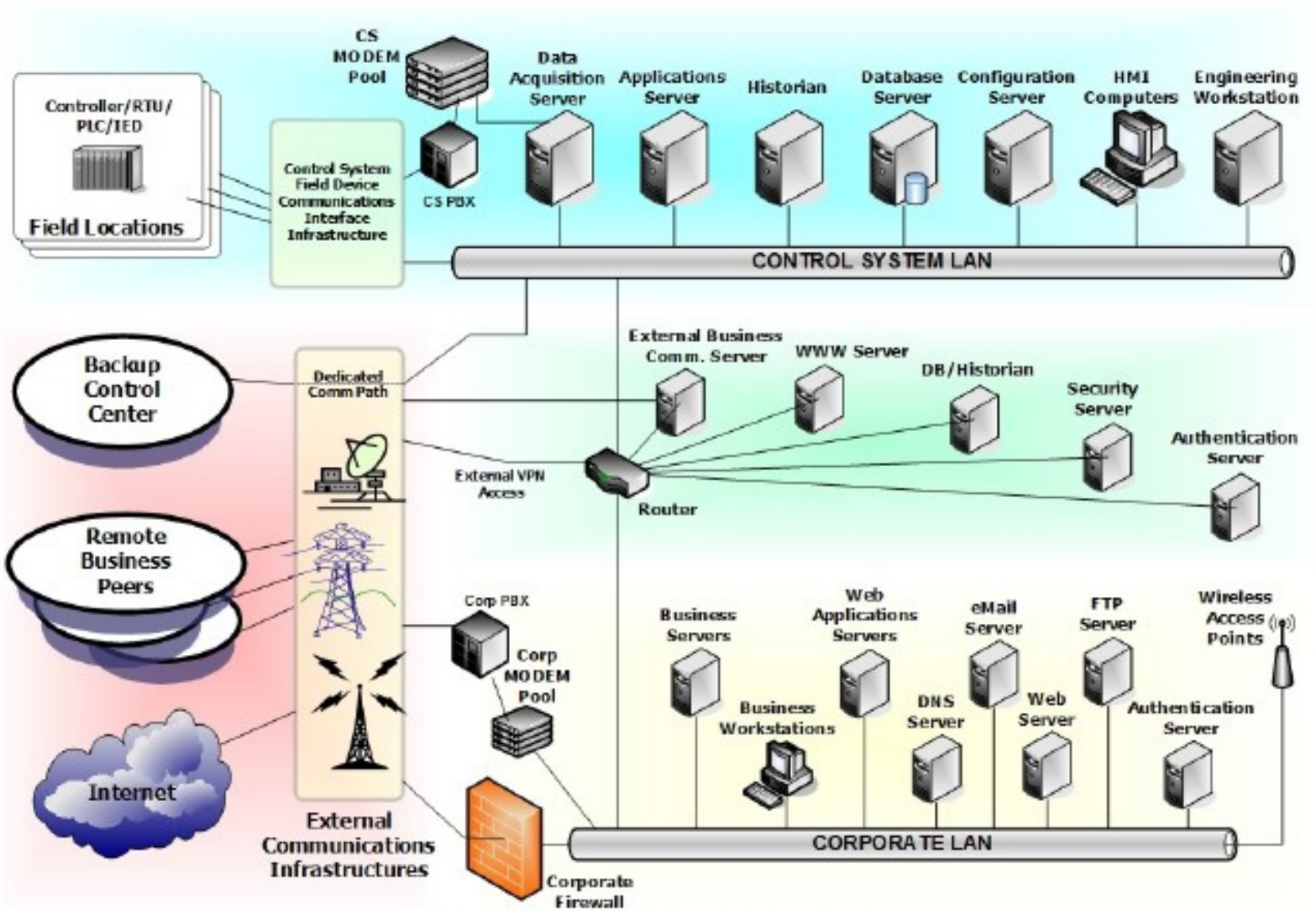
Sistemas SCADA - Interface



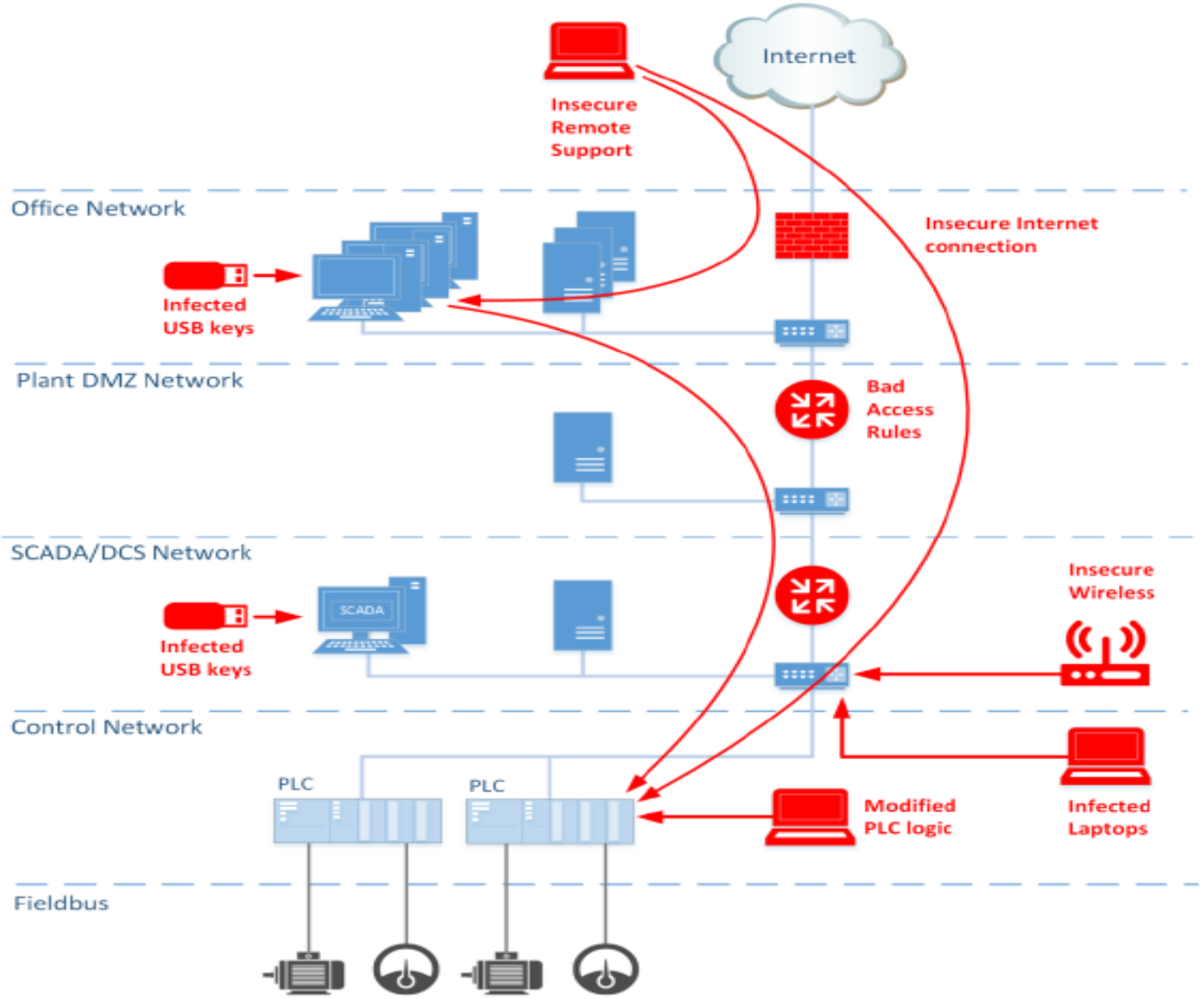
Sistemas SCADA – Ontem



Sistemas SCADA – Arquitetura típica

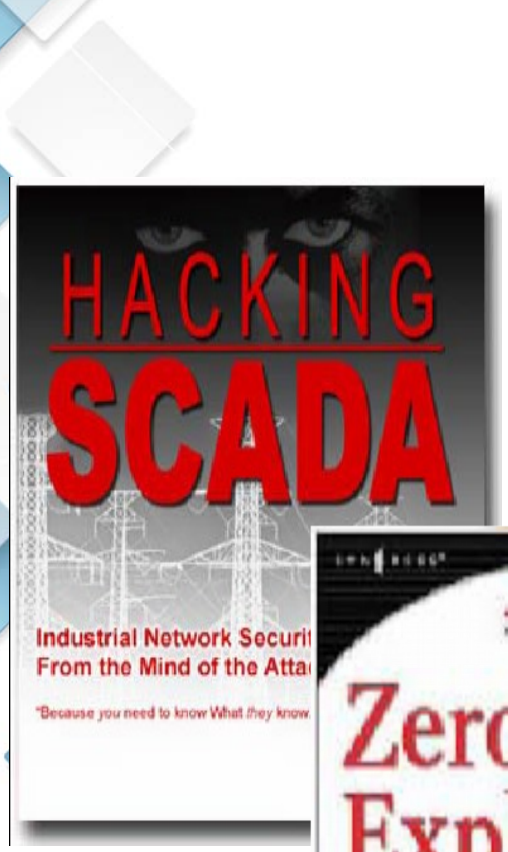


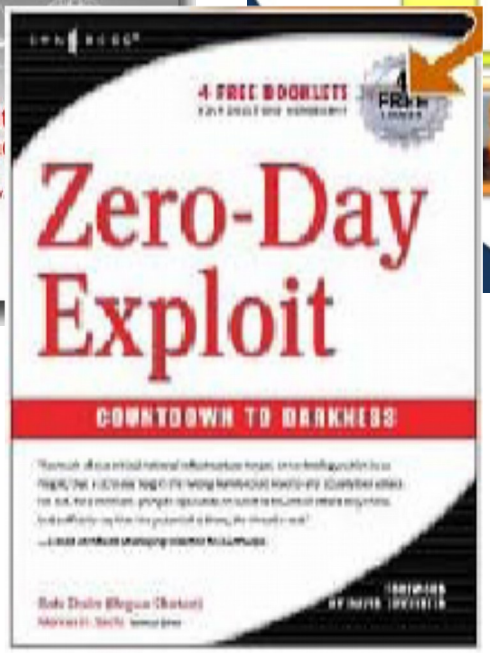
Sistemas SCADA – Vetores de ataques

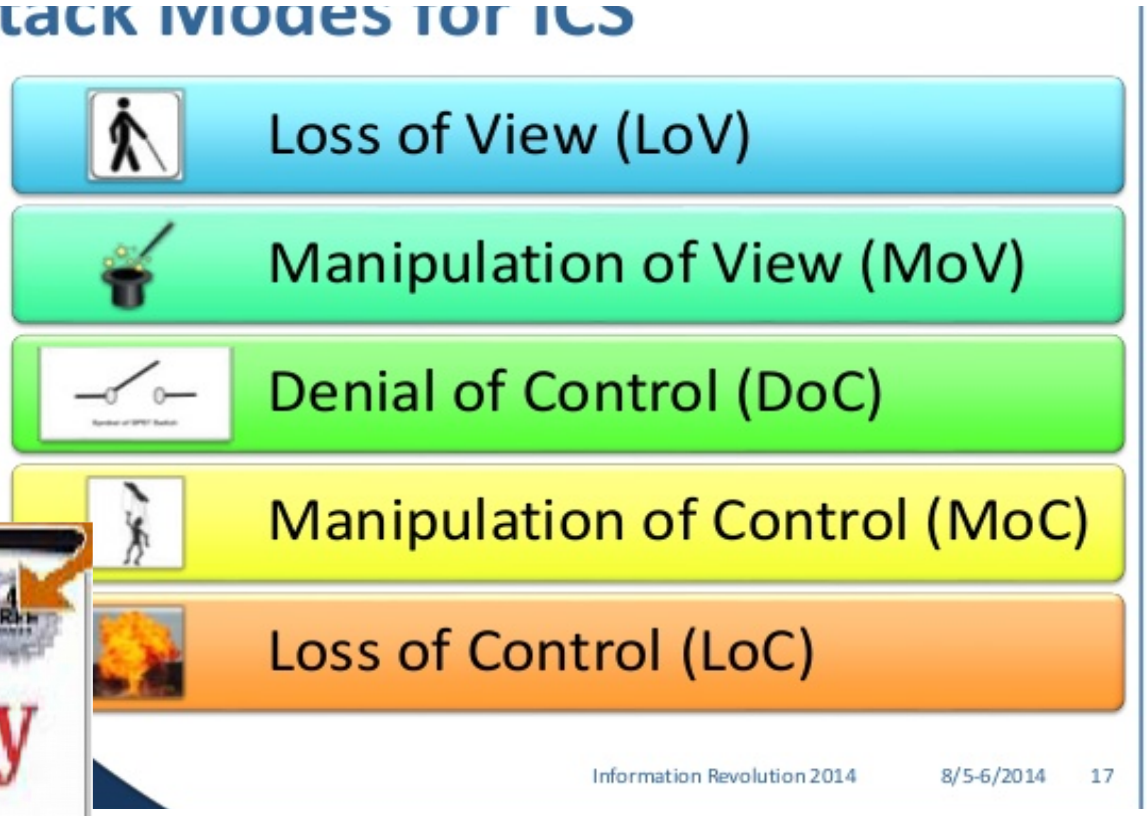


ITEM DE SEGURANÇA	Na Tecnologia da Informação	Nos Sistemas de Controle
Antivírus	Amplamente utilizado	Difícil ou impossível implantação
Suporte da tecnologia	2 a 3 anos, com fornecedores diversos	Acima de 20 anos, com um único fornecedor
Terceirização	Amplamente utilizada	Utilizada, mas muito especializada
Aplicação de patches	Agendamento regular	Muito rara
Troca de gestão	Normal	Complexa
Tempo de conteúdo crítico	Normalmente atrasos são aceitos	Atrasos são inaceitáveis
Disponibilidade	Normalmente atrasos são aceitos	24 x 7 x 365 (contínua)
Consciência de segurança	Moderada/alta, tanto no setor público como no privado	Pobre, exceto para segurança física
Teste ou Auditoria de Segurança	Parte de uma boa Política de Segurança	Raros ou ocasionais
Segurança Física	Segura (servidores, salas-cofre etc.)	Remota / Automatizada

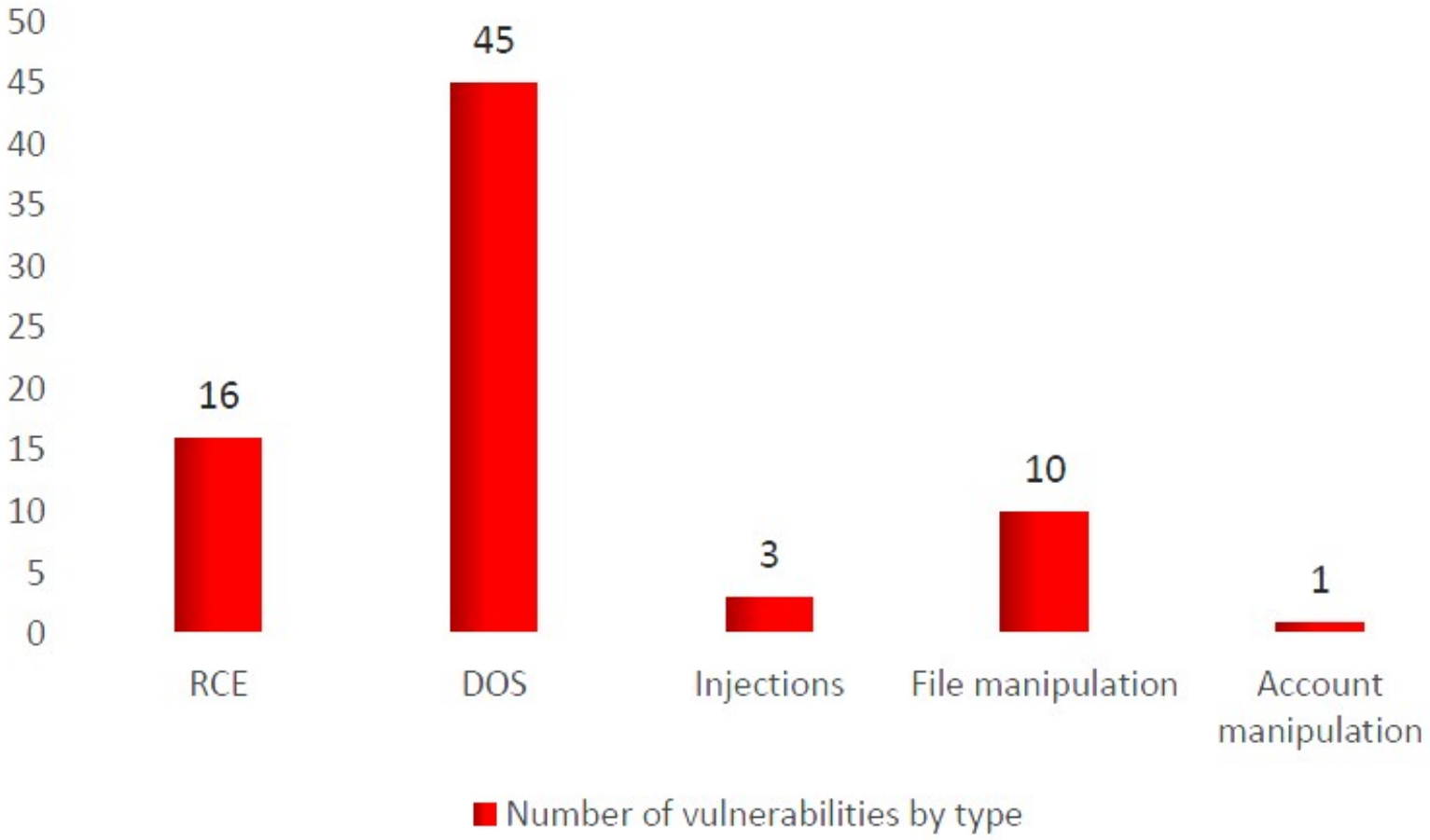
Sistemas SCADA – Tipos de Ataques





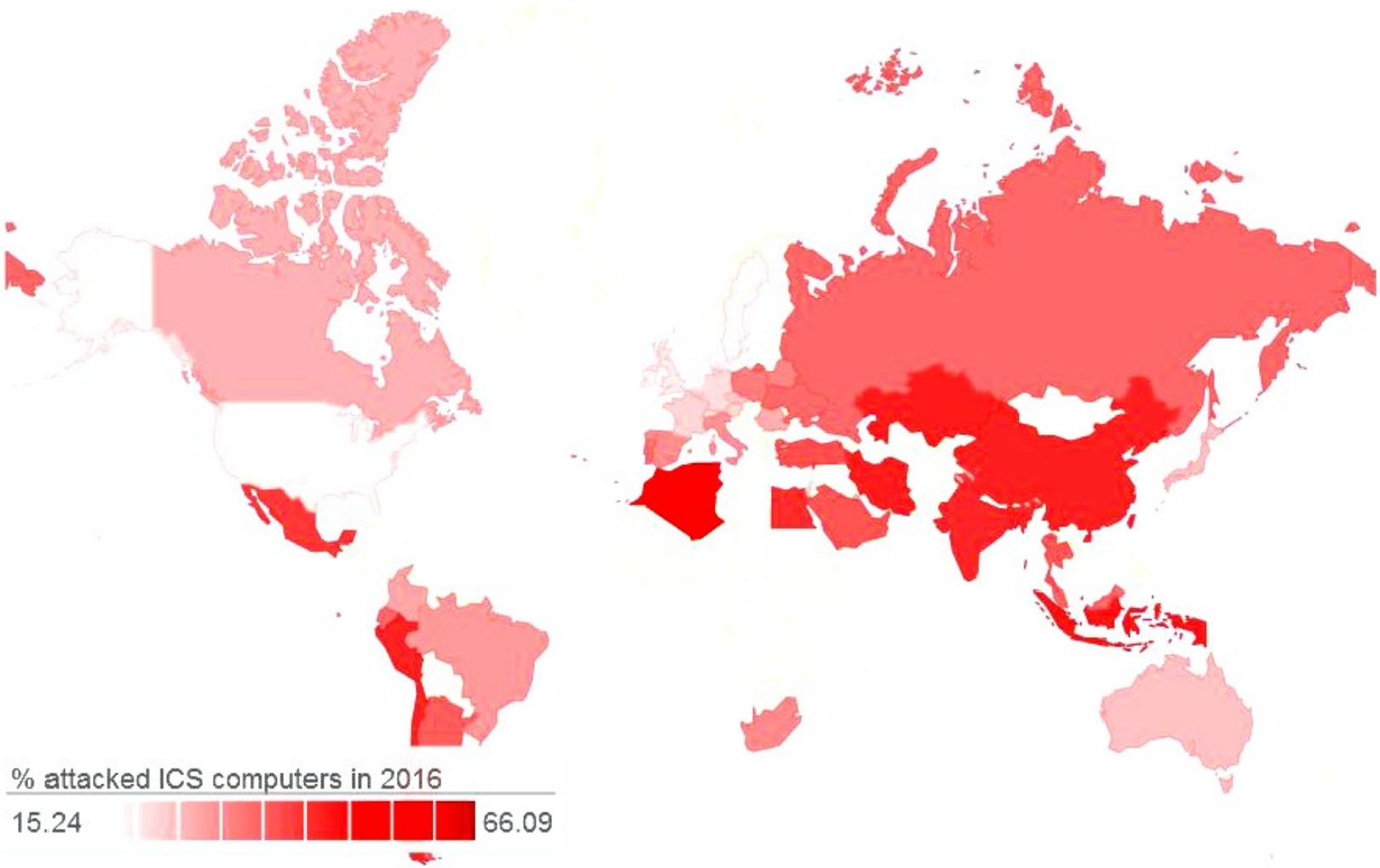


Sistemas Scada – Vulnerabilidades



Distribution of vulnerabilities uncovered by Kaspersky Lab in 2016 according to the ways in which they can be used

Sistemas Scada – Ataques por Países

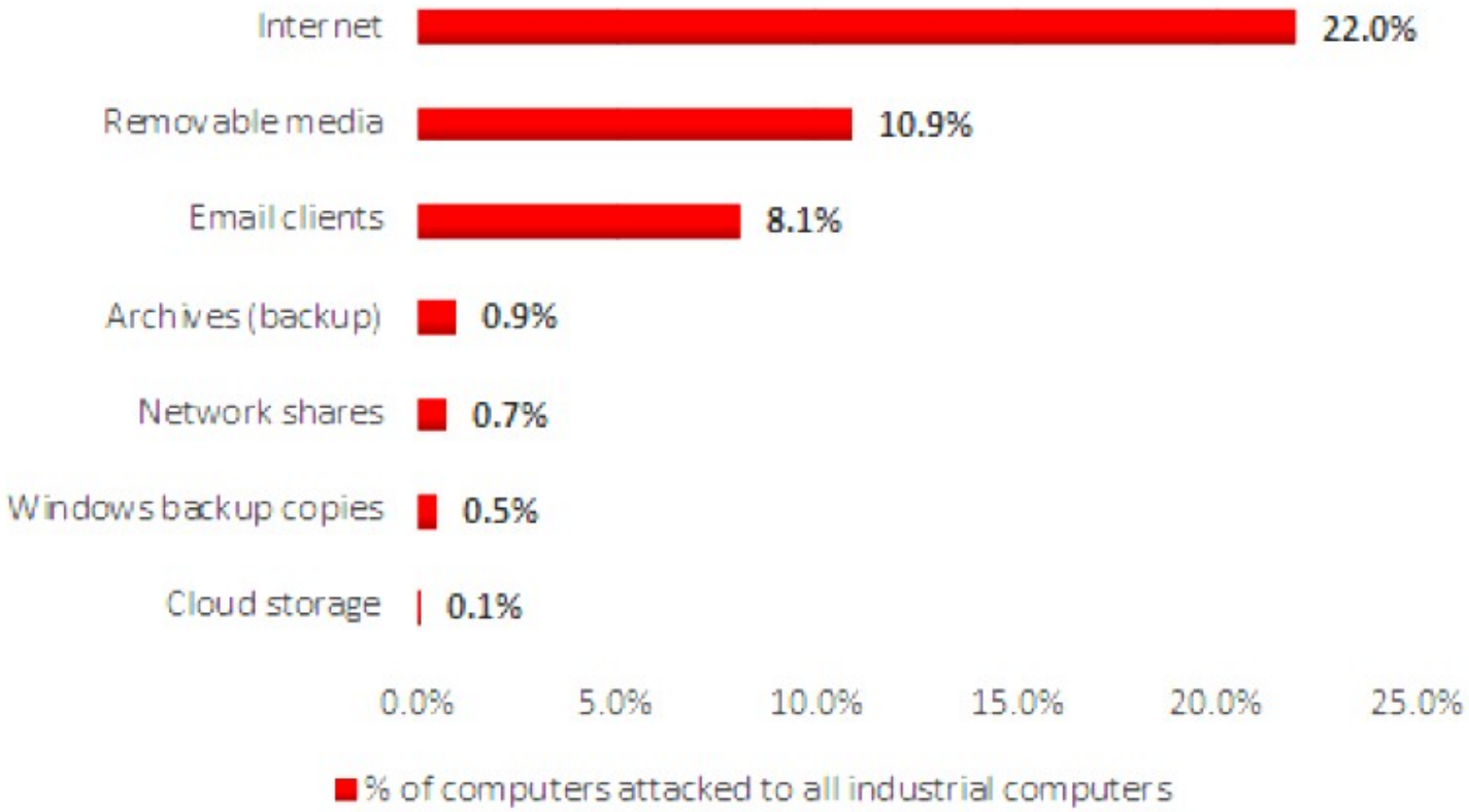


Geographical distribution of attacks against industrial systems (second half of 2016)

Sistemas Scada – Ataques por Países

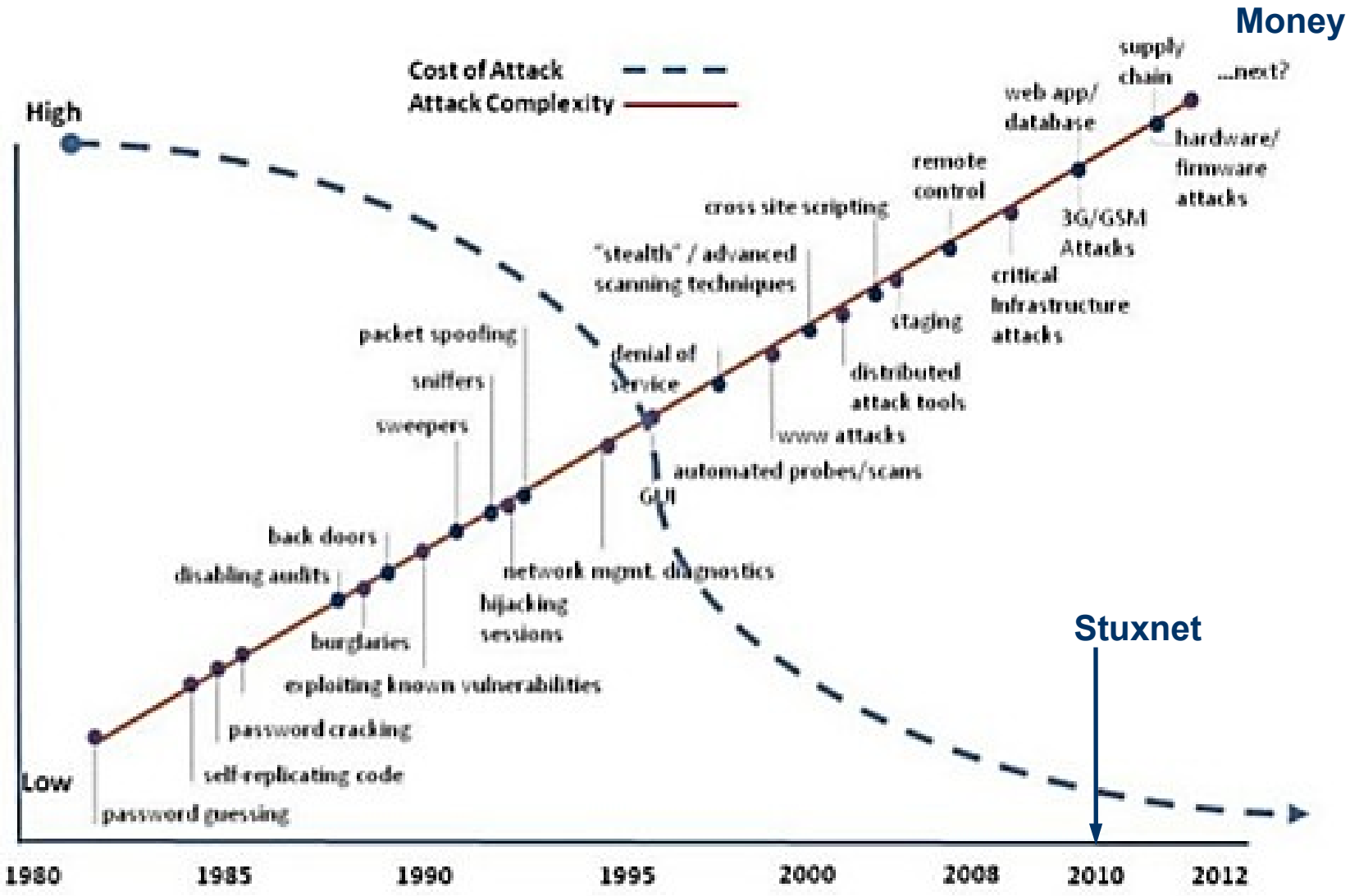
	Country*	% of systems attacked
1	Vietnam	66.09
2	Algeria	65.56
3	Morocco	60.39
4	Tunisia	60.17
5	Indonesia	55.69
6	Bangladesh	54.19
7	Kazakhstan	54.14
8	Iran	53.89
9	China	53.31
10	Peru	53.08
11	Chile	52.75
12	India	52.48
13	Egypt	51.61
14	Mexico	49.58
15	Turkey	46.20

Sistemas Scada – Fontes de Ameaça

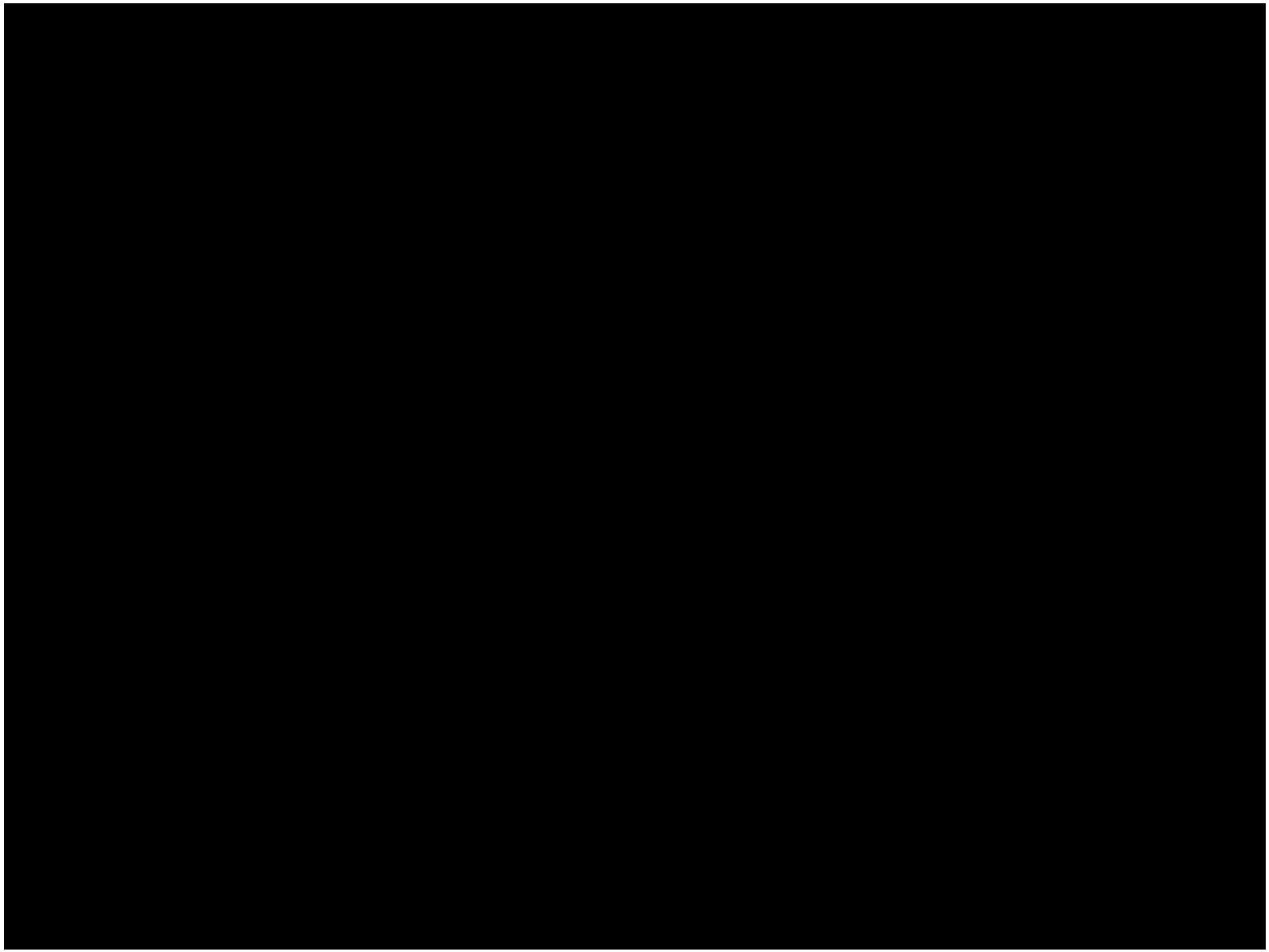


Sources of threats blocked on industrial computers (second half of 2016)

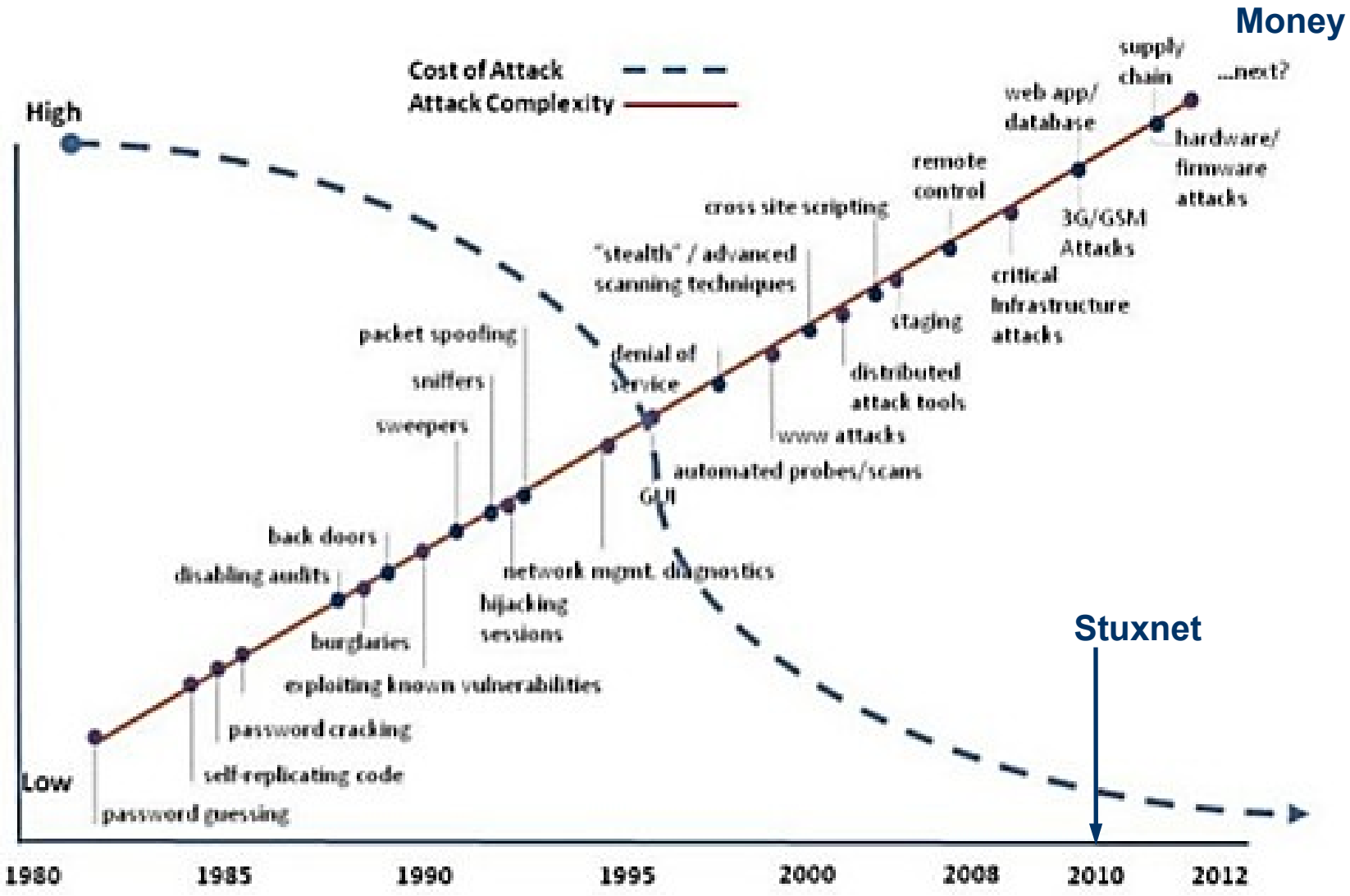
Ataques Cibernéticos: *Custo x Complexidade*



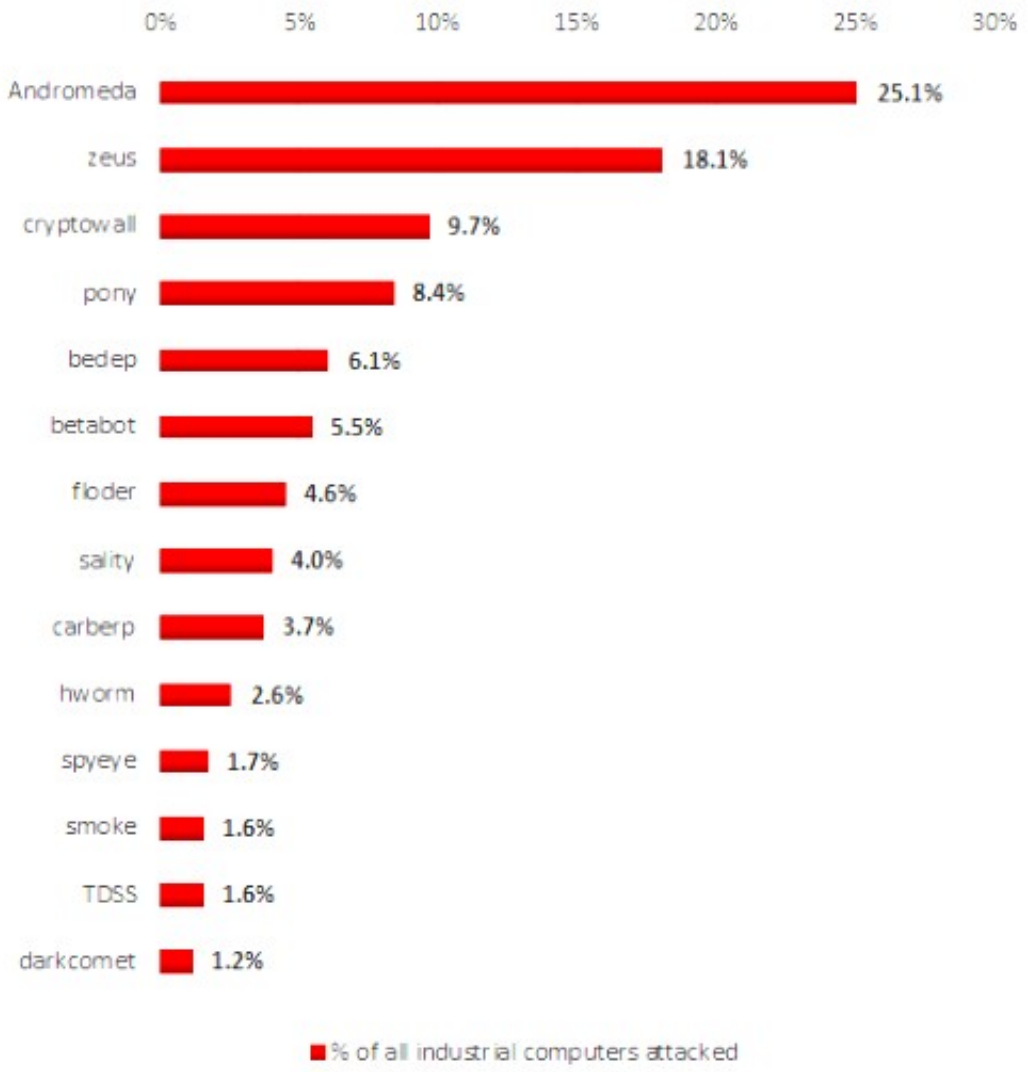
Stuxnet: divisor de águas



Ataques Cibernéticos: *Custo x Complexidade*



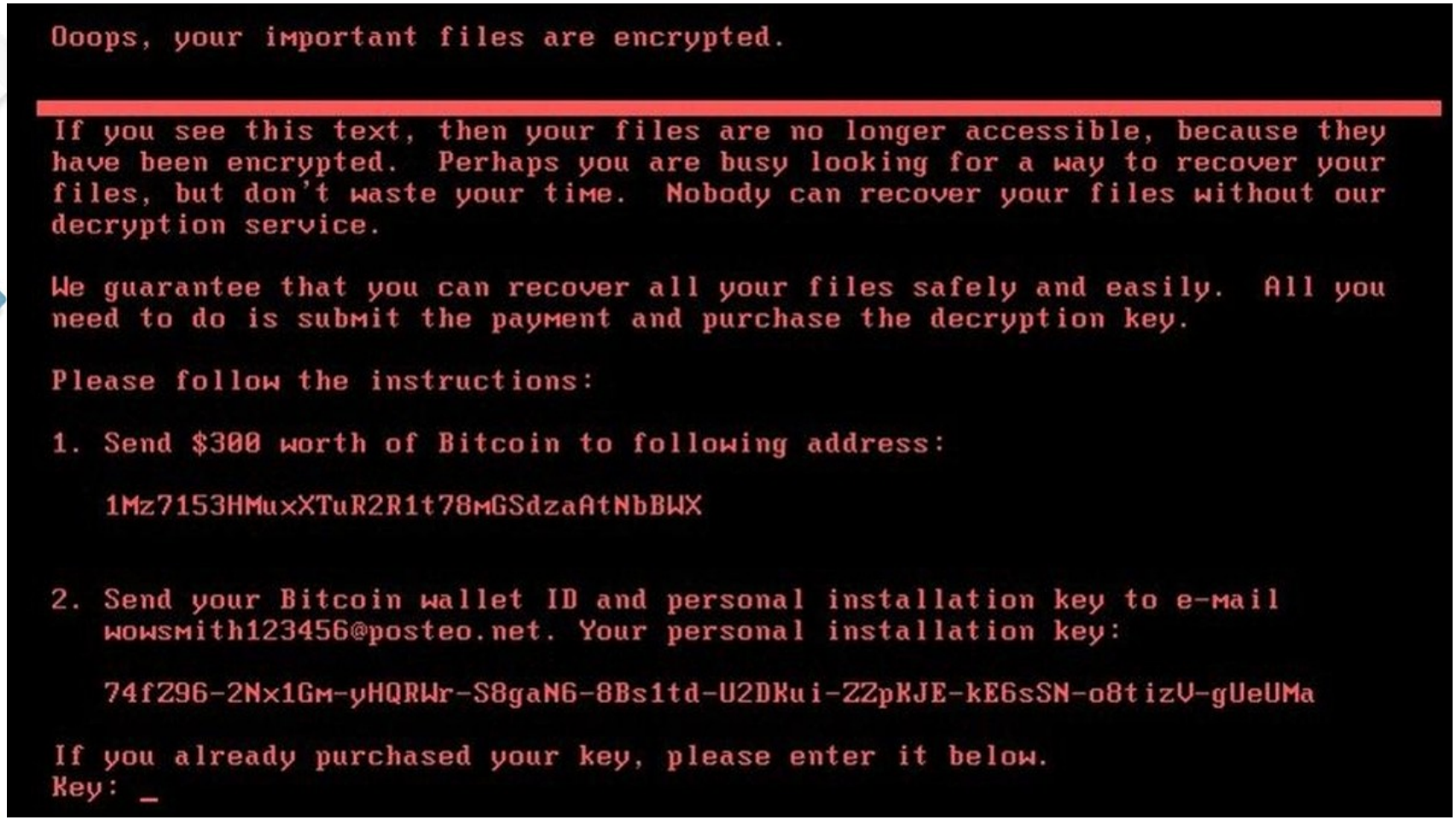
Sistemas Scada – Fontes de Ameaça



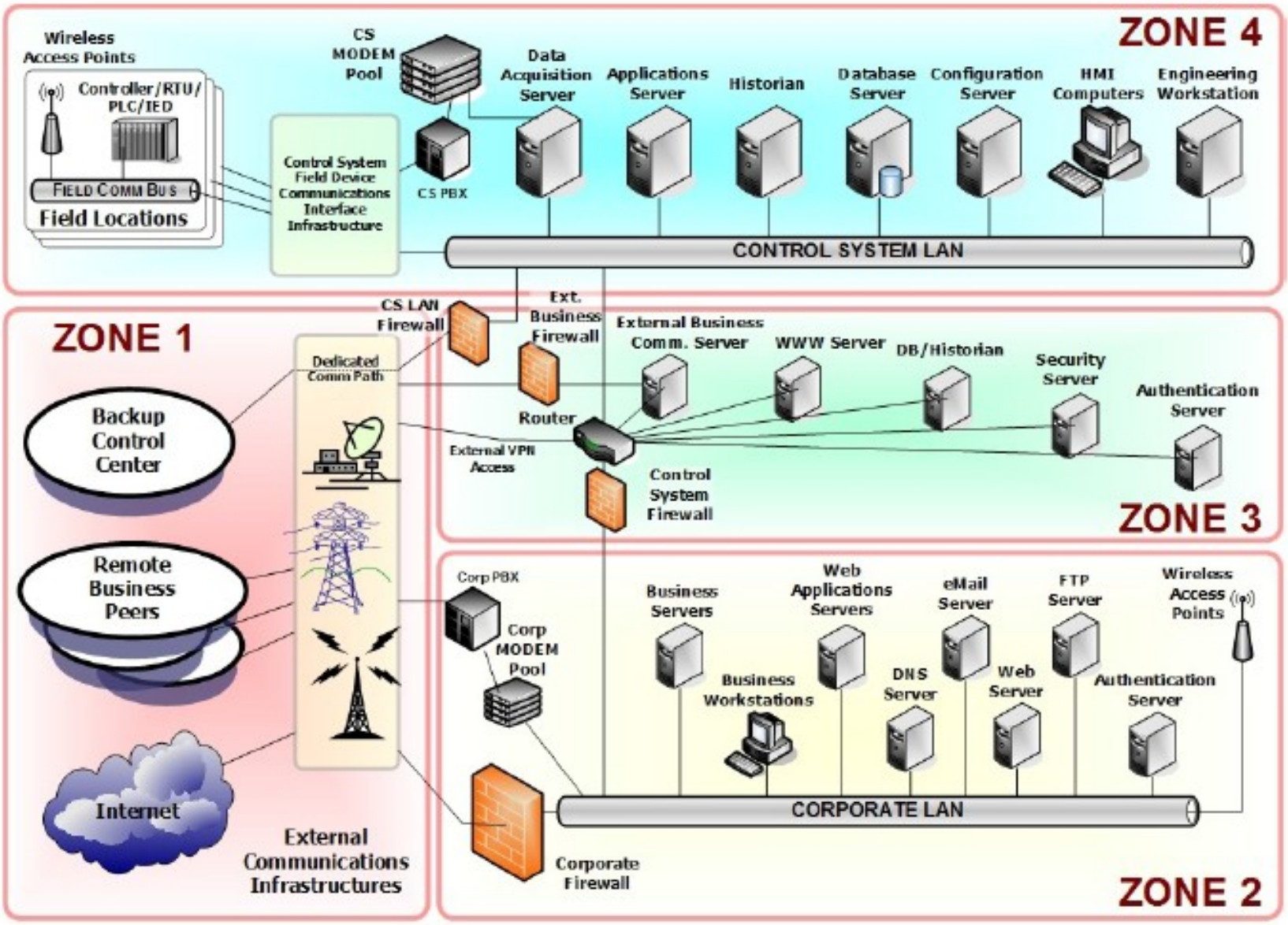
Distribution of industrial computers attacked by botnet agents by bot families

Ataques Cibernéticos: *Ransomware*

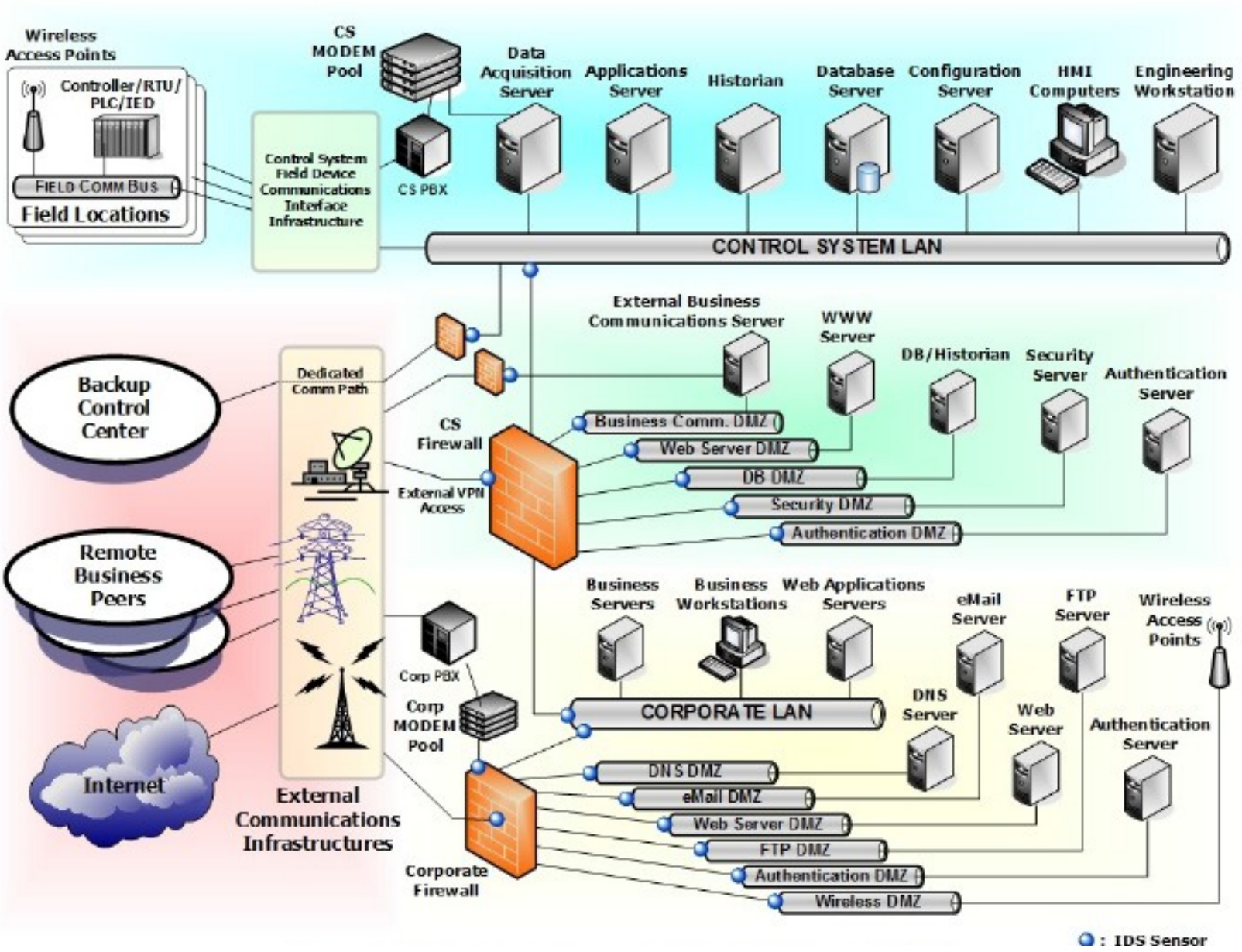
Ataques Cibernéticos: *Ransomware*



Sistemas SCADA – Rede segmentada



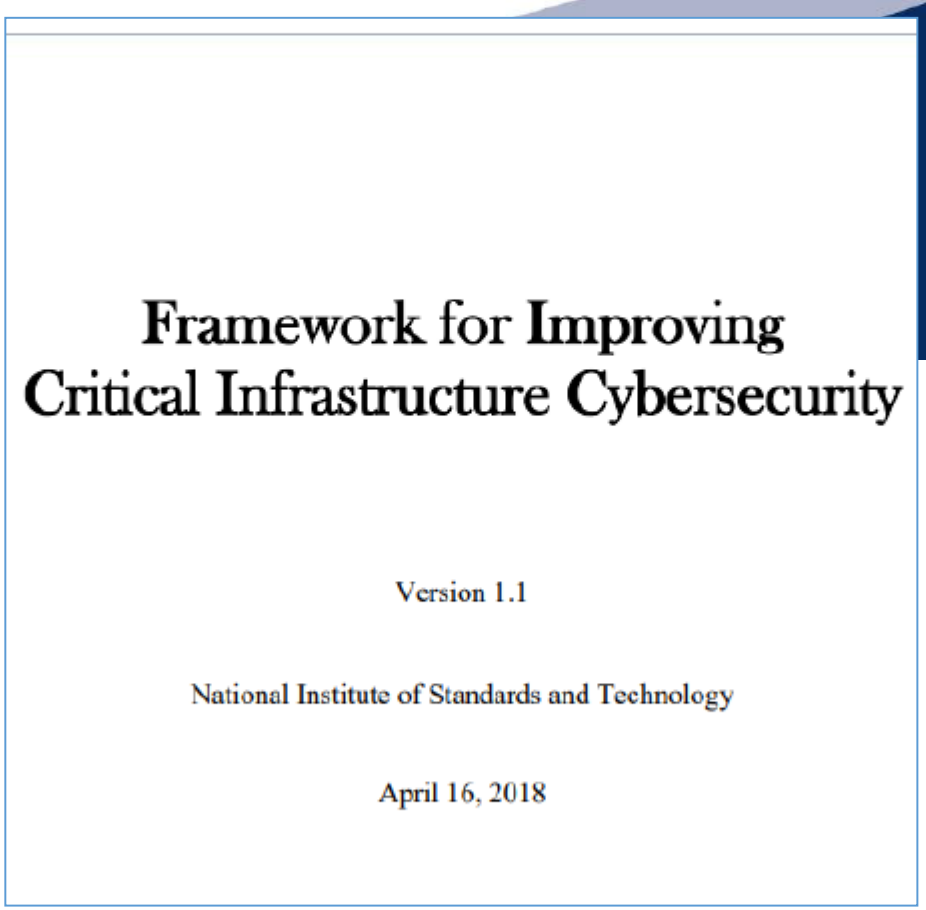
Sistemas SCADA – Rede mais segura



Boas Práticas em Segurança Cibernética de Infraestruturas Críticas

Setting the Standard for Automation™

ISA 99 /IEC 62443



Obrigado!

GABINETE DE
SEGURANÇA INSTITUCIONAL

PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL